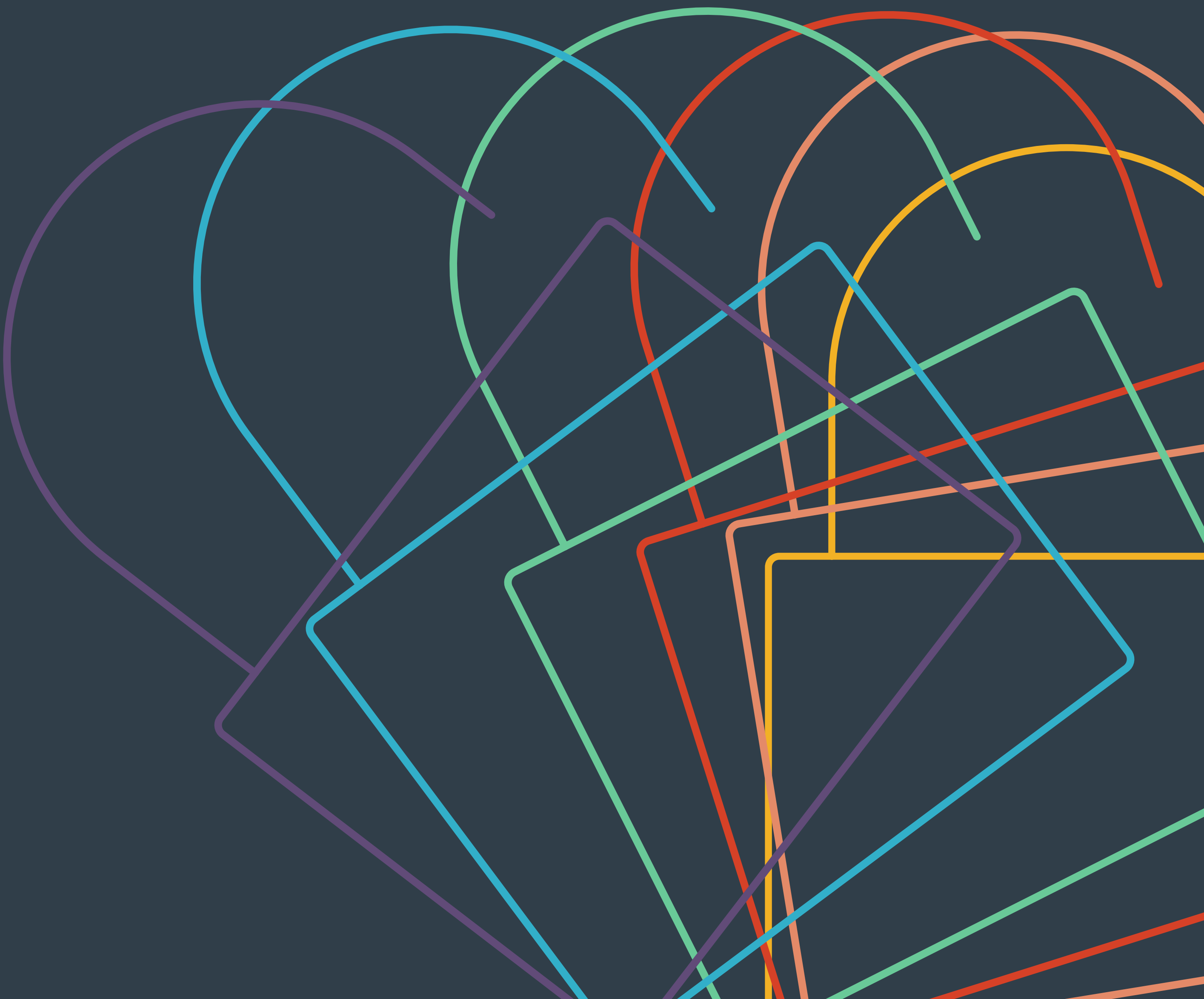
Australian Government
IP Australia

Multi-factor authentication user guide

For IP Australia's online services portal



Contents

About this guide

This guide is for anyone using our online services. It explains how to register and use multi-factor authentication (MFA) to securely access your account.

From **8 September 2025**, MFA will be **mandatory** for all users.

This guide is particularly relevant for:

- patent and trade marks attorneys
- business owners managing their own intellectual property (IP)
- legal representatives acting on behalf of clients
- any individual or organisation accessing IP Australia's online services.

The portal allows users to:

- apply for new IP rights (trade marks, patents, designs, plant breeder's rights)
- renew and manage existing IP rights
- view and respond to correspondence
- make secure payments
- update account and contact details.

More information about the portal can be found at Manage my IP.

Why you need MFA

Multi-factor authentication (MFA) is a security process that requires 2 or more verification factors to log in. It helps ensure that only authorised users can access an account, even if a password is compromised.

MFA usually combines:

- **something you know** – such as your password
- **something you have** – such as a one-time code from an app or security key.

IP Australia requires MFA to:

- align with Australian Government cybersecurity standards
- protect sensitive IP data
- reduce the risk of fraudulent activity.

MFA methods you can use

You can choose one of the following methods to set up MFA on the online services portal:

1. Authentication app (recommended)

A mobile authentication app that generates a time-based one-time passcode (TOTP). The 6-digit passcode refreshes every 30 seconds and are required at login.

App	Description	Support page	Google Play	Apple App Store
Google Authenticator	A widely used, simple, and lightweight authenticator app from Google.	Support	Google Play	App Store
Microsoft Authenticator	Feature-rich and supports TOTP, push notifications, and backup via Microsoft account.	Support	Google Play	App Store
Authy by Twilio	Offers encrypted cloud backup and multi-device support. Excellent for users with multiple phones.	Support	Google Play	App Store
FreeOTP	Open-source app developed by Red Hat. Minimalist, privacy-focused option.	Support	Google Play	App Store
Okta Verify	Ideal for users working in enterprise environments that use Okta Identity Services.	Support	Google Play	App Store

Any other authenticator app that supports the standard TOTP protocol (RFC 6238) will alsowork, including:

- 1Password
- Duo Mobile
- LastPass Authenticator.

Note: Authenticator apps don't transfer automatically to new devices unless you've enabled a backup feature (available in apps like Microsoft Authenticator and Authy).

2. Security key

An FIDO2/WebAuthn-compliant security key is a hardware device you connect to your computer or phone to login to systems and applications.

This can be:

- a USB device (for example, YubiKey)
- biometric device (for example, a fingerprint reader or facial recognition)
- an NFC-enabled token (tap the device against your phone or computer to verify).

These are supported if your browser and system support WebAuthn security keys.

Recovery code

During MFA setup, a one-time recovery code will be generated. This is your backup access method if your app or device is lost. Your recovery code:

- is shown only once during setup
- should be stored offline or in a secure password manager
- is valid for **one use only.**

It is important to save your Recovery Code in a safe place during initial set up. If you lose access to your account, you will be able to use the Recovery Code to log in on a different app or device. If you have not kept a copy of your Recovery Code and lose access to your account, you will need to call the Contact Centre on 1300 651 010 (9am to 5pm AEDT, Monday to Friday) to reinstate access.

When you log in with a recovery code, online services will issue a new one. Save the new code securely as it replaces the old one.

Note: Email-based MFA isn't currently supported for online services. If you lose your recovery code, you can call the Contact Centre during business hours to have your MFA reset.

Important information before you start

Before you register for MFA, make sure you do the following.

- Go to your email settings and **add @ipaustralia.gov.au to your list of safe senders** to avoid missing important notifications.
- **Download and install your chosen authentication app** prior to starting MFA registration (if using an app-based method).
- **Keep your browser session open.** If you close it, setup will resume when you next log in.
- Record your recovery code in a password manager or offline document. Once generated, your recovery code will be shown only once.

One account, multiple users (corporate account)

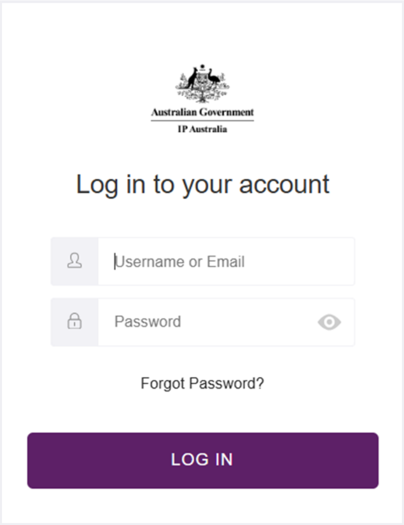
If your business currently shares login details for a single user account across multiple users, you'll need to switch to a corporate account. This ensures each user can authenticate on their own device.

To switch, call our Contact Centre on 1300 651 010.

Registering for MFA and choosing an authentication method

Step 1: Log in to the online services portal

- Visit online services.
- Enter your username/email and password.
- Select **LOG IN.**



Australian Government
IP Australia

Log in to your account

Username or Email

Password

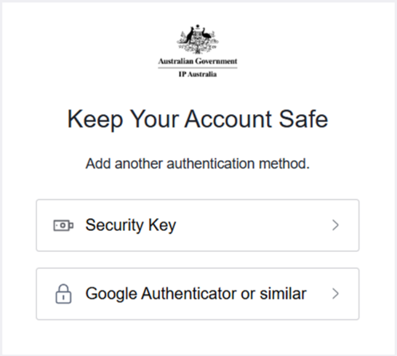
Forgot Password?

LOG IN

Step 2: Choose your authentication method

Next, the system will prompt you to set up MFA.

- Select **Google Authenticator or similar** for app-based codes.
- Select **Security key** if using a physical security device.



Australian Government
IP Australia

Keep Your Account Safe

Add another authentication method.

Security Key

Google Authenticator or similar

Step 3: Set up the authentication app

- Open your authentication app and select **Add Account** (or tap the “+” symbol – wording may vary).
- Use your phone’s camera to scan the QR code displayed on the portal.
- If you can’t scan – manually enter the setup key shown below the QR code.
- Your app will now generate a new 6-digit code every 30 seconds.

For help with your setup, see the support links listed under ***Authentication app (recommended).***

Note: Every time you visit the QR code screen on the portal, a new unique setup key is generated. If you return to the setup screen later, you must re-scan the updated code and remove the previous account entry from your authentication app.

Step 4: Enter the one-time code

- Enter the current 6-digit code from your app into the field provided.
- Select **Continue.**

Step 5: Save your recovery code

- You will be presented with a unique, single-use recovery code.
- Copy or write this down and store it in a secure location (for example, password manager or offline).
- Confirm by ticking **I have safely recorded this code.**
- Select **Continue** to complete setup.

Confirmation and email notification

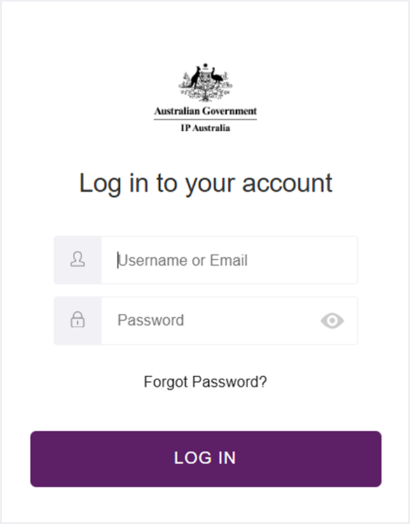
- A success message will appear on screen.
- A confirmation email will be sent to your registered address.
- Your account is now MFA protected.

Logging in with MFA enabled (authentication app)

Once MFA is configured, you'll need to complete an additional verification step every time you log in.

Step 1: Log in to the online services portal

- Visit online services.
- Enter your username/email and password.
- Select **LOG IN.**



Australian Government
IP Australia

Log in to your account

Username or Email

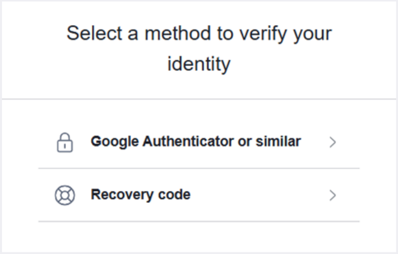
Password

Forgot Password?

LOG IN

Step 2: Provide the authentication code

- Select Google Authenticator or similar

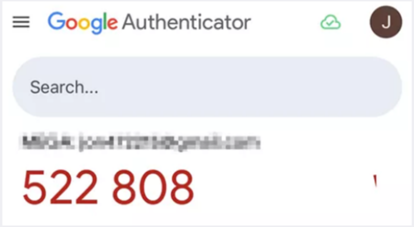


Select a method to verify your identity

Google Authenticator or similar >

Recovery code >

- Open your authenticator app and locate the 6-digit code.
- Example from *Google Authenticator:*



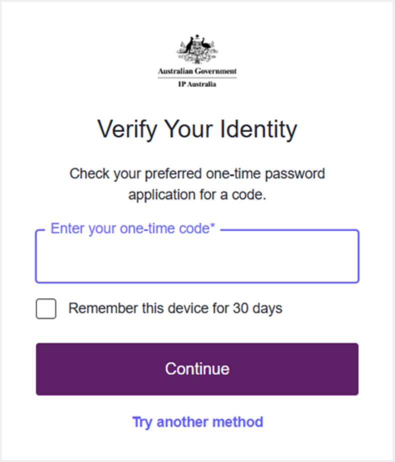
Google Authenticator

Search...

[redacted]

522 808

- Enter the 6 digits into the one-time code field (30-second limit before refresh)

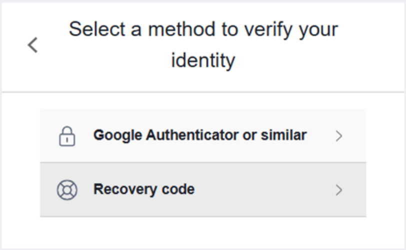

Australian Government
IP Australia
Verify Your Identity
Check your preferred one-time password application for a code.
Enter your one-time code*
□ Remember this device for 30 days
Continue
Try another method

- Tick **Remember this device for 30 days** – only on trusted devices (optional).
- Select **Continue** to access your account.

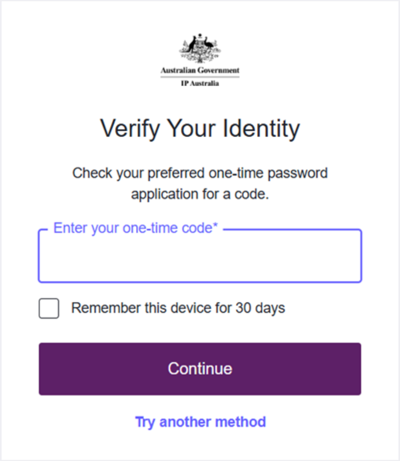
Alternate login using recovery code

If you lose access to your authenticator app:

- Select **Try another method**.
- Select **Recovery code**.


Select a method to verify your identity
Google Authenticator or similar
Recovery code

- Enter the recovery code you saved during setup.


Australian Government
IP Australia
Verify Your Identity
Check your preferred one-time password application for a code.
Enter your one-time code*
□ Remember this device for 30 days
Continue
Try another method

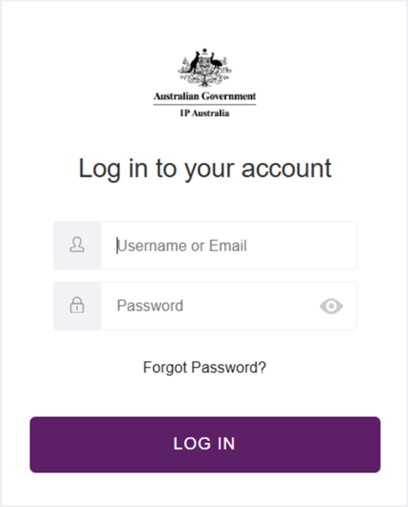
- Select **Continue.**

Reminder: Each recovery code is valid for one-time use only. When you log in with a recovery code, online services will issue a new one. Save the new code securely as it replaces the old one.

Registering for MFA using a security key

Step 1: Log in to the online services portal

- Visit online services.
- Enter your username/email and password.
- Select **LOG IN.**



Australian Government
IP Australia

Log in to your account

Username or Email

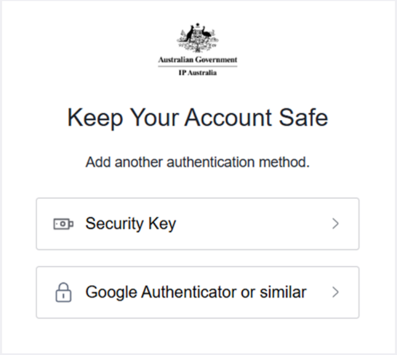
Password

Forgot Password?

LOG IN

Step 2: Provide the authentication code

- Select **Security Key** when prompted to set up MFA.
- Select **Continue**.



Australian Government
IP Australia

Keep Your Account Safe

Add another authentication method.

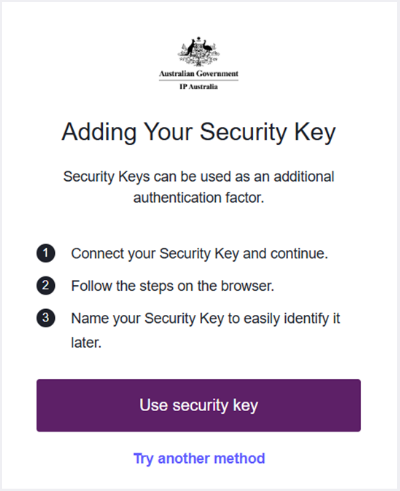
Security Key

Google Authenticator or similar

Step 3: Connect your security key

The system will present instructions for registering your security key.

- Insert or connect your security key to your device
  - Follow the steps in your browser.
  - Name your security key to help identify it later.
  - Select **Use security key.**



Australian Government
IP Australia

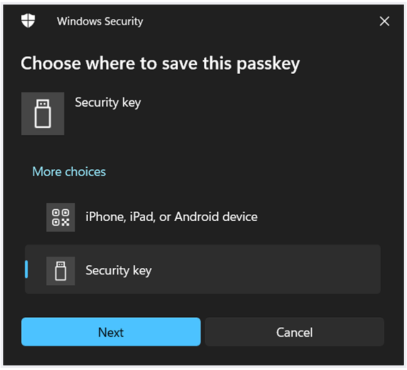
Adding Your Security Key

Security Keys can be used as an additional authentication factor.

1. Connect your Security Key and continue.
2. Follow the steps on the browser.
3. Name your Security Key to easily identify it later.

Step 4: Choose where to save the passkey

- A prompt from your operating system will appear.
- Select **Security key** (for USB or NFC devices) and then **Next.**

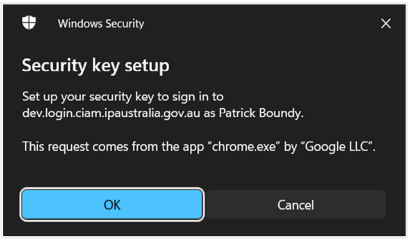


Windows Security

Choose where to save this passkey

Step 5: Complete security key set up in the browser

- When prompted, confirm that you want to set up your security key for the IP Australia online services portal.
  - Select **OK**.



Windows Security

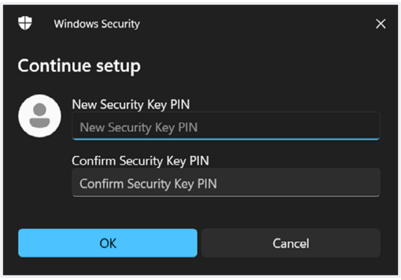
Security key setup

Set up your security key to sign in to dev.login.ciam.ipaustralia.gov.au as Patrick Boundy.

This request comes from the app "chrome.exe" by "Google LLC".

Step 6: Create a security key PIN

- If you haven't previously set a PIN on your security key, you will be asked to create one.
- Enter and confirm the new PIN.
- Select **OK**.


Windows Security

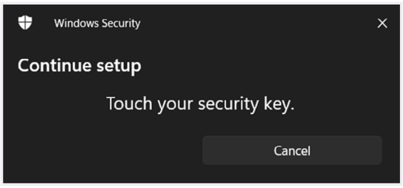
Continue setup

New Security Key PIN: New Security Key PIN

Confirm Security Key PIN: Confirm Security Key PIN

Step 7: Touch your security key

- When prompted, physically interact with your security key (for example, press the button or touch the sensor) to complete the registration.

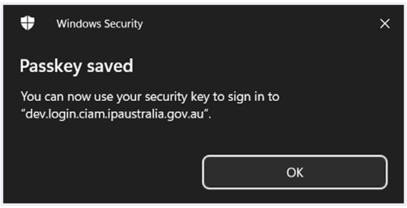

Windows Security

Continue setup

Touch your security key.

Step 8: Confirm setup

- Once the process is complete, you will see a confirmation that your passkey has been saved and can now be used to sign in to the portal.
- Select **OK**.

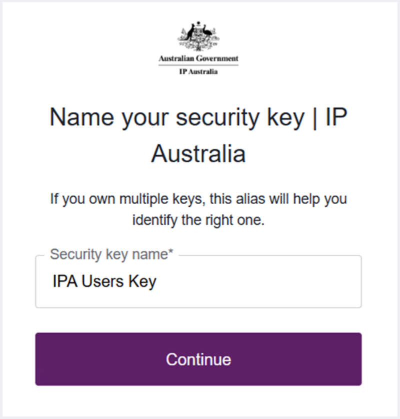

Windows Security

Passkey saved

You can now use your security key to sign in to "dev.login.ciam.ipaustralia.gov.au".

Step 9: Name your security key

- Enter a name for your security key (for example, IP Australia trade mark key) to help identify it if you have multiple keys.
- Select **Continue.**


Australian Government
IP Australia

Name your security key | IP Australia

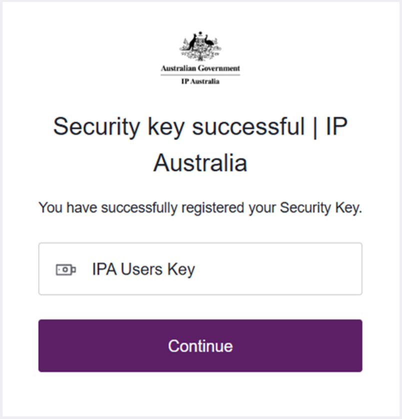
If you own multiple keys, this alias will help you identify the right one.

Security key name*: IPA Users Key

Step 10: Confirm set up and save recovery code

The portal will display a confirmation message stating that your security key has been successfully registered:

- Select **Continue**.

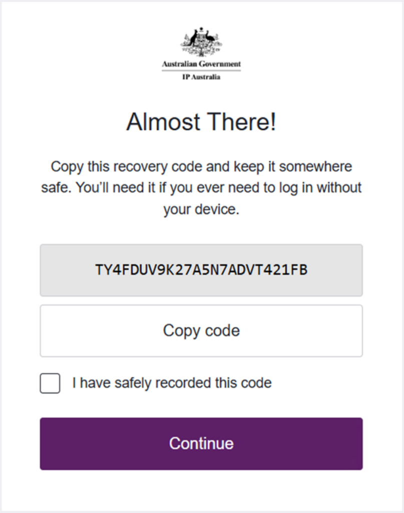


Australian Government
IP Australia

Security key successful | IP Australia

You have successfully registered your Security Key.

A unique, single-use recovery code will be shown:



Australian Government
IP Australia

Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.

TY4FDUV9K27A5N7ADVT421FB

- Copy this code or write it down and store it in a secure location, such as a password manager or offline document.
- Tick **I have safely recorded this code** to confirm.
- Select **Continue** to complete your MFA setup.

Your security key is now registered for MFA.

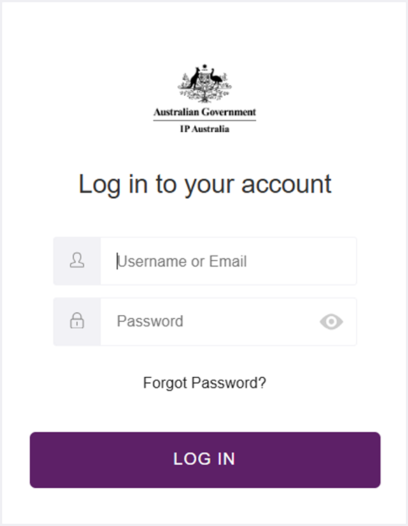
Reminder: Each recovery code is valid for one-time use only. When you log in with a recovery code, online services will issue a new one. Save the new code securely as it replaces the old one.

Logging in with MFA enabled (security key)

Once MFA is configured, you'll need it every time you log in.

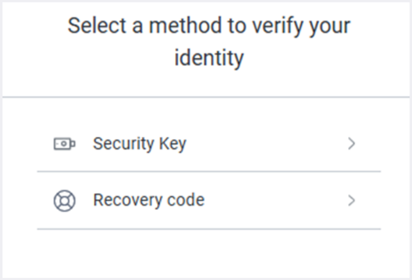
Step 1: Enter your credentials

- Visit online services.
- Enter your username/email and password.
- Select **LOG IN.**

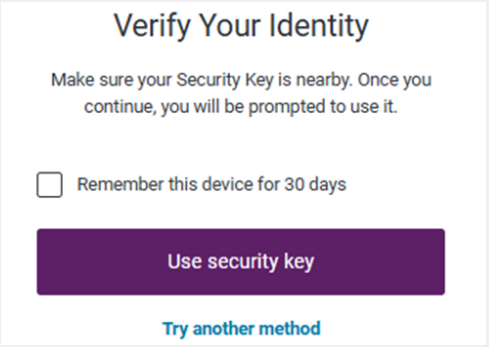


Step 2: Select authentication method

- Select **Security Key** as your method to verify your identity.



- When prompted, select **Use Security Key**.

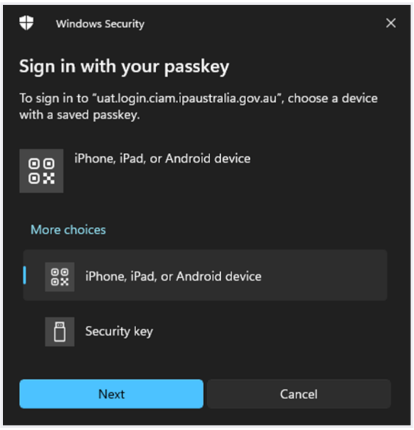


Verify Your Identity

Make sure your Security Key is nearby. Once you continue, you will be prompted to use it.

Step 3: Verify with your security key

- You will be presented with a Windows Security prompt.



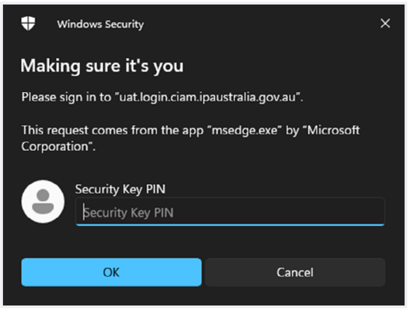
Windows Security

Sign in with your passkey

To sign in to "uat.login.ciam.ipaustralia.gov.au", choose a device with a saved passkey.

iPhone, iPad, or Android device
More choices
iPhone, iPad, or Android device
Security key
Next
Cancel

- Select **Security Key** and continue with **Next** (wording may vary depending on your operating system or browser).
- Enter your **Security Key PIN** when prompted and select **OK**.



Windows Security

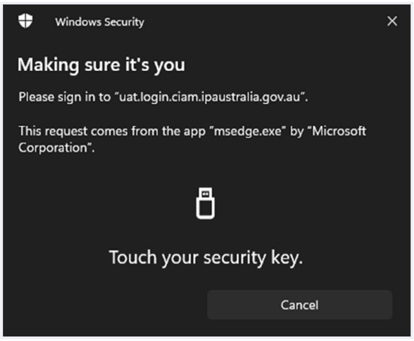
Making sure it's you

Please sign in to "uat.login.ciam.ipaustralia.gov.au".

This request comes from the app "msedge.exe" by "Microsoft Corporation".

Security Key PIN

- Touch your security key (for example, press the button or touch the sensor) when prompted.



Windows Security

Making sure it's you

Please sign in to "uat.login.ciam.ipaustralia.gov.au".

This request comes from the app "msedge.exe" by "Microsoft Corporation".

Touch your security key.

You have now successfully logged in to your account.

Changing or resetting your MFA method

Once your MFA is registered, you can't change it yourself through online services. If you need to switch methods (for example, moving from an app to a security key, or changing phones), you'll need to request a reset.

You should request a reset if:

- you've purchased a new mobile phone and didn't transfer your existing authenticator app
- you've reset or uninstalled your authenticator app without backup
- you want to switch from one MFA method to another
- you've lost access to your app and don't have your recovery code
- you've had a security incident and need to reset your MFA method.

Get in touch for MFA reset support. You can find our details on the Contact us page.

Troubleshooting

Issue	Resolution
Code expired	Wait for the next 30-second cycle and enter a new code.
Incorrect code	Check your app time settings and try again with new code.
Locked out after 5 failed attempts	Wait 15 minutes, then try logging in again.
QR code doesn't scan	Enter the setup key manually.
Didn't save recovery code	Call IP Australia support to verify your identity and request an MFA reset.
Lost device	Use recovery code or contact support.