ImmiAccount Security Enhancements Multi-factor Authentication

Information for Organisations Using ImmiAccount

19 March 2025

The Department of Home Affairs is enhancing ImmiAccount security by introducing Multi-factor Authentication (MFA). MFA protects a user's ImmiAccount by adding a second layer of security in addition to a password, strengthens account security and aligns with Australian Government cyber security standards.

Authentication Options

New and existing users will be required to set up one of two authentication options. Authentication will be required each time users log in or make account changes to their ImmiAccount.

> **Option 1:** Use an authenticator app (e.g. Microsoft or Google Authenticator) on a mobile device or personal computer to generate a rotating 6-digit code to enter into ImmiAccount. This is the most secure and recommended option.

> **Option 2:** Receive a 6-digit email token to authenticate. The 6-digit code is sent to the registered email address. This option is available for users who cannot use an authenticator app.

Implementation Timeline

A testing phase will commence mid-May 2025 to help identify and resolve, any issues prior to the MFA full release. Participants will be asked to set up their MFA and login. They will receive support materials and be asked for their feedback. To volunteer for testing, email your **ImmiAccount username** to **MFA.Project.Launch@homeaffairs.gov.au** by 25 April 2025**.**

Please note, only individual user accounts (not shared or group emails) are eligible.

The full release of MFA is scheduled to commence in mid-June 2025 when MFA will become mandatory for all users.

Support & Resources

Once fully implemented, MFA support materials will be available on the Department's website located under Applying online in ImmiAccount. This information will be available in 16 languages.

Preparing for MFA

Do Not Share ImmiAccount User Credentials

Sharing ImmiAccount credentials is prohibited under the ImmiAccount Terms and Conditions (Sections 5.1 and 5.6). To ensure compliance and to maintain security, organisations should appoint one or more Organisation Account Administrators (OAAs) to manage staff access appropriately.

The OAA role enables authorised individuals within an organisation to:

- Approve access for new users
- Invite staff to create an account or assign additional OAAs
- Recover access in the event of a lost password or MFA
- Suspend inactive accounts
- Remove accounts from the organisation.

Important: All account holders can view applications under their organisation's 'Organisation Applications' section.

For instructions on setting up the OAA role, visit **Manage your organisation accounts** on the Department's website.

Third Party Software

Third-party software used to automate ImmiAccount processes may be impacted by the introduction of MFA. 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.

Frequently asked questions

Q: What if I do not have a smart phone or cannot use an authentication app?
A: You can use option 2: email token to authenticate. A 6-digit code is emailed to your registered email address.

Q: How long is the 6-digit authentication code valid?
A: 30 seconds via an authenticator app and 15 minutes via email token.

Q: Do I need to use MFA when accessing VEVO for Organisations or LEGENDcom?
A Yes. MFA will be required for all system access through ImmiAccount.

Q: My organisation uses an API to access VEVO for Organisation. Will MFA affect this?
A: No. If your organisation registered to use the VEVO B2B API, this will not change.

Q: Is the timeout feature inside ImmiAccount changing?
A: No. The inactivity timeout of 30 minutes and the hard session timeout of 4 hours remain, regardless of activity. This will not change as part of the MFA initiative.

Q: Can I change my existing ImmiAccount username?
A: No. Usernames are unique and cannot be changed. However, email addresses can be updated.

Q: Are the ImmiAccount Terms and Conditions changing?
A: Yes. The sharing of user credentials for VEVO organisations and LEGENDcom will no longer be allowed. All users will need their own individual ImmiAccount.