iAm - Duo Account Security

Getting Started

Center for Teaching and Learning (CTL)
100 Administration Bldg., Memphis, TN 38152
Phone: 901.678.8888
Email: itstrainers@memphis.edu
Center for Teaching and Learning Website

5/15/2017

Brought to you by:
umiTech & The Center for Teaching & Learning
Table of Contents

Setting up Duo Account Security ................................................................. 3
Installing on a Mobile Phone .................................................................... 5
Installing on a Tablet ................................................................................ 9
Using a Landline (Home Phone, Desk Phone, etc.) ........................................ 14
How to Disable Duo Authentication? ...................................................... 15
Using the Duo Mobile Application in location with poor cell coverage or no WIFI ...... 17
How to enable cookies in Chrome, Firefox, IE, Opera or Safari ................. 19
  From Chrome ................................................................................. 19
  From FireFox ............................................................................. 20
  From Internet Explorer ............................................................. 21
  From Safari .............................................................................. 22
What data is stored by Duo? .................................................................. 23
Why Do I Need This? ........................................................................ 23
I need to reactivate Duo Mobile ............................................................. 23
I have stopped receiving push notifications on Duo Mobile ..................... 23
I lost my phone ............................................................................... 24
My hardware token stopped working. ..................................................... 24
I received an authentication notification that I did not request. What should I do? .. 25
I am not able to install Duo Mobile ....................................................... 25
Supported Devices ............................................................................. 25
Service Desk Request ......................................................................... 26
  Submitting a Ticket ..................................................................... 26
  Call the ITS Service Desk (901-678-8888) on a 24x7 basis .......... 26
  Email umTech .......................................................................... 26
Important Links ................................................................................ 26
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.
2. Select Duo Account Security

![Duo Account Security Image]

3. Choose from the available selection the type of device to add. You will select from mobile phone, tablet, or land line. Click Continue.

![Device Selection Image]
Installing on a Mobile Phone

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

2. Select the type of mobile phone. Click **Continue**.

3. 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.
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 for IOS or "Add Account" for Android) and scan the QR code. 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.
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 check the box beside **Remember me for 7 days** 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 phone.

8. Next, launch the Duo Mobile app. A message from the Duo App will tell you that there is a Request Waiting, Tap to Respond. Tap the request to accept the push and gain access.

9. Tap Approve and access to the system will be granted.
Installing on a Tablet

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.

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 for iOS or "Add Account" for Android) and scan the QR code. 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 check the box beside **Remember me for 7 days** 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 tell you that there is a **Request Waiting, Tap to Respond**. Tap the request to accept the push and gain access.

9. Tap **Approve** and access to the system will be granted.
Using a Landline (Home Phone, Desk Phone, etc.)

1. Click to select Duo Account Security

2. Choose from the available selection the type of device to add. Select Landline (Home phone, Desk phone, etc.). Click Continue.

3. The system will then call the telephone line. You will hear a brief message and will be prompted to hit any key on the phone for access.
How to Disable Duo Authentication?

1. Navigate to Navigate to the iAm Identity Management site. Log in with your UUID and Password. Click Login.

2. Click on the Disable Duo Button.
3. Once the Duo Authentication is disabled, you will see a message that says “Duo is currently disabled for your account”.

![Duo Account Security screen]

**Duo Account Security**

Duo is currently disabled for your account.

Duo protects your account by requiring a secondary confirmation of your identity at log-in, using a physical device in your possession. This confirmation can be provided in a variety of ways, depending on the device you use for enrollment:

- **Duo Mobile App (recommended)** - A push notification is sent to your smartphone. You simply review the request and tap “Approve” to authenticate. Cellular or Wi-Fi access is required to use this method.
- **SMS Text Message** - A seven-digit passcode is sent to your smartphone.
- **Phone Call** - You receive an automated phone call that requires you to press any key to authenticate.

If you routinely login from the same computer or device, you may choose to have Duo remember it for 7 days, during which time you will only be prompted for your passcode when trying to login.

You can disable Duo account protection at any time.

Need Help? Contact the ITS Service Desk at (901) 872-5800.
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.

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

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.

![Firefox Settings](image1)

**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*.

![Firefox Privacy Settings](image2)
From Internet Explorer

Step 1: Open settings — Launch Internet Explorer, 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.

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.
From Safari

**Step 1: Navigate the settings panel** — 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 silhouetted *Privacy* tab located in the top navigation bar.

![Safari Settings Panel]

**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.

![Privacy Settings Panel]
What data is stored by Duo?

The only data that Duo Security stores is your UUID and information about your second factor, such as a phone number or the serial number for your token. Duo never has access to your password.

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

If you get a new phone you'll need to re-activate Duo Mobile. You may enroll the new device yourself via iAM.

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 WiFi 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 these sort of issues, if there is a reliable internet connection available. Similarly, the issue may be resolved by turning off the WiFi 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 previously enrolled a second authentication device you can login to iAM to delete your lost or stolen phone. If you aren’t able to log in to Duo at all then the ITS Service Desk can disable the missing phone for authentication and help you log in using another method. While it’s important that you contact ITS, if you lose your phone and cannot disable it yourself, remember that your password will still protect your account.

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

Upon completing the training covered in this course, faculty, staff, and students are able to receive additional training help and resources. Such help can be located as follows:

Service Desk Request

Submitting a Ticket

- Login URL:
  - Here is a link to our service desk ticketing system
  - After logging in, choose the link Request Help or Services.
  - Choose Request Help or Services.

Call the ITS Service Desk (901-678-8888) on a 24x7 basis (Excluding Some Holidays)

- Call the Service Desk for immediate assistance with login problems or issues with using the Service Desk Request Form.

Email umTech

- Email at umtech@memphis.edu (Using this email will automatically generate a help desk ticket). Please keep your Service Desk ticket number for faster assistance.

Important Links

- Explore the umTech Website
- Center for Teaching and Learning (CTL) Website
- Search our Training and Documentation