

WSU Tech VPN FAQ

We have updated the way VPN works! Please read below and if you have questions please reach out to WSU Tech IT.



Why are we doing this?

Our VPN services are important for our ability to operate; however, like all remote technologies they give bad actors the same abilities. As the education sector is highly targeted, WSU Tech is working to keep ahead of the threats by making changes to the way VPN operates to protect our institution.

VPN services are the most highly targeted services. We need to protect our students and the institution!

Who does this impact?

These services are not required and are optional for those with a specific need. If you do not have that need, you can stop here.

This impacts anyone that has used the Fortinet VPN service. This does not impact those using Remote Desktop Services (RDS). If you are currently using RDS and it meets your needs, no more action is required.

What are the new VPN portals?

Employee VPN

There is now an employee VPN portal – This is only to be used by staff and facility for accessing the WSU Tech network. This portal provides general access to the WSU Tech network, much like the old VPN setup. However, there is a change: this portal can only be accessed via a device that is owned and operated by WSU Tech. Personal devices will be rejected as part of the login checks. Multi-Factor Authentication (MFA) is required to access VPN services.

Student VPN

Student VPN is only used for specific programs where remote desktop services are not able to meet specific program needs. This VPN gives highly limited access for only those programs. If you are an instructor with a need for your students to use the student VPN, contact IT prior. As student VPN has limited access, students are able to use personal devices. MFA is also required to access student VPN.

I am a remote worker; how does this impact my remote work?

If you are a full-time remote worker:

If you use Remote Desktop Services (RDS) today, and that solution works for you, no change is required.

If you are a full-time remote worker that is currently using a personal device for full-time remote work, please contact IT and your manager to get you issued a WSU Tech owned and managed device.

If you are a hybrid worker, or work from home some of the time:

If RDS has been working for you, no changes are required. If you need VPN to work from home, and you do not have a WSU Tech laptop or other device please contact IT and your manager.

When will these changes go into effect?

All changes are in effect now.

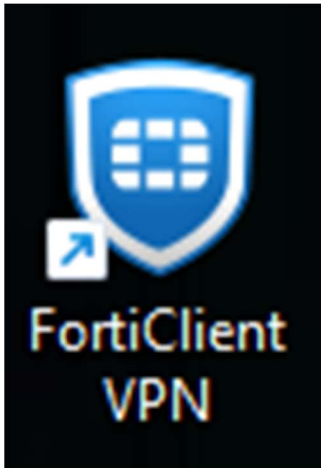
I have questions that are not addressed here

Please reach out to IT or, if it is related to remote work, your direct manager.

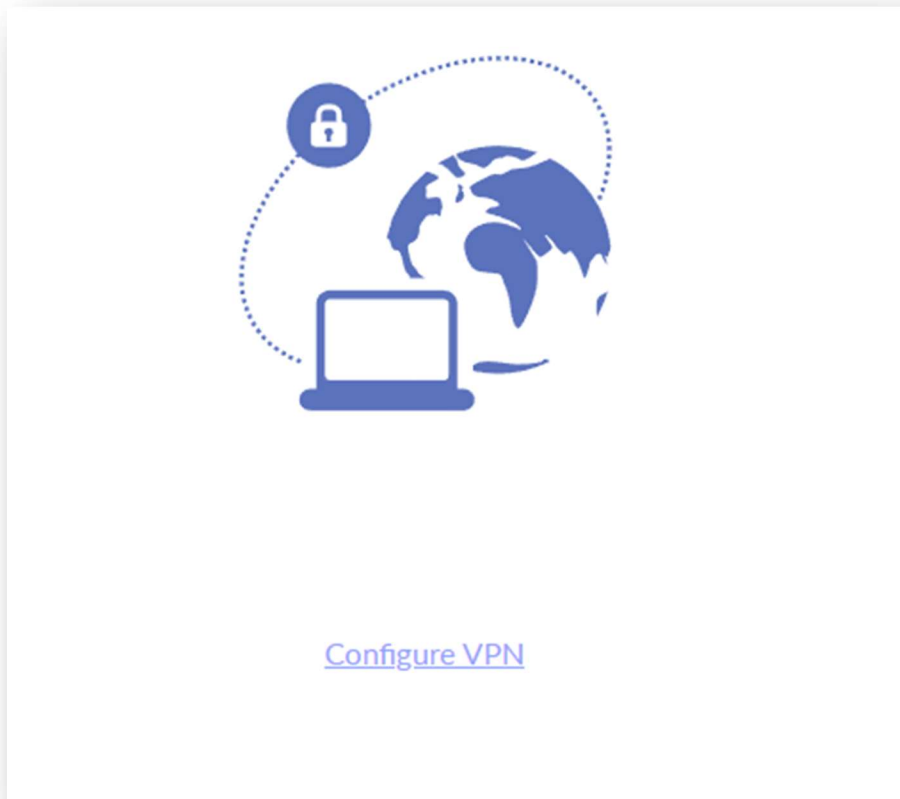
How To Connect to FortiClient VPN

Duo Multi-Factor Authentication (MFA) is required to access WSU Tech Resources on VPN.

1. When you are signed into your device you will see a blue shield for FortiClient. This will be shown on the left side of your desktop.



2. When FortiClient opens, select Configure VPN.



3. Please copy the settings in the picture below into your VPN connection settings and save. **The remote Gateway will need to be adjusted:**

<https://vpn.wsutech.edu:4443/employee>

<https://vpn.wsutech.edu:4443/student>

New VPN Connection

VPN: **SSL-VPN** | IPsec VPN | XML

Connection Name: WSU Tech

Description:

Remote Gateway: vpn.wsutech.edu ✕
+Add Remote Gateway

Customize port: 4443

Single Sign On Settings:

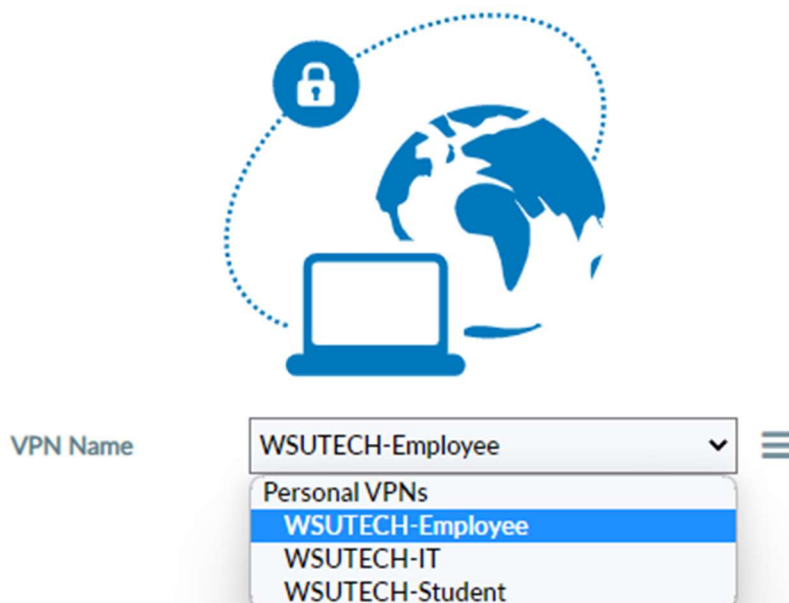
- Enable Single Sign On (SSO) for VPN Tunnel
- Use external browser as user-agent for saml user authentication
- Enable auto-login with Azure Active Directory

Client Certificate: None ▾

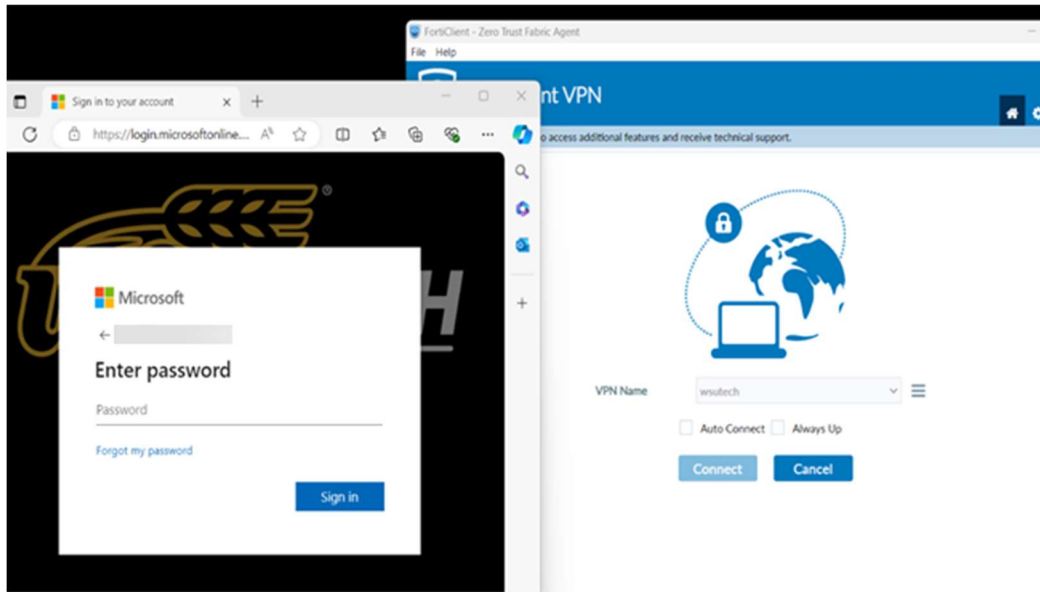
Enable Dual-stack IPv4/IPv6 address

Cancel Save

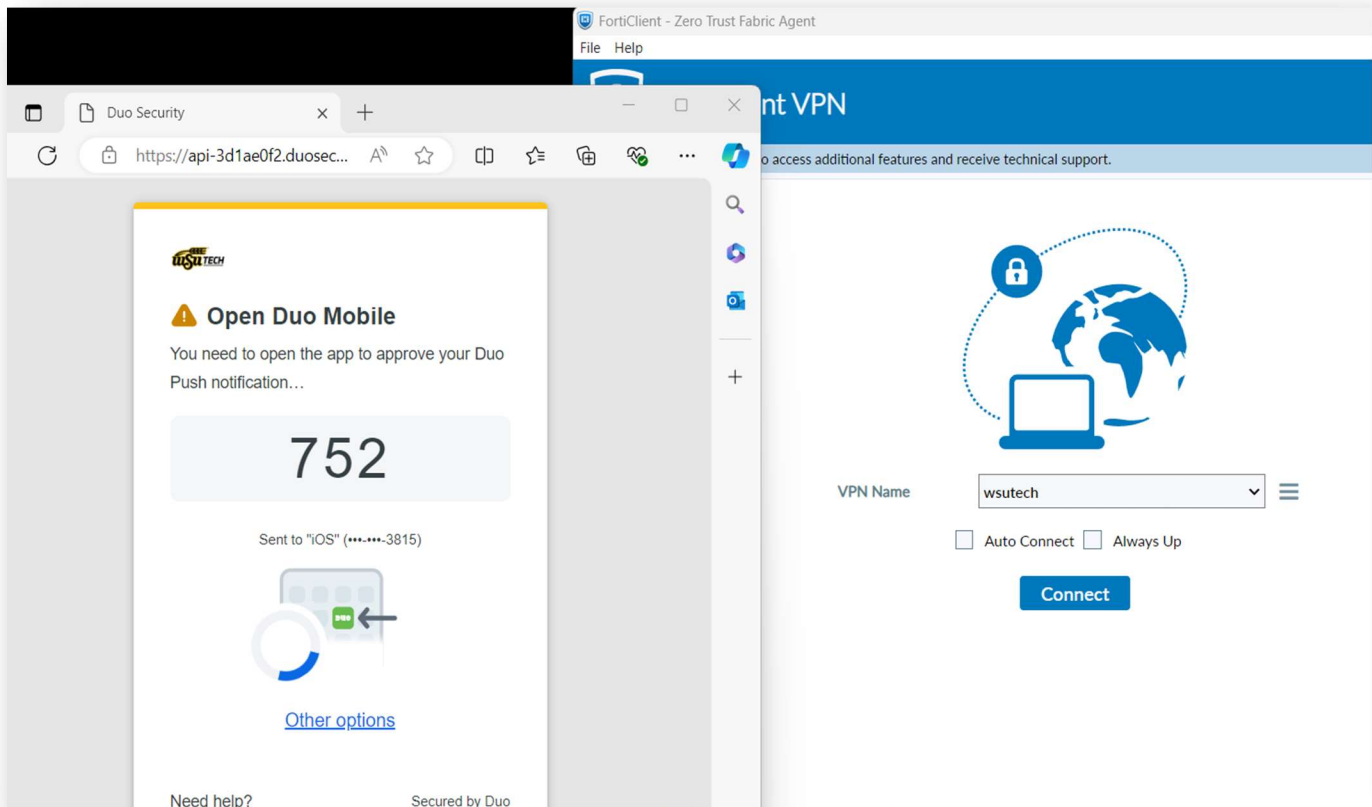
4. Open the FortiClient. Press Connect to log into the VPN. On the next step, an external browser will open for you to sign in with your WSU Tech credentials.





5. The external browser will open a Microsoft login page for you to authenticate with your WSU Tech email and password. After selecting sign in, you will be prompted to use Duo for MFA:



6. Next, open Duo on your mobile device to approve your Duo push notification to get connect to VPN. Step.11 will show the established connection of an active VPN. **Please follow the instructions below if Duo is not set up or downloaded onto your mobile device.**
7. If you do not have Duo set up: You will be presented with the “Welcome to Duo Security” page. Please press **Get Started** after signing in with your WSU Tech Microsoft account.




Welcome to Duo Security

Your organization uses Duo Security to protect your identity. Create an account to get started.

[Learn more about Duo](#)





[Get started](#)

8. Select **Duo Mobile** to then enter in a phone number that you would like to set up Duo with.



First, add a device

You'll use this to log in with Duo. You can add another option later.

-  **Windows Hello** Recommended >
Use Windows Hello on this device
-  **Duo Mobile** >
Get a notification or code on your device
-  **Security key** >
Use a security key
-  **Phone number** >
Get a text message


[Need help?](#) Secured by Duo

[< Back](#)

Enter your phone number

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

Country code **Phone number**



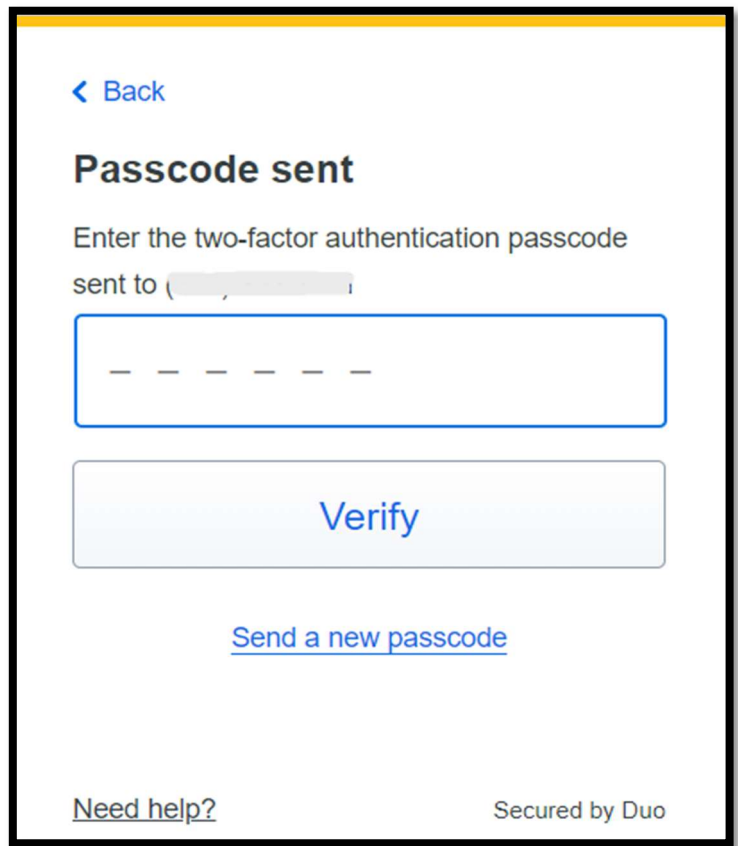
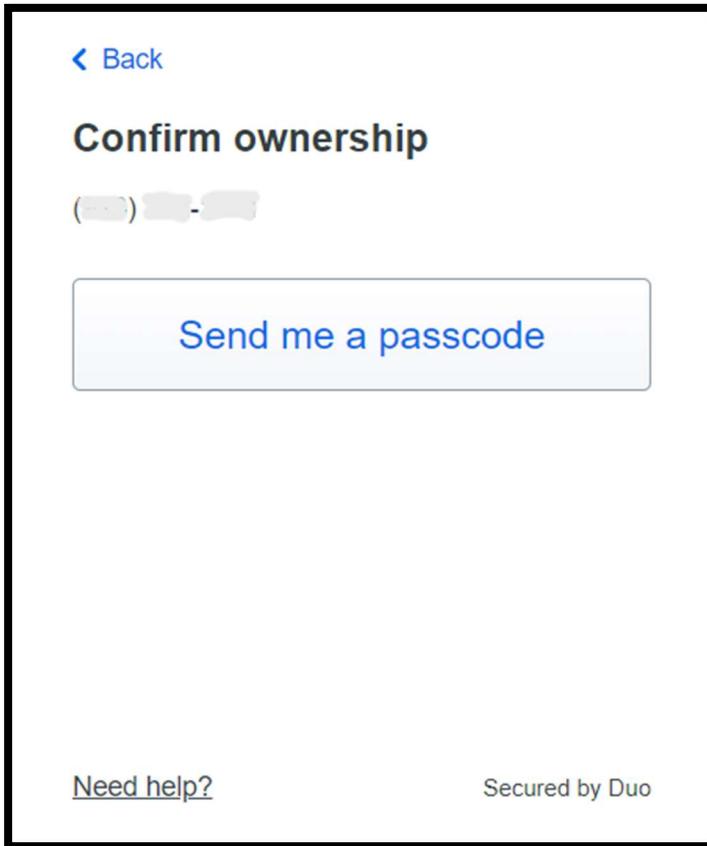
Example: "201-555-5555"

[Continue](#)

[I have a tablet](#)

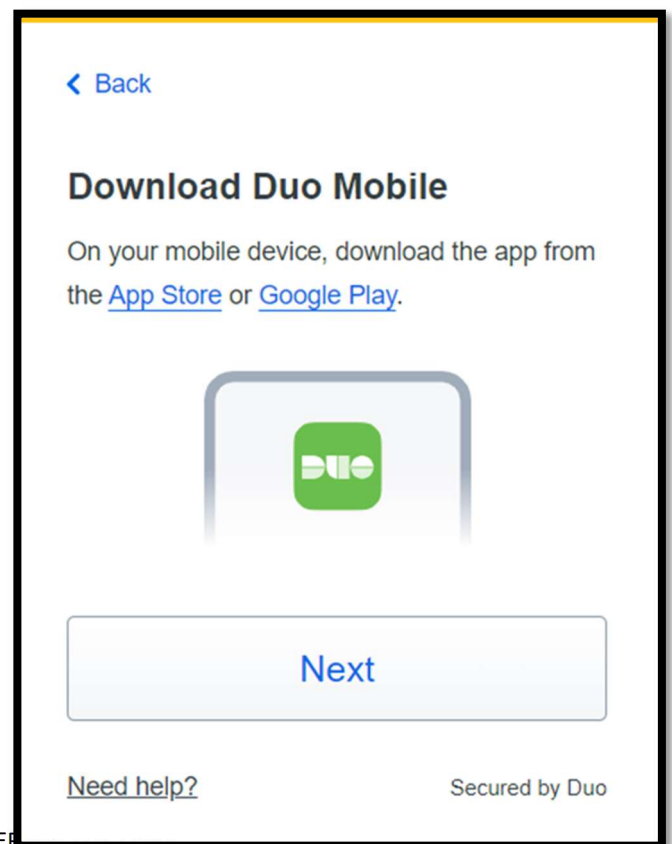
[Need help?](#) Secured by Duo

9. To confirm ownership of the number being used for Duo press **Send me a passcode** to verify the code that will be sent to your mobile device.

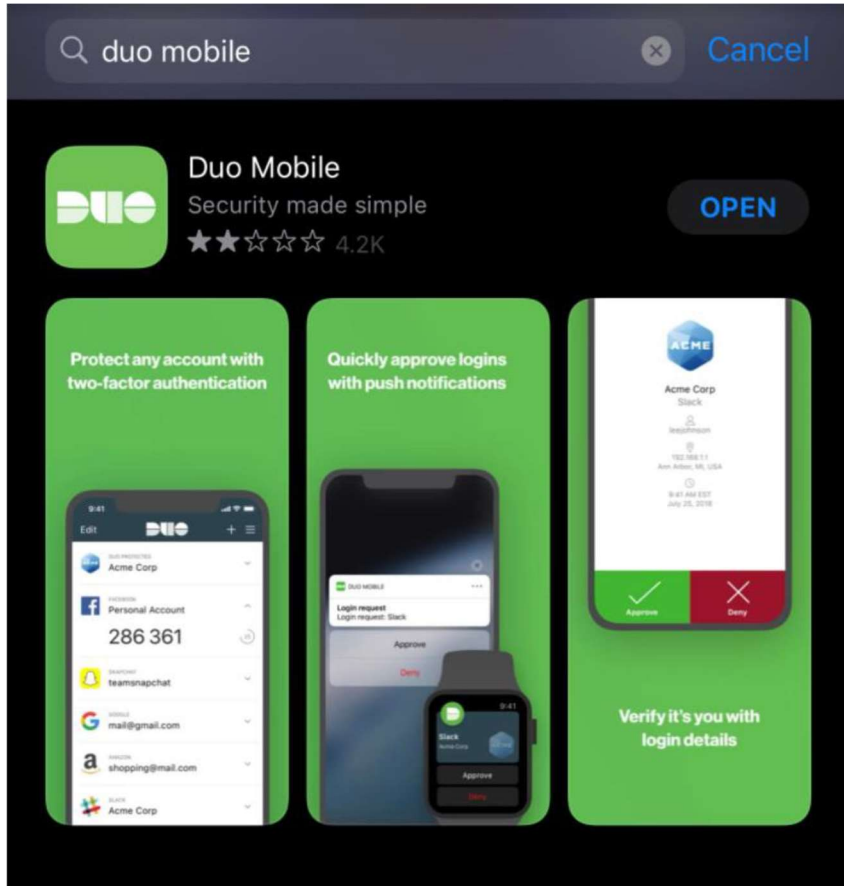


10. Now that you have verified your phone number to set up Duo,

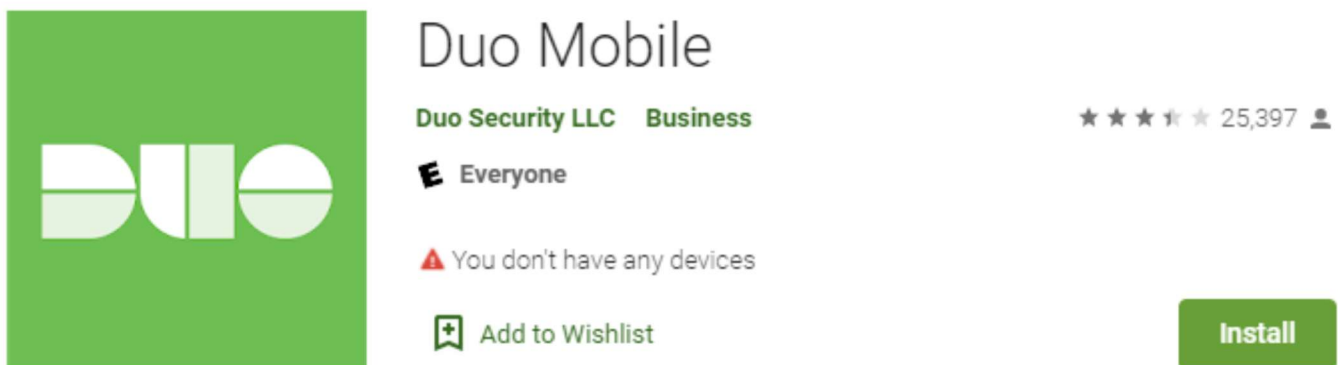
Please download the Duo Mobile app.



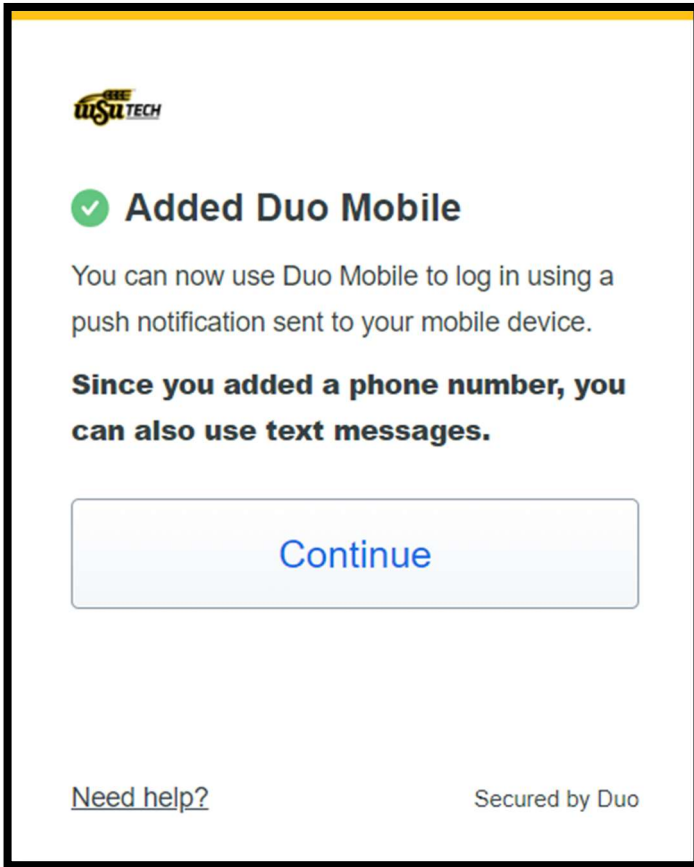
For iOS users, open the App Store and search for the “Duo Mobile” app. Tap the **Get** and then **Install** buttons.



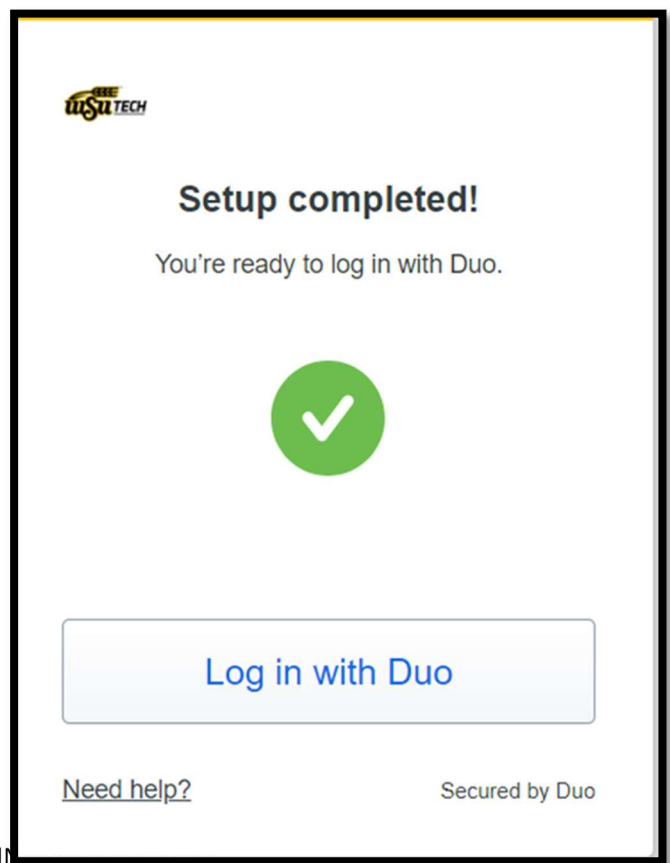
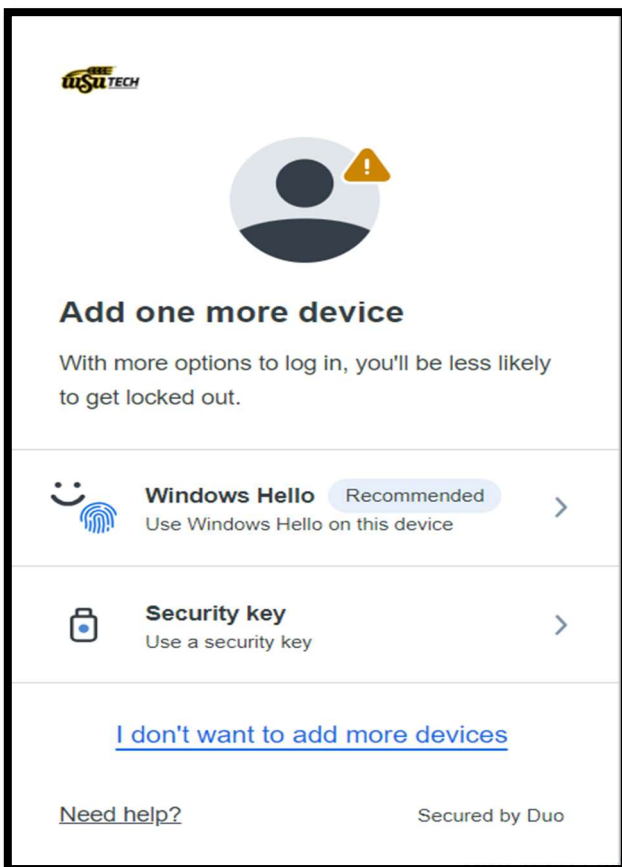
For Android Users, open the Google Play Store and search for the “Duo Mobile” app. Tap the **Install** button.



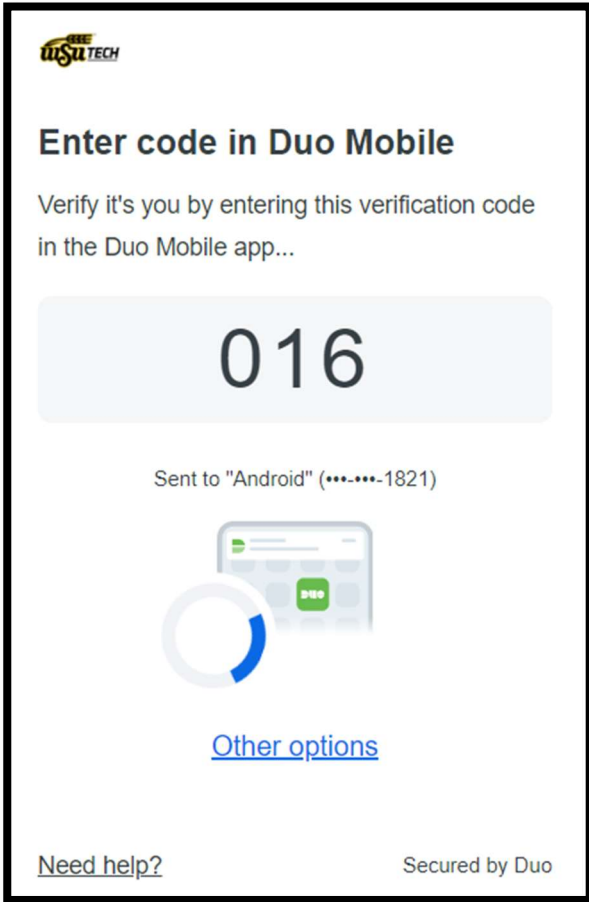
11. Now that Duo is installed you can continue.



12. If you do not wish to add an additional device...Please continue by selecting 'I don't want to add more devices' to complete the set up and sign into Duo.



13. Next, open your mobile device to verify the code on your Duo Mobile app to finalize the access to connect to the VPN.



14. You are now connected to the VPN.



VPN Name WSU TECH
IP Address [REDACTED]
Username [REDACTED]@wsutech.edu
Duration 00:02:05
Bytes Received 0 KB
Bytes Sent 82.29 KB

Disconnect