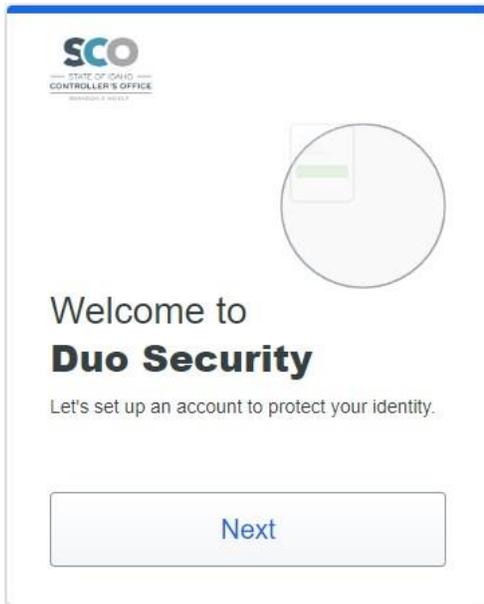


DUO - Initial Device Registration

Upon successful sign-in with your StateID and strong password, which is your first factor of authentication, you will see a new screen with a prompt welcoming you. Click NEXT.

Also click NEXT, on the next Two(2) informational prompts.



SCO
STATE OF IDAHO
CONTROLLER'S OFFICE
INTEGRITY & SAFETY

Welcome to
Duo Security

Let's set up an account to protect your identity.

Next

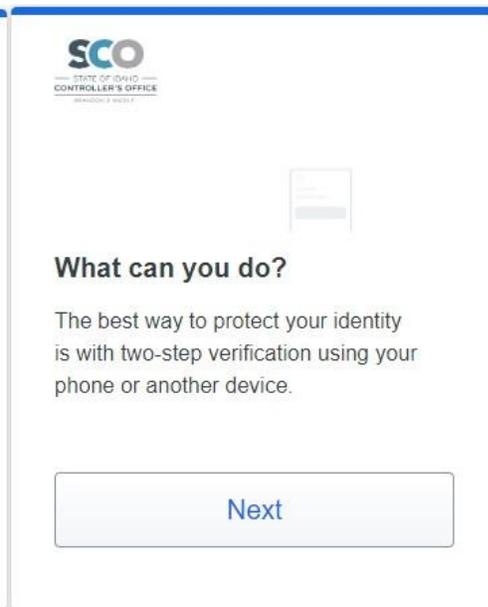


SCO
STATE OF IDAHO
CONTROLLER'S OFFICE
INTEGRITY & SAFETY

Did you know?

97% of data breaches start by stealing your identity.

Next

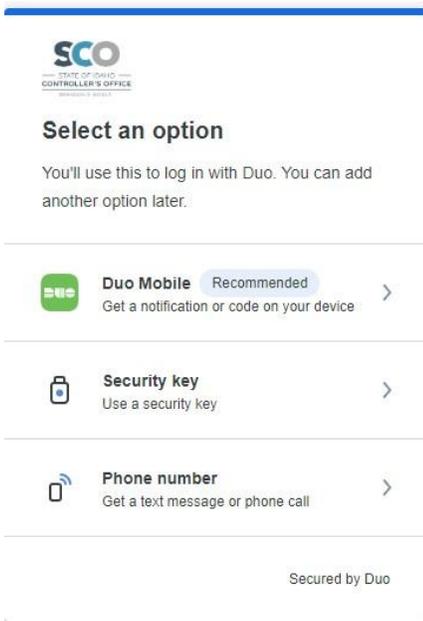


SCO
STATE OF IDAHO
CONTROLLER'S OFFICE
INTEGRITY & SAFETY

What can you do?

The best way to protect your identity is with two-step verification using your phone or another device.

Next

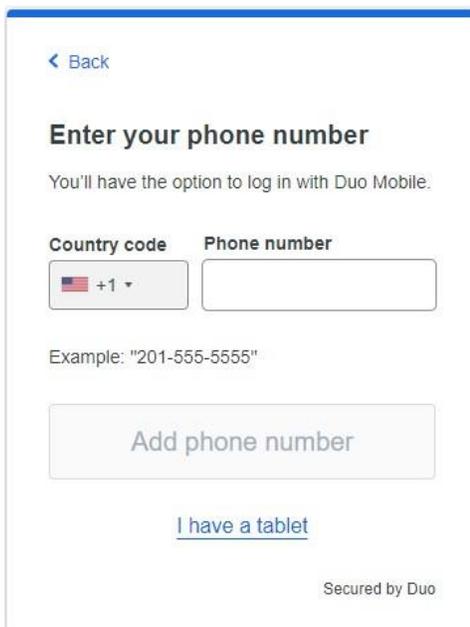


Select the type of device you are registering, based on the authentication method your device can support and your own personal preference.

DUO MOBILE (Recommended):

If you selected DUO Mobile, next enter your phone number with area code. Punctuation is allowed, but not necessary. Then Select ADD PHONE NUMBER

You may also see a I HAVE A LANDLINE checkbox. Please check this if you only have a landline and require a call instead of an SMS/Text.



If you click I HAVE A TABLET, skip down and follow the TABLET instructions.

← Back

Is this correct?

(208) 994-1039

Yes, it's correct

[No, I need to change it](#)

Secured by Duo

Verify the number is correct, then select YES, IT'S CORRECT

Or select NO, I NEED TO CHANGE IT, and correct any mistakes

If your device is a Smart Phone, DUO needs to verify that you have this device/number in your possession and at your disposal, in order to validate that you may use it.

Select SEND ME A PASSCODE, if you want to receive a SMS/Text to verify the device is in your possession.

Select OR CALL MY PHONE, if you want to receive an audio Phone Call to verify the device is in your possession.

← Back

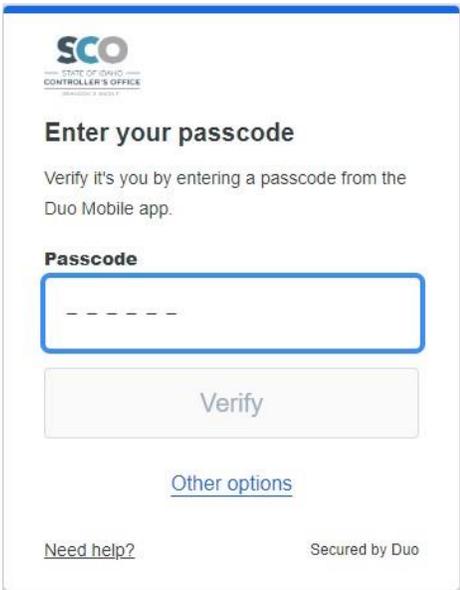
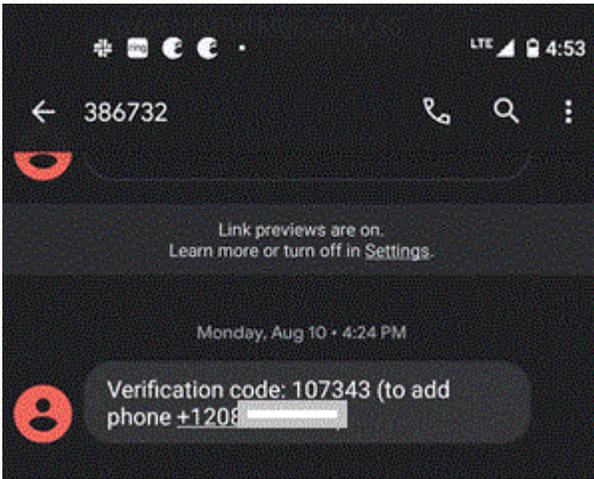
Confirm ownership

(208) 994-1039

Send me a passcode

[Or call my phone](#)

Secured by Duo



The text 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 device verification will say: Verification code:

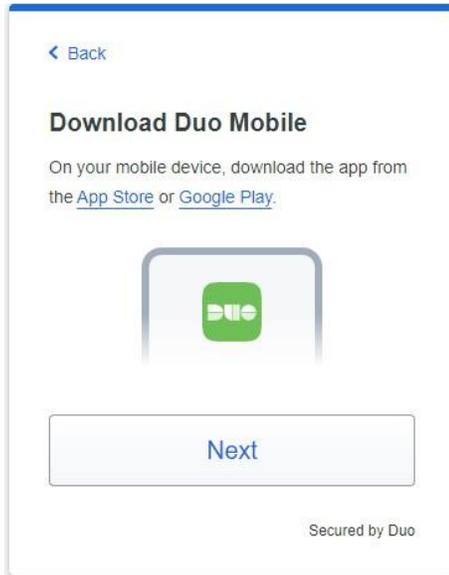
*****IMPORTANT*** If you receive this SMS Text and have not pressed the DUO Enter a Passcode button in the last 60 seconds or so, please ignore the text.**

Simply enter the 6-digit verification code into the field displayed. Then Select VERIFY

Selecting OTHER OPTIONS will allow you to change your mind on the authentication method and select something else.

The call will come from an 817 number, and is an automated voice. It will state “Your verification code is #####.” This will be repeated 3 (Three) times.

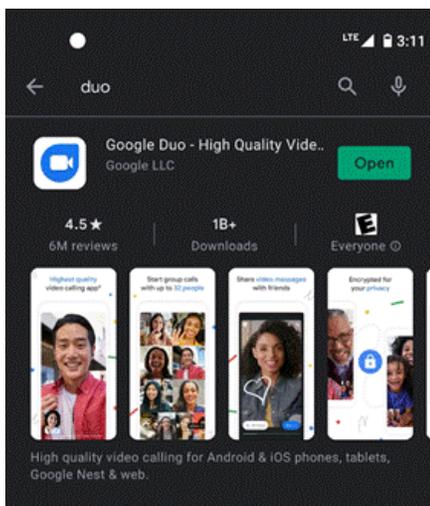
Tablet: If you have a tablet, start below:



For Smart Phones and Tablets, you are then instructed to Install DUO Mobile from your phone's App Store.

Select NEXT when the app has been installed OR if you already have DUO installed for use in your own agency.

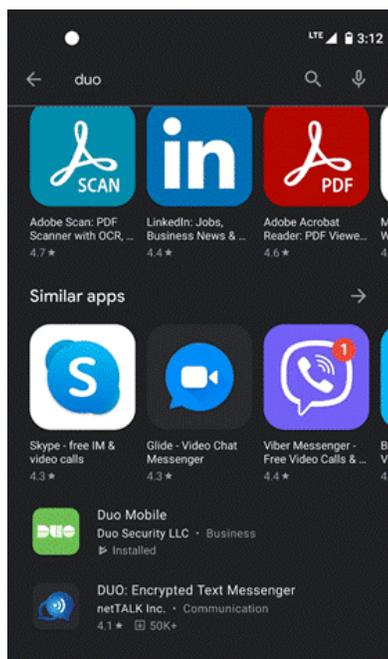
***Even if you already use DUO for your own agency, you still must continue this device registration process to use DUO for the SCO Enterprise Dashboard and Luma.**



If you DO NOT have DUO Mobile app installed on your device, access your App Store and install it now.

Be sure to search for “duo mobile”. If you search for “duo”, you will see Google Duo as the first result. ****THIS IS NOT the correct app****

In this case, scroll down further and you will see DUO Mobile as another result. Select DUO Mobile and tap the Install button to install it.



[← Back](#)

Scan this code in Duo Mobile

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



[Get an activation link instead](#)

Secured by Duo

On this screen, follow the instructions summarized below to enroll your smartphone device with DUO Mobile. This will require using your phone camera to "capture" the QR code displayed on the browser.

If you select GET AN ACTIVATION LINK INSTEAD, it will send you an email to your DUO registered email address with an activation link. You **MUST** open this email on your **SmartPhone** and click the link in order for this method to work.

Open the DUO Mobile app.

The "+" option is on the top right of the DUO Mobile app.
Select the + (PLUS) sign.

You will notice that your rear-facing camera activates on your smartphone and you can see what the camera is displaying on the smartphone screen.

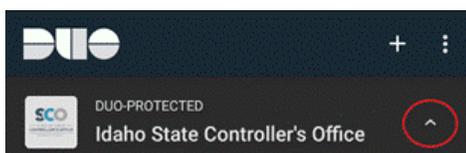
At this time, hold your smartphone right up to the computer screen where the square barcode is displayed. The screen will flash and you should see a message stating Account Created or Account Added.

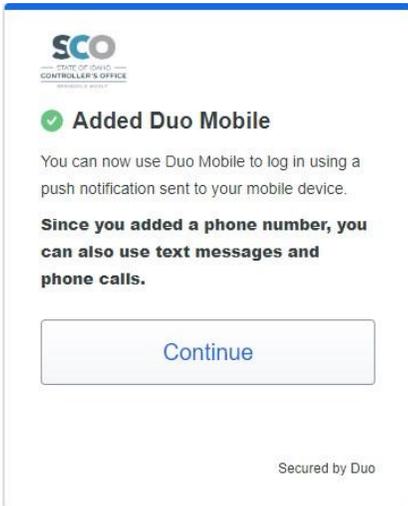
If you try for several minutes and your phone cannot properly scan the barcode on your computer screen, select the GET AN ACTIVATION LINK INSTEAD link.



DUO Mobile will now display this account in your smartphone app, and the Dashboard sign-in screen will display a green checkmark as displayed, showing you have successfully activated this device in DUO Mobile.

Select CONTINUE.

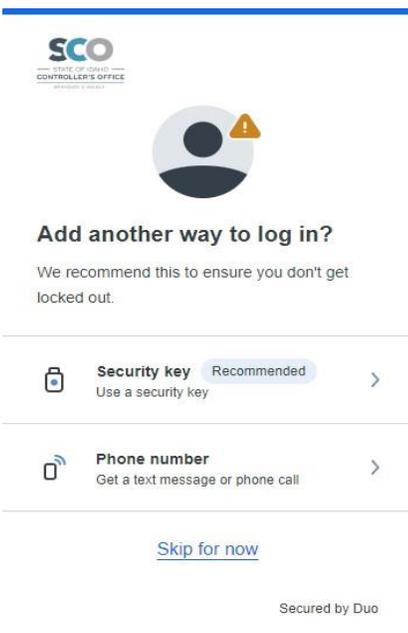


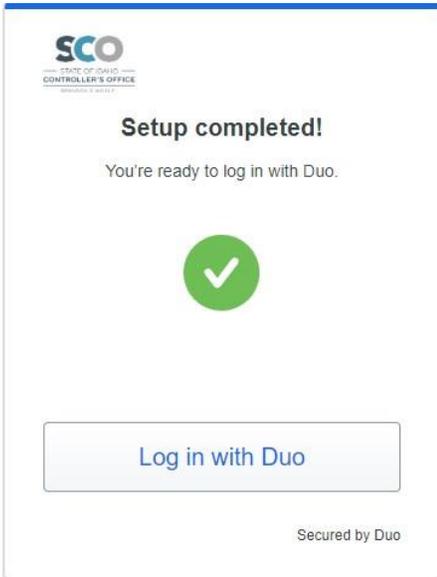


DUO will then prompt you to add another way to log in, which is a best practice when using MFA.

Feel free to add a secondary device that you can use to authenticate with DUO, for instance, if you forgot your Smart Phone at home, you could add your office desk phone using the PHONE NUMBER option. You could then use this device in the case where you forgot the first one.

Select SKIP FOR NOW if you do not need or want to setup a secondary device at this time.



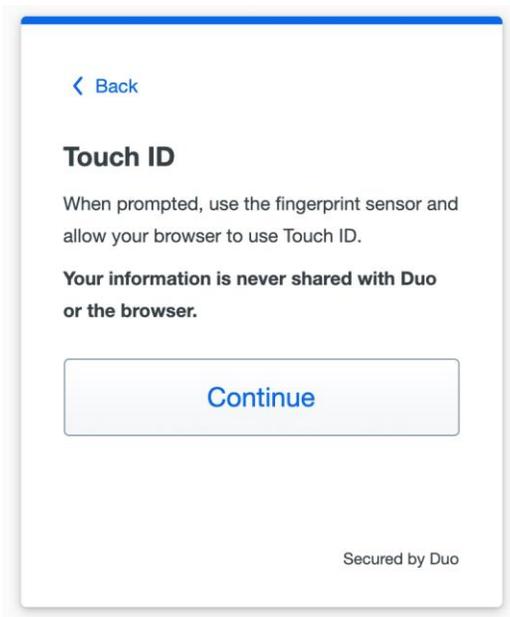


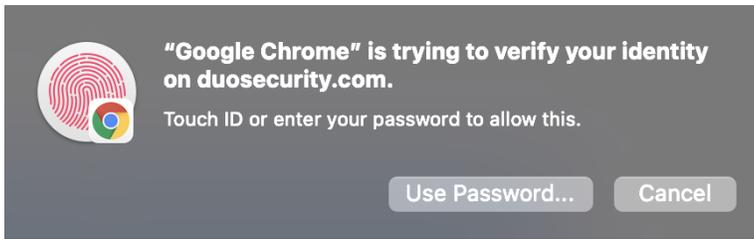
Once your MFA device is validated, you will see this screen.

You have fully and successfully enrolled your device or phone number with DUO.

Select LOG IN WITH DUO to proceed with the sign in process.

Read the Touch ID information and select CONTINUE

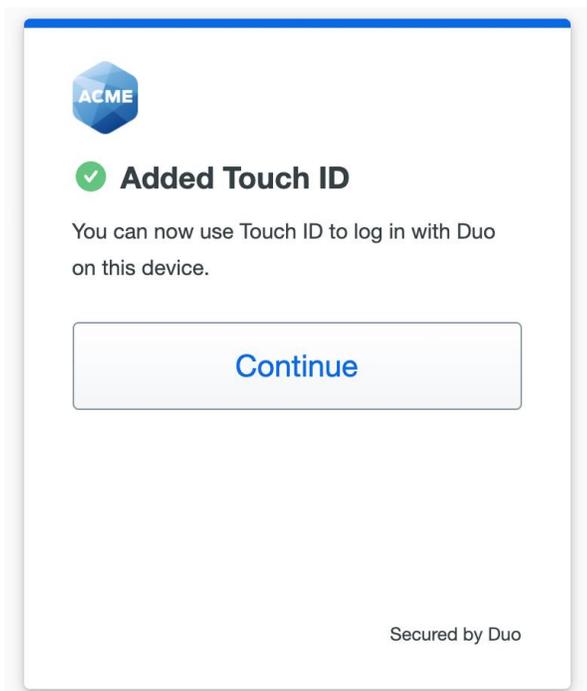




Chrome prompts you to verify your identity on duosecurity.com. Some browsers prompt may look slightly different, but read the guidance on the window and it will direct you on what you need to do.

Place your finger on the Touch ID button in the Touch bar to complete Touch ID enrollment.

When you receive confirmation that you added Touch ID as a verification method, select CONTINUE.





FIPS 140-2
VALIDATED

SECURITY KEY

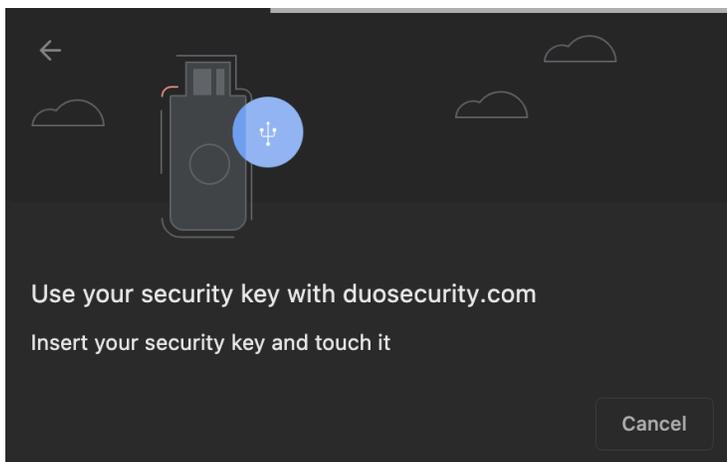
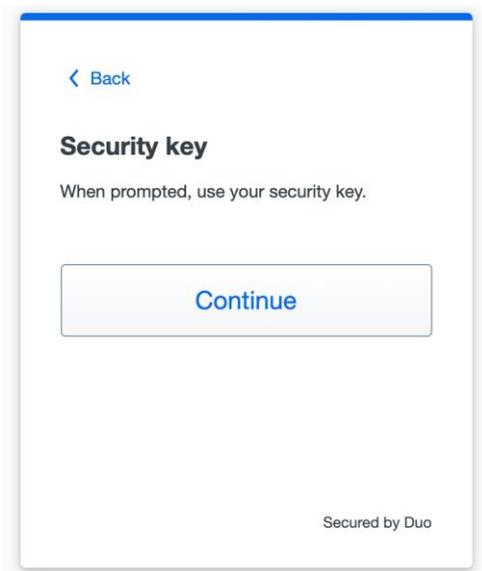
Since DUO is protecting government data, the Idaho SCO recommends a key that is FIPS 140-2 compliant, meaning that it meets a global standard of security for government data.

SCO recommends the Yubikey 5 NFS FIPS, and can provide these keys to agencies at an agreed-upon cost.

<https://www.yubico.com/product/yubikey-5-nfc-fips/>

Keys are very lightweight and of solid build. They can withstand being on a keychain or lanyard without damage. There is a hole provided in the key for attachment to such. Keys have no battery and are passively powered, and therefore, have no expiration. The circle with the "Y" on it is a touch-sensitive button with a light. During the authentication process, the "Y" flashes green to notify the user that a touch is required. The user must press the button for at least 1 second or it is not recognized as a touch.

Read the security key information and select CONTINUE



The security key is detected as an external USB HID keyboard. Because of this, it is not blocked by Windows Group Policy denials on USB Removeable storage devices.

Yubikeys interact with the browser and OS directly for prompt windows. Some browsers display the prompts with slightly different order or wording, but generally when a security key is registered, the first prompt asks the user to plug in the security key (if it is not already plugged in), the next prompt asks the user if the browser can interact with the key, and then the user is prompted to touch the key.

For authentications, only the first and last prompt are shown. If a key is already plugged in, the user is only prompted once to touch the key button.

Upon successful engaging of the Security key button, the key is registered and the user may select CONTINUE.

