Delta
eSourcing

# Multi-Factor Authentication guidance

## Setting up multi-factor authentication

Below is a step-by-step guide on how to set-up MFA on Delta when you login.

We recommend you download either Google or Microsoft's authenticator app on your device.

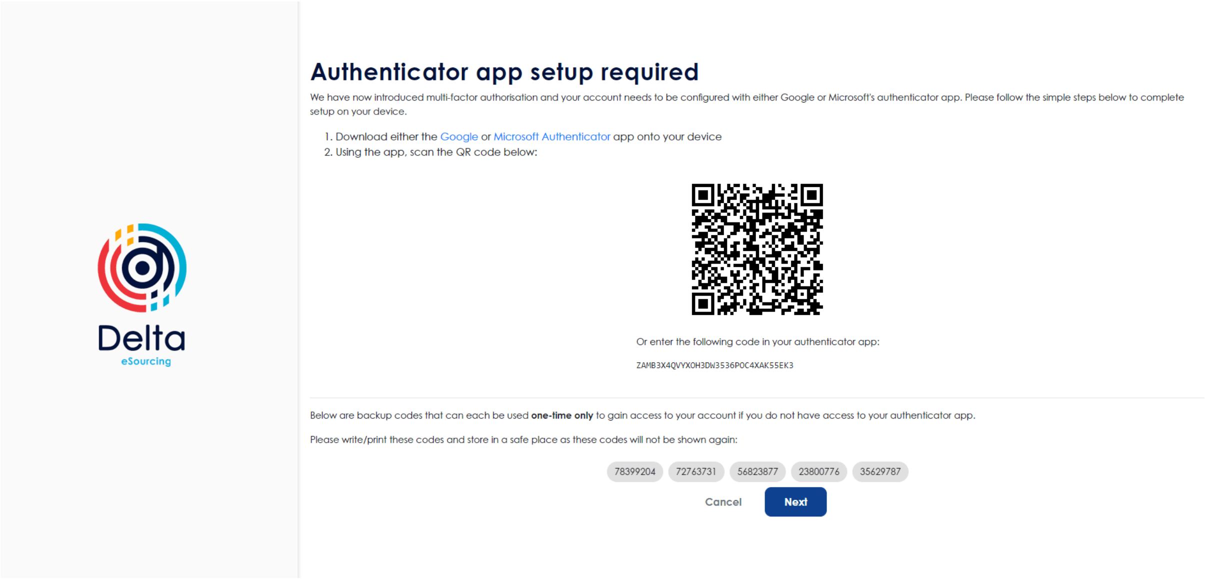
### Step 1:

When you visit the Delta login, the first screen will look exactly the same. Simply enter your usual username and password.

### Step 2:

Next you will need to set up the authenticator app. Please note that you will need to download either the Google or Microsoft authenticator app onto your device in advance.

Scan the QR code on the screen using the authenticator app and you will be shown a token code for the next step.



## Authenticator app setup required

We have now introduced multi-factor authorisation and your account needs to be configured with either Google or Microsoft's authenticator app. Please follow the simple steps below to complete setup on your device.

1. Download either the Google or Microsoft Authenticator app onto your device
2. Using the app, scan the QR code below:

Or enter the following code in your authenticator app:

ZAMB3X4QVYXOH3DW3536POC4XAK55EK3

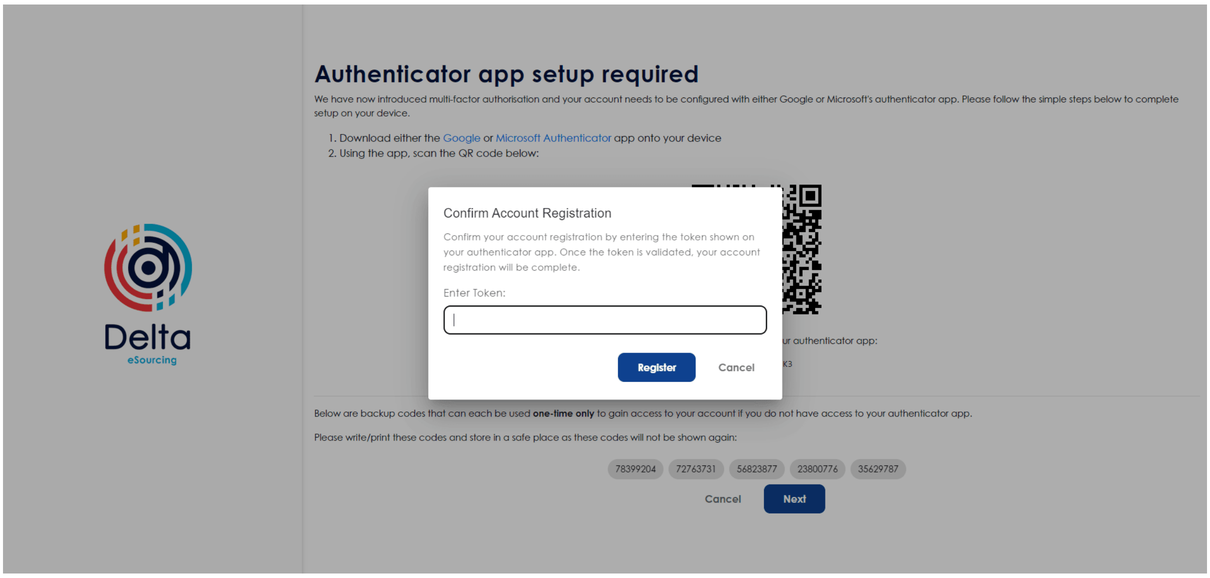
Below are backup codes that can each be used **one-time only** to gain access to your account if you do not have access to your authenticator app.

Please write/print these codes and store in a safe place as these codes will not be shown again:

78399204 72763731 56823877 23800776 35629787

## Step 3:

Enter the token code from your authenticator app and then click ‘Register’.



Confirm Account Registration

Confirm your account registration by entering the token shown on your authenticator app. Once the token is validated, your account registration will be complete.

Enter Token:

Delta
eSourcing

Authenticator app setup required

We have now introduced multi-factor authorisation and your account needs to be configured with either Google or Microsoft's authenticator app. Please follow the simple steps below to complete setup on your device.

1. Download either the Google or Microsoft Authenticator app onto your device
2. Using the app, scan the QR code below:

Below are backup codes that can each be used one-time only to gain access to your account if you do not have access to your authenticator app.

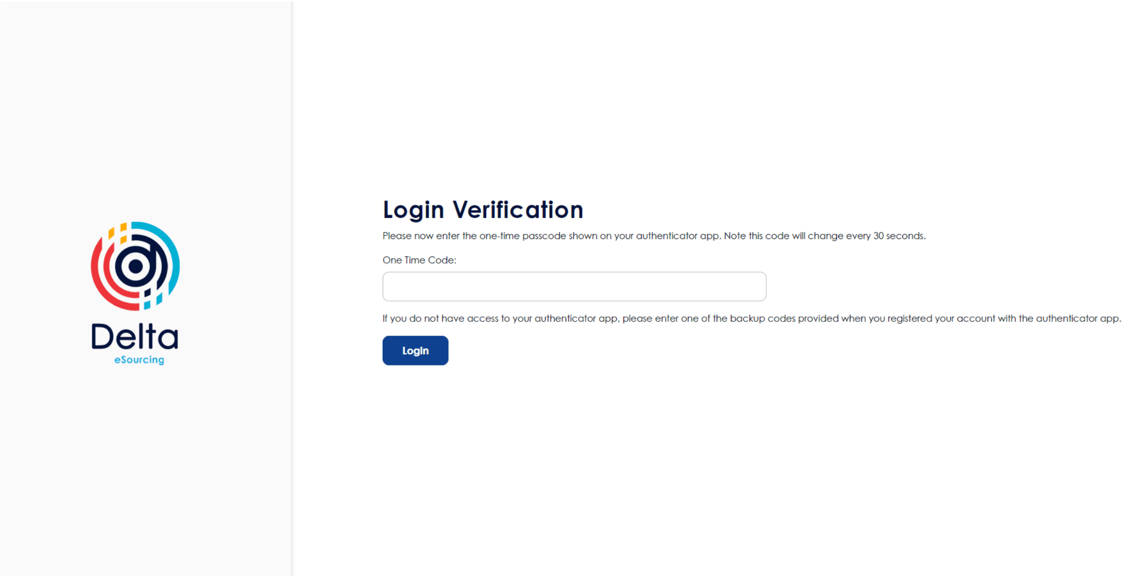
Please write/print these codes and store in a safe place as these codes will not be shown again:

78399204 72763731 56823877 23800776 35629787

Cancel Next

## Step 4:

Next you will be shown a one-time passcode on your authenticator app. Please enter that into the box shown on screen and click ‘Login’.



## Login Verification

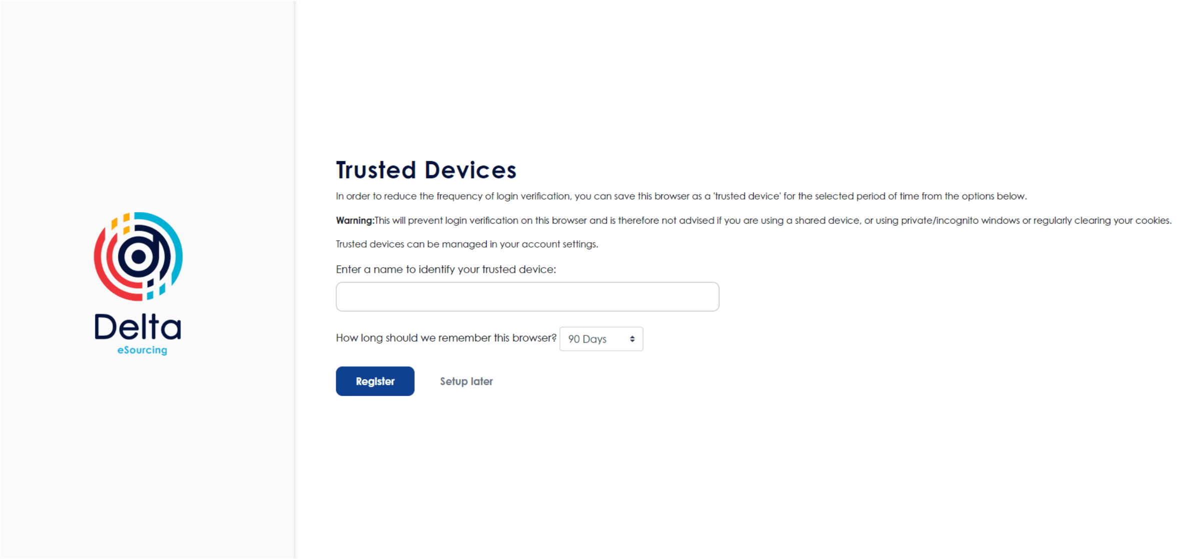
Please now enter the one-time passcode shown on your authenticator app. Note this code will change every 30 seconds.

One Time Code:

If you do not have access to your authenticator app, please enter one of the backup codes provided when you registered your account with the authenticator app.

## Step 5:

In order to reduce the frequency of login verification, you can opt to trust the browser that you are logging in from. If you choose to set this up, simply name the device and choose how long you would like to remember the browser. The options are 30, 60 or 90 days. Then click ‘Register’. You can also choose to skip this step and set up at a later date.



## Trusted Devices

In order to reduce the frequency of login verification, you can save this browser as a 'trusted device' for the selected period of time from the options below.

**Warning:**This will prevent login verification on this browser and is therefore not advised if you are using a shared device, or using private/incognito windows or regularly clearing your cookies.

Trusted devices can be managed in your account settings.

Enter a name to identify your trusted device:

How long should we remember this browser? 90 Days

## Step 6:

You will now be logged in to the Delta platform and can continue to use it as needed. The next time you log in to Delta you will use your username and password as before but will then be asked to enter a one-time passcode from the authenticator app. This is MFA. Simply open your authenticator app and enter the passcode shown. Please note that the passcode refreshes every 30 seconds.

## Shared accounts

We are aware that many Delta users have shared accounts – for example, multiple users using the same username and password to access the Delta platform.

For Delta buyers, there are two options:

### Option 1:

One member of your team sets up the authenticator originally and then provides the token to each user who can then log in with the shared login. Each user then selects to trust their device for 90 days, which allows them to log in without the token for 90 days. However, they will need to get a token every 90 days.

### Option 2:

Each team member is invited to the organisation using their own email address and then has their own login username and password, allowing them to set up their individual authenticator meaning they wouldn't be sharing. Each user would then need to ask the asset owner for all the tenders they work on to add them to the email alert preferences so they continue to get system emails for those tenders. There is no limit to how many Delta user accounts you can have within your organisation.

We would recommend option 2 as this means that each individual Delta user within your team has their own logins and is responsible for their own authenticator app access codes. You can do this easily by inviting individual users to your organisation via Account Settings.

To do this, simply login to the shared Delta account and follow the steps below:

Go to Account Settings and then:

1. Organisation Settings
2. User Management
3. Invite new users
4. Add email
5. Enter the team members email address
6. Enter their role
7. Select which Organisation Group the invited user to be assigned to
8. Click 'Add email'. You can continue to 'Add email' for all individuals you would like to be invited.
9. Once all emails have been added, click 'Next'.
10. Click invite

Invited users will receive an email from Delta informing them that they have been invite to Delta eSourcing on behalf of the organisation and will receive instructions on how to complete their registration.

Please note, each new user would need to edit their email preferences so that any Delta communications and alerts go to the shared inbox instead of the individual's email inbox, if this is the preferred option.

For suppliers, one person would set up the authenticator originally and then provide the token to each user who would log in with the shared login. Each user then selects to trust their device for 90 days, which allows them to lo gin without a token for 90 days. However, they will need to get a token every 90 days.

# Frequently Asked Questions

## I don’t have a mobile phone

Please note that it is your organisation’s responsibility to ensure that your teams have downloaded and set up the Google or Microsoft authenticator application on either their work or personal mobile devices.

There are other ways to access an authenticator app without a mobile device, but your IT department should be able to advise the best option for your organisation. We would recommend that any issues you have regarding your chosen authenticator app are directed either to the app provider or your IT department initially.

Please ensure you have the authentication service setup prior to a tender submission deadline to prevent any issues.

For any help or advice regarding shared accounts, please contact our Helpdesk team at helpdesk@delta-esourcing.com.