iAM - DUO Account Security

Getting Started

umTech
100 Administration Bldg., Memphis, TN 38152
Phone: 901.678.8888
Email: umtech@memphis.edu
umTech Website
Table of Contents

Setting up DUO Account Security ................................................................. 3
Setting Up DUO on a Mobile Phone ............................................................ 5
Installing on a Tablet ................................................................................... 10
DUO Token ................................................................................................. 15
  Acquiring and Using a DUO Token .......................................................... 15
Using Self-Service Bypass Codes *(For Students Only)* .................................. 16
Using Bypass Codes ................................................................................... 20
Changed your Phone? How to set up DUO on Your New Phone .................... 23
  To set up DUO on your new phone, please complete the following steps: ...... 26
Using the DUO Mobile Application in location with poor cell coverage or no WIFI ... 31
How to enable cookies in Chrome, Firefox, IE, Opera or Safari ...................... 33
  From Chrome .......................................................................................... 33
  From Firefox ......................................................................................... 34
  From Microsoft Edge .............................................................................. 35
  From Safari ........................................................................................... 36
Why Do I Need This? .................................................................................. 37
I need to reactivate DUO Mobile. ................................................................. 37
I have stopped receiving push notifications on DUO Mobile ......................... 38
I lost my phone .......................................................................................... 38
I have an international number and am having trouble using DUO. .............. 38
My hardware token stopped working .......................................................... 38
I received an authentication notification that I did not request, what should I do? ... 39
I am not able to install DUO Mobile .......................................................... 39
Supported Devices ..................................................................................... 39
Locating Help Resources .......................................................................... 40
  Submitting a Service Request ............................................................... 40
Important Links ......................................................................................... 40
Purpose

DUO Account Security or two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

Audience

This training material is designed for university staff, faculty and students that will be accessing any of the UofM’s enterprise applications through Single Sign On (SSO).
iAM DUO Account Security

Setting up DUO Account Security

1. Navigate to the iAM Identity Management site. Log in with your UUID and Password. Click Login. **Note: If you cannot log into iAM, use the Reset Your Password option.**
2. Once logged in, select DUO Account Security

3. Choose from the available selection the type of device to add. You will select Mobile phone, Tablet, or Landline. Click Continue.
Setting Up DUO on a Mobile Phone

*Note*: Effective January 2022, our service does not allow the use of callback, or SMS texting.

1. If choosing mobile phone, enter your mobile number. Click **Continue**.

   *Note*: If adding a device with a non-U.S. number, enter your full phone number, starting with the country code, as digits only—no spaces or dashes (+Country Code/City Code/Number). If you experience any issues using DUO with your mobile phone, follow the instructions on page 10 to add the device as a tablet.

2. Select the type of mobile phone. Click **Continue**.
3. Using the device, you will use to authenticate, download the DUO Mobile App from the App Store for an iPhone/iPad or in Google Play for android or tablet. Install to the app. **Note: The DUO application may be restricted in some international countries and see the following link to download the DUO Mobile APK App directly from DUO website.**

4. Return to iAM site. Tap “OK” when asked if DUO Mobile should be able to send push notifications. If you have installed the app, click the **I have DUO Mobile** button.
5. Once the Application has installed on your phone, launch the DUO Mobile app. Tap the “+” button, then under Add Account, click Use QR code. Scan the barcode, then click Continue. You can use the Default Name, University of Memphis, click Done.

Note: If you do not see the barcode click “I am unable to scan the barcode above” this will reveal an activation link from your device.

You can also activate Duo Mobile by clicking this activation link from your device: 
https://

Select the activation link.
6. Once the barcode has been scanned or you’ve used the initialization link, you are ready to use DUO Account Security. The next time that you log into the SSO system with your UUID and Password, you will also be prompted to authenticate with your phone. From this screen, select Send me a push to have a notification sent to your phone. You may also check the box beside A) Trust Browser if you want the system to bypass DUO Authentication for the next week (this is device specific). The browser cookie settings must be set to allow local data to be set See instructions for each browser located on page 19. B) Other options will take you to a screen that will list all your other registered devices.

7. Your other options will be listed on screen as the picture below. Note: this is an unusually long list of devices, not everyone will have such a lengthy list. Select an option and follow the on-screen instructions.
8. Once the push has been sent, you will receive a notification on your phone.

9. Next, launch the DUO Mobile app. A message from the DUO App will ask if you are logging in to UofM Single Sign-On? Tap **Approve** and access to the system will be granted.
Verified DUO Push

The verification code option for DUO Push provides additional security against push harassment and fatigue attacks by asking the user to enter a verification code while approving a DUO Push authentication request. It also provides improved fraud reporting from end-users by directing them toward the fraud report option in DUO Mobile when they receive unexpected DUO Push login requests.

When a user logs into an application that shows the DUO Universal Prompt and has push verification enabled in its effective policy they will see a numeric code three to six digits in length (based on your preference) in the prompt which must be entered to approve the DUO Push request on their authentication device. This ensures users cannot accidentally approve login requests when they aren’t actively logging in to the application.

Verified DUO Push requires:

- DUO Mobile 4.16.0 or later on Android 8 or later.
- DUO Mobile 4.17.0 or later on iOS 13 or later.
- A DUO-protected browser-based application with the DUO Universal Prompt activated.
Installing on a Tablet

*Note:* This method is also used for non-tablet mobile devices with international phone numbers that are experiencing issues using DUO.

1. Click to select DUO Account Security.

2. Choose from the available selection the type of device to add. Select Tablet. Click Continue.
3. Download the DUO Mobile App from the App Store for an iPhone/iPad or in Google Play for android or tablet. Tap get and then install to download the app. **Note:** The DUO application may be restricted in some international countries and the client will need to download the DUO Mobile APK App directly from DUO website.

4. Tap OK when asked if DUO Mobile should be able to send push notifications. If you have installed the app, click the I have DUO Mobile button.
5. Once the Application has installed, open the DUO Mobile app. Next, launch the DUO Mobile app. Tap the “+” button, then under Add Account, click Use QR code. Scan the barcode, then click Continue. You can use the Default Name, University of Memphis, click Done. **Note**: if you do not see the barcode click “I am unable to scan the barcode above” this will reveal an activation link from your device. Click Continue.

6. Once the barcode has been scanned, you are ready to use DUO Account Security. The next time that you log into the SSO system with your UUID and Password, you will also be prompted to authenticate with your phone. From this screen, select Send me a Push in order to have a notification sent to your phone. You may also click, Yes Trust this browser, if you want the system to bypass DUO Authentication for the next week (this is device specific). The browser cookie settings must be set to allow local data to be set. See detailed instructions for each browser.
7. Once the push has been sent you will receive a notification on your tablet.

8. Next, launch the DUO Mobile app. A message from the DUO App will ask if you are logging in to UofM Single Sign-On? Tap Approve and access to the system will be granted.
DUO Token

What is a DUO Token? The DUO token is a small, thumb-sized device that generates 6-digit codes or tokens to be used during DUO sign-on. DUO tokens can be used to generate a code or token when an individual has no usable phone options or if traveling internationally. The token will need to be kept near or on the person to whom it is assigned, as it will be needed whenever you attempt to login and authenticate to secure sites at the UofM with DUO.

The device requires no internet connection, no phone number, and is suitable for situations where the mobile app or phone cannot be used, such as in secure areas or when traveling. **Note:** Each time you press the green button on your DUO Token, it invalidates the previous code.

DUO tokens must be assigned to specific user accounts and cannot be shared. For faculty and staff, a DUO token can be requested via the following Service Desk form. DUO tokens are available for $20 and can be charged to a departmental index #. Tokens that are lost or damaged are subject to a $20 replacement fee. Students can order a DUO Token on this web page. Following the process below should allow you to successfully Authenticate utilizing your assigned DUO Token. **Note:** There will be a 5-7 day time period for clients to pick up the DUO token, once notified. The DUO token MUST be picked up in person by the requestor, on the main campus at the Administration Building room 100. It cannot be picked up from someone else other than the original requestor.

Acquiring and Using a DUO Token

1. Fill out a DUO token request using the appropriate Service Desk form. *(Note: see above paragraph)*

2. You will receive an email saying your token is ready and the location for picking up your DUO token. Pick up your DUO token.

3. Whenever you attempt to login a system protected by DUO, press green button, and enter token number on token when prompted by DUO for authentication.
Using Self-Service Bypass Codes (For Students Only)

**Note:** This documentation is for users who know their password but need to add a device in DUO. This feature is for students only and is not available for faculty or staff.

1. To use the self-service bypass codes log into iAM.

2. Click **Forgot your username?**

3. A) Enter your **First Name**, **Last Name** and **Birthday** as directed by screen. **Note:** You can manually enter the date (MM/DD/YY) or use the drop-down calendar. B) Click **Continue**.
4. A) Verify Via DUO or B) Generate a DUO Bypass Code.

![DUO Verification Screen]

5. Next, A) Enter the last 4 digits of your Social Security number. B) Click Verify.

![DUO Bypass Code Generation Screen]

6. You will see the following on your screen once you verify. Click Login to iAM Account Management to return to iAM login screen.

![Login to IAM Account Management]

7. You will need to log into your personal email to access the bypass code. 
Note: Your personal email may look different than the image below.

![Bypass Code Email]

umTech | Page 17
8. Once you have clicked Login Into iAM Account Management, you will log into iAM again. Enter your A) UofM credentials (uuid and password associated with it), then B) Click Login.

![Login into iAM Account Management](image)

9. At the DUO screen, click Bypass Code.

10. A) Enter the Bypass Code from your email, B) Click Verify Code.

![DUO screen with Bypass Code option](image)
11. From the iAM Menu Click DUO Account Security.

12. Click Add New Device to register your new device.
Using Bypass Codes

1. To use Bypass Codes log into iam.memphis.edu. Click on DUO Account Security.

2. Click on Bypass Codes.
3. Save your DUO backup codes You can A) Print them, write them down, take a screenshot, or photo. If you lose or do not have access to your device(s), you can use one of the following bypass codes to authenticate. When you are finished click B) Continue. **Note:** These are single-use codes. Keep these backup codes somewhere safe but accessible.

4. Log into IAM again. Enter your A) UofM credentials (uuid and password associated with it), then B) Click Login.
5. At the DUO screen, click **Bypass Code**.

   ![Bypass Code Screen]

6. Enter the **Bypass Code**.

   ![Bypass Code Input]

   **Note:** *These are single-use codes. Keep these backup codes somewhere safe but accessible.*
Changed your Phone? How to set up DUO on Your New Phone

If your phone number has not changed, ***access iam.memphis.edu*** when the DUO Authentication screen comes up:

1. Select "Other Options"

![Check for a Duo Push](image-url)
2. Select "Bypass code".

![Bypass Code Option]

(Note: This feature not available for some accounts.)

3. Your phone will receive a text.

![Text Message]

UofM passcode (will expire in 1 hour): **1400472**
4. A) Enter the code texted to your phone, then B) Click Verify.

5. Once you do so, you will be able to authenticate and access your account. Once you have accessed Identity Management [iam.memphis.edu], you may update/reactivate your device under "DUO Account Security" to enable the "push" feature on your device.
To set up DUO on your new phone, please complete the following steps:

1. Install the DUO Mobile application on your new phone.

2. On a computer, visit iam.memphis.edu and sign in with your UUID and password.
3. **Select Other options.**

![Check for a Duo Push](image)

- **Check for a Duo Push:** Verify it's you by approving the notification...
  - Sent to iOS

- **Other options**

4. **Next, select Text message passcodes.**

![Other options to log in](image)

- **Other options to log in**
  - **Duo Push**
    - Send to iOS
  - **Duo Push**
    - Send to Android
  - **Duo Mobile passcode**
    - Enter a code from the Duo Mobile app
  - **Hardware token**
    - Enter a code from your hardware token
  - **Text message passcode**
    - Send to "iOS" [------8759]
5. Your phone will receive a text.

![Image of text message]

6. A) Enter the code texted to your phone, then B) Click Verify.

![Image of passcode entry screen]

8. Click on Activate or Reset/Activate.
9. A QR code will appear. A) Open the DUO Mobile app, press the + symbol to add an account and click **Use QR Code**. Use your camera to scan the barcode then click continue. You should be able to receive push notifications on your new phone.

10. If you do not have a computer or are using the device you are trying to set up, you will need to select the "**I am unable to scan barcode above**" link when you sign into IAM and go to the DUO Account Security page. It will open the DUO Application automatically on your phone and the account will be added.
Using the DUO Mobile Application in location with poor cell coverage or no WIFI

You can use the DUO Mobile app to generate a passcode to use as a second factor.

1. To generate a one-time passcode, open the app and tap the green key icon next to "University of Memphis".

2. The app will generate a one-time passcode to enter at time of log in.
3. The next time that you log into the SSO system with your UUID and Password, you will also be prompted to authenticate.

4. Click on the **Enter a Bypass Code**, then enter one-time passcode.

Once you have entered the one-time passcode bypass code, click **verify**.
How to enable cookies in Chrome, Firefox, IE, Opera or Safari

To ensure your “Trust this browser?” is operational, you need to enable Cookies in your web browser. Here are directions for the most used browsers.

From Chrome

Step 1: Open settings — With Google Chrome open, click the Chrome menu icon represented by three horizontal bars or 3 small dots in the upper-right corner of the browser window. Next, click the Settings option from the menu. Next click the Show Advanced Settings option at the bottom of the page, followed by the gray Content Settings button located beneath the Privacy section.

Step 2: Enable cookies — Check the radial selection directly left of the Allow Local Data to be Set option near the top of the resulting pop-up window to enable browser cookies. Click the Done button in the bottom-right corner when finished. Close the settings tab.
From Firefox

Step 1: Open settings — Open Mozilla Firefox, click the menu icon in the upper-right corner of the browser window represented by three horizontal bars and select Preferences from the right side of the resulting drop-down menu. Afterward, click the masked Privacy tab located to the left side of the window and select the Use Custom Settings for History option in the drop-down menu of the panel’s History section.

Step 2: Enable cookies — Check the box directly left of the Accept Cookies from Sites option near the middle of the History section to enable browser cookies. Use the drop-down menu beneath the checkbox to ensure Accept Third-party Cookies is set to Always.
From Microsoft Edge

**Step 1: Open settings** — Launch Microsoft Edge, click the Tools menu icon represented by the cog in the upper-right corner of the browser window, and select *Internet Options* near the bottom of the resulting drop-down menu. Then, click the Privacy tab located in the top navigation bar.

![Internet Options](image1)

**Step 2: Enable cookies** — Move the slider within the Settings section of the Privacy tab all the way to the bottom to accept all browser cookies. Then, click the gray *Advanced* button near the bottom of the slider and check the box directly left of the *Override Automatic Cookie Handling* option to access first and third-party cookie blocking. Click the gray *OK* button located at the bottom of the window when finished.

![Advanced Privacy Settings](image2)
From Safari

Step 1: Choose the Safari Preferences — Launch Safari, click Safari in upper-left corner of the main menu bar, and select the Preferences option near the top of the drop-down menu. Afterward, click the Privacy tab located in the top navigation bar.

Step 2: Enable cookies — Check the radial click beside the Always Allow option located directly right of Cookies and Website Data to enable browser cookies. Click the Close button in the top-left corner when finished.
Why Do I Need This?

Passwords are increasingly easy to compromise. They can often be stolen, guessed, or hacked — you might not even know someone is accessing your account.

Two-factor authentication adds a second layer of security, keeping your account secure even if your password is compromised. With DUO, you'll be alerted right away (on your phone) if someone is trying to login as you.

This second factor of authentication is separate and independent from your username and password — DUO never sees your password.

I need to reactivate DUO Mobile.

When using DUO on a mobile device, if you change your device, you will need to register it in DUO. Log into IAM and deactivate the old device and activate the new one.

Here are the steps:

1. Log into IAM — https://iam.memphis.edu/
3. You will see a list of devices and phone numbers, select the device to Reset/Reactivate or press the Delete button to delete the device.

4. Select the device to Reset/Reactivate. Click on Reset/Reactivate and follow the onscreen steps. You now have Reset/Reactivated your device.
I have stopped receiving push notifications on DUO Mobile

You may have trouble receiving push requests if there are network issues between your phone and our service. Many phones have trouble determining whether to use the Wi-Fi or cellular data channel when checking for push requests, and simply turning the phone to airplane mode and back to normal operating mode again often resolves this sort of issues, if there is a reliable internet connection available. Similarly, the issue may be resolved by turning off the Wi-Fi connection on your device and using the cellular data connection.

Check the time and date on your phone and make sure they are correct. If the date and time on your phone are manually set, try changing your device’s configuration to sync date and time automatically with the network.

If neither of these suggestions work, you can login to iAM, remove your device — provided you have a backup — and re-activate DUO Mobile.

I lost my phone

If you have lost your phone, please contact the ITS Service Desk at 901.678.8888 or by email at umtech@memphis.edu.

I have an international number and am having trouble using DUO.

For mobile devices with international phone numbers that are having trouble using DUO, follow the instructions on page 10 to add your device as a tablet. International phone numbers should be entered in the correct format: The plus sign (+) followed by the country code and full number with no spaces or dashes. Example: +911234567890.

My hardware token stopped working

Your token can get "out of sync" if the button is pressed too many times in a row and the generated passcodes aren’t used for login. In some cases, this can happen by accident if the token is stored next to other objects in a pocket, backpack, etc. Tokens can typically be re-synchronized by attempting to authenticate using three consecutively generated passcodes.

Contact the ITS Service Desk if your token stops working or if you can’t log in with the passcodes it generates.
I received an authentication notification that I did not request, what should I do?

An un-requested authentication attempt might be an indication of fraudulent activity, or it could be a service configured to automatically log in, such as a computer logged in overnight.

If you believe the request is fraudulent, reject the push notification and change your credentials.

I am not able to install DUO Mobile

The minimum supported operating system version for DUO Mobile 3.1.0 and above is iOS 6.0. Users installing DUO Mobile for the first time with devices running pre-iOS 6.0 need to download DUO Mobile from the App Store using the iTunes application on a Mac or PC computer. You must be signed in with the same iTunes account you plan to use with your phone.

When the download is complete, open the App Store on your pre-iOS 6.0 device, and install DUO Mobile. You will be prompted with an alert informing you will receive the latest compatible version of DUO Mobile (v3.0.2).

Contact the ITS Service Desk if further assistance is required.

Supported Devices

Click your device to learn more:

- iPhone & iPad
- Android
- Cell Phones & Landlines
- Hardware Token
Locating Help Resources

umTech offers support to faculty, staff, and students, provides additional assistance, and resources. Such help can be located as follows:

**Submitting a Service Request**
Login URL: [Click here for our service desk ticketing system](#). After logging in, choose the appropriate form request for services.

**Contact the ITS Service Desk — 901.678.8888 any day of the week! (Excluding Some Holidays)**

- **ITS Service Desk Walk-In hours (Admin Building Room 100):**
  - Monday - Friday 8:00 am - 4:30 pm

- **The ITS Service Desk Call Center hours:**
  - Monday - Friday 8:00 am - 8:00 pm
  - Saturday 10:00 am - 2:00 pm
  - Sunday 1:00 pm - 5:00 pm

Contact the Service Desk for assistance with technical login problems or issues. ALL incoming calls after hours will be handled by voicemail services. If you require assistance after 8:00 pm, please leave a message or submit a service request.

Voice messages will be checked regularly and receive priority response the following business day. You may also email umTech at umtech@memphis.edu. (Using this email will automatically generate a service request).

**Important Links**
- [Explore the umTech Website](#)
- [Search the Solutions Page](#)