Enable Two-Step authentication

> ***NOTE***
>
> Two-Step Verification may also be known as Multi-Factor Authentication (MFA).
>
> Two-Step Verification is enforced on all Manager Accounts.
>
> A verified email address will need to be set as the account user ID before enabling Two-step verification on the account

The following steps outline how a user can authenticate their device.

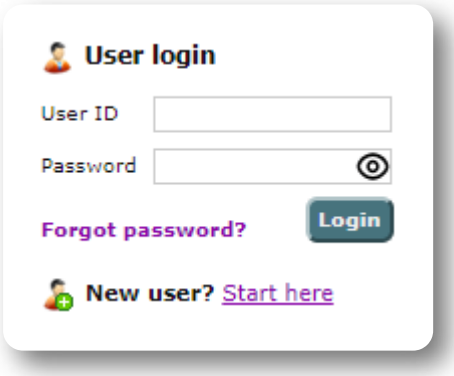
Please note the following:

‣ Do not select public devices/hardware as 'a trusted device'.

‣ A user is required to complete the full validation process on their first login. After the first login attempt users will then have the option to select 'This is a trusted, secure device' before logging in. This option means users will not have to validate before every login attempt after that, but only occasionally.

How to enable Two-Step Verification:

1. Login to Maxcourse with your user ID and password



2. You will need a mobile device with an authentication app installed.

   Maxcourse is compatible with most authenticator apps such as:

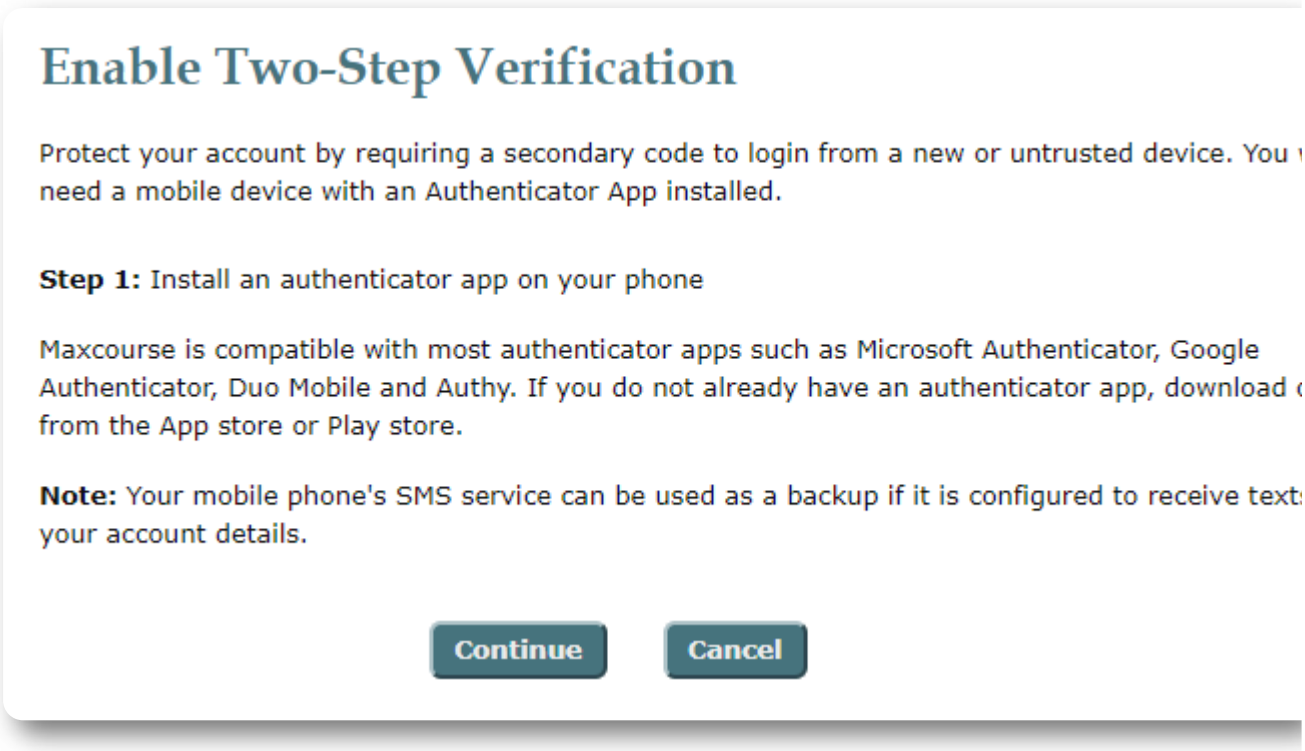
   ‣ Microsoft Authenticator

   ‣ Google Authenticator

   ‣ Duo Mobile

   ‣ Authy

   When you have a mobile device with an authentication app installed, select continue.



3. Using your **authentication app**, add your Maxcourse account.

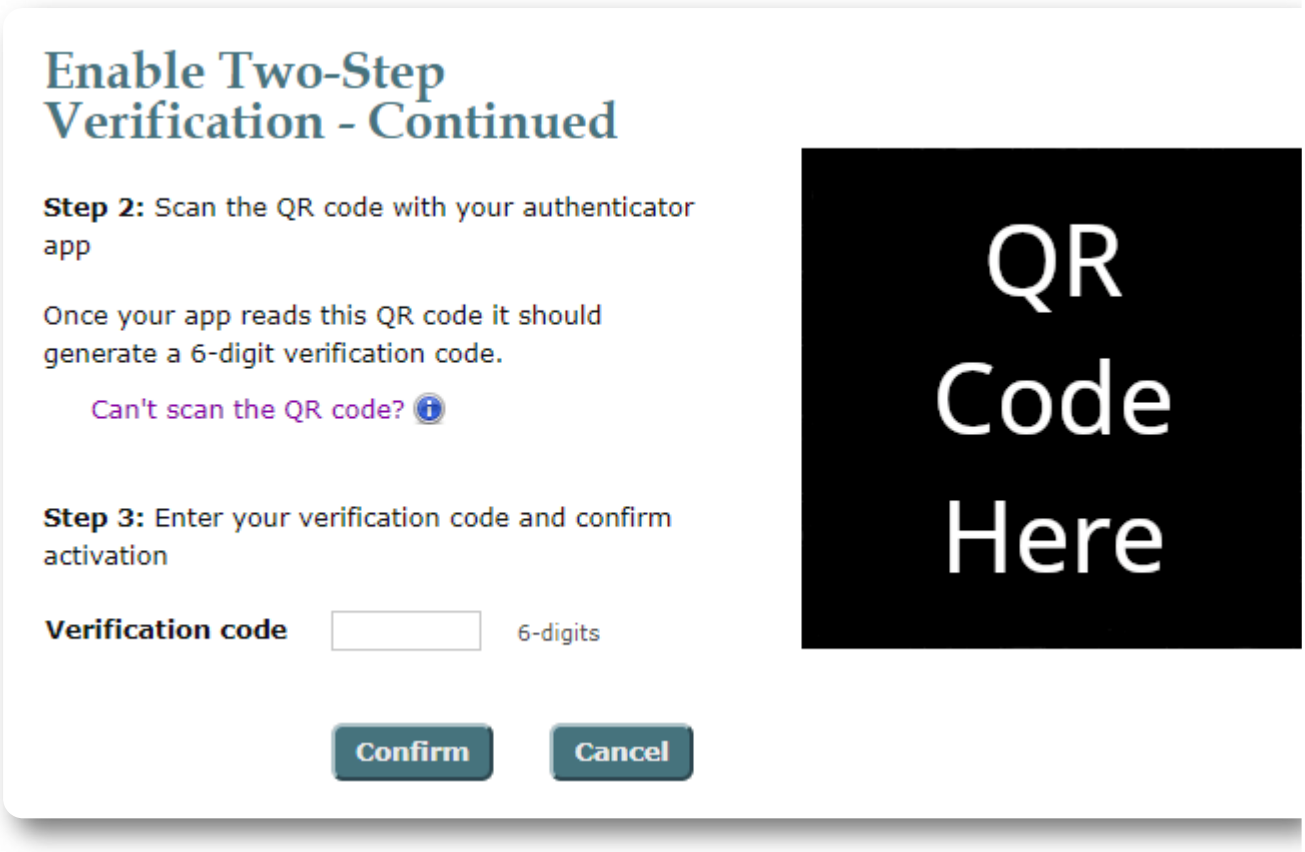
For example, you can do this:

For Microsoft authenticator, select the plus button.

For Google authenticator, select the plus button.

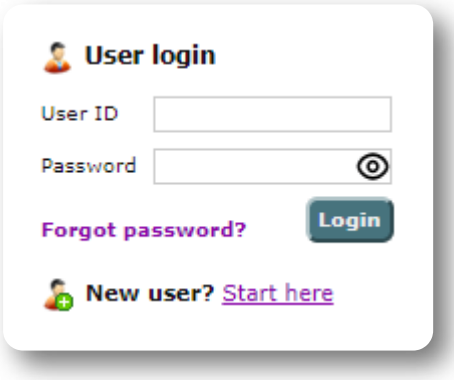
Once you have selected the option to app an account, there will be the ability to scan a QR code.

After scanning the QR code, you will be able to see a verification code. Entre the 6-digit verification code and then select confirm.



4. After you have logged in, log out of your account.

5. Log back into your account.



6. On the User Login - Two-Form Verification page, entre the updated 6-digit verification code.

If you are on a trusted device which is not public, select the check box to trust this device. Enabling this option will reduce the number of times you need to use this secondary validation method.

NOTE

A trusted device is one that requires a personal login to access and is kept secure.

This will finalise the secondary verification process.

Benefits of enabling Two-Step Verification

Using two methods of authentication enhances the security of a system, protecting your personal data - which may include personal identification or financial assets—from being accessed by an unauthorised third party that may have been able to discover, for example, a single password.