



Microsoft Azure AD  
Self-Service Password Reset  
**SSPR - Enrolment**  
User Guide

# Enrolment & Managing Authentication (SSPR)

Microsoft Azure AD .....	1
Introduction.....	3
1. Objective .....	3
Accessing Security Information .....	3
1. Access Security Info Web Portal .....	3
Setting Up Authentication Methods.....	5
1. Microsoft Authenticator App Registration.....	5
2. Mobile/Alternate/Office Phone Configuration.....	7
3. Set Up Security Questions .....	8
Managing Authentication Methods.....	9
1. Change Authentication Method .....	9
2. Add an Additional Authentication Method.....	10
3. Delete Existing Authentication Method .....	10
Error Messages.....	11
Login Issues.....	11
Temporarily Blocked.....	11
Acronym List.....	12
Review History .....	12
Version History.....	12
Contact eHS Service Desk.....	12

## 1. Objective

The objective of the **Self-Service Password Reset (SSPR)** is to empower individuals to reset their own password without the need to contact the Service Desk for assistance.



**IMPORTANT:** This process is only used when your password has been forgotten. If you know your password, use the standard process to update an expiring password – starting with CTRL-ALT-DEL

This **Self-Service Password Reset (SSPR) User Guide** contains the steps to enrol as well as background information to better understand the SSPR enrolment process within the Saskatchewan health system. Enrolment instructions can be located at <https://www.ehealthsask.ca/WIKI/Pages/default.aspx>

**To reset or unlock your password using SSPR, see Password Management / Unlock Network Account User Guide.**

## Accessing Security Information

### If you use VDI / VMware Horizon:



**Not all functionality is available using VDI (Virtual Desktop)**, however, those using VDI are encouraged to enrol and set up authentication method(s) for future initiatives.

#### **You ARE able to do the following:**

- **Enrol and add authentication method(s)** for future use (*i.e. external access similar to Mobile Duo*)
- Use the SSPR Portal to proactively **reset password**
- Use the SSPR Portal to **unlock your account** provided you have not forgotten the password as;

#### **You Are NOT able to:**

- Use the **Windows Desktop "Reset Password" option.**

### If you use myeHealth to access the following applications:



If you have a **myeHealth** account, continue resetting your password through the myeHealth portal site: <https://services.ehealthsask.ca/myehealth/> for these applications in addition to using this **Self-Service Password Reset** functionality for your network account.

## 1. Access Security Info Web Portal

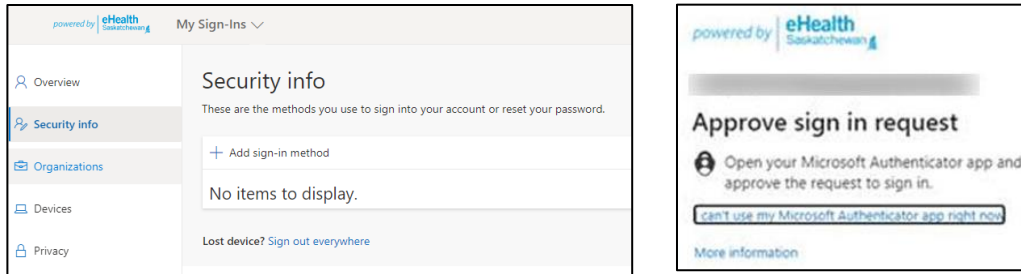


**NOTE:** The recommended browser is **Microsoft Edge** on a company managed device. When using Edge you will not be prompted to authenticate.



**IMPORTANT:** If you change mobile devices you must re-register for SSPR.

- a. To begin the enrolment process, proceed to: <https://aka.ms/mysecurityinfo> and your web browser should open and present you with the following Security info page:

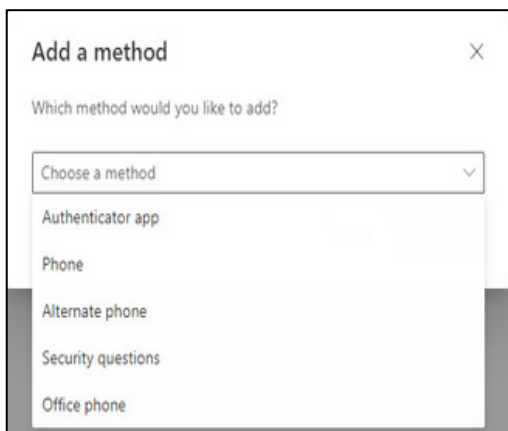


**NOTE:** You may be presented an authentication request prompt if you already have a method configured for authentication.

- b. Click + Add sign-in method link.



- c. From the Add a method popup, choose your preferred method and follow the instructions in the appropriate section below.



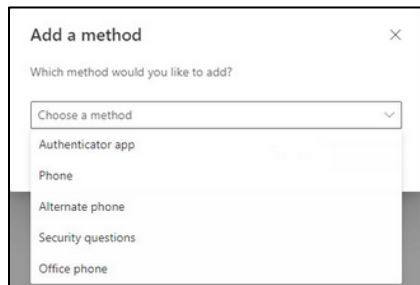
## Setting Up Authentication Methods

**NOTE:** It is recommended that at least 2 methods be registered in the instance where a mobile device gets lost or broken.

### 1. Microsoft Authenticator App Registration

#### Recommended and most secure method

**NOTE:** If you are already registered with MS Authenticator with your account do not delete the account entry from your phone.



**IMPORTANT:** If you change mobile devices you must re-register.

- a. **Download** and **install** the Microsoft Authenticator app on your **mobile** device before proceeding. The Microsoft Authenticator app is available for the following devices:

- *iOS* (Requires iOS 11.0 or later)
- *Android* (Version 6.0 and up)



Screenshots may not appear exactly as shown. Your make & model of mobile device may have slightly different screens. (*i.e. Android vs iPhone*). For more information refer to:

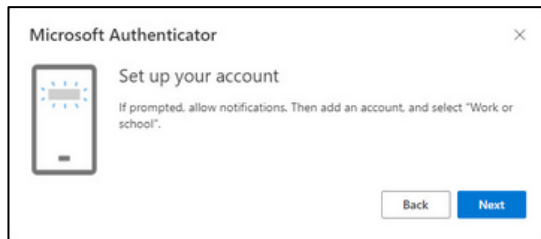
- <https://www.microsoft.com/en-us/security/mobile-authenticator-app>
- <https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app>



**NOTE:** Microsoft 365 services require modern versions of mobile operating systems.

- b. Once the Microsoft Authenticator app is downloaded and installed, using your desktop/web browser, continue to the registration process by clicking **Next**.

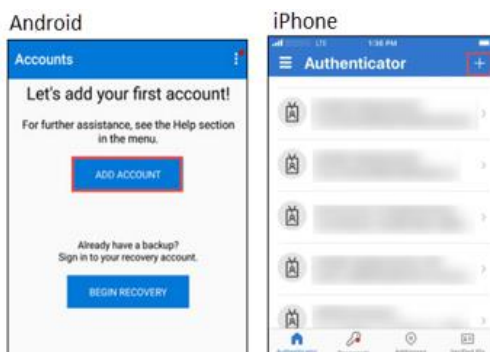
- c. When prompted with **Set up your account** window, click **Next**.



- d. Leave this QR code for now as you will scan it with your mobile phone below.

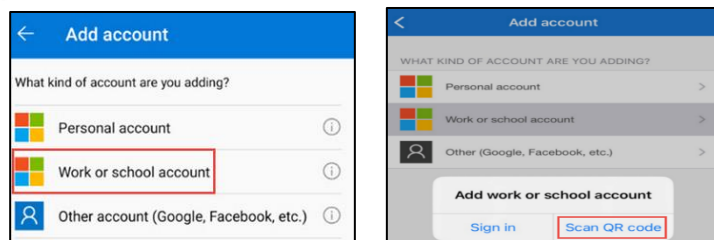


- e. On your mobile phone open the **Microsoft Authenticator app** and select **Add Account**.



**NOTE:** If this is not the first time using the Authenticator app, you may click on the **three dots** or **+** **symbol** on the top right corner, and then select **Add Account**.

- f. Select **Work or school account**.



- g. On your mobile phone, you may receive a permission request from the Authenticator app to use the camera, click **Allow**. Use your mobile camera to scan the QR code.

- h. Scan the QR code shown on the desktop/web browser

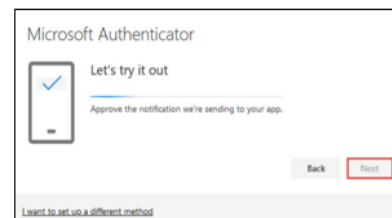
**NOTE:** The mobile phone will open the camera app to scan the QR code. Scan the QR code on the desktop/web browser using camera app.  
If necessary click on the **Can't scan image** button to manually enter code into your mobile app.



- i. Select **Let's try it out**, and **Approve** the sign-in request that you have received on your mobile phone.

You should receive a prompt on your mobile phone.

**NOTE:** In your web browser, a **Notification approved** message will appear. Click **Next**.



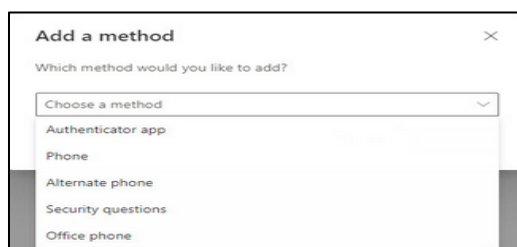
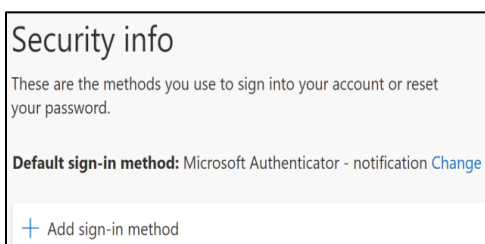
The Microsoft Authenticator enrolment process has now been successfully completed.

## 2. Mobile/Alternate/Office Phone Configuration

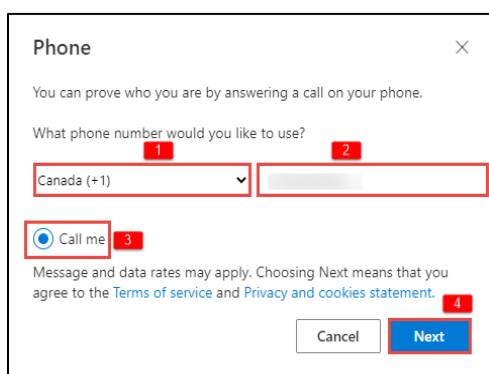
**NOTE:** An automated voice call is made to the phone number you provide. Answer the call and press # in the phone keypad to authenticate.  
(MS does not support phones lines that have extensions).



- a. To Add a phone authentication method, click the **+ Add sign-in method**, Select **Phone**, and click **Add**.



- b. Select the **correct country** and **enter your phone number**, including area code, and choose **Call Me** to verify the sign-in. Click **Next**.



### IMPORTANT:

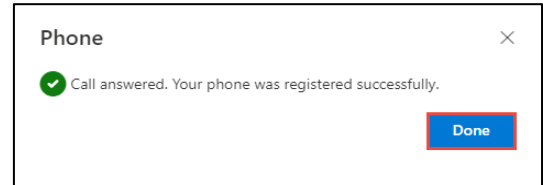
- Phones that use **extensions** are NOT supported. Ensure to use a direct line.  
(i.e. 306xxxxxxx)
- Phones set up in a **hunt group** are NOT supported.  
(i.e. multiple phones ring from the same number at the same time)

- c. The Microsoft Authentication System will phone the number you entered.

You must answer the phone and press the # key to successfully authenticate.



- d. A **Success message** will be displayed on your desktop. Click **Next** and **Done**.

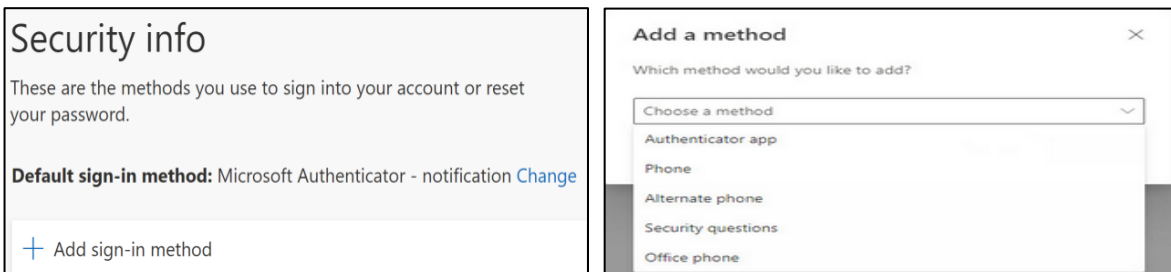


The Mobile Phone enrolment process has been successfully completed.

### 3. Set Up Security Questions

**Caution:** While using Security questions for an SSPR authentication method is available, this method will not be used for external connectivity (remote access) in the future, (e.g. multi factor authentication or MFA).

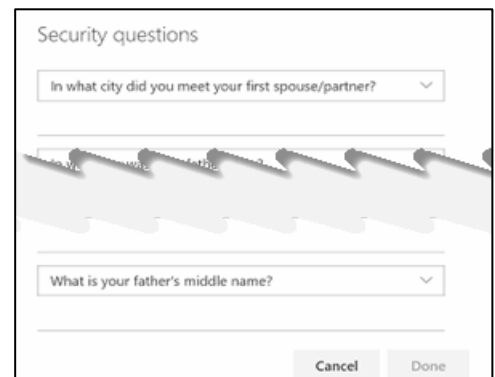
- a. To configure security questions, click on the option **Add sign-in method**. Under **Which method would you like to add?**, click the drop down arrow and select **Security questions**. Click **Add**.



- b. You will be required to select **5 predetermined security questions**. From the drop-down menu, select questions from the predefined list.

**NOTE:** For security purposes, do not use questions and answers that are easily guessed or used in other systems such as a banking app or CRA (federal Canadian Revenue Agency).

Once you have entered the answers, click **Done**.



The Security Question enrolment process has now been successfully completed



## Managing Authentication Methods

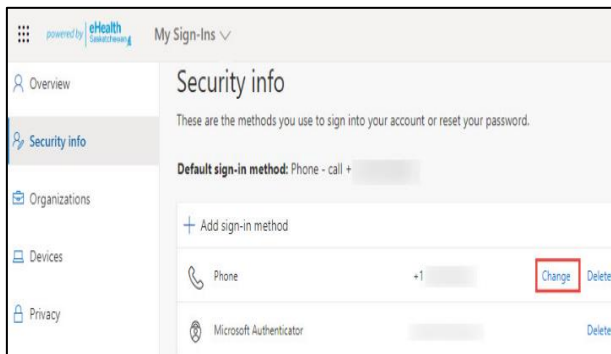
### [Change Authentication Method](#)

### [Add an additional Authentication Method](#)

### [Delete an existing Authentication Method](#)

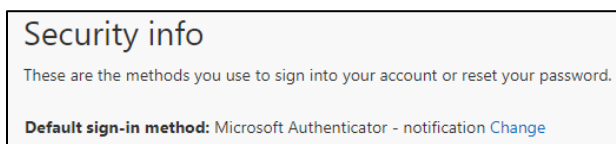
## 1. Change Authentication Method

- a. Navigate to: <https://mysignins.microsoft.com/security-info> and select **Change**.

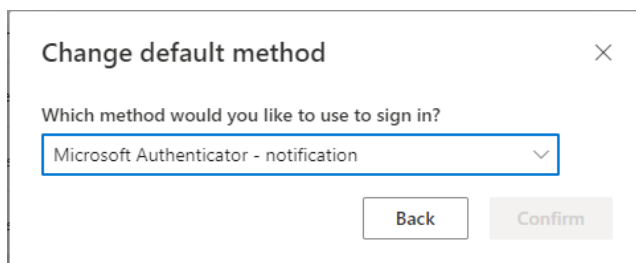


**NOTE:** if methods are already registered, you may see a Multifactor Authentication request before you access the Security Info web portal.

- b. Select the **Change** link on the method requiring updating, enter the new information and click **Next** to validate the change.
- c. You can also change the default method used for authentication. The **Default sign-in method** is configured at the time of the enrolment. The example below shows an individual who has enrolled with Microsoft Authenticator as their default.



- d. Click the **Change** button and select the new default method, click **Confirm**.



## 2. Add an Additional Authentication Method

- a. To add an additional method of authentication, click on **+ Add sign-in method**. This will provide alternate options to add (*e.g. authenticator app or to add an alternative phone*).



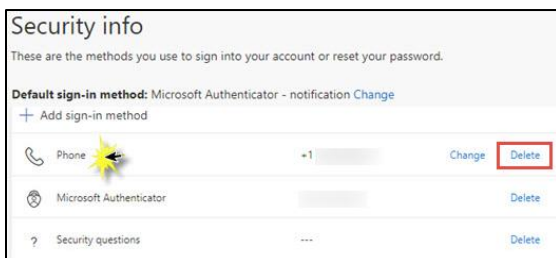
Refer to the [Microsoft Authenticator Registration](#) section to **add the Authenticator app**.

You have successfully added an additional authentication method

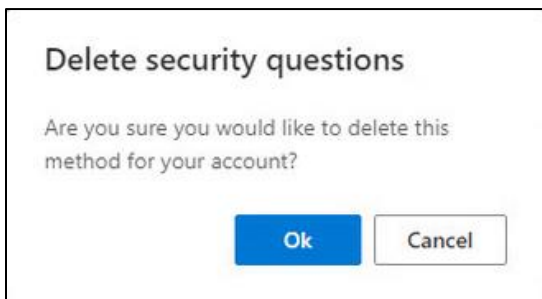
## 3. Delete Existing Authentication Method

**IMPORTANT:** If you delete all methods of authentication, you may lock yourself out of your network account. In this event, please [contact the eHS Service Desk](#) for assistance.

- a. In the event that your device is stolen, lost, or retired, there is the option to delete the existing authentication method.



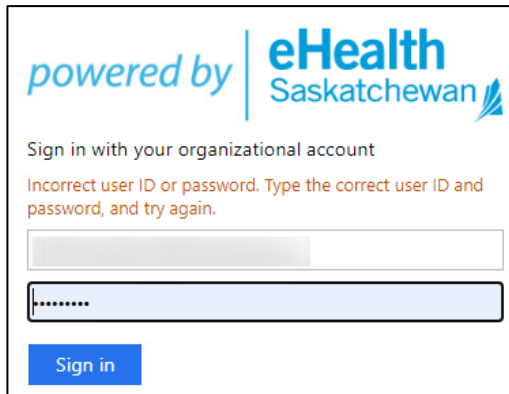
- b. Select the sign-in method you wish to remove. Click **Delete**.
- c. Click **Ok**.



You have successfully removed the authentication method

### Login Issues

Customer receives ***"Incorrect user ID or password. Type the correct user ID and password, and try again."***



powered by | **eHealth**  
Saskatchewan

Sign in with your organizational account

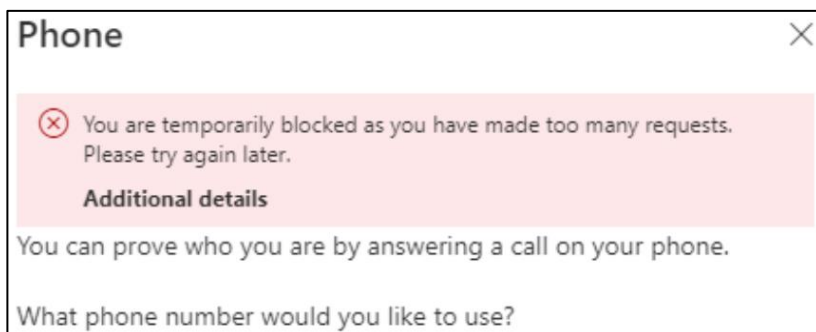
Incorrect user ID or password. Type the correct user ID and password, and try again.

[Sign in](#)

- This message can be viewed if your account is locked. Message can appear if another customer account has the same email address.
- For any duplicate accounts the recommended login method is using the following format:  
Domain\username (i.e. HEALTH/jsmith)
- If login still fails when using Domain\username, a ticket should be escalated to [eHS Service Desk](#) to unlock the account.
- If login using Domain\username is successful, a ticket should be escalated to [eHS Service Desk](#) to remove duplicate account.
- You will have 5 attempts to login using your network account (i.e. workstation login username/password) credentials before your account is locked out.

### Temporarily Blocked

Customer receives ***"You are temporarily blocked as you have made too many requests. Please try again later."*** error message.



**Phone** [X]

⊗ You are temporarily blocked as you have made too many requests. Please try again later.

**Additional details**

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

What phone number would you like to use?

- This occurs when customer has completed **5 attempts within 1 hour**. After 5 attempts customers are prevented from trying again for 24 hours to prevent the account from being compromised.

- This message only takes place for failed SSPR attempts (i.e. password reset, adding/removing authentication methods too soon etc.).
- This feature prevents your account from being compromised:
  - Attempting to validate phone number 5 times in 1 hour.
  - Attempting to use security questions 5 times in 1 hour.
  - Attempting to reset password for same account 5 times in 1 hour.

## Acronym List

AD	Active Directory (Microsoft centralized management directory services)
Andr	Android
App	Mobile device application/software/widget
eHS	eHealth Saskatchewan
iOS	iPhone Operating System
MS	Microsoft
QR code	Quick Response code. Type of matrix barcode (or two-dimensional barcode)
SHA	Saskatchewan Health Authority
SSPR	Self-Service Password Reset
VDI	Virtual Desktop Interface

## Review History

Reviewed by	Review Date	Reason
KM Team Lead	October 4, 2022	Self-Service Password Reset Option
KM Team Lead	October 31, 2022	Final Review
KM Team Lead	November 3, 2022	Add decision step for end-user
KBA WP	November 23, 2022	Modify '30 minute timeout to 15' lockout step
KM Team Lead	November 28, 2022	VDI, SD contact information etc.
KM Team Lead	December 2, 2022	2 documents.
KBA WP	December 7, 2022	Enrolment
KBA WP	December 8, 2022	Modify Enrolment
KBA WP	December 13, 2022	Modify Enrolment
KBA WP	December 14, 2022	Add Wiki Link
KBA WP	December 21, 2022	Add Error Messages

## Version History

Version	Implemented by	Revision Date	Approval	Reason
1.0	KBA, WP	October 4, 2022	KM Team Lead	Initial Documentation
2.0	KBA, WP	October 28, 2022	KM Team Lead	Updates
3.0	KBA, WP	November 3, 2022	KM Team Lead	Add 'options' decision step
4.0	KBA, WP	November 23, 2022	KM Team Lead	Modify '30 minute timeout to 15' lockout step
5.0	KM Team Lead	November 28, 2022	KM Team Lead	VDI limitation
6.0	KBA, WP & KM TL	December 2, 2022	KM Team Lead/Comms	Split out into 2 documents
7.0	KBA WP	December 7, 2022	KBA/Comms	Enrolment
8.0	KBA WP	December 8, 2022	KBA/Comms	Modify Enrolment
9.0	KBA WP	December 13, 2022	KBA/Comms	Modify Enrolment
10.0	KBA WP	December 14, 2022	KBA/Comms	Add Wiki Link
11.0	KBA WP	December 21, 2022	KBA/Comms	Add Error Messages
12.0	KBA WP	March 13, 2022	KBA/Comms	Updated version