



Руководство администратора

Платформа 2FA Protectimus
Интеграция по протоколу RADIUS

Вер. 1.0.4 RU
от 12 мая 2021



Содержание

Процесс интеграции/ деплой программного комплекса	4
Сервер аутентификации Protectimus	5
Начало работы с SaaS-сервисом Protectimus	5
Начало работы с On-Premise платформой Protectimus	5
Работа с системой Protectimus	6
Ресурсы	6
Ключ API	7
Активация API	7
Настройка Protectimus RProxy	9
Порядок применения обновлений системы	12
Наши контакты	13
Корпоративная информация	13

Процесс интеграции/ деплой программного комплекса

Один из возможных способов взаимодействия с платформой или сервисом Protectimus - использование протокола RADIUS.

Интеграция решений заключается в запуске и настройке Protectimus RProxy, а также в настройке любых других устройств или приложений, поддерживающих протокол RADIUS.

Настройка политики аутентификации позволит отправлять запрос на аутентификацию по протоколу RADIUS, который будет принят и обработан компонентом Protectimus RProxy. В свою очередь, компонент RProxy, приняв запрос, обратится к серверу аутентификации Protectimus для проверки одноразового пароля от пользователя.

Существует несколько способов поставки сервера аутентификации Protectimus. Для ускорения процесса организации надежной аутентификации, бесплатного тестирования решения, а также для переноса всех забот на “чужие плечи” предназначен сервис, который поставляется по модели SaaS.

Вторым вариантом является установка платформы Protectimus на собственном оборудовании. Такой вариант позволит настроить аутентификацию в изолированной среде.

Также, при необходимости, специалисты Protectimus могут подготовить индивидуальный кластер в облаке по требованиям заказчика.

Функциональность системы сохраняется независимо от выбранного варианта размещения сервера. Для переключения между вариантами размещения сервера достаточно будет изменить несколько настроек для подключения к API по новому адресу.

Перейдем к более детальному рассмотрению процесса интеграции.

Сервер аутентификации Protectimus

Сервер аутентификации Protectimus доступен в двух вариантах:

- **Сервис** - облачное SAAS-решение для быстрого старта и эффективного внедрения двухфакторной аутентификации. К Вашим услугам: облачная платформа, доступная 24/7, удобные средства мониторинга и управления, а также широкий спектр токенов.
- **Платформа** - комплексное решение двухфакторной аутентификации, располагаемое в Вашем окружении, для полного контроля над всеми аспектами функционирования системы аутентификации, в том числе и базой данных пользователей и другой чувствительной информацией. Платформа аутентификации и инструкция по ее установке предоставляется по запросу в службу поддержки Protectimus по адресу support@protectimus.com.

ВНИМАНИЕ! Мы предлагаем начать тестирование с облачным сервисом, чтобы ускорить процесс интеграции. Для переключения между облачными и локальными серверами достаточно лишь изменить несколько строк в файле конфигурации.

Начало работы с SaaS-сервисом Protectimus

Для начала использования SaaS-сервиса перейдите на страницу регистрации <https://service.protectimus.com>, заполните регистрационную форму и нажмите кнопку «Регистрация». Письмо для подтверждения регистрации будет отправлено на указанный Вами электронный адрес. После перехода по ссылке в письме Ваш адрес будет подтвержден, и Вы сможете использовать Protectimus Cloud Authentication Service - облачное (SaaS) решение.

Начало работы с On-Premise платформой Protectimus

Если Вы хотите, чтобы все компоненты системы двухфакторной аутентификации находились в Вашей инфраструктуре, наше решение также доступно в виде On-Premise платформы которая устанавливается в окружении клиента.

Скачать платформу и инструкцию по ее установке на Windows можно здесь: <https://www.protectimus.com/platform/ru/>

Инструкции по разворачиванию платформы двухфакторной аутентификации Protectimus на других операционных системах предоставляется по запросу в службу поддержки Protectimus по адресу support@protectimus.com.

Работа с системой Protectimus

Ресурсы

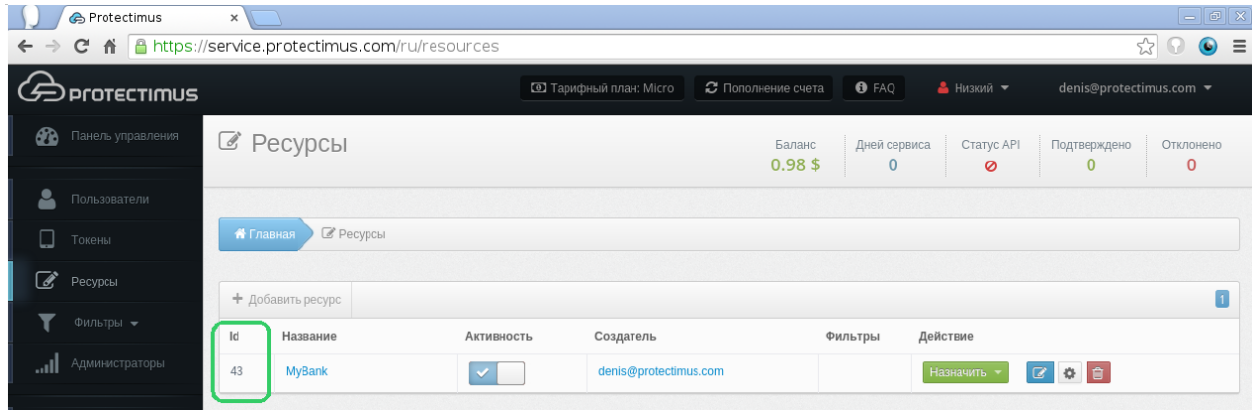
Ресурсы служат для логического объединения пользователей и токенов и удобного управления ими. Чтобы создать ресурс нажмите на кнопку “Ресурсы” в меню слева, а затем нажмите на кнопку “Добавить ресурс” в заголовке таблицы. После этих действий Вы попадете на страницу добавления ресурса, где обязательно необходимо указать только название ресурса, остальные параметры - по желанию

The screenshot displays the 'Добавить ресурс' (Add Resource) page in the Protectimus web application. The browser address bar shows 'https://service.protectimus.com/ru/resources/create'. The top navigation bar includes the Protectimus logo, a sidebar menu with options like 'Панель управления', 'Пользователи', 'Токены', 'Ресурсы', 'Фильтры', 'Администраторы', 'Статистика', 'Платежи', and 'События', and a top right area with account details and a balance of 1.97 \$. The main form contains the following fields and controls:

- Название ресурса:** A text input field containing 'MyBank'.
- Разрешенные IP адреса:** A text input field with a placeholder 'добавить IP' and a warning icon.
- Проверка по IP активирована:** A checkbox that is currently unchecked.
- Количество неуспешных попыток входа до блокировки:** A slider control set to the value 5.
- Активность:** A checkbox that is checked.

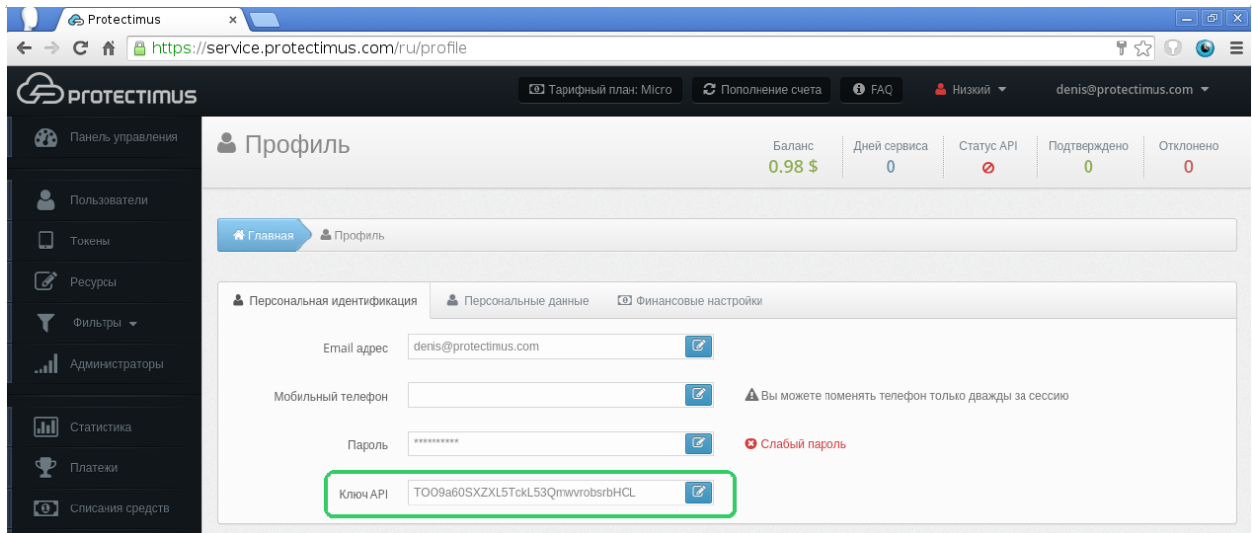
At the bottom of the form are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel). A warning message at the bottom right states: 'Разрешить обращение к этому ресурсу через API. Если этот параметр будет выключен - аутентификация на этом ресурсе будет невозможна.'

После создания ресурса Вы попадете на страницу со списком доступных ресурсов, где увидите только что созданный ресурс. Кроме прочего, в таблице будет отображен id ресурса, который будет использован в настройках подключения к Protectimus.



Ключ API

Также, для подключения к Protectimus пригодится ключ к API, который находится в профиле пользователя. Чтобы перейти в профиль пользователя нажмите на своем логине в правом верхнем углу интерфейса и выберите пункт “Профиль” из выпадающего списка.



Активация API

В случае использования SaaS-решения необходимо активировать тарифный план для работы API. Для этого перейдите в раздел “Тарифные планы” <http://service.protectimus.com/pricing> и активируйте подходящий Вам тарифный план. Пока Вы не активируете тарифный план с Вашего счета не будут списываться средства, но Вы также не сможете использовать API. Вы сможете деактивировать тарифный план в любой момент, если по каким-то причинам Вам не нужно будет пользоваться сервисом больше одного дня. При первой деактивации тарифа за текущие сутки со счета

единоразово списывается плата за использование сервиса согласно расценкам активного тарифа. При активном тарифном плане плата взимается раз в сутки автоматически.

После активации тарифного плана значок статуса API перейдет в состояние “Включено”, что означает готовность сервиса к работе через API.



Система Protectimus готова к использованию. Токены для аутентификации пользователей по SMS или e-mail будут созданы автоматически при первом логине пользователя. Также, доступны к использованию и другие типы токенов, их создание возможно через сервер Protectimus. Для получения дополнительной информации об использовании других типов токенов, обратитесь к службе поддержки Protectimus.

Настройка Protectimus RProxy

Для получения последней версии Protectimus RProxy необходимо обратиться в службу поддержки по адресу support@protectimus.com.

Для работы RProxy на машине должна быть установлена Java версии 8.

Запуск RProxy осуществляется командой:

```
java -jar RProxy.jar
```

Конфигурирование RProxy выполняется путём задания настроек в файле **rproxy.properties**, который должен быть расположен в той же папке, что и запускаемый файл.

Задайте в файле **rproxy.properties** следующие значения:

Настройка RADIUS	
<code>rproxy.radius.secret</code>	Секрет, который будет использоваться прокси-сервером аутентификации и вашим сервером RADIUS.
<code>rproxy.radius.port</code>	Порт на котором будет запущен RADIUS сервер.
<code>rproxy.re-enter-otp</code>	Если для параметра <code>rproxy.re-enter-otp</code> задано значение <code>true</code> , статический пароль не запрашивается после неудачной проверки OTP-пароля.

Настройка проверки первого фактора аутентификации (статического пароля)		
<code>primary-authenticator</code>	Этот параметр указывает, где именно будет проверяться пароль пользователя.	
	Возможные варианты :	
	1. PROTECTIMUS - проверка пароля будет осуществляться на сервисе PROTECTIMUS <code>primary-authenticator = PROTECTIMUS</code> 2. LDAP - пароль будет проверяться на стороне LDAP (AD). Для этого нужно заполнить соответствующие параметры:	
	<code>ldap.url</code>	Имя хоста или IP-адрес вашего контроллера домена.

	<code>ldap.search-base</code>	LDAP DN группы или подразделения, содержащего всех пользователей, которым вы хотите разрешить вход.
	<code>ldap.account-name</code>	Название учетной записи домена, у которой есть разрешение на привязку к вашему каталогу и выполнение поиска.
	<code>ldap.account-password</code>	Пароль, соответствующий учетной записи домена.
	<code>ldap.query-attribute</code> <code>ldap.principal-attribute</code>	Если вы хотите аутентифицировать пользователя с помощью «sAMAccountName» вместо «userPrincipalName», укажите атрибуты "query-attribute" и "principal-attribute" соответственно.
3. Если проверка пароля не требуется (например сервис поддерживает N фактор), оставьте параметр пустым. В этом случае будет проверяться только OTP		

Настройка подключения к сервису PROTECTIMUS	
<code>protectimus.login</code>	Ваш логин в системе PROTECTIMUS.
<code>protectimus.api-key</code>	Ваш ключ API в системе PROTECTIMUS.
<code>protectimus.resource-id</code>	ID ресурса, созданного Вами в системе PROTECTIMUS.
<code>protectimus.api-url</code>	Если Вы используете облачный сервис PROTECTIMUS, укажите следующий API URL: <code>https://api.protectimus.com/</code> Если Вы используете on-premise платформу Protectimus, API URL будет выглядеть примерно так: <code>protectimus.api.url=http://127.0.0.1:8080/</code>
<code>protectimus.username.normalization</code>	Когда нормализация включена (<code>protectimus.username.normalization = true</code>), любая

	информация о домене удаляется из имени пользователя, то есть независимо от того, как указано имя пользователя "username", "DOMAIN \ username", или "username@domain.com", оно будет преобразовано в одно "username"
--	---

Пример конфигурационного файла:

```
#-----RADIUS Server-----
rproxy.radius.port = 1812
rproxy.radius.secret = secret
rproxy.re-enter-otp = true
primary-authenticator = LDAP

#-----Protectimus API-----
protectimus.login = test@protectmus.com
protectimus.api-key = apikey
protectimus.resource-id = 1
protectimus.api-url = https://api.protectimus.com/
protectimus.username.normalization = true

#-----LDAP-----
ldap.account-name = cn=user,dc=example,dc=com
ldap.account-password = password
ldap.url = ldap://localhost:389
ldap.search-base = dc=example,dc=com
ldap.query-attribute = sAMAccountName
ldap.principal-attribute = userPrincipalName
```

Теперь вам нужно настроить ваше устройство или приложение для связи с Proxy по протоколу RADIUS.

Для настройки используйте `rproxy.radius.port` и `rproxy.radius.secret`

Порядок применения обновлений системы

Для обновления системы, нужно запросить новую версию ПО. После чего, в случае обновления платформы, стоит заменить полученный WAR архив в папку TOMCAT_HOME/webapps, в случае с работой с контейнером сервлетов, или же в PLATFORM_DIR для работы с Jetty. После проведенных манипуляций с заменой WAR архива, стоит перезапустить сервер приложений.

Для обновления RProxy, аналогично требуется запросить свежую версию ПО. Полученным JAR архивом заменить текущий. Перезапустить.

Наши контакты

Проблемы, вопросы, обратная связь:

support@protectimus.com

Потенциальное партнерство, продажи:

sales@protectimus.com

Телефон:

Ирландия +3 537 688 899 22

United Kingdom: +44 20 3808 7124

США: +1 786 796 66 64

Ukraine: +38 057 706 21 24

Russia: +7 499 677 16 34

Корпоративная информация

Protectimus Limited

Carrick House

49 Fitzwilliam Square

Dublin 02, N578

Ireland