



Law School Computing Services User Memo

First-Time Password Setup for a new Loyola Universal ID (UVID)

Memo Number: #7
Revised: 1/20/22

Overview

This document will describe the steps new Loyola users need to follow to do the First-Time password setup for a new Loyola Universal ID (UVID). Loyola issues all current students, staff and faculty a Loyola Universal ID (UVID). This one ID and its associated password are used to login on a Loyola computer, your Loyola email and a number of other Loyola systems.

You manage the password for your UVID by using Loyola's Self Service Password Reset (SSPR) Management Tool. The Self Service Password Reset Tool is accessible 24/7 and can be accessed from a web browser.

Once you change your initial password following the steps below eventually your password will expire and you will be required to change it. Your UVID password will expire every 180 days and you will need to change the password as required by university policy.

The steps in this document are only for changing your initial password you received when your UVID was issued to you. In the future when you want or need to change your password you can follow the steps in Law School Computing Services User Memo No. 9 "Managing Your Loyola UVID Password". To get a copy of this document, please go to this link: <https://www.luc.edu/media/lucedu/law/technology/pdfs/9ManagingYourLoyolaUVIDPassword.pdf>

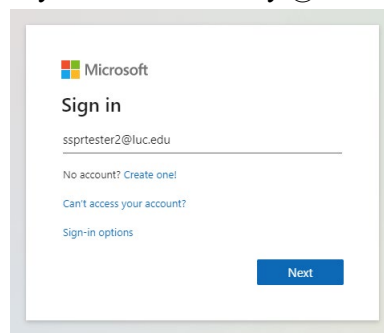
Important Note: When someone is new to Loyola they are issued a UVID and a temporary initial password. The new UVID and initial password will not work on any Loyola system except the Self Service Password Reset Tool. The initial password must be changed and a second factor for authentication must be setup by following the directions below in the First Time Setup section.

First Time Setup

To follow the steps in this section, you must use the Loyola Universal ID (UVID) and temporary initial password that was issued to you. If you do not know your UVID and/or initial password, you will need to contact the university ITS Service Desk by email at itsservicedesk@luc.edu or by phone at (773) 508-4487 to get this information.

Step 1: In a web browser navigate to <https://portal.office.com>

Step 2: Enter your Loyola University UVID followed by @luc.edu (Example: youruvid@luc.edu)

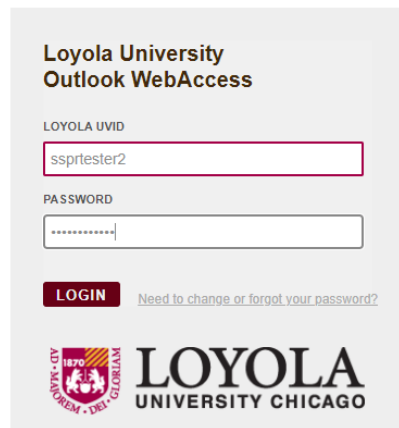


Step 3: On the next screen enter your UVID and Default Password.

-Your Loyola UVID is the first part of your Loyola email address, the part before the @luc.edu.

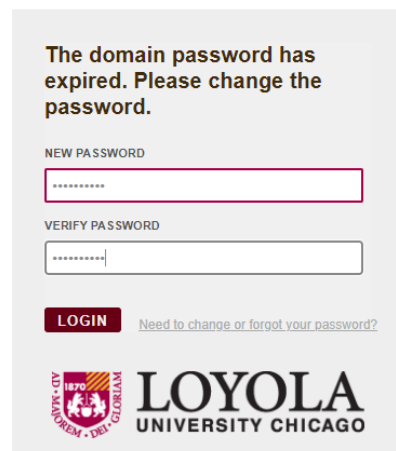
-Your temporary initial password follows this format: LUCflmmddy!

- LUC (all CAPS)
- **F** = first initial of you legal first name (**must be lower case**)
- **l** = first initial of your legal last name (**must be lower case**)
- **mm** = 2 digits for the month of birth (**must be 2 digits, may include a preceding zero**)
- **dd** = 2 digits for the day of birth (**must be 2 digits, may include a preceding zero**)
- **yy** = last 2 digits of year of birth
- **NOTE:** LUC is capitalized and there is an ! (exclamation mark) at the end

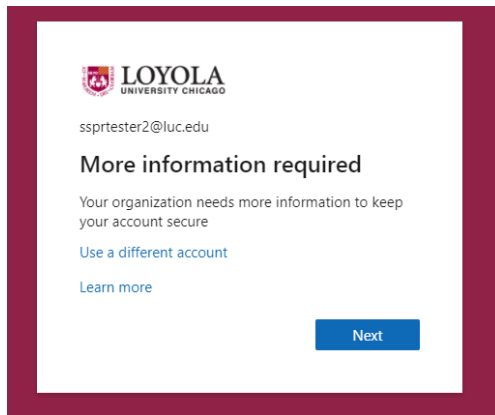


Step 4: Create a new password – the new password must meet the following requirements:

- At least 12 characters in length but no more than 20 characters
- At least 1 uppercase character (in addition to lower case)
- 2 of the following:
 - At least 1 number
 - At least 1 symbol
- Password cannot be one of your last 10 recently used passwords
 - At least 1 symbol



Step 5: You'll be presented a "More information is required" screen, click the "Next" button.



Step 6: Do not skip this step. Select the method you would like to use for your second factor for authentication. You must choose either the Microsoft Authenticator Mobile App option or the Phone (Text Message or Call) option for your second factor for Authentication.

There is a section for each of the methods below in this document that has the steps required to complete the second factor for Authentication setup.

Follow the directions in the first section below titled "Steps to complete the setup for Microsoft Authenticator Mobile App" if you want to use the Microsoft Authenticator Mobile App option **or** follow the directions in the section titled "Steps to complete the setup for Phone (Call /Text Message)" in the second section below if you want to use the Phone (Text Message or Call) option.

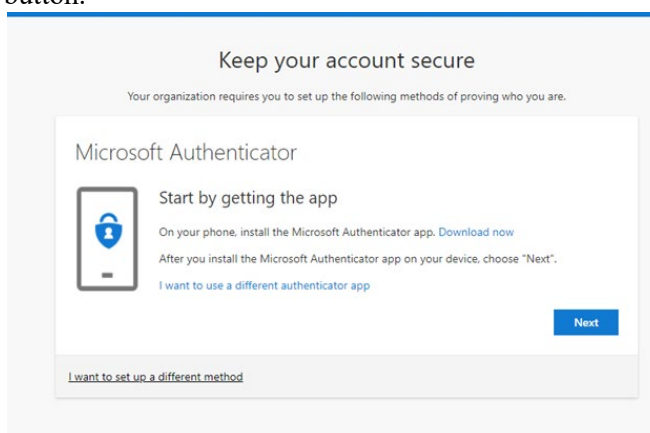
Steps to complete the setup for Microsoft Authenticator Mobile App

If you have chosen Phone (Call / Text Message) option as your second Authentication method, please skip to the next section.

When you first start you should see the screen below in your web browser that says "Start by getting the app". **Do not click the "Next" button on this screen yet.**

Leave the screen in your browser and take out your mobile phone and download the free "**Microsoft Authenticator**" app. You will get this from the Apple App Store for an iOS device or the Google Play Store for an Android device and install the app on your phone.

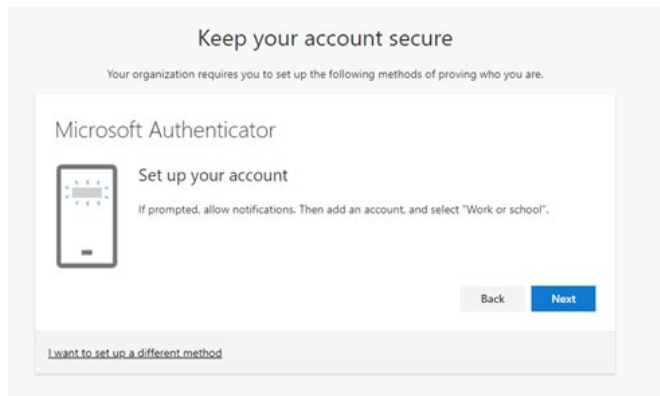
After you have the app **installed and open on your phone**, go back to the web browser and you should see the screen below and click the "Next" button.



On the next screen you will see the screen below in your web browser that says “Set up your account”. **Do not click the “Next” button on this screen yet.**

1. Follow the prompts on your **mobile phone** screen in the Microsoft Authenticator Mobile app.
2. Select “**Add an account**” followed by “**Work or School**“, allow notifications and access when prompted.
3. Stop when the app on your phone shows the QR code scanner screen.

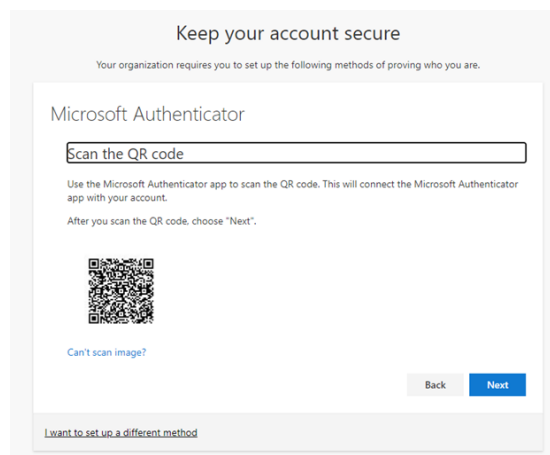
Now click the “Next” button on the screen in your web browser to continue to the next step.



Next you will see the screen below in the web browser that says “Scan the QR code”. **Do not click the “Next” button on this screen yet.**

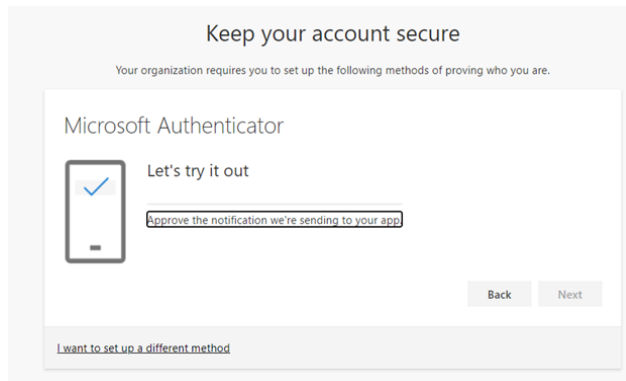
On your mobile phone the Authenticator app should still be at the QR code scanner screen where you left it in the step above.

1. Aim your mobile phone’s camera at your computer screen at the QR code in the window in your browser (the window will look like the image below).
2. Line up the box in the QR code scanner screen on your phone in the app with the QR code in the browser window until the code is scanned.
3. Once the code is scanned click the “Next” button on the screen in your web browser to continue to the next step.



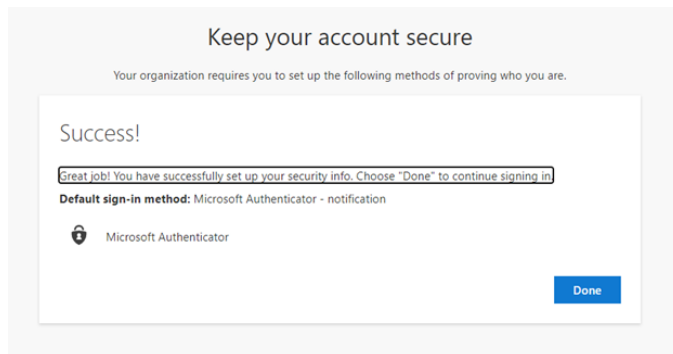
Next you will see the screen below in your web browser that says “Let’s try it out”.

1. Click the “Next” button on this screen.



2. After you clicked “Next” in the previous step, pick up your mobile phone. A test authentication will be sent to the Authentication app on your mobile phone.
3. You should see a notification pop up in the app on your phone. Select “Approve” on your phone when prompted.

After you select “Approve” for the Authentication pop up in the app on your phone, you should see the screen below in your web browser telling you “Success”. Click “Done” and the process is complete.

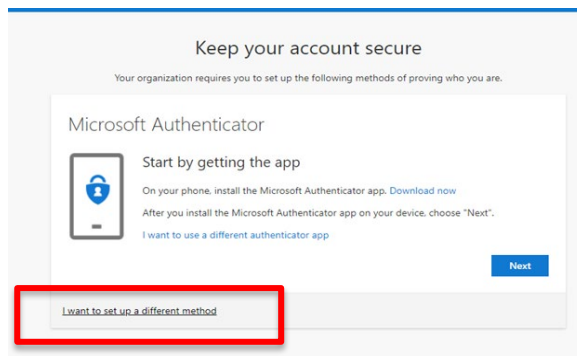


Steps to complete the setup for Phone (Call /Text Message)

If you already completed the steps for the Microsoft Authenticator App as your second Authentication method in the previous section, you do not need to do this section.

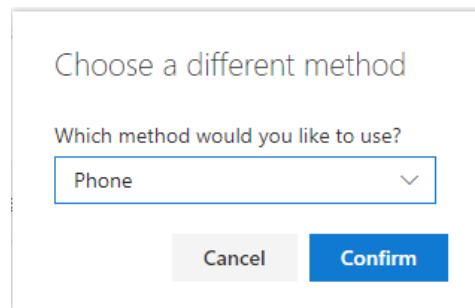
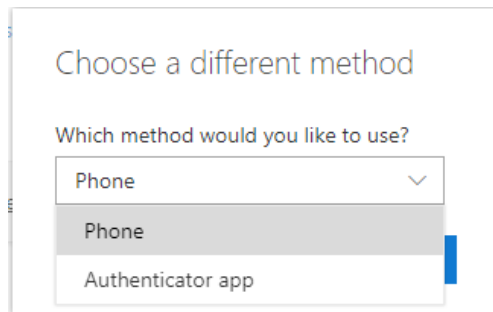
When you first start you should see the screen below in your web browser that says “Start by getting the app”. **Do not click the “Next” button on this screen yet.**

Click on the link at the bottom of the window “I want to setup a different method” option.



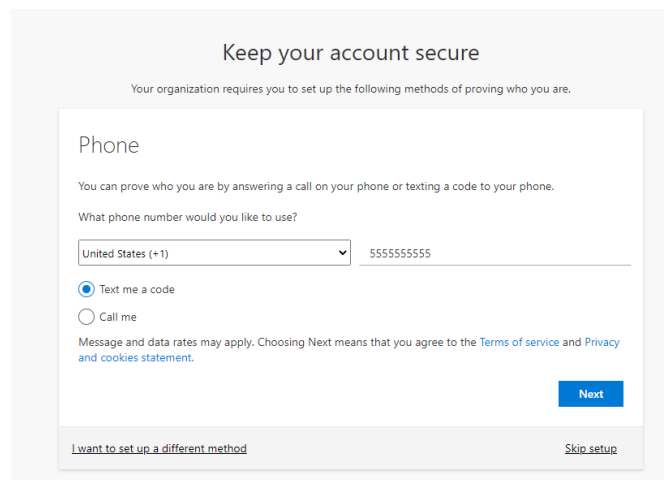
Next, in your browser window you should see the screen below asking you to “Choose a different method”.

From the drop down menu select “**Phone**” and then click the “Confirm” button.



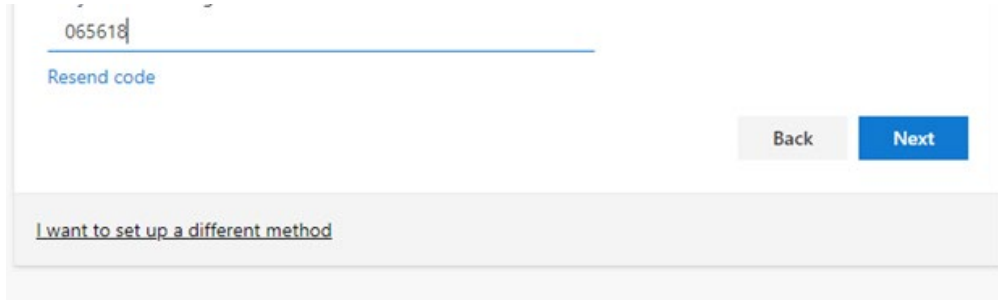
Next you will see the window below in your browser.

1. Enter your phone number
2. Select the method to use as your second factor for authentication, pick either “Text me a code” or “Call me”.
3. Click the “Next” button.

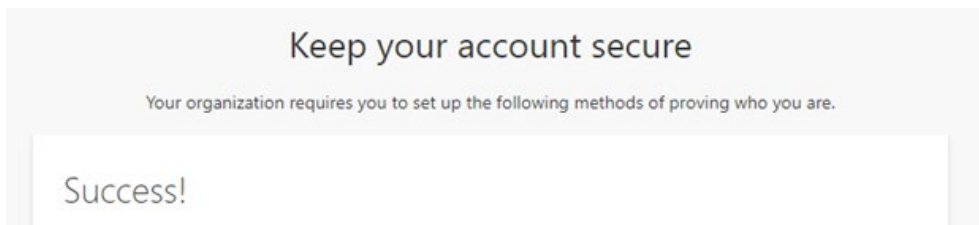
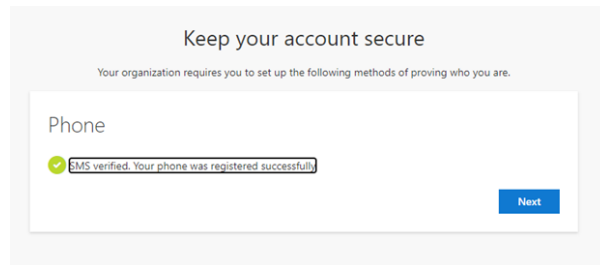


Next you will see the screen below in your browser window. You will either receive a code via text message sent to the phone number you entered in the previous step or you will receive an automated phone call giving the code to the phone number you entered in the previous step, whichever you chose.

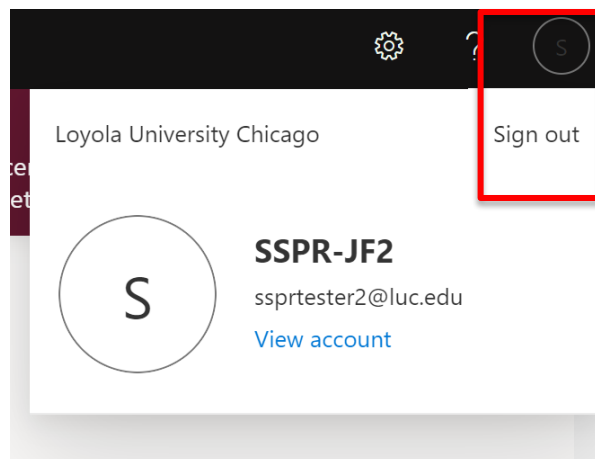
Enter the code that you receive on the screen in your web browser and click “Next”.



Next you will see the screen below in your web browser. If you see the green check mark, you have successfully registered the authentication method. Click “Next”.



Next logout by clicking on the top right Icon and selecting "Sign out".



You have now completed the setup. You can now use your UVID and new password you just setup, along with your secondary authentication method when required to access Loyola systems such as LOCUS, your Loyola email account and other resources.

For more information about the Self Service Password Reset (SSRP) Management Tool go to luc.edu/password if you have questions about or need assistance using the SSPR Tool contact Law School Computing Services (LSCS) by email at lscs-info@luc.edu or by phone at 312-915-7192 or the University ITS Service Desk by email at its servicedesk@luc.edu or via phone at 773-508-4487.