CALIFORNIA STATE UNIVERSITY
LONG BEACH

Division of Information Technology

Microsoft (MS) Multi-Factor Authentication (MFA) with MS Authenticator App

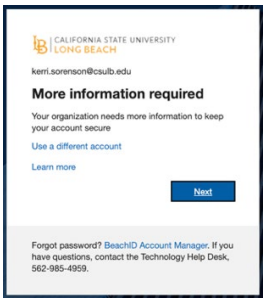
Need-to-Know

- MFA means when you log into certain campus applications, you provide two authentications of your identity.
- The first authentication method is your Beach ID login.
- The recommended second method is the MS Authenticator mobile app
    - SMS text message and phone call options are also available. For employees without a compatible device, a hardware token can be requested.
- MFA is required to access University provided MS services (Campus email, OneDrive, Office, and SharePoint)
- Once MFA is enabled for the campus, you will be prompted with an on-screen setup when accessing any University provided MS service.
- After setup, each time you access a Microsoft or CMS related service through the Campus Single Sign-On (SSO) you will be prompted for MFA.
    - MFA will also be required for Microsoft products you have installed on your computer such as Outlook or Office; however, your MFA approval will be remembered, and you won't be prompted again unless you've been inactive in that application for 90 days or you change your password.

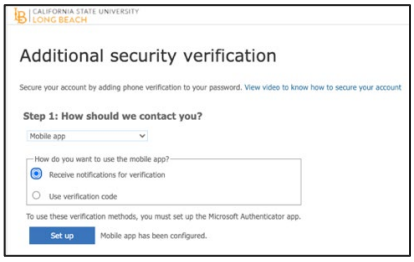
MS Authenticator App Set Up

After MFA is enabled for the campus, launch Campus email, OneDrive, Office, or SharePoint.

You will be prompted with a web browser message “More information required”. Click “**Next**.”



Select “**Mobile app**” from the dropdown then click “**Set up**”.



Follow the prompts on the “**Configure mobile app**” window to:

1. Install the MS Authenticator app on your smartphone
2. Add a “work or school account”
3. Scan the QR image

When finished with setup on your smartphone, return to your computer browser session and click “**Next**.”

A test notification will be sent to your mobile app. Tap “**Approve**.” Your setup is complete.

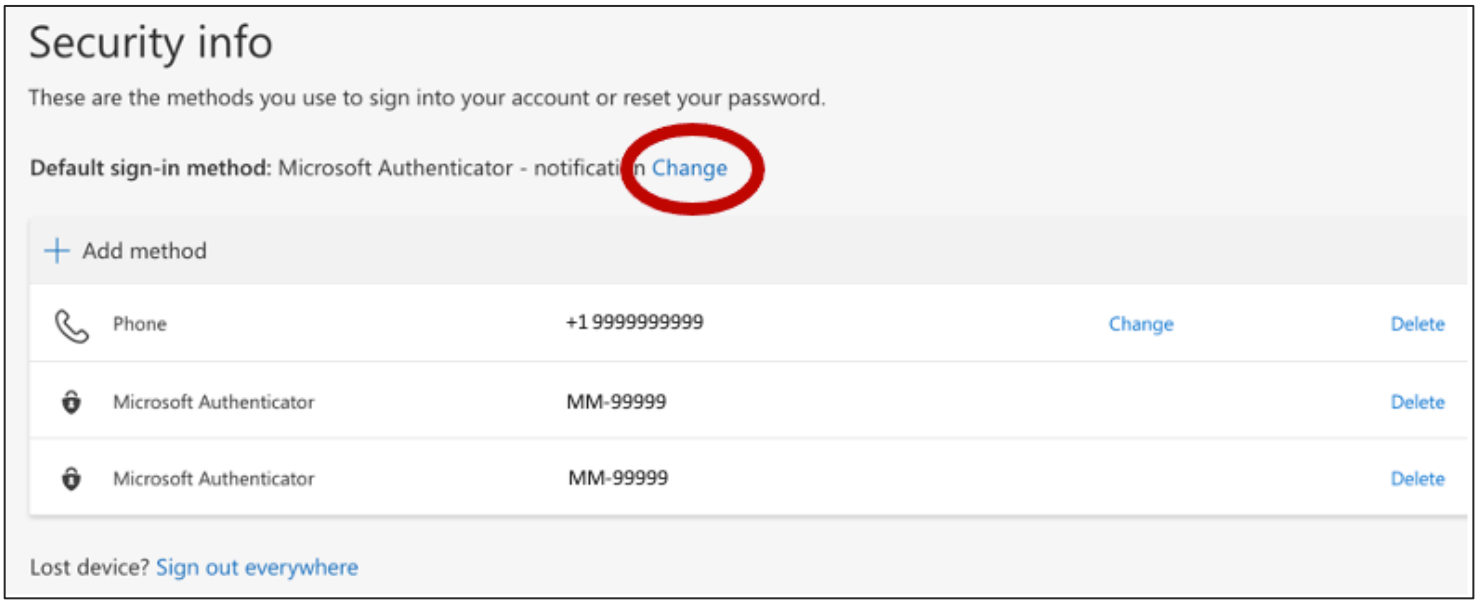
Manage Devices

1. In a web browser, login to Single Sign On (SSO) at https://sso.csulb.edu
2. Select any MS service (Campus email, OneDrive, Office, or SharePoint).
3. From within the service, click your personal icon in the upper right corner.
4. Click “View Account.”
5. Click “Security Info.”
6. Click “Add method” to add a new device or change/delete to manage current devices. It is recommended you add multiple devices, even if you don't plan to use them. This will ensure you have alternative access in the event you lose a device or get a new phone.

Manage Default Authentication Device

To change the default sign-in method, click “Change” then select one of the following:

- Microsoft Authenticator
- Phone - Call
- Phone - Text



Help

For assistance with MFA, please visit http://helpdesk.csulb.edu and search for “MFA” or contact the Technology Helpdesk at helpdesk@csulb.edu or 562-985-4959.