Enabling Multi-Factor Authentication (MFA) for the NIFC Org

These workflows cover MFA logins for both mobile and desktop use. Having trouble? See this help document.

Preparation

Before you start, you will need:

- NIFC AGOL credentials (ex. jsmith_nifc)
- A primary mobile device
- The Microsoft Authenticator app installed on your primary mobile device
- A smidge of patience and a dash of confidence

Install Microsoft Authenticator on your **primary mobile device**(s) from the App Store, Google Play, or your agency's app hub. You do not need to create an account in the Microsoft Authenticator app. If you are using the Authenticator app for the first time you may need to click the "Scan a QR code" button when you begin using the app.

Multiple mobile devices can be used to provide MFA authentication codes for ArcGIS Online. You can use a personal device, work device, shared office tablet, etc., but **you will need to have access to the mobile device whenever you log in to the NIFC Org**. Unfortunately, there is no way to set up MFA without a mobile device.

Have the mobile device(s) with the Microsoft Authenticator app available for the following steps.

Click here to jump to the SINGLE DEVICE workflow (page 8).

Click here to jump to the MULTIPLE DEVICES workflow (page 2).

Multiple Devices Workflow

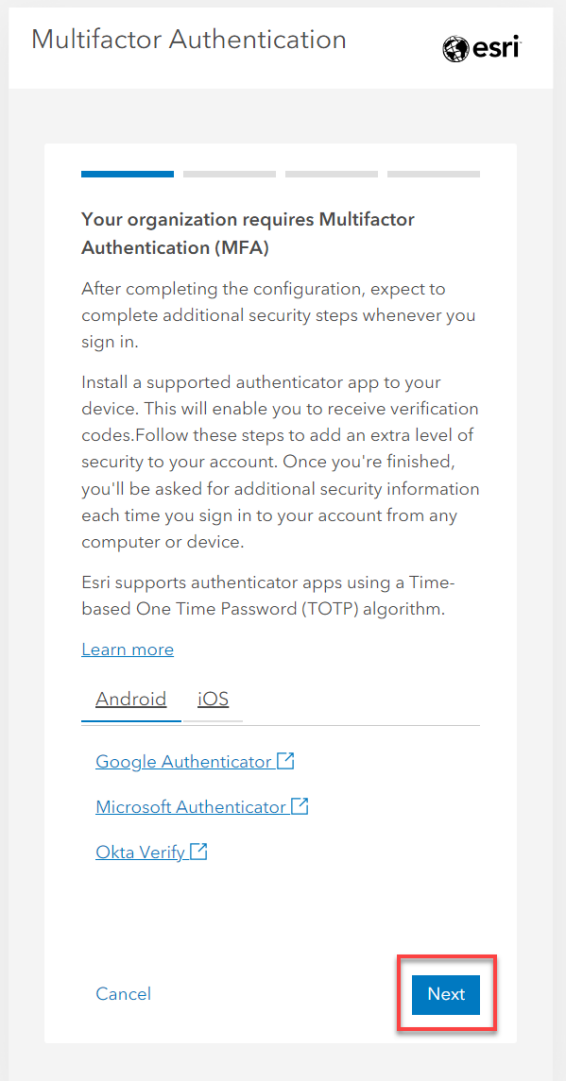
Click here to jump to the SINGLE DEVICE workflow (page 8).

1. **On your computer or secondary mobile device**, open a web browser and log in to your NIFC Org account at www.arcgis.com. After you login to AGOL the MFA setup process will automatically begin in the browser.

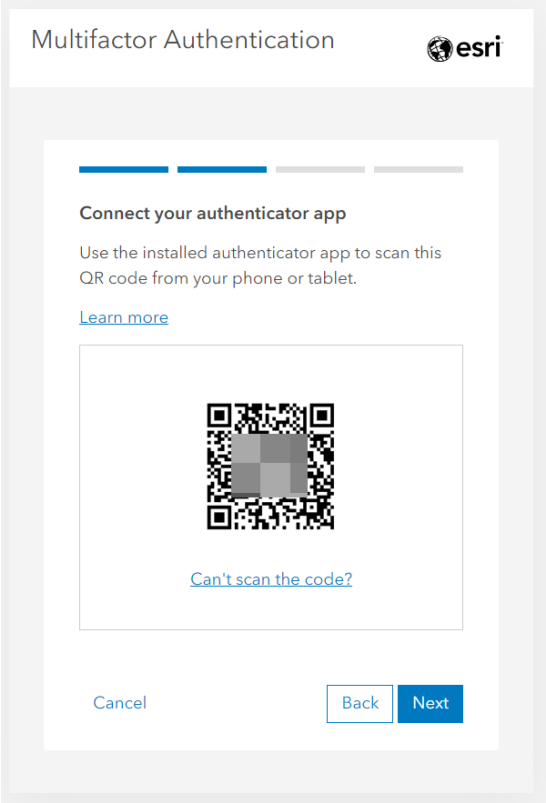
2. **On your primary mobile device**, open up the Microsoft Authenticator app

3. Multifactor Authentication dialog will begin on the **computer/secondary device**.

   Click Next



4. A QR code will appear. **TAKE A SCREENSHOT OF THE QR CODE.** You will need this QR code later if you want to add another device (if you do not do this, then you will need to self-reset your MFA via the Support Request Form). Treat this QR code as a password and store it appropriately. (Note that the QR code displayed to the right is obscured for security.)

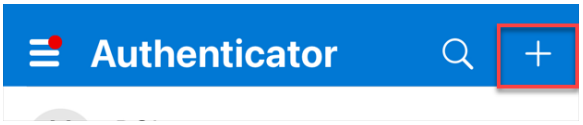


DO NOT USE YOUR DEVICE'S CAMERA APP TO SCAN THIS QR CODE!

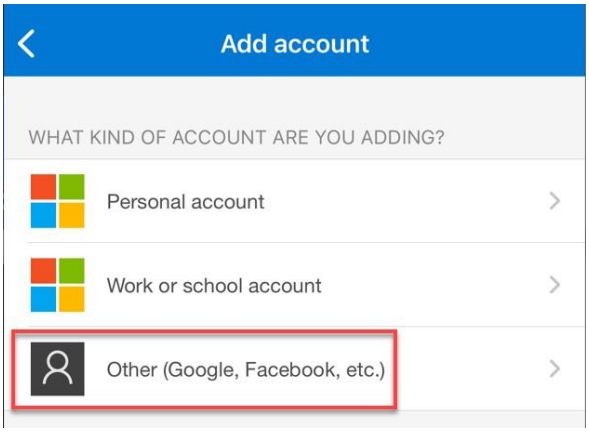
You will scan it from within the Authenticator app (Steps 5-7).

DO NOT click Next yet. If you did, click Back to return to the QR code page.

5. On the **primary mobile device**, open the Authenticator app (Microsoft Authenticator is the preferred choice). **Click the + to add a new account.**

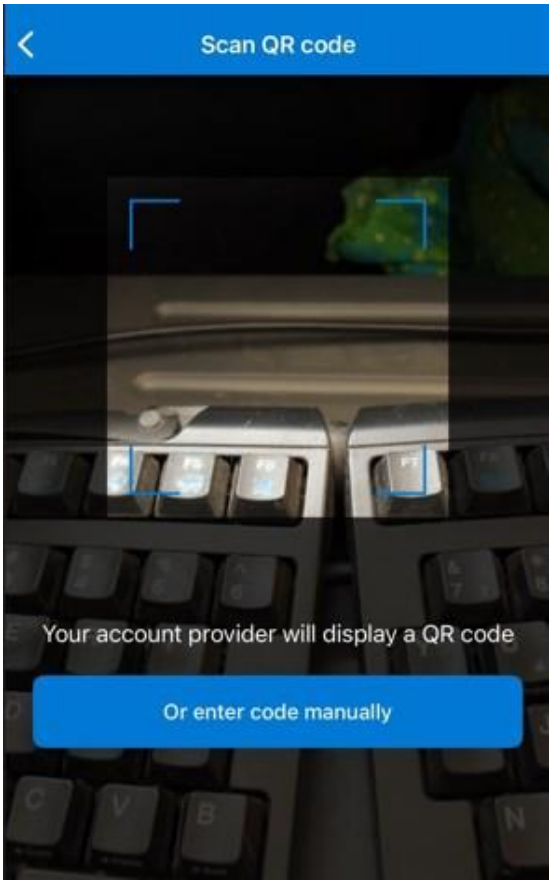


6. Add an "Other" type account.



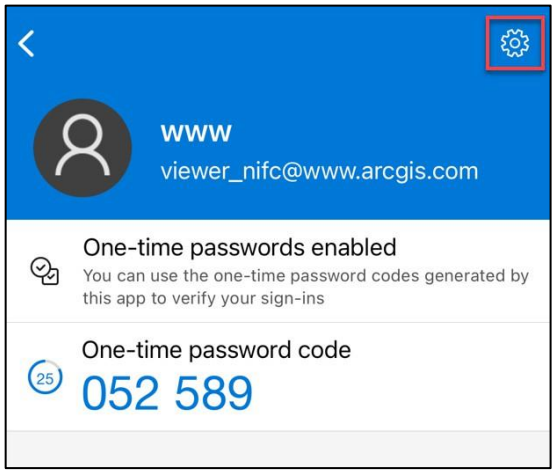
7. The QR code reader within the Authenticator app will open. **Scan the QR code that appears on your computer/secondary device.**

   To reiterate, you will be using the Authenticator app on your **primary mobile device** to scan the QR code on the **computer/secondary mobile device**

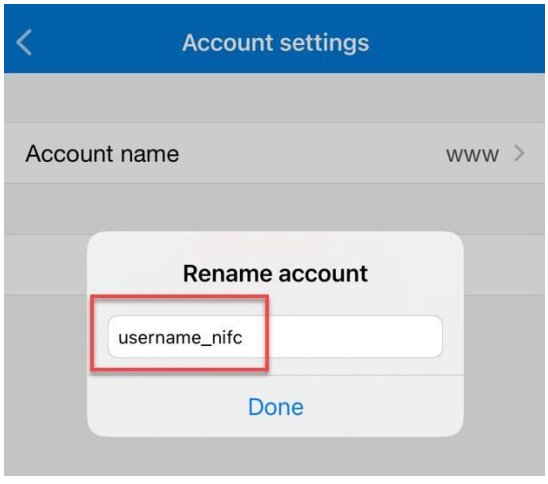


8. The Authenticator app will then display a 6-digit code. Before you use this code, name this account so it will not be confused with others that may be added at a later time.

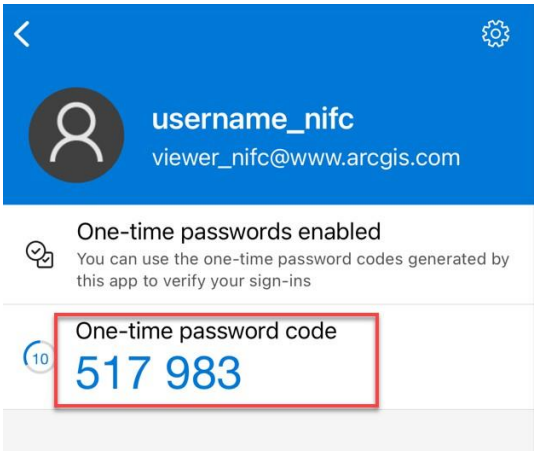
   Click the Settings icon in the upper right corner.



9. **Rename the account to your NIFC Org username. Click Done.**



10. **Locate the 6-digit code**



11. **Type the 6-digit code into the MFA dialog on your computer/secondary device**.

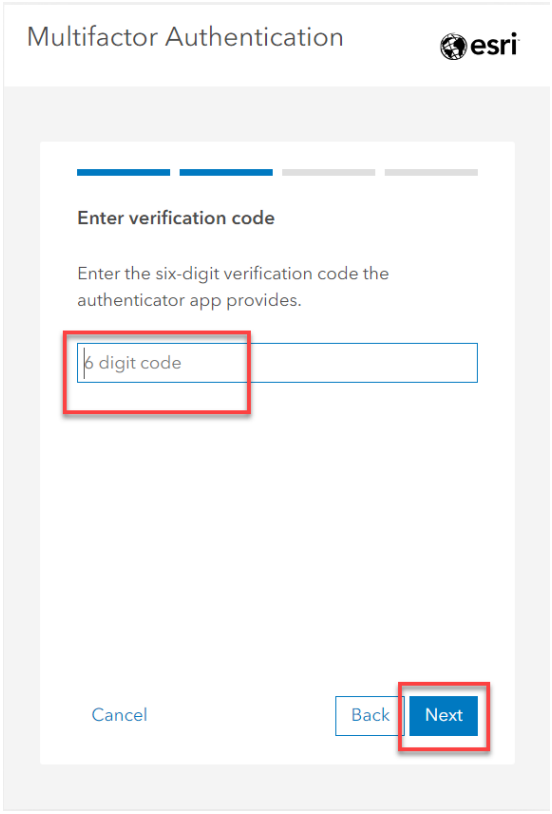
    Do not include a space.

    Notice that each 6-digit code in the Authenticator app times out after 30 seconds.

    If the 6-digit code times out just grab the new code.

    If you receive an error message then check that both of your device times are synchronized. If they are more than 30 seconds off then the codes will not match the MFA system and will be invalid.

    If you run into more errors review the MFA Troubleshooting Guide for help.



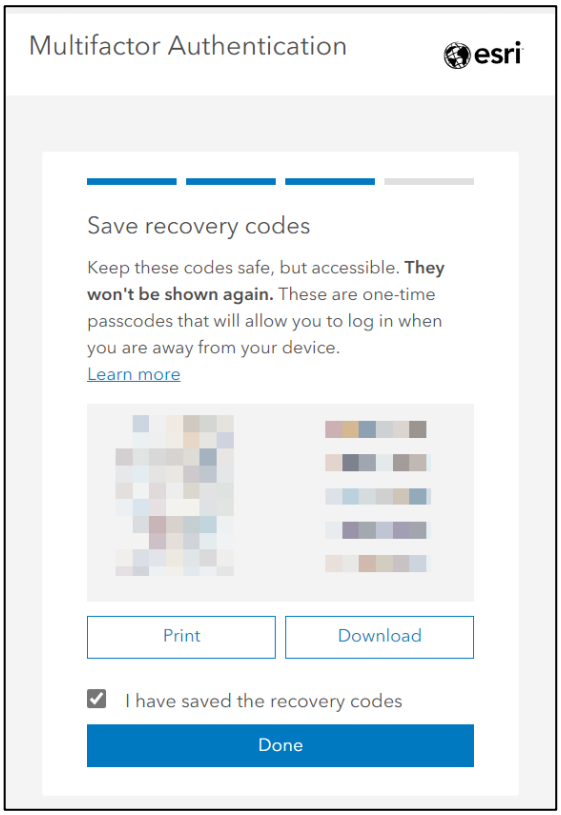
    Click Next.

12. ***Important!!*** The next screen will show a set of 10 recovery codes. **Download and save these in case you are ever without the device that has the Authenticator app.** (Codes in example have been blurred for security.)

    You should not use these codes for regular sign-ins, you should instead be using the 6-digit code in the Authenticator app.

    Only use these recovery codes if you don't have access to the Authenticator app and still need to log in.

    If new recovery codes are needed (you've used the first set of 10) go to step 14 to retrieve a new set of 10 codes.

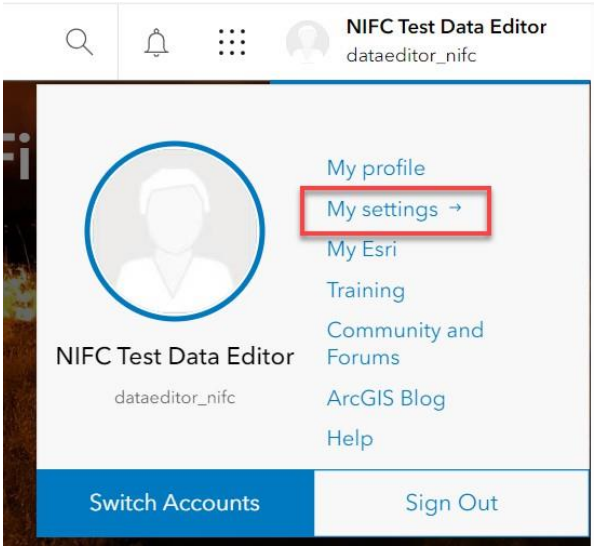


13. **MFA set up is complete!**

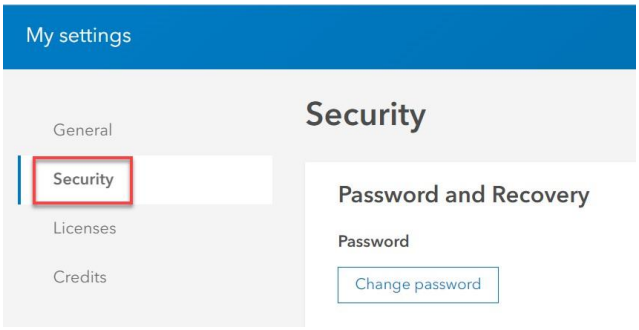
    If you were using someone else's device to setup MFA you can now log out on their device and log in on your primary device.

    The next step to generate new recovery codes is optional. You should only need to do this if you run out of the original 10 recovery codes (that you saved in Step 12.)

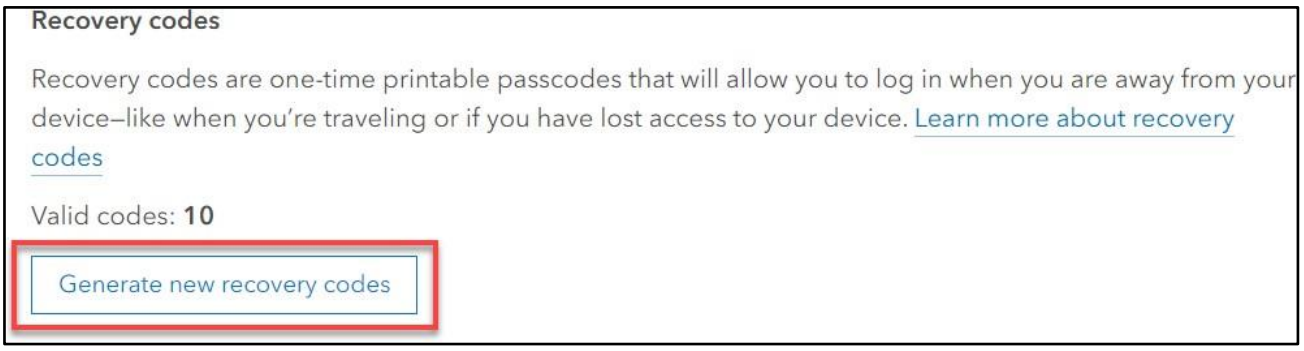
14. While logged into your NIFC Org device on your desktop computer, open your profile (in the upper right hand corner) and click on My Settings.



15. Open the Security tab and scroll down to the Recovery code section.



Click on “Generate new recovery codes” to retrieve a new set of 10 codes. You now have 10 new recovery codes that you can use to log in.



The next page marks the start of the <u>One Device Workflow</u>. If you followed steps 1-13 of the Multiple Devices Workflow then your MFA is setup and you do not need to complete the next workflow.

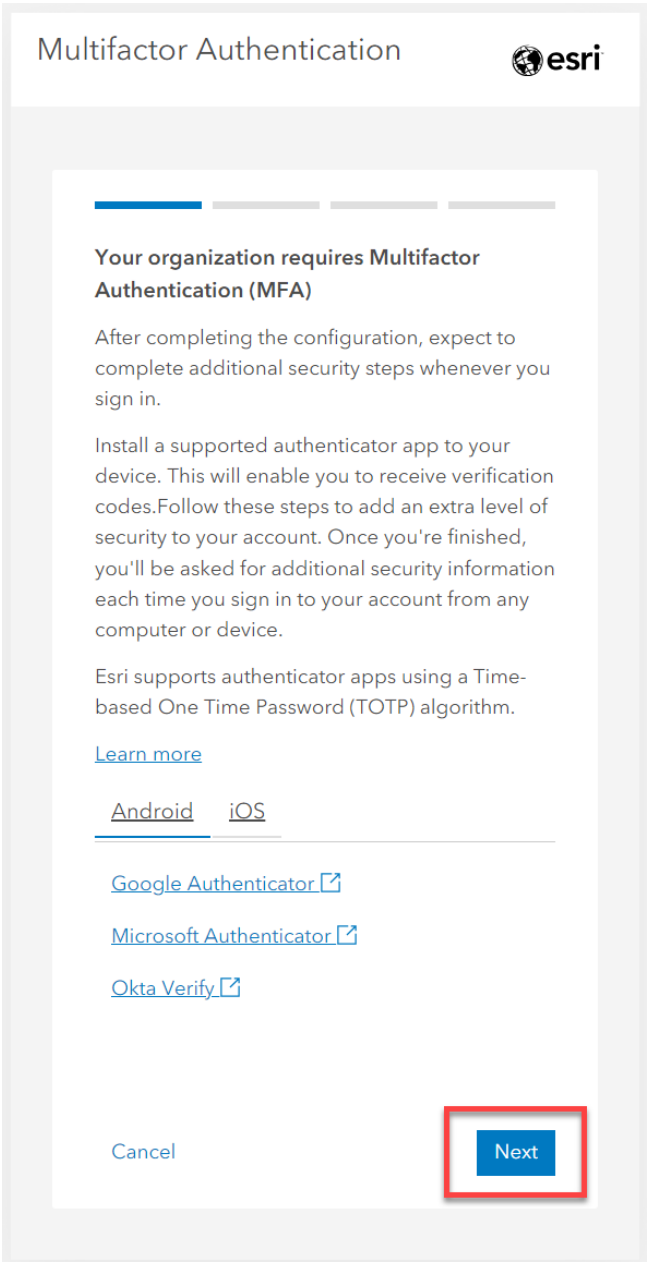
Single Device Workflow

[Click here to jump to the MULTIPLE DEVICES workflow (page 2).]

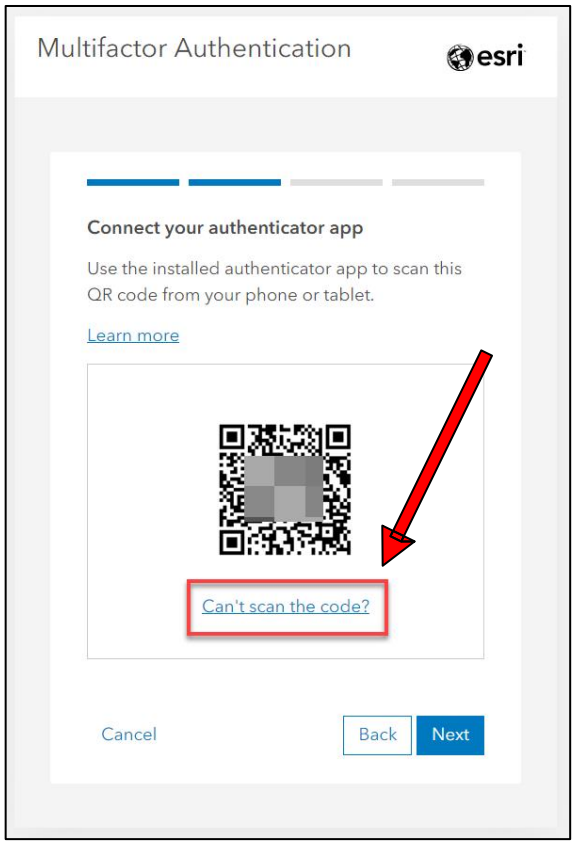
1. **Open a web browser** and log into the NIFC ArcGIS Online Org on your mobile device: https://www.arcgis.com

2. If you see another ArcGIS Online Org (i.e. USFS, FWS, etc.) click the "**Sign in to your account on ArcGIS Online**" link and sign in there. Enter your username and password and click Sign In.

3. **Click Next** on the Multifactor Authentication prompt:



4. A QR code will appear. **TAKE A SCREENSHOT OF THE QR CODE!** You will need this QR code later if you want to add another device (if you do not do this, then you will need to self-reset your MFA via the Support Request Form). Treat this QR code as a password and store appropriately. (Note that the QR code displayed to the right is obscured for security.)



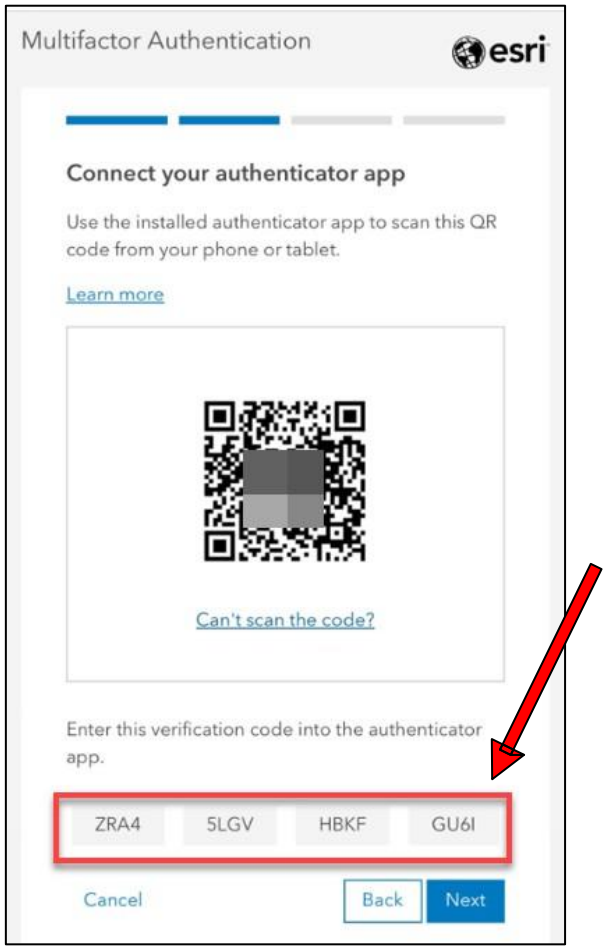
5. Under the QR code, **click on the "Can't scan the code?" link**.

DO NOT USE ANY OF YOUR DEVICES'S CAMERA APPS to scan this QR code!

You will not scan this QR code at all in this single device workflow.

6. A 16-digit verification code will appear that will need to be entered in the authenticator app manually.

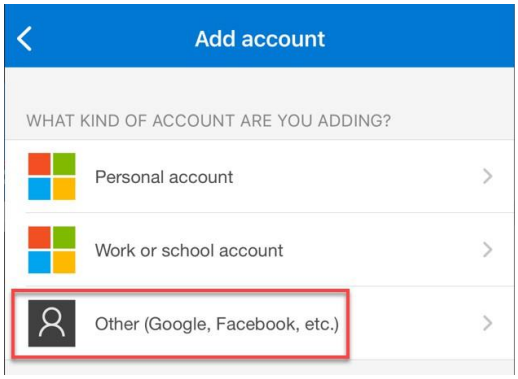
   Copy the entire 16-digit code, if that doesn't work then write down these codes separately so you'll only have to switch between your device's browser and authenticator app once.



Double check that the 16-digit code you type in to the Authenticator app perfectly matches the code provided!!

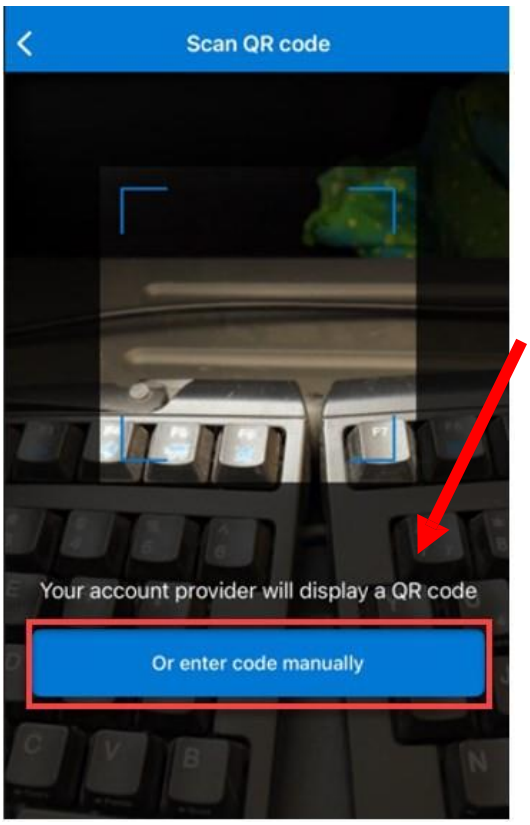
The Authenticator app will accept any 16-digit code and if any of the digits are incorrect then your MFA setup will not work in the end.

7. Switch to your Authenticator app, **click the + to add a new account.**

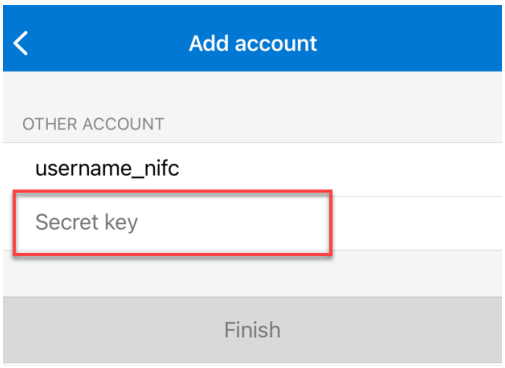


8. **Select "Other"**

9. The QR scanner will open; below it, click on **"Or enter code manually"**

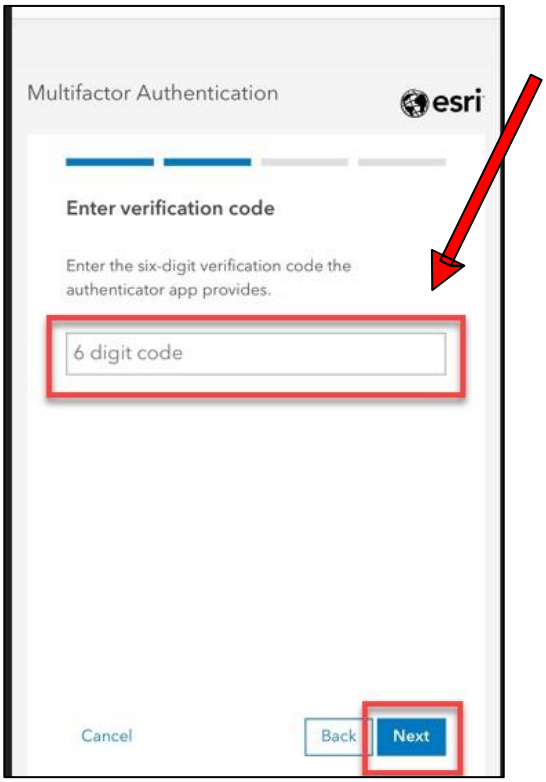


10. **Give the account a name.** It is recommended to name the account with the NIFC Org username, in case there are other accounts using the Authenticator app. **Enter in the 16-digit security key with no spaces (**it is not case sensitive) **that you copied in Step 6.**



11. The Authenticator app will then give you a 6-digit code to enter; **remember this code or copy it.**

12. **Open the web browser and then enter this 6-digit code into the ArcGIS Online account. Do not include a space when typing in the code. Click "Next".**



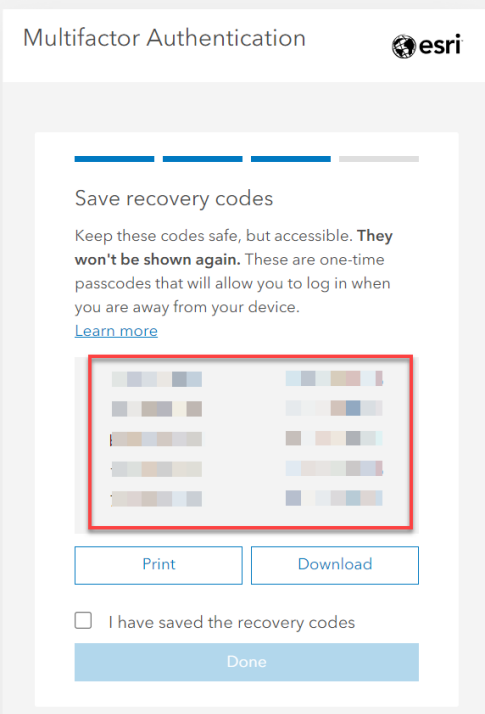
Notice that the 6-digit code times out after 30 seconds, copy a new code if it expires before there is time to copy it.

13. ***Important!!*** The next screen will show a set of 10 recovery codes. **Download and save these in case you are ever without the device that has the Authenticator app.** (Codes in example have been blurred for security.)

    You should not use these codes for regular sign-ins, you should instead be using the 6-digit code in the Authenticator app.

    Only use these recovery codes if you don't have access to the Authenticator app and still need to log in.

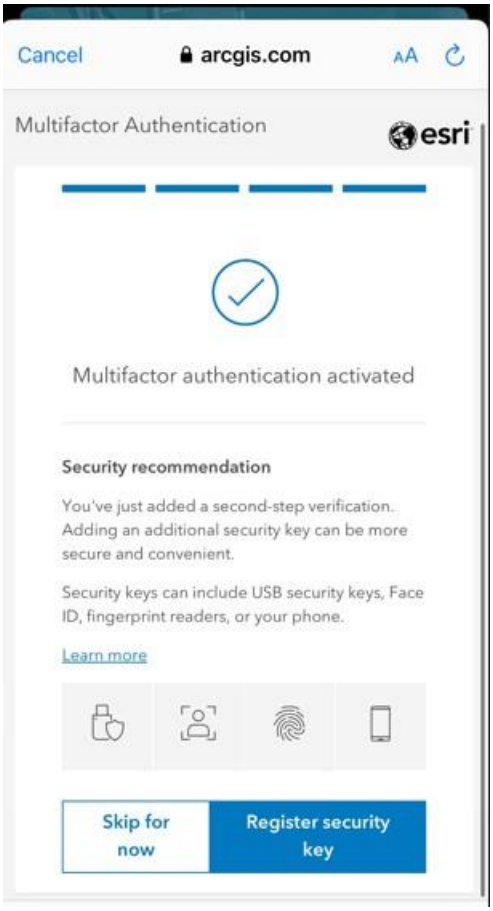
    If new recovery codes are needed (you've used the first set of 10) go to step 15 to retrieve a new set of 10 codes.



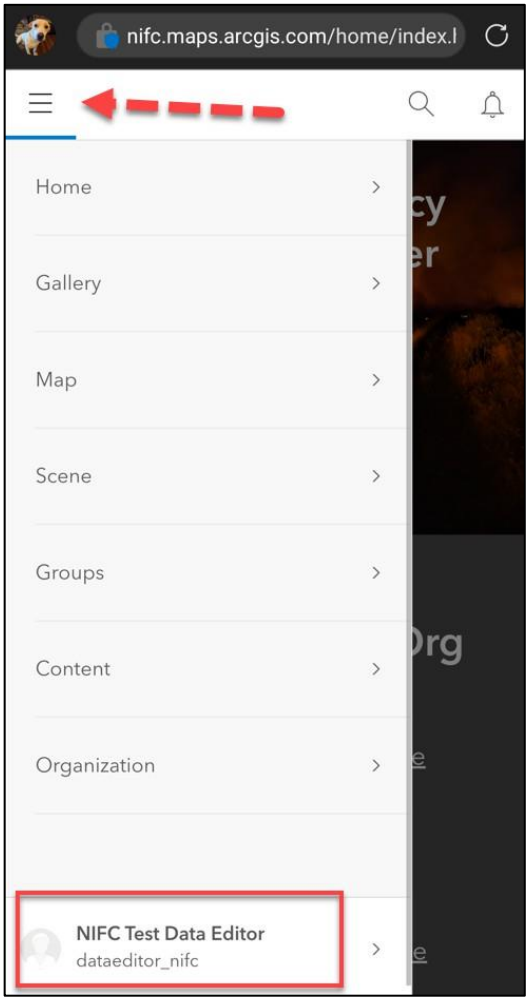
14. **MFA set up is complete!**

    You can select **Skip for Now** to complete the MFA process.

    The next step to generate new recovery codes is optional.



15. To generate a new set of recovery codes while on your mobile device, **sign into your NIFC Org account in a web browser (not in Field Maps).** Tap on the hamburger button, click your profile, then tap on My Settings.



16. Tap on General then select the Security section

17. Scroll down to Recovery codes section and click on Generate new recovery codes. 10 new codes will become available to you.

If you have any questions, please reach out to

wildfireresponse@firenet.gov.

Brought to You By:

WFIGS
Wildland Fire
Interagency Geospatial Services

Recovery codes (from Esri documentation)

You can print or download recovery codes from your settings page. Recovery codes are one-time use codes that provide second-step verification when you sign in to your ArcGIS account. Signing in using recovery codes is useful when you lose physical access to your authenticator devices—such as losing access to your phone while traveling or if your phone or security keys are stolen. To sign in using a recovery code, you must provide a valid username and password. Once the username and password are validated, you see an option to enter a recovery code.

Generated recovery codes are only presented once. ArcGIS Online does not store these codes for retrieving later. It is important to print and save these codes in a safe but accessible location, such as a personal password manager, as soon as they are generated. Recovery codes can be generated as part of the initial setup of multifactor authentication or directly from the **Security** tab of your settings page.

It is recommended that you generate a new set of recovery codes in the following instances:

- You think you have lost access to your codes, or your recovery codes have been compromised.
- Only a few unused recovery codes are remaining.

Once new recovery codes are generated, the previous set of recovery codes becomes invalidated.