



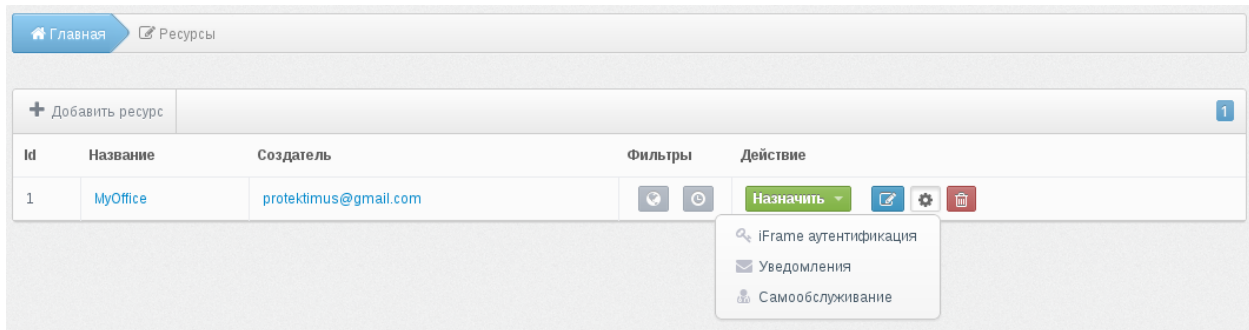
# IFrame виджет. Инструкция по интеграции

Версия 1.00  
от 26 мая 2014

### Настройка IFrame-виджета для простой интеграции

Для аутентификации пользователей Вы можете использовать IFrame-виджет. При его использовании пользователю будет предложено ввести данные аутентификации в разработанной нами форме. После ввода данных мы произведем аутентификацию и отправим Вам уведомление о ее результатах на указанный Вами адрес.

Чтобы включить механизм для Вашего ресурса зайдите в раздел IFrame-аутентификация, который доступен по нажатию на кнопку с изображением шестеренки в списке ресурсов.



На открывшейся странице Вам нужно будет указать следующие параметры:

- Success URL - на этот адрес будет отправлено уведомление в случае успешной аутентификации пользователя.
- Fail URL - на этот адрес будет отправлено уведомление, если пользователь подряд ввел неверные данные большее количество раз, чем это позволено на текущем ресурсе.
- Пароль - Protectimus будет использовать этот пароль для подтверждения уведомления, которое отправляется на Success или Fail URL.
- Подтверждение пароля - указанный выше пароль для подтверждения корректности ввода.
- Активность - разрешает или запрещает работу механизма на этом ресурсе.

После настройки разместите IFrame для входа пользователей на своей странице.

Он должен обращаться по адресу:

<https://api.protectimus.com/plugins/authentication>

передавая следующие параметры: client\_id, auth\_type, resource\_id resource\_name user\_id user\_login token\_id.

Некоторые из них являются обязательными, другие - нет.

**client\_id** - обязательный параметр, представляет Ваш ID компании, который доступен на вкладке “Персональные данные” страницы профиля <http://service.protectimus.com/profile>

**auth\_type** - обязательный параметр, указывает на тип аутентификации пользователя, который Вы хотите использовать. Параметр может принимать следующие значения:

0 - аутентификация токена, т.е. проверка валидности предоставленного OTP. Этот тип соответствует методу `authenticate/token` в API. При использовании этого типа токен должен быть назначен на ресурс.

1 - аутентификация пользователя по паролю. Соответствует методу `authenticate/user-password` в API. Пользователь должен быть назначен на ресурс, а также у пользователя должен быть задан пароль.

2 - аутентификация пользователя по одноразовому паролю. Соответствует методу `authenticate/user-token` в API. Для использования этого типа токен должен быть назначен на ресурс вместе с пользователем.

3 - аутентификация пользователя по статическому и одноразовому паролю. Соответствует методу `authenticate/user-password-token` в API. Пользователь должен быть назначен на ресурс вместе с токеном, если Вы хотите использовать этот метод.

**resource\_id** и **resource\_name** - идентификатор и имя ресурса. Необходимо указать один из этих параметров, чтобы мы могли определить на каком ресурсе необходимо выполнять аутентификацию пользователя.

По параметру **user\_login** или **user\_id** определяется пользователь, для которого будет производиться аутентификация. Если ни один из этих параметров не указан, то пользователю будет предложено ввести логин самостоятельно.

**token\_id** - идентификатор токена, с которого должен быть проверен OTP. Этот параметр необходим только для случая аутентификации токена, который не связан с пользователем на ресурсе (тип аутентификации `auth_type=0`).

В iFrame будет сформирован набор полей, которые пользователь должен заполнить для аутентификации на Вашем ресурсе.

В случае успешной аутентификации мы отправим Вам POST-запрос по адресу, который Вы указали в качестве Success URL в настройках iFrame-аутентификации ресурса.

Если же пользователь подряд введет неверные данные для аутентификации большее количество раз, чем это позволено на текущем ресурсе, то он будет заблокирован и POST-запрос будет отправлен на указанный Вами адрес Fail URL.

Таким образом, пользователь будет перенаправлен по указанным Вами адресам в зависимости от результатов аутентификации.

В POST-запросе будут представлены все параметры, которые Вы указали при формировании iFrame, кроме них, будут добавлены следующие параметры:

**datetime** - время, когда была проведена аутентификация, представлена в формате: "yyyy-MM-dd HH:mm:ss";

**auth\_user\_id** - идентификатор пользователя, для которого была проведена аутентификация;

**auth\_user\_login** - логин пользователя, для которого была проведена аутентификация;

**auth\_token\_id** - идентификатор токена, для которого была проведена аутентификация;

**hash\_source** - строка, которая будет преобразована с помощью HMAC чтобы подтвердить целостность нашего сообщения. Эта строка состоит из набора остальных параметров, разделенных точкой с запятой;

**hash** - результат преобразования строки **hash\_source** с помощью алгоритма HMAC. Этот параметр представлен в HEX-формате. Более детальные пояснения о том, как формируется хэш смотрите далее.

Параметры **auth\_user\_id**, **auth\_token\_login** не будут представлены, если в аутентификации участвовал только токен. Если же в аутентификация прошла без использования токена, то отсутствующим будет параметр **auth\_token\_id**.

Для подтверждения целостности наших сообщений мы формируем строку **hash\_source** из набора всех переданных Вам параметров, разделенных точкой с запятой. очередность этих параметров в строке следующая:

```
client_id;auth_user_id;auth_user_login;auth_token_id;resource_id;resource_name;user_id;user_login;token_id;custom_params;datetime
```

Полученную строку **hash\_source** мы преобразуем с помощью алгоритма HMAC, в качестве хеширующей функции используется SHA1, в качестве пароля - пароль, указанный Вами в настройках iFrame-аутентификации текущего ресурса. Результат работы алгоритма преобразовывается в HEX-формат и передается Вам в параметре **hash**.

Рассмотрим это более подробно на основании предыдущего примера:

Вы создали пользователя с паролем, назначили ему токен, а потом назначили этот токен вместе с пользователем на ресурс с именем "MyOffice". ID Вашей компании, который представлен в профиле: "1". Чтобы аутентифицировать пользователя по паролю и OTP на этом ресурсе Вам достаточно настроить iFrame-аутентификацию на ресурсе и вставить следующий код на страницу логина:

```
<iframe  
src="https://api.protectimus.com/plugins/authentication?client_id=1&resource_name=MyOffice&auth_type=3">  
Ваш браузер не поддерживает iFrame  
</iframe>
```

Пользователю будет показано окно, где он должен будет ввести свой логин и пароль, если пароль правильный - у пользователя будет запрошен OTP.

Пользователь вводит логин “protector”, свой пароль, и OTP, сгенерированный его токеном.

После этого, мы отправим Вам POST-запрос, который будет содержать следующие параметры:

- auth\_token\_id = 5
- auth\_user\_id = 5
- auth\_user\_login = protector
- client\_id = 1
- datetime = 2014-05-14 18:00:47
- hash = 98548B070F5A4A3D2719FE3FE39146C2174060E6
- hash\_source = 1;5;protector;5;MyOffice;2014-05-14 18:00:47
- resource\_name = MyOffice

В настройках iFrame-аутентификации был указан пароль “pass”, в результате преобразования строки 1;5;protector;5;MyOffice;2014-05-14 18:00:47 по алгоритму HMAC на базе SHA-1 с использованием пароля “pass” получили результат в HEX-формате:

```
98548B070F5A4A3D2719FE3FE39146C2174060E6
```