Meadows Urquhart Acree & Cook, LLP
Certified Public Accountants

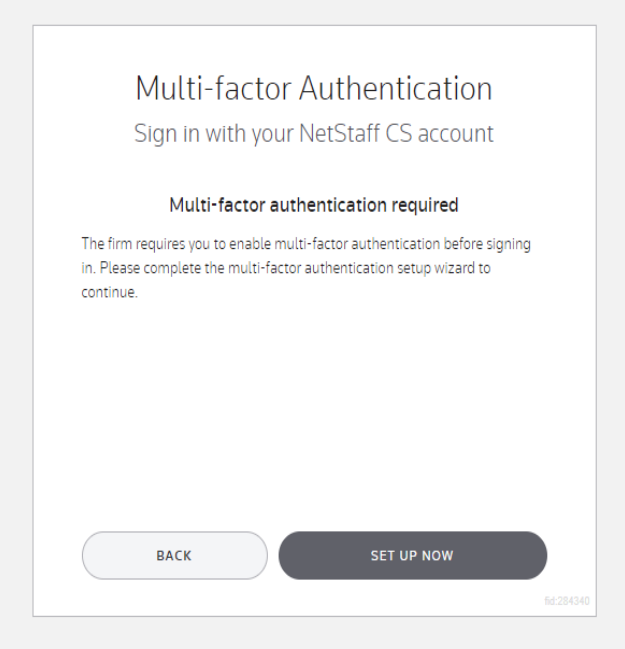
How To Set Up Multi-Factor Authentication: Accessing Your Client Portal

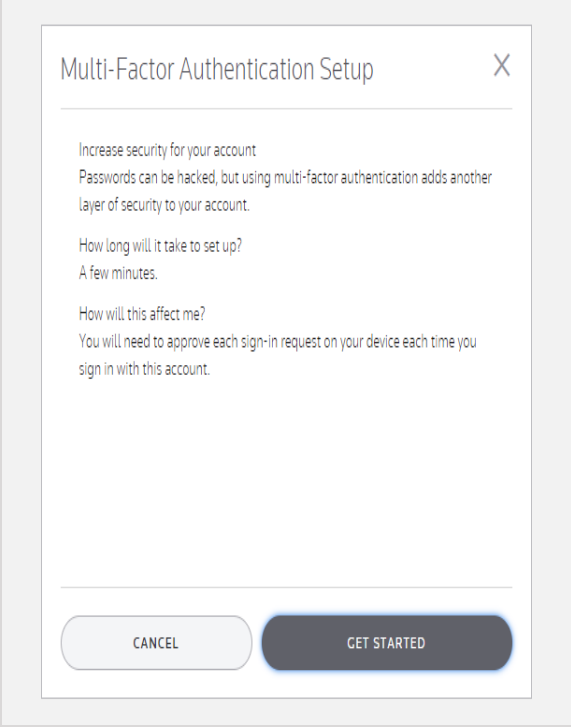
Introduction

The purpose of this guide is to ease the transition into using multi-factor authentication by walking our clients through the step-by-step process of setup. The value of having a multi-factor authenticator is that adds an extra layer of protection to keep our clients' sensitive financial information secure and free from information fraud and identity theft. While initial setup may take a few minutes, once the multi-factor authenticator in place it is incredibly quick to use.

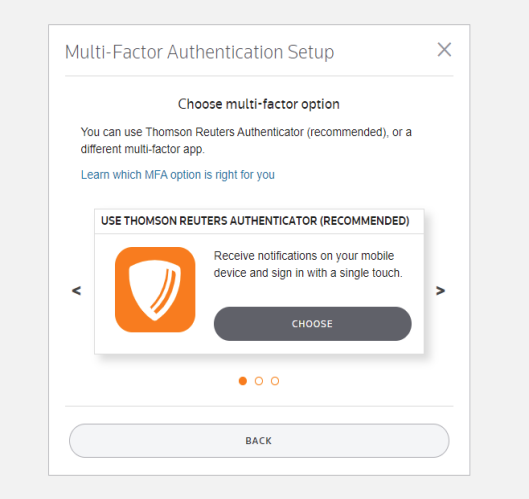
Setting Up Multi-Factor Authentication

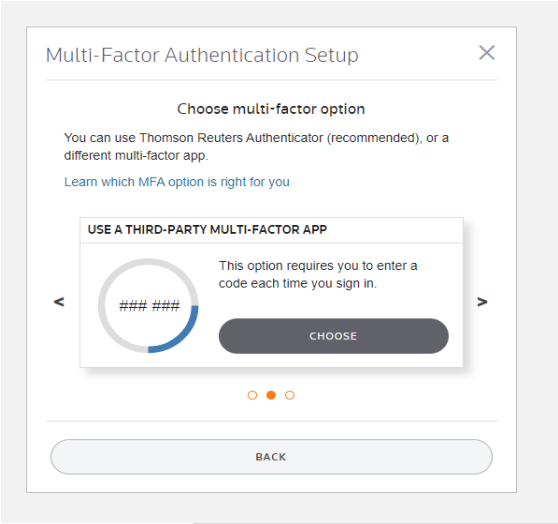
The next time you go to login to your client portal, this message will pop up, with the second one following:

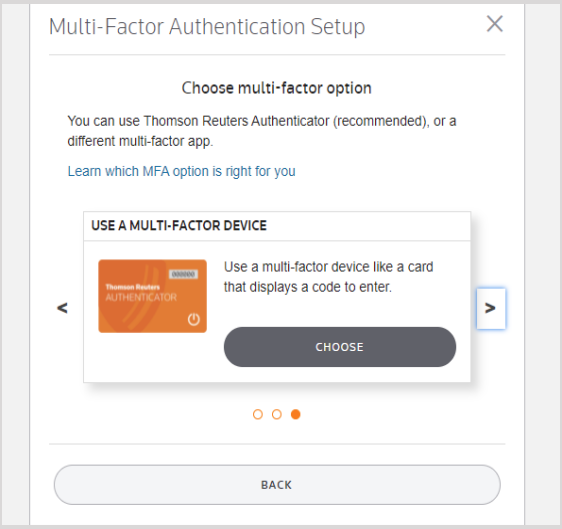




You will then be presented with three options for setting up multi-factor authentication: 1) The Thompson Reuters App, 2) A Third Party Authenticator App, or 3) The Thompson Reuters Card. Let's look at each of these three options below:





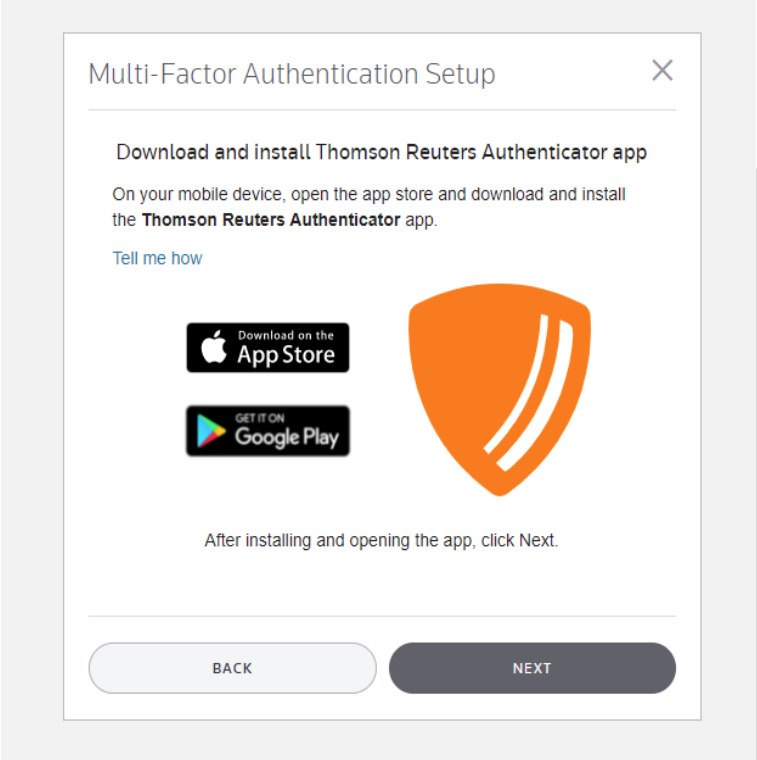


There are three options for setting up multi-factor authentication:

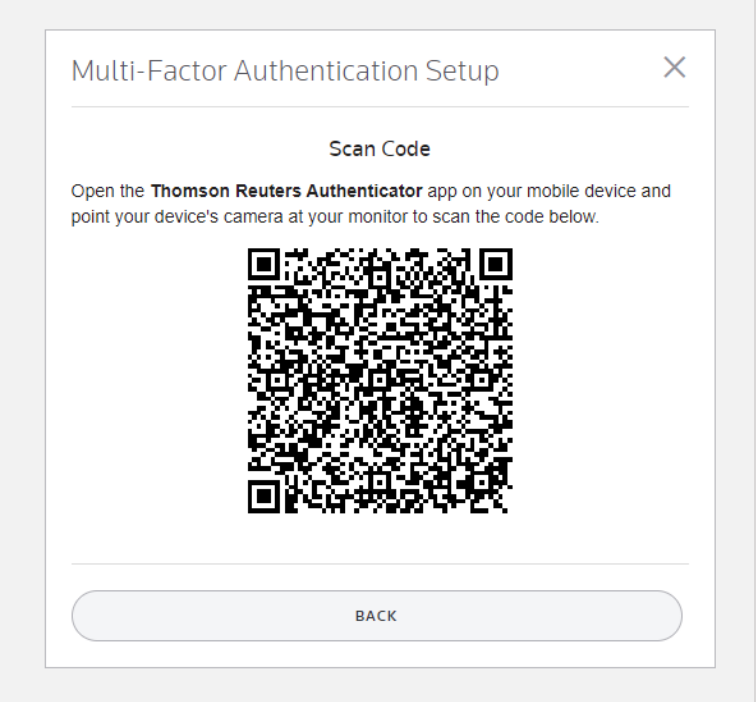
1. The Thompson Reuters App
2. A Third Party Authenticator App
3. The Thompson Reuters Card

Option 1: The Thompson Reuters App

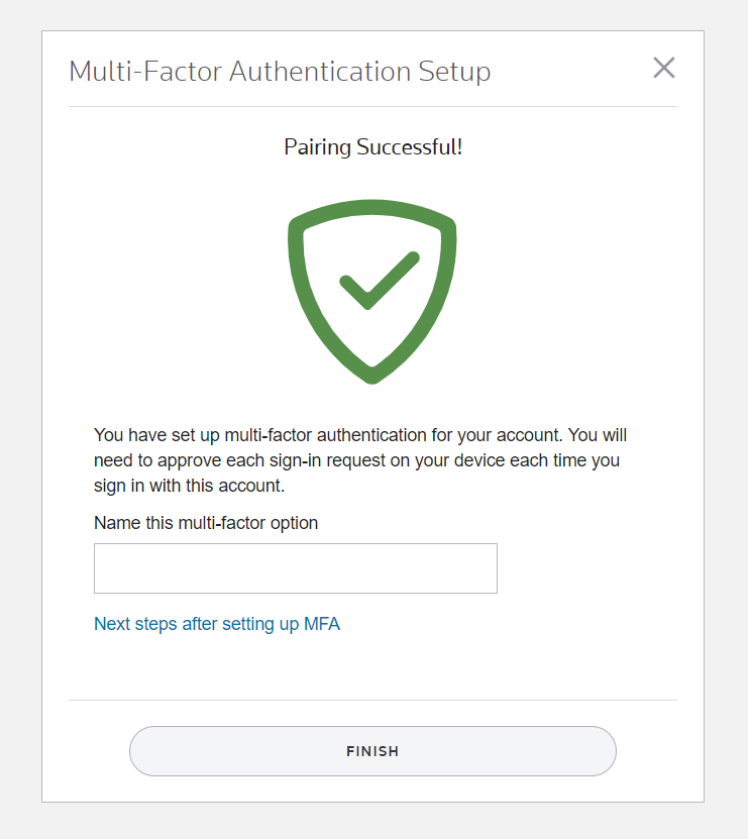
First, let's look at the option for choosing the Thompson Reuters App. This option works well if you have a smartphone. Follow the prompts on the screen and your phone to download the app, then click next.



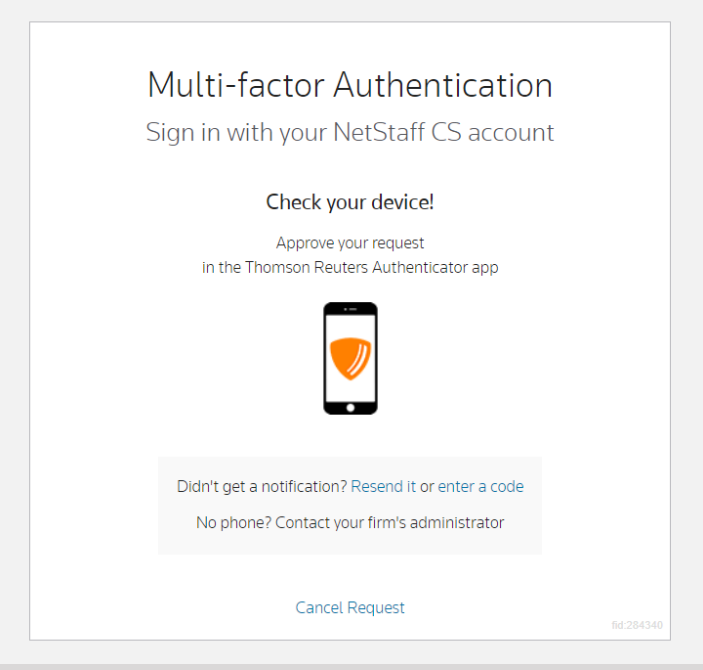
Open the Thompson Reuters App and point your camera at the screen to scan the code. You may need to allow the app to acess your camera in settings (if so, follow the prompts on your screen to turn camera access on, then return to the app).



You will get a message saying “pairing successful,” and a prompt will come up on the screen for you to name your authenticator. When you are done, click “Finish” and you will be set up!



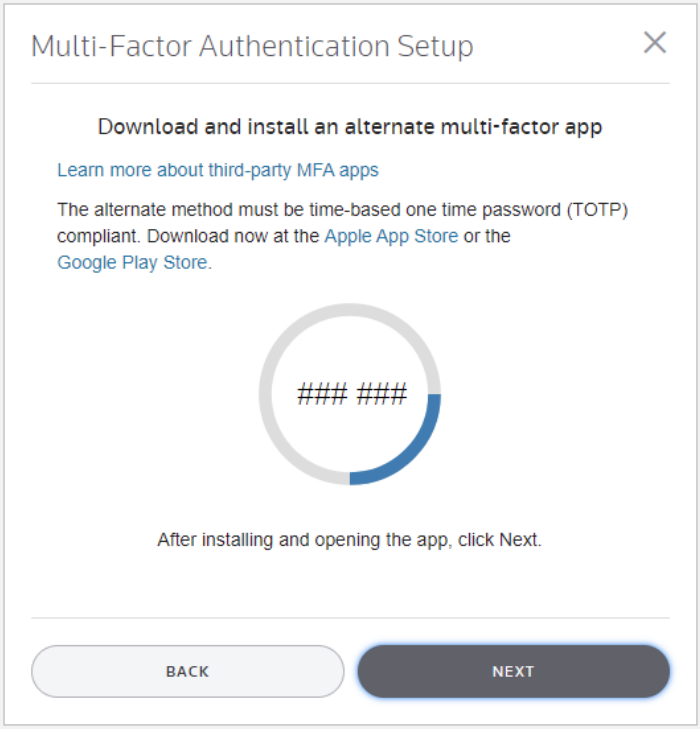
The next time you go to sign in, after entering your username, password, and checking the box, you should get this prompt to check your device. Open the Thompson Reuters app and either check the green arrow or opt to enter the code on your computer. Once the verifcation process is complete, you should be into your portal.

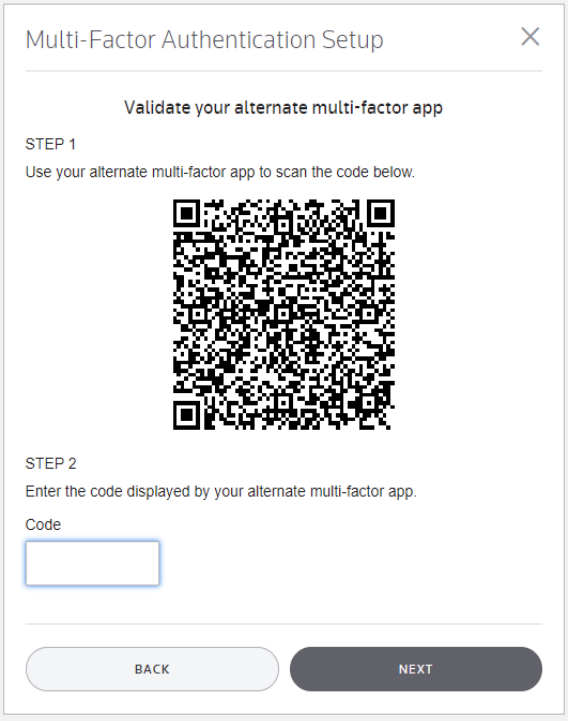


Option 2: A Third Party Authenticator App

A thrid party authenticator app works much in the same way as the Thompson Reuters app and is a good option if you already have a multi-factor authenticator (MFA) app on your phone and don't want to have more than one app (for example, if you are already using an MFA app for work.) If you don't already have a MFA app, we would recommend going with option 1, since Thompson Reuters support team cannot assist with third-party software, should you run into any technical difficulties.

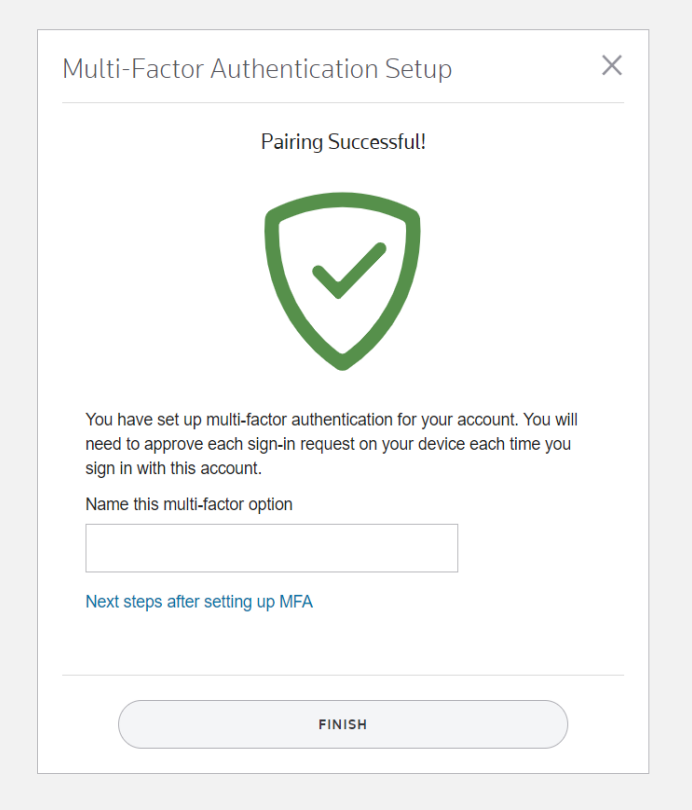
If you decide to go with option 2, select it from the options page (show on page 2 of this guide) by clicking the right arrow. Once you confirm you have your desired MFA app on your phone, click next.



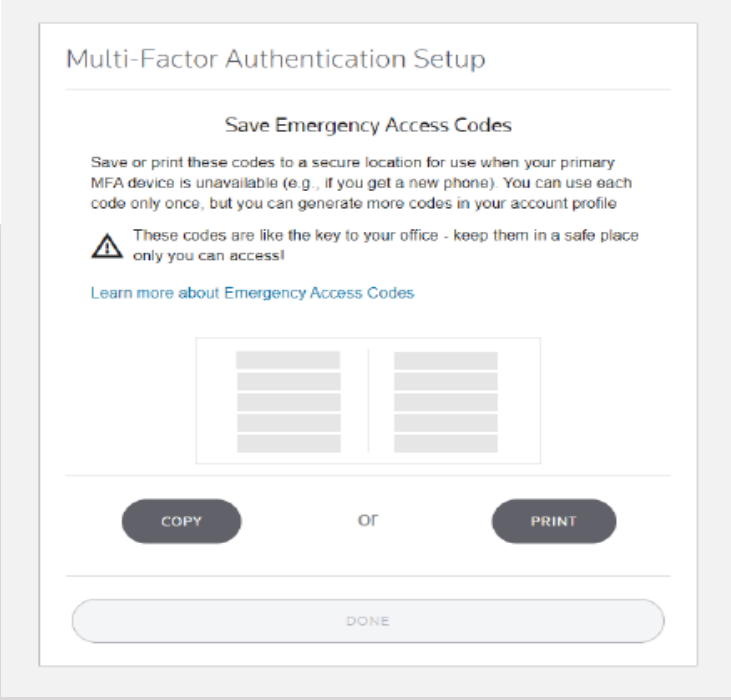


Open your MFA app and scan the QR code on the screen. Next follow the prompts in your app to link your account with it and enter the code displayed in your multi-factor app on the computer screen and hit next.

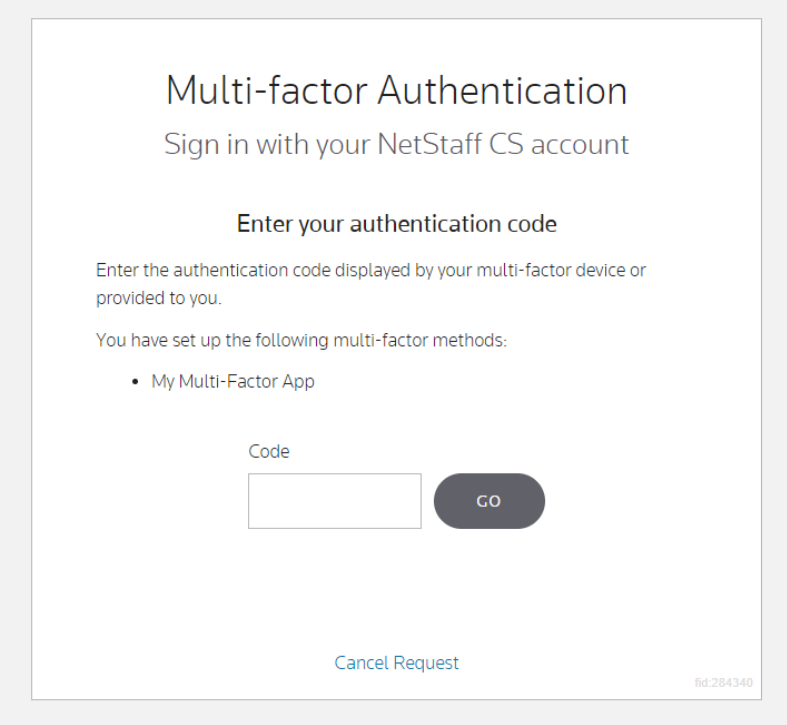
As with the first option, you will get a message saying “pairing successful,” and a prompt will come up on the screen for you to name your authenticator. When you are done, click “Finish.”



As part of the setup process for a third party MFA app, you will receive emergency access codes to use in case for some reason your MFA device is not working or is unavailable (for example, if you get a new phone). As the screen says, keep these codes in a safe place. They only work once, but will allow you access to your portal where you can change your multi-factor authentication method (more on how to do this on page 9) for access in the future.



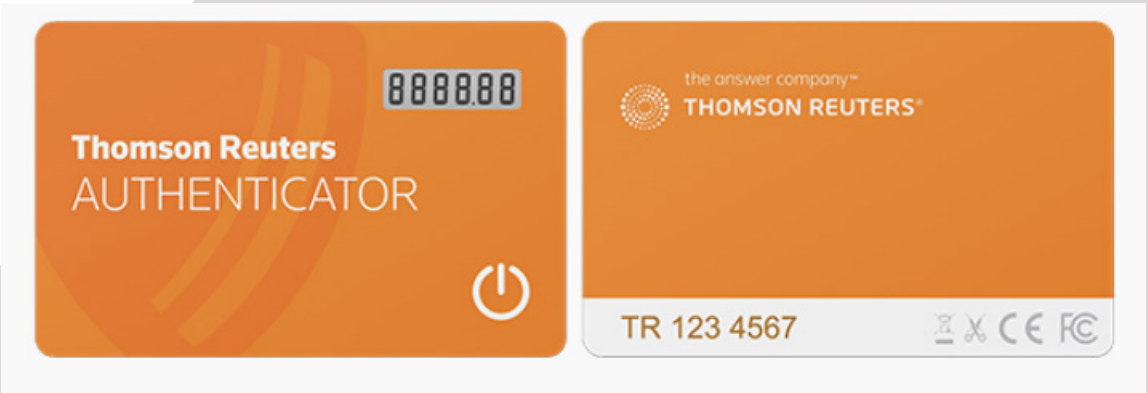
The next time you go to sign in, after entering your username, password, and checking the box, you should get this prompt to check your device. Open your MFA app and enter the code on your computer. Once the verifcation process is complete, you should be into your portal.



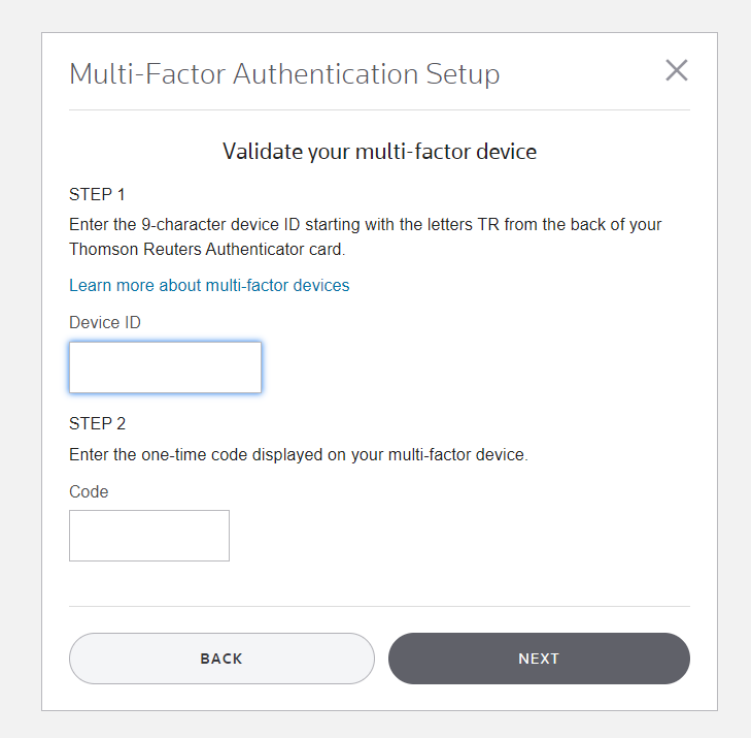
Option 3: The Thompson Reuters Authenticator Display Card

The third and final option for setting up multi-factor authentication is to use the Thompson Reuters (TR) Card. This option is great if you do not have a smart phone and therefore are unable to download one of the two MFA apps, or if you would like to use it as a backup to your mobile device. The cost of the TR card is $35.59 each if purchasing one - two cards, with the price per card decreasing the more cards you purchase. Click here to purchase a TR card(s).

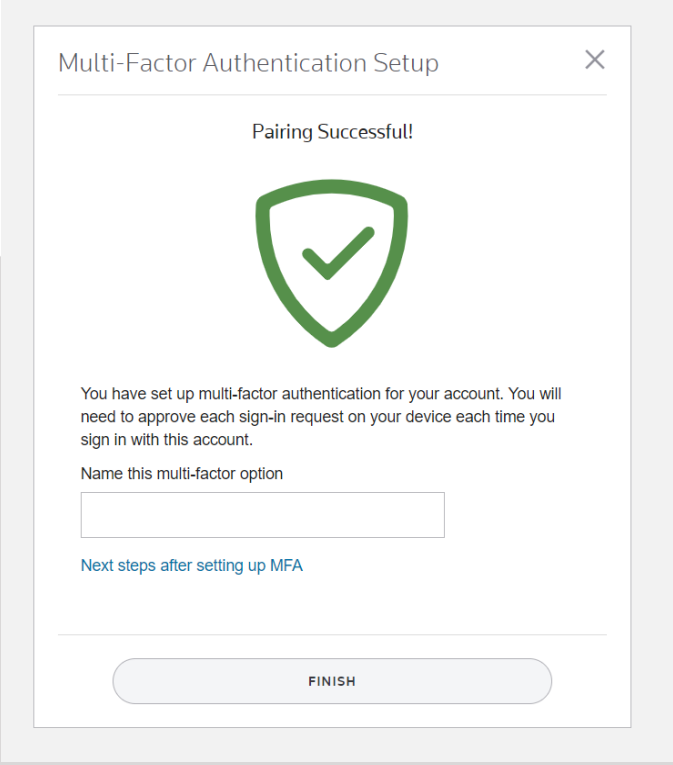
These cards are the size of a credit card and are easy to use. Simply press the button in the bottom right corner and enter the 6 digit code that appears in the display window in the top right each time you sign into your account.



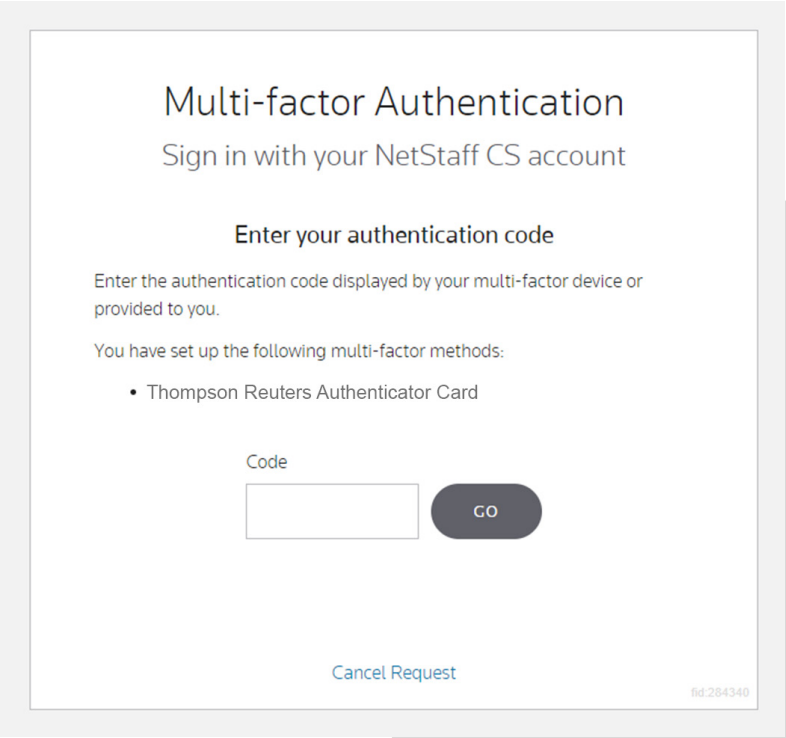
The first time you go to link your card to your account, enter the 9-character code beginning with TR on the back of your card into the first window on your computer screen. After that, press the on button (if it is not on already) and enter your 6 digit code into the second window on the computer screen.



You will get a message saying “pairing successful,” and a prompt will come up on the screen for you to name your authenticator. When you are done, click “Finish” and you will be set up!



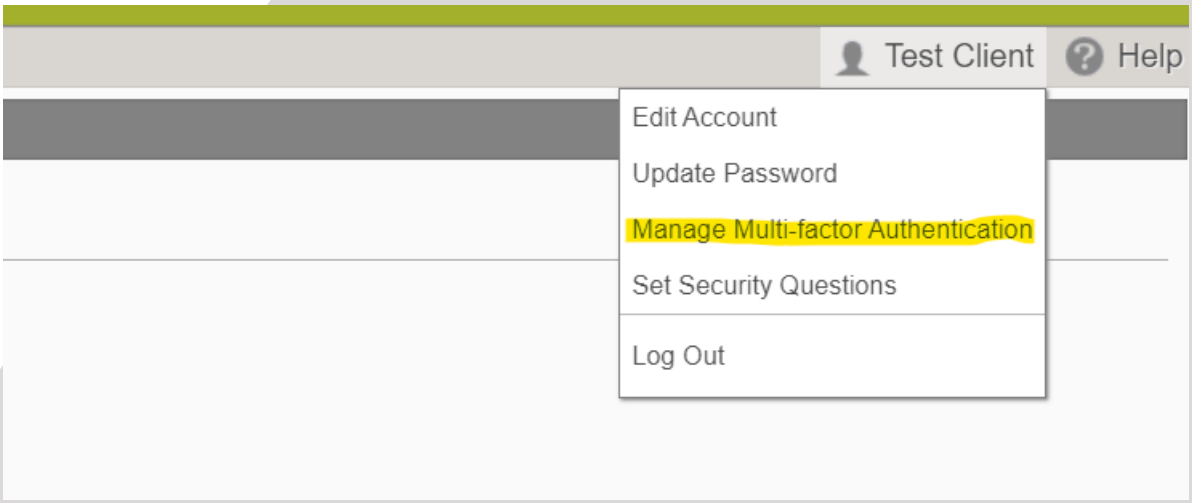
The next time you go to sign in, you should not need to enter the 9 character code on the back of your TR card, just the 6 digit code that appears in the display window in the top right on the front of your card. Enter the code when prompted, and you should be into your account.



How to Change Your Multi-Factor Authentication Method

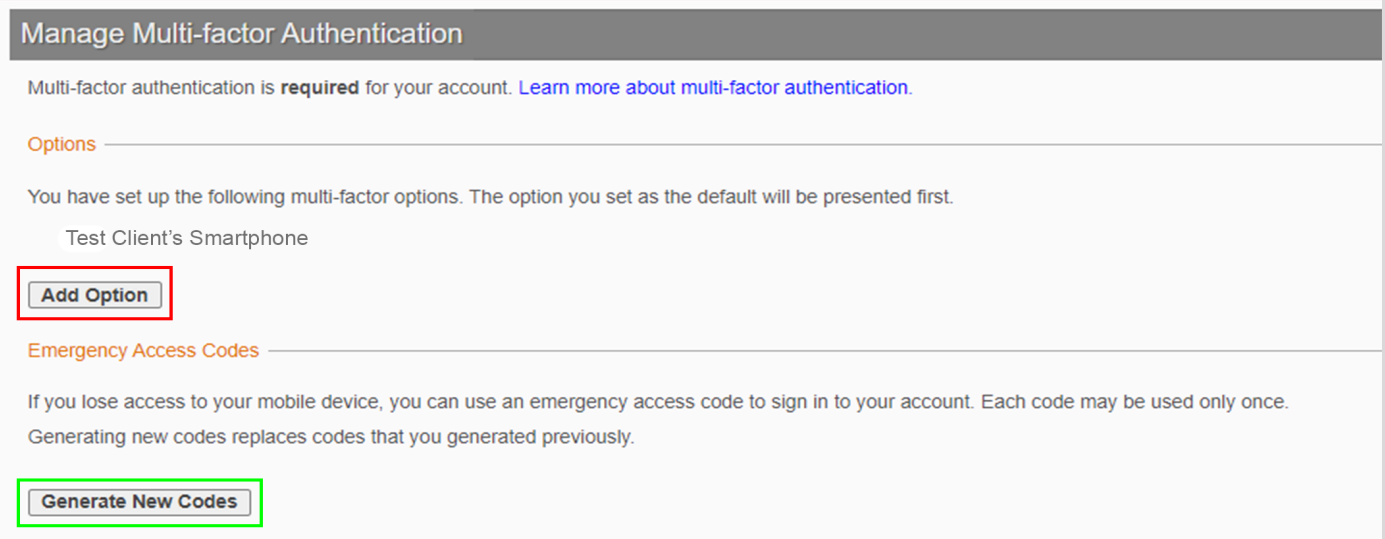
There may be a time you want to change your method of multi-factor authentication in the future (for example, if you get a new smartphone, get rid of your smartphone, or want to try a different method). To do this, you will need to sign in and use your current method of multi-factor authentication (or one of the emergency codes, if your third-party authenticator is not working).

Once you are inside your portal, click on your name on the upper right side of the screen. A drop-down menu should appear, and from that menu select “Manage Multi-factor Authentication” (highlighted in yellow below).

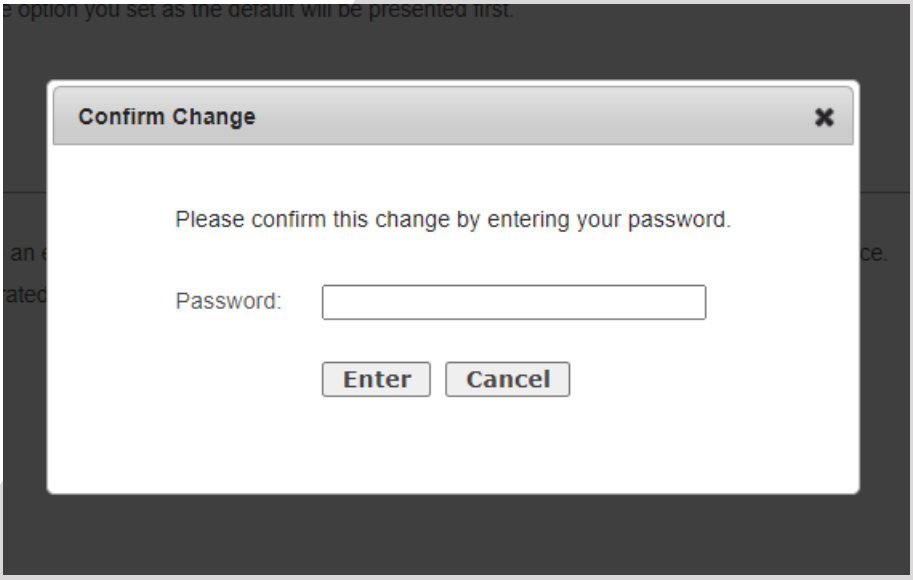


You should see the opiton you are currently using for multi-factor authentication, as well as a button to add an option below it (outlined in red). Click this to add another method for multi-factor authentication.

You will also see an option to generate new emergency codes, should you need them. If you decide to generate new codes, keep those in a safe place and discard your old codes, as they will no longer work. This option is outlined in green below.



It will ask you to confirm this change by entering your password.



This will take you back to the first page of multi-factor authentication setup where the whole process begins (see page 1 of this guide). Choose whichever option of MFA works best for you and follow the prompts to set it up.

Troubleshooting

If you run into any technical difficulties along the way, Thompson Reuters has a webpage setup to help you troubleshoot. They cover issues such as having a lost or new device, MFA setup issues, and login issues after MFA setup. Please refer to this webpage if you encounter difficulty (pictures of the webpage shown below).

Multi-factor authentication (MFA) troubleshooting

+ Show expandable text

Use this article to troubleshoot multi-factor authentication (MFA) issues with your account, your device, or your software. Before following any instructions listed here, find out which account type you have:

- *Example of Thomson Reuters ID (TRID) login.*
- *Example of NetStaff CS, Virtual Office, Software as a Service login*

Lost or new device

If you lose, replace, or reset your MFA device you'll lose the MFA pairing for your account.

- **If you have a backup MFA option** enabled, see Remove MFA devices from an account to remove or add a new device. Otherwise, your firm administrator can generate a temporary access code for your account.
- **If your admin account is inaccessible** and another admin is not available, contact Support at 800.968.0600 for help.

TRID instructions for administrators

+ Generate a temporary code for another account

NetStaff CS administrators

+ Generate a temporary code for another account

MFA Setup issues

Use the links below to learn more about specific issues you may encounter after setup.

+ "We're unable to verify your profile information"
+ "Something went wrong"
+ "Timed out waiting for Scan. Please go back and try again"
+ Unable to scan the QR code when pairing your login credentials to the mobile app.

Login issues after MFA setup

+ Mobile device doesn't receive approval request
+ Application does not prompt for MFA when signing in
+ Approved sign in on device, but website or application times out waiting for approval
+ Device asks for fingerprint scan, facial recognition or a passcode, but these are not enabled.
+ Receiving MFA prompt on Apple Watch, but can't approve the login request.
+ Nothing happens when I approve the log in attempt on the device.
+ Prompted to set up MFA when e-filing in UltraTax CS, but it is already enabled.

If after referencing this webpage you still have questions, our team is happy to help! You can contact our office at 804-249-5786.