

Cisco Secure Client VPN Connecting on an Android Transcript

This video will walk you through how to connect to the NAU Cisco Secure Client VPN on an Android using Two-Step Verification. Please note this video was filmed using a Google Pixel 7. First, you need to ensure your account has been configured to use Two-Step Verification. To learn how to do this, please view the knowledge base article on the ITS website or visit <https://id.nau.edu/two-step>. You will also need to ensure you have Cisco Secure Client installed on your device. Please view our other training videos on how to download Cisco Secure Client.

Once your account is configured to use Two-Step Verification and you have Cisco Secure Client installed on your device, open Cisco Secure Client on your device. If this is the first time you are using Cisco Secure Client on your Android, you will need to agree to the license agreement. Tap “ok”. Tap “Connections”, tap the plus sign in the lower right-hand corner. In the “server address” field, enter “vpn.nau.edu”. Tap the checkmark on your keypad, then tap “Done”. Tap the back arrow in the upper left-hand corner. Tap the button next to “AnyConnect VPN”. You will be prompted to enter your NAU userid and password in their respective fields. In the “second password” field, enter “push” to send a push notification through DUO mobile, or enter the 6-digit verification code provided to you by either your two-step fob, or from within the Duo Mobile phone app. Tap the checkmark on your keypad, then tap “Connect”. If you enter “push” you will receive a notification from your Duo Mobile app. Tap the Duo alert and then tap the green check mark to approve this access. Please note: First time users will need to confirm the connection request the first time they use the connection, tap “ok”.

You are now connected to the NAU Cisco AnyConnect VPN on your mobile device.

It is important to remember that if you ever receive the Two-Step notification when you are not trying to access a site on your own to tap the red X to deny access and notify ITS as soon as possible.