Стартовая страница Dell Data Protection | Access

Страница **Dell Data Protection | Access**– это стартовая страница для доступа к функциям данного приложения. Из этого окна можно можно вызывать следующие инструменты.

System Access Wizard (Мастер доступа к системе)
Access Options (Режимы доступа)
Self-Encrypting Drive (Самошифрование диска)
Advanced Options (Расширенные возможности)

В нижнем правом углу окна есть ссылка с названием **advanced (расширенные)**, которую можно щелкнуть для вызова расширенных возможностей.

В нижней части страницы advanced options (расширенные возможности) можно щелкнуть ссылку **home (стартовая страница)** чтобы вернуться назад, на стартовую страницу.

System Access Wizard

Мастер доступа к системе запускается автоматически при первом запуске приложения **Dell Data Protection | Access**. Этот мастер поможет выполнить настройку всех аспектов системы, включая то, как выполняется вход в систему (например, только при помощи пароля или отпечатка пальца и пароля) и где он выполняется (в Windows, пре-Windows или в обоих случаях). Кроме того, если в системе есть диск с шифрованием, его также можно настроить с помощью данного мастера.

Функции администратора

Пользователи, которым были назначены административные права в системе Windows, имеют право выполнять в приложении **Dell Data Access | Protection** следующие функции, которые отсутствуют у обычных пользователей.

- Устанавливать / изменять системный пароль (для пре-Windows)
- Устанавливать / изменять пароль для жесткого диска
- Устанавливать / изменять пароль администратора
- Устанавливать / изменять пароль владельца TPM
- Устанавливать / изменять пароль администратора ControlVault
- Перезагружать систему
- Архивировать и восстанавливать учетные данные
- Устанавливать и изменять PIN-код администратора смарт-карты
- Очищать / сбрасывать смарт-карты
- Включать / отключать защищенный вход Dell для Windows
- Настройка политики входа в систему Windows
- Управлять дисками с самошифрованием, включая функции:
    - включение / выключение защиты дисков самошифрованием;
    - включение / выключение синхронизации паролей Windows (WPS);
    - включение / выключение SSO;
    - выполнение криптографического стирания.

Удаленное управление

Организация может настроить среду, в которой функции обеспечения безопасности, осуществляемые приложением **Dell Data Protection | Access** на нескольких платформах, будут управляться централизованно (т.е. с помощью удаленного управления). В этом случае инфраструктура безопасности Windows, например Active Directory, может использоваться для безопасного управления определенными возможностями приложения **Dell Data Protection | Access**.

Если компьютер управляется удаленно (т.е. "принадлежит" удаленному администратору), то локальное администрирование функциональных возможностей **Dell Data Protection | Access** будет запрещено; а окна управления приложения не будут доступны локально. Следующие функции поддерживают дистанционное управление.

- Модуль TPM (Trusted Platform Module)
- Хранилище ControlVault
- Вход в систему пре-Windows
- Перезагрузка системы
- Пароли доступа к BIOS
- Политика входа в Windows
- Диски с самошифрованием
- Регистрация отпечатков пальцев и смарт-карт

Чтобы получить дополнительную информацию об использовании выпускаемого Wave Systems сервера ERAS (EMBASSY® Remote Administration Server) для дистанционного управления, обратитесь к торговому представителю компании Dell или посетите сайт dell.com.

Режимы доступа

Из окна Access Options (Режимы доступа) можно выбрать способ, которым будет осуществляться доступ к системе.

Если какие-либо режимы были настроены в приложении **Dell Data Protection | Access**, то они будут отображаться на стартовой странице вместе с другими имеющимися режимами доступа (например, change password for Pre-Windows login (Изменить пароль для входа в систему пре-Windows). Имеющиеся режимы представлены в виде ярлыков, при щелчке на которые открываются соответствующие окна для выполнения определенных задач (например, для изменения пароля пре-Windows или регистрации отпечатка пальца).

Общие сведения
Во-первых, можно указать, когда выполняется вход (в Windows, пре-Windows или обе системы) и как (например, с помощью отпечатка пальца или пароля). Можно выбрать один или два режима входа, сочетающих использование отпечатка пальца, смарт-карты и пароля. Предлагаемые режимы зависят от политик входа в систему, применяемых в данной среде, а также от того, какие режимы поддерживаются используемой платформой.

Отпечаток пальца
Если в системе имеется устройство распознавания отпечатков пальцев, можно зарегистрировать новый или обновить существующий отпечаток, используемый для входа в систему. Как только отпечатки пальцев зарегистрированы, можно одним прикосновением пальца к устройству распознавания отпечатков входить в систему Windows, пре-Windows или в обе эти системы, в зависимости от того, какие варианты выбраны в окне General Access Options (Общие параметры доступа). Дополнительную информацию смотри в разделе Enrolling User Fingerprints (Регистрация отпечатков пальцев пользователей).

Вход в систему пре-Windows
Если задано, что пользователи должны входить в систему пре-Windows, необходимо настроить Системный пароль (иногда называемые паролем пре-Windows) для доступа в систему пре-Windows. Как только эта настройка будет выполнена, администратор может изменить пароль в любое время.

Также на этом экране можно отключить вход в систему пре-Windows; для этого необходимо ввести текущий системный пароль, проверить его правильность, а затем нажать кнопку **Disable (Отключить)**.

Смарт-карта
Если указано, что пользователи должны применять смарт-карту для входа в систему, необходимо выполнить регистрацию одной или нескольких традиционных (контактных) или бесконтактных смарт-карт. Щелкните ссылку **Enroll another smartcard (Зарегистрировать другую смарт-карту)**, чтобы запустить мастер регистрации смарт-карт. Регистрация означает настройку смарт-карты для использования при входе в систему.

После регистрации смарт-карты можно изменить или настроить PIN-код этой карты, используя ссылку **Change or setup my smartcard PIN (Изменить или настроить PIN-код смарт-карты)**.

Вход в систему пре-Windows

Когда настраивается вход в систему пре-Windows, необходимо выполнить аутентификацию (с помощью пароля, отпечатка пальца или смарт-карты) при включении системы перед загрузкой Windows. Возможность входа в систему пре-Windows обеспечивает дополнительную защиту системы, предотвращая доступ в Windows и на данный компьютер неавторизованных пользователей (например, если компьютер был украден).

Из окна входа в систему пре-Windows администратор может настроить вход в пре-Windows, а также создать или изменить пароль пре-Windows (системный пароль); если этот пароль уже был установлен, из этого окна можно отключить в ход в систему пре-Windows. При настройке входа в систему пре-Windows автоматически запускается мастер, выполняющий следующие действия.

- Системный пароль: настраивается системный пароль (также называемый паролем пре-Windows) для доступа в пре-Windows. Этот пароль также используется в качестве резервного в случаях, когда для пользователя предусмотрены дополнительные факторы аутентификации (например, для получения доступа к системе, если возникли проблемы с устройством распознавания отпечатков пальцев).
- Отпечаток пальцев или смарт-карта: отпечаток пальцев или смарт-карта настраивается для использования при входе в систему пре-Windows, также указывается, будет ли этот фактор аутентификации использоваться вместо аутентификации паролем пре-Windows или в дополнение к нему.
- Single Sign On: по умолчанию аутентификация пре-Windows (по паролю, отпечатку пальца или смарт-карте) будет также использоваться для автоматического входа в систему Windows (эта технология называется "Single Sign On"). Для отключения этой возможности установите флажок "I want to login again at Windows (Необходим повторный вход в Windows".
- Если в BIOS установлен пароль жесткого диска в дополнение к паролю пре-Windows, появляется возможность изменить или отменить этот пароль жесткого диска.

Примечание. Не все устройства распознавания отпечатков пальцев можно использовать для аутентификации в пре-Windows. Если устройство распознавания не совместимо, зарегистрировать отпечатки пальцев можно будет только для входа в систему Windows. Чтобы выяснить, совместимо ли конкретное устройство, обратитесь к системному администратору или см. список поддерживаемых устройств распознавания отпечатков пальцев на сайте support.dell.com .

Отключение входа в систему пре-Windows
Также в этом окне можно отключить вход в систему пре-Windows; для этого необходимо ввести текущий пароль пре-Windows (системный пароль), проверить его правильность, а затем нажать кнопку **Disable (Отменить)**. Обратите внимание, что при отключении входа в систему пре-Windows любые ранее зарегистрированные отпечатки пальцев или смарт-карты остаются зарегистрированными.

Регистрация отпечатков пальцев

Пользователи могут регистрировать или обновлять отпечатки пальцев, которые позволяют выполнять аутентификацию для входа в систему пре-Windows или Windows. На вкладке Fingerprint (Отпечатки пальцев) рисунок с изображением руки показывает, были ли зарегистрированы отпечатки пальцев и каких именно. Щелкните ссылку **Enroll another (Зарегистрировать другие)**, чтобы запустить мастер регистрации отпечатков пальцев, помогающий выполнить процесс регистрации. "Регистрация" означает сохранение отпечатка пальцев для последующего использования при входе в систему. Для выполнения регистрации отпечатков необходимо, чтобы допустимое устройство распознавания отпечатков пальцев было правильно установлено и настроено.

Примечание. Не все устройства распознавания отпечатков пальцев можно использовать для входа в систему пре-Windows. Если попытаться выполнить регистрацию в пре-Windows с помощью несовместимого распознающего устройства, будет выдано сообщение об ошибке. Чтобы выяснить, совместимо ли конкретное устройство, обратитесь к системному администратору или см. список поддерживаемых устройств распознавания отпечатков пальцев на сайте support.dell.com.

При регистрации отпечатков пальцев предлагается ввести пароль Windows для удостоверения личности пользователя. Если того требует политика безопасности, также выдается приглашение ввести пароль пре-Windows (системный пароль). Пароль пре-Windows может использоваться для доступа к системе, если возникает проблема с устройством распознавания отпечатков пальцев.

Примечания.

- В процессе регистрации рекомендуется снимать не менее двух отпечатков пальцев.
- Перед активацией функций аутентификации по отпечаткам пальцев необходимо убедиться в том, что отпечатки пальцев правильно зарегистрированы.
- При изменении устройства распознавания отпечатков пальцев в системе необходимо повторно выполнить регистрацию отпечатков с помощью нового устройства распознавания. Переключение между двумя разными устройствами распознавания отпечатков пальцев не рекомендуется.
- Если при регистрации отпечатков пальцев часто выдаются сообщения sensor lost focus (расфокусировка датчика), это может означать, что компьютер не определил устройство для чтения отпечатков пальцев. Если используется внешнее устройство для распознавания отпечатков пальцев, отключение и последующее подключение устройства чтения отпечатков пальцев часто решает такую проблему.

Очистка зарегистрированных отпечатков пальцев
Можно удалить зарегистрированные отпечатки пальцев из системы, щелкнув ссылку **Remove fingerprint (Удалить отпечатки пальцев)** или щелкнув (для отмены выбора) зарегистрированный отпечаток пальца в мастере регистрации отпечатков пальцев.

Для удаления конкретного пользователя, зарегистрировавшего свои отпечатки пальцев для аутентификации в пре-Windows, администратор может отменить все отпечатки пальцев этого пользователя.

Примечание. Если в процессе регистрации отпечатков пальцев выдаются сообщения об ошибках, дополнительную информацию см. по адресу wave.com/support/Dell.

Регистрация смарт-карт

Страница **Dell Data Protection | Access** дает возможность использовать традиционные (контактные) или бесконтактные смарт-карты для входа в систему с учетной записью Windows или для аутентификации в пре-Windows. На вкладке Smartcard (Смарт-карта) щелкните ссылку **Enroll another smartcard (Зарегистрировать другую смарт-карту)**, чтобы запустить мастер регистрации смарт-карт, помогающий выполнить процесс регистрации. Регистрация означает настройку смарт-карты для использования при входе в систему.

Для выполнения регистрации необходимо, чтобы допустимое устройство аутентификации смарт-карт было правильно установлено и настроено.

Примечание. Чтобы выяснить, совместимо ли конкретное устройство, обратитесь к системному администратору или см. список поддерживаемых смарт-карт на сайте support.dell.com.

Регистрация
При регистрации смарт-карт предлагается ввести пароль Windows для удостоверения личности пользователя. Если того требует политика безопасности, также выдается приглашение ввести пароль пре-Windows (системный пароль). Пароль пре-Windows может использоваться для доступа к системе, если возникает проблема с устройством чтения смарт-карт.

Во время процедуры регистрации выдается приглашение ввести PIN-код смарт-карты, если таковой установлен. Если политика безопасности требует использования PIN-кода, а он не задан, будет предложено создать PIN-код.

Примечания.

- Как только пользователь зарегистрируется для использования смарт-карты в пре-Windows, его нельзя удалить из системы.
- Обычные пользователи могут изменять свой PIN-код для смарт-карты, а администратор может менять как административный PIN-код, так и пользовательские PIN-коды.
- Администратор может сбросить смарт-карту; после выполнения такого сброса смарт-карту нельзя использовать для аутентификации при входе в Windows или пре-Windows, пока не будет выполнена повторная регистрация.

Примечание. Для аутентификации сертификатов TPM администраторы могут зарегистрировать сертификаты TPM, выполнив процесс регистрации смарт-карт в Microsoft Windows. Администраторам необходимо выбрать Wave TCG-Enabled CSP в качестве поставщика служб криптографии вместо Smart Card CSP для совместимости с этим приложением. Кроме того, должен быть включен защищенный вход Dell с соответствующей политикой типа аутентификации для клиента.

Примечание. Если выдается сообщение об ошибке, информирующее о том, что служба Smartcard Service не запущена, можно запустить или перезапустить эту службу, выполнив следующие действия.

- Из панели управления перейдите в окно "Администрирование", выберите "Службы", затем щелкните правой кнопкой мыши строку службы Smartcard и выберите "Пуск" или "Перезапустить".
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Диск с самошифрованием

Приложение **Dell Data Protection | Access** управляет функциями защиты дисков с самошифрованием, для которых аппаратно встроен механизм шифрования данных. Эта функциональность обеспечивает доступ к зашифрованным данным всем авторизованным пользователям, когда включено блокирование диска.

Окно Self-Encrypting Drive (Диск с самошифрованием) открывается щелчком по вкладке **Self-Encrypting Drive (Диск с самошифрованием)** в нижней части экрана. Эта вкладка отображается только в тех случаях, когда в системе имеется один или несколько дисков с самошифрованием (SED).

Щелкните ссылку **Setup (Настройка)**, чтобы запустить мастер настройки дисков с самошифрованием. В этом мастере будет создан пароль администратора диска, выполнена резервная копия этого пароля, а также применены настройки шифрования диска. Только системные администраторы могут запускать мастер настройки дисков с самошифрованием.

Важная информация. Как только диск будет настроен, включаются механизмы защиты данных и и блокирования диска. Если диск заблокирован, в его работе наблюдаются следующие особенности.

- Диск переходит в *заблокированный* режим при каждом отключении электропитания.
- Загрузка диска не начинается, пока пользователь не введет правильное имя пользователя и пароль в процессе аутентификации на экране входа в систему пре-Windows. До блокирования диска данные на нем доступны любому пользователю компьютера.
- Диск будет защищен даже если его подключить к другому компьютеру в качестве второго диска; для доступа к данным диска необходима аутентификация.

Как только диск настроен, в окне Self-Encrypting Drive (Диск с самошифрованием) отображается ссылка, позволяющая пользователям изменить свой пароль для этого диска. У администратора диска в этом окне также появляется возможность добавлять или удалять пользователей диска. Если был настроен внешний диск, от также отображается в этом окне и может быть разблокирован.

Примечание. Чтобы заблокировать связанный второй (внешний) диск, он должен быть обесточен независимо от компьютера.

Администратор диск может управлять его параметрами в окне **Advanced (Дополнительно)>Devices (Устройство)**. Дополнительную информацию см. в разделе Управление устройствами – диски с самошифрованием.

Настройка диска

Мастер настройки дисков с самошифрованием поможет выполнить процесс настройки дисков. При выполнении этого процесса следует помнить о следующих концептуальных моментах.

Администратор диска

Первый пользователь с правами системного администратора, настраивающий доступ к диску (а также пароль администратора диска), становится администратором этого диска; это единственный пользователь, который может изменять параметры доступа к диску. Чтобы гарантировать настройку первого пользователя в качестве администратора диска, необходимо установить флажок "I understand (Я понимаю)" для продолжения этого шага.

Пароль администратора диска
Матер предлагает создать пароль администратора диска и повторно ввести его для подтверждения. Необходимо ввести пароль Windows для аутентификации, прежде чем можно будет создать пароль администратора диска. Для создания этого пароля у текущего пользователя Windows должны быть права администратора.

Резервное копирование учетных данных диска
Укажите местоположение или нажмите кнопку **Обзор**, чтобы выбрать папку для сохранения резервной копии учетных данных администратора диска.

Важная информация.**!**

- Настоятельно рекомендуется всегда выполнять резервное копирование этих учетных данных, причем эта резервная копия должна храниться не на основном жестком диске системы (например, на съемном носителе). В противном случае, при утрате доступа к жесткому диску невозможно будет использовать и данную резервную копию.
- После такого как настройка диска выполнена, всепользователи должны будут вводить правильные имена пользователей и пароли (или отпечатки пальцев), перед загрузкой Windows, чтобы получить доступ к системе при последующем ее включении.

Добавление пользователя диска
Администратор диска может добавлять к диску других пользователей, являющихся действительными пользователями Windows. При добавлении пользователей к диску у администратора есть возможность запросить у пользователя смену пароля при первом входе в систему. Пользователь должен будет сменить свой пароль на экране аутентификации пре-Windows, чтобы диск разблокировался.

Дополнительные параметры

- *Single Sign On* — по умолчанию пароль диска с самошифрованием, вводимый на экране аутентификация пре-Windows, будет также использоваться для автоматического входа в систему Windows (эта технология называется "Single Sign On"). Для отключения этой возможности установите флажок "I want to login again at Windows (Необходим повторный вход при запуске Windows" при настройке параметров диска.
- *Вход в систему по отпечатку пальца* — на поддерживаемых платформах можно указать, что необходимо выполнять аутентификация для доступа к жесткому диску путем распознавания отпечатка пальца, вместо ввода пароля.
- *Поддержка спящего режима и режима ожидания (S3)* (если поддерживается на платформе) — если эта возможность доступна, диск с самошифрованием будет безопасно переключаться в спящий режим/режим ожидания (также называемый режимом S3) и при выходе из этого режима будет необходима аутентификация пре-Windows.

Примечания.

- Если включена поддержка S3, на пароли для шифрования диска накладываются все существующие ограничения паролей BIOS. Обратитесь к изготовителю аппаратного обеспечения за информацией об особых ограничениях пароля BIOS, которые могут существовать в системе.
- Не все диски с самошифрованием поддерживают режим S3. Во время настройки диска будет выдано уведомление о том, поддерживает этот диск спящий режим и режим ожидания или нет. Для тех дисков, которые не поддерживают данный режим, запросы S3 Windows будут автоматически преобразовываться в запросы на гибернацию, если этот режим разрешен (настоятельно рекомендуется активировать режим гибернации на своем компьютере).

- При первом входе в систему после включения функции Single Sign On (SSO), этот процесс приостановится на приглашении для входа в систему Windows. Необходимо будет ввести свою форму проверки подлинности Windows, которая будет надежно сохранена для следующих попыток входа в Windows. При следующей загрузке системы SSO будет автоматически выполнять вход в систему Windows. Этот же процесс необходим при смене параметров аутентификации пользователя Windows (смена пароля, отпечатков пальцев, PIN-кода смарт-карты). Если ПК находится на домене, а домен имеет политику, требующую нажатия ctrl+alt+del для входа в среду Windows, данная политика будет соблюдаться.

Внимание! При удалении приложения **Dell Data Protection | Access** необходимо вначале отменить защиту данных на диске с самошифрованием и разблокировать этот диск.

Функции для пользователей SED

Администраторы дисков с самошифрованием выполняют все обслуживание, необходимое для защиты дисков и их пользователей. Пользователи дисков, не являющиеся их администраторами, могут выполнять только следующие задачи.

- Изменять собственный пароль для диска
- Разблокировать диск

Эти задачи можно выполнять на вкладке **Self-Encrypting Drive (Диск с самошифрованием)** в приложении **Dell Data Protection | Access**.

Изменение пароля
Позволяет зарегистрированным пользователям создать новый пароль для аутентификации при обращении к диску. Необходимо ввести действующий пароль для диска с самошифрованием, прежде чем будет установлено новое значение пароля для этого диска.

Примечания.

- Это приложение приводит в действие политики длины пароля и его сложности для Windows, если они включены. Если политики паролей Windows не включены, максимальная длина пароля диска с самошифрованием составляет 32 символа. Обратите внимание, что максимальная длина составляет 127 символов, если не включен режим S3 (Спящий режим/режим ожидания).
- Пользовательский пароль диска с самошифрованием не зависит от пользовательского пароля Windows. Изменение или сброс пользовательского пароля Windows не влияет на пользовательский пароль для диска, если не была включена синхронизация паролей Windows. Подробные сведения см. в разделе Устройства: диски с самошифрованием.
- На некоторых неанглоязычных клавиатурах имеется ряд запрещенных символов, которые нельзя использовать в пароле диска с самошифрованием. Если пароль Windows содержит любой из этих запрещенных символов и активирована синхронизация паролей Windows, произойдет сбой в процессе синхронизации, и появится сообщение об ошибке.

Разблокирование диска
Функция разблокирования диска позволяет зарегистрированному пользователю разблокировать заблокированный диск. Если режим блокирования включен, диск переключается в заблокированное состояние при каждом выключении питания ПК. При включении питания компьютера необходимо выполнить аутентификацию для доступа к диску, введя пароль на экране аутентификации пре-Windows.

Примечания.

- Если на компьютере имеются несколько учетных записей пользователей дисков с самошифрованием, работающих одновременно, то при переключении в режим энергосбережения (т.е. режим ожидания/спящий режим или режим гибернации) возможны затруднения.
- На экране аутентификации пре-Windows "пользователь 1", "пользователь 2" и т.д. заменяются на имена пользователей диска в версиях приложения, локализованных для следующих языков: китайский, японский, корейский и русский.

Расширенные возможности

Расширенные возможности в приложении **Dell Data Protection | Access** позволяют пользователю с административными привилегиями управлять следующими аспектами приложения.

Обслуживание
Пароли
Устройства

Примечание. Только пользователи с административными правами могут изменять расширенные возможности; обычные пользователи могут просматривать, не внося изменений.

Обслуживание

Окно Maintenance (Обслуживание) может использоваться администраторами для настройки предпочтений входа в систему Windows, перезагрузки системы для подготовки ее к перенастройке, а также для архивации и восстановления учетных данных пользователей, хранящихся в защищенном системном оборудовании. Подробную информацию см. в следующих разделах.

Предпочтения доступа

Окно Access Preferences (Предпочтения доступа) позволяет администраторам указать предпочтения для входа в систему Windows для всех пользователей системы.

Включить защищенный вход в систему
Возможность заменить стандартный экран Windows, вызываемый при нажатии клавиш CTRL-ALT-DEL позволяет использовать другие факторы аутентификации вместо пароля для доступа к Windows (или в дополнение к нему). Можно добавить в качестве второго фактора отпечаток пальцев, чтобы повысить защищенность процесса входа в систему Windows. Также для входа в Windows можно добавить дополнительные факторы аутентификации, например, применение смарт-карты или сертификата TPM.

Примечания.

- Параметр Enabling Dell Secure login (Разрешить защищенный вход Dell) действует на всех пользователей системы.
- Рекомендуется, чтобы этот режим включался ПОСЛЕ того, как все пользователи зарегистрируют свои отпечатки пальцев или смарт-карты.
- При первом входе в систему после установки этого режима пользователю будет предложено выполнить аутентификацию в Windows в соответствии со стандартной политикой, а затем при следующем запуске нужно будет использовать новые факторы аутентификации.

Disable Dell Secure login (Отключить защищенный вход Dell)
В этом режиме при входе в систему Windows отключаются все функции, заданные в приложении **Dell Data Protection | Access**. При выборе этого режима активируется стандартная политика входа в систему Windows.

Примечания.

- Если при попытке входа возникает ошибка, связанная с защищенным входом в систему Windows, попробуйте отключить и повторно включить режим защищенного входа Dell.
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Перезагрузка системы

Функция перезагрузки системы используется для сброса данных обо всех пользователях со всех аппаратных средств защиты в системе; эта функция используется, например, при перенастройке компьютера. Эта функция стирает все пароли в системе, за исключением паролей пользователей Windows, а также все данные на аппаратных устройствах (т.е. в хранилище ControlVault, модуле TPM, устройствах распознавания отпечатков пальцев). Для дисков с самошифрованием эта функция также отключает защиту данных, так что информация с этих дисков становится общедоступной.

Необходимо подтвердить, что действительно требуется перезагрузка системы, а затем нажать кнопку **Далее**. Для перезагрузки системы потребуется ввести пароли для каждого из следующих средств аппаратной защиты, если они были настроены.

- Пароль владельца TPM
- Пароль хранилища ControlVault
- Пароль администратора BIOS
- Системный пароль BIOS (пре-Windows)
- Пароль жесткого диска (BIOS)
- Пароль администратора диска с самошифрованием

Примечание. Для дисков с самошифрованием необходим только пароль администратора диска; пароли всех пользователей диска не требуются.

Важная информация. Единственным способом восстановить данные, сброшенные при перезагрузке системы, будет восстановление из ранее выполненной архивной копии. Если такой архив отсутствует, восстановить данные невозможно. Для дисков с самошифрованием удаляются только данные настройки; персональные данные для такого диска не удаляются.

Архивирование и восстановление учетных данных

Функциональная возможность архивирования и восстановления учетных данных используется для создания резервной копии и восстановления учетных данных всех пользователей (информации о входе в систему и шифровании), хранимой в ControlVault и модуле TPM. Резервная копия этих данных очень важна при повторной инициализации компьютеров или для восстановления данных в случае отказа оборудования. В такой ситуации можно просто восстановить все учетные данные на новом компьютере из спасенного архивного файла.

Можно выбрать, выполнять ли архивирование или восстановление для одного пользователя или для всех пользователей системы.

Учетные данные пользователя содержат данные, используемые в пре-Windows, например зарегистрированные отпечатки пальцев или смарт-карту, а также ключи, хранимые в TPM. Модуль TPM будет создавать ключи, как запрашивается защищенным приложением; например, при создании цифрового сертификата будут создаваться ключи в TPM.

ПРИМЕЧАНИЕ. Возможность архивирования ключей TPM в приложении **Dell Data Protection | Access** см. в документации по используемому защищенному приложению. Обычно поддерживаются приложения, в которых для генерации ключей используется технология “Wave TCG-Enabled CSP”.

Архивирование учетных данных
Для архивирования учетных данных необходимо выполнить следующие действия.

- Указать, архивируются ли учетные данные для самого пользователя или для всех пользователей системы.
- Обеспечить аутентификацию для аппаратной защиты, введя системный пароль (для пре-Windows), пароль администратора ControlVault и пароль владельца TPM.
- Создать пароль для резервной копии учетных данных.
- Указать местоположение архива, используя кнопку **Обзор**. Необходимо убедиться, что на случай сбоя жесткого диска в качестве местоположения архива выбран съемный носитель, например, флэш-дисковод или сетевой диск.

Важное примечание.

- Запишите путь доступа к архиву, поскольку пользователю понадобиться эта информация при восстановлении учетных данных.
- Запишите пароль для резервной копии учетных данных, чтобы данные можно было восстановить. Это очень важно, потому что каких-либо процедур восстановления этого пароля не предусмотрено.
- Если пароль владельца TPM неизвестен, обратитесь к системному администратору или к инструкции по настройке TPM в компьютере.

Восстановление учетных данных
Для восстановления учетных данных необходимо выполнить следующие действия.

- Указать, восстанавливаются ли учетные данные для самого пользователя или для всех пользователей системы.
- Открыть папку, содержащую архив, и выбрать файл архива.
- Ввести пароль для резервной копии учетных данных, который был задан при создании архива.
- Обеспечить аутентификацию для аппаратной защиты, введя системный пароль (для пре-Windows), пароль администратора ControlVault и пароль владельца TPM.

Примечания.

- Если выдается сообщение об ошибке, в котором сказано, что произошел сбой при восстановлении учетных данных, и уже предпринято несколько попыток восстановления с тем же результатом, попытайтесь выполнить восстановление из другого архива. Если и эта попытка завершится неудачно, создайте новый архив с учетными данными и попытайтесь выполнить восстановление из этого нового архива,
- Если выдается сообщение об ошибке, в котором сказано, что ключи TPM не могут быть восстановлены, создайте архив учетных данных, а затем очистите TPM в BIOS. Чтобы очистить TPM, перезагрузите компьютер, затем нажмите клавишу **F2** после запуска, чтобы открылось окно с настройками BIOS, затем перейдите в раздел Security>TPM Security. Затем повторно установите владельца TPM и попытайтесь восстановить учетные данные еще раз.
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Управление паролями

Из окна Password Management (Управление паролями) администратор может создавать или изменять следующие пароли, обеспечивающие защиту системы.

- Системный пароль (также известен как пароль пре-Windows)*
- Пароль администратора*
- Пароль жесткого диска*
- Пароль хранилища ControlVault
- Пароль владельца TPM
- Главный пароль TPM
- Пароль для хранилища паролей TPM
- Пароль диска с самошифрованием

Примечания.

- Отображаются только те пароли, которые применимы к конфигурации используемой платформы; поэтому вид данного окна может меняться в зависимости от конфигурации системы и ее состояния
- Пароли, рядом с которыми указан звездочка (*) являются паролями BIOS и их также можно изменить в системе BIOS.
- Пароли уровня BIOS нельзя создавать или изменять, если администратор BIOS запретил изменения паролей.
- Щелчок ссылки **setup (настройка)** для диска с самошифрованием запускает мастер настройки дисков с самошифрованием; щелчок ссылки **manage (управление)** позволяет изменить один или несколько паролей для дисков с самошифрованием.
- Щелчок ссылки **manage (управление)** для хранилища паролей TPM открывает окно, в котором можно просматривать или изменять пароли, защищающие ключи TPM. При создании ключа TPM, требующего пароля, выбирается произвольный пароль, который затем записывается в хранилище. Нельзя управлять хранилищем паролей TPM, если не создан главный пароль TPM.

Правила сложности пароля Windows

Приложение **Dell Data Protection | Access** обеспечивает соответствие следующего пароля правилам сложности пароля Windows для данного компьютера.

- Пароль владельца TPM

Чтобы определить политику сложности пароля Windows для этого компьютера, выполните следующие действия.

1. Перейдите на "Панель управления".
2. Щелкните дважды "Средства администрирования".
3. Дважды щелкните "Локальная политика безопасности"
4. Раскройте вкладку "Политики учетной записи" и выберите "Политика паролей".

Устройства

Окно Devices (Устройства) используется администраторами для управления всеми аппаратными средствами защиты, установленными в системе. Для каждого устройства можно просмотреть его состояние и дополнительные подробные сведения, например версию микропрограммного обеспечения. Щелкните ссылку **show (показать)**, чтобы просмотреть информацию по каждому из устройств или ссылку **hide (скрыть)**, чтобы свернуть этот раздел. В зависимости от аппаратной комплектации используемой платформы для управления доступны следующие устройства.

Модуль TPM (Trusted Platform Module)
Хранилище ControlVault®
Диск с самошифрованием
Информация об устройстве аутентификации

Модуль TPM (Trusted Platform Module)

Необходимо активировать чип безопасностиTPM и назначить владельца TPM, чтобы можно было использовать расширенные возможности защиты, доступные при работе приложения **Dell Data Protection | Access** с TPM.

Окно TPM в приложении **Device Management (Управление устройствами)** отображается только в том случае, если в системе обнаружен модуль TPM.

Управление TPM

Эти функции позволяют администратору системы управлять модулем TPM.

Состояние

Отображается состояние модуля TPM: *активен* или *неактивен*. Состояние "активен" означает, что модуль TPM активирован в BIOS и готов к настройке (т.е., можно назначить его владельца). Нельзя управлять модулем TPM и использовать его функции защиты, если этот модуль TPM не активен (выключен).

Если модуль TPM обнаружен в системе, но не активен (выключен), можно включить его, щелкнув ссылку **activate (активировать)** в данном окне, не входя в BIOS. После включения TPM с помощью данной функции, компьютер необходимо перезагрузить. В ходе перезагрузки в некоторых случаях выдается приглашение, предлагающее подтвердить изменения.

Примечание. Возможность включать (активировать) модуль TPM из этого приложения поддерживается не для всех платформ. Если она не поддерживается, необходимо будет включить ее в системном BIOS. Для этого перезагрузите систему, нажмите клавишу **F2** до загрузки Windows и откройте экрана настройки BIOS, затем перейдите в раздел Security>TPM Security и активируйте TPM.

Из приложения также можно *деактивировать* модуль TPM, щелкнув ссылку **deactivate (деактивировать)**; деактивация TPM сделает его недоступным для реализации расширенных функций защиты. Но деактивация не изменяет каких-либо параметров TPM, а также не удаляет и не изменяет никаких данных или ключей, хранящихся в этом модуле TPM.

Владелец назначен

Отображает состояние владельца (т.е. "владелец назначен") и позволяет установить или изменить владельца TPM. Необходимо назначить владелец TPM, чтобы стали доступны возможности защиты этого модуля. Прежде чем установить владельца, модуль TPM должен быть включен (активирован).

Процесс установки владельца включает создание пароля владельца TMP пользователем (с правами администратора). После того как пароль задан и установлены права владения, TPM готов к работе.

Примечание. Пароль владельца TPM должен соответствовать Правилам сложности пароля Windows, предусмотренным для системы.

Важная информация. Очень важно не потерять и не забыть пароль владельца TPM, поскольку он необходим для доступа к расширенным функциям защиты TPM в **Dell Data Protection | Access**.

Заблокирован
Отображается состояние модуля TPM: *заблокирован* или *разблокирован*. "Блокирование" — это функция защиты модуля TPM; он входит в заблокированное состояние после определенного числа неверных попыток ввода пароля пользователя TPM. Владелец TPM может разблокировать модуль TPM из этого окна; необходим ввод пароля владельца TPM.

Примечания.

- Если выдается сообщение об ошибке, в котором говорится, что не удалось назначить владельца TPM, сбросьте настройки TPM в системном BIOS и повторите попытку назначения владельца. Чтобы очистить TPM, перезагрузите компьютер, затем нажмите клавишу **F2** после запуска, чтобы открылось окно с настройками BIOS, затем перейдите в раздел Security>TPM Security.
- Если выдается сообщение об ошибке, в котором говорится, что не удается изменить пароль владельца TPM, выполните архивирование данных TPM (архивирование учетных данных), сбросьте настройки TPM в BIOS, повторно установите владельца TPM и восстановите данные TPM (восстановление учетных данных).
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Хранилище Dell ControlVault®

Dell ControlVault® (CV) — это защищенное аппаратное хранилище для учетных данных, используемых для входа в систему пре-Windows (например, данные о паролях пользователей или зарегистрированных отпечатках пальцев). Окно ControlVault в приложении **Device Management (Управление устройствами)** отображается только в том случае, если в системе обнаружено хранилище ControlVault.

Управление ControlVault

Эти функции позволяют администратору системы управлять системным хранилищем ControlVault.

Состояние
Отображается состояние ControlVault: *активное* или *неактивное*. "Неактивное" состояние подразумевает, что хранилище ControlVault не доступно для сохранения данных в системе. См. в документации по системе Dell, как определить присутствие в системе хранилища ControlVault.

Пароль
Указывает, был ли установлен пароль для администратора ControlVault, и позволяет настраивать пароль или изменять его (если пароль уже был установлен). Только администратор системы может устанавливать или изменять пароль. Пароль администратора ControlVault необходим для осуществления следующих операций.

- Выполнение архивирования и восстановления учетных данных.
- Сброс пользовательских данных (для всех пользователей).

Примечание. Если попытка архивирования или восстановления выполняется в момент, когда пароль для администратора ControlVault не установлен, администратору предлагается создать такой пароль.

Зарегистрированные пользователи
Показывает, имеются ли у каких-либо пользователей зарегистрированные учетные данные для входа в систему (например, пароли, отпечатки пальцев или смарт-карты), которые бы в данный момент находились в хранилище ControlVault.

Очистка пользовательских данных
В какой-то момент может потребоваться очистка данных в хранилище ControlVault; например, если у пользователя возникнут проблемы при использовании или регистрации учетных данных пре-Windows для аутентификации. В этом окне могут быть сброшены все данные, хранящиеся в ControlVault, как для одного пользователя, так и для всех пользователей.

Необходимо ввести пароль администратора ControlVault, чтобы очистить все пользовательские данные на платформе. Затем будет предложено ввести системный пароль (для пре-Windows), если зарегистрированы какие-либо учетные данные пре-Windows. После того, как все пользовательские данные будут очищены, пароль администратора ControlVault и системный пароль сбрасываются; обратите внимание, что это единственный способ сбросить пароль администратора ControlVault.

Примечание. Как только будут очищены все пользовательские данные, выдается приглашение перезагрузить компьютер. Для правильной работы системы необходимо выполнить перезагрузку.

Если требуется очистить учетные данные одного пользователя, пароль администратора ControlVault устанавливать не обязательно. При нажатии **clear user data (очистка пользовательских данных)** предлагается выбрать пользователя, учетные данные которого в ControlVault требуется сбросить. Как только выбран пользователь, предлагается выбрать системный пароль (только если зарегистрированы учетные данные пре-Windows).

Примечания.

- Если выдается сообщение об ошибке, в котором сообщается, что невозможно создать пароль администратора ControlVault, необходимо заархивировать имеющиеся учетные данные, очистить все данные пользователей в хранилище ControlVault, перезагрузить компьютер и попытаться создать пароль снова.
- Если выдается сообщение об ошибке, в котором сообщается, что учетные данные для отдельного пользователя не могут быть очищены в ControlVault, необходимо заархивировать имеющиеся учетные данные, попытаться очистить данные всех пользователей, а затем очистить данные для этого отдельного пользователя.
- Если выдается сообщение об ошибке, в котором сообщается, что учетные данные для всех пользователей не могут быть очищены в ControlVault, необходимо рассмотреть возможность выполнения перезагрузки системы. **Важная информация.** Ознакомьтесь с разделом системы справки Reset System (Перезагрузка системы), прежде чем выполнять перезагрузку, поскольку в результате ее будут сброшены ВСЕ данные защиты пользователей.
- Если выдается сообщение об ошибке, в котором сообщается, что не удается создать резервную копию данных ControlVault и TPM, отключите функцию TPM в настройках BIOS своей системы. Для этого перезагрузите компьютер и нажмите клавишу **F2** при запуске, чтобы открыть экран настроек BIOS, затем перейдите в раздел Security>TPM Security. Затем вновь активируйте TPM и попытайтесь заархивировать данные ControlVault.
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Диск с самошифрованием: расширенные возможности

Приложение **Dell Data Protection | Access** управляет функциями защиты дисков с самошифрованием, для которых аппаратно встроен механизм шифрования данных. Эта возможность управления обеспечивает доступ к зашифрованным данным всем авторизованным пользователям, когда включено блокирование диска.

Эта вкладка отображается в окне **Device Management (Управление устройствами)** только в тех случаях, когда в системе имеется один или несколько дисков с самошифрованием (SED).

Важная информация. Как только диск будет настроен, включаются механизмы защиты данных самошифрованием и и блокирования диска.

Управление дисками
Эти функции позволяют администратору диска управлять настройками безопасности диска. Изменения настроек безопасности вступают в силу после выключения привода.

Защита данных
Отображается состояние *включена* или *выключена* для защиты данных диска с самошифрованием. Состояние "включена" означает, что защита диска была настроена; но, пока *блокирование* диска не будет включено, пользователям не надо аутентифицироваться при обращении к диску на уровне пре-Windows.

Отсюда можно отключить защиту данных диска с самошифрованием. Если защита отключена, все расширенные функции защиты диска с самошифрованием также отключаются и диск работает как обычный жесткий диск. При отключении защиты данных также удаляются все настройки безопасности, включая учетные данные администраторов и пользователей диска. Но эта функция не изменяет и не удаляет с диска какие-либо пользовательские данные.

Блокирование
Отображается состояние *включено* или *выключено* для дисков с самошифрованием. Информацию о поведении блокированных дисков см. в разделе Диск с самошифрованием.

Возможно потребуется временно отключить блокирование диска, что можно сделать из данного окна. Не рекомендуется делать это, поскольку при отключении блокирования не требуется учетных данных для доступа к диску и любой пользователь системы сможет обратиться к данным на диске. При отключении блокирования диска неудаляются какие-либо настройки безопасности, включая учетные данные администратора и пользователей диска, а также сохраняются все пользовательские данные на диске.

Внимание! При удалении приложения **Dell Data Protection | Access** необходимо вначале отменить защиту данных на диске с самошифрованием и разблокировать этот диск.

Администратор диска

Показывает действующего администратора диска. Отсюда администратор диска может выбрать нового администратора из числа пользователей диска. Новый администратор должен быть действительным пользователем Windows в данной системе и обладать правами администратора. В систем может быть только один администратор дисков.

Пользователи диска

Отображаются зарегистрированные пользователи диска, а также число пользователей, зарегистрированных в данный момент. Максимальное число поддерживаемых пользователей зависит от используемого диска с самошифрованием (в настоящее время поддерживается 4 пользователя для дисков Seagate и 24 пользователя для дисков Samsung).

Синхронизация пароля Windows

Функция синхронизации пароля Windows (WPS) автоматически устанавливает пользователям пароли для дисков с самошифрованием такими же, как их пароль Windows. Эта функция не предусмотрена для использования администратором дисков, она применяется только для пользователей дисков. Функция WPS может использоваться в корпоративной среде, где пароли должны меняться через определенный промежуток времени (например, каждые 90 дней); если эта функция включена, все пароли для дисков с самошифрованием у пользователей будут обновляться автоматически при изменении соответствующих паролей Windows.

Примечание. Если включена синхронизация паролей Windows (WPS), пользователю нельзя изменить пароль для диска с самошифрованием; необходимо изменить пароль Windows такого пользователя, чтобы автоматически поменялся его пароль для дисков.

Запомнить последнее имя пользователя

Если включена эта функция, последнее введенное имя пользователя будет отображаться по умолчанию в поле **Username (Имя пользователя)** на экране аутентификации пре-Windows.

Выбор имени пользователя

Если включена эта функция, пользователям видны имена всех пользователей диска в поле **Username (Имя пользователя)** на экране аутентификации пре-Windows.

Криптографическое стирание

Эта функция позволяет "стереть" все данные на диске с самошифрованием. При этом фактического удаления данных не происходит, но удаляются ключи, применяемые для шифрования данных, после чего данные становятся непригодными для использования. Не существует способов восстановить данные после криптографического стирания; при этом также отключается защита данных на дисках с самошифрованием и диски могут быть перенастроены.

Примечания.

- Если выдается сообщение об ошибке, связанной с функциями управления дисками с самошифрованием, полностью выключите компьютер (именно выключите, а не перезагрузите), а затем вновь запустите систему.
- Если требуется более подробная информация по конкретным сообщениям об ошибках, см. ее на странице wave.com/support/Dell.

Информация об устройстве аутентификации

В окне Authentication Device Information (Информация об устройстве аутентификации) в приложении **Device Management (Управление устройствами)** отображаются сведения обо всех подключенных устройствах аутентификации (таких как, устройство распознавания отпечатков пальцев, традиционные и бесконтактные устройства чтения смарт-карт) и их состоянии.

Техническая поддержка

Техническую поддержку для программного обеспечения **Dell Data Protection | Access** можно получить по адресу http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

В состав приложения **Dell Data Protection | Access** входит продукт Wave TCG-Enabled CSP, доступ к которому при необходимости предоставляется либо напрямую из приложения, либо путем выбора из списка установленных поставщиков служб криптографии (CSP). Когда это возможно, выбирайте “Wave TCG-Enabled CSP”, чтобы обеспечить создание модулем TPM ключей и передачу управление этими ключами и их паролями приложению **Dell Data Protection | Access**.

Wave Systems TCG-Enabled CSP позволяет приложениям использовать функции, доступные для платформ, соответствующих требованиям TCG, напрямую через интерфейс MSCAPI. Это модуль MSCAPI CSP с поддержкой TPM, обеспечивающий функциональность асимметричных ключей и дополнительный уровень безопасности TPM независимо от специализированных требований поставщика Trusted Software Stack (TSS).

Примечание. Если для ключейTPM, созданных Wave TCG-enabled CSP, требуется пароль и пользователь создал главный пароль TPM, индивидуальные пароли для ключей будут создаваться произвольно и сохраняться в хранилище паролейTPM.