NEED MICROSOFT AUTHENTICATOR FOR REPLACEMENT PHONE

NOTE: In this procedure you will be performing tasks on your mobile device and your PC. If you have any problems with these instructions, use chat or call the Help Desk for assistance.

These instructions are to be used when you previously had a Microsoft Authenticator and you have gotten a new or replacement mobile device.

1. If you don’t still have your old phone, your Microsoft Authenticator token must be reset in Azure. You will need to contact the Help Desk via chat (if you are able to get on the corporate network) or via phone at 877-828-4357. Let the agent know you got a new phone and need your Microsoft Authenticator token reset. They will reset the account and should be able to walk you through the steps using the registration page: <https://aka.ms/setupsecurityinfo> to get a NEW Microsoft Authenticator token.
2. If you still have your old phone, you can use the token on that phone to login to the Microsoft Authenticator registration page.

Graphical user interface, text, application, chat or text message, email

Description automatically generated

1. First, delete any old Microsoft Authenticator tokens you might have. There is a limit of 5 so minimizing this list to only the current token you have is a good idea. Click the Delete button and then confirm on the next screen:  
   Graphical user interface, application

   Description automatically generated
2. Once you have deleted old tokens, you can then click “Add sign-in method” to add a new authenticator.

Graphical user interface, text, application

Description automatically generated

1. Use the pulldown on the “Add a method” window to select “Authenticator app” and then click the “Add” button.

Graphical user interface, application

Description automatically generated

* 1. Inside Microsoft Authenticator on your phone, delete the old token (but leave the application installed). On the phone, click the + (or other button depending on device type) to add a new token to your phone. **NOTE:** On Android devices, tap the three dots, then **Add account**.  
       
     **IMPORTANT:** You may receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You MUST select **Allow** so the Authenticator app can access your camera to take a picture of the QR code in the next step.  
       
     Graphical user interface, application

     Description automatically generated
  2. Tap **Work or school account**. The QR code scanner on your phone opens.  
       
     Qr code

     Description automatically generated

1. Back on the laptop, click “Next”

Graphical user interface, text, application, email

Description automatically generated

1. Click Next on this screen:

Graphical user interface, application

Description automatically generated

1. Now you can scan the QR code from your phone and you will see the token get added. Back on the PC click the “next” button.

A picture containing graphical user interface

Description automatically generated

1. The system will then send an approve request to your mobile device. Depending on how your device is configured or what features it supports, you may need to unlock the screen with your unlock code, use TouchID, or FaceID to approve the request.

Graphical user interface, text, application

Description automatically generated

1. Once approved, the screen will report a success. Click the “Next” button.

Graphical user interface, application

Description automatically generated

1. You will then see this screen indicating a successful token registration. You can now use your token to log in to Lumen applications that use Microsoft Authenticator.

Graphical user interface, text, application, email

Description automatically generated

1. If you have any problems getting the token registered, please contact the Help Desk.

MS Authenticator Replacement Device Setup Document Version 1.1

1. 6/15/22 – First version.