

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

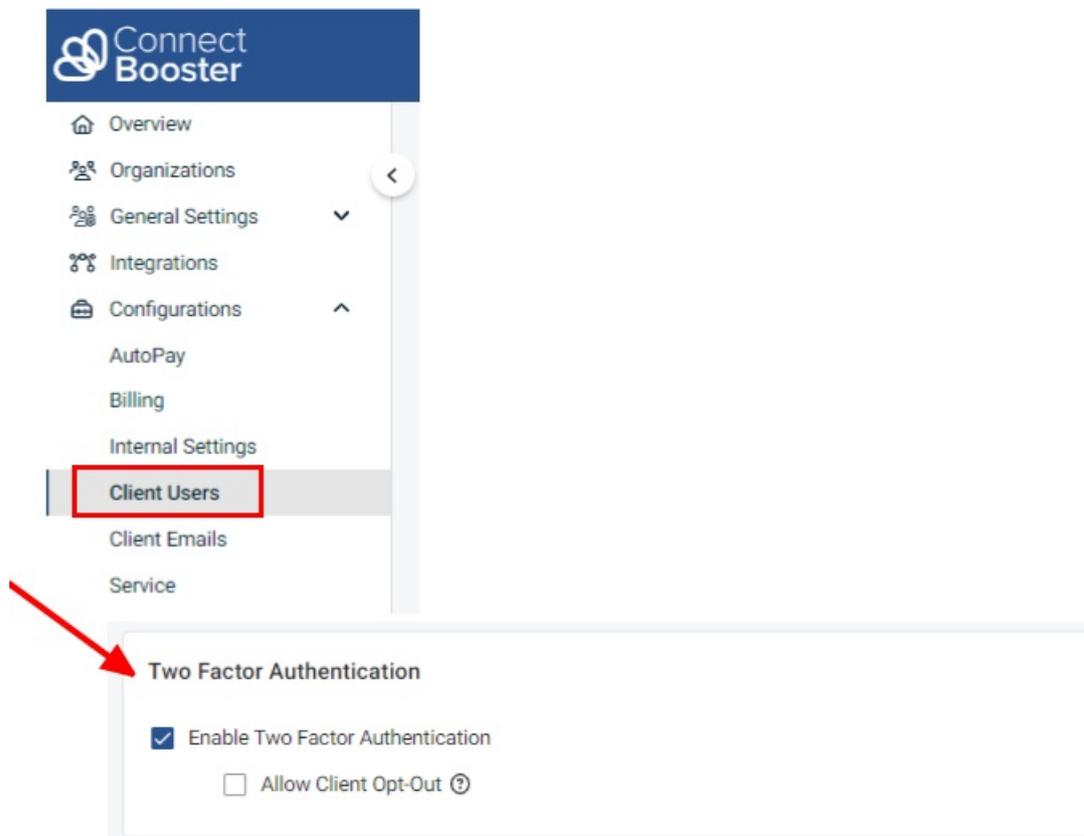
This function allows you to further secure your client's account login via one-time use, SMS text messages.

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

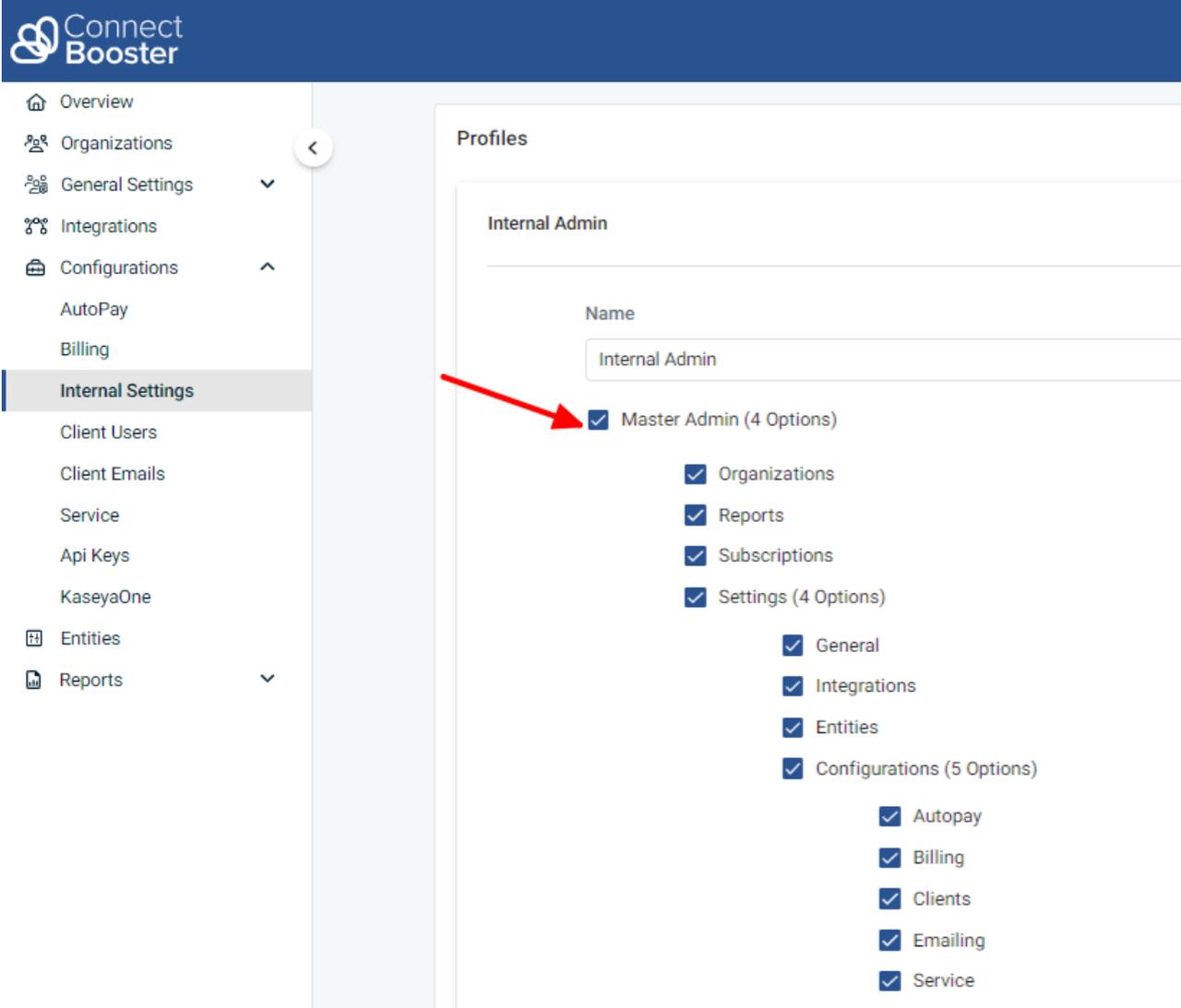
Our SMS based 2-Factor will send a text message code to the enrolled mobile phone number.

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.



The screenshot displays the 'Connect Booster' portal interface. On the left is a navigation sidebar with the following menu items: Overview, Organizations, General Settings (with a dropdown arrow), Integrations, Configurations (with an up arrow), AutoPay, Billing, Internal Settings (highlighted with a blue bar), Client Users, Client Emails, Service, Api Keys, KaseyaOne, Entities, and Reports (with a dropdown arrow). The main content area is titled 'Profiles' and shows a configuration for the 'Internal Admin' profile. A text input field labeled 'Name' contains the text 'Internal Admin'. Below this, a list of permissions is shown, all of which are checked with blue checkmarks. A red arrow points to the 'Master Admin (4 Options)' checkbox. The permissions listed are: Organizations, Reports, Subscriptions, Settings (4 Options) (which includes General, Integrations, Entities, and Configurations (5 Options) including Autopay, Billing, Clients, Emailing, and Service).

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**.

YOUR LOGO HERE

Enter Email *

Please enter valid email.

Enter Password *

Please enter password

[Sign In](#)

[Reset Login or Password](#)

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

YOUR LOGO HERE

To further improve the security and privacy of your account, please provide a phone number to receive your one-time-use security code via SMS text message.

This phone number will be used to verify your identity at login each time you access your account.

Phone Number

Send Authentication Code

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

YOUR LOGO HERE

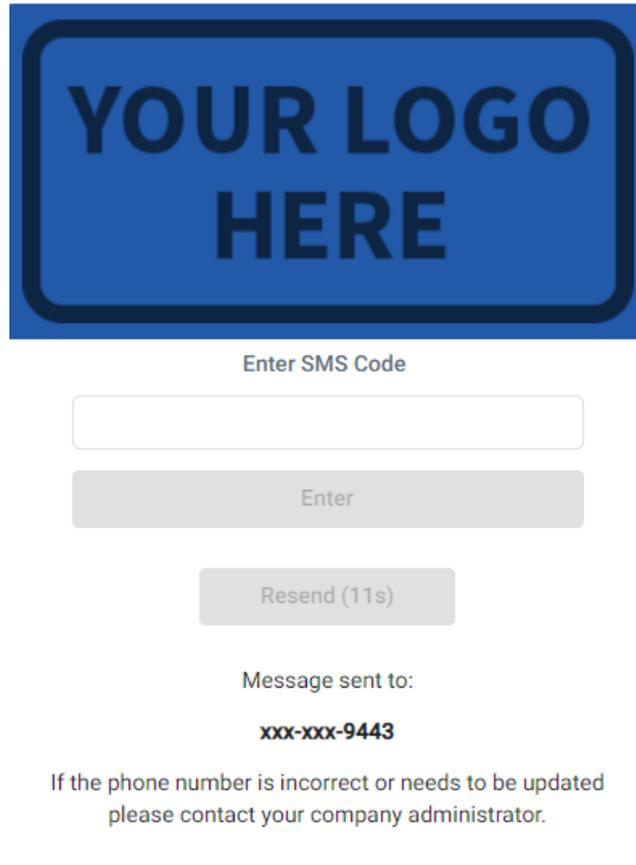
An authentication code has been sent to:

Please enter the code that was sent to your phone in the confirmation box below.

Verification Code

Verify Code

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



YOUR LOGO
HERE

Enter SMS Code

Enter

Resend (11s)

Message sent to:
xxx-xxx-9443

If the phone number is incorrect or needs to be updated
please contact your company administrator.

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.

Two Factor Authentication

Enable Two Factor Authentication

Allow Client Opt-Out ?

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

**YOUR LOGO
HERE**

To further improve the security and privacy of your account, please provide a phone number to receive your one-time-use security code via SMS text message.

This phone number will be used to verify your identity at login each time you access your account.

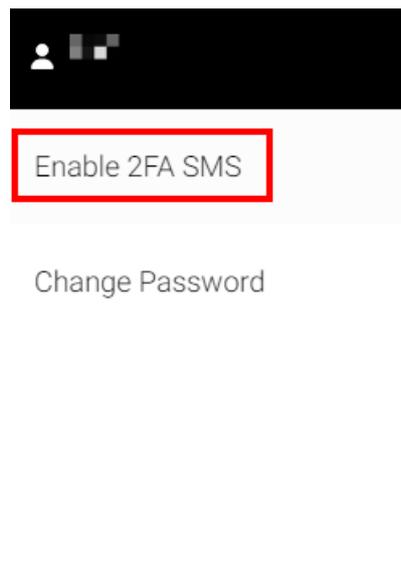
Phone Number

Send Authentication Code

Skip For Now

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.

Enable Two Factor Authentication with SMS

To further improve the security and privacy of your account, you can enroll in Two Factor Authentication SMS (2FA SMS).

Your phone number will be used to send you a one-time-use security code via SMS text message to verify your identity at login each time you access your account.

If you choose to enable 2FA SMS, you will be logged out and the enrollment process will take place the next time you login.

No Thanks

Enable 2FA SMS

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".

The screenshot shows the 'Demo Company' overview page. On the left is a sidebar with links: Organization Details, Balance, Open Invoices (4), Organization Credits, and Pending Payments. The main content area has a header with 'Back to Organizations' and 'Customer Portal'. Below is the 'Organization Details' section, which includes a table with columns: ADDRESS, CONTACTS, LAST LOGIN, and EMAILING. The table contains one row with the following data: ADDRESS: Test Address, TestCity, ND 58103; CONTACTS: 1; LAST LOGIN: 03-08-2018 11:34:41 PM, @example.com; EMAILING: Send Account Summary, View Email History. A red arrow points to the 'Organization Details' link above the table.

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

The screenshot shows the contact details for 'Demo Owner'. It includes fields for 'Email Address 1' (demo@example.com) and 'Related Company 1' (Demo Company). A 'Profile' dropdown menu is set to 'Admin'. At the bottom, there are two buttons: 'Email' and 'Reset Two Factor'. The 'Reset Two Factor' button is highlighted with a red box. Below these buttons are 'Undo Changes' and 'Save' buttons.

This completes the manual reset for an organization account.

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