



**Guide**

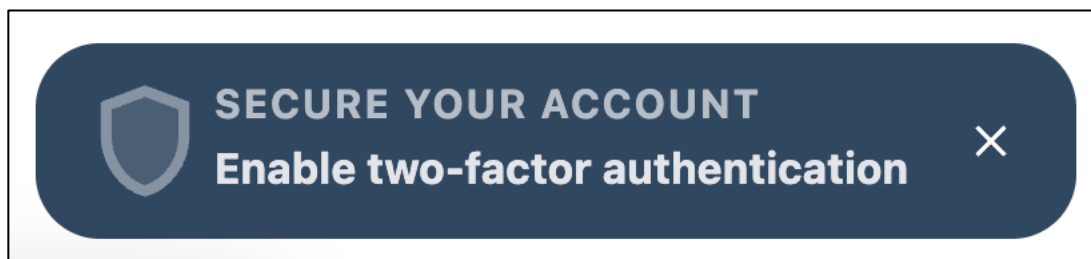
# **Two-Factor Authentication**

## 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>
<b>Twilio Authy Application .....</b>	<b>6</b>
<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.



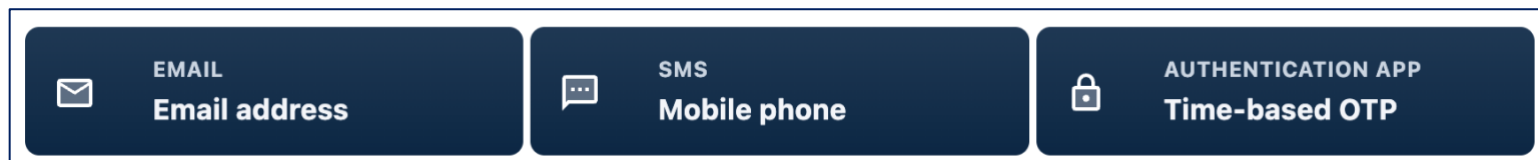
## Here's an example of how 2FA works:

- 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**

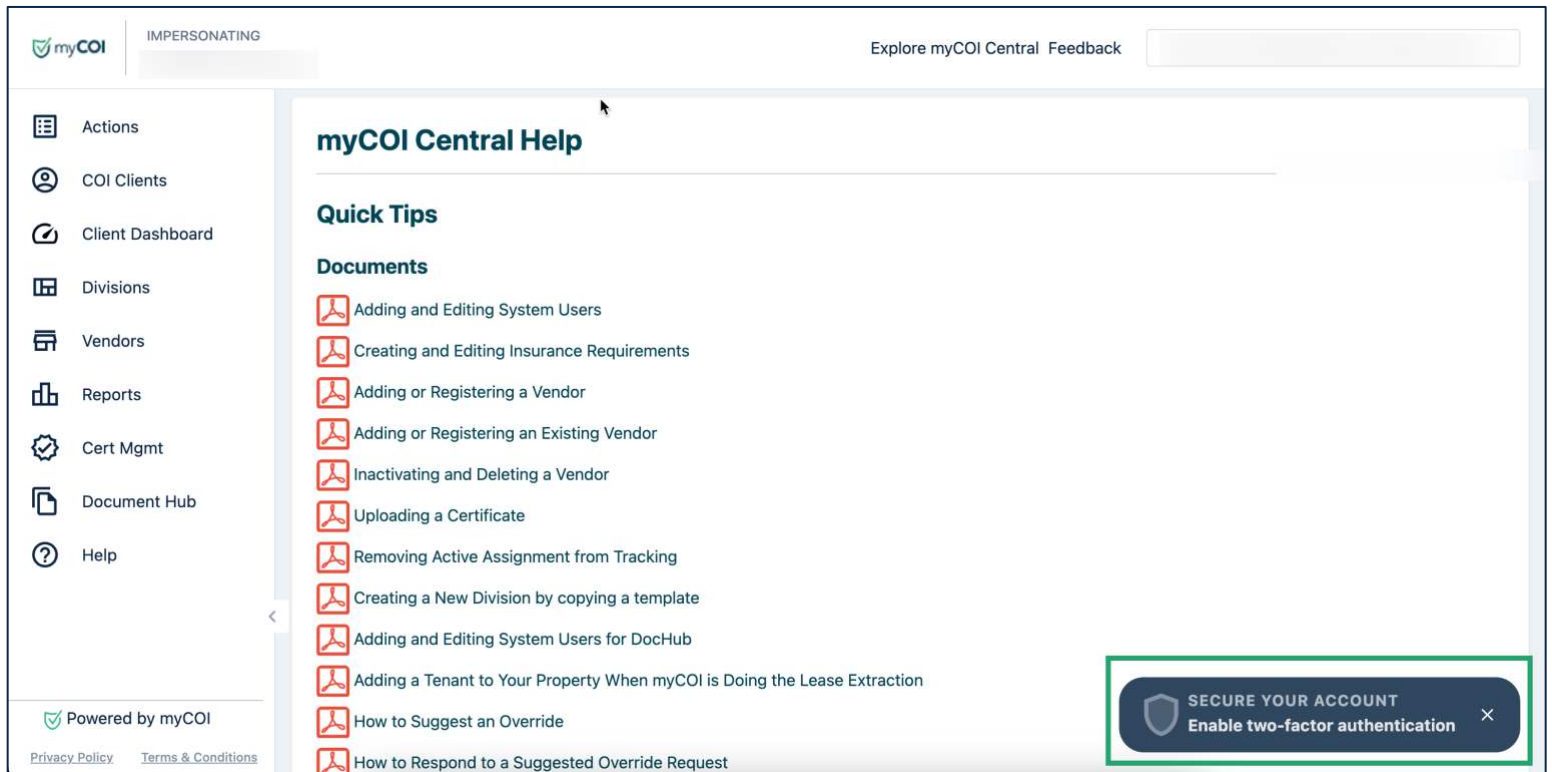


## 2FA - Time-based OTP Instructions

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.



myCOI Central Help

Quick Tips

Documents

- Adding and Editing System Users
- Creating and Editing Insurance Requirements
- Adding or Registering a Vendor
- Adding or Registering an Existing Vendor
- Inactivating and Deleting a Vendor
- Uploading a Certificate
- Removing Active Assignment from Tracking
- Creating a New Division by copying a template
- Adding and Editing System Users for DocHub
- Adding a Tenant to Your Property When myCOI is Doing the Lease Extraction
- How to Suggest an Override
- How to Respond to a Suggested Override Request

SECURE YOUR ACCOUNT  
Enable two-factor authentication

### Step#2:

Select **Time-based OTP**

To begin, select one of the following factors:



EMAIL  
Email address



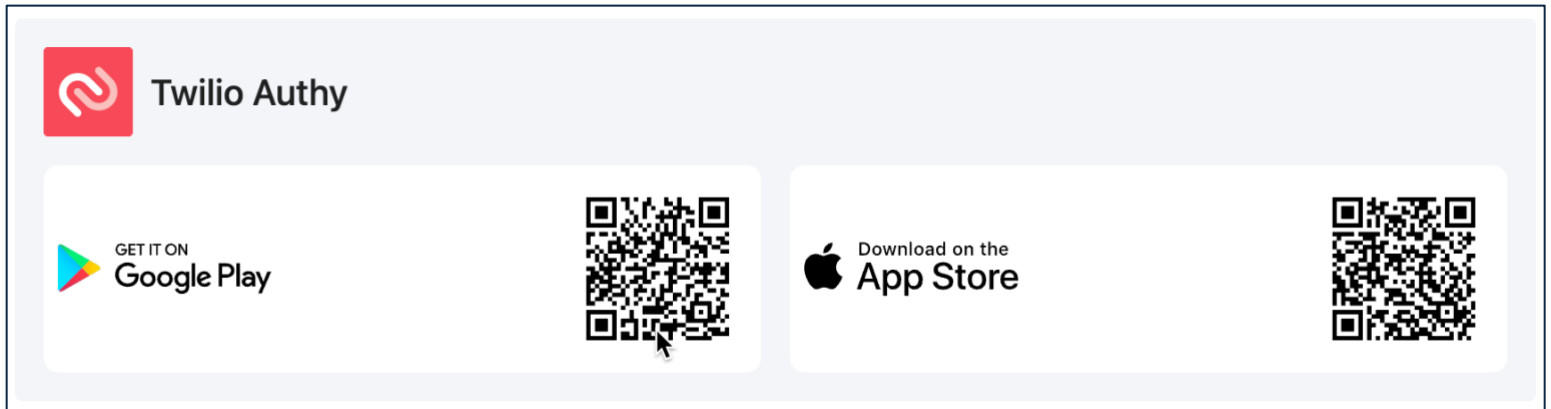
SMS  
Mobile phone



AUTHENTICATION APP  
Time-based OTP

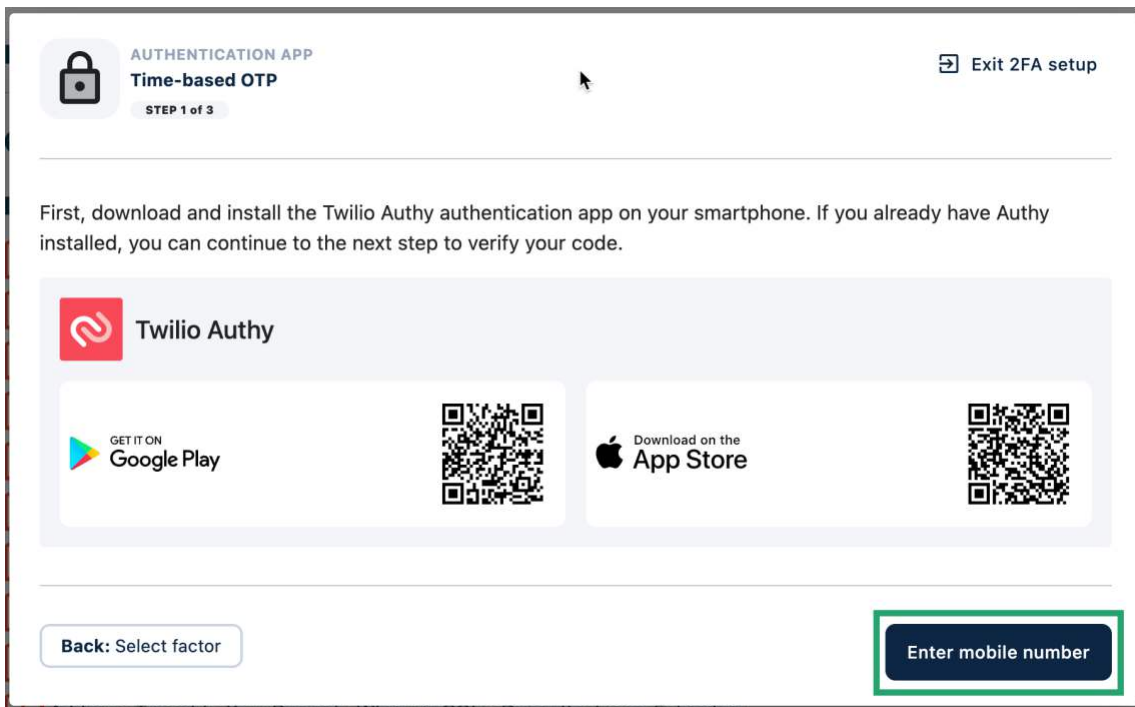
### Step#3:

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



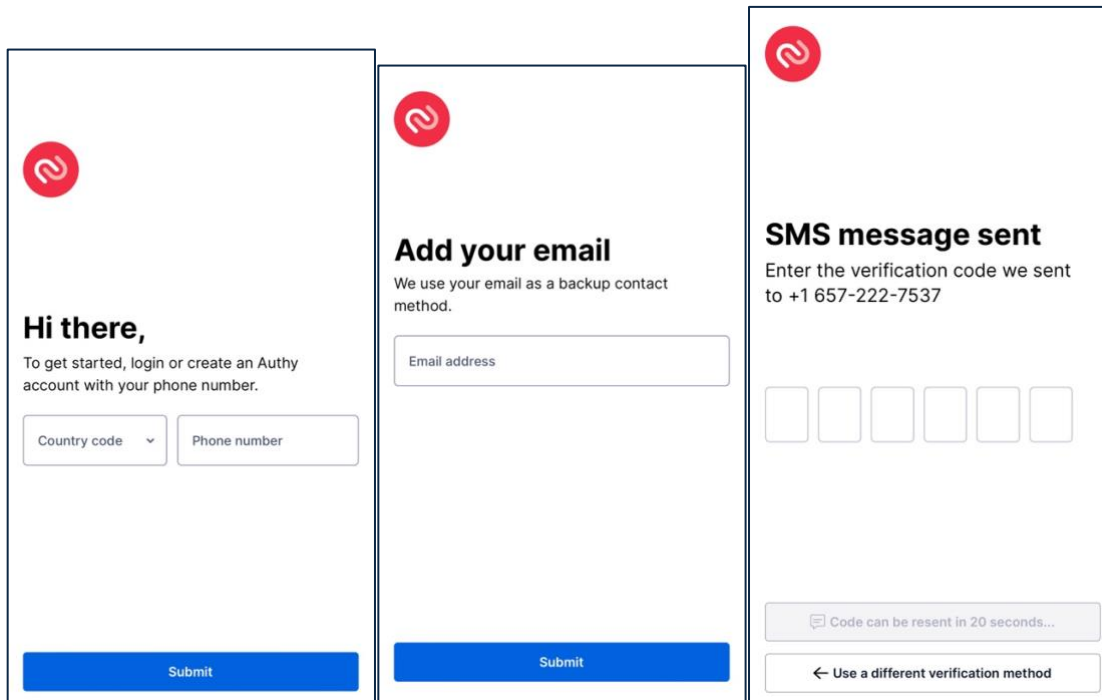
### Step#4:

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:



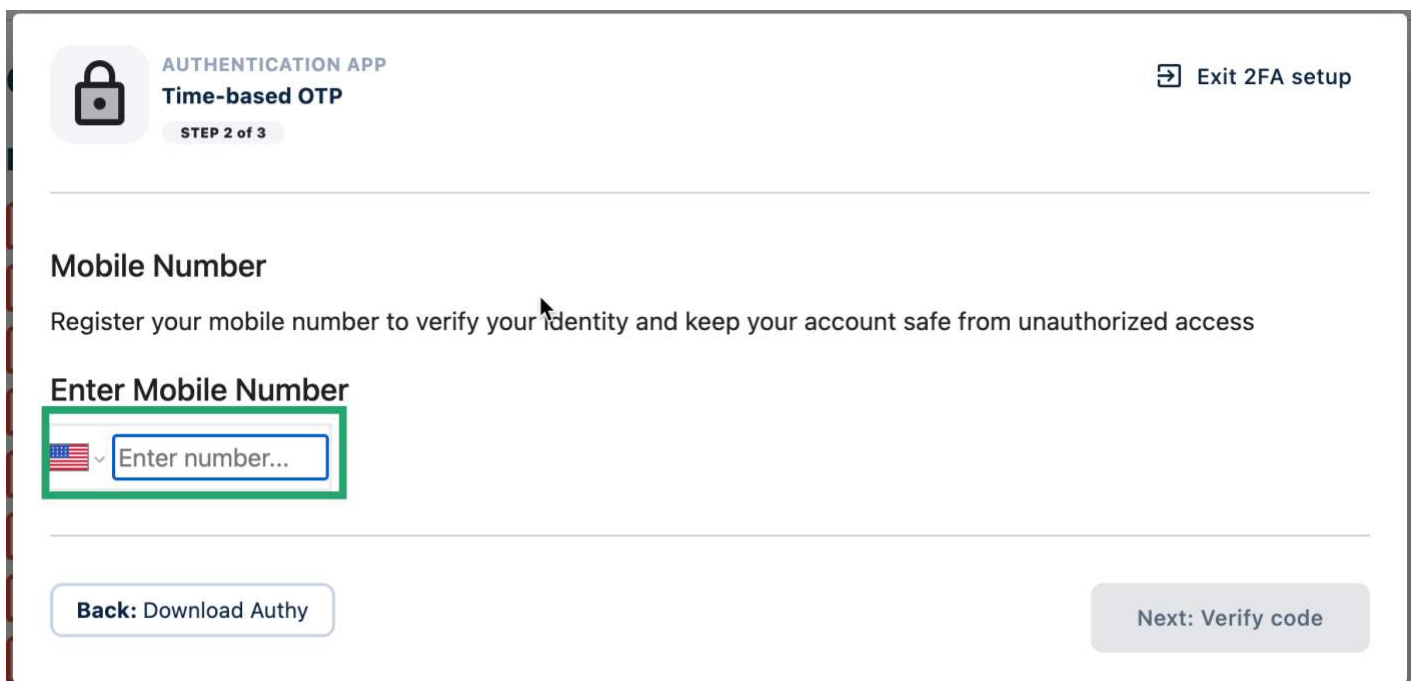
The first screenshot shows a welcome screen with the Twilio logo and the text "Hi there, To get started, login or create an Authy account with your phone number." It includes input fields for "Country code" and "Phone number" and a "Submit" button.

The second screenshot shows the "Add your email" screen with the Twilio logo and the text "Add your email We use your email as a backup contact method." It includes an "Email address" input field and a "Submit" button.

The third screenshot shows the "SMS message sent" screen with the Twilio logo and the text "SMS message sent Enter the verification code we sent to +1 657-222-7537". It includes a six-digit verification code input field, a "Code can be resent in 20 seconds..." message, and a "Use a different verification method" button.

### Step#5:


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



The screenshot shows the "AUTHENTICATION APP Time-based OTP" screen, labeled "STEP 2 of 3". It includes a "Back: Download Authy" button and a "Next: Verify code" button. The main content area is titled "Mobile Number" and contains the text "Register your mobile number to verify your identity and keep your account safe from unauthorized access". Below this is the "Enter Mobile Number" section, which includes a country code selector (currently showing the US flag) and an "Enter number..." input field. The input field is highlighted with a green border.

## Step#6:

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




AUTHENTICATION APP  
Time-based OTP  
STEP 3 of 3

Exit 2FA setup

### Scan QR code

Add a new account in your auth app and scan the QR code using your phone's camera.



### Verify Code

After scanning the barcode, enter the 6-digit code generated by Authy.


Verification Code

Verify code

Back: Enter mobile number

## 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.**




AUTHENTICATION APP  
Time-based OTP  
2FA Enabled

You're done! Close this.

### Scan QR code

Add a new account in your auth app and scan the QR code using your phone's camera.



### Verify Code

After scanning the barcode, enter the 6-digit code generated by Authy.

Verification Code

✓ 2FA enabled

### Two-factor auth, enabled!

You can now [close this](#) and tackle your tasks.

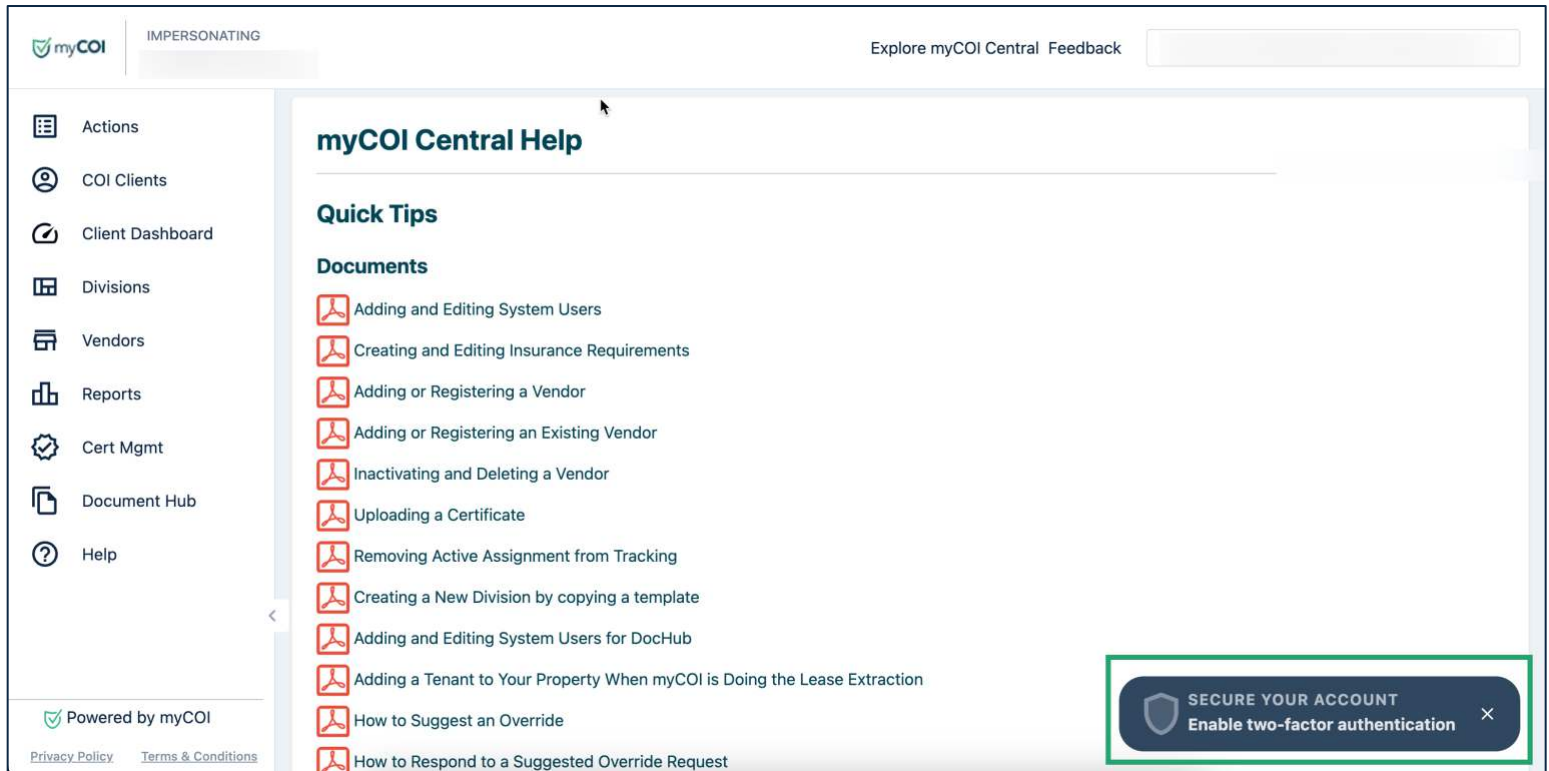
Back: Send Code

# 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.



myCOI Central Help

**Quick Tips**

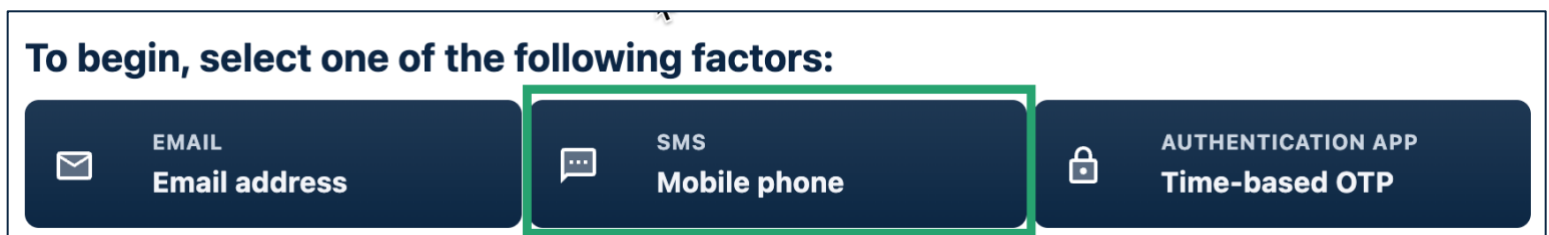
**Documents**

- Adding and Editing System Users
- Creating and Editing Insurance Requirements
- Adding or Registering a Vendor
- Adding or Registering an Existing Vendor
- Inactivating and Deleting a Vendor
- Uploading a Certificate
- Removing Active Assignment from Tracking
- Creating a New Division by copying a template
- Adding and Editing System Users for DocHub
- Adding a Tenant to Your Property When myCOI is Doing the Lease Extraction
- How to Suggest an Override
- How to Respond to a Suggested Override Request

**SECURE YOUR ACCOUNT**  
Enable two-factor authentication

## Step#2:

Select **SMS, Mobile Phone**



**To begin, select one of the following factors:**

**EMAIL**  
Email address


**SMS**  
Mobile phone

**AUTHENTICATION APP**  
Time-based OTP



### 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




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**



SMS

Mobile phone 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

123

Verify and enable 2FA


Send new code in 4

---

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.**



SMS

Mobile phone two-factor authentication

2FA Enabled

You're done! Close this.

---

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

Verification Code

123

✓ 2FA enabled

---

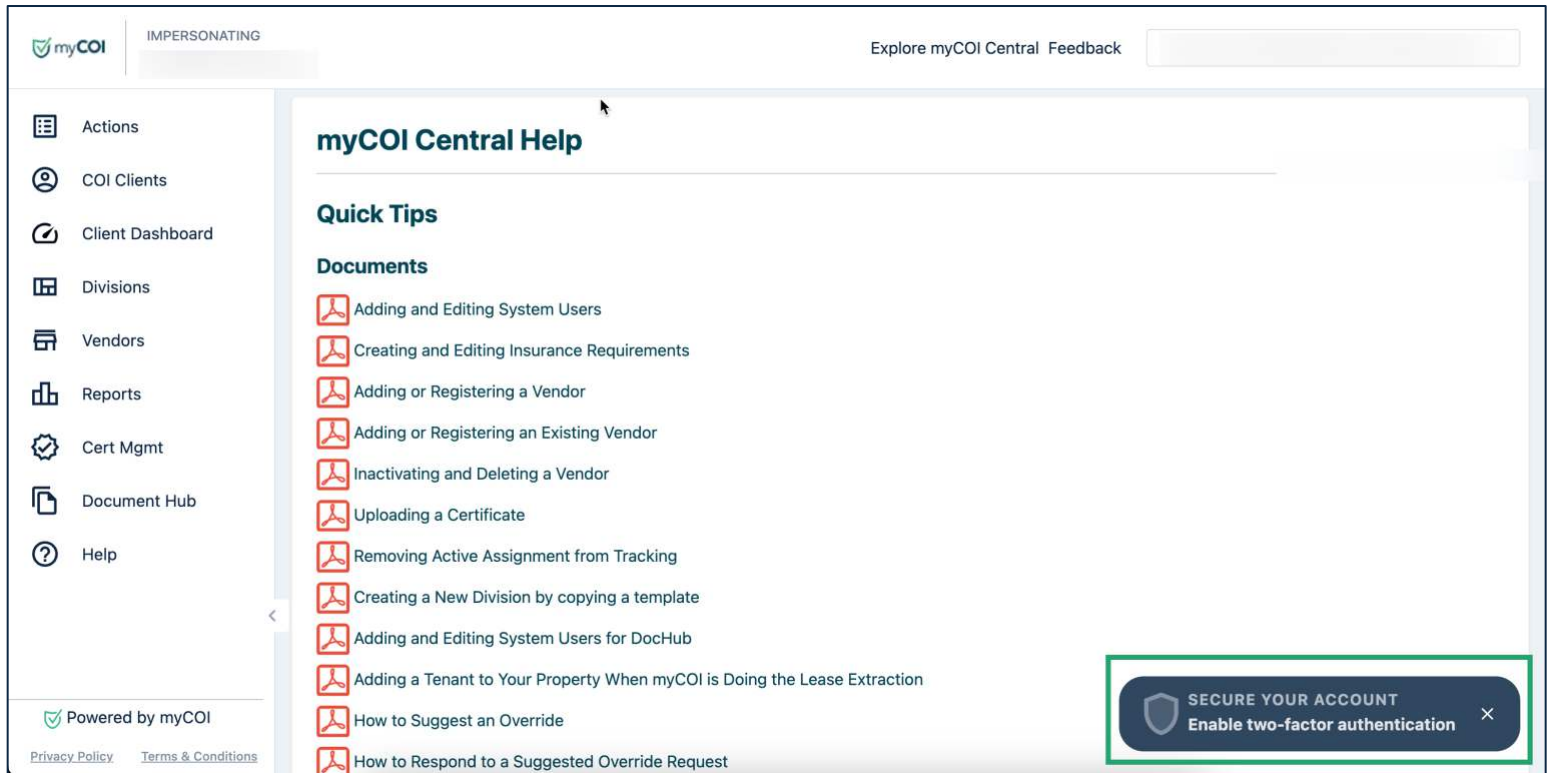
Back: Send Code

## 2FA - Email Address

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

### Step#1:

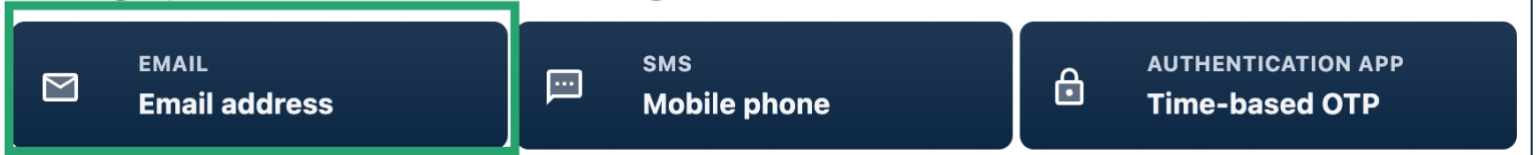
Select the **Secure Your Account, Enable two-factor authentication** on the bottom right.



### Step#2:

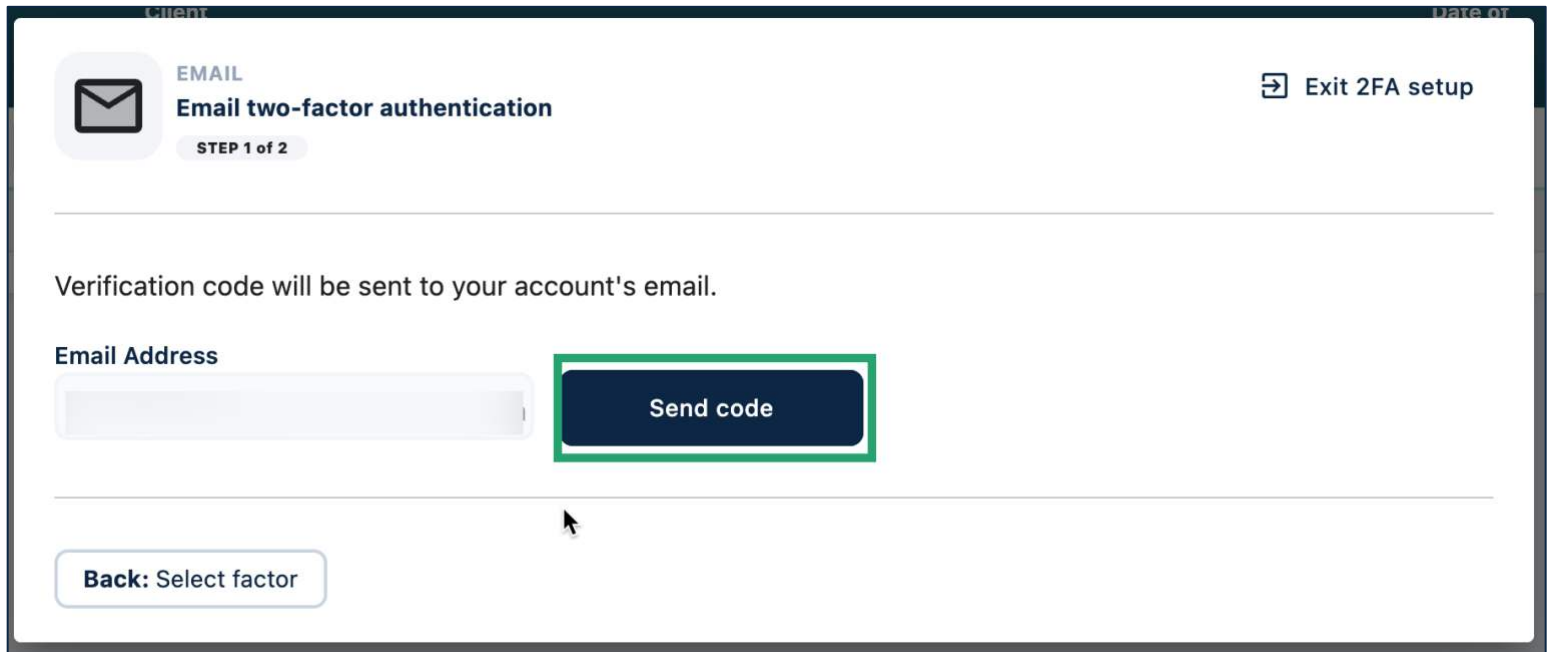
Select **SMS, Mobile Phone**

To begin, select one of the following factors:



### Step#3:

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



EMAIL  
Email two-factor authentication  
STEP 1 of 2

Exit 2FA setup

Verification code will be sent to your account's email.

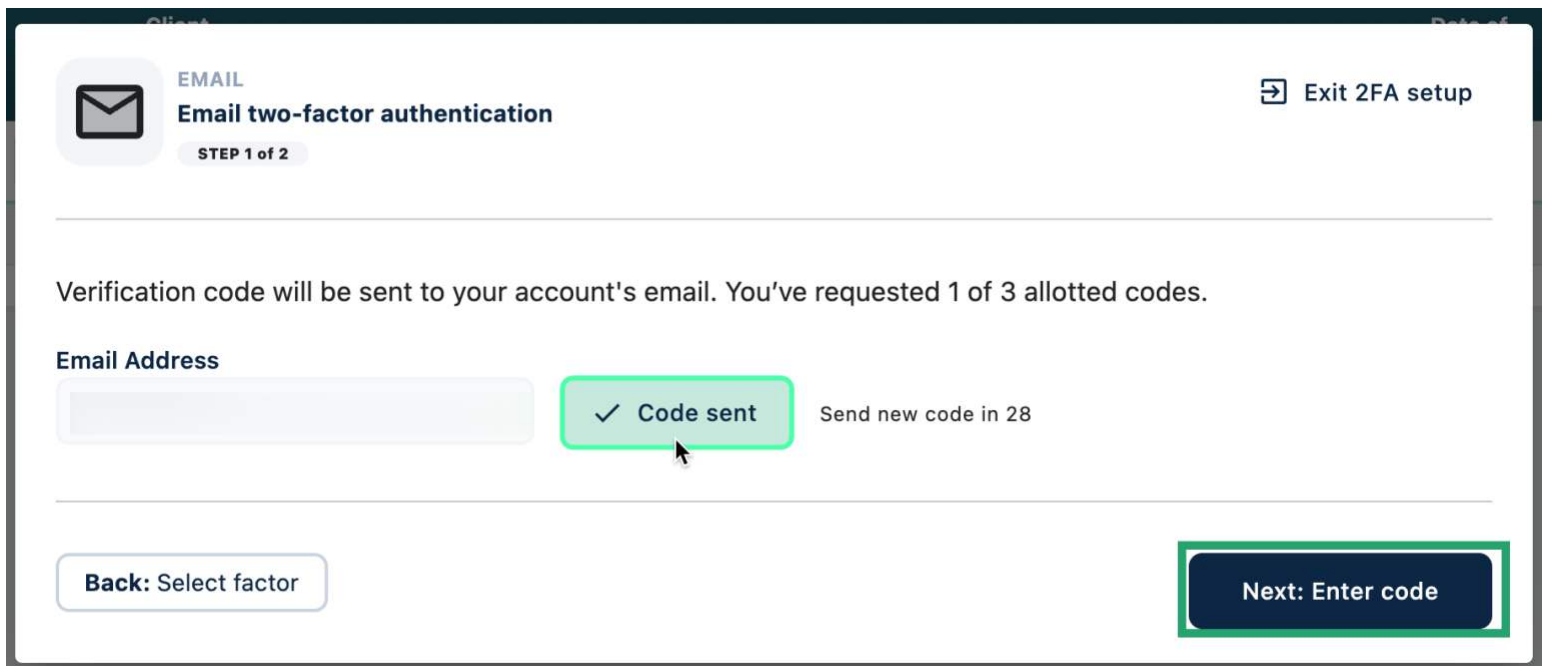
Email Address

Send code

Back: Select factor

### Step#4:

Select **Enter code**



EMAIL  
Email two-factor authentication  
STEP 1 of 2

Exit 2FA setup

Verification code will be sent to your account's email. You've requested 1 of 3 allotted codes.

Email Address

✓ Code sent Send new code in 28

Back: Select factor

Next: Enter code

## Step#5:

User will receive an email with the verification code.

### TWO-FACTOR AUTH

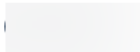
Here's your code



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:**



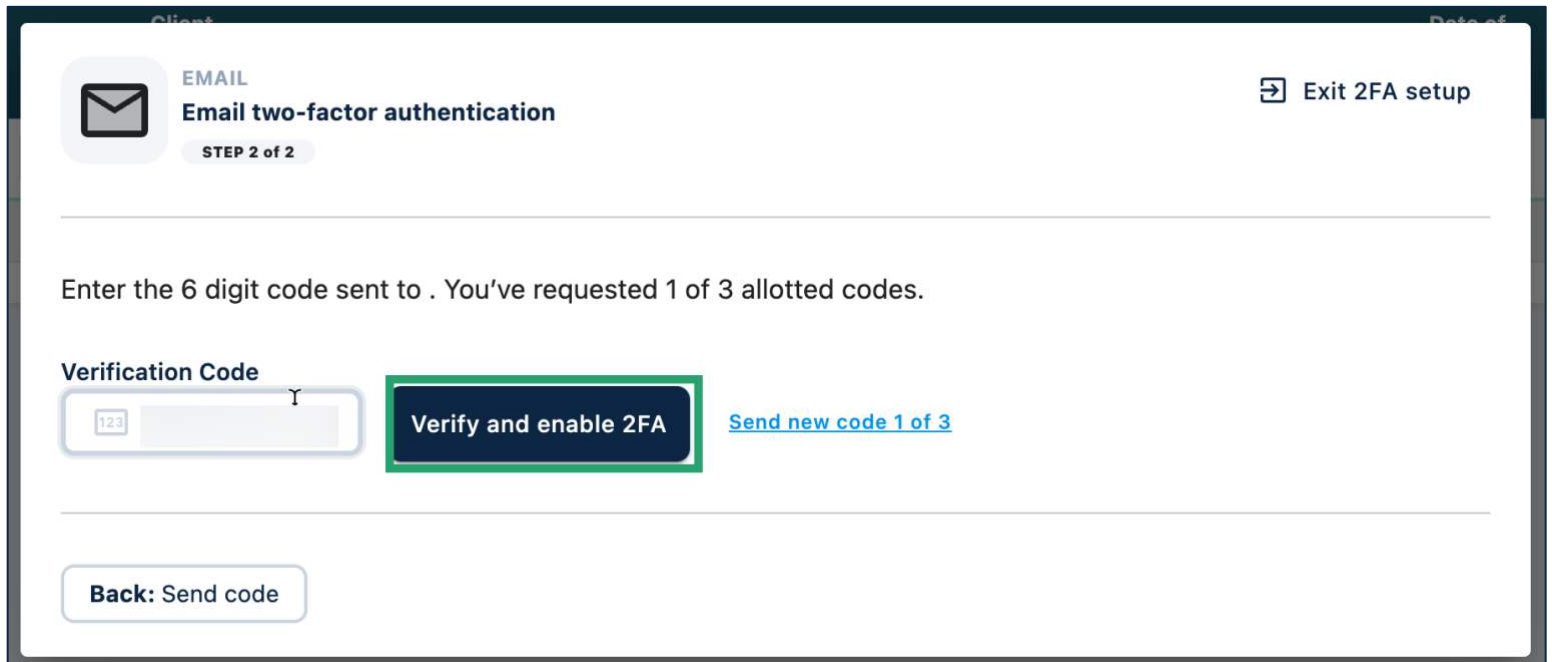
Please note that this code will expire within 5 minutes from the time it was generated.

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**.



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

123

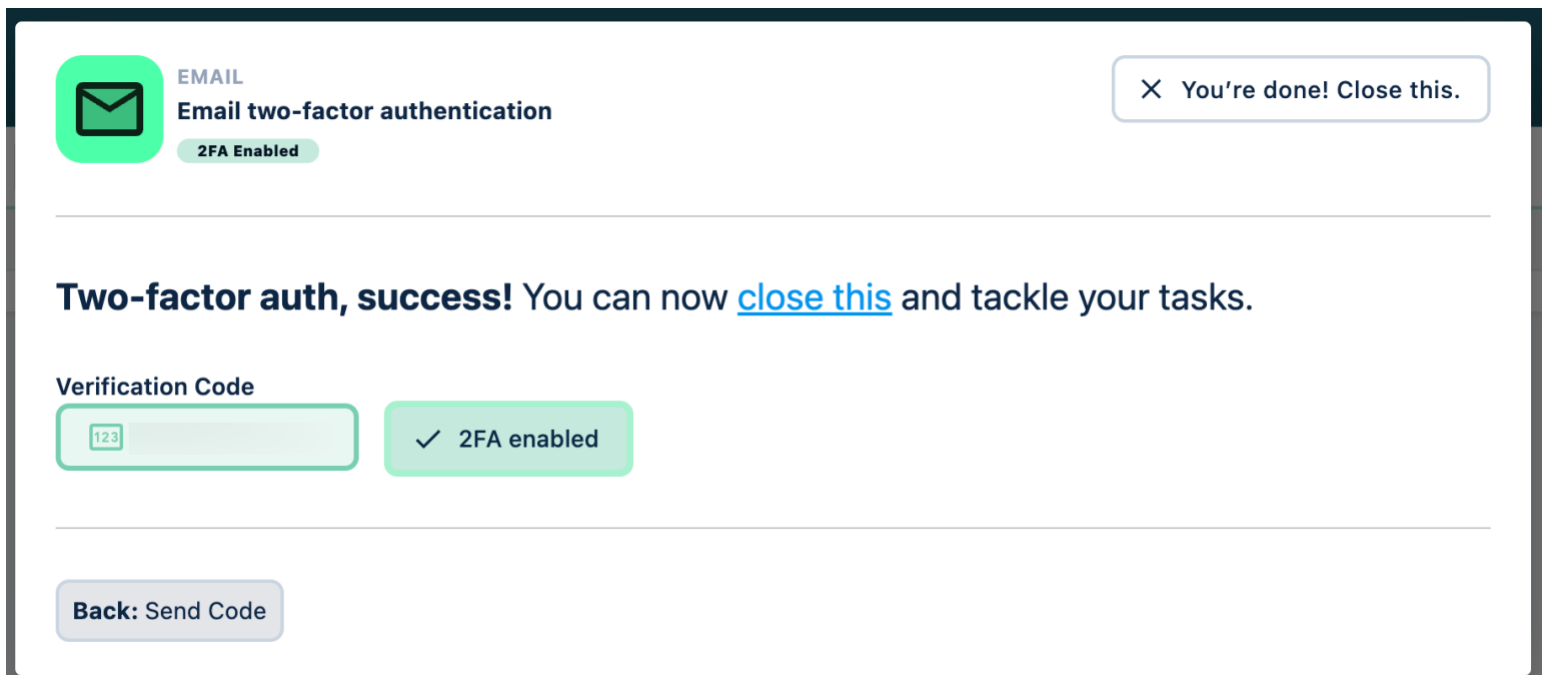
Verify and enable 2FA

[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

You're done! Close this.

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

Verification Code

123

✓ 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.