DUO – Authentication

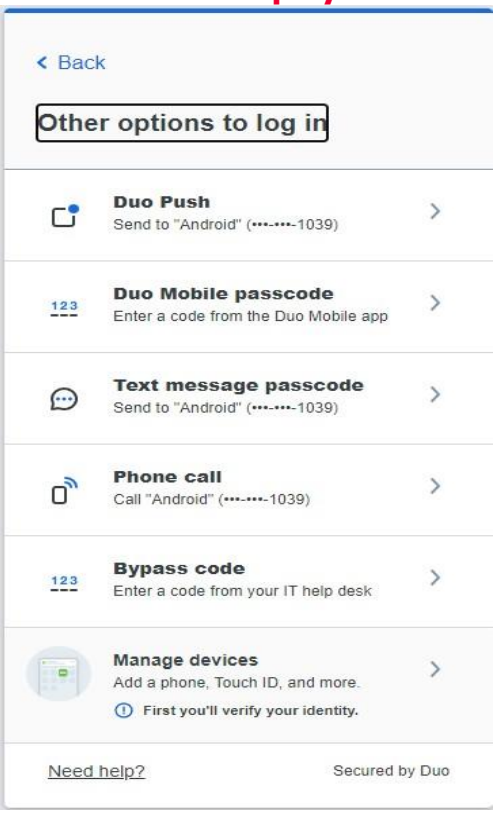
Note For Users signing-in to DUO for the very first time:
The first time a user accesses the DUO Prompt once enrolled, Duo evaluates the supported authentication methods for that type of application and then automatically selects the most secure authentication option available to the user according to this ordered preference:

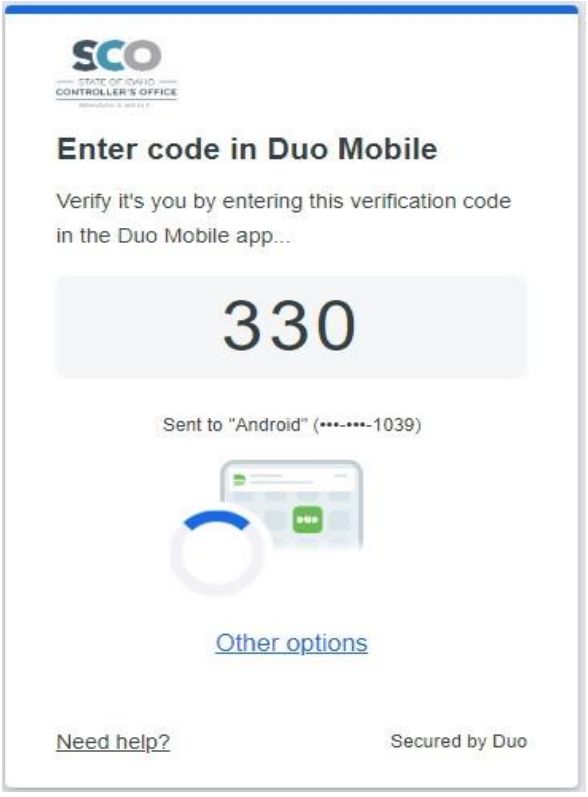
1. **Touch ID**
2. **Security Key**
3. **DUO Push**
4. **DUO Mobile Passcode**
5. **SMS/Text Passcode**
6. **Phone Call**

This means if you enrolled a SmartPhone with the DUO Mobile App, you will be automatically launched into a DUO Push authentication, since that is the preferred authentication for users with SmartPhone devices. This will be the experience for the majority of users.

Users with Security Keys enrolled will automatically launch into the Security Key authentication, non-SmartPhones will automatically launch into the SMS/Text passcode, Landlines the Phone Call option, etc....

Once the user successfully fulfills their first DUO Prompt, DUO will remember the authentication method used and default to that method for future sign-ins. If a user wants to "change back" to another method, or try another method, selecting OTHER OPTIONS will display a list of available authentication methods to choose from.





DUO PUSH

**Be sure to have your registered device near you before signing-in. You only have 60 seconds to respond to the DUO Push notification before it times out.

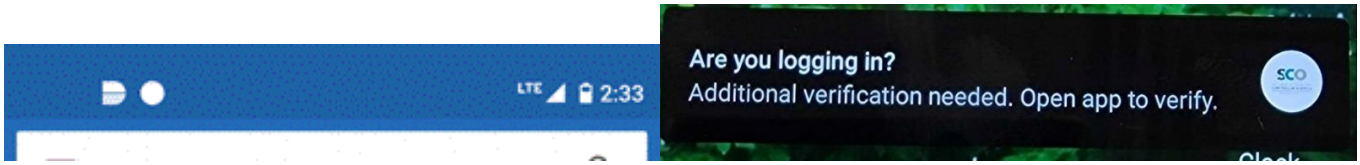
The browser will display a 3-digit code, and ask you to verify in your DUO Mobile app that it is truly you who is requesting authentication.

This code prevents you from EVER making a mistake and approving a DUO Push where you were not the one who was requesting it.

Read on to see how to complete the DUO Verified Push.

The DUO Push notification looks like this illustration. Tap the notification when you see it.
You may want to unlock your phone ahead of time to make this easier

If the notification has already gone away (between 3 and 10 seconds usually) you can access it by swiping down from the top of your phone, the way you normally access previous notifications OR by opening the DUO Mobile app.



This is what the DUO notification symbol is for phones which display notification symbols on the top menu bar. (The one shaped like a "D")

If you cannot find the notification, simply open the DUO Mobile app, or if you happen to have DUO Mobile open right when you select "Send Me a Push", you will see this prompt at the top of the app.
Tap the Green bar to open the Request.

When you tap the DUO Push notification, you are taken immediately to the larger DUO Verified Push screen.

You must enter the 3-digit code from the browser (pictured above) into these 3 boxes. Select the first box to bring up your phone keyboard and type them in.

Select VERIFY.

IMPORTANT
Only Approve authentications that are for YOUR StateID (which is displayed underneath the person icon) and which YOU initiated.

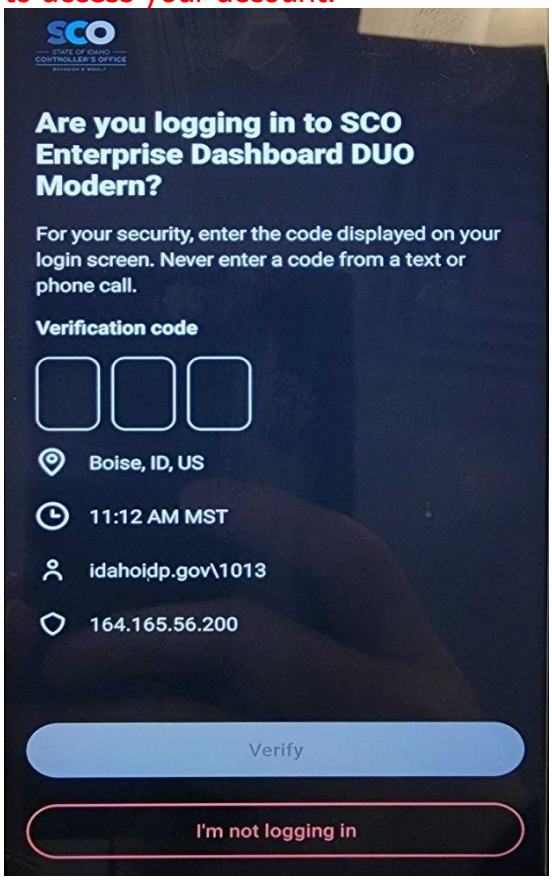
*If you receive a DUO Push Notification and HAVE NOT initiated the push yourself in the last 60 seconds or so, Select I'M NOT LOGGING IN (use the time listed to determine when the notification was sent)

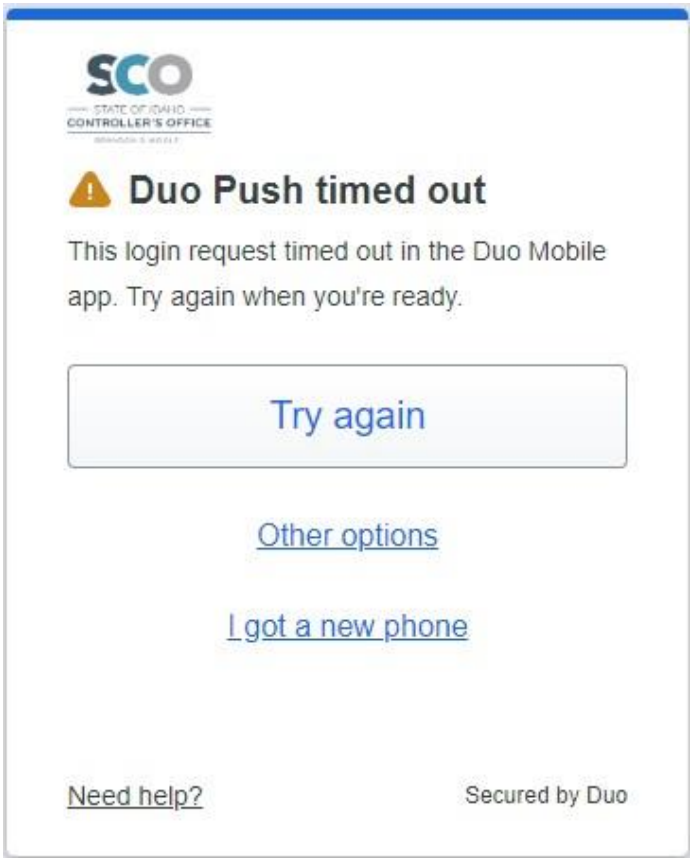
*You will be asked whether this is a suspicious login? Select YES Or NO

If you select YES, you will see

"Thank you, We've notified your DUO Administrator" Select OK

SCO Security will be notified at this time and will launch an investigation into who is attempting to access your account.





IF YOU DO NOT RECEIVE the DUO PUSH AT ALL

- This is a normal occurrence when your registered device is on some types of wifi
- Do not contact the SCO ServiceDesk

The Enterprise Dashboard DUO screen will display this message after 60 seconds.

Be Aware: You only have Three (3) Attempts before DUO Locks your account for 2 hours.

SCO Recommends you select TRY AGAIN **One(1)** more time, and if that also times out, select OTHER OPTIONS.

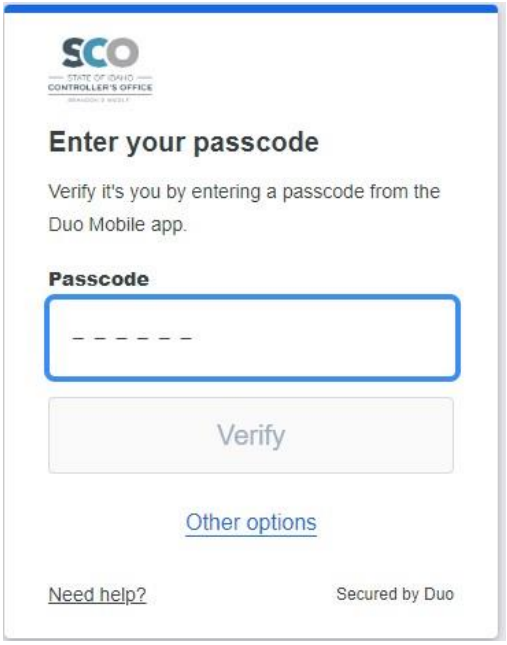
If you have a new phone, select I GOT A NEW PHONE and follow the prompts (described in more detail below)

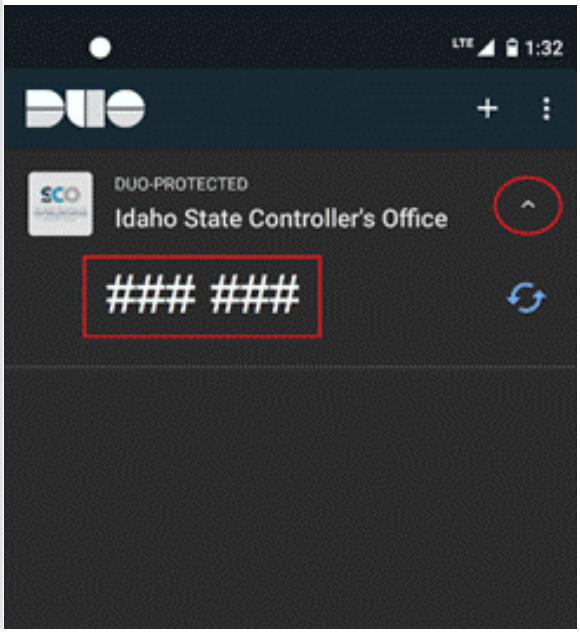
DUO MOBILE PASSCODE

If you select the DUO Mobile Passcode authentication method, you will see this screen.

If you have the DUO Mobile app on your smartphone and select this option, you will NOT receive an SMS Text. Rather, you must open your DUO Mobile app to obtain the passcode, illustrated below.

NOTE If you have the DUO Mobile app, only use this option if your data plan is inoperable or you cannot receive a DUO Push. If this is not the case, we recommend using the DUO Push option if it is at all possible; it is far more secure.





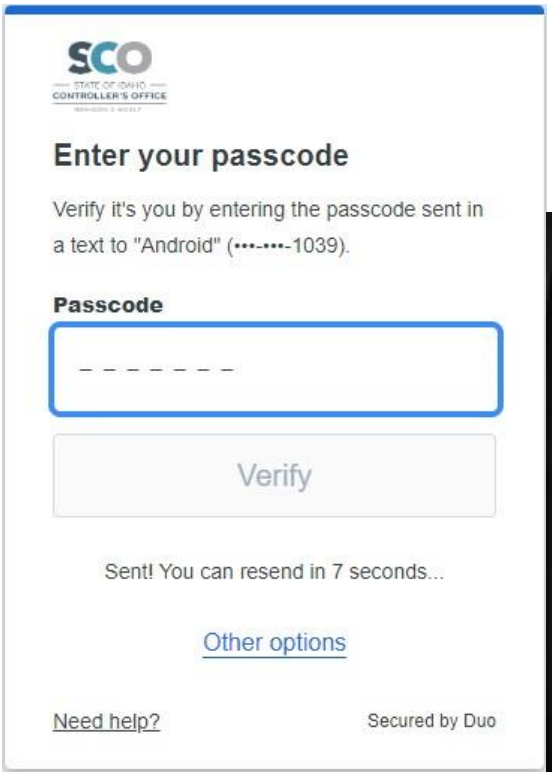
Open the DUO Mobile App, find the tile that states DUO-Protected: Idaho State Controllers Office MFA, and tap the down arrow on the right side. You will then see a 6-digit passcode.

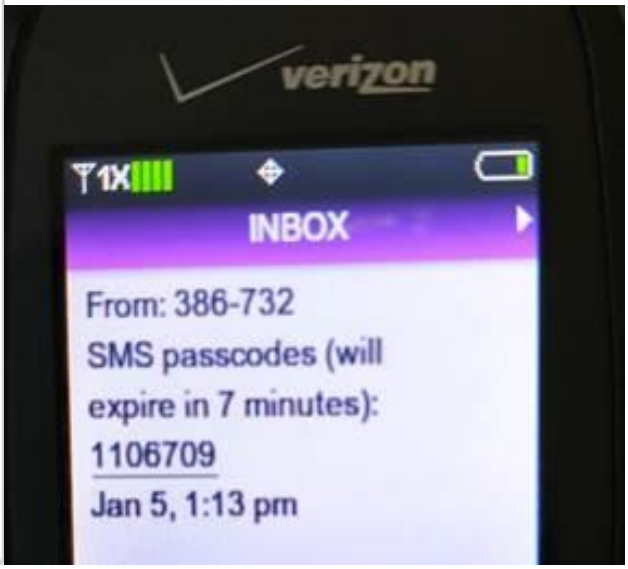
Enter this passcode in the browser, and select VERIFY

TEXT MESSAGE PASSCODE

If you DO NOT have the DUO Mobile app on your phone, or have a feature phone (non-Smart phone), you need to select TEXT MESSAGE PASSCODE, and then will receive an SMS text from DUO.

This will display on the browser while you wait for the text.





The text on a feature phone looks similar to this. The text will come from the short-code number that represents the State of Idaho DUO account, which is **386-732**. **THIS number is not the passcode.**

The text heading for a sign-in authentication will say: SMS passcodes (will expire in 7 minutes):

Enter the 7-digit passcode you then see in the empty field that says (ex. 1106709) on the sign-in and select VERIFY

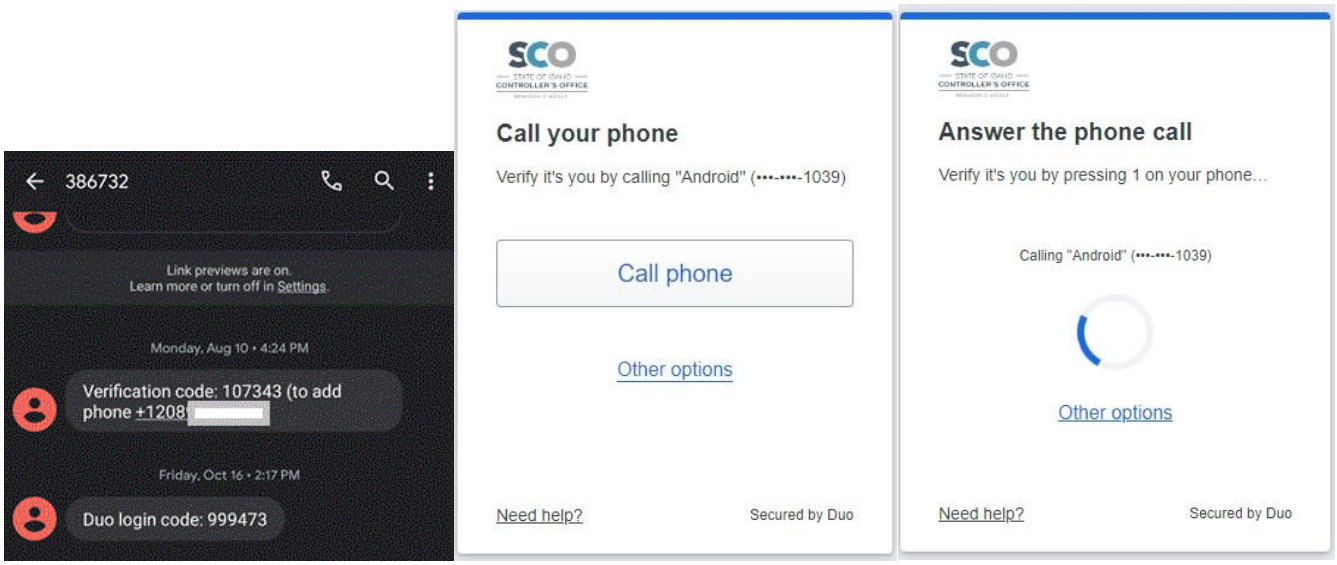
IMPORTANT If you receive this SMS Text and have not pressed the Text Message Passcode authentication method in the last 60 seconds or so, please ignore the text.

The text on a smartphone will come from the short-code number that represents the State of Idaho DUO account, which is **386732**. **THIS number is not the passcode.**

The text heading for a sign-in authentication will say: Duo login code:

Enter the 7-digit passcode you then see in the empty field that says (ex. 999473) on the sign-in and select VERIFY

IMPORTANT If you receive this SMS Text and have not pressed the Text Message Passcode authentication method in the last 60 seconds or so, please ignore the text.



PHONE CALL

Select CALL PHONE.

The call you receive will be an automated voice; this is normal.
It will say the following:

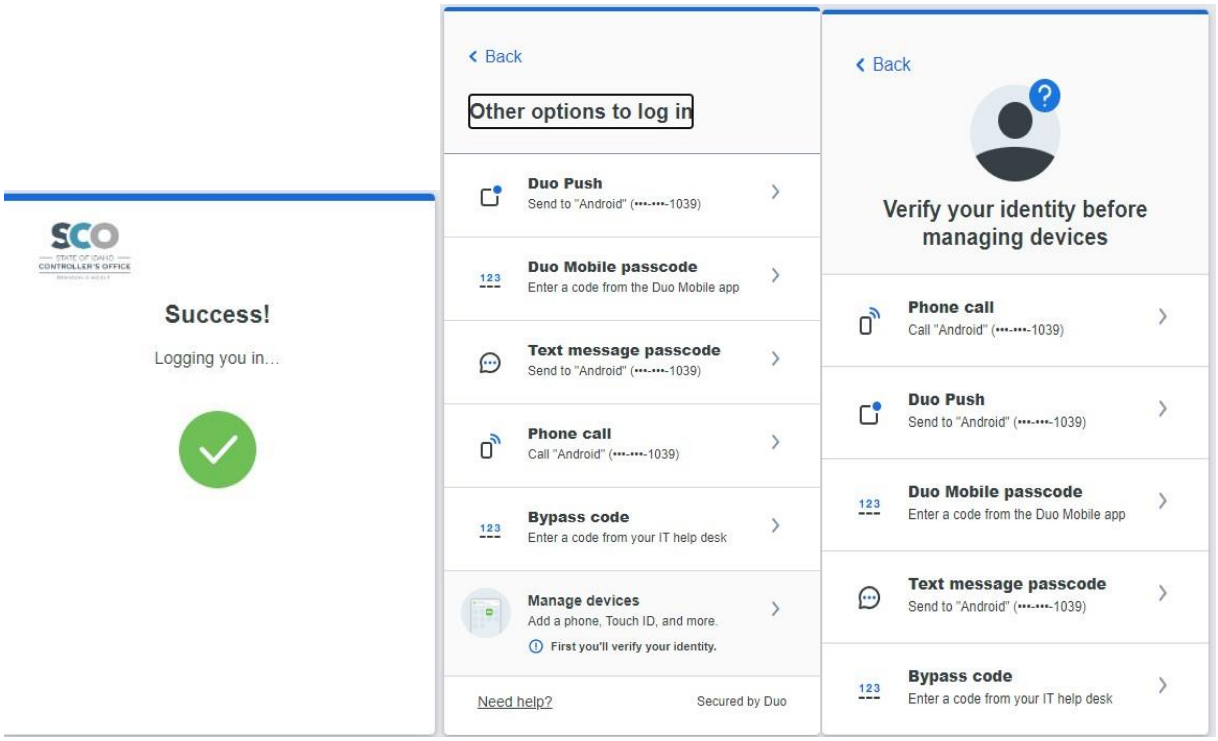
"Welcome to DUO. If you were not expecting this call, please press 9 (Nine) to report fraud, otherwise, press 1 (One) on your phone to login."

On a smartphone, you may need to tap the proper option to show your keypad, then press 1 to authorize this authentication.

The call will be from 208-334-3100, and if you redial this number, you will reach the State of Idaho Controllers Office main line.

IMPORTANT If you receive this phone call and have not selected a DUO Phone Call option in the last 20 seconds or so, press 9 (Nine) to report fraud.

When you successfully fulfill any of the authentication methods above, you will receive this Success screen on the browser.



MANAGE DEVICES (ADD NEW PHONE, SECURITY KEY, LANDLINE, ETC…)

To access Manage Devices screen, select MANAGE DEVICES,

**There is no limit to registered devices

You will need to successfully authenticate to DUO with an existing device before you will be allowed to Manage Devices.

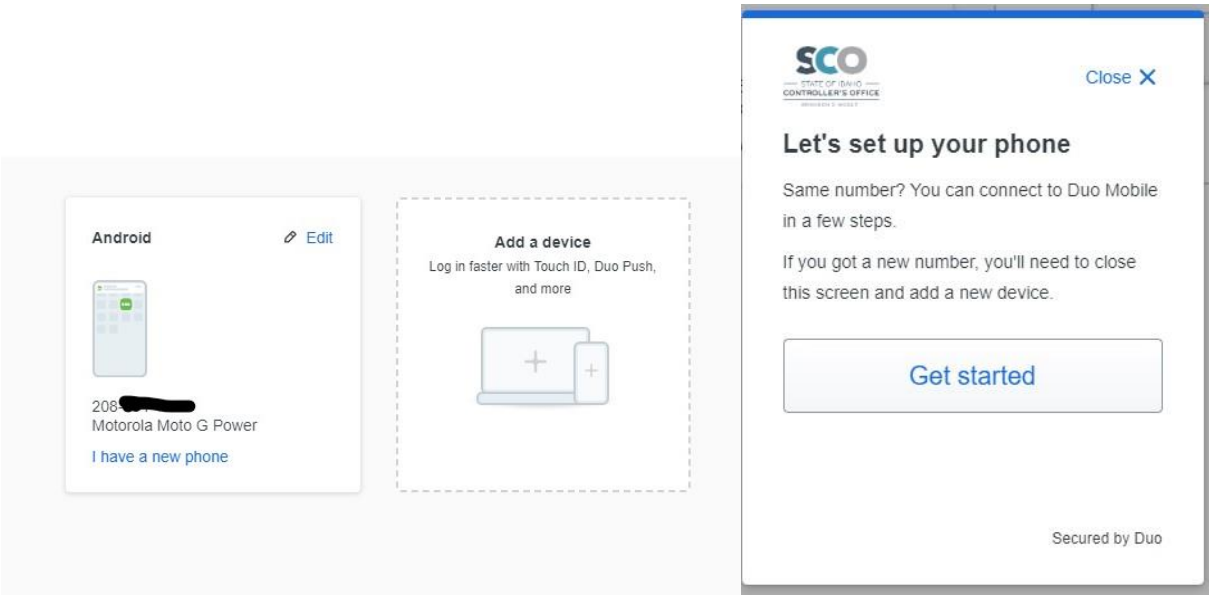
Select the DUO Authentication method of choice, and authenticate.

Your existing DUO enrolled devices will display as an icon on this screen; for example, the Android Phone icon on the illustration.

Select ADD A DEVICE to add a new DUO device of any type.

The EDIT link only allows you to rename the device in this screen, NOT change phone numbers or device types for your existing device.

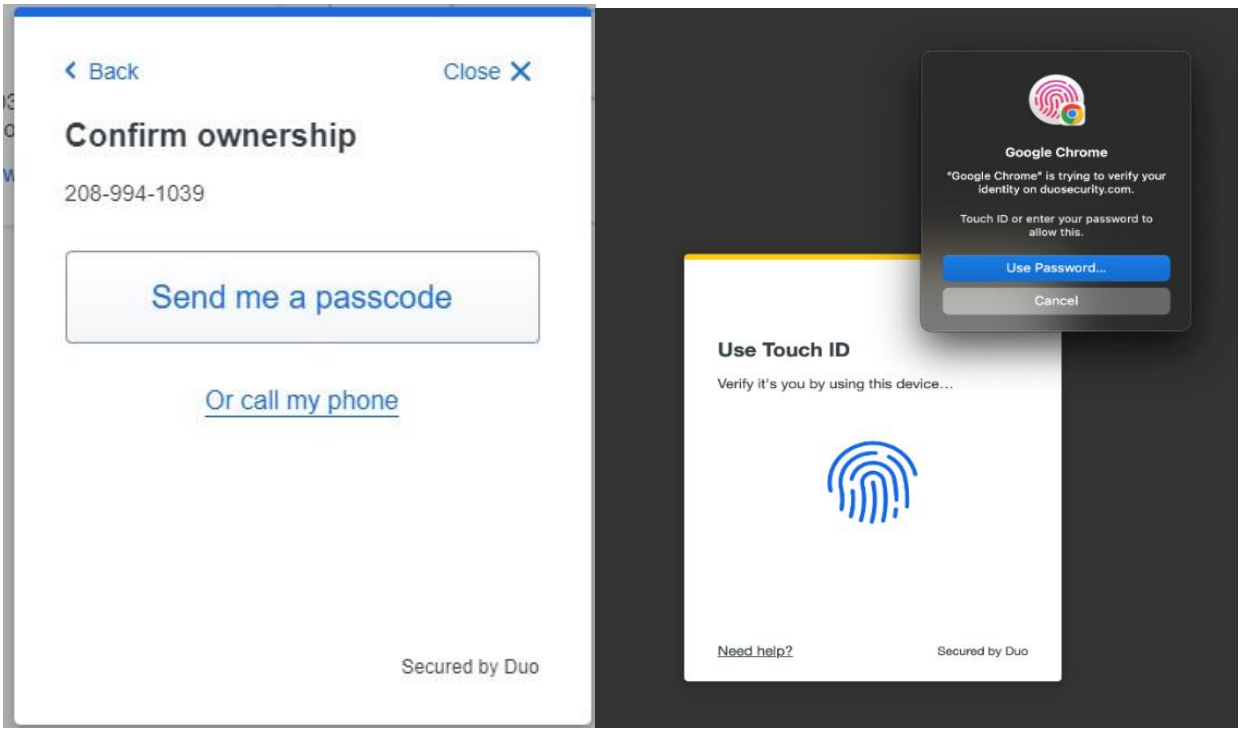
Select I HAVE A NEW PHONE to add a new phone as your DUO device.



I HAVE A NEW PHONE

IMPORTANT
Add your new SmartPhone to DUO BEFORE wiping your old SmartPhone!!!

It does not matter if you add your new SmartPhone to DUO before or after you change your simcard over to it.
Much like initial device registration, follow the prompts to confirm ownership of your new device.



TOUCH ID

In order to use Touch ID with Duo, make sure you have the following:

- A MacBook Pro, MacBook Air, or Apple Magic Keyboard with a Touch ID button.
- A fingerprint enrolled in Touch ID (see how to do this at the Apple Support site).
- Chrome 70 or later. Safari and other browsers on macOS are not supported.

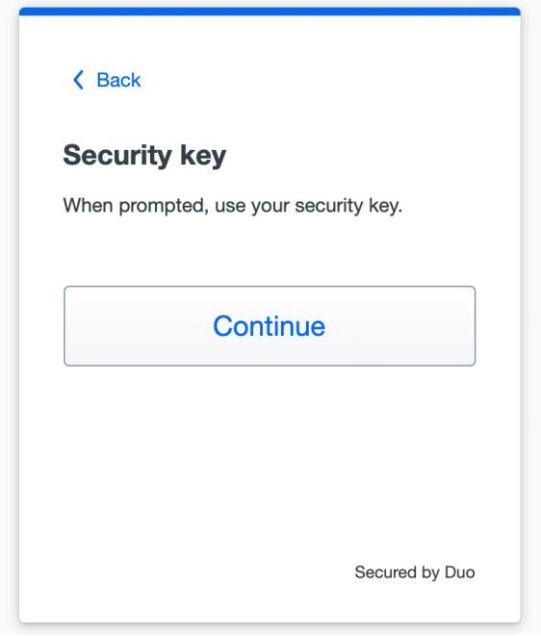
If you have more than one MacBook with which you'd like to approve Duo login requests using Touch ID, you'll need to add each of them separately as a new Touch ID device in Duo.

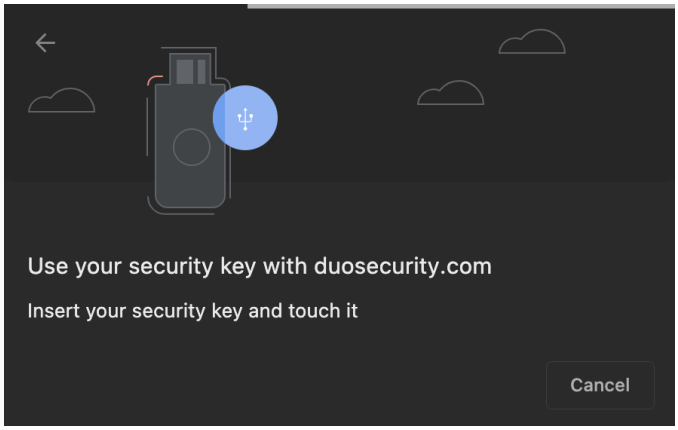
SECURITY KEY

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 can't be used with the Universal Prompt.
- 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.





Your browser will prompt you to insert your key into your USB if it is not already, then you will be prompted to press the button on the key.