THOMSON REUTERS®

MULTI-FACTOR AUTHENTICATION - ADMINISTRATOR GUIDE

FOR TAX YEAR 2021

Last Updated: October 06, 2021

THOMSON REUTERS®

COPYRIGHT NOTICE

TABLE OF CONTENTS

CHAPTER 1: MULTI-FACTOR AUTHENTICATION: INTRODUCTION

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

WHAT IS MULTI-FACTOR AUTHENTICATION?

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.

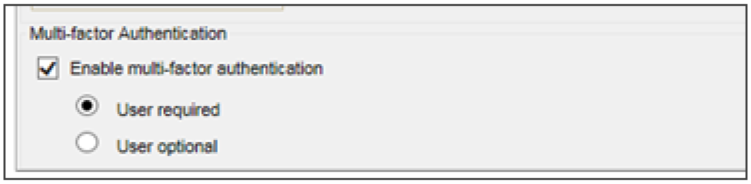
CHAPTER 2: SETTING UP AND IMPLEMENTING MFA IN YOUR FIRM

By default, MFA is an optional feature that individual users can opt into by enabling it for their own accounts. If desired, RS administrators can enable a setting that requires that all staff members log in with MFA.

We ***strongly recommend*** that you use MFA to provide the highest level of security for your firm and client data. MFA requires a mobile device with the Thomson Reuters Authenticator application installed.

By default, MFA is ***optional***. Firms can set it up if they choose. You can make MFA a required security feature for staff. This setting requires the administrator rights to change the setting.

1. Select **Admin > Firm Config**.
2. Select the **Security Options** tab.
3. Under the heading **Multi-factor Authentication**, select the options you wish to use.



Multi-factor Authentication

☑ Enable multi-factor authentication

● User required

○ User optional

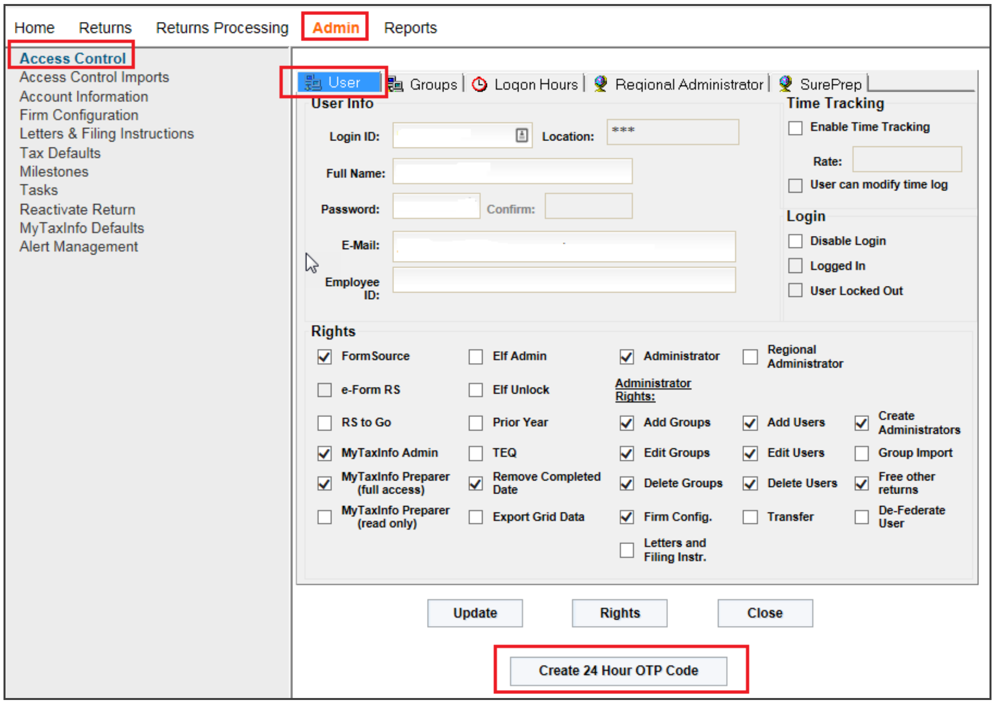
Figure 2:1

- **Required**: When MFA is required, users will be prompted to set up MFA at their next login, after which they must use a mobile device with the Thomson Reuters Authenticator application to log in to the RS system.
- **Optional**: When MFA is optional, users will not be prompted to set up MFA, but they can opt in to using the Thomson Reuters Authenticator application to provide an additional layer of security for their RS logins.

CHAPTER 3: GENERATING A TEMPORARY LOGIN CODE

When a user cannot log in using MFA — such as when users leave their phones at home or a phone is damaged — users with administrative permissions can generate a temporary, 24-hour numerical code to enable the user to log in.

1. Go to **Admin > Access Control**.
2. Select the user who needs the temporary code.
3. Select **User**.
4. At the bottom of the screen, locate the button labeled **Generate 24-Hour OTP for this User**.
5. Click the button. Generating the code disables any codes previously located for that user's account.



User Info

Login ID:
Location: ***
Full Name:
Password:
Confirm:
E-Mail:
Employee ID:

Time Tracking

□ Enable Time Tracking

Rate:

□ User can modify time log

Login

□ Disable Login

□ Logged In

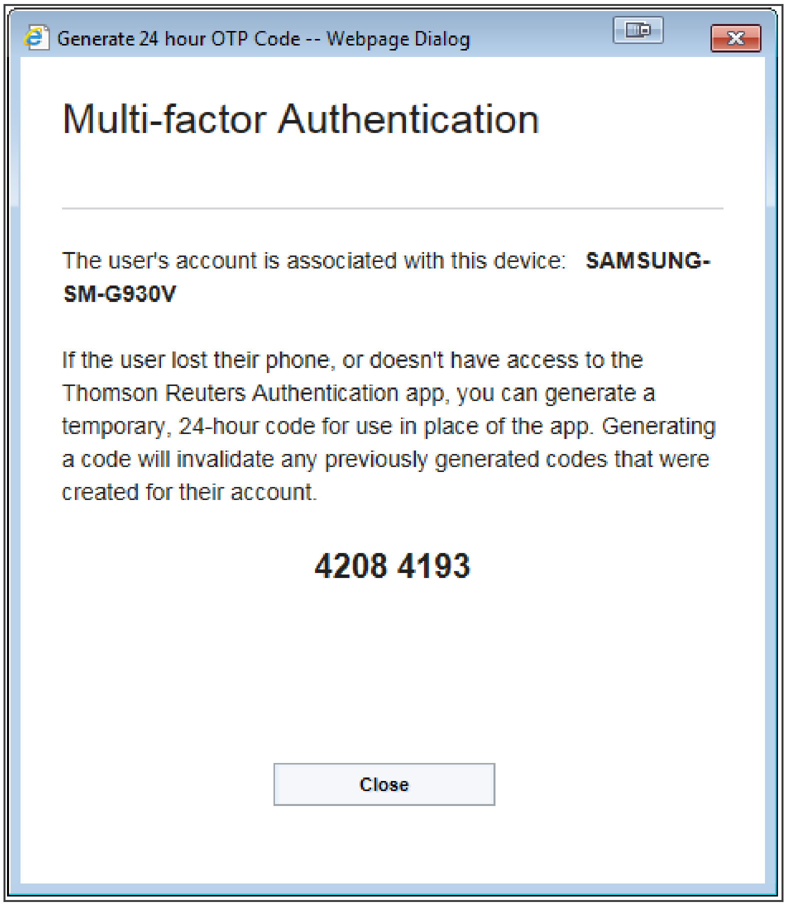
□ User Locked Out

Rights

☑ FormSource	□ Elf Admin	☑ Administrator	□ Regional Administrator	
□ e-Form RS	□ Elf Unlock	Administrator Rights:		
□ RS to Go	□ Prior Year	☑ Add Groups	☑ Add Users	☑ Create Administrators
☑ MyTaxInfo Admin	□ TEQ	☑ Edit Groups	☑ Edit Users	□ Group Import
☑ MyTaxInfo Preparer (full access)	☑ Remove Completed Date	☑ Delete Groups	☑ Delete Users	☑ Free other returns
□ MyTaxInfo Preparer (read only)	□ Export Grid Data	☑ Firm Config.	□ Transfer	□ De-Federate User
		□ Letters and Filing Instr.		

Figure 3:1

6. A dialog appears to the right with the temporary code.



Multi-factor Authentication

The user's account is associated with this device: **SAMSUNG-SM-G930V**

If the user lost their phone, or doesn't have access to the Thomson Reuters Authentication app, you can generate a temporary, 24-hour code for use in place of the app. Generating a code will invalidate any previously generated codes that were created for their account.

4208 4193

Figure 3:2

7. Send the code to the user.

8. Click **Close**.