JUNE 11, 2024

Self-Service Password Reset (SSPR) Instructions

Follow the instructions below to successfully reset your own password.
Passwords must be at least 16 characters and contain at least 3 of 4 of them.

- a minimum of 1 lower case letter [a-z] and
- a minimum of 1 upper case letter [A-Z] and
- a minimum of 1 numeric character [0-9] and
- a minimum of 1 special character: ~!@#$%^&*()-_+={}[]|\;:"<>,./?

HSHS (Hospital Sisters Health System) passwords must be changed every 365 days.
Note: See Help section at the bottom for some Helpful Tips for setting your password

HOW TO ACCESS THE PASSWORD RESET LINKS:

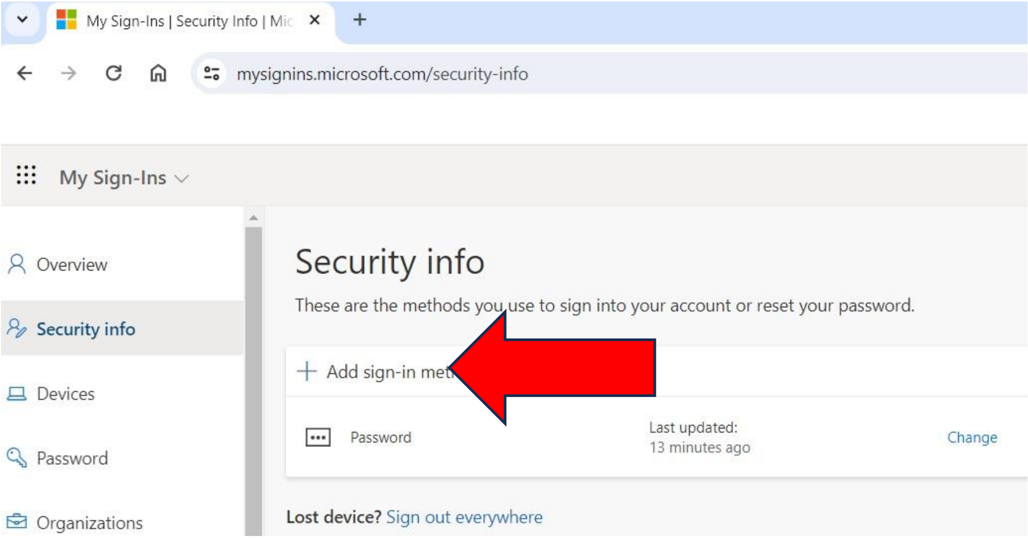
You can access the link to SSPR via the

- HSHS Intranet-System Wide Helpful Links-Colleague Password Reset
- ServiceNow—Search Self Service Password Reset
- support.hshs.org-Colleague Password Reset Helpful Links

REGISTER FOR PASSWORD RESET

1. Registration is required prior to using SSPR. Go to the website below to register for self-service password reset:
   https://mysignins.microsoft.com/security-info

2. Choose ***the Add sign-in method*** & enter information to register for SSPR. Add at least 2 methods in addition to the password method to be able to reset your password.



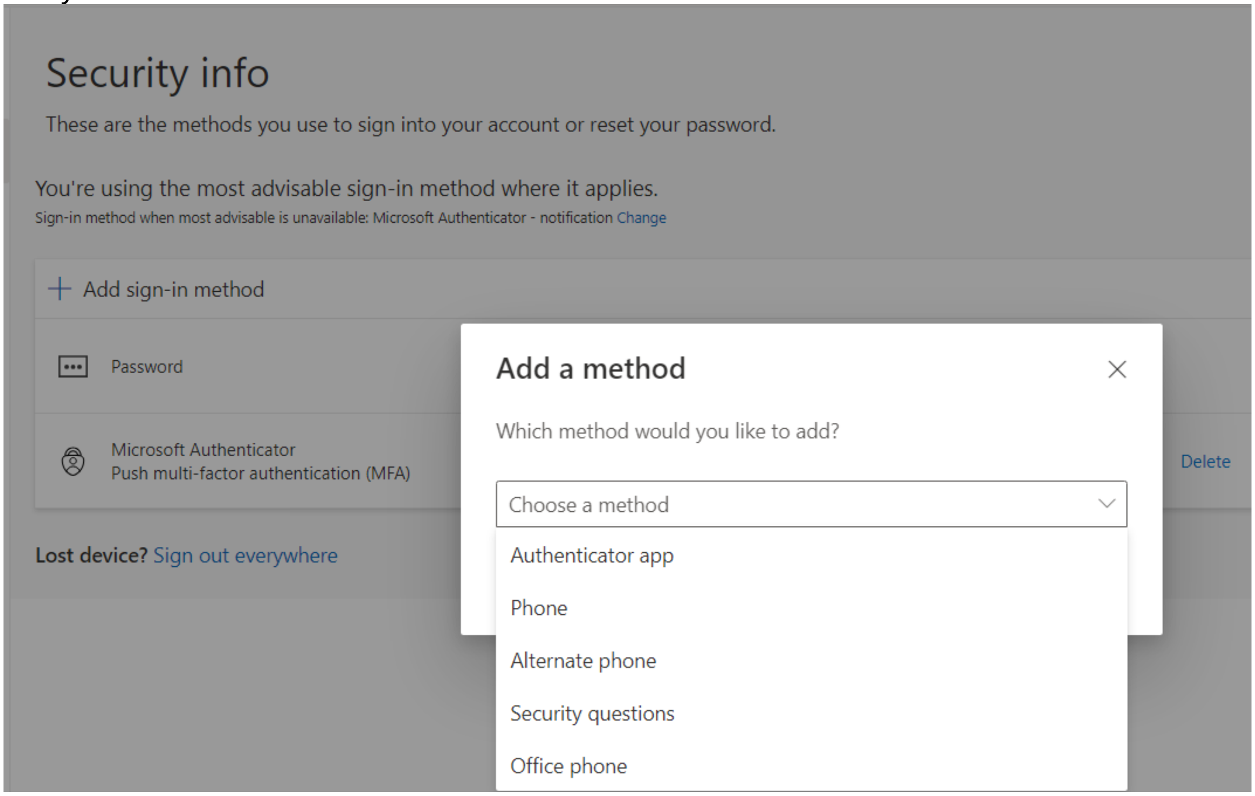
Security info

These are the methods you use to sign into your account or reset your password.

Password Last updated: 13 minutes ago

Lost device? Sign out everywhere

3. Select the ***Choose a method*** drop down list. Remember you must do this 2 times so that you have 2 methods.



Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change

Password

Microsoft Authenticator
Push multi-factor authentication (MFA)

Lost device? Sign out everywhere

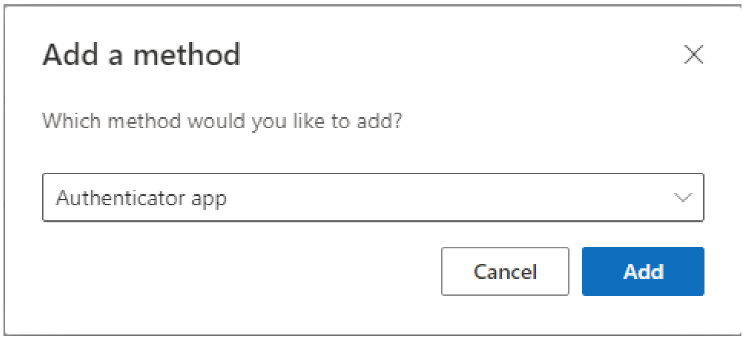
Add a method

Which method would you like to add?

If you choose to select the ***Authenticator*** app follow the additional steps below. If not skip RESET **<u>YOUR PASSWORD WHEN YOU KNOW YOUR PASSWORD</u>** section below.

4. Download the ***Microsoft Authenticator*** app on your mobile device from the App Store or Google Play Store. *Note: If on a HSHS Wi-Fi network, turn off Wi-Fi*.

5. Select the ***Add*** button.

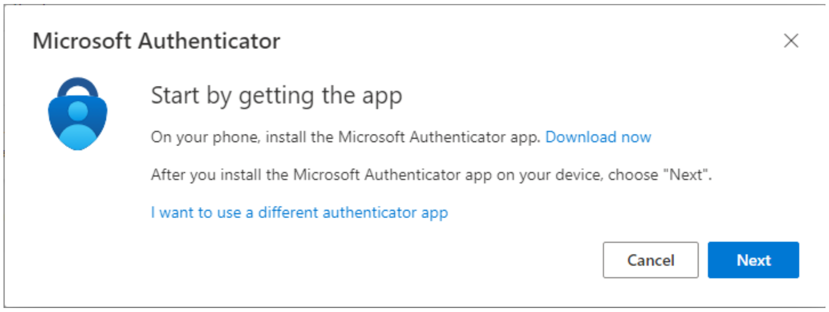


Add a method

Which method would you like to add?

Authenticator app

6. Select the ***Next*** button.



Microsoft Authenticator

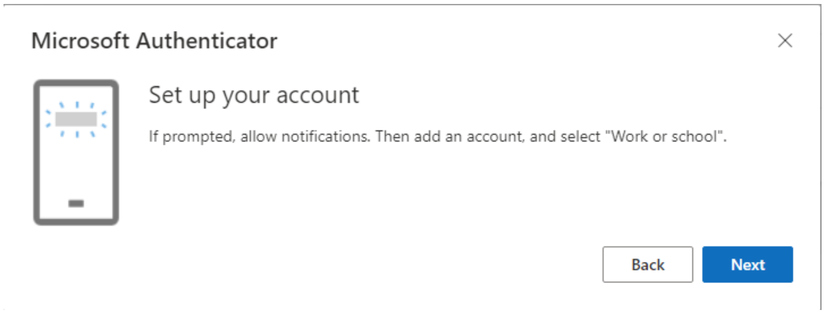
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

7. Follow the directions on the screen by performing the actions on your mobile device, then select the ***Next*** button.

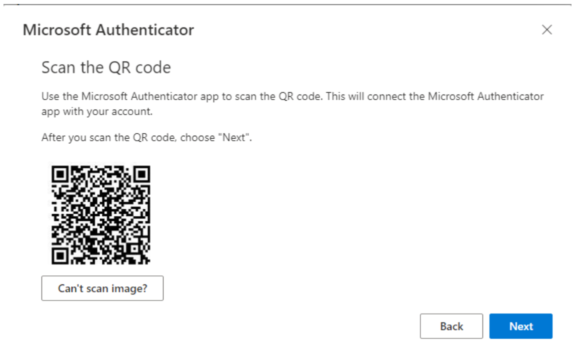


Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

8. Follow the instructions on the screen, then select the ***Next*** button.



Microsoft Authenticator

Scan the QR code

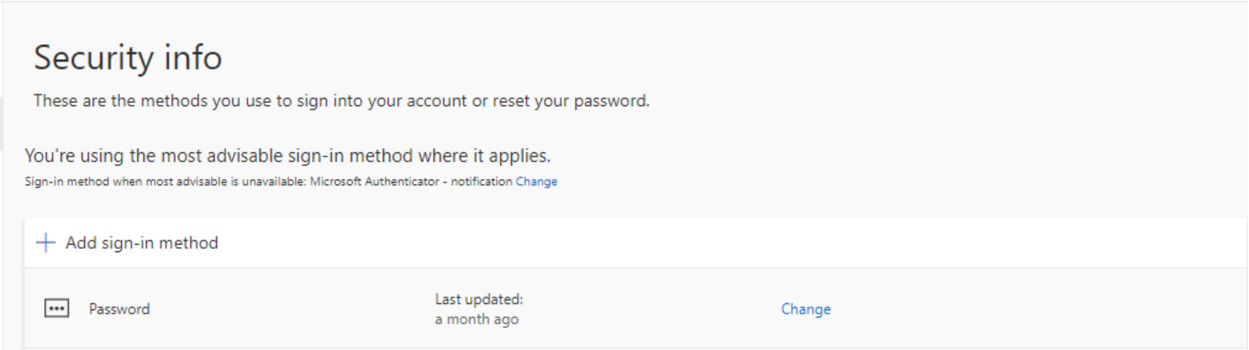
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

RESET YOUR PASSWORD WHEN YOU KNOW YOUR PASSWORD

1. If you know your current password, click the link below.
   https://mysignins.microsoft.com/security-info

2. Select the ***Change*** link.



Security info

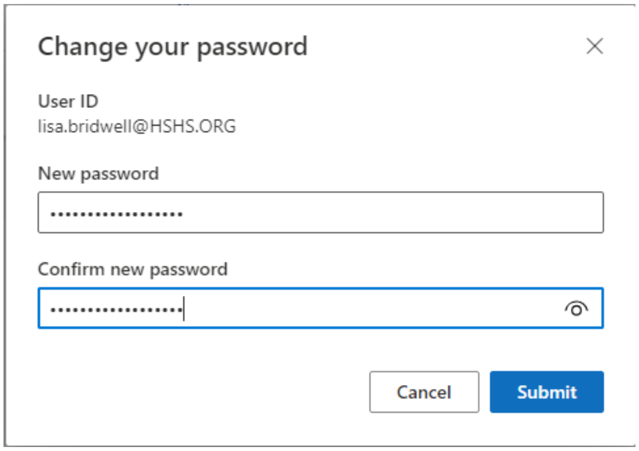
These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change

Password	Last updated: a month ago	Change

3. Enter your new password in both the ***new password*** and ***confirm new password*** fields, then click the ***Submit*** button.



Change your password

User ID
lisa.bridwell@HSHS.ORG

New password
••••••••••••••••••

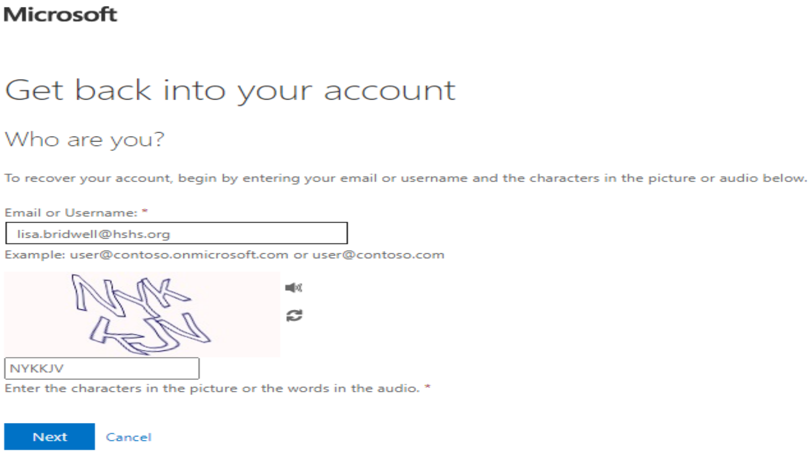
Confirm new password
••••••••••••••••••

RESET YOUR PASSWORD WHEN YOU DO NOT KNOW YOUR PASSWORD

1. If you forgot your password and have registered **2 methods**, launch the link below:

   https://passwordreset.microsoftonline.com

2. Complete the fields on the screen, then select the ***Next*** button.



Microsoft

Get back into your account

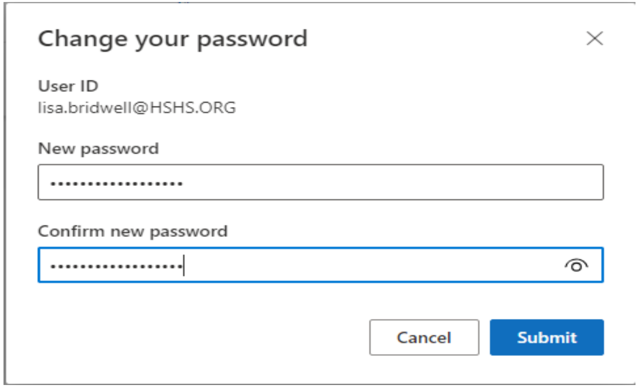
Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username: *
lisa.bridwell@hshs.org
Example: user@contoso.onmicrosoft.com or user@contoso.com

NYKKJV
Enter the characters in the picture or the words in the audio. *

3. Enter your new password in both the ***new password*** and ***confirm new password*** fields, then select the ***Submit*** button.



Change your password

User ID
lisa.bridwell@HSHS.ORG

New password
••••••••••••••••••

Confirm new password
••••••••••••••••••

IMPORTANT INFORMATION ABOUT PASSPHRASES

Know the reasoning behind the rules:
The rules around creating passphrases and passwords exist for a reason. If you are not careful to take precautions with your passphrases and passwords, threat actors can choose from an ever-growing list of methods to break into your devices and accounts and access your information.
Shorter passwords are much easier to hack. You can make it more difficult for threat actors to hack into your devices and accounts if you use lengthy passphrases or more complex passwords.

What is a passphrase?
A passphrase is a more secure form of a password. People use passphrases for the same reasons and in the same way as a password. A passphrase is typically longer and can even contain spaces. A passphrase can also contain symbols, and it does not need to be grammatically correct. Suggestions are using a favorite lyric, movie quote or other phrase that is personal to you and can easily satisfy complex rules and requirements for passwords like punctuation and uppercase and lowercase letters.

Why are passphrases awesome:

1. Passphrases are easier to remember than passwords. A random collection of numbers and symbols can be difficult to keep track of, which can mean that users often make it simpler to remember them. A passphrase is usually not as hard to remember.
2. Passphrases are difficult to crack through brute force. Many password-cracking tools work to break down 10-character passwords. Since passphrases are longer, they can be much more secure and safe from these tools.
3. Most major applications and OS (operating systems) allow for up to 127 characters and the use of passphrases for optimal security.

A passphrase can easily satisfy complex rules and requirements for passwords, as most allow for punctuation and uppercase and lowercase letters.