

Setting up Multi-Factor Authentication User Guide

March 2022

What is changing?

To protect and secure your work information, AHS is expanding the use of Multi-Factor Authentication (MFA) for accessing the Microsoft Outlook Web Access application either remotely or using an AHS device logged-in with a shared ID.

Without MFA, AHS email has only one layer of protection – your password. If someone gets your username and password, they will have access to your AHS email, putting our systems at risk.

With MFA, anyone attempting to access your email will need access to your MFA authentication method before access is granted. This additional security step helps protect your information and our systems from unauthorized access, or harmful emails that could be infected with malware.

How Multi-Factor Authentication (MFA) works:

When using Microsoft **Outlook Web Access (OWA)** to access your AHS email remotely or from an AHS workstation logged in with a shared ID, you will be prompted for the second method of authentication, as follows:

1. You will enter your AHS username and password in the Microsoft Outlook Web Access.
2. You will be asked to authenticate using your preferred method.
3. You will allow or deny access to your AHS email.

There are several methods of authentication you can set up:

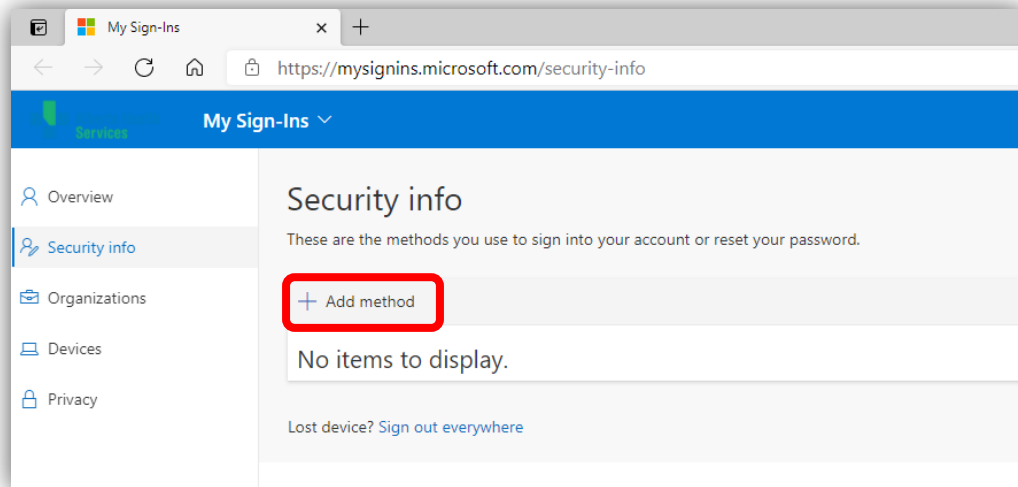
- Using the Microsoft Authenticator app on iOS or Android mobile device.
- Receiving a call or text to a cellphone.
- Receiving a call to an office phone or landline.

You must set up **at least one authentication method**, even if you never connect to your AHS email remotely. We recommend that you set up at least two methods in case you do not have your primary options available. When selecting methods, consider ways in which you log on remotely and will need to use MFA - at home or travelling, using a smartphone or tablet, etc., and pick methods that you will be available to you at those times and locations.

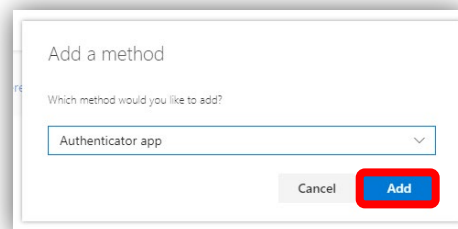
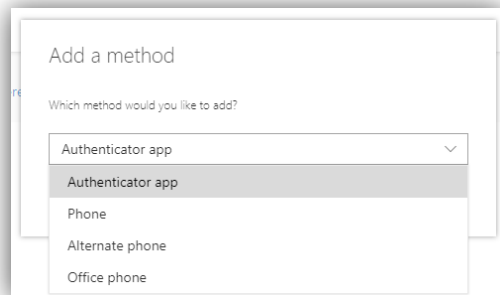
You can change - add, delete, or update - your methods at any time by visiting <https://mysignins.microsoft.com/security-info>.

Setting up your Multi-Factor Authentication methods

1. On your computer open this link in Microsoft Edge browser
<https://mysignins.microsoft.com/security-info>. This screen will open. Click on **+ Add method**



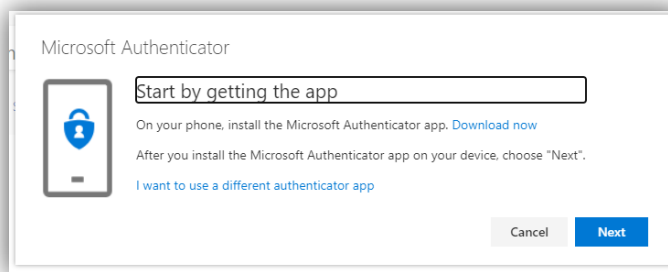
2. This screen will pop up. Click on the drop-down box and select your preferred method. We recommend the Authentication App as the securest option; this requires a cellphone or tablet. Click **Add** once you have made your selection



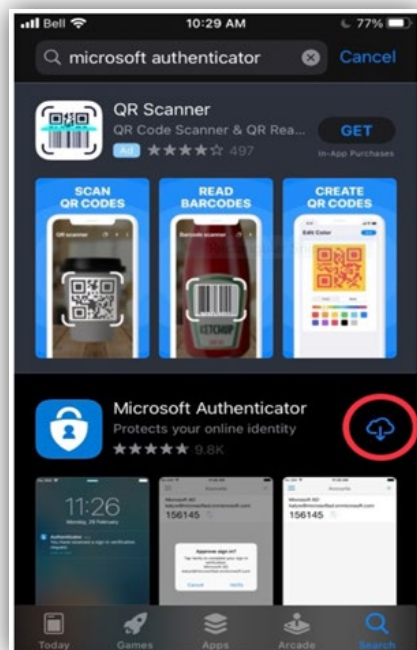
- | | | |
|--------------------------------|---|------------------------------------|
| a. Microsoft Authenticator App | - | continue to step 3 |
| b. Phone (call or a text) | - | go to step 14 |
| c. Office phone | - | go to step 19 |
| d. Alternate phone (call only) | - | go to step 24 |

Setting up the Microsoft Authenticator App

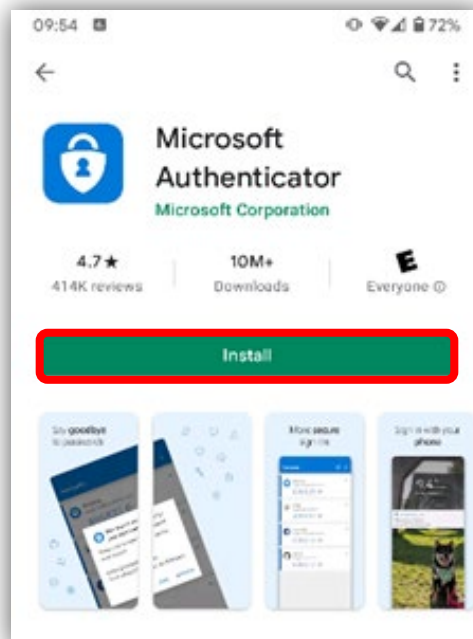
This method requires a cellphone or tablet. Once installed the Microsoft Authenticator app can be used either to receive a notification or generate a code that can be used for authentication. A code can be generated when the device is not connected to a cellular network or wi-fi. The easiest way to complete the set-up of the authenticator app is to have two devices to work with, the cellphone or tablet you are installing the app on and a computer to follow the set-up steps.



4. For iPhone, go to the **App Store**. On Android, go to the **Google Play Store**. Once on the respective app store, search for "**Authenticator**". You will see a few authenticator products. Be sure to select **Microsoft Authenticator**. Tap on the Download or Install Icon

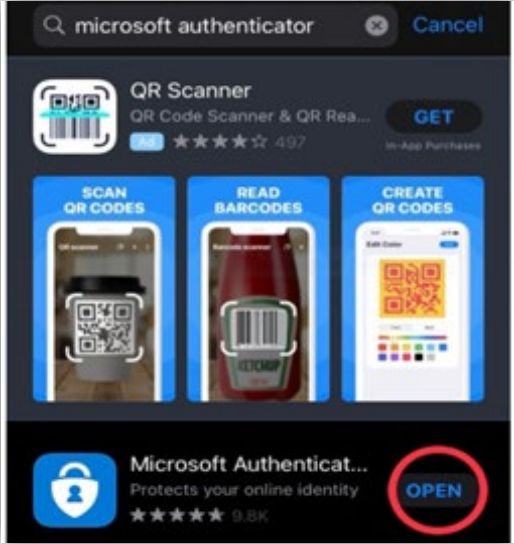


iOS Screen

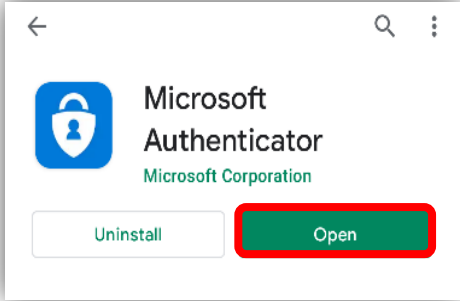


Android Screen

5. Once the download is complete, tap **Open**.

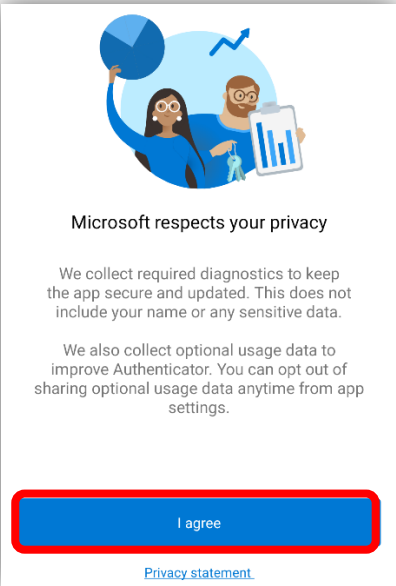


iOS screen

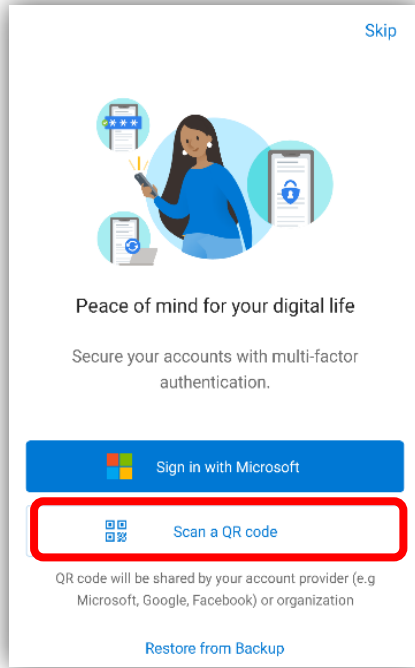


Android screen

6. Tap **I agree** on the 'Your Privacy Matters' screen.

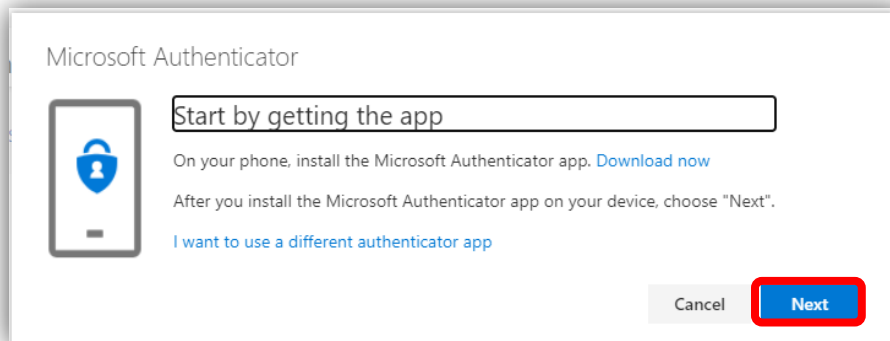


7. The following screen will appear. Tap on **Scan a QR code** button.

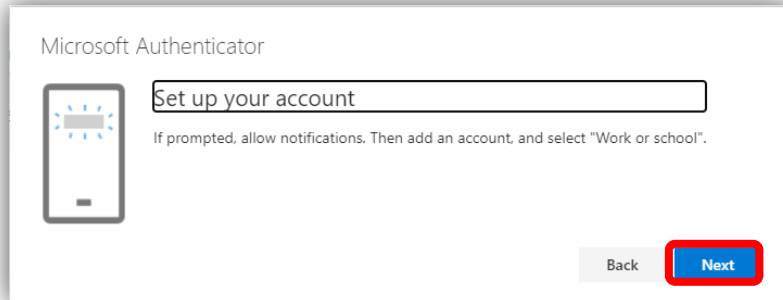


If prompted select the option to set up a work/school account.

8. Once the camera is activated, return to your computer/laptop and click **Next**.

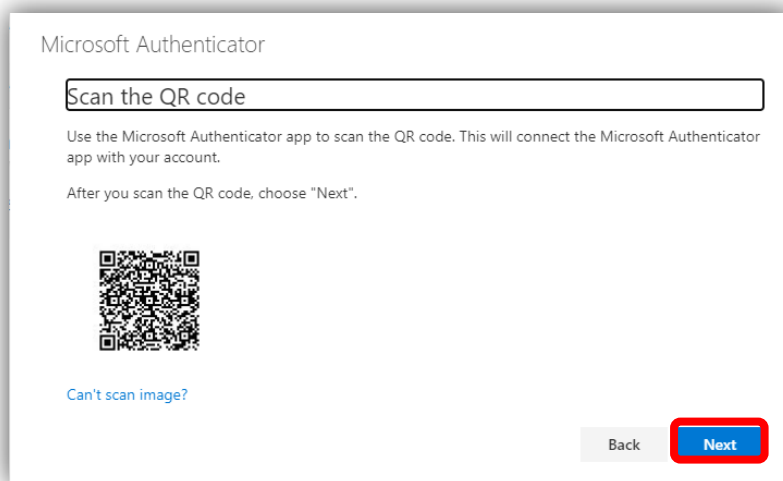


9. When the 'Set up your account' screen appears, click **Next**



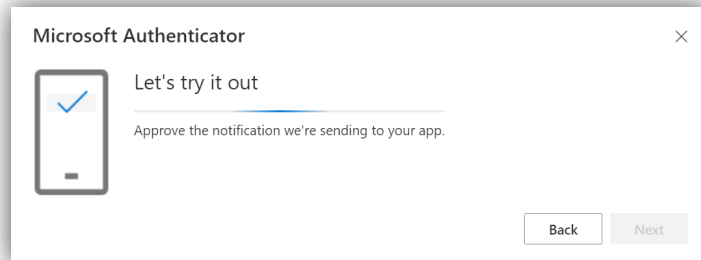
Note: if you have an existing Alberta Health Service account set up in your Microsoft Authenticator app this will need removing by following these steps:

- a. In the App, tap the existing Alberta Health Service account
 - b. Tap gear symbol in the top right corner
 - c. Tap remove account
 - d. Tap to confirm remove account
 - e. Add account
 - a. Work or school account
10. Use the camera on your phone or tablet to scan the bar code that appears on your screen.
- Note: Do not** scan the barcode in the screenshot below, this will not work.

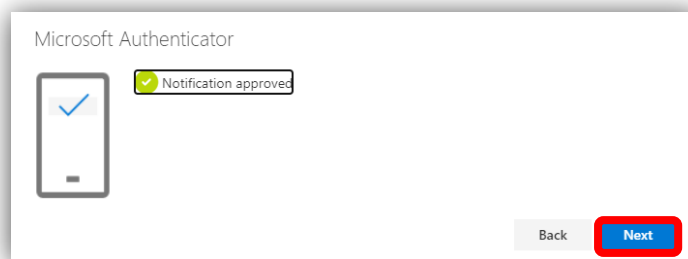


Once the scan is complete a message will appear on your cellphone or tablet confirming that the Alberta Health Services account has been added. Click **Next** on the computer screen.

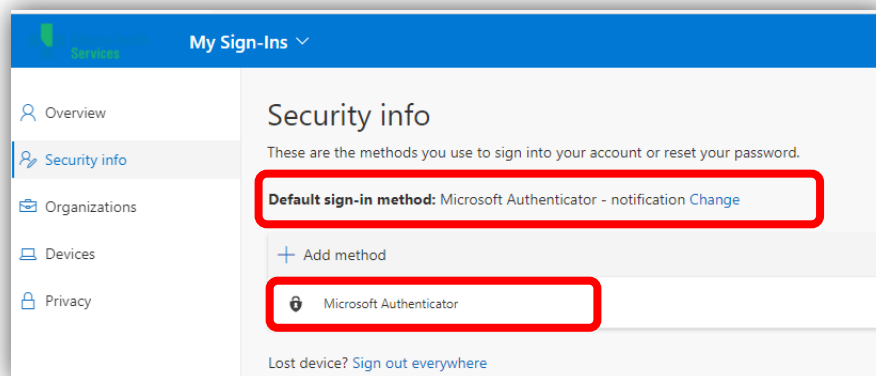
11. When the 'Let's try it out' screen appears you will receive a notification on your cellphone or tablet to Allow or Deny access to your AHS email. Tap **Allow**.



12. Once you have allowed access the computer screen will change to confirm that the notification was approved. Click **Next**.



13. Congratulations, your Authenticator App has now been successfully set up and is your default method of multi-factor authentication. This method will automatically be contacted when additional authentication is required.

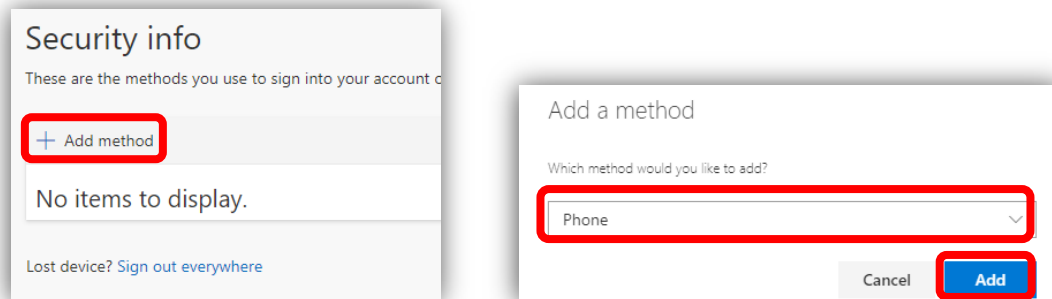


We highly recommended that you add a second method for authenticating, just in case you do not have access to the cellphone or tablet that the authenticator app is installed on.

- a. A Phone to receive a call or a text - go to [step 14](#)
- b. An Office phone to receive a call - go to [step 19](#)
- c. An Alternate phone to receive a call - go to [step 24](#)

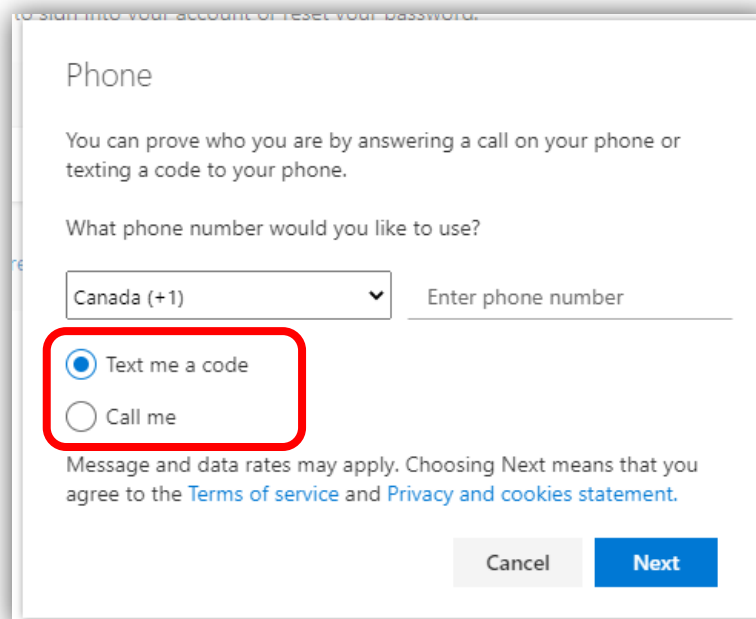
Setting up a Cellphone

14. This method of authentication requires a cellphone or mobile device with cellular service. Click the **+ Add method** and proceed to select **Phone** from the dropdown menu then click **Add**.



15. The following screen will appear, note there are two possible ways to authenticate with your cellular phone:
- **Text me a code:** You will receive a numerical code via SMS that you will be prompted to enter when authenticating your login.
 - **Call me:** When attempting to login, you will receive a phone call in which an automated message will prompt you to press a key to authenticate the login.

Select your preferred choice from the bullet points below, whichever option you choose will be the default method. Note, that you can also choose to use the non-default method to authenticate later when logging in.



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?

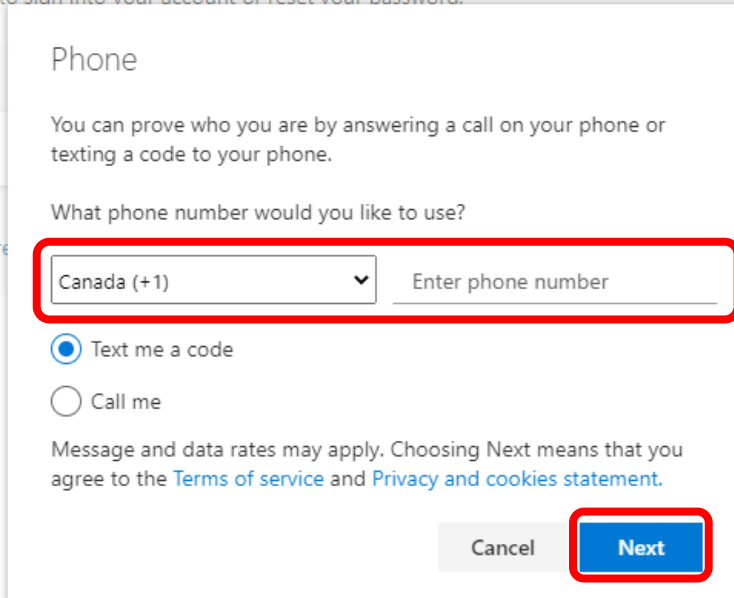
Canada (+1) Enter phone number

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](#).

Cancel Next

16. Under the first drop-down box, select the region as **Canada (+1)**, then type your **Phone number** in the adjacent field.



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?

Canada (+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](#).

Cancel Next

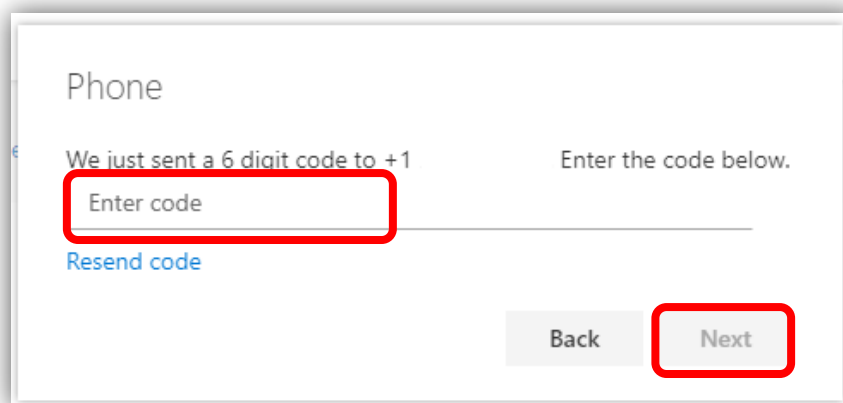
Afterward, click **Next**.

17. You will now be prompted to authenticate using your cellphone by one of two methods, depending on which option you selected in Step 15.

a. If you selected **Text me a code**:

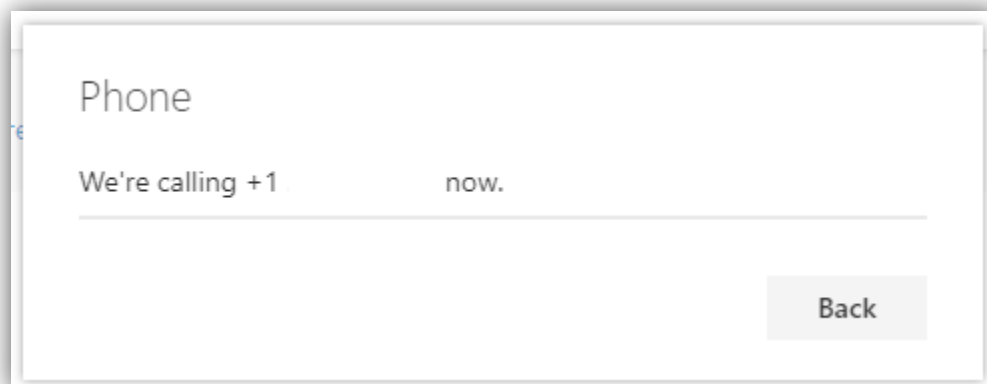
The following screen will appear. You should have received an SMS text message containing the 6-digit code.

Note: If you did not receive a text message with the code, double-check that the phone number is correct, then click **Resend code**.



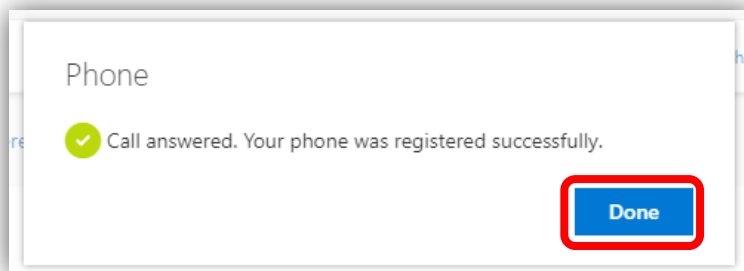
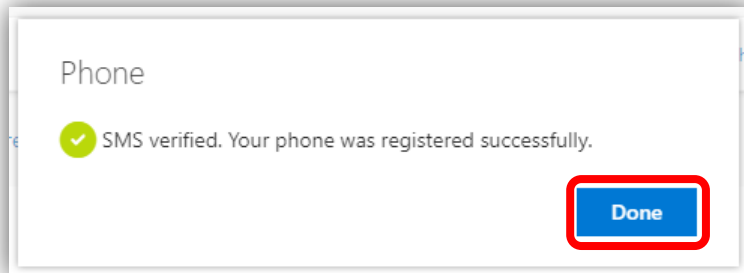
Enter the 6-digit code into the field, then click **Next**.

b. If you selected **Call my phone**:



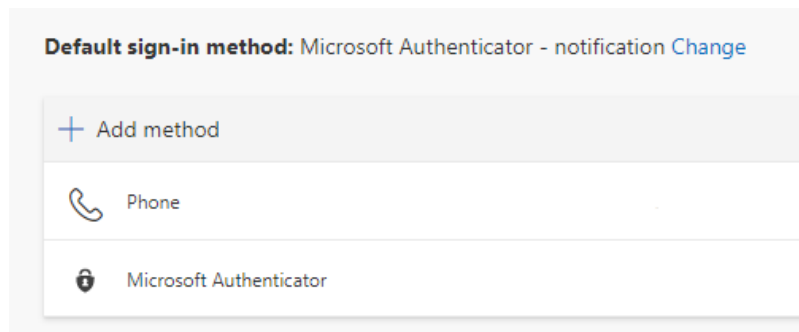
Answer the call, and follow the instructions relayed by the automated message. You will be prompted to Press **Pound (#)** to allow access.

18. Upon completing the authentication, you will see either of the following messages:



Click **Done**.

You are now set up to use your phone as a method of authentication.



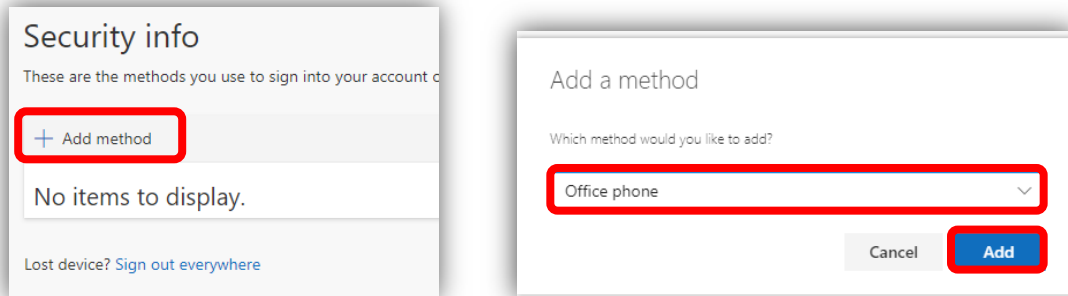
To set up

- a. The Microsoft Authenticator App - go back to [step 3](#)
- b. An Office phone to receive a call - continue to [step 19](#)
- c. An Alternate phone to receive a call - go to [step 24](#)

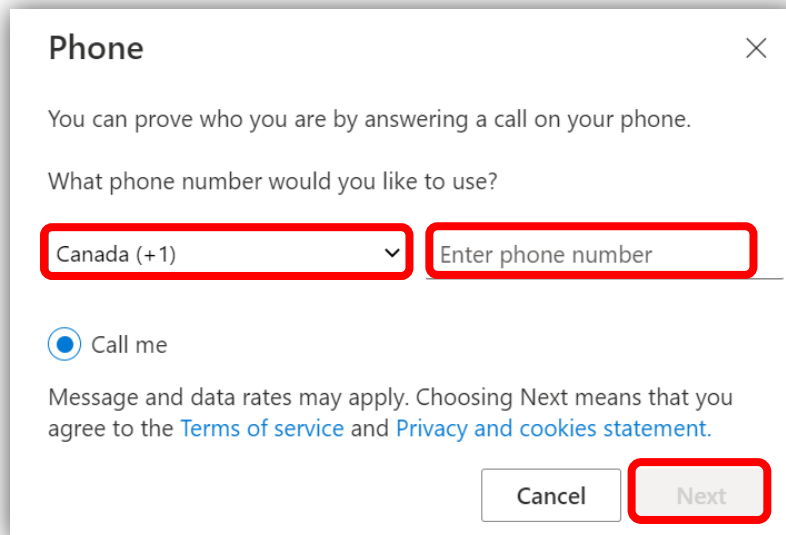
Setting up an Office phone

This method of authentication requires a landline that is not a Lync phone.

19. Click on **+ Add method**, proceed to select **Office Phone** from the dropdown menu. Click **Add** after making your selection.



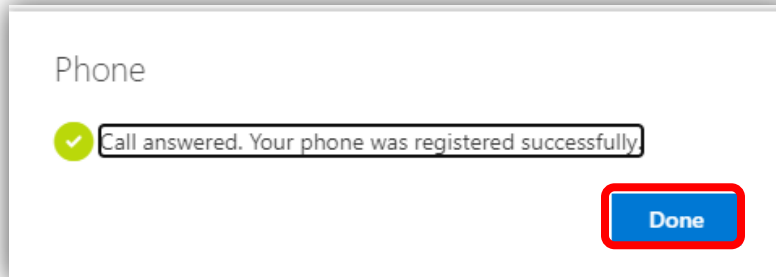
20. Enter the country code and the phone number in the fields and click **Next**.



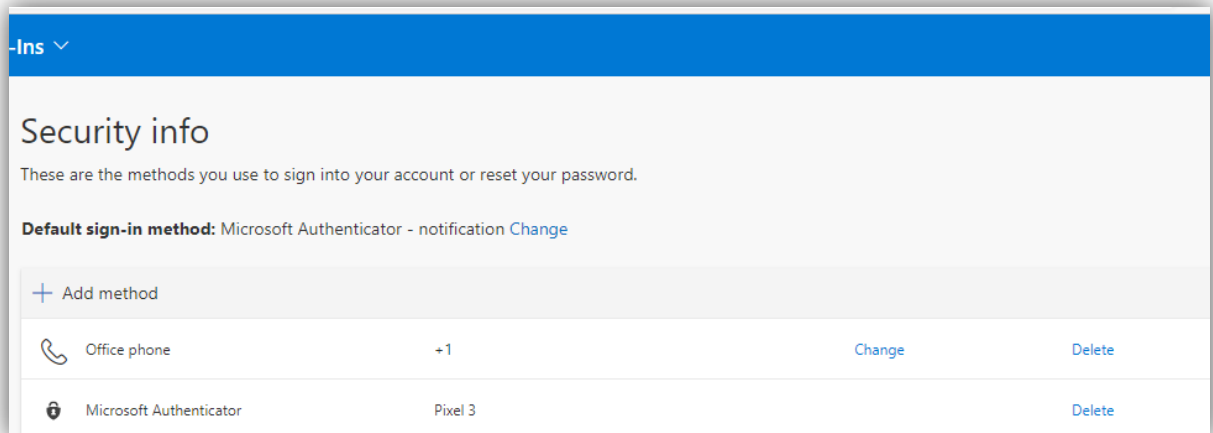
21. The following screen will appear, and you will receive a phone call. Answer the call, and follow the instructions. You will be prompted to Press **Pound (#)** to allow access.



22. Upon completing, you will see the following message. Click **Done** to complete the setup.



23. You will now see the Office phone as an authentication method with the number you set up.



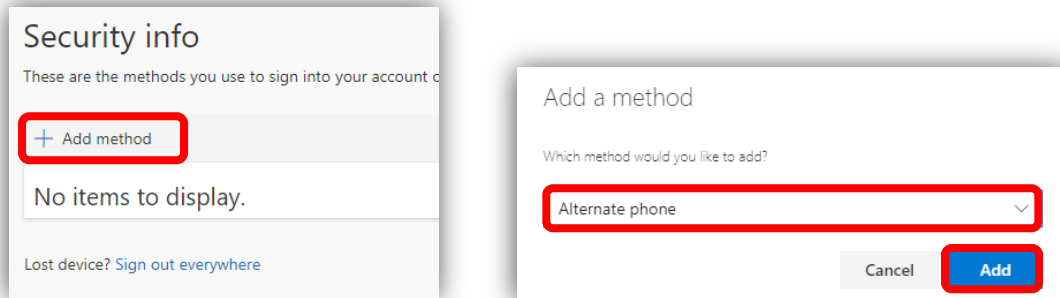
To set up

- a. The Microsoft Authenticator App - go back to [step 3](#)
- b. A Phone to receive a call or text - go back to [step 19](#)
- c. An Alternate Phone to receive a call - continue to [step 24](#)

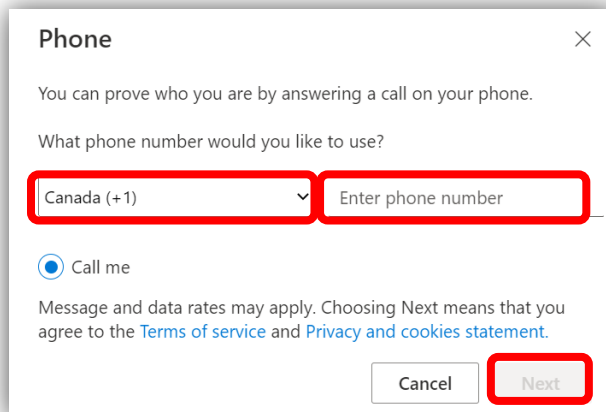
Setting up an Alternate Phone

This method of authentication requires any type of phone that is not a Lync phone.

24. Click on **+ Add method** and select **Alternate Phone** from the dropdown menu. Click **Add** after making your selection.



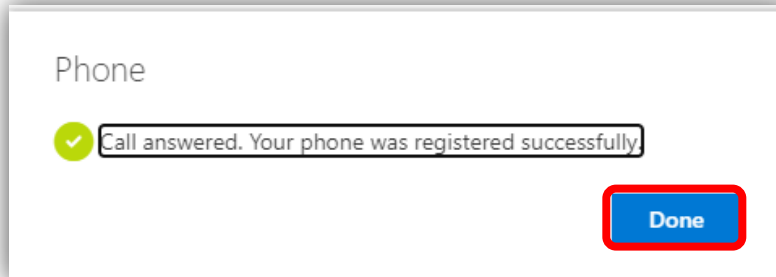
25. Enter the country code and the phone number in the fields and click **Next**.



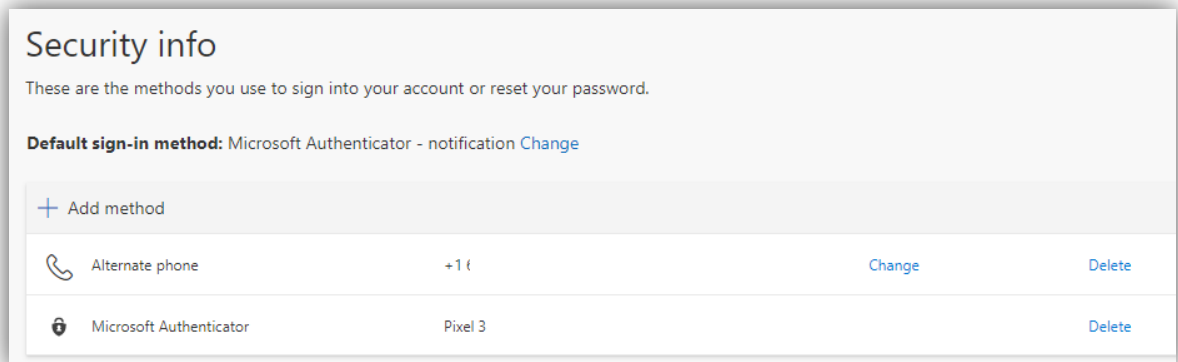
26. The following screen will appear, and you will receive a phone call. Answer the call, and follow the instructions. You will be prompted to Press **Pound (#)**.



27. After you Press Pound # you will see the following message. Click **Done** to complete the setup.



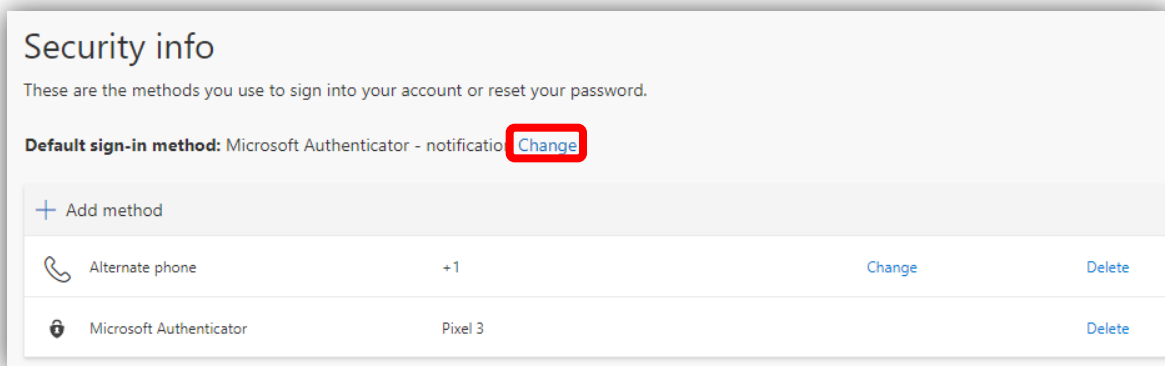
28. You will now see the Alternate phone as an authentication option and the number you set up.



Changing your authentication methods

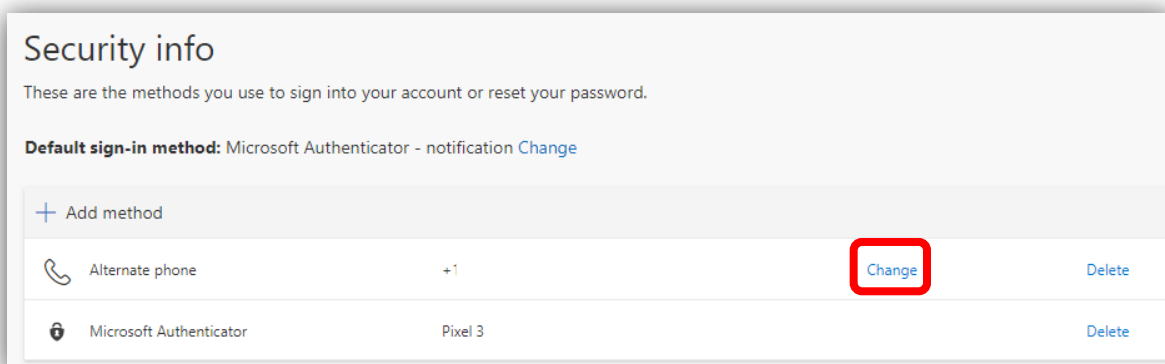
You can change your authentication methods at any time by returning to the <https://mysignins.microsoft.com/security-info> page. If you are not connected to the AHS network, you will need to authenticate using one of your existing authentication methods.

To change your default authentication method, click on **Change** to the right of your existing default method.



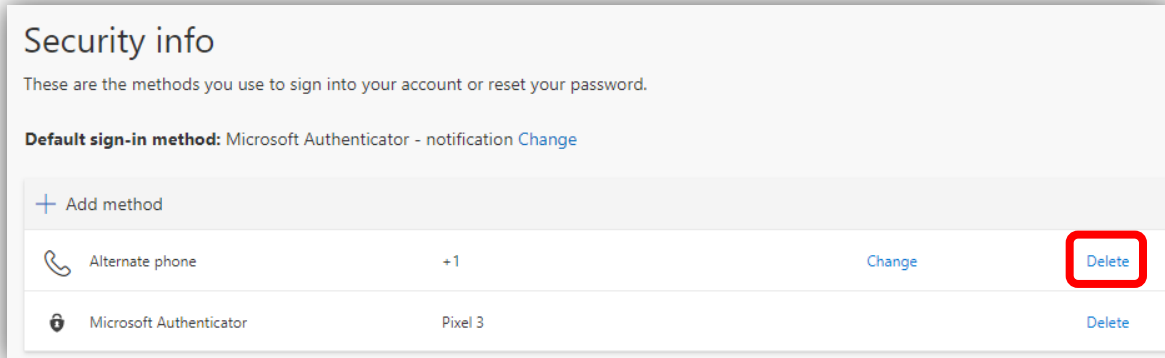
A drop-list will appear with all your available authentication methods, select your preferred default method and click **Confirm**. You will see the default sign in method change to your new preferred method.

To change any phone number, click on **Change** beside the phone number you want to change



Update the country code and phone number to your new number and click **Next**. You will receive either a call or text, depending on the option you are updating to complete the set-up of your new number.

To delete an authentication method, click **Delete** beside the option you want to remove



You will be asked to confirm you would like to delete this method? Click **OK**. After a short pause the method will be deleted from your list.

Note, if you delete your default sign-in method you will need to select a new default sign-in method.