HP ProtectTools

Начало работы

Первая редакция: январь 2011 г.

Номер документа: 638391-251

Содержание

1 Безопасность: введение

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 (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.
HP ProtectTools Security Manager (для пользователей)	• Позволяет пользователям настраивать параметры, заданные администратором. • Позволяет администраторам предоставлять пользователям ограниченное управление некоторыми модулями HP ProtectTools.

Набор доступных программных модулей может отличаться в зависимости от модели компьютера.

Программные модули HP ProtectTools могут быть предустановлены, предварительно загружены или доступны для загрузки на веб-сайте HP. Дополнительную информацию см. в разделе http://www.hp.com.

ПРИМЕЧАНИЕ. В данном руководстве предполагается, что применимые модули программного обеспечения HP ProtectTools уже установлены.

Функции HP ProtectTools

В следующей таблице приведены основные функции модулей HP ProtectTools.

Модуль	Ключевые функции
Консоль администрирования HP ProtectTools (для администраторов)	• Установка и настройка уровней безопасности и способов защищенного входа с помощью мастера настройки Security Manager. • Настройка параметров, скрытых от пользователей. • Настройка доступа пользователей и параметров Device Access Manager. • Добавление и удаление пользователей HP ProtectTools и просмотр состояния пользователей с помощью средств администратора.
HP ProtectTools Security Manager (для пользователей)	• Упорядочивание, настройка и изменение паролей. • Настройка и изменение учетных данных пользователя, например, пароля Windows, отпечатков пальцев, смарт-карты. • Настройка и изменение очистки и уничтожения File Sanitizer, а также других параметров. • Просмотр параметров Device Access Manager. • Настройка Computrace for HP ProtectTools. • Настройка предпочтений, а также таких функций, как резервное копирование и восстановление.
Credential Manager for HP ProtectTools (Password Manager)	• Сохранение, упорядочивание и защита имен пользователей и паролей. • Настройка экранов входа для быстрого и безопасного доступа к веб-сайтам и программам. • Сохранение имен пользователей и паролей для доступа к веб-сайтам в Password Manager. При следующем посещении веб-сайта сведения для входа будут заполнены и отправлены автоматически с помощью программы Password Manager. • Создание более надежных паролей для улучшения защиты учетной записи. Password Manager автоматически вводит и отправляет данные.
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.
File Sanitizer for HP ProtectTools	• Уничтожает цифровые ресурсы (важную информацию, такую как файлы приложений, данные журнала или сети и прочие конфиденциальные данные) на компьютере и периодически выполняет очистку удаленных ресурсов на жестком диске.

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 записываемым устройствам для конкретных лиц или групп пользователей.
Privacy Manager for HP ProtectTools (только на некоторых моделях)	• Используется для получения сертификатов авторизации, которые подтверждают источник, целостность и безопасность связи при использовании электронной почты Microsoft и документов Microsoft Office.
Computrace for HP ProtectTools (приобретается отдельно)	• 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. • Для активации необходимо отдельно приобрести подписки для отслеживания и трассировки.
Embedded Security for HP ProtectTools (только на некоторых моделях)	• Для защиты от несанкционированного доступа к данным пользователя и учетным данным, хранящимся на компьютере, используется микросхема встроенной системы безопасности Trusted Platform Module (TPM). • Дает возможность создания личного защищенного диска, который используется для защиты данных о файлах и папках пользователя. • Поддерживает операции с защищенными цифровыми сертификатами для сторонних приложений (например Microsoft Outlook и Internet Explorer).

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.

Credential Manager for HP ProtectTools

Программа Credential Manager (часть службы Security 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 Credential Manager, чтобы совместить веб-ссылки с различными именами пользователя и паролями. Когда она переходит на веб-сайт и выполняет вход в систему, Credential Manager подставляет учетные данные автоматически. Если ей потребуется просмотреть имена пользователя и пароли, Credential Manager может показать их.

Credential 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 Credential Manager for HP ProtectTools. После этого он внедряет Credential Manager 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

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.

Как Embedded Security for HP ProtectTools, так и Drive Encryption for HP ProtectTools не предоставляют 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.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools используется для окончательного удаления данных, в том числе данных о деятельности в обозревателе Интернета, временных файлов, ранее удаленных данных или любой другой информации. File Sanitizer можно настроить так, чтобы он запускался вручную или автоматически по расписанию, заданному пользователем.

Пример 1. Юрист, которому часто приходится иметь дело с важной информацией клиентов, хочет обеспечить возможность удаления файлов без восстановления. File Sanitizer используется для уничтожения удаленных файлов также, как шредер — для уничтожения бумажных документов, практически без возможности их восстановления.

Обычно при удалении данных в Windows они не удаляются с жесткого диска окончательно. Вместо этого секторы жесткого диска помечаются как доступные для дальнейшего использования. До того, как данные будут перезаписаны, их легко восстановить при помощи простых средств, доступных в Интернете. File Sanitizer перезаписывает сектор случайными данными (при необходимости — неоднократно), таким образом обеспечивая невозможность чтения или восстановления удаленных данных.

Пример 2. Исследователю требуется автоматически уничтожать удаленные данные, временные файлы, отчеты о действиях в обозревателе и т. п. при выключении системы. Она использует File Sanitizer для автоматического уничтожения по расписанию любых стандартных файлов или пользовательских файлов.

Device Access Manager for HP ProtectTools

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. Кроме того, администратор может назначать, когда и на какой промежуток времени диск будет доступен. Примером может служить ситуация, в которой внешним поставщикам требуется доступ к компьютерам компании, но они не должны иметь

возможность копировать данные на устройства USB. С помощью Device Access Manager for HP ProtectTools администраторы могут ограничивать доступ к оборудованию и управлять этим доступом.

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.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools используется для защиты связи по электронной почте. Пользователь имеет возможность создавать и отсылать электронные сообщения, которые сможет открыть только авторизованный получатель. Служба Privacy Manager защищает пользователей от утечки данных или их перехвата злоумышленниками.

Пример 1. Биржовой маклер хочет быть уверенным в том, что электронные сообщения получают только определенные клиенты, и никто другой не сможет сфальсифицировать почтовый ящик и перехватить письмо. Он оформляет себе и своим клиентам подписку на Privacy Manager. Privacy Manager назначает каждому пользователю сертификат для проверки подлинности. При работе с данным средством маклер и его клиенты должны пройти проверку подлинности перед обменом электронными сообщениями.

Privacy Manager for HP ProtectTools упрощает процесс отправки и получения электронных сообщений, при котором получатель проверен и авторизован. Почтовая служба также может быть зашифрована. Способ шифрования схож с тем, который обычно применяется при платежах кредитной картой в Интернете.

Пример 2. Генеральный директор хочет сделать так, чтобы только члены совета директоров могли просматривать информацию, которую он отправляет по электронной почте. Он использует возможность шифрования электронных сообщений, которые отправляют и получают директора. Служба Privacy Manager Certificate of Authentication предоставляет генеральному директору и членам совета директоров копии ключа шифрования, так что только они сами могут расшифровывать конфиденциальные сообщения.

Computrace for HP ProtectTools (в прошлом LoJack Pro)

Computrace for HP ProtectTools (приобретается отдельно) — это служба для отслеживания местоположения украденного компьютера при выходе пользователя в Интернет.

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.

Computrace for HP ProtectTools также может использоваться для удаленного управления компьютерами, узнавания их расположения и отслеживания использования.

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.

Embedded Security for HP ProtectTools (только на некоторых моделях)

Embedded Security for HP ProtectTools предоставляет возможность создания личного защищенного диска. Пользователь может создать виртуальный диск, полностью скрытый до тех пор, пока не будет выполнено обращение к нему. Embedded Security применяется в случаях, когда часть данных требуется хранить в секрете, а все остальные данные не должны быть зашифрованы.

Пример 1. Компьютером менеджера склада постоянно пользуются в течение дня разные работники. Менеджер хочет зашифровать и спрятать конфиденциальные данные склада, хранящиеся на этом компьютере. Ему требуется такая степень безопасности, при которой данные останутся зашифрованными, даже если жесткий диск будет украден. Он принимает решение активировать Embedded Security и перемещает конфиденциальные данные на личный защищенный диск. Сам менеджер может ввести пароль и получить доступ к защищенным данным точно так же, как к любому другому диску. Когда менеджер выходит из системы или перезагружает личный защищенный диск, он становится невидимым и его невозможно открыть без ввода пароля. Сотрудники не видят конфиденциальные данные, когда работают с этим компьютером.

Ключи шифрования в Embedded Security защищены микросхемой TPM (Trusted Platform Module), расположенной на материнской плате. Это единственное средство шифрования, которое отвечает минимальным требованиям для защиты от попыток подобрать пароль для дешифровки. С помощью Embedded Security также можно зашифровать весь диск или электронное сообщение.

Пример 2. Биржевой маклер хочет перенести крайне важные и секретные данные на другой компьютер с помощью переносного диска. Ей необходимо быть уверенной в том, что диск может быть открыт только на этих двух компьютерах, даже если пароль попадет в руки злоумышленников. Чтобы расшифровать данные на втором компьютере с помощью необходимых ключей, она использует для переноса Embedded Security TPM. Даже при использовании пароля расшифровка данных может быть выполнена только на двух физических компьютерах.

Достижение ключевых целей безопасности

Модули HP ProtectTools могут совместно работать для предоставления решений по различным аспектам безопасности, включая следующие ключевые цели безопасности.

- Защита от умышленной кражи.
- Ограничение доступа к важным данным.
- Предотвращение несанкционированного доступа из внутренних или внешних местоположений.
- Создание надежных политик паролей.

Защита от целенаправленной кражи

Примером целенаправленной кражи является хищение компьютера, содержащего конфиденциальные данные и информацию о клиентах, при прохождении спецконтроля в аэропорту. Следующие функции помогают защитить данные от целенаправленной кражи.

- Включение функции проверки подлинности перед загрузкой ограничивает доступ к операционной системе. См. следующие разделы:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- С помощью функции «Личный защищенный диск», предлагаемой модулем Embedded Security for HP ProtectTools, можно зашифровать секретную информацию, что предотвращает неавторизованный доступ к ней. См. раздел:
  - Embedded Security for HP ProtectTools
- С помощью Computrace можно найти украденные компьютеры. См. раздел:
  - Computrace for HP ProtectTools

Ограничение доступа к важным 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 записываемым устройствам, чтобы секретную информацию невозможно было распечатать или скопировать с жесткого диска на переносные носители.

Предотвращение несанкционированного доступа из внутренних или 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. См. следующие разделы:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager позволяет не допустить попадания паролей к неавторизованным пользователям и делает невозможным доступ к приложениям, защищенным паролем.
- 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.
- File Sanitizer обеспечивает безопасное удаление данных, уничтожая важные файлы и папки или очищая удаленные ресурсы на жестком диске (выполняя запись поверх данных, которые были удалены, но все еще поддаются восстановлению).
- Privacy Manager предоставляет сертификаты авторизации при использовании электронной почты Microsoft или документов Microsoft Office, что делает более безопасным процесс отправки и получения важной информации.

Формирование политики 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.

Дополнительные элементы безопасности

Назначение ролей в системе безопасности

В системе управления безопасностью компьютера (особенно в больших организациях) важным практическим приемом является разделение ответственности и полномочий между различными типами администраторов и пользователей.

ПРИМЕЧАНИЕ. В небольших организациях или при индивидуальном использовании эти роли могут принадлежать одному и тому же лицу.

Для HP ProtectTools обязанности и полномочия в системе безопасности могут быть распределены согласно следующим ролям.

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

  ПРИМЕЧАНИЕ. Многие функции программы HP ProtectTools могут настраиваться начальником системы безопасности в сотрудничестве с компанией HP. Дополнительную информацию см. на веб-сайте HP по адресу: 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 следовать практическим советам по ограничению прав конечных пользователей и возможностей доступа для них.

Неавторизованные пользователи не должны иметь прав администратора.

Управление паролями HP ProtectTools

Большая часть функций HP ProtectTools Security Manager защищена паролями. В следующей таблице приведен список часто используемых паролей, программные модули, в которых задаются пароли, и функции паролей.

В этой таблице также указаны пароли, задаваемые и используемые только ИТ-администраторами. Все остальные пароли могут задаваться рядовыми пользователями или администраторами.

Пароль HP ProtectTools	Модуль	Функция
Пароль на вход в Windows	Панель управления Windows® или HP ProtectTools Security Manager	Может использоваться для входа вручную и проверки подлинности при доступе к функциям Security Manager.
Пароль Security Manager для резервного копирования и восстановления	Security Manager, для отдельных пользователей	Защищает доступ к файлу резервного копирования и восстановления Security Manager.

Пароль HP ProtectTools	Модуль	Функция
PIN-код смарт-карты	Credential Manager	Может использоваться для многофакторной проверки подлинности. Может использоваться для проверки подлинности в Windows. Авторизует пользователей Drive Encryption, если выбран маркер смарт-карты.
Пароль маркера аварийного восстановления	Embedded Security, ИТ-администратор	Защищает доступ к маркеру аварийного восстановления, который является резервным файлом для микросхемы встроенной системы безопасности.
Пароль владельца	Embedded Security, ИТ-администратор	Защищает систему и микросхему TPM от неавторизованного доступа ко всем функциям владельца в службе Embedded Security.
Пароль администратора BIOS	Computer Setup, ИТ-администратор	Защищает доступ к служебной программе Computer Setup.

Создание безопасного пароля

При создании паролей необходимо учитывать требования конкретной программы. Однако в общем случае рекомендуется принимать во внимание следующие правила, способствующие созданию надежных паролей и уменьшению вероятности несанкционированного раскрытия пароля.

- Используйте пароли, содержащие более 6 символов, предпочтительно более 8 символов.
- Включайте в пароль буквы разного регистра.
- Используйте, по возможности, сочетание букв, цифр, специальных символов и знаков пунктуации.
- В ключевом слове рекомендуется вместо букв подставлять специальные символы или цифры. Например, вместо буквы I или L можно использовать цифру 1.
- Используйте сочетания слов из двух или более языков.
- Вставляйте в середину слова или фразы числа или специальные символы, например «Mary2-2Cat45».
- Не следует использовать пароль, который встречается 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 пароль. Достаточно изменять только пару соседних букв.
- Записанный пароль не следует хранить на видном месте рядом с компьютером.
- Не сохраняйте пароль в файле на компьютере, например в файле электронной почты.
- Не используйте учетные записи общего пользования и не сообщайте никому свой пароль.

Резервное копирование и восстановление учетных данных HP ProtectTools

Модуль Backup and Restore for HP ProtectTools может использоваться для выбора параметров и учетных данных HP ProtectTools и их резервного копирования.

2 Начало работы с мастером настройки

Мастер настройки Security Manager поможет вам включить доступные функции безопасности, которые применяются ко всем пользователям данного компьютера. Также можно управлять этими функциями на странице «Функции безопасности» консоли администрирования.

Для настройки функций безопасности с помощью мастера настройки Security Manager выполните перечисленные ниже действия.

1. Откройте HP ProtectTools Security Manager при помощи элемента рабочего стола HP ProtectTools Security Manager на боковой панели Windows или значка Security Manager в области уведомлений, расположенной в правом углу панели задач.

Цвет значка на элементе рабочего стола HP ProtectTools указывает на одно из следующих состояний:

- Красный — программа HP ProtectTools не настроена или возникла проблема с одним из модулей ProtectTools.
- Желтый — проверьте страницу Applications Status (Состояние приложений) в программе Security Manager для изменения необходимых параметров.
- Синий — программа HP ProtectTools настроена и работает правильно.

В нижней части элемента отображается сообщение с указанием на одно из двух следующих условий:

- **Настроить сейчас** — администратору необходимо щелкнуть элемент, чтобы запустить мастер настройки Security Manager для настройки учетных данных проверки подлинности для компьютера.

  Мастер настройки является независимым приложением.

- **Зарегистрировать сейчас** — пользователь должен щелкнуть элемент, чтобы запустить мастер «Приступая к работе» Security Manager для регистрации учетных данных проверки подлинности.

  На панели мониторинга Security Manager отображается мастер «Приступая к работе».

- **Проверить сейчас** — щелкните элемент для отображения дополнительных сведений на странице «Состояние приложений безопасности».

ПРИМЕЧАНИЕ. Элемент рабочего стола HP ProtectTools недоступен в Windows XP.

— или —

Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**. На левой панели щелкните **Мастер настройки**.

2. Прочтите страницу приветствия и щелкните **Далее**.

3. Подтвердите свои идентификационные данные с помощью пароля Windows и нажмите кнопку **Далее**.

   Если пароль Windows еще не создан, будет предложено его создать. Пароль Windows требуется для защиты учетной записи Windows от несанкционированного доступа и для использования функций Security Manager.

4. На странице SpareKey выберите три контрольных вопроса и введите ответ на каждый вопрос, после чего щелкните **Далее**.

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

ПРИМЕЧАНИЕ. Данная установка SpareKey применима только к пользователю с правами администратора.

5. Включите функции безопасности, установив соответствующие флажки, после чего щелкните **Далее**.

   Чем больше функций вы выберите, тем надежнее будет защищен компьютер.

ПРИМЕЧАНИЕ. Данные настройки применимы ко всем пользователям. Если какие-то флажки останутся неустановленными, мастер настройки не станет предлагать пользователям зарегистрировать те учетные данные.

- Функция **Безопасный вход в систему Windows** — защищает учетные записи Windows, запрашивая для доступа использование определенных учетных данных.
- **Drive Encryption** защищает данные с помощью шифрования жестких дисков, делая информацию недоступной для чтения без соответствующей авторизации.
- **Функция безопасности при предварительной загрузке** защищает компьютер, запрещая несанкционированный доступ пользователей до запуска Windows.

  ПРИМЕЧАНИЕ. Функция безопасности при предварительной загрузке недоступна, если система BIOS ее не поддерживает.

6. Мастер настройки предложит вам зарегистрироваться или «зарегистрировать» свои учетные данные.

   Если не доступно ни устройство считывания отпечатков пальцев, ни смарт-карта или веб-камера, вам будет предложено ввести пароль Windows. После регистрации вы можете использовать любые зарегистрированные учетные данные для подтверждения идентификации в любых случаях, в которых это потребуется.

ПРИМЕЧАНИЕ. Регистрация этих учетных данных применима только к пользователю с правами администратора.

7. На последней странице мастера нажмите кнопку **Finish** (Готово).

   Откроется начальная страница панели мониторинга Security Manager.

3 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 панели мониторинга Security Manager доступны дополнительные приложения (только на некоторых моделях), которые помогают в восстановлении компьютера при его утере или краже.

С помощью данной консоли 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
- Добавление дополнительных приложений Security Manager

Открытие консоли администрирования HP ProtectTools

Для выполнения задач администратора, таких как установка системных политик или настройка программного обеспечения, откройте консоль следующим образом.

- Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.

  – или –

  На левой панели Security Manager выберите **Администрирование** и щелкните **Консоль администрирования**.

Использование консоли администрирования

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

▲ Чтобы открыть консоль администрирования HP ProtectTools, нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.

– или –

На левой панели Security Manager выберите **Администрирование** и щелкните **Консоль администрирования**.

Консоль состоит из следующих компонентов.

- **Главная страница** — позволяет настроить следующие параметры безопасности:
  - **Повышение уровня защиты системы**
  - **Необходима надежная проверка подлинности**
  - **Управление пользователями HP ProtectTools**
  - **Узнайте возможности централизованного управления HP ProtectTools**
- **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** — предоставляет расширенное меню из ссылок для приложений Security Manager, которые защищают ваши данные.
- **Централизованное управление** — отображает вкладки для доступа к дополнительным решениям, обновлениям продуктов и сообщениям.
- **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 по 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.

- **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 **Политика входа** нажмите стрелку вниз и выберите категорию пользователя.
   - **Для администраторов данного компьютера**
   - **Для пользователей, не являющихся администраторами**
3. Укажите учетные данные проверки подлинности, которые будут запрашиваться для выбранной категории пользователя.
4. Выберите, будут ли при проверке подлинности пользователя запрашиваться какие-либо ОТДЕЛЬНЫЕ или же ВСЕ указанные учетные данные.
5. Щелкните **Применить**.

Политика сеанса

Для установки политик, определяющих учетные данные, которые запрашиваются в течение сеанса Windows для доступа к приложениям HP ProtectTools, выполните следующие действия.

1. На левой панели консоли администрирования выберите **Безопасность** и щелкните **Проверка подлинности**.
2. На вкладке **Политика сеанса** нажмите стрелку вниз и выберите категорию пользователя.
   - **Для администраторов данного компьютера**
   - **Для пользователей, не являющихся администраторами**
3. Нажмите стрелку вниз и выберите учетные данные для проверки подлинности, которые будут запрашиваться для выбранной категории пользователя.
   - **Требуется один из указанных элементов учетных данных**

     ПРИМЕЧАНИЕ. Снятие флажков для всех учетных данных имеет такой же эффект, как выбор параметра **Проверка подлинности не требуется**.
   - **Требуются все указанные учетные данные**
   - **Проверка подлинности не требуется** — Выбор данного параметра удаляет все учетные данные из окна.
4. Щелкните **Применить**.

Значения настроек

1. Установите этот флажок для включения следующего параметра или снимите его для его отключения.

   Разрешить одношаговый вход в систему — позволяет пользователям данного компьютера пропускать проверку при входе в систему Windows, если проверка подлинности проводилась в системе BIOS или на уровне зашифрованного диска.
2. 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 указать 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. Установите флажок, чтобы включить проверку подлинности SpareKey при входе в систему Windows, или снимите флажок, чтобы ее выключить.
2. Выберите контрольные вопросы, которые предлагаются пользователям во время регистрации SpareKey. Можно определить до трех пользовательских вопросов или же позволить пользователям ввести собственную кодовую фразу.
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.

Смарт-карта

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

- **Параметры** — настройка автоматической блокировки компьютера при извлечении смарт-карты.

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, недоступны.

▲ Щелкните **Применить**.

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, можно настроить уровень безопасности для программы распознавания лица Face Recognition.

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. Щелкните **Учетные данные** и выберите **Лицо**.

3. 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.

4. Щелкните **Дополнительно** и настройте расширенную безопасность. Подробнее см. Дополнительные параметры пользователя на стр. 44.

5. Щелкните **Применить**.

Настройка приложений

Для настройки установленных приложений HP ProtectTools Security Manager можно использовать «Параметры».

Чтобы изменить параметры приложений, выполните следующие действия.

1. На левой панели консоли администрирования в разделе **Приложения** щелкните **Параметры**.
2. Установите флажок, расположенный рядом с определенным параметром, для включения или снимите его для отключения.
3. Щелкните **Применить**.

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.

Вкладка приложений

Параметры, которые здесь отображаются, могут изменяться при добавлении новых приложений к Security Manager. Ниже приведены минимальные параметры, которые отображаются по умолчанию.

- **Состояние приложений** — включается функция отображения состояния всех приложений.
- **Password Manager** — включает Password Manager для всех пользователей компьютера.
- **Privacy Manager** — включается Privacy Manager для всех пользователей компьютера.
- **Включение ссылки «Централизованное управление»** — позволяет всем пользователям компьютера добавлять приложения в программу HP ProtectTools Security Manager нажатием **Централизованное управление**.

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

Централизованное управление

Могут быть доступны дополнительные приложения для добавления новых сервисов управления в Security Manager. Администратор этого компьютера может отключить эту

функцию на странице «Параметры». На странице «Централизованное управление» расположены две вкладки.

- **Бизнес-решения** — для проверки наличия новых приложений при наличии подключения к Интернету можно перейти на веб-сайт DigitalPersona (http://www.digitalpersona.com/).
- **Обновления и сообщения**
  - Чтобы запросить сведения о новых приложениях и обновлениях, установите флажок **Сообщать о новых приложениях и обновлениях**.
  - Чтобы настроить расписание для автоматической проверки наличия обновлений, выберите количество дней.
  - Для проверки наличия обновлений щелкните **Проверить сейчас**.

4 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:

- Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.
- Дважды щелкните значок **HP ProtectTools** в области уведомлений в правом углу панели задач.
- Правой кнопкой мыши щелкните значок **HP ProtectTools**, затем щелкните **Открыть HP ProtectTools Security Manager**.
- Щелкните элемент рабочего стола **HP ProtectTools**.
- Нажмите сочетание клавиш ctrl+Windows+h, чтобы открыть меню **Быстрый доступ к Security Manager**.

  Для получения сведений об изменении сочетания клавиш см. Параметры на стр. 38.

Использование панели мониторинга Security Manager

Панель мониторинга Security Manager является центральным местоположением для простого доступа к функциям, приложениям и параметрам Security Manager.

▲ Чтобы открыть панель мониторинга Security Manager, нажмите **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.

На панели мониторинга отображаются следующие компоненты:

- **Идентификационная карта** — отображаются имя пользователя Windows и выбранное изображение, определяющее учетную запись пользователя, вошедшего в систему.
- **Приложения безопасности** — отображается расширенное меню из ссылок для настройки следующих категорий безопасности:
  - **Начальная страница** — управляет паролями, настраивает учетные данные проверки подлинности или проверяет состояние приложений безопасности.
  - **Состояние** — проверяет состояние приложений безопасности HP ProtectTools.

ПРИМЕЧАНИЕ. Приложения, не установленные на компьютере, не отображаются в следующем списке.

- **Мои учетные записи** — управляет учетными данными проверки подлинности с помощью программ Password Manager и Credential Manager, пароля, SpareKey, смарт-карты, лица и отпечатков пальцев.
- **Мои данные** — управляет безопасностью данных с помощью программ Drive Encryption и File Sanitizer.
- **Мой компьютер** — управляет безопасностью компьютера с помощью программы Device Access Manager.
- **Мои соединения** — управляет безопасностью соединений с помощью программы Privacy Manager.
- **Администрирование** — разрешает администраторам доступ к следующим параметрам:
  - **Консоль администрирования** — позволяет администраторам управлять безопасностью и пользователями.
  - **Централизованное управление** — разрешает администраторам доступ к дополнительным решениям, обновлениям продуктов и сообщениям.
- **Дополнительно** — отображает команды для доступа к дополнительным функциям, среди которых:
  - **Настройки** — выполнение индивидуальных настроек Security Manager.
  - **Архивация и восстановление** — выполнение архивации 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 программе Security Manager. Данный значок расположен в правой верхней части окна, рядом со значками сворачивания и развертывания.

Состояние приложений безопасности

Можно просматривать состояние установленных приложений безопасности в двух местоположениях:

- **Элемент рабочего стола HP ProtectTools**

  Цвет заголовка в верхней части элемента HP ProtectTools меняется, отображая общее состояние безопасности установленных приложений безопасности.

  - **Красный** — предупреждение
  - **Желтый** — внимание: не настроено
  - **Синий** — OK

  В нижней части элемента отображается сообщение с указанием на одно из двух следующих условий:

  - **Настроить сейчас** — администратору необходимо щелкнуть элемент, чтобы запустить мастер настройки Security Manager для настройки учетных данных проверки подлинности для компьютера.

    Мастер настройки является независимым приложением.

  - **Зарегистрировать сейчас** — пользователю необходимо щелкнуть элемент, чтобы запустить мастер «Приступая к работе» Security Manager для регистрации учетных данных проверки подлинности.

    На панели мониторинга Security Manager отображается мастер «Приступая к работе».

  - **Проверить сейчас** — щелкните элемент для отображения дополнительных сведений на странице «Состояние приложений безопасности».

- **Страница «Состояние приложений безопасности»** — щелкните **Состояние** на панели мониторинга Security Manager для отображения общего состояния установленных приложений безопасности и состояния каждого приложения в отдельности.

Мои данные для входа

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

- **Password Manager** — 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 или смарт-карты.
- **Credential Manager** — средства для простого изменения пароля Windows, регистрации отпечатков пальцев и подготовки смарт-карты.

Администраторы могут добавлять приложения, щелкнув **Администрирование**, а затем **Централизованное управление** в нижнем левом углу панели мониторинга.

Password Manager

Password Manager 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, смарт-карты или пароля Windows.

Password Manager предоставляет следующие возможности:

- Добавление, изменение или удаление регистрационных имен на вкладке **Управление**.
- Использование быстрых ссылок для запуска обозревателя по умолчанию и входа на веб-сайты или в программы после настройки Password Manager.
- Перетаскивание быстрых ссылок для организации тематических разделов.
- Быстрая оценка любых паролей с точки зрения угроз безопасности и автоматическая генерация сложных надежных паролей для доступа к новым веб-сайтам.

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.

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

В контекстном меню отображаются следующие элементы:

- **Добавить [somedomain.com] в список Password Manager** — позволяет добавить учетную запись для текущего экрана входа на веб-сайт.
- **Открыть Password Manager** — запускает Password Manager.
- **Параметры значка** — позволяет указать условия, при которых отображается значок **Password Manager**.
- **Справка** — отображает справку по программе Security Manager.

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

В контекстном меню отображаются следующие параметры:

- **Заполнить учетную запись** — ввод данных в поля учетной записи и подтверждение ввода (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 для входа.
- **Открыть Password Manager** — запускает Password Manager.
- **Справка** — отображает справку по программе 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 **Учетные записи**, 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 **Password Manager**, 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 Password Manager**.
   - 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**. Некоторые параметры зависят от наличия подключенных к компьютеру устройств безопасности. Например, использование сочетания клавиш ctrl+Windows+h, считывание отпечатков пальцев или установка смарт-карты.
   - **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.** Чтобы включить безопасность VeriSign VIP, установите флажок **Я хочу иметь безопасность VIP на данном веб-сайте**.

Данный параметр отображается только для веб-сайтов, на которых доступно Защита личных данных VeriSign (VIP). При поддержке веб-сайтом данного параметра можно также выбрать автоматическую вставку кода безопасности VIP при обычном способе проверки подлинности.

д. Щелкните **OK**, выберите метод проверки подлинности, который необходимо использовать (отпечатки пальцев, пароль или лицо), а затем войдите в систему при помощи выбранного метода проверки подлинности.

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

е. 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.
- Если Password Manager не может определить все поля учетной записи, появится сообщение с запросом на продолжение. Щелкните **Да**.
- Откроется диалоговое окно с заполненными полями учетной записи. Щелкните значок для каждого поля и перетащите его в соответствующее поле учетной записи, затем нажмите кнопку для входа на веб-сайт.

ПРИМЕЧАНИЕ. После использования ручного режима ввода данных учетной записи для веб-сайта необходимо продолжить использовать этот метод для входа на этот веб-сайт в будущем.

ПРИМЕЧАНИЕ. Ручной режим ввода данных учетной записи доступен только в браузере Internet Explorer 8.

- 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 **Password Manager**, 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.
   - Чтобы включить безопасность VeriSign VIP, установите флажок **Я хочу иметь безопасность VIP на данном веб-сайте**.

     Данный параметр отображается только для веб-сайтов, на которых доступна безопасность VeriSign VIP. При поддержке веб-сайтом данного параметра можно также выбрать автоматическую вставку кода безопасности VIP при обычном способе проверки подлинности.
   - 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 учетных записей

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 **Учетные записи** 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 **Учетные записи** в Password Manager.

Для отображения меню **Учетные записи** выполните следующие действия.

1. Нажмите сочетание клавиш для **Password Manager** (заводской настройкой по умолчанию является ctrl+Windows +h). Чтобы изменить сочетание клавиш, на панели мониторинга Security Manager щелкните **Password Manager** и выберите **Параметры**.
2. Выполните считывание отпечатков пальцев (на компьютере со встроенным или подключенным устройством считывания 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 панели управления Security Manager щелкните **Password Manager**.
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 панели управления Security Manager щелкните **Password Manager** 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. Добавление учетных записей на стр. 32.
  - **Редактировать** — редактирует учетную запись. Подробнее см. 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. 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.

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

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 стрелку со значком и выберите **Параметры значка** для настройки метода обработки Password Manager возможных веб-сайтов для входа.

   - **Предлагать добавлять учетные данные для экранов входа в систему** — щелкните этот параметр, чтобы Password Manager всегда предлагал добавить учетную запись при отображении экрана входа, для которого не задана учетная запись.
   - **Исключить этот экран** — установите этот флажок, чтобы Password Manager не предлагал добавить учетную запись при отображении данного экрана входа.

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

     - Во время отображения учетной записи ранее исключенного веб-сайта или страницы программы откройте панель мониторинга Security Manager и щелкните **Password Manager**.
     - 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. Добавление учетных записей на стр. 32.
     - Значок **Password Manager** отображается при каждом открытии данного экрана входа на веб-сайт или в программу.
2. Чтобы отключить параметр отображения запроса на добавление учетных записей для экранов входа в систему, установите флажок.
3. Для доступа к дополнительным параметрам Password Manager от несанкционированного доступа щелкните **Password Manager** и на панели мониторинга Security Manager нажмите **Параметры**.

Защита личных данных VeriSign (VIP)

Можно создать маркеры доступа VeriSign VIP для использования с веб-сайтами, на которых имеется защита VeriSign VIP. Данные маркеры используются Password Manager для создания автоматических учетных записей, которые используют маркеры, перемещенные в экраны входа в систему с защитой VeriSign VIP или вручную введенные в указанные поля.

Можно включить VeriSign VIP и создать маркер с панели мониторинга Security Manager или на любом веб-сайте, имеющем VeriSign VIP. Для использования маркера необходимо зарегистрировать его на каждом веб-сайте, на котором он будет использоваться.

После регистрации и первого использования маркер может (необязательно) быть присоединен к обычным учетным данным для входа в систему и отправлен вместе с ними. Для сайтов, на которых присоединение маркеров не разрешено, можно перетащить или вручную ввести сведения о маркере.

Чтобы включить VeriSign VIP и создать маркер VeriSign VIP с панели мониторинга Security Manager, выполните следующие действия.

1. Откройте панель управления Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. Щелкните **Password Manager** и нажмите **VIP**.
3. Щелкните **Получить VIP**.

   Маркер VeriSign VIP создан и отображается на странице VeriSign VIP. Теперь маркер будет отображаться при каждом входе на страницу.

Чтобы включить VeriSign VIP и создать маркер VeriSign VIP с веб-сайта, выполните следующие действия.

1. Password Manager выдает предупреждения при каждом посещении веб-сайта с VeriSign VIP.
2. Создайте учетную запись для экрана. Подробнее см. Добавление учетных записей на стр. 32.
3. В диалоговом окне «Создать учетную запись» выберите **Я хочу иметь дополнительную защиту учетной записи с помощью VIP**.

Чтобы зарегистрировать маркер VeriSign VIP для веб-сайта, выполните следующие действия.

1. Войдите в систему веб-сайта с VeriSign VIP вручную или с помощью учетной записи Password Manager.
2. Щелкните отображаемый воздушный шар VeriSign VIP, чтобы создать учетную запись для данного сайта.
3. В диалоговом окне «Добавить учетную запись в Password Manager» выберите **Я хочу иметь безопасность VIP на данном веб-сайте**.

   Данный параметр отображается только для сайтов, на которых доступна безопасность VeriSign VIP. При поддержке веб-сайтом данного параметра можно также выбрать автоматическую вставку кода безопасности VIP при обычном способе проверки подлинности.

Параметры

Можно задать параметры для индивидуальной настройки HP ProtectTools Security Manager:

1. **Предлагать добавлять учетные данные для экранов входа в систему** — когда определен экран входа на веб-сайт или в программу, значок **Password Manager** отображается со знаком «плюс», показывая, что можно добавить учетную запись для этого экрана, в которой будет сохранен пароль для входа. Для отмены этой функции в диалоговом окне «Параметры значка» снимите флажок **Предлагать добавлять учетные записи для экранов входа в систему**.

2. **Открывать Password Manager сочетанием клавиш ctrl+win+h** — по умолчанию меню **Быстрый доступ к Password Manager** 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 пользователя, чтобы убедиться в том, что он действительно тот, за кого себя выдает. 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
- Смарт-карта
- Лицо

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 панели мониторинга Security Manager выберите **Credential Manager** 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 «Приступая к работе» 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 **Далее**.

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 в вашем компьютере имеется встроенный или внешний считыватель отпечатков пальцев, то во время первоначальной настройки в мастере «Приступая к работе» HP ProtectTools Security Manager запросит настройку или «регистрацию» отпечатков пальцев. Отпечатки пальцев также можно зарегистрировать на странице «Отпечатки пальцев» в **Credential Manager** на панели мониторинга Security Manager.

1. Отображается контурный рисунок двух ладоней. Отпечатки пальцев, которые уже зарегистрированы, выделены зеленым цветом. Щелкните палец на контурном рисунке ладони.

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

2. После выбора пальца на регистрацию запрос на его считывание будет отображаться, пока регистрация не будет успешно завершена. Зарегистрированный отпечаток пальца выделяется на контурном рисунке зеленым цветом.

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 руководства «Приступая к работе» 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.

Настройка смарт-карты

Чтобы можно было использовать смарт-карту для проверки подлинности, администраторы должны инициализировать и зарегистрировать 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 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 ActivIdentity.

1. Вставьте карту в устройство чтения.

2. Нажмите кнопку **Пуск**, выберите **Все программы** и щелкните **Средство инициализации PIN-кода ActivClient**.

3. Введите и подтвердите PIN-код.

4. Щелкните **Далее**.

   Программное обеспечение смарт-карты предоставит ключ разблокировки. Большинство смарт-карт автоматически блокируется после пятикратного ввода неверного PIN-кода. Ключ используется для разблокировки карты.

5. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.

6. Щелкните **Учетные данные** и далее **Смарт-карта**.

7. Выберите вкладку **Администрирование**.

8. Убедитесь, что выбрано **Настройка смарт-карты**.

9. Введите PIN-код, щелкните **Применить** и следуйте инструкциям на экране.

10. 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. Под пунктом **Централизованное управление** щелкните **Мастер настройки**.

2. На странице приветствия щелкните **Далее** и введите свой пароль Windows.

3. На странице SpareKey щелкните **Пропустить настройку SpareKey** (если только вы не хотите обновить сведения о SpareKey).

4. На странице Включение средств безопасности щелкните **Далее**.

5. На странице Выберите учетные данные убедитесь, что выбрано **Настройка смарт-карты** и щелкните **Далее**.

6. На странице Смарт-карта введите PIN-код и щелкните **Далее**.

7. Щелкните **Готово**.

Пользователи также могут зарегистрировать смарт-карту в Security Manager. Дополнительные сведения см. в справке программного обеспечения HP ProtectTools for Security Manager.

Настройка смарт-карты

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

- **Параметры** — настройка автоматической блокировки компьютера при извлечении смарт-карты.

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, недоступны.

▲ Щелкните **Применить**.

Регистрация сцен для входа в систему с помощью функции распознавания лица

Если в вашем компьютере имеется встроенная или подключенная веб-камера, то во время первоначальной настройки в мастере «Приступая к работе» HP ProtectTools Security Manager запросит настройку или «регистрацию» сцен. Сцены также можно зарегистрировать на странице «Вход в систему с помощью лица» в **Credential Manager** на панели мониторинга 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 сцену через мастер «Приступая к работе», выполните следующие действия.

1. На странице мастера «Лицо» щелкните **Дополнительно** и настройте расширенную безопасность. Подробнее см. Дополнительные параметры пользователя на стр. 44.
2. Щелкните **ОК**.
3. Щелкните **Пуск** или, если сцены уже были зарегистрированы, щелкните **Зарегистрировать новую сцену**.
4. Если дополнительных параметров безопасности не выбрано, вам будет предложено выбрать дополнительный параметр безопасности. Следуйте инструкциям на экране, а затем щелкните **Далее**. Подробнее см. Дополнительные параметры пользователя на стр. 44.
5. Щелкните значок **Камера** и следуйте инструкциям на экране.

   Следуйте инструкциям на экране и обязательно смотрите в объектив во время съемки сцен.
6. Щелкните **Далее**.
7. Щелкните **Готово**.

Также можно зарегистрировать сцены через панель мониторинга Security Manager:

1. Откройте панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. В разделе **Мои учетные записи** щелкните **Credential Manager**, а затем **Лицо**.
3. Щелкните **Дополнительно** и настройте расширенную безопасность. Подробнее см. Дополнительные параметры пользователя на стр. 44.
4. Щелкните **ОК**.
5. Щелкните **Пуск** или, если сцены уже были зарегистрированы, щелкните **Зарегистрировать новую сцену**.
6. Если дополнительных параметров безопасности не выбрано, вам будет предложено выбрать дополнительный параметр безопасности. Следуйте инструкциям на экране, а затем щелкните **Далее**. Подробнее см. Дополнительные параметры пользователя на стр. 44.
7. Щелкните значок **Камера** и следуйте инструкциям на экране.

   Следуйте инструкциям на экране и обязательно смотрите в объектив во время съемки сцен.

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

Дополнительные параметры пользователя

Данные параметры также отображаются на странице «Дополнительная защита», если не выбрано никакой дополнительной безопасности.

1. Откройте панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. В разделе **Мои учетные записи** щелкните **Credential Manager** и выберите **Лицо**.
3. Щелкните **Дополнительно**, чтобы настроить следующие параметры безопасности:

   a. Вкладка **Безопасность** — выберите один из следующих параметров:

   - **Без дополнительной безопасности** — выберите данный параметр, если для входа в систему с помощью лица дополнительная безопасность не требуется.
   - **Использовать PIN-код для дополнительной безопасности** — выберите данный параметр при необходимости использовать PIN-код, определенный пользователем, для входа в систему с помощью лица.
     - Щелкните **Создать PIN-код**.
     - Введите пароль Windows.
     - Введите новый PIN-код, а затем подтвердите его с помощью повторного ввода.

       После создания PIN-кода можно выбрать один из следующих параметров: **Изменить**, **Сбросить** или **Удалить PIN-код**.
   - **Использовать Bluetooth для дополнительной безопасности** — выберите данный параметр. чтобы объединить телефон с устройством Bluetooth с программой Face Recognition. При входе в систему Windows после проверки подлинности лица Face Recognition также проверяет присутствие телефона с Bluetooth, объединенного с программой. Если телефон присутствует (Bluetooth включен), то вход в систему Windows разрешен.
     - Убедитесь, что Bluetooth включен и на компьютере, и на телефоне.

       Если телефон с устройством Bluetooth отсутствует, то будет предложено включить его и перезапустить процесс входа в систему. Через 30 секунд работа окна входа в систему Face Recognition приостанавливается. Для инициации процесса входа в систему щелкните значок **Камера**. Если телефон с устройством Bluetooth отсутствует, то для входа в систему можно использовать обычный пароль Windows.
     - Щелкните **Добавить**.
     - Когда отобразится устройство Bluetooth, выберите его и щелкните **Далее**.

Щелкните **ОК**.

б. 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.
- **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.

Щелкните **ОК**.

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 заменить изображение и 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 панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. Щелкните идентификационную карту в левом верхнем углу панели мониторинга.
3. Щелкните окно с отображением имени пользователя Windows для данной учетной записи, введите новое имя и щелкните **Сохранить**.

Для смены отображаемого изображения выполните следующие действия.

1. Откройте панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. Щелкните идентификационную карту в левом верхнем углу панели мониторинга.
3. Нажмите **Выбрать изображение**, щелкните изображение, а затем **Сохранить**.

Настройка пользовательских параметров

Вы можете задать параметры для индивидуальной настройки HP ProtectTools Security Manager. На панели управления Security Manager щелкните **Дополнительные параметры** и выберите **Индивидуальные параметры**. Доступные параметры отображаются на двух вкладках: **Общие** и **Отпечатки пальцев**.

Вкладка «Общие»

Внешний вид — отображать 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.

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

  - **Включить звуковую обратную связь** — по окончании процесса считывания отпечатков пальцев Security Manager воспроизводит звуки, соответствующие определенным событиям. Можно назначить этим событиям новые звуки, выбрав их на вкладке **Звуки** на панели управления Windows, также можно отключить звуковую обратную связь, сняв этот флажок.

  - **Отображать обратную связь качества сканирования**

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

    Снимите этот флажок, чтобы отображались результаты считывания 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.

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 панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. В левой части панели мониторинга 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 панель мониторинга Security Manager. Подробнее см. Открытие Security Manager на стр. 28.
2. В левой части панели мониторинга 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**.

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

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

Мастер установки HP ProtectTools Security Manager позволяет администраторам Windows активировать Drive Encryption, выполнять резервное копирование ключа шифрования, выбирать диски и отменять выбор. Дополнительные сведения см. в справке программного обеспечения HP ProtectTools Security Manager.

Программа Drive Encryption позволяет выполнять следующие задачи.

- Выбор параметров Drive Encryption:
  - Активация пароля с защитой TPM
  - Шифрование и расшифровка отдельных дисков или разделов с использованием программного шифрования
  - Шифрование и расшифровка отдельных дисков с самошифрованием с использованием аппаратного шифрования
  - Добавление дополнительной защиты путем отключения режимов сна или ожидания для того, чтобы проверка подлинности перед загрузкой выполнялась в любом случае.

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

- Создание резервных ключей
- Восстановление ключа Drive Encryption
- Включение проверки подлинности перед загрузкой Drive Encryption с использованием пароля, зарегистрированных отпечатков пальцев или PIN-кода смарт-карты

Открытие программы Drive Encryption

Администраторы могут получать доступ к Drive Encryption из консоли администрирования HP ProtectTools.

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели щелкните **Drive Encryption**.

Общие задачи

Запуск Drive Encryption для стандартных жестких дисков

Для стандартных жестких дисков используется программное шифрование. Для активации Drive Encryption выполните следующие действия.

1. Используйте мастер установки HP ProtectTools Security Manager для активации программы Drive Encryption.
2. Следуйте указаниям на экране до отображения страницы **Включение средств безопасности**, затем выполните шаг 4.

– или –

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели щелкните значок **+** слева от элемента **Безопасность** для отображения доступных возможностей.
3. Щелкните **Функции**.
4. Установите флажок **Drive Encryption**, затем щелкните **Далее**.

ПРИМЕЧАНИЕ. Если диск для шифрования не выбран, активируется проверка подлинности перед загрузкой Drive Encryption, но шифрование дисков не будет выполняться.

5. В разделе **Диски для шифрования** установите флажок для жесткого диска, который необходимо зашифровать, и нажмите **Далее**.
6. Чтобы выполнить резервное копирование ключа шифрования, установите запоминающее устройство в соответствующее гнездо.

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

7. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для устройства хранения, на которое будет записан ключ шифрования.
8. Щелкните **Далее**.

ПРИМЕЧАНИЕ. Компьютер будет перезапущен.

Drive Encryption активировано. Шифрование диска может занять несколько часов, в зависимости от объема диска.

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

Запуск Drive Encryption для дисков с самошифрованием

Для дисков с самошифрованием, соответствующих спецификации Trusted Computing Group's OPAL может использоваться как программное, так и аппаратное шифрование. Чтобы

активировать Drive Encryption для дисков с самошифрованием, выполните следующие действия.

1. Используйте мастер установки HP ProtectTools Security Manager для запуска программы Drive Encryption.
2. Следуйте указаниям на экране до отображения страницы **Включение средств безопасности**, затем выполните шаг 4 для программного или аппаратного шифрования.

ПРИМЕЧАНИЕ. Если на компьютере нет дисков с самошифрованием, соответствующих спецификации Trusted Computing Group's OPAL, аппаратное шифрование невозможно, а программное используется по умолчанию.

Если компьютер оборудован и дисками с самошифрованием, и стандартными дисками, аппаратное шифрование недоступно, а программное используется по умолчанию.

– или –

Программное шифрование

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели щелкните значок **+** слева от элемента **Безопасность** для отображения доступных возможностей.
3. Щелкните **Функции**.
4. Установите флажок **Drive Encryption**, затем щелкните **Далее**.
5. В разделе **Диски для шифрования** установите флажок для жесткого диска, который необходимо зашифровать, и нажмите **Далее**.
6. Чтобы выполнить резервное копирование ключа шифрования, установите запоминающее устройство в соответствующее гнездо.

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

7. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для устройства хранения, на котором необходимо сохранить ключ шифрования.
8. Щелкните **Применить**.

   ПРИМЕЧАНИЕ. Компьютер перезагрузится.

   Drive Encryption активировано. Шифрование диска может занять несколько часов, в зависимости от объема диска.

Аппаратное шифрование

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели щелкните значок **+** слева от элемента **Безопасность** для отображения доступных возможностей.

3. Щелкните **Функции**.

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

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

Если отображается более одного диска, флажки установлены автоматически, но из можно отредактировать.

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

5. Убедитесь, что в нижней части экрана установлен флажок **Использование шифрования жесткого диска**.

6. В разделе **Диски для шифрования** установите флажок для жесткого диска, который необходимо зашифровать, и нажмите **Далее**.

7. Чтобы выполнить резервное копирование ключа шифрования, установите запоминающее устройство в соответствующее гнездо.

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

8. В разделе **Резервное копирование ключей Drive Encryption** установите флажок для устройства хранения, на которое будет записан ключ шифрования.

9. Щелкните **Применить**.

ПРИМЕЧАНИЕ. Компьютер потребуется перезапустить.

Drive Encryption активировано. 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.

▲ Следуйте указаниям на экране до отображения страницы **Включение средств безопасности**, затем выполните шаг 4.

– или –

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.

2. На левой панели щелкните значок **+** слева от элемента **Безопасность** для отображения доступных возможностей.

3. Щелкните **Функции**.

4. Снимите флажок **Drive Encryption**, затем щелкните **Далее**.

Начнется деактивация Drive Encryption.

ПРИМЕЧАНИЕ. Если использовалось программное шифрование, начнется расшифровка. Она может занять несколько часов, в зависимости от объема диска. После завершения расшифровки Drive Encryption деактивируется.

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

После деактивации компьютер потребуется перезапустить.

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 использовании аппаратного шифрования убедитесь, что компьютер выключен. Если компьютер не был выключен и произойдет перезагрузка, экран проверки подлинности перед загрузкой Drive Encryption не отобразится.

ПРИМЕЧАНИЕ. При выходе из режима ожидания или сна проверка подлинности перед загрузкой Drive Encryption не отображается для программного или аппаратного шифрования, если оно не отключено.

При выходе из режима гибернации проверка подлинности перед загрузкой Drive Encryption отображается.

ПРИМЕЧАНИЕ. Если администратор Windows включил функцию защиты перед загрузкой в программе HP ProtectTools Security Manager, вход в систему может быть выполнен немедленно после включения компьютера, а не на экране входа Drive Encryption.

1. Щелкните имя пользователя, затем введите пароль Windows или PIN-код смарт-карты, или же проведите зарегистрированным пальцем.

ПРИМЕЧАНИЕ. Поддерживаются следующие смарт-карты:

Смарт-карты

- Смарт-карта ActivIdentity 64K V2C
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

Устройства считывания PCMCIA

- Внутреннее устройство считывания Express Card 54 SCR3340
- SCR 201
- SCR 243 (также торговая марка HP)
- ActivCard
- Omnikey 4040
- Cisco

Устройства считывания USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Терминал смарт-карт HP

2. Нажмите кнопку **ОК**.

ПРИМЕЧАНИЕ. При использовании ключа восстановления для входа в систему на экране входа Drive Encryption появится запрос на ввод пароля, PIN-кода смарт-карты или отпечатка пальца на экране входа Windows.

Защитите данные путем шифрования жесткого диска

Настоятельно рекомендуется использовать мастер установки HP ProtectTools Security Manager для защиты данных путем шифрования жесткого диска:

1. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
2. Щелкните **Параметры**.
3. Для дисков с самошифрованием выберите разделы диска, которые требуется зашифровать.

ПРИМЕЧАНИЕ. Это также применяется в случае наличия и стандартных жестких дисков, и дисков с самошифрованием.

– или –

- Для дисков с аппаратным шифрованием выберите диск или диски, которые требуется зашифровать. Должен быть выбран хотя бы один диск.

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. Откройте программу HP ProtectTools Security Manager.
2. В разделе **Мои данные** щелкните **Drive Encryption**.

   При программном шифровании в поле **Состояние диска** отображается одно из следующих состояний.

   - Включено
   - Отключено
   - Не зашифрован
   - Зашифровано
   - Шифрование
   - Расшифровка

   При аппаратном шифровании в поле **Состояние диска** отображается следующее состояние.

   - Зашифрован

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

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. Аппаратное шифрование нельзя изменить на странице «Параметры».

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

Программное шифрование

- Не зашифрован
- Зашифрован
- Выполняется шифрование
- Выполняется расшифровка

Аппаратное шифрование

- Зашифровано

Шифрование и расшифровка отдельных дисков (только для программного шифрования)

Администраторы могут использовать страницу «Параметры» для шифрования одного или нескольких жестких дисков на компьютере или расшифровки уже зашифрованного диска.

1. Откройте консоль администрирования HP ProtectTools.
2. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
3. Щелкните **Параметры**.
4. В диалоговом окне **Состояние диска** установите или снимите флажки для дисков, которые необходимо зашифровать или расшифровать, затем нажмите **Применить**.

ПРИМЕЧАНИЕ. При выполнении шифрования или расшифровки диска в строке выполнения отображается оставшееся время выполнения процесса во время текущего сеанса.

Если во время выполнения процесса шифрования компьютер выключается или переход в режим сна, ожидания или гибернации, а затем перезапускается, отображение оставшегося времени сбрасывается на начало, но действительный процесс шифрования продолжается с места остановки. Экран выполнения, на котором отображаются проценты, и оставшееся время будут изменяться более быстро, чтобы отразить предыдущее выполнение.

ПРИМЕЧАНИЕ. Динамические разделы не поддерживаются. Если раздел отображается как доступный, но не шифруется, если его выбрать, — этот раздел является динамическим. Динамические разделы образуются в результате сжатия для создания новых разделов в Управлении дисками.

Перед преобразованием раздела в динамический появляется предупреждение.

Резервное копирование и восстановление (задача администратора)

Когда активно Drive Encryption, администраторы могут использовать страницу «Резервное копирование ключа шифрования» для копирования ключа на съемный носитель и выполнения восстановления.

Резервное копирование ключей шифрования

Администраторы могут выполнить резервное копирование ключа шифрования для зашифрованного диска на съемное устройство хранения.

⚠ **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 жесткому диску.

1. Откройте консоль администрирования HP ProtectTools.
2. На левой панели щелкните значок **+** слева от **Drive Encryption** для отображения доступных возможностей.
3. Щелкните **Резервное копирование ключа шифрования**.
4. Установите запоминающее устройство, на которое собираетесь скопировать ключ шифрования.
5. В разделе **Дисковод** установите флажок для этого устройства хранения.
6. Щелкните **Резервные ключи**.
7. Прочитайте информацию, отображающуюся на следующей странице, и щелкните **Далее**. Ключ шифрования сохраняется на выбранном запоминающем устройстве.

Восстановление ключа шифрования

Администратор может восстановить ключ шифрования со съемного носителя, на который он был сохранен:

1. Включите компьютер.
2. Установите съемное запоминающее устройство с резервным ключом.
3. После открытия диалогового окна входа Drive Encryption for HP ProtectTools щелкните **Параметры**.
4. Нажмите **Восстановление**.
5. Выберите файл, содержащий резервный ключ, или щелкните **Обзор**, чтобы найти его, затем щелкните **Далее**.
6. При появлении диалогового окна подтверждения щелкните **ОК**.

Компьютер запустится.

ПРИМЕЧАНИЕ. Настоятельно рекомендуется сбросить пароль после выполнения восстановления.

6 Privacy Manager for HP ProtectTools (только на некоторых моделях)

Privacy Manager for HP ProtectTools предоставляет расширенные возможности безопасного входа в систему (проверки подлинности) для проверки источника, целостности и безопасности связи при работе с электронной почтой или документами Microsoft® Office.

Privacy Manager оптимизирует инфраструктуру безопасности, которую предоставляет HP ProtectTools Security Manager, и включает следующие способы безопасного входа в систему.

- Проверка подлинности по отпечаткам пальцев
- Пароль Windows®
- Смарт-карта
- Распознавание лица

В Privacy Manager можно использовать любой из перечисленных способов безопасного входа в систему.

Открытие Privacy Manager

Чтобы открыть Privacy Manager, выполните следующие действия.

- Чтобы перейти к функциям именно Outlook в Microsoft Outlook на вкладке **Сообщение** в группе **Конфиденциальность** щелкните **Безопасная отправка**.
- Чтобы перейти к большинству функций в документах Microsoft Office, на вкладке **Главная страница** в группе **Конфиденциальность** щелкните **Подписать и зашифровать**.
- Чтобы перейти к дополнительным функциям, откройте панель мониторинга HP ProtectTools Security Manager.
  - Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP**, выберите **HP ProtectTools Security Manager** и щелкните **Privacy Manager**.

    – или –
  - Щелкните элемент рабочего стола **HP ProtectTools**.

    – или –
  - Щелкните правой кнопкой значок **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач, выберите **Privacy Manager** и щелкните **Конфигурация**.

Процедуры настройки

Управление сертификатами Privacy Manager

Сертификаты Privacy Manager обеспечивают защиту данных и сообщений при помощи технологии шифрования «инфраструктура открытых ключей». Инфраструктура открытых ключей требует наличия у пользователей ключей шифрования и сертификата Privacy Manager, выданного центром сертификации. В отличие от большинства программ шифрования данных и проверки подлинности, которые требуют лишь периодической проверки подлинности, Privacy Manager требует проверки подлинности каждый раз, когда вы подписываете сообщение электронной почты или документ Microsoft Office при помощи ключа шифрования. Privacy Manager обеспечивает надежность и безопасность процесса сохранения и отправки важной информации.

Certificate Manager позволяет выполнять следующие задачи.

- Запрос сертификата Privacy Manager на стр. 62
- Получение предварительно назначенного корпоративного сертификата Privacy Manager на стр. 63
- Настройка сертификата Privacy Manager по умолчанию на стр. 65
- Импорт стороннего сертификата на стр. 63
- Просмотр сведений о сертификате Privacy Manager на стр. 64
- Обновление сертификата Privacy Manager на стр. 64
- Настройка сертификата Privacy Manager по умолчанию на стр. 65
- Удаление сертификата Privacy Manager на стр. 65
- Восстановление сертификата Privacy Manager на стр. 65
- Отзыв сертификата Privacy Manager на стр. 66

Запрос сертификата Privacy Manager

Для доступа к функциям Privacy Manager необходимо запросить и установить сертификат Privacy Manager (из Privacy Manager), используя действительный адрес электронной почты. Адрес электронной почты необходимо задать как учетную запись в Microsoft Outlook на том же компьютере, с которого запрашивается сертификат Privacy Manager.

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Выберите **Запросить сертификат Privacy Manager**.
3. Прочтите текст на странице «Добро пожаловать» и щелкните **Далее**.
4. Ознакомьтесь с лицензионным соглашением на странице «Лицензионное соглашение».
5. Убедитесь, что флажок рядом с пунктом **Установите флажок, чтобы принять условия лицензионного соглашения** установлен, а затем щелкните **Далее**.
6. Введите необходимую информацию на странице «Сведения о вашем сертификате» и щелкните **Далее**.
7. На странице «Запрос сертификата принят» щелкните **Готово**.

Вы получите сообщение электронной почты через Microsoft Outlook с сертификатом Privacy Manager во вложении.

Получение предварительно назначенного корпоративного сертификата Privacy Manager

1. В Outlook откройте полученное сообщение электронной почты, в котором указано, что вам предварительно назначен корпоративный сертификат.
2. Щелкните **Получить**.

Вы получите сообщение электронной почты через Microsoft Outlook с сертификатом Privacy Manager во вложении.

Чтобы установить сертификат, см. Настройка сертификата Privacy Manager на стр. 63.

Настройка сертификата Privacy Manager

1. После получения сообщения электронной почты с сертификатом Privacy Manager во вложении откройте это сообщение и нажмите кнопку **Установить** в правом нижнем углу сообщения (в Outlook 2007 или Outlook 2010) или в левом верхнем углу (в Outlook 2003).
2. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
3. На странице «Сертификат установлен» щелкните **Далее**.
4. На странице «Резервное копирование сертификата» укажите расположение и имя файла резервной копии или щелкните **Обзор**, чтобы перейти к его расположению.

⚠ **ПРЕДУПРЕЖДЕНИЕ.** Сохраните файл в расположении, не находящемся на жестком диске, и храните его в безопасном месте. Файл предназначен для личного использования и необходим для восстановления сертификата Privacy Manager и соответствующих ключей.

5. Введите и подтвердите пароль, а затем щелкните **Далее**.
6. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
7. Если требуется начать процесс приглашения доверенного контакта, следуйте инструкциям на экране, начиная с шага 2 раздела Добавление доверенных контактов с использованием контактов Microsoft Outlook на стр. 68.

   – или –

   Если нажать **Отмена**, см. Управление доверенными контактами на стр. 66 для получения сведений о добавлении доверенного контакта позже.

Импорт стороннего сертификата

Вы, возможно, сможете выполнить импорт стороннего сертификата в Privacy Manager с помощью мастера импорта сертификата.

Для использования этой функции параметр **Позволить использование стороннего сертификата** в консоли администрирования HP ProtectTools должен быть включен на странице «Параметры» под разделом **Privacy Manager**.

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Перейдите на вкладку **Certificate Manager** и щелкните **Импортировать сертификаты**.

   Эта кнопка не отображается, если импорт сертификатов запрещен.
3. Выберите импорт сертификата, уже установленного на данный компьютер, или сертификата, сохраненного в качестве файла PFX (Personal Information Exchange/ PKCS#12), и щелкните **Далее**.

   - Для импорта сертификата, установленного на данный компьютер, выберите нужный сертификат и щелкните **Далее**.
   - Чтобы выбрать сертификат PFX, щелкните **Обзор**, перейдите к папке, в которой содержится файл PFX, и щелкните **Далее**. Введите пароль для файла PFX и щелкните **Далее**.
4. Когда процесс импорта будет завершен, щелкните **Далее**.
5. У вас есть возможность резервного копирования импортированного сертификата.

   Рекомендуется сохранять резервную копию в папку, расположенную не на жестком диске вашего компьютера.

Просмотр сведений о сертификате Privacy Manager

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Щелкните Сертификат Privacy Manager.
3. Щелкните **Сведения о сертификате**.
4. После просмотра сведений щелкните **ОК**.

Обновление сертификата Privacy Manager

Когда срок действия сертификата Privacy Manager будет близок к завершению, вы получите уведомление о необходимости его обновления:

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Щелкните **Обновить сертификат**.
3. Следуйте инструкциям на экране для получения нового сертификата Privacy Manager.

ПРИМЕЧАНИЕ. В процессе обновления сертификата Privacy Manager прежний сертификат Privacy Manager не замещается. Получите новый сертификат Privacy Manager и установите его, следуя процедуре, описанной в Запрос сертификата Privacy Manager на стр. 62.

Для корпоративных сертификатов, выданных вашей компанией с использованием Microsoft Certificate Authority, администратор CA обновит ваш сертификат с помощью того же личного ключа, который использовался в первоначальном сертификате, или же оформит новый сертификат, используя тот же личный ключ.

Настройка сертификата Privacy Manager по умолчанию

В Privacy Manager отображаются только сертификаты Privacy Manager, даже если на компьютеры установлены дополнительные сертификаты от других центров сертификации.

Если на компьютере имеется несколько сертификатов Privacy Manager, установленных из Privacy Manager, можно указать один сертификат по умолчанию.

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Щелкните сертификат Privacy Manager, который следует использовать по умолчанию, и нажмите **По умолчанию**.
3. Щелкните **ОК**.

ПРИМЕЧАНИЕ. Сертификат Privacy Manager, установленный по умолчанию, использовать необязательно. Из функций Privacy Manager можно выбрать использование любого сертификата Privacy Manager.

Удаление сертификата Privacy Manager

После удаления сертификата Privacy Manager вы не сможете открывать файлы или просматривать данные, зашифрованные при помощи этого сертификата. Если сертификат Privacy Manager был удален случайно, его можно восстановить из файла резервной копии, созданного в процессе установки сертификата. Подробнее см. Восстановление сертификата Privacy Manager на стр. 65.

Для удаления сертификата Privacy Manager выполните следующие действия.

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Щелкните сертификат Privacy Manager, который следует удалить, и нажмите **Дополнительно**.
3. Нажмите **Удалить**.
4. При появлении диалогового окна подтверждения щелкните **Да**.
5. Щелкните **Закрыть**, а затем **Применить**.

Восстановление сертификата Privacy Manager

В процессе установки сертификата Privacy Manager необходимо создать резервную копию сертификата. Резервную копию также можно создать на странице «Перенос». Резервную копию можно использовать при переносе на другой компьютер или для восстановления сертификата на том же компьютере.

1. Откройте Privacy Manager и щелкните **Перенос**.
2. Щелкните **Восстановить**.
3. На странице «Файл переноса» щелкните **Обзор**, чтобы перейти к файлу DPPSM, созданному в процессе резервного копирования, и нажмите **Далее**.
4. Введите пароль, использованный при создании резервной копии, и щелкните **Далее**.
5. Щелкните **Готово**.

Подробнее см. Настройка сертификата Privacy Manager на стр. 63 или Резервное копирование сертификатов Privacy Manager и доверенных контактов на стр. 76.

Отзыв сертификата Privacy Manager

Если у вас возникли опасения, что ваш сертификат Privacy Manager подвергается риску, его можно отозвать:

ПРИМЕЧАНИЕ. Отозванный сертификат Privacy Manager не удаляется. Этот сертификат по-прежнему можно использовать для просмотра шифруемых файлов.

1. Откройте Privacy Manager и щелкните **Сертификаты**.
2. Щелкните **Дополнительно**.
3. Щелкните сертификат Privacy Manager, который следует отозвать, и нажмите **Отозвать**.
4. При появлении диалогового окна подтверждения щелкните **Да**.
5. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
6. Следуйте инструкциям на экране.

Управление доверенными контактами

Доверенный контакт — это пользователь, с которым вы обменялись сертификатами Privacy Manager, что обеспечивает надежную связь с этим пользователем.

Trusted Contacts Manager позволяет выполнять следующие задачи.

- Просмотр сведений о доверенных контактах
- Удаление доверенных контактов
- Проверка состояния отзыва для доверенных контактов (дополнительно)

Добавление доверенных контактов

Добавление доверенных контактов производится в 3 шага:

1. Вы отправляете доверенному контакту приглашение по электронной почте.
2. Доверенный контакт отвечает на ваше сообщение.
3. После получения ответа по электронной почте от доверенного контакта нажмите **Принять**.

Приглашения по электронной почте для доверенных контактов можно направлять отдельным получателям или всем контактам в адресной книге Microsoft Outlook.

Для добавления доверенных контактов см. следующие разделы.

ПРИМЕЧАНИЕ. Чтобы ответить на приглашение стать доверенным контактом, у получателей на компьютерах должен быть установлен Privacy Manager или альтернативный клиент. Сведения об установке альтернативного клиента см. на веб-сайте DigitalPersona по адресу http://digitalpersona.com/privacymanager/download.

Добавление доверенного контакта

1. Откройте Privacy Manager, щелкните **Trusted Contacts Manager** и нажмите **Пригласить контакты**.

   – или –

   В Microsoft Outlook щелкните стрелку вниз рядом с пунктом **Безопасная отправка** на панели инструментов, а затем выберите **Пригласить контакты**.

2. Если откроется диалоговое окно «Выбрать сертификат» щелкните сертификат Privacy Manager, который следует использовать, и нажмите **ОК**.

3. При появлении диалогового окна «Приглашение доверенного контакта» ознакомьтесь с информацией и щелкните **ОК**.

   Автоматически создается сообщение электронной почты.

4. Введите электронный адрес получателей, которых нужно добавить в качестве доверенных контактов.

5. Внесите изменения в текст и поставьте подпись (необязательно).

6. Щелкните **Отправить**.

ПРИМЕЧАНИЕ. Если вы не получили сертификат Privacy Manager, появится сообщение о том, что для отправки запроса доверенного контакта необходим сертификат Privacy Manager. Нажмите **ОК**, чтобы запустить мастер запроса сертификата. Подробнее см. Запрос сертификата Privacy Manager на стр. 62.

7. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

ПРИМЕЧАНИЕ. После получения сообщения электронной почты получателем доверенного контакта, он должен открыть это сообщение и щелкнуть **Принять** в правом нижнем углу сообщения, а затем нажать **ОК**, когда откроется диалоговое окно подтверждения.

8. После получения ответа по электронной почте от получателя, который принимает приглашение стать доверенным контактом, щелкните **Принять** в правом нижнем углу сообщения.

   Откроется диалоговое окно с подтверждением добавления получателя в список доверенных контактов.

9. Нажмите **ОК**.

Добавление доверенных контактов с использованием контактов Microsoft Outlook

1. Откройте Privacy Manager, щелкните **Trusted Contacts Manager** и нажмите **Пригласить контакты**.

   – или –

   В Microsoft Outlook щелкните стрелку вниз рядом с пунктом **Безопасная отправка** на панели инструментов, а затем выберите **Пригласить мои контакты Outlook**.

2. Когда откроется страница «Приглашение доверенного контакта», выберите электронные адреса получателей, которых нужно добавить в качестве доверенных контактов, и щелкните **Далее**.

3. Когда откроется страница «Отправка приглашения», щелкните **Готово**.

   Автоматически создается сообщение электронной почты, в котором приведены выбранные электронные адреса Microsoft Outlook.

4. Внесите изменения в текст и поставьте подпись (необязательно).

5. Щелкните **Отправить**.

ПРИМЕЧАНИЕ. Если вы не получили сертификат Privacy Manager, появится сообщение о том, что для отправки запроса доверенного контакта необходим сертификат Privacy Manager. Нажмите **ОК**, чтобы запустить мастер запроса сертификата. Подробнее см. Запрос сертификата Privacy Manager на стр. 62.

6. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

ПРИМЕЧАНИЕ. После получения сообщения электронной почты получателем доверенного контакта, он должен открыть это сообщение и щелкнуть **Принять** в правом нижнем углу сообщения, а затем нажать **ОК**, когда откроется диалоговое окно подтверждения.

7. После получения ответа по электронной почте от получателя, который принимает приглашение стать доверенным контактом, щелкните **Принять** в правом нижнем углу сообщения.

   Откроется диалоговое окно с подтверждением добавления получателя в список доверенных контактов.

8. Нажмите **ОК**.

Просмотр сведений о доверенных контактах

1. Откройте Privacy Manager и щелкните **Доверенные контакты**.

2. Щелкните Доверенный контакт.

3. Щелкните **Сведения о контакте**.

4. После просмотра сведений щелкните **ОК**.

Удаление доверенного контакта

1. Откройте Privacy Manager и щелкните **Доверенные контакты**.
2. Щелкните доверенный контакт, который нужно удалить.
3. Щелкните **Удалить контакт**.
4. При появлении диалогового окна подтверждения щелкните **Да**.

Проверка состояния отзыва для доверенного контакта

Чтобы узнать, был ли сертификат Privacy Manager отозван доверенным контактом, выполните следующие действия.

1. Откройте Privacy Manager и щелкните **Доверенные контакты**.
2. Щелкните Доверенный контакт.
3. Нажмите кнопку **Дополнительно**.

   Откроется диалоговое окно «Расширенное управление доверенными контактами».
4. Нажмите **Проверить отзыв**.
5. Щелкните **Закрыть**.

Общие задачи

Privacy Manager может использоваться со следующими продуктами Microsoft.

- Microsoft Outlook
- Microsoft Office

Использование Privacy Manager с Microsoft Outlook

Когда Privacy Manager установлен, на панели инструментов Microsoft Outlook отображается кнопка «Конфиденциальность», а на панели инструментов каждого сообщения Microsoft Outlook отображается кнопка «Безопасная отправка». При нажатии стрелки вниз рядом с кнопками **Конфиденциальность** или **Безопасная отправка** можно выбрать следующие функции.

- **Подписать и отправить сообщение** (только кнопка «Безопасная отправка») — эта функция добавляет цифровую подпись в сообщение электронной почты и отправляет его после проверки подлинности с использованием выбранного способа безопасного входа в систему.
- **Запечатать для доверенных контактов и отправить сообщение** (только кнопка «Безопасная отправка») — эта функция добавляет цифровую подпись, шифрует сообщение электронной почты и отправляет его после проверки подлинности с использованием выбранного способа безопасного входа в систему.
- **Пригласить контакты** — эта функция позволяет отправлять приглашение доверенному контакту. Подробнее см. Добавление доверенного контакта на стр. 67.
- **Пригласить контакты Outlook** — эта функция позволяет отправлять приглашение стать доверенным контактом всем контактам в адресной книге Microsoft Outlook. Подробнее см. Добавление доверенных контактов с использованием контактов Microsoft Outlook на стр. 68.
- **Открыть Privacy Manager** — функции «Сертификаты», «Доверенные контакты» и «Параметры» позволяют открыть Privacy Manager для добавления, просмотра или изменения текущих параметров. Подробнее см. Управление сертификатами Privacy Manager на стр. 62, Управление доверенными контактами на стр. 66 или Настройка Privacy Manager для Microsoft Outlook на стр. 70.

Настройка Privacy Manager для Microsoft Outlook

1. Откройте Privacy Manager, щелкните **Параметры** и выберите вкладку **Электронная почта**.

   – или –

   На главной панели инструментов Microsoft Outlook щелкните стрелку вниз рядом с **Безопасная отправка** (**Конфиденциальность** в Outlook 2003) и нажмите **Параметры**.

   – или –

   На панели инструментов сообщения электронной почты Microsoft щелкните стрелку вниз рядом с пунктом **Безопасная отправка**, а затем нажмите **Параметры**.

2. Выберите нужные действия при отправке защищенной электронной почты и нажмите **ОК**.

Подписание и отправка сообщения электронной почты

1. В Microsoft Outlook щелкните **Создать** или **Ответить**.
2. Введите тело электронного сообщения.
3. Щелкните стрелку вниз рядом с **Безопасная отправка** (**Конфиденциальность** в Outlook 2003), а затем нажмите **Подписать и отправить**.
4. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

Запечатывание и отправка сообщения электронной почты

Запечатанные сообщения электронной почты, имеющие цифровую подпись и печать (зашифрованные) могут просматриваться только пользователями, указанными в списке доверенных контактов.

Чтобы запечатать и отправить сообщение доверенному контакту, выполните следующие действия.

1. В Microsoft Outlook щелкните **Создать** или **Ответить**.
2. Введите тело электронного сообщения.
3. Щелкните стрелку вниз рядом с **Безопасная отправка** (**Конфиденциальность** в Outlook 2003), а затем нажмите **Запечатать для доверенных контактов и отправить**.
4. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

Просмотр запечатанного сообщения электронной почты

При открытии запечатанного сообщения в заголовке сообщения электронной почты отображается метка уровня безопасности. Метка уровня безопасности предоставляет следующие сведения:

- Какие учетные данные использовались для проверки личных данных подписавшего сообщение
- Продукт, использовавшийся для проверки учетных данных подписавшего сообщение

Использование Privacy Manager в документах Microsoft Office 2007

После установки сертификата Privacy Manager Certificate на правой стороне панели инструментов всех документов Microsoft Word, Microsoft Excel и Microsoft PowerPoint отображается кнопка «Подписать и зашифровать». При нажатии стрелки вниз рядом с **Подписать и зашифровать**, можно выбрать следующие функции.

- **Подписать документ** — данная функция добавляет цифровую подпись к документу.
- **Добавить строку подписи перед подписанием** (только в Microsoft Word и Microsoft Excel) — по умолчанию строка подписи добавляется, когда выполняется подписание или шифрование документа Microsoft Word или Microsoft Excel. Для отключения этой функции щелкните **Добавить строку подписи**, чтобы снять флажок.
- **Зашифровать документ** — данная функция добавляет цифровую подпись и шифрует документ.

- **Снять шифрование** — данная функция снимает шифрование с документа.
- **Открыть Privacy Manager** — функции «Сертификаты», «Доверенные контакты» и «Параметры» позволяют открыть Privacy Manager для добавления, просмотра или изменения текущих параметров. Подробнее см. Управление сертификатами Privacy Manager на стр. 62, Управление доверенными контактами на стр. 66 или Настройка Privacy Manager для Microsoft Office на стр. 72.

Настройка Privacy Manager для Microsoft Office

1. Откройте Privacy Manager, щелкните **Параметры** и выберите вкладку **Документы**.

   – или –

   На панели инструментов документа Microsoft Office щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем выберите **Параметры**.

2. Выберите настраиваемые действия и нажмите **ОК**.

Подписание документа Microsoft Office

1. Создайте и сохраните документ в Microsoft Word, Microsoft Excel или Microsoft PowerPoint.
2. Щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем нажмите **Подписать документ**.
3. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
4. При появлении диалогового окна подтверждения ознакомьтесь с информацией и щелкните **ОК**.

Если позже потребуется изменить документ, выполните следующие действия.

1. Нажмите кнопку **Office** в левом верхнем углу экрана.
2. Щелкните **Подготовить**, а затем **Пометить как окончательный**.
3. При появлении диалогового окна подтверждения щелкните **Да** и продолжите работу.
4. После внесения изменений снова подпишите документ.

Добавление строки подписи при подписании документа Microsoft Word или Microsoft Excel

Privacy Manager позволяет добавлять строку подписи при подписании документа Microsoft Word или Microsoft Excel:

1. Создайте и сохраните документ в Microsoft Word или Microsoft Excel.
2. Щелкните меню **Начальная страница**.
3. Щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем нажмите **Добавить строку подписи**.

ПРИМЕЧАНИЕ. Если функция «Добавить строку подписи перед подписанием» выбрана, рядом с ней стоит флажок. По умолчанию эта функция включена.

4. Щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем нажмите **Подписать документ**.

5. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

Добавление предполагаемых подписантов в документ Microsoft Word или Microsoft Excel

В документ можно добавить несколько строк подписи, назначив предполагаемых подписантов. Предполагаемый подписант — это пользователь, который назначен владельцем документа Microsoft Word или Microsoft Excel для добавления строки подписи в документ. Предполагаемыми подписантами можете быть вы или иной пользователь, который может подписать документ по вашему желанию. Например, если вы готовите документ, который должны подписать все члены вашего отдела, вы можете добавить строки подписи для этих пользователей внизу последней страницы документа с указаниями подписать к определенной дате.

Для добавления предполагаемого подписанта в документ Microsoft Word или Microsoft Excel выполните следующие действия.

1. Создайте и сохраните документ в Microsoft Word или Microsoft Excel.

2. Щелкните меню **Вставка**.

3. В группе **Текст** на панели инструментов щелкните стрелку вниз рядом с пунктом **Строка подписи** и нажмите **Поставщик подписи Privacy Manager**.

   Откроется диалоговое окно «Настройка подписи».

4. В окне под пунктом **Предполагаемый подписант** введите имя предполагаемого подписанта.

5. В окне под пунктом **Указания подписанту** введите сообщение для предполагаемого подписанта.

ПРИМЕЧАНИЕ. Это сообщение отобразится на месте заголовка и при подписании документа будет удалено или заменено должностью пользователя.

6. Установите флажок **Показать дату подписания в строке подписи**, чтобы отобразилась дата.

7. Установите флажок **Показать должность подписанта в строке подписи**, чтобы отобразилась должность.

ПРИМЕЧАНИЕ. Владелец документа назначает предполагаемых подписантов для своего документа. Флажки **Показать дату подписания в строке подписи** и/или **Показать должность подписанта в строке подписи** должны быть установлены для того, чтобы предполагаемый подписант мог указать дату и/или заголовок в строке подписи.

8. Нажмите **ОК**.

Добавление строки подписи предполагаемого подписанта

Когда предполагаемые подписанты откроют документ, их имена будут указаны в скобках, что обозначает необходимость их подписи.

Чтобы подписать документ, выполните следующие действия.

1. Дважды щелкните нужную строку подписи.
2. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.

   Строка подписи будет показана согласно параметрам, заданным владельцем документа.

Шифрование документа Microsoft Office

Документ Microsoft Office можно зашифровать для вас и ваших доверенных контактов. Если документ зашифрован и закрыт, вы и доверенные контакты из списка должны выполнить проверку подлинности перед его открытием.

Чтобы зашифровать документ Microsoft Office, выполните следующие действия.

1. Создайте и сохраните документ в Microsoft Word, Microsoft Excel или Microsoft PowerPoint.
2. Щелкните меню **Начальная страница**.
3. Щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем нажмите **Зашифровать**.

   Откроется диалоговое окно «Выберите доверенные контакты».
4. Щелкните имя доверенного контакта, который сможет открывать документ и просматривать его содержимое.

   ПРИМЕЧАНИЕ. Чтобы выбрать несколько имен доверенных контактов, удерживайте клавишу ctrl и выберите нужные имена.
5. Нажмите **ОК**.

Если позже потребуется изменить документ, выполните действия, указанные в Снятие шифрования с документа icrosoft Office на стр. 74. После снятия шифрования в документ можно вносить изменения. Чтобы повторно зашифровать документ, выполните действия в данном разделе.

Снятие шифрования с документа icrosoft Office

После снятия шифрования с документа Microsoft Office вам и вашим Доверенным контактам больше не требуется выполнять проверку подлинности, чтобы открывать и просматривать его содержимое.

Чтобы снять шифрование с документа Microsoft Office, выполните следующие действия.

1. Откройте зашифрованный документ документ Microsoft Word, Microsoft Excel или Microsoft PowerPoint.
2. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
3. Щелкните меню **Начальная страница**.
4. Щелкните стрелку вниз рядом с **Подписать и зашифровать**, а затем нажмите **Снять шифрование**.

Отправка зашифрованного документа Microsoft Office

Зашифрованный документ Microsoft Office можно приложить к электронному сообщению без подписания или шифрования самого сообщения. Для этого создайте и отправьте сообщение электронной почты с подписанным или зашифрованным документом как обычное сообщение с вложением.

Однако в целях обеспечения максимальной безопасности рекомендуется зашифровать сообщение электронной почты при прикреплении подписанного или зашифрованного документа Microsoft Office.

Чтобы отправить запечатанное сообщение электронной почты с подписанным и/или зашифрованным документом Microsoft Office, выполните следующие действия.

1. В Microsoft Outlook щелкните **Создать** или **Ответить**.
2. Введите тело электронного сообщения.
3. Вложите документ Microsoft Office.
4. Подробнее см. Запечатывание и отправка сообщения электронной почты на стр. 71.

Просмотр подписанного документа Microsoft Office

ПРИМЕЧАНИЕ. Для просмотра подписанного документа Microsoft Office необязательно иметь сертификат Privacy Manager.

При открытии подписанного документа Microsoft Office в строке состояния внизу окна документа появится значок «Цифровая подпись».

1. Щелкните значок **Цифровые подписи**, чтобы переключить отображение диалогового окна «Подписи», в котором отображаются имена всех пользователей, подписавших документ, и дату подписания каждым пользователем.
2. Для просмотра дополнительных сведений о каждой подписи правой кнопкой мыши щелкните имя в диалоговом окне «Подписи» и выберите **Сведения о подписях**.

Просмотр зашифрованного документа Microsoft Office

Для просмотра зашифрованного документа Microsoft Office на другом компьютере необходимо установить Privacy Manager. Также необходимо восстановить Сертификат Privacy Manager, который использовался для шифрования файла.

Если ваш сертификат был утерян, для просмотра зашифрованного документа Microsoft Office необходимо восстановить сертификат Privacy Manager, который использовался при шифровании файла.

Если обладателю доверенного контакта требуется просмотреть зашифрованный документ Microsoft Office, ему необходим сертификат Privacy Manager и установленный на компьютере Privacy Manager. Кроме того, доверенный контакт должен быть выбран владельцем зашифрованного документа Microsoft Office.

Дополнительные задачи

Перенос сертификатов Privacy Manager и доверенных контактов на другой компьютер

Сертификаты Privacy Manager и Доверенные контакты можно безопасно перенести на другой компьютер или выполнить резервное копирование для сохранности данных. Для этого выполните резервное копирование данных в файл, защищенный паролем, в сети или на съемном запоминающем устройстве, а затем восстановите файл на другом компьютере.

Резервное копирование сертификатов Privacy Manager и доверенных контактов

Для резервного копирования сертификатов Privacy Manager и доверенных контактов в файл, защищенный паролем, выполните следующие действия.

1. Откройте Privacy Manager и щелкните **Перенос**.
2. Щелкните **Резервное копирование**.
3. На странице «Выберите данные», укажите категории данных, которые следует включить в файл переноса, и щелкните **Далее**.
4. На странице «Файл переноса» укажите имя файла или щелкните **Обзор**, чтобы перейти к расположению, а затем нажмите **Далее**.
5. Введите и подтвердите пароль, а затем щелкните **Далее**.

ПРИМЕЧАНИЕ. Храните пароль в безопасном месте: он понадобится для восстановления файла переноса.

6. Выполните проверку подлинности с применением выбранного способа безопасного входа в систему.
7. На странице «Файл переноса сохранен» щелкните **Готово**.

Восстановление сертификатов Privacy Manager и доверенных контактов

Для восстановления сертификатов Privacy Manager и доверенных контактов на другом компьютере в рамках процесса переноса или на том же компьютере выполните следующие действия.

1. Откройте Privacy Manager и щелкните **Перенос**.
2. Щелкните **Восстановить**.
3. На странице «Файл переноса» щелкните **Обзор**, чтобы перейти к файлу, а затем нажмите **Далее**.
4. Введите пароль, использованный при создании файла резервной копии, и щелкните **Далее**.
5. На странице «Файл переноса» щелкните **Готово**.

Центр администрирования Privacy Manager

Ваш экземпляр Privacy Manager может являться частью централизованной установки, настроенной вашим администратором. Можно включить или отключить одну или несколько из следующих функций.

- **Политика использования сертификатов** — вас могут ограничить использованием сертификатов Privacy Manager, выданных Comodo, или вам может быть разрешено использовать цифровые сертификаты, выданные другими центрами сертификации.
- **Политика шифрования** — возможности шифрования могут быть включены или отключены в Microsoft Office или Microsoft Outlook.

7 File Sanitizer for HP ProtectTools

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

ПРИМЕЧАНИЕ. Данная версия File Sanitizer поддерживает только жесткий диск компьютера.

Уничтожение

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

При выборе профиля уничтожения (**Высокая безопасность**, **Средняя безопасность** или **Низкая безопасность**) автоматически определяется список ресурсов и метод их стирания. Также можно настроить профиль уничтожения, указав количество циклов уничтожения, ресурсы на уничтожение, ресурсы для подтверждения перед уничтожением и ресурсы на удаление из списка на уничтожение. Подробнее см. Выбор или создание профиля уничтожения на стр. 83.

Можно установить автоматическое расписание уничтожения, а также можно вручную запустить процесс уничтожения с помощью значка **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач. Подробнее см. Настройка расписания уничтожения на стр. 82, Уничтожение отдельного ресурса вручную на стр. 87 или Уничтожение всех выбранных элементов вручную на стр. 88.

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

Очистка свободного пространства

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

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

ПРИМЕЧАНИЕ. Очистку свободного пространства можно выполнять от случая к случаю для ресурсов, удаленных посредством выбора **Параметры простого удаления** в программе File Sanitizer, посредством перемещения в корзину Windows или посредством удаления ресурсов вручную. Очистка свободного пространства исключает какую-либо защиту уничтоженных ресурсов.

Можно установить автоматическое расписание очистки свободного пространства, а также можно вручную запустить процесс очистки свободного пространства с помощью значка **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач. Подробнее см. Установка расписания очистки свободного пространства на стр. 82 или Запуск очистки свободного пространства вручную на стр. 88.

Открытие программы File Sanitizer

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.
2. Щелкните **File Sanitizer**.

– или –

- Дважды щелкните значок **File Sanitizer** на рабочем столе.

– или –

- Щелкните правой кнопкой значок **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач, выберите **File Sanitizer** и далее **Открыть File Sanitizer**.

Процедуры настройки

Настройка расписания уничтожения

Можно выбрать предопределенный профиль уничтожения или создать собственный. Подробнее см. Выбор или создание профиля уничтожения на стр. 83. Также можно в любое время удалить ресурсы вручную. Подробнее см. Использование последовательности клавиш для запуска уничтожения на стр. 86.

ПРИМЕЧАНИЕ. Запланированное задание запускается в определенное время. Если в запланированное время система отключена или находится в режиме сна или ожидания, программа File Sanitizer не будет пытаться повторно запустить задание.

1. Откройте File Sanitizer и щелкните **Уничтожить**.
2. Выберите один или несколько параметров уничтожения:
   - **Завершение работы Windows** — уничтожает все выбранные ресурсы при выключении Windows.

     ПРИМЕЧАНИЕ. При выключении открывается диалоговое окно, запрашивающее подтверждение уничтожения выбранных ресурсов.

     Щелкните **Да** для отмены уничтожения или **Нет** для выполнения уничтожения.
   - **Открытие веб-браузера** — уничтожает все выбранные ресурсы сети, например, URL-журнала браузера при открытии браузера.
   - **Закрытие веб-браузера** — уничтожает все выбранные ресурсы сети, например, URL-журнала браузера при закрытии браузера.
   - **Последовательность клавиш** — позволяет задавать последовательность клавиш для запуска процесса уничтожения. Подробнее см. Использование последовательности клавиш для запуска уничтожения на стр. 86.

   ПРИМЕЧАНИЕ. Файл DLL уничтожается и удаляется из системы только в том случае, если он был перемещен в корзину.
3. Чтобы запланировать время для уничтожения выбранных ресурсов, установите флажок **Запустить средство установки расписания**, введите пароль Windows и выберите день и время.
4. Щелкните **Применить**.

Установка расписания очистки свободного пространства

Очистку свободного пространства можно выполнять от случая к случаю для ресурсов, удаленных посредством выбора **Параметры простого удаления** в программе File Sanitizer, посредством перемещения в корзину Windows или посредством удаления ресурсов вручную. Очистка свободного пространства исключает какую-либо защиту уничтоженных ресурсов.

ПРИМЕЧАНИЕ. Запланированное задание запускается в определенное время. Если в запланированное время система отключена или находится в режиме сна или ожидания, программа File Sanitizer не будет пытаться повторно запустить задание.

1. Откройте File Sanitizer и щелкните **Очистка**.
2. Чтобы запланировать время для очистки удаленных данных с жесткого диска, установите флажок **Запустить средство установки расписания**, введите пароль Windows и выберите день и время.
3. Щелкните **Применить**.

ПРИМЕЧАНИЕ. Процесс очистки свободного пространства может занять достаточно длительное время. Хотя очистка свободного пространства выполняется в фоновом режиме, повышенное использование процессора может повлиять на производительность компьютера.

Выбор или создание профиля уничтожения

Можно указать метод стирания и выбрать ресурсы на уничтожение, выбрав предопределенный профиль или создав собственный профиль.

Выбор предопределенного профиля уничтожения

При выборе предопределенного профиля уничтожения автоматически определяется список ресурсов и метод их стирания. Также можно просматривать предопределенный список ресурсов, выбранных на уничтожение.

1. Откройте File Sanitizer и щелкните **Параметры**.
2. Щелкните предопределенный профиль уничтожения:
   - **Высокая защита**
   - **Средняя защита**
   - **Низкая защита**
3. Для просмотра ресурсов, выбранных на уничтожение, щелкните **Просмотр подробных сведений**.
   a. **Выбранные элементы будут уничтожены, и отобразится подтверждающее сообщение. Невыбранные элементы будут уничтожены без подтверждающего сообщения.** — установите флажок для отображения подтверждающего сообщения до уничтожения элемента или снимите флажок для уничтожения элемента без отображения подтверждающего сообщения.

      ПРИМЕЧАНИЕ. Даже если для ресурса флажок снят, этот актив будет уничтожен.

   б. Щелкните **Применить**.
4. Щелкните **Применить**.

Настройка профиля уничтожения

При создании профиля уничтожения можно указать количество циклов уничтожения, ресурсы на уничтожение, ресурсы для подтверждения перед уничтожением и ресурсы на удаление из списка на уничтожение.

1. Откройте File Sanitizer, щелкните **Параметры**, выберите **Расширенные параметры безопасности** и щелкните **Просмотр подробных сведений**.
2. Выберите количество циклов уничтожения.

ПРИМЕЧАНИЕ. Выбранное количество циклов уничтожения будет выполнено для каждого ресурса. Например, если выбрано 3 цикла уничтожения, алгоритм затемнения данных выполняется 3 раза. Если выбраны циклы уничтожения высокой безопасности, процесс уничтожения может занять достаточно длительное время. Однако, чем больше циклов уничтожения, тем меньше вероятность восстановления этих данных.

3. Чтобы выбрать ресурсы, которые нужно уничтожить, выполните следующие действия.
   a. Под пунктом **Доступные параметры уничтожения** выберите ресурс и щелкните **Добавить**.
   б. Для добавления специального ресурса щелкните **Добавить специальный параметр**, затем выберите или введите путь к файлу или папке.
   в. Щелкните **Открыть** и далее **ОК**.
   г. Под пунктом **Доступные параметры уничтожения** выберите специальный ресурс и щелкните **Добавить**.

   Для удаления ресурса из доступных параметров уничтожения выберите ресурс и щелкните **Удалить**.
4. **Выбранные элементы будут уничтожены, и отобразится подтверждающее сообщение. Невыбранные элементы будут уничтожены без подтверждающего сообщения.** — установите флажок для отображения подтверждающего сообщения до уничтожения элемента или снимите флажок для уничтожения элемента без отображения подтверждающего сообщения.

ПРИМЕЧАНИЕ. Даже если для ресурса флажок снят, этот актив будет уничтожен.

   Для удаления ресурса из списка на уничтожение выберите ресурс и щелкните **Удалить**.
5. Чтобы защитить файлы и папки от автоматического уничтожения, выполните следующие действия.
   a. Под пунктом **Не уничтожать следующие объекты** щелкните **Добавить**, а затем выберите или введите путь к файлу или папке.
   б. Щелкните **Открыть** и далее **ОК**.

   Для удаления ресурса из списка на исключение выберите ресурс и щелкните **Удалить**.
6. Щелкните **Применить**.

Настройка профиля простого удаления

Профиль простого удаления выполняет стандартное удаление ресурса без его уничтожения. Можно настроить профиль простого удаления, указав ресурсы на простое удаление, ресурсы для подтверждения перед выполнением простого удаления и ресурсы на удаление из списка на простое удаление.

ПРИМЕЧАНИЕ. При выборе **Параметры простого удаления** может быть случайно выполнена очистка свободного пространства для ресурсов, удаленных вручную или с помощью корзины Windows.

1. Откройте File Sanitizer, щелкните **Параметры**, выберите **Параметры простого удаления** и щелкните **Просмотр подробных сведений**.
2. Выберите ресурсы, которые нужно удалить.
   a. Под пунктом **Доступные параметры удаления** выберите ресурс и щелкните **Добавить**.
   б. Для добавления специального ресурса щелкните **Добавить специальный параметр**, выберите или введите путь к имени файла или папки, а затем щелкните **ОК**.
   в. Выберите специальный ресурс и щелкните **Добавить**.

   Для удаления ресурса из доступных параметров удаления выберите ресурс и щелкните **Удалить**.
3. **Выбранные элементы будут уничтожены, и отобразится подтверждающее сообщение. Невыбранные элементы будут уничтожены без подтверждающего сообщения.** — установите флажок для отображения подтверждающего сообщения до уничтожения элемента или снимите флажок для уничтожения элемента без отображения подтверждающего сообщения.

   ПРИМЕЧАНИЕ. Даже если для ресурса флажок снят, этот актив будет уничтожен.

   Для удаления ресурса из списка на удаление выберите ресурс и щелкните **Удалить**.
4. Для защиты ресурсов от автоматического удаления выполните следующие действия.
   a. В разделе **Не удалять следующие объекты** щелкните **Добавить**, а затем выберите или введите путь к файлу или папке.
   б. Щелкните **Открыть** и далее **ОК**.

   Для удаления ресурса из списка на исключение выберите ресурс и щелкните **Удалить**.
5. Щелкните **Применить**.

Общие задачи

File Sanitizer (Очистка файлов) позволяет выполнять следующие задачи.

- Уничтожение данных по нажатию комбинации клавиш. Эта функция позволяет задать сочетание клавиш, например ctrl+alt+s, для уничтожения данных. Дополнительные сведения см. в разделе Использование последовательности клавиш для запуска уничтожения на стр. 86.
- Уничтожение данных с помощью значка File Sanitizer. Эта функция схожа с перетаскиванием объектов в Windows. Дополнительные сведения см. в разделе Использование значка File Sanitizer на стр. 87.
- Уничтожение отдельных или всех выбранных объектов вручную. Эта функция позволяет уничтожать данные вручную, не дожидаясь следующего запланированного цикла уничтожения. Дополнительные сведения см. в разделе Уничтожение отдельного ресурса вручную на стр. 87 или Уничтожение всех выбранных элементов вручную на стр. 88.
- Запуск очистки свободного пространства вручную. Эта функция позволяет вручную запустить очистку свободного пространства. Дополнительные сведения см. в разделе Запуск очистки свободного пространства вручную на стр. 88.
- Прерывание уничтожения или очистки свободного места. Эта функция позволяет остановить выполняемое уничтожение или очистку свободного пространства. Дополнительные сведения см. в разделе Прерывание процесса уничтожения или очистки свободного пространства на стр. 88.
- Просмотр файлов журнала. Эта функция позволяет просмотреть журналы уничтожения и очистки свободного пространства, в которые записываются ошибки и сбои при выполнении последней операции. Дополнительные сведения см. в разделе Просмотр файлов журнала на стр. 88.

ПРИМЕЧАНИЕ. Уничтожение и очистка свободного пространства могут занять длительное время. Хотя уничтожение и очистка свободного места выполняются в фоновом режиме, производительность компьютера может снизиться из-за возросшей загрузки процессора.

Использование последовательности клавиш для запуска уничтожения

1. Откройте File Sanitizer и щелкните **Уничтожить**.
2. Установите флажок **Последовательность клавиш**.
3. В появившемся окне введите символ.
4. Установите флажок **CTRL** или **ALT**, затем установите флажок **SHIFT**.

   Например, для запуска автоматического уничтожения с помощью клавиши s и сочетания клавиш ctrl+shift, введите в окно s, а заетм выберите параметры **CTRL** и **SHIFT**.

ПРИМЕЧАНИЕ. Убедитесь, что выбрана последовательность клавиш, отличающаяся от имеющихся последовательностей клавиш.

Чтобы запустить процесс уничтожения с помощью последовательности клавиш, выполните следующие действия.

1. Нажмите и удерживайте клавишу shift и либо клавишу ctrl, либо alt (или другую указанную комбинацию) во время нажатия выбранного символа.
2. При появлении диалогового окна подтверждения щелкните **Да**.

Использование значка File Sanitizer

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

1. Перейдите к документу или папке на уничтожение.
2. Перетащите ресурс к значку **File Sanitizer** на рабочем столе.
3. При появлении диалогового окна подтверждения щелкните **Да**.

Уничтожение отдельного ресурса вручную

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

1. Щелкните правой кнопкой значок **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач, выберите **File Sanitizer** и далее **Уничтожить один ресурс**.
2. При появлении диалогового окна поиска перейдите к ресурсу на уничтожение и нажмите **OK**.

ПРИМЕЧАНИЕ. Выбранным ресурсом может быть отдельный файл или папка.

3. При появлении диалогового окна подтверждения щелкните **Да**.

– или –

1. Щелкните правой кнопкой мыши значок **File Sanitizer** на рабочем столе и выберите **Уничтожить один ресурс**.
2. При появлении диалогового окна поиска перейдите к ресурсу на уничтожение и нажмите **OK**.
3. При появлении диалогового окна подтверждения щелкните **Да**.

– или –

1. Откройте File Sanitizer и щелкните **Уничтожить**.
2. Нажмите кнопку **Обзор**.
3. При появлении диалогового окна поиска перейдите к ресурсу на уничтожение и нажмите **OK**.
4. При появлении диалогового окна подтверждения щелкните **Да**.

Уничтожение всех выбранных элементов вручную

1. Щелкните правой кнопкой значок **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач, выберите **File Sanitizer** и далее **Уничтожить сейчас**.
2. При появлении диалогового окна подтверждения щелкните **Да**.

– или –

1. Щелкните правой кнопкой мыши значок **File Sanitizer** на рабочем столе и выберите **Уничтожить сейчас**.
2. При появлении диалогового окна подтверждения щелкните **Да**.

– или –

1. Откройте File Sanitizer и щелкните **Уничтожить**.
2. Нажмите кнопку **Уничтожить сейчас**.
3. При появлении диалогового окна подтверждения щелкните **Да**.

Запуск очистки свободного пространства вручную

1. Щелкните правой кнопкой значок **HP ProtectTools** в области уведомлений в дальнем правом углу панели задач, выберите **File Sanitizer** и далее **Очистить сейчас**.
2. При появлении диалогового окна подтверждения щелкните **Да**.

– или –

1. Откройте File Sanitizer и щелкните **Очистка свободного пространства**.
2. Щелкните **Очистить сейчас**.
3. При появлении диалогового окна подтверждения щелкните **Да**.

Прерывание процесса уничтожения или очистки свободного пространства

Во время выполнения процесса уничтожения или очистки свободного пространства отображается сообщение поверх значка HP ProtectTools Security Manager в области уведомлений, в правом углу панели задач. В данном сообщении приводятся сведения о процессе уничтожения или очистки свободного пространства (ход выполнения в процентах), а также предоставляется возможность отмены.

▲ Для отмены процесса щелкните сообщение и нажмите **Стоп**.

Просмотр файлов журнала

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

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

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

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

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

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

8 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. Неуправляемые классы устройств на стр. 102.

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. Войти в систему в качестве администратора.
2. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
3. На левой панели щелкните **Device Access Manager**.

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.
- **Конфигурация 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®
- 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 затем **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. Щелкните **Применить**.

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

4. Щелкните **ОК**.

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:

1. В операционной системе Windows 7 щелкните **Пуск**, выберите **Панель управления**, а затем **Система и безопасность**.

   – или –

   В операционной системе Windows Vista® щелкните **Пуск**, выберите **Панель управления**, а затем **Система и ее обслуживание**.

   – или –

   В операционной системе Windows XP щелкните **Пуск**, выберите **Панель управления**, а затем **Производительность и обслуживание**.

2. Щелкните **Администрирование**, затем щелкните **Службы**.
3. Выберите службу **HP ProtectTools Device Locking/Auditing**.
4. Для запуска службы щелкните **Пуск**.

   – или –

   Чтобы остановить запущенную систему, щелкните **Стоп**.

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 устройств, 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:

- **Список устройств** — отображает 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.
- **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.

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 как он является пользователем без 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. Группа администраторов устройств на стр. 100.

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**.

К альтернативным методам управления принадлежностью к данной группе относятся:

- В операционных системах Windows 7 Professional или Windows Vista пользователей в группу можно добавлять, используя стандартную оснастку консоли управления Microsoft (MMC) «Локальные пользователи и группы».
- В операционных системах Windows 7, Windows Vista или Windows XP Home под учетной записью с правами администратора напечатайте в окне командной строки следующее:

  ```
  net localgroup "Device Administrators" username /add
  ```

  В данной команде «username» — это имя пользователя, которого необходимо добавить в данную группу.

Служба поддержки 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

9 Обнаружение похищенных устройств

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. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.
3. На левой панели Security Manager щелкните **Обнаружение похищенных устройств**.
4. Для запуска мастера активации программы Computrace щелкните кнопку **Активировать сейчас**.
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**.

10 Embedded Security (Встроенная система безопасности) для HP ProtectTools (только на некоторых моделях)

ПРИМЕЧАНИЕ. Для использования модуля Embedded Security (Встроенная система безопасности) для HP ProtectTools в компьютере необходимо установить микросхему TPM (модуль доверяемой платформы).

Embedded Security (Встроенная система безопасности) для HP ProtectTools защищает компьютер от несанкционированного доступа к данным пользователя и учетным данным. Этот программный модуль обеспечивает следующие защитные функции:

- расширенная шифрованная файловая система Microsoft® (EFS) для шифрования файлов и папок;
- создание личного защищенного диска (PSD) для защиты данных пользователя;
- функции управления данными, например создание резервной копии и восстановление иерархии ключей;
- поддержка работы приложений сторонних разработчиков (например Microsoft Outlook и Internet Explorer) с безопасными цифровыми сертификатами при использовании программного обеспечения встроенной системы безопасности.

Встроенная микросхема безопасности TPM дополняет и позволяет использовать прочие службы безопасности HP ProtectTools Security Manager. Например, служба Credential Manager for HP ProtectTools может использовать встроенную микросхему как фактор проверки подлинности при входе пользователя в Windows.

Процедуры настройки

⚠ **ПРЕДУПРЕЖДЕНИЕ.** Чтобы снизить риски, ИТ-администратору настоятельно рекомендуется незамедлительно инициализировать микросхему встроенной системы безопасности. При сбое инициализации этой микросхемы неавторизованный пользователь или компьютерный вирус сможет захватить контроль над компьютером и задачами владельца (например, получить доступ к архиву аварийного восстановления или настройкам доступа для пользователей).

Чтобы включить и инициализировать микросхему встроенной системы безопасности, выполните действия, описанные в следующих разделах.

Включение микросхемы встроенной системы безопасности в Computer Setup.

Микросхему встроенной системы безопасности необходимо включить в мастере быстрой инициализации или в программе Computer Setup.

Включение микросхемы встроенной системы безопасности в программе Computer Setup.

1. Откройте меню начальной установки компьютера при включении или перезапуске компьютера, нажав f10, пока в левом нижнем углу экрана отображается сообщение «f10 = ROM Based Setup».
2. Если пароль администратора не установлен, выберите с помощью клавиш со стрелками **Security** (Безопасность), выберите **Setup password** (Установка пароля) и нажмите enter.
3. Введите пароль в поля **New password** (Новый пароль) и **Verify new password** (Подтверждение нового пароля), затем нажмите клавишу f10.
4. В меню **Security** (Безопасность) с помощью клавиш со стрелками выберите **TPM Embedded Security** (Встроенная система безопасности TPM), затем нажмите клавишу enter.
5. В области **Embedded Security** (Встроенная система безопасности), если устройство не отображается, выберите **Available** (Доступна).
6. Выберите **Embedded security device state** (Состояние устройства встроенной системы безопасности) и измените это настройку на **Enable** (Включено).
7. Нажмите клавишу f10 для принятия изменений конфигурации модуля Embedded Security (Встроенная система безопасности).
8. Для сохранения настроек и выхода из программы Computer Setup используйте клавиши со стрелками, чтобы выбрать **File** (Файл), щелкните значок **Save Changes and Exit** (Сохранить изменения и выйти) в нижнем левом углу экрана и следуйте инструкциям на экране.

Инициализация микросхемы встроенной системы безопасности

В рамках процедуры инициализации модуля Embedded Security (Встроенная система безопасности) выполняются следующие операции.

- Задается пароль владельца микросхемы встроенной системы безопасности, который защищает доступ ко всем функциям владельца, находящимся на микросхеме встроенной системы безопасности.
- Настраивается архив для аварийного восстановления, который представляет собой защищенную область хранения, где для всех пользователей можно зашифровать основные ключи пользователей.

Для инициализации микросхемы встроенной системы безопасности выполните следующие действия.

1. Щелкните правой кнопкой значок **HP ProtectTools Security Manager** в области уведомлений в дальнем правом углу панели задач, выберите **Embedded Security Initialization**.

   Открывается мастер инициализации модуля Embedded Security (Встроенная система безопасности) HP ProtectTools.

2. Следуйте указаниям на экране.

Настройка основной учетной записи пользователя

Настройка учетной записи основного пользователя модуля Embedded Security (Встроенная система безопасности) выполняет следующие задачи:

- задает основной ключ пользователя, защищающий зашифрованную информацию, и устанавливает пароль основного ключа пользователя для защиты этого ключа;
- задает личный защищенный диск (PSD) для хранения зашифрованных файлов и папок.

ПРЕДУПРЕЖДЕНИЕ. Защита пароля основного ключа пользователя. Без этого пароля невозможен доступ к зашифрованной информации или ее восстановление.

Для настройки учетной записи основного пользователя и включения функций безопасности пользователя выполните следующие действия.

1. Если не открыт мастер инициализации пользователя Embedded Security, нажмите **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.
2. На левой панели нажмите **Embedded Security** (Встроенная система безопасности), затем нажмите **Параметры пользователя**.
3. На правой панели, в области **Функции Embedded Security** (Встроенная система безопасности), выберите **Настройка**.

   Открывается мастер инициализации пользователя модуля Embedded Security (Встроенная система безопасности).
4. Следуйте указаниям на экране.

ПРИМЕЧАНИЕ. Для использования защищенной электронной почты необходимо сначала настроить почтовый клиент на использование цифрового сертификата, созданного с помощью встроенной системы безопасности. Если цифровой сертификат недоступен, необходимо получить его от центра сертификации. Сведения о настройке электронной почты и получении цифрового сертификата см. справке почтового клиента.

Общие задачи

После настройки учетной записи основного пользователя можно выполнять следующие задачи:

- шифрование файлов и папок;
- передача и прием зашифрованной электронной почты.

Использование личного защищенного диска

После настройки PSD при следующем входе в систему выдается запрос на ввод пароля для основного ключа пользователя. Если пароль для основного ключа пользователя введен правильно, пользователь получает доступ к PSD непосредственно из проводника Windows.

Шифрование файлов и папок

При работе с зашифрованными файлами необходимо учитывать следующие правила.

- Возможно шифрование файлов и папок только из разделов NTFS. Файлы и папки из разделов FAT зашифровать невозможно.
- Невозможно шифрование системных и архивированных файлов, а зашифрованные файлы невозможно заархивировать.
- Временные папки должны быть зашифрованы, поскольку они могут представлять интерес для хакеров.
- При первом шифровании файла или папки правила восстановления настраиваются автоматически. В случае утраты сертификатов шифрования или личных ключей эти правила обеспечивают возможность использования агента восстановления для дешифровки данных.

Для шифрования файлов и папок выполните следующие действия.

1. Правой кнопкой мыши щелкните шифруемый файл или папку.
2. Нажмите кнопку **Encrypt** (Зашифровать).
3. Выберите один из следующих вариантов.
   - **Применить изменения только к этой папке.**
   - **Применить изменения к этой папке, вложенным папкам и файлам.**
4. Нажмите кнопку **OK**.

Отправка и получение зашифрованной электронной почты

Встроенная система безопасности позволяет отправлять и получать зашифрованные сообщения электронной почты, но процедуры зависят от программы, используемой для доступа к электронной почте. Дополнительные сведения см. в справке встроенной системы безопасности и справке клиента электронной почты.

Изменение пароля основного пользователя

Изменение пароля основного пользователя.

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **HP ProtectTools Security Manager**.
2. На левой панели нажмите **Embedded Security** (Встроенная система безопасности), затем нажмите **Параметры пользователя**.
3. На правой панели в разделе **Основной пароль пользователя** нажмите **Изменить**.
4. Введите старый пароль, затем задайте и подтвердите новый пароль.
5. Нажмите кнопку **OK**.

Дополнительные задачи

Администраторы могут выполнять следующие задачи в Embedded Security.

- Архивация и восстановление учетных данных Embedded Security, параметров Embedded Security и личных защищенных дисков
- Изменение пароля владельца
- Сброс пароля пользователя
- Безопасный перенос учетных данных для безопасного доступа пользователя с исходной платформы на платформу назначения

Резервное копирование и восстановление

Функция резервного копирования модуля Embedded Security (Встроенная система безопасности) создает архив, содержащий сертификационные данные, которые должны быть восстановлены в аварийной ситуации.

Создание файла резервной копии

Для создания файла резервной копии выполните следующие действия.

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели нажмите **Embedded Security** (Встроенная система безопасности), затем нажмите **Резервное копирование**.
3. На правой панели щелкните **Настроить**. Откроется мастер резервного копирования HP Embedded Security for ProtectTools.
4. Следуйте указаниям на экране.

Восстановление сертификационных данных из файла резервной копии

Для восстановления данных из файла резервной копии выполните следующие действия.

1. Нажмите кнопку **Пуск**, выберите **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели нажмите **Embedded Security** (Встроенная система безопасности), затем нажмите **Резервное копирование**.
3. На правой панели щелкните **Restore all** (Восстановить все). Откроется мастер резервного копирования HP Embedded Security for ProtectTools.
4. Следуйте указаниям на экране.

Изменение пароля владельца

Администраторы могут изменить пароль владельца.

1. Нажмите кнопку **Пуск**, щелкните **Все программы**, щелкните **HP** и выберите **Консоль администрирования HP ProtectTools**.
2. На левой панели нажмите **Embedded Security** (Встроенная система безопасности), затем нажмите **Дополнительно**.
3. На правой панели, в области **Пароль владельца**, нажмите **Изменить**.
4. Введите старый пароль владельца, затем задайте и подтвердите новый пароль владельца.
5. Нажмите кнопку **OK**.

Повторное задание пароля пользователя

Администратор может помочь пользователю сбросить забытый пароль. Дополнительные сведения см. в справке программы.

Перемещение ключей с помощью мастера перемещения

Перемещение представляет собой дополнительную задачу администратора, позволяющую управлять ключами и сертификатами, выполнять восстановление и перенос ключей и сертификатов.

Подробные сведения о переносе см. в справке программы встроенной системы безопасности.

11 Ограничения локализованных паролей

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

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.

Например, в некоторых японских версиях Windows XP IME по умолчанию называется Microsoft IME Standard 2002 для японского языка, что в действительности меняет раскладку клавиатуры на E0010411. Однако это IME, а не раскладка клавиатуры. (Схема кодов раскладок клавиатуры зарезервирована Microsoft для IME, что расширяет концепцию раскладок клавиатуры). Поскольку это не раскладка клавиатуры, которая может быть представлена в среде ввода с клавиатуры для экрана ввода пароля проверки безопасности перед загрузкой BIOS или экрана HP Drive Encryption, все пароли, введенные с помощью этого IME, будут отклонены HP ProtectTools. Microsoft IME Standard 2002 для японского языка также отличается от «общего имени» в Microsoft Windows Vista®. Windows сопоставляет некоторые IME с раскладками клавиатуры. В этих случаях IME поддерживается HP ProtectTools, поскольку используется определение базовой раскладки клавиатуры (шестнадцатеричный код).

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 й, хотя для его вывода требуются 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)	з, и, а и й с нажатой клавишей caps lock - З, И, А и Й в Windows.	з, и, а и й с нажатой клавишей caps lock - з, и, а и й при проверке безопасности перед загрузкой BIOS.	з, и, а и й с нажатой клавишей caps lock - з, и, а и й 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 Ў, ¤, ‘, ’, Ґ и Ч в верхнем ряду отклоняются. ◦ Клавиши е, ® и Ю во втором ряду отклоняются. ◦ Клавиши б, р и ш в третьем ряду отклоняются. ◦ Клавиша ж в нижнем ряду отклоняется.	нет	нет

Язык	Windows	BIOS	Drive Encryption
Чешский	◦ Клавиша р отклоняется. ◦ Клавиша į отклоняется. ◦ Клавиша ц отклоняется. ◦ Клавиши ė, э и ї отклоняются. ◦ Клавиши ģ, ķ, ļ, ņ и ŗ отклоняются.	нет	нет
Словацкий	Клавиша ї отклоняется.	◦ Клавиши ль, нь и є отклоняются при вводе с клавиатуры, но принимаются при вводе с программной клавиатуры. ◦ Мертвая клавиша ю выводит два символа.	нет
Венгерский	Клавиша ї отклоняется.	Клавиша ю выводит два символа.	нет

Язык	Windows	BIOS	Drive Encryption
Словенский	Клавиша їЇ отклоняется в Windows, клавиша alt создают мертвую клавишу в BIOS.	Клавиши ъ, Ъ, щ, Щ, є, Є, њ, Њ, љ и Љ отклоняются в BIOS.	нет
Японский	Только для Windows XP стандартная раскладка клавиатуры «Японская», 411, полностью поддерживается. Один IME, широко представленный в XP как Microsoft Standard IME 2002, как правило, не поддерживается. Однако эмпирическая проверка показала, что этот IME – почти аналог раскладки клавиатуры 411 при вводе простых символов. Поэтому этот IME программно переключается на раскладку 411 при защите BIOS и HP Drive Encryption с помощью локализованных японских паролей. Лучше использовать Microsoft Office 2007 IME, если он доступен. Несмотря на название IME в действительности это поддерживаемая раскладка клавиатуры 411.	нет	нет

Чт 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. Щелкните **Пуск**, выберите **Панель управления**, а затем **Язык и региональные стандарты**.
  2. Выберите вкладку **Языки**.
  3. Нажмите кнопку **Подробнее**.
  4. На вкладке **Параметры** нажмите кнопку **Добавить**, чтобы добавить поддерживаемую клавиатуру (добавьте клавиатуры США для языка вода «Китайский»).
  5. Установите поддерживаемые клавиатуры для языка ввода по умолчанию.
  6. 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. Неподдерживаемые символы перечислены на Обработка специальных клавиш на стр. 118.
  2. Снова запустите мастер настройки Security Manager, затем введите новый пароль Windows.

Глоссарий

автоматическое уничтожение
Уничтожение по расписанию, установленному в модуле File Sanitizer (Очистка файлов).

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.

виртуальный ключ
Служба безопасности, которая работает аналогично смарт-картам и устройствам чтения карт. Маркер сохраняется либо на жестком диске компьютера, либо в реестре Windows. При входе с использованием виртуального маркера пользователю предлагается ввести PIN-код для завершения авторизации.

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

вход
Объект в Security Manager, содержащий имя пользователя, пароль и, возможно, другую выбранную информацию. Его можно использовать для входа в другие программы и на веб-сайты.

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

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

доверенное сообщение
Сеанс связи, при котором от доверенного отправителя доверенному контакту отправляются доверенные сообщения.

доверенный контакт
Принявший приглашение доверенного контакта.

доверенный отправитель
Доверенный контакт, отправляющий подписанные и зашифрованные сообщения электронной почты и документы Microsoft Office.

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.

запечатать для доверенных контактов
Задача, которая добавляет цифровую подпись, шифрует и отправляет сообщение электронной почты после проверки подлинности пользователя (с помощью выбранного способа защищенного входа).

идентификационная карточка
Элемент рабочего стола Windows, который служит для визуальной идентификации рабочего стола с помощью имени пользователя и выбранного изображения. Щелкните идентификационную карту, чтобы открыть консоль администрирования HP ProtectTools.

класс устройств
Все устройства одного типа, например дисководы.

ключ
См. *способ безопасного входа в систему*.

ключ USB
Устройство безопасности, на котором хранится информация, идентифицирующая пользователя. Как и смарт-карта или устройство считывания биометрических данных, оно используется для проверки подлинности владельца компьютера.

кнопка «Send Securely» (Защищенная отправка)
Программная кнопка, отображаемая на панели инструментов сообщений электронной почты Microsoft Outlook. Нажатие этой кнопки позволяет подписать и зашифровать сообщение электронной почты Microsoft Outlook.

кнопка Sign and Encrypt (Подпись и шифрование)
Программная кнопка, отображаемая на панели инструментов приложений Microsoft Office. Нажав кнопку, можно подписать, зашифровать или снять шифрование в документе Microsoft Office.

комбинация клавиш
Комбинация определенных клавиш, которая при нажатии запускает автоматическое уничтожение данных, например ctrl+alt+s.

консоль
Место, где можно просмотреть и изменить параметры консоли администрирования HP ProtectTools и задействовать ее функции.

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.

очистка свободного места
Защищенная запись случайных данных поверх удаленных объектов для искажения содержимого удаленного объекта.

панель мониторинга
Место, где можно просмотреть и изменить параметры программы Security Manager for HP ProtectTools и задействовать ее функции.

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.

получатель доверенного контакта
Пользователь, получающий приглашение стать доверенным контактом.

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.

предполагаемый подписывающий
Пользователь, выбранный владельцем документа Microsoft Word или Microsoft Excel для добавления строки подписи к документу.

преобразование

Задача, обеспечивающая управление, восстановление и передачу сертификатов Privacy Manager и доверенных контактов.

приглашение доверенного контакта
Отправленное сообщение электронной почты с предложением стать доверенным контактом.

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.

простое удаление
Удаление ссылки Windows на объект. Содержимое объекта остается на жестком диске до тех пор, пока поверх него не будут записаны скрывающие его данные при очистке свободного места.

профиль надежного удаления
Выбранный способ удаления и список объектов.

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.

сертификат Privacy Manager
Цифровой сертификат, требующий проверки подлинности при каждом его использовании для криптографических операций, например для подписания и шифрования сообщений электронной почты и документов Microsoft Office.

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.

список доверенных контактов
Список, в котором перечислены доверенные контакты.

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

строка подписи
Место для визуального представления цифровой подписи. После подписания документа здесь будут показаны имя подписывающего и способ проверки. Также будут включены дата подписи и название подписывающего пользователя.

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

уничтожение
Выполнение алгоритма, который скрывает данные, содержащиеся в объекте.

уничтожение вручную

Немедленное уничтожение выбранного объекта или объектов, не использующее расписание автоматического надежного удаления.

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
Фотография легитимного пользователя, которая будет использоваться для проверки подлинности.

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

цикл надежного удаления
Количество выполнений алгоритма надежного удаления для каждого объекта. Чем больше количество выполняемых циклов надежного удаления, тем в большей безопасности находится компьютер.

цифровая подпись
Данные, отправляемые с файлом, которые подтверждают идентификацию отправителя и целостность подписанного файла.

цифровой сертификат
Электронные учетные данные, подтверждающие идентификацию лица или компании путем связывания данных о владельце цифрового сертификата с парой электронных ключей, используемых для подписи цифровой информации.

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.

ATM
Automatic Technology Manager позволяет администраторам сети управлять компьютерами дистанционно на уровне BIOS.

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.

HP SpareKey
Резервная копия ключа шифрования диска.

JITA
Своевременная проверка подлинности.

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

PSD
Устройство Personal Secure Drive, которое предоставляет защищенную область для хранения важной информации.

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

P

C

У

S

W