

Интеграция Рутокен и LastPass

LastPass - программа для хранения паролей, разработанная компанией [LastPass](#). Она существует в виде плагинов для Internet Explorer, Google Chrome, Mozilla Firefox, Opera и Apple Safari. Пароли в LastPass защищены мастер-паролем и могут быть синхронизированы с любым другим браузером. LastPass также имеет заполнитель форм, что позволяет автоматизировать ввод паролей и заполнение форм. Плагин поддерживает генерацию паролей, расшаривание данных и журналирование входа на сайты.

Внимание



Для аутентификации с использованием электронных идентификаторов требуется корпоративный или премиум аккаунт LastPass.

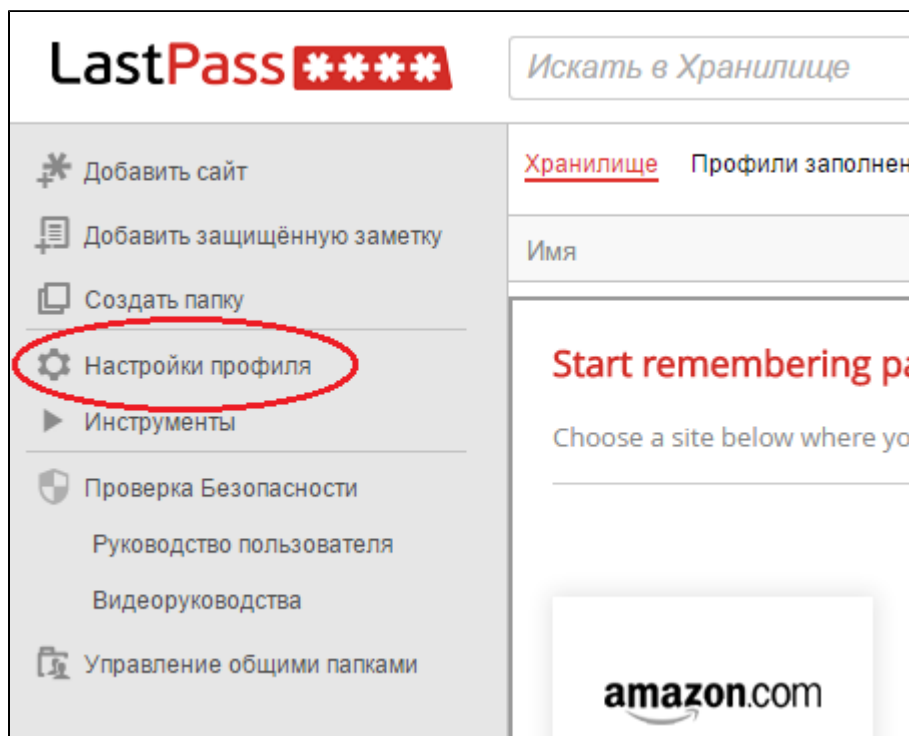
Аутентификация в LastPass по смарт-картам и токенам Рутокен настраивается очень просто:

1) Если у вас нет RSA2048 сертификата на токене, его можно получить в инфраструктуре вашей компании, создать бесплатно на одном из соответствующих интернет-ресурсов, выписать самостоятельно или, при желании, купить. На безопасность авторизации в LastPass это не повлияет. Для самостоятельного выписывания сертификата можно использовать, к примеру, OpenSSL, графическую надстройку XCA или, если есть возможность, Microsoft Certification Authority, встроенный в Windows Server. Инструкции можно легко найти в интернете. Также сертификаты можно бесплатно получить на таких ресурсах как, например, [Comodo](#) или [StartSSL](#).

2) Поскольку LastPass работает с токенами и смарт-картами через библиотеки стандарта PKCS#11, нам необходимо будет ей обзавестись.

- Пользователям Windows достаточно установить [драйвера](#) с нашего сайта.
- Для Linux необходимо взять с нашего сайта [пакет DEB/RPM](#) и установить его. Также, при необходимости, по той же ссылке можно взять саму библиотеку и самостоятельно установить ее в /usr/lib или /usr/lib64 для x86 или x64 версии ОС соответственно.
- В OS X библиотека PKCS#11 устанавливается с помощью [модуля поддержки](#) "Связки Ключей" или вручную скачивается с нашего сайта и размещается в /usr/lib.

3) Далее для включения многофакторной аутентификации в LastPass перейдем в "Хранилище LastPass" ("My LastPass Vault") в "Настройки профиля"...



... на вкладку Multifactor options.

Настройки профиля

Общие

Multifactor Options

Trusted Devices

Mobile Devices

Запрещенные адреса

Equivalent Domains

Правила URL

Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

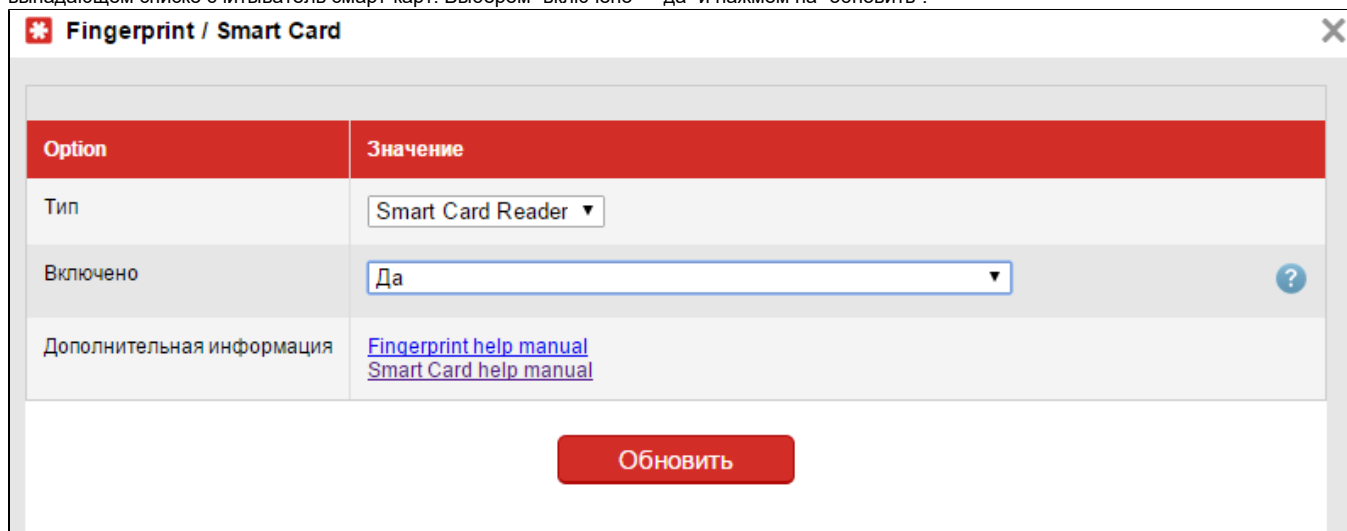
?

Multifactor Option	Имя	Описание	Страна	Действие
	Google Authenticator	Generates one time verification codes on your smart phone. Can also be used with Microsoft Authenticator.	Отключено	
	Toopher	Sends push notifications to your smart phone to verify your login.	Отключено	
	Duo Security	Generates one time verification codes or sends push notifications to your smart phone.	Отключено	
	Transakt	Sends an Accept/Reject notification to your smart phone.	Отключено	
	Grid	Printable spreadsheet of numbers and letters used to enter different values when logging in.	Отключено	

Нас интересует нижний блок для Премиум пользователей.

FOR PREMIUM USERS				
Multifactor Option	Имя	Описание	Страна	Действие
	YubiKey	USB device that generates one time verification codes.	Отключено	
	Fingerprint / Smart Card	Support for fingerprint sensors and card readers.	Отключено	
	Sesame	Software application that can be placed on a USB key to generate one time verification codes.	Отключено	

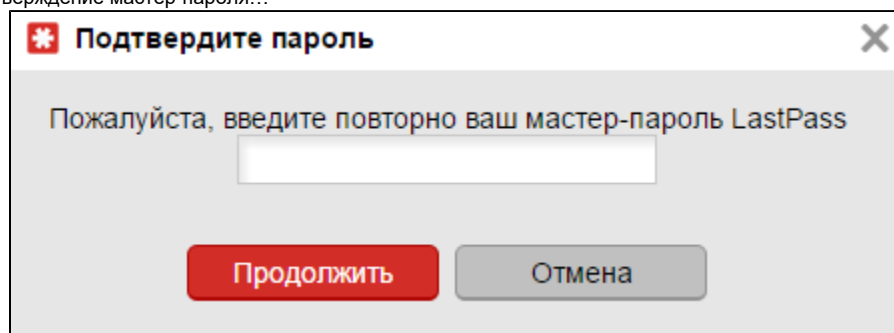
4) Зайдем в настройки аутентификации Fingerprint/SmartCard. В случае, если библиотека PKCS#11 установлена корректно, мы увидим в выпадающем списке считыватель смарт-карт. Выберем "включено — да" и нажмем на "обновить".



Option	Значение
Тип	Smart Card Reader ▼
Включено	Да ▼
Дополнительная информация	Fingerprint help manual Smart Card help manual

Обновить

5) Будет запрошено подтверждение мастер-пароля...

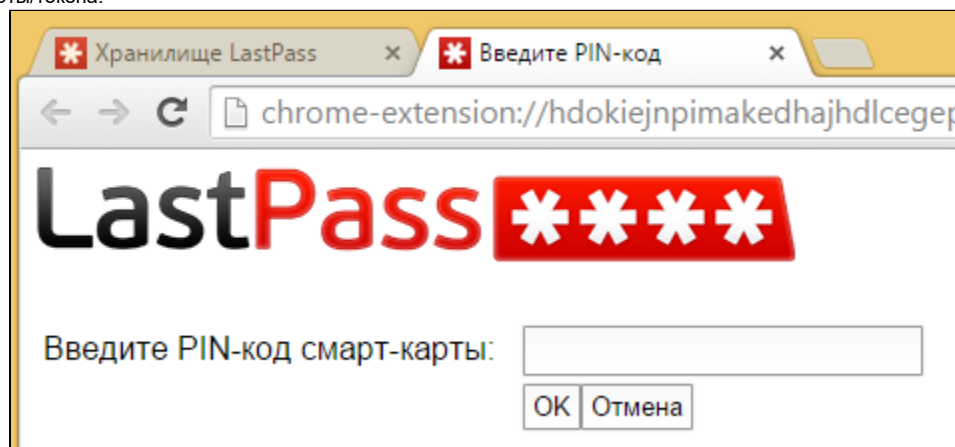


Подтвердите пароль

Пожалуйста, введите повторно ваш мастер-пароль LastPass

Продолжить Отмена

... и пин-код смарт-карты/токена.



Хранилище LastPass x Введите PIN-код x

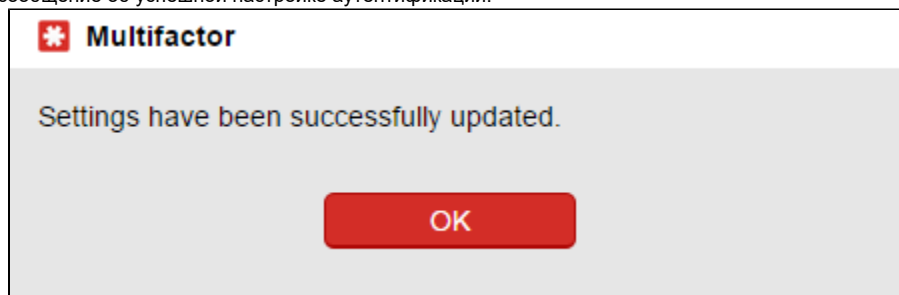
chrome-extension://hdokiejnpimakedhajhdlcegep...

LastPass ****

Введите PIN-код смарт-карты:

OK Отмена

После чего мы получим сообщение об успешной настройке аутентификации.



Multifactor

Settings have been successfully updated.

OK

Теперь для разблокировки сохраненных паролей в LastPass достаточно лишь подключить электронный идентификатор и ввести его пин-код.