

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

The screenshot shows a login interface with the title 'User login' and a user icon. It contains two input fields: 'User ID' and 'Password'. The 'Password' field has a toggle icon (an eye) to the right. Below the fields is a 'Login' button. To the left of the button is a link 'Forgot password?'. At the bottom, there is a link 'New user? Start here' with a plus icon.

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.

Enable Two-Step Verification

Protect your account by requiring a secondary code to login from a new or untrusted device. You need a mobile device with an Authenticator App installed.

Step 1: Install an authenticator app on your phone

Maxcourse is compatible with most authenticator apps such as Microsoft Authenticator, Google Authenticator, Duo Mobile and Authy. If you do not already have an authenticator app, download it from the App store or Play store.

Note: Your mobile phone's SMS service can be used as a backup if it is configured to receive text messages with your account details.

Continue

Cancel

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 add 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. Enter the 6-digit verification code and then select confirm.

Enable Two-Step Verification - Continued

Step 2: Scan the QR code with your authenticator app

Once your app reads this QR code it should generate a 6-digit verification code.

[Can't scan the QR code?](#) 

Step 3: Enter your verification code and confirm activation

Verification code 6-digits


Confirm

Cancel


QR
Code
Here

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


5. Log back into your account.

 **User login**

User ID

Password 

[Forgot password?](#)

 **New user?** [Start here](#)

6. On the User Login - Two-Form Verification page, enter 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.

User Login - Two-Form Verification

Please enter the 6-digit one time verification code generated by your authenticator app.

Verification code

6-digits

☒ This is a trusted, secure device ⓘ

Login

Cancel

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.