

Microsoft Self-Service Password Reset (SSPR)

Managing your enterprise password and multi-factor authentication options via Self Service Password Reset service (SSPR)

Instructional Videos

[Microsoft Entra MFA Token Setup](#)

FAQ

What is multi-factor authentication?

MFA is commonly referred to as dual-factor or two-factor authentication. It is a method of confirming a user's identity by requiring a combination of two different forms of authentication. For a user to successfully access a system or application with MFA enabled, they must provide "something they know" and "something they have". At BCM, the "something you know" will be your ECA username and password" and the "something you have" will be a random six-digit number known as a BCM MFA Token which will be regenerated every 30 seconds on your personal mobile device.

What is a BCM MFA token?

A BCM MFA token is a random six-digit number that changes every 30 seconds. It is unique to each user and is used as a second form of authentication in addition to your Baylor username and password when signing in to certain BCM systems or applications.

What is Microsoft Self-Service Password Reset (SSPR)?

Microsoft Self-Service Password Reset (SSPR) is a service within the Microsoft Entra ID, where you can reset your password and setup authentication methods without requiring intervention from IT administrators.

Do I need to register with SSPR?

You will need to register your account with SSPR to make use of the service. The registration process is a wizard driven experience which walks a user through the setup of an MFA verification option.

What tasks can I perform with SSPR ?

Using SSPR, you can perform the following tasks on your account:

- Manage BCM enterprise password
- Manage multi-factor authentication options

Which MFA Options are available to me in Microsoft SSPR?

Microsoft SSPR provides Multi-Factor Authentication (MFA) for an additional layer of security during the password reset process and general authentication to applications . You are required to configure at least one of the options below, but you may configure several MFA options if you like:

- **Microsoft Authenticator App:** with this option, you can receive push notifications or generate verification codes. This is the recommended option, as it is the most user-friendly. *You will need to install the Microsoft Authenticator app on your smartphone if you choose to use this method.*
- **Authenticator App:** Users can choose to set up Google Authenticator to generate verification codes. *You will need to install the Google Authenticator app on your smart phone if you choose to use this method.*
- **SMS:** Users can receive a text message with a verification code to verify their identity.

How do I access SSPR?

NOTE: To use SSPR, you must first fully register your account.

You can access SSPR on your computer via: <https://bcm.edu/myaccount>

How do I register with SSPR using the Microsoft Authenticator method.

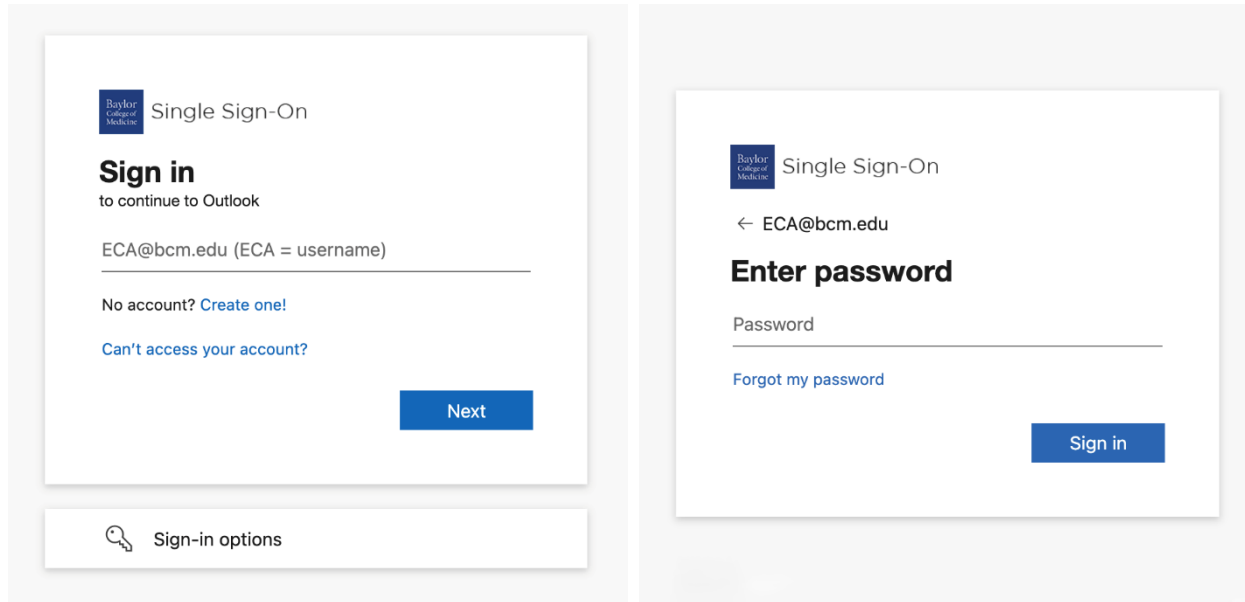
New users are required to register with SSPR and establish an MFA option. *Once you have registered, you can then use SSPR to manage your password and your MFA options*

NOTE: *Users that have not completed SSPR registration will automatically prompted to register when accessing any SSO application.*

- On your **computer** browse to: <https://bcm.edu/myaccount>
- Authenticate:

1.

- a. Enter your sign-in in the format: ECA@bcm.edu
- b. Enter Password
- c. Update your password, only if this is your first time signing in





Single Sign-On

u123456@bcm.edu

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

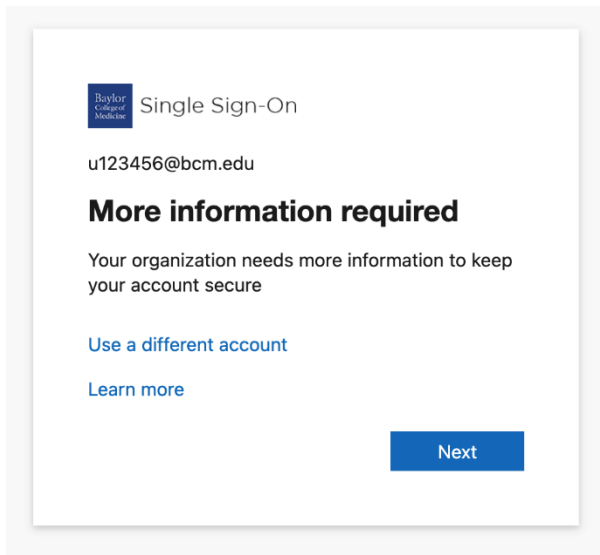
Confirm password

Sign in

Provide additional information:

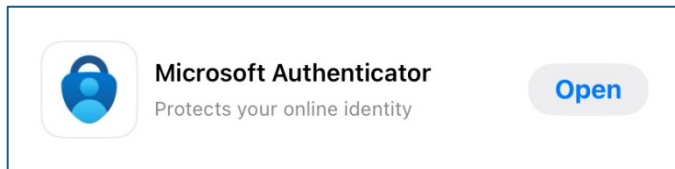
When accessing SSPR for the first time, you will be asked to provide additional information to fully register. This wizard process will guide you through the registration process, which consists of the setup of your MFA (Multi Factor Authentication) options.

Click "**next**" on prompt below to continue

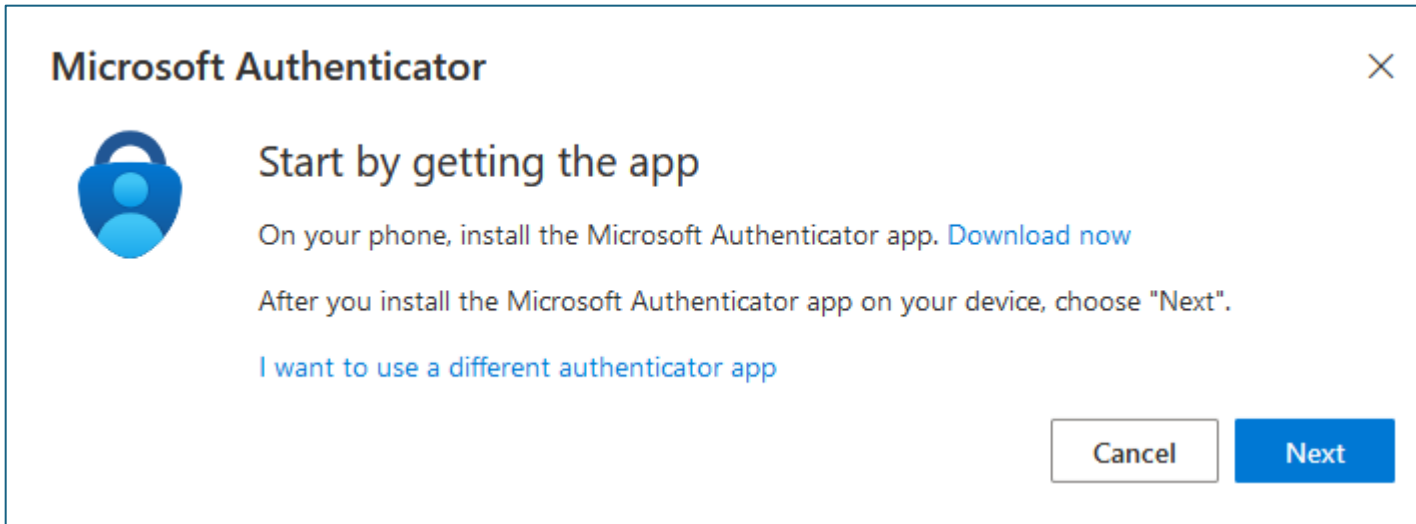


You will be prompted to install the Microsoft Authenticator app on your phone.

NOTE: Ensure you are downloading the correct app by comparing the logo below and verifying that it is the "Microsoft" Authenticator.



Click "**next**" on prompt below to continue, once you have completed the application installation on your smart phone.



Click "**next**" on the "**on computer**" side prompt shown below to continue to set up your account.

Then, Follow the "**on phone**" side instructions below.

ON COMPUTER

ON PHONE

Microsoft Authenticator



Set up your account

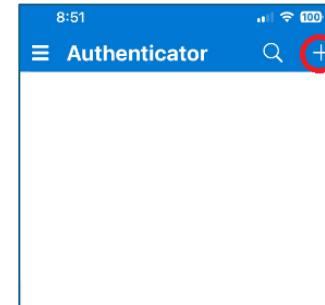
If prompted, allow notifications. Then add an account, and select "Work or school".

Back

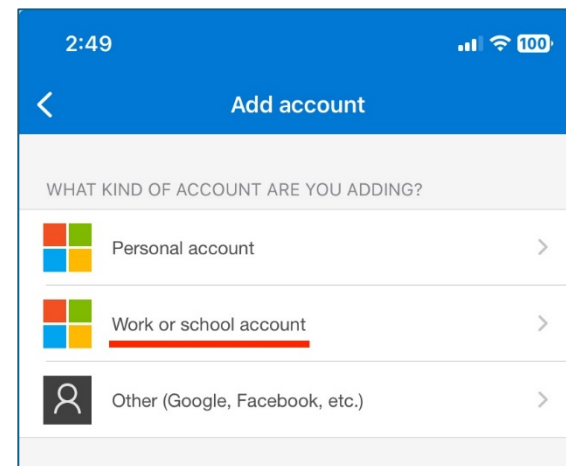
Next

Open Microsoft Authenticator App on phone

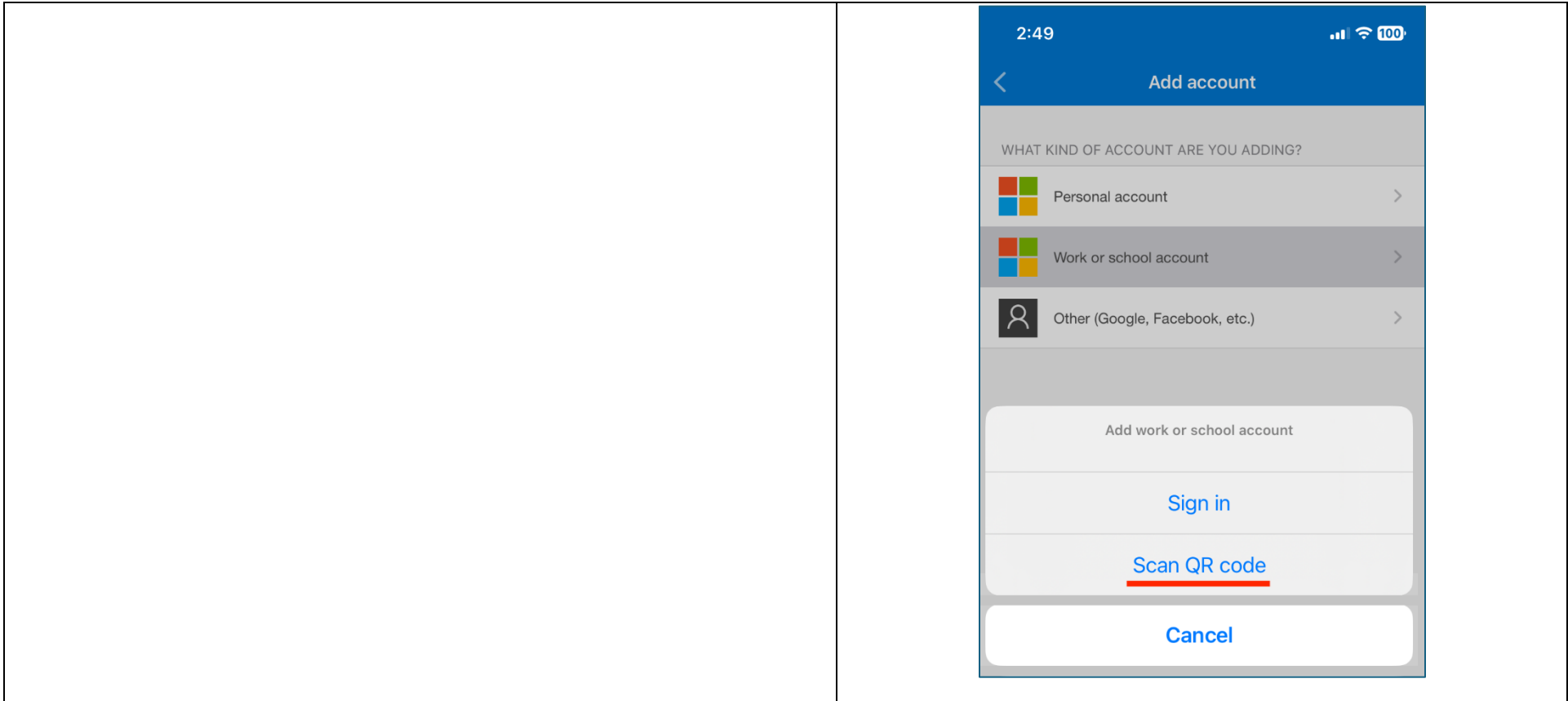
Add account by clicking the "+" or clicking the "Add Account" button:



select **"work or school account"**



select **"scan QR code"**

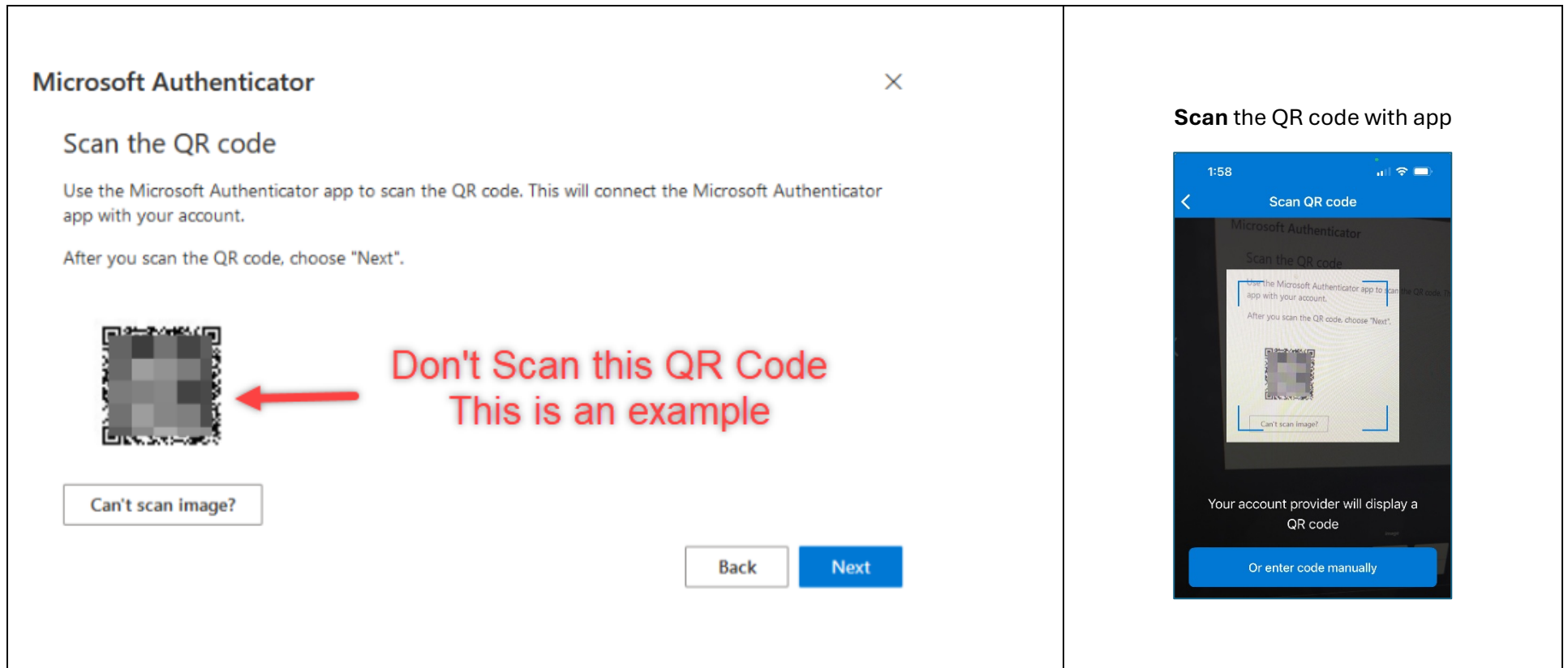


Scan the QR code with your phone, as shown on the "phone side" below.

Please follow the steps until you reach the 'Success' message. Failure to complete all the steps will leave your registration unusable.

ON COMPUTER

ON PHONE



Click "**Next**" on the prompt shown "**on computer**" side above.

You will now be prompted to **test** the registration.

Enter the **number** displayed on the prompt shown "**on computer**" side below, **into** the **Microsoft Authenticator App** on your phone.

ON COMPUTER

ON PHONE

Microsoft Authenticator

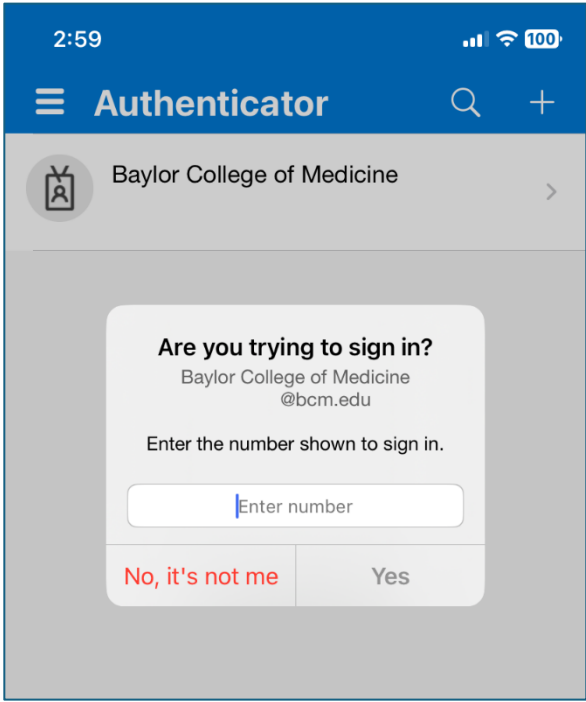
Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

23

Back Next

Enter number displayed on page into phone app and **tap 'yes'** option.



Once you successfully verify proper operation by entering the number in the app, you will see the approval message below.

Click "**next**" on the prompt below to continue.

Microsoft Authenticator



✔ Notification approved

Back

Next

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

Skip setup

You have successfully registered with SSPR and configured Microsoft authenticator.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

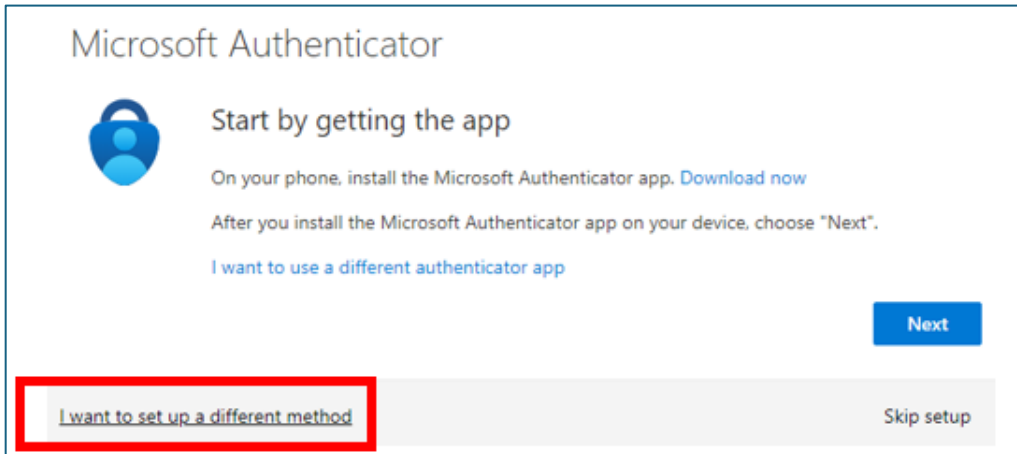


Microsoft Authenticator

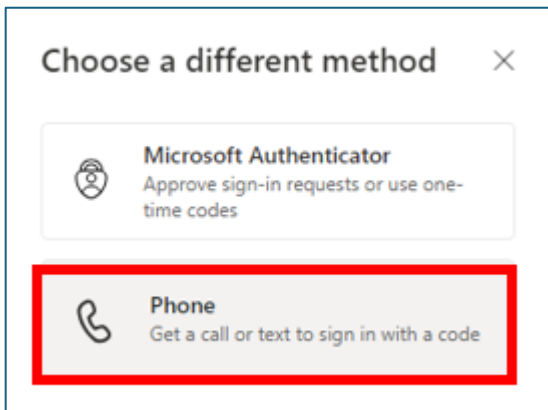
Done

How do I register with SSPR using the SMS method:

When Prompted to choose a different method



Choose **phone**



Enter your mobile phone number and click **next**

Keep your account secure

Phone

You can prove who you are by receiving a code on your phone.

What phone number would you like to use?

United States (+1)

Receive a code

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

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

You will receive a text message with a verification code, **enter** the **code** and click **Next**

Keep your account secure

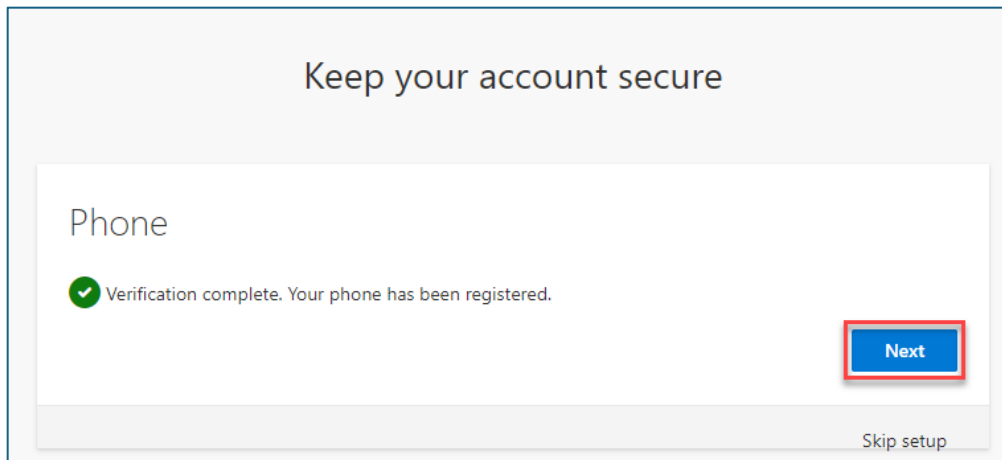
Phone

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

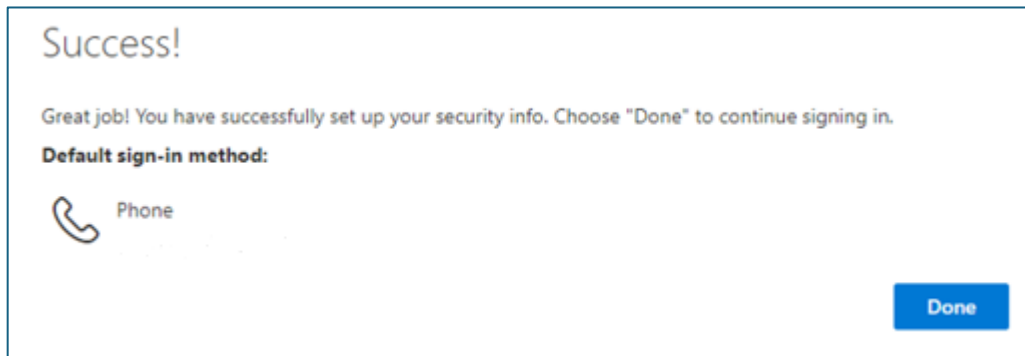
[Resend code](#)

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

if the code is correct, the verification step will complete, click **next**



You have successfully registered with SSPR and configured SMS token.



Using SSPR

Using SSPR, you can perform the following tasks on your account:

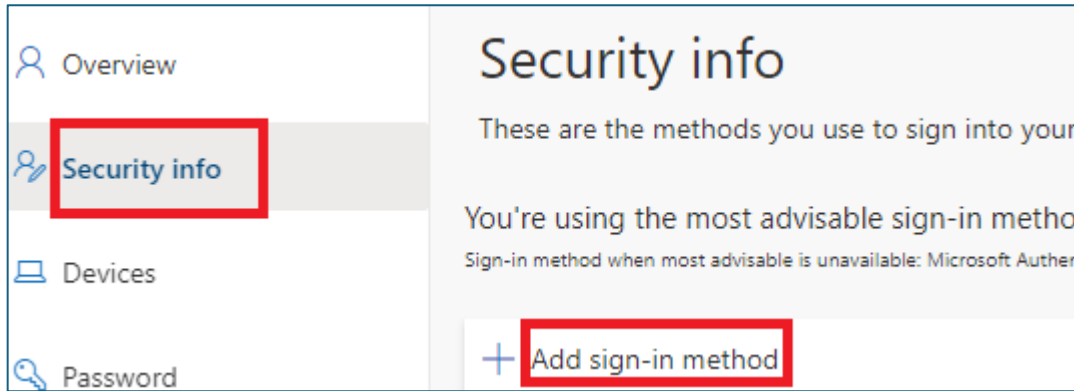
- Manage multi-factor authentication options
- Manage BCM enterprise password

Managing MFA options

ADD:

You can add other MFA verification methods that may be used for access. Giving you the ability to choose the MFA method at logon that is the most appropriate for your situation.

To add, select the **security info** section, and click "**Add sign-in method**"



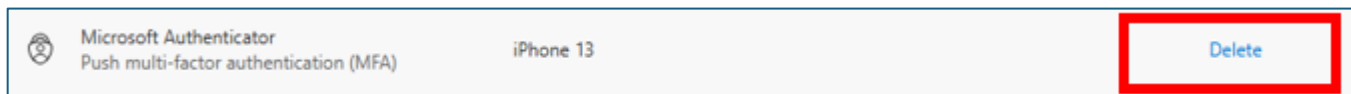
Then **select** the authentication method that you would like to add follow the instructions.

Available options:

- Microsoft Authenticator app
- Authenticator App (Select this option if you want to scan into Google Authenticator or Twilio Authy)
- SMS

REMOVE:

To remove an MFA option, click "**delete**" on the option you would like to remove and follow prompts:



UPDATE DEFAULT MFA SELECTION:

You can set which MFA method will be prompted by default, from the following options:

1. **App based authentication - notification** [This is the "push authentication" method which provides you a two digit number to enter into the app. *This method requires data service on phone.*]
2. **App based authentication or hardware token - code** [This method allows you to enter the 6-digit code that is displayed in authenticator app]

3. **Phone - text** [Only available if you have registered an SMS option]

[learn how to use my new Microsoft MFA token](#)

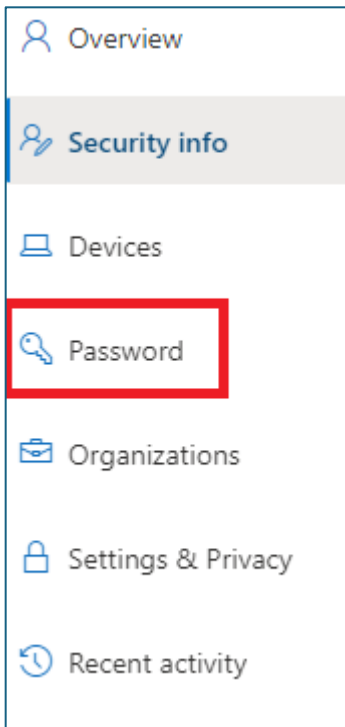
To update the default sign-in method, click "**change**" link, select method and click "**Confirm**" button.



How to Update Your Password Using Microsoft SSPR

Access the SSPR Portal by browsing to: <https://bcm.edu/myaccount>

Click the **password** option from left navigation options



Enter your New Password and click **Submit**

Change your password ✕

User ID
[redacted]@bcm.edu

New password

Confirm new password



If your password meets the complexity requirements, but you still receive the message below, your password is either determined to be a weak password or one that is found on the dark web. Please ensure your new password is unique, strong and one that you haven't used before.

New password

Your password doesn't meet policy requirements. Choose a different password.

After successfully resetting the password, you will receive confirmation that the process is complete. Your new password is now ready for consumption.