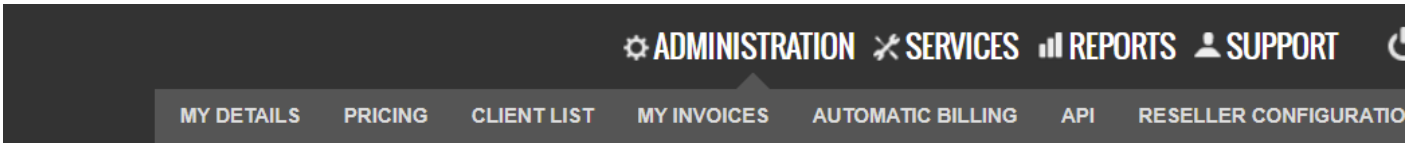
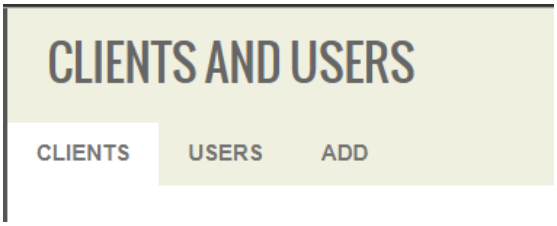
Security Token How-To

1. Choose user

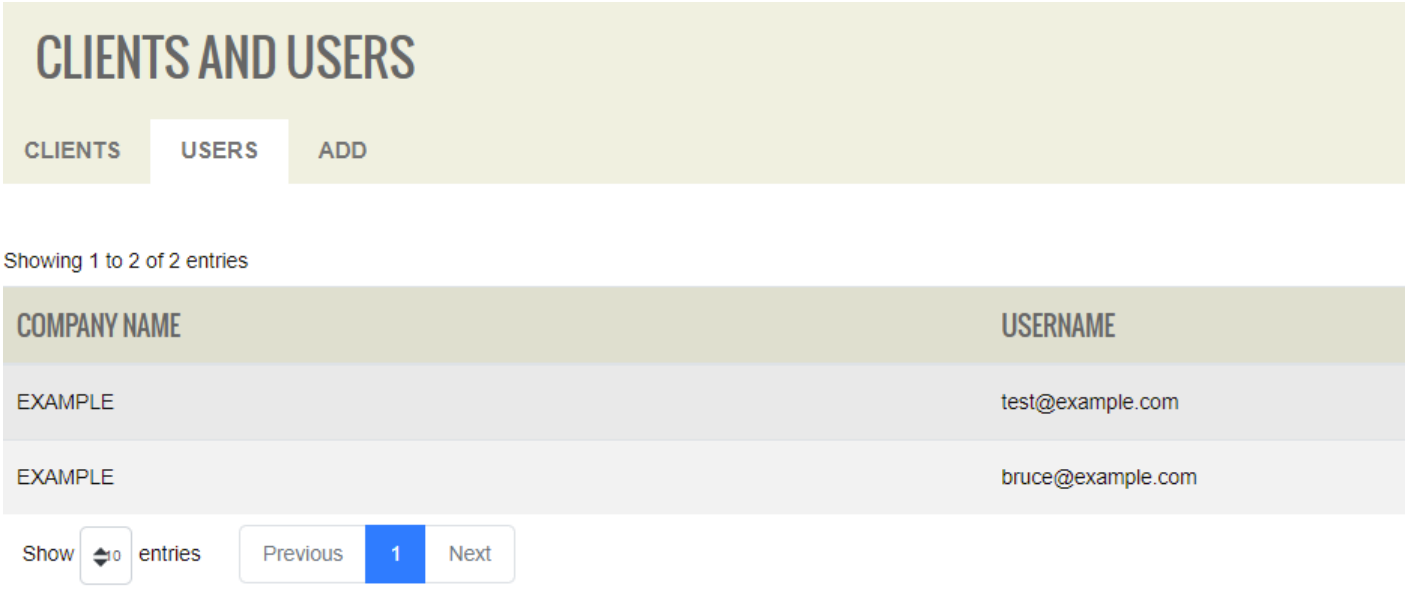
Log into the portal using your username and password and navigate to **ADMINISTRATION** -> **MY DETAILS**



Click on **MY DETAILS**. The **CLIENTS AND USERS PAGE** is displayed.



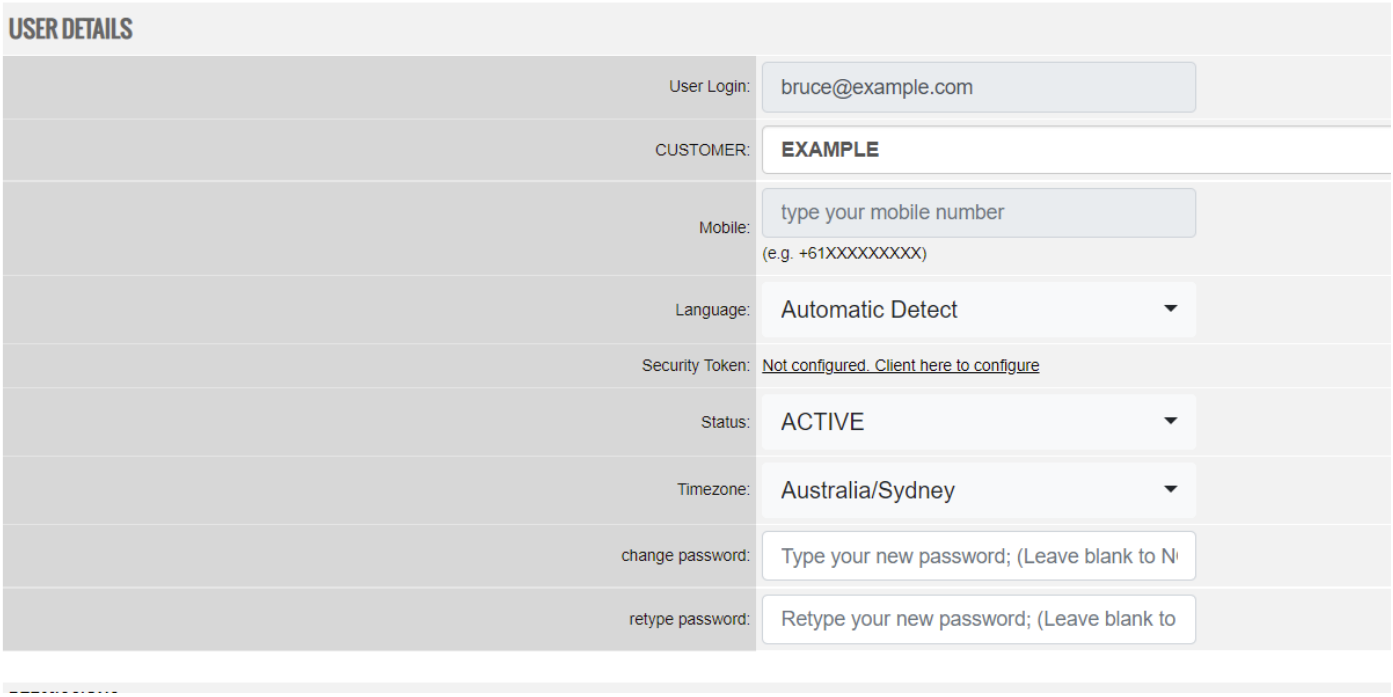
Click **USERS** to display the assigned users under your **CLIENT** (customer) account, and select a **USER** to edit



---

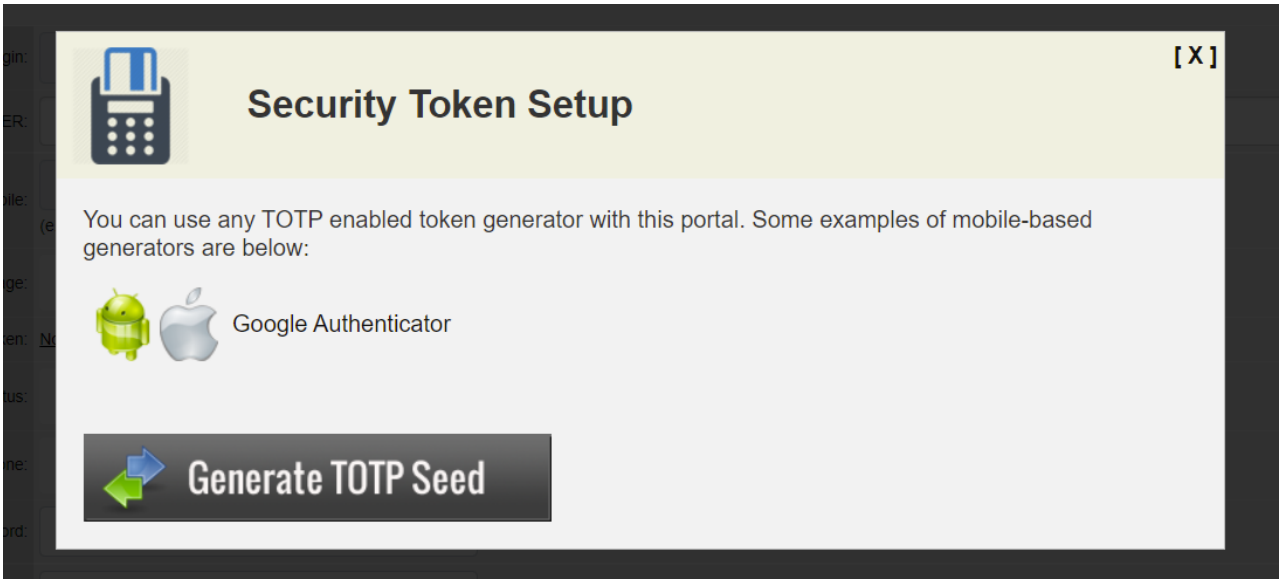
2. Find token link

Note your user details, there should be a **SECURITY TOKEN** link visible ready to be used for the first time.



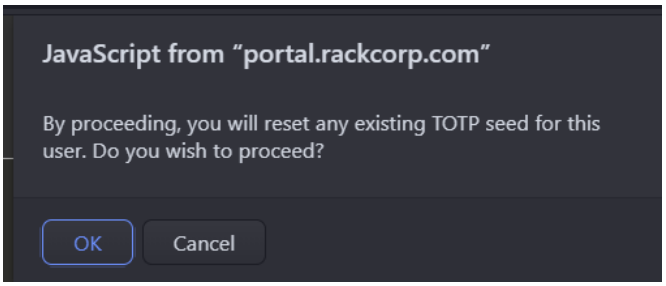
3. Security token setup

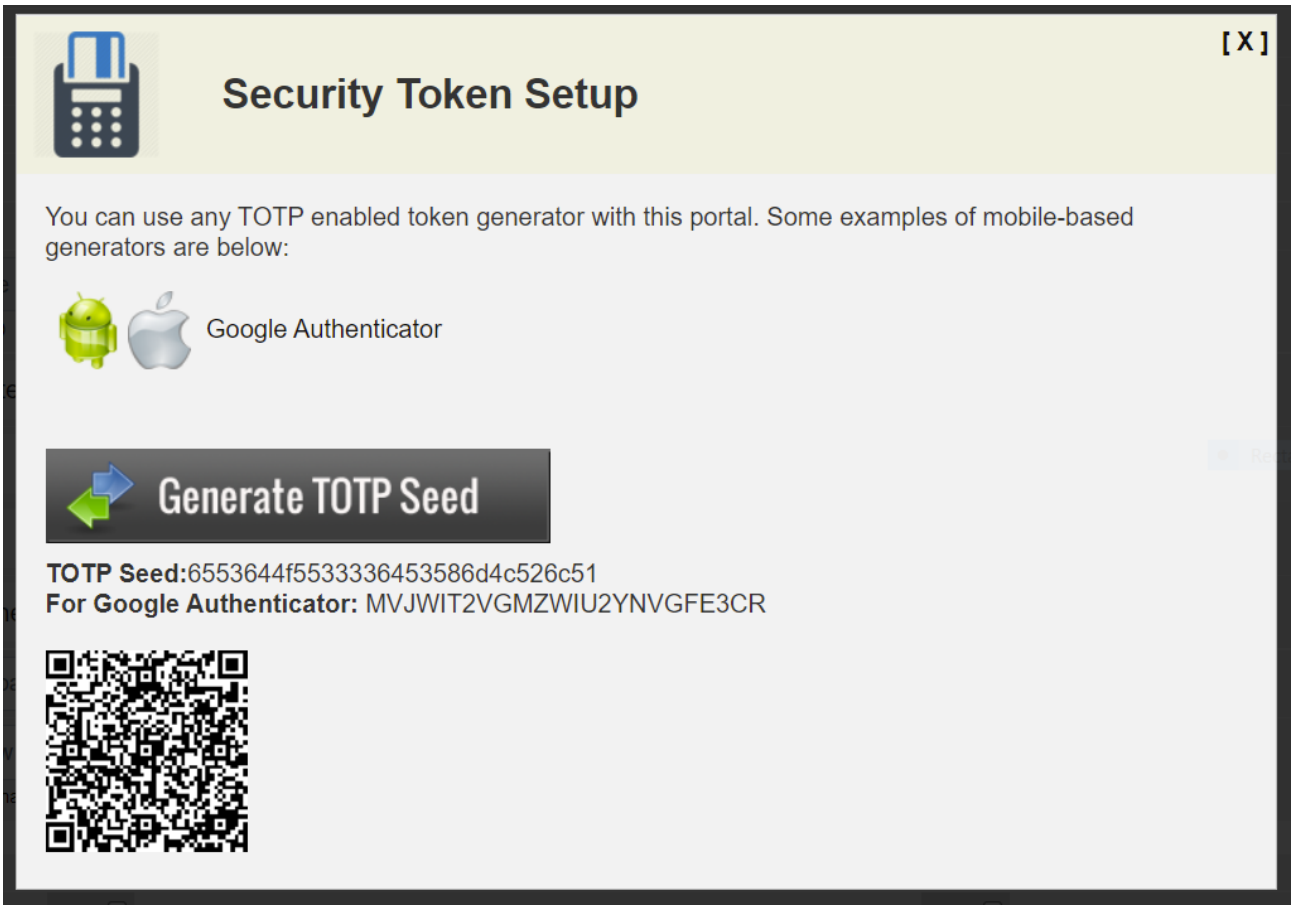
The security token setup window is displayed where you can generate your key to add to your desired authenticator application.



4. Connect TOTP Seed

Once the **Generate** button is pressed, a TOTP Seed key and a Google Authenticator key are displayed. For convivence, a QR code is generated that can be scanned by an authenticator app.





> We strongly recommend that a separate physical device such as a phone, tablet or hardware key be used for multi factor authentication.

Google authenticator for mobile devices can scan the generated QR code using the device camera to retrieve the token key and setup your authentication.

For desktop authenticators such as a YubiKey hardware key, a screen capture function is available where it can capture the generated displayed QR code from the screen.

Otherwise for applications such as WinAuth you will need to copy and paste the URL to the QR code image or manually input the key code into the authenticator.

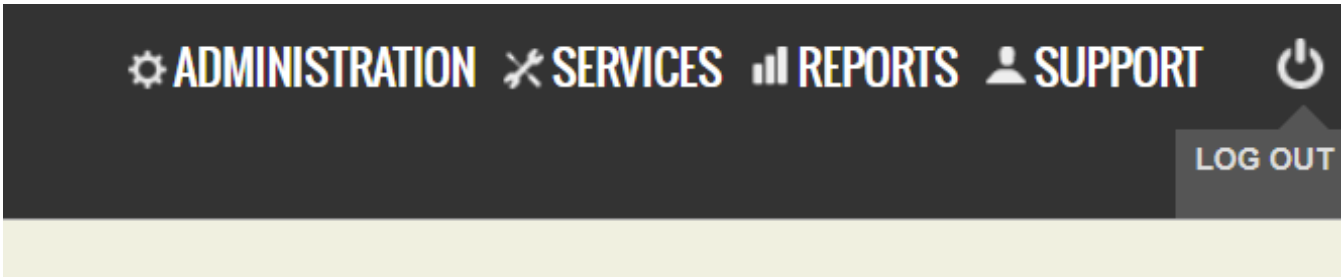
> Once the key generator window is closed, your keys are no longer accessible using this function and need to be regenerated and you are returned to your user details.

---

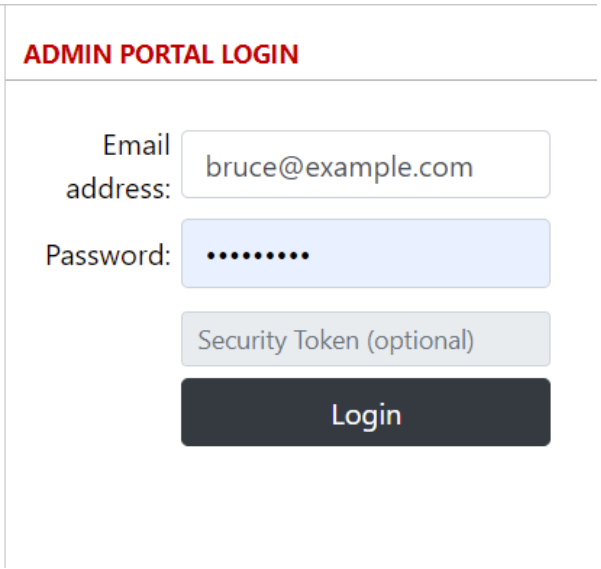
5. Performance check

Once your authenticator is setup, it is advisable to test it before setting your user preferences to enforce Two-Factor Authentication on login, should the key be wrong technical support will need to reset the users access.

Navigate to **POWER** and click **LOGOUT**



You are returned to the RackCorp portal login at portal.rackcorp.com or your company's white label link



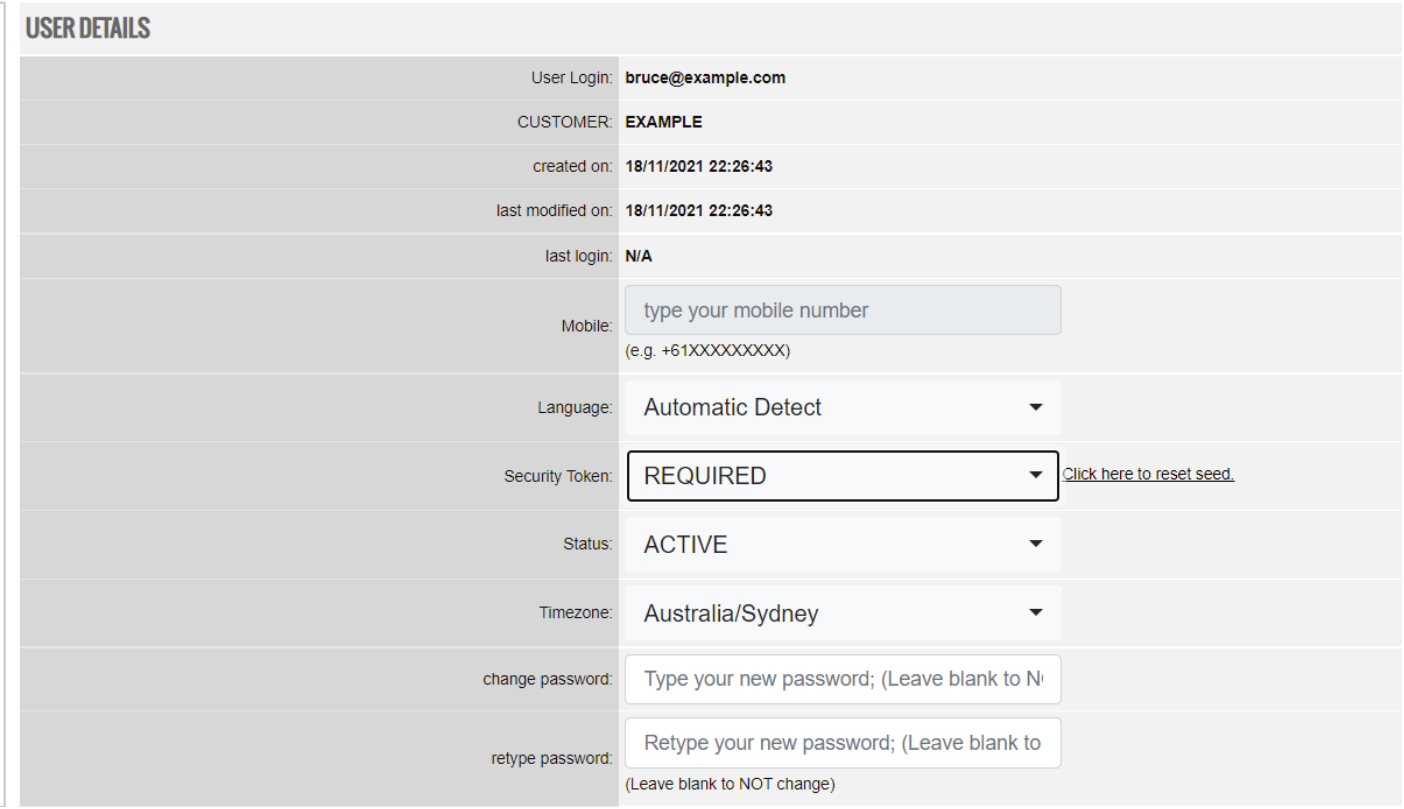
At this step, using your new authenticator to generate the Security Token and input it into the field and login, log back into the portal.

Should this be successful progress to step **6**. otherwise check your authenticator for most current code or contact RackCorp Technical Support.

---

6. Configure security token for a user

Should you login successfully after configuring 2FA, The final step to Security Token setup is to select whether two factor authentication is mandatory required or not on login by selecting **REQUIRED** or **NOT REQUIRED**.



---

7. Final test

Perform a final test of your new 2FA settings. As per step **5,** log out of the RackCorp Portal and then login using your newly setup Two Factor Authentication in addition to your username and password.

You should have be able to login successfully and can continue using our services.

Revision #23
Created 18 November 2021 11:47:46 by RackCorp
Updated 10 August 2023 06:24:43 by KonS