Настройка портала самообслуживания

Версия 1.0.0
от 10.10.2016

Содержание

Общая информация

Механизм самообслуживания позволяет пользователям самостоятельно выполнять ряд действий по выпуску и обслуживанию токенов, а также их собственных данных. Набор доступных пользователю действий определяет администратор системы. Портал самообслуживания подключается и настраивается индивидуально для каждого ресурса.

Для того, чтобы пользователь смог получить доступ к порталу самообслуживания, он должен быть назначен на соответствующий ресурс. Кроме того, у него должен быть установлен пароль в Protectimus или указан адрес электронной почты, на который будет приходить код подтверждения для входа в портал. Если же указаны и пароль, и адрес электронной почты, то вход будет осуществляться по паролю. После выпуска и назначения на ресурс токена для пользователя при входе также будет запрошен и пароль с этого токена.

Задать пользователю пароль, указать его адрес электронной почты и другую информацию можно при создании пользователя. Также можно отредактировать существующую запись. Для редактирования информации о пользователе, найдите его в списке всех пользователей и нажмите на его логине. После чего, Вы попадете на страницу просмотра детальной информации пользователя. Далее, перейдите на вкладку “Действия” и нажмите кнопку “Редактировать”, после чего внесите необходимые правки и сохраните изменения.

Некоторые вспомогательные компоненты, например Protectimus RPrproxy, могут автоматически создавать пользователей, уже готовых к использованию портала самообслуживания. Например, при работе RPrproxy с Citrix NetScaler Gateway.

Включение механизма самообслуживания

Для включения механизма самообслуживания, откройте страницу просмотра детальной информации о ресурсе, нажав на его имени в списке ресурсов, и перейдите на вкладку “Самообслуживание”. Перед Вами появится окно, изображенное на рисунке 1.

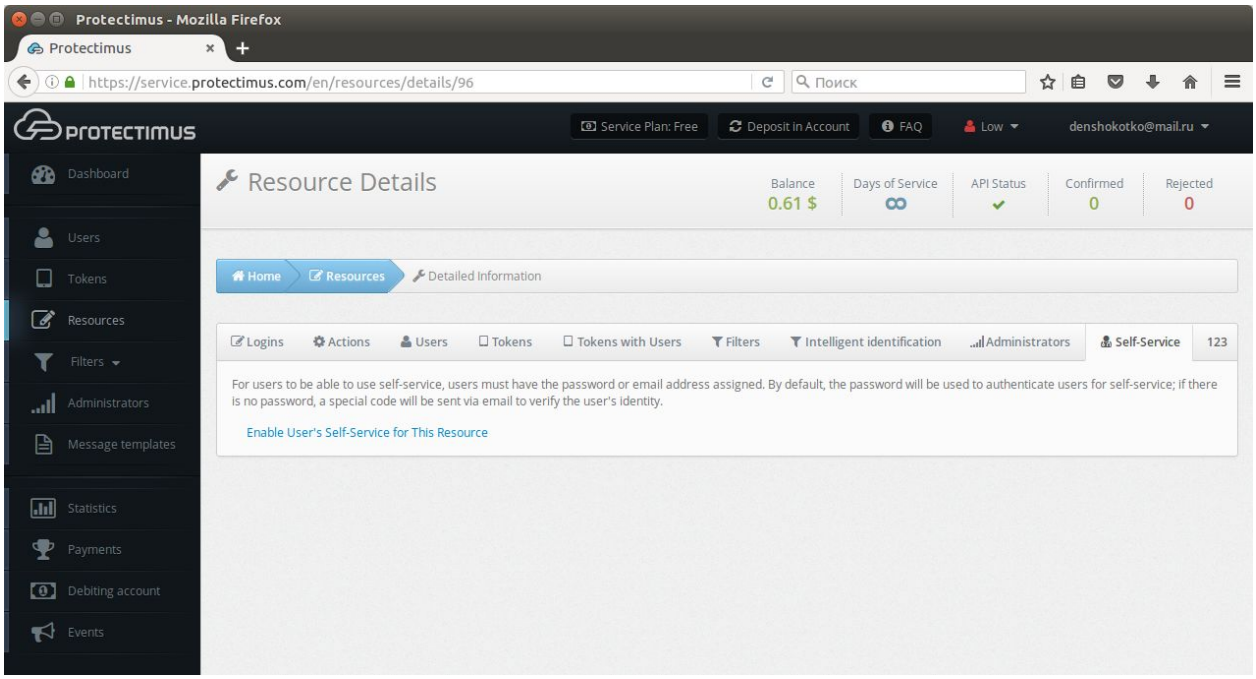

Рисунок 1. Вкладка включения механизма самообслуживания

При нажатии на ссылку “Включить самообслуживание пользователей для этого ресурса” откроется окно создания адреса портала самообслуживания, показанное на рисунке 2. В поле ввода Вам необходимо задать завершающую часть адреса портала, его алиас. Полный адрес портала будет состоять из адреса сервера аутентификации и алиаса, который Вы задали. Например, если Вы работаете с SaaS-сервисом Protectimus и указали алиас “portal”, то ссылка для пользователей будет выглядеть следующим образом: https://service.protectimus.com/selfservice/portal

Если же Вы самостоятельно разворачиваете платформу аутентификации в своем окружении, то часть адреса *“service.protectimus.com”* должна быть заменена на адрес платформы, например: https://localhost:8080/selfservice/portal

Рисунок 2. Создание алиаса портала самообслуживания

После нажатия на кнопку “Сохранить”, Вы увидите список доступных пользователю действий, изображенный на рисунке 3. По умолчанию, все действия отключены.

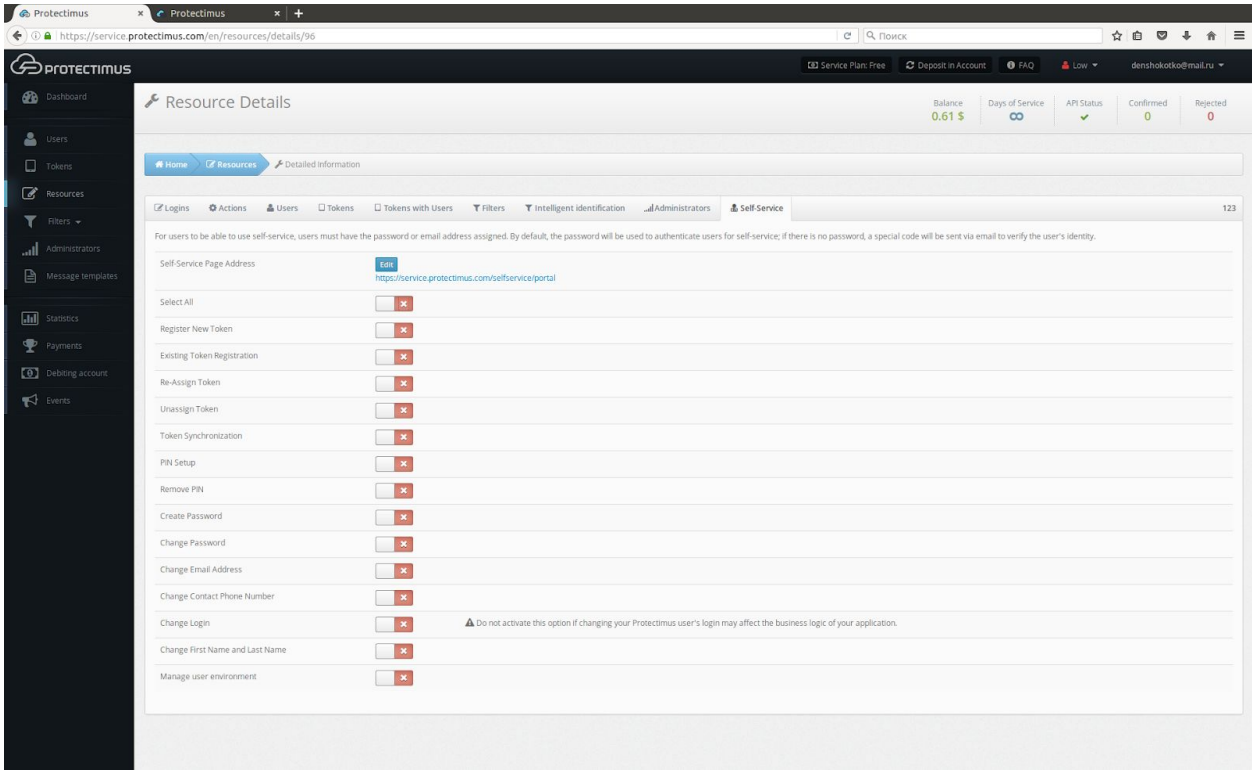

Рисунок 3. Список действий доступных пользователю в портале самообслуживания

После включения всех действий, главная страница самообслуживания будет иметь вид, представленный на рисунке 4. Если же какое-либо из действий будет отключено либо недоступно для конкретного пользователя, то оно не будет представлено на данной странице. Порядок расположения доступных действий на странице также может меняться.

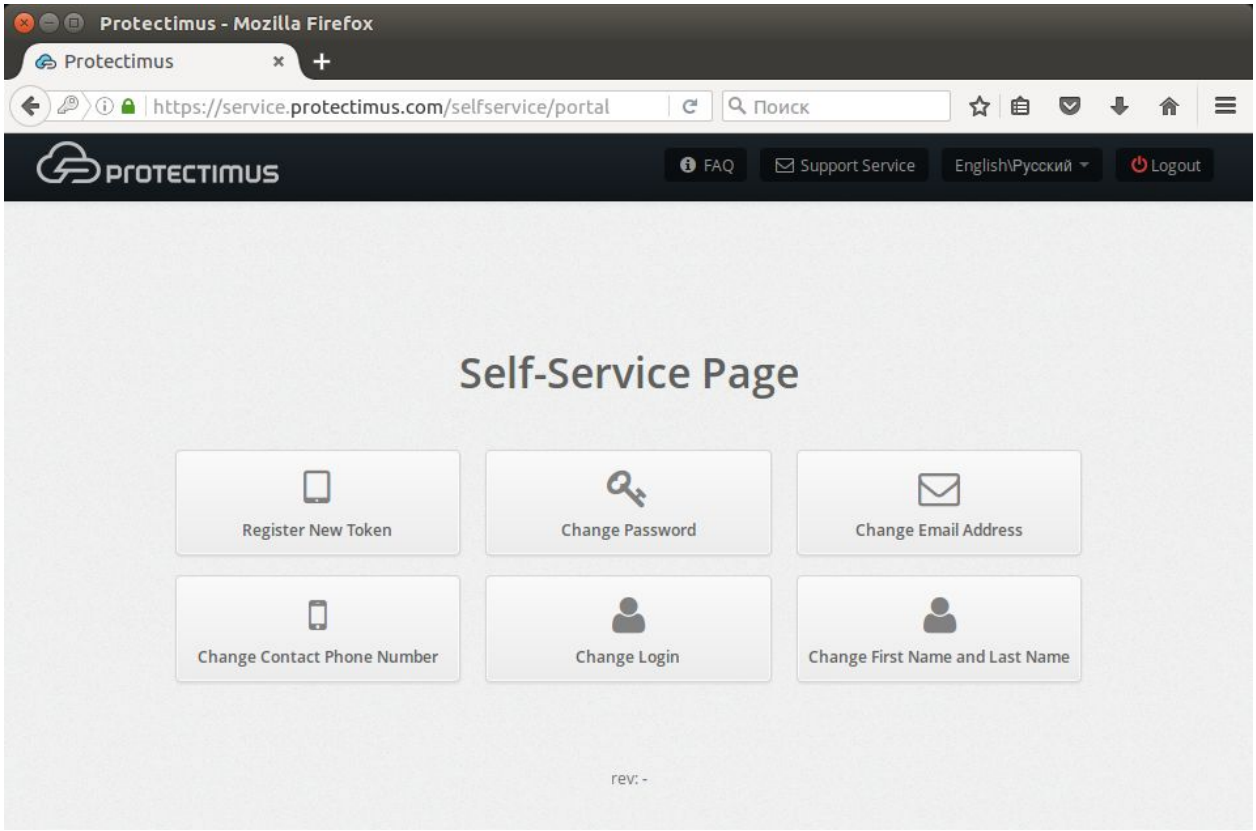

Рисунок 4. Вид страницы самообслуживания при включении всех действий

Названия действий, представленных на рис. 3, говорят сами за себя, рассмотрим особенности их применения:

- *Регистрация нового токена*. Позволяет пользователю создавать, выпускать и назначать себе токены. При включении этого действия, появится список типов токенов, которые будут доступны пользователю в портале. Вы можете оставить только те типы токенов, с которыми планируется работа, чтобы не смущать пользователей обилием других вариантов. После того, как пользователь создаст токен, он будет назначен на этот ресурс как “токен с пользователем”. Начиная с этого момента, для входа в портал у него будет запрашиваться одноразовый пароль, сгенерированный с помощью его токена.

- *Назначение существующего токена*. Позволяет пользователю подтвердить получение токена. Полезно при использовании физических токенов. Получив комплект токенов, Вы назначаете их на ресурс и передаете пользователям удобным для Вас способом, а пользователь, при получении токена, самостоятельно укажет серийный номер полученного устройства и подтвердит владение этим устройством с помощью OTP.

- *Перевыпуск токена*. Позволяет пользователю заменить существующий токен на новый. После выполнения данного действия, старый токен больше не будет доступен.

- *Отменить назначение токена.* Позволяет разорвать связь между токеном с пользователем и ресурсом. При этом, связь пользователя с токеном остается. По сути, назначение на ресурс переходит из режима “токен с пользователем” в режим “пользователь”.

- *Синхронизация токена.* Позволяет синхронизировать токены, если время или счетчик на устройстве и сервере рассинхронизировались (актуально для аппаратных аппаратных токенов, работающих по алгоритму TOTP и OCRA). Чаще всего используется для работы с физическими токенами, т.к. Protectimus Smart имеет встроенную функцию синхронизации. Важно отметить, что Protectimus Smart будет синхронизироваться по времени с основными серверами Protectimus, поэтому, если Вы используете платформу, необходимо, чтобы время на ней также было выставлено корректно.

- *Настройка PIN-кода*. Позволяет пользователю подключить дополнительный PIN-код к токену. Включив эту функцию, пользователь будет обязан вводить установленный 4-х значный код в поле для ввода OTP до или после самого OTP, в зависимости от его выбора. К примеру, если пользователь установил PIN-код “1111”, выбрал ввод PIN-кода после OTP, а токен сгенерировал одноразовый код “123456”, то при входе в систему, в поле для ввода OTP пользователю нужно будет ввести следующую комбинацию: “1234561111”.

- *Удаление PIN-кода.* Разрешает пользователю отменить использование PIN-кода.

- *Создание пароля.* Позволяет пользователю создать себе пароль в Protectimus.

- *Изменение пароля.* Разрешение изменять пароль в Protectimus.

- *Изменение почты.* Разрешение изменять адрес электронной почты в Protectimus.

- *Изменение контактного телефона.* Разрешение изменять телефонный номер в Protectimus.

- *Изменение логина.* Разрешение изменять логин в Protectimus. Важно: чаще всего, при интеграции с другими сервисами, связь между системами устанавливается именно по логину, поэтому его изменение пользователем только в одной из систем может привести к невозможности его идентификации в Protectimus и нарушении логики работы при обращении из сторонних сервисов.

- *Изменение имени и фамилии.* Разрешение менять имя и фамилию в Protectimus.

- *Работа с окружением пользователя.* Экспериментальная функция интеллектуальной идентификации пользователя. При входе пользователя в систему, оценивается процент соответствия параметров его текущего окружения со значением параметров его обычного окружения.

Проверка механизма самообслуживания

Для того, чтобы лучше понять, как работает механизм самообслуживания рекомендуем администратору создать тестового пользователя и проверить работу желаемых функций самостоятельно.

Рассмотрим шаги, которые нужно выполнить для проверки работоспособности службы создания токенов:

1) Включите механизм самообслуживания и включите функцию создания токенов, как описано выше.

2) Создайте пользователя и укажите для него пароль и/или адрес электронной почты, к которой Вы имеете доступ.

3) Перейдите на страницу “Ресурсы” и назначьте созданного пользователя на ресурс.

4) Откройте портал самообслуживания по адресу, который указывался при его создании.

5) Введите логин созданного пользователя.

6) Введите пароль пользователя или код, который пришел на его электронную почту. При этом, если у пользователя были указаны и пароль, и адрес электронной почты, вход осуществляется по паролю. Если данные были указаны корректно, Вы должны получить страницу со списком доступных действий.

7) Для создания программного токена Protectimus Smart, нажмите на кнопку “Создать новый токен” и в открывшемся модальном окне перейдите на вкладку “Программные токены”. При разрешенной работе со всеми видами токенов, модальное окно будет иметь вид, представленный на рисунке 5.

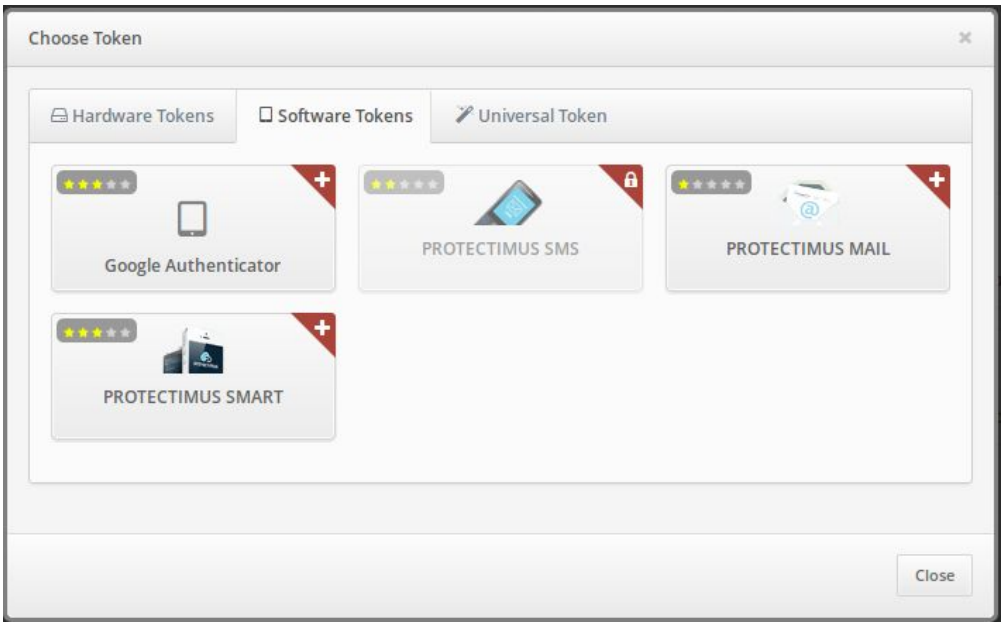

Рисунок 5. Окно выбора типа создаваемого токена

8) Выберите токен Protectimus Smart, введите желаемое имя токена и нажмите на кнопку “Показать QR-код”. Окно будет иметь вид, представленный на рисунке 6.

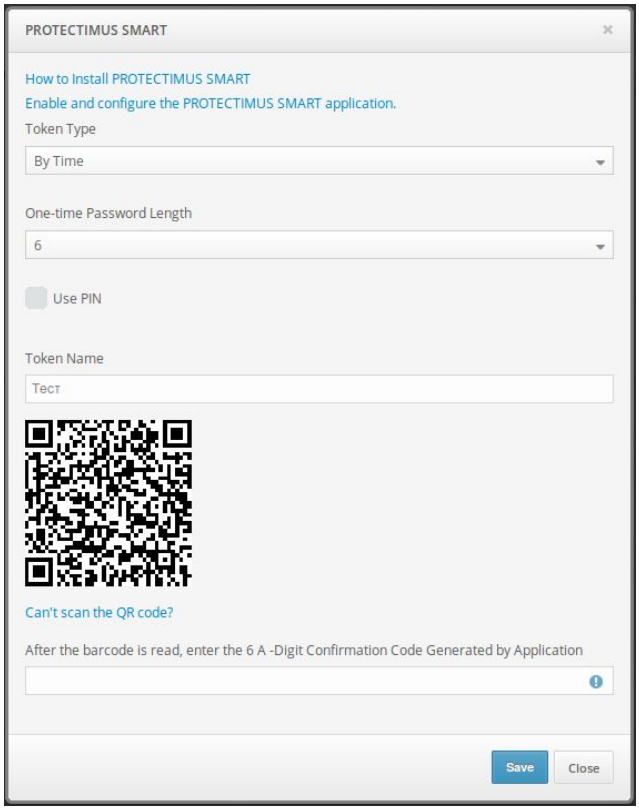

Рисунок 6. Окно создания токена Protectimus Smart

9) Установите и откройте приложение Protectimus Smart на Вашем смартфоне, если этого не было сделано раньше.

10) Выберите действие “Добавить токен” на главном экране или вызовите его из контекстного меню.

11) У Вас будет запрошен способ создания токена: “Сканировать” - добавление через QR-код, или “Вручную” - ввести данные самостоятельно. Выберите способ “Сканировать”.

12) В приложении откроется сканер QR-кодов, наведите его на QR-код. При успешном сканировании, токен будет создан и в приложении будет отображатся OTP, приложение будет выглядеть как показано на рисунке 7.

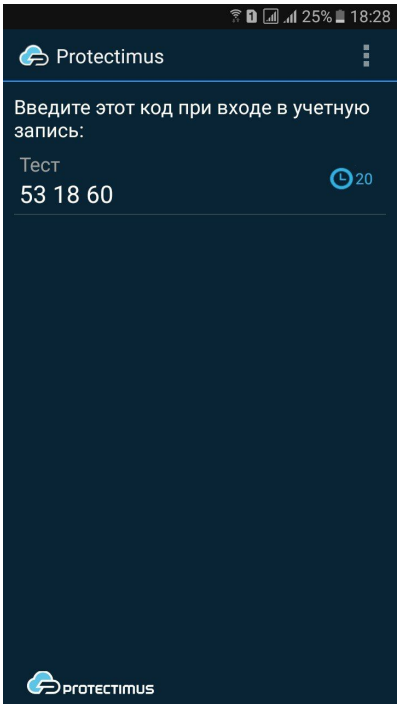

Рисунок 7. Приложение Protectimus Smart с созданным токеном

13) Введите OTP в поле для ввода и нажмите “Сохранить”. Токен будет создан, и Вы увидите сообщение об этом. При возникновении трудностей с созданием токена, нужно синхронизировать устройство с сервером. Для этого подключите устройство к Интернет, в меню приложения выберите “Настройки” - “Коррекция времени”, нажмите “Синхронизировать”. После успешной синхронизации, попробуйте снова ввести OTP.

При успешном завершении всех этапов, токен будет создан, и Вы увидите его в списке токенов в Protectimus, при этом будет указано, что он назначен пользователю, который его создал, как показано на рисунке 8.

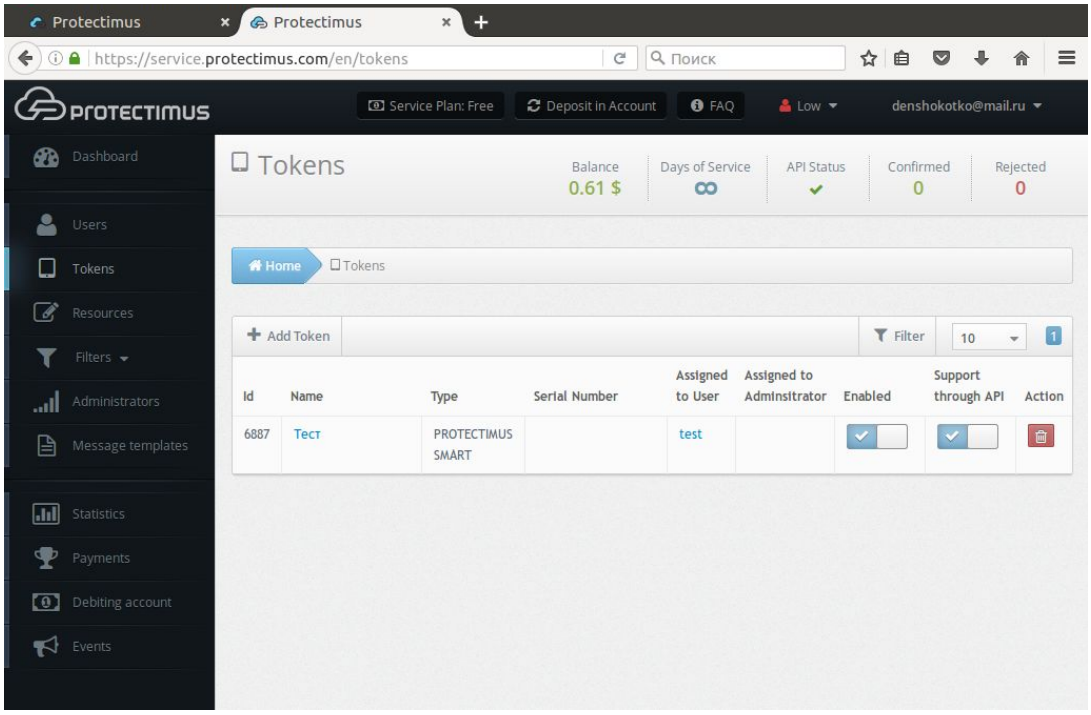

Рисунок 8. Токен, созданный через механизм самообслуживания

При этом, на ресурсе пользователь перейдет из режима назначения “Пользователь” в “Токен с пользователем”, что можно проверить на странице просмотра детальной информации о ресурсе, на вкладке “Токены с пользователями”, рисунок 9.

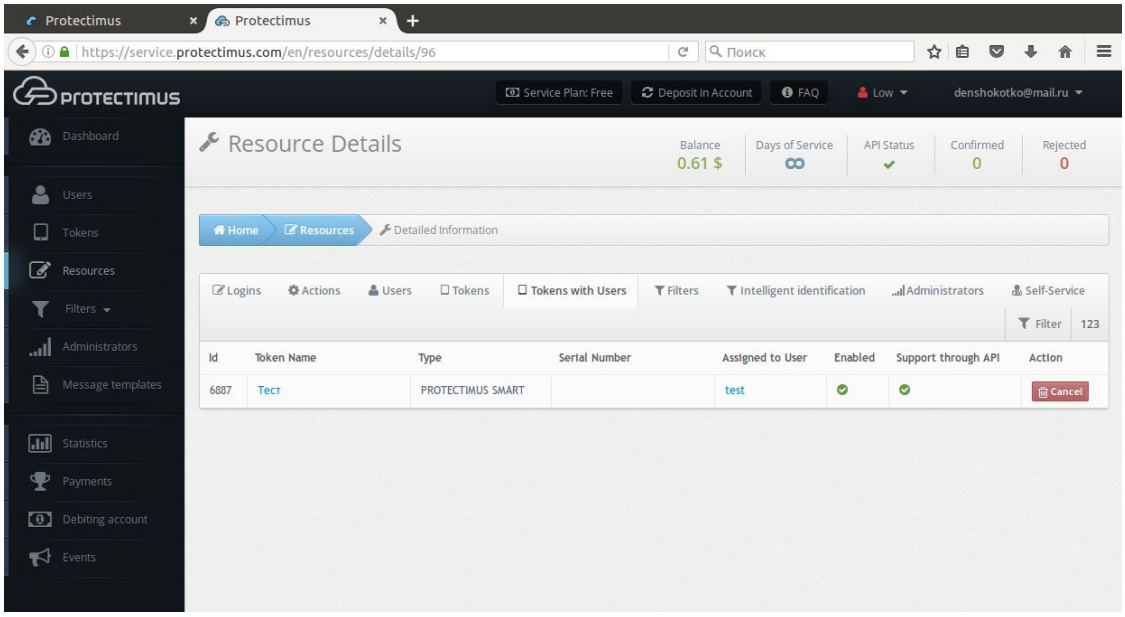

Рисунок 9. Назначенные на ресурс токены с пользователями

Проверить работу токена можно на странице просмотра детальной информации о токене на вкладке “Проверка OTP”, рисунок 10.

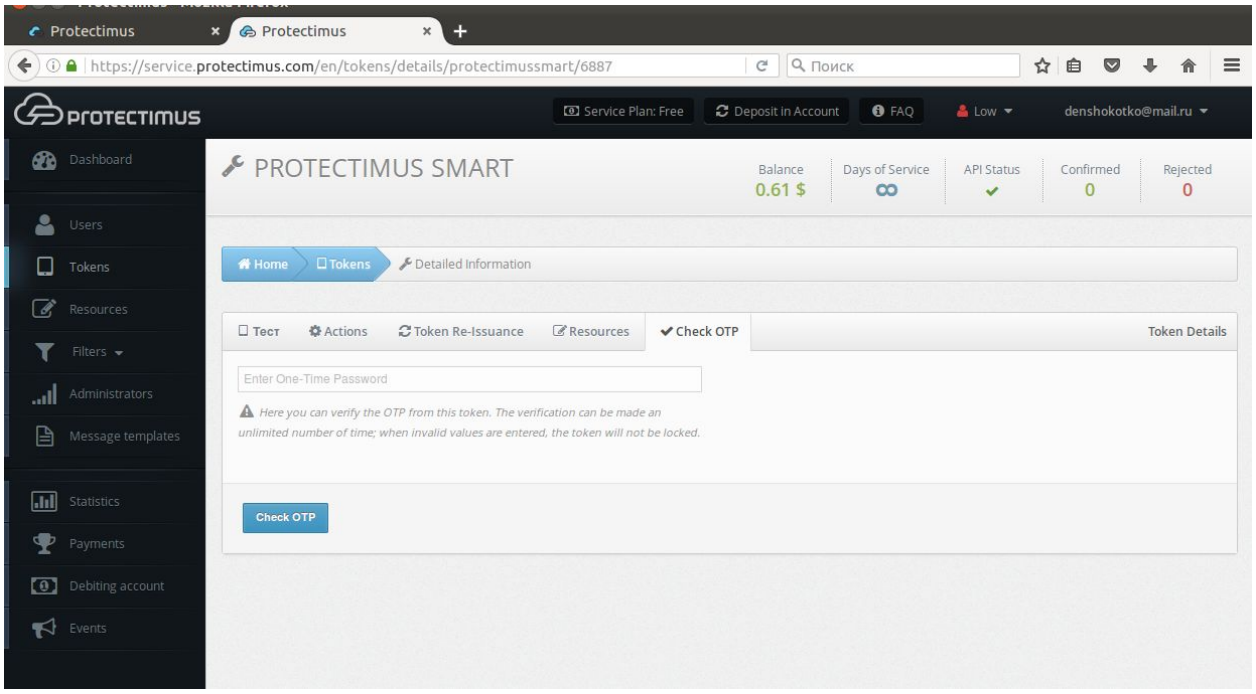

Рисунок 10. Вкладка проверки OTP для токена.

Для проверки, введите OTP из токена и нажмите на кнопку проверки. Результат проверки будет показан во всплывающем уведомлении справа.

Утеря и выход из строя токенов

При утере или невозможности дальнейшего использования токена, пользователь может создать запрос на сброс токена через механизм самообслуживания. Для этого при входе в портал ему необходимо ввести свой логин и нажать на ссылку “Восстановить доступ” под окном ввода пароля и OTP. При этом пользователь увидит экран, показанный на рисунке 11, где он может выбрать, что именно он забыл или потерял.

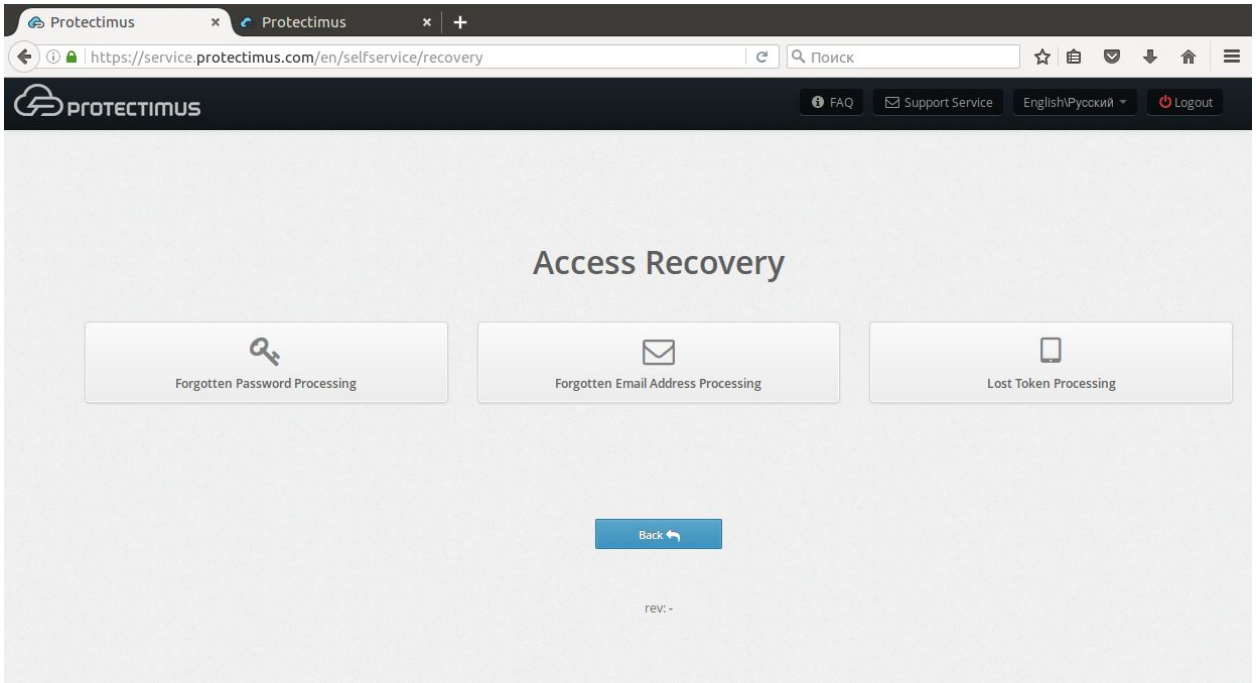

Рисунок 11. Восстановление доступа пользователем

При выборе каждого из вариантов, пользователю будет предложено подтвердить свою личность оставшимися аутентификаторами. К примеру, если пользователь потерял токен, ему будет предложено ввести пароль и/или код подтверждения с электронной почты, как показано на рисунке 12.

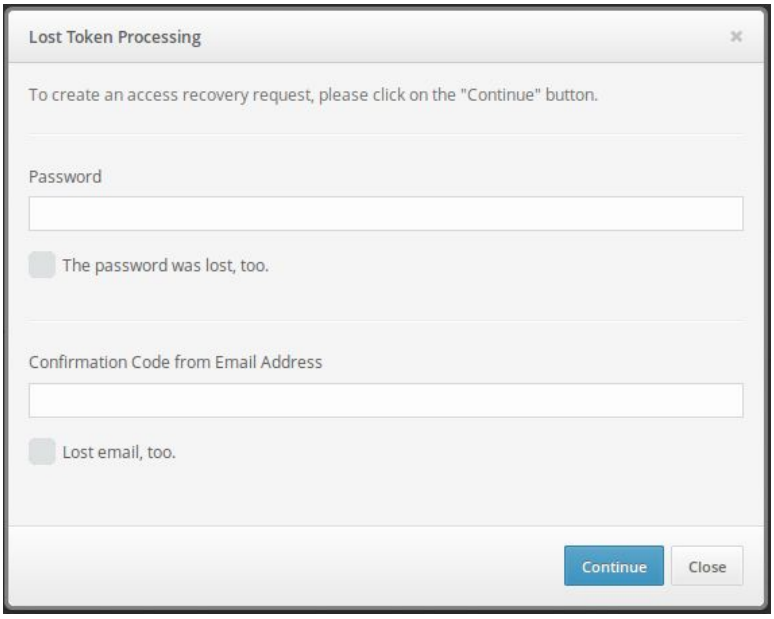

Рисунок 12. Запрос на обработку утерянного токена.

При этом, возможна ситуация, когда пользователь забыл пароль и даже потерял доступ к электронной почте, что можно отметить соответствующими чек-боксами. Если пользователь воспользуется ими, ему будет предложено ввести новые данные для доступа к системе.

После ввода кодов подтверждения и других запрашиваемых данных, в системе будет создан запрос на обработку проблемы пользователя. Администратор сможет увидеть его перейдя в раздел “Проблемы пользователей”, изображенном на рисунке 13. Для перехода в раздел, нажмите на имя учетной записи в правом верхнем углу интерфейса и выберите “Проблемы пользователей”.

Стоит отметить, что на странице нотификаций Вы можете подключить уведомление о возникновении проблем у пользователей.

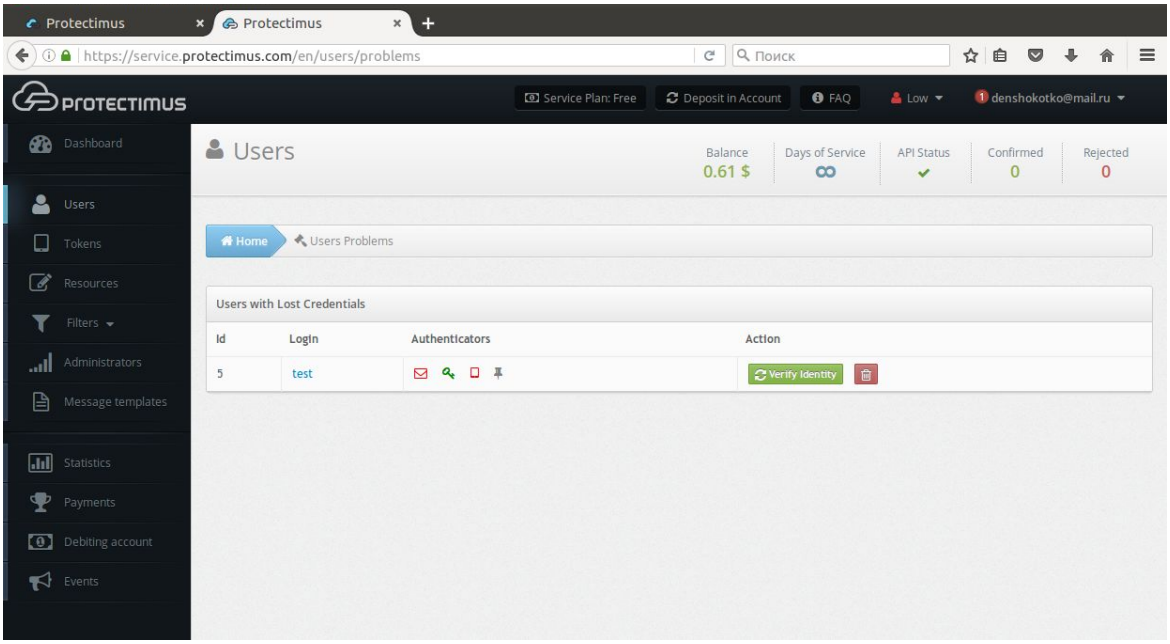

Рисунок 13. Страница просмотра проблем пользователей.

На этой странице видно, что пользователь с логином test потерял токен и не смог подтвердить свою личность кодом с электронной почты - значки токена и e-mail в колонке “Аутентификаторы” отмечены красным, но пользователь подтвердил свою личность вводом пароля - значок пароля отмечен зеленым. Серым же цветом отмечены аутентификаторы, которых не было у пользователя изначально.

Обнаружив такую проблему администратору следует связаться с пользователем, выяснить причины проблемы и провести принятую в компании процедуру идентификации, после чего можно одобрить запрос нажатием кнопки “Подтвердить личность”. Если же запрос был создан ошибочно или есть подозрение о мошеннических намерениях, запрос можно просто удалить нажатием соответствующей кнопки.

В случае подтверждения утери токена администратором, токен с пользователем останется назначенным на ресурс, но токен будет отключен (в таблице со списком токенов в колонке “Включен” будет соответствующий значок). Это позволит пользователю войти в портал самообслуживания без токена и перевыпустить его, если это действие разрешено в портале. Если пользователь запрашивал обработку забытого пароля или изменение адреса электронной почты, он также будет заменен на тот, что пользователь вводил во время создания запроса.

Если пользователь вспомнит утерянные данные до того, как запрос будет обработан, он может просто войти в портал со старыми данными и запрос будет удален автоматически. Такая же схема сработает и при попытке мошеннического восстановления данных - при логине реального пользователя, запрос будет удален.

Заметки для интеграций через компонент RProxy

Компонент Rproxy в состоянии самостоятельно подготавливать пользователей к работе с механизмом самообслуживания.

Рассмотрим работу на примере интеграции с Citrix NetScaler Gateway: если пользователь Active Directory находится в группе, которой указан вход с токеном Smart, но его еще нет в Protectimus или у него там ещё не создан токен, то пользователь будет добавлен в Protectimus и назначен на ресурс. Для пользователя будет указан адрес электронной почты из стандартного или заданного в конфигурации атрибута учетной записи.

Администратору достаточно добавить пользователя в группу для использования Smart-токенов[1] и включить механизм самообслуживания.

После этого, при входе через NetScaler пользователь вводить свой логин и пароль, ему отображается информация о том, что необходимо создать токен через портал самообслуживания.

Открыв портал самообслуживания пользователь вводит свой логин, получает и вводит код подтверждения с электронной почты и проходит процедуру создания токена. После успешного создания токена при входе через NetScaler у пользователя уже будут запрашиваться два фактора: пароль и OTP с выпущенного токена.

[1] При этом, пользователь не должен состоять в группах для входа по e-mail и SMS, т.к. вместо токена для аутентификации будут использоваться эти каналы.

Заключение

Механизм самообслуживания позволяет автоматизировать значительную часть работы администратора и ускорить работу с пользователями. Рекомендуется к использованию в организациях с большим количеством сотрудников, а также при их дислокации в различных географических зонах.

При возникновении дополнительных вопросов обращайтесь в службу поддержки Protectimus.

Контактная информация

Наши службы

Потенциальное партнерство, продажи:

sales@protectimus.com

Проблемы, вопросы, обратная связь:

support@protectimus.com

Корпоративная информация

Protectimus Solutions LLP

https://www.protectimus.com