Microsoft Authenticator

Guide to setting up Microsoft Authenticator for you Barweb Account

- What is Microsoft Authenticator?
- Setting Up Microsoft Authenticator

What is Microsoft Authenticator?

A Faster and Safer Way to Protect Your Account

Microsoft Authenticator is a free app from Microsoft that helps verify your identity when signing in to your Microsoft 365 account.

Instead of waiting for a text message containing a security code, Microsoft Authenticator sends a notification directly to your phone. You simply tap **Approve** to confirm it's you.

In most cases, it is quicker, easier, and more secure than receiving codes by SMS.

Why Do I Need It?

When you sign in to your email, you use your password as the first layer of security.

The second layer, often called Multi-Factor Authentication (MFA), helps protect your account if somebody manages to obtain your password.

Traditionally, this second step has often been a code sent via text message. While this has improved security for many years, cybercriminals have become increasingly successful at intercepting or bypassing SMS verification methods.

Microsoft Authenticator provides a stronger and more reliable alternative.

How Does It Work?

When you sign in from a new device or location:

1. Enter your email address and password.
2. A notification appears on your phone.
3. Open the notification and tap **Approve or match 2 digits**
4. You're signed in.

That's it.

No waiting for a text message.

No copying and typing six-digit codes.

Why Is It Better Than SMS?

Faster

SMS messages can take time to arrive.

Authenticator notifications are usually immediate and only require a single tap.

More Reliable

Text messages rely on your mobile carrier.

Authenticator works using an internet connection and can function over Wi-Fi, even when mobile reception is poor.

More Secure

Cybercriminals can sometimes trick mobile providers into moving your phone number to another SIM card. This is known as "SIM swapping".

Because Microsoft Authenticator is linked directly to your device rather than your phone number, it provides much stronger protection against these types of attacks.

Is It Difficult To Use?

Not at all.

Most people find Microsoft Authenticator easier than SMS after the initial setup.

Once configured, approving a sign-in usually takes only a few seconds.

For many users there is less typing, fewer delays, and fewer issues than receiving text messages.

What If I Get a New Phone?

Changing phones is common and expected.

If you replace your device, Microsoft Authenticator can be configured on your new phone. As with any security system, we recommend contacting support if you're changing devices and are unsure of the process.

Keeping more than one sign-in method registered also helps ensure you can always access your account if something happens to your phone.

Is Microsoft Authenticator Safe?

Yes.

Microsoft Authenticator is developed and maintained by Microsoft and is used by millions of people worldwide.

Importantly:

- Your password is not stored in the app.
- Your fingerprint or facial recognition information never leaves your device.
- The app helps verify that it is really you signing in.

Using Microsoft Authenticator significantly reduces the risk of somebody gaining unauthorised access to your account.

Microsoft Is Retiring SMS Authentication

Microsoft has announced that Microsoft-provided SMS and voice authentication services will be retired from Microsoft Entra ID from **1 February 2027**. Before this, Microsoft is encouraging organisations and users to move to stronger sign-in methods such as Microsoft Authenticator and passkeys.

This change is being made across Microsoft's platform to improve security and reduce the risks associated with SMS-based authentication.

For this reason, users who currently rely on text message codes are encouraged to begin using Microsoft Authenticator as soon as possible.

Our Recommendation

We recommend that all users install Microsoft Authenticator and make it their primary sign-in method.

Benefits include:

- Faster sign-ins
- Fewer problems with delayed text messages
- Better protection against cybercrime
- Works from anywhere with an internet connection

 Ready for Microsoft's upcoming authentication changes

Microsoft Authenticator is one of the simplest steps you can take to improve both the security and convenience of accessing your email and Microsoft 365 account.

Setting Up Microsoft Authenticator

To install Authenticator on your iOS device

Scan the QR code

Or download and install Authenticator from the Apple app store.

Get the app

To install Authenticator on your Android device

Scan the QR code



Or download and install Authenticator from the Google Play store.

Get the app

Upon first install you will have to agree to Microsoft privacy policy and it's required permissions.

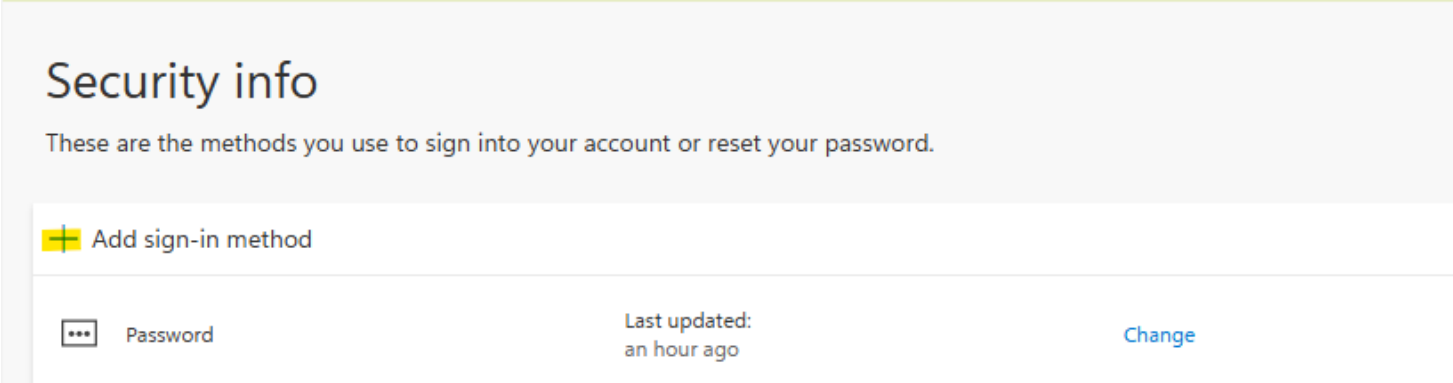
Add a work or school account using a QR code

To add an account by scanning a QR Code, do the following from your computer:

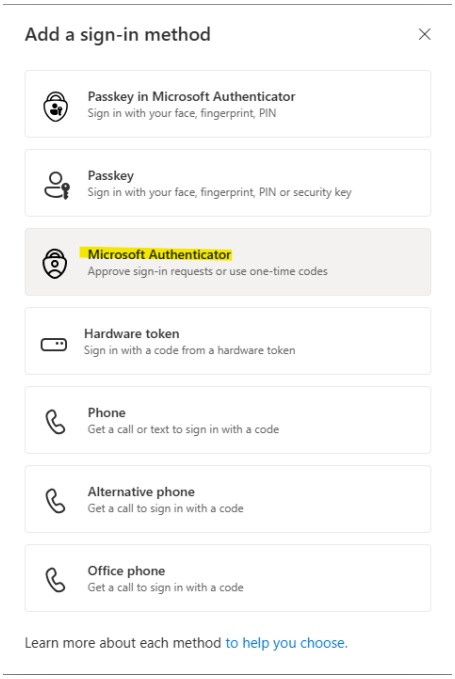
Sign in to the **Security info** page of your account at mysignins.microsoft.com/security-info.

Sign in

Select + Add sign-in method.

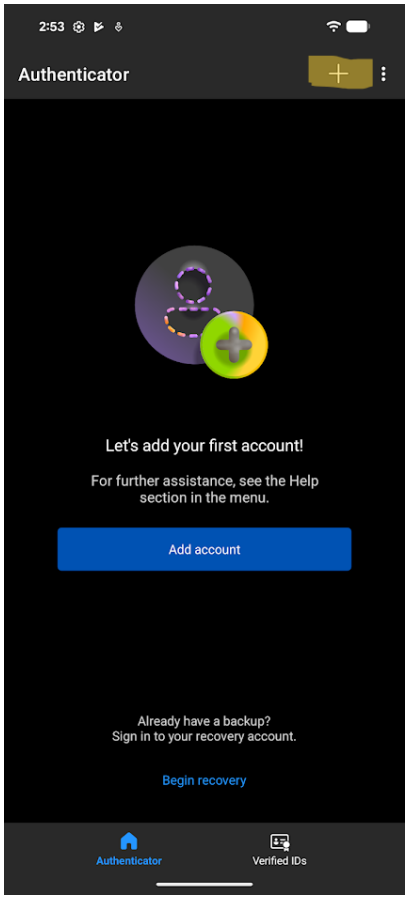


Choose **Microsoft Authenticator** from the dropdown and select **Add**.



If you already have Authenticator installed on your phone, select **Next** to display a QR code.

Open Authenticator on your phone and select the plus icon + and select **Add account.**



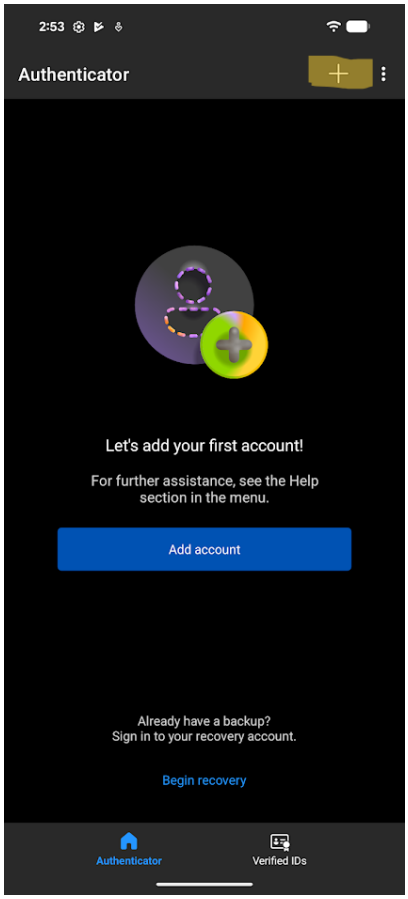
Select **Work or school account** then tap **Scan a QR Code**.

Your account is now added to Microsoft Authenticator

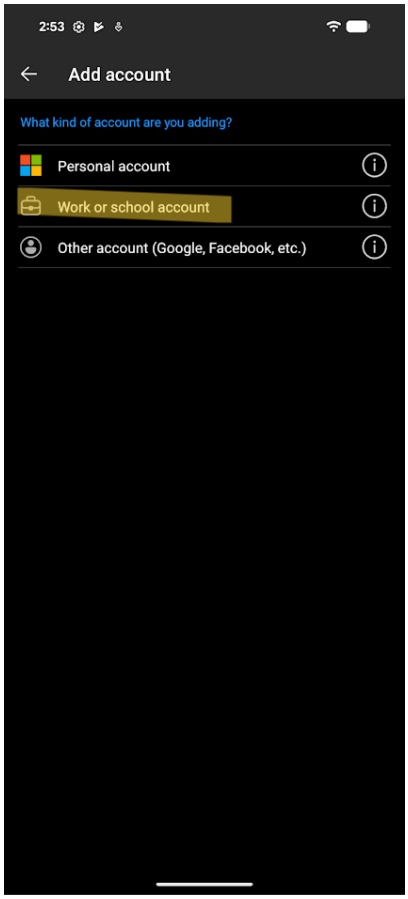
Add a work or school account using your credentials

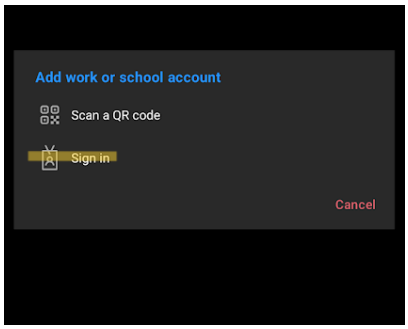
To add an account by signing into your work or school account using your credentials:

Open Authenticator and select the plus icon + on the top menu bar.



Tap **Work or school account** and select **Sign in**.



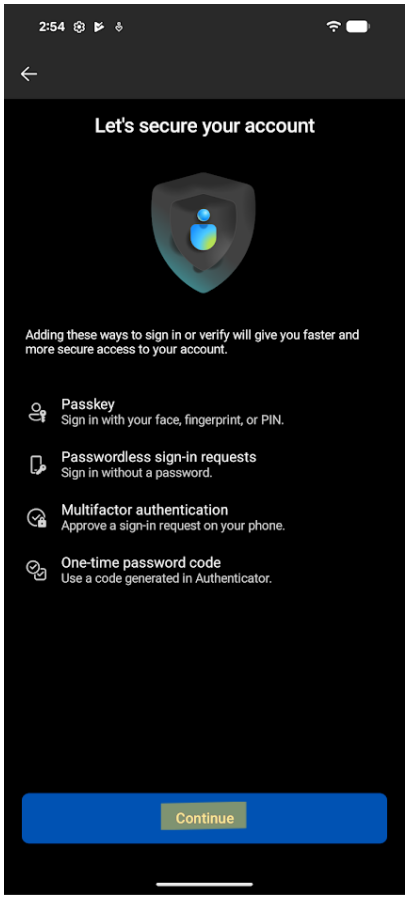


If your phone already has Microsoft accounts configured, select your **QldBar account**. Otherwise, tap **Use another account**.

Enter your ****@qldbar.asn.au email address and password

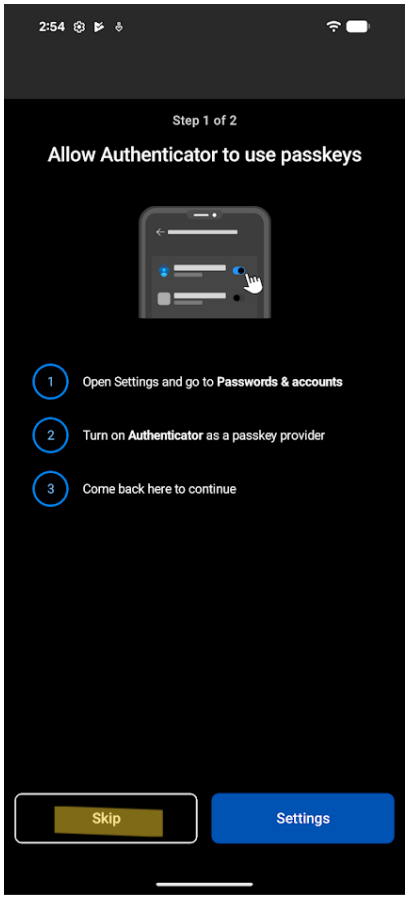
Complete the existing **SMS verification process** by selecting **Text** and entering the code sent to your mobile phone.

When greeted with the **Let's secure your account** tap **Continue**



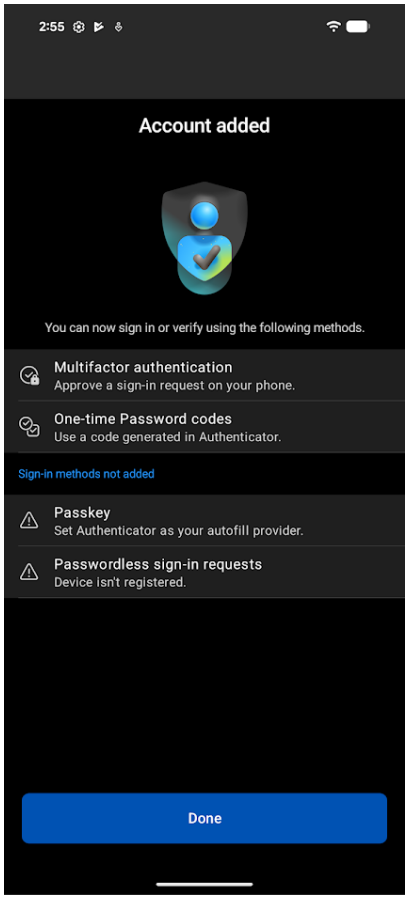
You may be prompted to create a passkey. A passkey allows you to sign in using your device PIN, fingerprint, or facial recognition instead of a password or text message code. The passkey remains on your device and is not shared with Barweb.

You can choose **Skip for now** if you do not wish to create a passkey at this time.



If prompted to register the device, tap **skip**

You should now have your QldBar account added to your authenticator app.


2:55
Account added
You can now sign in or verify using the following methods.
Multifactor authentication
Approve a sign-in request on your phone.
One-time Password codes
Use a code generated in Authenticator.
Sign-in methods not added
Passkey
Set Authenticator as your autofill provider.
Passwordless sign-in requests
Device isn't registered.
Done