

Multi-Factor Authentication User Guide

June 3, 2025

Contents

What is changing?	2
How Multi-Factor Authentication works:	3
Setting up your Multi-Factor Authentication methods	4
Setting up the Microsoft Authenticator App	5
Setting up a Cellphone.....	10
Setting up an Office phone	14
Setting up an Alternate Phone.....	16
Changing your authentication methods	18
ServiceNow	20
What's Changing?.....	20
What is User Principal Name (UPN)?	20
Logging in on the network.....	20
Logging in off the network	21
ServiceNow Login Process – Off AHS Network.....	21
Unified Access Portal (UAP)	22
What's Changing?.....	22
How to register your account for passwordless sign in with authenticator?	22
Logging into UAP	25
Logging into other applications using passwordless sign in.	26

What is changing?

MFA is a security enhancement that requires users to present two or more methods to verify their identity during log-in using an app on their cellphone, receiving a text message, or by phone call to a cellphone or landline.

With Multi-Factor Authentication (MFA), users logging into a web facing application on a personal or AHS device externally (without a NetMotion connection) will be prompted to authenticate using one of the MFA methods they have set up. This additional step helps secure your information and AHS systems from unwanted access and harmful emails that could be infected with malware.

To improve security, AHS is expanding the use of Multi-Factor Authentication to several web-facing applications and services. The applications in scope of this rollout include:

- Microsoft Outlook – Launched 2022
- Learning Evaluation Support System (LESS) – Launched August 2023
- Project Portfolio Management (PPM) – Launched August 2023
- Insite – Launched Sept. 2023
- SharePoint – Launched Sept. 2023
- My AHS – launched September 2023
- CapitalCare Staffnet – Launched October 2023
- Covenant Learning Connection (CLC) – Launched October 2023
- CompassionNet– Launching October 2023
- ServiceNow Launching March 2024
- Siren
- Ivanti
- Stollery and Peds
- MyLearningLink
- Unified Access Portal (UAP)
- Scheduling system for Cancer Care Centers
- CPAR -Alberta Blue Cross
- Plantir Foundry - COVID Analytics
- AVBS – Salesforce
- Infor - Provincial Staff Scheduling System
- ePHIS - Electronic Public Health Information System
- Privileged Account Management – Safeguard
- Data Document Manager (DDM)

How Multi-Factor Authentication works:

When accessing web facing applications or through a browser, you will be prompted for a second method of authentication. Using ServiceNow as an example:

1. You will enter your AHS username and password in ServiceNow.
2. You will be asked to authenticate using your preferred method.
3. You will allow or deny access to ServiceNow.

There are several methods of authentication you can set up:

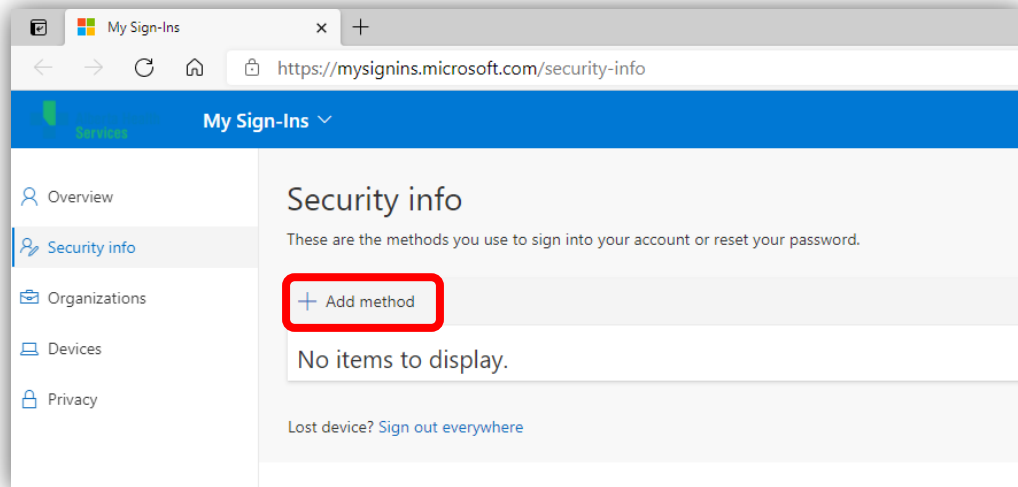
- Using the Microsoft Authenticator app on iOS or Android mobile device
- Receiving a call or text to a cellphone
- Receiving a call to an office phone or landline

You must set up at least two authentication methods. When selecting methods, consider where you will need to use MFA. At home, using a smartphone or tablet while traveling, etc., and choose methods that you will have available at those times and locations.

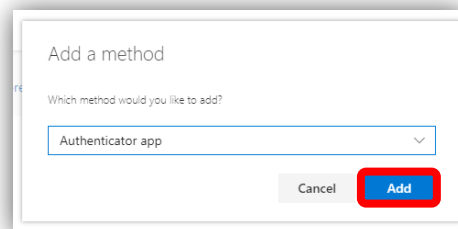
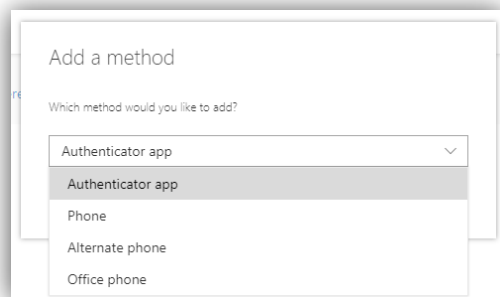
You can add, delete, or update your MFA authentication methods at any time by visiting <https://mysignins.microsoft.com/security-info>.

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.

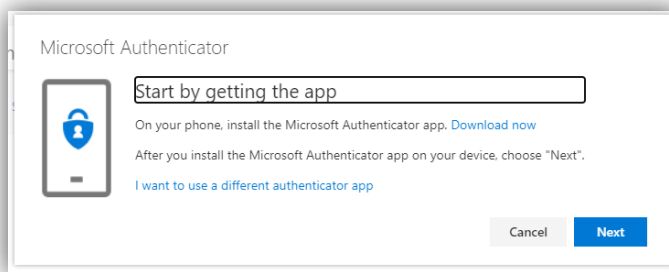


- | | | |
|--------------------------------|---|------------------------------------|
| a. Microsoft Authenticator App | - | continue to step 3 |
| b. Phone (call or a text) | - | go to step 14 |
| c. Office phone | - | go to step 19 |
| d. Alternate phone (call only) | - | go to step 24 |

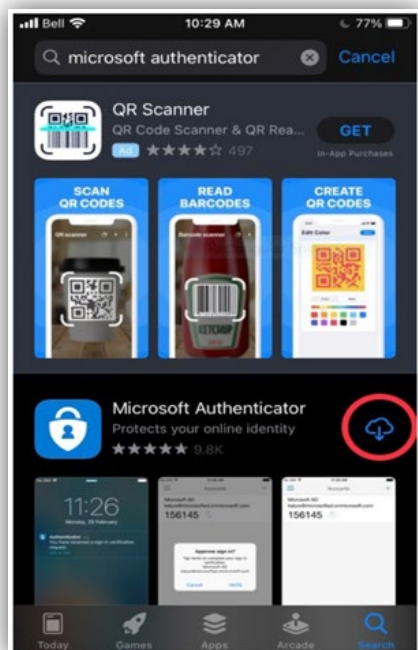
Setting up the Microsoft Authenticator App

This method requires a cellphone or tablet. Once installed the 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 2 devices to work with, the cellphone or tablet you are installing the app on and a computer to follow the set-up steps.

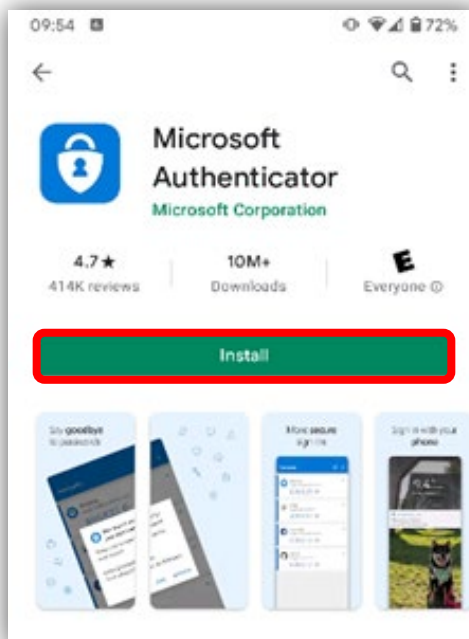
- Download the Microsoft Authenticator App from either the App Store or Google play on your mobile device. **Note:** If you already have the app on your device, go to step 9.



- 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

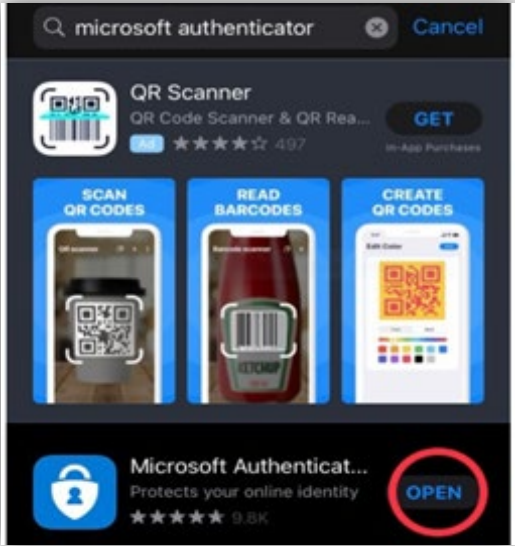


iOS Screen

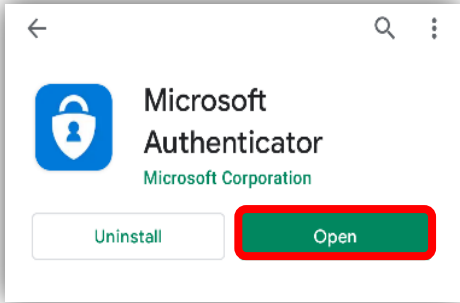


Android Screen

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

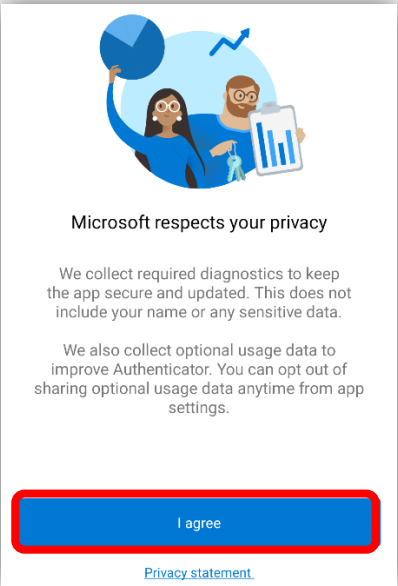


iOS screen

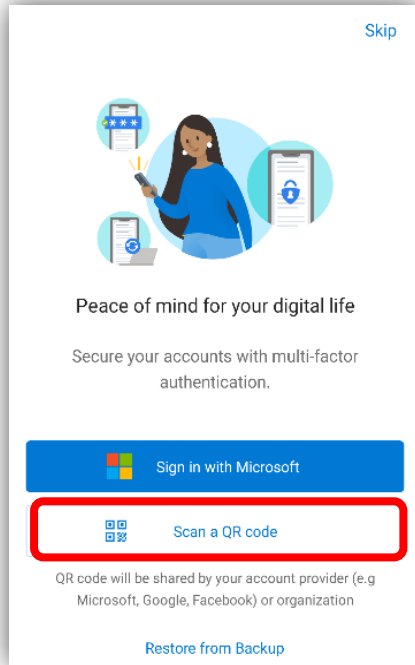


Android screen

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

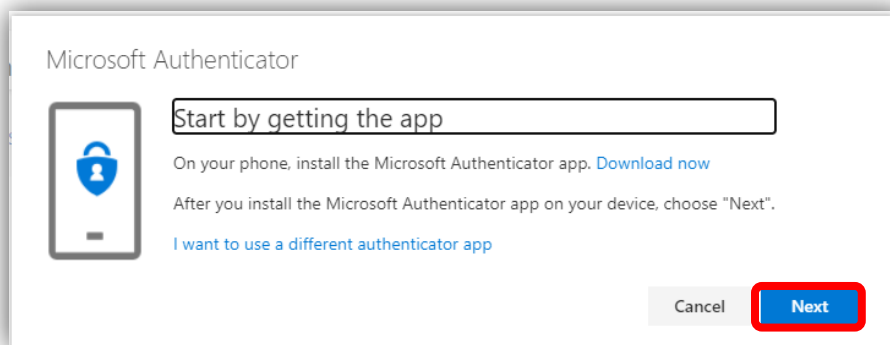


7. The following screen will appear. Tap on **Scan a QR code** button.

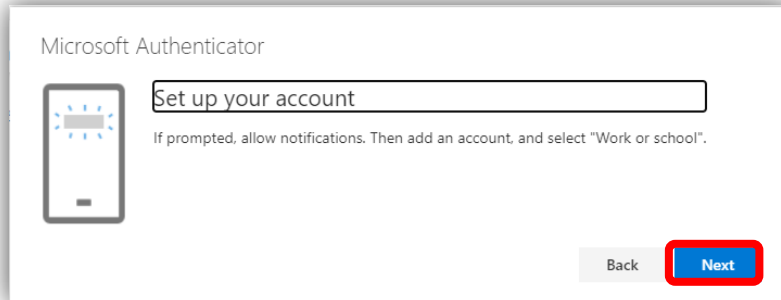


If prompted select the option to set up a work/school account.

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



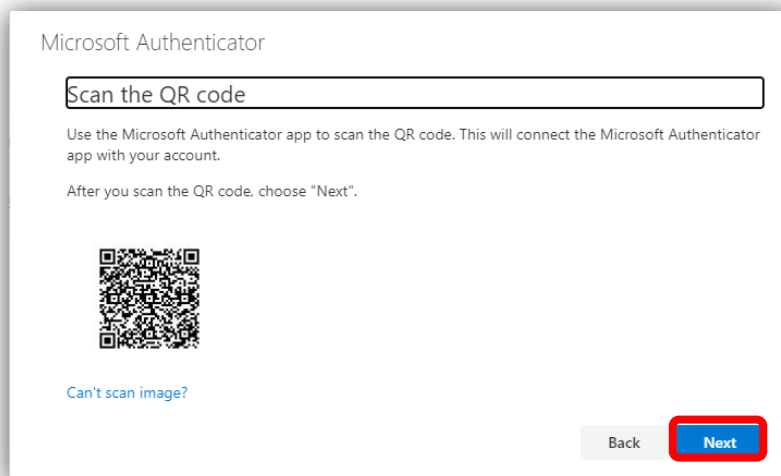
9. When the Set up your account screen appears, click **Next**



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:

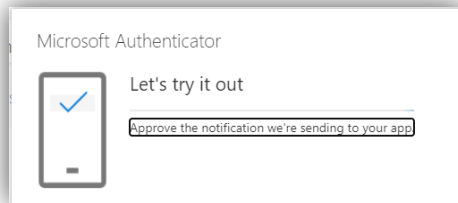
- a. In the App, tap the existing Alberta Health Service account
 - b. Tap gear symbol in the top right corner
 - c. Tap remove account
 - d. Tap to confirm remove account
 - e. Add account
 - a. Work or school account
10. Use the camera that opens within the Microsoft Authenticator App to scan the bar code that appears on your screen.

Note: Do not scan the barcode in the screenshot below, this will not work.

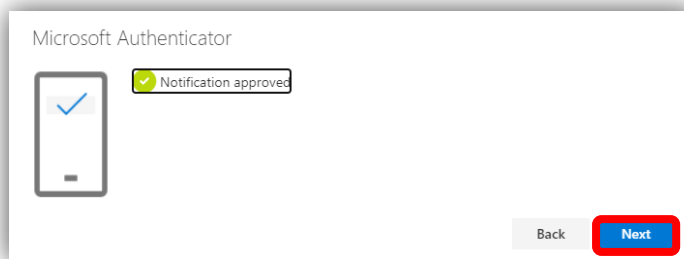


Once the scan is complete a message will appear on your cellphone or tablet that the Alberta Health Services account has been added. Click **Next** on the computer screen.

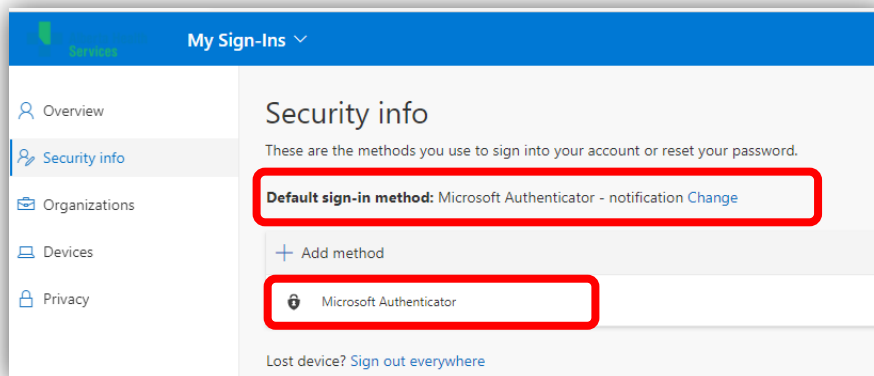
11. When the Let's try it out screen appears you will receive a notification on your cellphone or tablet to Allow or Deny access to your AHS email. Tap **Allow**.



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.

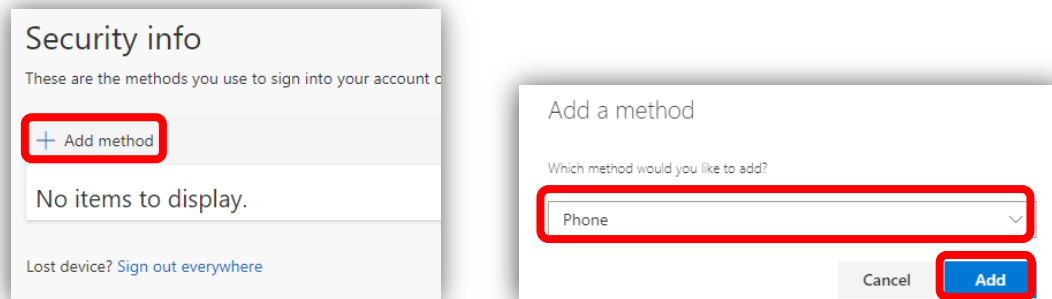


We recommended that you add a second method for authenticating just in case you do not have access to the cellphone or tablet the authenticator app is installed on.

- 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](#)

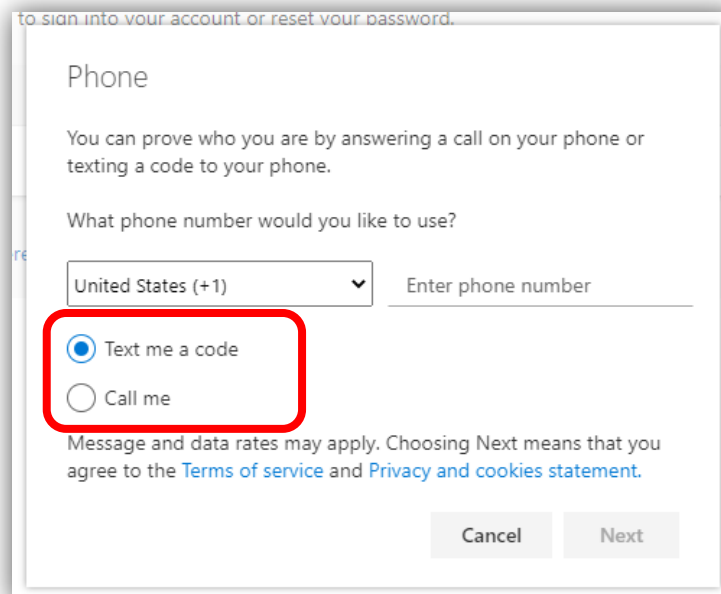
Setting up a Cellphone

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**.

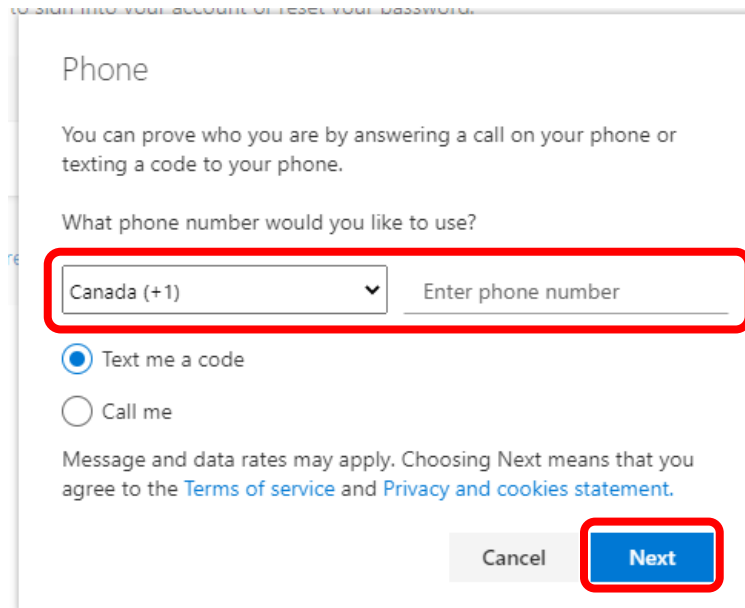


15. The following screen will appear, note there are two possible ways to authenticate with your cellular phone:
- **Text me a code:** You will receive a numerical code via SMS that you will be prompted to enter when authenticating your login.
 - **Call me:** When attempting to login, you will receive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



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

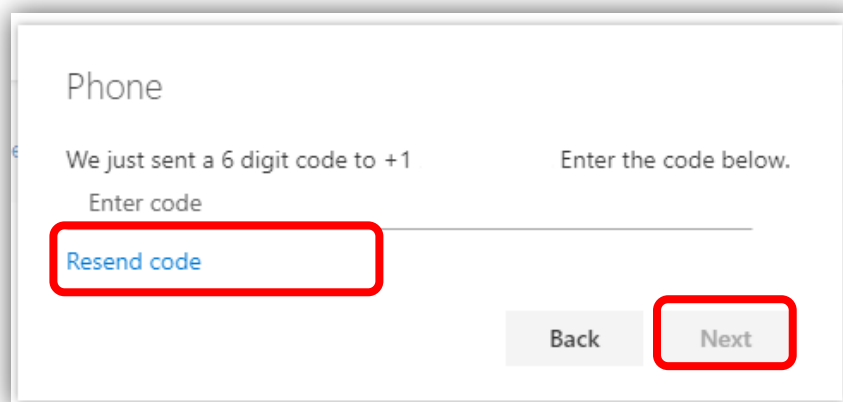
Call me

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**.



Phone

We just sent a 6 digit code to +1 Enter the code below.

Enter code

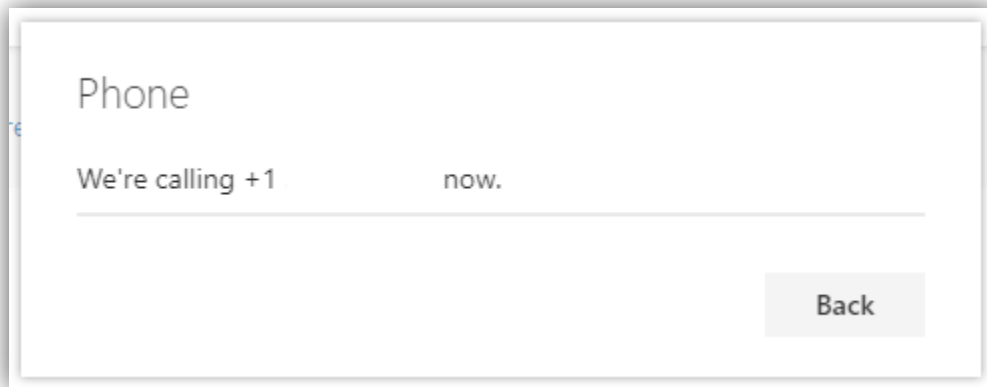
Resend code

Back Next

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

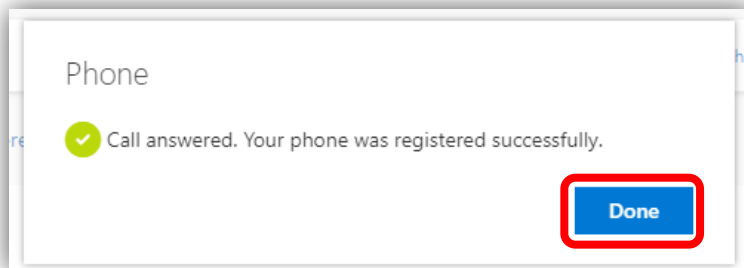
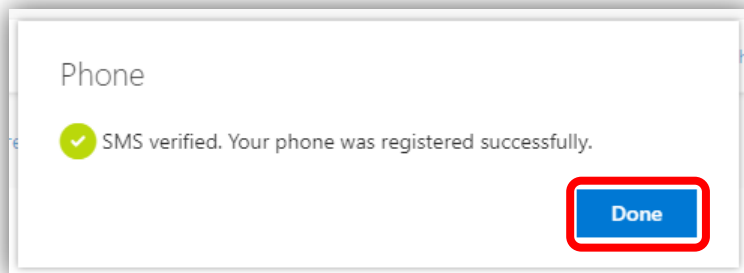
b. If you selected **Call my phone**:

The following screen will appear, and you will receive a phone call.



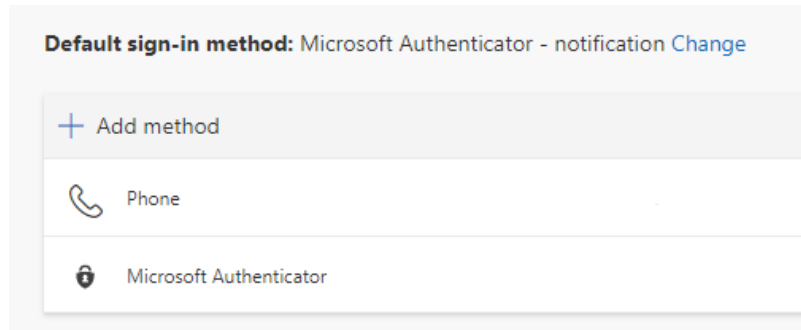
Answer the call, and follow the instructions relayed by the automated message. You will be prompted to dial the **Pound (#)** to allow access.

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.



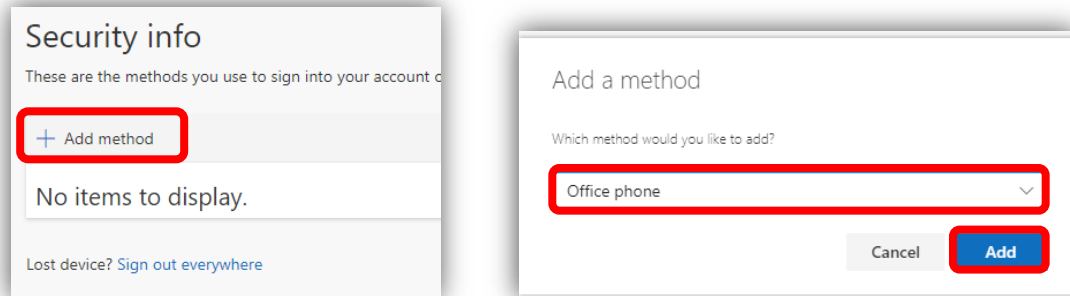
To set up

- 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.



Security info

These are the methods you use to sign into your account

+ Add method

No items to display.

Lost device? [Sign out everywhere](#)

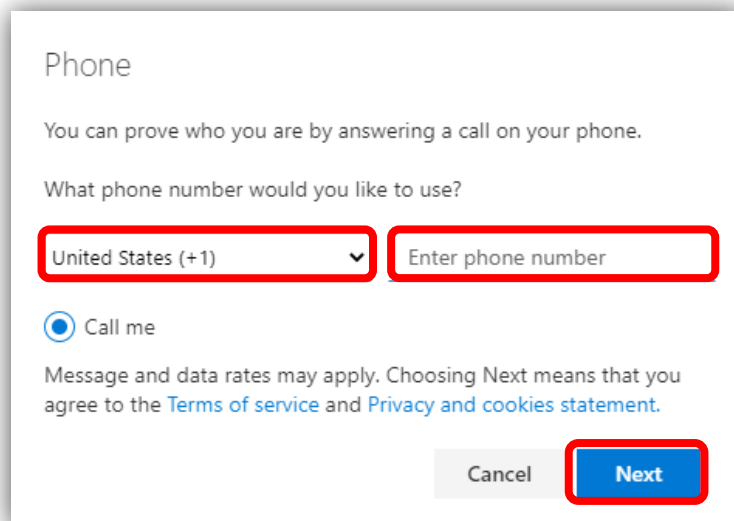
Add a method

Which method would you like to add?

Office phone

Cancel Add

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



Phone

You can prove who you are by answering a call on your phone.

What phone number would you like to use?

United States (+1) Enter phone number

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

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 dial the **Pound (#)** to allow access.

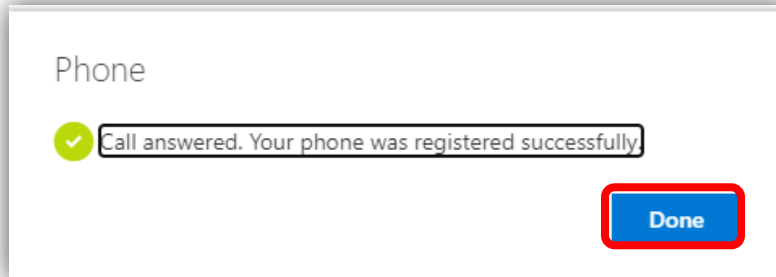


Phone

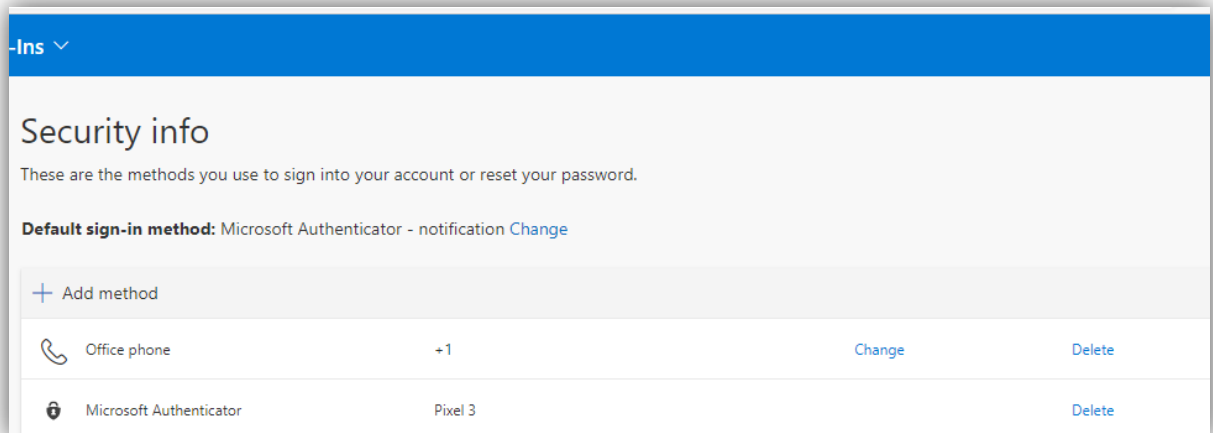
We're calling +1 now.

Back

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.



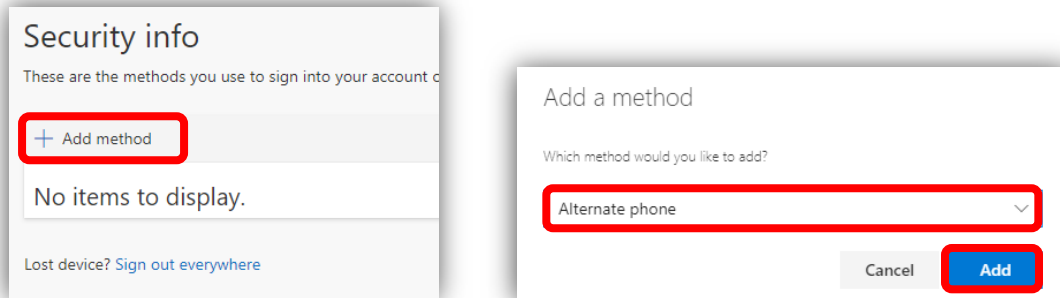
To set up

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

Setting up an Alternate Phone

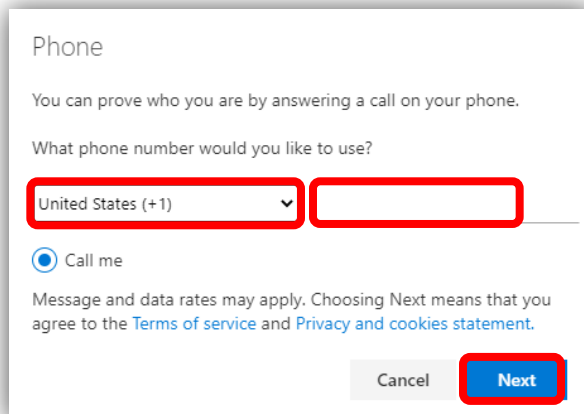
This method of authentication requires any type of phone that is not a Lync phone.

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



The first screenshot shows the 'Security info' page with the text 'These are the methods you use to sign into your account'. A red box highlights the '+ Add method' button. Below it, it says 'No items to display.' and 'Lost device? [Sign out everywhere](#)'. The second screenshot shows the 'Add a method' page with the text 'Which method would you like to add?'. A red box highlights the 'Alternate phone' dropdown menu. At the bottom right, there are 'Cancel' and 'Add' buttons, with the 'Add' button highlighted by a red box.

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



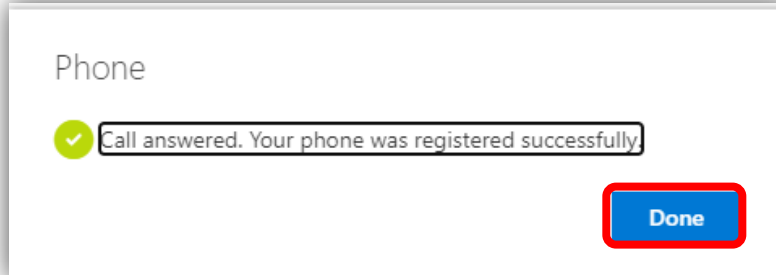
The screenshot shows the 'Phone' setup screen. It has the text 'You can prove who you are by answering a call on your phone.' and 'What phone number would you like to use?'. There is a dropdown menu showing 'United States (+1)' and an empty text input field, both highlighted with red boxes. Below these is a radio button labeled 'Call me' which is selected. At the bottom, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

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 dial the **Pound (#)**.

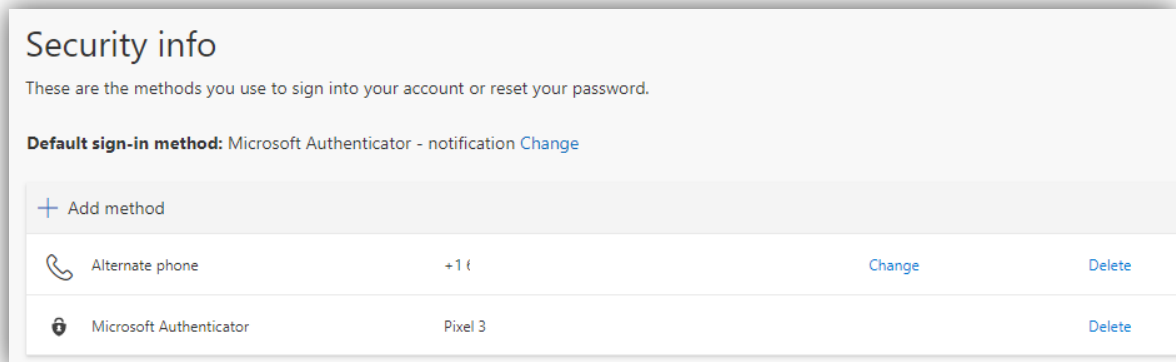


The screenshot shows the 'Phone' screen during a verification call. It has a text field containing 'We're calling +1' and 'now.'. At the bottom right, there is a 'Back' button highlighted with a red box.

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



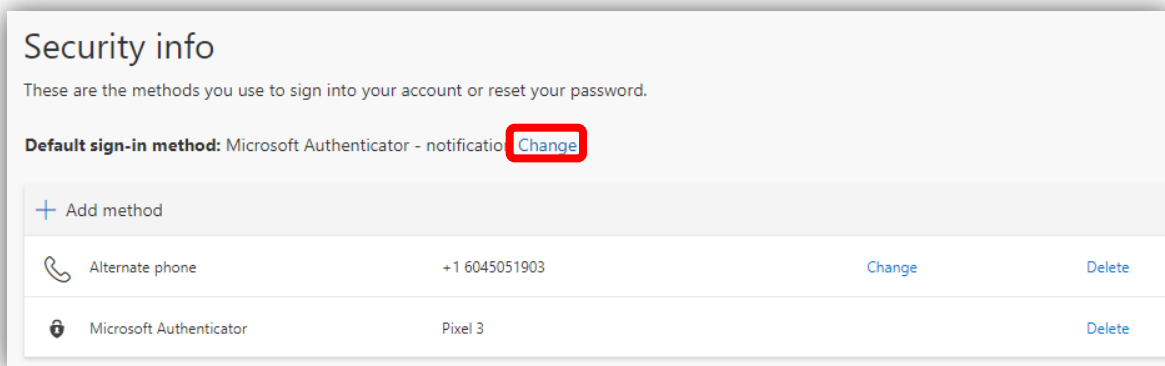
28. You will now see the Alternate phone as an authentication option and the number you set up.



Changing your authentication methods

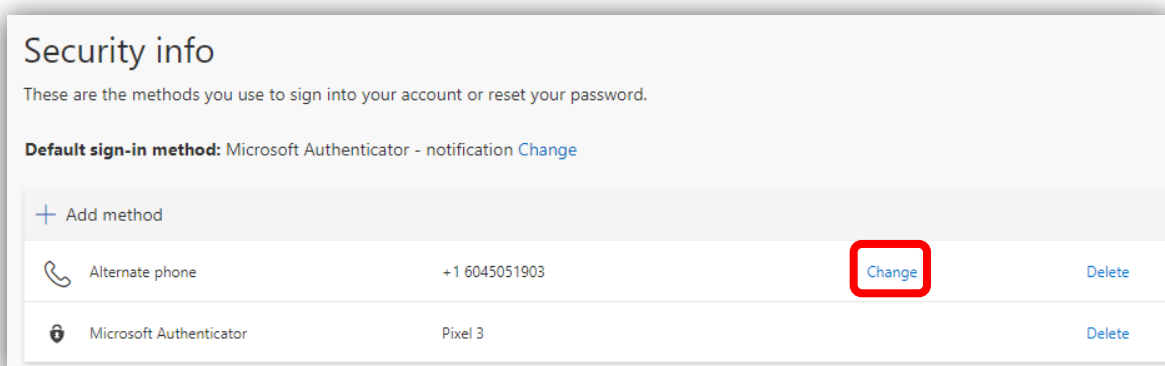
You can change your authentication methods at any time by returning to the <https://mysignins.microsoft.com/security-info> page. If you are not connected to the AHS network, you will need to authenticate using one of your existing authentication methods.

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



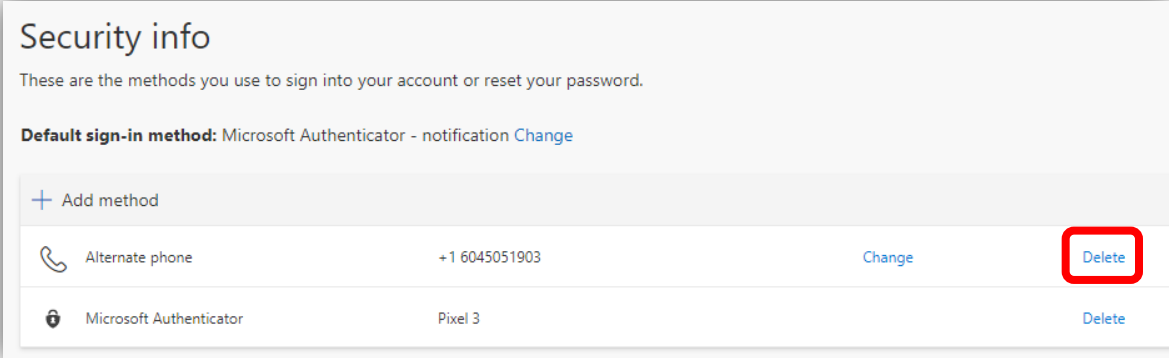
A drop-list will appear with all your available authentication methods, select your preferred default method, and click **Confirm**. You will see the default sign in method change to your new preferred method.

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 setup 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.

ServiceNow

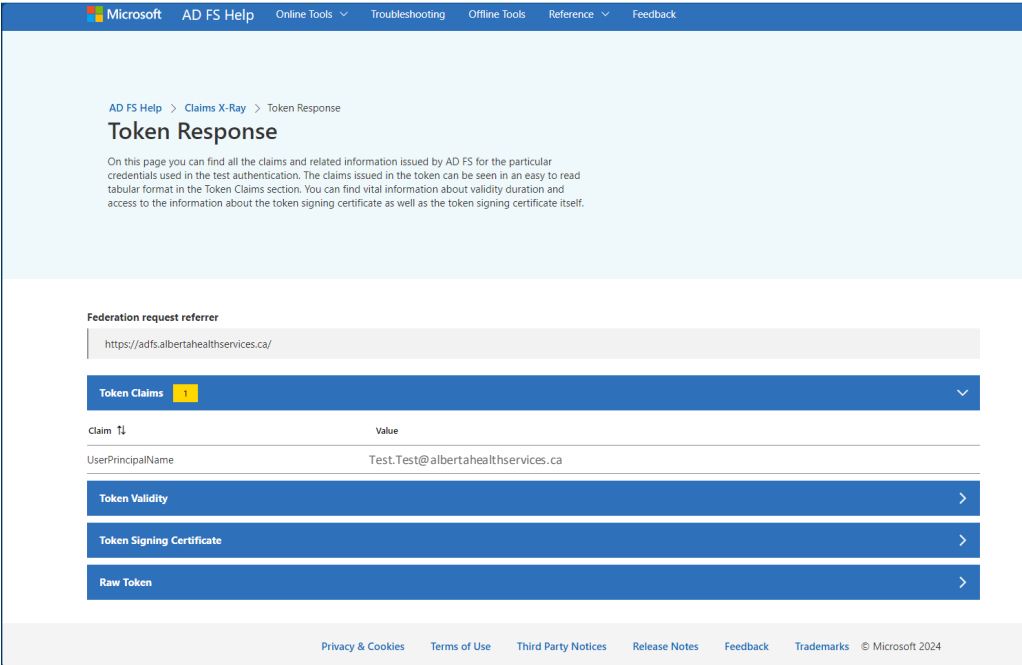
What's Changing?

ServiceNow will migrate to MS Entra (formerly Microsoft Azure) Authentication platform as our Identify Provider and will be enabled for Multi-Factor Authentication (MFA). Your login page and your login experience will change.

After the change you can no longer use your username to login to ServiceNow, MS Entra uses a User Principal Name (UPN) instead of username credentials.

What is User Principal Name (UPN)?

The User Principal Name (UPN) is like a SIN number in AHS active directory. Microsoft Entra and cloud applications require UPNs across organizations to authenticate users. For most users, the UPN is their full AHS email (firstname.lastname@albertahealthservices.ca). When logging into Microsoft Office 365 applications like Outlook and Teams the UPN is required, and you may have already been logging in using these credentials. You can find your UPN at <https://upnlookup.albertahealthservices.ca>.



The screenshot shows the Microsoft AD FS Help page for 'Token Response'. The breadcrumb trail is 'AD FS Help > Claims X-Ray > Token Response'. The page title is 'Token Response'. Below the title is a paragraph explaining that the page provides claims and related information issued by AD FS for specific credentials. The main content area includes a 'Federation request referrer' field with the value 'https://adfs.albertahealthservices.ca/'. Below this is a 'Token Claims' section with a dropdown arrow. A table displays the claims:

Claim	Value
UserPrincipalName	Test.Test@albertahealthservices.ca

Below the table are several expandable sections: 'Token Validity', 'Token Signing Certificate', and 'Raw Token', each with a right-pointing arrow. The footer contains links for 'Privacy & Cookies', 'Terms of Use', 'Third Party Notices', 'Release Notes', 'Feedback', and 'Trademarks', along with the copyright notice '© Microsoft 2024'.

Logging in on the network

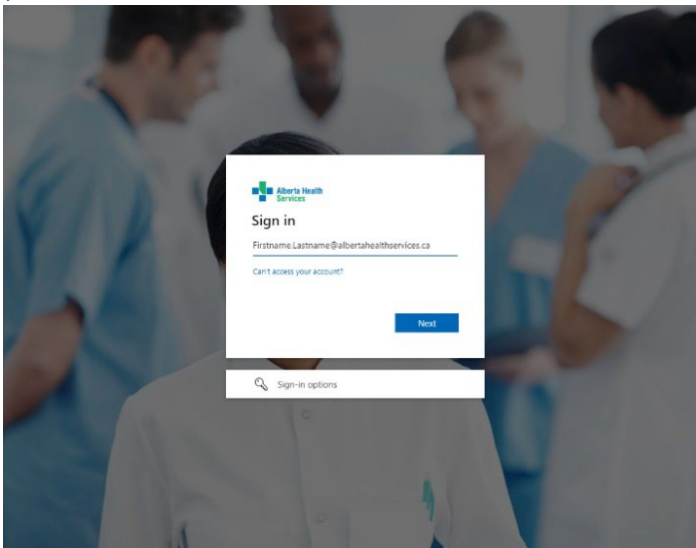
Users authenticated on an AHS device with a NetMotion connection will not be prompted for MFA. Additionally, you will not have to authenticate again to use ServiceNow as your credentials are now being passed.

Logging in off the network

Users logging in to ServiceNow on a personal device or an AHS device without a Net Motion connection will be prompted to authenticate using one of the MFA methods they have set up. Note: If you complete MFA for another AHS application (e.g., Insite) you will not be prompted to do MFA again.

ServiceNow Login Process – Off AHS Network

1. When you first attempt to login to ServiceNow (or other AHS application), you will be challenged for MFA. If you don't know your UPN, go to <https://upnlookup.albertahealthservices.ca> and put your UPN in the username field.



2. Verify your identity using the MFA options you setup.



3. You will be granted access to ServiceNow.


Unified Access Portal (UAP)

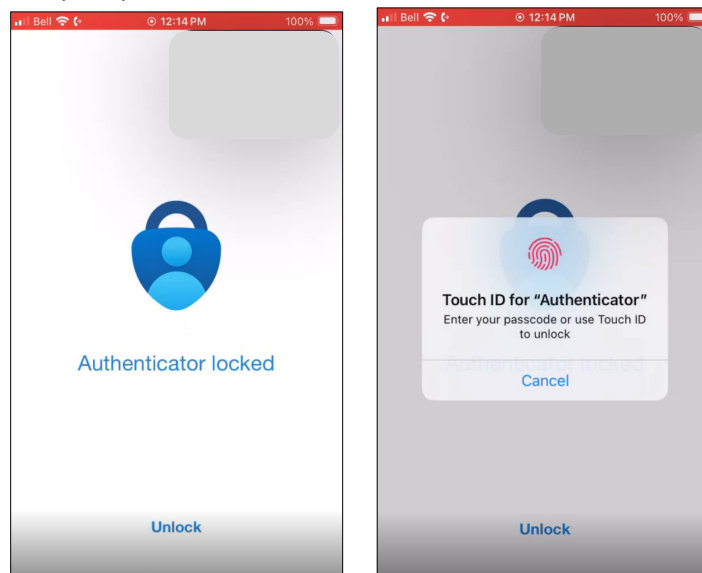
What's Changing?

To enhance security and reduce phishing attacks, the Unified Access Portal (UAP) will migrate to the Microsoft Azure Authentication platform as our identity provider and will be enabled for Multi-Factor Authentication (MFA). As a result, your login experience will change.

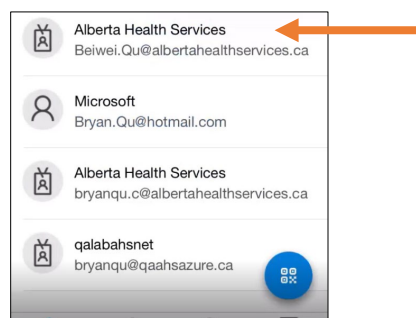
When logging into UAP **off the AHS network**, you will be prompted for MFA. You will need to setup the Microsoft Authenticator app on your phone as your primary authentication method in MS Azure instead of receiving a text or phone call to authenticate on your device. After setting up the app as your authentication method, you will not have to enter your password, which will allow you to login faster.

How to register your account for passwordless sign in with authenticator?

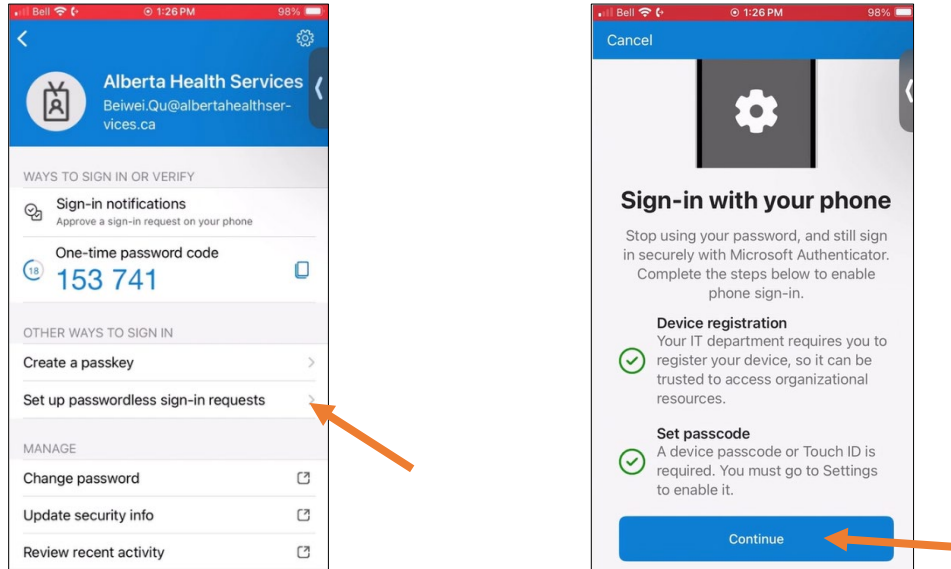
1. Open the Microsoft Authenticator app.
 - a) Click unlock.
 - b) Use your passcode or biometrics to authenticate.



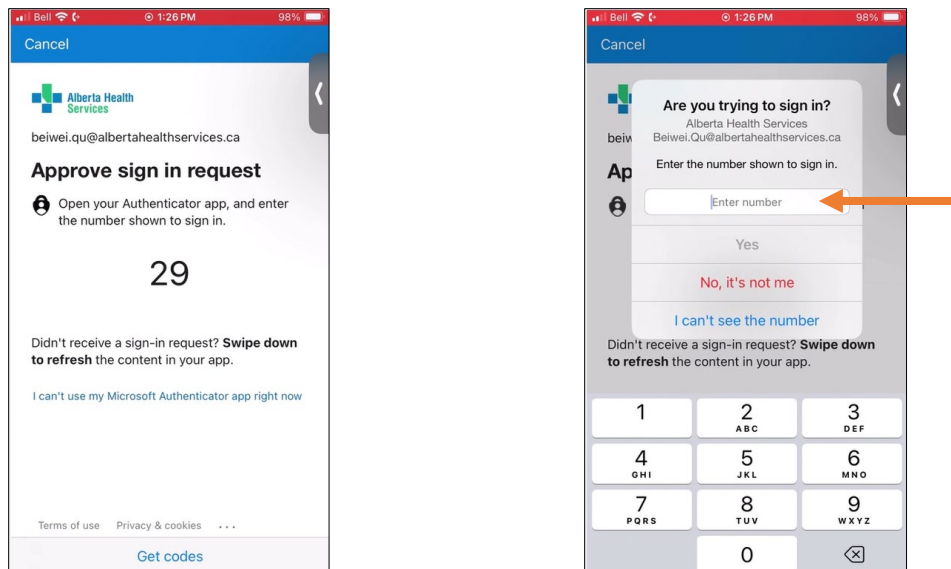
2. Select your Albert Health Services account.



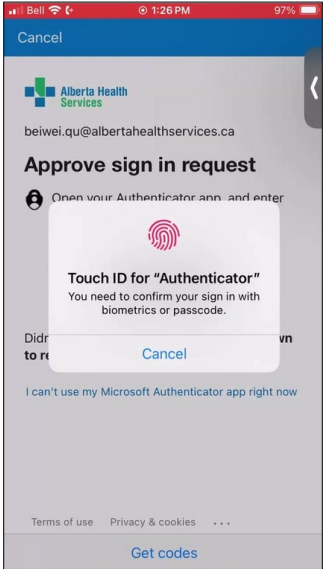
3. Click “Set up passwordless sign-in requests. Then click “Continue.”



4. You will see a two-digit number appear on your phone. Enter the number in your Authenticator App.



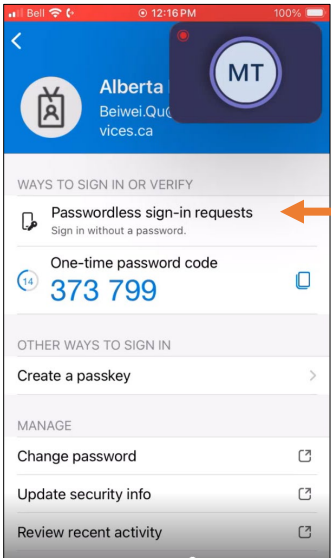
5. If prompted, authenticate using your biometrics or passcode.



6. Your passwordless sign-in will be activated.

Note: Only applications where passwordless authentication is permitted will allow you to use this feature. If you try to use this feature on an application where it is not permitted, you will get an error message. If the last application you used required a password, the next time you try to authenticate, you will have to click use an app instead to use the passwordless option.

7. You can now see passwordless sign-in requests enabled in the Authenticator app.



Logging into UAP

1. Go to the MyApps (Citrix Applications).

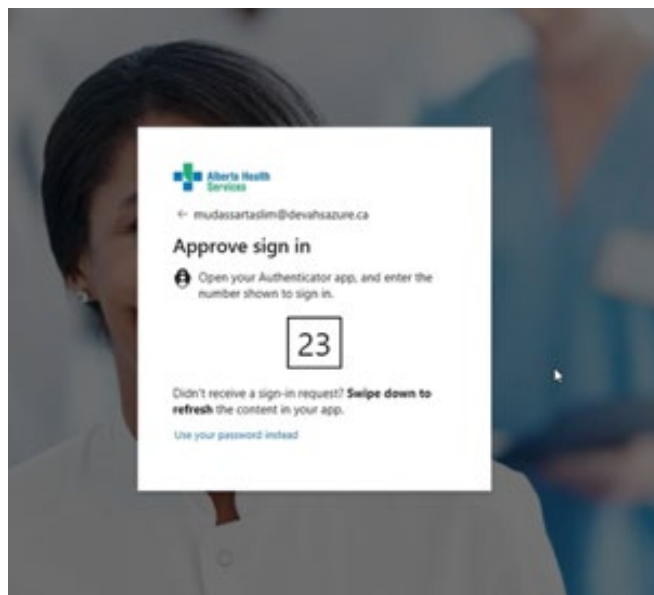
Internal Staff Tools

AHS staff, physicians, volunteers and approved partners can access the secure tools below **while outside the AHS network. Unauthorized access is strictly prohibited.**

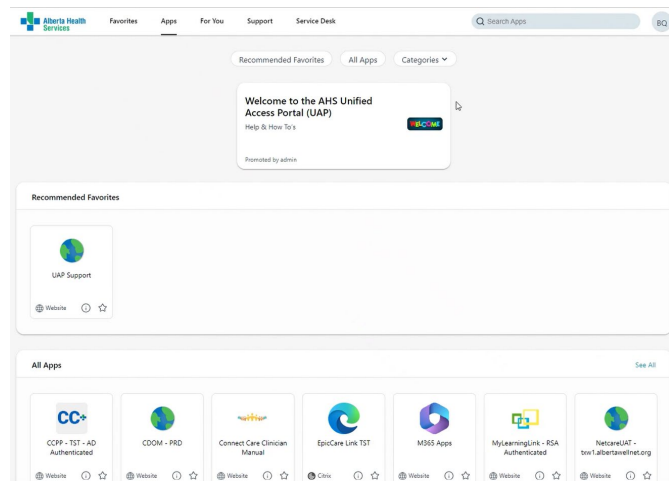
- [Forget Your Password?](#)
- [Insite](#) (AHS Intranet)
- [MyApps](#) (Citrix Applications) ←
- [Remote Access With RSA Tokens](#)
- [MyLearningLink](#) | [Resources](#)
- [MySafetyNet](#) (Report Worker Incidents)
- [Staff Directory](#)

2. Now when you sign in you will be prompted for MFA (the two-digit code). Enter the two-digit code in the Microsoft Authenticator app. **Note:** The system will remember the last sign-in option you used and will use it going forward, so you will be prompted with the passwordless login the next time you sign in.

If you are unable to use Microsoft Authenticator and you need to use the password, click “Use your password instead.”



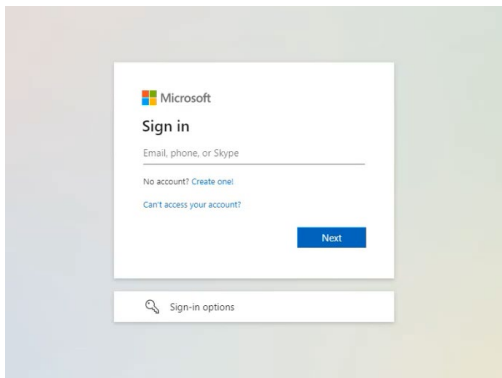
3. Once you enter the numbers in the app, you will be granted access to UAP.



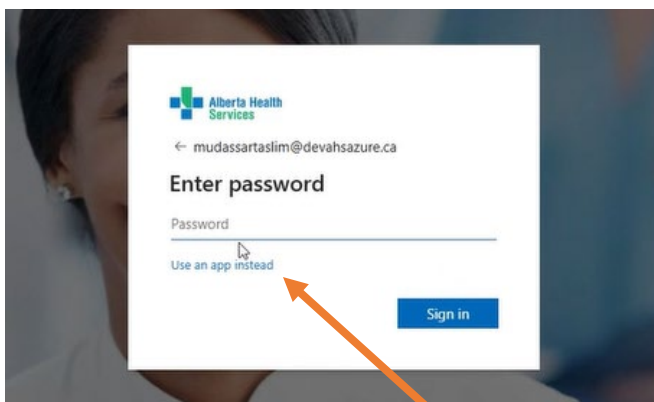
Logging into other applications using passwordless sign in.

When you log into other applications (e.g., Microsoft Outlook) off the network, you will be able to use the passwordless s. You will see the “Use an app instead” under the password field.

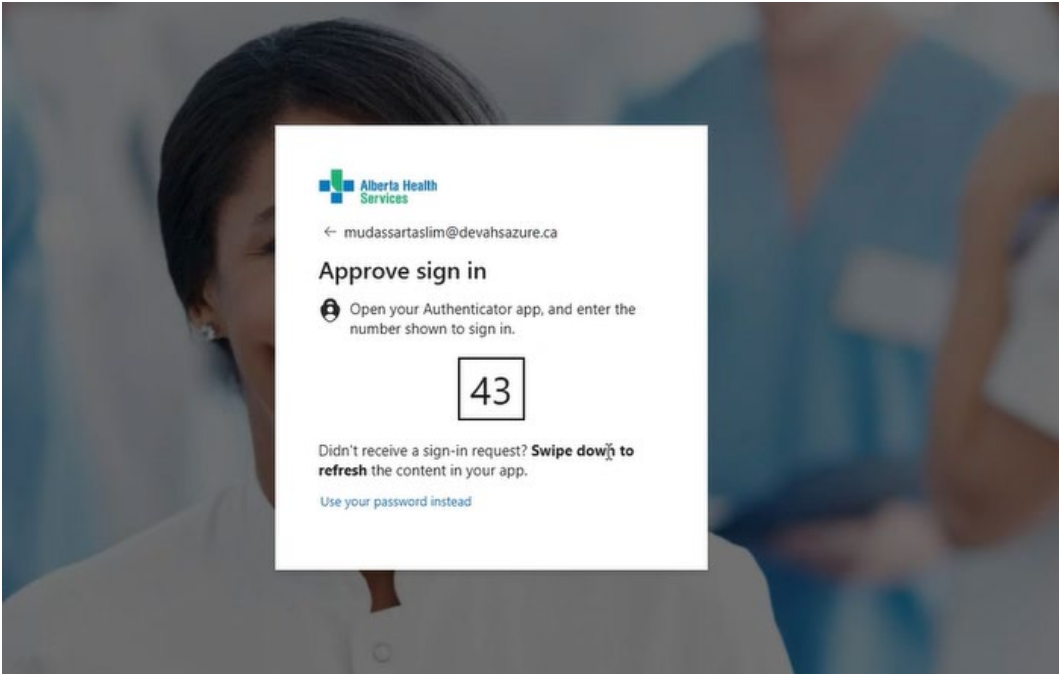
1. Go to Microsoft Outlook and enter your AHS username.



2. Under the password field, click “Use an app instead.”



The Approve sign in dialogue box will open.



- 4. Enter the number in your Microsoft Authenticator app to approve the sign in. The sign in will be approved and the application will open when you go to it.

