OFFICE OF INFORMATION TECHNOLOGY

One government, empowered by innovative technical collaboration

Getting Started with Multi-Factor Authentication
v8/19/21.1

To improve the security and privacy of employee accounts and State of Alaska data the Office of Information Technology (OIT) is making Multi-Factor Authentication (MFA) available for Office 365 and other services that use Azure Active Directory (i.e. Outlook, Teams, OneDrive, etc.) to SOA Executive Branch Departments.

Multi-Factor Authentication (MFA) is a common and effective tool against compromised passwords. It is used frequently by banking and commerce websites throughout the world. It uses two or more independent means of evidence to confirm the identity of a user accessing an application or service. You are already familiar with providing a username and password; this is something you *know*. The second method utilizes something you *have*, namely a device or phone number. The intent is to increase security with minimal impact on work.

To get started, select and setup your preferred method,

A. Microsoft authenticator app notifications (most secure) – Page 2
B. Text Message PIN (alternative) – Page 4
C. Call back to a phone number (alternative) – Page 5

Additional information is available on the OIT MFA Resource Page:
Multi-Factor Authentication, Office of Information Technology, State of Alaska

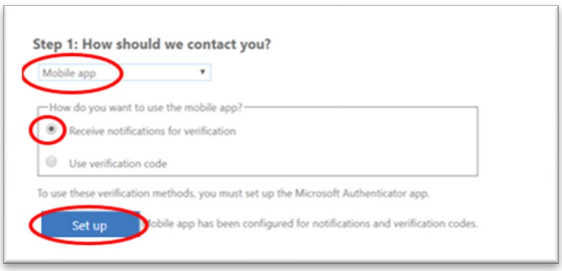
Method A: Using Microsoft Authenticator App notifications on an IOS/Android device

Using a mobile app for MFA requires you to respond to an in-app approval notification after you enter your SOA login credentials (name and password) on your computer for your Office 365 account.

To set up:

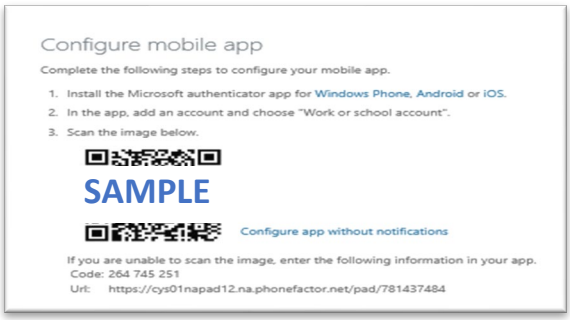
1. Install the free “Microsoft Authenticator” app on your mobile device from your app store.

2. On your computer, navigate to aka.ms/mfasetup and log in using your SOA credentials.



3. Select “Mobile App” as the method of contact.

4. Select “Receive notifications for verification.”



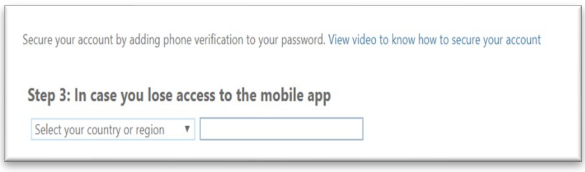
5. Select “Set Up.” A window displaying a QR code will appear.

6. On your mobile device, open the Microsoft Authenticator app and add a “Work or School Account.”

7. Scan the QR code with your mobile device camera. (There are alternate instructions if the QR scan doesn’t work)

8. When the mobile app displays a 6-digit code, select “Next” on the computer screen. You will now receive a text notification. *You do not need to enter the code. If you are unable to scan the QR code, follow the prompts on the computer screen for alternate verification.*

9. On your mobile device, Approve the test notification.



10. On your computer, you will be prompted to add a phone number as a back-up verification method. Select “United States (+1)” as your country or region, enter the desired phone number in the format (###) ###-### and select “Done.”

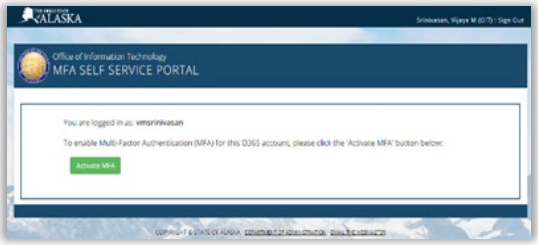
    This phone number will serve as back-up if you lose access to the mobile app. Consider providing a phone number that is not associated with the device where the app is installed.

On the next screen, confirm your preferred and back-up verification options.

11. MFA is now set up but not active. Please complete Activation.

12. Activation can be completed with one click in a self-service protal, https://aws.state.ak.us/mfa/

    Login with your SOA credentials and click on the 'Activate MFA' button.



13. Once you have enabled MFA on your SOA O365 account, it may take up to 60 minutes for it be activated in the system. Once activated, you will begin to receive notifications on your mobile device.

Additional Information

1. Current applications used by MFA includes, but is not limited to:

   - Microsoft Teams
   - Microsoft OneDrive for Business
   - AlaskaNow
   - Microsoft Outlook on the Web
   - Microsoft Stream
   - VPN

2. Some users may need to delete and re-add SOA email, Skype, or similar accounts on mobile devices after MFA is enabled.

3. None of the MFA options and combinations triggered DOPLR concern during an initial review for opt-in (voluntary) MFA.

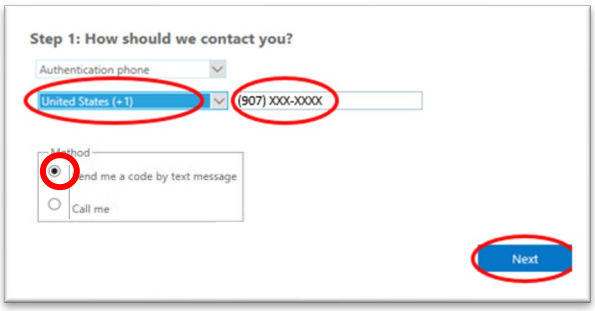
4. Use a personal device for MFA does not make it subject to search or seizure without a search warrant.

Method B: Using text messages to receive a PIN

Using text messages for MFA requires you to enter a code sent to your phone via text message after you enter your SOA login credentials (name and password) for your Office 365 account.

To set up:

1. On your computer, navigate to aka.ms/mfasetup and log in using your SOA credentials.

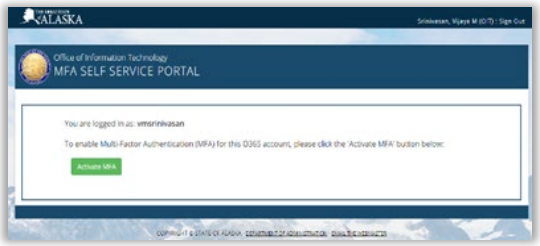


2. Select “Authentication phone” as the method of contact.
3. From the dropdown menu, set your country or region to “United States (+1)”
4. Enter a phone number capable of receiving text messages in the format (###) ###-####.
5. Select “Send me a code by text message” as the method and select “Next.”

6. You will now be prompted to verify your phone by entering a code sent via text message to the phone number provided. Once you retrieve the code from your phone, enter it, and select “Verify.”

7. Once you have successfully verified your phone, click “Done.” On the next screen, you will be prompted to add a back-up verification option. Select “Alternate authentication phone” and provide the country/region code and phone number to complete this process.
8. MFA is now set up but not active. Please complete Activation.
9. Activation can be completed with one click in a self-service protal, https://aws.state.ak.us/mfa/

   Login with your SOA credentials and click on the ‘Activate MFA’ button.



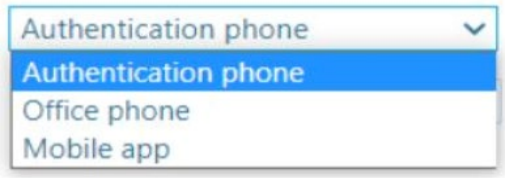
10. Once you have enabled MFA on your SOA O365 account, it may take up to 60 minutes for it be activated in the system. Once activated, you will begin to receive notifications on your mobile device.

Method C: Using Authentication Phone to call back for confirmation

Using Call Back for MFA requires you to specify a phone number in the application so that you may receive a phone call at the number of your choice in order to be authenticated after you enter your SOA login credentials (name and password) for your Office 365 account.

To set up:

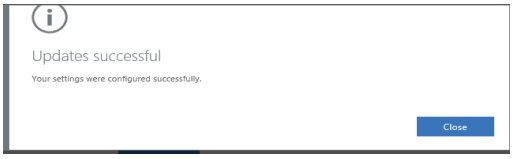
1. Open the site https://aka.ms/mfasetup in a web browser and login with your SOA enterprise credentials.



2. Select the Authentication Phone in the application for the call back.
   IMPORTANT: Setup a second MFA method if you use a Teams Phone or Cisco Soft Phone number to prevent getting locked out when changing passwords.

3. Once you have selected a phone number for call back, when authentication is needed, you will receive a phone call. When prompted, press # and you will be authenticated for access.

4. Once you have completed Step 3 above, you will see “Update Successful”.



5. MFA is now set up but not active. Please complete Activation

6. Activation can be completed with one click in a self-service protal, https://aws.state.ak.us/mfa/

   Login with your SOA credentials and click on the ‘Activate MFA’ button.

Once you have enabled MFA on your SOA O365 account, it may take up to 60 minutes for it be activated in the system.