HP ProtectTools

Начало работы

Первая редакция: Август 2012 г.

Номер документа: 702113-251

Содержание

1 Введение в безопасность

Программное обеспечение HP ProtectTools Security Manager предоставляет функции обеспечения безопасности, защищающие от несанкционированного доступа к компьютеру, сетям и критическим данным.

Приложение	Средства
Консоль администрирования HP ProtectTools Security Manager (для администраторов)	• Для доступа требуются права® администратора Microsoft Windows. • Предоставляет доступ к модулям, настраиваемым администраторами и недоступным для пользователей. • Позволяет выполнять настройку безопасности и задает параметры или требования для всех пользователей.
Пользовательская консоль HP ProtectTools Security Manager (для пользователей)	• Позволяет пользователям настраивать параметры, заданные администратором. • Позволяет администраторам предоставлять пользователям ограниченное управление некоторыми модулями HP ProtectTools.

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

Программные модули HP ProtectTools могут быть предварительно установлены, предварительно загружены или доступны для загрузки с веб-сайта HP. Дополнительные сведения см. на веб-сайте http://www.hp.com.

ПРИМЕЧАНИЕ. Инструкции в этом руководстве предполагают, что вы уже знакомы с программными модулями HP ProtectTools.

Функции HP ProtectTools

В следующей таблице описаны ключевые функции модулей HP ProtectTools.

Модуль	Ключевые функции
Консоль администрирования HP ProtectTools Security Manager	Администраторы могут выполнять следующие функции: • Мастер настройки Security Manager используется для настройки уровней безопасности и способов безопасного входа в систему. • Настройка параметров, скрытых от пользователей. • Активация Activate Drive Encryption и настройка доступа пользователей. • Настройка политик и доступа пользователей Device Access Manager. • Использование инструментов администратора для добавления и удаления пользователей HP ProtectTools и просмотра состояния пользователей.
Пользовательская консоль HP ProtectTools Security Manager	Обычные пользователи могут выполнять следующие функции: • Просмотр параметров состояния шифрования и Device Access Manager. • Активация Computrace для HP ProtectTools. • Настройка предпочтений, а также таких функций, как резервное копирование и восстановление.
Диспетчер учетных данных	Обычные пользователи могут выполнять следующие функции: • Изменение имен пользователей и паролей. • Настройка и изменение учетных данных пользователя, например пароля Windows, отпечатков пальцев, изображений лиц, смарт-карты, проксимити карты и бесконтактной карты.
Password Manager	Обычные пользователи могут выполнять следующие функции: • Упорядочивание и настройка имен пользователей и паролей. • Создание более надежных паролей для улучшения защиты учетной записи. Password Manager автоматически вводит и отправляет данные. • Упрощение процесса входа благодаря функции единого входа, которая автоматически запоминает и применяет учетные данных пользователя.
Drive Encryption for HP ProtectTools (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).

Модуль	Ключевые функции
Программа Device Access Manager for HP ProtectTools (только на некоторых моделях)	• 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.
Обнаружение похищенных устройств (Computrace for HP ProtectTools, 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 службы безопасности HP ProtectTools и примеры ее типичного использования

В большинстве служб безопасности HP ProtectTools предусмотрена как проверка подлинности пользователя (обычно с помощью пароля), так и административный резервный доступ в случае, если пароль потерян, забыт, недоступен, или в любой другой ситуации, когда корпоративной безопасности требуется доступ.

ПРИМЕЧАНИЕ. Некоторые службы безопасности HP ProtectTool разработаны для ограничения доступа к данным. Данные, потеря которых менее опасна для пользователя, чем утечка, должны быть зашифрованы. Рекомендуется хранить 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.

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. Старательный бухгалтер получил повышение и стал руководителем финансового отдела. 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. Главный бухгалтер решает организовать все веб-ссылки, имена пользователей компании и пароли в диспетчере паролей. После этого он внедряет диспетчер паролей для всех сотрудников, чтобы они могли работать с учетными записями, не зная при этом учетных данных, с помощью которых входят в системы.

Drive Encryption for HP ProtectTools (только на некоторых моделях)

Drive Encryption используется для ограничения доступа к данным на всем жестком диске или дополнительном диске. Drive Encryption также используется для управления дисками с самошифрованием.

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.

Drive Encryption for HP ProtectTools не предоставляет доступ к зашифрованным данным даже если диск удален, поскольку обе службы привязаны к материнской плате.

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.

Программа Device Access Manager for HP ProtectTools (только на некоторых моделях)

С помощью Device Access Manager for HP ProtectTools администраторы могут ограничивать доступ к оборудованию и управлять этим доступом. Служба Device Access Manager for HP ProtectTools может использоваться для блокирования неавторизованного доступа к флэш-накопителям USB, используемым для копирования данных. Она также ограничивает доступ к дискам CD и DVD, управляет устройствами USB, сетевыми подключениями и т. п. Примером может служить ситуация, в которой внешним поставщикам требуется доступ к компьютерам компании, но они не должны иметь возможность копировать данные на устройства USB.

Пример 1. Менеджер медицинской компании часто работает с личными медицинскими записями, а также с данными своей компании. Сотрудникам требуется доступ к этим данным, однако крайне важно, чтобы их не копировали на устройства USB или другие внешние накопители. Сеть защищена, но компьютер оборудован устройствами для записи компакт-дисков и портами USB, что дает возможность скопировать и украсть данные. Менеджер

использует Device Access Manager, чтобы отключить порты USB и запретить запись компакт-дисков. При этом, когда порты USB заблокированы, 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 for HP ProtectTools (в прошлом LoJack Pro) (приобретается отдельно)

Computrace for HP ProtectTools (приобретается отдельно) — это служба для отслеживания местоположения украденного компьютера при выходе пользователя в Интернет. Computrace for HP ProtectTools также может использоваться для удаленного управления компьютерами, узнавания их расположения и отслеживания использования.

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 ProtectTools могут совместно использоваться для предоставления решений для различных проблем безопасности, включая следующие цели обеспечения безопасности:

- 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.
  - Security Manager for HP ProtectTools — см. HP ProtectTools Security Manager на стр. 29.
  - Drive Encryption for HP ProtectTools — см. Drive Encryption for HP ProtectTools (только на некоторых моделях) на стр. 46.
- 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 for HP ProtectTools — см. Обнаружение похищенных устройств (только на некоторых моделях) на стр. 67.

Ограничение доступа к секретным данным

Предположим, в вашем офисе работает контрактный аудитор, который получил доступ к компьютеру для проверки секретной финансовой информации; вам нужно сделать так, чтобы он не мог распечатать файлы или сохранить их компакт-диске или другом записываемом устройстве. Доступ к данным помогут ограничить следующие функции:

- Device Access Manager for HP ProtectTools позволяет менеджеру по информационным технологиям ограничить доступ к устройствам связи, чтобы секретную информацию невозможно было скопировать с жесткого диска. См. раздел Конфигурация класса устройств на стр. 57.

Предотвращение несанкционированного доступа из внутренних и внешних местоположений

Несанкционированный доступ к незащищенным рабочим компьютерам подвергает серьезной опасности корпоративные сетевые ресурсы, например, информацию о финансовых службах, данные администрации или отдела разработчиков, а также личные медицинские записи или финансовые отчеты. Для предотвращения несанкционированного доступа используются следующие функции:

- Включение функции проверки подлинности перед загрузкой ограничивает доступ к операционной системе.
  - Security Manager for HP ProtectTools — см. HP ProtectTools Security Manager на стр. 29.
  - Drive Encryption for HP ProtectTools — см. Drive Encryption for HP ProtectTools (только на некоторых моделях) на стр. 46.
- Security Manager помогает обеспечить невозможность получения несанкционированным пользователем паролей или доступа к приложениям, защищенным паролем. См. раздел HP ProtectTools Security Manager на стр. 29.
- Device Access Manager for HP ProtectTools позволяет менеджеру по информационным технологиям ограничить доступ к записываемым устройствам, чтобы секретную

информацию невозможно было скопировать с жесткого диска. См. раздел Device Access Manager for HP ProtectTools (только на некоторых моделях) на стр. 55.

Создание политик стойких паролей

Для компаний, которым требуется использование политики стойких паролей для десятков веб-приложений и баз данных, служба Security Manager предлагает защищенный репозиторий для паролей и удобную функцию единого входа. См. раздел HP ProtectTools Security Manager на стр. 29.

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 ProtectTools права и обязанности в области безопасности могут быть разделены на следующие роли:

- Начальник системы безопасности — устанавливает уровень безопасности компании или сети и определяет, какие службы безопасности внедрять в организации (например, Drive Encryption).

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

- Администратор службы информационных технологий — применяет службы безопасности, выбранные начальником системы безопасности, и управляет ими. Он также может включать и отключать некоторые функции. Например, если начальник системы безопасности решил внедрить смарт-карты, ИТ-администратор может разрешить как режим паролей, так и режим смарт-карт.

- Пользователь — использует службы безопасности. Например, если начальник системы безопасности и ИТ-администратор ввели в системе смарт-карты, пользователь может назначить PIN-код карты и использовать ее для аутентификации.

ПРЕДУПРЕЖДЕНИЕ. Администраторам рекомендуется использовать «оптимальные методы» при ограничении прав конечных пользователей и ограничении доступа пользователей.

Неавторизованным пользователям не должны предоставляться права администратора.

Управление паролями HP ProtectTools

Большинство функций HP ProtectTools Security Manager защищены паролями. В следующей таблице 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 ProtectTools	Установлен в следующем модуле	Функция
Пароль для входа в Windows	Панель управления Windows или HP ProtectTools Security Manager	Может использоваться для входа в систему вручную и для проверки подлинности для доступа к различным функциям Security Manager.
Пароль резервного копирования и восстановления Security Manager	Security Manager, для отдельных пользователей	Защита доступа к файлу резервного копирования и восстановления Security Manager.
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 посредине, 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.

Резервное копирование учетных данных и параметров

Можно выполнить резервное копирование учетных данных следующими способами.

- Использование Drive Encryption for HP ProtectTools для выбора и резервного копирования учетных данных HP ProtectTools.
- Использование инструмента резервного копирования и восстановления HP ProtectTools Security Manager в качестве центрального места для выполнения резервного копирования и восстановления учетных данных безопасности из одного из установленных модулей HP ProtectTools.

2 Приступая к работе

Для настройки параметров HP ProtectTools используйте мастер настройки HP Client Security или мастер настройки HP ProtectTools Security Manager.

По завершении работы с мастером настройки HP Client Security состояние приложения отображается на панели мониторинга HP Client Security.

Мастер настройки HP Client Security

ПРИМЕЧАНИЕ. Для администрирования HP ProtectTools требуются права администратора.

Мастер настройки HP Client Security помогает настроить наиболее часто используемые функции Security Manager. Если вы ранее не применяли мастер настройки HP Client Security, вы можете запустить мастер настройки HP Client Security одним из следующих способов:

- С экрана запуска щёлкните по приложению **HP Client Security** или коснитесь его.

  – или –

  С рабочего стола Windows щёлкните гаджет **HP ProtectTools** или коснитесь его.

Страницы отображаются в следующем порядке:

1. **Пароль Windows** — введите ваш пароль Windows.

   Этим вы обеспечите защиту вашей учётной записи Windows с использованием надёжной проверки подлинности.

2. Ключ **SpareKey** — для регистрации варианта с использованием SpareKey выберите три контрольных вопроса.

3. **Enroll fingerprints** (Регистрация отпечатков пальцев) — если установлен считыватель отпечатков пальцев и соответствующий драйвер, вы можете зарегистрировать отпечатки пальцев. Вы должны выбрать и зарегистрировать по крайней мере 2 отпечатка пальцев.

4. **Drive Encryption** — если установлена программа Drive Encryption for HP ProtectTools, вы можете активировать шифрование основного жёсткого диска:

   - Программное шифрование для обычного жёсткого диска
   - Аппаратное шифрование, если обнаружен диск с самошифрованием.

   До активации шифрования вы должны сохранить ключ шифрования на одном или нескольких из следующих устройств:

ПРИМЕЧАНИЕ. Если вы отмените мастер настройки в данный момент, вы не сможете активировать проверку подлинности Windows и Drive Encryption.

- **Съёмные носители**, такие как USB флэш-накопители формата FAT 32.
  - Этот вариант выбирается по умолчанию в случае определения единственного съёмного носителя до отображения страницы Drive Encryption.
  - Если определяются 2 или несколько съёмных носителей, выберите один из отображаемых носителей.
- **SkyDrive** — этот вариант доступен при определении подключения к Интернету.

  Требуется® идентификатор Windows Live ID. Введите ваш идентификатор и пароль или зарегистрируйтесь для их получения.

5. На странице «Finish» (Готово) отображается уведомление об успешности операции и вам предлагается перезагрузить компьютер для активации функции Drive Encryption.

Мастер настройки HP ProtectTools Security Manager

ПРИМЕЧАНИЕ. Для администрирования HP ProtectTools требуются права администратора.

Мастер настройки HP ProtectTools Security Manager — помощь при настройке параметров Security Manager. Помимо параметров мастера настройки, в консоли администрирования администраторы могут настраивать многочисленные дополнительные функции безопасности. Они применяются к компьютеру и всем пользователям, которые совместно его используют.

Для запуска мастера настройки HP ProtectTools Security Manager:

▲ Щёлкните **Мастер настройки** в левой панели консоли администрирования и следуйте инструкциям на экране до завершения настройки.

Администраторы могут запустить консоль администрирования с пользовательской консоли HP ProtectTools Security Manager. Подробнее см. раздел Консоль администрирования HP ProtectTools Security Manager на стр. 17.

Security Manager и ее приложения доступны всем пользователям, которые совместно используют данный компьютер.

Панель мониторинга HP Client Security

Если вы ранее выполнили настройку с использованием мастера настройки HP Client Security, для открытия HP Client Security выполните следующие действия:

▲ С пускового экрана наберите `hp`, затем выберите **HP Client Security**.

На панели мониторинга отображается краткий обзор функций и соответствующее состояние для каждого приложения.

▲ Для отображения дополнительной информации по выбранному приложению щёлкните по строке приложения или коснитесь её:

- Наличие кнопки **Настроить** указывает на то, что данное приложение ещё не настроено. Нажмите кнопку или коснитесь её, чтобы открыть страницу приложения для его настройки.
- **Параметры** указывает на приложение со статусом OK. Нажмите кнопку или коснитесь её для доступа к параметрам данного приложения.

- Для настройки пользователем запускается **Пользовательская консоль**.
- Для выполнения настроек, требующих прав администратора, запускается **Консоль администрирования**.
- После открытия консоли пользователя или консоли администрирования **Панель мониторинга состояния** остаётся открытой, и после выполнения настроек и закрытия консоли информация о состоянии обновляется.

3 Руководство по быстрой настройке для малых компаний

В этой главе демонстрируются основные действия по активации наиболее распространенных и полезных параметров HP ProtectTools для малых предприятий. Это программное обеспечение предоставляет множество инструментов и параметров, позволяющих точно настраивать предпочтения и управление доступом. В этом руководстве по быстрой настройке рассматривается быстрая и простая настройка каждого модуля. Для получения дополнительных сведений просто выберите нужный модуль и щелкните **?** или нажмите кнопку «Справка» в правом верхнем углу. Эта кнопка автоматически предоставит информацию о текущем отображающемся окне.

Приступая к работе

1. С рабочего стола Windows откройте HP ProtectTools Security Manager двойным щелчком по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.
2. Введите пароль Windows или создайте его.
3. Запустите мастер настройки и выполните указанные действия.

ПРИМЕЧАНИЕ. По умолчанию программа HP ProtectTools Security Manager настроена на политику надёжной проверки подлинности.

Этот параметр предназначен для защиты от несанкционированного доступа при входе в Windows и должен использоваться при необходимости повышенной защиты, если пользователи часто отходят от своих систем в течение дня. Если необходимо изменить этот параметр, щелкните вкладку «Политика сеанса» и выберите нужные параметры.

Чтобы настроить HP ProtectTools Security Manager на проверку подлинности только один раз при входе в Windows, выполните следующую процедуру.

1. С рабочего стола Windows откройте HP ProtectTools Security Manager двойным щелчком по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.
2. На левой панели щелкните **Администрирование** и затем щелкните **Консоль администрирования**.
3. На левой панели в разделе **Система** выберите **Проверка подлинности** из группы **Безопасность**.
4. Щелкните вкладку **Политика сеанса** и затем выберите требования к сочетанию данных для входа. Для отмены этого выбора щёлкните **Восстановить значения по умолчанию**.
5. По завершении нажмите кнопку **Применить**.

Password Manager

Пароли! Их у нас у всех немало – особенно если вы регулярно посещаете веб-сайты или используете приложения, требующие ввода данных для входа. Обычный пользователь либо использует один и тот же пароль для всех приложений и веб-сайтов, либо начинает применять

творческий подход к созданию паролей и быстро забывает, какой пароль придуман для какого приложения.

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.

ПРИМЕЧАНИЕ. Выделены области, которые будут использоваться Password Manager сейчас и для последующих посещений.

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 Password Manager, используйте один из следующих двух способов.

- Используйте сочетание клавиш ctrl+Windows+h, чтобы открыть Password Manager, затем щелкните **Открыть** для запуска и проверки подлинности сохраненного ярлыка.

  – или –

- Выберите **Управление** в диспетчере паролей для открытия HP ProtectTools Security Manager, чтобы изменить учетные данные.

Функция **Правка** диспетчера паролей позволяет вам просматривать и изменять имя, имя пользователя и даже показать пароли.

HP ProtectTools for Small Business позволяет выполнять резервное копирование и (или) копирование на другой компьютер всех учетных данных и параметров.

Device Access Manager for HP ProtectTools

Device Access Manager может использоваться для ограничения использования различных внешних и внутренних запоминающих устройств, чтобы ваши данные оставались защищенными на жестком диске и не покидали вашу организацию. Примером может служить предоставление доступа пользователей к данным, но запрет их копирования на компакт-диск,

музыкальный проигрыватель или USB-накопитель. Ниже приведен простой способ настройки этих ограничений.

1. С рабочего стола Windows откройте пользовательскую консоль HP ProtectTools Security Manager двойным щелчком по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.
2. На левой панели HP ProtectTools Security Manager выберите **Администрирование** и щелкните **Консоль администрирования**.
3. Щелкните **Device Access Manager** и затем щелкните **Конфигурация класса устройств**.
4. Далее необходимо выбрать пользователей, у которых останется доступ, а остальные останутся заблокированными.
5. Выберите аппаратные устройства для ограничения, затем нажмите кнопку **Применить** для завершения процесса.
6. Выберите **Добавить**, щёлкните **Расширенный** и затем щелкните **Поиск**.
7. Выберите желаемого пользователя и щелкните **OK > OK > Применить**.

   Ваш выбор отображается в окне **Пользователи/группы**.
8. Выберите **Класс устройств**, который будет использовать пользователь, выберите **Разрешить** или **Отказать**, и затем щелкните **Применить**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools используется для защиты данных путем шифрования всего жесткого диска. Данные на жестком диске останутся защищенными при хищении компьютера и/или в случае извлечения жесткого диска из исходного компьютера и его установки на другом компьютере.

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 множество программных модулей синхронизируют пароли автоматически, включая учетные записи пользователей Windows, домены, Drive Encryption for HP ProtectTools, Password Manager и HP ProtectTools Security Manager.

Используйте следующие простые шаги для активации Drive Encryption for HP ProtectTools.

1. С рабочего стола Windows откройте HP ProtectTools Security Manager двойным щелчком по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.
2. На левой панели щелкните **Администрирование** и затем щелкните **Консоль администрирования**.
3. На левой панели щелкните **Мастер настройки**.
4. Выберите **Далее** на экране приветствия.
5. Введите пароль Windows для запуска мастера активации, затем щелкните **Далее**.
6. Пропустите SpareKey, если это не требуется.
7. Установите флажок **Drive Encryption**, затем щелкните **Далее**.
8. Выберите диск для шифрования, затем щелкните **Далее**.

9. Окно настройки Drive Encryption запрашивает USB флэш-накопитель или другое внешнее устройство для хранения ключа восстановления зашифрованных данных. Обеспечьте безопасное и надёжное хранение этого ключа восстановления, поскольку он используется для восстановления данных или для доступа к диску в случае утери или ошибки пароля проверки подлинности перед загрузкой.
10. Щелкните **Далее**, завершите процесс, затем щелкните **Готово**. Извлеките флэш-накопитель USB, затем по готовности перезагрузите компьютер.
11. При запуске системы Drive Encryption запросит ввод пароля Windows. Введите пароль и нажмите кнопку **ОК**.

ПРИМЕЧАНИЕ. Во время шифрования диска работа компьютера может казаться замедленной. По завершении шифрования рабочие характеристики компьютера придут в норму. По мере доступа к данным на диске они шифруются или расшифровываются в соответствии с требованиями администратора.

Проверка подлинности Drive Encryption будет «передаваться по цепочке» через вход в Windows непосредственно на рабочий стол Windows, таким образом вам не потребуется вводить пароль дважды.

4 Консоль администрирования HP ProtectTools Security Manager

Программное обеспечение HP ProtectTools Security Manager предоставляет функции обеспечения безопасности, защищающие от несанкционированного доступа к компьютеру, сетям и критическим данным. Администрирование HP ProtectTools Security Manager обеспечивается благодаря функции консоли администрирования.

На пользовательской консоли Security Manager доступны дополнительные приложения (только на некоторых моделях), которые помогают в восстановлении компьютера при его утере или краже.

С помощью консоли администрирования локальный администратор может выполнять следующие задачи:

- Включение или отключение функций безопасности
- Ввод необходимых учетных данных для проверки подлинности
- Управление пользователями компьютера
- Настройка параметров, характерных для данного устройства
- Настройка установленных приложений Security Manager

Приступая к работе

Для настройки параметров HP ProtectTools используйте мастер настройки HP Client Security или мастер настройки HP ProtectTools Security Manager.

По завершении работы с мастером настройки HP Client Security состояние приложения отображается на панели мониторинга HP Client Security.

Мастер настройки HP Client Security

ПРИМЕЧАНИЕ. Для администрирования HP ProtectTools требуются права администратора.

Мастер настройки HP Client Security помогает настроить наиболее часто используемые функции Security Manager. Если вы ранее не применяли мастер настройки HP Client Security, вы можете запустить мастер настройки HP Client Security одним из следующих способов:

▲ С экрана запуска щёлкните по приложению **HP Client Security** или коснитесь его.

– или –

С рабочего стола Windows щёлкните гаджет **HP ProtectTools** или коснитесь его.

Страницы отображаются в следующем порядке:

1. **Пароль Windows** — введите ваш пароль Windows.

   Этим вы обеспечите защиту вашей учётной записи Windows с использованием надёжной проверки подлинности.

2. Ключ **SpareKey** — для регистрации варианта с использованием SpareKey выберите три контрольных вопроса.

3. **Enroll fingerprints** (Регистрация отпечатков пальцев) — если установлен считыватель отпечатков пальцев и соответствующий драйвер, вы можете зарегистрировать отпечатки пальцев. Вы должны выбрать и зарегистрировать по крайней мере 2 отпечатка пальцев.

4. **Drive Encryption** — если установлена программа Drive Encryption for HP ProtectTools, вы можете активировать шифрование основного жёсткого диска:

   - Программное шифрование для обычного жёсткого диска
   - Аппаратное шифрование, если обнаружен диск с самошифрованием.

   До активации шифрования вы должны сохранить ключ шифрования на одном или нескольких из следующих устройств:

   ПРИМЕЧАНИЕ. Если вы отмените мастер настройки в данный момент, вы не сможете активировать проверку подлинности Windows и Drive Encryption.

   - **Съёмные носители**, такие как USB флэш-накопители формата FAT 32.
     - Этот вариант выбирается по умолчанию в случае определения единственного съёмного носителя до отображения страницы Drive Encryption.
     - Если определяются 2 или несколько съёмных носителей, выберите один из отображаемых носителей.
   - **SkyDrive** — этот вариант доступен при определении подключения к Интернету.

     Требуется ® идентификатор Windows Live ID. Введите ваш идентификатор и пароль или зарегистрируйтесь для их получения.

5. На странице «Finish» (Готово) отображается уведомление об успешности операции и вам предлагается перезагрузить компьютер для активации функции Drive Encryption.

Мастер настройки HP ProtectTools Security Manager

ПРИМЕЧАНИЕ. Для администрирования HP ProtectTools требуются права администратора.

Мастер настройки HP ProtectTools Security Manager — помощь при настройке параметров Security Manager. Помимо параметров мастера настройки, в консоли администрирования администраторы могут настраивать многочисленные дополнительные функции безопасности. Они применяются к компьютеру и всем пользователям, которые совместно его используют.

Для запуска мастера настройки HP ProtectTools Security Manager:

▲ Щёлкните **Мастер настройки** в левой панели консоли администрирования и следуйте инструкциям на экране до завершения настройки.

Администраторы могут запустить консоль администрирования с пользовательской консоли HP ProtectTools Security Manager. Подробнее см. раздел Консоль администрирования HP ProtectTools Security Manager на стр. 17.

Security Manager и ее приложения доступны всем пользователям, которые совместно используют данный компьютер.

Панель мониторинга HP Client Security

Если вы ранее выполнили настройку с использованием мастера настройки HP Client Security, для открытия HP Client Security выполните следующие действия:

▲ С пускового экрана наберите `hp`, затем выберите **HP Client Security**.

На панели мониторинга отображается краткий обзор функций и соответствующее состояние для каждого приложения.

▲ Для отображения дополнительной информации по выбранному приложению щёлкните по строке приложения или коснитесь её:

- Наличие кнопки **Настроить** указывает на то, что данное приложение ещё не настроено. Нажмите кнопку или коснитесь её, чтобы открыть страницу приложения для его настройки.
- **Параметры** указывает на приложение со статусом ОК. Нажмите кнопку или коснитесь её для доступа к параметрам данного приложения.
- Для настройки пользователем запускается **Пользовательская консоль**.
- Для выполнения настроек, требующих прав администратора, запускается **Консоль администрирования**.
- После открытия консоли пользователя или консоли администрирования **Панель мониторинга состояния** остаётся открытой, и после выполнения настроек и закрытия консоли информация о состоянии обновляется.

Открытие консоли администрирования HP ProtectTools

Консоль администрирования HP ProtectTools используется для административных задач, таких как установка системных политик или настройка программного обеспечения. Доступ к консоли администрирования можно получить, открыв HP ProtectTools Security Manager:

1. С рабочего стола Windows выполните двойной щелчок по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.

   – или –

   С **панели управления** выберите **Система и безопасность** и затем выберите **HP ProtectTools Security Manager**.

2. На левой панели пользовательской консоли HP ProtectTools Security Manager выберите **Администрирование** и выберите **Консоль администрирования**.

Использование консоли администрирования

Консоль администрирования HP ProtectTools является центральным местоположением для управления функциями и приложениями HP ProtectTools Security Manager.

1. С рабочего стола Windows выполните двойной щелчок по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.

   – или –

   С **панели управления** выберите **Система и безопасность** и затем выберите **HP ProtectTools Security Manager**.

2. На левой панели пользовательской консоли HP ProtectTools Security Manager выберите **Администрирование** и выберите **Консоль администрирования**.

В Консоли администрирования отображаются следующие выбранные параметры в области «Главная страница» на левой панели.

- **Система** — выполняется настройка следующих функций безопасности и проверки подлинности для пользователей и устройств.
  - **Безопасность**
  - **Пользователи**
  - **Учетные данные**
- **Приложения** — позволяет настраивать параметры HP ProtectTools Security Manager и приложений Security Manager.
- **Данные** — позволяет настраивать параметры Drive Encryption (только на некоторых моделях).
- **Computer** (Компьютер) — позволяет настраивать параметры для Device Access Manager
- **Setup Wizard** (Мастер настройки) — помогает при настройке HP ProtectTools Security Manager.
- **О программе** — отображается информация о программе HP ProtectTools Security Manager (номер версии и сведения об авторских правах).
- **Рабочая область** — отображаются экраны приложений.

  ? — отображает справку Консоли администрирования. Данный значок расположен в правой верхней части рамки окна, рядом со значками сворачивания и развертывания.

Настройка системы

Доступ к группе **Система** можно получить через панель меню в левой части консоли администрирования HP ProtectTools. Можно использовать приложения данной группы для управления политиками и параметрами компьютера, его пользователями и устройствами.

Группа **Система** содержит следующие приложения.

- **Security** (Безопасность) — управление функциями, проверкой подлинности и параметрами, определяющее способ взаимодействия пользователей и компьютера.
- **Пользователи** — установка, управление и регистрация пользователей данного компьютера.
- **Учетные данные** — управление параметрами встроенных или подключенных к компьютеру устройств безопасности.

Настройка проверки подлинности на компьютере

Используя приложение проверки подлинности, вы можете установить политики для доступа к компьютеру. Можно указать учетные данные, которые будут запрашиваться при проверке подлинности каждого класса пользователей для входа в систему Windows, на веб-сайт или в программу в течение сеанса пользователя.

Для настройки проверки подлинности на компьютере выполните следующие действия.

1. На левой панели консоли администрирования выберите **Безопасность** и щелкните **Проверка подлинности**.
2. Для настройки проверки подлинности при входе в систему перейдите на вкладку **Политика входа**, внесите изменения и щелкните **Применить**.
3. Для настройки проверки подлинности сеанса перейдите на вкладку **Политика сеанса**, внесите изменения и щелкните **Применить**.

Политика входа

Для установки политик, определяющих учетные данные, которые запрашиваются при входе в систему Windows для проверки подлинности пользователя, выполните следующие действия.

1. На левой панели консоли администрирования выберите **Безопасность** и щелкните **Проверка подлинности**.
2. На вкладке **Logon Policy** (Политика входа) выберите категорию пользователя, напр., администраторы или обычные пользователи.
3. Щёлкните учетные данные для проверки подлинности для отображения диалогового окна редактирования.
4. Для требования сочетания двух учетных данных для проверки подлинности щелкните стрелку вниз для выбора учетных данных, затем щелкните **ОК**.
5. Для удаления учетных данных щелкните **X** или щелкните учетные данные правой кнопкой мыши, затем щелкните **Удалить**.
6. Щелкните **Да** в диалоговом окне конфигурации.
7. Для подтверждения возможности пользователей входа в систему щелкните **Проверка возможности входа HP ProtectTools**.
8. Чтобы восстановить исходные значения параметров, щелкните **Восстановить значения по умолчанию**.
9. Щелкните **Применить**.

Политика сеанса

Для установки политик, определяющих учетные данные, которые запрашиваются в течение сеанса Windows, выполните следующие действия:

1. На левой панели консоли администрирования выберите **Безопасность** и щелкните **Проверка подлинности**.
2. На вкладке **Политика сеанса** выберите категорию пользователя, напр., администраторы или обычные пользователи.
3. Щёлкните учетные данные для проверки подлинности для отображения диалогового окна редактирования.
4. Для требования сочетания двух учетных данных для проверки подлинности щелкните стрелку вниз для выбора учетных данных, затем щелкните **ОК**.
5. Для удаления учетных данных щелкните **X** или щелкните учетные данные правой кнопкой мыши, затем щелкните **Удалить**.
6. Щелкните **Да** в диалоговом окне конфигурации.
7. Для подтверждения возможности пользователей входа в систему щелкните **Проверка возможности входа HP ProtectTools**.
8. Чтобы восстановить исходные значения параметров, щелкните **Восстановить значения по умолчанию**.
9. Щелкните **Применить**.

Параметры

Чтобы разрешить пользователям этого компьютера пропускать вход в систему Windows, если проверка подлинности уже была выполнена на уровне BIOS или Drive Encryption, выполните следующие действия.

1. На левой панели консоли администрирования выберите **Безопасность** и щелкните **Параметры**.
2. **Разрешить одношаговый вход в систему** — установите флажок, чтобы разрешить одношаговый вход или снимите флажок, чтобы отключить его
3. Щелкните **Применить**.

Управление пользователями

С помощью приложения «Пользователи» вы можете контролировать и управлять пользователями HP ProtectTools данного компьютера.

Все пользователи HP ProtectTools записываются и проверяются в соответствии с политиками, установленными Security Manager, вне зависимости от того, зарегистрировали ли они необходимые учетные данные, которые позволяют соответствовать этим политикам, или нет.

Для управления пользователями выберите один из следующих параметров.

- Для добавления дополнительных пользователей щелкните **Добавить**.
- Для удаления пользователя выберите пользователя и щелкните **Удалить**.

- Для настройки дополнительных учетных данных пользователя выберите пользователя и щелкните **Зарегистрировать**.
- Для просмотра политик определенного пользователя выберите пользователя и просмотрите политики в нижнем окне.

Учетные данные

В приложении учетных данных можно настроить параметры, доступные для любого встроенного или подключенного устройства безопасности, которое распознается HP ProtectTools Security Manager.

SpareKey

Можно разрешить или запретить проверку подлинности SpareKey при входе в систему Windows и управлять контрольными вопросами, которые предлагаются пользователям во время регистрации SpareKey.

1. Выберите контрольные вопросы, которые предлагаются пользователям во время регистрации SpareKey.

   Можно определить до трех пользовательских вопросов или же позволить пользователям ввести собственную кодовую фразу.

2. Чтобы разрешить восстановление SpareKey для входа в Windows, установите флажок.
3. Щелкните **Применить**.

Отпечатки пальцев

Если в вашем компьютере имеется встроенный или внешний считыватель отпечатков пальцев, на странице «Отпечатки пальцев» отображаются следующие вкладки.

- **Регистрация** — выберите минимальное и максимальное количество отпечатков пальцев, которое пользователь сможет зарегистрировать.

  Также можно стереть все данные со считывателя отпечатков пальцев.

  ПРЕДУПРЕЖДЕНИЕ. Стирание всех данных из считывателя отпечатков пальцев приведет к удалению отпечатков пальцев всех пользователей, включая администраторов. Если политика входа в систему требует только отпечатки пальцев, всем пользователям может быть запрещен вход в систему компьютера.

- **Чувствительность** — чтобы настроить чувствительность устройства считывания отпечатков пальцев при считывании, передвиньте ползунок.

  Если отпечаток пальца систематически не считывается, возможно, необходимо установить более низкую чувствительность. 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.

- **Дополнительно** — выберите один из следующих параметров, чтобы настроить режим экономии энергии для считывателя отпечатков пальцев и улучшить визуальный отклик:

  - **Оптимизированный** — считыватель отпечатков пальцев активируется по запросу. При первом использовании считывателя может наблюдаться небольшая задержка реакции.
  - **Экономия энергии** — считыватель отпечатков пальцев отвечает медленнее, но для его использования требуется меньший расход энергии.
  - **Полная мощность** — считыватель отпечатков пальцев всегда готов к использованию, но при этом режиме затрачивается наибольший объем энергии.

Лицо

Если в вашем компьютере имеется встроенная или внешняя веб-камера, а также установлена программа Face Recognition, чтобы сбалансировать удобство использования компьютера и обеспечение его безопасности, администраторы могут настроить уровень безопасности для программы распознавания лица Face Recognition.

1. Щелкните **Учетные данные** и выберите **Лицо**.
2. Для большего удобства переместите ползунок влево, а для большей точности переместите ползунок вправо.

   - **Удобство** — переместите ползунок в положение «Удобство» для облегчения получения доступа зарегистрированными пользователями в критических ситуациях.
   - **Баланс** — переместите ползунок в положение «Баланс» для обеспечения баланса между безопасностью и удобством работы, или в случаях, когда на компьютере хранится важная информация или компьютер расположен в месте, где могут произойти попытки несанкционированного доступа.
   - **Точность** — переместите ползунок в положение «Точность», чтобы усложнить доступ пользователей, когда зарегистрированные сцены или освещение не соответствуют норме, а также для предотвращения ложной идентификации.

3. Чтобы восстановить исходные значения параметров, щелкните **Восстановить значения по умолчанию**.
4. Щелкните **Применить**.

Смарт-карта

Чтобы можно было использовать смарт-карту для проверки подлинности, администраторы должны инициализировать ее. Windows поддерживает большинство стандартных смарт-карт CSP и PKCS11.

Инициализация смарт-карты

HP ProtectTools Security Manager может поддерживать большое количество разных смарт-карт. Количество и тип символов, используемых в качестве PIN-кода, может отличаться. Производитель смарт-карты должен предоставить средства для установки сертификата и безопасности и управления PIN-кодом, который HP ProtectTools будет использовать в алгоритме безопасности.

ПРИМЕЧАНИЕ. Должно быть установлено программное обеспечение промежуточного слоя смарт-карты.

1. Получите и установите ПО промежуточного слоя для используемой смарт-карты (например, ActivClient 6.x для смарт-карты ActivIdentity).
2. Вставьте смарт-карту в устройство чтения.
3. Инициализация (форматирование) смарт-карты.
   a. Запустите средство инициализации смарт-карт, или оно может отобразиться при установке смарт-карты в устройство чтения.
   б. Следуйте инструкциям на экране для настройки ПИН-кода.
   в. Сохраните код разблокировки для последующего использования.
4. Создание пары ключей и сертификата.
   a. Запустите **Консоль администрирования HP ProtectTools**.
   б. Щелкните **Учетные данные**, щелкните **Смарт-карта**, затем щелкните вкладку **Администрирование**.
   в. Убедитесь, что выбрано **Инициализация смарт-карты**.
   г. Введите PIN-код, щелкните **Применить** и следуйте инструкциям на экране.

   После успешной инициализации смарт-карты необходимо ее зарегистрировать.

Регистрация смарт-карты

После инициализации смарт-карты администраторы могут зарегистрировать ее в качестве метода проверки подлинности на консоли администрирования HP ProtectTools:

1. Щелкните **Мастер настройки**.
2. На экране **приветствия** нажмите кнопку **Далее**.
3. Введите пароль Windows и щелкните **Далее**.
4. На странице **SpareKey** щелкните **Пропустить настройку SpareKey** (если только вы не хотите обновить сведения о SpareKey), затем щелкните **Далее**.

5. На странице **Включение средств безопасности** щелкните **Далее**.
6. На странице **Выберите учетные данные** убедитесь, что выбрано **Смарт-карта**, и щелкните **Далее**.
7. На странице **Смарт-карта** введите PIN-код и щелкните **Далее**.
8. Щелкните **Готово**.

Пользователи также могут зарегистрировать смарт-карту в пользовательской консоли Security Manager. Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager, щелкнув синий значок **?** в правой верхней части страницы «Смарт-карта».

Настройка смарт-карты

Если в вашем компьютере имеется встроенная или внешняя смарт-карта, страница «Смарт-карта» содержит две вкладки.

- **Параметры** — установите флажок **Блокировка компьютера при удалении смарт-карты** для настройки автоматической блокировки компьютера при извлечении смарт-карты, затем щелкните **Применить**.

ПРИМЕЧАНИЕ. Компьютер блокируется только в том случае, если смарт-карта использовалась в качестве учетных данных проверки подлинности при входе в систему Windows. При извлечении смарт-карты, которая не использовалась для входа в систему Windows, компьютер не блокируется.

- **Администрирование** — выберите один из следующих параметров:
  - **Инициализация смарт-карты** — подготовка смарт-карты для использования с HP Protect Tools. Если смарт-карта была ранее инициализирована не в HP ProtectTools (содержит асимметричную пару электронных ключей и соответствующий сертификат), нет необходимости инициализировать ее за исключением тех случаев, когда желательна инициализация с определенным сертификатом.
  - **Сменить PIN-код смарт-карты** — позволяет сменить PIN-код смарт-карты.
  - **Стереть только данные HP ProtectTools** — стирает только сертификат HP ProtectTools, созданный в процессе инициализации карты. Остальные данные на карте не стираются.
  - **Стереть все данные на смарт-карте** — стирает все данные на определенной смарт-карте. Карта больше не может использоваться с HP ProtectTools или любым другим приложением.

ПРИМЕЧАНИЕ. Функции, не поддерживаемые вашей смарт-картой или соответствующим ПО промежуточного слоя, недоступны.

▲ Щелкните **Применить**.

Бесконтактная карта

Бесконтактная карта – это небольшая пластиковая карта, содержащая компьютерную микросхему. Если на компьютере имеется устройство считывания бесконтактной карты, установлен соответствующий драйвер производителя и бесконтактная карта выбрана как

учетные данные для проверки подлинности, можно использовать бесконтактную карту для проверки подлинности. HP ProtectTools поддерживает следующие типы бесконтактных карт.

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

▲ Для настройки бесконтактной карты поднесите ее к устройству чтения, следуйте инструкциям на экране, а затем щелкните **Далее**.

Проксимити карта

Проксимити карта – это небольшая пластиковая карта, содержащая компьютерную микросхему. Если на компьютере имеется устройство считывания проксимити карты, установлен соответствующий драйвер производителя и проксимити карта выбрана как учетные данные для проверки подлинности, можно использовать проксимити карту совместно с другими учетными данными для обеспечения дополнительного уровня безопасности.

▲ Для настройки проксимити карты поднесите ее к устройству чтения, затем щелкните **Применить**.

Bluetooth

Если на компьютере имеется функция Bluetooth,® Bluetooth выбрано как учетные данные для проверки подлинности и телефон с функцией Bluetooth подключен к компьютеру, можно использовать телефон с функцией Bluetooth совместно с другими учетными данными для обеспечения дополнительного уровня безопасности. Укажите параметры Bluetooth.

▲ Чтобы разрешить автоматическую проверку подлинности, установите флажок, затем щелкните **Применить**.

ПИН-код

Если ПИН-код выбран как учетные данные проверки подлинности, можно использовать ПИН-код совместно с другими учетными данными для обеспечения дополнительного уровня безопасности. Укажите параметры ПИН-кода.

1. Нажмите клавишу со стрелкой вверх или вниз, чтобы выбрать минимальную длину ПИН-кода.

   Максимальное разрешенное число цифр — 8.

2. Нажмите **Применить**.

Приложения

На странице «Параметры» в области «Приложения» на левой панели Административной консоли находятся две вкладки, позволяющие настроить поведение текущих установленных приложений HP ProtectTools Security Manager.

▲ На левой панели консоли администрирования в разделе **Приложения** щелкните **Параметры**.

Вкладка «Общие сведения»

Приведенные ниже параметры доступны на вкладке **Общие сведения**.

- **Не запускать мастер настройки для администраторов автоматически** — выберите этот параметр, чтобы мастер настройки не запускался автоматически при входе в систему.
- **Не запускать мастер «Приступая к работе» для пользователей автоматически** — выберите этот параметр, чтобы пользовательская установка не запускалась автоматически при входе в систему.

1. Установите флажок, расположенный рядом с определенным параметром, для включения, или снимите его для отключения.
2. Нажмите **Применить**.

Вкладка приложений

Администраторы могут включать и отключать следующие приложения.

- **Состояние** — установите этот флажок, чтобы включить все приложения, или снимите его, чтобы отключить все приложения.
- **Диспетчер паролей** — включает диспетчер паролей для всех пользователей компьютера.

1. Установите флажок, расположенный рядом с определенным параметром, для включения, или снимите его для отключения.
2. Нажмите **Применить**.

Для восстановления заводских значений параметров всех приложений нажмите кнопку **Восстановление значений по умолчанию**.

Данные

Раздел «Данные» на левой панели Административной консоли позволяет настраивать параметры следующих приложений:

- **Drive Encryption** — настройка параметров и отображение состояния диска. Для получения дополнительных сведений см. справку о программном обеспечении Drive Encryption, щелкнув синий значок **?** в правой верхней части страницы Drive Encryption.

Компьютер

Раздел «Компьютер» на левой панели Административной консоли позволяет настраивать параметры приложения Device Access Manager.

- Простая конфигурация
- Конфигурация класса устройств
- Конфигурация своевременной проверки подлинности
- Дополнительные параметры

Дополнительные сведения см. в справке программного обеспечения Device Access Manager, щелкнув синий значок **?** в правой верхней части страницы Device Access Manager.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager позволяет существенно повысить уровень безопасности компьютера.

Можно использовать предварительно загруженные приложения Security Manager, а также дополнительные приложения, которые можно загрузить из Интернета прямо сейчас.

- Управление регистрационными именами и паролями.
- Простое изменение вашего пароля для операционной системы Windows®.
- Установка параметров программ.
- Использование отпечатков пальцев для дополнительной защиты и удобства.
- Регистрация одной или нескольких сцен для проверки подлинности.
- Настройка смарт-карты для проверки подлинности.
- Резервное копирование и восстановление программных данных.
- Добавление других программ.

Открытие Security Manager

Программу Security Manager можно открыть одним из следующих способов:

▲ С рабочего стола Windows выполните двойной щелчок по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.

– или –

С **панели управления** выберите **Система и безопасность** и затем выберите **HP ProtectTools Security Manager**.

Использование пользовательской консоли Security Manage

Пользовательская консоль Security Manager является центральным местоположением для простого доступа к функциям, приложениям и параметрам Security Manager. На пользовательской консоли отображаются следующие компоненты:

- **Идентификационная карта** — отображаются имя пользователя Windows и пиктограмма, определяющие учетную запись пользователя, вошедшего в систему.
- **Приложения безопасности** — отображается расширенное меню из ссылок для настройки следующих категорий безопасности:
  - **Начальная страница** — управление паролями, настройка учетных данных проверки подлинности или проверка состояния приложений безопасности.
  - **Обнаружение похищенных устройств** — Computrace for HP ProtectTools (приобретается отдельно)

- **Мои учетные записи** — управление учетными данными для проверки подлинности с Password Manager и Credential Manager.
- **Мои данные** — управление безопасностью данных с помощью программы Drive Encryption.

ПРИМЕЧАНИЕ. Эта функция не отображается если данное приложение не установлено.

- **Мой компьютер** — управление безопасностью компьютера с помощью программы Device Access Manager.

ПРИМЕЧАНИЕ. Эта функция не отображается если данное приложение не установлено.

- **Administration** (Администрирование) — предоставление администраторам доступа к **Консоли администрирования** для управления параметрами безопасности и пользователями.
- **Advanced** (Дополнительно) — отображение команд для доступа к дополнительным функциям, среди которых:
  - **Пользовательские параметры** — выполнение индивидуальных настроек Security Manager.
  - **Резервное копирование и восстановление** — выполнение резервного копирования и восстановления данных.
  - **О программе** — отображается информация о программе HP ProtectTools Security Manager (номер версии и сведения об авторских правах).
- **Рабочая область** — отображаются экраны приложений.
- **?** — отображает справку по пользовательской консоли Security Manager. Данный значок расположен в правой верхней части рамки окна, рядом со значками сворачивания и развертывания.

Ваша персональная идентификационная карта

Ваша идентификационная карта однозначно идентифицирует вас как владельца данной учетной записи Windows, отображая ваши выбранные имя и изображение. Она хорошо заметна в верхнем левом углу страниц Security Manager.

Вы можете изменить способ отображения своего имени. По умолчанию отображается ваше полное имя пользователя Windows и изображение, выбранное во время установки Windows.

Для изменения отображаемого имени выполните следующие действия.

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. Щелкните идентификационную карту в левом верхнем углу пользовательской консоли.
3. Щелкните окно с отображением имени пользователя Windows для данной учетной записи, введите новое имя и щелкните **Сохранить**.

Мои данные для входа

Приложения, включенные в эту группу, позволяют задавать различные параметры идентификационных данных.

- **Диспетчер паролей** — создание быстрых ссылок и управление ими. Быстрые ссылки позволяют открывать веб-сайты и запускать программы. Вход выполняется после проверки подлинности с помощью пароля Windows, отпечатков пальцев, лица, смарт-карты, проксимити карты, бесконтактной карты, телефона с функцией Bluetooth или ПИН-кода.
- **Диспетчер учётных данных** — предоставляет средства для простого изменения пароля Windows, регистрации отпечатков пальцев, регистрации лица и настройки смарт-карты, бесконтактной карты, проксимити карты, телефона с функцией Bluetooth или ПИН-кода.

Администраторы могут получать доступ к доступным дополнительным приложениям безопасности, щелкнув **Администрирование**, а затем **Централизованное управление** в левом нижнем углу панели управления.

Password Manager

Диспетчер паролей позволяет упростить вход в Windows, 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, лица, смарт-карты, проксимити карты, бесконтактной карты, ПИН-кода или пароля Windows.

Password Manager предоставляет следующие возможности:

Вкладка «Управление»

- Добавление, изменение или удаление регистрационных имен.
- Использование быстрых ссылок для запуска обозревателя по умолчанию и входа на веб-сайты или в программы после настройки диспетчера паролей.
- Перетаскивание быстрых ссылок для организации тематических разделов.
- Быстрая оценка любых паролей с точки зрения угроз безопасности.

Вкладка «Надежность пароля»

- Проверка надежности отдельных паролей, используемых для веб-сайтов и приложений, а также оценка общей надежности пароля.
- 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».

▲ Щелкните значок **Password Manager** для отображения контекстного меню, из которого можно выбрать следующие варианты.

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

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

В контекстном меню отображаются следующие элементы:

- **Добавить [somedomain.com] в список диспетчера паролей** — позволяет добавить учетную запись для текущего экрана входа.
- **Открыть диспетчер паролей** — запускает диспетчер паролей.
- **Параметры значка** — позволяет указать условия, при которых отображается значок диспетчера паролей.
- **Справка** — отображает справку Security Manager.

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 вводятся в поля данных для входа автоматически, после чего ввод подтверждается (если указано подтверждение создания или последнего изменения учетной записи).
- **Изменить учетную запись** — изменение учетной записи для данного веб-сайта.
- **Добавить учетную запись** — добавление учетной записи в диспетчер паролей.
- **Открыть диспетчер паролей** — запускает диспетчер паролей.
- **Справка** — отображает справку Security Manager.

ПРИМЕЧАНИЕ. Администратор этого компьютера может настроить Security Manager 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. Вы можете использовать эти учетные записи после выбора веб-сайта или программы. Можно также выбрать учетную запись из меню **Быстрый доступ к Password Manager**, и Password Manager откроет веб-сайт или программу и выполнит вход.

Чтобы добавить учетную запись, выполните следующие действия.

1. Откройте экран входа на веб-сайт или в программу.
2. Щелкните стрелку на значке **Диспетчер паролей**, затем выберите один из следующих вариантов в зависимости от того, относится ли входной экран к веб-сайту или к программе:
   - Для веб-сайта щелкните **Добавить [имя домена] в список диспетчера паролей**.
   - Для программы щелкните **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. Для открытия этого диалогового окна также можно щелкнуть **Добавить учетную запись** на вкладке

Управление Password Manager, используя сочетание клавиш ctrl+Windows+h или проведя отпечатком пальца.

а. Чтобы заполнить поле учетной записи предварительно заданной информацией, щелкайте стрелки справа от поля.

б. Для просмотра пароля данной учетной записи щелкните **Показать пароль**.

в. Чтобы заполнять поля учетной записи, но не подтверждать их, снимите флажок **Автоматически подтверждать данные учетной записи**.

г. Щелкните **ОК**, выберите метод проверки подлинности, который необходимо использовать (отпечатки пальцев, лицо, смарт-карта, проксимити карта, 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, щелкните **Дополнительные поля**.

- Установите этот флажок для каждого поля, которое требуется для учетной записи, или снимите этот флажок для полей, которые не требуются для учетной записи.
- Щелкните **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 на то, что можно использовать зарегистрированные учетные данные для входа в систему.

Изменение учетных записей

Для изменения учетной записи выполните следующие действия.

1. Откройте экран входа на веб-сайт или в программу.
2. Для открытия диалогового окна, в котором можно редактировать информацию учетной записи, щелкните стрелку на значке **Диспетчер паролей**, затем щелкните **Изменить учетную запись**. Поля учетной записи на экране и соответствующие им поля в диалоговом окне выделяются жирной оранжевой рамкой.

   Для открытия этого диалогового окна также можно щелкнуть **Изменить заданную учетную запись** на вкладке **Управление Password Manager**.
3. Измените сведения учетной записи.
   - Чтобы заполнить поле для входа в систему **Имя пользователя** с одним из предварительно заданных вариантов, щелкните стрелку вниз справа от поля.
   - Чтобы заполнить поле для входа в систему **Пароль** одним из предварительно заданных вариантов, щелкните стрелку вниз справа от поля.
   - Для добавления полей с экрана в учетную запись щелкните **Дополнительные поля**.
   - Для просмотра пароля данной учетной записи щелкните **Показать пароль**.
   - Чтобы заполнять поля учетной записи, но не подтверждать их, снимите флажок **Автоматически подтверждать данные учетной записи**.
4. Нажмите кнопку **ОК**.

Использование меню «Быстрый доступ к Password Manager»

Password Manager обеспечивает быстрый и простой доступ к веб-сайтам и программам, для которых созданы учетные записи. Дважды щелкните учетную запись программы или веб-сайта в меню **Быстрый доступ к Password Manager** или на вкладке **Управление** в Password Manager, чтобы открыть экран входа и заполнить данные учетной записи.

После создания учетной записи она автоматически добавляется в меню **Быстрые ссылки** в Password Manager.

Для отображения меню **Быстрые ссылки** выполните следующие действия.

1. Нажмите сочетание клавиш для **Диспетчера паролей** (заводской настройкой по умолчанию является ctrl+Windows +h). Чтобы изменить сочетание клавиш, на пользовательской консоли Security Manager дважды щелкните **Диспетчер паролей** и выберите **Параметры**.
2. Выполните сканирование отпечатков пальцев (на компьютере со встроенным или подключенным считывателем отпечатков пальцев) или введите пароль Windows.

Группировка учетных записей по категориям

Для систематизации учетных записей создайте одну или несколько категорий. Затем перетащите учетные записи в выбранные категории.

Для добавления категории выполните следующие действия.

1. На пользовательской консоли Security Manager щелкните **Диспетчер паролей**.
2. Щелкните вкладку **Управление** и нажмите **Добавить категорию**.
3. Введите имя категории.
4. Нажмите кнопку **ОК**.

Для добавления учетной записи в категорию выполните следующие действия.

1. Поместите указатель мыши над требуемой учетной записью.
2. Нажмите и удерживайте левую кнопку мыши.
3. Перетащите учетную запись в список категорий. Если указатель мыши находится над категорией, ее имя подсвечивается.
4. Отпустите кнопку мыши, если подсвечена требуемая категория.

Учетные записи не перемещаются в выбранную категорию, а только копируются туда. Вы можете добавить одну и ту же учетную запись в несколько категорий. Чтобы просмотреть все учетные записи, щелкните **Все**.

Управление учетными записями

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

Учетные записи перечислены на вкладке **Управление**. Если для входа на один и тот же веб-сайт создано несколько учетных записей, каждая такая запись отображается под именем веб-сайта и располагается с отступом вправо.

Для управления учетными записями выполните следующие действия.

▲ На пользовательской консоли Security Manager щелкните **Диспетчер паролей** и перейдите на вкладку **Управление**.

- **Добавление учетной записи** — щелкните **Добавить учетную запись** и следуйте инструкциям на экране.
- **Ваши учетные записи** — щелкните существующую учетную запись, выберите один из следующих параметров и следуйте инструкциям на экране:
  - **Открыть** — открывает веб-сайт или программу, для которых имеется учетная запись.
  - **Добавить** — добавляет учетную запись. Подробнее см. раздел Добавление учетных записей на стр. 32.
  - **Правка** — редактирование учетной записи. Подробнее см. раздел Изменение учетных записей на стр. 33.
  - **Удалить** — удаляет веб-сайт или программу, для которых имеется учетная запись.
- **Добавить категорию** — щелкните **Добавить категорию** и следуйте инструкциям на экране. Подробнее см. раздел Группировка учетных записей по категориям на стр. 34.

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

1. Откройте экран входа на веб-сайт или в программу.
2. Щелкните значок **Password Manager** для отображения его контекстного меню.
3. Щелкните **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.

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

На вкладке **Надежность пароля** красный, желтый и зеленый индикаторы состояния указывают надежность отдельных паролей, используемых для веб-сайтов и приложений, а также общую надежность пароля.

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. Щелкните значок и выберите **Параметры значка** для настройки метода обработки диспетчером паролей возможных веб-сайтов для входа.

   - **Предлагать добавлять учетные данные для экранов входа в систему** — щелкните этот параметр, чтобы диспетчер паролей 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.

     Для добавления учетной записи для ранее исключенного экрана выполните следующие действия.

     - Во время отображения учетной записи ранее исключенного веб-сайта или страницы программы откройте пользовательскую консоль Security Manager и щелкните **Диспетчер паролей**.
     - Щелкните **Добавить учетную запись**.

       Откроется диалоговое окно добавления учетной записи с указанием экрана входа на веб-сайт или программы в поле **Текущий экран**.
     - Щелкните **Продолжить**.

       Отображается экран «Добавить учетную запись в Password Manager».
     - Следуйте инструкциям на экране. Подробнее см. раздел Добавление учетных записей на стр. 32.
     - Значок **Password Manager** отображается при каждом открытии данного экрана входа на веб-сайт или в программу.

   Не отображать запросы на добавление данных для входа к экранам входа в систему — выберите переключатель.

2. Для доступа к дополнительным параметрам диспетчера паролей дважды щелкните **Диспетчер паролей** и на пользовательской консоли Security Manager нажмите **Параметры**.

Параметры

Можно задать параметры для индивидуальной настройки Password Manager:

1. **Предлагать добавлять учетные данные для экранов входа в систему** — когда определен экран входа на веб-сайт или в программу, значок диспетчера паролей отображается со знаком «плюс», показывая, что можно добавить учетную запись для этого экрана в меню **Учетные записи**. Чтобы отключить эту функцию, снимите флажок **Запрос на добавление данных для входа к экранам входа в систему**.
2. **Открывать диспетчер паролей сочетанием клавиш ctrl+win+h** — по умолчанию меню **Быстрый доступ к диспетчеру паролей** открывается сочетанием клавиш ctrl+Windows +h. Для изменения сочетания клавиш щелкните этот параметр, затем нажмите новое сочетание клавиш. Сочетания могут включать одну или несколько из следующих клавиш: ctrl, alt или shift, а также любую алфавитную или цифровую клавишу.
3. Щелкните **Применить**, чтобы сохранить изменения.

Credential Manager

Security Manager использует учетные данные для проверки подлинности пользователя. Администратор данного компьютера может указать, какие учетные данные могут использоваться для подтверждения ваших идентификационных данных при входе в Windows, на веб-сайты или в программы.

Доступные учетные данные могут различаться в зависимости от встроенных или подключенных к компьютеру устройств безопасности. Поддерживаемые учетные данные, требования и текущее состояние отображаются при щелчке **Credential Manager** в разделе **Мои учетные записи**. Могут отображаться следующие варианты:

- Пароль
- SpareKey
- Отпечатки пальцев
- Лицо
- Смарт-карта
- Бесконтактная карта
- Проксимити карта
- Bluetooth
- ПИН-код

Для регистрации или изменения учетных данных щелкните ссылку и следуйте инструкциям на экране.

Изменение пароля Windows

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

Чтобы изменить пароль Windows, выполните следующие действия.

1. На пользовательской панели Security Manager выберите **Диспетчер учетных данных** и щелкните **Пароль**.
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. Щелкните **Изменить**, чтобы немедленно заменить текущий пароль на введенный вами новый пароль.

Настройка SpareKey

SpareKey позволяет получать доступ к компьютеру (на поддерживаемых платформах) посредством ответа на три контрольных вопроса из списка, определенного администратором.

Во время первоначальной настройки в мастере «HP ProtectTools Security Manager» HP ProtectTools Security Manager запросит настройку персонального SpareKey.

Для настройки SpareKey выполните следующие действия.

1. На странице мастера SpareKey выберите три контрольных вопроса и введите ответ на каждый вопрос.
2. Щелкните **Создать**.

Выбрать другие вопросы или изменить ответы можно на странице SpareKey в **Credential Manager**.

После настройки SpareKey можно получать доступ к компьютеру, используя SpareKey с экрана входа в систему при предварительной загрузке или с экрана приветствия Windows.

Регистрация отпечатков пальцев

Если администратор выбрал «Отпечатки пальцев» на экране **Выберите учетные данные**, и в вашем компьютере имеется встроенное или внешнее устройство считывания отпечатков пальцев, мастер настройки HP ProtectTools Security Manager поможет вам настроить, или «зарегистрировать», отпечатки пальцев: Отпечатки пальцев также можно зарегистрировать на странице «Отпечатки пальцев» в **Диспетчере учетных данных** на пользовательской консоли Security Manager.

1. На странице мастера «Отпечатки пальцев» отображается контурный рисунок двух ладоней. Отпечатки пальцев, которые уже зарегистрированы, выделены подсветкой. Щелкните палец на контурном рисунке ладони.

ПРИМЕЧАНИЕ. Для удаления ранее зарегистрированного отпечатка пальца щелкните соответствующий палец.

2. Вам будет предлагаться считывание пальца, пока отпечаток пальца не будет успешно зарегистрирован. Зарегистрированный отпечаток пальца выделяется подсветкой на контурном рисунке.
3. Необходимо зарегистрировать, по крайней мере, два пальца. Предпочтительно зарегистрировать отпечатки указательного и среднего пальцев. Для регистрации отпечатков других пальцев повторите шаги 1 и 2.
4. Щелкните **Далее** и следуйте инструкциям на экране.

ПРЕДУПРЕЖДЕНИЕ. В процессе регистрации отпечатков пальцев с помощью мастера информация о них не сохранится, пока вы не щелкните **Далее**. Если вы ненадолго оставите компьютер в бездействии или закроете программу, внесенные изменения **не будут** сохранены.

Регистрация сцен для входа в систему с помощью лица

Если вы выбрали вход в систему при помощи функции распознавания лица, и если в вашем компьютере имеется встроенная или подключенная веб-камера, то мастер настройки HP ProtectTools Security Manager запросит настройку регистрации сцен. Сцены также можно зарегистрировать на странице «Вход в систему с помощью лица» в **Диспетчере учетных данных** на пользовательской консоли Security Manager.

Для использования входа в систему с помощью функции распознавания лица необходимо зарегистрировать одну или несколько сцен. После успешной регистрации можно также зарегистрировать новую сцену, если возникли трудности во время входа в систему, так как изменилось одно или несколько из следующих условий.

- Лицо значительно изменилось с последней регистрации.
- Освещение сильно отличается от освещения при предыдущих регистрациях.
- Вы носили (или нет) очки во время последней регистрации.

ПРИМЕЧАНИЕ. При возникновении проблем с регистрацией сцен попробуйте приблизиться к веб-камере.

Чтобы зарегистрировать новую сцену в мастере настройки HP ProtectTools Security Manager, выполните следующие действия:

1. На странице мастера «Вход в систему с помощью лица» щелкните **Дополнительно** и настройте дополнительные параметры. Подробнее см. раздел Дополнительные параметры пользователя на стр. 40.
2. Щелкните **ОК**.
3. Щелкните **Пуск** или, если сцены уже были зарегистрированы, щелкните **Зарегистрировать новую сцену**.
4. Во время регистрации сцены можно просмотреть демонстрацию, щёлкнув **Воспроизвести видео**.

   Если это первоначальная регистрация, появится диалоговое окно с запросом на просмотр демонстрации. Щелкните **Да** или **Нет**.
5. В условиях низкой освещенности программное обеспечение может автоматически увеличить яркость экрана. Щёлкните значок **Лампочка** для изменения освещения фона.
6. Щелкните значок **Камера** и следуйте инструкциям на экране.

   ПРИМЕЧАНИЕ. Во время съемки сцен обязательно смотрите в объектив, поворачивая голову соответствующим образом.
7. Щелкните **Далее**.

Также можно зарегистрировать сцены через пользовательскую консоль Security Manager:

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В разделе **Мои учетные записи** щелкните **Credential Manager**, а затем **Лицо**.
3. Щелкните **Дополнительно** для настройки дополнительных параметров. Подробнее см. раздел Дополнительные параметры пользователя на стр. 40.
4. Щелкните **ОК**.
5. Щелкните **Пуск** или, если сцены уже были зарегистрированы, щелкните **Зарегистрировать новую сцену**.
6. Если вам будет предложено указать пароль Windows, введите его и щелкните **Далее**.
7. Во время регистрации сцены можно просмотреть демонстрацию, щёлкнув **Воспроизвести видео**.

   Если это первоначальная регистрация, появится диалоговое окно с запросом на просмотр демонстрации. Выберите **Да** или **Нет**.
8. В условиях низкой освещенности программное обеспечение может автоматически увеличить яркость экрана. Щёлкните значок **Лампочка** для изменения освещения фона.
9. Щелкните значок **Камера** и следуйте инструкциям на экране.

   ПРИМЕЧАНИЕ. Во время съемки сцен обязательно смотрите в объектив, поворачивая голову соответствующим образом.

Для получения дополнительных сведений см. справку о программном обеспечении Face Recognition, щелкнув синий значок **?** в правой верхней части страницы «Регистрация лица».

Проверка подлинности

После регистрации одной или нескольких сцен можно использовать лицо для проверки подлинности при входе в компьютер или при запуске нового сеанса Windows.

1. После того, как запустится экран проверки подлинности и камера зафиксирует лицо, у пользователя есть 5 секунд для запуска процесса входа в систему. Если проверка подлинности пройдена успешно, вы получите доступ к компьютеру.
2. Если время, отведенное на вход при помощи функции распознавания лица, истекает, работа программы Face Recognition приостанавливается. Щелкните значок **Камера** для возобновления процесса проверки подлинности.

ПРИМЕЧАНИЕ. Если освещение недостаточное и вам не удается выполнить вход с помощью программы Face Recognition, вы можете ввести пароль Windows для входа в компьютер.

3. Если после входа в компьютер программа Face Recognition запрашивает добавление дополнительных сцен, чтобы упростить возможность входа в систему при следующих сеансах, щелкните **Да**.

Режим работы в темноте

При слабом уровне освещения во время процесса входа в систему при помощи функции распознавания лица цвет фона автоматически становится белым, чтобы обеспечить лучшее освещение лица.

Чтобы вручную переключить цвет фона для экрана входа при помощи функции распознавания лица, щелкните значок **Лампочка**.

Обучение

Если не удалось выполнить вход в систему при помощи функции распознавания лица, но пользователь ввел правильный пароль, может появиться запрос на сохранение набора изображений для повышения шансов на успешный вход в систему при помощи функции распознавания лица в будущем.

Удаление сцены

Для удаления зарегистрированной сцены выполните следующие действия.

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В разделе **Мои учетные записи** щелкните **Credential Manager**, а затем **Лицо**.
3. Щелкните сцену, которую необходимо удалить, а затем щелкните значок **Корзина**.
4. Щелкните **ОК** в диалоговом окне подтверждения.

Дополнительные параметры пользователя

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В разделе **Мои учетные записи** щелкните **Credential Manager** и выберите **Лицо**.

3. Щелкните **Дополнительно**, чтобы настроить следующие параметры:

   Вкладка **Другие параметры** — установите флажки, чтобы включить один или несколько из следующих параметров, либо снимите флажок, чтобы отключить параметр. Эти параметры применяются только к текущему пользователю.

   - **Воспроизведение звука при событии распознавания лица** — воспроизводит звук при успешном входе в систему с помощью функции распознавания лица или при его сбое.
   - **Prompt to update scenes when logon fails** (Запрос обновления сцен при ошибке входа в систему) — если не удалось выполнить вход в систему при помощи функции распознавания лица, но пользователь ввел правильный пароль, может появиться запрос на сохранение набора изображений для повышения шансов на успешный вход в систему при помощи функции распознавания лица в будущем.
   - **Запрос регистрации новой сцены при ошибке входа в систему** — если не удалось выполнить вход в систему при помощи функции распознавания лица, но пользователь ввел правильный пароль, может появиться запрос на регистрацию новой сцены для повышения шансов на успешный вход в систему при помощи функции распознавания лица в будущем.

4. Чтобы восстановить исходные значения параметров, щелкните **Восстановить значения по умолчанию**.

5. Щелкните **ОК**.

Настройка смарт-карты

Если в компьютере имеется встроенное или внешнее устройство чтения смарт-карт и администратор установил смарт-карту как учетные данные проверки подлинности и выполнил действия, описанные в справке программы Консоль администрирования HP ProtectTools, мастер настройки HP ProtectTools Security Manager запросит вставку и настройку смарт-карты. Смарт-карту также можно настроить на странице «Смарт-карта» в **Диспетчере учетных данных** на пользовательской консоли Security Manager.

ПРИМЕЧАНИЕ. Чтобы можно было использовать смарт-карту, администратор должен инициализировать ее.

Инициализация смарт-карты

HP ProtectTools Security Manager может поддерживать большое количество разных смарт-карт. Количество и тип символов, используемых в качестве PIN-кода, может различаться. Производитель смарт-карты должен предоставить средства для установки сертификата безопасности и управления PIN-кодом, который HP ProtectTools будет использовать в алгоритме безопасности.

Администраторы могут инициализировать смарт-карту с помощью программного обеспечения производителя и консоли администрирования HP ProtectTools. Дополнительные сведения см. в справке программного обеспечения консоли администрирования HP ProtectTools.

Регистрация смарт-карты

После инициализации смарт-карты пользователи могут зарегистрировать ее в Security Manager:

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.

2. Щелкните **Credential Manager** и далее **Смарт-карта**.

3. Убедитесь, что выбрано **Настройка**.
4. Введите пароль Windows и PIN-код и щелкните **Сохранить**.

Администраторы также могут зарегистрировать смарт-карту на консоли администрирования HP ProtectTools. Дополнительные сведения см. в справке программного обеспечения консоли администрирования HP ProtectTools.

Изменение PIN-кода смарт-карты

Чтобы изменить PIN-код смарт-карты, выполните следующие действия.

1. Вставьте отформатированную и инициализированную смарт-карту.
2. Выберите **Изменить PIN-код смарт-карты**.
3. Введите старый PIN-код, а затем введите и подтвердите новый PIN-код.

Бесконтактная карта

Бесконтактная карта – это небольшая пластиковая карта, содержащая компьютерную микросхему. Если на компьютере имеется устройство считывания бесконтактной карты, администратор установил соответствующий драйвер производителя и установил бесконтактную карту в качестве учетных данных проверки подлинности, бесконтактную карту можно использовать в качестве учетных данных проверки подлинности. HP ProtectTools поддерживает следующие типы бесконтактных карт.

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

▲ Для настройки бесконтактной карты поднесите ее к устройству чтения, следуйте инструкциям на экране, а затем щелкните **Применить**.

Проксимити карта

Проксимити карта – это небольшая пластиковая карта, содержащая компьютерную микросхему. Если на компьютере имеется устройство считывания проксимити карты, администратор установил соответствующий драйвер производителя и установил проксимити карту в качестве учетных данных проверки подлинности, проксимити карту можно использовать совместно с другими учетными данными для обеспечения дополнительного уровня безопасности.

▲ Для настройки проксимити карты поднесите ее очень близко к устройству чтения, следуйте инструкциям на экране, а затем щелкните **Применить**.

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 щелкните **Регистрация**.
3. Щелкните **ОК** в диалоговом окне подтверждения.

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 настроить новый ПИН-код, введите его, а затем повторите ввод для подтверждения.

Администрирование

Администраторы могут получить доступ к консоли администрирования и централизованному управлению, щёлкнув **Администрирование** и затем выбрав **Консоль администрирования** в левой нижней панели пользовательской консоли HP ProtectTools Security Manager.

Дополнительные сведения см. в справке программного обеспечения консоли администрирования HP ProtectTools.

Дополнительно

Доступ к следующим параметрам можно получить, щелкнув **Дополнительно** в нижней левой части пользовательской консоли:

- **Пользовательские параметры** — выполнение индивидуальных настроек Security Manager.
- **Резервное копирование и восстановление** — позволяет выполнять резервное копирование и восстановление данных Security Manager.
- **О программе** — отображается информация о версии Security Manager

Настройка пользовательских параметров

Вы можете задать параметры для индивидуальной настройки HP ProtectTools Security Manager. На пользовательской консоли Security Manager выберите **Дополнительно** и затем щёлкните **Пользовательские параметры**. Доступные параметры отображаются на двух вкладках: **Общие параметры** и **Отпечаток пальца**.

Вкладка «Общие»

Внешний вид — Показать значок в области уведомлений панели задач

- Чтобы включить отображение значка на панели задач, установите этот флажок.
- Чтобы отключить отображение значка на панели задач, снимите этот флажок.

Вкладка «Отпечатки пальцев»

ПРИМЕЧАНИЕ. Вкладка **Отпечатки пальцев** доступна только в случае, если на компьютере имеется считыватель отпечатков пальцев, и установлен правильный драйвер.

- **Быстрые действия** — используйте быстрые действия для выбора задачи Security Manager, которая будет выполняться при удержании определенной клавиши во время считывания отпечатков пальцев.

  Чтобы назначить быстрое действие одной из перечисленных клавиш, щелкните параметр **(клавиша) + отпечаток пальца** и выберите в меню одну из доступных задач.

- **Звуковой сигнал при сканировании отпечатка пальца** — отображается, только если доступно устройство считывания отпечатков пальцев. Используйте этот параметр для настройки обратной связи в процессе считывания отпечатков пальцев.

  - **Включить звуковой сигнал** — по окончании процесса считывания отпечатков пальцев Security Manager воспроизводит звуки, соответствующие определенным событиям. Можно назначить этим событиям новые звуки, выбрав их на вкладке **Звуки** в параметрах «Звук» на панели управления Windows, также можно отключить звуковой сигнал, сняв этот флажок.
  - **Отображать обратную связь качества сканирования**

    Установите этот флажок, чтобы отображались все результаты сканирования вне зависимости от их качества.

    Снимите этот флажок, чтобы отображались результаты сканирования только хорошего качества.

Резервное копирование и восстановление данных

Рекомендуется создавать резервные копии данных Security Manager на регулярной основе. Частота 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 копирует только данные программ Password Manager и Face Recognition. Drive Encryption имеет независимый способ резервного копирования. Отсутствуют резервные копии данных Device Access Manager и информации проверки подлинности по отпечатку пальца.

Для приема копии данных перед их восстановлением сначала необходимо установить на соответствующем компьютере HP ProtectTools Security Manager.

Для создания резервной копии данных выполните следующие действия.

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В левой части пользовательской консоли щелкните **Дополнительно** и выберите **Резервное копирование и восстановление**.
3. Щелкните **Резервное копирование данных**.
4. Выберите модули, которые нужно включить в резервную копию. В большинстве случаев выбираются все модули.
5. Подтвердите идентификационные данные.
6. Введите имя файла хранения. По умолчанию файл сохраняется в папке «Документы». Чтобы указать другое местоположение, щелкните **Обзор**.

7. Введите пароль для защиты файла.
8. Щелкните **Готово**.

Для восстановления данных выполните следующие действия.

1. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В левой части пользовательской консоли щелкните **Дополнительно** и выберите **Резервное копирование и восстановление**.
3. Щелкните **Восстановление данных**.
4. Выберите ранее созданный файл хранения. Введите путь в имеющееся поле или щелкните **Обзор**.
5. Введите пароль, используемый для защиты файла.
6. Выберите модули, данные которых нужно восстановить. В большинстве случаев выбираются все перечисленные модули.
7. Подтвердите пароль Windows.
8. Щелкните **Готово**.

6 Drive Encryption for HP ProtectTools (только на некоторых моделях)

Drive Encryption for HP ProtectTools обеспечивает полную защиту данных путем шифрования данных компьютера. При активации Drive Encryption необходимо зарегистрироваться на экране входа Drive Encryption, который отображается до ® запуска операционной системы Windows.

HP ProtectTools Security Manager (мастер настройки HP Client Security, Advanced Setup Wizard (расширенный мастер настройки) или консоль администрирования) позволяет администраторам Windows активировать Drive Encryption, выполнять резервное копирование ключа шифрования, выбирать диски или разделы для шифрования и отменять выбор. Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager.

Программа Drive Encryption позволяет выполнять следующие задачи.

- Настройка параметров Drive Encryption.
  - Активация пароля с защитой TPM
  - 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 программе шифрования диска Drive Encryption, открыв пользовательскую консоль HP ProtectTools Security Manager.

1. С рабочего стола Windows выполните двойной щелчок по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.

   – или –

   С **панели управления** выберите **Система и безопасность** и затем выберите **HP ProtectTools Security Manager**.

2. На левой панели пользовательской консоли HP ProtectTools Security Manager выберите **Administration** (Администрирование) и выберите **Administrative Console** (Консоль администрирования).

3. На левой панели консоли администрирования HP ProtectTools выберите **Drive Encryption**.

Общие задачи

Активация Drive Encryption для стандартных жестких дисков

Шифрование стандартных жестких дисков выполняется с помощью шифрования программного обеспечения. Для активации Drive Encryption выполните следующие действия.

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.

2. В левой панели щёлкните **мастер настройки**.

3. Установите флажок **Drive Encryption**, затем щелкните **Далее**.

4. Для резервного копирования ключа шифрования подключите внешнее устройство, чтобы записать на него этот ключ. Данный ключ должен использоваться для доступа к данным в случае безуспешности использования других методов.

5. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для запоминающего устройства, на котором необходимо сохранить ключ шифрования.

6. Щелкните **Далее**.

ПРИМЕЧАНИЕ. Появится запрос на перезагрузку компьютера. После перезагрузки отобразится 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.

Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager.

Активация Drive Encryption для дисков с функцией самошифрования данных

Диски с функцией самошифрования данных, соответствующие требованиям спецификации OPAL организации TCG к управлению дисками с функцией самошифрования, могут шифроваться как с помощью шифрования программного обеспечения, так и с помощью

аппаратного шифрования. Чтобы активировать Drive Encryption для дисков с функцией самошифрования данных, выполните следующие действия.

ПРИМЕЧАНИЕ. Аппаратное шифрование доступно, только если ВСЕ диски компьютера являются дисками с самошифрованием и соответствуют требованиям спецификации OPAL организации TCG к управлению дисками с функцией самошифрования. В этом случае доступен параметр **Использовать аппаратное шифрование диска**, и можно использовать программное или аппаратное шифрование.

Если компьютер оборудован и дисками с самошифрованием, и стандартными дисками, параметр **Использовать аппаратное шифрование диска** недоступен, можно использовать только программное шифрование. Подробнее см. раздел Активация Drive Encryption для стандартных жестких дисков на стр. 47.

- Используйте мастер настройки HP ProtectTools Security Manager для активации программы Drive Encryption.

– или –

Шифрование программного обеспечения

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.
2. В левой панели щёлкните **мастер настройки**.
3. Установите флажок **Drive Encryption**, затем щелкните **Далее**.

   ПРИМЕЧАНИЕ. Если внизу экрана доступен параметр **Использовать аппаратное шифрование диска**, снимите флажок.

4. В разделе **Диски для шифрования** установите флажок для жесткого диска, который необходимо зашифровать, затем щелкните **Далее**.
5. Чтобы выполнить резервное копирование ключа шифрования, вставьте запоминающее устройство в соответствующее гнездо.
6. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для запоминающего устройства, на котором необходимо сохранить ключ шифрования.
7. Щелкните **Применить**.

   ПРИМЕЧАНИЕ. Компьютер перезагрузится.

   Программа Drive Encryption успешно активирована. Шифрование диска может занимать несколько часов, в зависимости от размера диска.

Аппаратное шифрование

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.
2. В левой панели щёлкните **мастер настройки**.
3. Установите флажок **Drive Encryption**, затем щелкните **Далее**.
4. Если внизу экрана доступен флажок **Использовать аппаратное шифрование диска**, он должен быть установлен.

   Если флажок снят или недоступен, применяется программное шифрование Подробнее см. раздел Активация Drive Encryption для стандартных жестких дисков на стр. 47.

5. В разделе **Диски для шифрования** установите флажок для жесткого диска, который необходимо зашифровать, затем щелкните **Далее**.

ПРИМЕЧАНИЕ. Если отображается всего один диск, флажок установлен автоматически и недоступен для редактирования.

Если отображается более одного диска, диск 0 также будет установлен автоматически и недоступен для редактирования, но параметр для выбора дополнительных жестких дисков для аппаратного шифрования станет доступным.

Кнопка **Далее** недоступна, если не выбран по крайней мере один диск.

6. Чтобы выполнить резервное копирование ключа шифрования, вставьте запоминающее устройство в соответствующее гнездо.
7. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для запоминающего устройства, на котором необходимо сохранить ключ шифрования.
8. Щелкните **Применить**.

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

Программа Drive Encryption успешно активирована. Шифрование диска может занять несколько минут.

Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager.

Деактивация программы Drive Encryption

Администраторы могут использовать мастер установки HP ProtectTools Security Manager для деактивации программы Drive Encryption. Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager.

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.
2. В левой панели щёлкните **мастер настройки**.
3. Снимите флажок **Drive Encryption**, затем щелкните **Далее**.

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 предоставляет параметр **Отключить режим сна для повышения безопасности**, предотвращающий переход в режим сна или ожидания.

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

ПРИМЕЧАНИЕ. Если администратор Windows включил функцию защиты перед загрузкой в программе HP ProtectTools Security Manager и One-Step Logon включен (по умолчанию), вход в систему может быть выполнен немедленно после проверки подлинности перед загрузкой без необходимости повторной проверки подлинности на экране входа в программу Drive Encryption.

Вход одного пользователя:

- На странице **Вход в систему** введите пароль Windows, PIN-код смарт-карты, ключ SpareKey, выполните вход с помощью функции распознавания лица или же проведите зарегистрированным пальцем.

Вход нескольких пользователей:

1. На экране **Выберите пользователя для входа** выберите пользователя для входа в раскрывающемся списке, затем щелкните **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

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (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.

Защитите данные путем шифрования жесткого диска

Настоятельно рекомендуется использовать мастер настройки HP ProtectTools Security Manager для защиты данных путем шифрования жесткого диска. После активации жесткие диски или разделы могут быть зашифрованы с помощью следующих действий.

1. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
2. Щелкните **Параметры**.
3. 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)

Страница «Управление шифрованием» в Drive Encryption позволяет администраторам просматривать и изменять состояние Drive Encryption (оно может быть включено, неактивно, или может быть активным аппаратное шифрование), а также просматривать состояние шифрования всех жестких дисков компьютера.

ПРИМЕЧАНИЕ. Для аппаратного шифрования на странице параметров Drive Encryption могут быть выбраны только дополнительные жесткие диски, или можно отменить их выбор.

- Если отображается состояние «Отключено», Drive Encryption еще не активировано администратором Windows и не защищает жесткий диск. Используйте мастер настройки HP ProtectTools Security Manager для активации программы Drive Encryption.
- Если состояние шифрования – «Включено», программа Drive Encryption активирована и настроена. Диск находится в одном из следующих состояний.

Шифрование программного обеспечения

- Не зашифрован
- Зашифрован
- Выполняется шифрование
- Выполняется расшифровка

Аппаратное шифрование

- Зашифрован
- Не зашифровано (для дополнительных дисков)

Использование улучшенной безопасности с TPM (только на некоторых моделях)

Если активирован доверенный платформенный модуль (TPM) и выбрана функция улучшенной безопасности Drive Encryption Enhanced Security with TPM (шифрование диска с TPM), пароль шифрования диска будет защищен микросхемой безопасности TPM. При извлечении жесткого диска и его установки на другом компьютере доступ к нему будет запрещен.

ПРЕДУПРЕЖДЕНИЕ. Владение TPM не передается консоли Windows TPM.msc.

ПРИМЕЧАНИЕ. Поскольку пароль защищен микросхемой безопасности TPM, при переносе жесткого диска на другой компьютер данные становятся доступны только при переносе параметров TPM на этот же компьютер.

ПРИМЕЧАНИЕ. Параметр TPM должен быть включен в BIOS Setup.

Шифрование и расшифровка отдельных разделов дисков (только программное шифрование)

Администраторы могут использовать страницу «Параметры» Drive Encryption для шифрования одного или нескольких разделов жестких дисков на компьютере или расшифровки уже зашифрованных разделов дисков.

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.
2. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
3. Щелкните **Параметры**.
4. В окне **Состояние диска** установите или снимите флажки для дисков, которые требуется зашифровать или расшифровать, затем щелкните **Применить**.

ПРИМЕЧАНИЕ. При шифровании или расшифровке раздела в строке выполнения отображается ход выполнения шифрования в процентах или оставшееся время для завершения процесса.

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.

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.

ПРИМЕЧАНИЕ. Для сохранения ключа шифрования необходимо использовать запоминающее устройство USB формата FAT32 или FAT16. Для резервного копирования могут использоваться карты памяти Memory Stick USB, карты памяти Secure Digital (SD) или MultiMedia Card (MMC).

1. Запустите **Консоль администрирования HP ProtectTools**. Подробнее см. раздел Открытие консоли администрирования HP ProtectTools на стр. 19.
2. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
3. Щелкните **Резервное копирование ключей шифрования**.

4. Вставьте запоминающее устройство, которое использовалось для резервного копирования ключа шифрования.

ПРИМЕЧАНИЕ. Для сохранения ключа шифрования необходимо использовать запоминающее устройство USB формата FAT32. Для резервного копирования могут использоваться карты памяти Memory Stick USB, карты памяти Secure Digital (SD) или MultiMedia Card (MMC). В некоторых случаях может использоваться SkyDrive.

5. В разделе **Устройство** установите флажок для запоминающего устройства, на котором требуется сохранить ключ шифрования.
6. Щелкните **Резервные ключи**.
7. Прочитайте информацию, отображающуюся на следующей странице, и щелкните **ОК**. Ключ шифрования сохраняется на выбранном запоминающем устройстве.

Восстановление доступа к активированному компьютеру с помощью резервных ключей

Администраторы могут выполнять восстановление, используя ключ Drive Encryption, созданный на съемном запоминающем устройстве во время активации, или путем выбора параметра **Резервное копирование ключей Drive Encryption** в Security Manager.

1. Установите съемное запоминающее устройство с резервным ключом.
2. Включите компьютер.
3. После открытия диалогового окна входа Drive Encryption for HP ProtectTools щелкните **Параметры**.
4. Выберите **Восстановление**.
5. Введите путь к файлу или имя файла, содержащего резервный ключ, затем щелкните **Восстановить**.

   – или –

   Щелкните **Обзор** для поиска нужного файла резервного копирования, щелкните **ОК**, а затем **Восстановить**.
6. При появлении диалогового окна подтверждения щелкните **ОК**.

   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 в программе Drive encryption перед загрузкой требует правильного ответа на секретные вопросы для доступа к компьютеру. Дополнительные сведения о настройке восстановления ключа SpareKey см. в справке программного обеспечения Security Manager.

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

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

   ПРИМЕЧАНИЕ. Если SpareKey не инициализирован в Security Manager, кнопка **SpareKey** недоступна.

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.

Отображение состояния шифрования

Пользователи могут отображать состояние шифрования из программы HP ProtectTools Security Manager.

ПРИМЕЧАНИЕ. Администраторы могут изменять состояние Drive Encryption с помощью консоли администрирования HP ProtectTools.

1. Запустите **Пользовательскую консоль HP ProtectTools**. Подробнее см. раздел Открытие Security Manager на стр. 29.
2. В разделе **Мои данные** щелкните **Drive Encryption**.

   При программном или аппаратном шифровании отображается одно из следующих состояний шифрования диска.

   - Включено
   - Отключено

   При программном шифровании состояние шифрования диска отображается как одно из следующего для каждого жесткого диска или раздела жесткого диска.

   - Не зашифрован
   - Зашифровано
   - Шифрование
   - Расшифровка

   При аппаратном шифровании отображается одно из следующих состояний шифрования диска.

   - Не зашифрован
   - Зашифровано

   При выполнении шифрования или расшифровки диска в строке выполнения отображается ход выполнения в процентах и оставшееся время выполнения шифрования или расшифровки.

7 Device Access Manager for HP ProtectTools (только на некоторых моделях)

Программа HP ProtectTools 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. 65.

Администраторы операционной системы Windows® используют программу HP ProtectTools Device Access Manager для управления доступом к устройствам системы и защиты от несанкционированного доступа:

- Профили устройств создаются для каждого пользователя, чтобы определить устройства, доступ к которым разрешен или не разрешен для этого пользователя.
- Своевременная проверка подлинности (JITA) позволяет предопределенным пользователям осуществлять собственную проверку подлинности для получения доступа к устройствам, которые в других случаях выдают отказ.
- Администраторы и надежные пользователи могут быть исключены из списка на ограничение на доступ к устройству, наложенное программой Device Access Manager, путем их добавления в группу администраторов устройств. Принадлежностью к группе можно управлять с помощью дополнительных параметров.
- Доступ к устройствам может предоставляться или запрещаться, исходя из принадлежности к группе, либо для конкретных пользователей.
- Для устройств таких классов как дисководы компакт-дисков и дисков DVD доступ для чтения и доступ для записи может предоставляться или запрещаться отдельно.

Открытие программы Device Access Manager

1. Войдите в систему в качестве администратора.
2. Запустите **HP ProtectTools Security Manager** с панели мониторинга **HP Client Security**.

   – или –

   С рабочего стола Windows выполните двойной щелчок по значку **HP ProtectTools** в области уведомлений в правом углу панели задач.

   – или –

   С **панели управления** выберите **Система и безопасность** и затем выберите **HP ProtectTools Security Manager**.

3. На левой панели пользовательской консоли HP ProtectTools Security Manager выберите **Administration** (Администрирование) и выберите **Administrative Console** (Консоль администрирования).

4. В левой панели консоли администрирования щёлкните **Device Access Manager**.

Обычный пользователь может просматривать политику HP ProtectTools Device Access Manager с помощью HP ProtectTools Security Manager. Данная консоль обеспечивает просмотр «только для чтения».

Процедуры настройки

Настройка доступа к устройствам

Программа HP ProtectTools Device Access Manager предлагает четыре представления:

- **Простая конфигурация** — разрешает или запрещает доступ к классам устройств, исходя из принадлежности к группе администраторов устройств.
- **Конфигурация класса устройств** — разрешает или запрещает доступ к типам устройств или определенным устройствам для определенных пользователей или групп.
- JITA — настраивает своевременную проверку подлинности (JITA), разрешая выбранным пользователям доступ к дисководам DVD/CD-ROM или съемным носителям посредством собственной проверки подлинности.
- **Дополнительные параметры** — настраивает список буквенных обозначений дисков, для которых программа Device Access Manager не будет ограничивать доступ, например C или системный диск. Из данного представления также можно управлять вхождением в группу администраторов устройств.

Простая конфигурация

Администраторы могут использовать представление **Простая конфигурация** для разрешения или запрещения прав доступа к следующим классам устройств для всех пользователей, не являющихся администраторами устройств:

- Все съемные носители (дискеты, флэш-накопители USB и т. д.)
- Все DVD-устройства/дисководы компакт-дисков
- Все последовательные и параллельные порты
- Все устройства Bluetooth

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

- Все модемы
- Все устройства PCMCIA/ExpressCard
- Все устройства 1394

Для разрешения или запрещения доступа к классу устройств для всех пользователей, не являющихся администраторами устройств, выполните следующие действия:

1. На левой панели Консоли администрирования HP ProtectTools щелкните **Device Access Manager** и **Простая конфигурация**.
2. На правой панели для запрещения доступа установите флажок напротив класса устройств или определенного устройства. Снимите флажок для разрешения доступа к классу устройств или определенному устройству.

   Если поле флажка недоступно, значения, оказывающие влияние на сценарий доступа, изменены в представлении **Конфигурация класса устройств**. Для возврата заводских значений щелкните **Сброс** в представлении **Конфигурация класса устройств**.
3. Нажмите **Применить**.

   ПРИМЕЧАНИЕ. Если фоновая служба не работает, откроется диалоговое окно, в котором будет предложено запустить ее. Щелкните **Да**.
4. Нажмите **OK**.

Запуск фоновой службы

При первом определении и применении новой политики автоматически запускается фоновая служба HP ProtectTools Device Locking/Auditing, и задается ее автоматический запуск при каждой загрузке системы.

ПРИМЕЧАНИЕ. Профиль устройств необходимо определить до того, как на экране появится запрос фоновой службы.

Кроме того, администраторы могут запускать или останавливать эту службу.

При остановке службы Device Locking/Auditing блокировка устройств не прекращается. Блокировка устройств осуществляется двумя компонентами:

- Служба Device Locking/Auditing
- Драйвер DAMDrv.sys

При запуске службы запускается драйвер устройств, но при остановке службы остановка драйвера не происходит.

Чтобы определить, работает ли фоновая служба, откройте окно командной строки и напечатайте `sc query flcdlock`.

Чтобы определить, работает ли драйвер устройства, откройте окно командной строки и напечатайте `sc query damdrv`.

Конфигурация класса устройств

Администраторы могут просматривать и изменять списки пользователей и групп, которым разрешен или запрещен доступ к классам устройств или определенным устройствам.

В представлении **Конфигурация класса устройств** содержатся следующие разделы:

- **Device List** (Список устройств) — отображаются все классы устройств и устройства, которые установлены на систему или могли быть установлены на систему ранее.
  - Защита обычно применяется к классу устройств. Выбранный пользователь или группа смогут осуществлять доступ к любому устройству, принадлежащему к классу устройств.
  - Защита может также применяться к определенным устройствам.
- **User List** (Список пользователей) — отображает всех пользователей и группы, которым разрешен или запрещен доступ к выбранному классу устройств или определенному устройству.
  - Запись в списке пользователей может быть сделана для определенного пользователя или для группы, к которой принадлежит пользователь.
  - Если запись пользователя или группы в списке пользователей отсутствует, параметр был унаследован от класса устройств в списке устройств или от папки класса.
  - Управление некоторыми классами устройств, например DVD-устройствами и дисководами компакт-дисков может в последствии осуществляться посредством разрешения или запрещения доступа отдельно для операций чтения и записи.

    В отношении других устройств или классов права доступа для чтения и записи могут быть унаследованы. Например, доступ для чтения может быть унаследован от более высокого класса, но доступ на запись может быть отдельно запрещен для пользователя или группы.

    ПРИМЕЧАНИЕ. Если флажок **Чтение** не установлен, запись управления доступом не распространяется на доступ к устройству для чтения, но доступ для чтения не запрещен.

    ПРИМЕЧАНИЕ. Группа администраторов не может быть добавлена к списку пользователей. Вместо этого используйте группу администраторов устройств.

    Пример 1 — если пользователю или группе отказано в доступе для записи к устройству или классу устройств:

    Тому же пользователю, той же группе или члену той же группы может предоставляться доступ для записи или доступ для чтения и записи только к устройству ниже этого устройства в иерархии устройств.

    Пример 2 — если пользователю или группе разрешен доступ для записи к устройству или классу устройств:

    Тому же пользователю, той же группе или члену той же группы может быть запрещен доступ для записи или доступ для чтения и записи только к тому же устройству или устройству ниже этого устройства в иерархии устройств.

    Пример 3 — если пользователю или группе разрешен доступ для чтения к устройству или классу устройств:

    Тому же пользователю, той же группе или члену той же группы может быть запрещен доступ для чтения или доступ для чтения и записи только к тому же устройству или устройству ниже этого устройства в иерархии устройств.

    Пример 4 — если пользователю или группе запрещен доступ для чтения к устройству или классу устройств:

Тому же пользователю, той же группе или члену той же группы может предоставляться доступ или доступ для чтения и записи только к устройству ниже этого устройства в иерархии устройств.

Пример 5 — если пользователю или группе разрешен доступ для чтения и записи к устройству или классу устройств:

Тому же пользователю, той же группе или члену той же группы может быть запрещен доступ для записи или доступ для чтения и записи только к тому же устройству или устройству ниже этого устройства в иерархии устройств.

Пример 6 — если пользователю или группе отказано в доступе для чтения и записи к устройству или классу устройств:

Тому же пользователю, той же группе или члену той же группы может предоставляться доступ для чтения или доступ для чтения и записи только к устройству ниже этого устройства в иерархии устройств.

Запрещение доступа для пользователя или группы

Чтобы не допустить доступ пользователя или группы к устройству или классу устройств, выполните следующие действия.

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. В списке устройств щелкните класс устройств, параметры которого необходимо настроить.
   - **Класс устройств**
   - **Все устройства**
   - **Отдельное устройство**
3. Под заголовком **Пользователь/группы** щелкните пользователя или группу, которой необходимо запретить доступ, и затем щелкните **Запретить**.
4. Щелкните **Применить**.

ПРИМЕЧАНИЕ. Если для пользователя на одном уровне установлены параметры запрета и разрешения, запрет доступа имеет приоритет над разрешением доступа.

Разрешение доступа для пользователя или группы

Чтобы предоставить доступ к устройству или классу устройств пользователю или группе, выполните следующие действия.

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. В списке устройств щелкните один из следующих элементов:
   - **Класс устройств**
   - **Все устройства**
   - **Отдельное устройство**
3. Щелкните **Добавить**.

   Откроется диалоговое окно **Выбор пользователей или групп**.

4. Щелкните **Дополнительно** и затем **Поиск**, чтобы найти пользователей или группы для добавления.
5. Щелкните пользователя или группу, которую необходимо добавить к списку доступных пользователей или групп и затем щелкните **ОК**.
6. Щелкните **ОК** повторно.
7. Щелкните **Разрешить**, чтобы предоставить этому пользователю доступ.
8. Щелкните **Применить**.

Разрешение доступа к классу устройств для одного пользователя из группы

Чтобы разрешить пользователю доступ к классу устройств, запретив доступ для всех остальных членов группы, к которой принадлежит пользователь, выполните следующие действия.

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. В списке устройств щелкните класс устройств, параметры которого необходимо настроить.
   - **Класс устройств**
   - **Все устройства**
   - **Отдельное устройство**
3. Под заголовком **Пользователь/группы** выберите группу, которой необходимо запретить доступ, и затем щелкните **Запретить**.
4. Перейдите к папке, которая находится ниже требуемого класса, и затем добавьте определенного пользователя.
5. Щелкните **Разрешить**, чтобы предоставить этому пользователю доступ.
6. Щелкните **Применить**.

Разрешение доступа к определенному устройству для одного пользователя из группы

Администраторы могут разрешать доступ к определенному устройству, запретив доступ для всех остальных членов группы, к которой принадлежит пользователь (для всех устройств класса):

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. В списке устройств щелкните класс устройств, параметры которого необходимо настроить, и затем перейдите к папке, которая находится ниже него.
3. Под заголовком **Пользователь/Группы** щелкните **Разрешить** рядом с группой, которой необходимо предоставить доступ.
4. Щелкните **Запретить** рядом с группой, которой необходимо запретить доступ.
5. Перейдите к определенному устройству, доступ к которому необходимо разрешить для пользователя в списке устройств.
6. Щелкните **Добавить**.

   Откроется диалоговое окно **Выбор пользователей или групп**.

7. Щелкните **Дополнительно** и затем **Поиск**, чтобы найти пользователей или группы для добавления.
8. Щелкните пользователя, которому необходимо предоставить доступ, и затем щелкните **ОК**.
9. Щелкните **Разрешить**, чтобы предоставить этому пользователю доступ.
10. Щелкните **Применить**.

Удаление параметров для пользователя или группы

Чтобы удалить доступ к устройству или классу устройств пользователю или группе выполните следующие действия:

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. В списке устройств щелкните класс устройств, параметры которого необходимо настроить.
   - **Класс устройств**
   - **Все устройства**
   - **Отдельное устройство**
3. Под заголовком **Пользователь/группы** щелкните пользователя или группу, которую необходимо удалить и затем щелкните **Удалить**.
4. Щелкните **Применить**.

Сброс конфигурации

ПРЕДУПРЕЖДЕНИЕ. При сбросе конфигурации происходит отмена всех изменений, внесенных в конфигурацию устройств, и возвращение заводских значений всех параметров.

ПРИМЕЧАНИЕ. Не выполнен сброс страницы «Дополнительные параметры».

Чтобы вернуть заводские значения всех параметров конфигурации, выполните следующие действия.

1. На левой панели консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация класса устройств**.
2. Щелкните **Сброс**.
3. При появлении запроса на подтверждение щелкните **Да**.
4. Щелкните **Применить**.

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 со включенной JITA смогут иметь доступ к некоторыми устройствам, политики которых, созданные в представлениях **Конфигурация класса устройств** или **Простая конфигурация**, были ограничены.

- **Сценарий** — политика простой конфигурации настроена на запрет любой попытки доступа к дисководу DVD/CD-ROM пользователем без прав администратора устройств.
- **Результат** — пользователь со включенной JITA, пытающийся получить доступ к дисководу DVD/CD-ROM, получает сообщение «Доступ запрещен» так же, как и пользователь без доступа JITA. Затем отображается сообщение в облаке, запрашивающее подтверждение на получение доступа JITA. При щелчке облака отображается диалоговое окно проверки подлинности пользователя. После успешного ввода пользователем учетных данных предоставляется доступ к дисководу DVD/CD-ROM.

Период JITA может иметь разрешение на определенное количество минут или 0 минут. Период JITA, равный 0 минут, не истекает. Пользователи будут иметь доступ к устройству с момента проверки подлинности и до момента выхода из системы.

Период JITA также может быть продлен при условии настройки данной функции. В данном сценарии за 1 минуту до истечения периода JITA пользователи могут щелкнуть запрос на продление доступа без повторной проверки подлинности.

Вне зависимости от того, ограничен или нет период JITA, 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 доступны для следующих классов устройств:

- Дисководы DVD/CD-ROM
- Съемные носители

Создание JITA для пользователя или группы

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

1. На левой панели Консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация JITA**.
2. В раскрывающемся меню устройства выберите **Съемные носители** или **Дисководы DVD/CD-ROM**.
3. Щелкните **Запретить**, чтобы добавить пользователя или группу в конфигурацию JITA.
4. Установите флажок **Включено**.
5. Установите необходимый период JITA.
6. Щелкните **Применить**.

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

Создание продлеваемой JITA для пользователя или группы

Администраторы могут разрешать пользователям или группам доступ к устройствам, используя своевременную проверку подлинности, которая может быть продлена пользователем до истечения срока ее действия.

1. На левой панели Консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация JITA**.
2. В раскрывающемся меню устройства выберите **Съемные носители** или **Дисководы DVD/CD-ROM**.
3. Щелкните **+**, чтобы добавить пользователя или группу в конфигурацию JITA.
4. Установите флажок **Включено**.
5. Установите необходимый период JITA.
6. Установите флажок **Расширяемая**.
7. Щелкните **Применить**.

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

Отключение JITA для пользователя или группы

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

1. На левой панели Консоли администрирования HP ProtectTools щелкните **Device Access Manager** и затем **Конфигурация JITA**.
2. В раскрывающемся меню устройства выберите **Съемные носители** или **Дисководы DVD/CD-ROM**.
3. Выберите пользователя или группу, чью JITA необходимо отключить.
4. Снимите флажок **Включено**.
5. Щелкните **Применить**.

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

Дополнительные параметры

Дополнительные параметры обеспечивают следующие функции:

- Управление группой администраторов устройств
- Управление буквенными обозначениями дисков, к которым программа Device Access Manager всегда разрешает доступ.

Группа администраторов устройств используется для исключения надежных пользователей (надежных для разрешения доступа к устройствам) из списка на ограничение, наложенное политикой Device Access Manager. К надежным пользователям обычно относятся системные администраторы. Подробнее см. раздел Группа администраторов устройств на стр. 64.

Представление **Дополнительные параметры** также позволяет администратору настраивать список буквенных обозначений дисков, к которым программа Device Access Manager не будет ограничивать доступ ни для одного пользователя.

ПРИМЕЧАНИЕ. При настройке списка буквенных обозначений дисков должны быть запущены фоновые службы Device Access Manager.

Чтобы запустить эти службы, выполните следующие действия.

1. Примените политику простой конфигурации, например, запрет любой попытки доступа к съемным носителям пользователем без прав администратора устройств.

   – или –

   Откройте окно командной строки с правами администратора и введите:

   ```
   sc start flcdlock
   ```

   Нажмите клавишу enter.

2. После запуска служб список дисков может быть изменен. Введите буквенные обозначения устройств, которыми не должна управлять программа Device Access Manager.

   Буквенные обозначения дисков отображаются для физических жестких дисков или разделов.

   ПРИМЕЧАНИЕ. Вне зависимости от нахождения системного диска (обычно C) в данном списке, доступ к нему всегда разрешен для любого пользователя.

Группа администраторов устройств

При установке программы Device Access Manager создается группа администраторов устройств.

Группа администраторов устройств используется для исключения надежных пользователей (надежных для разрешения доступа к устройствам) из списка на ограничение, наложенное политикой Device Access Manager. К надежным пользователям обычно относятся системные администраторы.

ПРИМЕЧАНИЕ. Добавление пользователя к группе администраторов устройств не означает автоматическое разрешение доступа к устройствам для этого пользователя. В представлении **Конфигурация класса устройств** при отказе группе пользователей в доступе к устройству, группе администраторов устройств должен быть разрешен доступ, чтобы участники этой группы имели доступ к устройству. Однако представление **Простая конфигурация** может использоваться для отказа в доступе к классам устройств для всех пользователей, не являющихся членами группы администраторов устройств.

Чтобы добавить пользователя к группе администраторов устройств, выполните следующие действия.

1. В представлении **Дополнительные параметры** щелкните **+**.
2. Введите имя надежного пользователя.
3. Щелкните **OK**.
4. Щелкните **Применить**.

Поддержка устройств eSATA

Чтобы программа Device Access Manager осуществляла контроль устройств eSATA, необходимо выполнить следующие настройки:

1. При запуске системы диск должен быть подключен.
2. С помощью представления **Дополнительные параметры** убедитесь, что буквенное обозначение диска eSATA отсутствует в списке дисков, к которым программа Device Access Manager разрешает доступ. Если буквенное обозначение диска eSATA в списке присутствует, удалите его, а затем щелкните **Применить**.
3. Контроль устройства может осуществляться с помощью класса устройств на съемных носителях, используя представление **Простая конфигурация** или **Конфигурация класса устройств**.

Неуправляемые классы устройств

Программа HP ProtectTools Device Access Manager не управляет следующими классами устройств:

- Устройства ввода/вывода
  - Биометрические устройства
  - Мышь
  - Клавиатура
  - Принтер
  - Принтеры «Plug and play» (PnP)
  - Обновление принтера
  - Инфракрасные устройства интерфейса пользователя
  - Устройство чтения смарт-карт
  - Последовательный мульти-порт
  - Дисковод
  - Контроллер гибкого диска (FDC)
  - Контроллер жесткого диска (HDC)
  - Класс устройств интерфейса пользователя (HID)
- Питание
  - Батарея
  - Дополнительная поддержка управления питанием (APM)
- Разное
  - Компьютер
  - Декодер
  - Дисплей
  - Процессор
  - Система

- Неизвестно
- Объем
- Снимок объема
- Устройства безопасности
- Ускоритель операций по безопасности
- Единый драйвер дисплея Intel®
- Драйвер носителя
- Устройство для смены носителя
- Многофункциональные устройства
- Legacard
- Сетевой клиент
- Сетевая служба
- Сетевой перенос
- Адаптер SCSI

8 Обнаружение похищенных устройств (только на некоторых моделях)

Computrace for HP ProtectTools (приобретается отдельно) используется для удаленного отслеживания, управления и нахождения компьютера.

После активации настройка Computrace for HP ProtectTools выполняется в центре поддержки пользователей Absolute Software. В центре поддержки администратор может настроить Computrace for HP ProtectTools для наблюдения за своим компьютером или управления им. Если систему будет украдена или перемещена в другое место, центр поддержки поможет правоохранительным органам найти и вернуть компьютер. После настройки Computrace продолжит работу даже в случае очистки или замены жесткого диска.

Активация Computrace for HP ProtectTools.

1. Выполните подключение к Интернету.
2. Откройте пользовательскую консоль Security Manager. Подробнее см. раздел Открытие Security Manager на стр. 29.
3. На левой панели Security Manager щелкните **Обнаружение похищенных устройств**.
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.

▲ Для получения дополнительных сведений о программ Computrace for HP ProtectTools нажмите **Подробнее**.

9 Ограничения локализованных паролей

На уровнях проверки безопасности перед загрузкой и HP Drive Encryption поддержка локализации пароля ограничена, как описано в следующих разделах.

Что делать при отклонении пароля

Пароли могут отклоняться по следующим причинам.

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

  1. Используя **панель управления**, добавьте поддерживаемую раскладку клавиатуры (добавьте клавиатуры США для языка вода «Китайский»).
  2. Установите поддерживаемые клавиатуры для языка ввода по умолчанию.
  3. Перезапустите программу HP ProtectTools, затем снова введите пароль.

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

  1. Измените пароль Windows, чтобы в нем содержались только поддерживаемые символы. Дополнительные сведения о неподдерживаемых символах см. в справке программного обеспечения консоли администрирования HP ProtectTools.
  2. Снова запустите мастер настройки HP ProtectTools Security Manager, затем введите новый пароль Windows.

На уровнях проверки безопасности перед загрузкой и HP 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.

На уровнях проверки безопасности перед загрузкой и HP Drive Encryption IME не поддерживаются. Пароль Windows нельзя ввести с помощью IME во время проверки безопасности перед загрузкой или на экране входа HP Drive Encryption, 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 ProtectTools поддерживает эту конфигурацию.

ВНИМАНИЕ! При развертывании программы HP ProtectTools 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)», после чего 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 завершится ошибкой, если пользователь использует символы второй раскладки, отсутствующие в изначальной (например, ē).

ПРИМЕЧАНИЕ. Администраторы могут решить эту проблему с помощью функции управления пользователями HP ProtectTools, удалив пользователя из программы HP ProtectTools, выбрав нужную раскладку клавиатуры в операционной системе и снова запустив мастер настройки Security Manager для этого 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, хотя 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 перед загрузкой BIOS 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 перед загрузкой BIOS и в HP Drive Encryption этот пароль необходимо вводить с нажатой клавишей alt справа для нижнего регистра и клавишей alt справа вместе с клавишей caps lock для верхнего регистра.

- Неподдерживаемые символы перечислены в следующей таблице.

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, а é с нажатой клавишей caps lock – Ç, È, À, и É в Windows.	ç, è, à, а é с нажатой клавишей caps lock – ç, è, à, и é при проверке безопасности перед загрузкой BIOS.	ç, è, à, а 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

Язык	Windows	BIOS	Drive Encryption
Чешский	◦ Клавиша ğ отклоняется. ◦ Клавиша į отклоняется. ◦ Клавиша ų отклоняется. ◦ Клавиши ė, ı и ż отклоняются. ◦ Клавиши ģ, ķ, ļ, ņ и ţ отклоняются.	нет	нет
Словацкий	Клавиша ż отклоняется.	◦ Клавиши š, ś и ş отклоняются при вводе с клавиатуры, но принимаются при вводе с программной клавиатуры. ◦ Мертвая клавиша ţ выводит два символа.	нет
Венгерский	Клавиша ż отклоняется.	Клавиша ţ выводит два символа.	нет
Словенский	Клавиша żŻ отклоняется в Windows, клавиша alt создаёт мертвую клавишу в BIOS.	úКлавиши , Ú, ů, Ů, ş, Ş, ś, Ś, š, и Š отклоняются в BIOS.	нет
Японский	Лучше использовать Microsoft Office 2007 IME, если он доступен. Несмотря на название IME в действительности это поддерживаемая раскладка клавиатуры 411.	нет	нет

Глоссарий

администратор
См. *Администратор Windows*.

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

активация
Задача, которую необходимо выполнить для доступа к функциям Drive Encryption (Шифрование дисков). Модуль Drive Encryption (Шифрование дисков) активируется в мастере установки HP ProtectTools. Активация модуля шифрования дисков доступна только администратору. В действия по активации входят активация программы, шифрование диска, создание учетной записи пользователя и создание на съемном запоминающем устройстве первоначальной копии ключа шифрования резервной копии.

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

биометрия
Категория учетных данных для проверки подлинности, которая использует для идентификации пользователя физические характеристики, например отпечаток пальца.

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 Security Manager, содержащий имя пользователя и пароль (а также, возможно, другую выбранную информацию), который может использоваться для доступа к веб-узлам 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.

Консоль администрирования
Центральное местоположение для доступа администраторов и управления функциями и параметрами в HP ProtectTools.

криптография

Практика шифрования и расшифровки данных таким образом, чтобы их могли расшифровать только определенные лица.

Микросхема встроенной системы безопасности Trusted Platform Module (TPM)
Общее обозначение микросхемы встроенной системы безопасности HP ProtectTools. TPM авторизует компьютер, а не пользователя, сохраняя информацию данной хостовой системы, например, ключи шифрования, цифровые сертификаты и пароли. TPM минимизирует риск утечки данных с компьютера при физическом похищении или атаке внешнего хакера.

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 с помощью которой можно использовать Security Manager для доступа к Интернету и приложениям Windows, для которых требуется ввод пароля.

отпечаток пальца
Цифровое представление отпечатка пальца пользователя. Фактическое изображение отпечатка пальца никогда не сохраняется в Security Manager.

пароль отзыва
Пароль, создаваемый при запросе пользователем цифрового сертификата. Этот пароль требуется, когда пользователю необходимо отозвать свой цифровой сертификат. Таким образом только пользователь может отозвать сертификат.

перезагрузка
Процесс перезапуска компьютера.

ПИН-код
Личный идентификационный номер.

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.

поставщик криптографических услуг
Поставщик или библиотека криптографических алгоритмов, которые используются в правильно определенных интерфейсах для выполнения некоторых криптографических функций.

проверка подлинности
Процесс выяснения, разрешено ли пользователю выполнять определенные задачи, например, иметь доступ к компьютеру, изменять настройки определенных программ или просматривать защищенные данные.

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.

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.

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

смарт-карта
Небольшой предмет, по форме и размеру похожий на кредитную карту, на котором хранится информация, идентифицирующая владельца. Используется для авторизации владельца компьютером.

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

удостоверение
В программе HP ProtectTools Security Manager совокупность учетных данных и настроек, которая воспринимается как учетная запись или профиль определенного пользователя.

учетная запись Windows
Профиль пользователя, который имеет право доступа к сети или определенному компьютеру.

учетные данные
Средства, с помощью которых пользователь подтверждает право на выполнение определенных задач в процессе проверки подлинности.

фоновая служба
Фоновая служба HP ProtectTools Device Locking/Auditing, которая должна работать для того, чтобы политики управления доступом к устройствам могли применяться. Она находится на панели управления в приложении «Службы» под параметром администрирование. Если фоновая служба не работает, программа HP ProtectTools Security Manager будет пытаться запустить ее при применении политик управления доступом к устройствам.

фоновая сцена
Изображение зарегистрированного пользователя для проверки подлинности.

центр сертификации (CA)
Служба, выдающая сертификаты, которые требуются для инфраструктуры открытых ключей.

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)
Экран входа, отображаемый до запуска Windows. Пользователи должны вводить имена пользователя Windows и пароли или PIN-коды смарт-карт. В большинстве случаев ввод верных сведений на экране входа Drive Encryption предоставляет доступ непосредственно к Windows без необходимости повторного входа на экране входа Windows.

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.

JITA
Своевременная проверка подлинности.

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

SATA device mode (Режим устройств SATA)
Режим передачи данных между компьютером и запоминающими устройствами, такими как жесткие и оптические диски.

TXT
Технология доверенного исполнения (Trusted Execution Technology).

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

Указатель

J

P

S

T

U

W