Multi Factor Authentication for Client Portal

What is Multi-Factor Authentication?

- Multi factor authentication is an added level of security to protect your confidential information in case your log in credentials are ever compromised. It works by sending a code to your connected device before allowing a log in.

Is This Required?

- **Yes.** This has been optional in the past, but with ever increasing security threats, this step will no longer be optional.
    - ***Please note that some tutorials/steps may still refer to it as optional, however, the provider is moving toward making this a required step, so it should no longer be treated as optional.**

How do I set this up?

- See the pages that follow for step-by-step instructions on getting your account set up.

Will I need my device every time I log in?

- Yes, you will not be able to log in without your connected device. Make sure to save the emergency access codes provided at setup in case of new/lost device. However, you can always generate an emergency code, see the following pages for how to do this.
    - ***Please note that LKR does not store your MFA codes. We can help you with generating a new emergency code, but we cannot “reset” anything on our end.**

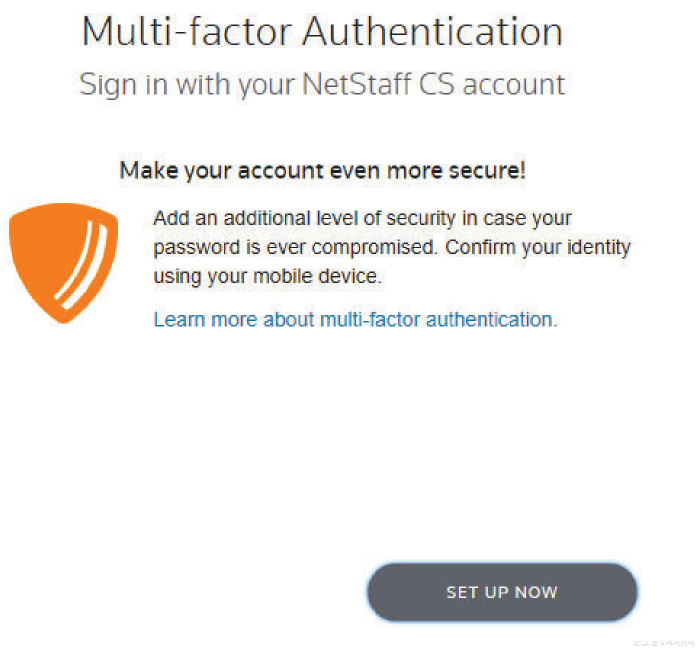
I am following the steps but am not getting a code, why?

- If you are using the Thomson Reuters App you should get a notification and be able to quickly sign in.
    - Open the app to troubleshoot if you don’t see a notification.
- If you are using a third-party app, you will have to open the app each time to retrieve a code.

You can contact us at 336-274-3700 if you have questions.

Using Multi-Factor Authentication on the Client Portal

Cick “Set Up Now” then “Get Started



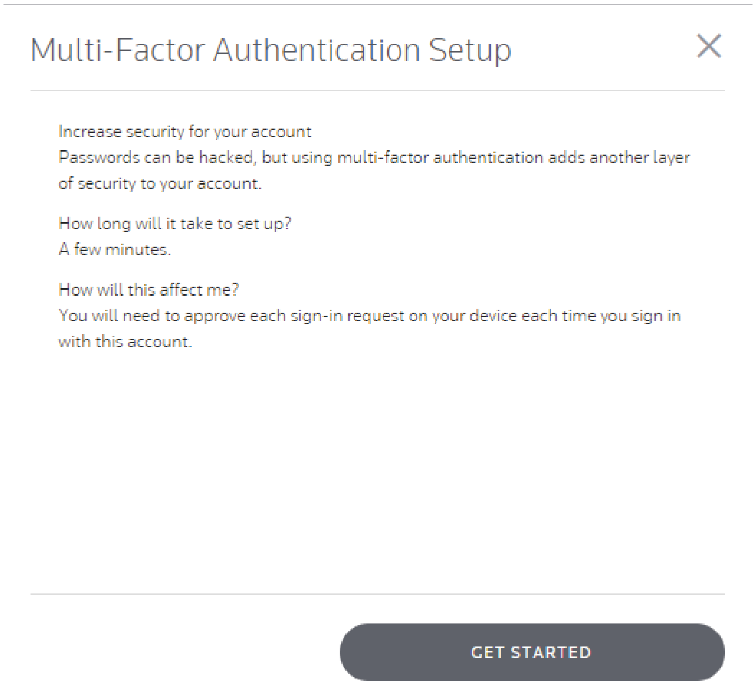
Multi-factor Authentication

Sign in with your NetStaff CS account

Make your account even more secure!

Add an additional level of security in case your password is ever compromised. Confirm your identity using your mobile device.

Learn more about multi-factor authentication.



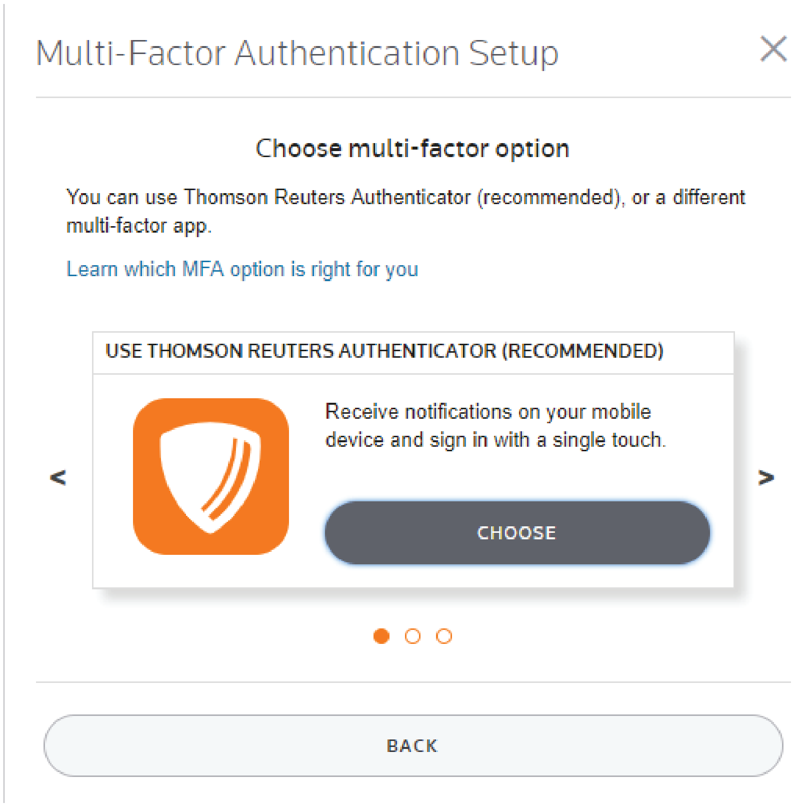
Multi-Factor Authentication Setup

Increase security for your account
Passwords can be hacked, but using multi-factor authentication adds another layer of security to your account.

How long will it take to set up?
A few minutes.

How will this affect me?
You will need to approve each sign-in request on your device each time you sign in with this account.

If you click Choose on ‘Thomson Reuters Authenticator’



Multi-Factor Authentication Setup

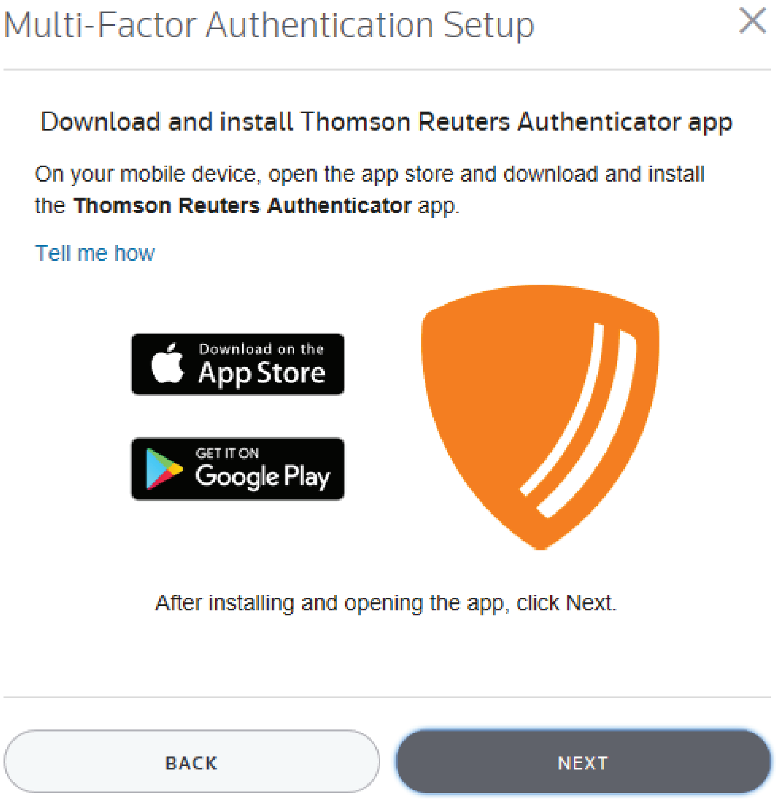
Choose multi-factor option

You can use Thomson Reuters Authenticator (recommended), or a different multi-factor app.

Learn which MFA option is right for you

USE THOMSON REUTERS AUTHENTICATOR (RECOMMENDED)

Receive notifications on your mobile device and sign in with a single touch.



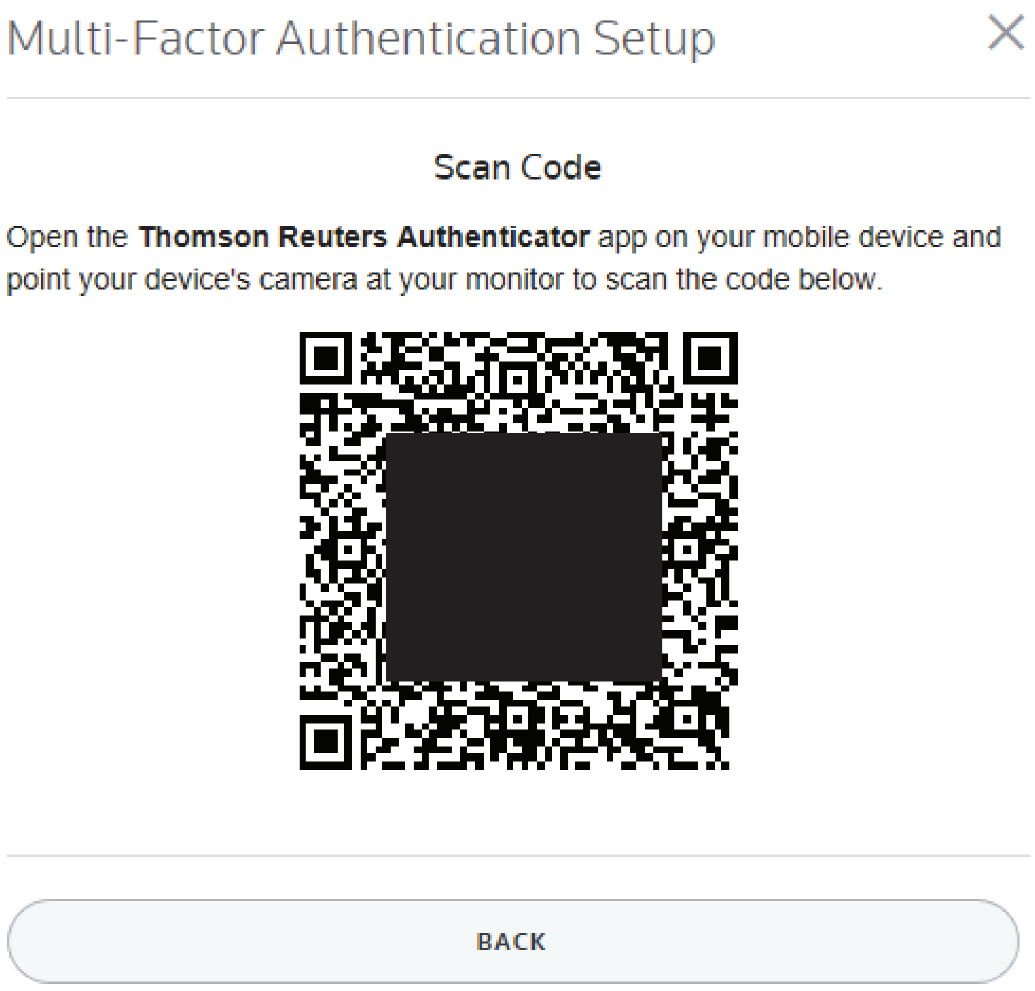
Multi-Factor Authentication Setup

Download and install Thomson Reuters Authenticator app

On your mobile device, open the app store and download and install the **Thomson Reuters Authenticator** app.

Tell me how

After installing and opening the app, click Next.



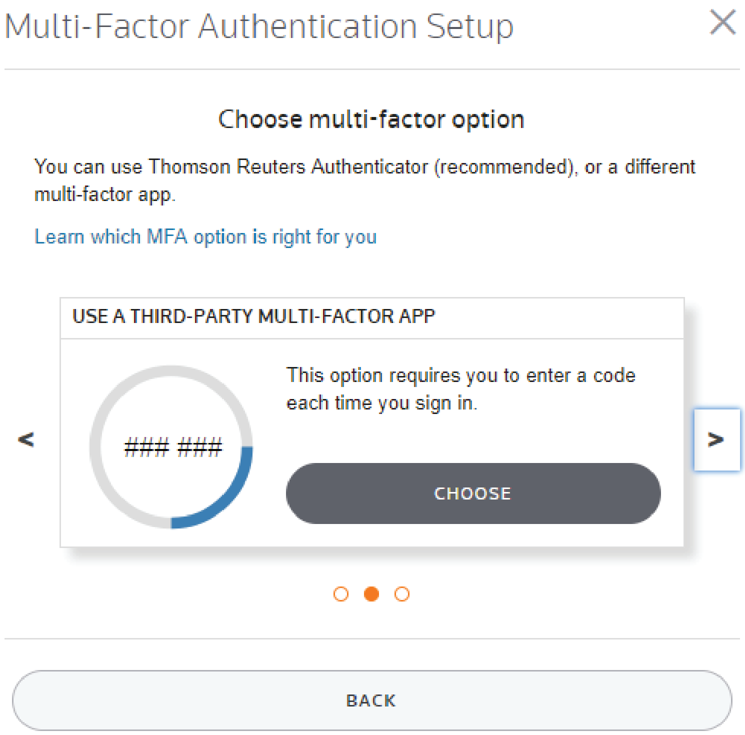
Multi-Factor Authentication Setup

Scan Code

Open the **Thomson Reuters Authenticator** app on your mobile device and point your device's camera at your monitor to scan the code below.

[redacted]

If you click Choose on ‘Third-Party Multi-Factor App’



Multi-Factor Authentication Setup

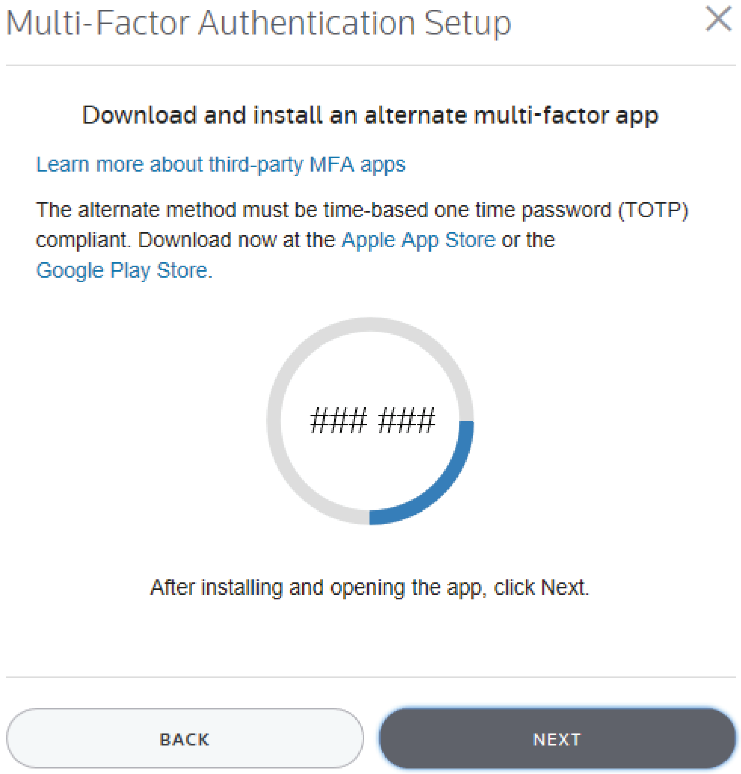
Choose multi-factor option

You can use Thomson Reuters Authenticator (recommended), or a different multi-factor app.

Learn which MFA option is right for you

USE A THIRD-PARTY MULTI-FACTOR APP

This option requires you to enter a code each time you sign in.



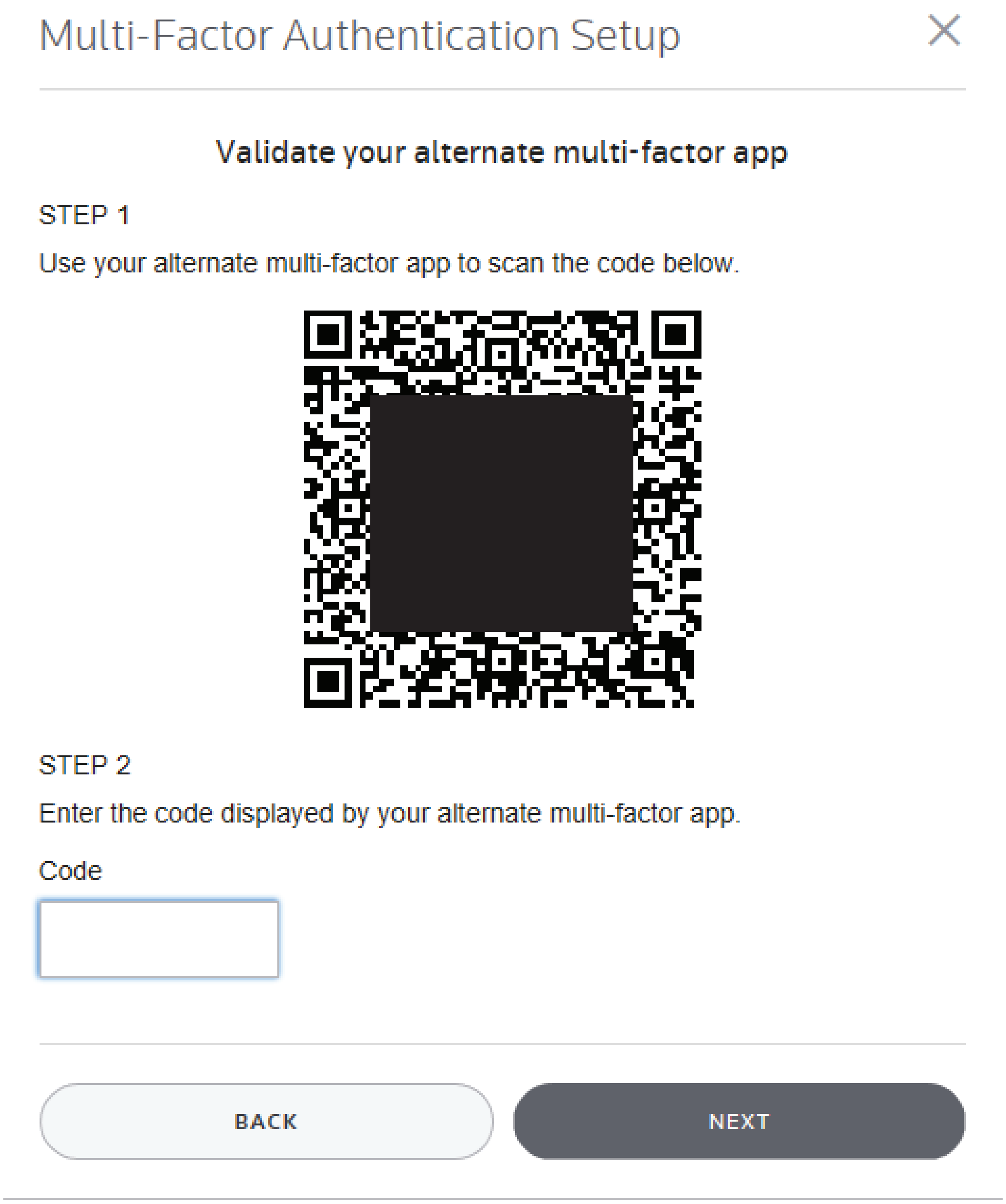
Multi-Factor Authentication Setup

Download and install an alternate multi-factor app

Learn more about third-party MFA apps

The alternate method must be time-based one time password (TOTP) compliant. Download now at the Apple App Store or the Google Play Store.

After installing and opening the app, click Next.



Multi-Factor Authentication Setup

Validate your alternate multi-factor app

STEP 1

Use your alternate multi-factor app to scan the code below.

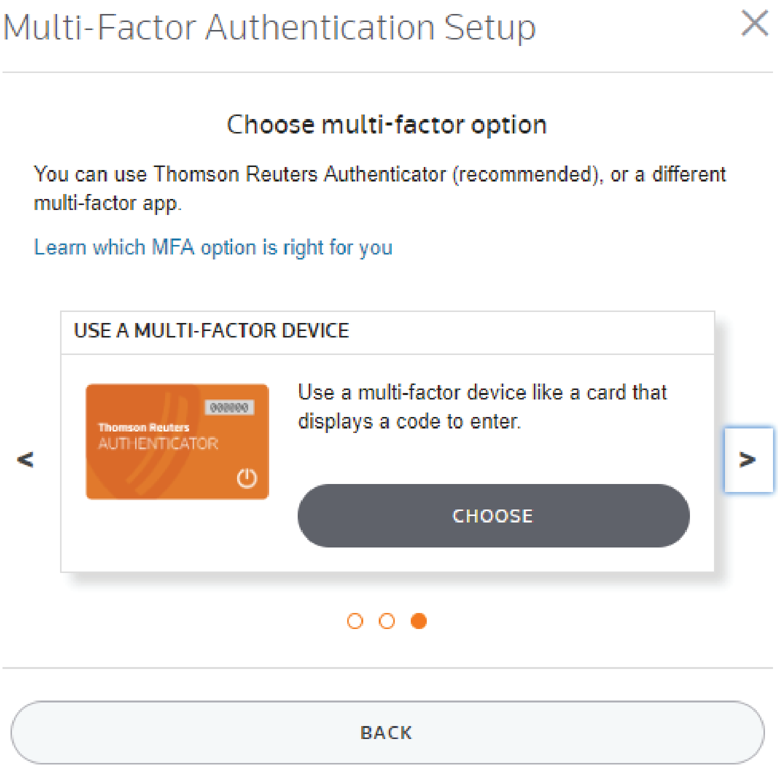
[redacted]

STEP 2

Enter the code displayed by your alternate multi-factor app.

Code

Last option is to use an authenticator card. (we haven’t had anyone use this method)



Multi-Factor Authentication Setup

Choose multi-factor option

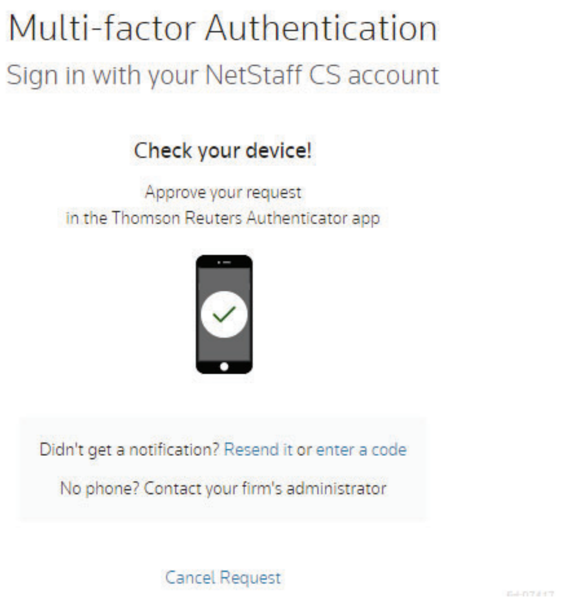
You can use Thomson Reuters Authenticator (recommended), or a different multi-factor app.

Learn which MFA option is right for you

USE A MULTI-FACTOR DEVICE

Use a multi-factor device like a card that displays a code to enter.

Once setup, the next time you attempt login, you will be prompted for the multi-factor authentication



Multi-factor Authentication

Sign in with your NetStaff CS account

Check your device!

Approve your request
in the Thomson Reuters Authenticator app

Didn't get a notification? Resend it or enter a code

No phone? Contact your firm's administrator

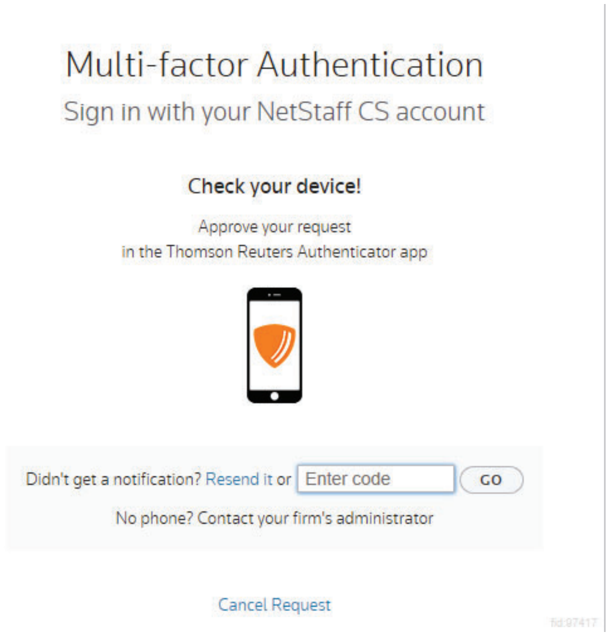
Cancel Request

fid:97417

On the device, click the notification (if you gave the app permission to send notifications) or open the Authenticator app used.

If the Thomson Authenticator app, you may click the green check to approve the login attempt.

If a third-party Authenticator app (Google, Microsoft, LastPass, etc.), you may have to click “enter a code” (on the prompt above) and input the code the app is displaying at that time. These codes reset every 30 seconds.



Multi-factor Authentication

Sign in with your NetStaff CS account

Check your device!

Approve your request
in the Thomson Reuters Authenticator app

Didn't get a notification? Resend it or Enter code GO

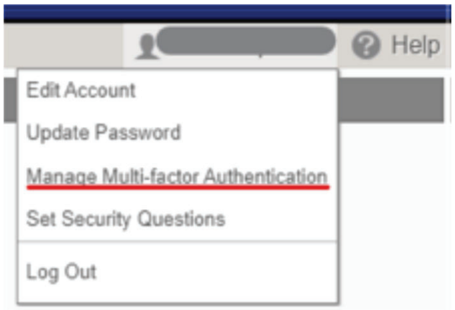
No phone? Contact your firm's administrator

Cancel Request

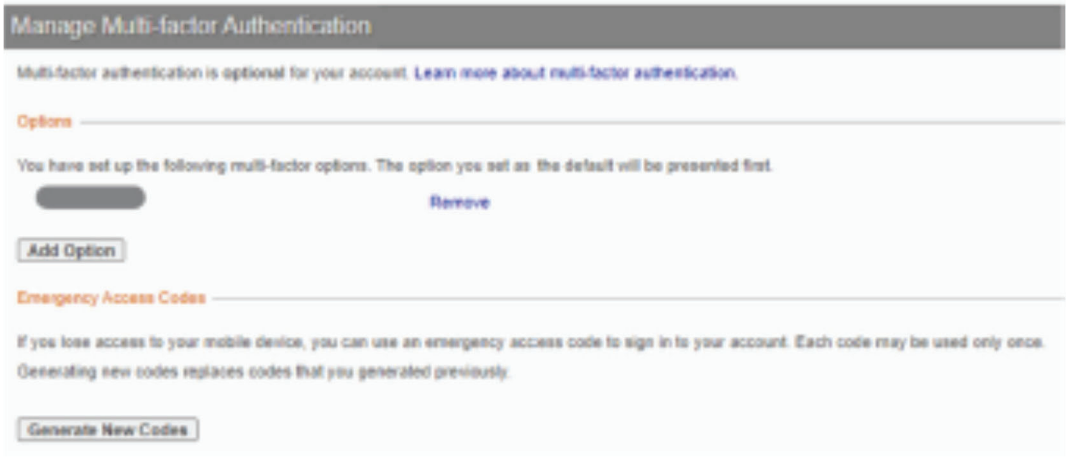
fid:97417

New/Lost device? Don’t have your device with you?

Click on your name in the top right corner and select Manage Multi-factor Authentication



If you have already setup MFA, this is also where you can add a new device, if replacing your phone, but still have the old one to login with. See emergency codes at the end, for the case you lose/break a phone. You can generate new codes here, if you didn’t save them during the setup.



Manage Multi-factor Authentication

Multi-factor authentication is optional for your account. Learn more about multi-factor authentication.

Options

You have set up the following multi-factor options. The option you set as the default will be presented first.

[redacted] Remove

Add Option

Emergency Access Codes

If you lose access to your mobile device, you can use an emergency access code to sign in to your account. Each code may be used only once. Generating new codes replaces codes that you generated previously.

Generate New Codes