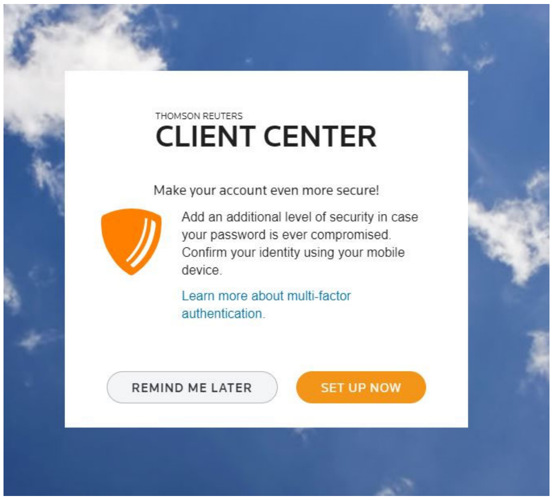


THOMSON REUTERS
CLIENT CENTER

Make your account even more secure!

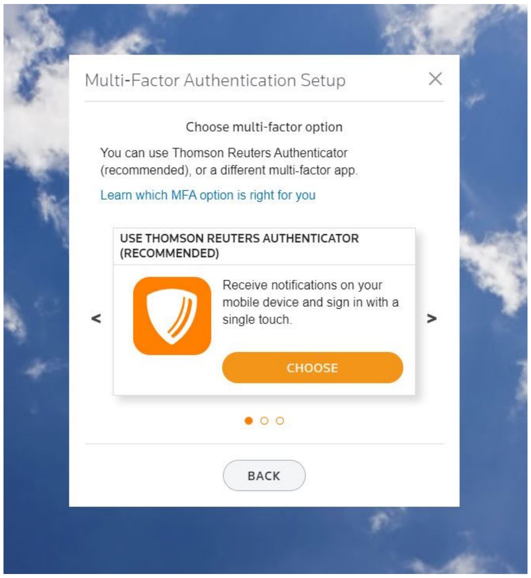
Add an additional level of security in case your password is ever compromised. Confirm your identity using your mobile device.

Learn more about multi-factor authentication.

Multi-Factor authentication (MFA) allows you to use a mobile device to add an additional layer of security to your online account. After it is set up, anyone trying to gain access to your account will need both your password and the mobile device that is linked to access your account.

To set up Multi-Factor authentication, begin by going to https://onvio.us/clientcenter/en/us/

Then enter your username and password. If you have not already set up Multi-Factor authentication, you will see the reminder screen shown to the left. Select the orange "Set Up Now" In order to begin the setup process.



Multi-Factor Authentication Setup

Choose multi-factor option

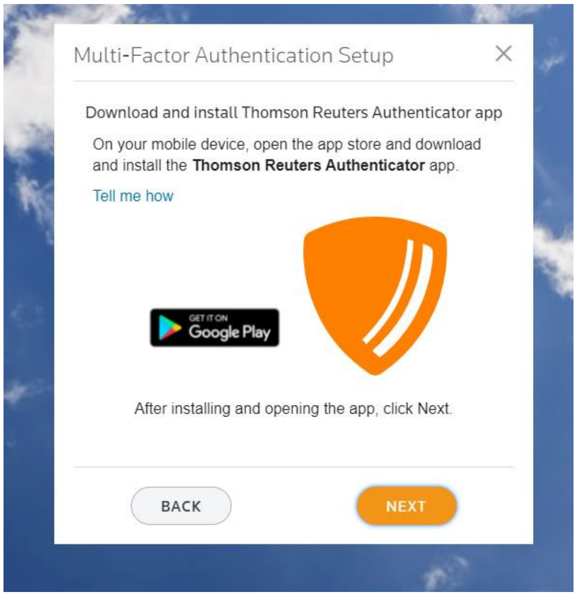
You can use Thomson Reuters Authenticator (recommended), or a different multi-factor app.

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.

The first step is to choose the method to use for authentication. We suggest using the first option. This uses the Thomson Reuters Authenticator app. The following instructions will be for setting up MFA with the Thomson Reuters app. We do not have support in place to help you if you choose one of the other methods.



Multi-Factor Authentication Setup

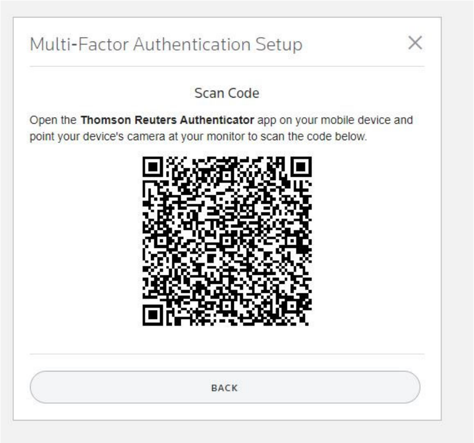
Download and install Thomson Reuters Authenticator app

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.

Once you choose the method, you will be directed to download the Thomson Reuters authenticator app onto the mobile device that you would like to use. You can find it in either the Google Play store or the Apple store. Just search for "Thomson Reuters Authenticator" and choose the app with the orange shield icon. Once you have found and installed the app go to the next page of the setup process.

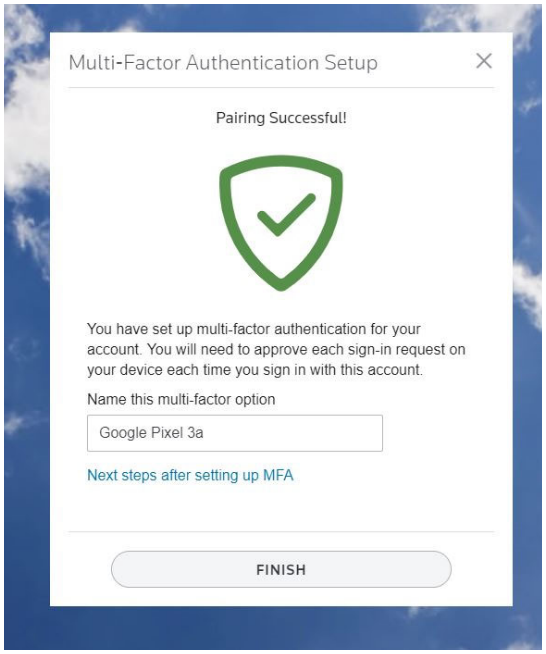


Scan Code

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

The next step will link the app on your phone to your online account. You will need to open up the app on your phone and use it to take a picture of the QR code on the computer screen. The app should automatically open to the right screen, but if it doesn't look like it is trying to take a picture, look in the upper right hand corner for a little + which should open up the scanner/camera.

You don't have to click anything to scan the code. Just hold the phone up so that the QR code shows in the view screen on the phone.

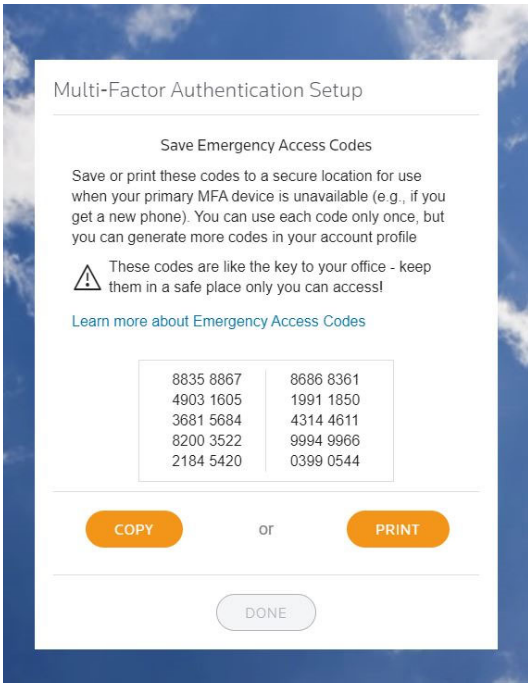

Multi-Factor Authentication Setup
Next steps after setting up MFA
FINISH

Pairing Successful!

You have set up multi-factor authentication for your account. You will need to approve each sign-in request on your device each time you sign in with this account.

Name this multi-factor option: Google Pixel 3a

Once you scan the QR code, you need to name the device that you are using. Name it something that you will recognize, so that someday when you need to change devices it is easy to tell the new and old one's apart. If all it says is iPhone, for example, it will be hard to tell which label belongs to the new phone if you add another iPhone when you next upgrade devices.


Multi-Factor Authentication Setup
Learn more about Emergency Access Codes
COPY
or
PRINT
DONE

Save Emergency Access Codes

Save or print these codes to a secure location for use when your primary MFA device is unavailable (e.g., if you get a new phone). You can use each code only once, but you can generate more codes in your account profile

⚠ These codes are like the key to your office - keep them in a safe place only you can access!

8835 8867	8686 8361
4903 1605	1991 1850
3681 5684	4314 4611
8200 3522	9994 9966
2184 5420	0399 0544

After you name your device, the last step that you will be prompted to do is to copy a list of emergency access codes. These codes are each good for a one time access to your online account. Keep at least a couple of them in a secure place so that you can get into your account if you change or lose your phone.

If you don't have a code available and you change phones without adding the new phone, you will be locked out of your account. The authentication process is linked to your actual physical device, not to your cell number, so it will not automatically swap to your new phone.

If you do get locked out, give us a call and we can help you get a new one-time access code.

See the tutorial on "Changing MFA devices", for info on how to change devices without getting locked out of your account.