



Setting Up Multifactor Authentication

When setting up your multifactor authentication (MFA) account, you will need an authenticator application downloaded to your mobile device (i.e., a cell phone or tablet) and access to a computer.

To set up your MFA account, you will need to complete the following activities:

1. **Select and download an authenticator app to your mobile device.** We recommend using either Duo, Google Authenticator, or Microsoft Authenticator. Instructions are outlined in the *Selecting and Downloading an Authenticator App* section below.
2. **Log into IRIS.** Go to http://community.connectwithiris.org/users/sign_in on a computer.
3. **Set up the connection between your downloaded authenticator app and your IRIS login.** Instructions on this process are outlined in the *Setting up Your MFA Account* section below.
4. **Provide the 6-digit code.** Enter the 6-digit code produced in your authenticator app into IRIS.
5. **Log into IRIS.** On your computer, log into IRIS once more with your username and password.

Selecting and Downloading an Authenticator App

You may use any authenticator app; however, IRIS Support is only able to provide setup guidance for our recommended apps (i.e., Duo, Google Authenticator, and Microsoft Authenticator).

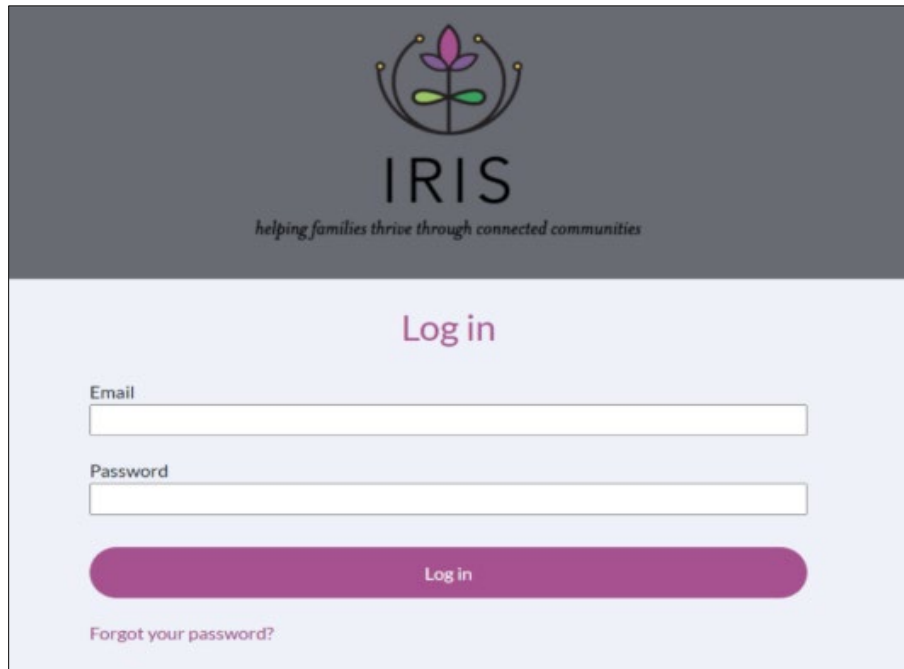
To download an authenticator app, visit the Google Play store or the Apple store on your mobile device, search for an authenticator app, then download it.

Duo Mobile, Google Authenticator, and Microsoft Authenticator are available for both Apple iOS and Android.

Setting Up Your MFA Account

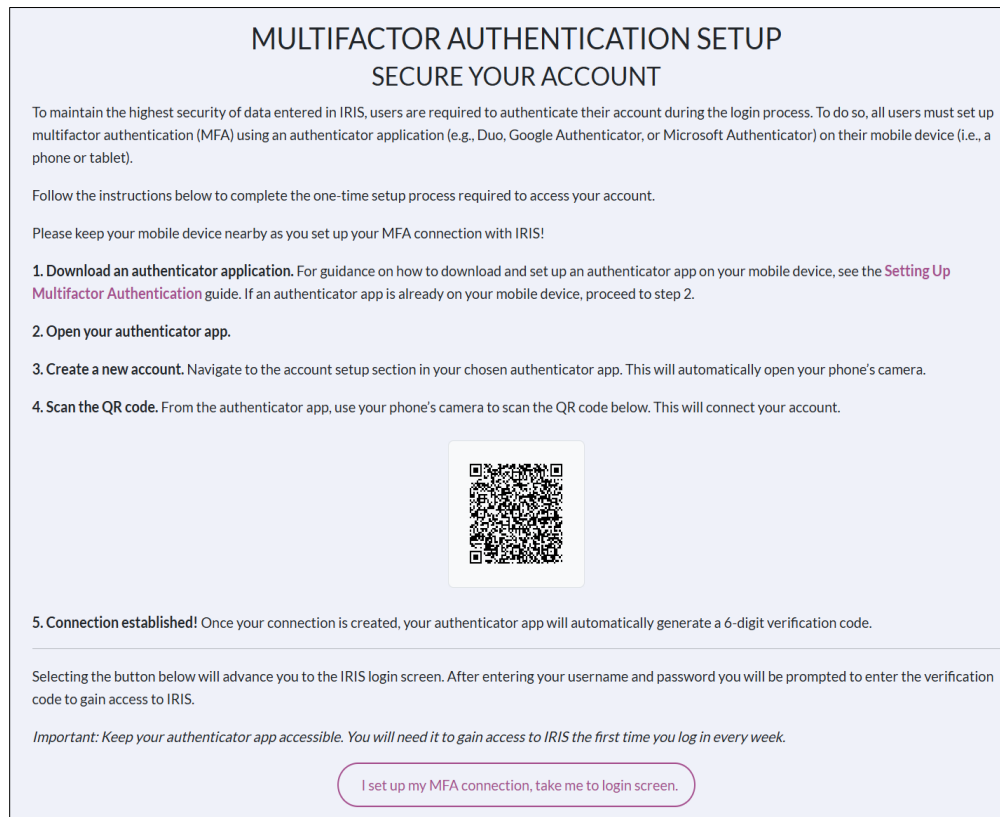
You will need your mobile device and your computer to complete the following steps.

1. Log into IRIS at http://community.connectwithiris.org/users/sign_in on a computer using a supported browser (Apple Safari, Google Chrome, Microsoft Edge, or Mozilla Firefox).



The image shows the IRIS login page. At the top, there is a logo consisting of a stylized flower with a green stem and leaves, enclosed in a circular frame with three dots. Below the logo, the word "IRIS" is written in a large, bold, sans-serif font. Underneath "IRIS", the tagline "helping families thrive through connected communities" is written in a smaller, italicized font. The main heading "Log in" is centered in a large, bold, sans-serif font. Below this, there are two input fields: "Email" and "Password". Each field has a light blue border and a light blue background. Below the "Password" field is a large, rounded rectangular button with a blue gradient and the text "Log in" in white. At the bottom left, there is a link that says "Forgot your password?" in a smaller, italicized font.

2. Upon your first log in, you will encounter the MFA setup page with instructions and a QR code that you will scan in the following steps.



The image shows the Multifactor Authentication Setup page. The title "MULTIFACTOR AUTHENTICATION SETUP" is centered in a bold, sans-serif font. Below it, the subtitle "SECURE YOUR ACCOUNT" is also centered in a bold, sans-serif font. The main text explains that to maintain the highest security, users are required to authenticate their account during the login process. It lists the steps: 1. Download an authenticator application, 2. Open your authenticator app, 3. Create a new account, and 4. Scan the QR code. A QR code is displayed in the center of the page. Below the QR code, it states that once the connection is established, the authenticator app will generate a 6-digit verification code. At the bottom, there is a button that says "I set up my MFA connection, take me to login screen." in a blue gradient with white text. The page also includes a link to the "Setting Up Multifactor Authentication" guide.


MULTIFACTOR AUTHENTICATION SETUP
SECURE YOUR ACCOUNT

To maintain the highest security of data entered in IRIS, users are required to authenticate their account during the login process. To do so, all users must set up multifactor authentication (MFA) using an authenticator application (e.g., Duo, Google Authenticator, or Microsoft Authenticator) on their mobile device (i.e., a phone or tablet).

Follow the instructions below to complete the one-time setup process required to access your account.

Please keep your mobile device nearby as you set up your MFA connection with IRIS!

1. **Download an authenticator application.** For guidance on how to download and set up an authenticator app on your mobile device, see the [Setting Up Multifactor Authentication](#) guide. If an authenticator app is already on your mobile device, proceed to step 2.
2. **Open your authenticator app.**
3. **Create a new account.** Navigate to the account setup section in your chosen authenticator app. This will automatically open your phone's camera.
4. **Scan the QR code.** From the authenticator app, use your phone's camera to scan the QR code below. This will connect your account.



5. **Connection established!** Once your connection is created, your authenticator app will automatically generate a 6-digit verification code.

Selecting the button below will advance you to the IRIS login screen. After entering your username and password you will be prompted to enter the verification code to gain access to IRIS.

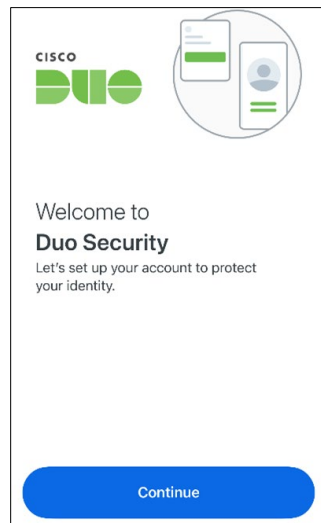
Important: Keep your authenticator app accessible. You will need it to gain access to IRIS the first time you log in every week.

[I set up my MFA connection, take me to login screen.](#)

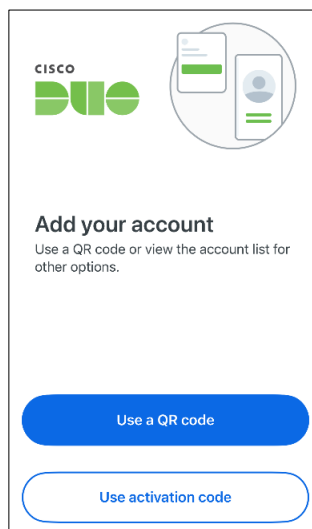
3. Open your chosen authenticator app in your mobile device to begin adding your new IRIS MFA account.
4. We have provided guidance on how to set up [Duo Mobile](#), [Google Authenticator](#), and [Microsoft Authenticator](#). Skip to the correct section below depending on the application you have installed.

Duo Mobile

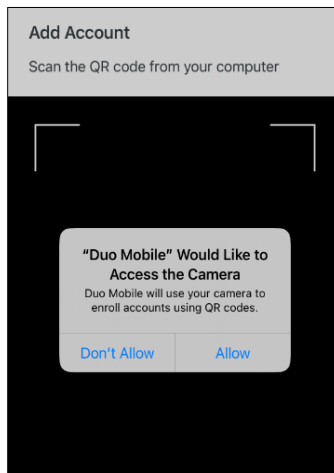
- Open the app on your mobile device and tap on the **Continue** button.



- Click on **Use a QR code**.

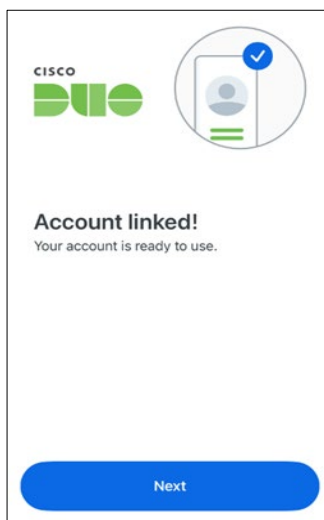


- When prompted, click **Allow** on the "Authenticator Would Like to Access the Camera" message. Then scan the QR code in IRIS with your camera.



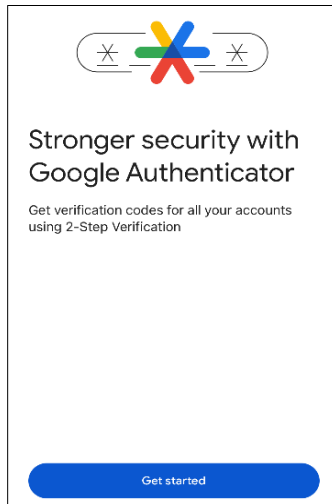
- We recommend setting your account name to "IRIS," so it is easy to identify each time you log into IRIS.

- Click **Next** on the "Account linked!" page. Duo is now set up and ready for use.

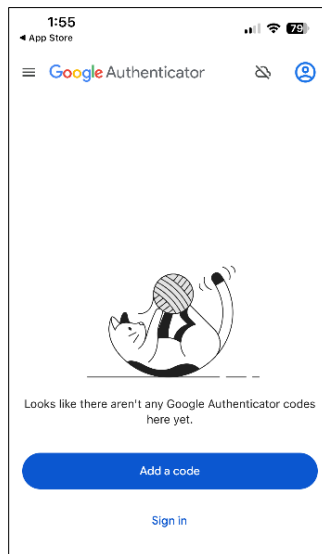


Google Authenticator

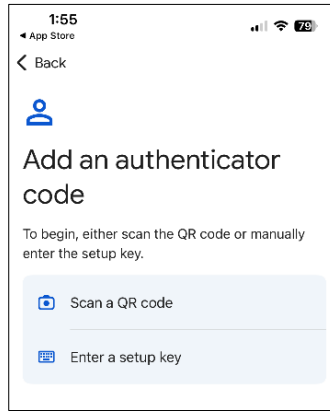
- Open the app on your mobile device and tap on the **Get Started** button.



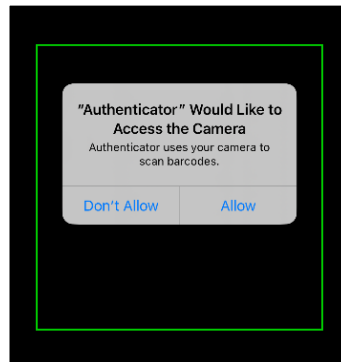
- You will have the option to either log in with your Google account or use the app without logging in.



- Click on **Scan a QR code**.



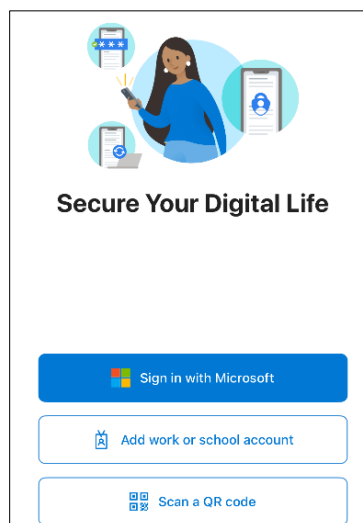
- If prompted, click **Allow** on the "Authenticator Would Like to Access the Camera" message.



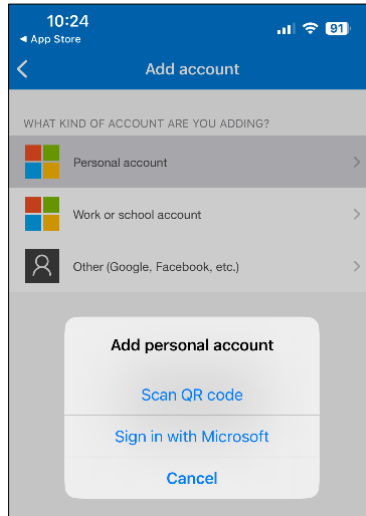
- Scan the QR code in IRIS with your camera. Google Authenticator is now set up and ready for use.

Microsoft Authenticator

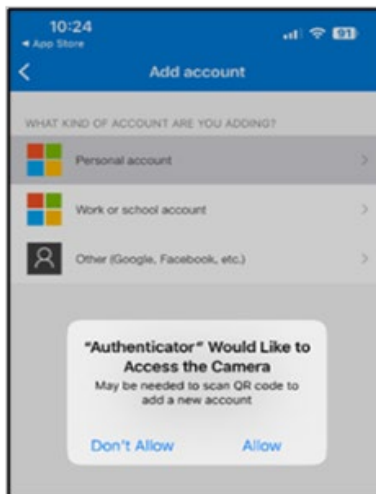
- Open the app on your device. On the home screen of the app, click **Scan a QR code**.



- Select the type of account you are adding based on your preferences, then select **Scan QR Code** on the pop up.



- After clicking **Scan QR Code**, the app will ask for permission to access the device's camera. Click **Allow**.



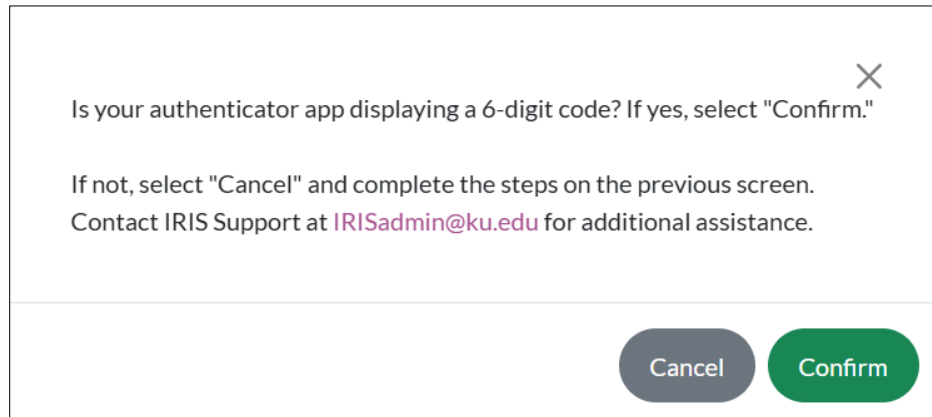
- Using the scanning feature in the app, scan the QR code in IRIS. Microsoft Authenticator is now set up and ready for use.
5. After scanning the QR code in IRIS, your authenticator app should display a 6-digit code. This indicates you have successfully created your IRIS MFA account.

*If you don't see a 6-digit code, click **Cancel** and retry the setup process.*

- Click the **I set up my MFA connection, take me to login screen** button.



- Click **Confirm** on the pop up to return to the IRIS login page.



- Log in once again with your email and password.
- Enter the 6-digit verification code displayed in your authenticator app on the authenticate your account page.

The "Authenticate your account" page has a light blue background. At the top is the title "Authenticate your account" in bold. Below it is the instruction "Enter 6-digit code from your Multifactor Authentication app." followed by a row of six white input boxes with gray borders. The first box is highlighted with a blue border. Below the input boxes is a large purple button labeled "Verify". Underneath the button is the text "Open your authenticator app (like Google Authenticator) and enter the 6-digit code displayed for this account". Below that is a link: "Need help setting up your authenticator app? [Check out our setup guide](#) for step-by-step instructions." At the bottom is a section titled "NOTICE TO USERS" containing a paragraph about University of Kansas policies and security.

- The page will automatically verify you. Success! You are logged into IRIS.