THOMSON REUTERS®

MULTI-FACTOR AUTHENTICATION - USER GUIDE

FOR TAX YEAR 2020

Last Updated: December 09, 2020

THOMSON REUTERS®

COPYRIGHT NOTICE

TABLE OF CONTENTS

CHAPTER 1: MULTI-FACTOR AUTHENTICATION

Thomson Reuters ***strongly recommends*** that you use multi-factor authentication to provide the highest level of security for your firm and client data.

WHAT DOES MULTI-FACTOR AUTHENTICATION DO?

Multi-factor authentication adds an additional layer of security that helps protect your firm's confidential data. Many of your online accounts or software applications are currently protected by a login and password. That password is the single factor in the authentication process — the way that those applications or services confirm your identity.

Multi-factor authentication adds at least one more layer of identity verification to that process so your protection against hacking and fraud attempts is stronger and more secure than a simple password. That additional layer can take many forms, such as a physical ID card, a digital confirmation code, or even your fingerprint. You use multi-factor authentication every time you pay a transaction using a debit card or withdraw cash from an ATM: your debit card is one factor and your PIN is another.

HOW DOES MFA WORK?

Thomson Reuters provides multi-factor authentication through the Thomson Reuters Authenticator application. After installing the mobile application on your smartphone and pairing that device with your application login credentials, you'll use the Authenticator to confirm your identity every time you log in to the Thomson Reuters RS system. You do so via a notification that is sent to the Authenticator mobile application, which you can quickly approve on your mobile device.

Software that works with Thomson Reuters Authenticator allows you to authenticate on three levels:

1. Something you **KNOW** (your login and password)
2. Something you **HAVE** (your mobile device with the Thomson Reuters Authenticator application)
3. Something you **ARE** (your fingerprint, if your device has Touch ID enabled)

Using multi-factor authentication makes it difficult for anyone else to use your login, as any would-be hacker must either have your mobile device at hand. If you decide to enable fingerprint authentication, hacking becomes impossible.

CHAPTER 2: USING THE THOMSON REUTERS AUTHENTICATOR APPLICATION

The Thomson Reuters Authenticator mobile application is part of our multi-factor authentication system, which is an additional layer of security that protects the sensitive data within your Thomson Reuters applications.

If you've enabled multi-factor authentication but you cannot access your mobile device, contact your firm's administrator — they can generate a 24-hour code that enables you to log in to your applications while you're unable to access the mobile application.

DOWNLOADING THE APPLICATION

The Thomson Reuters Authenticator application is available for both Apple and Android devices. You can click the appropriate button at this link:

https://tax.thomsonreuters.com/cs-professional-suite/security/authenticator-app/

You can also go to the applicable app store for your devices, and run a search for *Thomson Reuters Authenticator*.

Thomson Reuters has numerous mobile applications, so be careful to install the right one. The application with the icon shown below is the application you need to install. Click the icon, and then click **Install** on the application's page.

Figure 2:1

This icon will appear on your smartphone once the application is installed.

CHAPTER 3: SETTING UP MULTI-FACTOR AUTHENTICATION FOR YOUR LOGIN

Multi-factor authentication provides the highest level of security for your login. Follow the steps below to set up multi-factor authentication to verify your RS login using a mobile device.

REQUIRED MULTI-FACTOR AUTHENTICATION

If your firm ***requires*** multi-factor authentication, you will be prompted to set it up the first time you log in. Follow these steps.

1. Enter your login and password.
2. Follow the setup instructions to set up multi-factor authentication. These require you to download and install the Thomson Reuters Authenticator application to your mobile device and scan a QR code. For more information, follow the instructions below.

OPTIONAL MULTI-FACTOR AUTHENTICATION

If your firm has made multi-factor authentication optional, you will not be prompted to set it up. To enable multi-factor authentication for your login, follow these steps.

1. Log in to the RS system.
2. Select **Options** in the upper-right corner.

3. Select **MFA Settings** from the left menu.

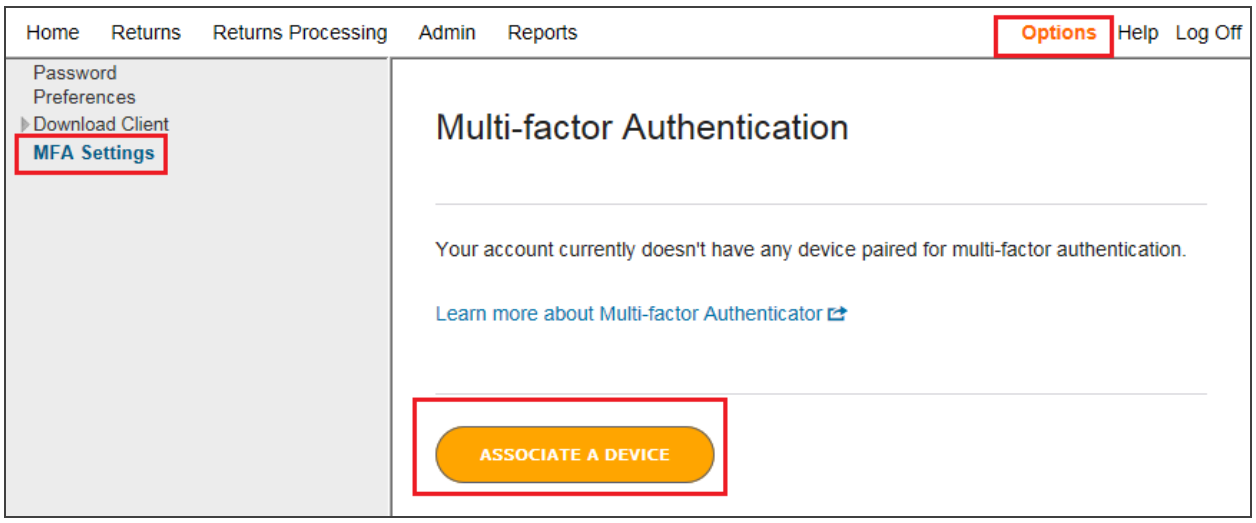

Figure 3:1

4. Click **Associate a Device**.

5. The following screen appears. Click **Set Up Multi-Factor**.

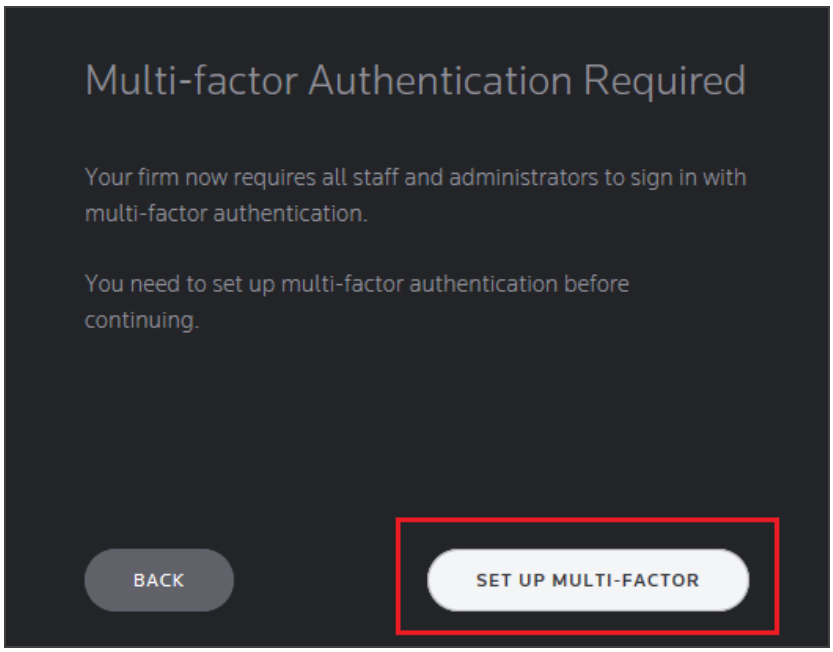

Figure 3:2

6. Click **Get Started** on the next screen.

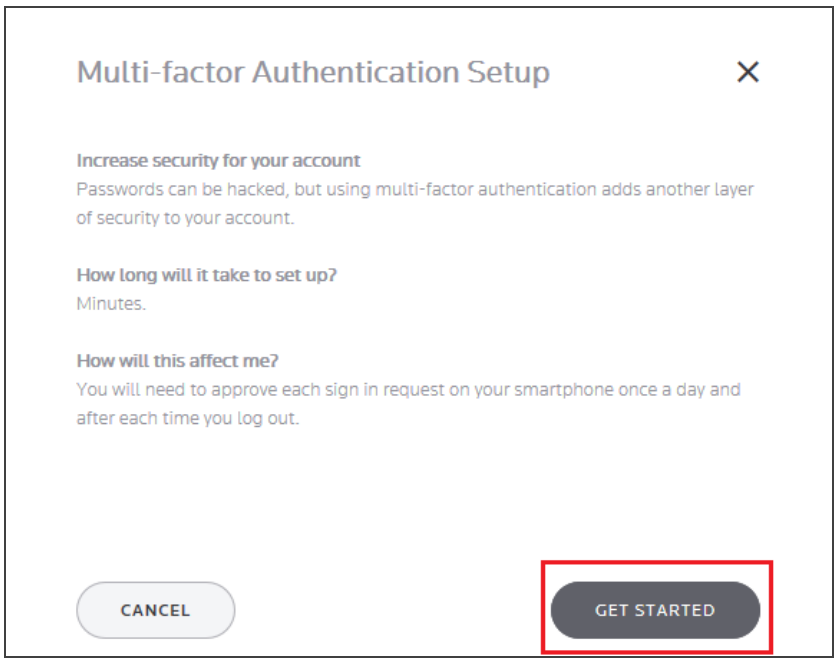

Figure 3:3

7. If you have not already done so, the next screen instructs you to download and install the Thomson Reuters Authenticator application to your mobile device. Click **Next**.

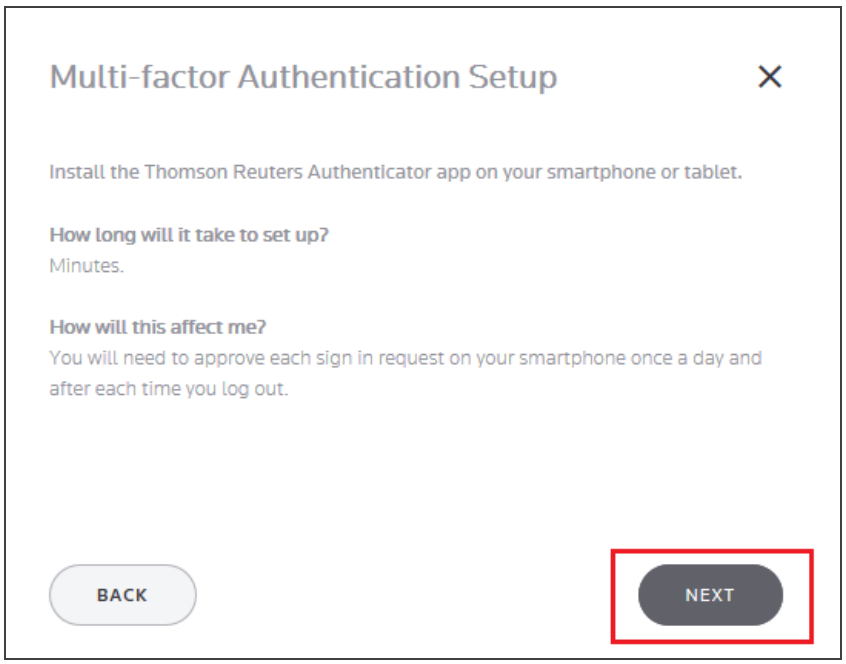

Figure 3:4

8. Click the appropriate button for your mobile device, and install the application. Then click **Next**.

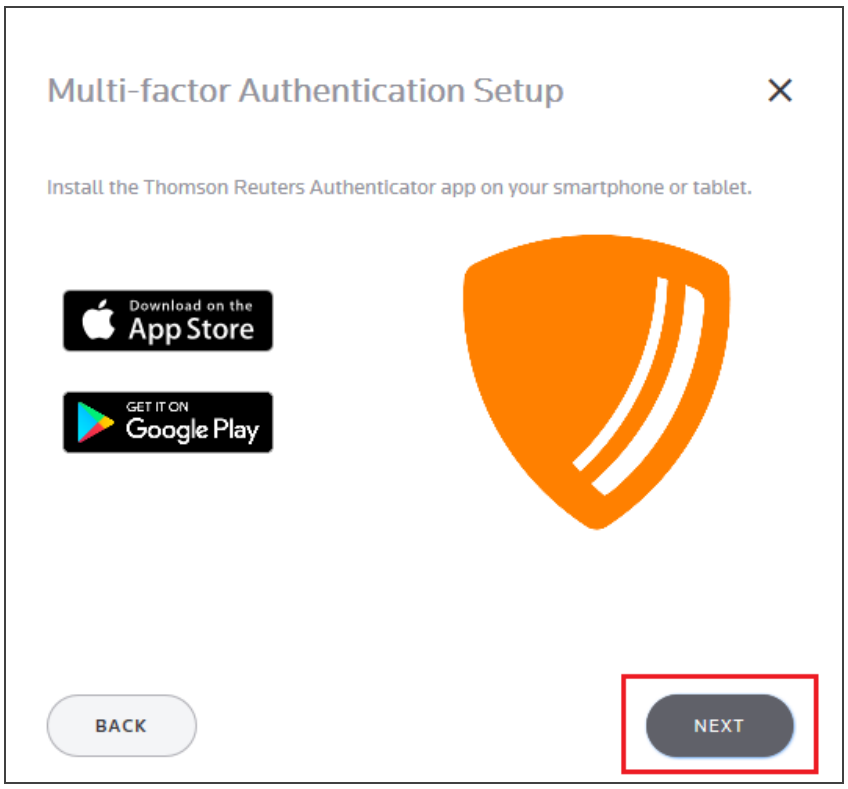

Figure 3:5

9. Follow the setup instructions to configure multi-factor authentication, which require you to download and install the Thomson Reuters Authenticator application to your mobile device and scan a QR code. See **Pairing Your Device with Your Login Credentials (page 9)**.

If you have previously used the Authenticator application with another account, you must access the application's settings before you can scan. Open the application, tap **Settings**, tap **Add Account**, then scan the QR code.

CHAPTER 4: PAIRING YOUR DEVICE WITH YOUR LOGIN CREDENTIALS

To begin using multi-factor authentication with the Thomson Reuters login credentials that you use to access your applications, you need to link your mobile device with that account.

1. After you install the Authenticator application on your mobile device, click **Next** in the setup wizard to display the QR code.

Figure 4:1

2. On your mobile device, tap the **Scan QR Code** button and point the camera at the QR code in the setup wizard. Your mobile device will automatically scan the code.

3. You will see a **Success** screen on your mobile device, and the following screen will appear on your computer.

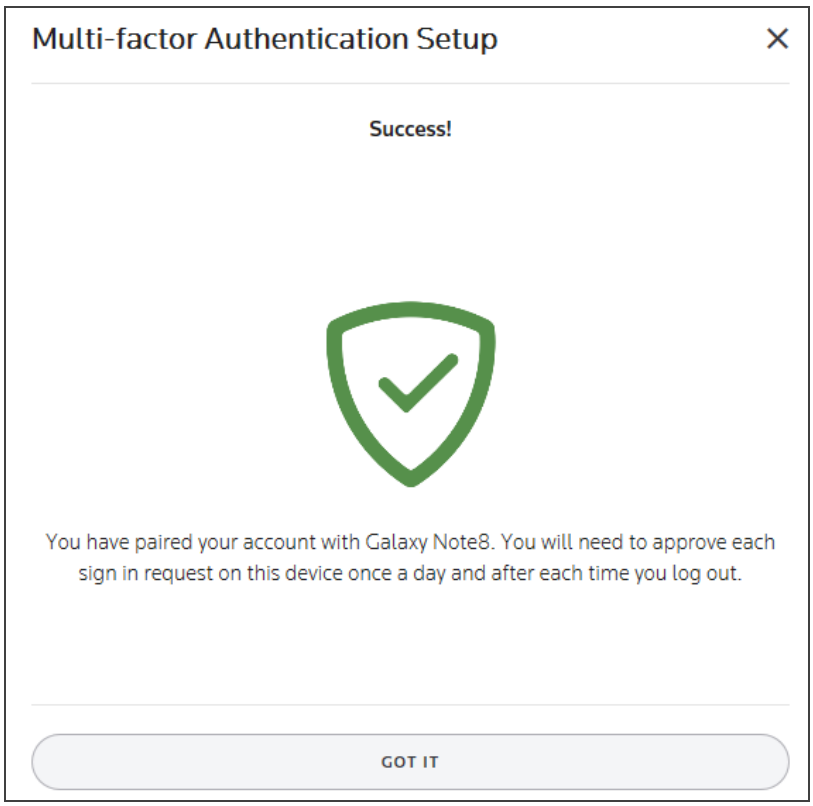

Figure 4:2

4. Click **Got It**. A screen appears showing the device now associated with your login.

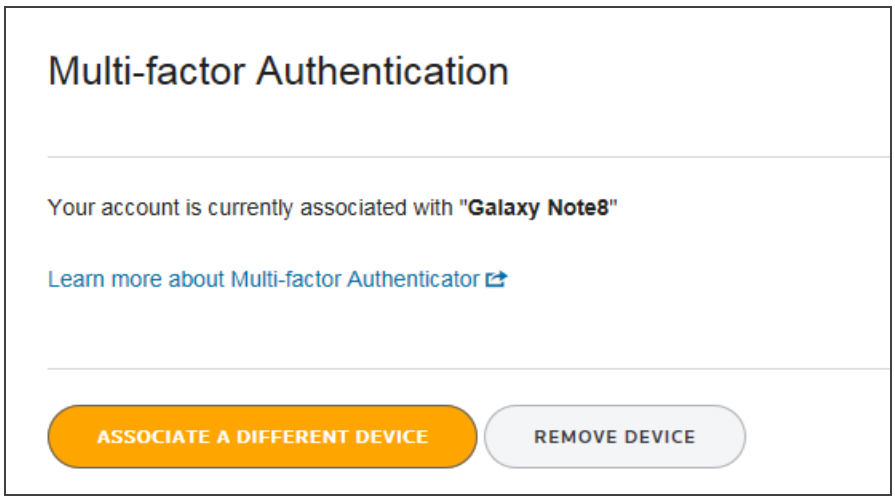

Figure 4:3

5. You can click **Associate a Different Device** to add another device for your login credentials. You will go through the same steps for each device you add.

6. After your mobile device scans the code, the Thomson Reuters Authenticator mobile application is successfully paired to your account. You will use the mobile application each time you sign in to your Thomson Reuters applications.

If you choose to use your fingerprint to approve authentication requests, you must enable screen lock, and at least one fingerprint has to be registered in your device's settings.

VERIFYING YOUR IDENTITY WHEN LOGGIN IN

If you have multi-factor authentication enabled for your account, you'll use the Thomson Reuters Authenticator mobile application to verify your identity when you log in to your Thomson Reuters applications.

1. Open your Thomson Reuters application and sign in using the appropriate login credentials.
2. On your mobile device, you will receive a notification from the Thomson Reuters Authenticator that prompts you to approve or deny the sign-in attempt.

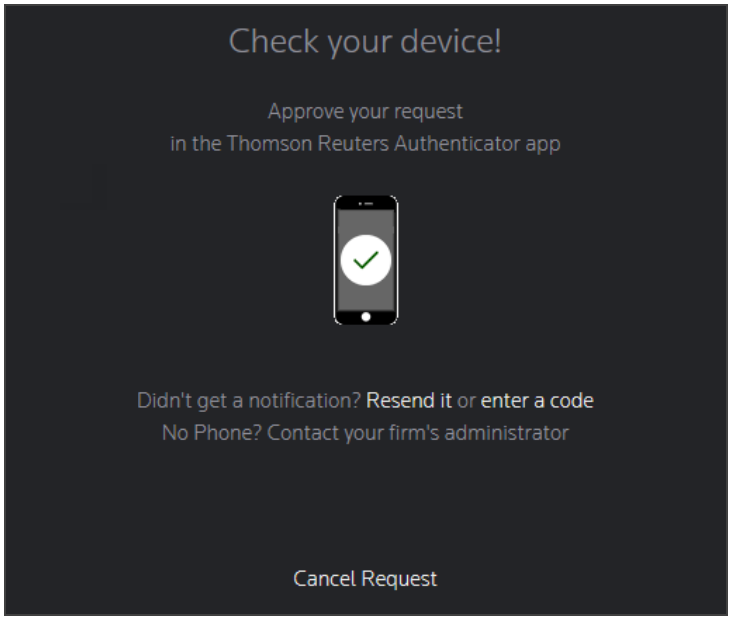

Figure 4:4

3. Tap **Approve** or the green check mark (✓)in the mobile application to confirm your sign-in.

If you did not receive an approval request through the mobile application, you can generate a code from the application to enable you to log in.

1. Open the mobile application.
2. Tap the **Generate a code** button.
3. On the **Generate Code** screen in the mobile application, you'll see a six-digit number listed for the Thomson Reuters application that you wish to access.

4. To sign in to that application, enter the generated number in the application sign-in screen.

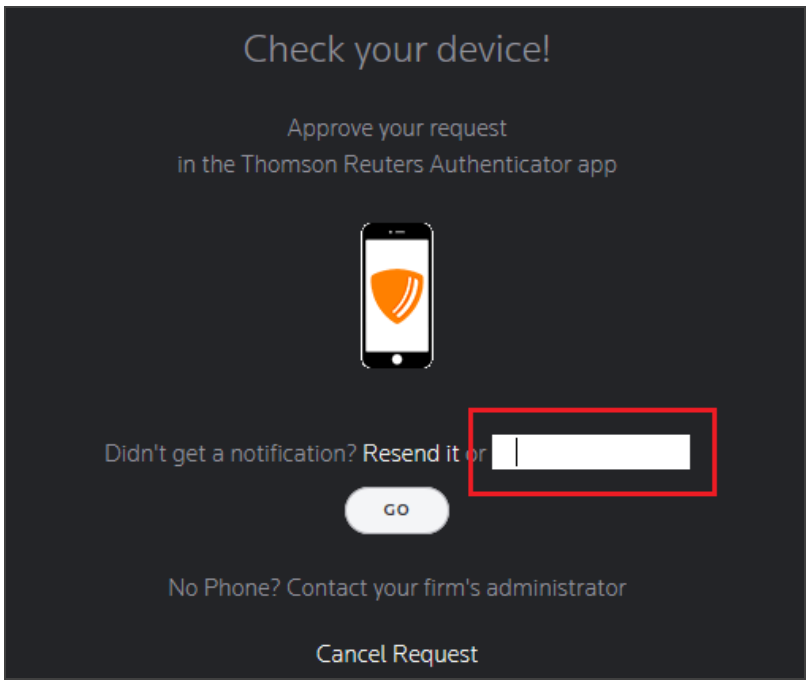

Figure 4:5

5. These codes expire and regenerate every 30 seconds, so act quickly!

SWITCHING MOBILE DEVICES FOR MULTI-FACTOR AUTHENTICATION

To change the mobile device that you use to log in with multi-factor authentication, follow these steps.

1. Click **Options** in the upper-right corner of the screen.
2. Select **MFA Settings** from the left menu.

3. Click the **Associate With A Different Device** button.

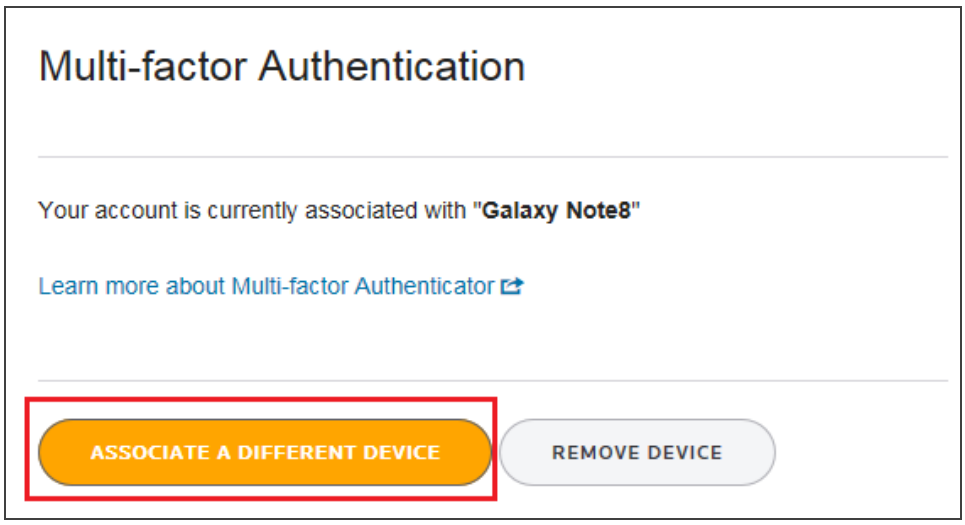

Figure 4:6

If your firm has made multi-factor authentication optional, click the **Remove Device** button, and then add a new device.

4. Enter your password, and click **Submit**.
5. If multi-factor authentication is ***optional***, click the **Add Multi-Factor Authentication** button. If not, continue to the next step.
6. Follow the setup instructions to configure multi-factor authentication, which require you to download and install the Thomson Reuters Authenticator application to your mobile device and scan a QR code.

If you have previously used the Authenticator app with another account you must access the application's settings before you can scan. Open the application, tap **Settings**, tap **Add Account**, then scan the QR code.

DISABLING MULTI-FACTOR AUTHENTICATION

We recommend that you use multi-factor authentication to provide the highest level of security for your login. However, if your firm has made multi-factor authentication optional, you can follow these steps to disable multi-factor authentication for your login.

1. Click **Options** in the upper-right corner of the screen.
2. Select **MFA Settings** from the left menu.

3. Click the **Remove Device** button.

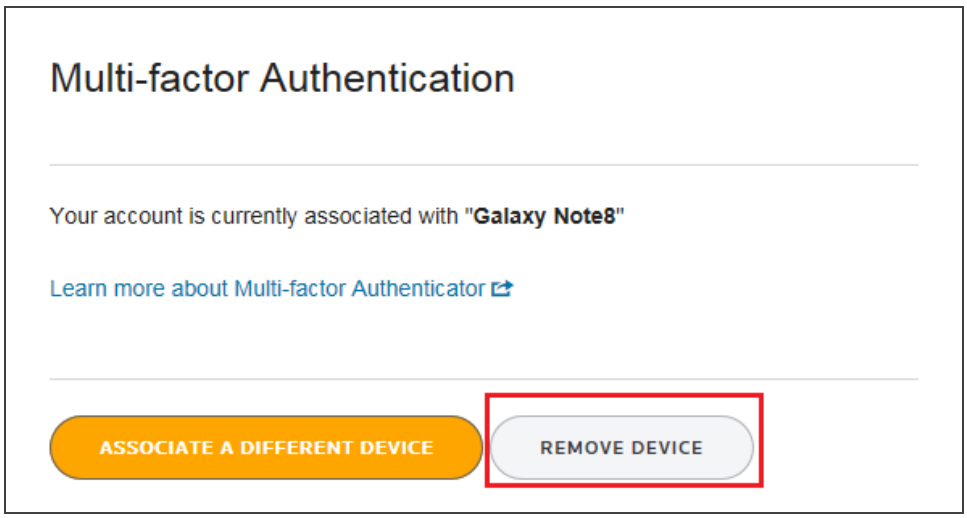

Figure 4:7

4. With multi-factor authentication disabled, you will no longer need to verify your login using your mobile device.

If you want to enable multi-factor authentication again, follow the steps above and click the **Add Multi-Factor Authentication** button. Then enter your password and follow the setup instructions to configure multi-factor authentication, which require you to download and install the Thomson Reuters Authenticator application to your mobile device and scan a QR code.

CHAPTER 5: LOGGING IN WITHOUT ACCESS TO YOUR MOBILE DEVICE

When you cannot log in using multi-factor authentication — for example, if you left your phone at home, or your phone is lost or damaged — your RS Administrator can generate a temporary, 24-hour numerical code to enable you to log in.

You can use this numerical code one time only. It expires after one use or 24 hours after issuance, whichever comes first.

CHAPTER 6: TROUBLESHOOTING

INTERNET EXPLORER

If the QR Code is not displayed or Firm Admins are not able to generate 24-hour code, please make sure to have the following settings in Internet Explorer.

At this time, MFA works only in Internet Explorer.

1. Navigate to **Internet Options > Security > Trusted Sites**.
2. Select **Custom level**.

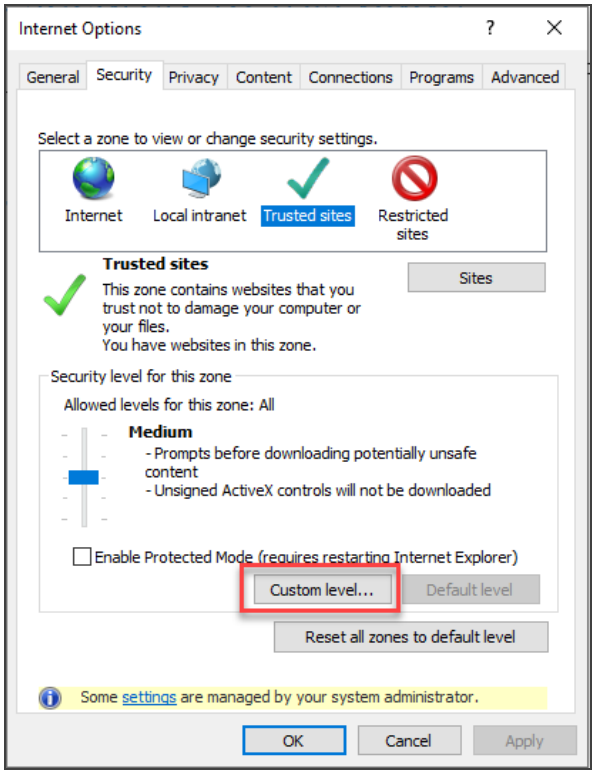

Figure 6:1

3. Scroll down until you reach the **Miscellaneous** section. When you reach the line for **Access data sources across domains**, select **Enable**.

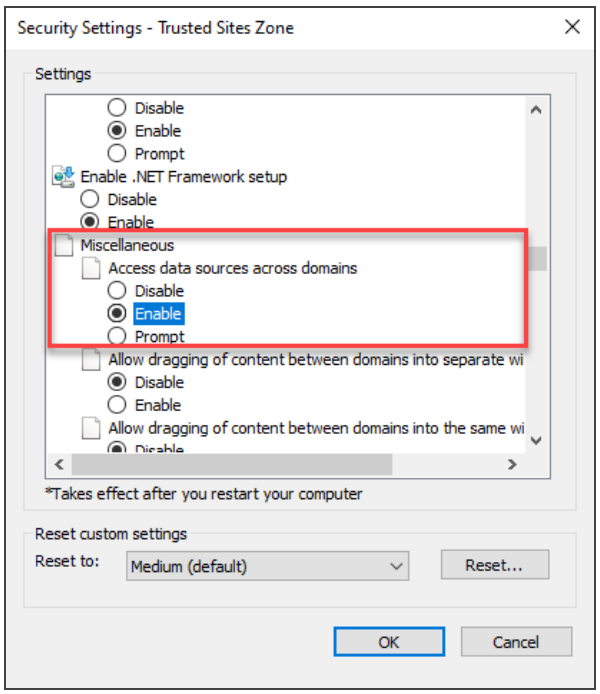

Figure 6:2

4. Close the browser, and then reopen. Try to login with MFA.