OFFICE OF INFORMATION TECHNOLOGY

One government, empowered by innovative technical collaboration

Getting Started with Multi-Factor Authentication
V20250227

Microsoft Entra MFA for end users

What is MFA?

Multi-Factor Authentication (MFA) adds another factor beyond just your password to validate whoever signing in to your account is actually you - this can be done via an automated phone call, a text, or an app on your phone. Microsoft Entra MFA in this article uses Microsoft's Entra ID service (similar to Office365) to provide this, though there are other service providers that do similar in theory.

Why do I need MFA?

As technology generally becomes more powerful, so too does the technology malicious actors, hackers, bad guys, etc. have. Passwords by themselves were once much more effective, but today they're easier than ever to break or bypass. To combat this, MFA adds a "something you have" factor (e.g. a particular phone) to the "something you know" factor (your password) - even if your password is leaked, someone would still probably need your phone to sign-in.

Enrolling in MFA

There are two steps to set up MFA:

1. Setting up the authentication method, such as a phone number or the Microsoft Authenticator App.
2. Opting in to MFA enforcement for your account. For some departments, the enforcement may be automated - please consult with your regular helpdesk team if you have questions.

Step 1: Registering an MFA Method

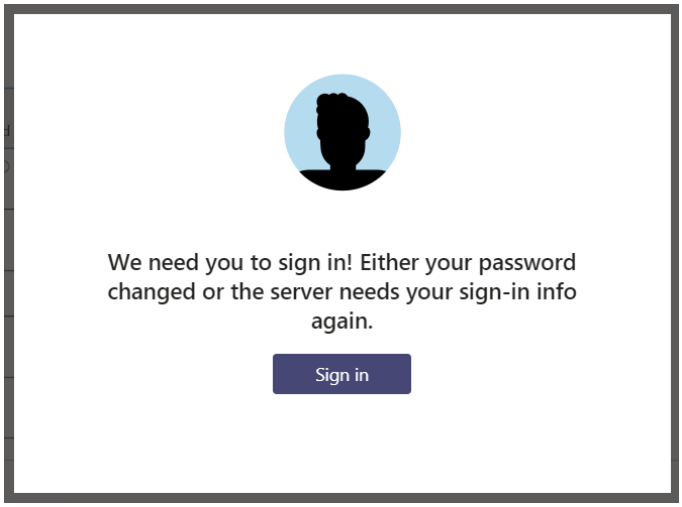
Getting Started with Multi-Factor Authentication

To set up a secondary authentication method, start here.

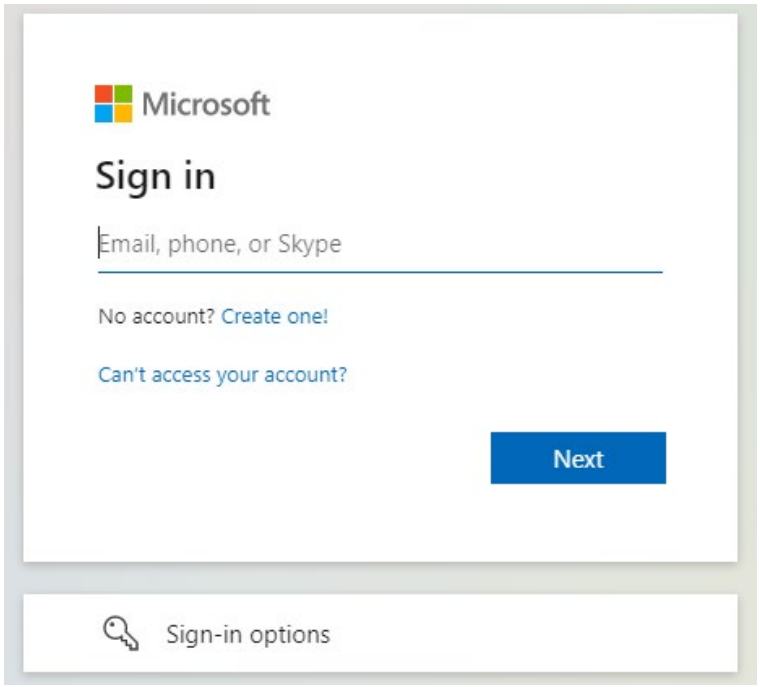
1. Go to : https://aka.ms/mfasetup (for best experience, we recommend starting this from a PC).

   You may also be prompted to go to this page on sign-in if your IT admin has specifically enforced MFA for your account.

   Prompt in Teams



   Prompt in Microsoft Online

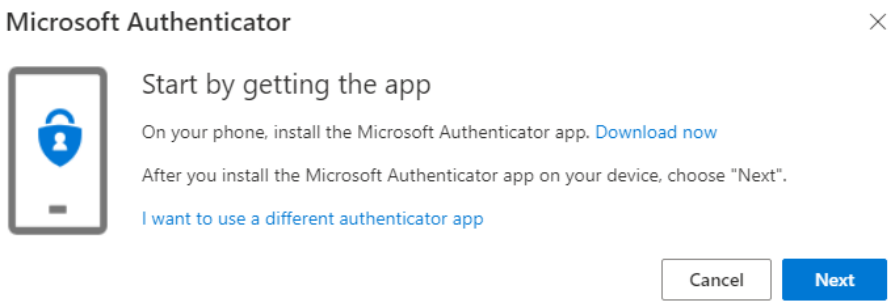


2. After signing in again, you'll be brought to the **Additional security verification** page. From here, you can configure the type of MFA you'd like to use. There are three main options, as below. You can use more than one, to have an alternate available as a backup.

MFA Option A: Mobile app - Microsoft Authenticator (recommended)

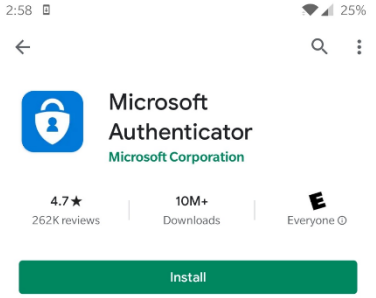
The Microsoft Authenticator app is for many the most convenient form of MFA. With the authenticator app, you can receive notifications about sign-ins and approve/deny them from your phone, or you can use a rotating One-time passcode (OTP).

1. Setting up the mobile app will require installing the Microsoft Authenticator app on your mobile (iOS/Android) device. You'll need an Internet connection on your mobile device to download the app.



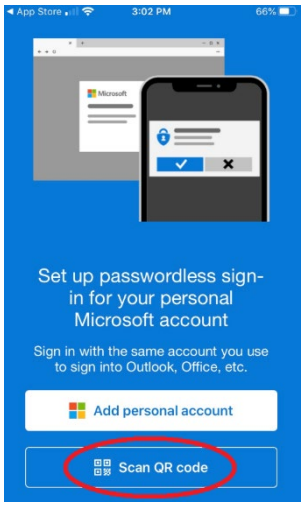
Authenticator app on Apple iOS

Authenticator App on Android



2. After installing the app, open it. Assuming you have MFA screen open on a PC or other device, select the option to Scan QR code.

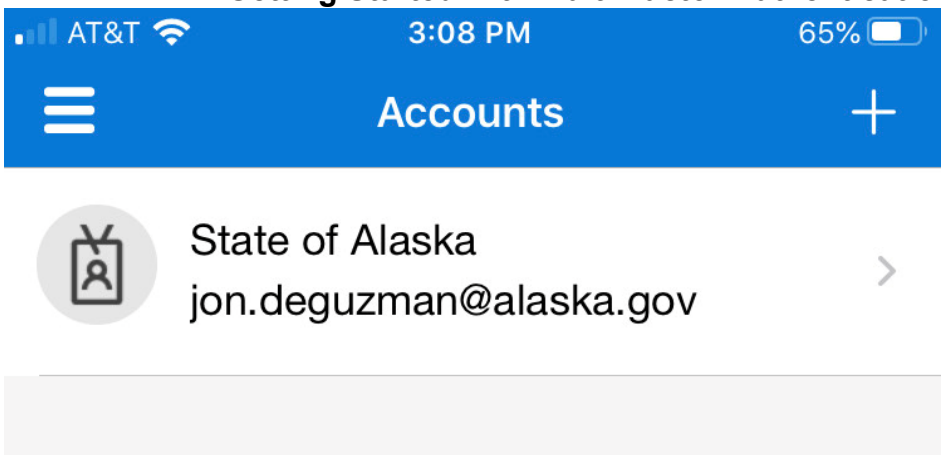
   Scan QR Code Option in Authenticator App



3. Scan the QR code presented to you in the "Configure mobile app" instructions.

   Note: you may be prompted to accept alerts from Microsoft Authenticator. You'll need to accept these, or else the process will fail. If it fails, just accept the alert notification and restart the process, which will generate a new QR code you can use to scan successfully.

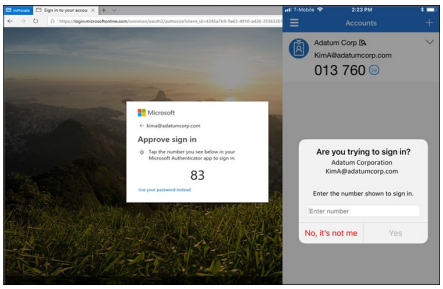
4. After scanning your QR code, the Microsoft Authenticator app on your phone should now be configured with your O365 account.



5. You can use either the notification method or the one-time password code option.
    1. **Via push notifications with Number Matching**

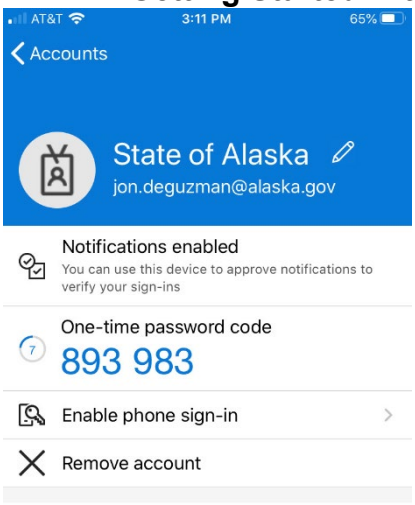
        Some details vary between iOS / Android.

        After completing your first-factor authentication (password), you'll be presented with a two-digit number. When you interact with the push notification for the Microsoft Authenticator app, you'll enter this number into the prompt to complete the authentication.

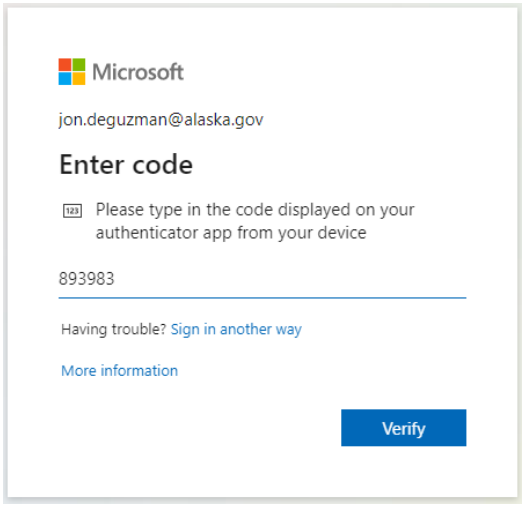


    2. **Via one-time password code (OTP)**

        After clicking on your account, you can see your current One-time password code. Keep in mind that this code refreshes every 30 seconds.



When prompted during logins, enter the One-time password code currently displayed in your Microsoft Authenticator app.



After verifying with the correct code, you'll be signed into O365.

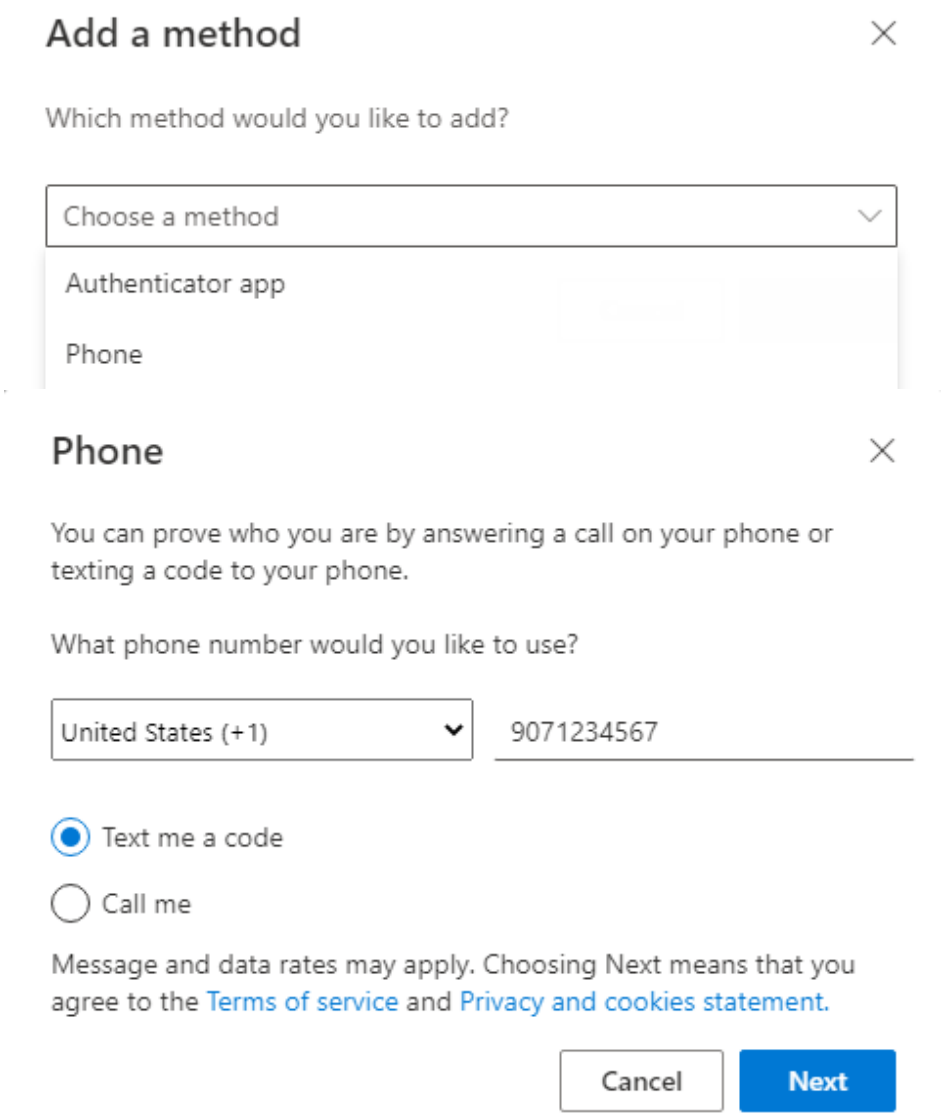
After setting up this authentication method, you may set up another MFA method or opt-in to enforcement as per step 2.

MFA Option B: Authentication phone (voice call or text message)

If you choose **Authentication phone** you can specify a phone number to use to receive the verification code, by phone or text message.

If you receive phone calls via Microsoft Teams or a Cisco softphone (computer-based calling), do not use that phone number alone for receiving MFA prompts. Signing in to Teams Phone to receive calls will also require MFA, and Cisco softphones may require signing in to VPN (itself requiring MFA) before they can receive calls if you are teleworking.

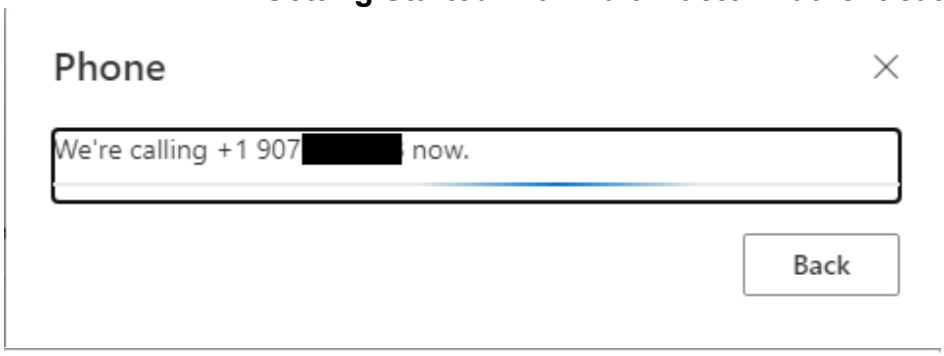
Adding an authentication phone

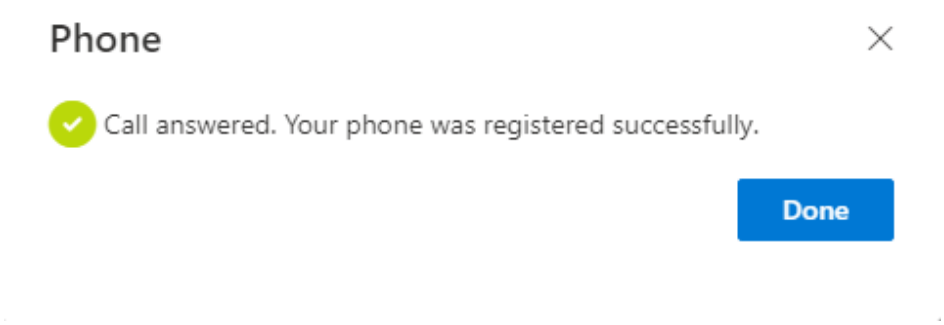


Phone numbers may either be called, or sent a text message.

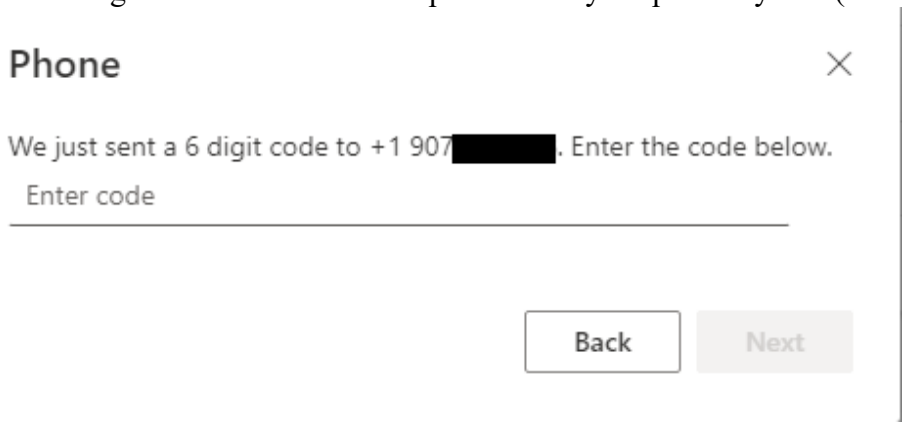
Choosing the call option will call the phone, and prompt you by phone to press the # key.

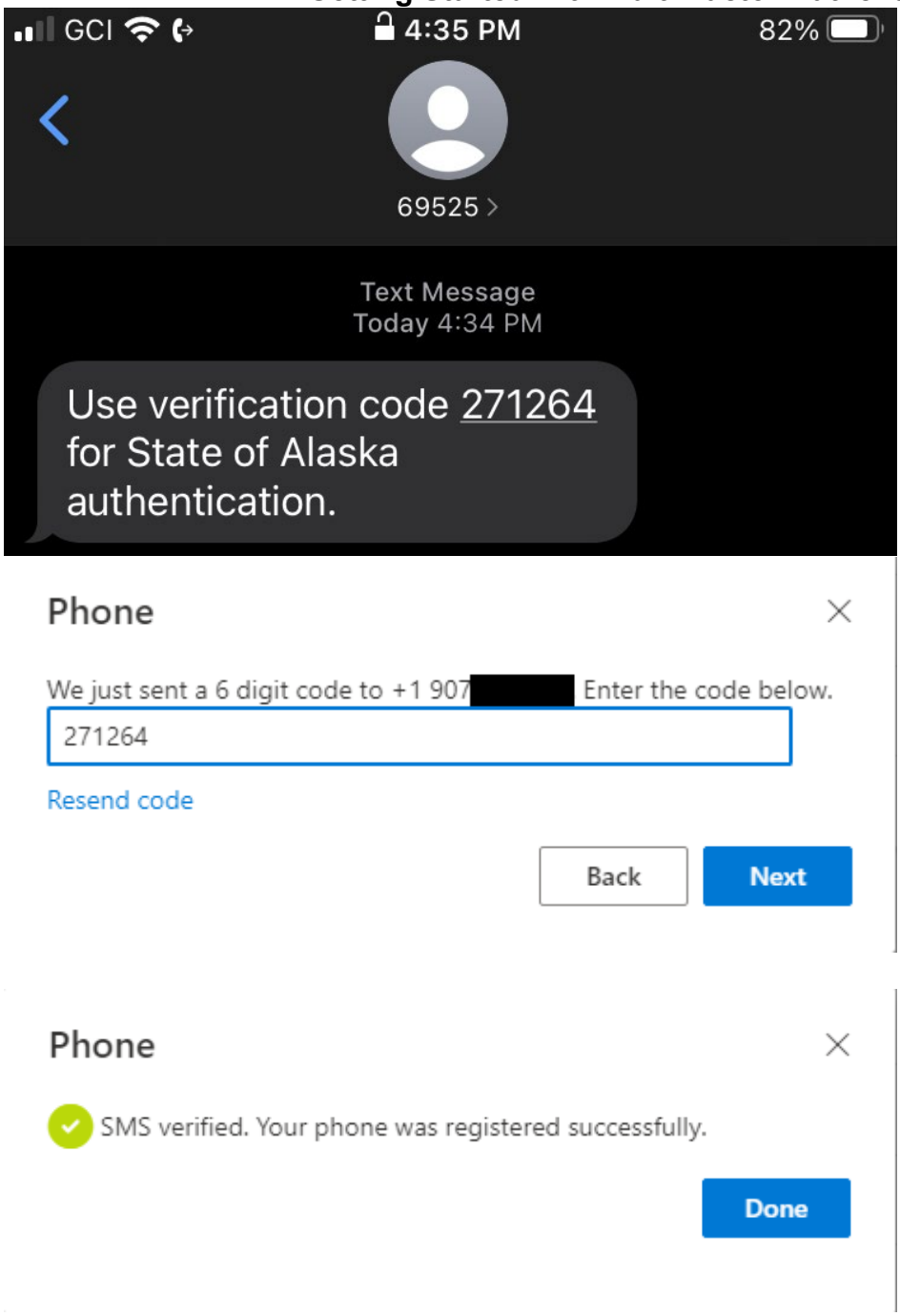
Getting Started with Multi-Factor Authentication





Text messages will send a one-time passcode to your phone by text (SMS).

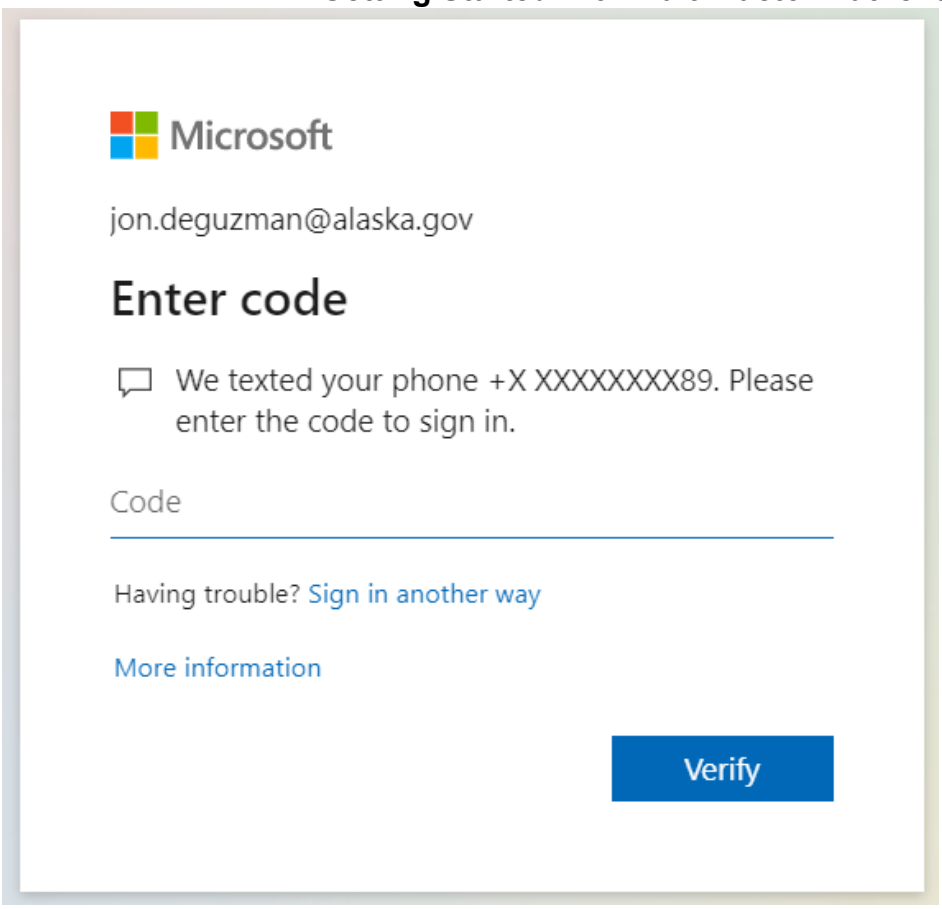




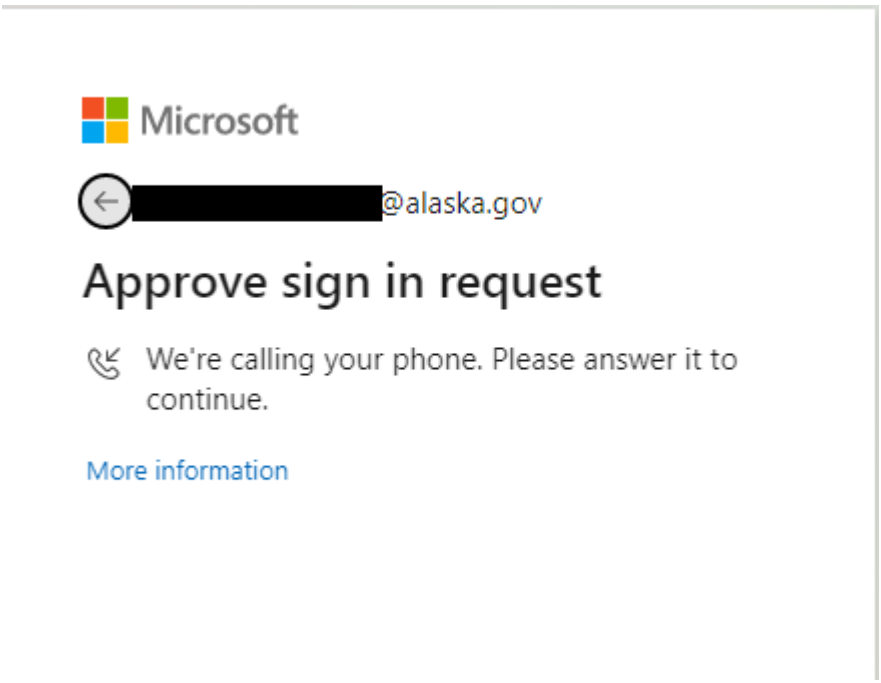
Once the verification code has been entered correctly. Click **Done**.

The authentication phone verification method is now configured. Whenever you log into O365, you'll be presented with the following screen:

Getting Started with Multi-Factor Authentication



or



After verifying with the correct one time passcode or with voice call verification, you'll be signed into O365.

After setting up this authentication option, you may set up another MFA method or opt-in to enforcement as per step 2.

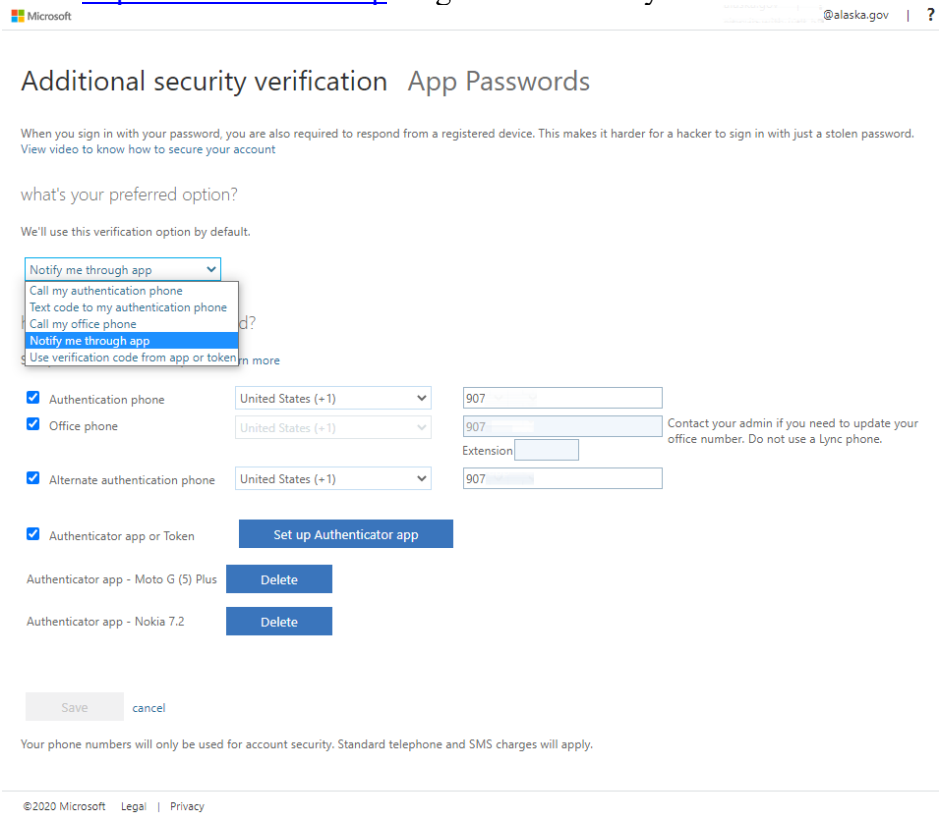
MFA Option C: Physical tokens

Some departments have opted to use physical hardware devices that can provide the one-time passcode required, similar to the phone app. These do have a cost associated with them, so quantities are limited. Please contact your admin staff or IT support if you need this option.

Managing MFA after set up

After you've set up MFA for the first time, you can change items like your default method, add additional methods, or remove old methods (e.g. if you switch phones).

1. Go to https://aka.ms/mfasetup - sign in if necessary.



2. Check or uncheck boxes for whatever authentication methods you prefer to have available.
3. Use the drop-down menu to select your preferred method. The other methods will be available as backups unless you uncheck them.

Step 2: Opting in to MFA enforcement

After you've set up a secondary authentication method, you can opt-in to enforcement.

Note:

- Some departments choose to enforce MFA for users without action required by the end user
- If you opt-in to enforcement without having set up a method, you may be required to set up a second factor before signing in to any O365 services, VPN, et cetera. Some applications, like Outlook 2016/2019, may not be able to redirect you appropriately to sign up for MFA - if in doubt try signing in to portal.office.com via a web browser, like Google Chrome or Mozilla Firefox.

To opt-in to enforcement:

- Go to https://aws.state.ak.us/mfa/ and click "Activate MFA". This will take an hour or so to sync the MFA enforcement. If you see a message saying "MFA has already been enabled on your account." you do not need to take any further action.
- Ask your helpdesk to assist.

Troubleshooting

iOS Mail App

If you have issues with the iOS mail app and repeated prompts for MFA, try removing and re-adding your alaska.gov account from your phone, or removing it from the Mail app and using the Outlook for iOS app instead.

Common Questions

Q: What applications need MFA?

A: Most Microsoft Office 365 applications will, including Outlook, OneDrive for Business, Stream, Teams; as will certain applications such as SOA VPN. Windows logins and many other non-Microsoft applications (e.g. IRIS) will not.

Q: Do I need to use MFA every time I sign-in?

A: For most applications, no - you'll only need to authenticate once with a particular application, until you change your password again. If you use a web browser to access these apps, you may have to authenticate with your second factor once per session.

Q: Do I need to setup MFA separately for each different computer or device I'm using?

A: No, you can set up your authentication methods once for your account (e.g. via the https://aka.ms/mfasetup link), and then they apply for any device you use thereafter.

Getting Started with Multi-Factor Authentication

Q: Do I need to use a particular authentication method?

A: No. Many users find the Microsoft Authenticator app the most convenient, but you can use any one of the authentication methods, or multiple of them.

Q: What happens if I don't have access to my usual authentication method (e.g. authenticator app)?

A: You can set up multiple authentication methods, with a default and some back ups. If the default you selected is not available, you will have a link to use another method. If you have no access to any of your methods, please contact your IT support for assistance.

Q: Are there authentication options when I don't have Internet or phone service?

A: The one-time password code option in the Microsoft Authenticator app has will function without the mobile phone itself having network/phone connectivity (e.g. even in airplane mode). The physical token option will also show a usable one-time passcode regardless of network connectivity. In either case you'll still need network connectivity on the device you're connecting with (e.g. laptop connecting to webmail).

Q: If I'm using my cell phone, do I need to set up my cell phone number anywhere else (e.g. Outlook)?

A: No, you just need to put it in the MFA set up page. It does not need to be in the directory.

Q: Will my cell phone number show up elsewhere if I put in for MFA set up?

A: No. It's specific to the MFA process, and will not show up in Outlook from MFA set up alone.

Q: Can I use app passwords?

A: Please do not use these unless directed to by your IT staff. There are some risks/limitations to app passwords that can cause problems in some circumstances.

Q: Can I use my office phone number?

A: This is not recommended for most staff as Teams Phones may require you to use MFA to receive calls, and most departments have switched to Teams Phone.

Q: Does this MFA effort include signing in to Windows (e.g. my laptop or desktop computer)?

A: No, not at this time.

Q: Does the Microsoft Authenticator App give SOA the ability to control my phone or access personal data on my device?

A: No. State of Alaska administrators may be able to see the name of the device but do not have control over or access to the device itself, similar to how listing a home phone number for contact does not give an organization control over that phone number. See: https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-faq#registering-a-device

Q: If I join another organization as a guest (e.g. via Microsoft Teams), does my MFA transfer over?

A: Not quite. Other organizations may require their guests to use MFA separately, and have their own separate list of registered MFA methods. You can use a single Authenticator app to store MFA information for multiple organizations at once, though they will show as separate accounts in the app (e.g. as "State of Alaska" peter.parker@alaska.gov and separately as "Shield Corporation" peter.parker_alaska.gov#EXT#@shieldcorp.onmicrosoft.com). If you have already used MFA to sign in to your alaska.gov account, unfortunately the other organization likely has no way to verify that and may prompt you separately for MFA.

Q: What username should I use to sign in to State of Alaska (SOA) resources that require MFA, such as State of Alaska's VPN, if I don't have an alaska.gov mailbox?

A: In most cases if you have a pre-created, sponsored SOA account, then sign in to SOA resources such as VPN will require you to use a username like fmlast4soa@alaska.gov. This is a username (sometimes called a "User Principal Name" or "UPN" in this format), but not technically a functional email address (no email can or should be sent to it); the @ alaska.gov portion indicates which of Microsoft's hosted identity platforms (Entra ID "tenants") you are trying to sign in to, such as SOA's instance. This does not apply to "Guests" invited to and exclusively for Microsoft Teams, which can usually leverage inter-tenant authentication to let a Guest authenticate in their home tenant with own organization's credentials.