2-Factor for Organizations

Last Modified on 02/02/2024 2:16 pm CST

Exciting news! Our ConnectBooster Support documentation is moving to a new location. Be sure to bookmark the new link below.

https://help.cb.kaseya.com/help/Content/0-HOME/Home.htm

2-Factor Authentication for Organizations

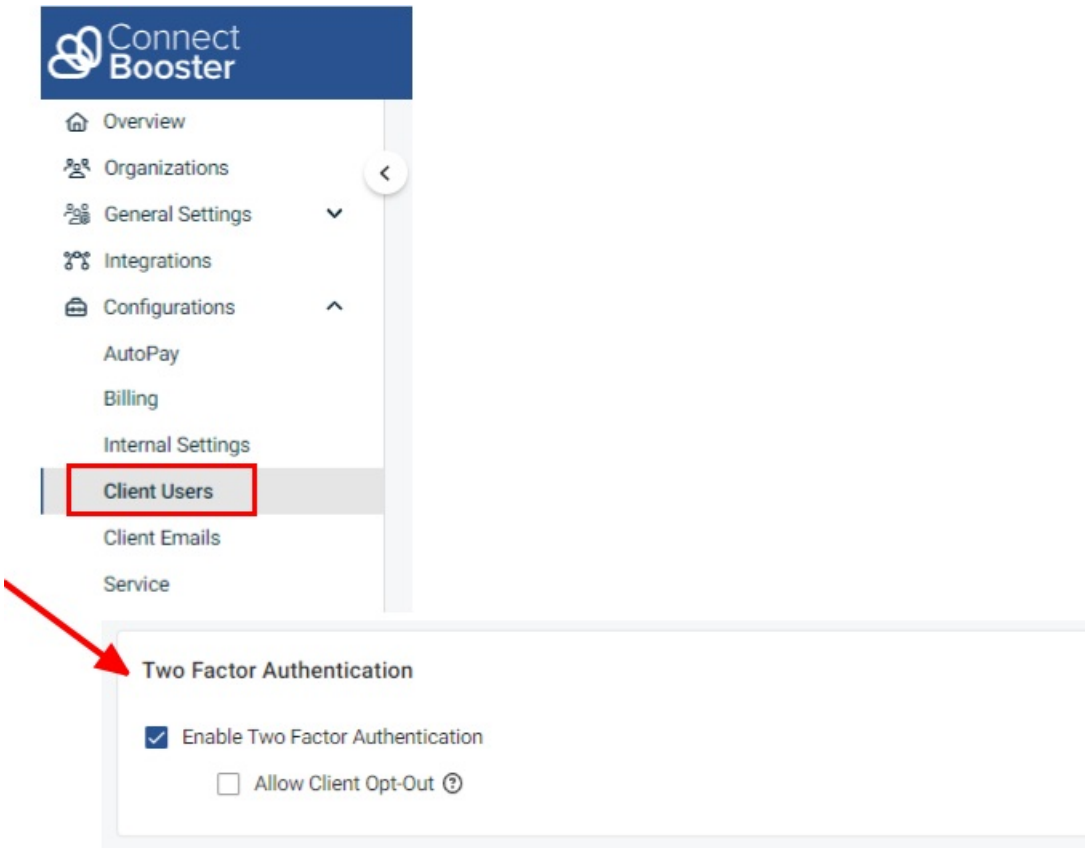
This function allows you to further secure your client's account login via one-time use, SMS text messages.

If enabled on your portal, **ALL** Organization logins will immediately be forced to enroll on their next login attempt. Additionally, you can decide if you want to give your organizations the option to enroll, or "**Opt-Out**", if they choose.

Setup Instructions

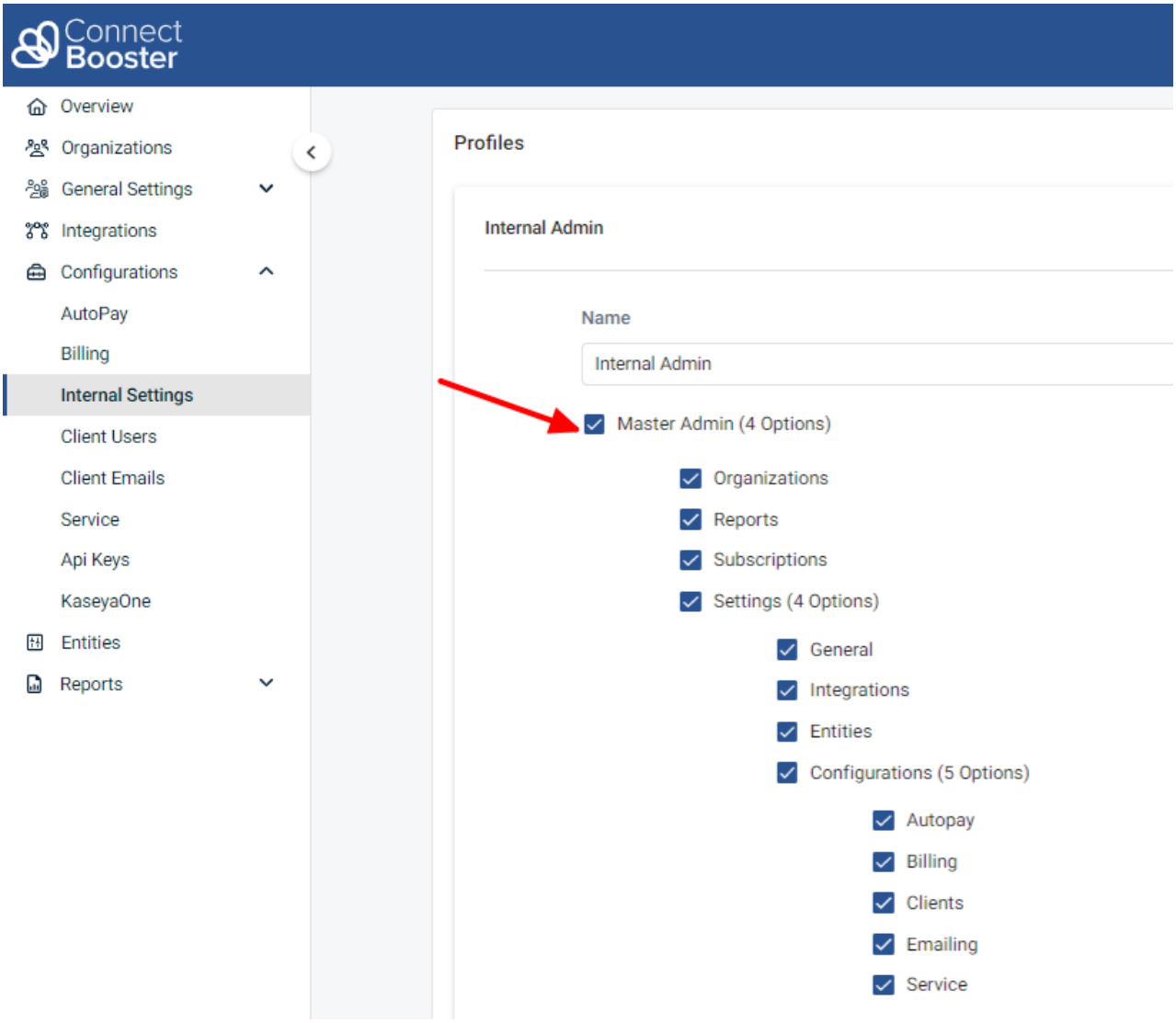
Our SMS based 2-Factor will send a text message code to the enrolled mobile phone number.

To get started, login to your portal and navigate to *Configurations + Client Users.* Expand the Two Factor Authentication header, select the check box and save your changes.



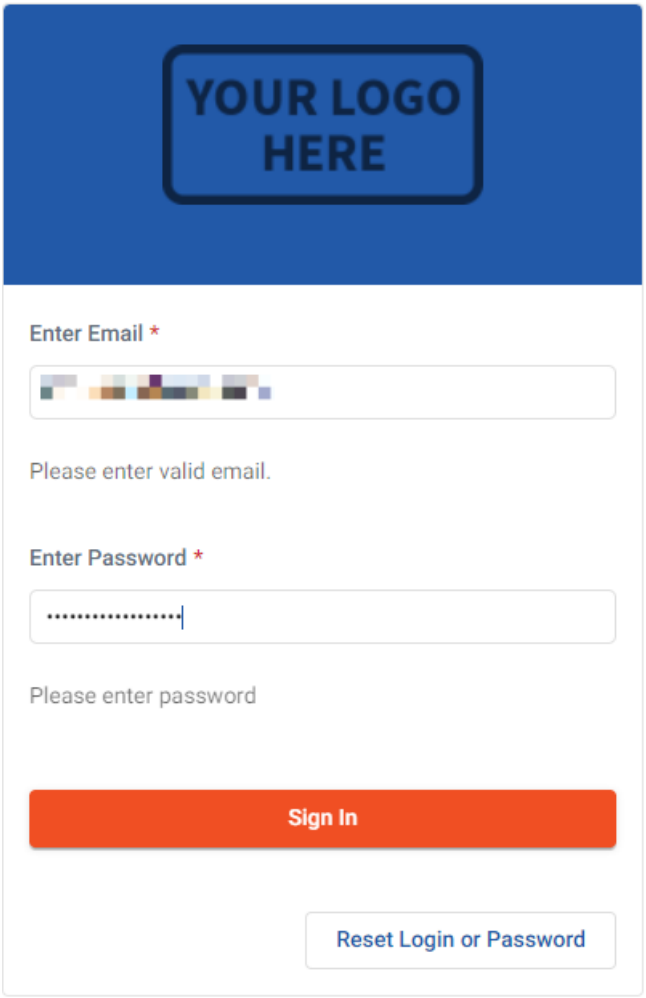
> If you ***don't see this option***, your account may not have high enough profile privileges to enable this feature within the portal.

Please check that the "Profile", selected for your account is the same as a Profile with the "Master Admin" option enabled.

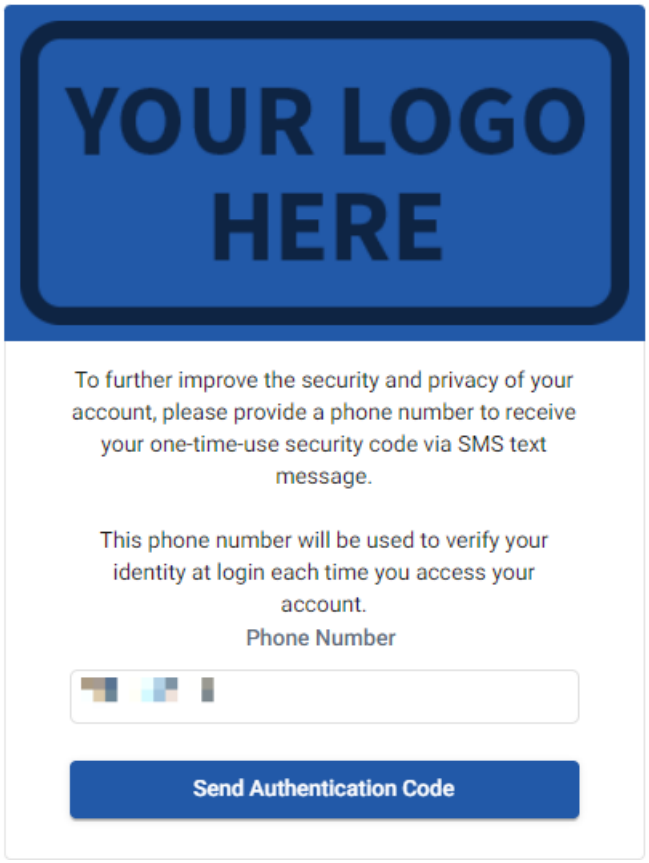


Once enabled on your portal, the ***next*** login via your organization's standard username/password will begin the enrollment process.

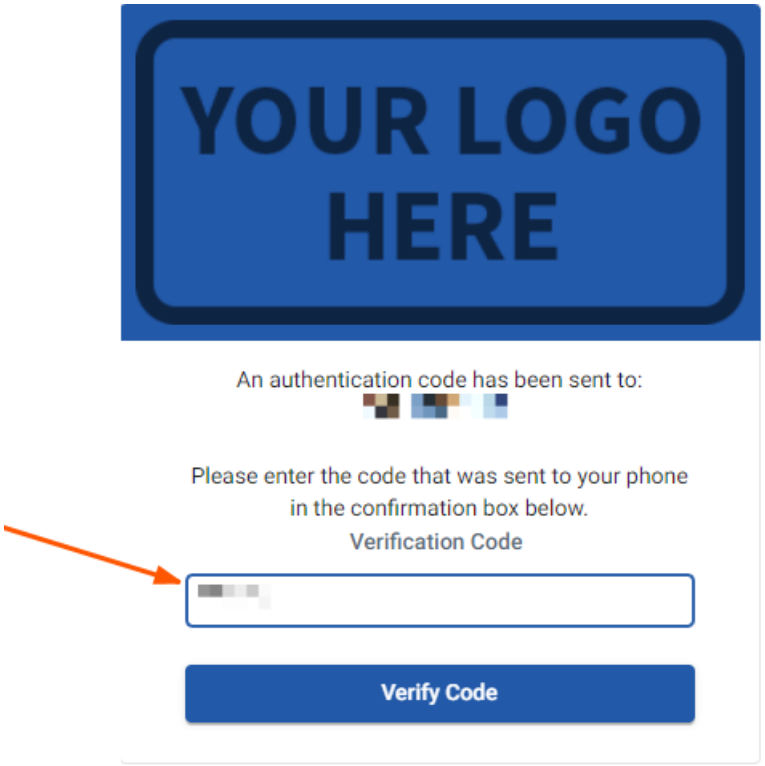
> This will now be a requirement for **all your organizations**.



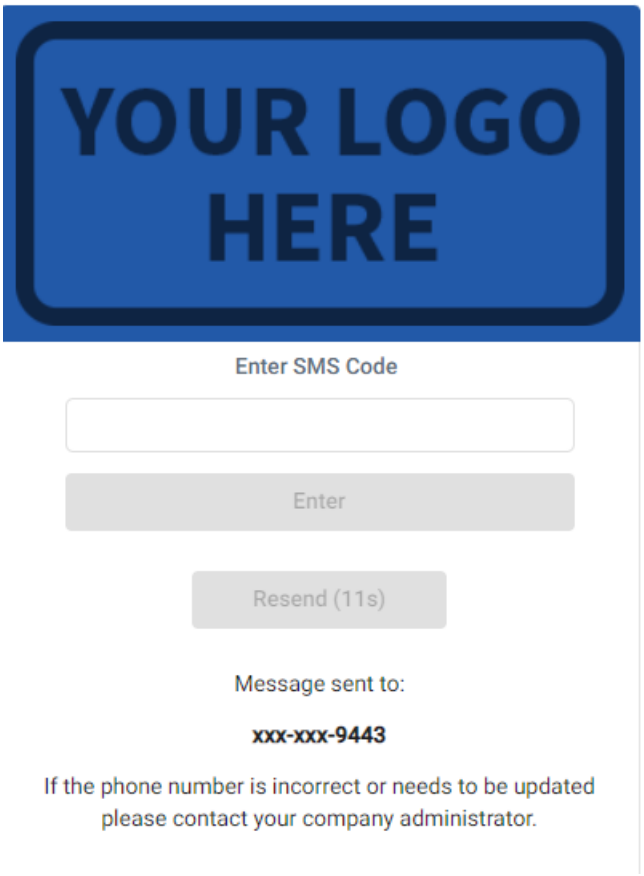
After initial successful login, your client will be prompted to enter a phone number.



The organization will need to confirm the first received text message. After validation, the client will need to re-enter username/password to login.



After that initial setup, *subsequent* login attempts will simply require to enter your SMS code going forward.

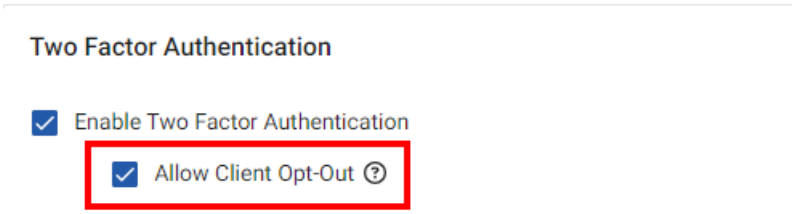


Congratulations, that's it! Your organization accounts are now protected via 2-factor authentication.

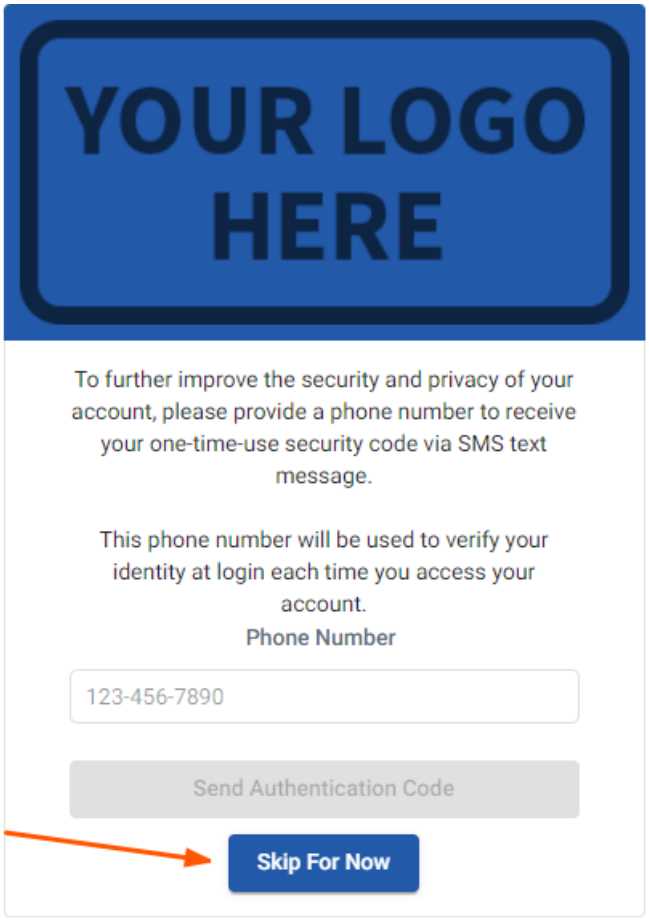
> If you decide to later turn this off and re-enable in the future, all previously configured organizations will need to follow the enrollment steps again.

2FA Client Opt-Out

If you elect to give your clients the choice of doing 2FA, this can be enabled under the main "TWO FACTOR AUTHENTICATION" section.

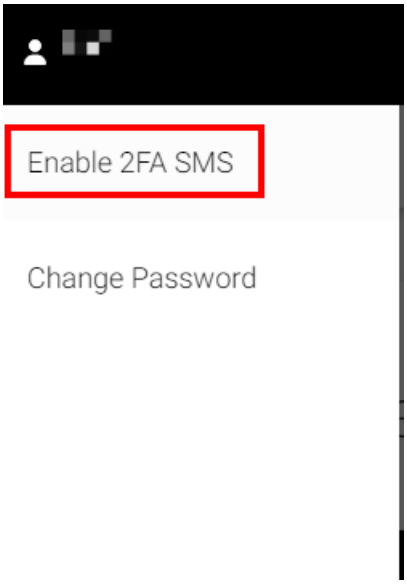


Once enabled, the enrollment screen is slightly modified with a button allowing the user to skip.

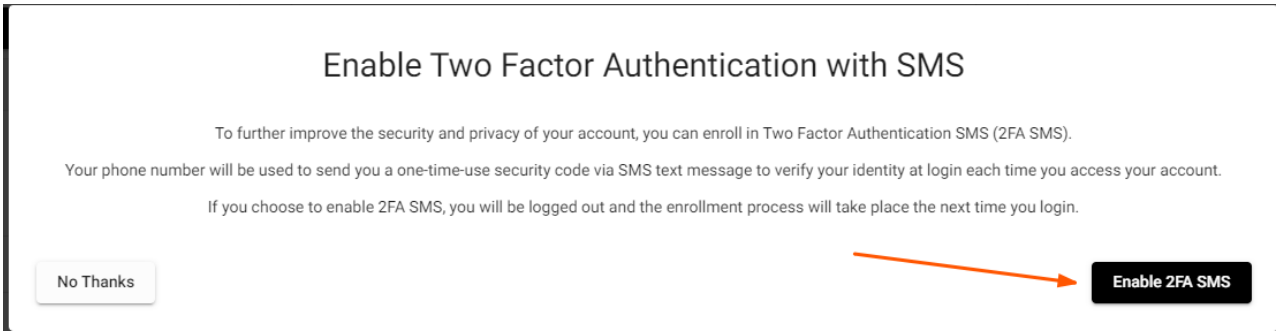


If the user selects "**Skip for Now**", this preference is remembered, and the client is directed straight to the main dashboard on subsequent attempts.

If the user decides to enroll with 2FA at a later time, this can be done by navigating to the top left 3-bar menu, and selecting "**Enable 2FA SMS**".



The user will have a dialog window to confirm their intentions, and will be ***logged out***, if enabled.

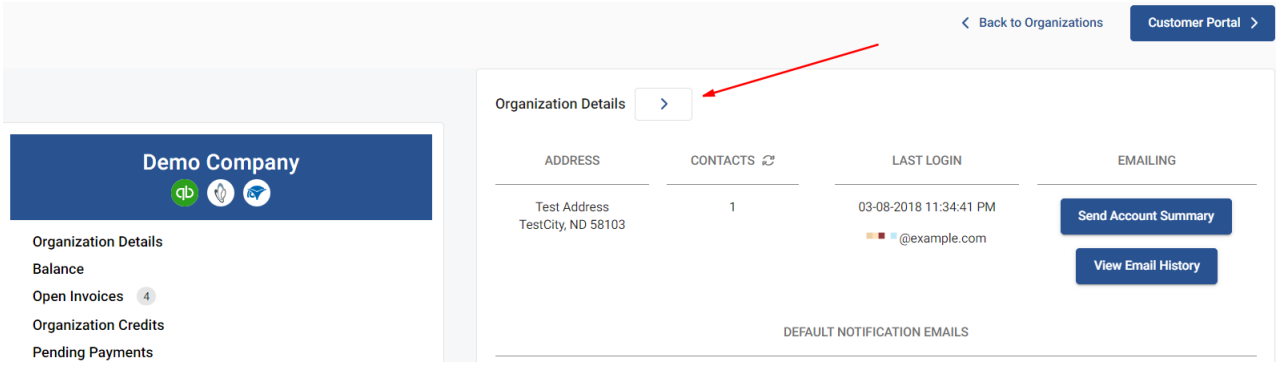


Troubleshooting

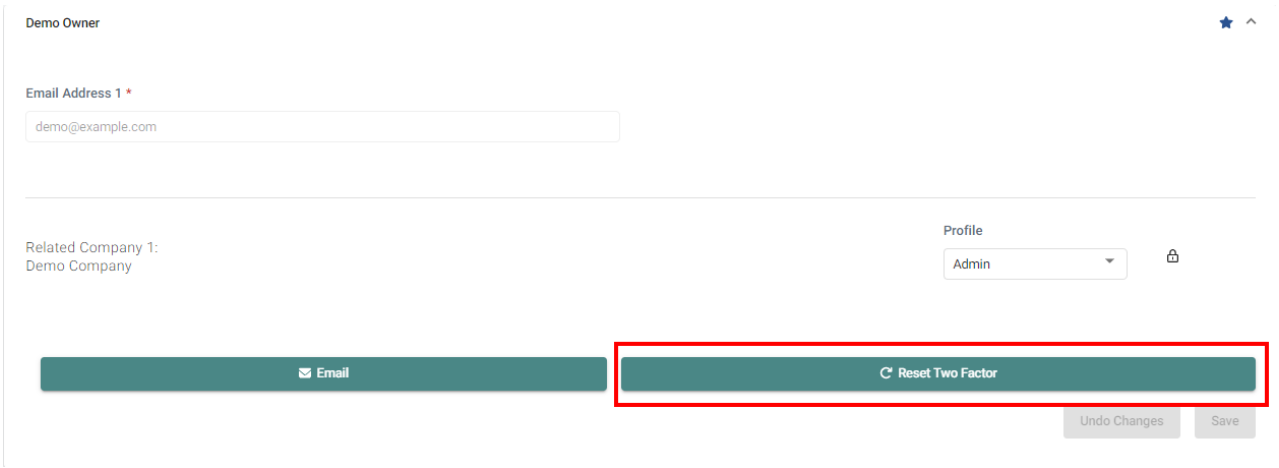
If your organization does not have access to or needs a different mobile phone number tied to the account, the "enrollment" process will need to be repeated.

Another Admin from your organization can do a "**RESET**" under the given organization's account. This **ONLY** does a reset for the account in question and does **NOT** force other organizations to "re-enroll".

On the company overview page, click on "Organization Details".



Find the contact in question, and expand for details. Select **"RESET TWO FACTOR".**



This completes the manual reset for an organization account.

Note: doing a "reset" also clears the saved "***Skip For Now***" preference on the contact.