OFFICE OF INFORMATION TECHNOLOGY

One government, empowered by innovative technical collaboration

# Getting Started with Multi-Factor Authentication

***Update***
**V05/18/22.1**

To improve the security and privacy of employee accounts and State of Alaska data, the Office of Information Technology (O.I.T.) is making Multi-Factor Authentication (M.F.A.) required for Office 365 and other Azure Active Directory services (i.e., Outlook, Teams, OneDrive, etc.) to S.O.A. Executive Branch Departments.

Multi-Factor Authentication (M.F.A.) 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.

Two Step Setup

I. **Selection/Setup**: Select a method of verification that works best for you, A) Microsoft authenticator app notification, B) text message PIN, or C) Call back to a phone number D) Security Key authentication

   Instructions are listed below for each method. Complete the setup for your chosen method.

II. **Activation**: Login to the activation portal, https://aws.state.ak.us/mfa/ and enable M.F.A. It may take up to 60 minutes after activation for the system to update and start sending prompts.

**Note**: M.F.A. is not active until both steps are complete.

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

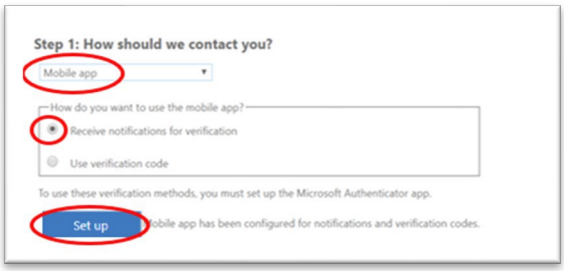
Using a mobile app for M.F.A. requires you to respond to an in-app approval notification after you enter your S.O.A. login credentials (name and password) on your computer for your Office 365 account.

**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/mfa.setup and log in using your S.O.A. credentials.

3. Select "Mobile App" as the method of contact.

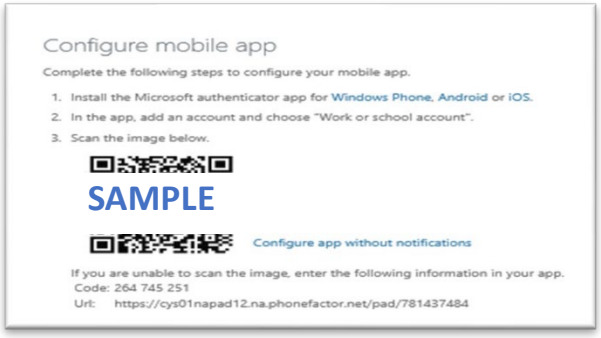



4. Select "Receive notifications for verification."

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."

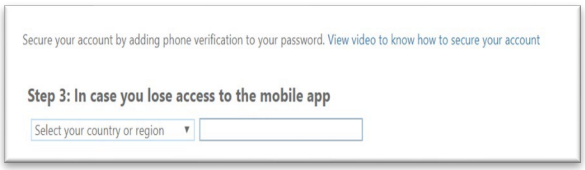
7. Scan the QR code with your mobile device camera. (There are alternate instructions if the QR scan doesn't work)




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. M.F.A. is now set up but not active. Please complete Activation.

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

    Login with your S.O.A. credentials and click on the'Activate M.F.A.' button.


*13.* Once you have enabled M.F.A. on your S.O.A. O365account, 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. *Please review Additional Information at the end of this document.*

**Method B: Using text messages to receive a PIN**

Using text messages for M.F.A. requires you to enter a code sent to your phone via text message after you enter your S.O.A. 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 S.O.A.credentials.

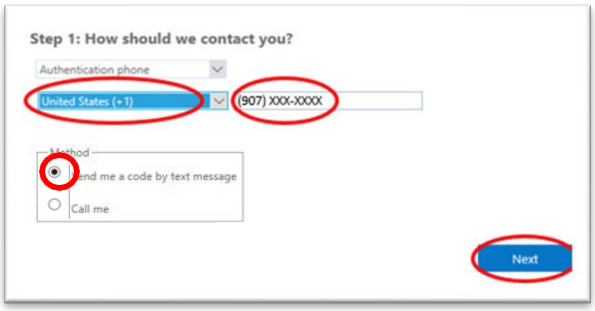
2. Select "Authentication phone" as the method of contact.

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. M.F.A. is now set up but not active. Please complete Activation.

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

   Login with your S.O.A. credentials and click on the 'Activate M.F.A.' button.

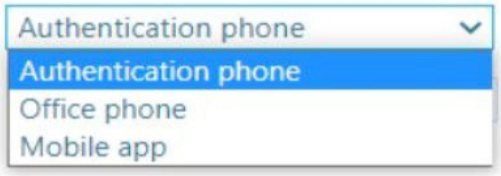

10. Once you have enabled M.F.A. on your S.O.A. O365account, it may take up to 60 minutes for it be activated in the system. Once activated, you will begin to receive notifications on your mobile device. Please review Additional Information at the end of this document

**Method C: Using Authentication Phone to call back for confirmation**

Using Call Back for M.F.A. 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 S.O.A. 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 S.O.A. enterprise credentials.




2. Select the Authentication Phone (Mobile, Office or Alternate Phone) in the application for the call back.

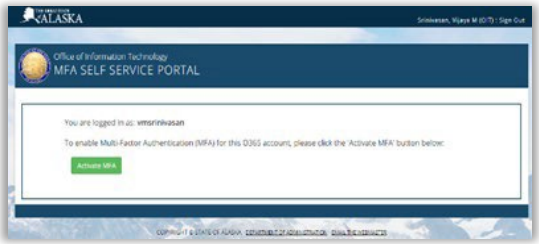
3. Once you have selected a phone number for call back, when authentication is needed, you will receive a phone call. When prompted, press # and you will be authenticated for access.


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

5. M.F.A. is now set up but not active. Please complete Activation.


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

   Login with your S.O.A. credentials and click on the 'Activate M.F.A.' button.




7. Once you have enabled M.F.A. on your S.O.A. O365account, 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. Please review Additional Information at the end of this document.

**Method D: Physical Security Keys**

Using Physical Security Keys for M.F.A. requires you to either insert the physical key in your computer or enter a code that is displayed on your physical key after you enter your S.O.A. login credentials (name and password) on your computer for your Office 365 account.

Physical Security Keys provide a multifactor authentication option when the recommended mobile app or text/call back options are not viable and should be considered as a secondary option to the text/call back or authenticator app.

**To Set Up – Refer to the Security Key Enrollment Guide for your specific key**

**Additional Information**

1. Remember to access the self-service portal to activate M.F.A. after you set it up.

2. Users who have M.F.A. enabled on their S.O.A. enterprise accounts will be required to use M.F.A. when accessing applications that use Microsoft Azure Active Directory (A.A.D.). This list of applications is expected to grow. It currently includes, but is not limited to:

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

3. In most cases, apps like Teams or Outlook will only need to authenticate once the first time you sign in. If you need to sign in on another computer, close the web browserfor some browser-based apps, you may need to provide your second factor again.
   Some users may need to delete and re-add S.O.A. email, Skype, or similar accounts onmobile devices after M.F.A. is enabled.
   Microsoft's M.F.A. options do not distinguish between personal and business devices. Departmental policies on issuance of S.O.A. devices and use of personal devices for S.O.A.business apply. Check your department's policy if you have questions. None of the M.F.A.options and combinations triggered DOPLR concern during an initial review for opt-in (voluntary) M.F.A.

4. Using a personal device for M.F.A.—whether by means of a text, call back, or mobile app —does not subject that device to a public records request because the device would at most contain (at the time of the request) an expired code that had been used for logging into a state system: i.e., a transitory record that is no longer persevered or appropriate to preserve for its informational value or as evidence of the agency's organization or operation.
   Also, using a personal device neither increases nor decreases the risk that the device would be subject to search or seizure in a criminal matter—unless an issue in the criminal matter was about access to a state system that was accessed using M.F.A.. Per Alaska statue 12.35.020 and 12.35.025, warrants may be issued for search and/ or seizure of any property, personal or work, if used in conjunction with the commission (or the intent of commissioner) of a criminal act.

5. If needed, M.F.A. can be disabled by submitting a request ticket in the AlaskaNow portal. This is not an option if M.F.A. is mandatory for your department or division.