Overview

This job aid describes how to connect to VPN using Duo Mobile. The method you use to log in depends on a number of issues, including: the device you enrolled with Duo Mobile, if you need to use a different method than your default (or primary), if you’re traveling, and more.

Contact the Service Desk (734-936-8000) if you need further assistance.

Have the following items with you:
- Your computer
- Your U-M Duo registered device

Table of Contents

Overview........................................................................................................................................... 1
Duo Mobile Push................................................................................................................................... 2
Duo Mobile App Passcode...................................................................................................................... 2
Phone Call............................................................................................................................................... 2
Passcodes via Text Message.................................................................................................................... 3
Duo Hardware Token............................................................................................................................ 3
Temporary Passcode............................................................................................................................. 4
Advanced Login Feature (Switching Authentication Options at the Login Screen)......................... 4
Login Considerations When Traveling.................................................................................................. 5
ReSync Hard Token............................................................................................................................... 5
Duo Mobile Push

1. Go to the start menu of your computer then click Cisco AnyConnect Secure Mobility Client.
   - If prompted, click Connect.

2. Enter your username.
3. Enter your Level-1 password.
4. Click OK to trigger the U-M Duo Two-Factor process.

Duo immediately sends a notification to your mobile device. Depending on how you configured notifications for your device, you may need to open the notification.

5. Complete the approval process using your smart device.

Duo Mobile App Passcode

1. Open the Duo Mobile application on your mobile device.
2. Tap the key icon to generate a six-digit passcode.
   - If the key icon changes color, this indicates that you exceeded the time limit for using the passcode. If this happens, simply tap the key again to generate a new passcode.

3. Go to the start menu of your computer then click Cisco AnyConnect Secure Mobility Client.
   - If prompted, click Connect.

4. Enter your username.
5. Enter your Level-1 password followed by ^#### (the six-digit passcode generated by the Duo Mobile application. Example: mypassword^123456).
6. Click the OK button to trigger the U-M Duo Two-Factor process.

Phone Call

1. Go to the start menu of your computer then click Cisco AnyConnect Secure Mobility Client.
   - If prompted, click Connect.
2. Enter your **username**.
3. Enter your **Level-1 password**.
4. Click **OK** to trigger the U-M Duo Two-Factor process.
   - This initiates a phone call to the number you registered with your U-M Duo account.
5. Answer the **phone call**.
   A. Press 1 on your phone to complete the process.
   B. Press 9 to report fraud if you did not initiate the U-M Duo Two-Factor process.

### Passcodes via Text Message

1. Go to the start menu of your computer then click **Cisco AnyConnect Secure Mobility Client**.
   - If prompted, click **Connect**.
2. Enter your **username**.
3. Enter your **Level-1 password** followed by `^SMS` (Example: mypassword^SMS).
4. Click the **OK** button.
   - This sends a text message to the device you registered.
5. Open the **text message** on your device.

   - The text message includes a group of 10 passcodes. These passcodes last for 12 hours.
6. Return to the Cisco AnyConnect Secure Mobility **log in window**. Your *username* should already appear by default.
7. Enter your **Level-1 password** followed by `^########` (the six-digit passcode retrieved from the Duo text. Example: mypassword^123456).
8. Click the **OK** button to trigger the U-M Duo Two-Factor process.

### Duo Hardware Token

1. Generate a six-digit passcode by tapping the **green button** on your hardware token.
2. Go to the start menu of your computer then click **Cisco AnyConnect Secure Mobility Client**.
   - If prompted, click **Connect**.
3. Enter your **username**.

4. Enter your **Level-1 password** followed by ^##### (the six-digit passcode retrieved from the Duo hardware token. Example: mypassword^123456).

5. Click the **OK** button to trigger the U-M Duo Two-Factor process.

**Temporary Passcode**

1. Contact the Service Desk (734-936-8000) and request a temporary passcode (valid for 12 hours).

2. Go to the start menu of your computer then click **Cisco AnyConnect Secure Mobility Client**.

   - If prompted, click **Connect**.

**Advanced Login Feature (Switching Authentication Options at the Login Screen)**

This feature is useful when you want to use a method other than your primary/default option - it is recommended that you have multiple devices/phones registered. Example: having two landlines registered and needing to use a secondary.

1. Go to the start menu of your computer then click **Cisco AnyConnect Secure Mobility Client**.

   - If prompted, click **Connect**.
2. Enter your **username**.

3. Enter your **Level-1 password** followed by **one of the commands below**. The command overrides your default authentication option.

   **A.** Push commands: use one of these options to have a push notification sent to a different device.
   - ^push1: The first device registered to your U-M Duo account.
   - ^push2: The second device registered to your U-M Duo account.
   - ^push3: The third device registered to your U-M Duo account.

   **B.** Phone call commands: use one of these options to have a phone call initiated to a different phone (landline or cell phone).
   - ^phone1: The first device registered to your U-M Duo account.
   - ^phone2: The second device registered to your U-M Duo account.
   - ^phone3: The third device registered to your U-M Duo account.

4. Click the **OK** button to trigger the U-M Duo Two-Factor process.

**Login Considerations When Traveling**

- **International travel**
  - If you purchase a phone for use abroad or take a loaner, you can enroll that device in Duo and use it for two-factor authentication when traveling.
    - Enroll the device ahead of time. You’ll need to authenticate using whatever Duo option you have enrolled in when you enroll the new device, so it is best to do that before your trip if at all possible.
    - Use what works. If the device you’re using while traveling is a basic, non-smart phone, you can authenticate using a phone call to it or passcodes sent via text message. You can install the Duo Mobile app on a tablet without a phone number.
  
- **Restrictions apply for some destinations. See Travel to Embargoed Countries for details.**

---

**ReSync Hard Token**

Sometimes Duo hardware tokens can go out of sync with the system. If this occurs, it impacts your login ability and you will not have a successful login. Resyncing your token is the first line of troubleshooting, similar to rebooting a computer when it doesn’t work, or turning off a phone to reset it.

To resync your token:

1. **Go to your profile page**.
2. **Click Security Settings**.
3. **Go to U-M Duo Hardware Token**.
4. **Click the Resync U-M Token button** on your UMHS Profile page. This process will generate three EPCS Duo token passcodes that when entered correctly will complete the resync process.
5. **Press the button** on your U-M Duo token to generate your first passcode.
6. Enter the **passcode**. Wait for the first passcode to disappear from the token window then generate a second passcode.

7. Enter the second **passcode**. Wait for the second passcode to disappear from the token window and then generate a third passcode.

8. Enter the third **passcode**.

9. Click the **Resync Now** button.

10. Click **OK** to the process is complete message.

11. Click **Test U-M Token** button.

12. Generate **passcode** on your U-M Duo hardware token.

13. Enter **passcode** in field.

14. The **Click to Test** button will indicate if the test was successful.

---

**If it still doesn’t work after resyncing, then contact the Service Desk for assistance.**