Loyola Digital Experience
MFA Quick Guide

Setting Up Your Account for Azure Multi-Factor Authentication

Logging into an application that uses Azure Multi-Factor Authentication combines two factors for authentication:

- **First factor** – UVID plus your network password
  - ➢ *Note: For Loyola Secure Access (LSA), PIN code is no longer used*
- **Second factor** – App-based push notification or code, text message, or phone call.

To start, you will need set up your verification methods so that you can receive notifications or codes that will be used as a second factor in the authentication process. Below is a list of second factor contact methods:

Contact Method	Second Factor Options
Mobile device application ***Note:*** *Microsoft's Authenticator app needs to be downloaded to your* [Android](#) *or* [iOS](#) *device for this method* *Also, if you travel **internationally**, the mobile device application can still generate verification codes without cellular service or an internet connection.*	❖ **Receive notifications for verification** – pushes notification to authenticator app on mobile device. Select **Approve** to authenticate or **Deny** if you do not recognize the sign-on attempt. **OR** ❖ **Use verification code** – generates a verification code that updates every 30 seconds. Enter most current verification code displayed in the app into the sign-in screen when prompted.
Text to mobile device	❖ **Text message –** sends a text message containing a verification code. Enter the verification code provided in the text message into the sign-in screen when prompted.
Call to mobile device or phone	❖ **Phone call** – automated voice call to the phone number provided. Answer the call and press # on the phone keypad to authenticate.
Physical Token	❖ **Use verification code** – generates a verification code that updates every 30 seconds. Enter most current verification code in the sign-in screen when prompted. *Only available if the other second factor options are not available to you by logging an* [incident](#)*, via email at* ITSServiceDesk@luc.edu*,or via phone at 773-508-4487*

Loyola Digital Experience
MFA Quick Guide

Initial Verification Setup – *First-time setup only*
Note: your account must already be opted in / enrolled for O365 MFA.

Step 1 – Navigate to https://portal.office.com/ and enter your LUC email address. If prompted to "Pick an account", select your LUC account.

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

Next

Step 2 – Enter your Loyola username and password.

**Loyola University
Outlook WebAccess**

LOYOLA UVID

PASSWORD

LOGIN   Need to change or forgot your password?

LOYOLA
UNIVERSITY CHICAGO

Step 3 – If you have not previously set up MFA, the screen below will appear. Click **Next**.

Microsoft

■■■■■■■@luc.edu

More information required

Your organization needs more information to keep
your account secure

Use a different account

Learn more

<div align="center">

Next

</div>

Step 4 – Set up your primary contact method

❖ To use the **Mobile App** as the contact method (recommended), install Microsoft's "Authenticator"
app (available for _Android_ and _iOS_) on your phone or tablet and complete the following steps.

1. Select **Mobile app** from the **"Step 1: How should we contact you?"** drop-down list.
2. Select either **"Receive notifications for verification" (recommended) to** receive push
   notifications in the Microsoft Authenticator app, or **"Use verification code" to receive 6-digit
   codes that refresh periodically** in the Microsoft Authenticator app. Then click **Set up.**

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app ▼

┌─ How do you want to use the mobile app? ─────────────┐
│ ○ Receive notifications for verification   │
│   │
│ ○ Use verification code   │
└──┘

To use these verification methods, you must set up the Microsoft Authenticator app.
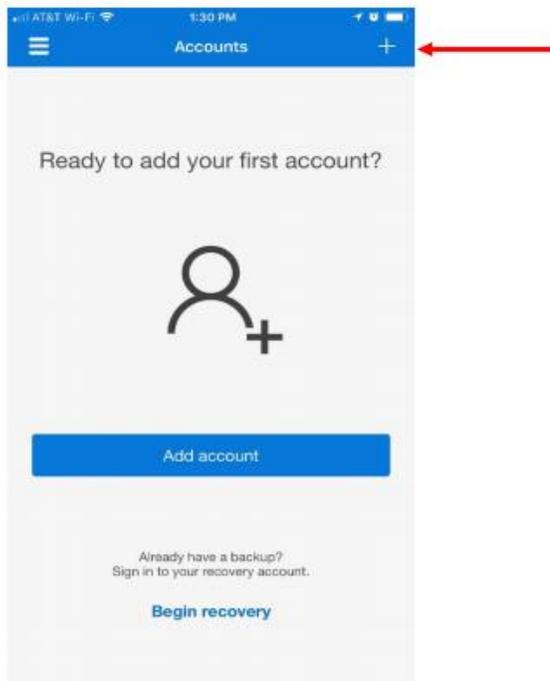
Set up   Please configure the mobile app.

Next

3. Open Microsoft's Authenticator app on your mobile device. The first time you open the app, you may receive a prompt like the one below. Tap **Allow**.
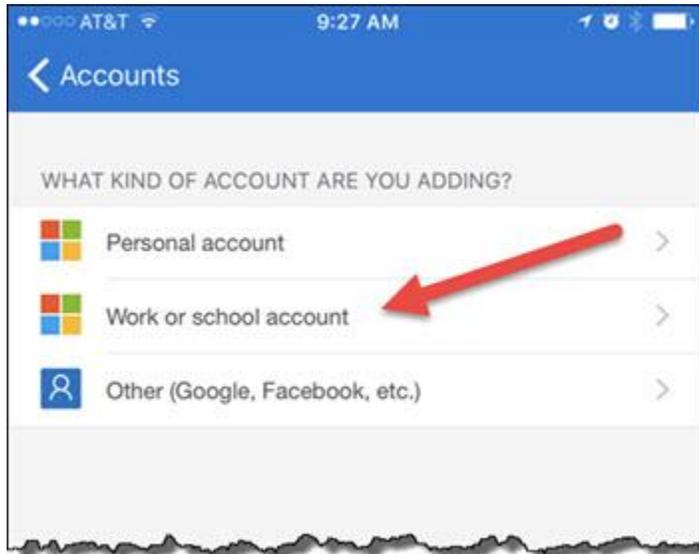

4. Tap the **plus (+) symbol** or **Add account.**   (On Android devices, select the three dots, then **Add account**.) If prompted for a backup, tap **Continue.**
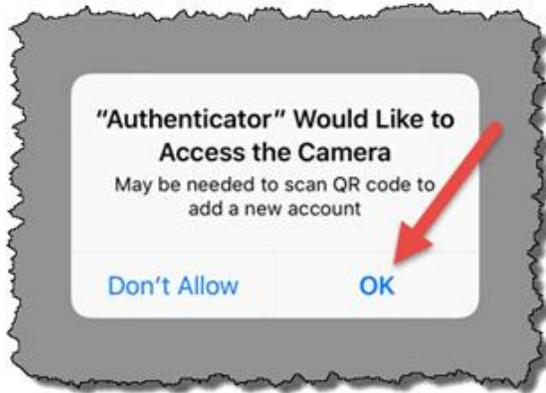
5. Tap the **Work or school account** option.

6. A QR code scanner will launch within the app. The first time you open the app, you may be prompted with **"Authenticator" Would Like to Access the Camera** - tap **OK** as you will need to scan the QR code using the device's camera.

7. Make sure that your camera is enabled and then scan the QR code on the "Configure mobile app" page using the **Scan QR code** screen on your phone to configure the mobile app. Click **Next** on the "Configure mobile app" page.

8. After the phone and application have been verified, approve the notification sent to your phone (or enter the 6-digit code if that is what you chose).
9. Click **Done**.

Note: If your camera is not working properly, you can enter your code manually. To add your account to the mobile app manually, use the following steps instead of scanning the QR code:
1. Select "**Or enter code manually**" in the Scan QR code screen on your phone.
2. Enter the code and the URL that are provided on the "Configure mobile app" page underneath the QR code. This info goes in the **Code** and **URL** boxes on the mobile app.
3. Then select **Finish** to complete the activation.
4. After the phone and application is verified, approve the notification sent to your phone.
5. Click **Done**.

10. Choose your country/region from the drop-down list and enter your phone number. Click **Next**.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 3: In case you lose access to the mobile app

United States (+1)

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

❖ If – instead of Microsoft's Authenticator app – you would like to use your phone number as the primary contact method, select **Authentication Phone** from the drop-down list and complete the following steps. If you have already set up the app, please skip to "Step 5".

1. Choose your country/region from the drop-down list and enter your phone number.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

United States (+1)

┌─ Method ─────────────────────────┐
│ ○ Send me a code by text message │
│   │
│ ⦿ Call me   │
└───────────────────────────────────┘

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

2. Select the preferred method for your mobile phone – either "Send me a code by text message" or "Call me", then click **Next**.
3. Follow the instructions provided on the screen, then click **Verify**.
4. Click **Done** after the verification is complete **on the next screen**.

Step 5 – An initial application password will be provided to you. If needed, this type of password can be used with an application that does not support MFA. Please see the guide on App Passwords for more information. Click **Done**.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 4: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. Learn more

Get started with this app password:

Done

Loyola Digital Experience
MFA Quick Guide

Managing Your Settings for Two-Step Verification

This section will allow you to modify your default and backup verification options. We highly recommend that you set up multiple authentication methods with Microsoft Azure MFA so that a backup method is available if you do not have access to your primary device.

1. Open to the "Additional security verification" page at https://aka.ms/MFASetup and log in.

2. Select one of the options from the drop-down menu under "What's your preferred option?" to choose your primary verification method:
   - Call my authentication phone → use with your mobile or office phone
   - Text code to my authentication phone → use with your mobile device
   - Notify me through app → use with Microsoft's Authenticator app
   - Use verification code from app or token → use with Microsoft's Authenticator app or a physical token
   - Call my office phone → currently not configurable – use the "Call my authentication phone" if you want to use your office phone as your preferred option

3. Check the box related to your default verification option and fill in the corresponding fields.

4. If you did not set up the Microsoft Authenticator app during initial setup but would like to, more detail can be found under Step 4 of this guide's section on Setting Up Your Account for Azure Multi-Factor Authentication.

5. Add an alternate verification method (optional) by checking more than one verification option. For example, if "Authenticator App or Token" is your default verification option, you might want to check "Authentication phone" as well and fill in your office phone number for use as an alternate verification method if you lose your mobile device.

6. Select **Save** to complete your changes. If you made a change to your preferred option, follow any prompts that appear to verify that change.