



[Guide](#)

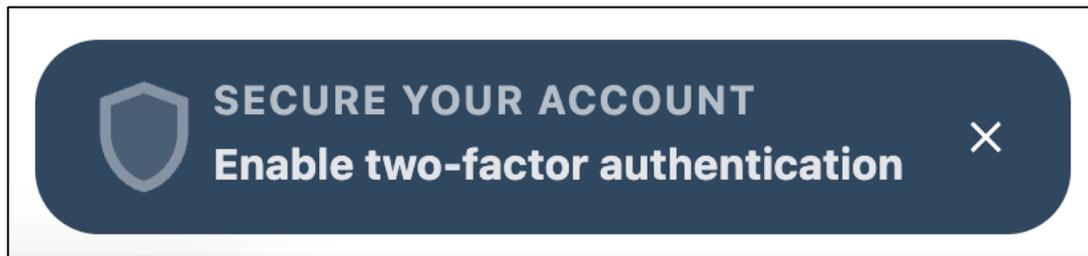
Two-Factor Authentication

Table of Contents

<i>What is two-factor authentication?</i>	<i>3</i>
<i>Here's an example of how 2FA works:</i>	<i>3</i>
<i>3 options of 2FA to select from at myCOI.....</i>	<i>3</i>
<i>2FA - Time-based OTP Instructions</i>	<i>4</i>
Twilio Authy Application	6
<i>2FA - SMS, Mobile Phone Instructions</i>	<i>8</i>
<i>2FA – Email Address</i>	<i>11</i>
<i>FAQ's.....</i>	<i>15</i>

What is two-factor authentication?

- Two-factor authentication (also known as **2FA**) is an extra layer of security that helps protect your accounts from unauthorized access.
- It does this by requiring you to provide two different pieces of evidence, or "factors," before you can log in.
- The first factor is something you know, like your password. The second factor is something you have, like your phone.



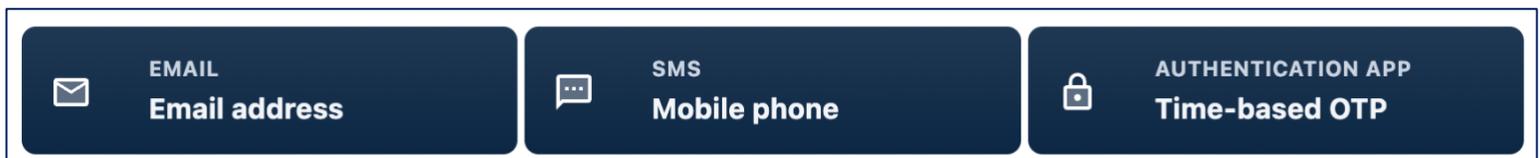
Here's an example of how 2FA works:

- You try to log in to your account.
- The system prompts you to enter your password.
- After you enter your password, the system sends a code to your phone via email, text, or an authenticator app.
- You enter the code to complete the login process.
- This extra step makes it much harder for someone to hack into your account.

3 options of 2FA to select from at myCOI

At myCOI users will have the options to select from three different two-factor authentication choices.

- **Email Address**
- **Mobile Phone**
- **Time-based OTP**

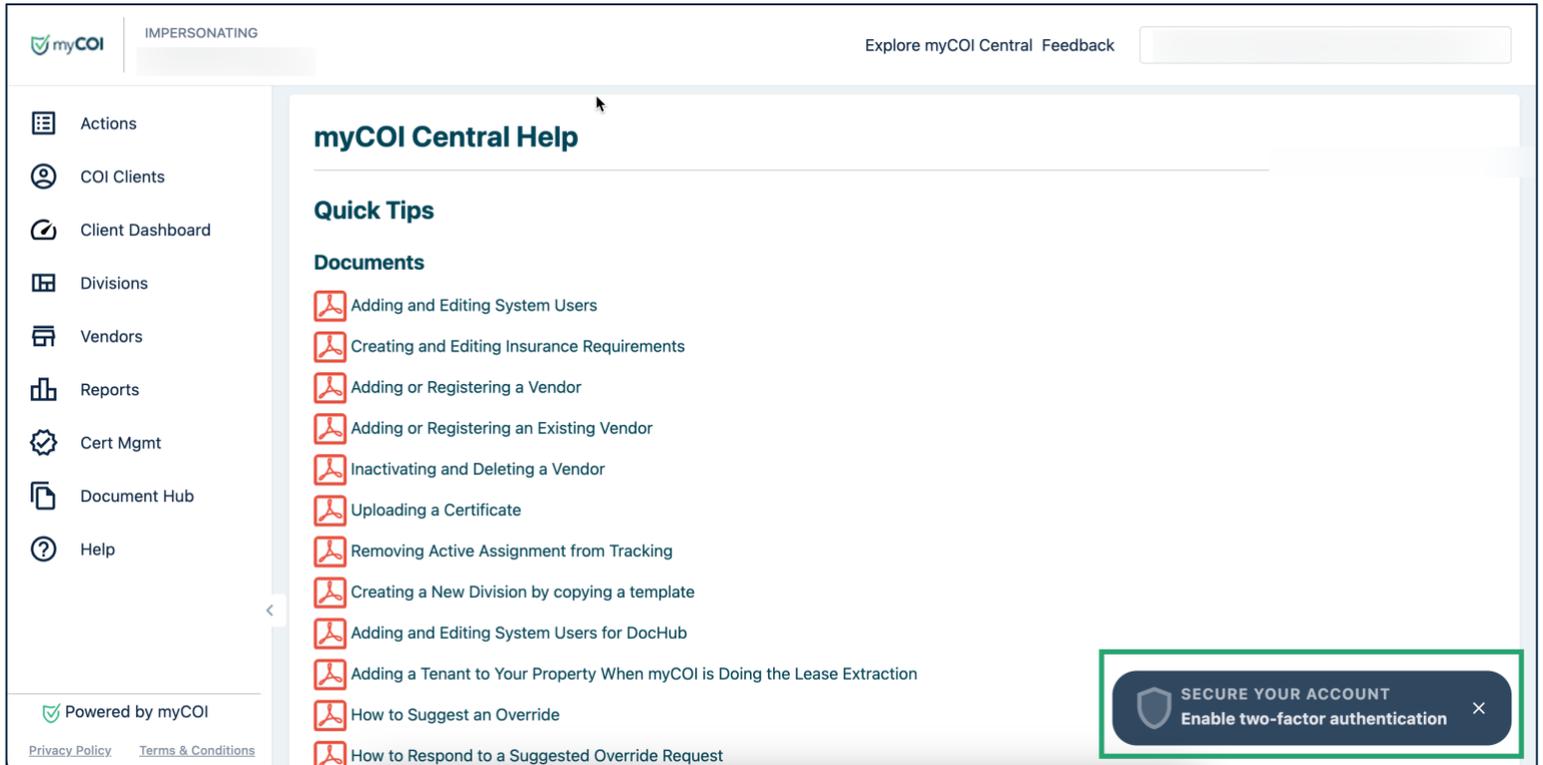


2FA - Time-based OTP Instructions

To setup two-factor authentication using Time-Based OTP option, follow the direction below:

Step#1:

Select the **Secure Your Account, Enable two-factor authentication** on the bottom right.



Step#2:

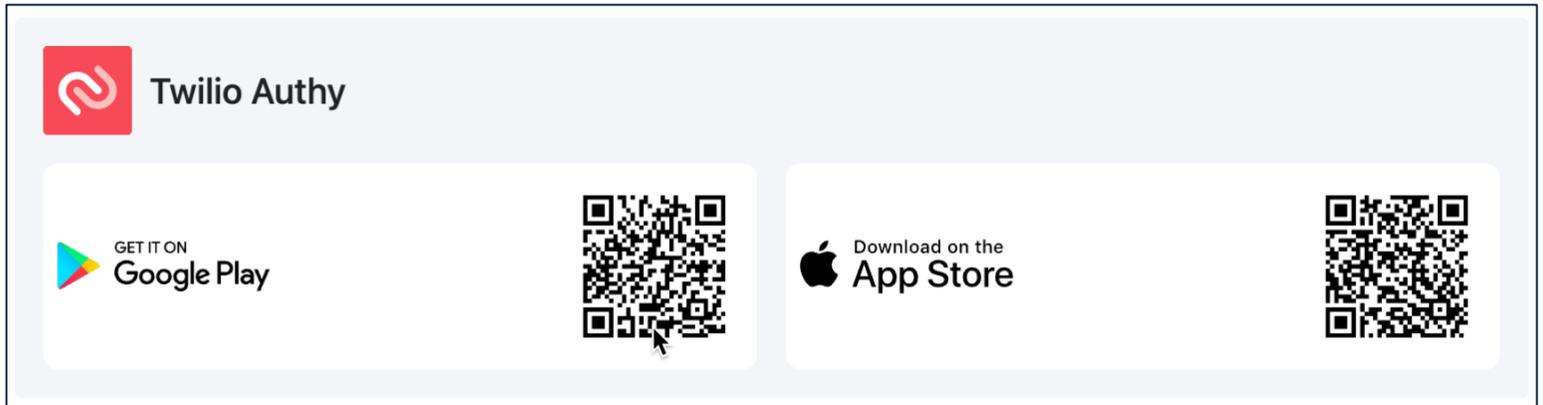
Select **Time-based OTP**

To begin, select one of the following factors:



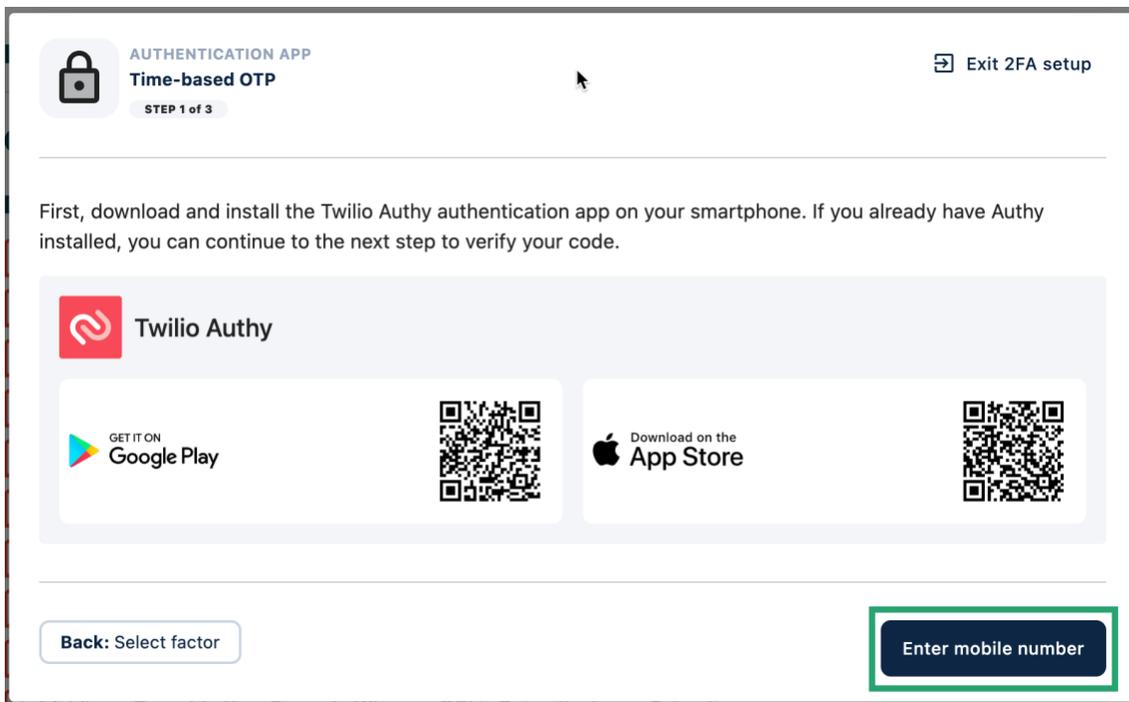
Step#3:

Users will need to download the Twilio Authy application. The application is available on both Google Play and Apple's App store.



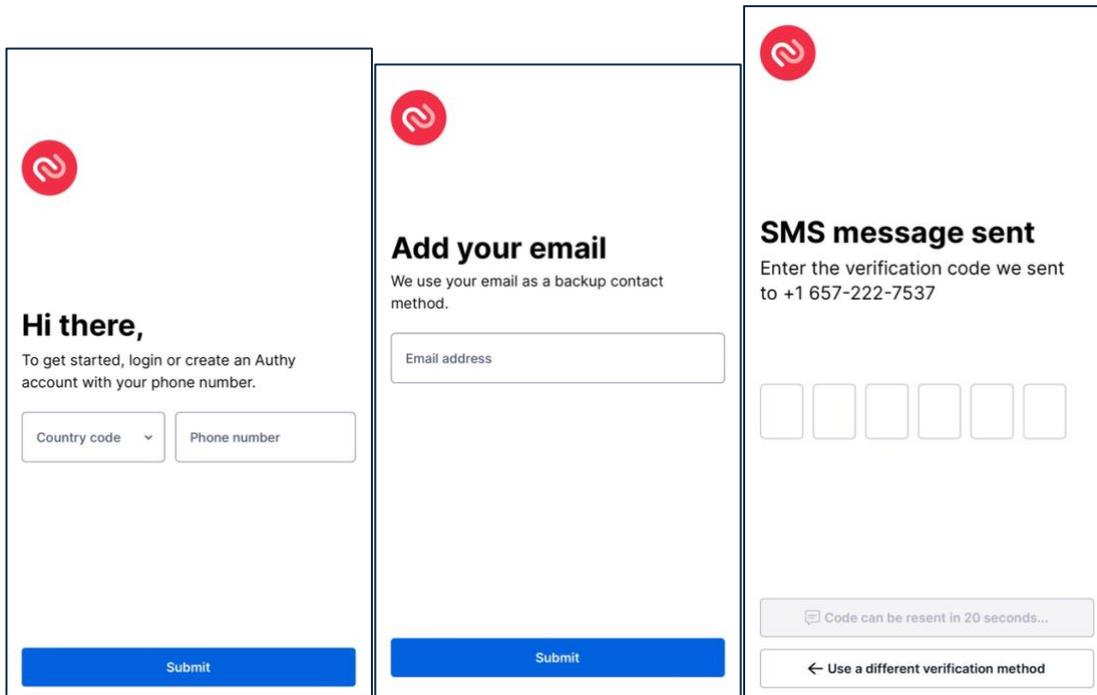
Step#4:

Once the Twilio Authy application have been downloaded, proceed to **Enter mobile number**.



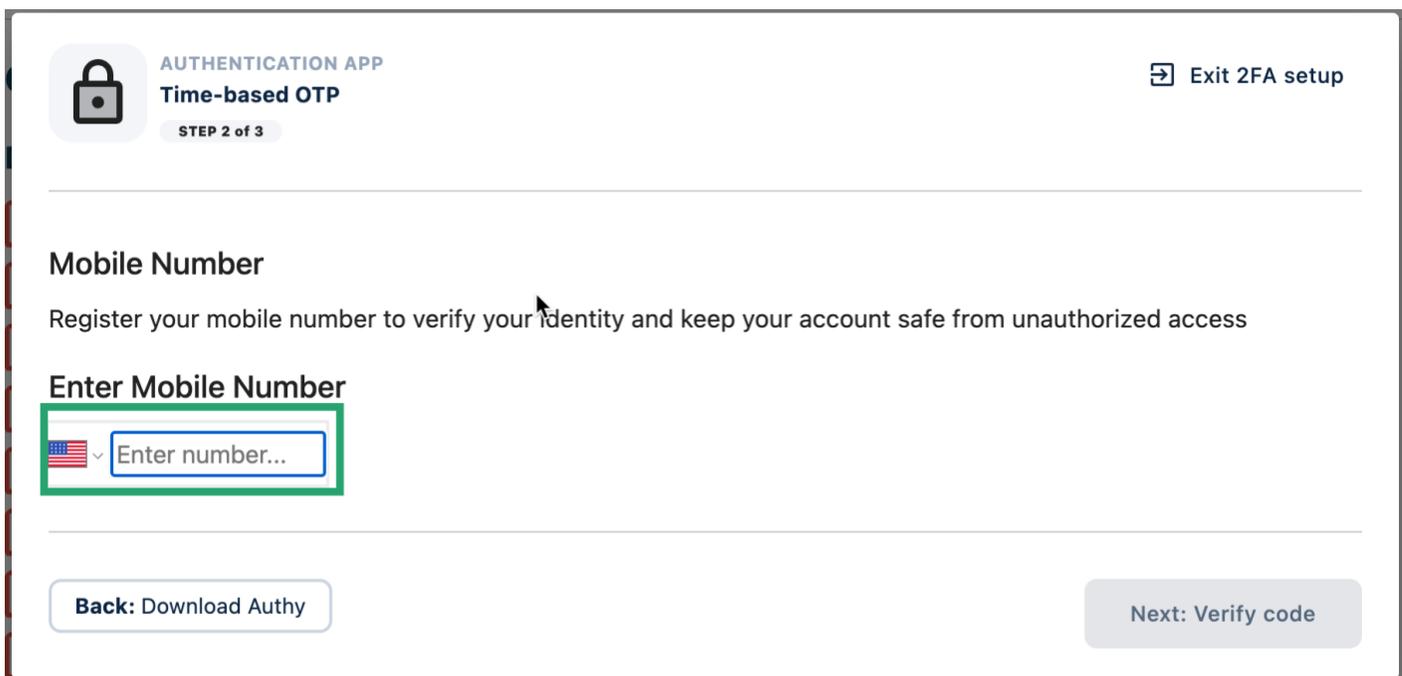
Twilio Authy Application

Quick Twilio Authy Application set up process. Follow the steps on the screen below:



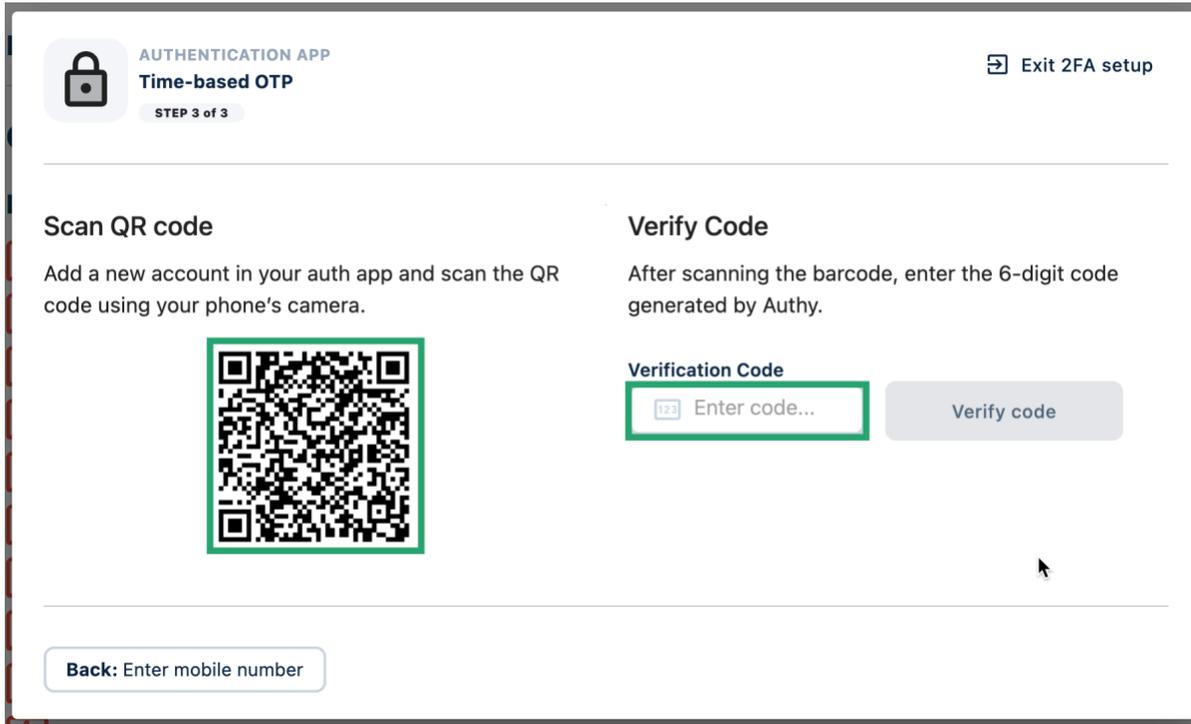
Step#5:

Enter the mobile number that will be used for two-factor authentication.



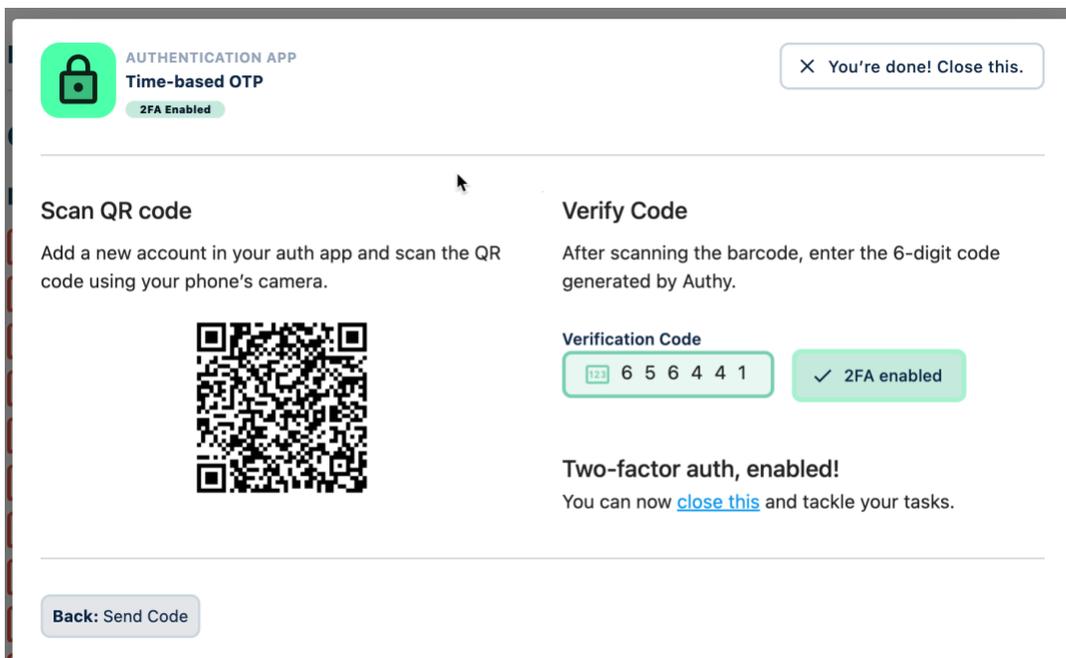
Step#6:

Users can either **scan the QR code** or **enter the 6-digit code** generated by Authy.



Step#7:

Once the user has entered the verification code, the window will update and two-factor authentication using **Time-Based OTP have been activated.**

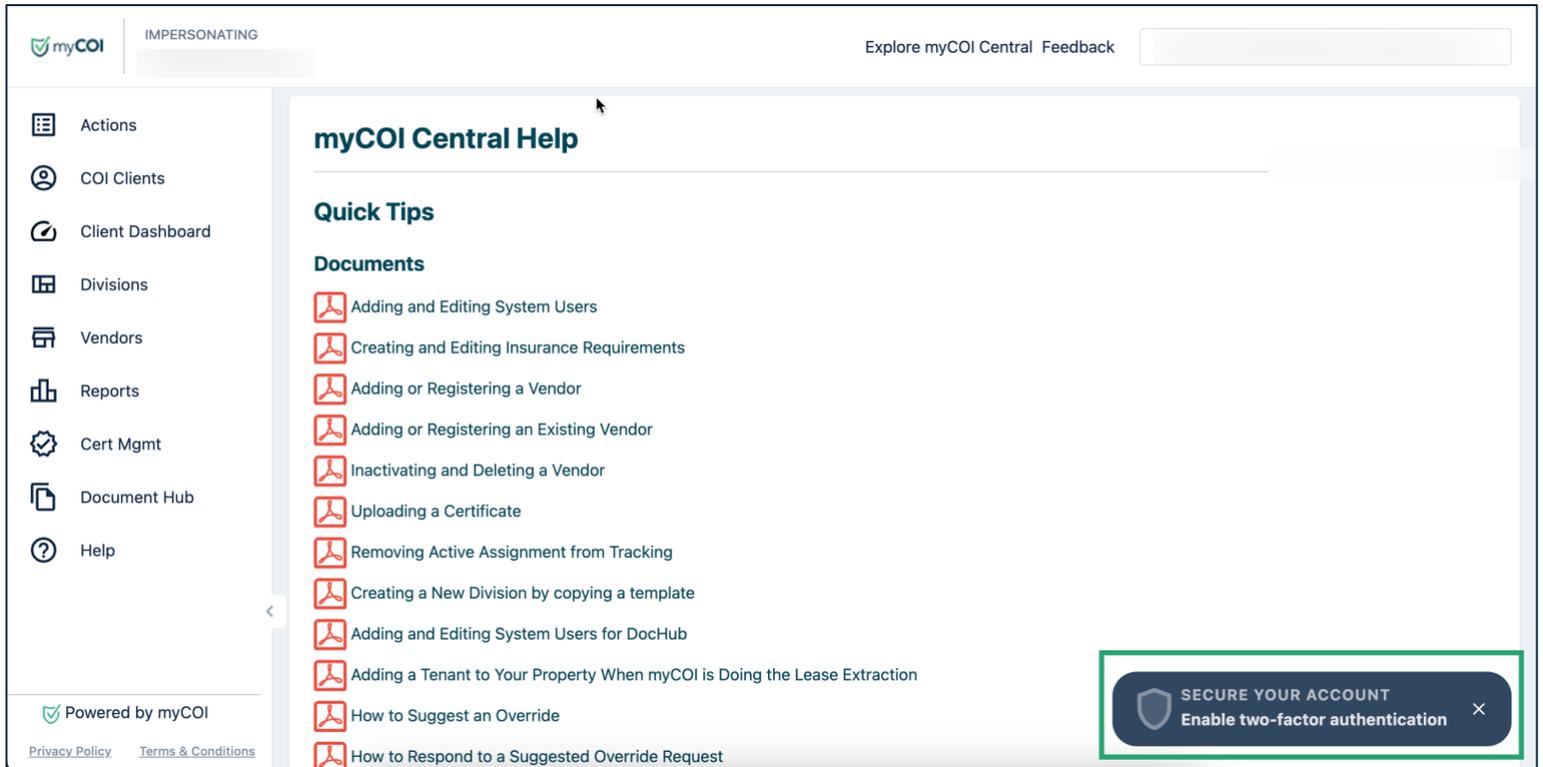


2FA - SMS, Mobile Phone Instructions

To setup two-factor authentication using SMS, Mobile Phone option, follow the direction below:

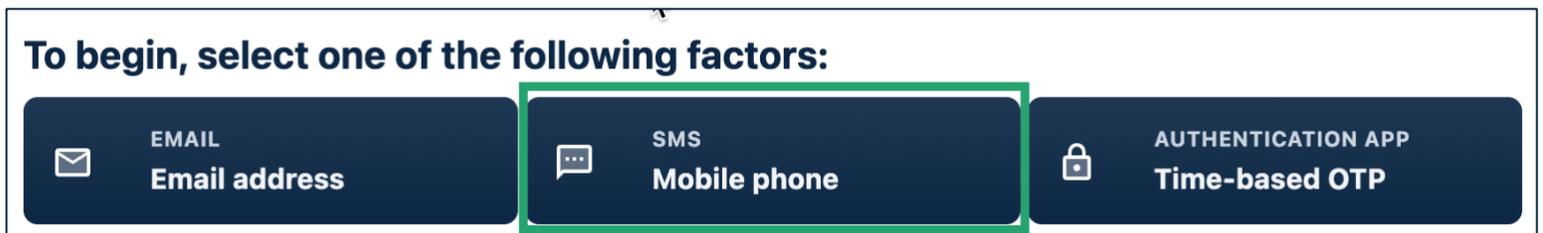
Step#1:

Select the **Secure Your Account, Enable two-factor authentication** on the bottom right.



Step#2:

Select **SMS, Mobile Phone**



Step#3:

Enter the **mobile phone number** that the two-factor authenticator code will be sent to and click Send code.

SMS
Mobile phone two-factor authentication
STEP 1 of 2

Exit 2FA setup

Enter a mobile number. We'll send a verification code.

Mobile Number

Enter number... Send code

Back: Select factor

Step#4:

Select **Enter Code**

SMS
Mobile phone two-factor authentication
STEP 1 of 2

Exit 2FA setup

Enter a mobile number. We'll send a verification code. You've requested 1 of 3 allotted codes.

Mobile Number

Code sent Send new code in 24

Back: Select factor

Next: Enter code

Step#5:

Select **Verify and Enable 2FA**

The screenshot shows a mobile interface for setting up two-factor authentication. At the top left, there is a speech bubble icon with three dots, followed by the text 'SMS' and 'Mobile phone two-factor authentication'. Below this, it says 'STEP 2 of 2'. At the top right, there is a link that says 'Exit 2FA setup'. The main content area contains the instruction: 'Enter the 6 digit code sent to [redacted] You've requested 1 of 3 allotted codes.' Below this is a 'Verification Code' input field containing '123'. To the right of the input field is a dark blue button with white text that says 'Verify and enable 2FA', which is highlighted with a green border. To the right of the button is the text 'Send new code in 4'. At the bottom left, there is a button that says 'Back: Enter mobile number'.

Step#6:

Once the user has entered the verification code, the window will update and two-factor authentication using **SMS, Mobile Phone have been activated.**

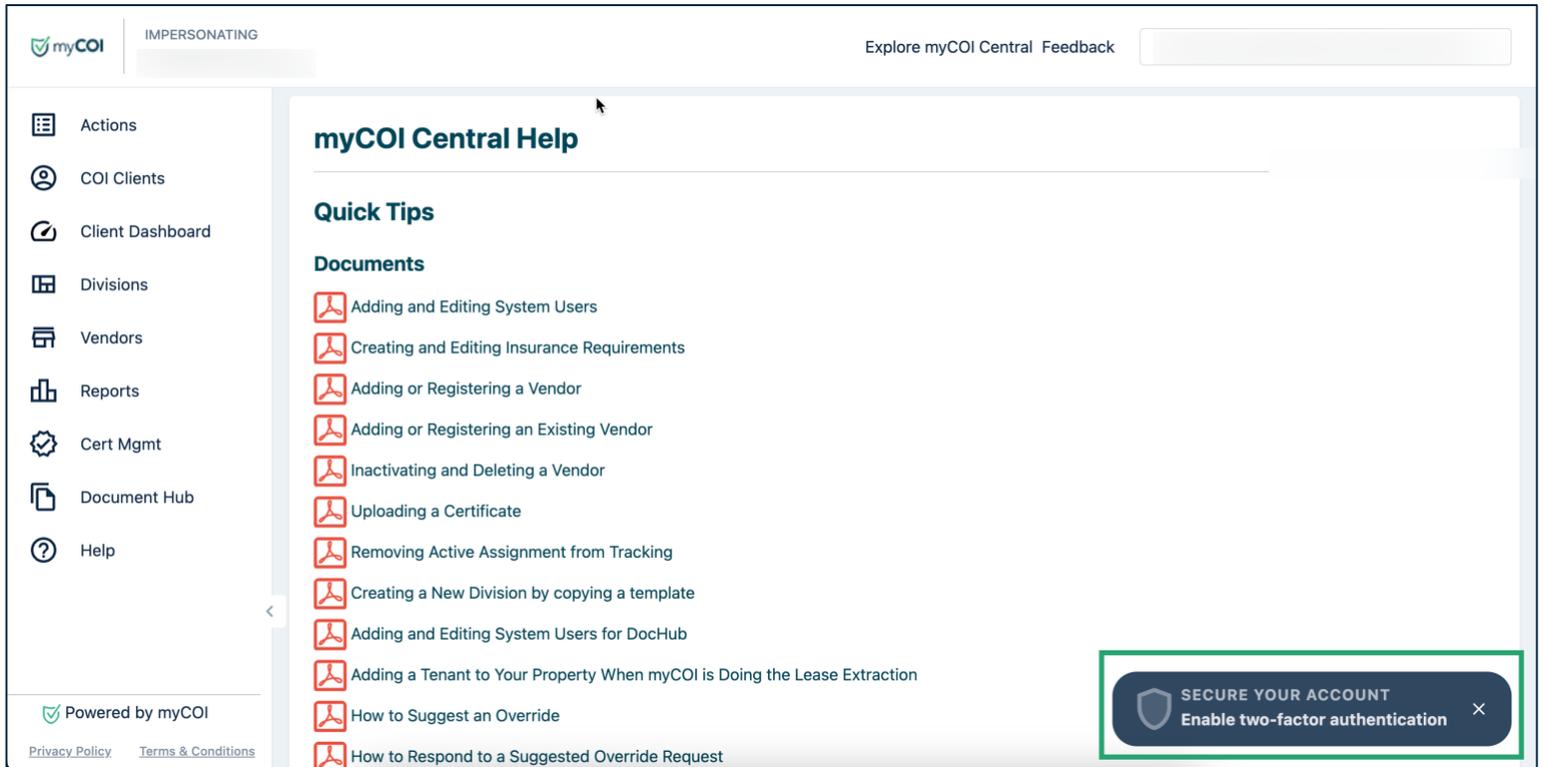
The screenshot shows the success screen for two-factor authentication. At the top left, there is a green speech bubble icon with three dots, followed by the text 'SMS' and 'Mobile phone two-factor authentication'. Below this, it says '2FA Enabled'. At the top right, there is a button that says 'X You're done! Close this.'. The main content area contains the message: 'Two-factor auth, success! You can now [close this](#) and tackle your tasks.' Below this is a 'Verification Code' input field containing '123'. To the right of the input field is a green button with white text that says '✓ 2FA enabled'. At the bottom left, there is a button that says 'Back: Send Code'.

2FA - Email Address

To setup two-factor authentication using Email Address option, follow the direction below:

Step#1:

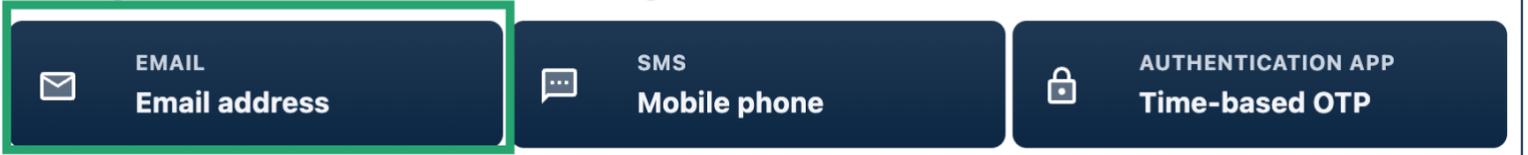
Select the **Secure Your Account, Enable two-factor authentication** on the bottom right.



Step#2:

Select **SMS, Mobile Phone**

To begin, select one of the following factors:



Step#3:

Select **Send code**, after entering email address.

The screenshot shows the 'EMAIL' section of the 'Email two-factor authentication' setup. It is labeled 'STEP 1 of 2'. At the top right, there is a link to 'Exit 2FA setup'. The main text states: 'Verification code will be sent to your account's email.' Below this, there is an 'Email Address' input field. To the right of the input field is a dark blue button labeled 'Send code', which is highlighted with a green border. At the bottom left, there is a button labeled 'Back: Select factor'.

Step#4:

Select **Enter code**

The screenshot shows the same 'EMAIL' section of the 'Email two-factor authentication' setup. It is labeled 'STEP 1 of 2'. At the top right, there is a link to 'Exit 2FA setup'. The main text states: 'Verification code will be sent to your account's email. You've requested 1 of 3 allotted codes.' Below this, there is an 'Email Address' input field. To the right of the input field is a green button labeled '✓ Code sent', which is highlighted with a green border. To the right of this button, the text 'Send new code in 28' is visible. At the bottom left, there is a button labeled 'Back: Select factor'. At the bottom right, there is a dark blue button labeled 'Next: Enter code', which is highlighted with a green border.

Step#5:

User will receive an email with the verification code.

TWO-FACTOR AUTH

Here's your code



Hello myCOI user,

We received a request to authenticate your account. To confirm this was you, we've generated a unique two-factor authentication (2FA) code.

Your myCOI (Dev) verification code is:

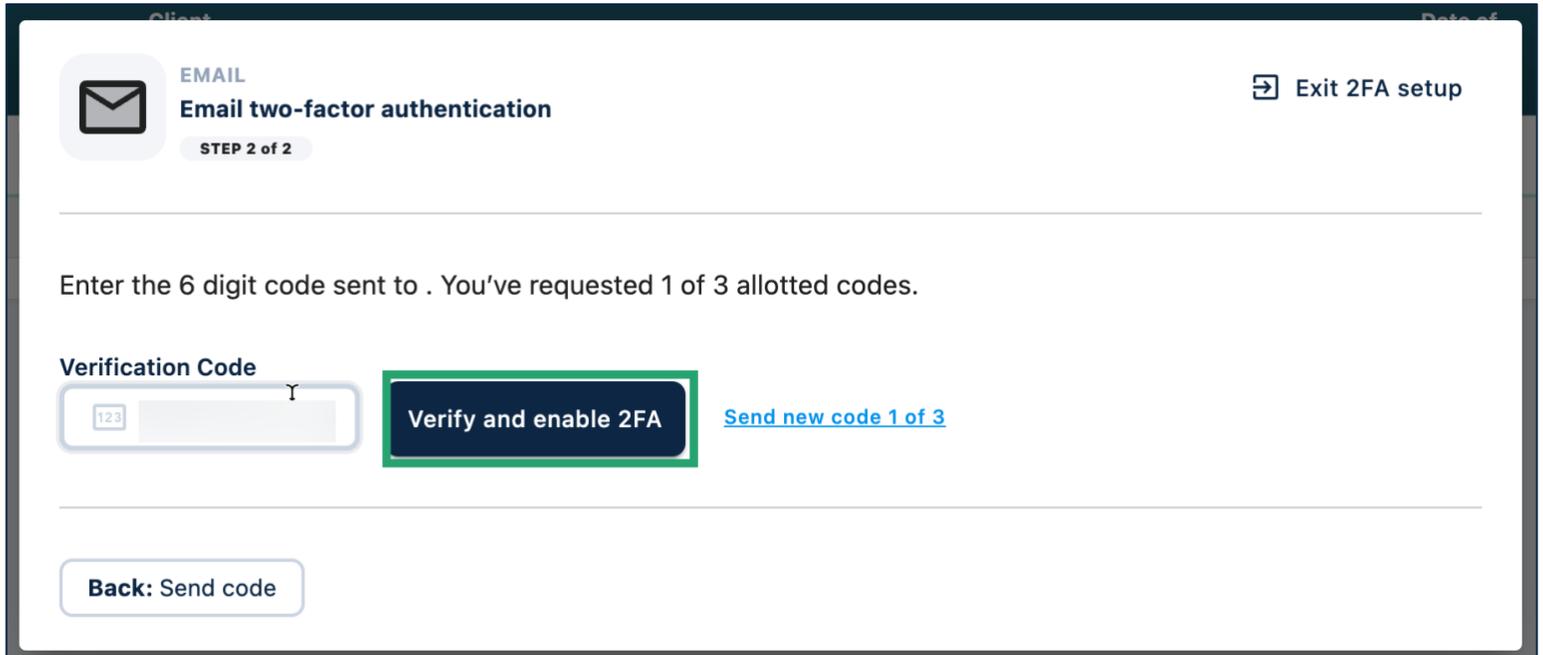
Please note that this code will expire within 5 minutes from the time it was generated.

If you did not request this code, someone else may be trying to access your account. We recommend changing your password immediately and contacting our support team for further assistance.

Remember, we will never ask you to share your 2FA code or password via email or phone.

Step#6:

Enter the verification code and select **Verify and enable 2FA**.



Client: _____ Date of: _____

 EMAIL
Email two-factor authentication
STEP 2 of 2

[Exit 2FA setup](#)

Enter the 6 digit code sent to . You've requested 1 of 3 allotted codes.

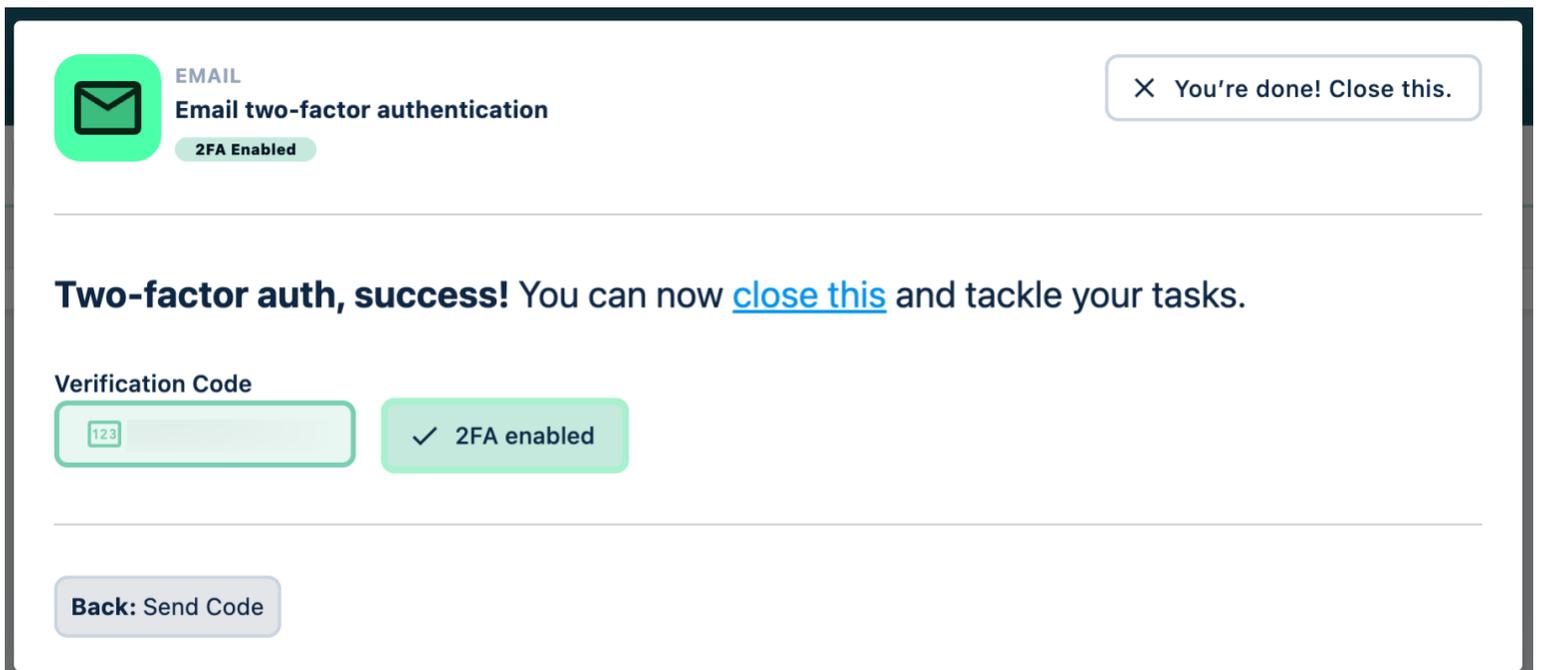
Verification Code

Verify and enable 2FA [Send new code 1 of 3](#)

[Back: Send code](#)

Step#7:

Once the user has entered the verification code, the window will update and two-factor authentication using **Email have been activated**.



 EMAIL
Email two-factor authentication
2FA Enabled

[X You're done! Close this.](#)

Two-factor auth, success! You can now [close this](#) and tackle your tasks.

Verification Code

✓ 2FA enabled

[Back: Send Code](#)

FAQ's

What is Two-Factor Authentication?

Two-factor authentication (also known as **2FA**) is an extra layer of security that helps protect your accounts from unauthorized access. It does this by requiring you to provide two different pieces of evidence, or "factors," before you can log in. The first factor is something you know, like your password. The second factor is something you have, like your phone.

How does Two-Factor Authentication work?

You try to log in to your account. The system prompts you to enter your password. After you enter your password, the system sends a code to your phone via email, text, or an authenticator app. You enter the code to complete the login process.