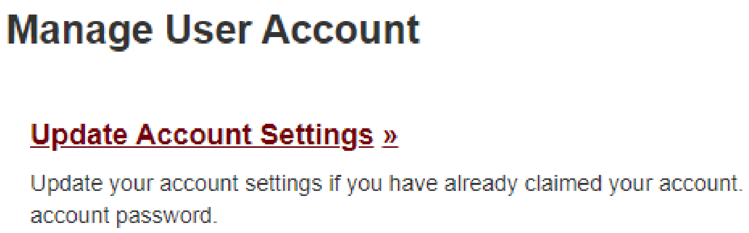
Full Instructions:

1. Navigate to https://myaccount.sc.edu
2. Select **Update Account Settings** at the top of the page

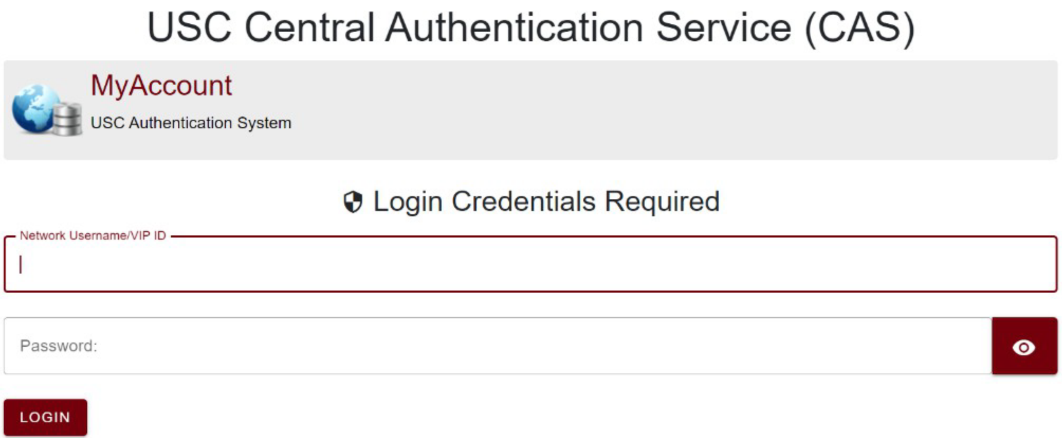


Manage User Account

Update Account Settings »

Update your account settings if you have already claimed your account.
account password.

3. Log in using your USC Network Username and password



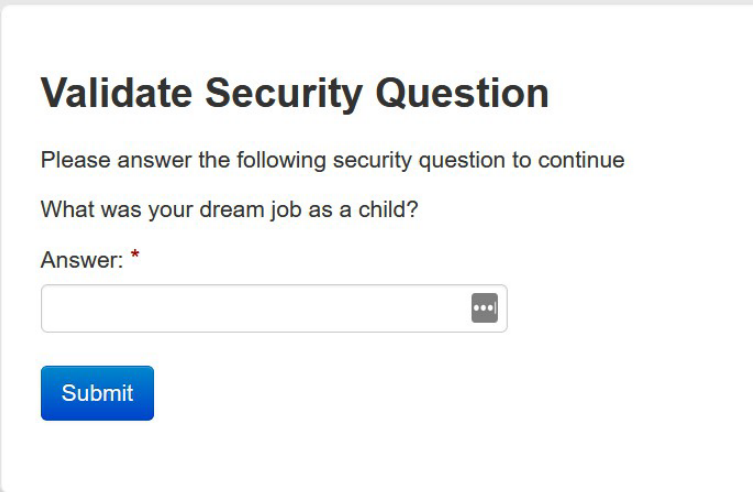
USC Central Authentication Service (CAS)

MyAccount

USC Authentication System

Login Credentials Required

4. Type answer to the security question that displays and click **Submit**



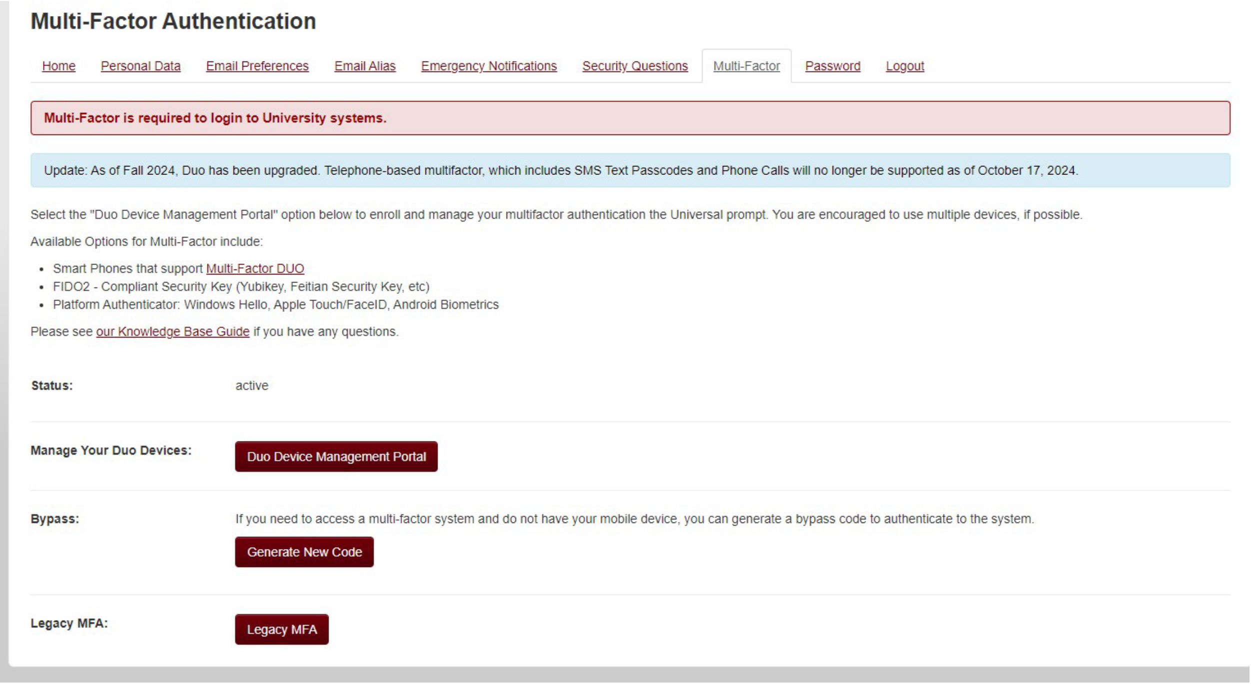
Validate Security Question

Please answer the following security question to continue

What was your dream job as a child?

Answer: *

5. Click **Multi-Factor** (The content in the image may differ slightly from what you see.)



Multi-Factor Authentication

Multi-Factor is required to login to University systems.

Update: As of Fall 2024, Duo has been upgraded. Telephone-based multifactor, which includes SMS Text Passcodes and Phone Calls will no longer be supported as of October 17, 2024.

Select the "Duo Device Management Portal" option below to enroll and manage your multifactor authentication the Universal prompt. You are encouraged to use multiple devices, if possible.

Available Options for Multi-Factor include:

- Smart Phones that support Multi-Factor DUO
- FIDO2 - Compliant Security Key (Yubikey, Feitian Security Key, etc)
- Platform Authenticator: Windows Hello, Apple Touch/FaceID, Android Biometrics

Please see our Knowledge Base Guide if you have any questions.

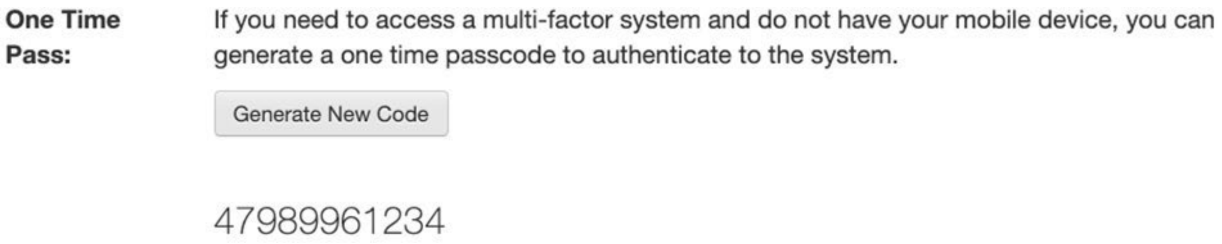
Status: active

Manage Your Duo Devices:

Bypass: If you need to access a multi-factor system and do not have your mobile device, you can generate a bypass code to authenticate to the system.

Legacy MFA:

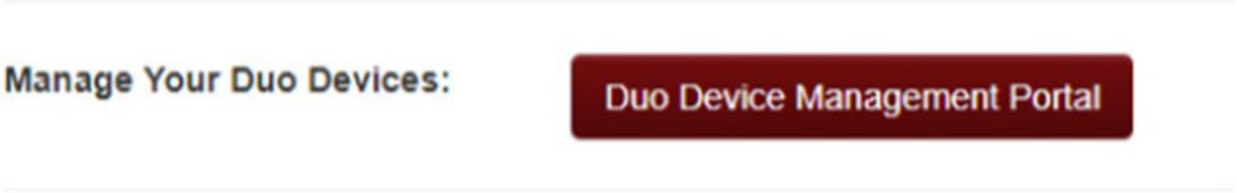
*6. Click **Generate New Code** to generate a one-time passcode before entering the Duo Device Management Portal. You will need this code to manage devices until you register a new device.*



One Time Pass: If you need to access a multi-factor system and do not have your mobile device, you can generate a one time passcode to authenticate to the system.

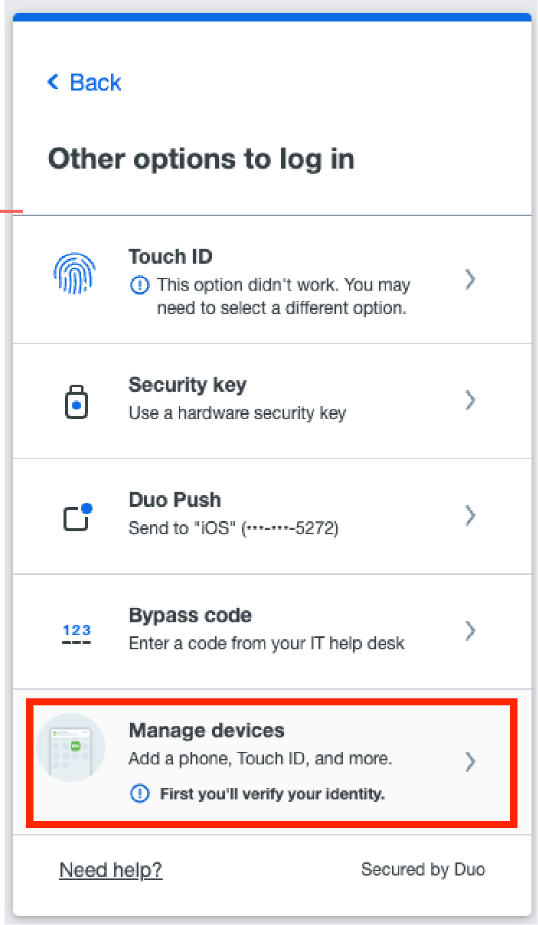
47989961234

7. Click **Duo Device Management Portal**



Manage Your Duo Devices:

8. Select **Manage Devices** at the bottom of the list of your registered Duo devices



Other options to log in

Touch ID
This option didn't work. You may need to select a different option.

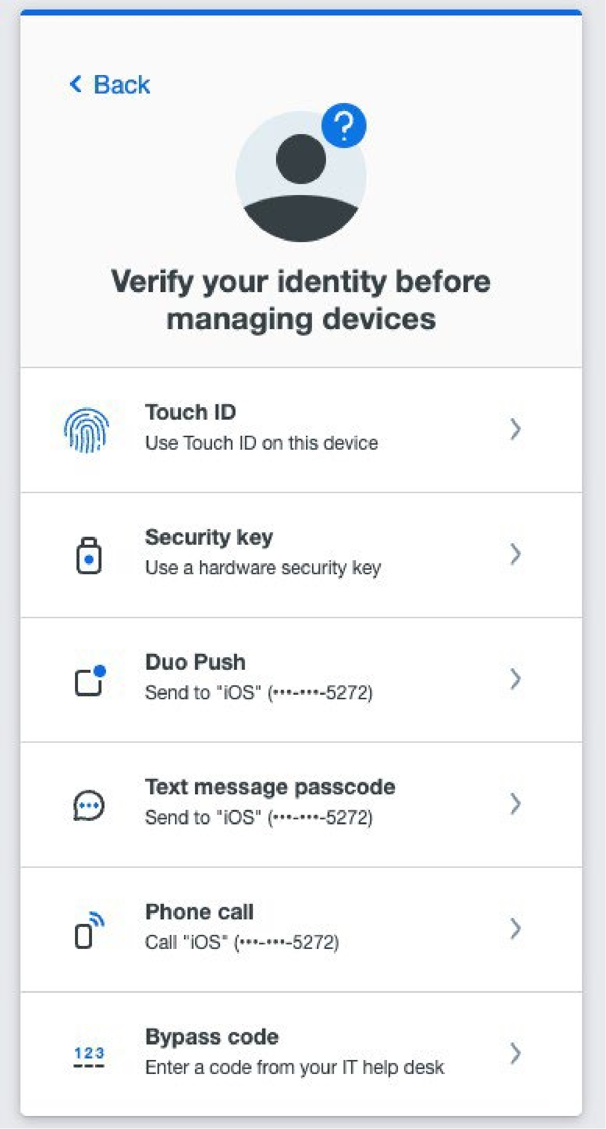
Security key
Use a hardware security key

Duo Push
Send to "iOS" (•••-•••-5272)

Bypass code
Enter a code from your IT help desk

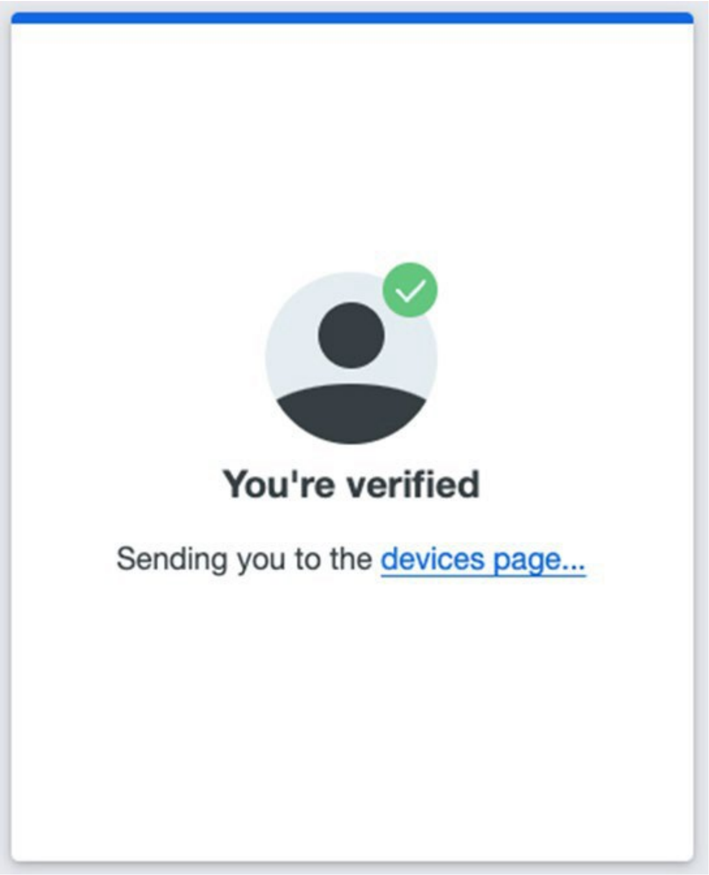
Manage devices
Add a phone, Touch ID, and more.
First you'll verify your identity.

9. Select "Bypass Code" then enter the code from Step 7.



< Back
Verify your identity before managing devices
Touch ID
Use Touch ID on this device
Security key
Use a hardware security key
Duo Push
Send to "iOS" (•••-•••-5272)
Text message passcode
Send to "iOS" (•••-•••-5272)
Phone call
Call "iOS" (•••-•••-5272)
Bypass code
Enter a code from your IT help desk

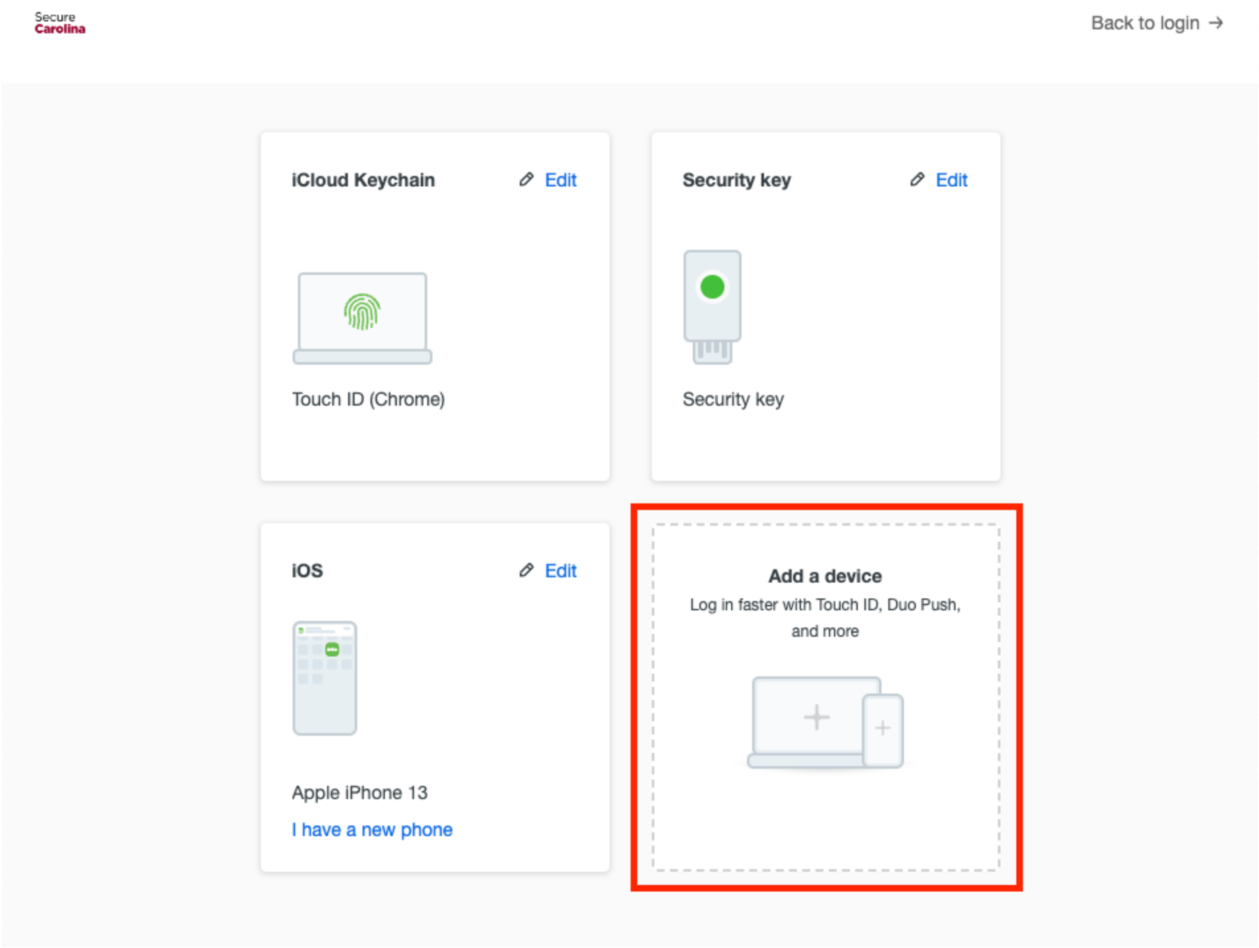
10. After verification, you will be taken to the Device Management Page



You're verified

Sending you to the devices page...

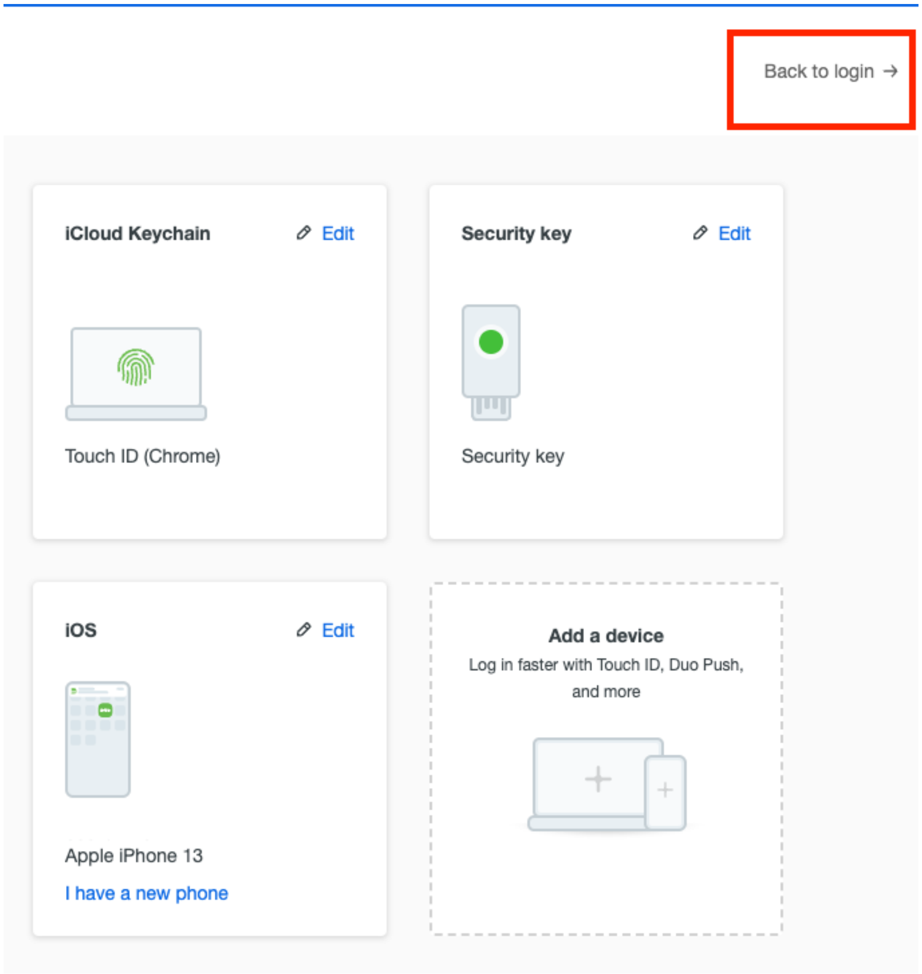
11. Select **Add a device** to add a new device



13. The options available to add will differ based on operating system, hardware, and the browser you are using. Duo will automatically find all available options

14. Follow the on-screen prompts to add a device. Specific instructions for the DUO Mobile app start on Page 8 of this document. YubiKey setup instruction start on Page 12.

15. Once you have successfully added a device in the Duo Device Management Portal, click Back to login -> in the upper-right corner of the Duo Device Management Portal



Log in faster with Touch ID, Duo Push, and more

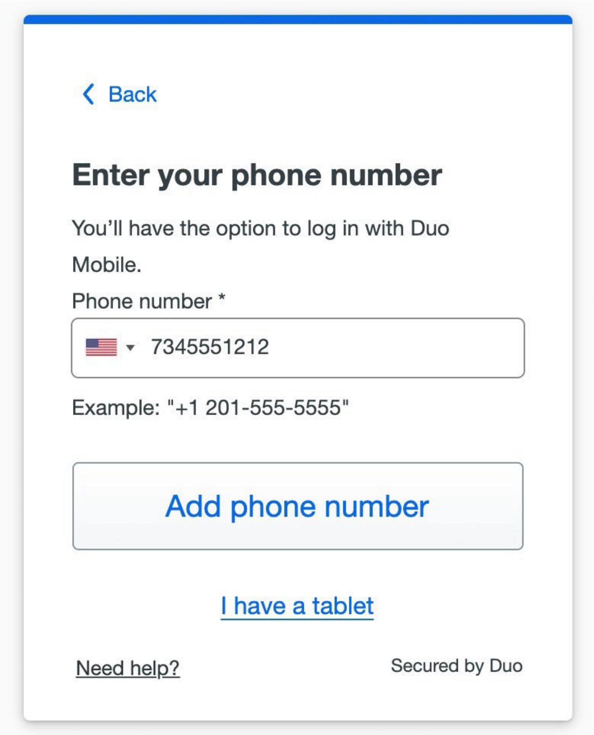
9. You can now close your browser tab or window

Duo Mobile

Duo Mobile is an app that runs on iOS and Android phones and tablets. It's fast and easy to use and doesn't require cell services. Duo pushes login requests to Duo Mobile when you have mobile data or Wi-Fi connectivity to the internet. When you have no data service, you can generate passcodes with Duo Mobile for logging in to applications.

The current version of Duo Mobile supports iOS 13.0 or greater and Android 8 or greater.

1. Select your country from the drop-down list and type your mobile phone number, and then click **Add phone number**.

   Enter your phone number

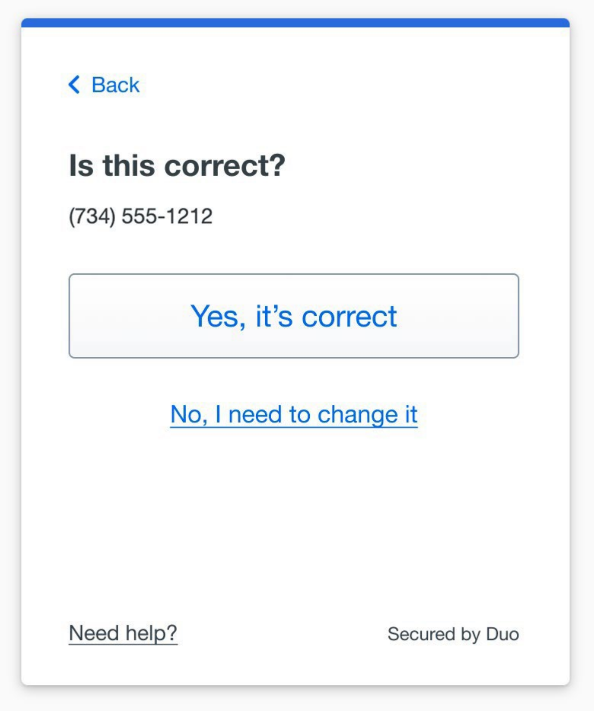
   You'll have the option to log in with Duo Mobile.

   Phone number * 7345551212

   Example: "+1 201-555-5555"

   If you're going to use Duo Mobile on a tablet (like an iPad) with no phone service, don't enter a phone number and click **I have a tablet** instead.

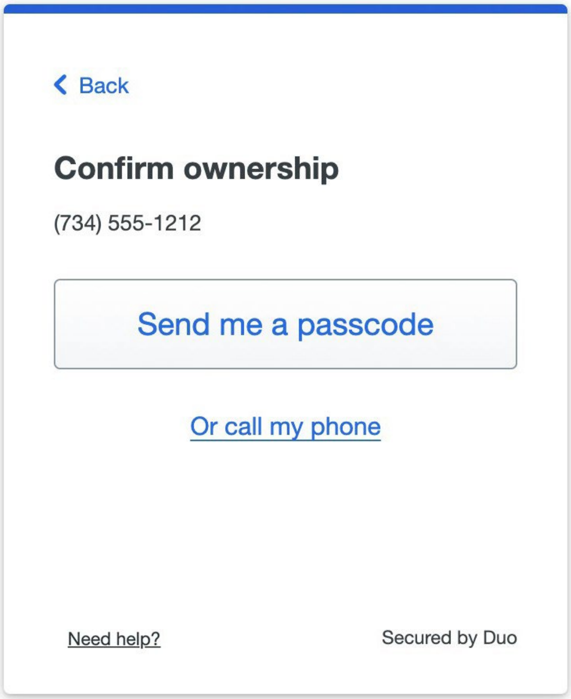
2. If you entered a phone number, double-check that you entered it correctly and click **Yes, it's correct** to continue (or **no, I need to change it** to go back and enter the number again).



Is this correct?

(734) 555-1212

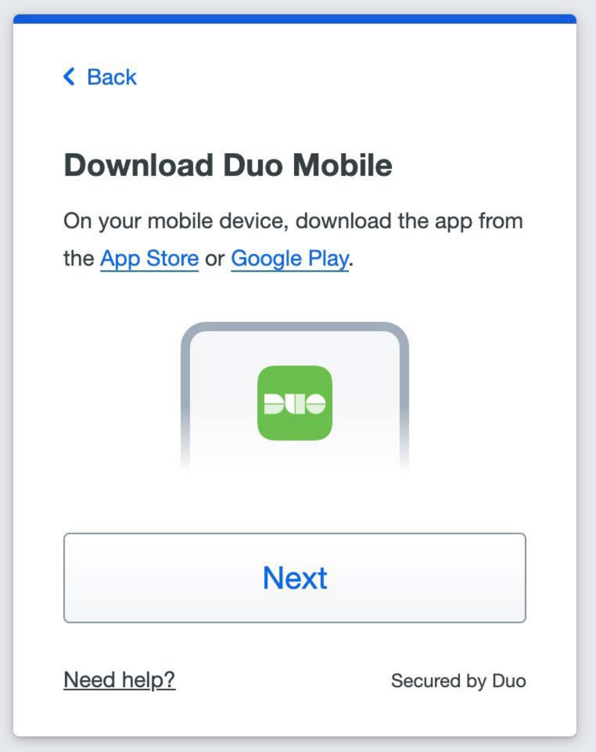
If the phone number you entered already exists in Duo as the authentication device for another user then you'll need to enter a code sent to that number by phone call or text message to confirm that you own it. Choose how you want to receive the code and enter it to complete verification and continue.



Confirm ownership

(734) 555-1212

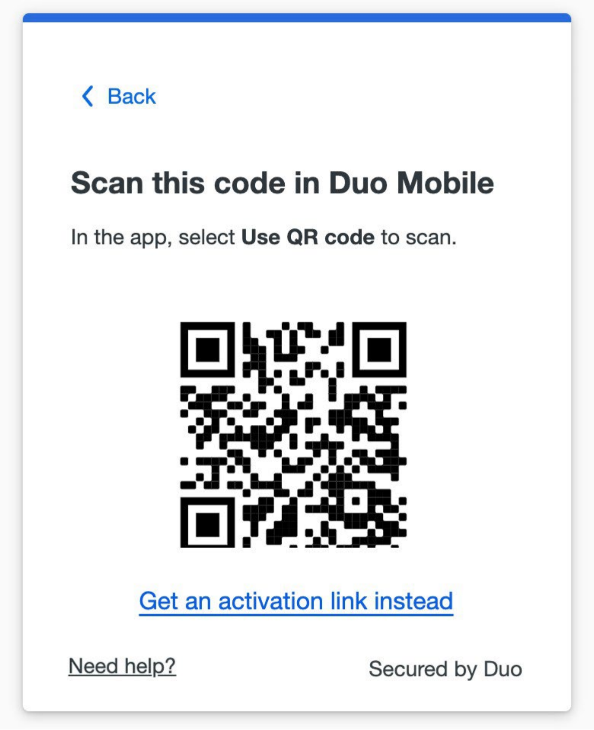
3. Download and install Duo Mobile on your phone or tablet from the Google Play Store or Apple App Store. Once you have Duo Mobile installed click **Next**.



Download Duo Mobile

On your mobile device, download the app from the App Store or Google Play.

4. Open the Duo Mobile app on your phone or tablet and add this account by scanning the QR code shown on-screen.



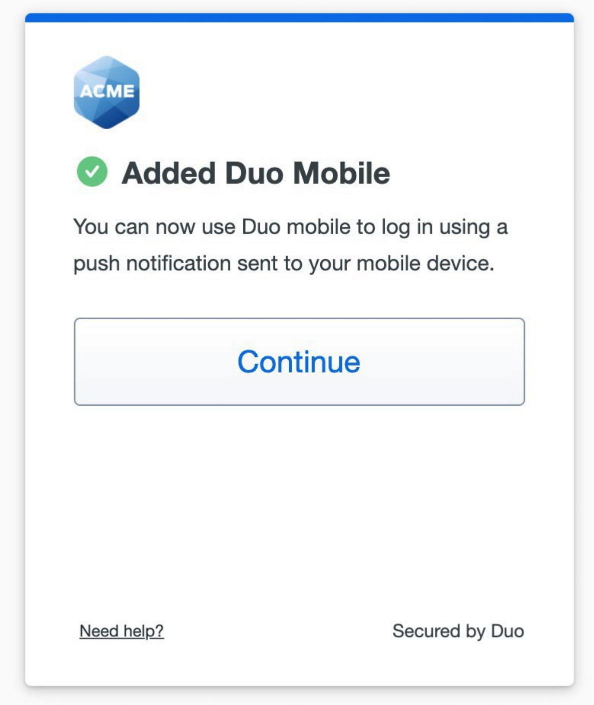
Scan this code in Duo Mobile

In the app, select **Use QR code** to scan.

If you aren't able to scan the QR code, tap **Get an activation link instead** and then enter your email address to send the activation link to yourself. Follow the instructions in the email to activate the new account in Duo Mobile.

If you're on a mobile device, tap **Open Duo Mobile** to activate the new account in Duo Mobile.

5. When you receive confirmation that Duo Mobile was added click **Continue**.



Added Duo Mobile

You can now use Duo mobile to log in using a push notification sent to your mobile device.

You can now log in to Duo-protected applications with Duo Push or with a Duo Mobile passcode.

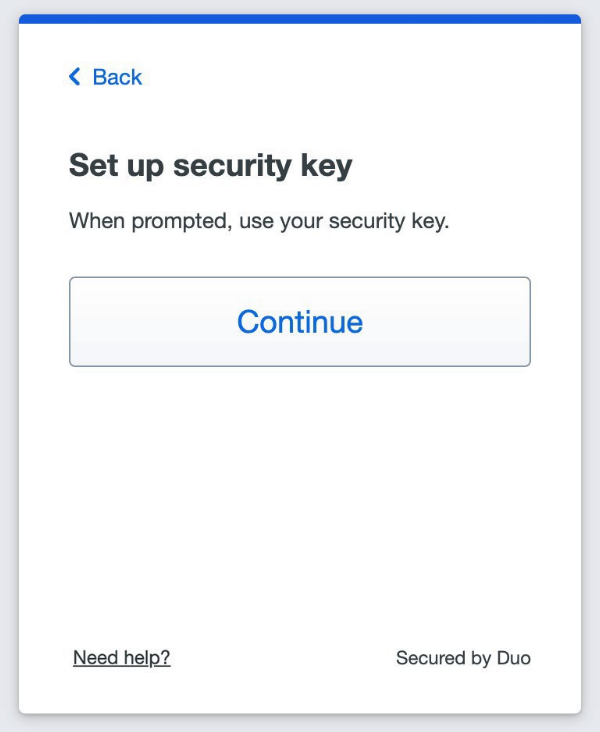
Security Key

A security key is an external device that when tapped or when the button is pressed sends a signed response back to Duo to validate your login. Duo uses the WebAuthn authentication standard to interact with your security keys. You may also see WebAuthn referred to as "FIDO2".

To use a security key with Duo, make sure you have the following:

- A supported security key. WebAuthn/FIDO2 security keys from Yubico or Feitian are good options. U2F-only security keys (like the YubiKey NEO-n) can't be used with the Universal Prompt.
    - If your organization requires user verification of your security key with a PIN or biometric then your security key must support FIDO2.
- A supported browser: Chrome, Safari, Firefox, or Edge. Refer to the Universal Prompt browser support table for minimum browser versions with security key support in Duo.

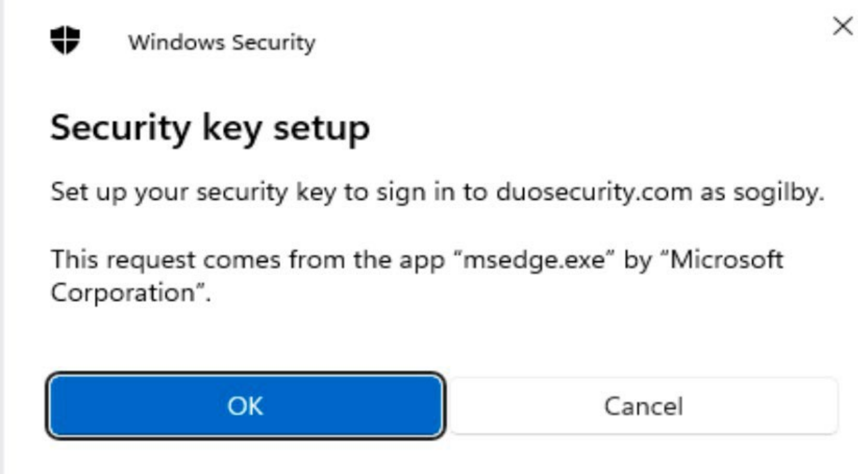
1. Read the security key information and click **Continue**.



Set up security key

When prompted, use your security key.

2. Follow the browser prompts to complete enrollment of your security key, allowing Duo to access information about your security key during setup (Windows example using Edge shown).



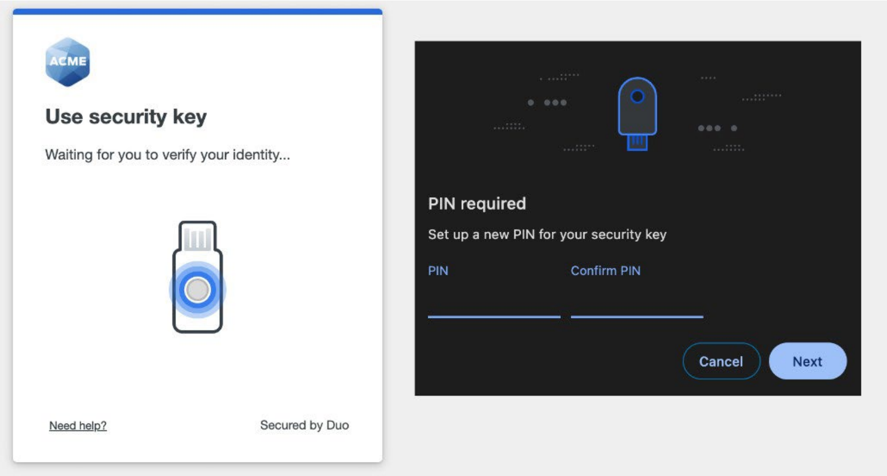
Windows Security

Security key setup

Set up your security key to sign in to duosecurity.com as sogilby.

This request comes from the app "msedge.exe" by "Microsoft Corporation".

3. If your organization requires user verification and you have not already configured a PIN or biometric for your security key you will need to do that now (Chrome example shown). If you already set your PIN or configured biometrics for your security key, then you'll need to enter your PIN or scan your biometric to complete setup.



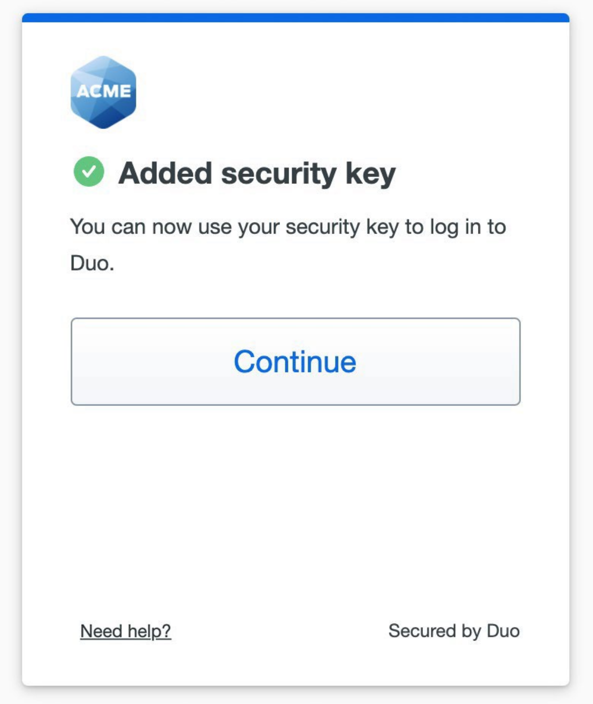
Use security key

Waiting for you to verify your identity...

PIN required

Set up a new PIN for your security key

4. When you receive confirmation that you added your security key as a verification method click **Continue**.



Added security key

You can now use your security key to log in to Duo.

You can now log in to Duo-protected applications that show the Duo prompt in a web browser using your security key.