Duo Multi-Factor Authentication (MFA): Frequently Asked Questions (FAQs)

What is the Duo Multi-Factor Authentication (MFA) service?

The goal of MFA is to create a layered defense to make it more difficult for an unauthorized person to access your information. MFA adds a step to the login process and requires you to prove your identity after entering a CaneID and password by responding to a prompt using a mobile device, landline, tablet, or **token**.

To learn more about MFA, including **an enrollment guide**, please review the "*Reference Material for MFA*" section below.

Who will use the Duo MFA service?

Any University of Miami faculty or staff member who uses any **University of Miami Single Sign-On (UMSSO)-enabled application or service**, such as Blackboard, CaneID, CaneLink, MyUM, and/or Workday, will have access to this service. At this time, the service is available via opt-in enrollment.

When will I need to use the Duo MFA service?

Multi-factor authentication is used to access any UMSSO (Single Sign-on) enabled applications/service, including Blackboard, CaneID, CaneLink, MyUM, Workday, etc.

Why should faculty and staff at UM use the Duo MFA service?

With increasing security attacks across higher education institutions, passwords alone are not a sufficient way to protect resources. Duo MFA decreases the risk of a compromise.

What data is stored by Duo MFA?

The only data that Duo stores for is the subscriber's CaneID (Duo does <u>NOT</u> know your password) and information about your second factor, such as a phone number (if using a phone for the service) or the serial number of your **token** (if not using a phone for the service).

What if I lose my phone?

Contact the UMIT Service Desk at (305) 284-6565 or itsupportcenter@miami.edu immediately if your phone is lost or stolen. The UMIT Service Desk will disable it for authentication and assist you to register another device. Remember: Your CaneID and password (first-level authentication) will continue to protect your account even if your phone is lost.

I am going to be traveling abroad. How can I continue to use Duo MFA?

In a perfect situation where you have Internet access, and the Duo mobile application is installed, activated, and running on your mobile device, the push method is best. If you don't have Internet access, you will be able to receive an SMS text or a phone call from Duo to verify your authenticity. If your phone is on airplane mode (no Internet access or phone service), you can still authenticate using a Duo passcode (just select the key symbol on the Duo Mobile app screen and generate a passcode).

Do I need a smartphone to use Duo MFA?

A smartphone is the best choice since it provides the greatest level of security and allows you to use the Duo Mobile app. The app generates passcodes for login and can receive push notifications for easy, one-tap authentication. However, a smartphone is not required to use the service. You can also select a landline or get a **token**.

I don't have a smartphone. Will I be able to Duo MFA on my regular cell phone?

Yes, any cell phone will work, but it will not include the advantages of the Duo Mobile app (passcodes, prompts, etc.) and may result in regular cell phone charges in order to call back and authenticate (depending on your phone service).

What if I wanted to use a landline at my office instead of my personal phone?

You may use a landline instead of a mobile device; however, you need to take into consideration the stationary nature of a landline. Even if you work almost exclusively at your desk in your office (where the landline is located), you might on rare occasions need to have access to your UM-protected services from home or from a remote location (such as a conference).

I have a Windows tablet, but it does not seem to be compatible with Duo MFA. What should I do?

Certain Windows platforms are not supported by Duo Mobile, so they will not work with MFA. Specifically, those with a full Windows operating system are not supported. Those with a mobile operating system, such as Windows Phone or Windows Mobile, are supported (and will work for MFA).

If the Windows platform on your device does not have an App store and is not supported, then there are a number of other device options available to enroll.

Can I use multiple phones, or am I restricted to one phone?

You can set up Duo MFA on multiple mobile devices (phones, tablets, etc.).

Can I change to a different phone with a different number after I have the Duo MFA service?

Yes, you can change to a different phone with a different number. You will need to reactivate Duo MFA on the new device, and if it's a different type of device (for example, if you're going from Android to iPhone), then you will need to make sure that you select the new phone type before reactivating.

Does the Duo Mobile app access other apps or data on my phone?

It does not access your other apps or other data on your phone; it uses some base functionality of the phone and a certificate that identifies your phone to ensure accurate identification.

I'm having a problem finding the Duo Mobile app in my smartphone's app store.

If you are having a problem finding the Duo Mobile app via search, it can be accessed directly by clicking on the direct link to the application:

- From App Store for iOS/Apple devices: **https://itunes.apple.com/us/app/duo-mobile/id422663827?mt=8**
- From Google Play for Android devices: **https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=en**

I'm often in a location where I have poor cell coverage; how can I use the Duo MFA service?

In cases where cell coverage is not available, use the Duo Mobile app to generate a passcode. If you're not using a smartphone (and therefore do not have access to the app), then generate passcodes in advance.

I use a landline for my Duo MFA service, and I'm going away for a week. Can I still use the Duo MFA service?

Yes, you can forward your service to another phone.

Do the SMS (text) passcodes provide by Duo expire? If so, how long are the passwords available for use?

Passcodes are set to expire in 1 hour and are only good for one use, so once a passcode has been used to authenticate into two-factor authentication, it is expired and cannot be used again.

I'm trying to log into my Duo MFA service on my phone, but it tells me I can't. What should I do?

Before attempting to troubleshoot any multi-factor problem, make sure that your CaneID and password are correct.

If this is the first time that you've used the service on this particular phone, then make sure that the enrollment process has been completed and then try again.

If you've used the service on this phone before and cannot login, then make sure that phone is not locked. If it is locked, then unlock the phone and start the mobile app (if on a smartphone) and try again.

Make sure that you're using the correct mobile device. If you're using a new device (even if you have the same phone number), then reactivate the Duo Mobile app for the new device. (If you're changing types of phone, such as going from an Android to an iPhone, then select the new type of phone before reactivating.)

If the service is still not working, then contact the UMIT Service Desk.

I'm getting an invalid security certificate error when attempting to authenticate using Duo Push on my iPhone. What should I do?

Please try rebooting your iPhone device and retry Duo Push authentication. If problems persist, please contact the UMIT Service Desk to request a re-activation: (305) 284-6565 or itsupportcenter@miami.edu.

The 'Remember me for 30 days' option is grayed-out and cannot be selected. What should I do?

Please first try clearing the cookies from the browser of your mobile or desktop device. Then confirm your browser is configured to allow third party cookies. This option is typically found in the "Advanced or Advanced Options" section within your browser settings.

Duo Multi-Factor Authentication (MFA): Troubleshooting FAQs

Internet Browser Doesn't Remember Me

The "Remember Me" functionality requires persistent cookies in your browser. If your browser is not remembering that you checked the "Remember Me" box, then check the cookie settings of your browser. To find information on the cookie settings of your browser, click the following link to search Google: **browser cookie settings**.

Chrome's "incognito" setting, Firefox's "private window," and Internet Explorer's/Edge's "InPrivate""settings will affect this behavior and the "Remember Me" feature will not work.

"Remember me for 30 days" while Blocking Cookies

If you set your browser to block all cookies, the "Remember Me" feature will not work. To fix this, allow "duosecurity.com" as a trusted exception:

- *Internet Explorer*
    1. Close Internet Explorer.
    2. Click the **Start** button.
    3. Type: **internet options**
    4. As you type, results will appear and change. Select **Internet Options**.
    5. Select the **Privacy** tab.
    6. Under the **Settings** heading, click the **Sites** button.
    7. In the **Address of website:** text box, type **duosecurity.com**
    8. Click the **Allow** button.
    9. Click **OK**.
    10. Click **OK** to close the Internet Properties window.

- *Firefox*
    1. In Firefox, in the top-right of the window, click the hamburger **menu** button represented by three horizontal lines.
    2. Click the **Options** icon.
    3. In the left pane, select **Privacy**.
    4. To the right of **Accept cookies from sites**, click the **Exceptions...** button.
    5. In the **Address of website:** text box, type: **duosecurity.com**
    6. Click the **Allow** button.
    7. Click the **Save Changes** button. You may close the Options tab.

- *Chrome*
    1. In Chrome, near the top-right of the window, click the hamburger **menu** button represented by three horizontal lines.
    2. From the drop-down list, select **Settings**.
    3. Scroll to the bottom of the Settings.
    4. Click the **Show advanced settings...** link.
    5. Under the **Privacy** heading, click the **Content settings...** button.
    6. Click the **Manage exceptions...** button.
    7. Under **Hostname pattern**, in the text box, type: **duosecurity.com**
    8. Verify that the drop-down list to the right is set to **Allow**.
    9. Click the **Done** button.
    10. To close the Content settings window, click the **Done** button.

Duo Mobile App Errors, Problems or Connection Issues, and Duo Push Not Received

Occasionally you may experience connectivity issues between your mobile device and the Duo Mobile app such as not receiving Duo Push notifications or timeout errors. This problem is often resolved by refreshing the Duo Mobile app:

1. If you recently disabled or turned off your phone's airplane mode, wait 5 minutes before proceeding.
2. On your device, start the Duo Mobile app.
3. Between the UM logo and the key, tap and pull down on the window, and then release.
4. The app will be refreshed.

Duo Window Frame Doesn't Load or is Blank

Go to the **Duo Security Status** webpage, and look for any interruption of service. If that webpage does not list any issues, then one of these conditions may be causing the problem:
- You have a firewall installed on your device and it is preventing your browsers from reaching Duo.
- You have Parental Controls or other restrictions on your device and that is preventing your browsers from reaching Duo.

Nuance Dragon 13 Web Extension causes 2-Factor to Fail

There are two separate methods for both Firefox and Chrome. Each method is listed below:

- *Method 1 for Google Chrome: Disable the Nuance Dragon 13 Web Extension*
    1. Click the **Customize and control Google Chrome** button, which is represented by three horizontal lines, in the top-right of the browser.
    2. Select **Settings**.
    3. Under **Chrome** at the top-left of the page, click **Extensions**.
    4. Deselect the **Enable** check box for **Dragon Web Extension**.
    5. Return to the address of your failed Login attempt and try again. You will need to retype the address.
    6. After providing valid credentials for Login, the Duo interface should now be accessible.

- *Method 2 for Google Chrome: Use an Incognito Window*
    1. Click the **Customize and control Google Chrome** button, which is represented by three horizontal lines, in the top-right of the browser.
    2. Select **New incognito window**.
    3. Browse to the address of the failed Login attempt in the new incognito window.
    4. After providing valid credentials for Login, the Duo interface should now be accessible.

- *Method 1 for Firefox: Disable the Nuance Dragon 13 Web Extension*
    1. Click the **Open menu** button, which is represented by three horizontal lines, in the top-right of the browser.
    2. Select **Add-ons**.
    3. Click the **Disable** button for **Dragon Web Extension**.
    4. Return to the address of your failed Login attempt and try again. You will need to retype the address.
    5. After providing valid credentials for Login, the Duo interface should now be accessible.

- *Method 2 for Firefox: Use a New Private Window*
    1. Click the **Open menu** button, which is represented by three horizontal lines, in the top-right of the browser.
    2. Select **New Private Window**.
    3. Browse to the address of the failed Login attempt in the New Private Window.
    4. After providing valid credentials for Login, the Duo interface should now be accessible.