HP Client Security

Начало работы

Издание 1-е: август 2013 г.

Номер документа: 735339-251

Содержание

1 Приступаем к работе с приложением HP Client Security Manager

HP Client Security позволяет защищать данные, устройства и идентификационные данные, таким образом повышая безопасность вашего компьютера.

Доступные на компьютере программные модули могут различаться в зависимости от модели.

Программные модули HP Client Security могут быть предустановлены, предварительно загружены или доступны для загрузки на веб-сайте HP. Дополнительные сведения см. на веб-сайте http://www.hp.com.

ПРИМЕЧАНИЕ. В инструкциях данного руководства предполагается, что у вас уже установлены подходящие программные модули HP Client Security.

Функции HP Client Security

В следующей таблице приведены основные функции модулей HP Client Security.

Модуль	Ключевые функции
Программа HP Client Security Manager	Администраторы могут выполнять следующие функции: • Защита вашего компьютера перед загрузкой Windows® • Защита вашей учетной записи Windows с помощью строгой проверки подлинности • Управление учетными записями и паролями для интернет-сайтов и приложений • Простая смена вашего пароля операционной системы Windows. • Использование отпечатков пальцев для дополнительной защиты и удобства • Настройка смарт-карты, бесконтактной карты или проксимити карты для проверки подлинности • Использование вашего телефона с функцией Bluetooth в качестве средства идентификации • Задание ПИН-кода для расширения возможностей проверки подлинности • Настройка политики входа и сеанса • Архивация и восстановление программных данных • Добавление дополнительных приложений, таких как HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager и HP Computrace. Пользователи могут выполнять следующие функции: • Просматривать параметры статуса шифрования и Device Access Manager. • Активировать Computrace. • Настраивать пользовательские параметры, а также параметры резервного копирования и восстановления данных.
Password Manager	Обычные пользователи могут выполнять следующие функции: • Упорядочивание и настройка имен пользователей и паролей. • Создавать более надежные пароли, повышающие безопасность учетных записей электронной почты и веб-записей. Диспетчер паролей автоматически вводит и отправляет данные. • Упрощение процесса входа благодаря функции единого входа, которая автоматически запоминает и применяет учетные данных пользователя. • Отмечать учетную запись как скомпрометированную, чтобы получать предупреждения о других учетных записях со сходными учетными данными. • Импортировать учетные данные с поддерживаемого браузера.

Модуль	Ключевые функции
HP Drive Encryption (только на некоторых моделях)	• Обеспечивает полное шифрование жесткого диска. • Включает проверку подлинности перед загрузкой для расшифровки данных и доступа к ним. • Предоставляет возможность активации дисков с самошифрованием (только на некоторых моделях).
Программа HP Device Access Manager	• Позволяет менеджерам по информационным технологиям контролировать доступ к устройствам на основании профилей пользователей. • Запрещает неавторизованным пользователям удаление данных с использованием внешних хранилищ данных и предотвращает попадание вирусов в систему с внешних носителей. • Позволяет администраторам запрещать доступ к устройствам связи для конкретных лиц или групп пользователей.
HP Trust Circles	• Обеспечивает безопасность файлов и документов. • Шифрует файлы, размещенные в указанных пользователем папках, и обеспечивает их защиту в пределах круга доверия. • Позволяет использовать файлы и совместно работать с ними только членам круга доверия.
Обнаружение похищенных устройств (Computrace, приобретается отдельно)	• Для активации необходимо отдельно приобрести подписки для отслеживания и трассировки. • Обеспечивает безопасное отслеживание ресурсов. • Отслеживает деятельность пользователей, а также изменения, связанные с оборудованием или программным обеспечением. • Остается активным даже после форматирования или замены жесткого диска.

Описание продукта HP Client Security и примеры практического использования

Большинство продуктов HP Client Security имеют проверку подлинности пользователя (как правило, пароль) и административное резервное копирование, позволяющее получить доступ, если пароли утеряны, недоступны или забыты, а также для доступа службы корпоративной безопасности.

ПРИМЕЧАНИЕ. Некоторые из продуктов HP Client Security разработаны для ограничения доступа к данным. Шифрование данных требуется в тех случаях, когда предпочтительнее их потерять, чем поставить под угрозу их безопасность. Рекомендуется создать резервную копию всех данных в безопасном месте.

Password Manager

Программа Password Manager сохраняет имена пользователей и пароли. Она может использоваться для выполнения следующих задач.

- Сохранение имен пользователя и паролей для доступа к Интернету или электронной почте.
- Автоматический вход в систему веб-сайта или электронной почты.
- Управление проверками подлинности и их организация.
- Выбор ресурса сети или Интернета и непосредственный переход по ссылке.
- Просмотр имен и паролей при необходимости.
- Отмечать учетную запись как скомпрометированную, чтобы получать предупреждения о других учетных записях со сходными учетными данными.
- Импортировать учетные данные с поддерживаемого браузера.

Пример 1. Снабженец крупного производителя проводит большую часть рабочих транзакций через Интернет. Кроме того, она часто посещает несколько популярных веб-сайтов, для которых требуются учетные данные. Она заботится о безопасности, поэтому не использует один и тот же пароль для разных учетных записей. Она решила использовать Диспетчер паролей, чтобы совместить веб-ссылки с различными именами пользователя и паролями. Когда она переходит на веб-сайт и выполняет вход в систему, диспетчер паролей подставляет учетные данные автоматически. Если ей потребуется просмотреть имена пользователя и пароли, диспетчер паролей может показать их.

Password Manager также может использоваться для управления проверками подлинности и их организации. Это средство дает пользователю возможность выбрать ресурс сети или Интернета и непосредственно перейти по ссылке. Пользователь также может при необходимости просматривать имена пользователя и пароли.

Пример 2: Трудолюбивый работник был повышен и теперь будет управлять целым отделом бухгалтерского учета. Сотрудникам этого отдела приходится входить в системы множества клиентских веб-сайтов, для каждого из которых используются разные учетные данные. Этими данными пользуются совместно различные работники, так что стоит вопрос конфиденциальности. Сотрудник решает упорядочить все веб-ссылки, имена и пароли пользователей компании при помощи Диспетчера паролей. После завершения сотрудник разворачивает Диспетчер паролей другим сотрудникам, чтобы они могли работать с веб-записями, не зная учетных данных, которые для них используются.

HP Drive Encryption (только на некоторых моделях)

HP Drive Encryption используется для ограничения доступа к данным на всем жестком или дополнительном диске компьютера. Drive Encryption может управлять самошифрующимися дисками.

Пример 1. Врач хочет быть уверенным, что только он сам имеет доступ к данным, хранящимся на жестком диске его компьютера. Он активирует службу Drive Encryption, которая выполняет проверку подлинности перед загрузкой Windows. Когда эта служба установлена, получить доступ к жесткому диску можно только после ввода пароля перед запуском операционной системы. Доктор может защитить диск еще надежней, выбрав шифрование данных с помощью параметра самошифрования.

Пример 2. Администратору больницы требуется сделать так, чтобы доступ к данным больничного компьютера имели только врачи и авторизованные сотрудники, сохраняя в секрете личные пароли. Отдел информационных технологий добавляет администратора,

врачей и всех авторизованных сотрудников в качестве пользователей Drive Encryption. Теперь загрузить компьютер или домен могут только те сотрудники, которым это разрешено, используя свои личные имена и пароли.

HP Device Access Manager (только на некоторых моделях)

HP Device Access Manager позволяет администраторам ограничивать доступ к оборудованию и управлять им. Device Access Manager позволяет блокировать несанкционированный доступ к флэш-накопителям USB, откуда данные могут быть скопированы. Кроме того, можно ограничить доступ к дисководам CD/DVD, управлению устройствами USB, сетевым соединениям и т.д. Например, когда внешние поставщики должны иметь доступ к компьютерам компании, но не должны иметь возможности копировать данные на накопитель USB.

Пример 1: Менеджер медицинской компании-поставщика часто работает с личными медицинскими записями и данными своей компании. Сотрудникам нужен доступ к этим данным, однако крайне важно, чтобы данные не переносились с компьютера при помощи накопителя USB или любого другого внешнего носителя. Сеть защищена, но на компьютерах есть устройства записи компакт-дисков и USB-порты, используя которые можно скопировать или украсть данные. С помощью Device Access Manager менеджер отключает USB-порты и устройства записи компакт-дисков так, чтобы их нельзя было использовать. Несмотря на блокировку USB-портов, мышь и клавиатура продолжают работать.

Пример 2. В страховой компании требуется сделать так, чтобы сотрудники не могли загружать или устанавливать личные программы или данные, принесенные из дома. Некоторым сотрудникам нужен доступ к портам USB на всех компьютерах. Менеджер по информационным технологиям использует Device Access Manager, чтобы разрешить доступ для некоторых сотрудников и блокировать внешний доступ для всех остальных.

Computrace (приобретается отдельно)

Computrace (приобретается отдельно) – это служба, которая может отследить местоположение украденного компьютера, когда пользователь подключится к Интернету. Кроме того, Computrace позволяет находить и удаленно управлять компьютерами, а также следить за использованием компьютера и приложений.

Пример 1. Директор школы поручил отделу информационных технологий следить за всеми школьными компьютерами. После проведения инвентаризации компьютеров, ИТ-администратор зарегистрировал все компьютеры в системе Computrace, чтобы найти их в случае кражи. Некоторое время назад обнаружилось, что несколько компьютеров пропали из школы. Администратор поставил в известность органы власти и сотрудников Computrace. Компьютеры были найдены и возвращены в школу.

Пример 2. Агентству недвижимости требуется управлять компьютерами по всему свету и устанавливать на них обновления. Оно использует Computrace для отслеживания этих компьютеров и установки обновлений, в результате чего не приходится отправлять сотрудника ИТ-отдела для работы с каждым компьютером.

Достижение ключевых целей безопасности

Модули HP Client Security могут работать вместе, формируя решения различных вопросов в области безопасности, в том числе:

- Защита от целенаправленной кражи
- Ограничение доступа к секретным данным

- Предотвращение несанкционированного доступа из внутренних и внешних местоположений
- Создание политик стойких паролей

Защита от целенаправленной кражи

Примером целенаправленной кражи может быть кража компьютера, содержащего конфиденциальные данные и информацию о клиентах в пункте досмотра аэропорта. Для предотвращения целенаправленной кражи используются следующие функции:

- Включение функции проверки подлинности перед загрузкой ограничивает доступ к операционной системе.
  - Программа HP Client Security — См. Программа HP Client Security на стр. 14.
  - HP Drive Encryption — см. HP Drive Encryption (только на некоторых моделях) на стр. 33.
- Шифрование помогает предотвратить доступ к данным даже при извлечении жесткого диска и его установке в незащищенной системе.
- С помощью Computrace можно найти украденные компьютеры.
  - Computrace — см. Обнаружение похищенных устройств (только на некоторых моделях) на стр. 59.

Ограничение доступа к секретным данным

Предположим, аудитор, выполняющий проверку компании, получил доступ к компьютеру с конфиденциальной финансовой информацией. Необходимо предотвратить возможность печати конфиденциальных файлов или их сохранения на внешнем носителе, например на компакт-диске. Следующая функция позволяет ограничить доступ к данным.

- HP Device Access Manager позволяет ИТ-менеджерам ограничить доступ к коммуникационным устройствам, чтобы конфиденциальную информацию было невозможно скопировать с жесткого диска. См. раздел Системное представление на стр. 48.

Предотвращение несанкционированного доступа из внутренних и внешних местоположений

Несанкционированный доступ к незащищенную компьютеру, предназначенному для коммерческих задач, представляет собой весьма реальную опасность для корпоративных сетевых ресурсов, таких как информация от финансовых служб, руководителя или проектно-конструкторской группы, и для персональной информации, такой как медицинские карточки

пациентов или персональная финансовая отчетность . Для предотвращения несанкционированного доступа используются следующие функции:

- Включение функции проверки подлинности перед загрузкой ограничивает доступ к операционной системе. (см. раздел HP Drive Encryption (только на некоторых моделях) на стр. 33.
- HP Client Security позволяет предотвратить получение неавторизованными пользователями паролей или доступа к приложениям, защищенным паролями. См. раздел Программа HP Client Security на стр. 14.
- HP Device Access Manager позволяет ИТ-менеджерам ограничить доступ к устройствам записи, чтобы конфиденциальную информацию было невозможно скопировать с жесткого диска. См. раздел HP Device Access Manager (только на некоторых моделях) на стр. 47.

Создание политик стойких паролей

Если вступает в силу политика компании, которая требует использования политики надежных паролей для десятков веб-приложений и баз данных, Диспетчер паролей обеспечивает защищенное хранилище для паролей и функцию единого входа в систему. См. раздел Password Manager на стр. 21.

Элементы дополнительной защиты

Назначение ролей безопасности

При управлении безопасностью компьютера (в особенности для больших организаций) рекомендуется разделить права и обязанности для различных типов администраторов и пользователей.

ПРИМЕЧАНИЕ. В небольшой организации или для индивидуального использования эти роли могут принадлежать одному лицу.

Для HP Client Security права и обязанности в области безопасности могут быть разделены на следующие роли:

- Сотрудник службы безопасности — определяет уровень безопасности для компании или сети и определяет функции безопасности для развертывания, такие как Drive Encryption.

  ПРИМЕЧАНИЕ. Множество функций HP Client Security может быть настроено сотрудником службы безопасности вместе с HP. Дополнительные сведения см. на веб-сайте http://www.hp.com.

- ИТ-администратор — применяет и управляет функциями безопасности, определенными сотрудником службы безопасности. Может также включить и отключать некоторые функции. Например, если сотрудник службы безопасности решил развернуть смарт-карты, ИТ-администратор может включить режимы пароля и смарт-карты.
- Пользователь — использует функции безопасности. Например, если сотрудник службы безопасности и ИТ-администратор включили смарт-карты для системы, пользователь может установить PIN-код смарт-карты для проверки подлинности.

ПРЕДУПРЕЖДЕНИЕ. Администраторам рекомендуется следовать рекомендациям по ограничению прав конечных пользователей и доступа пользователей.

Неавторизованным пользователям не должны предоставляться права администратора.

Управление паролями HP Client Security

Большинство функций HP Client Security защищены паролями. В следующей таблицы перечислены часто используемые пароли, программные модули, в которых устанавливается пароль и функция пароля.

Пароли, устанавливаемые и используемые только ИТ-администраторами, также указаны в этой таблице. Все остальные пароли могут устанавливаться обычными пользователями и администраторами.

Пароль HP Client Security	Установлен в следующем модуле	Функция
Пароль для входа в Windows	Панель управления Windows или HP Client Security	Может использоваться для входа вручную и проверки подлинности при доступе к функциям HP Client Security.
Пароль резервного копирования и восстановления HP Client Security	HP Client Security, отдельным пользователем	Защищает доступ к файлу резервного копирования и восстановления HP Client Security.
ПИН смарт-карты	Диспетчер учетных данных	Может использоваться как многофакторная проверка подлинности. Может использоваться как проверка подлинности Windows. Проверка подлинности пользователей Drive Encryption, если выбрана смарт-карта.

Создание безопасного пароля

При создании паролей необходимо следовать спецификациям, установленным программой. Однако обычно рекомендуется соблюдать следующие правила для создания надежных паролей и уменьшения шансов компрометации паролей:

- Используйте пароли, состоящие более чем из 6 символов, предпочтительно более 8.
- Используйте буквы различных регистров в пароле.
- По возможности используйте как буквы, так и цифры, и включайте специальные символы и знаки препинания.
- В ключевом слове заменяйте буквы специальными символами или цифрами. Например, можно использовать цифру 1 для букв I и L.
- Сочетайте слова из 2 или более языков.
- Разделите слово или фразу числами или специальными символами посередине, например, «Mary2-2Cat45».
- Не используйте пароль, существующий в словаре.
- Не используйте в качестве пароля свое имя или любую другую личную информацию, например дату рождения, клички домашних животных, девичью фамилию матери и т.д., даже если вы записываете слово в обратном порядке.
- Регулярно меняйте пароли. Можно изменить всего несколько символов.
- Если записать пароль, не храните его в общедоступном месте рядом с компьютером.

- Не сохраняйте пароль в файле, таком как сообщение электронной почты, на компьютере.
- Не предоставляйте другим свои учетные данные и не говорите никому свой пароль.

Создание резервной копии учетных данных и параметров

Вы можете использовать инструмент «Резервное копирование и восстановление» из HP Client Security в качестве централизованного средства, с помощью которого можно выполнять резервное копирование и восстановление учетных данных для безопасного доступа из некоторых установленных модулей HP Client Security.

2 Приступая к работе

Чтобы настроить HP Client Security для работы с вашими учетными данными, запустите приложение HP Client Security одним из следующих способов. После завершения работы мастера пользователем он не может быть повторно запущен этим пользователем.

1. Щелчком мыши или касанием выберите приложение **HP Client Security** на начальном экране или экране приложений (Windows 8).

   – или –

   Щелчком мыши или касанием выберите элемент **HP Client Security Gadget** на рабочем столе Windows (Windows 7).

   – или –

   На рабочем столе Windows двойным щелчком мыши или двойным касанием выберите значок **HP Client Security** в области уведомлений, расположенной в крайней правой части панели задач.

   – или –

   На рабочем столе Windows щелчком мыши или касанием выберите значок **HP Client Security** в области уведомлений, затем выберите **Open HP Client Security** (Открыть HP Client Security).

2. Мастер настройки HP Client Security запущен, отображается страница приветствия.

3. Прочитайте информацию на экране приветствия, введите пароль Windows, чтобы подтвердить свои идентификационные данные, затем щелчком мыши или касанием выберите **Далее**.

   При отсутствии пароля Windows вам будет предложено создать его. Пароль Windows необходим для защиты вашей учетной записи Windows от несанкционированного доступа пользователей, а также для использования функций HP Client Security.

4. На странице HP SpareKey выберите три контрольных вопроса. Введите ответ на каждый вопрос и щелкните **Далее**. Пользователь может использовать собственные вопросы. Дополнительную информацию см. в разделе HP SpareKey – восстановление пароля на стр. 16.

5. На странице «Отпечатки пальцев» зарегистрируйте как минимум требуемое количество отпечатков пальцев, затем щелчком мыли или касанием выберите **Далее**. Дополнительную информацию см. в разделе Отпечатки пальцев на стр. 15.

6. На странице Drive Encryption активируйте функцию шифрования, создайте резервную копию ключа шифрования, затем щелчком мыши или касанием выберите **Далее**. Подробнее см.справку по программному обеспечению HP Drive Encryption.

ПРИМЕЧАНИЕ. Эти действия применимы к сценарию, когда пользователь является администратором, а мастер настройки HP Client Security не был ранее настроен администратором.

7. На последней странице мастера щелчком мыши или касанием выберите **Готово**.

   На данной странице отображается состояние функций и учетных данных.

8. Мастер настройки HP Client Security обеспечивает активацию службы «Своевременная проверка подлинности» и File Sanitizer. Подробнее см. справку программного обеспечения HP Device Access Manager и HP File Sanitizer.

ПРИМЕЧАНИЕ. Эти действия применимы к сценарию, когда пользователь является администратором, а мастер настройки HP Client Security не был ранее настроен администратором.

Открытие программы HP Client Security

HP Client Security можно открыть одним из следующих способов:

ПРИМЕЧАНИЕ. Работа мастера настройки HP Client Security должна быть завершена перед запуском HP Client Security.

- Щелчком мыши или касанием выберите приложение **HP Client Security** на начальном экране или экране приложений.

  – или –

  Щелчком мыши или касанием выберите элемент **HP Client Security** на рабочем столе Windows (Windows 7).

  – или –

  На рабочем столе Windows двойным щелчком мыши или двойным касанием выберите значок **HP Client Security** в области уведомлений, расположенной в крайней правой части панели задач.

  – или –

  На рабочем столе Windows щелчком мыши или касанием выберите значок **HP Client Security** в области уведомлений, затем выберите **Open HP Client Security** (Открыть HP Client Security).

3 Руководство по быстрой настройке для малых компаний

В этой главе описано задействование наиболее распространенных и полезных параметров HP Client Security для малого бизнеса. Многочисленные инструменты и параметры этого программного обеспечения позволяют выполнить тонкую настройку в соответствии с индивидуальным предпочтениями и установить управление доступом. Руководство по быстрой установке направлено на уменьшение усилий и времени установки для каждого модуля. Для получения дополнительной информации выберите нужный модуль и нажмите кнопку **?** или «Справка» в верхнем правом углу. Автоматически отобразится справочная информация, которая относится к открытому окну.

Приступая к работе

1. На рабочем столе Windows откройте HP Client Security, дважды щелкнув значок **HP Client Security** в области уведомлений в крайнем правом углу панели задач.
2. Введите пароль Windows или создайте его.
3. Завершите настройку HP Client Security.

Чтобы приложение HP Client Security проводило только одну проверку подлинности при входе в Windows, см. Функции безопасности на стр. 30.

Password Manager

Каждый из нас имеет множество паролей – особенно при регулярном посещении веб-сайтов или использовании приложений, требующих входа. Обычный пользователь использует один пароль для всех приложений и веб-сайтов или подходит к этому вопросу творчески и быстро забывает о том, какой пароль для какого приложения нужен.

Диспетчер паролей может автоматически запоминать ваши пароли или давать вам возможность выбирать, какие сайты запоминать, а какие пропускать. После входа в операционную систему вашего компьютера диспетчер паролей будет подставлять ваши пароли или учетные данные для зарегистрированных в нём приложений или веб-сайтов.

При доступе к любому приложению или веб-сайту, требующему ввод учетных данных, Password Manager автоматически распознает сайт и запросит, требуется ли программному обеспечению запоминать ваши данные. Если необходимо исключить некоторые сайты, можно отклонить запрос.

Чтобы начать сохранять расположения в Интернете, имена пользователей и пароли, выполните следующие действия.

1. Для примера, перейдите на зарегистрированный веб-сайт или приложение и затем щелкните значок диспетчера паролей в левом верхнем углу веб-страницы для добавления учетных данных для данной страницы.
2. Назначьте ссылке название (дополнительно) и введите имя пользователя и пароль в Password Manager.

3. По завершении нажмите кнопку **ОК**.
4. Password Manager также может сохранять имя пользователя и пароль для общих сетевых ресурсов и подключенных сетевых дисков.

Просмотр и управление сохраненными проверками подлинности в Password Manager

Password Manager позволяет просматривать, управлять, выполнять резервное копирование и запускать проверку подлинности из центрального местоположения. Password Manager также поддерживает запуск сохраненных файлов из системы Windows.

Чтобы открыть Диспетчер паролей, используйте сочетание клавиш Ctrl+клавиша Windows+h, а затем щелкните **Вход** для запуска и проверки подлинности сохраненного ярлыка.

Параметр **Изменить** в диспетчере паролей позволяет просмотреть и изменить имя или имя для входа, а также показать пароли.

С помощью HP Client Security для малого бизнеса можно выполнить резервное копирование всех учетных данных и параметров и/или скопировать их на другой компьютер.

HP Device Access Manager

Device Access Manager позволяет ограничивать использование различных внутренних и внешних устройств хранения данных. Таким образом, ваши данные будут в безопасности на жестком диске и не покинут пределы вашей организации. Например, пользователю можно разрешить доступ к вашим данным, но запретить их копирование на компакт-диск, личный музыкальный плеер или запоминающее устройство USB.

1. Откройте **Device Access Manager** (см. Запуск Device Access Manager на стр. 48).

   Отображается доступ для текущего пользователя.
2. Чтобы изменить доступ для пользователей, групп или устройств, щелчком мыши или касанием выберите **Изменить**. Дополнительную информацию см. в разделе Системное представление на стр. 48.

HP Drive Encryption

HP Drive Encryption используется для защиты данных путем шифрования всего жесткого диска. Данные на жестком диске останутся защищенными, даже если будет украден компьютер и/или с оригинального компьютера будет снят жесткий диск и помещен в другой компьютер.

Дополнительным преимуществом в отношении безопасности является то, что Drive Encryption запрашивает должную проверку подлинности с использованием вашего имени пользователя и пароля до загрузки операционной системы. Этот процесс называется проверкой подлинности перед загрузкой.

Для упрощения использования различные программные модули синхронизируют пароли автоматически, включая учетные записи пользователей Windows, домены, HP Drive Encryption, Диспетчер паролей и HP Client Security.

Для получения сведений по настройке HP Drive Encryption во время начальной настройки с помощью мастера настройки HP Client Security см. Приступая к работе на стр. 10.

4 Программа HP Client Security

Начальная страница HP Client Security – это центральный узел для простого доступа к функциям, приложениям и параметрам HP Client Security. Начальная страница содержит три раздела:

- **ДАННЫЕ** – доступ к приложениям, используемым для управления защитой данных.
- **УСТРОЙСТВО** – доступ к приложениям, используемым для управления защитой устройств.
- **ИДЕНТИФИКАЦИОННЫЕ ДАННЫЕ** – регистрация учетных данных для проверки подлинности и управление ими.

Поместите курсор над иконкой приложения для отображения описания приложения.

HP Client Security может предоставить ссылки на параметры пользователя и параметры администрирования в нижней части страницы. Для получения доступа к дополнительным параметрам и функциям HP Client Security щелчком мыши или касанием выберите значок **Gear** (параметры).

Функции, приложения и параметры работы с идентификационными данными

Функции, приложения и параметры работы с идентификационными данными, предоставляемые HP Client Security, помогают управлять различными параметрами ваших цифровых идентификационных данных. Щелчком мыши или касанием выберите одну из следующих иконок на начальной странице HP Client Security, затем введите свой пароль Windows:

- **Отпечатки пальцев** – регистрация учетных данных отпечатков пальцев и управление ими.
- **SpareKey** – настройка и управление вашими учетными данными HP SpareKey, которые можно использовать для входа в компьютер, если другие учетные данные были утеряны или перемещены. Приложение также позволяет восстановить забытый пароль.
- **Пароль Windows** – простой доступ для смены пароля Windows.
- **Устройства Bluetooth** – регистрация ваших устройств Bluetooth и управление ими.
- **Карты** – регистрация смарт-карт, бесконтактных карт и карт бесконтактного ввода и управление ими.
- **ПИН-код** – регистрация учетных данных ПИН-кода и управление ими.
- **RSA SecurID** – позволяет зарегистрировать вашими учетными данными RSA SecurID и управлять ими (если выполнена соответствующая установка).
- **Password Manager** – управление паролями для учетных записей интернет-служб и онлайн приложений.

Отпечатки пальцев

Мастер настройки HP Client Security поможет вам настроить или «зарегистрировать» отпечатки пальцев.

Можно также зарегистрировать или удалить ваши отпечатки пальцев на странице «Отпечатки пальцев», доступ к которой можно легко получить, щелчком мыши или касанием выбрав значок **Отпечатки пальцев** на начальной странице HP Client Security.

1. На странице «Отпечатки пальцев» проводите пальцем для считывания отпечатков до тех пор, пока регистрация не будет успешно завершена.

   Необходимое количество пальцев, которые надо зарегистрировать, указано на странице. Предпочтительно зарегистрировать отпечатки указательного или среднего пальцев.

2. Для удаления ранее зарегистрированных отпечатков пальцев щелчком мыши или касанием выберите **Удалить**.

3. Для регистрации дополнительных пальцев щелчком мыши или касанием выберите **Enroll an additional fingerprint** (Зарегистрировать дополнительный отпечаток пальца).

4. Перед тем как покинуть страницу, щелчком мыши или касанием выберите **Сохранить**.

⚠ **ПРЕДУПРЕЖДЕНИЕ.** В процессе регистрации отпечатков пальцев с помощью мастера информация о них не сохранится, пока вы не щелкните **Далее**. После определенного периода бездействия или при закрытии программы внесенные изменения **не** сохраняются.

- Для доступа к параметрам администрирования отпечатков пальцев, где администраторы могут задать настройки регистрации, точность и другие параметры, щелчком мыши или касанием выберите **Administrative Settings** (Параметры администрирования) (требуются права администратора).
- Для доступа к настройкам отпечатков пальцев пользователя, где вы можете задать параметры, регулирующие внешний вид и поведение приложения распознавания отпечатков пальцев, щелчком мыши или касанием выберите **Настройки пользователя**.

Параметры администрирования отпечатков пальцев

Администраторы могут назначать настройки регистрации, точность и другие параметры для считывателя отпечатков пальцев. Требуются права администратора.

- Для доступа к параметрам администрирования для учетных данных отпечатков пальцев щелчком мыши или касанием выберите **Administrative Settings** (Параметры администрирования) на странице «Отпечатки пальцев».

- **Регистрация пользователя** – выберите минимальное и максимальное количество отпечатков пальцев, которое пользователь сможет зарегистрировать.
- **Recognition** (Распознавание) – чтобы настроить чувствительность устройства считывания отпечатков пальцев при касании пальцем, передвиньте ползунок.

  Если отпечаток пальца систематически не считывается, возможно, необходимо установить более низкий предел распознавания. Более высокий параметр увеличивает чувствительность при считывании отпечатков пальцев до нескольких вариантов, и поэтому уменьшает возможность ложной идентификации. Параметр **Средняя – Высокая** обеспечивает отличное сочетание безопасности и удобства.

Настройки отпечатков пальцев пользователя

На странице «Настройки отпечатков пальцев пользователя» можно указать параметры, регулирующие внешний вид и поведение распознавания отпечатков пальцев.

▲ Для доступа к настройкам пользователя для учетных данных отпечатков пальцев щелчком мыши или касанием выберите **Настройки пользователя** на странице «Отпечатки пальцев».

- **Включить звуковой сигнал** – по окончании процесса считывания отпечатков пальцев HP Client Security по умолчанию воспроизводит звуки, соответствующие определенным событиям. Можно назначить этим событиям новые звуки, выбрав их на вкладке «Звуки» в параметрах «Звук» на панели управления Windows, или отключить звуковой сигнал, сняв флажок.
- **Показать реакцию на качество сканирования** – установите этот флажок, чтобы отображались все результаты считывания вне зависимости от их качества. Снимите этот флажок, чтобы отображались результаты считывания только хорошего качества.

HP SpareKey – восстановление пароля

Приложение HP SpareKey позволяет получить доступ к компьютеру (на поддерживаемых платформах) посредством ответа на три контрольных вопроса.

HP Client Security предложит вам настроить персональное приложение HP SpareKey во время первоначальной настройки в мастере настройки HP Client Security.

Для настройки HP SpareKey выполните следующие действия:

1. На странице мастера HP SpareKey выберите три контрольных вопроса и введите ответ на каждый вопрос.

   Можно выбрать вопрос из предложенного списка или ввести свой собственный вопрос.

2. Щелчком мыши или касанием выберите **Регистрация**.

Для удаления HP SpareKey:

▲ Щелчком мыши или касанием выберите **Удалить SpareKey**.

После настройки SpareKey можно получать доступ к компьютеру, используя SpareKey на экране проверки подлинности при включении питания или на экране приветствия Windows.

Выбрать другие вопросы или изменить ответы можно на странице SpareKey, доступ к которой можно получить через иконку Password Recovery (Восстановление пароля) на начальной странице HP Client Security.

Для доступа к разделу «Параметры HP SpareKey», где администратор может назначить настройки учетных данных HP SpareKey, щелчком мыши выберите **Параметры** (требуются права администратора).

Программа HP SpareKey Settings

На странице «Параметры HP SpareKey» можно указать параметры, регулирующие поведение и использование учетных данных HP SpareKey.

▲ Для запуска страницы «Параметры HP SpareKey» щелчком мыши или касанием выберите **Параметры** на странице HP SpareKey (требуются права администратора).

Администраторы могут задать следующие настройки:

- Указать вопросы, которые будут отображаться для каждого пользователя при настройке HP SpareKey.
- Добавить до трех специальных вопросов в список, предоставляемый пользователям.
- Выбрать, разрешать ли пользователям записывать собственные вопросы безопасности.
- Указать, какая среда проверки подлинности (Windows или проверка подлинности при включении питания) разрешает использование HP SpareKey для восстановления пароля.

Пароль Windows

HP Client Security позволяет упростить и ускорить процесс изменения пароля Windows по сравнению с использованием панели управления Windows.

Чтобы изменить пароль Windows:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите **Пароль Windows**.
2. Введите текущий пароль в текстовое поле **Текущий пароль Windows**.
3. Введите новый пароль в текстовое поле **Новый пароль Windows**, затем введите его еще раз в текстовое поле **Подтверждение нового пароля**.
4. Щелчком мыши или касанием выберите **Изменить**, чтобы немедленно заменить текущий пароль на введенный вами новый пароль.

Устройства Bluetooth

Если администратор установил Bluetooth в качестве учетных данных проверки подлинности, можно настроить телефон с функцией Bluetooth совместно с другими учетными данными для обеспечения дополнительного уровня безопасности.

ПРИМЕЧАНИЕ. Поддерживаются только телефоны с функцией Bluetooth.

1. Убедитесь, что функция Bluetooth включена на компьютере и телефон с функцией Bluetooth установлен в режим обнаружения. Для подключения телефона может потребоваться ввести автоматически созданный код на устройстве Bluetooth. В зависимости от параметров конфигурации устройства Bluetooth может потребоваться сравнение кодов создания пары между компьютером и телефоном.
2. Чтобы зарегистрировать телефон, выберите его, затем щелчком мыши или касанием выберите **Регистрация**.

Для доступа к странице Параметры устройства Bluetooth на стр. 17, где администратор может назначить настройки для устройств Bluetooth, щелчком мыши выберите **Параметры** (требуются права администратора).

Параметры устройства Bluetooth

Администраторы могут указать следующие настройки, которые регулируют поведение и использование учетных данных устройств Bluetooth:

Автоматическая проверка подлинности

- **Используйте ваше подключенное зарегистрированное устройство Bluetooth в автоматическом режиме при проверке личных данных** – установите флажок, чтобы

разрешить пользователям использовать учетные данные Bluetooth для проверки подлинности без действий со стороны пользователя, или снимите флажок, чтобы отключить эту функцию.

Присутствие Bluetooth

- **Заблокируйте компьютер, когда ваше зарегистрированное устройство Bluetooth перемещается за пределы досягаемости вашего компьютера** – установите флажок, чтобы заблокировать компьютер в случае, если устройство Bluetooth, подключенное при входе систему, окажется вне пределов досягаемости вашего компьютера, или снимите флажок, чтобы отключить эту функцию..

ПРИМЕЧАНИЕ. Модуль Bluetooth на вашем компьютере должен поддерживать эту функцию, чтобы она работала.

Карты

HP Client Security может поддерживать несколько видов идентификационных карт, которые представляют собой маленькие пластиковые карточки с компьютерным чипом. В их число входят смарт-карты, бесконтактные карты и карты бесконтактного считывания. Если одна из этих карт и соответствующее устройство считывания подключены к компьютеру, и администратор установил соответствующий драйвер производителя и назначил карту в качестве учетных данных проверки подлинности, – эту карту можно использовать в качестве учетных данных проверки подлинности.

Производитель смарт-карты должен предоставить средства для установки сертификата безопасности и управления ПИН-кодом, который HP Client Security будет использовать в алгоритме безопасности. Количество и тип символов, используемых в качестве ПИН-кода, могут различаться. Чтобы можно было использовать смарт-карту, администратор должен инициализировать ее.

HP Client Security поддерживает следующие типы смарт-карт:

- CSP
- PKCS11

HP Client Security поддерживает следующие типы бесконтактных карт:

- Бесконтактные карты памяти HID iCLASS
- Бесконтактные карты памяти MiFare Classic 1k, 4k и mini

HP Client Security поддерживает следующие типы карт бесконтактного считывания:

- Карты бесконтактного считывания HID

Чтобы зарегистрировать смарт-карту:

1. Вставьте карту в подключенное устройство считывания.
2. Когда карта распознана, введите ПИН-код карты и затем щелчком мыши или касанием выберите **Регистрация**.

Чтобы изменить ПИН-код смарт-карты:

1. Вставьте карту в подключенное устройство считывания.
2. Когда карта распознана, введите ПИН-код карты и затем щелчком мыши или касанием выберите **Проверить**.
3. Щелчком мыши или касанием выберите **Сменить ПИН-код**, затем введите новый ПИН-код.

Чтобы зарегистрировать бесконтактную карту или карту бесконтактного считывания:

1. Поместите карту на устройство считывания или очень близко к нему.
2. Когда карта распознана, щелчком мыши или касанием выберите **Регистрация**.

Чтобы удалить зарегистрированную карту:

1. Поднесите карту к устройству считывания.
2. Только для смарт-карт: введите назначенный ПИН-код карты, затем щелчком мыши или касанием выберите **Проверить**.
3. Щелчком мыши или касанием выберите **Удалить**.

После регистрации карты данные о ней отобразятся в разделе **Enrolled Cards** Зарегистрированные карты. При удалении карты она удаляется из списка.

Для доступа к разделу «Параметры карт бесконтактного считывания, бесконтактных карт и смарт-карт», где администраторы могут назначать настройки учетных данных карт, щелчком мыши или касанием выберите **Параметры** (требуются права администратора).

Параметры карт бесконтактного считывания, бесконтактных и смарт-карт

Для доступа к параметрам карты щелчком мыши или касанием выберите список и затем щелчком мыши или касанием нажмите на появившуюся стрелку.

Чтобы изменить ПИН-код смарт-карты:

1. Поднесите карту к устройству считывания
2. Введите назначенный ПИН-код карты, затем щелчком мыши или касанием выберите **Продолжить**.
3. Введите и подтвердите новый ПИН-код, затем щелчком мыши или касанием выберите **Продолжить**.

Для инициализации ПИН-кода смарт-карты:

1. Поднесите карту к устройству считывания
2. Введите назначенный ПИН-код карты, затем щелчком мыши или касанием выберите **Продолжить**.
3. Введите и подтвердите новый ПИН-код, затем щелчком мыши или касанием выберите **Продолжить**.
4. Щелчком мыши или касанием выберите **Да**, чтобы подтвердить инициализацию.

Для очистки данных на карте:

1. Поднесите карту к устройству считывания
2. Введите назначенный ПИН-код карты, (только для смарт-карт), затем щелчком мыши или касанием выберите **Продолжить**.
3. Щелчком мыши или касанием выберите **Да**, чтобы подтвердить удаление.

ПИН-код

Если администратор установил ПИН-код в качестве учетных данных проверки подлинности, можно настроить ПИН-код совместно с другими учетными данными для обеспечения дополнительного уровня безопасности.

Чтобы назначить новый ПИН-код:

▲ Введите ПИН-код, введите его снова для подтверждения, затем щелчком мыши или касанием выберите **Применить**.

Для удаления ПИН-кода:

▲ Щелчком мыши или касанием выберите **Удалить**, затем щелчком мыши или касанием выберите **Да** для подтверждения.

Для доступа к разделу «Параметры ПИН-кода», где администраторы могут назначить настройки учетных данных ПИН-кода, щелчком мыши или касанием выберите **Параметры** (требуются права администратора).

Параметры PIN

На странице «Параметры ПИН-кода» можно задать минимальную и максимальную допустимую длину учетных данных ПИН-кода.

RSA SecurID

Если администратор установил RSA в качестве учетных данных для проверки подлинности, и выполнены следующие условия, можно зарегистрировать или удалить учетные данные RSA SecurID.

ПРИМЕЧАНИЕ. Требуется подходящая программа настройки.

- Пользователь должен быть создан на сервере RSA.
- Маркер RSA SecurID, назначенный данному пользователю или компьютеру, должен быть подключен к домену сервера RSA.
- На вашем компьютере установлено программное обеспечение SecurID.
- Доступно подключение к правильно настроенному серверу RSA.

Чтобы зарегистрировать учетные данные RSA SecurID:

▲ Введите имя пользователя и код доступа RSA SecurID (код маркера RSA SecurID или ПИН +код маркера, в зависимости от используемой среды), затем щелчком мыши или касанием выберите **Применить**.

После успешной регистрации отобразится сообщение: «Учетные данные RSA SecurID успешно зарегистрированы», и станет активной кнопка «Удалить».

Чтобы удалить учетные данные RSA SecurIDl:

▲ Щелкните мышью **Удалить**, затем выберите **Да** во всплывающем диалоговом окне в ответ на вопрос: «Вы уверены, что хотите удалить учетные данные RSA SecurID?».

Password Manager

Password Manager упрощает открытие веб-сайтов и приложений, а также обеспечивает дополнительный уровень безопасности. Его можно использовать для создания более надежных паролей, которые не нужно будет записывать или запоминать. Вы сможете быстрее и проще входить в систему с помощью идентификации отпечатков пальцев, смарт-карты, карты бесконтактного ввода, бесконтактной карты, ПИН-кода, учетных данных RSA или пароля Windows.

ПРИМЕЧАНИЕ. Из-за постоянно меняющейся структуры экранов входа интернет-сайтов Password Manager не может постоянно поддерживать все веб-сайты.

Password Manager предоставляет следующие возможности:

Страница Password Manager

- Щелчком мыши или касанием выберите учетную запись для автоматического запуска веб-страницы или приложения и выполните вход.
- Используйте категории для организации ваших учетных записей.

Надежность пароля

- Быстрая оценка любых паролей с точки зрения угроз безопасности.
- При добавлении данных для входа проверьте надежность отдельных паролей, используемых для веб-сайтов и приложений.
- Надежность пароля обозначается красным, желтым и зеленым индикаторами состояния.

Значок **Password Manager** отображается в верхнем левом углу веб-страницы или экрана входа приложения. Если для данного веб-сайта или приложения еще не создана учетная запись, на значке отображается символ «плюс».

▲ Щелчком мыши или касанием выберите значок **Password Manager** для отображения контекстного меню, из которого можно выбрать следующие варианты:

- Добавить [somedomain.com] в Password Manager
- Открыть Password Manager
- Параметры значка
- Справка

Для веб-страниц и программ, учетные записи для которых еще не созданы

В контекстном меню отображаются следующие параметры:

- **Добавить [somedomain.com] в список Password Manager** – позволяет добавить учетную запись для текущего экрана входа.
- **Открыть Password Manager** – запуск Password Manager.

- **Параметры значка** – позволяет указать условия, при которых отображается значок **Password Manager**.
- **Справка** – отображение справки HP Client Security.

Для веб-страниц и программ, учетные записи для которых уже созданы

В контекстном меню отображаются следующие параметры:

- **Ввод данных для входа** – отображение страницы **Проверка идентификационных данных**. После успешной проверки подлинности данные для входа помещаются в поля данных для входа, после чего ввод подтверждается (если указано подтверждение создания или последнего изменения учетной записи).
- **Edit Logon** (Изменение учетной записи) – изменение учетной записи для данного веб-сайта.
- **Добавить учетную запись** – добавление учетной записи в Password Manager.
- **Открыть Password Manager** – запуск Password Manager.
- **Справка** – отображение справки HP Client Security.

ПРИМЕЧАНИЕ. Администратор данного компьютера может настроить HP Client Security так, что он будет запрашивать несколько наборов учетных данных в процессе проверки идентификационных данных.

Добавление учетных записей

Вы можете просто добавить учетную запись для входа на веб-сайт или в программу, введя информацию один раз. После этого Password Manager будет автоматически вводить информацию вместо вас. Можно использовать эти учетные записи после выбора веб-сайта или программы.

Чтобы добавить учетную запись, выполните следующие действия:

1. Откройте экран входа на веб-сайт или в программу.
2. Щелчком мыши или касанием выберите значок **Password Manager**, затем щелчком мыши или касанием выберите один из следующих вариантов в зависимости от того, относится ли экран входа к веб-сайту или к программе:
   - Для веб-сайта щелчком мыши или касанием выберите **Add [domain name] to Password Manager** (Добавить [имя домена] в список Password Manager).
   - Для программы щелчком мыши или касанием выберите **Add this logon screen to Password Manager** (Добавить этот экран входа в список Password Manager).
3. Введите данные учетной записи. Поля учетной записи на экране и соответствующие им поля в диалоговом окне выделяются жирной оранжевой рамкой.
   а. Чтобы заполнить поле учетной записи предварительно заданной информацией, щелчком мыши или касанием нажимайте стрелки справа от поля.
   б. Для просмотра пароля данной учетной записи щелчком мыши или касанием выберите значок **Показать пароль**.
   в. Чтобы заполнять поля учетной записи, но не подтверждать их, снимите флажок **Автоматически подтверждать данные учетной записи**.
   г. Щелчком мыши или касанием нажмите **OK** для выбора метода проверки подлинности, который необходимо использовать (отпечатки пальцев, смарт-карта,

карта бесконтактного ввода, бесконтактная карта, телефон с функцией Bluetooth, ПИН-код или пароль), и войдите в систему при помощи выбранного метода проверки подлинности.

Со значка **Password Manager** исчезнет знак «плюс». Это означает, что была создана учетная запись.

д. Если Password Manager не определяет поля учетной записи, щелчком мыши или касанием выберите **Дополнительные поля**.

- Установите флажки напротив каждого поля, требуемого для входа, и снимите ненужные флажки.
- Щелчком мыши или касанием выберите **Закрыть**.

При каждом доступе к данному веб-сайту или каждом открытии данной программы в верхнем левом углу веб-сайта или экрана входа приложения отображается значок **Password Manager**, указывающий, что можно использовать зарегистрированные учетные данные для входа в систему.

Изменение учетных записей

Для редактирования учетной записи:

1. Откройте экран входа на веб-сайт или в программу.
2. Для открытия диалогового окна, в котором можно редактировать информацию учетной записи, щелчком мыши или касанием выберите значок **Password Manager**, затем щелкните мышью или коснитесь **Edit Logon** (Изменение учетной записи).

   Поля учетной записи на экране и соответствующие им поля в диалоговом окне выделяются жирной оранжевой рамкой.

   Также можно редактировать информацию учетной записи на странице Password Manager, щелчком мыши или касанием выбрав учетную запись для отображения функций редактирования, а затем выбрав **Правка**.
3. Измените информацию учетной записи.

   - Чтобы отредактировать **Имя учетной записи** введите новое имя в соответствующее поле.
   - Чтобы добавить или отредактировать имя **Категории**, введите или измените имя в поле **Категория**.
   - Чтобы выбрать поле входа в систему **Имя пользователя** с одним из предварительно заданных вариантов, щелчком или касанием выберите стрелку вниз справа от поля.

     Предварительно заданные варианты доступны только при редактировании учетной записи с помощью команды «Правка» в контекстном меню значка Password Manager.
   - Чтобы выбрать поле входа в систему **Пароль** с одним из предварительно заданных вариантов, щелчком или касанием выберите стрелку вниз справа от поля.

     Предварительно заданные варианты доступны только при редактировании учетной записи с помощью команды «Правка» в контекстном меню значка Password Manager.
   - Для добавления полей с экрана в учетную запись щелчком мыши или касанием выберите **More fields** (Дополнительные поля).
   - Для просмотра пароля данной учетной записи щелчком мыши или касанием выберите значок **Показать пароль**.

- Чтобы заполнять поля учетной записи, но не подтверждать их, снимите флажок **Автоматически подтверждать данные учетной записи**.
- Чтобы пометить пароль данной учетной записи как скомпрометированный, установите флажок **This password is compromised** (Данный пароль скомпрометирован).

  После сохранения изменений другие учетные записи, имеющие аналогичный пароль, будут также помечены как скомпрометированные. Вы можете зайти в каждую помеченную таким образом учетную запись и изменить пароли при необходимости.

4. Щелчком мыши или касанием выберите **OK**.

Использование меню «Быстрый доступ к Password Manager»

Password Manager обеспечивает быстрый и простой доступ к веб-сайтам и программам, для которых созданы учетные записи. Чтобы открыть экран входа, двойным щелчком мыши или двойным касанием выберите учетную запись программы или веб-сайта в меню **Password Manager Quick Links** (Быстрый доступ к Password Manager) или на странице Password Manager в приложении HP Client Security и затем введите данные учетной записи.

После создания учетной записи она автоматически добавляется в меню **Quick Links** (Быстрые ссылки) в Password Manager.

Для отображения меню **Quick Links** (Быстрые ссылки) выполните следующие действия.

▲ Нажмите сочетание клавиш **Диспетчера паролей** (Ctrl+клавиша Windows +h – сочетание по умолчанию). Чтобы изменить сочетание клавиш, на начальной странице HP Client Security щелкните **Password Manager**, а затем щелчком или касанием выберите **Параметры**.

Группировка учетных записей по категориям

Для систематизации учетных записей создайте одну или несколько категорий.

Чтобы присвоить категорию учетной записи:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите **Password Manager**.
2. Щелчком мыши или касанием выберите учетную запись, затем щелчком мыши или касанием выберите **Правка**.
3. В поле **Категория** введите имя категории.
4. Щелчком мыши или касанием выберите **Сохранить**.

Чтобы удалить учетную запись из категории:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите **Password Manager**.
2. Щелчком мыши или касанием выберите учетную запись, затем щелчком мыши или касанием выберите **Правка**.
3. В поле **Категория** очистите имя категории.
4. Щелчком мыши или касанием выберите **Сохранить**.

Чтобы переименовать категорию:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите **Password Manager**.
2. Щелчком мыши или касанием выберите учетную запись, затем щелчком мыши или касанием выберите **Правка**.
3. В поле **Категория** измените имя категории.
4. Щелчком мыши или касанием выберите **Сохранить**.

Управление учетными записями

Password Manager упрощает управление сведениями учетной записи, такими как имя пользователя и пароль, и позволяет управлять множеством учетных записей из центрального узла.

Учетные записи перечислены на странице Password Manager.

Для управления учетными записями выполните следующие действия:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите **Password Manager**.
2. Щелчком мыши или касанием выберите существующую учетную запись, затем выберите один из следующих параметров и следуйте инструкциям на экране:
   - **Редактировать** – редактирование учетной записи. Дополнительную информацию см. в разделе Изменение учетных записей на стр. 23.
   - **Вход** – выполнить вход в выбранную учетную запись.
   - **Удалить** – удалить данные для входа в выбранную учетную запись.

Для добавления учетной записи для входа на веб-сайт или в программу выполните следующие действия.

1. Откройте экран для входа на веб-сайт или в программу.
2. Щелчком мыши или касанием выберите значок **Password Manager** для отображения его контекстного меню.
3. Щелчком мыши или касанием выберите **Add Logon** (Добавить учетную запись) и следуйте инструкциям на экране.

Оценка надежности пароля

Использование надежных паролей для доступа к веб-сайтам и программам является важным условием защиты идентификационных данных пользователей.

Password Manager выполняет мониторинг и упрощает повышение уровня безопасности с помощью мгновенного автоматического анализа надежности каждого пароля, используемого для доступа к веб-сайтам и программам.

При создании в Password Manager данных для входа в учетную запись во время ввода пароля под ним появляется цветная полоса для обозначения надежности пароля. Цвета имеют следующие значения:

- **Красный** – низкая надежность
- **Желтый** – средняя надежность
- **Зеленый** – высокая надежность

Параметры значка Password Manager

Password Manager пытается идентифицировать экраны входа на веб-сайты и в программы. При определении экрана входа, для которого не имеется учетной записи, Password Manager предлагает добавить учетную запись для данного экрана. При этом отображается значок **Password Manager** со знаком «плюс».

1. Щелчком или касанием выберите значок, затем щелчком или касанием выберите **Параметры значка** для настройки метода обработки Password Manager возможных веб-сайтов для входа.
   - **Prompt to add logons for logon screens** (Предлагать добавлять учетные данные для экранов входа в систему) – щелчком мыши или касанием выберите этот параметр, чтобы Password Manager всегда предлагал добавить учетную запись при отображении экрана входа, для которого не задана учетная запись.
   - **Исключить этот экран** – установите этот флажок, чтобы Password Manager не предлагал добавить учетную запись при отображении данного экрана входа.
   - **Не отображать запросы на добавление данных для входа к экранам входа в систему** – выберите переключатель.
2. Для добавления учетной записи для ранее исключенного экрана выполните следующие действия:
   а. Выполните вход на ранее исключенный веб-сайт.
   б. Чтобы Диспетчер паролей запомнил пароль к данному сайту, щелчком мыши или касанием выберите **Запомнить** во всплывающем диалоговом окне для сохранения пароля и создания учетной записи для экрана входа.
3. Для доступа к дополнительным параметрам Password Manager щелчком мыши или касанием выберите значок Password Manager, затем щелчком мыши или касанием выберите **Открыть Password Manager** и на странице Password Manager щелчком мыши или касанием выберите **Параметры**.

Импорт и экспорт учетных записей

На странице HP Password Manager «Импорт и экспорт» можно импортировать учетные записи, сохраненные в веб-браузерах на вашем компьютере. Также можно импортировать данные из файла резервной копии HP Client Security и экспортировать данные в файл резервной копии HP Client Security.

▲ Чтобы запустить страницу «Импорт и экспорт» щелчком мыши или касанием выберите **Import and export** (Импорт и экспорт) на странице Password Manager.

Чтобы импортировать пароли из браузера:

1. Щелчком мыши или касанием выберите браузер, из которого хотите импортировать пароли (отображаются только установленные браузеры).
2. Снимите флажки со всех учетных записей, пароли к которым вы не хотите импортировать.
3. Щелчком мыши или касанием выберите **Импорт**.

При импорте и экспорте данных выполнение файла резервной копии HP Client Security может осуществляться через связанные ссылки (в разделе **Other Options** (Другие возможности)) на странице «Импорт и экспорт».

ПРИМЕЧАНИЕ. Эта функция выполняет импорт и экспорт только данных Password Manager. Подробную информацию о резервном копировании и восстановлении дополнительных данных HP Client Security, см. в Резервное копирование и восстановление данных на стр. 31.

Чтобы импортировать данные из файла резервной копии HP Client Security:

1. На странице «Импорт и экспорт» Password Manager щелчком мыши или касанием выберите **Import data from an HP Client Security backup file** (Импорт данных из файла резервной копии HP Client Security).
2. Подтвердите идентификационные данные.
3. Выберите ранее созданный файл резервной копии или введите путь к нему в специальном поле, затем щелчком мыши или касанием выберите **Обзор**.
4. Введите пароль, используемый для защиты файла, затем щелчком мыши или касанием выберите **Далее**.
5. Щелчком мыши или касанием выберите **Восстановить**.

Чтобы экспортировать данные из файла резервной копии HP Client Security:

1. На странице «Импорт и экспорт» Password Manager щелчком мыши или касанием выберите **Export data from an HP Client Security backup file** (Экспорт данных из файла резервной копии HP Client Security).
2. Подтвердите свои идентификационные данные, затем щелчком мыши или касанием выберите **Далее**.
3. Введите имя файла резервной копии. По умолчанию файл сохраняется в папке «Документы». Чтобы указать другое местоположение файла, щелчком мыши или касанием выберите **Обзор**.
4. Введите и подтвердите пароль, используемый для защиты файла, затем щелчком мыши или касанием выберите **Сохранить**.

Настройки

Можно задать параметры для индивидуальной настройки Password Manager:

- **Запрос на добавление данных для входа к экранам входа в систему** – если определен экран входа на веб-сайт или в программу, значок **Password Manager** отображается со знаком «плюс», показывая, что можно добавить учетную запись для этого экрана в меню **Logons** (Учетные записи).

  Чтобы отключить эту функцию, снимите флажок **Запрос на добавление данных для входа к экранам входа в систему**.

- **Открывать Диспетчер паролей сочетанием клавиш ctrl+win+h** – по умолчанию меню **Быстрый доступ к Диспетчеру паролей** открывается сочетанием клавиш ctrl+клавиша Windows+h.

  Для изменения сочетания клавиш щелчком мыши или касанием выберите этот параметр, затем введите новое сочетание клавиш. Сочетания могут включать одну или несколько из следующих клавиш: ctrl, alt или shift, а также любую алфавитную или цифровую клавишу.

  Нельзя использовать сочетания клавиш, зарезервированные для Windows или приложений Windows.

- Для восстановления значений параметров по умолчанию щелчком мыши или касанием выберите **Восстановить значения по умолчанию**.

Дополнительные параметры

Администраторы могут получить доступ к следующим параметрам, выбрав значок **Gear** (параметры) на начальной странице HP Client Security.

- **Administrator Policies** (Политики администратора) – возможность настраивать политики входа и сеанса для администраторов.
- **Standard User Policies** (Политики обычных пользователей) – возможность настраивать политики входа и сеанса для обычных пользователей.
- **Функции безопасности** – возможность повысить безопасность вашего компьютера, защитив учетную запись Windows с помощью строгой проверки подлинности и/или активировав проверку подлинности перед пуском Windows.
- **Пользователи** – возможность управления пользователями и их учетными данными.
- **My Policies** (Мои политики) – возможность просматривать свои политики проверки подлинности и состояние регистрации.
- **Резервное копирование и восстановление** – возможность резервного копирования и восстановления данных HP Client Security.
- **О программе HP Client Security** – отображение информации о версии HP Client Security.

Политики администратора

Можно настраивать политики входа и сеанса для администраторов данного компьютера. Задаваемые здесь политики входа управляют учетными данными, необходимыми локальному администратору для входа в систему Windows. Задаваемые здесь политики сеанса управляют учетными данными, необходимыми для проверки локальным администратором учетных данных во время сеанса Windows.

По умолчанию все новые или измененные политики вступают в силу после выбора **Применить** щелчком мыши или касанием.

Чтобы добавить новую политику:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Administrator Policies** (Политики администратора).
3. Щелчком мыши или касанием выберите **Add new policy** (Добавить новую политику).
4. Щелчком мыши выберите стрелку вниз для выбора первичных и вторичных (дополнительных) учетных данных для новой политики, затем щелчком мыши или касанием выберите **Добавить**.
5. Щелкните **Применить**.

Чтобы отложить применение новой или измененной политики:

1. Щелчком мыши или касанием выберите **Enforce this policy immediately** (Применить данную политику немедленно).
2. Выберите **Enforce this policy on the specific date** (Применить данную политику в определенный день).
3. Введите дату или используйте всплывающий календарь для выбора даты, когда данная политика будет применена.
4. При желании можно выбрать, когда напомнить пользователям о новой политике.
5. Щелкните **Применить**.

Политики обычных пользователей

Можно настраивать политики входа и сеанса для обычных пользователей данного компьютера. Задаваемые здесь политики входа управляют учетными данными, необходимыми обычному пользователю для входа в систему Windows. Задаваемые здесь политики сеанса управляют учетными данными, необходимыми для проверки обычным пользователем учетных данных во время сеанса Windows.

По умолчанию все новые или измененные политики вступают в силу после выбора **Применить** щелчком мыши или касанием.

Чтобы добавить новую политику:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Standard User Policies** (Политики обычных пользователей).
3. Щелчком мыши или касанием выберите **Add new policy** (Добавить новую политику).
4. Щелчком мыши выберите стрелку вниз для выбора первичных и вторичных (дополнительных) учетных данных для новой политики, затем щелчком мыши или касанием выберите **Добавить**.
5. Щелкните **Применить**.

Чтобы отложить применение новой или измененной политики:

1. Щелчком мыши или касанием выберите **Enforce this policy immediately** (Применить данную политику немедленно).
2. Выберите **Enforce this policy on the specific date** (Применить данную политику в определенный день).
3. Введите дату или используйте всплывающий календарь для выбора даты, когда данная политика будет применена.
4. При желании можно выбрать, когда напомнить пользователям о новой политике.
5. Щелкните **Применить**.

Функции безопасности

Можно активировать функции безопасности HP Client Security, которые помогают защитить компьютер от несанкционированного доступа.

Для настройки функций безопасности:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Функции безопасности**.
3. Включите функции безопасности, установив соответствующие флажки, после чего щелчком мыши или касанием выберите **Применить**. Чем больше функций вы выберите, тем надежнее будет защищен компьютер.

   Данные настройки применяются ко всем пользователям.

   - **Windows Logon Security** (Безопасный вход в систему Windows) – защита ваших учетных записей Windows, которая требует использовать учетные данные HP Client Security для доступа.
   - **Pre-Boot Security (Power-on authentication)** (Функция безопасности при предварительной загрузке (Проверка подлинности при включении питания)) - защита вашего компьютера перед пуском Windows. Эта функция недоступна, если система BIOS ее не поддерживает.
   - **Разрешить One Step Logon** – данный параметр позволяет пропустить процедуру входа в систему Windows, если проверка подлинности была ранее проведена на уровне проверки подлинности при включении питания или на уровне Drive Encryption.
4. Щелчком мыши или касанием выберите **Пользователи**, затем щелчком мыши или касанием выберите иконку пользователя.

Пользователи

Вы можете контролировать пользователей HP Client Security и управлять ими.

Чтобы добавить в HP Client Security еще одного пользователя Windows:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Пользователи**.

3. Щелчком мыши или касанием выберите **Add another Windows user to HP Client Security** (Добавить в HP Client Security еще одного пользователя Windows).
4. Введите имя пользователя, которого нужно добавить, затем щелчком мыши или касанием выберите **OK**.
5. Введите пользовательский пароль Windows.

   Иконка добавленного пользователя отобразится на странице пользователей.

Чтобы удалить пользователя Windows из HP Client Security:

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Пользователи**.
3. Щелчком мыши или касанием выберите имя пользователя, которого нужно удалить.
4. Щелчком мыши или касанием выберите **Удалить пользователя**, затем щелчком мыши или касанием выберите **Да** для подтверждения.

Для отображения сводной информации о политика входа в систему и сеансах, активированных пользователем:

▲ Щелчком мыши или касанием выберите **Пользователи**, затем щелчком мыши или касанием выберите иконку пользователя.

Мои политики

Можно отображать свои политики проверки подлинности и состояние регистрации. На странице «Мои политики» также есть ссылки на страницы «Политики администраторов» и «Политики обычных пользователей».

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. Щелчком мыши или касанием выберите значок **My Policies** (Мои политики).

   Отображаются политики входа в систему и политики сеанса, активированные для текущего пользователя в системе.

На странице «Мои политики» также есть ссылки на Политики администратора на стр. 28 и Политики обычных пользователей на стр. 29.

Резервное копирование и восстановление данных

Рекомендуется регулярно выполнять резервное копирование данных HP Client Security. Частота резервного копирования данных зависит от частоты их изменений. Например, если вы каждый день добавляете новые учетные записи, лучше всего создавать резервные копии ежедневно.

Резервные копии также можно использовать при переходе на другой компьютер. Эти операции также называются импортом и экспортом.

ПРИМЕЧАНИЕ. Эта функция выполняет резервное копирование только Password Manager. Drive Encryption имеет независимый способ резервного копирования. Отсутствуют резервные копии данных Device Access Manager и информации проверки подлинности по отпечатку пальца.

На любом компьютере, который будет получать резервные копии данных перед тем, как они будут восстановлены из файла резервной копии, необходимо установить HP Client Security.

Для создания резервной копии данных выполните следующие действия.

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Administrator Policies** (Политики администратора).
3. Щелчком мыши или касанием выберите **Резервное копирование и восстановление**.
4. Щелчком мыши или касанием выберите **Резервное копирование**, затем пройдите проверку ваших идентификационных данных.
5. Выберите модуль, который нужно включить в резервное копирование, затем щелчком мыши или касанием выберите **Далее**.
6. Введите имя файла хранения. По умолчанию файл сохраняется в папке «Документы». Чтобы указать другое местоположение файла, щелчком мыши или касанием выберите **Обзор**.
7. Введите и подтвердите пароль для защиты файла.
8. Щелчком мыши или касанием выберите **Сохранить**.

Для восстановления данных выполните следующие действия.

1. На начальной странице HP Client Security щелчком мыши или касанием выберите значок **Gear** (Параметры).
2. На странице «Дополнительные параметры» щелчком мыши или касанием выберите **Administrator Policies** (Политики администратора).
3. Щелчком мыши или касанием выберите **Резервное копирование и восстановление**.
4. Щелчком мыши или касанием выберите **Восстановить**, затем пройдите проверку ваших идентификационных данных.
5. Выберите ранее созданный файл хранения. Введите путь к файлу в специальное поле. Чтобы указать другое местоположение файла, щелчком мыши или касанием выберите **Обзор**.
6. Введите пароль, используемый для защиты файла, затем щелчком мыши или касанием выберите **Далее**.
7. Выберите модули, данные которых нужно восстановить.
8. Щелчком мыши или касанием выберите **Восстановить**.

5 HP Drive Encryption (только на некоторых моделях)

HP Drive Encryption обеспечивает полную защиту данных путем шифрования данных компьютера. После активации приложения Drive Encryption потребуется ввести учетные данные на экране входа Drive Encryption, который отображается перед загрузкой ОС Windows®.

Экран HP Client Security Home позволяет администраторам Windows активировать Drive Encryption, выполнять резервное копирование ключа шифрования и выбирать диски или разделы для шифрования и отменять выбор. Подробнее см. справку по программному обеспечению HP Client Security.

Программа Drive Encryption позволяет выполнять следующие задачи.

- Настройка параметров Drive Encryption.
  - Шифрование или расшифровка отдельных дисков или разделов с помощью шифрования программного обеспечения
  - Шифрование или расшифровка отдельных дисков с функцией самошифрования данных с помощью аппаратного шифрования
  - Усиление безопасности путем отключения спящего или ждущего режима для выполнения проверки подлинности перед загрузкой Drive Encryption

ПРИМЕЧАНИЕ. Могут быть зашифрованы только внутренние жесткие диски SATA и внешние жесткие диски eSATA.

- Создание резервных ключей
- Восстановление доступа к зашифрованному компьютеру с помощью резервных ключей или HP SpareKey
- Включение проверки подлинности перед загрузкой Drive Encryption с использованием пароля, зарегистрированных отпечатков пальцев или PIN-кода для некоторых смарт-карт

Открытие программы Drive Encryption

Администраторы могут получить доступ к Drive Encryption, открыв HP Client Security:

1. На начальном экране щелкните или коснитесь приложения **HP Client Security** (Windows 8).

   – или –

   На рабочем столе Windows двойным щелчком мыши или двойным касанием выберите значок **HP Client Security** в области уведомлений, расположенной в крайней правой части панели задач.

2. Щелчком мыши или касанием выберите значок **Drive Encryption**.

Общие задачи

Активация Drive Encryption для стандартных жестких дисков

Для стандартных жестких дисков используется программное шифрование. Для шифрования диска или его раздела выполните следующие действия.

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. Установите флажок для диска или раздела, который надо зашифровать, а затем щелчком мыши или касанием выберите **Резервное копирование ключа**.

ПРИМЕЧАНИЕ. Для повышения уровня безопасности установите флажок **Отключить режим сна для повышения безопасности**. После отключения режима сна полностью исключается риск сохранения в памяти учетных данных, используемых для разблокировки диска.

3. Выберите один или несколько параметров резервного копирования, а затем щелчком мыши или касанием выберите **Резервное копирование**. Дополнительную информацию см. в разделе Резервное копирование ключей шифрования на стр. 38.
4. Во время резервного копирования ключа шифрования можно продолжить работу. Не перезагружайте свой компьютер.

ПРИМЕЧАНИЕ. Появится запрос на перезагрузку компьютера. После перезагрузки откроется окно шифрования диска перед загрузкой, требующее проверки подлинности перед загрузкой Windows.

Drive Encryption активировано. Шифрование выбранного раздела(-ов) диска диска может занять несколько часов, в зависимости от числа и размера раздела(-ов) диска.

Подробнее см. справку по программному обеспечению HP Client Security.

Активация Drive Encryption для дисков с функцией самошифрования данных

Для дисков с самошифрованием, соответствующих спецификации Trusted Computing Group's OPAL, может использоваться как программное, так и аппаратное шифрование. Аппаратное шифрование выполняется намного быстрее, чем программное. Однако при этом нельзя выбрать для шифрования отдельные разделы дисков. Шифруется весь диск, включая все разделы.

Чтобы выполнить шифрование отдельных разделов, нужно использовать программное шифрование. Убедитесь, что флажок **Разрешить аппаратное шифрование только для дисков с функцией самошифрования данных (SED)** снят.

Чтобы активировать Drive Encryption для дисков с самошифрованием, выполните следующие действия:

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. Установите флажок для диска, который надо зашифровать, а затем щелчком мыши или касанием выберите **Резервное копирование ключа**.

ПРИМЕЧАНИЕ. Для повышения уровня безопасности установите флажок **Отключить режим сна для повышения безопасности**. После отключения режима сна полностью исключается риск сохранения в памяти учетных данных, используемых для разблокировки диска.

3. Выберите один или несколько параметров резервного копирования, а затем щелчком мыши или касанием выберите **Резервное копирование**. Дополнительную информацию см. в разделе Резервное копирование ключей шифрования на стр. 38.
4. Во время резервного копирования ключа шифрования можно продолжить работу. Не перезагружайте свой компьютер.

ПРИМЕЧАНИЕ. В случае дисков с самошифрованием данных вам будет предложено выключить компьютер.

Подробнее см. справку по программному обеспечению HP Client Security.

Деактивация программы Drive Encryption

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. Снимите флажки для всех зашифрованных дисков и щелчком мыши или касанием выберите **Применить**.

   Начнется деактивация программы Drive Encryption.

ПРИМЕЧАНИЕ. Если использовалось программное шифрование, начнется расшифровка. Это может занять несколько часов, в зависимости от размера раздела(-ов) диска зашифрованного жесткого диска. После завершения расшифровки Drive Encryption деактивируется.

Если использовалось аппаратное шифрование, диск расшифровывается за несколько минут, после чего Drive Encryption деактивируется.

После деактивации Drive Encryption в случае аппаратного шифрования появится запрос на выключение компьютера или перезагрузку компьютера, если используется программное шифрование.

Вход в систему после активации программы Drive Encryption

При включении компьютера после активации программы Drive Encryption, если учетная запись пользователя зарегистрирована, необходимо войти в систему на экране входа Drive Encryption.

ПРИМЕЧАНИЕ. При выходе из режима ожидания или сна проверка подлинности перед загрузкой Drive Encryption не отображается для программного или аппаратного шифрования. Аппаратное шифрование предусматривает параметр **Отключить режим сна для повышения безопасности**, которая предотвращает переход в режим сна или ждущий режим при включении.

При выходе из режима гибернации проверка подлинности перед загрузкой Drive Encryption отображается для программного или аппаратного шифрования.

ПРИМЕЧАНИЕ. Если администратор Windows активировал функцию проверки безопасности перед загрузкой BIOS в HP Client Security, и если активирована функция One-Step Logon (по умолчанию), вход в систему может быть выполнен немедленно после проверки подлинности во время предзагрузки BIOS, без необходимости повторной проверки подлинности на экране входа в Drive Encryption.

Вход одного пользователя:

- На странице **Вход в систему** введите пароль Windows, ПИН-код смарт-карты, ключ SpareKey или проведите зарегистрированным пальцем.

Вход нескольких пользователей:

1. На странице **Выберите пользователя для входа** выберите пользователя для входа в раскрывающемся списке и щелчком мышки или касанием нажмите **Далее**.
2. На экране **Вход в систему** введите пароль Windows или PIN-код смарт-карты или же проведите зарегистрированным пальцем.

ПРИМЕЧАНИЕ. Поддерживаются следующие смарт-карты:

Поддерживаемые смарт-карты

- Gemalto Cyberflex Access 64k V2c

ПРИМЕЧАНИЕ. При использовании ключа восстановления для входа в систему на экране входа Drive Encryption для доступа к учетным записям пользователей на экране входа Windows требуются дополнительные учетные данные.

Шифрование дополнительных жестких дисков

Мы настоятельно рекомендуем использовать HP Drive Encryption для защиты своих данных с помощью шифрования жесткого диска. После активации жесткие диски или разделы могут быть зашифрованы с помощью следующих действий.

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. При использовании шифрования программного обеспечения выберите разделы диска для шифрования.

   ПРИМЕЧАНИЕ. Это также применимо при шифровании дисков разного типа: одного или нескольких стандартных жестких дисков и одного или нескольких дисков с функцией самошифрования данных.

– или –

- Для дисков с аппаратным шифрованием выберите дополнительный диск или диски, которые требуется зашифровать.

Дополнительные задачи

Управление Drive Encryption (задача администратора)

Администраторы могут использовать Drive Encryption для просмотра и изменения состояния шифрования («Не зашифровано» или «Зашифровано») всех жестких дисков компьютера.

- Если состояние шифрования – «Включено», программа Drive Encryption активирована и настроена. Диск находится в одном из следующих состояний.

Шифрование программного обеспечения

- Не зашифровано
- Зашифрован
- Выполняется шифрование
- Выполняется расшифровка

Аппаратное шифрование

- Зашифрован
- Не зашифровано (для дополнительных дисков)

Шифрование и расшифровка отдельных разделов дисков (только программное шифрование)

Администраторы могут использовать Drive Encryption для шифрования одного или нескольких разделов жесткого диска на компьютере или расшифровки ранее зашифрованных разделов диска.

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. В диалоговом окне **Состояние диска** установите или снимите флажки для разделов дисков, которые необходимо зашифровать или расшифровать, затем щелчком мыши или касанием выберите **Применить**.

ПРИМЕЧАНИЕ. При шифровании или расшифровке раздела в строке выполнения отображается ход выполнения шифрования в процентах.

ПРИМЕЧАНИЕ. Динамические разделы не поддерживаются. Если раздел отображается как доступный, но его не удается зашифровать, этот раздел является динамическим. Динамический раздел является результатом сжатия раздела для создания нового раздела в «Управлении дисками».

Если раздел будет преобразован в динамический раздел, отобразится предупреждение.

Управление дисками

- **Псевдоним** — для облегчения идентификации можно давать имена дискам или их разделам.
- **Отключенные диски** — Drive Encryption может отслеживать диски, которые были удалены из компьютера. Диск, удаленный из компьютера, автоматически помещается в «Список отключенных дисков». Если диск возвращается в систему, он снова появится в «Списке подключенных дисков».

- Если больше нет необходимости отслеживать отключенный диск или управлять им, можно удалить отключенный диск из списка отключенных дисков.
- Drive Encryption остается активным, пока не сняты флажки для всех подключенных дисков, а список отключенных дисков пуст.

Резервное копирование и восстановление (задача администратора)

Если программа Drive Encryption активирована, администраторы могут выполнять резервное копирование ключей шифрования на съемные носители, а также восстановление ключей на странице «Резервное копирование ключа шифрования».

Резервное копирование ключей шифрования

Администраторы могут выполнять резервное копирование ключа шифрования для зашифрованного диска на съемное запоминающее устройство.

⚠ **ПРЕДУПРЕЖДЕНИЕ.** Необходимо хранить запоминающее устройство с резервным ключом в надежном месте, поскольку, если вы забудете пароль, потеряете смарт-карту и для вас не зарегистрированы отпечатки пальцев, это устройство останется единственным способом доступа к компьютеру. Место хранения также должно быть безопасным, поскольку запоминающее устройство разрешает доступ к Windows.

1. Запустите **Drive Encryption**. Дополнительную информацию см. в разделе Открытие программы Drive Encryption на стр. 33.
2. Установите флажок для диска, затем щелчком мыши или касанием выберите **Резервное копирование ключа**.
3. В разделе **Создать ключ восстановления HP Drive Encryption** выберите один или несколько следующих параметров:
   - **Съемный накопитель** — установите флажок, затем выберите устройство хранения данных, на которое будет сохранен ключ шифрования.
   - **SkyDrive** — установите этот флажок. Компьютер должен быть подключен к интернету. Войдите в Microsoft SkyDrive, затем щелчком мыши или касанием выберите **Да**.

     ПРИМЕЧАНИЕ. Для использования резервной копии ключа HP Drive Encryption, который хранится на SkyDrive, необходимо загрузить его со SkyDrive на съемное устройство хранения данных, а затем вставить съемное устройство хранения данных в компьютер.
   - **TPM** (только на некоторых моделях) — позволяет восстанавливать данные, используя пароль TPM.

     ⚠ **ПРЕДУПРЕЖДЕНИЕ.** Если TPM не установлен или поврежден компьютер, теряется доступ к резервным копиям. Если выбран этот метод, следует также выбрать другой метод резервного копирования.
4. Щелчком мыши или касанием выберите **Резервное копирование**.

   Ключ шифрования сохраняется на выбранном запоминающем устройстве.

Восстановление доступа к активированному компьютеру с помощью резервных ключей

Администраторы могут выполнять восстановление данных с помощью ключа Drive Encryption, резервная копия которого сохранена на съемном устройстве хранения данных, или выбрав параметр **Резервное копирование ключа** в Drive Encryption.

1. Установите съемное запоминающее устройство с резервным ключом.
2. Включите компьютер.
3. После открытия диалогового окна входа HP Drive Encryption щелчком мыши или касанием выберите **Восстановление**.
4. Введите путь/имя файла, который содержит резервную копию вашего ключа, затем щелчком мыши или касанием выберите **Восстановление**.
5. При появлении диалогового окна подтверждения щелчком мыши или касанием выберите **OK**.

   Отображается экран входа Windows.

ПРИМЕЧАНИЕ. При использовании ключа восстановления для входа в систему на экране входа Drive Encryption для доступа к учетным записям пользователей на экране входа Windows требуются дополнительные учетные данные. Настоятельно рекомендуется сбросить пароль после выполнения восстановления.

Выполнение восстановления HP SpareKey

Восстановление SpareKey перед загрузкой Drive Encryption требует правильного ответа на секретные вопросы для доступа к компьютеру. Дополнительные сведения о настройке восстановления SpareKey см. в справке по программному обеспечению HP Client Security.

Для выполнения восстановления HP SpareKey, если вы забыли пароль, выполните следующие действия.

1. Включите компьютер.
2. После открытия страницы Drive Encryption перейдите на страницу входа пользователя.
3. Щелкните **SpareKey**.

ПРИМЕЧАНИЕ. Если SpareKey не инициализирован в HP Client Security, кнопка **SpareKey** не активна.

4. Введите верные ответы на отображающиеся вопросы, затем щелкните **Вход**.

   Отображается экран входа Windows.

ПРИМЕЧАНИЕ. При использовании SpareKey для входа в систему на экране входа Drive Encryption для доступа к учетным записям пользователей на экране входа Windows требуются дополнительные учетные данные. Настоятельно рекомендуется сбросить пароль после выполнения восстановления.

6 HP File Sanitizer (только на некоторых моделях)

File Sanitizer позволяет выполнять безопасное уничтожение ненужных ресурсов (например: личных данных или файлов, данных журнала или сети или других компонентов данных) на жестком диске компьютера и периодически полностью очищать внутренний жесткий диск компьютера.

File Sanitizer не может быть использован для очистки следующих типов приводов.

- Твердотельные накопители (SSD), включая тома RAID на устройствах SSD
- Внешние диски с подключениями по интерфейсам USB, Firewire или eSATA

При попытке выполнения операции уничтожения или очистки накопителей SSD отобразится сообщение об ошибке, и операция не будет выполнена.

Уничтожение

Процесс уничтожения отличается от стандартного процесса удаления в системе Windows®. При уничтожении ненужного ресурса с помощью программы File Sanitizer файлы перезаписываются пустыми данными, что делает извлечение оригинального ресурса практически невозможным. Простой процесс удаления в системе Windows может оставить файл (или ресурс) на жестком диске без изменений или в состоянии, где для его восстановления можно использовать аналитические методы.

Можно запланировать время следующего уничтожения или вручную активировать уничтожение, выбрав значок **File Sanitizer** на начальном экране HP Client Security или с помощью значка **File Sanitizer** на рабочем столе Windows. Подробнее см. Настройка расписания уничтожения на стр. 42, Уничтожение щелчком правой кнопки мыши на стр. 44 или Запуск операции уничтожения вручную на стр. 45.

ПРИМЕЧАНИЕ. Файл DLL подлежит уничтожению и удалению из системы только после перемещения в корзину.

Очистка свободного пространства

Процесс удаления ресурса в системе Windows не полностью удаляет содержимое ресурса с жесткого диска. Система Windows удаляет только ссылку на ресурс или его расположение на жестком диске. Содержимое ресурса остается на жестком диске, пока в ту же область жесткого диска не будет записан другой ресурс с новой информацией.

Очистка свободного пространства позволяет безопасно записывать случайные данные поверх удаленных ресурсов во избежание просмотра пользователями оригинального содержимого удаленного ресурса.

ПРИМЕЧАНИЕ. Очистка свободного пространства исключает какую-либо защиту уничтоженных ресурсов.

Можно задать время следующей очистки свободного пространства или вручную активировать очистку свободного пространства ранее уничтоженных ресурсов, выбрав значок **File Sanitizer** на начальном экране HP Client Security или с помощью значка **File Sanitizer** на рабочем столе

Windows. Подробнее см. Установка расписания очистки свободного пространства на стр. 43, Запуск очистки свободного пространства вручную на стр. 45 или Использование значка File Sanitizer на стр. 44.

Запуск программы File Sanitizer (Очистка файлов)

1. На начальном экране щелкните или коснитесь приложения **HP Client Security** (Windows 8).

   – или –

   На рабочем столе Windows двойным щелчком мыши или двойным касанием выберите значок **HP Client Security** в области уведомлений, расположенной в крайней правой части панели задач.

2. В разделе **Данные** щелчком мыши или касанием выберите **File Sanitizer**.

– или –

▲ Двойным щелчком мыши или двойным касанием выберите значок **File Sanitizer** на рабочем столе Windows.

– или –

▲ Щелкните правой кнопкой мыши или коснитесь и удерживайте значок **File Sanitizer** на рабочем столе Windows, а затем выберите **Открыть File Sanitizer**.

Процедуры настройки

Уничтожение — File Sanitizer безопасно удаляет или уничтожает выбранные категории данных.

1. В разделе **Уничтожение** установите флажки для всех типов файлов, которые нужно уничтожить, или снимите флажки, если не хотите уничтожать эти файлы.

   - **Корзина** — уничтожает все элементы в корзине.
   - **Временные файлы системы** — уничтожает все файлы, находящиеся в папке временных файлов системы. Поиск следующих переменных среды осуществляется в следующем порядке, а первый обнаруженный путь считается системной папкой:
     - TMP
     - TEMP
   - **Временные файлы Интернета** — уничтожает копии веб-страниц, изображения и файлы мультимедиа, сохраненные веб-браузером для ускорения повторного обзора.
   - **Файлы cookie** — уничтожает все файлы, сохраняемые на компьютере веб-сайтами для запоминания пользовательских параметров, например, данных для входа.

2. Чтобы начать уничтожение, щелчком мыши или касанием выберите **Уничтожить**.

Очистка — записывает произвольные данные на свободное место и предотвращает восстановление удаленных элементов.

▲ Чтобы запустить очистку, щелчком мыши или касанием выберите **Очистить**.

Параметры File Sanitizer — установите флажок, чтобы включить какой-либо из следующих параметров или снимите флажок, чтобы отключить параметр:

- **Включить значок рабочего стола** — отображает значок File Sanitizer на рабочем столе Windows.
- **Включить правый щелчок** — позволяет щелчком правой кнопки мыши или касанием выбрать и удерживать ресурс, а затем выбрать **HP File Sanitizer – Уничтожить**.
- **Запросить пароль Windows перед уничтожением вручную** — требует проверку подлинности с помощью пароля Windows перед уничтожением элемента вручную.
- **Уничтожить файлы cookie и временные файлы Интернета при закрытии браузера** — уничтожение всех выбранных ресурсов сети, например, URL-журнала браузера, при закрытии браузера.

Настройка расписания уничтожения

Можно задать график выполнения автоматического уничтожения или в любое время уничтожить ресурсы вручную. Дополнительные сведения см. в разделе Процедуры настройки на стр. 41.

1. Откройте File Sanitizer и щелчком мыши или касанием выберите **Параметры**.
2. Чтобы запланировать время для уничтожения выбранных ресурсов, на вкладке **График уничтожения** выберите **Никогда**, **Один раз**, **Ежедневно**, **Еженедельно** или **Ежемесячно**, затем выберите день и время:
   - **а.** Щелчком мыши или касанием выберите часы, минуты или поле AM/PM.
   - **б.** Прокручивайте, пока необходимое значение не отобразится на том же уровне, что и на других полях.
   - **в.** Щелчком мыши или касанием выберите пустое пространство вокруг полей установки времени.
   - **г.** Повторите для каждого поля, пока не будет выбран правильный график.
3. Указаны следующие четыре типа ресурсов:
   - **Корзина** — уничтожает все элементы в корзине.
   - **Временные файлы системы** — уничтожает все файлы, находящиеся в папке временных файлов системы. Поиск следующих переменных среды осуществляется в следующем порядке, а первый обнаруженный путь считается системной папкой:
     - TMP
     - TEMP
   - **Временные файлы Интернета** — уничтожает копии веб-страниц, изображения и файлы мультимедиа, сохраненные веб-браузером для ускорения повторного обзора.
   - **Файлы cookie** — уничтожает все файлы, сохраняемые на компьютере веб-сайтами для запоминания пользовательских параметров, например, данных для входа.

При установке флажка эти ресурсы уничтожаются в запланированное время.

4. Чтобы выбрать дополнительные специальные ресурсы, которые нужно уничтожить, выполните следующие действия:

   а. В разделе **Запланировано к уничтожению** щелчком мыши или касанием выберите **Добавить папку** и перейдите к файлу или папке.

   б. Щелчком мыши или касанием выберите **Открыть**, затем щелчком мыши или касанием выберите **OK**.

   Чтобы удалить ресурс из списка «Запланировано к уничтожению», снимите флажок напротив этого ресурса.

Установка расписания очистки свободного пространства

Очистка свободного пространства исключает какую-либо защиту уничтоженных ресурсов.

1. Откройте File Sanitizer и щелчком мыши или касанием выберите **Параметры**.
2. Чтобы запланировать время следующей очистки жесткого диска, под **График очистки**, выберите **Никогда** , **Один раз**, **Ежедневно**, **Еженедельно**или **Ежемесячно**, а затем выберите день и время.

   а. Щелчком мыши или касанием выберите часы, минуты или поле AM/PM.

   б. Прокручивайте, пока необходимое время не отобразится на том же уровне, что и на других полях.

   в. Щелчком мыши или касанием выберите пустое пространство вокруг полей установки времени.

   г. Повторяйте, пока не будет выбран правильный график.

ПРИМЕЧАНИЕ. Процесс очистки свободного пространства может занять достаточно длительное время. Убедитесь, что компьютер подключен к источнику переменного тока. Хотя очистка свободного пространства выполняется в фоновом режиме, повышенное использование процессора может повлиять на производительность компьютера. Окончательную очистку свободного пространства можно выполнить по истечении нескольких часов или при бездействии компьютера.

Защита файлов от уничтожения

Чтобы защитить файлы и папки от уничтожения, выполните следующие действия:

1. Откройте File Sanitizer и щелчком мыши или касанием выберите **Параметры**.
2. В разделе **Не для уничтожения** щелчком мыши или касанием выберите **Добавить папку** и перейдите к файлу или папке.
3. Щелчком мыши или касанием выберите **Открыть**, затем щелчком мыши или касанием выберите **OK**.

ПРИМЕЧАНИЕ. Файлы из списка защищены, пока они находятся в списке.

Чтобы удалить ресурс из списка исключений, снимите флажок с ресурса.

Общие задачи

С помощью File Sanitizer можно выполнить следующие задачи:

- **Использовать значок File Sanitizer для запуска процесса уничтожения** — позволяет перетаскивать файлы на значок **File Sanitizer** на рабочем столе Windows. Подробнее см. Использование значка File Sanitizer на стр. 44.
- **Вручную уничтожить отдельный ресурс или все выбранные ресурсы** — уничтожает элементы, не ожидая запуска процесса уничтожения по графику. Подробнее см. Уничтожение щелчком правой кнопки мыши на стр. 44 или Запуск операции уничтожения вручную на стр. 45.
- **Вручную запустить очистку свободного пространства** — запускает процесс очистки свободного пространства в любое время. Подробнее см. Запуск очистки свободного пространства вручную на стр. 45.
- **Просмотр файлов журнала** — позволяет просматривать файлы журнала уничтожения и очистки свободного пространства, содержащие информацию об ошибках, возникших при последнем выполнении уничтожения или очистки свободного пространства. Подробнее см. Просмотр файлов журнала на стр. 45.

ПРИМЕЧАНИЕ. Уничтожение и очистка свободного пространства могут занять длительное время. Хотя уничтожение и очистка свободного места выполняются в фоновом режиме, увеличенная загрузка процессора может повлиять на производительность вашего компьютера.

Использование значка File Sanitizer

ПРЕДУПРЕЖДЕНИЕ. Уничтоженные данные восстановить невозможно. Внимательно выбирайте элементы на уничтожение вручную.

При запуске операции уничтожения вручную уничтожаются ресурсы из стандартного списка подлежащих уничтожению ресурсов, заданного в File Sanitizer (см. Процедуры настройки на стр. 41).

Можно запустить операцию уничтожения вручную одним из следующих способов:

1. Откройте File Sanitizer (см. Запуск программы File Sanitizer (Очистка файлов) на стр. 41) и щелчком мыши или касанием выберите **Уничтожить**.
2. При появлении диалогового окна подтверждения убедитесь, что ресурсы, которые нужно удалить, отмечены флажком, а затем щелчком мыши или касанием нажмите **OK**.

– или –

1. Щелкните правой кнопкой мыши или коснитесь и удерживайте значок **File Sanitizer** на рабочем столе Windows, затем щелчком мыши или касанием выберите **Уничтожить сейчас**.
2. При появлении диалогового окна подтверждения убедитесь, что ресурсы, которые нужно удалить, отмечены флажком, а затем щелчком мыши или касанием нажмите **Уничтожить**.

Уничтожение щелчком правой кнопки мыши

ПРЕДУПРЕЖДЕНИЕ. Уничтоженные ресурсы невозможно восстановить. Внимательно выбирайте элементы на уничтожение вручную.

Выбрав **Включить уничтожение щелчком правой кнопки мыши** в интерфейсе File Sanitizer, можно уничтожить ресурс следующим образом:

1. Перейдите к документу или папке, которые надо уничтожить.
2. Щелкните правой кнопкой мыши или коснитесь и удерживайте файл или папку, а затем выберите **HP File Sanitizer – Уничтожить**.

Запуск операции уничтожения вручную

⚠ **ПРЕДУПРЕЖДЕНИЕ.** Уничтоженные данные восстановить невозможно. Внимательно выбирайте элементы на уничтожение вручную.

При запуске операции уничтожения вручную уничтожаются ресурсы из стандартного списка подлежащих уничтожению ресурсов, заданного в File Sanitizer (см. Процедуры настройки на стр. 41).

Можно запустить операцию уничтожения вручную одним из следующих способов:

1. Откройте File Sanitizer (см. Запуск программы File Sanitizer (Очистка файлов) на стр. 41) и щелчком мыши или касанием выберите **Уничтожить**.
2. При появлении диалогового окна подтверждения убедитесь, что ресурсы, которые нужно удалить, отмечены флажком, а затем щелчком мыши или касанием нажмите **OK**.

– или –

1. Щелкните правой кнопкой мыши или коснитесь и удерживайте значок **File Sanitizer** на рабочем столе Windows, затем щелчком мыши или касанием выберите **Уничтожить сейчас**.
2. При появлении диалогового окна подтверждения убедитесь, что ресурсы, которые нужно удалить, отмечены флажком, а затем щелчком мыши или касанием нажмите **Уничтожить**.

Запуск очистки свободного пространства вручную

При запуске операции очистки вручную очищаются ресурсы из стандартного списка подлежащих очистке ресурсов, заданного в File Sanitizer (см. Процедуры настройки на стр. 41).

Можно запустить операцию уничтожения вручную одним из следующих способов:

1. Откройте File Sanitizer (см. Запуск программы File Sanitizer (Очистка файлов) на стр. 41) и щелчком мыши или касанием выберите **Очистить**.
2. При появлении диалогового окна подтверждения щелчком мыши или касанием выберите **OK**.

– или –

1. Щелкните правой кнопкой мыши или коснитесь и удерживайте значок **File Sanitizer** на рабочем столе Windows, затем щелчком мыши или касанием выберите **Очистить сейчас**.
2. При появлении диалогового окна подтверждения щелчком мыши или касанием выберите **Очистить**.

Просмотр файлов журнала

При каждом выполнении уничтожения или очистки свободного пространства создаются файлы журнала, содержащие сведения об ошибках. Файлы журнала всегда обновляются в соответствии с процессом уничтожения или очистки свободного пространства.

ПРИМЕЧАНИЕ. Успешно уничтоженные или очищенные файлы не отображаются в файлах журнала.

Один файл журнала создается для процессов уничтожения, а другой – для процессов очистки свободного пространства. Оба файла журнала находятся на жестком диске в следующих папках:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Имя пользователя]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Имя пользователя]*_DiskBleachLog.txt

В 64-битных системах файлы журнала находятся на жестком диске в следующих папках:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Имя пользователя]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Имя пользователя]*_DiskBleachLog.txt

7 HP Device Access Manager (только на некоторых моделях)

Программа HP Device Access Manager осуществляет контроль доступа к данным посредством отключения устройств передачи данных.

ПРИМЕЧАНИЕ. Некоторые устройства интерфейса пользователя/устройств ввода, такие как мышь, клавиатура, сенсорная панель и устройство считывания отпечатков пальцев, не контролируются программой Device Access Manager. Подробнее см. раздел Неуправляемые классы устройств на стр. 51.

Администраторы ОС Windows® могут использовать HP Device Access Manager для управления доступом к устройствами в системе и предотвращения несанкционированного доступа.

- Для каждого пользователя создаются профили устройств, определяющие набор разрешенных и запрещенных к использованию устройств.
- Политика своевременной проверки подлинности (JITA) позволяет заранее заданным пользователям проходить проверку подлинности для получения доступа к устройствам, который в иных случаях запрещен.
- Администраторы и доверенные пользователи могут быть исключены из списка ограничений на доступ к устройствам, установленного в Device Access Manager, путем добавления их в группу «Администраторы устройств». Управление членами этой группы осуществляется в пункте «Дополнительные параметры».
- Доступ к устройствам может быть разрешен или запрещен в зависимости от членства пользователя в группе или для отдельных пользователей.
- Для таких классов устройств, как дисководы CD и DVD, доступ для чтения и записи настраивается по отдельности.

Следующие параметры Device Access Manager автоматически настраиваются при завершении работы мастера настройки HP Client Security:

- Доступ к съемным носителям службы «Своевременная проверка подлинности» (JITA) разрешен для администраторов и пользователей.
- Политика устройства разрешает полный доступ к другим устройствам.

Запуск Device Access Manager

1. На начальном экране щелкните или коснитесь приложения **HP Client Security** (Windows 8).

   – или –

   На рабочем столе Windows двойным щелчком мыши или двойным касанием выберите значок **HP Client Security** в области уведомлений, расположенной в крайней правой части панели задач.

2. В разделе **Устройство**, щелчком мыши или касанием выберите **Device Permissions** (Разрешения).

   - Обычные пользователи могут просматривать свой текущий доступ к устройствам (см. Пользовательское представление на стр. 48).
   - Администраторы могут просматривать и изменять текущие настройки доступа к устройствам для данного компьютера, щелкнув мышью или коснувшись **Изменить** и затем введя пароль администратора (см. Системное представление на стр. 48).

Пользовательское представление

При выборе **Device Permission** (Разрешения) отображается пользовательское представление. В зависимости от политики обычные пользователи и администраторы могут просматривать собстенный доступ к классам устройств или отдельным устройствам на данном компьютере.

- **Current user** (Текущий пользователь) – отображается текущий пользователь в системе.
- **Класс устройств** – отображаются типы устройств.
- **Доступ** – отображаются ваши текущие настройки доступа к типам устройств или к определенным устройствам.
- **Длительность** – отображается ограничение по времени вашего доступа к дисководам CD/DVD-ROM или съемным дисководам.
- **Параметры** – администраторы могут выбирать, доступ к каким дискам управляется с помощью Device Access Manager.

Системное представление

В системном представлении администраторы могут разрешить или запретить группам «Пользователи» или «Администраторы» доступ к устройствам данного компьютера.

▲ Администраторы могут осуществлять доступ к системному представлению щелкнув мышью или коснувшись **Изменить**. Затем нужно ввести пароль администратора и выбать один из следующих параметров:

- **Device Access Manager** – чтобы включить или выключить Device Access Manager со службой «Своевременная проверка подлинности», щелкните мышью или коснитесь **Вкл.** или **Выкл.**
- **Users and groups on this PC** (Пользователи и группы данного ПК) – отображается группа «Пользователи» или «Администраторы», которым разрешен или запрещен доступ к выбранным классам устройств.
- **Класс устройств** – отображаются все классы устройств и устройства, которые установлены в системе или могли быть установлены в системе ранее. Чтобы расширить список, щелкните значок **+**. Показаны все устройства, подключенные к данному

компьютеру; группы «Администраторы» и «Пользователи» развернуты и показаны их участники. Чтобы обновить список устройств, щелкните круглую стрелку (значок обновления).

- Защита обычно применяется к классу устройств. Если установлено **Разрешить** доступ, выбранный пользователь или группа смогут осуществлять доступ к любому устройству, принадлежащему к данному классу устройств.
- Защиту также можно применить к определенным устройствам.
- Настройте службу «Своевременная проверка подлинности» (JITA), чтобы разрешить выбранным пользователям доступ к дисководам DVD/CD-ROM или съемным носителям посредством собственной проверки подлинности. Дополнительную информацию см. в разделе Конфигурация JITA на стр. 50.
- Разрешайте или запрещайте доступ к другим классам устройств, таким, как съемные носители (флэш-накопители USB), последовательные и параллельные порты, устройства Bluetooth®, модемы, устройства PCMCIA/ExpressCard, устройства 1394, устройства считывания отпечатков пальцев и чтения смарт-карт. Если отказано в доступе к устройству считывания отпечатков пальцев и устройству чтения смарт-карт, их можно использовать как учетные данные проверки подлинности, но на уровне политики сеанса их использовать нельзя.

  ПРИМЕЧАНИЕ. При использовании устройств Bluetooth в качестве учетных данных проверки подлинности доступ к устройству Bluetooth не должен ограничиваться политикой Device Access Manager.

- При выборе параметра на уровне групп или устройств пользователю предлагается применить параметр к дочерним объектам:

  Да – параметр распространится.

  Нет – Параметр не распространится.

- Управление некоторыми классами устройств, например, DVD-устройствами и дисководами компакт-дисков, может впоследствии осуществляться посредством разрешения или запрещения доступа отдельно для операций чтения и записи.

  ПРИМЕЧАНИЕ. Группа администраторов не может быть добавлена к списку пользователей.

- **Доступ** – щелчком мыши или касанием выберите стрелку вниз, затем выберите один из предложенных видов доступа, чтобы разрешить или запретить доступ:
  - **Allow – Full Access** (Разрешить – полный доступ)
  - **Allow – Read Only** (Разрешить – только для чтения)
  - **Allow – JITA Required** (Разрешить – требуется JITA) – подробнее см. Конфигурация JITA на стр. 50.

    Если выбран этот тип доступа, в разделе **Длительность**, щелчком мыши или касанием выберите стрелку вниз для выбора ограничения по времени.
  - **Deny** (Запретить)
- **Длительность** – щелчком мыши или касанием выберите стрелку вниз для выбора ограничения по времени для доступа к дисководам DVD/CD-ROM или съемным носителям (см. Конфигурация JITA на стр. 50).

Конфигурация JITA

Конфигурация JITA разрешает администраторам просматривать и изменять списки пользователей и групп, которым разрешен или запрещен доступ к устройствам, использующим своевременную проверку подлинности (JITA).

Пользователи с включенной службой JITA смогут иметь доступ к некоторыми устройствам, политики которых, созданные в представлении **Конфигурация класса устройств**, были ограничены.

Период JITA может иметь разрешение на определенное количество минут или не иметь ограничений. Пользователи с неограниченным периодом JITA будут иметь доступ к устройству с момента проверки подлинности и до момента выхода из системы.

Если период JITA у пользователя ограничен, за минуту до истечения периода JITA пользователю предложат продлить доступ. При выходе пользователя из системы или входе в систему другого пользователя период JITA истекает. При следующем входе пользователя в систему и его попытке получить доступ к устройству со включенной JITA отобразится запрос на ввод учетных данных.

JITA доступна для следующих классов устройств:

- Дисководы DVD/CD-ROM
- Съемные дисководы

Создание политики JITA для пользователя или группы

Администраторы могут разрешать пользователям или группам доступ к устройствам, используя службу «Своевременная проверка подлинности» (JITA).

1. Запустите **Device Access Manager**, затем щелчком мыши или касанием выберите **Изменить**.
2. Выберите пользователя или группу и в разделе **Доступ** для одной из категорий **Съемные дисководы** или **Дисководы DVD/CD-ROM** выберите щелчком мыши или касанием стрелку вниз и затем выберите **Allow – JITA Required** (Разрешить – требуется JITA).
3. В разделе **Длительность** щелчком мыши или касанием выберите стрелку вниз для выбора периода времени доступа JITA.

Для применения новых параметров JITA пользователю необходимо выйти из системы, а затем войти снова.

Отключение политики JITA для пользователя или группы

Администраторы могут запретить пользователям или группам доступ к устройствам, используя своевременную проверку подлинности.

1. Запустите **Device Access Manager**, затем щелчком мыши или касанием выберите **Изменить**.
2. Выберите пользователя или группу и в разделе **Доступ** для одной из категорий **Съемные дисководы** или **Дисководы DVD/CD-ROM** выберите щелчком мыши или касанием стрелку вниз и затем выберите **Deny** (Запретить).

При входе пользователя в систему и его попытке получить доступ к устройству в доступе будет отказано.

Настройки

Представление **Параметры** позволяет администраторам просматривать или изменять диски, доступ к которым управляется Device Access Manager.

ПРИМЕЧАНИЕ. При настройке списка буквенных обозначений дисков Device Access Manager должен быть включен (см. Системное представление на стр. 48).

Неуправляемые классы устройств

Программа HP Device Access Manager не управляет следующими классами устройств:

- Устройства ввода/вывода
  - CD-ROM
  - Дисковод
  - Контроллер гибкого диска (FDC)
  - Контроллер жесткого диска (HDC)
  - Класс устройств интерфейса пользователя (HID)
  - Инфракрасные устройства интерфейса пользователя
  - Мышь
  - Последовательный мульти-порт
  - Клавиатура
  - Принтеры «Plug and play» (PnP)
  - Принтер
  - Обновление принтера
- Питание
  - Дополнительная поддержка управления питанием (APM)
  - Батарея
- Разное
  - Компьютер
  - Декодер
  - Дисплей
  - Единый драйвер дисплея Intel®
  - Legacard
  - Драйвер носителя
  - Устройство для смены носителя
  - Устройства памяти
  - Монитор
  - Многофункциональные устройства

- Сетевой клиент
- Сетевая служба
- Сетевой перенос
- Процессор
- Адаптер SCSI
- Ускоритель операций по безопасности
- Устройства безопасности
- Система
- Неизвестно
- Объем
- Снимок объема

8 HP Trust Circles

HP Trust Circles – приложение, обеспечивающее безопасность файлов и документов, которое сочетает в себе шифрование файлов в папках и удобную возможность совместного использования документов участниками Trust Circle. Приложение шифрует файлы, помещенные в указанные пользователем папки, защищая их в рамках Trust Circle. После применения защиты только участники Trust Circle могут пользоваться и обмениваться файлами. Если защищенный файл получен пользователем, не являющимся участником Trust Circle, файл останется зашифрованным, и такой пользователь не получит доступ к его содержимому.

Открытие Trust Circles

1. Щелчком мыши или касанием выберите приложение **HP Client Security** на начальном экране.

   – или –

   На рабочем столе ОС Windows дважды щелкните значок **HP Client Security** в области уведомлений в правой части панели задач.

2. В разделе **Данные** щелчком мыши или касанием выберите **Trust Circles**.

Приступая к работе

Предусмотрены два способа отправки приглашений по электронной почте и ответов на них:

- **Using Microsoft® Outlook** (Используя Microsoft® Outlook) – использование Trust Circles вместе с Microsoft Outlook автоматизирует обработку любых приглашений в Trust Circle и ответов от других пользователей Trust Circle.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Используя Gmail, Yahoo, Outlook.com или другие службы электронной почты (SMTP)) – при вводе имени, электронного адреса и пароля приложение Trust Circles использует вашу службу электронной почты для отправки приглашений участникам, выбранным для вступления в ваш Trust Circle.

Для настройки основного профиля:

1. Введите ваше имя и электронный адрес, затем щелчком мыши или касанием выберите **Далее**.

   Имя видят все пользователи, приглашенные присоединиться к вашему Trust Circle. Электронный адрес используется для отправки и получения приглашений или ответов на них.

2. Введите пароль учетной записи электронной почты, затем щелчком мыши или касанием выберите **Далее**.

   Отправлено тестовое электронное сообщение, чтобы подтвердить точность настроек электронной почты.

ПРИМЕЧАНИЕ. Компьютер должен быть подключен к сети.

3. В поле **Trust Circle Name** (Имя Trust Circle) введите имя Trust Circle, затем щелчком мыши или касанием выберите **Далее**.

4. Добавьте участников и папки, затем щелчком мыши или касанием выберите **Далее**. Создан Trust Circle, который содержит все выбранные файлы, и по электронной почте рассылаются приглашения всем выбранным участникам. Если отправка приглашения невозможна по каким-либо причинам, отображается соответствующее уведомление. В любое время можно снова пригласить участников с помощью представления «Trust Circle», щелчком мыши выбрав **Your Trust Circles** (Ваши Trust Circles), а затем двойным щелчком мыши или двойным касанием выбрав Trust Circle. Дополнительную информацию см. в разделе Trust Circles на стр. 54.

Trust Circles

Можно создать Trust Circle при первоначальной настройке после ввода вашего электронного адреса или в представлении «Trust Circle»:

▲ В представлении «Trust Circle» щелчком мыши или касанием выберите **Create Trust Circle** (Создать Trust Circle), затем введите имя Trust Circle.

- Чтобы добавить участников в Trust Circle, щелчком мыши или касанием выберите значок **M+** рядом с **Members** (Участники) и следуйте инструкциям на экране.
- Чтобы добавить папки в Trust Circle, щелчком мыши или касанием выберите значок **+** возле **Папки** и следуйте инструкциям на экране.

Добавление папок в Trust Circle

Добавление папок в новый Trust Circle:

- При создании Trust Circle можно добавлять папки, щелчком мыши или касанием выбрав значок **+** возле **Папки** и затем следуя инструкциям на экране.

  – или –

- В Windows Explorer щелкните правой кнопкой мыши или коснитесь и удерживайте папку, которая не является частью Trust Circle, выберите **Trust Circle**, а затем выберите **Create Trust Circle from Folder** (Создать Trust Circle из папки).

СОВЕТ: Можно выбрать одну или несколько папок.

Добавление папок в существующий Trust Circle:

- В представлении «Trust Circle» щелчком мыши выберите **Your Trust Circles** (Ваши Trust Circles), двойным щелчком мыши или двойным касанием выберите существующий Trust Circle, чтобы отобразить текущие папки, щелчком мыши или касанием выберите значок **+** возле **Папки** и следуйте инструкциям на экране.

  – или –

- В Windows Explorer щелкните правой кнопкой мыши или коснитесь и удерживайте папку, которая не является частью Trust Circle, выберите **Trust Circle** и затем выберите **Add to existing Trust Circle from Folder** (Добавить в существующий Trust Circle из папки).

СОВЕТ: Можно выбрать одну или несколько папок.

После добавления папки в Trust Circle приложение Trust Circles автоматически зашифрует папку и ее содержимое. После завершения шифрования всех файлов отобразится

уведомление об этом. Кроме этого, на значках всех зашифрованных папок и значках файлов внутри этих папок отображается зеленый символ замка, обозначая их полную защиту.

Добавление участников в Trust Circle

Добавление участников в Trust Circle происходит в три этапа:

1. **Пригласить** – сначала владелец Trust Circle приглашает участников. Приглашение может быть отправлено нескольким пользователям или спискам/группам рассылки.
2. **Принять** – приглашенный пользователь получает приглашение и выбирает, принять его или отклонить. Если пользователь принимает приглашение, приглашающему отправляется ответ по электронной почте. Если приглашение отправлено группе, каждый участник получает отдельное приглашение и выбирает, принять его или отклонить.
3. **Зарегистрировать** – у приглашающего есть возможность решить в итоге, добавлять участника в Trust Circle или нет. Если приглашающий решает зарегистрировать участника, данному приглашенному пользователю отправляется письмо-подтверждение. Приглашающий и приглашенный пользователи могут дополнительно проверить безопасность процесса приглашения. Для приглашенного пользователя отображается проверочный код, который необходимо прочитать приглашающему по телефону. После проверки кода приглашающий может отправить окончательное регистрационное письмо.

Добавление участников в новый Trust Circle:

▲ При создании Trust Circle можно добавлять участников, щелчком мыши или касанием выбрав значок **M+** возле **Участники**, а затем следуя инструкциям на экране.

- Пользователи Outlook могут выбрать контакты из адресной книги Outlook и затем щелчком мыши выбрать **OK**.
- Пользователи других почтовых служб могут вручную добавлять новые электронные адреса в Trust Circle или получать их из списка адресов, зарегистрированных в Trust Circle.

Добавление участников в существующий Trust Circle:

▲ В представлении «Trust Circle» щелчком мыши выберите **Your Trust Circles** (Ваши Trust Circles), двойным щелчком мыши или двойным касанием выберите существующий Trust Circle, чтобы отобразить текущих пользователей, щелчком мыши или касанием выберите значок **M+** возле **Участники** и следуйте инструкциям на экране.

- Пользователи Outlook могут выбрать контакты из адресной книги Outlook и затем щелчком мыши выбрать **OK**.
- Пользователи других почтовых служб могут вручную добавлять новые электронные адреса в Trust Circle или получать их из списка адресов, зарегистрированных в Trust Circle.

Добавление файлов в Trust Circle

Можно добавлять файлы в Trust Circle одним из следующих способов:

- Скопируйте или переместите файл в существующую папку Trust Circle.

  – или –

- В проводнике Windows щелкните правой кнопкой мыши или коснитесь и удерживайте незашифрованный файл, выберите **Круг доверия**, а затем выберите **Зашифровать**. Вам будет предложено выбрать Trust Circle, в который следует добавить файл.

СОВЕТ: Можно выбрать один или несколько файлов.

Зашифрованные папки

Любой участник Trust Circle может просматривать и редактировать файлы, относящиеся к этому Trust Circle.

ПРИМЕЧАНИЕ. Trust Circle Manager/Reader не синхронизирует файлы между участниками.

Обмениваться файлами следует с помощью существующих средств, таких как электронная почта, FTP-сервер или облачные хранилища. Защита файлов, скопированных и перемещенных в Trust Circle или созданных в нем, выполняется немедленно.

Удаление папок из Trust Circle

Удаление папки из Trust Circle приводит к расшифровке папки и всего ее содержимого, а также снимет с них защиту.

- В представлении «Trust Circle» щелчком мыши или касанием выберите**Your Trust Circles** (Ваши Trust Circles), двойным щелчком мыши или двойным касанием выберите существующий Trust Circle, чтобы отобразить текущие папки, затем щелчком мыши или касанием выберите значок **trash can** (Корзина) возле этой папки.

  – или –

- В Windows Explorer щелкните правой кнопкой мыши или коснитесь и удерживайте папку, которая является частью Trust Circle, выберите **Trust Circle**, а затем выберите **Remove from trust circle** (Удалить из Trust Circle).

СОВЕТ: Можно выбрать одну или несколько папок.

Удаление файла из Trust Circle

Чтобы удалить файл из круга доверия, в проводнике Windows щелкните правой кнопкой мыши или коснитесь и удерживайте зашифрованный файл, выберите **Круг доверия**, выберите **Расшифровать файл**.

Удаление участников из Trust Circle

Невозможно удалить полностью зарегистрированного участника из Trust Circle. В качестве альтернативы можно создать новый Trust Circle со всеми другими участниками, переместить все файлы и папки в новый Trust Circle, а затем удалить старый Trust Circle. Это гарантирует, что участник не будет иметь доступ ко всем новым полученным файлам, однако у участника старого Trust Circle сохранится доступ ко всем ресурсам, к которым ранее был открыт общий доступ.

Если участник зарегистрирован не полностью (получил приглашение вступить в Trust Circle или отклонил приглашение вступить в Trust Circle), можно удалить такого участника из Trust Circle одним из следующих способов:

- В представлении «Trust Circle» щелчком мыши или касанием выберите **Your Trust Circles** (Ваши Trust Circles), затем двойным щелчком мыши или двойным касанием выберите Trust Circle, чтобы показать текущий список пользователей. Щелчком мыши или касанием выберите значок **trash can** (Корзина) возле имени пользователя, которого нужно удалить.
- В представлении «Trust Circle» щелчком мыши или касанием выберите **Members** (Участники), затем двойным щелчком мыши или двойным касанием выберите участника,

чтобы отобразить Trust Circles, в которых он состоит. Щелчком мыши или касанием выберите значок **trash can** (Корзина) возле Trust Circle, участника которого нужно удалить.

Удаление Trust Circle

Для удаления Trust Circle требуется право собственности.

▲ В представлении «Trust Circle» щелчком мыши или касанием выберите **Your Trust Circles** (Ваши Trust Circles), затем щелчком мыши или касанием выберите значок **trash can** (Корзина) возле Trust Circle, который нужно удалить.

Таким образом Trust Circle удаляется со страницы, а всем участникам Trust Circle отправляются письма с уведомлением об удалении Trust Circle. Все файлы и папки, которые входили в данный Trust Circle, расшифровываются.

Установка параметров

В представлении «Trust Circle» щелчком мыши или касанием выберите **Параметры**. Отображаются три вкладки

- **Настройки электронной почты**

Параметр	Описание
Имя пользователя	Отображается текущее имя пользователя. Чтобы сменить имя пользователя, введите новое имя в текстовом поле. Изменения сохраняются автоматически.
Электронный адрес	Отображается текущая учетная запись электронной почты. Чтобы изменить ее, щелчком мыши или касанием выберите **Change Email Settings** (Изменить параметры электронной почты) и следуйте инструкциям на экране.
Подтверждение нового участника	Выберите один из следующих вариантов: ◦ **Confirm Automatically** (Автоматическое подтверждение) – после получения уведомления о том, что пользователи приняли приглашение о вступлении в Trust Circle, их участи автоматически подтверждается без необходимости ручного ввода данных, а приглашенным пользователям отправляются электронные сообщения с подтверждением. ◦ **Confirm Manually** (Подтвердить вручную) – после получения уведомления о том, что пользователи приняли приглашение о вступлении в Trust Circle, для регистрации новых участников необходимо вручную ввести их данные в Trust Circle, после чего приглашенным пользователям отправляются электронные сообщения с подтверждением. ◦ **Require Verification** (Требуется проверка) – после получения уведомления о том, что пользователи приняли приглашение о вступлении в Trust Circle, требуется проверочный код для полной регистрации приглашенных пользователей. Владелец Trust Circle должен связаться с приглашенными пользователями и получить от них проверочный код. После ввода правильного кода рассылаются электронные сообщения с подтверждением.
Периодическая проверка подлинности	Периодическая проверка подлинности требует от пользователя ввода пароля Windows после определенного периода времени (в минутах), а также при выполнении конфиденциальных операций. Данный параметр позволяет пользователям включать и выключать проверку подлинности.

Параметр	Описание
Время ожидания проверки подлинности	Выберите определенный период времени (в минутах) между периодическими проверками подлинности.
Не показывать сообщение подтверждения	Установите флажок, чтобы отключить отображение сообщений подтверждения, или снимите флажок для отображения сообщений подтверждения.
Я хочу улучшить приложение HP Trust Circle с помощью функции анонимного отслеживания его использования	Установите флажок для участия в программе или снимите флажок, если не хотите участвовать.

- **Резервное копирование/восстановление**

Параметр	Описание
Резервное копирование	Копирует данные Trust Circle Manager/Reader (параметры и Trust Circles) в файл резервной копии. В случае сбоя или отказа системы можно использовать данный файл для восстановления и новой установки Trust Circles к состоянию, сохраненному в файле. **ПРИМЕЧАНИЕ.** Сохраняются только данные вашего приложения Trust Circle («Trust Circles», «Параметры» и «Участники»). Резервное копирование текущих файлов в папках Trust Circle не выполняется. Резервное копирование таких файлов выполняется отдельно. Чтобы выполнить резервное копирование параметров и данных пользователей Trust Circle: **1.** Щелчком мыши или касанием выберите **Резервное копирование**. **2.** Выберите имя и каталог для файла резервной копии, затем щелчком мыши или касанием выберите **Сохранить**. **3.** Введите пароль, подтвердите его, затем щелчком мыши или касанием выберите **OK**. Для восстановления данного файла необходим пароль.
Восстановление	Восстанавливает параметры и Trust Circles из файла резервной копии, как правило, после сбоя системы или перехода на другой компьютер. Чтобы восстановить параметры Trust Circle Manager и данные пользователей: **1.** Щелчком мыши или касанием выберите **Восстановить**. **2.** Перейдите к каталогу и файлу резервной копии, затем щелчком мыши или касанием выберите **Открыть**. **3.** Введите пароль, который был задан при создании резервной копии.

- **О программе** – отображается версия программного обеспечения Trust Circle Manager/Reader. Отображаются ссылки для обновления Trust Circle Manager до профессиональной версии или для отображения заявления HP о конфиденциальности.

9 Обнаружение похищенных устройств (только на некоторых моделях)

Computrace (приобретается отдельно) позволяет осуществлять для компьютера дистанционный контроль, управление и отслеживание.

После включения Computrace настраивается в Центре поддержки пользователей Absolute Software. В Центре поддержки пользователей администратор может настроить Computrace для наблюдения за компьютером и управления им. Если система перенесена в другое место или украдена, Центр поддержки пользователей может помочь местным властям в поиске и возврате компьютера. При соответствующей настройке Computrace может продолжить работать даже после стирания и замены жесткого диска.

Для включения Computrace:

1. Выполните подключение к Интернету.
2. Запустите программу HP Client Security. Дополнительную информацию см. в разделе Открытие программы HP Client Security на стр. 11.
3. Щелкните **Восстановление после кражи**.
4. Для запуска мастера активации программы Computrace нажмите кнопку **Запуск**.
5. Введите контактную информацию или данные кредитной карты, или укажите приобретенный заранее ключ продукта.

Мастер активации выполнит безопасную обработку данных о транзакции, а затем создаст для вас учетную запись пользователя на веб-сайте Центра поддержки пользователей Absolute Software. По завершении активации вы получите сообщение электронной почты с подтверждением и сведениями о вашей учетной записи Центра поддержки пользователей.

Если вы уже запускали мастер активации программы Computrace и у вас есть учетная запись в Центре поддержки пользователей, можете приобрести дополнительные лицензии, связавшись с представителем компании HP.

Для входа в систему Центра поддержки пользователей выполните следующие действия.

1. Перейдите по адресу https://cc.absolute.com/.
2. В полях **Имя пользователя** и **Пароль** укажите учетные данные, полученные в письме с подтверждением, затем щелкните кнопку **Войти в систему**.

Используя Центр поддержки пользователей, вы получаете следующие возможности.

- Наблюдение за своими компьютерами.
- Защита удаленных данных.
- Сообщение о краже компьютеров, на которых установлена программа защиты Computrace.

▲ Щелкните **Подробнее**, чтобы узнать больше про Computrace.

10 Ограничения локализованных паролей

На уровне проверки подлинности при включении питания и уровне HP Drive Encryption, поддержка локализации пароля ограничена. Дополнительную информацию см. в разделе На уровнях проверки подлинности при включении питания и Drive Encryption редакторы Windows IME не поддерживаются на стр. 60.

Что делать при отклонении пароля

Пароли могут отклоняться по следующим причинам.

- Пользователь использует неподдерживаемый IME. Это распространенная проблема языков с двухбайтовой кодировкой (корейский, японский, китайский). Для решения проблемы выполните следующее.

  1. Перейдите в **Панель управления** и добавьте поддерживаемую раскладку клавиатуры (добавьте клавиатуры Английский/США для языка ввода «Китайский»).
  2. Установите поддерживаемые клавиатуры для языка ввода по умолчанию.
  3. Запустите HP Client Security, затем введите пароль Windows.

- Пользователь использует неподдерживаемый символ. Для решения проблемы выполните следующее.

  1. Измените пароль Windows, чтобы в нем содержались только поддерживаемые символы. Подробнее о не поддерживаемых символах см. Обработка специальных клавиш на стр. 61.
  2. Запустите HP Client Security, затем введите пароль Windows.

На уровнях проверки подлинности при включении питания и Drive Encryption редакторы Windows IME не поддерживаются

В системе Windows пользователи могут выбрать IME (редактор метода ввода) для ввода сложных знаков и символов, например, японских или китайских символов, с помощью стандартной клавиатуры.

IME не поддерживаются на уровнях проверки подлинности при включении питания и Drive Encryption. Пароль Windows нельзя ввести с помощью IME при проверке подлинности при включении питания или на экране входа в систему HP Drive Encryption,так как это может привести к блокировке. В некоторых случаях Microsoft® Windows не отображает IME при вводе пользователем пароля.

Решение состоит в переходе на одну из следующих поддерживаемых раскладок клавиатуры, преобразуемую в раскладку 00000411:

- Microsoft IME для японского языка
- Раскладка клавиатуры «Японский»
- Office 2007 IME для японского языка — если Microsoft или третье лицо использует термин IME или редактор метода ввода, метод ввода в действительности может не быть IME. Это может вызвать путаницу, но программное обеспечение использует представление шестнадцатеричного кода. Таким образом, если IME соответствует поддерживаемой раскладке клавиатуры, программа HP Client Security поддерживает эту конфигурацию.

ВНИМАНИЕ! При развертывании программы HP Client Security пароли, веденные с использованием Windows IME, будут отклонены.

Изменения пароля с помощью раскладки клавиатуры, которая также поддерживается

Если пароль изначально установлен с использованием одной раскладки клавиатуры, например «Английский (США) (409)», а затем пользователь меняет пароль с помощью другой раскладки, которая также поддерживается, например, «Латиноамериканская (080A)», изменение пароля будет работать в HP Drive Encryption, но в BIOS оно вызовет ошибку при использовании символов второй раскладки, отсутствующих в изначальной (например, «é»).

ПРИМЕЧАНИЕ. Администраторы могут решить эту проблему с помощью страницы «Пользователи» HP Client Security (на которую можно перейти, выбрав значок **Gear** на начальной странице), удалив пользователя из HP Client Security, выбрав нужную раскладку клавиатуры в операционной системе и снова запустив мастер настройки HP Client Security для этого же пользователя. BIOS сохраняет нужную раскладку клавиатуры, и пароли, которые можно ввести с помощью нее, будут правильно установлены в BIOS.

Другая потенциальная проблема – использование различных раскладок клавиатуры с одинаковыми символами. Например, в обеих раскладках клавиатуры «США - международная» (20409) и «Латиноамериканская» (080A) есть символ «é», но для его вывода могут требоваться различные последовательности нажатия клавиш. Если пароль изначально установлен с раскладкой клавиатуры «Латиноамериканская», эта раскладка устанавливается в BIOS, даже если после этого пароль был изменен с использованием раскладки клавиатуры «США - международная».

Обработка специальных клавиш

- Китайский, словацкий, французский (Канада) и чешский языки

  При выборе пользователем одной из указанных раскладок клавиатуры и последующем вводе пароля (например, abcdef) при проверке безопасности при включении и в HP Drive Encryption этот пароль необходимо вводить с нажатой клавишей shift для нижнего регистра и клавишами shift и caps lock для верхнего регистра. Цифровые пароли необходимо вводить с помощью цифровой панели клавиатуры.

- Корейский язык

  При выборе пользователем поддерживаемой раскладки клавиатуры «Корейский» и последующем вводе пароля при проверке безопасности при включении и в HP Drive Encryption этот пароль необходимо вводить с нажатой клавишей alt для нижнего регистра и клавишами alt и caps lock для верхнего регистра.

- Неподдерживаемые символы перечислены в следующей таблице.

Language (Язык)	Windows	BIOS.	Drive Encryption
Арабский	Клавиши ﻻ, ﻷ и ﻹ выводят два символа.	Клавиши ﻻ, ﻷ и ﻹ выводят один символ.	Клавиши ﻻ, ﻷ и ﻹ выводят один символ.
Французский (Канада)	ç, è, à и é с нажатой клавишей caps lock – Ç, È, À и É в ОС Windows.	ç, è, à и é с нажатой клавишей caps lock – ç, è, à и é при проверке при включении.	ç, è, à и é с нажатой клавишей caps lock – ç, è, à и é в HP Drive Encryption.
Испанский	40a не поддерживается. Тем не менее, она может использоваться, поскольку программно преобразуется в c0a. Однако из-за незначительных различий раскладок испаноязычным пользователям рекомендуется установить раскладку клавиатуры Windows 1040a (Испанская 2) или 080a (Латинская Америка).	нет	нет
США - международная	◦ Клавиши ¡, ¤, ‘, ’, ¥ и × в верхнем ряду отклоняются. ◦ Клавиши å, ® и Þ во втором ряду отклоняются. ◦ Клавиши á, ð и ø в третьем ряду отклоняются. ◦ Клавиша æ в нижнем ряду отклоняется.	нет	нет
Czech	◦ Клавиша ğ отклоняется. ◦ Клавиша į отклоняется. ◦ Клавиша ų отклоняется. ◦ Клавиши ė, ı и ż отклоняются. ◦ Клавиши ģ, ķ, ļ, ņ и ŗ отклоняются.	нет	нет
Словацкий	Клавиша ż отклоняется.	◦ Клавиши š, ś и ş отклоняются при вводе с обычной клавиатуры, но принимаются при вводе с программной клавиатуры. ◦ Мертвая клавиша ţ выводит два символа.	нет
Hungarian	Клавиша ż отклоняется.	Клавиша ţ выводит два символа.	нет

Language (Язык)	Windows	BIOS.	Drive Encryption
Slovenian	Клавиша żŻ отклоняется в Windows, а клавиша alt создаёт мертвую клавишу в BIOS.	Клавиши ú, Ú, ů, Ů, ş, Ş, ś, Ś, š и Š отклоняются в BIOS.	нет
Японец	Лучше использовать Microsoft Office 2007 IME, если он доступен. Несмотря на название IME в действительности это поддерживаемая раскладка клавиатуры 411.	нет	нет

Глоссарий

автоматическое уничтожение
Уничтожение, запланированное в программе File Sanitizer.

администратор
См. *Администратор Windows*.

администратор Windows
Пользователь с полными правами доступа к изменению разрешений и управлению другими пользователями.

активация
Задача, которая должна быть выполнена для доступа к функциям Drive Encryption. Администраторы могут активировать Drive Encryption с помощью Мастера настройки HP Client Security или HP Client Security. Процесс активации состоит из активации программного обеспечения, шифрования диска и создания первоначальной резервной копии ключа шифрования на съемном запоминающем устройстве.

Аппаратное шифрование
Использование дисков с функцией самошифрования данных, соответствующих требованиям спецификации OPAL организации TCG к управлению дисками с функцией самошифрования, для выполнения мгновенного шифрования. Аппаратное шифрование выполняется мгновенно и занимает всего несколько минут. Шифрование программного обеспечения может занимать несколько часов.

архив аварийного восстановления
Защищенная область хранения, с помощью которой возможно перешифрование основных ключей пользователя с одной платформы ключей владельца на другую.

Бесконтактная карта
Пластиковая карта, содержащая компьютерную микросхему, которую можно использовать для проверки подлинности.

восстановление
Действие, при котором информация копируется из ранее созданной резервной копии обратно в программу.

Восстановление HP SpareKey
Возможность доступа к компьютеру путем правильного ответа на вопросы безопасности.

вход
Объект HP Client Security, содержащий имя пользователя и пароль (а также, возможно, другую выбранную информацию), который может использоваться для доступа к веб-сайтам или другим программам.

группа
Группа пользователей, имеющих один уровень разрешений или запретов на доступ к классу устройств или отдельным устройствам.

домен
Группа компьютеров, которые являются частью сети и используют общую базу данных каталогов. Домены имеют уникальные имена, для каждого из них задан набор общих правил и процедур.

идентификационная карточка
Элемент рабочего стола Windows, который служит для визуальной идентификации рабочего стола с помощью имени пользователя и выбранного изображения.

класс устройств
Все устройства одного типа, например дисководы.

Круг доверия
Обеспечивает включение данных, привязывая их к определенной группе доверенных пользователей. Это предотвратит случайную или преднамеренную передачу данных в чужие руки. Данные, защищенные технологией CryptoMill's Zero Overhead Key Management, криптографически привязываются к Trust Circle. Это предотвратит расшифровку документов или другой конфиденциальной информации за пределами круга доверия.

Менеджер/читатель круга доверия
Trust Circle Reader может принимать приглашения только от пользователей Trust Circle Manager. При этом Trust Circle Manager позволяет создавать Trust Circles. Его функции включают отправку пользователям приглашений о вступлении в Trust Circle и прием приглашений о вступлении в Trust Circle от других пользователей. После создания Trust Circle из равнозначных пользователей можно безопасно обмениваться файлами между участниками этого Trust Circle.

Микросхема встроенной системы безопасности Trusted Platform Module (TPM)
Проверка подлинности компьютера через TPM происходит быстрее, чем с участием пользователя, благодаря сохранению информации, относящейся к хост-системе (ключи шифрования, цифровые сертификаты и пароли). TPM сводит к минимуму угрозу безопасности находящейся на компьютере информации, которая может возникнуть вследствие физической кражи компьютера или внешней атаки хакера.

Начальная страница
Центральный узел для доступа и управления функциями и параметрами HP Client Security.

объект
Находящийся на жестком диске компонент данных, представляющими собой личные данные или файлы, журналы и другие данные, связанные с Интернетом, и т.д.

однократная регистрация
Служба, которая сохраняет данные проверки подлинности и позволяет использовать HP Client Security для доступа к Интернету и приложениям Windows, для которых требуется ввод пароля.

отпечаток пальца
Цифровое считывание изображения отпечатка пальца. В HP Client Security не хранится действительное изображение отпечатка вашего пальца.

Очистка свободного пространства
Запись случайных данных поверх удаленных ресурсов и неиспользуемого пространства. Данный процесс снижает существование удаленных ресурсов, поэтому восстановить исходный ресурс становится сложнее.

Папка Круг доверия
Любая папка, защищенная Trust Circle.

перезагрузка
Процесс перезапуска компьютера.

ПИН-код
Персональный идентификационный номер, используемый зарегистрированным пользователем для проверки подлинности.

подключенное устройство
Аппаратное устройство, подключенное к порту на компьютере.

политика управления доступом к устройству
Список устройств, к которым пользователю разрешен или запрещен доступ.

пользователь
Все пользователи, зарегистрированные в модуле Drive Encryption (Шифрование дисков). Пользователи, не являющиеся администраторами, имеют ограниченные права в программе Drive Encryption (Шифрование дисков). Они могут только регистрироваться (при наличии утверждения администратора) и выполнять вход.

проверка подлинности
Процесс проверки личности с помощью учетных данных, включая пароль Windows, отпечаток пальца, смарт-карту, бесконтактную карту или проксимити карту.

Проверка подлинности перед загрузкой Drive Encryption
Экран входа, отображаемый до запуска Windows. Пользователи должны ввести имя пользователя и пароль Windows или PIN-код смарт-карты либо считать зарегистрированный палец. При выборе одношагового входа в систему и вводе верных сведений на экране входа Drive Encryption выполняется вход в Windows, и повторный вход на экране входа Windows не требуется.

проверка подлинности при включении питания
Служба безопасности, которая выполняет проверку подлинности в определенной форме (например, при помощи смарт-карты, микросхемы безопасности или пароля) при включении компьютера.

Программное шифрование
Использование программного обеспечения для последовательного шифрования секторов жесткого диска. Этот процесс является более медленным по сравнению с аппаратным шифрованием

Проксимити карта
Пластиковая карта, содержащая компьютерную микросхему, которая может использоваться для проверки подлинности совместно с другими учетными данными для обеспечения дополнительного уровня безопасности.

расшифровка
Процедура, используемая в криптографии для преобразования зашифрованных данных в понятный текст.

Резервное копирование
Резервное копирование позволяет сохранить важную информацию из программы в другое место. Впоследствии информацию из резервной копии можно восстановить на этом или на другом компьютере.

Своевременная проверка подлинности
См. справку программного обеспечения HP Device Access Manager.

сетевая учетная запись
Учетная запись пользователя или администратора Windows на локальном компьютере, в рабочей группе или в домене.

смарт-карта
Аппаратное устройство, которое можно использовать с ПИН-кодом для проверки подлинности.

способ безопасного входа в систему
Способ, используемый для входа в компьютер.

удостоверение
Набор учетных данных и параметров, выступающих в качестве профиля или учетной записи для отдельного пользователя в HP Client Security.

уничтожение
Выполнение алгоритма, перезаписывающего данные, содержащиеся в ресурсе, пустыми данными.

уничтожение вручную
Незамедлительное уничтожение отдельного ресурса или выбранных ресурсов помимо графика уничтожения.

учетная запись Windows
Пользователь, авторизованный для входа в сеть или отдельный компьютер.

учетные данные
Определенная информация или аппаратное устройство, использующееся для проверки подлинности отдельного пользователя.

шифрование
Процедура, например, использование алгоритма, применяемая в криптографии для преобразования обычного текста в зашифрованный текст в целях предотвращения прочтения данных неуполномоченными пользователями. Существует много типов шифрования данных, они составляют основу сетевой безопасности. К основным типа шифрования относятся стандарт DES (Data Encryption Standard) и шифрование с открытым ключом.

экран входа в систему Drive Encryption (Шифрование дисков)
См. раздел «Проверка подлинности перед загрузкой Drive Encryption».

Bluetooth
Технология, использующая радиопередачи для компьютеров, принтеров, мышей, мобильных телефонов и других устройств для беспроводной коммуникации на коротком расстоянии, оборудованных устройством Bluetooth.

Drive Encryption (Шифрование диска)
Защищает данные путем шифрования жестких дисков, делая информацию на них нечитаемой для неавторизованных пользователей.

DriveLock
Служба безопасности, которая связывает жесткий диск и пользователя и требует от пользователя правильного ввода пароля DriveLock при запуске компьютера.

Encryption File System (EFS)
Система, которая зашифровывает все файлы и подпапки в выбранной папке.

PKI
Стандарт «Инфраструктуры открытых ключей», который определяет интерфейсы для создания, использования и администрирования сертификатов и криптографических ключей.

Windows Logon Security (Защита входа в Windows)
Защищает учетные записи Windows, запрашивая перед входом определенные учетные данные.

Указатель