Thomson Reuters Multi-factor Authentication (for your Tax Portal)
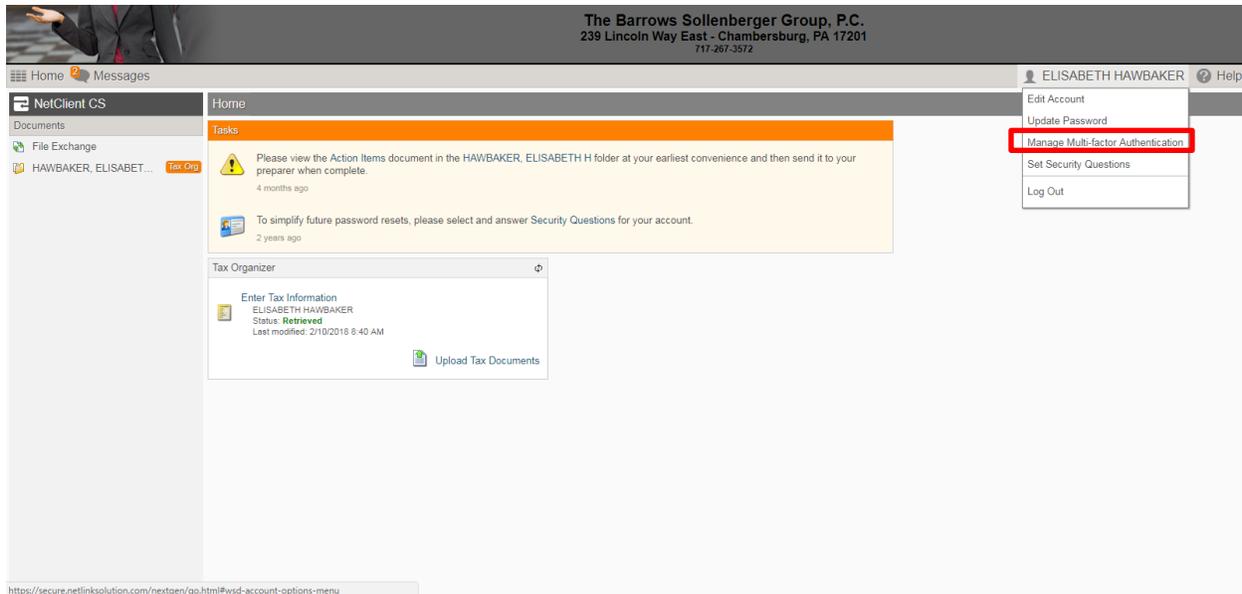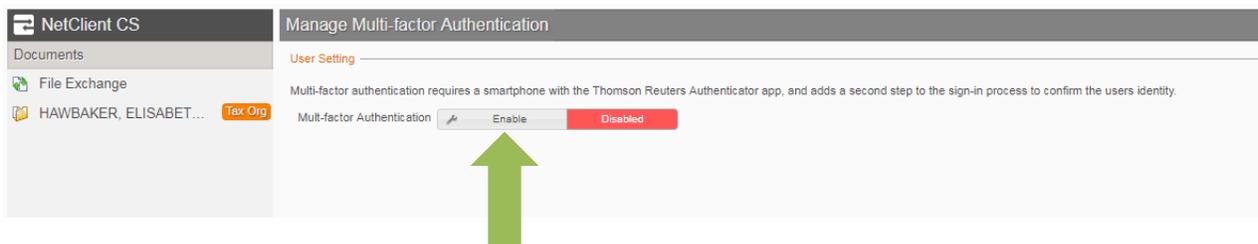
To activate the Multi-factor Authentication:

Log into your portal by going to http://63853.netlinksolution.com
- Click on your name in the upper right corner
    - o Select Manage Multi-factor Authentication from the drop down
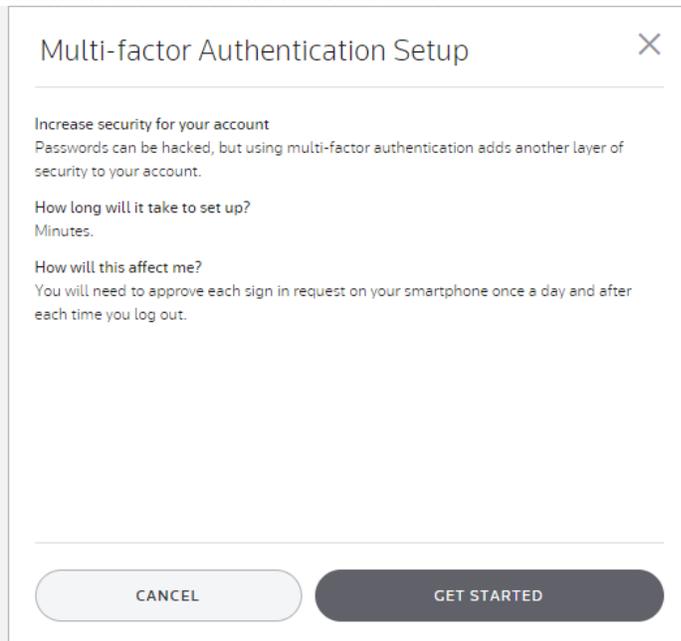

On the next screen, select Enable.

Enter your password in the pop up box and press Enter to confirm the change.
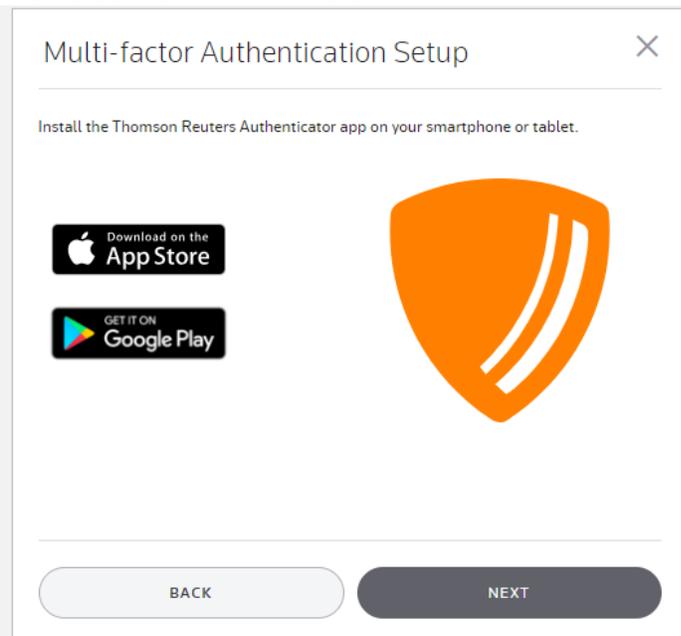
The next screen should look like this:


Select Get Started.
The next screen will look like this:

Download the Thomson Reuters Authenticator app on your device (smartphone or tablet). Search "Thomson Reuters Authenticator" in the *App Store* for Apple devices or *Google Play* for Samsung and Android devices or *Amazon App Store* for Amazon devices.
Once the Authenticator App is downloaded, hit Next on your computer screen.
Your computer will generate a QR code.

Multi-factor Authentication Setup ✕

Open the Thomson Reuters Authenticator app and scan the QR code below.
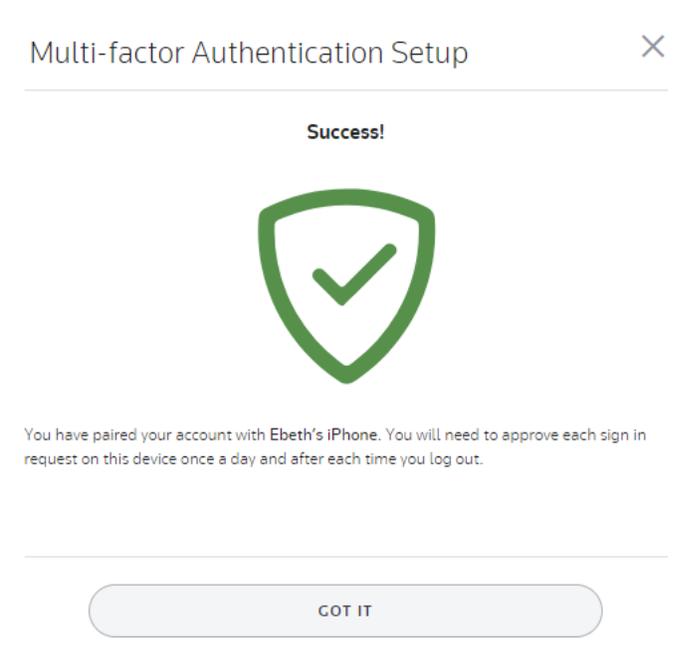

EXAMPLE

BACK
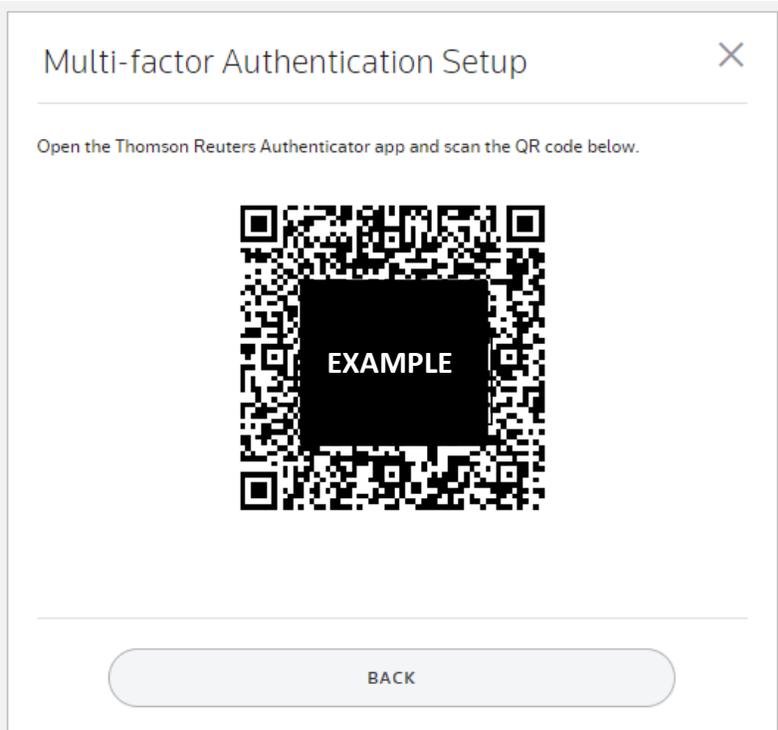
(This is an example only. Do not use this QR code for your log in. Your computer will generate a code specific to you).

Open your Thomson Reuters Authenticator app and scan the QR code that is on your computer screen.
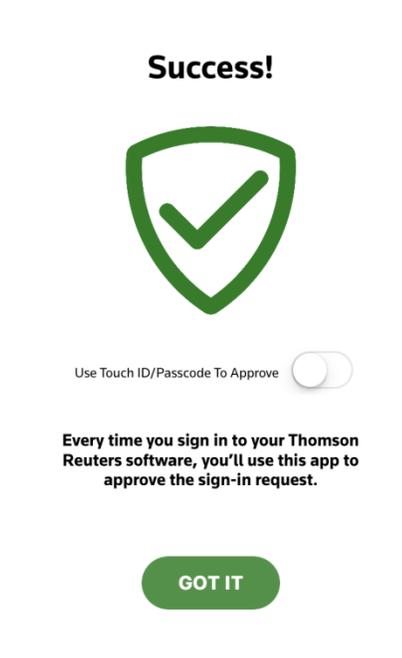
Both your computer and device screens should show success.

Computer:

Device (tablet or smart phone):

 App Store ᵃˡˡ �🔋 2:46 PM ⚡ ❋ 87%

Multi-factor Authentication Setup ✕

Success!

You have paired your account with Ebeth's iPhone. You will need to approve each sign in request on this device once a day and after each time you log out.

GOT IT

Success!

Use Touch ID/Passcode To Approve ⭘

Every time you sign in to your Thomson Reuters software, you'll use this app to approve the sign-in request.

GOT IT

If you have an Apple device, you may have the option to "Use Touch ID/Passcode to Approve."
See below for the difference between the 2 options (*Page 6**).
(If you have a Samsung device, you may have the option to set up "Use PIN to Approve Requests.")
You can enable either of these options later if you choose not to do it now (*Page 10*).

Select Got It on both screens.

The Enable tab on your computer screen should be green now.
You should also receive and automated email from Support (support@netlinksolution.com) letting you
know that "Your NetClient CS security settings have changed".
You do not need to respond to this email.

Your device may prompt you to sign in to Thomson Reuters (your Client Portal). This is the home screen
for this app.

Log out of your client portal by selecting Log Out from the drop down under your name.
    (It is very important that you log out each time. Just closing the browser or your computer does not
    log you out of your portal and anyone who can get access to your computer can get into your portal.
    Remember you have very important information stored on your portal that needs to be kept safe
    like your tax returns (including your social security number and bank account information if you
   elect to receive a direct deposit from the government on your taxes).
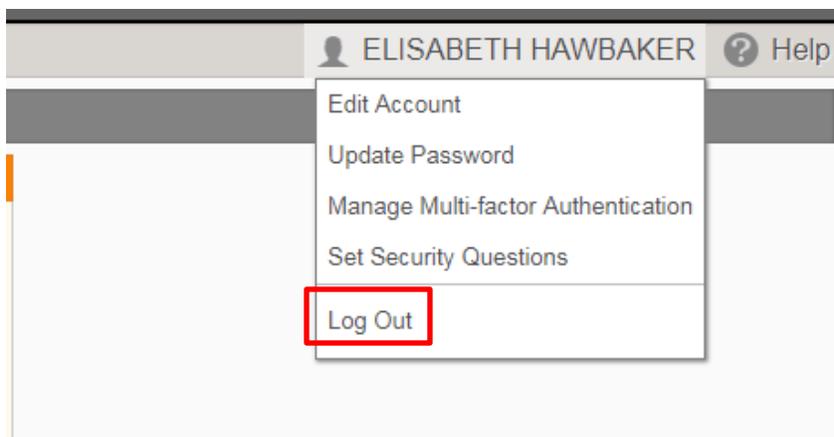
To log into your Client Portal with the Multi-factor Authentication:

When you attempt to log into Thomson Reuters (any time after you have the Multi-factor Authentication set up), you will get this notification on your computer:
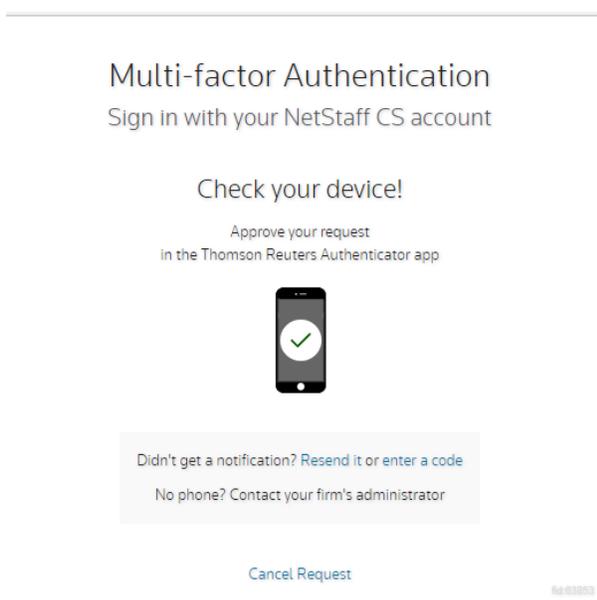
Open Thomson Reuters Authenticator app on your device to approve log in.

* If you haven't enabled the Touch ID option, your screen will look like this:
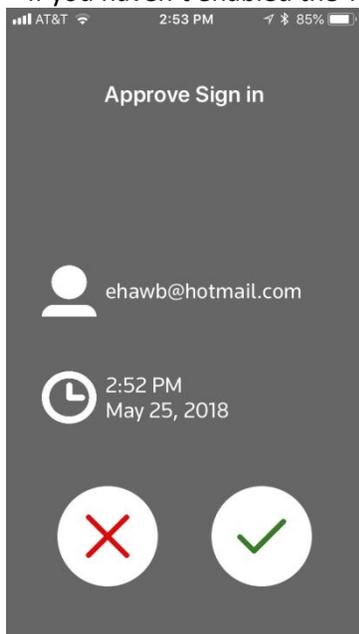
Select the green checkmark to approve the sign in.
(In the future, if you or your spouse are not currently trying to log into your portal and you get this notification on your device DO <u>NOT</u> hit the green check mark. Select the red "x" to deny access to your portal).

If you've enabled the Touch ID option your screen will look like this:
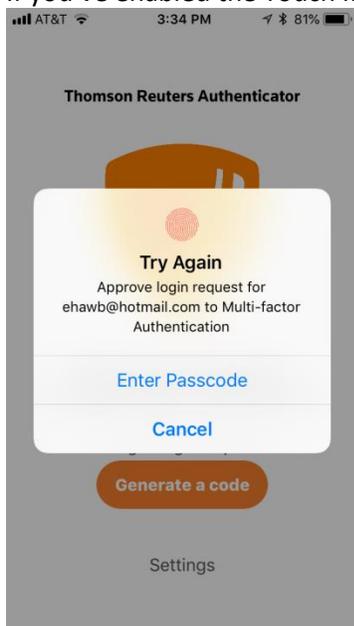
Use your fingerprint to approve the login request.
(In the future, if you or your spouse are not currently trying to log into your portal and you get this notification on your device DO <u>NOT</u> use your fingerprint to approve the login request. Select "Cancel" to deny access to your portal).

Note: If you are using a Samsung device and you turn on the Use PIN to Approve Requests, you will be prompted to enter the 4-digit PIN (you created during set up) to authorize the log in (Pg. 10 for details).

The Authentication process will time out after about 30 seconds. If this happens, you can resend the notification from your computer to your device by clicking Resend it.
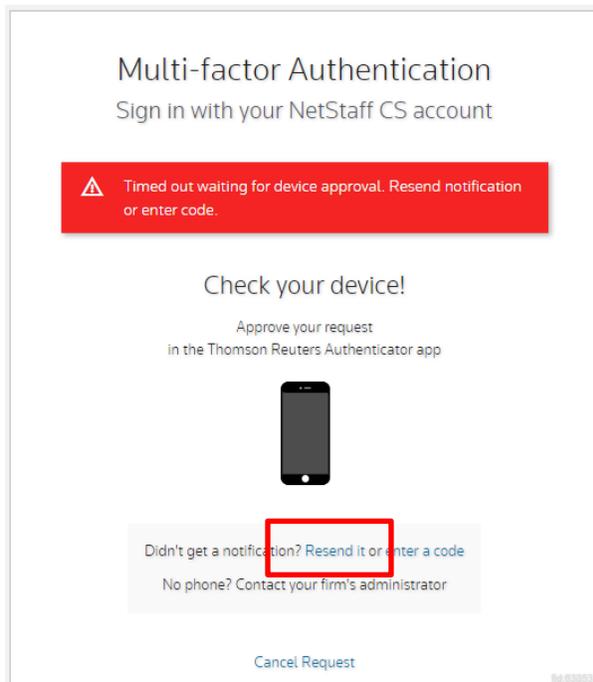
Then open the Thomson Reuters Authenticator app on your device and approve the log in.

Or you can generate a code from your device to enter into the computer by selecting Generate a code on your device:

Select enter a code on your computer screen.

Your computer screen will look like this:

On your device, select Generate a code.

Thomson Reuters Authenticator

**Sign in to your Thomson
Reuters software to get started.**

Not getting a request?

Generate a code

Settings

Your device will generate a code that you will need to type into your computer.

Device: Computer:

Generate Code   Done

257 768

Thomson Reuters ID

ehawb@hotmail.com

Add Account

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
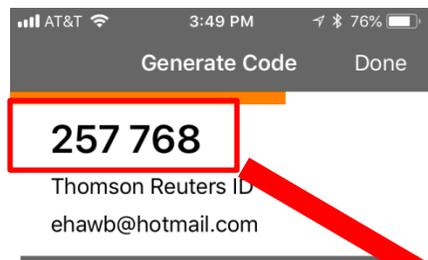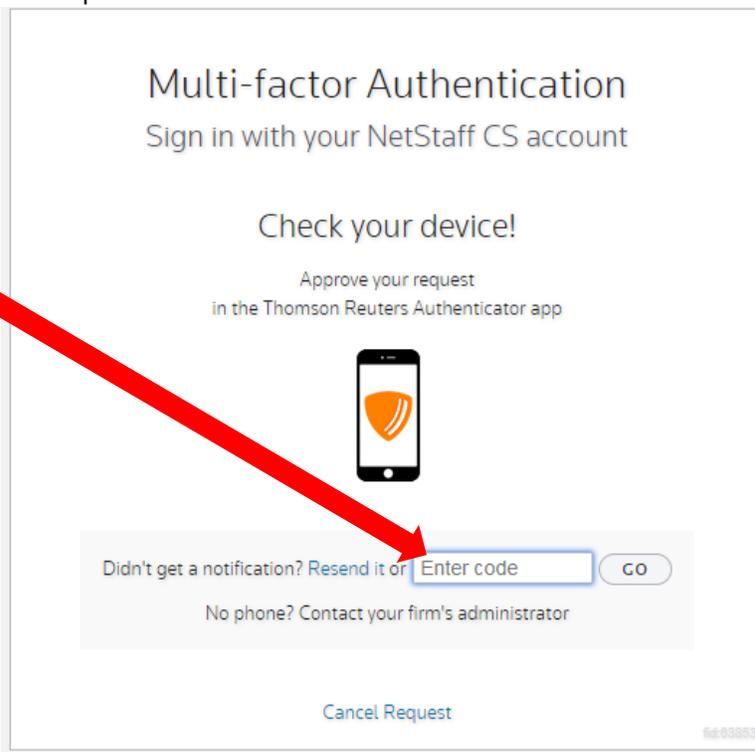
Codes are valid for 30 seconds. A new code is automatically generated every 30 seconds.

To turn the Use Touch ID/Passcode To Approve (Apple devices) option or Use PIN to Approve Requests (Samsung devices) option on or off:

Open your Thomson Reuters Authentication app on your device and select Settings.
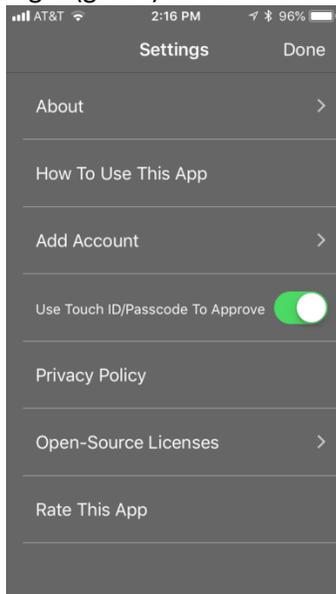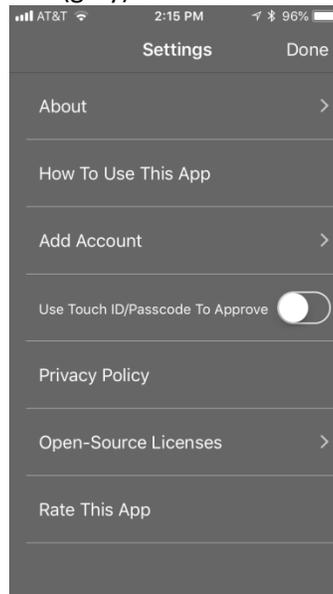

Press the Use Touch ID/Passcode To Approve switch *(On Samsung devices, this option will be called Use PIN to Approve Requests)*:

Right (green) to activate the Touch ID   Left (gray) to deactivate the Touch ID

Note: If you are using a Samsung device and you turn on the Use PIN to Approve Requests, you will be prompted to create a 4-digit PIN which you will need to key in to your device each time you log in.

If you do not have access to your device and need to log into your portal:

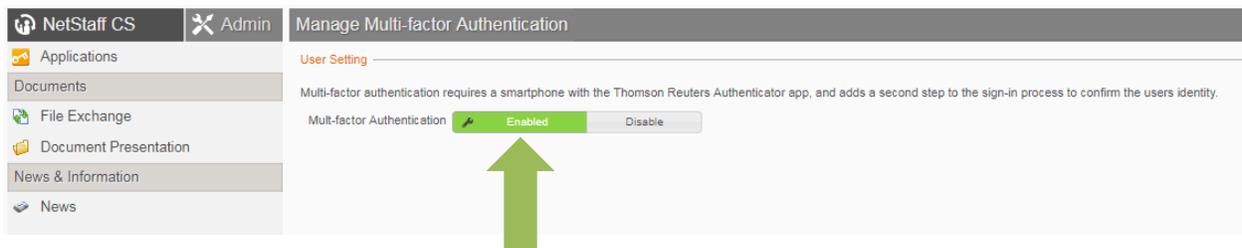You will need to contact us at 717 267 3572 to get a 24 hour temporary log in code.
We may ask you some questions to verify your identity. We want to ensure that we are giving access to your portal to the correct person!
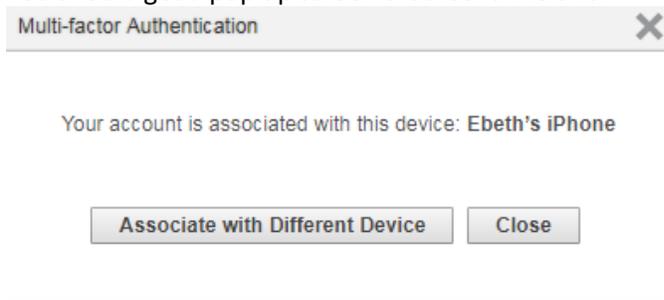
If you are replacing your device:

Log into your portal by going to http://63853.netlinksolution.com
Once you are logged in to your portal:
- Click on your name in the upper right corner
  - Select Manage Multi-factor Authentication from the drop down
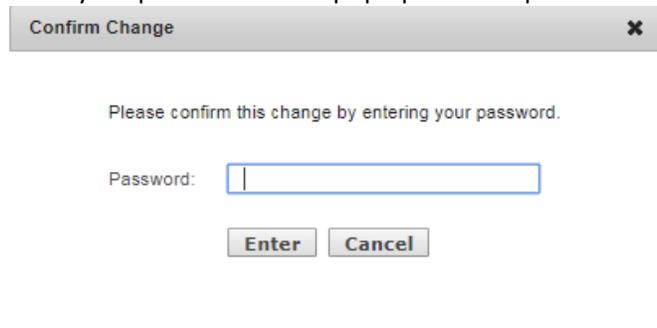 - On the next screen click Enabled

You should get a pop up screen that looks like this:

Select Associate with Different Device.
Enter your password in the pop up box and press Enter to confirm the change.

The next screen should be the Multi-factor Authentication set up. Follow the instructions starting on Page 2 of this document.

If you have lost or damaged your device:

You will need to contact us at 717 267 3572 to get a 24 hour temporary log in code.
We may ask you some questions to verify your identity. We want to ensure that we are giving access to your portal to the correct person!

If you have another device to activate, see the "If you are replacing your device" on Page 11.

If you do not enable another device, your Multi-factor Authentication will disable after temporary log in code expires. See Page 1 for instructions on how to reactivate the Multi-factor Authentication once you have your new device.