



Communities
& Justice

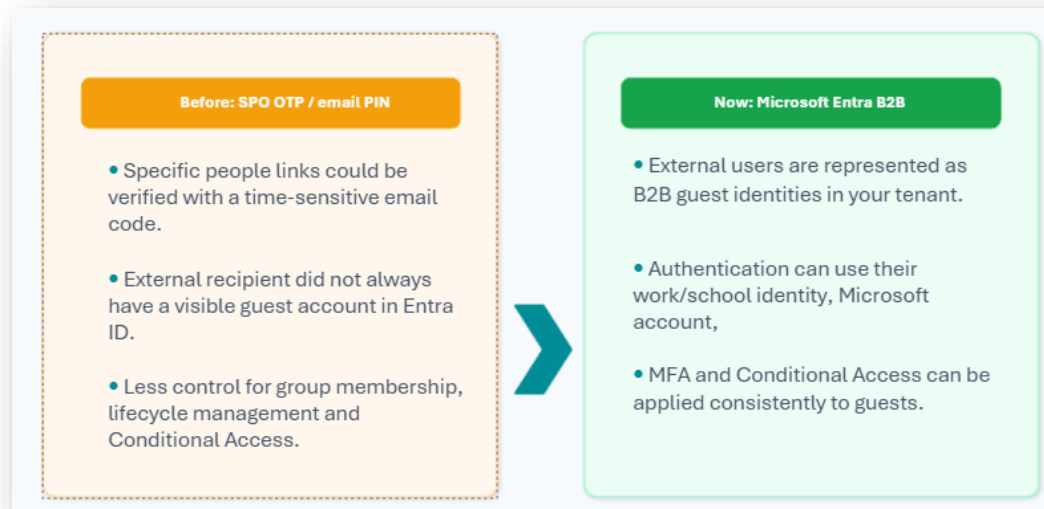
DCJ's Data Sharing Tools (O365)

Executive summary

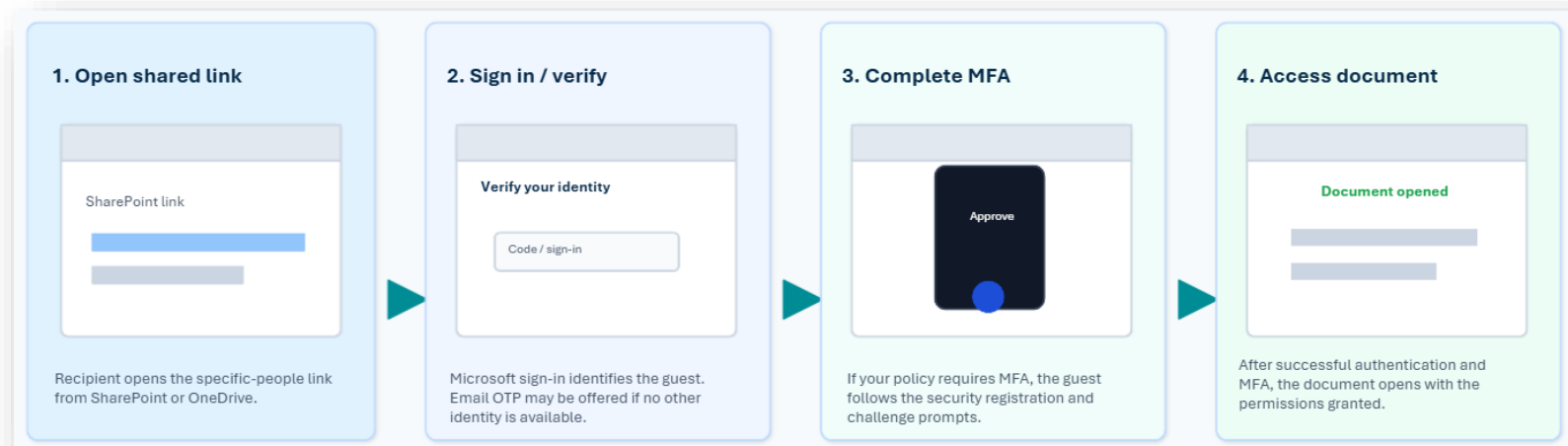
Microsoft has retired the use of one-time passcodes sent via email for accessing shared SharePoint and OneDrive content. As this authentication method provided a lower level of security, it is no longer supported.

External users must now sign in with a Microsoft account and verify their identity using the Microsoft Authenticator app. Once they enter their credentials, they will receive a prompt on their mobile device to approve the sign-in. In some cases, they may also be required to enter a number displayed on screen before approving the request.

This enhanced authentication process helps ensure that only the intended recipient can access the shared content, significantly reducing the risk of unauthorised access if an email account or password is compromised.



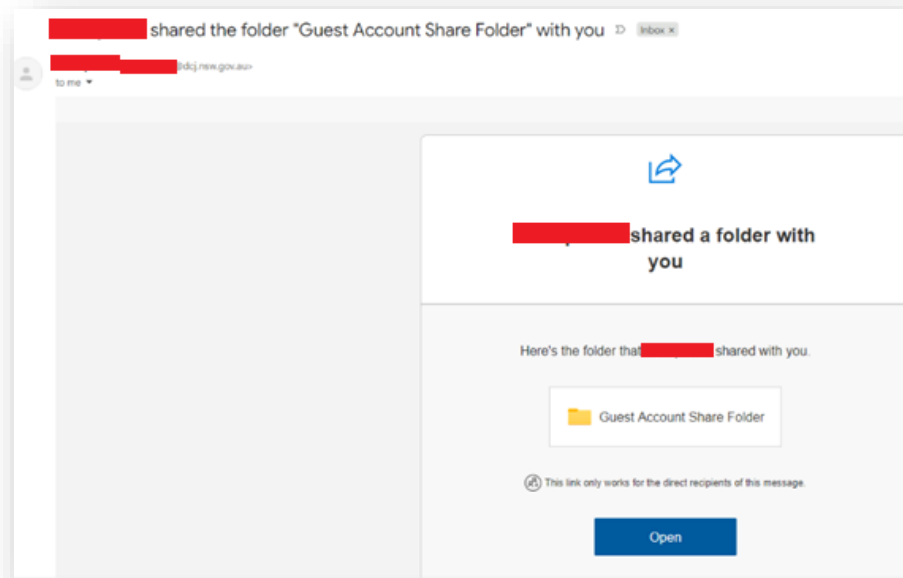
External user experience: access + MFA setup



Set up multifactor authentication

When a file or folder on DCJ SharePoint / OneDrive is shared with an external recipient, the recipient receives an access link at the email address used for sharing. To open the shared content, the recipient must set up multifactor authentication (MFA)

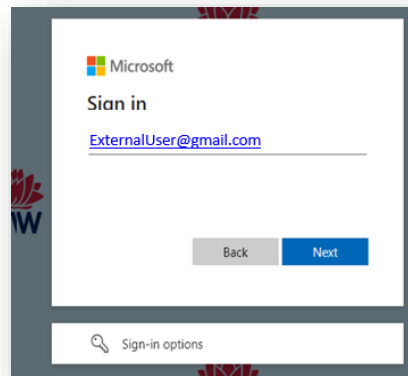
In this example, a OneDrive folder named “Guest Account Share Folder” has been shared with ExternalUser@gmail.com.



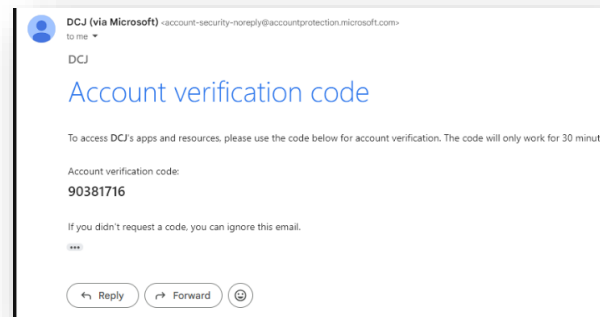
Set up multifactor authentication

Click **Open**. The user will then be prompted to **Sign in**.

The external recipient must enter the email address to which the file was shared. In this example, the user should enter **ExternalUser@gmail.com** and then click **Next**.

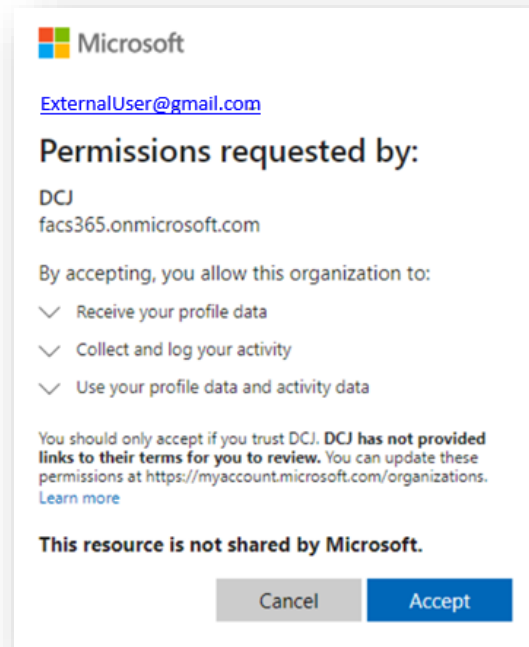


The user will be prompted to enter a verification code sent to their email address. Retrieve the code from the email, enter it in the verification field, and then click **Sign in** to access the shared file.



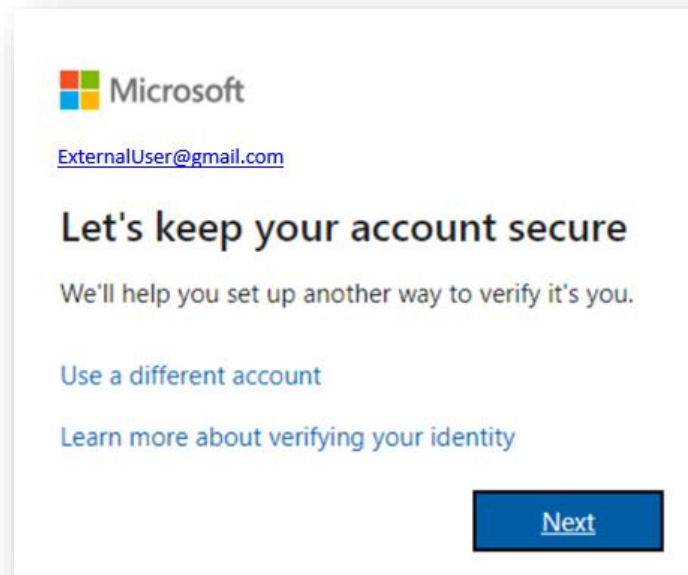
Set up multifactor authentication

DCJ Entra ID will request basic profile read permissions to complete the creation of the guest account required to access the shared resource. Review the permission request and click **Accept** to continue.



Set up multifactor authentication

The user will now be prompted to set up Multi-Factor Authentication (MFA) to enhance the security of their account. Click **Next** to begin the MFA configuration process.

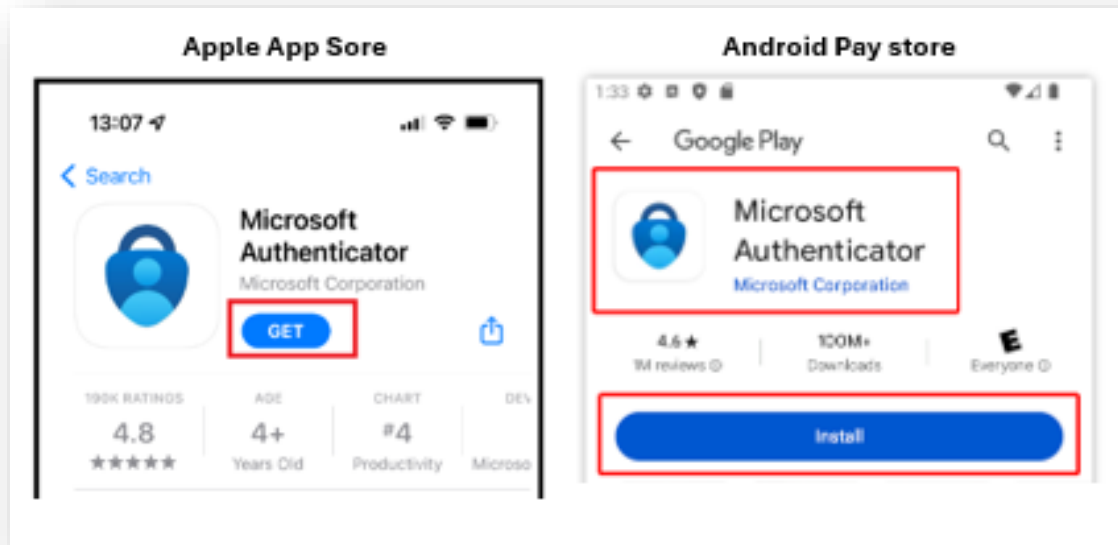


By default, Microsoft presents the option to configure Multi-Factor Authentication (MFA) using the **Microsoft Authenticator** app. Download and install the appropriate version of the app on your mobile device, then click **Next** to continue

Install the App

Apple devices use the App Store and Google devices use the Google Play Store.
Search for the Microsoft Authenticator app in your app store / play store on your Phone.

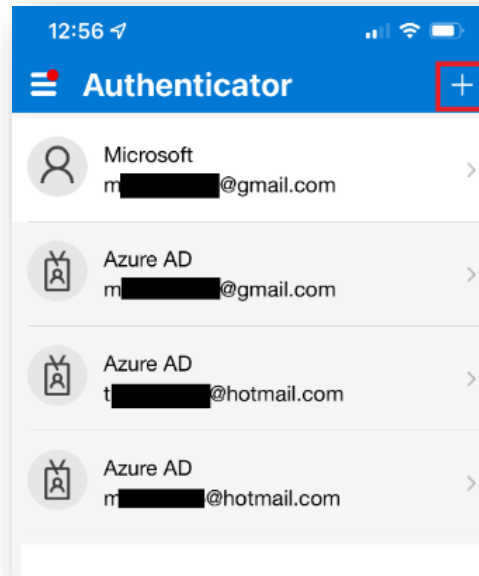
Tap on the **Get / Install** button



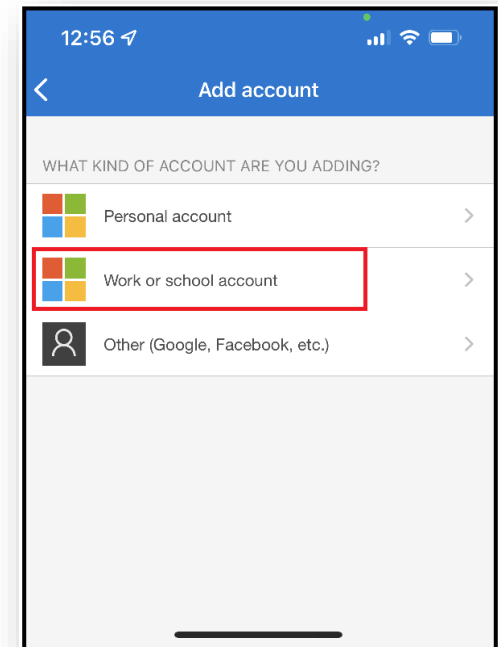
Configure the App

Once the Microsoft Authenticator app is installed, tap to open it. The first couple steps may vary slightly based on if the app had previously been installed or not.

Tap on the **+** (Plus) icon

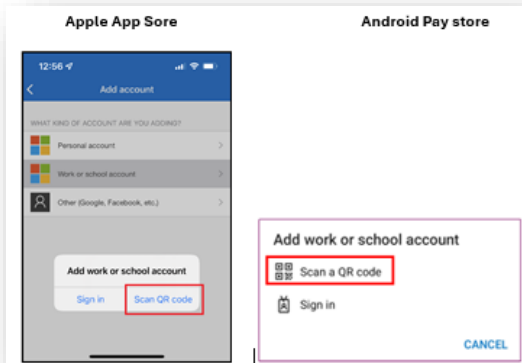


Tap on the **Work or school account** option

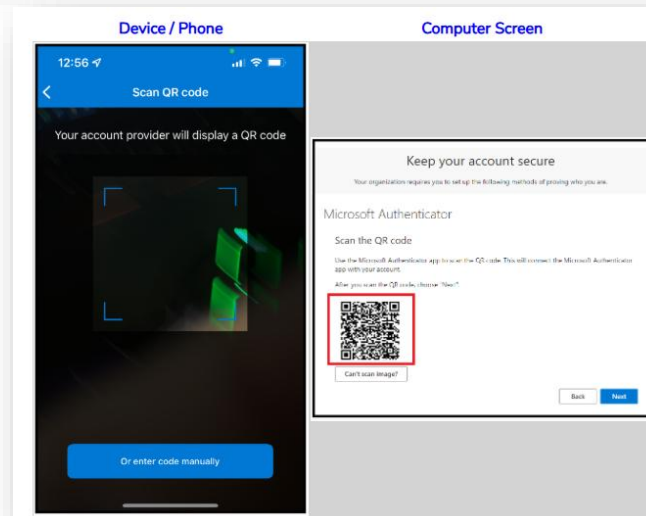
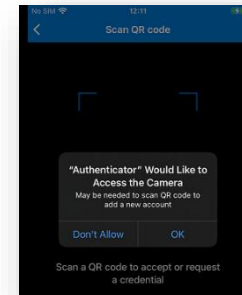


Install the App

Tap on the **Scan QR Code** button

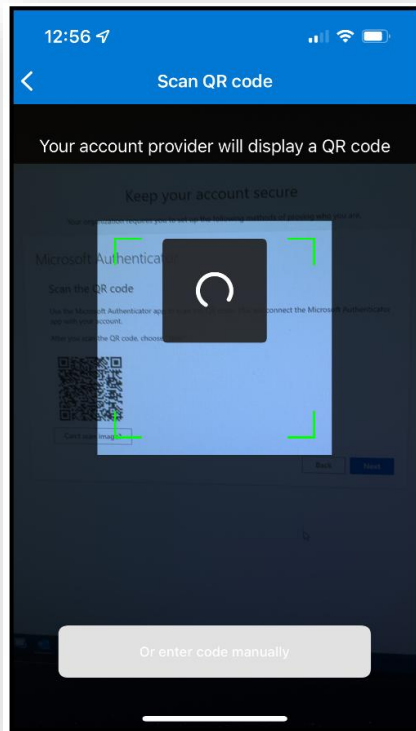


There may be a prompt asking for permission to use the camera. Tap **Approve** or **OK**.

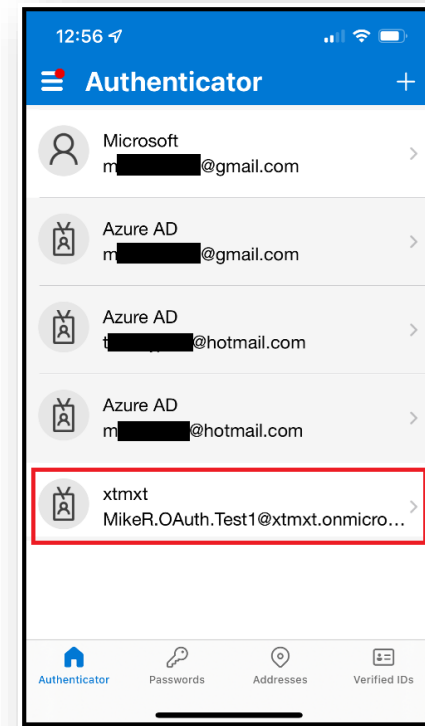


Configure the App

Once the Authenticator App recognizes the QR Code, there will be a brief loading screen.

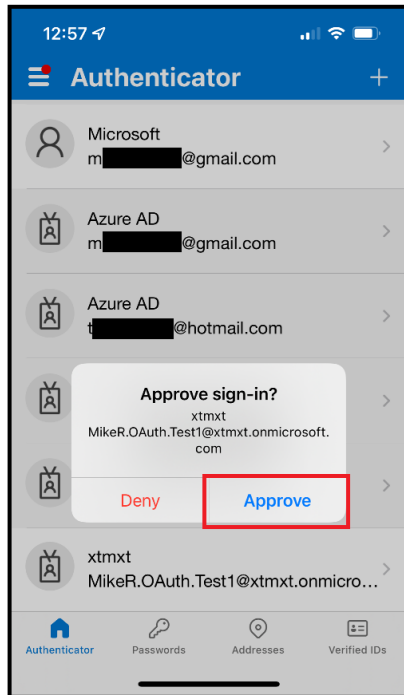


Notice the account is now listed on the Authenticator App.

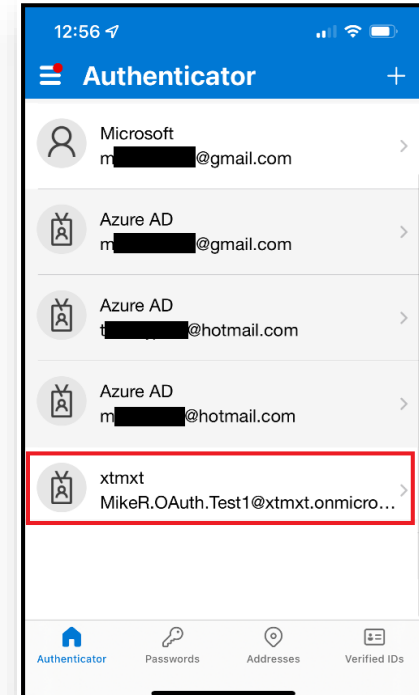


Approve the sign-in

Once successfully signed in, stay in the Microsoft Authenticator app.

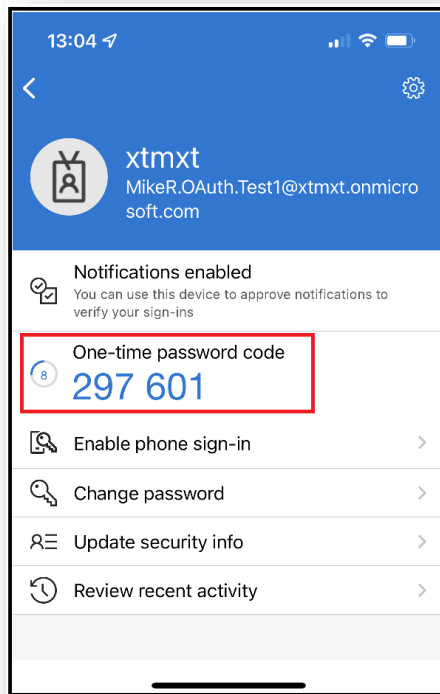


You should receive a prompt on your phone to verify your identity. If the prompt does not appear and you are instead asked to enter a code, proceed to the next step.

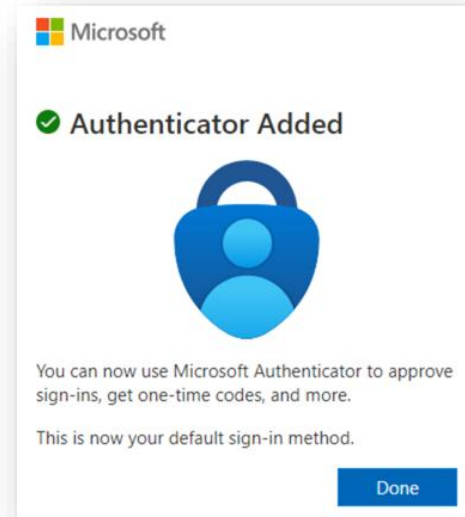


Approve the sign-in

Once successfully signed in, stay in the Microsoft Authenticator app.



This completes the multifactor authentication setup for the guest account.



Frequently Asked Questions

I am not receiving the verification code or sign-in email. What should I do?

Check your Junk/Spam folder and ensure you are using the same email address that the file was shared with. If the issue continues, contact the person who shared the file and ask them to verify the email address used.

Why does the link say I do not have permission to access the file?

This usually occurs when you sign in with a different email account than the one the file was shared with. Sign out and access the link using the exact email address that received the invitation.

Can I use a shared mailbox or team email address to access shared content?

No. The new authentication process is designed for individual user accounts. Shared mailboxes and generic email accounts are typically not supported for MFA registration and access.

I have already completed MFA. Why am I being asked to sign in again?

You may be required to re-authenticate periodically due to security settings or session expiry. Simply sign in again using your registered MFA method to continue accessing the shared content.

The verification notification is not appearing on my phone.

Open the Microsoft Authenticator app manually and check that notifications are enabled on your mobile device.

I scanned the QR code, but MFA setup failed.

Check that your mobile device has internet access and that you completed all steps in the Microsoft Authenticator registration process before closing the page.