Instructions for Setting Up Two Factor Authentication (2FA)

What is 2FA?

2FA is a verification process that requires users to specifically use at least two pieces of verification information, e.g. a password and a PIN.

Passwords can be compromised so 2FA immediately increases account security by requiring more than one form of verification to prove your identity when signing into a website or an application.

CSO users are currently using a Username and Password to sign in remotely to access their workstations. A second verification is now being added using the Microsoft Authenticator phone app on users' mobile phone.

Microsoft Authenticator App

The Microsoft Authenticator phone app gives you easy, secure access to online accounts, providing two-factor authentication for an extra layer of security. This Microsoft Authenticator phone app generates a six-digit code which users will be required to provide during the sign in process.

The app icon is a blue box with a white padlock and is available in the App store on your mobile phone.
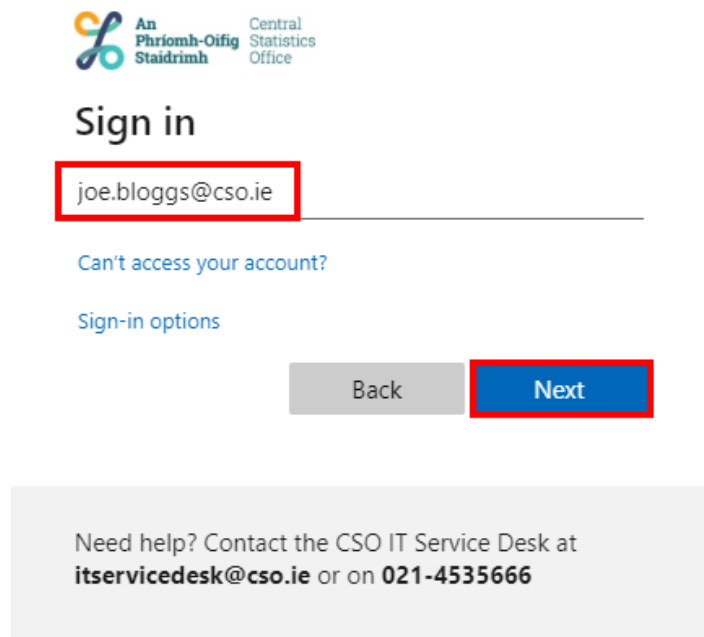

If you currently have a CSO issued mobile, the Microsoft Authenticator phone app will be already installed under your work profile.

Please note:
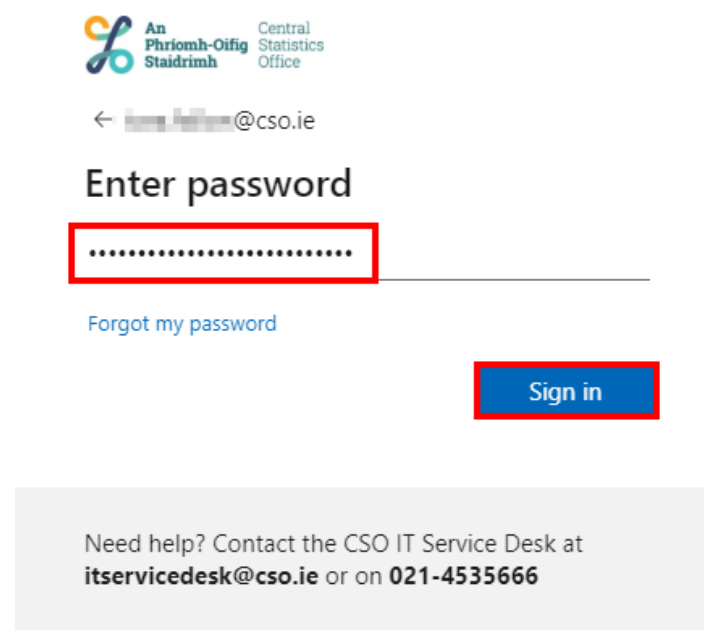Only the Microsoft Authenticator phone app is supported for use with https://sara.cso.ie:444

Setting Up 2FA

1. Log out of all **Citrix Sessions**.

2. On your **Home Device Browser**, go to the https://sara.cso.ie:444 (please note the addition of the colon and port number 444 from URL you currently use).

3. Enter your **CSO Email Address** as your username e.g. joe.bloggs@cso.ie, then click **Next**.

4. Enter your **CSO Network Password**, then click **Sign In.**

5. Click **Next.**

More information required

[blurred]@cso.ie

More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

Next

Need help? Contact the CSO IT Service Desk at
itservicedesk@cso.ie or on **021-4535666**

6. Click **Set up**.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up   Please configure the mobile app.

Next

©2020 Microsoft   Legal | Privacy

7. The **Configure mobile app** window will appear on your screen. Leave this window open and continue with the next steps on your mobile phone.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft Authenticator or any authenticator app for Windows Phone, Android or iOS.

2. In the app, add an account and choose "Other account".

3. Scan the image below.

If you are unable to scan the image, enter the following information in your app.
Account Name: Central Statistics Office ▓▓▓▓▓@cso.ie
Secret Key: ▓▓ ▓▓▓▓▓▓

If the app displays a six-digit code, choose "Next".

Next   cancel

8. If you currently have a CSO issued mobile, the **Microsoft Authenticator phone app** will be already installed under your work profile. If using a personal mobile phone, go to the Google Playstore (Android) or iOS App Store (iOS) and download the **Microsoft Authenticator phone app**. Once installed, open the **Microsoft Authenticator phone app.**

Please note:
Only the **Microsoft Authenticator phone app** is supported for use with https://sara.cso.ie:444

9. If this is the first time you are setting up the Microsoft Authenticator phone app on your mobile phone, proceed directly to **Step 10**. If you have used the Microsoft Authenticator phone app before on your mobile phone, proceed directly to **Step 13**.
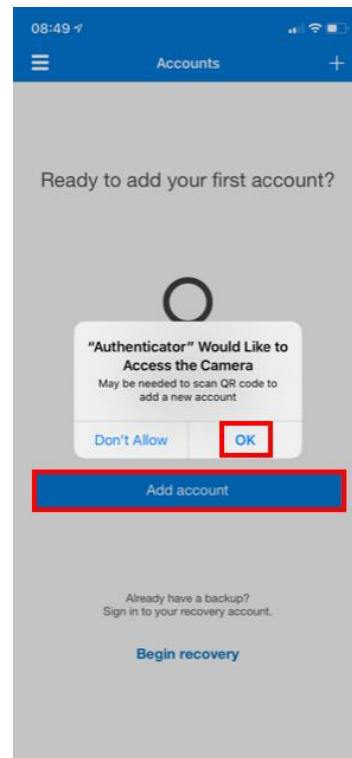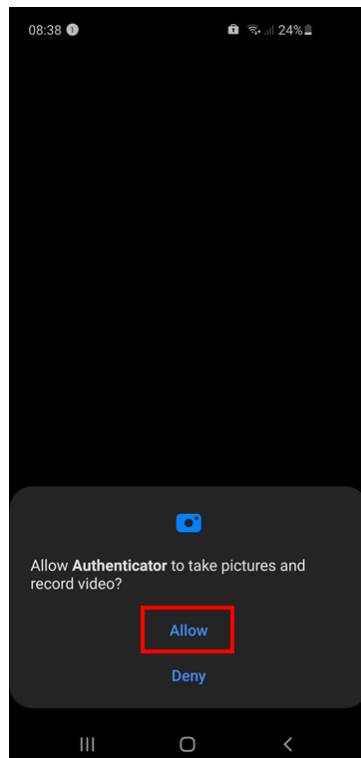
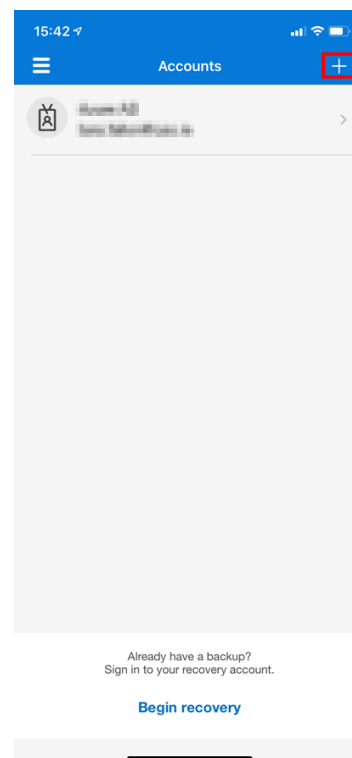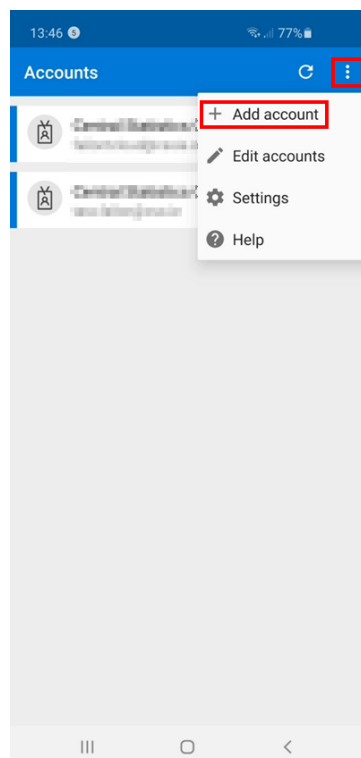10. Open the Microsoft Authenticator phone app, then click **Scan QR Code**.
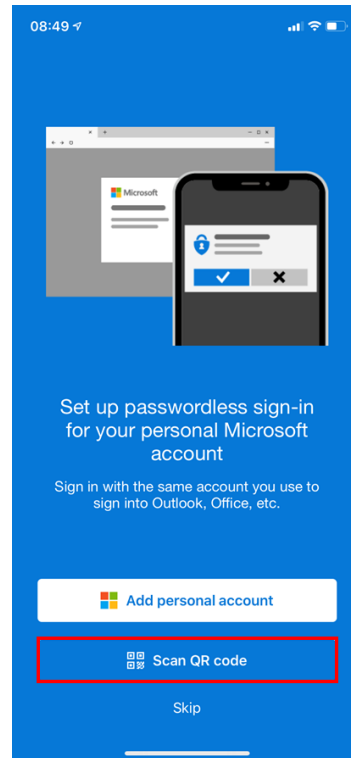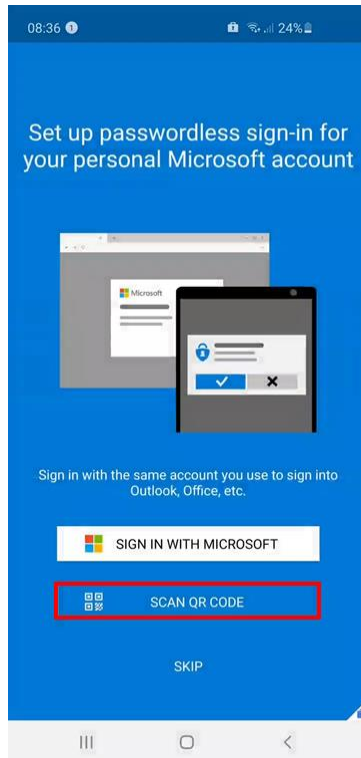
11. You will receive a Data Privacy prompt, click **OK**.
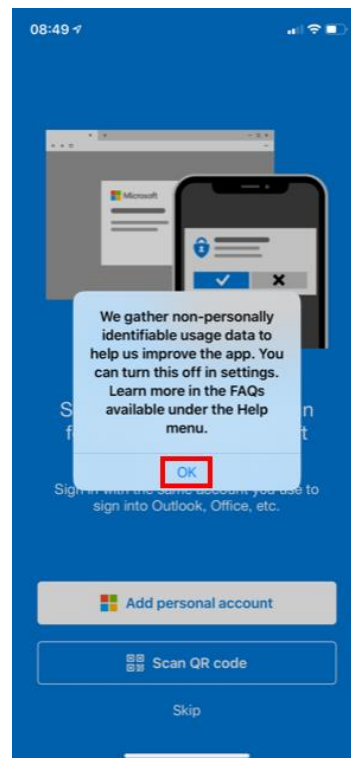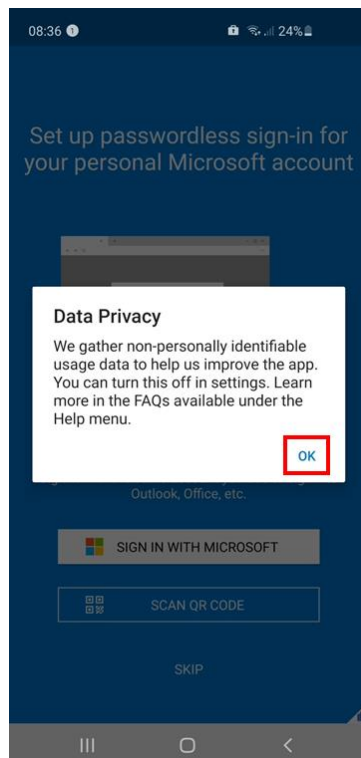
12. On Android = Allow Authenticator to take pictures and record video, click **Allow**.
   On iOS = Authenticator Would Like to Access the Camera, click **OK,** then click **Add Account.**
   Now proceed directly to **Step 15.**

13. Continuing from **Step 9**, open the Microsoft Authenticator phone app.
   On Android = click the **3 dots icon** in the upper right corner, then click **Add Account**.
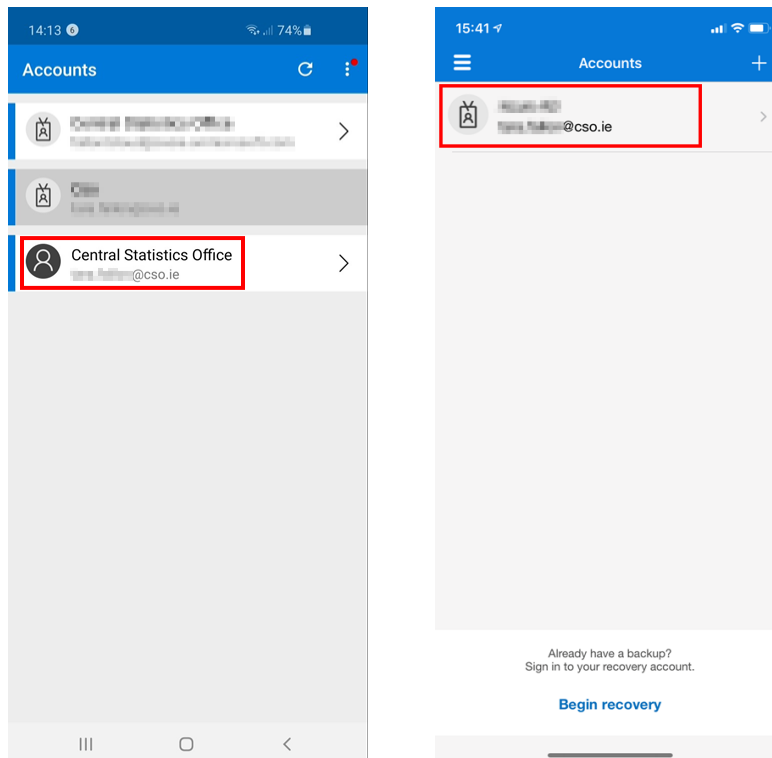   On iOS = click the **plus icon** in the upper right corner.

14. Click **Work or school account.**
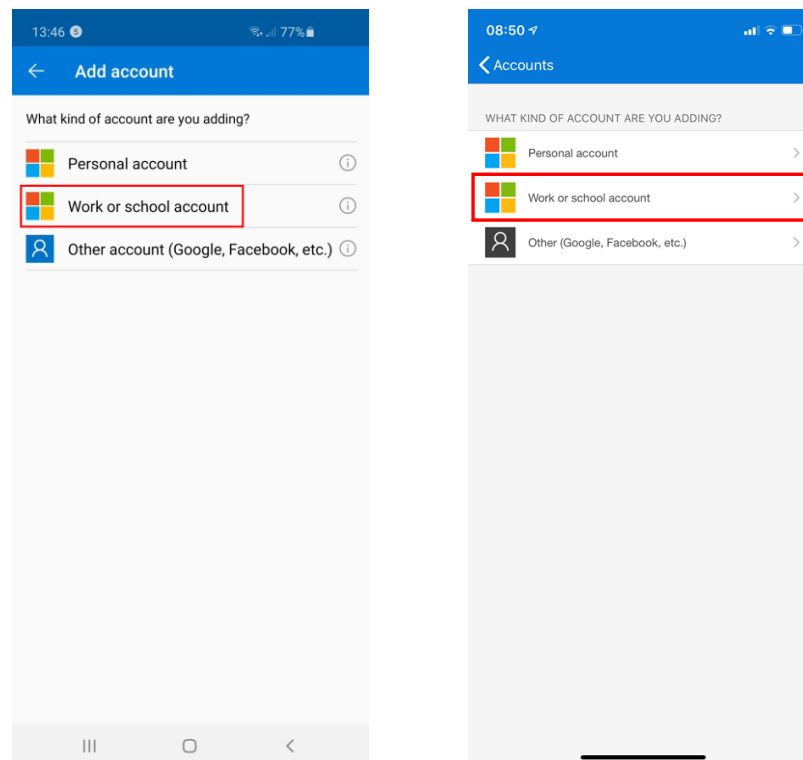
15. Point your mobile phone at the Configure mobile app screen currently open on your home device to scan the QR code.
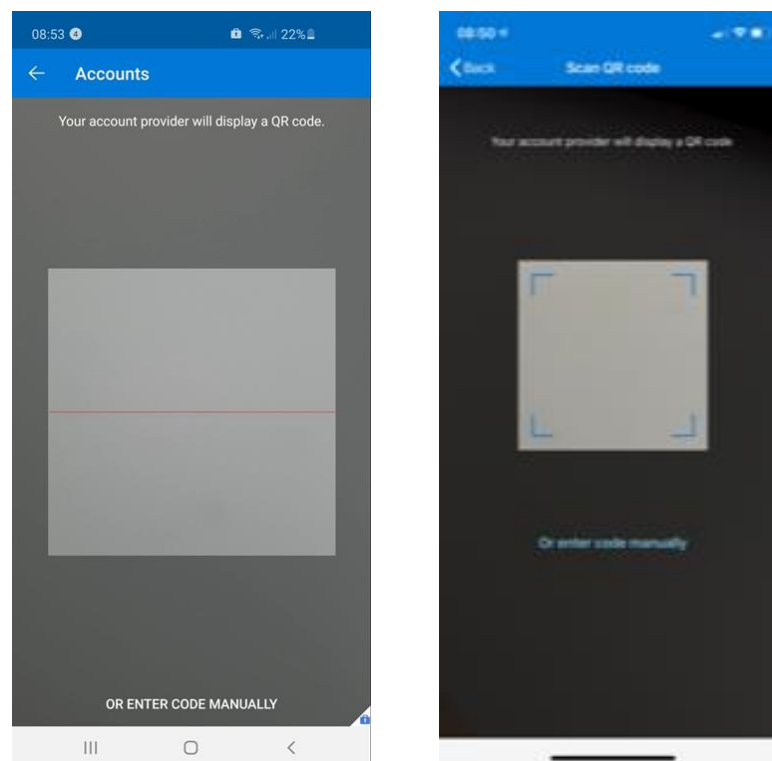
16. You will now see your account has been added to the Microsoft Authenticator phone app on your mobile phone.

17. Click on your new account within the Microsoft Authenticator phone app. This Microsoft Authenticator phone app will now display a six-digit code. This code changes every 30 seconds.
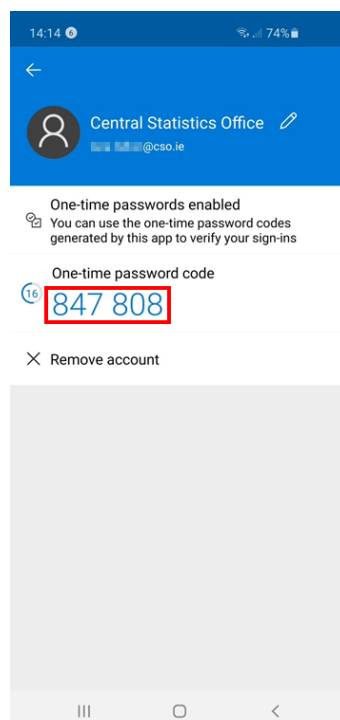
18. Back on your home device, on the Configure mobile app screen, click **Next.**

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft Authenticator or any authenticator app for Windows Phone, Android or iOS.

2. In the app, add an account and choose "Other account".

3. Scan the image below.

If you are unable to scan the image, enter the following information in your app.
Account Name: Central Statistics Office ▓▓▓▓▓@cso.ie
Secret Key: ▓▓ ▓▓▓ ▓▓▓

If the app displays a six-digit code, choose "Next".

Next   cancel

19. Click **Next.**

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app   ▾

┌─ How do you want to use the mobile app? ─────────
│ ◉ Use verification code
└──

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up   Mobile app has been configured for verification codes.

Next

20. Enter the six-digit code that is currently showing on your mobile phone into the Additional security verification screen on your home device, then click **Verify**.

21. If prompted, enter a back-up mobile phone number in case you lose access to the Microsoft Authentication phone app and click **Next.** Click **Done**.
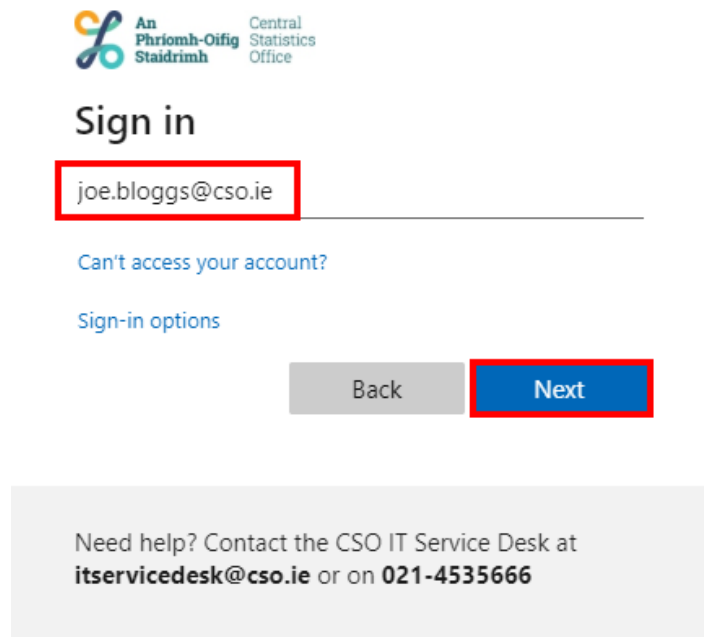
For more information on how to install the Microsoft Authenticator App and set-up 2FA, please see
https://youtu.be/Q8OzabuNwHI
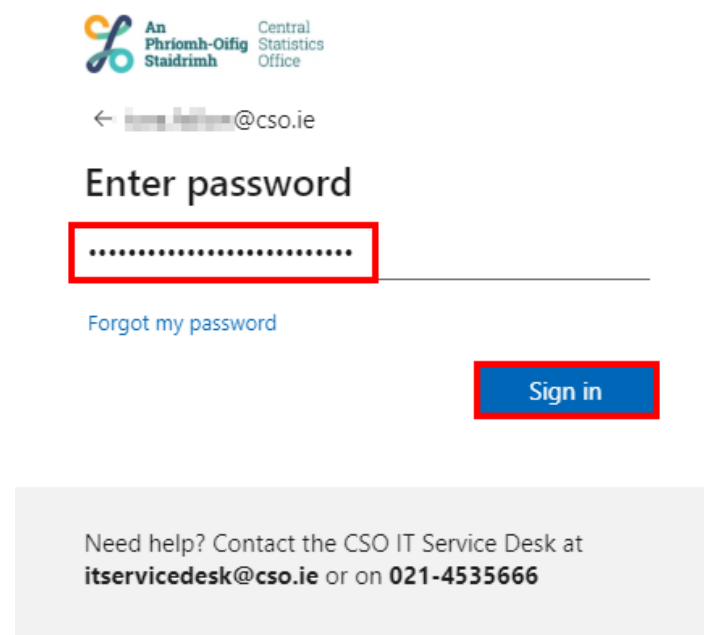
Sign in to CSO with 2FA

1. Now that you have successfully set-up 2FA, you will be required to use it each time you sign into CSO. On your **Home Device Browser**, go to the https://sara.cso.ie:444 (please note the addition of the colon and port number 444 from URL you currently use).

2. Enter your **CSO Email Address** as your username e.g. joe.bloggs@cso.ie, then click **Next**.

3. Enter your **CSO Network Password**, then click **Sign In.**

4. Open the Microsoft Authenticator phone app on your mobile phone. Click on your CSO account to display the six-digit code. Enter the six-digit code currently displayed in the Microsoft Authenticator phone app into the Enter Code box on your home device screen, then click Verify.

5. If prompted, click **Detect Receiver.**
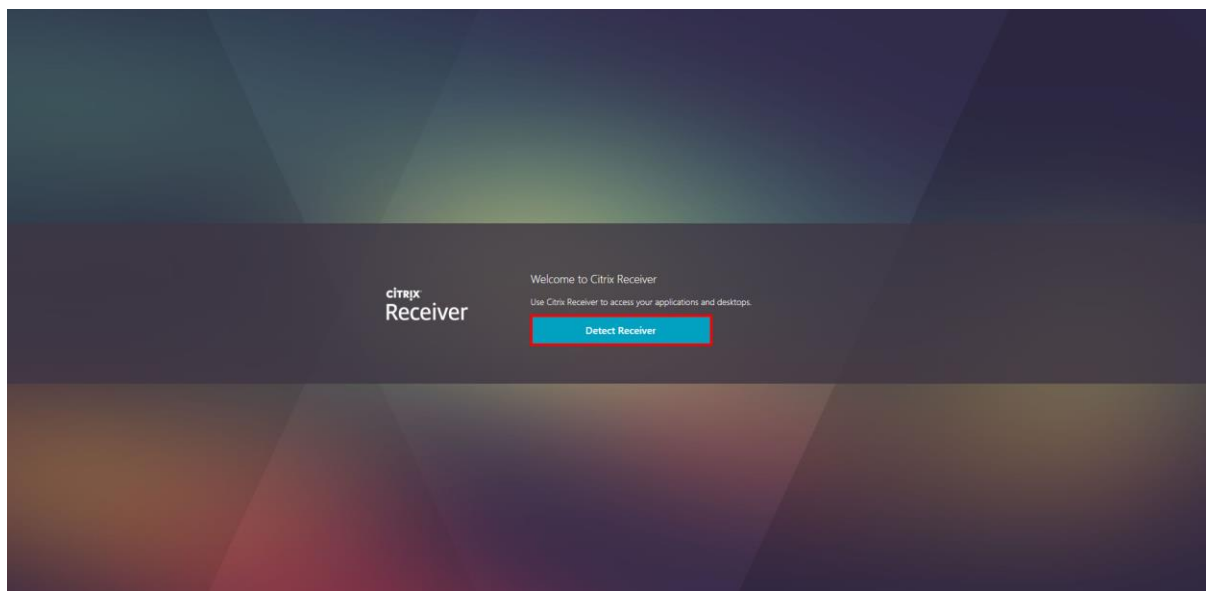
6. Tick the box beside **Always allow sara.cso.ire:444 to open links of this type in the associated app**, then click **Open**.

This site is trying to open Citrix Receiver Launcher.

https://sara.cso.ie:444 wants to open this application.

☑ Always allow sara.cso.ie:444 to open links of this type in the associated app

Open   Cancel

7. Click **Desktops**. Click on your assigned desktop to launch, then sign in as normal.