Multi-Factor Authentication FAQs

Setup Process

What are my authentication options?

- Duo Push: If the Duo Mobile app is installed on your smartphone or tablet, you can receive a push notification and can either approve or deny the authentication attempt.
- Phone call: You receive a phone call from Duo. The call will give instructions on approving or denying the authentication attempt. It will also allow you to indicate if it were a fraudulent call. Available for smartphone, basic cell phone, and landline phone.
- Pass codes via SMS: You can receive a one-time passcode via text message. This code will expire in 2 minutes, so you will need to use it promptly. Available for smartphone and cell phones with SMS service.
- Pass codes via Duo Mobile app: If you have the Duo Mobile app installed, you can receive a single pass code by tapping the key in the mobile app. This pass code must be used immediately. This is a good option if you do not have a good wireless or Wi-Fi signal on your phone. Available for smartphone & tablet.

  Refer to the authentication types in the table below for each device.

	Mobile Push	Mobile Passcode	Phone Call	SMS Text Message	Temporary Passcode
Enroll a smartphone (recommended)	X	X	X	X	
Enroll a tablet	X	X			
Enroll a basic cell phone			X	X	
Enroll a landline phone			X		
Call the UML IT Service Desk – 978-934-4357					X

Do I need a smartphone to use Duo?

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.

Any cell phone or even a landline will work, however, it will not include the advantages of the 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 don't have a cell phone?

If you don't have a cell phone, Duo allows you to use your landline phone. You would receive an automated phone call that requires you to hit "5" to confirm your identity.

Should I enroll more than one device in MFA using Duo?

Although not required, we recommend you enroll an additional device (such as a smartphone and desk phone) in MFA to avoid difficulties authenticating if you lose or don't have your only enrolled device with you.

What if I don't want to install the Duo App on my smartphone?

The Duo Mobile app provides the most user-friendly experience; however, there is no requirement to use it. As you go through the enrollment process, (1) indicate you are enrolling a Mobile Phone, (2) enter and verify your phone number, (3) specify Other (and cell phones) as your device type, and then (4) click Continue to Login to complete the process. When you log in, you will have both the phone call and passcode options available to you.

Using Duo

Do I have to use Duo every time I log in?
In general, no - you will have the option to "trust" the computer you are logging in from for 30 days. (This option requires you use the same browser and not clear your browser cache). Keep in mind the option to "trust" the computer is application specific. For some applications, like HR Direct, you can trust the computer for 30 days. Other applications (like VPN) may not have that option available.

There are several common reasons why you may not be able to select the option to remember your device.

- If you have configured Duo to automatically send you a push, text, or call instead of asking you which one to use
- If you are connecting via an iPad, iPhone, or Android device
- If your web browser does not have cookie support enabled. Make sure that cookies are enabled in Internet Explorer (if you're using Windows) or Safari (if you're using a Mac), or Chrome.

What if I don't have a data plan on my phone? What if I don't have a connection?
The Duo smart phone app provides options that work without a data plan, a texting plan or even a connection, if necessary. The app can generate the required code without need of either a telephone signal or data plan, and it can do so anywhere in the world.

Can I use a hardware token to authenticate?
If absolutely necessary, users can use a hardware token. Please contact Information Security (infosec@uml.edu) for more information.

Can I set Duo to automatically use a particular authentication method?
Yes. To do so, log in with your UML Email and password to www.uml.edu/duo, and select ***My Settings and Devices***. From this page you can configure Duo to automatically send you a push or a phone call.

How do I disable the automatic push or phone authentication feature if I no longer want it?
Go to the www.uml.edu/duo and log in with your Email address and password. **DON'T respond to the automatic push or phone call**. Instead select ***My Settings and Devices.*** You will be asked to authenticate and you can pick any option you want. Just make sure you respond to this new authentication request rather than the first one.

- Once you authenticate, you see the screen where you can manage this particular feature.
- Scroll to the bottom and change the "*When I log in*" option to "Ask me to choose an authentication method."
- Click *SAVE.*
- Click *Back to Login* to test.

Common Issues

I have a new device or phone number and the Duo App stopped working. What do I do?

If you have a new smartphone:

- If you get a new phone, even if the Duo app is restored from a cloud backup, it will lose its association with your account. If the phone number of your new phone is the same, you can still authenticate using the phone call or SMS text option, but the push option will not work until re-activated.
- You can re-activate your new phone by logging into the UML Duo Self-Service Portal (www.uml.edu/duo) and selecting the ***Add a New Device*** option. If your phone number is the same, set the authentication option to Phone Call and then select ***My Settings and Devices***. The phone you chose should ring, and you will need to answer, and press "1" to authenticate. From here, you can select the phone number of your new phone (assuming it's the same phone number) and select Reactivate Duo Mobile. This will prompt you to scan in a new QR barcode from the Duo app.
- If you have a new phone number or if you have difficulties with this process, you should contact your UMass Lowell IT Service Desk. Users with a new phone number will receive a temporary passcode with which they can use at the Add a new device option to then go through the above process. The UMass Lowell IT Service Desk may be reached at 978-934-4357.

If you have a new basic cell phone:

- If your phone number has not changed, no action is needed.
- Otherwise, contact the UMass Lowell IT Service Desk to receive a temporary passcode which you will use at the UML Duo Self Service portal (www.uml.edu/Duo). Log in and then select the ***Add a New Device*** option. From here, you can go through the process to add your new phone. The UMass Lowell Service Desk may be reached at 978-934-4357.

If you have a new tablet:

- If you get a new tablet, even if the Duo app is restored from a cloud backup, it will lose its association with your account. You can activate your new tablet by logging into the UML Duo Self Service portal (www.uml.edu/duo) and then selecting the ***Add a New Device*** option . If you have an alternative way to authenticate with Duo, you can use that to authenticate when choosing the *Add a new device* option.

- Otherwise, you should contact the UML IT Service Desk to receive a temporary passcode with which you can use at the ***Add a New Device*** option. Once you have authenticated, follow the on-screen instructions to add a new device. The UML IT Service Desk may be reached at 978-934-4357.

What if I don't have my phone?
You can contact the UML IT Service Desk at 978-934-4357. They will verify your identity and provide a temporary passcode. You may be able to use an alternative phone number, if you have set that up.

What if I lose my phone?
Please contact the UML IT Service Desk at 978-934-4357, to have them immediately lock your Duo account. They will provide you with a temporary passcode to authenticate.

Can I transfer my Duo Mobile app from one device to another?
While the app transfers from device to device, the configuration of each device is specific and will need to be re-activated on new devices.

How many chances will I get to authenticate?
You will have five chances to authenticate a request. After the fifth chance, your two-factor authentication will be deactivated and you will not be able to access the system you are attempting to log into.

I am getting a message that I am locked out. What do I do?
Your account will lock when there are too many failed attempts to authenticate. You will need to contact the UM IT Service Desk for assistance with your account.

Sometimes my phone doesn't receive a push notification like it should. What can I do?
Push notifications can get delayed when a user moves between or has weak cell/Wi-Fi signals. A quick fix is to open the Duo App, and pull down with your finger causing a manual refresh. This will prompt for any authentication requests that have not been responded too. Of course you can always select a different method of authentication (e.g., phone call, passcode) and that should also work.

Also, be sure that you have allowed the Duo app to send you push notifications. This must be enabled for you to receive a push notification without manually checking the app.

Why am I not getting the option to remember my device for 30 days?
There are several common reasons why you may not be able to select the option to remember your device.

- If you have configured Duo to automatically send you a push, text, or call instead of asking you which one to use
- If you are connecting via an iPad, iPhone, or Android device

- You are not using a web browser to access the application, or your web browser does not have cookie support enabled. Make sure that cookies are enabled in Internet Explorer (if you're using Windows) or Safari (if you're using a Mac), or Chrome.

My smartphone never receives a push notification. What can I do?
Ensure that you have allowed the Duo app to send you push notifications. This must be enabled for you to receive a push notification without manually checking the app.

Android Users: Go to settings > apps > Duo Mobile > Notifications , and make sure Duo is configured to allow notifications. (These instructions may vary if you are using a version of Android older than 6.0)

iPhone Users: Go to settings > notifications > Duo Mobile, and make sure "Allow Notifications" is set to on.

I'm often in a location where I have poor cell coverage. How can I use the Duo Service?
In cases where cell coverage is not available, use the Duo Mobile App to generate a passcode by selecting the key icon next to the "University of Massachusetts – Lowell" service in the list. Use the passcode as your second factor.

I'm getting an error message that says, "There was an error completing this request. If this problem persists, please contact your administrator. What do I do?
This error sometimes occurs after upgrading your phone. In any event, you should contact the IT Service Desk at 978-934-4357 and ask them to re-issue your Duo Mobile activation code, referencing this problem.

I'm receiving Push Notifications/Phone Calls/Text Messages from Duo even though I haven't logged into any applications. What should I do?
If you are receiving requests from Duo to approve a login that you did not initiate immediately prior to getting the notification from Duo, it's very likely that someone has your password and is attempting to login with your credentials. If this happens you should deny the request(s) and change your password immediately by calling the University IT Service desk at 978-934-4357 or visit the University self-service password reset page – mypassword.uml.edu

Why does it say my device is registered to someone else?
Duo MFA devices cannot be registered to more than one person. If you are trying to add a device (such as a home phone) that is shared with someone else, and that device has already been registered to another person, you will receive an error message.

About Duo

Can I opt-out of using multi-factor authentication via Duo?

No, enrollment for access to identified systems is mandatory. Consequently, for the increased protection of your own personal information, the information of our faculty, staff, students, and patients, as well as other UMass Lowell information systems, everyone with a UMass Lowell email address must enroll in Duo Security.

Can I use Duo internationally?

If you travel internationally, don't worry – Duo authentication can work without cellular service or a Wi-Fi connection. You have several options that may be useful:

1. **Smartphone** – Even with cellular service disabled or without a WiFi connection, you may use the Duo Mobile app to generate a **passcode** that you can use to authentication. Simply choose the *Enter a Passcode* option when you get the Duo authentication prompt. To generate the passcode, open the Duo Mobile app on your phone and tap the button with the KEY symbol.
2. **Hardware token** – if you don't have a smartphone and you travel internationally often, you may have the option of obtaining a hardware token (contact the IT Service Desk to start the process). Simply choose the *Enter a Passcode* option when you get the Duo authentication prompt and then enter the passcode that shows on the hardware token. Hardware tokens may be purchased in advance by contacting infosec@uml.edu.
3. **By-Pass Code** – If you won't have a smartphone and a hardware token is not an option, it is possible to get a bypass code that you can use for Duo authentication for the duration of your trip. Contact the IT Service Desk to request this option. Then, simply choose the *Enter a Passcode* option when you get the Duo authentication prompt and enter the bypass code that you were given.
4. **Normal options** – If you have cellular service or a Wi-Fi connection, then you can simply use whatever authentication technique you normally use. The push, passcode, and phone call options all work overseas. You can even add an international phone number as one of your authentication options.

What data is stored by Duo?

The only data that Duo stores for a user is the subscriber's primary username (UML email address) and information about your second factor, such as a phone number (if using a phone for the service) or the serial number of your hardware token (if not using a phone for the service).

Does it cost me anything to use the Duo service via my phone? If so, will I be reimbursed?

There is no cost to download or use the Duo Mobile smartphone app. If not using the Smartphone App, text messages and voice calls are sent only when you request them, and they would be billed by your carrier in the same way that any other text message or call would.

What does the Duo Mobile app access 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.

The Duo Mobile app will request access to the camera when activating the app (when using the QR barcode), but this is the only time that the camera will be activated by Duo Mobile. Under no circumstance does Duo Mobile activate devices such as microphone or GPS.

Where can I get more information?

End user documentation is available from guide.duosecurity.com