Australian Government
Department of Home Affairs

ImmiAccount
Security Enhancements

Q&A - ImmiAccount Multi-factor Authentication (MFA)

Law Council of Australia (LCA)

12 June 2025

The responses below address questions from LCA members specifically relating to ImmiAccount MFA. The ImmiAccount MFA roll out is purely an ImmiAccount security enhancement. The functionality within ImmiAccount has not been modified.

Sharing user credentials

Q: Can we share the same email to login to ImmiAccount?

A: Each ImmiAccount user must have their own user credentials when logging into ImmiAccount. There is no system restriction preventing you from creating an ImmiAccount using an email address that has been used to register other ImmiAccounts.

Q: Can I continue to share ImmiAccount login credentials/user accounts?

A: No. Stop sharing user credentials. Sharing ImmiAccount credentials is prohibited under the ImmiAccount Terms and Conditions (sections 5.1 and 5.6). All ImmiAccount users are required to have their own user credentials. If you are an organisation, consider creating an Organisation ImmiAccount. You can also appoint an Organisation Account Administrator (OAA) to help manage access in your organisation, see Manage your organisation accounts.

Q: Can I login to my colleagues ImmiAccount with their permission?

A: No. Sharing login credentials is prohibited.

Q: Can we register multiple people to receive a code? We use one email account for our team?

A: Sharing login credentials is prohibited. When you setup MFA, you can choose an Authenticator app or email option depending on your individual circumstances. If you are using the email option, there is no system restriction preventing you from setting up your MFA to use a group email address.

Organisation Account

Q: Are administrative employees allowed to create their own ImmiAccount?

A: Yes. All ImmiAccount users are required to have their own user credentials. Consider setting up an Organisation Account, using your business email address and not your personal email. When setting up your organisation account, you can appoint an Organisation Account Administrator to help other users in your organisation with their organisation access.

Q: What functions can an Organisation Account Administrator (OAA) perform?

A: An OAA can approve access for new organisation users, invite staff to create an account, reset passwords and Multi-factor Authentication (MFA), suspend and remove accounts. See our OAA User Guide for additional support with the functions that an OAA can manage.

Q: Can I request access to an organisation account as an individual user?

A: Yes. You can create or request access to join an organisation account via ImmiAccount – see Create your ImmiAccount. To create or join an organisation you will need to enter the organisation name and number (for Australian organisations this will be an ABN).

If you are creating an organisation account as an OAA, you need to ensure you select all other services you require in addition to OAA when creating your account.

Authentication options

Q: What authenticator options will be available?

A: You can select one of two available options for ImmiAccount MFA:

1. Authenticator app for mobile (e.g. Microsoft Authenticator) or PC (eg. KeePass)
2. Email token.

Q: Does the department have its own authenticator app?

A: No. The department does not have its own authenticator app.

Q: Can I receive a text message to authenticate?

A: No. The department does not currently offer a text message option.

Q: Are there free authenticators?

A: Several reputable authenticator apps including Google, Microsoft, Duo Mobile and KeePass are free. There are various free authenticator apps available in the iOS App Store and Android Google Play Store.

Q: Do I need to pay for KeePass authenticator?

A: KeePass is free password manager that can be used on your Personal Computer (PC) for ImmiAccount MFA. If you need help setting up KeePass, see our KeePass User Guide.

Q: Do I need to authenticate each time I login to ImmiAccount?

A: Yes. Similar to accessing your bank account online, you will need to perform MFA at each login.

Q: Do I need to authenticate every time I get kicked out of ImmiAccount, including when I log back in?

A: Yes. You will need to perform MFA each time you login.

Q: Does authentication last 24 hours?

A: No. You will need to perform MFA each time you login.

Q: If I leave ImmiAccount for 5 minutes do I need to log back in?

A: This remains the same as the current settings - user will be logged out after 30 minutes of inactivity or four hours regardless of activity.

Q: Can I switch the login option i.e. while in Australian use authenticator app and when I travel overseas, switch to email option?

A: Yes. MFA authentication method can be changed at any time after logging in using Manage Account.

Q: If we use email token first, can we change to app later on if wanted?

A: Yes. MFA authentication method can be changed at any time after logging in using Manage Account.

Q: Can we MFA whilst working from home or different locations?

A: Yes.

Q: Can I use an email token to authenticate?

A: Yes. Email token is an authentication option that will available when you setup MFA. Your authentication method can be changed at any time after logging into ImmiAccount using Manage Account.

Q: Will the required QR code be on the webpage from 18th June?

A: Yes. When you login to ImmiAccount from the 18th of June, you will be prompted to setup MFA. If you select the 'Authenticator App' option when you are prompted to setup MFA, and will be shown a QR code on-screen.

Q: Will I need to re-install the app if I lose my mobile device?

A: Yes.

Functionality

Q: Can I change my existing ImmiAccount username?

A: No. Usernames are unique and cannot be changed. However, email addresses can be updated.

Q: Will ImmiAccount be able to handle so many logins?

A: ImmiAccount has gone through multiple testing phases, both internally and externally, domestically and internationally, including system load testing with no issues.

Q: Will my ImmiAccount get suspended or disabled if not used for a period of time (e.g. 6 months)? Particularly for clients who don't use it much.

A: As is currently the case, your ImmiAccount will not be suspended or disabled after a period of disuse; you will, however need to verify an email address again if ImmiAccount is not used for six months or more.

Third Party Software

Q: Is the department communicating with Third Party Software organisations?

A: The department has been communicating with a number of third party vendors such as, Migration Manager and Officio. The department does not take any responsibility for the use of third-party software, in line with ImmiAccount Terms and Conditions (Sections 3.1h and 4.5). Users should liaise with their third-party vendor to manage any necessary updates.

Other systems accessed via ImmiAccount

Q: Is the access to LEGENDcom also through MFA?

A: Yes. MFA will be required for all system access through ImmiAccount.

Q: Can I still go into ImmiAccount and also VEVO and LEGENDcom separately?

A: Yes. You can still access VEVO and LEGENDcom. You will need to MFA.

Timing

Q: Why is this change happening in June?

A: The Australian Government Cyber Security Act 2024 and 2023-2030 Australian Cyber Security Strategy aim to enhance Australia's cyber resilience. Government systems such as ImmiAccount are expected to urgently comply with the enhanced security measures and implement MFA where appropriate. The department will introduce MFA to ImmiAccount on 18 June 2025 to comply with data protection regulations. Organisations using MFA also demonstrate a commitment to security, which is often required by industry standards.