Australian Government

Tuition Protection Service

Multi-factor authentication fact sheet

This fact sheet provides general information about multi-factor authentication (MFA), which will be a requirement for users to access Tuition Protection Service (TPS Online).

What is MFA?

MFA is one of the most effective ways to protect your information and account against unauthorised access. MFA is a cyber security measure that requires users to provide 2 or more proofs of identity to grant access to an account or application. Usually this is a password and a one-time use code generated by an authentication mobile app or sent to your email address.

You may be already using MFA, for example when you receive an authentication code by SMS text message or by email after entering your password to log into an online account. TPS Online MFA will be similar.

Why is MFA being implemented on TPS Online?

MFA is one of the best ways to protect against someone accessing your account by adding an extra layer of protection. MFA helps make your information more secure. Taking the extra step beyond just a password improves protection of your entities' information from potential hackers.

When will MFA be implemented on TPS Online?

Users accessing TPS Online will need to activate and then use MFA. Further information will be available soon on the TPS Online home page and on the TPS website. This information will guide you through the new process to access TPS Online.

What can I do now to prepare for MFA?

Decide whether to use email or a mobile app to receive authentication codes. You may need to review which authenticator is the best method for you.

If using a mobile app, download a compatible authentication mobile app from your chosen app store. The options are:

- Microsoft Authenticator
- Google Authenticator
- Duo
- FreeOTP.

Which email address should I use for MFA?

If you register to use MFA through an email, your email address registered in your TPS Online user profile and will be used to send the one-time use code to you when you log on. We strongly recommend that you use an email address that only you have access to. You should not use a shared email address.

What are the password requirements?

When logging in for the first time with temporary password, you will automatically be prompted to choose a new password. Your new password must be a strong password containing at least **14 characters**.

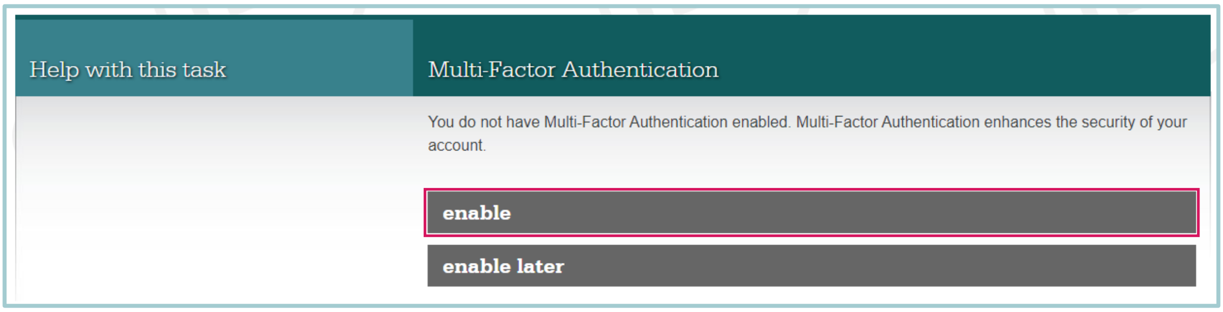
You are required to change your password:

- the first time you log onto the system, as you are only provided with a temporary password; or
- after your password has been reset by the TPS Support Team; or
- if your password expires.

For more information, please refer to the Australian Cyber Security Centre's Protect Yourself webpage for their advice on passwords.

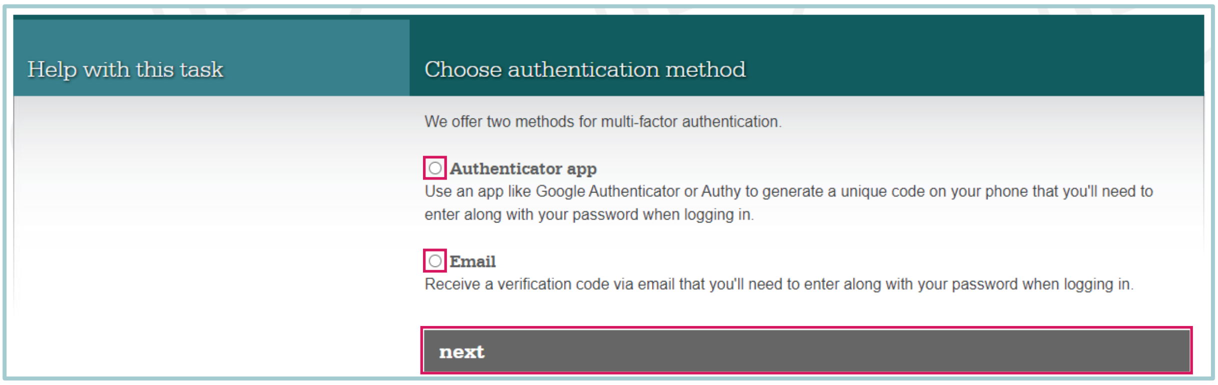
How do I enable MFA?

- To set up MFA, log into TPS Online.
- A 'Multi-Factor Authentication' task will appear on your home page.
- Click ***enable***



You do not have Multi-Factor Authentication enabled. Multi-Factor Authentication enhances the security of your account.

- You must indicate whether you would like to receive one-time codes through an authenticator application or via email
- Select **one of the circles** next to your preferred method, then press ***next***



We offer two methods for multi-factor authentication.

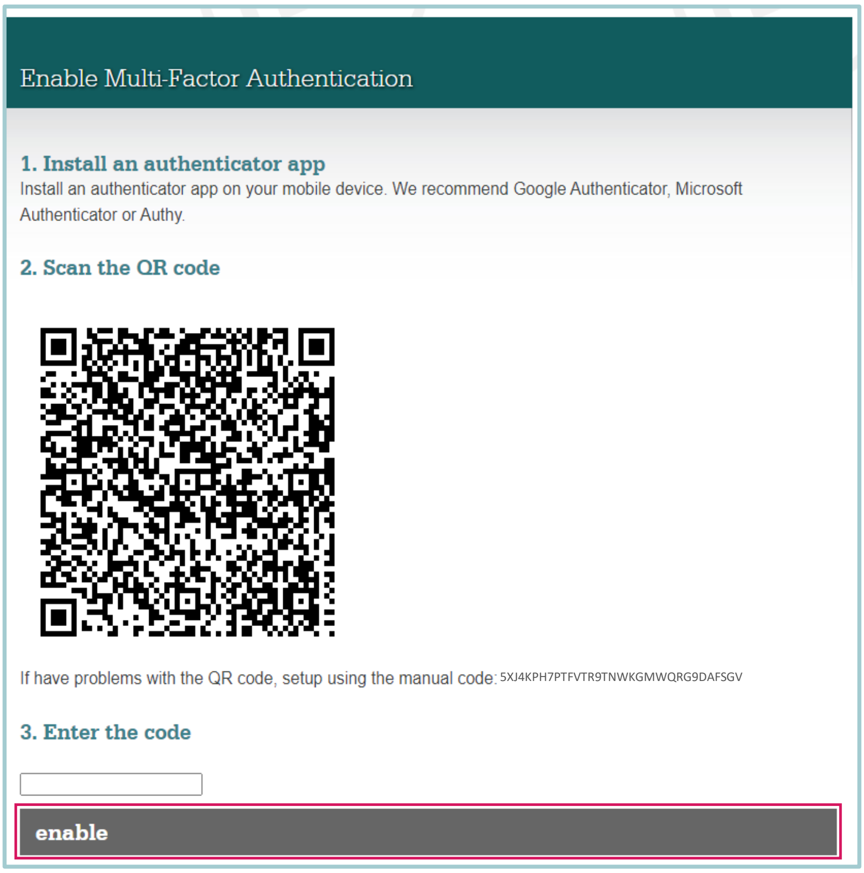
○ **Authenticator app**

Use an app like Google Authenticator or Authy to generate a unique code on your phone that you'll need to enter along with your password when logging in.

○ **Email**

Receive a verification code via email that you'll need to enter along with your password when logging in.

- If the authenticator app option is selected, you will be prompted **to install an authenticator application** on your smart phone
- **Scan the QR code on your screen**. A one-time verification code will be generated by your authenticator application.
- **Enter the code**, then press ***enable***



Enable Multi-Factor Authentication

1. Install an authenticator app

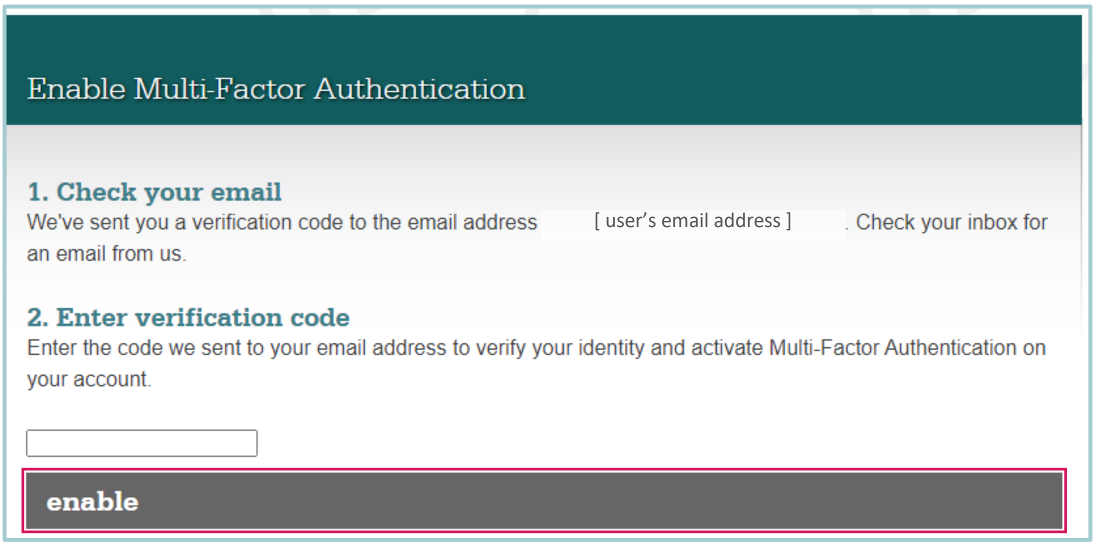
Install an authenticator app on your mobile device. We recommend Google Authenticator, Microsoft Authenticator or Authy.

2. Scan the QR code

If have problems with the QR code, setup using the manual code: 5XJ4KPH7PTFVTR9TNWKGMWQRG9DAFSGV

3. Enter the code

- If the email option is selected, a one-time verification code will be emailed to you
- **Enter the code** emailed to you, then press ***enable***



Enable Multi-Factor Authentication

1. Check your email

We've sent you a verification code to the email address [user's email address] . Check your inbox for an email from us.

2. Enter verification code

Enter the code we sent to your email address to verify your identity and activate Multi-Factor Authentication on your account.

- Once MFA has been set up, you will need to enter a one-time verification code every time you log into TPS Online
- Visit TPS Online and **enter your username and password**
- You will then be prompted to enter the one-time verification code generated by your authenticator application or emailed to you
- Once you **enter the code**, you will be able to access your TPS Online account

Where can I go for help with MFA?

More information is coming. Keep an eye on your inbox or on the TPS website for updates.

Need MFA support?

The TPS is here to help. Contact us by:

- email: support@tps.gov.au
- phone: 1300 131 798