Multi-Factor Authentication (MFA) Methods

Authentication Methods

It is very helpful to add additional authentication methods. This way if you're having trouble logging in, you can easily switch to a different method. Currently, there are five methods: Duo Mobile app, Passcode, Phone Call, U2F Authenticator, & Cisco AnyConnect.

If you're ever having trouble logging in (for instance: don't have your smartphone, don't have a wireless connection for your smartphone, or forgot your Duo Hardware Token) switch to a different authentication method. Click Cancel and choose one of your other methods.

Go to https://my.logon.ucla.edu and Sign In. This will bring up the authentication screen:

To add an additional authentication method, click Cancel and then click Add a new device. Shibboleth will first need to confirm it's you. Choose an authentication method to gain access. Then, choose your device type on the What type of device are you adding? screen. Click Continue and enter the required information.

It's also very helpful to automate a preferred authentication method. This will speed things up when you’re logging in. To set this up, click My Settings & Devices. Choose your Default Device. Then click the pull-down menu next to When I log in: and choose Automatically send this device a Duo Push.

Authentication Using Duo Mobile app
Tap on the notification on your smartphone or tablet to open the Duo Mobile app. Tap on Approve.

1. In many instances what actually happened is the user simply missed the notification. In this scenario, if the user opens their Duo Mobile app they will see their push waiting for them.
2. If #1 does not work, refresh the Duo Mobile app with pending pushes by doing a swipe-down from the top or your smartphone screen. This works very similarly to the email program. You do a swipe down, and you see the twirly at the top spinning to indicate a refresh is underway. Then, the push appears and all is well.
3. If neither #1 or #2 works, return to the website and have the push resent from there.

For iPhone 6S, iPhone 6S Plus, and iPhone 7 users: force touch the notification. This will bring up an Approve button. Tap approve. No need to open the Duo Mobile app.

For Apple Watch users: press approve on the Duo Mobile app on your watch.

Authentication Using Passcodes

Go to my.logon.ucla.edu and authenticate using your username/password, but then click Cancel.

Receive a text message with 10 seven-digit single-use passcodes as the second factor. Remember to keep these passcodes handy as backups.
Click Text me new codes.

Here is an example of a text message with passcodes.

Each passcode starts with the numbers 1 through 0. Enter the next passcode when requested by the UCLA Single Sign-On website. The website will tell you which one, i.e. "Your next SMS passcode starts with 3." Each passcode can only be used once. When you run out, you'll automatically be texted more passcodes.

SMS passcodes:
1594167  2346465
3406255  4390974
5386577  6612383
7934346  8210795
9138241  0713921
Press the button on your Duo Hardware Token generator to generate a six-digit passcode. Enter the passcode into the UCLA Single Sign-On website. You must do this within 10 minutes, or the passcode times out.

Tap the key icon to generate use-once passcode (does not require network connection).

Then tap passcode to copy it.
Click Enter a Passcode.

The passcodes come from the Duo Hardware token, Duo Mobile app, or SMS text message.

Enter the passcode and click Log In.
Authentication by *Phone Call*

Your smartphone, cell phone or landline will ring. You answer and hit any key. You’re done!

Authentication by *U2F Authenticator*
Insert the U2F into a USB port (if it's not already there). Press the button on the U2F. You're done.

**Authentication with *Cisco AnyConnect***

How you log in from home (or while away at a conference) using the Cisco AnyConnect VPN will depend on your Authentication Method:

For more information: [Authenticating Using Multi-Factor Authentication on the Campus VPN](#)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | After entering your password in Cisco AnyConnect, tap Approve in the Duo Mobile app to complete your VPN login. **What to do if you do not receive the Push notification:**  
   1. In many instances what actually happened is the user simply missed the notification. In this scenario, if the user opens their Duo Mobile app they will see their push waiting for them.  
   2. If #1 does not work, refresh the Duo Mobile app with pending pushes by doing a swipe-down from the top or your smartphone screen. This works very similarly to the email program. You do a swipe down, and you see the twirl at the top spinning to indicate a refresh is underway. Then, the push appears and all is well.  
   3. If neither #1 or #2 works, it might be due to a weak Digital Cellular or WiFi connection for the smartphone. Instead, switch input methods. Open your Duo Mobile app and tap the key icon. This generates a use-once passcode. This works even with no network connection. Enter your password in Cisco AnyConnect followed by / and your passcode. For instance: `mypassword/123456` |
| 2.   | Enter your password in Cisco AnyConnect followed by `/` and your passcode. For instance: `mypassword/123456` |
| 3.   | After entering your password in Cisco AnyConnect, answer your phone and hit any key to complete your VPN login |
| 4.   | After entering your password in Cisco AnyConnect, Press the button on the U2F to complete your VPN login |