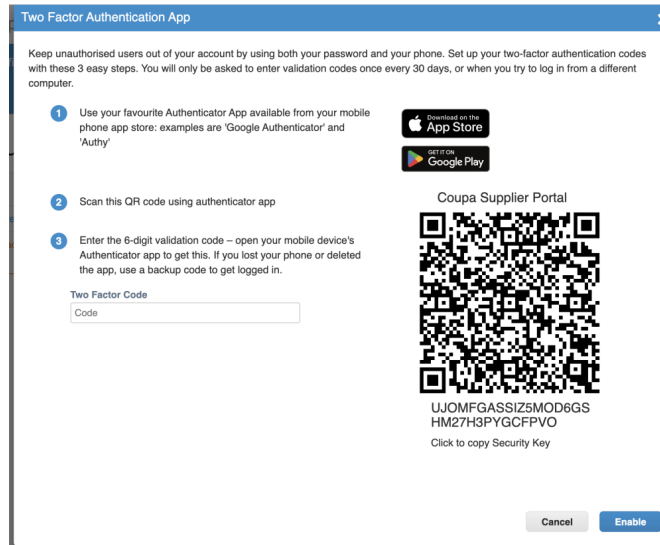




Two-Factor Authentication

How to set-up your two-Factor Authentication in your CSP

This guide will help you set-up two-factor authentication in your Coupa supplier portal (CSP). This is a Coupa Requirement to protect your company information.



Two-Factor Authentication for financial data

To ensure that your data is secure, Coupa have implemented Two-Factor Authentication (2FA) for all sensitive data.

To increase the security of your payment settings in Coupa, two-factor authentication is mandatory for sensitive payment accounts and/or sensitive account updates, such as changes to your legal entity, remit to and bank account information.

If you Don't have a Mobile Phone or Tablet: go to section 6

When you enable multi-factor authentication, you can choose from the following options:

- **For Payment Changes (Required for Changing Legal Entity or Remit-To):** Multi-factor authentication is required when creating or editing legal entities, remit-to, and bank account information.
- **For Both Account Access (Login) and Payment Changes:** Multi-factor authentication is required when logging in to the CSP. You don't have to reauthenticate when working with financial data because you already authenticated when logging in.

Depending on how you want to receive the verification codes, select one of the following options and set your preference as the default.

- **Via Authenticator App** to use an authenticator app available from the app store on your mobile phone.
- **Via Text Message** to use a code sent by text message to your phone number.

1.

How to Find 2FA

If you're setting up new or amending Two-Factor Authentication can be found by going to your name at the top right-hand side.

Click on your name and a pop up will appear, select Account settings.

My Account Settings will open

Select Security & Two-Factor Authentication

The screenshot shows the SIMON user interface. At the top left, the SIMON logo is highlighted with a red box. To its right are 'NOTIFICATIONS 3' and 'HELP'. Below the logo is the 'My Account Settings' section. A sidebar on the left contains 'Settings', 'Notification Preferences', and 'Security & Two-Factor Authentication', with the latter highlighted by a red box. The main content area is divided into two sections: 'User Details' and 'Change Password'. The 'User Details' section includes input fields for First Name (Simon), Last Name (Hunt), Email (testsuppliersh@gmail.com), Department, and Role, with a 'Save' button below. The 'Change Password' section includes input fields for Current Password, Password, and Password Confirmation, with a 'Save' button below. A note below the Password field states: 'Use at least 8 characters and include a number and a letter.'

2.

'Two Factor Authentication App'

Once you have selected Security & Two-Factor Authentication, the Two Factor Authentication App page opens.

If you have or want to set up the Authentication App on your mobile phone, please follow the instructions.

(you must have the app open before you can scan the QR code)

If you don't want to use the App and want to use SMS click the cancel button.

Two Factor Authentication App

Keep unauthorised users out of your account by using both your password and your phone. Set up your two-factor authentication codes with these 3 easy steps. You will only be asked to enter validation codes once every 30 days, or when you try to log in from a different computer.

- 1 Use your favourite Authenticator App available from your mobile phone app store: examples are 'Google Authenticator' and 'Authy'
- 2 Scan this QR code using authenticator app
- 3 Enter the 6-digit validation code – open your mobile device's Authenticator app to get this. If you lost your phone or deleted the app, use a backup code to get logged in.



Coupa Supplier Portal



MQW5BFFHJLF4GCQGP
UFUGM7W5LS4R6P6

Click to copy Security Key

Two Factor Code

Cancel

Enable

3.

'My Account security & Two-Factor Authentication'

You now have the option to set up SMS
Select the option you want for Two-Factor Authentication

(Recommended is Enable only for payment changes (Required for Legal Entity or Remit-To)

Tick Enable box for SMS

My Account Security & Two-Factor Authentication

[Settings](#)

[Notification Preferences](#)

[Security & Two-Factor Authentication](#)

Two-Factor Authentication

Enable only for Payment Changes (Required for changing Legal Entity or Remit-To)

Enable for Both Account Access (Login) and Payment Changes

Via Authenticator App Enabled

Enabled Using an Authenticator App available from your mobile phone app store

[Change Authentication App](#)

Via SMS Disabled

Enable Using SMS, a code will be sent to your mobile phone number. Enter verification code when prompted and select OK. SMS rates apply.

Show Recovery Codes

Regenerate Recovery Codes

4.

'Verify your mobile phone'

A pop-up box will appear asking for your mobile number.

Click the drop-down arrow on the phone number box, select your country and then enter your mobile number without the pre-leading zero

Select I'm not a robot.

Click send Code.

You will receive a text message with a 6-digit verification code, enter the code and click Enable.

The screenshot shows a 'Multi-factor Authentication by Phone' dialog box with a blue header and a close button (X) in the top right corner. The dialog is divided into three numbered steps:

- Step 1:** 'A code will be sent to your phone as an SMS Text Message (SMS rates may apply).' To the right is a 'Phone Number' field with a dropdown arrow and '+1' selected.
- Step 2:** 'Confirm Recaptcha'. Below this is a reCAPTCHA widget with an 'I'm not a robot' checkbox and the reCAPTCHA logo. To the right of the widget is a 'Send Code' button.
- Step 3:** 'Enter the 6-digit verification code sent to your phone.' Below this is an empty text input field.

At the bottom of the dialog are two buttons: 'Cancel' and 'Enable'.

5.

'Save your backup Codes'

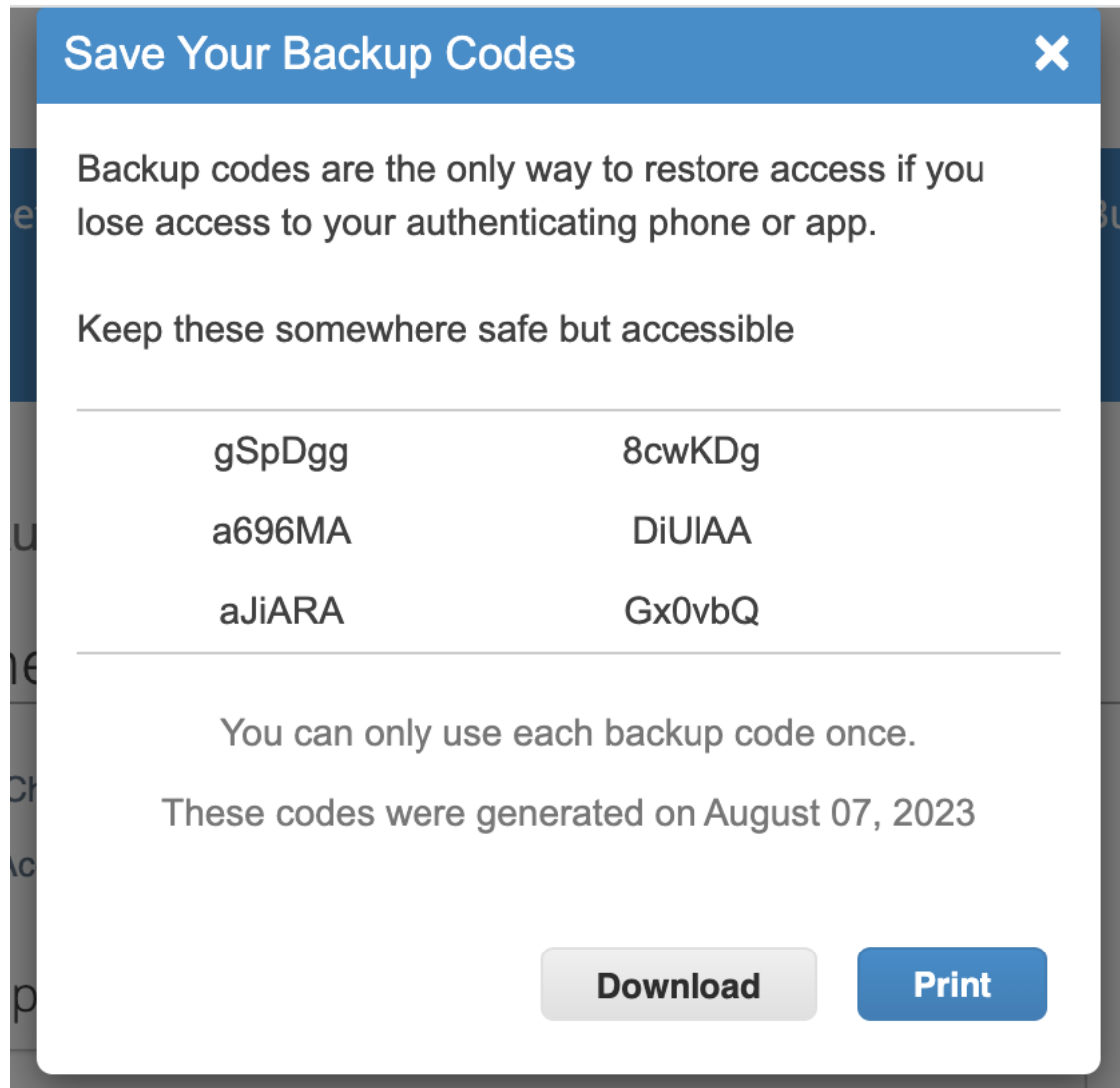
You will have this Pop-up save your Backup Codes

You can use one of the options to save or take a photo of your backup codes, If you ever loose your device, you will need these to regain access to your CSP account.

Once done close it by using the cross in the top right-hand corner

Your My Account Security & Two-Factor Authentication is now set up

Click the Home Button in the big blue bar to return to the Home screen.

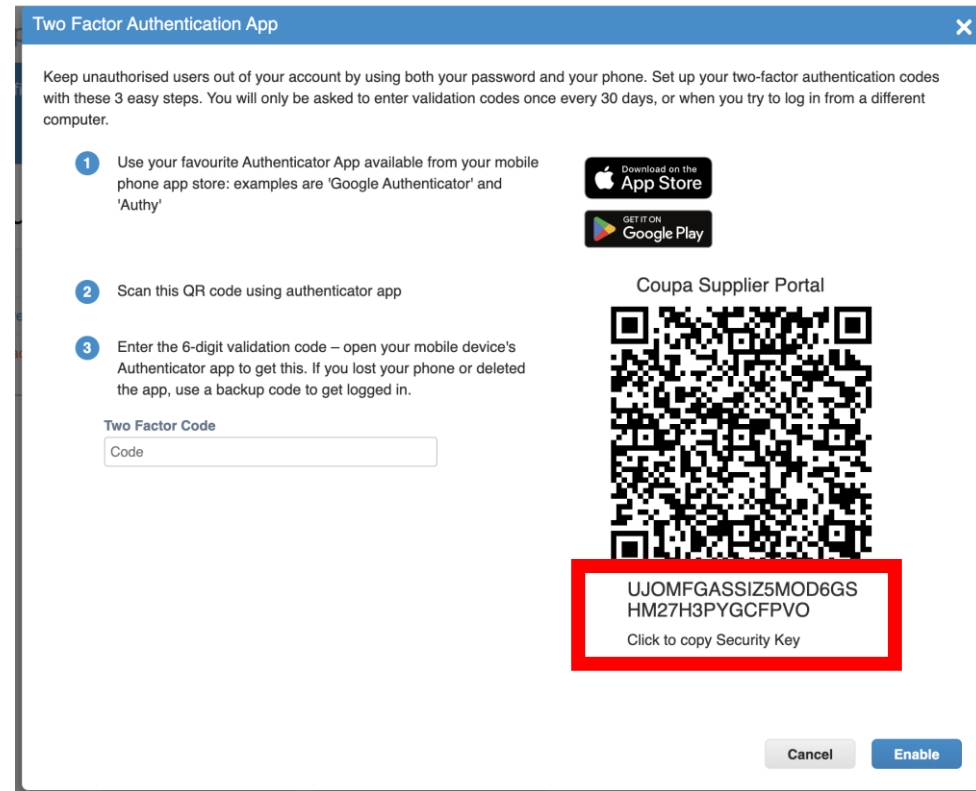


6.

'I don't have a Mobile device'

You can enable multi factor authentication through an authenticator app by using a browser extension listed below,

- Add the relevant extension to your browser:
- **Google Chrome** extension [authenticator](#). For more information, see [Install Google Authenticator](#).
- **Mozilla Firefox** extension [authenticator](#)
- **Microsoft Edge** extension [authenticator](#)
- Add the [authenticator](#) to your browser.
- Scan the QR code or copy the security key from the CSP page to the authenticator extension.
- Enter the Two Factor Code



For all Coupa supplier help and guides Click [here](#) for Mitie Suppliers website.