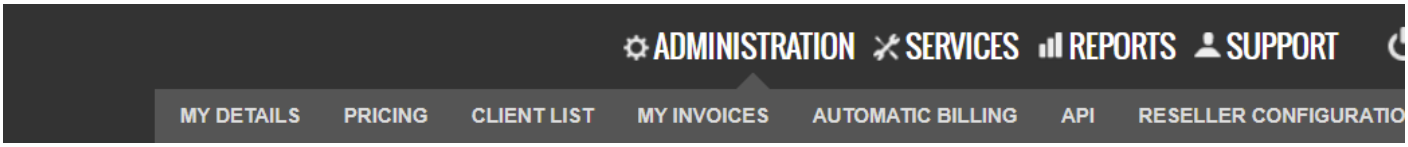
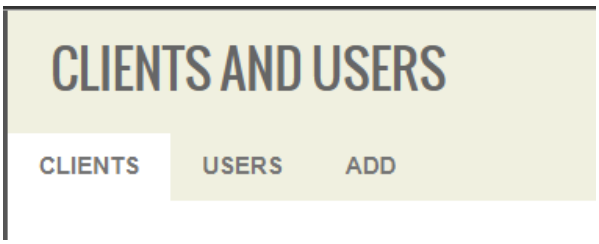
??? ????????? ????? ???????????

1. ???????? ???????????

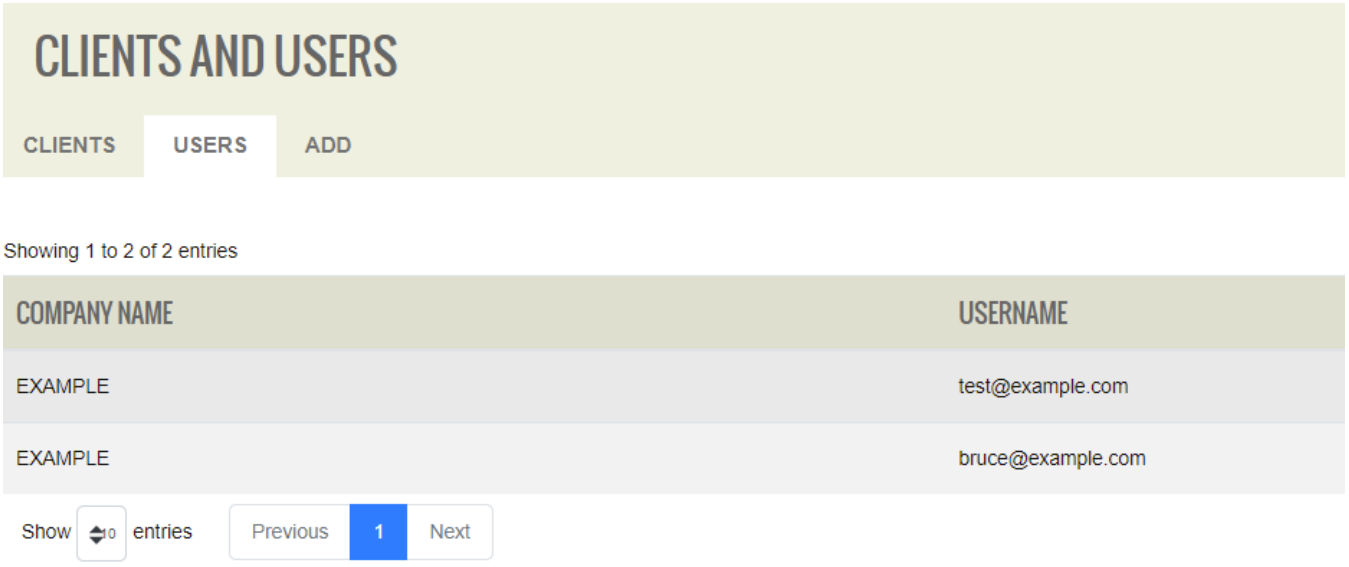
Войдите на портал, используя свое имя пользователя и пароль, и перейдите во вкладку **АДМИН (ADMINISTRATION)** -> **МОИ ДЕТАЛИ (MY DETAILS)**.



Далее на вкладке **МОИ ДЕТАЛИ (MY DETAILS),** войдите в раздел **КЛИЕНТЫ И ПОЛЬЗОВАТЕЛИ (CLIENTS AND USERS PAGE)**

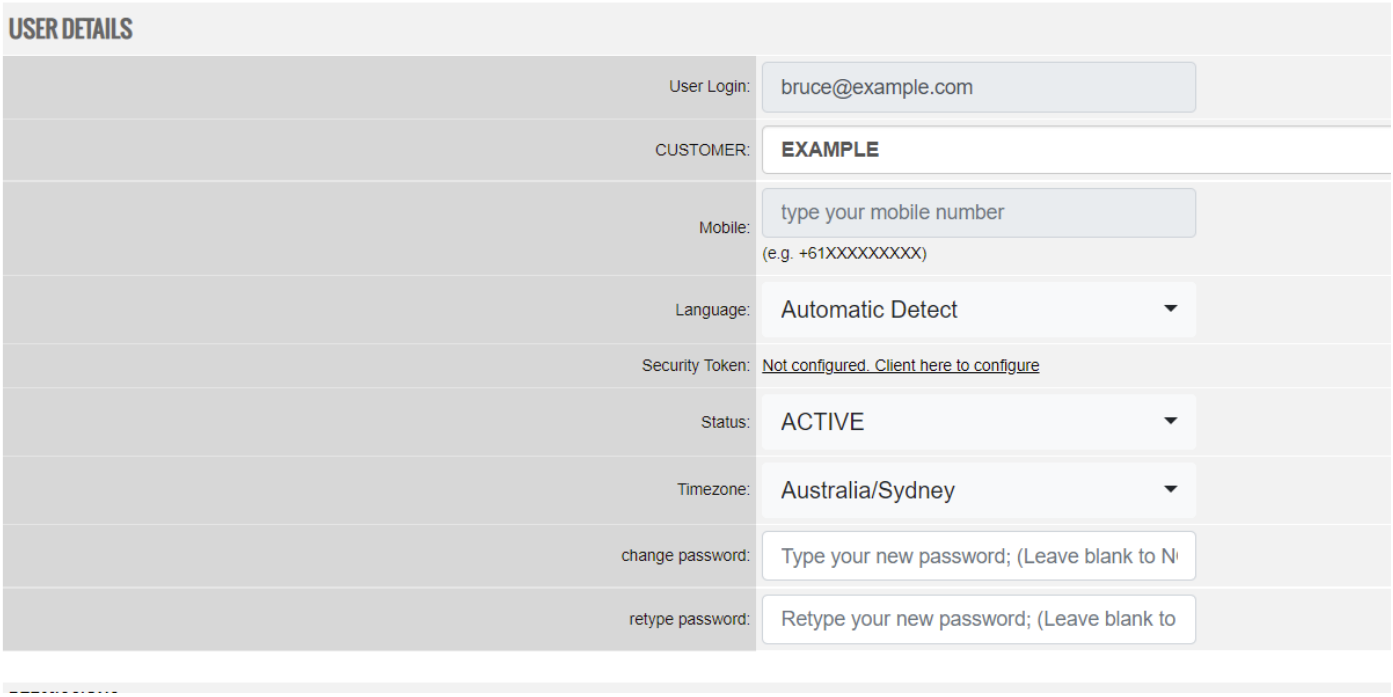


Далее кликните **ПОЛЬЗОВАТЕЛИ (USERS)** чтобы отобразить всех пользователей, которые были присвоены вашей учетной записи **КЛИЕНТА (CLIENT, customer)** и выберите любого **ПОЛЬЗОВАТЕЛЯ (USER)** для редактирования его параметров



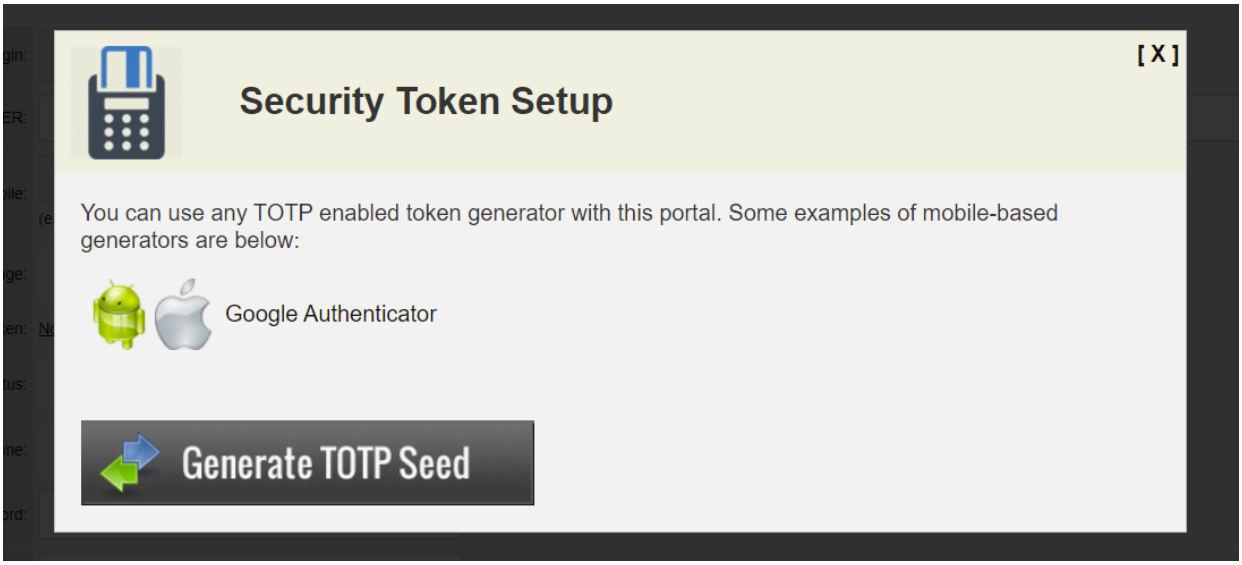
2. ??????? ?????? ?? ?????

Обратите внимание на параметры пользователя, **Токен Безопасности (SECURITY TOKEN)** будет доступен по ссылке, если он не настроен.



3. ???????????? ????? ????????????

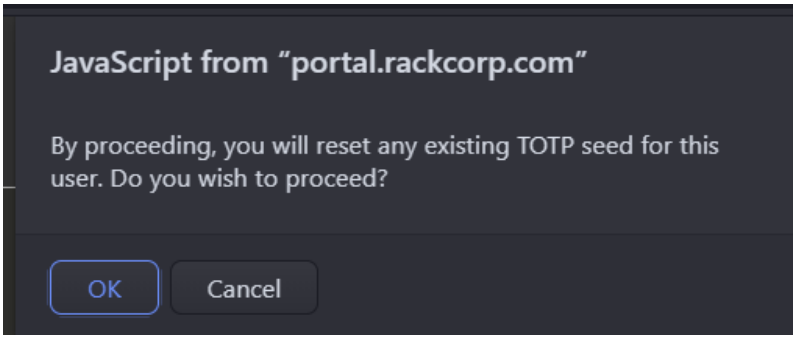
Далее по ссылке, откроется окно настройки токена безопасности, в котором вы можете сгенерировать свой ключ и добавить его в желаемое приложение аутентификатора.

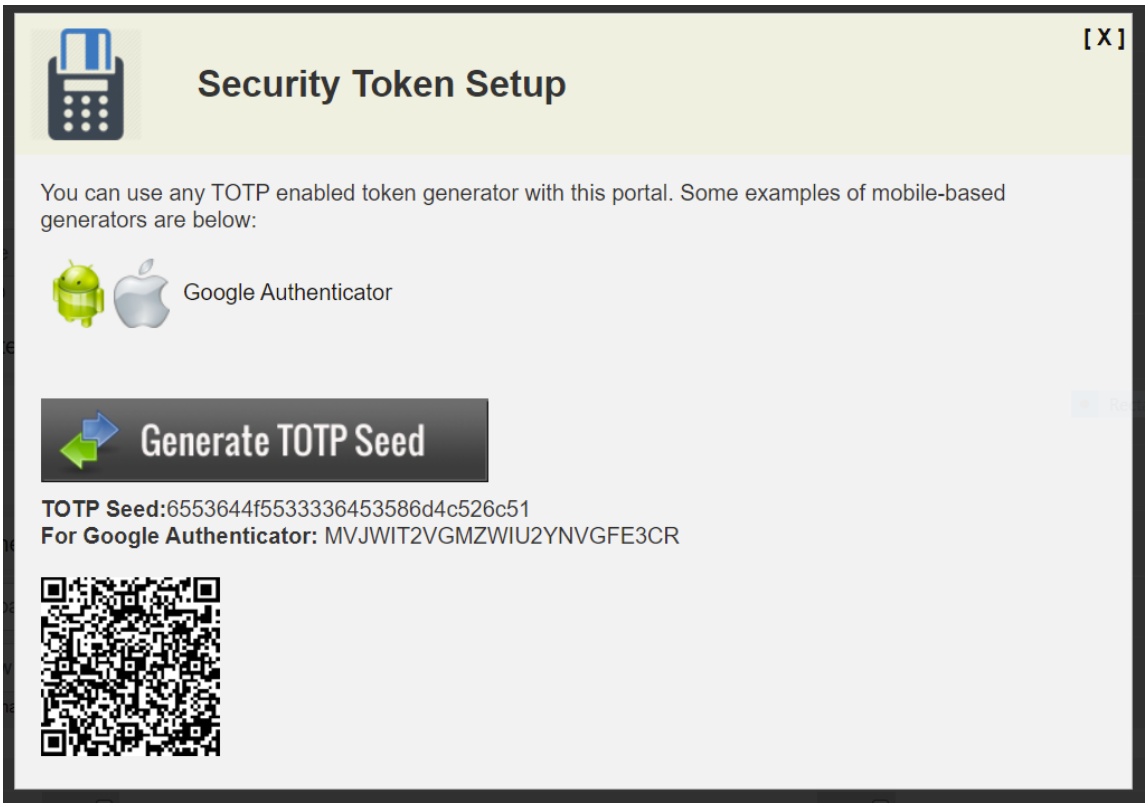


4. ?????????? TOTP Seed

После нажатия кнопки **Сгенерировать (Generate),** будет отображен TOTP Seed и ключ Google Authenticator. Для удобства генерируется QR-код, который можно сканировать с

помощью приложения-аутентификатора.





> Мы настоятельно рекомендуем использовать отдельное физическое устройство, такое как телефон, планшет или аппаратный ключ, для многофакторной аутентификации.

Аутентификатор Google для мобильных устройств может сканировать сгенерированный QR-код с помощью камеры устройства, чтобы получить ключ токена и настроить вашу аутентификацию.

Для настольных аутентификаторов, таких как аппаратный ключ YubiKey, доступна функция захвата экрана, позволяющая захватить сгенерированный отображаемый QR-код с экрана.

В противном случае для таких приложений, как WinAuth, вам нужно будет скопировать и вставить URL-адрес в изображение QR-кода или вручную ввести код ключа в аутентификатор.

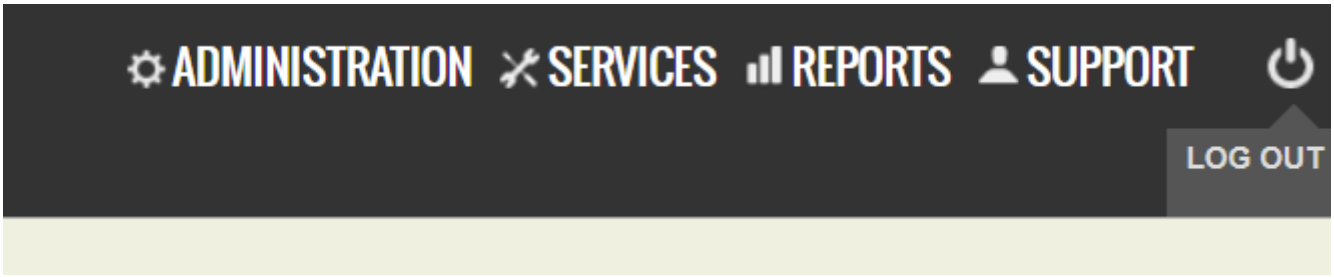
> Как только окно генератора ключей закроется, ваши ключи больше не будут доступны с помощью этой функции, и их необходимо будет сгенерировать заново.

---

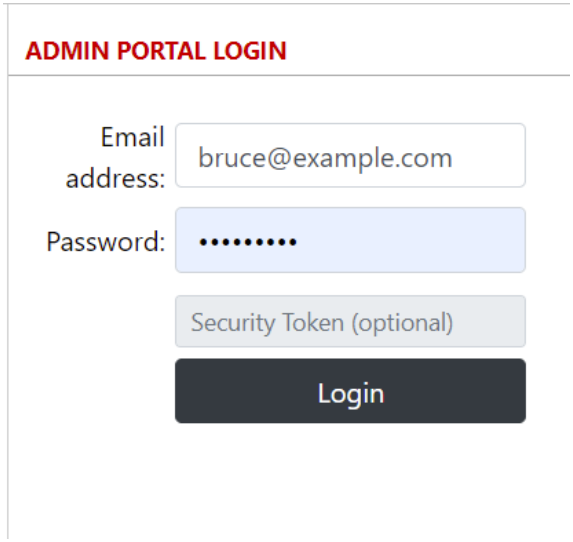
5. ???????? ???????????????

После того, как ваш аутентификатор настроен, рекомендуется протестировать его перед настройкой ваших пользовательских предпочтений для принудительной двухфакторной аутентификации при входе в систему. Если ключ будет неправильным, технической поддержке потребуется сбросить доступ пользователей.

Перейдите к **"Иконке отключения" (POWER)** and кликните **Выйти (LOGOUT).**.



Далее вы будете возвращены на страницу входа в портал.



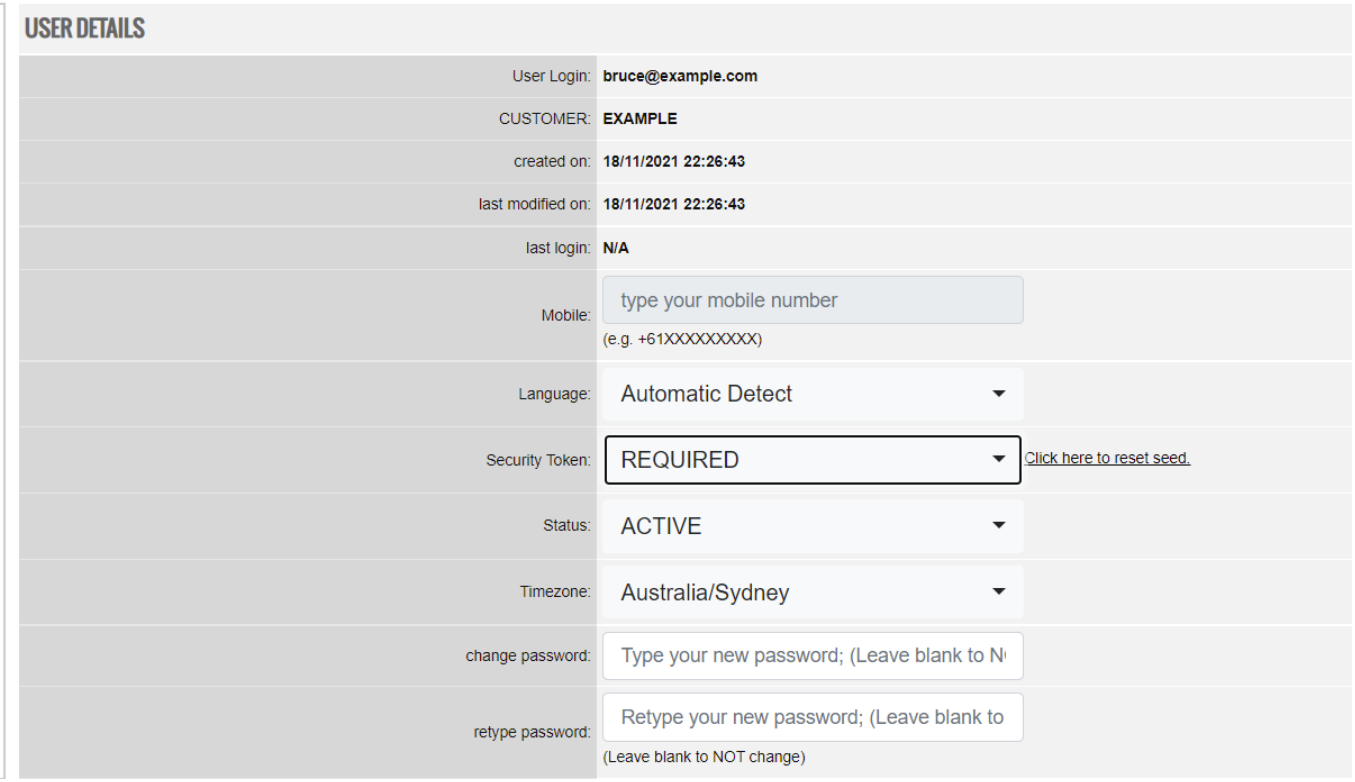
На этом этапе, используя ваш новый аутентификатор, сгенерируйте токен безопасности и введите его в поле и войдите в систему, снова войдите в портал.

Если это будет успешным, перейдите к шагу 6. В противном случае проверьте свой аутентификатор на наличие актуального кода или обратитесь в службу технической поддержки RackCorp.

---

6. ????????? ????? ???????????? ??? ????????????

Если Вы успешно вошли в систему после настройки 2FA, последним шагом настройки токена безопасности будет выбор обязательной двухфакторной аутентификации при входе в систему путем выбора **ТРЕБУЕТСЯ (REQUIRED)** или **НЕ ТРЕБУЕТСЯ (NOT REQUIRED)** в подразделе **ПОЛЬЗОВАТЕЛИ (USERS)** для выбранного пользователя.



---

7. ?????????????? ????

Выполните финальную проверку ваших новых настроек 2FA. В соответствии с **шагом 5:** выйдите из портала RackCorp, а затем войдите в систему, используя только что настроенную двухфакторную аутентификацию в дополнение к вашему имени пользователя и паролю.

Вы должны иметь возможность успешно войти в систему и продолжать пользоваться нашими услугами.

Revision #19
Created 22 November 2021 04:41:06 by KonS
Updated 13 January 2022 04:45:40 by KonS