

How to REGISTER for O365 Multifactor Authentication (MFA)

Introduction

This document provides guidelines on how to register for Multifactor Authentication (MFA) for State of Hawaii (SOH) Exchange Online accounts. If you desire access to Office 365 services outside of the SOH network, you will be required to do a one-time registration before accessing your Exchange Online services from devices NOT connected to the SOH network. Once registered, your Office 365 account will have nearly impenetrable protection from unauthorized external access as a secondary authentication factor will be required when logging in from outside the SOH network.

NOTES:

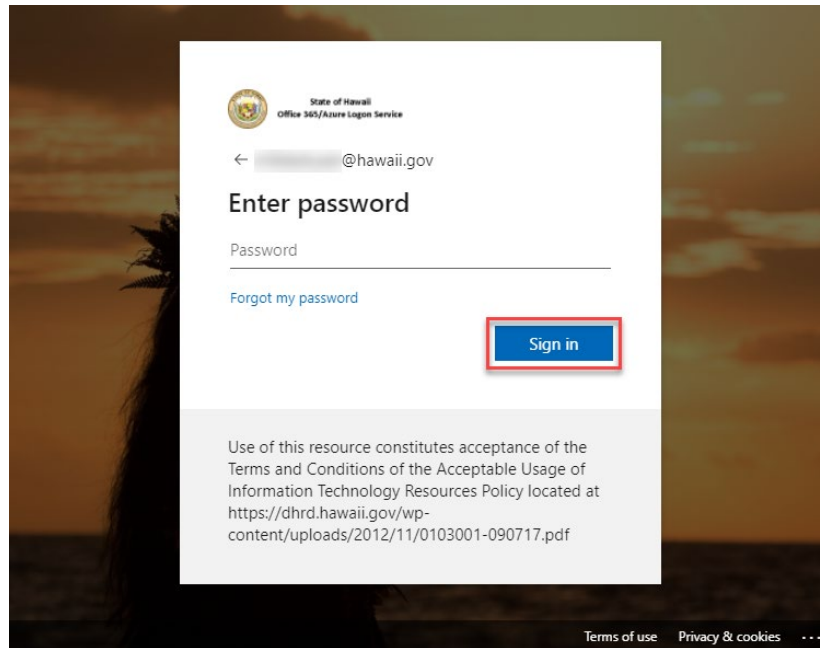
- Enabling MFA on an account is voluntary and a value-add capability with Office 365 access
- Registration requires the chosen authentication device to be functional to fully complete.
- Users will only be prompted for MFA when the Office 365 account is accessed from outside a SOH network connected device (ex. home, cellular network, public hot-spots). For this reason, we prohibit providing an office phone number as an authentication phone.
- MFA requires the user's awareness when they have made a request for authentication. Meaning the user has the option of denying the authorization if they did not submit the request themselves. A user must be aware if they deny three (3) consecutive authentication challenges, their account will go into a short lockout period and will be unable to access Office 365 resources for a few minutes. Once released from the lockout, any further consecutive denials will result in progressively longer lockout periods. This is important as an unprovoked authentication challenge could mean that the user's credentials have been compromised and malicious actors are attempting to access the account from outside the SOH network. Anytime this occurs, user should immediately change their password and inform their IT staff of the incident.
- A user can "miss" (or not answer) three (3) MFA challenges before the account locks.
- If you are not expecting an authentication prompt, you can decline the authentication:
 - By app: Press **Decline** upon receiving the notification
 - By phone: Press zero (0) then pound (#) to prevent anyone from accessing your account.
- If you have any questions or concerns, please contact the ETS Service Desk at ETS.ServiceDesk@hawaii.gov.

1. To access the registration page

- a. Open the following URL in a web browser:

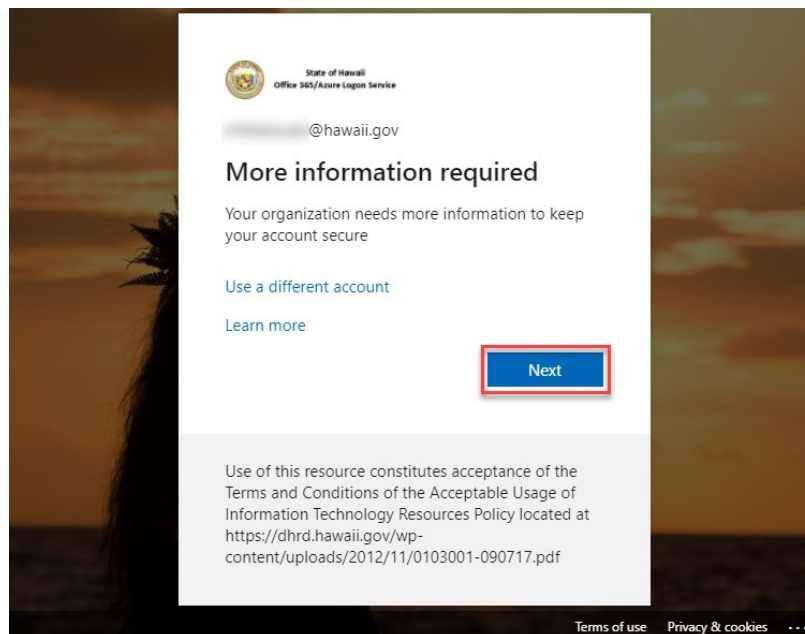
<https://aka.ms/MFASetup>

- b. Enter your State of Hawaii Office 365 email address and password.
- c. Click “Sign in.”



2. To begin registration

- a. Select **Next** button to begin the registration process



Registration Information – Read Only

The following is for informational purposes only and requires NO action. After reading this page, please proceed to Step 3.

Important: You will need to register using at least two (2) of the following options. We recommend registering for ONLY options a and b.

a. Authenticator App (Requires download to device)

i. Choose between **Receive notifications for verification** or **Use verification code**.

1. **Receive notifications for verification**: Notifications are pushed to your device for approval (requires network connection)

2. **Use verification code**: Use the app to provide a six-digit code (does not require network connection)

ii. **Receive notifications for verification method** is **RECOMMENDED** for devices that are regularly connected to a data or Wifi network and will incur a negligible data charge (less data than receiving an email). **Use verification code** is **RECOMMENDED** for devices that may not always be connected to a data or Wifi network or for users wanting to avoid data charges for push notifications.

b. Authentication Phone (Requires phone number)

i. Choose the appropriate country code; **United States (+1)** is default. The field CAN be configured with any phone number using the XXXXXXXXXX (10 digit) format.

ii. **Call Me** option is **RECOMMENDED** for this option. **Send me a code by text message** can be used but this method IS vulnerable for spoofing or hijacking but is still an option if desired.

iii. Most phone plans do not charge for incoming calls so no fees should be incurred by listing a non-SOH phone number. Text message charges will apply depending on plans; another reason why the text code option is not recommended.

c. Office Phone (Recommended for self-service password reset use only)

i. This method is automatically configured from the user's AD account and is non-editable. It requires the country code (+1 for US) to be entered in AD account.

ii. If you do NOT have an Office Phone number in the Active Directory, this will not be filled out automatically and cannot be configured. Please disregard.

MFA Fact Sheet link: <http://o365.hawaii.gov/o365/mfa-setup/>

To jump to the setup instructions for the **Mobile App**, click [here](#).

To jump to the setup of an **Authentication Phone**, click [here](#).

To set up both, you may continue through the document.

ETS **DOES NOT** recommend using the **Office Phone** option for MFA.

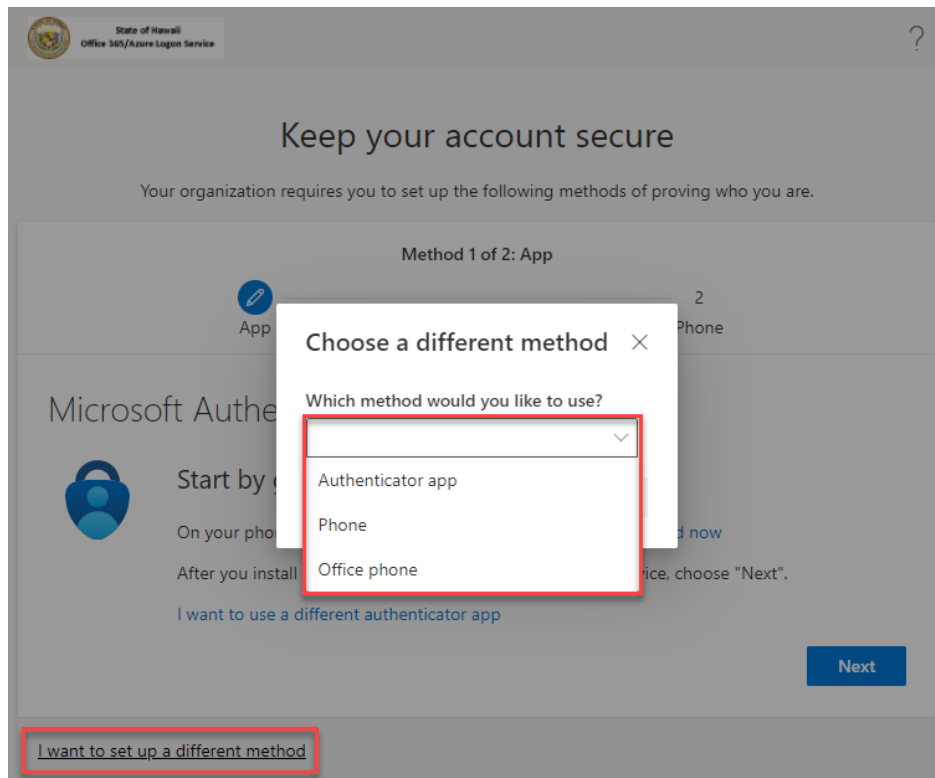
3. Converged MFA/SSPR setup

Microsoft has now allowed MFA registered options to be leveraged as methods to verify your identity to self-service password reset and vice versa. The only exception to this is you may **NOT use security questions you've set up for password reset as an MFA verification method**. This means that when you register MFA options, you are also registering options allowing you to reset your password yourself. This process can be initiated anytime you've forgotten your password. For instructions on how to initiate self-service password reset, please click [here](#) or scroll to the last section of this guide.

4. Registration

When you sign into <https://aka.ms/MFASetup>, you will be presented with options to register your MFA verification methods. These can be set up in any order.

- a. Start by selecting your primary MFA method. Default is the Microsoft Authenticator app, but you are free to choose alternate methods by selecting **I want to set up a different method** link.



- b. Once you choose your preferred option, you can continue to those option instructions below.

5. Registration Options

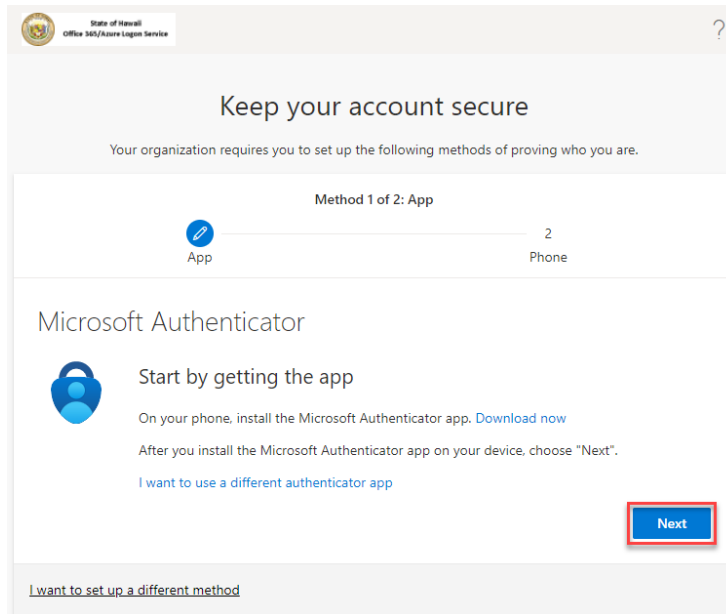
Authenticator App

The following details the **Authenticator App** verification option.

- a. On your mobile device, navigate to the appropriate App/Play Store and search for “Microsoft Authenticator” (pictured below). Install the app (you will need to provide your Apple/Google account and password) and continue with the next step on your browser.

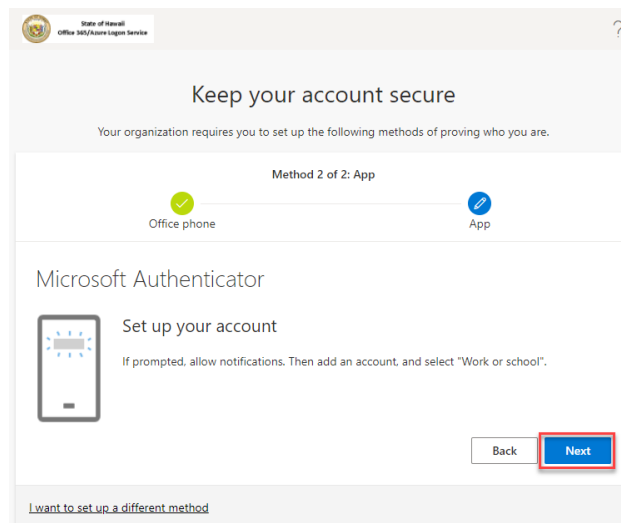


- b. Choose **Next** on Authenticator App from the dropdown menu (from Step 4a above)

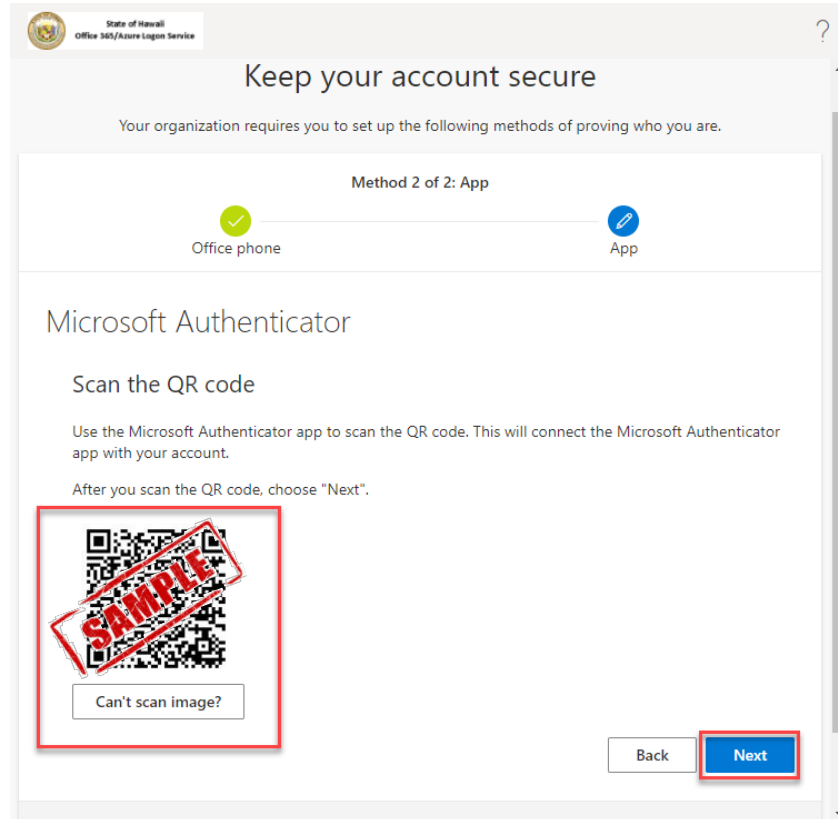


Note: You can choose an existing authenticator app if you'd rather not to use the Microsoft one

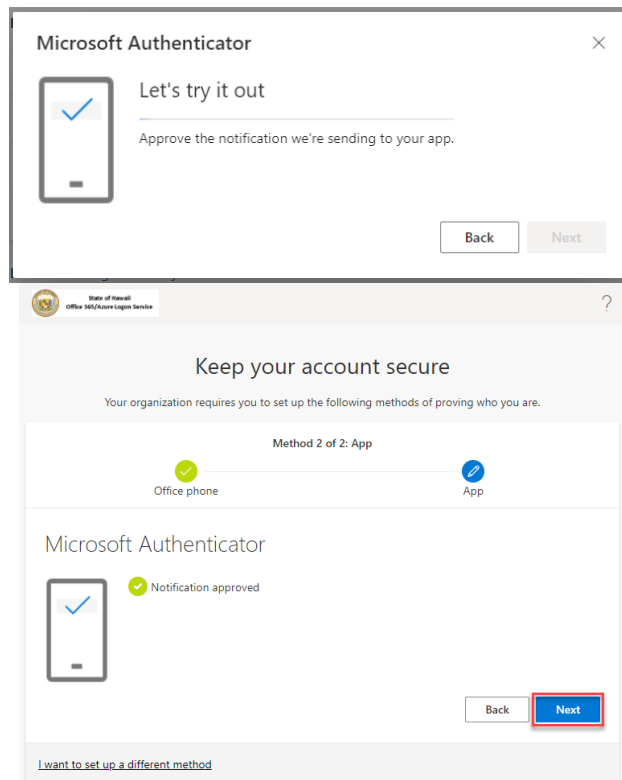
- c. Select **Next** after you've followed the on-screen instructions.



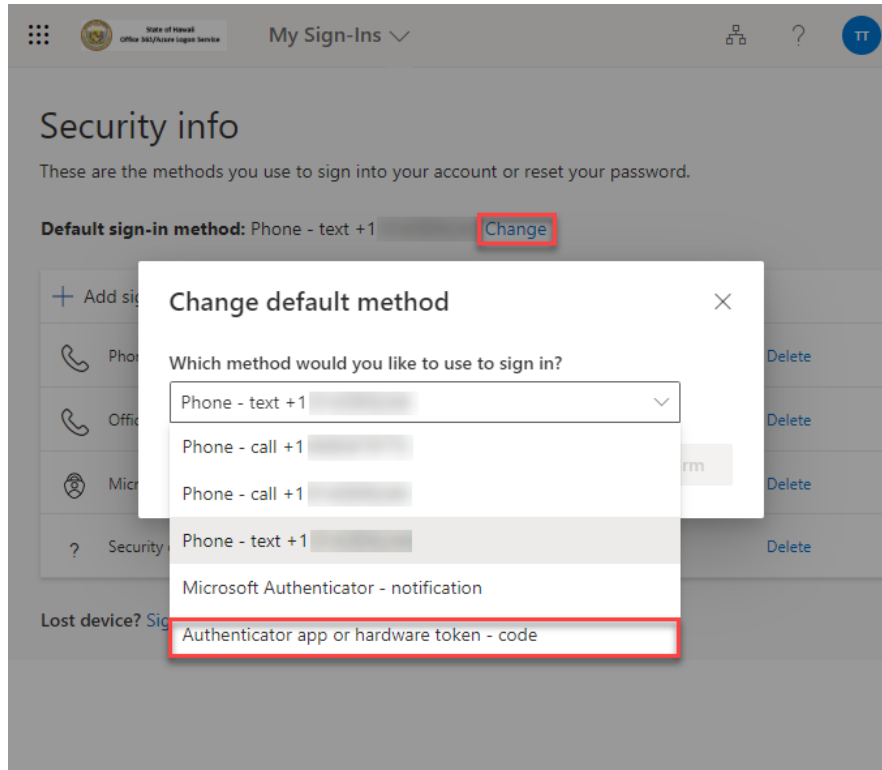
- d. Choose Scan QR Code on your app and move the camera over the QR code presented. Once the account shows up on your app, you can click **Next** button



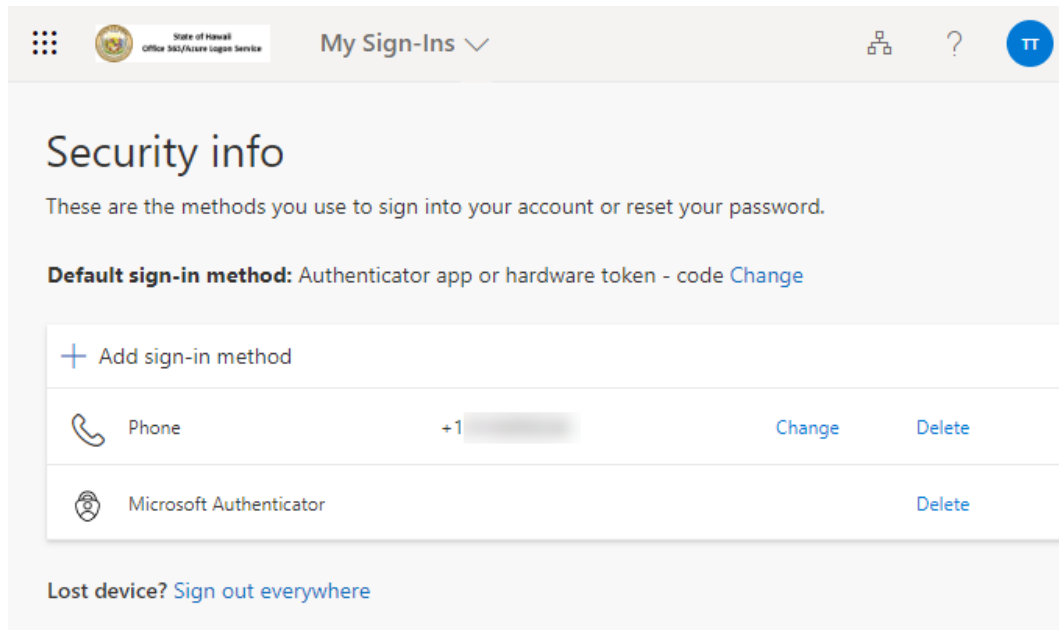
- e. When you register the authenticator app, ensure your device is near you and press **Approve** when you receive the prompt on your device to complete.



- f. If you would like to use **verification code** option, you'll be able to select the option once you've finalized your app registration. You'll be able to change your default MFA option by clicking the **Change** link. Then choose **Authenticator app or hardware token - code** option. Click **Confirm** to commit the change. This will set the authenticator app code as your default option.



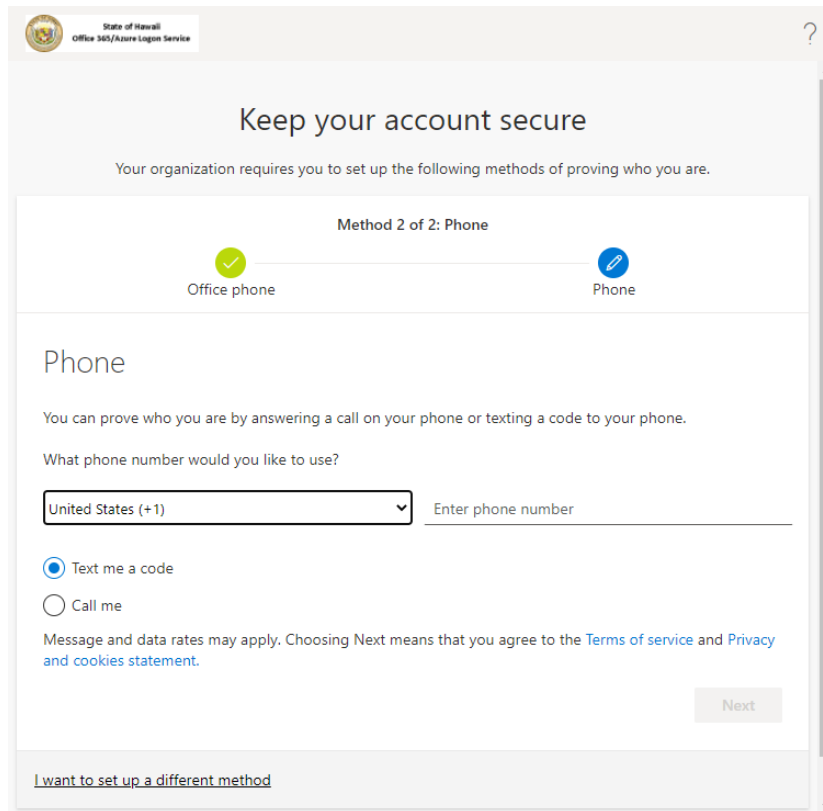
- g. You are now ready to choose a second (2nd) MFA option to register before completing the registration process. Once complete, you'll be presented with a list of your registered options.



Authentication Phone

The following details the **Phone** verification option.

- a. Choose **Phone** from the dropdown menu (from Step 4a above). Provide the phone number you wish to register.



State of Hawaii
Office 365/Azure Login Service

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

Office phone Phone

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1) Enter phone number

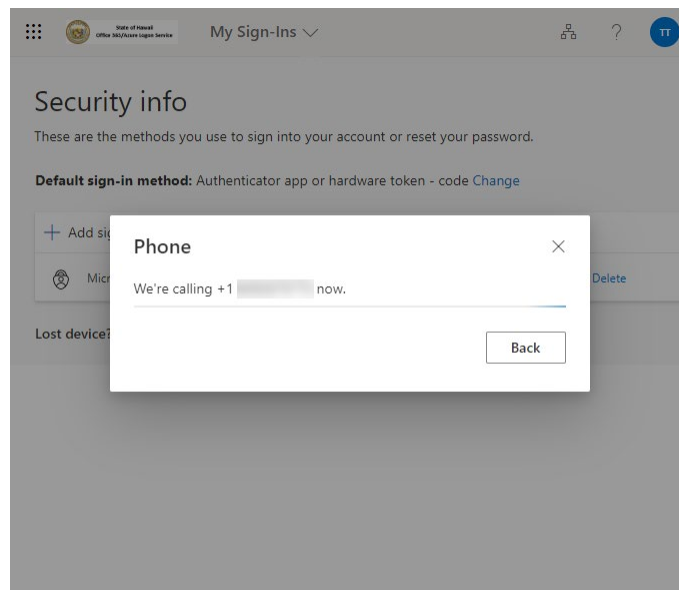
Text me a code
 Call me

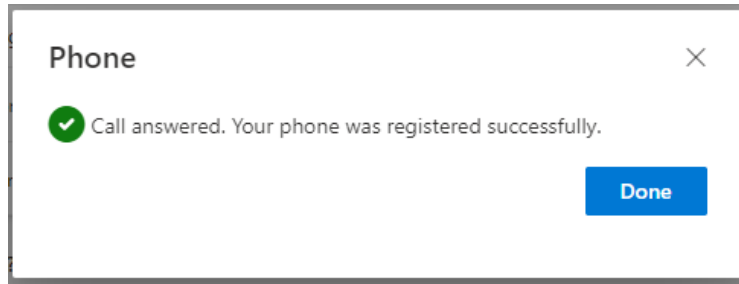
Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

[I want to set up a different method](#)

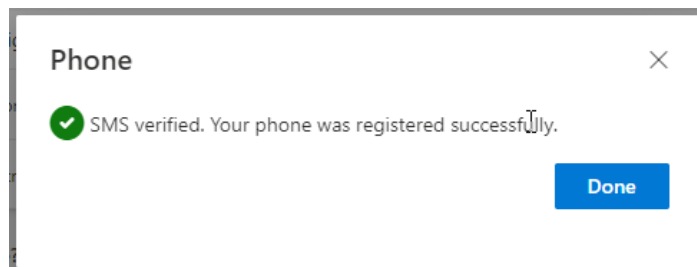
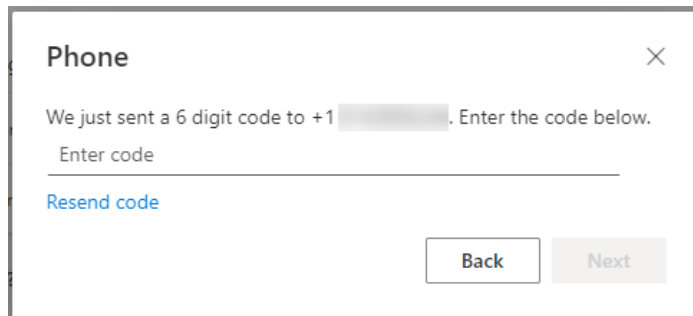
- b. Select the location **United States (+1)** and enter your phone number in XXXXXXXXXX format
 - i. If you select **Call me** and click **Next**: Once the call is received, press the pound/hash (#) key to accept the authentication. You can then end the call.



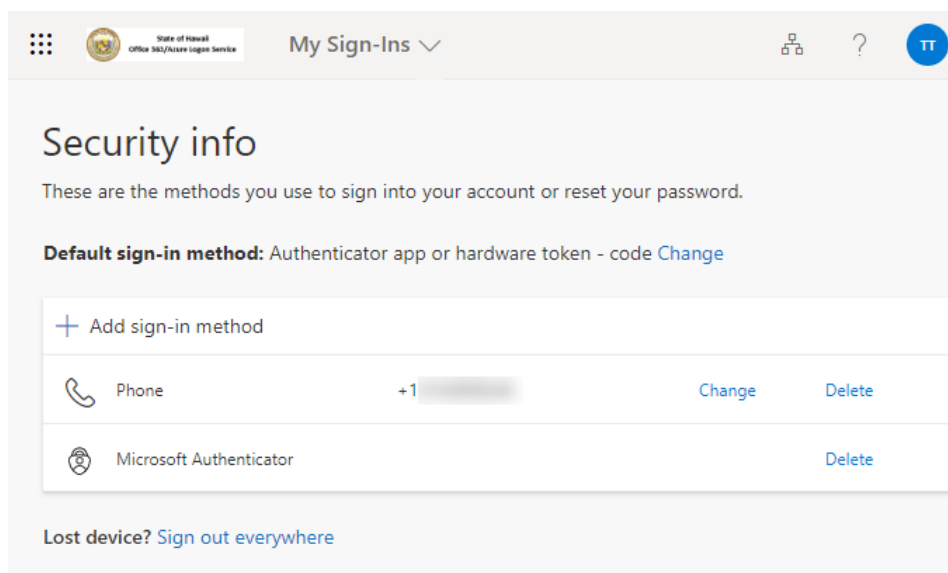


*Note: You do not need to talk into the phone at any point to respond to the phone call option. This might be useful information for those who believe that the phone option will be obtrusive and distracting. You can use this method even if your phone is silenced.

- ii. If you select the **Text me a code** and click **Next**: Once you receive the text message code, enter it into the area provided. Click **Next**.



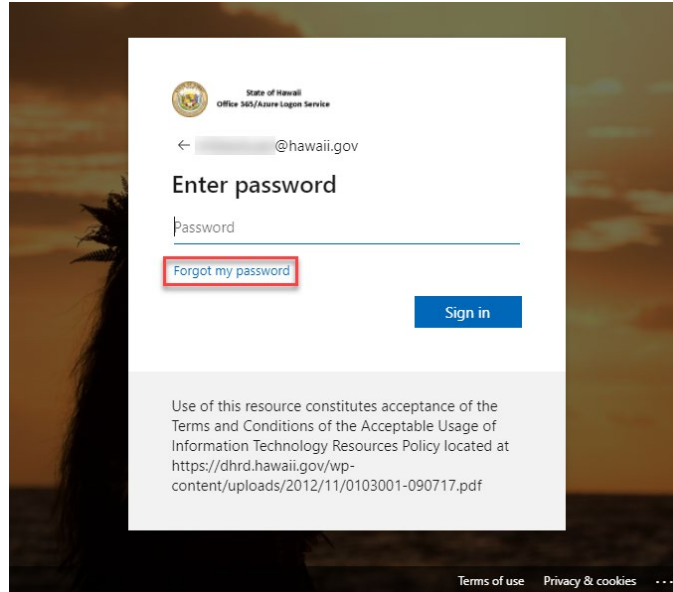
- c. Once complete, you'll be presented with a list of your registered options.



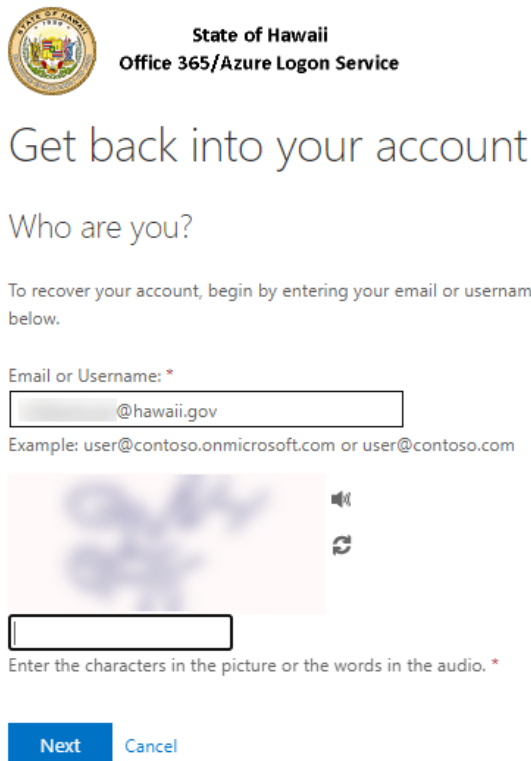
Self-Service Password Reset

With the verification option registration converged, you can now leverage the options you use to MFA for resetting your account password from anywhere. To reset your password at any time, follow these instructions:

- a. Navigate to <https://portal.office.com> or attempt to sign into any SSO enabled service. Enter your username and click **Next**.
- b. Select the **Forgot my password** link under where you can enter your password



- c. With your username already populated, fill out the Captcha prompt and click **Next**.

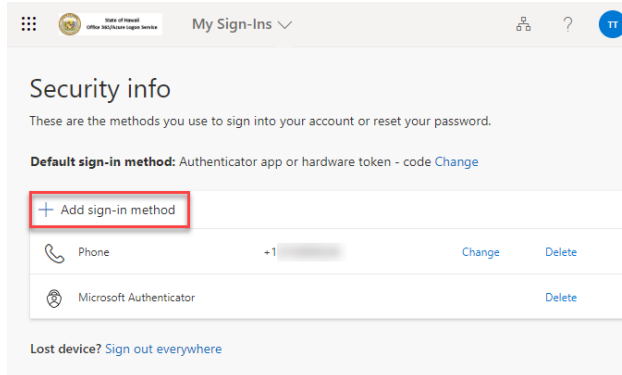


- d. You will need to complete two (2) separate verification steps before being able to reset your password. You can choose any options you've previously registered.

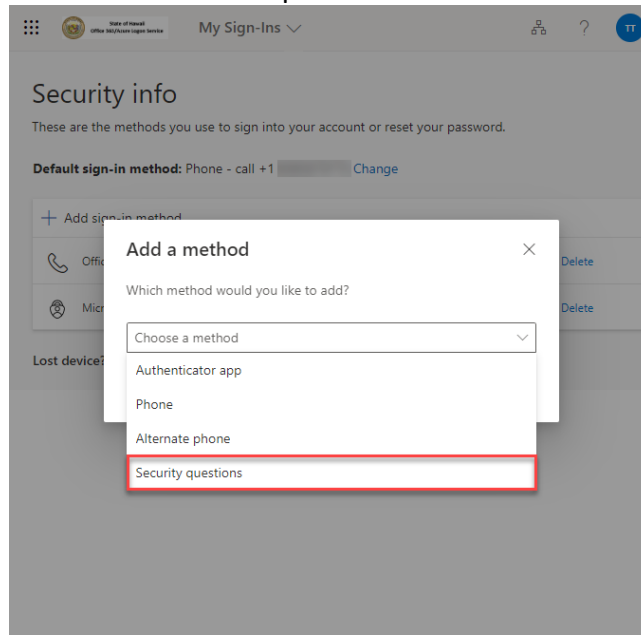
- e. Once you've verified through both of your required methods, you'll be presented with a screen to create a new password.

You do have 2 additional methods to register if you'd like to have more options available for SSPR verification: Office Phone and Security questions. The office phone is similar to the phone method described above. Security questions can be registered as follows:

a) Choose **Add a sign-in method**.



b) Select **Security questions** from the dropdown and click **Next**.



c) Pick 5 questions and provide answers and click **Done**.

