Setting Up Your Account for Azure Multi-Factor Authentication for Loyola Secure Access (LSA)

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**—Mobile device app-based push notification or code, text message, or a call to a dedicated phone number.

To start, you will need set up your verification methods on the “Additional security verification” page 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:

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Second Factor Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile device application*</td>
<td>- <strong>Receive notifications for verification</strong> – pushes notification to authenticator app on mobile device. Select <strong>Approve</strong> to authenticate or <strong>Deny</strong> not to authenticate</td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Use verification code</strong> – generates a verification code that updates every 30 seconds. Enter most current verification code displayed in the app in the sign-in screen</td>
</tr>
<tr>
<td>Text to mobile device</td>
<td>- <strong>Text message</strong> – sends a text message containing a verification code. Enter the verification code provided in the text message into the sign-in screen</td>
</tr>
<tr>
<td>Call to mobile device or phone</td>
<td>- <strong>Phone call</strong> – automated voice call to the phone number provided. Answer the call &amp; press # on the phone keypad to authenticate</td>
</tr>
<tr>
<td>Physical Token</td>
<td>- <strong>Use verification code</strong> – generates a verification code that updates every 30 seconds. Enter most current verification code in the sign-in screen. <strong>Only available if the other second factor options are not available to you by logging an incident,</strong> via email at <a href="mailto:itsservicedesk@LUC.edu">itsservicedesk@LUC.edu</a> or via phone at 773-508-4487</td>
</tr>
</tbody>
</table>
Loyola Digital Experience
MFA Quick Guide

Step 1 – Initial Verification Set up – First-time set up only

- Go to the “Additional security verification” page using the following link: https://aka.ms/MFASetup and login.

- Select one of the following values from the drop down under “Step 1: How should we contact you?”:
  1. **Authentication phone** – for text message or calls authentication phone
  2. **Office Phone** – *Currently, not configurable – however, see page 8 to set up office phone as a your “Authentication phone”
  3. **Mobile app** – *Recommended second factor method → Requires Microsoft Authenticator app be installed on your mobile device

- To use the **Mobile App** as the contact method, install the Microsoft Authenticator app on your phone or tablet, which is available for Android and iOS.

Select **Mobile app** from the “Step 1: How should we contact you?” drop-down list.

1. Select either “Receive notifications for verification” 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]
2. Once you have the **Microsoft Authenticator** app installed, open the Microsoft Authenticator app on your mobile device. The first time you open the app, you may be prompted with "**Authenticator** Would Like to Send You Notifications", as shown below:

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

5. The QR code scanner will launch on 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 your mobile phone’s camera:
"Authenticator" Would Like to Access the Camera
May be needed to scan QR code to add a new account

Don’t Allow  OK

Your account provider will display a QR code

Or enter code manually
6. 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. Select **Next** on the “Configure mobile app” page.

7. After the phone and application is verified, approve the notification sent to your phone.

8. Then select **Done**.

**If your camera is not working properly, you can select to enter your company information manually.**

To add an account to the mobile app manually, instead of using scanning the QR code, use the following steps:

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. Then select **Done**.
To use your **Mobile Phone** as the contact method, select **Authentication Phone** from the drop-down list.

1. Choose your country/region from the drop-down list, and enter your mobile phone number.
2. Select the preferred method for your mobile phone – either “Send me a code by text” or “Call Me”, then select **Next**.
3. Follow the instructions provided on the screen, then select **Verify**.
4. Click **Done** after the verification is complete on the next screen.

The **Office Phone** method is currently not configurable in this screen. However, you may still set up your office phone number as second factor method. See the **Step 2 – Managing Your Settings for Two-Step Verification** section on page 8 of this guide.
Step 2 – Managing Your Settings for Two-Step Verification

1. This step will allow to step up your **default or primary** as well as your **alternate** verification options.

   **Note:** We highly recommend that users to set up multiple authentication methods with Microsoft Azure MFA so that if you do not have access to your primary device, you can still use a backup device.

On the “**Additional security verification**” page, select one of the option from the dropdown under “what’s your preferred option?” for 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 Authenticator app
- Use verification code from app or token → use with Microsoft Authenticator app or 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 primary second factor authentication method

---

**Additional security verification**

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.

View video to know how to secure your account

**what’s your preferred option?**

We’ll use this verification option by default.

- Call my authentication phone
- Text code to my authentication phone
- Notify me through app
- Use verification code from app or token
- Call my office phone

**Office phone** is currently not configurable. You may use "Authentication phone" for your mobile or office phone number
2. Check the corresponding box related to your default verification option and fill in the corresponding fields.

3. If you did not set up the Microsoft Authenticator app in Step 1 but would like to in Step 2 – See pages 3-6 of this guide on how to set up Microsoft Authenticator app.

4. 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 and use it as alternate verification method if you leave your mobile device at home.

5. Note: Currently, the “Alternate authentication phone” field is used for account recovery only.

6. Select Save and your changes are completed.