

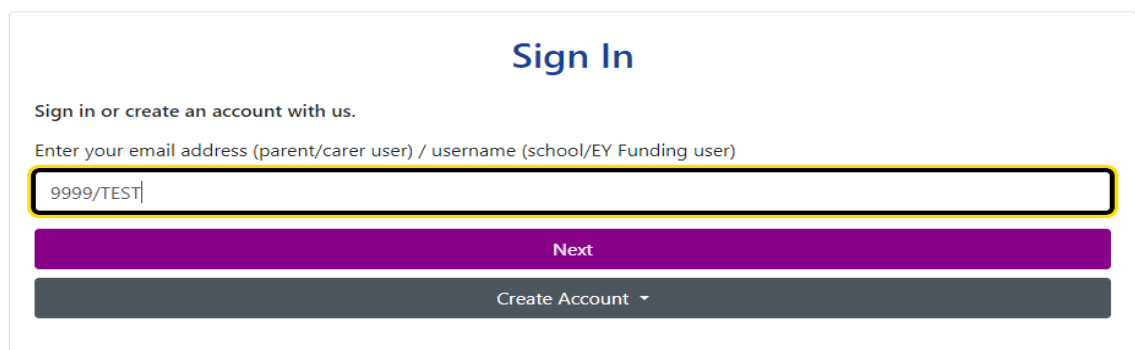
Using Two-Factor Authentication (2FA) to access Synergy

To access the Synergy School Access Module (SAM), Early Years Provider Portal, EISI Case Management and the Gateway Contact Centre and Professional Portal you will be required to sign into your account using Two-Factor Authentication (2FA).

To do this you will need to download an authenticator app (Microsoft Authenticator or Google Authenticator) to your mobile phone or web browser. The authenticator app generates a different one-time password code every time you log in, helping to add an extra layer of security to your account.

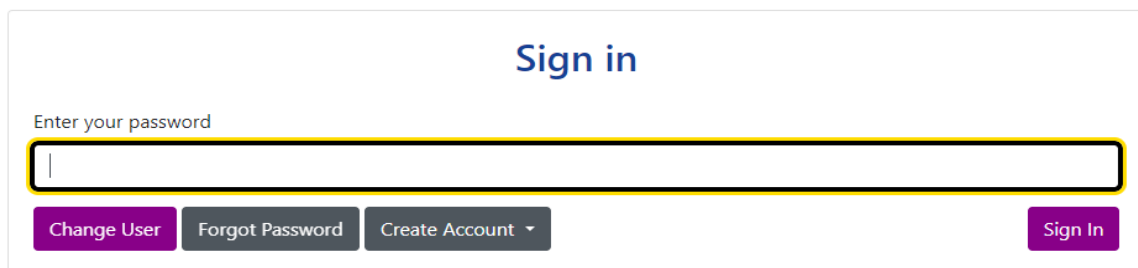
Accessing SYNERGY for the first time with 2FA

- Enter your **Username** and select **Next**.



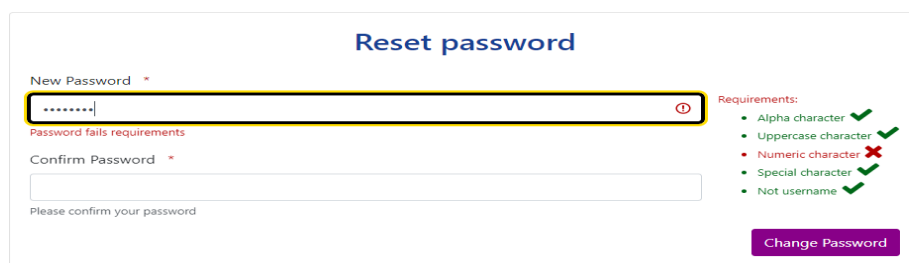
The 'Sign In' screen features a heading 'Sign In' in blue. Below it is the text 'Sign in or create an account with us.' followed by 'Enter your email address (parent/carer user) / username (school/EY Funding user)'. A text input field contains '9999/TEST|'. Below the input field are two buttons: a purple 'Next' button and a grey 'Create Account' button with a dropdown arrow.

- Enter your **Password** and select **Sign In**.



The 'Sign in' screen features a heading 'Sign in' in blue. Below it is the text 'Enter your password'. A password input field is shown. Below the input field are four buttons: 'Change User', 'Forgot Password', 'Create Account' with a dropdown arrow, and a purple 'Sign In' button.

- The first time you sign in with your username and temporary password you will be prompted to change the password. Please make sure the new password meets our password policy requirements



The 'Reset password' screen features a heading 'Reset password' in blue. It has two input fields: 'New Password' (with a red asterisk) and 'Confirm Password' (with a red asterisk). The 'New Password' field contains '.....' and has a red 'x' icon to its right. Below the 'New Password' field is the text 'Password fails requirements'. Below the 'Confirm Password' field is the text 'Please confirm your password'. To the right of the input fields is a 'Requirements:' section with a list: 'Alpha character' (green check), 'Uppercase character' (green check), 'Numeric character' (red X), 'Special character' (green check), and 'Not username' (green check). At the bottom right is a purple 'Change Password' button.

- The first time you sign in with your username and password you will see the details below informing you of **2FA Enrolment**. Select **OK** to continue.

2FA Enrolment

Your Local Authority has mandated that Two-Factor Authentication (2FA) is enabled on your user account. Please complete Two-Factor Authentication setup in order to sign in.

You can find out more about Two-Factor Authentication using the help button below.


Help ▾

OK

- The next screen displays information on **2FA Enrolment**. When you have downloaded one of the authenticator apps, you will be required to scan the **QR code** to set up the account. Scanning the QR code will also generate a 2FA password code. Select **Next** to continue.

2FA Enrolment

You can set up two-factor authentication (2FA) for your account using the below QR code:



Steps:

1. Open your chosen 2FA app
2. Add a new account
3. Scan the QR code to add the account
4. You will see that the account has been added with a rotating code.
5. Click "Next"

If you can't scan the QR code, please click *Reveal Secret* below. This will display the secret that you can enter into your 2FA app.

Help ▾

Reveal Secret

Next

- Enter the **2FA Code** generated by the authenticator app and select **Confirm**.

2FA Enrolment

In order to complete the setup of your 2FA, you need to confirm the code displayed in the app.

The code refreshes every 30 seconds so you do not need to remember it.

Confirm your 2FA Code

Back

Help ▾

Confirm

- **2FA Enrolment** is complete. Each time you sign in you will need to use the authenticator app to obtain a code which you will enter. Select **Finish**.

2FA Enrolment

You have now configured your two-factor authentication and will be prompted for the code when signing in.

Finish

How to sign in once you have set up 2FA

- Enter your **Username** and select **Next**.

Sign In

Sign in or create an account with us.

Enter your email address (parent/carer user) / username (school/EY Funding user)

9999/TEST

Next

Create Account ▾

- Enter your **Password** and select **Sign In**.

Sign in

Enter your password

Change User Forgot Password Create Account ▾

Sign In

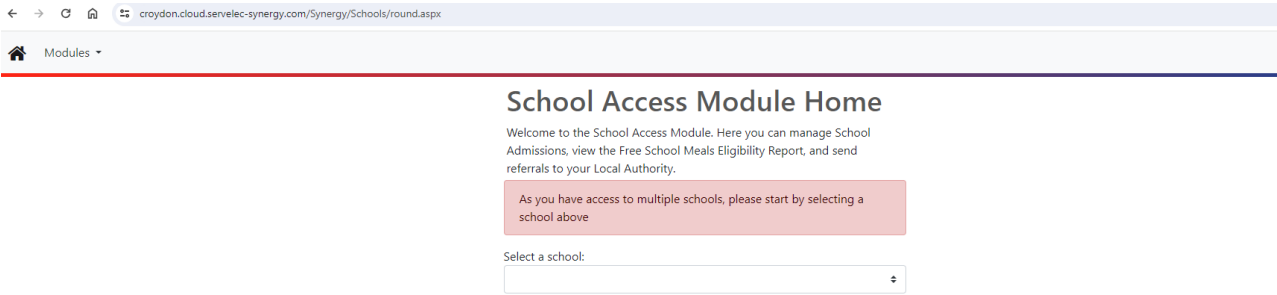
- Enter your **two-factor authentication code** and select **Verify**

Sign in

Enter your two-factor authentication code

Verify

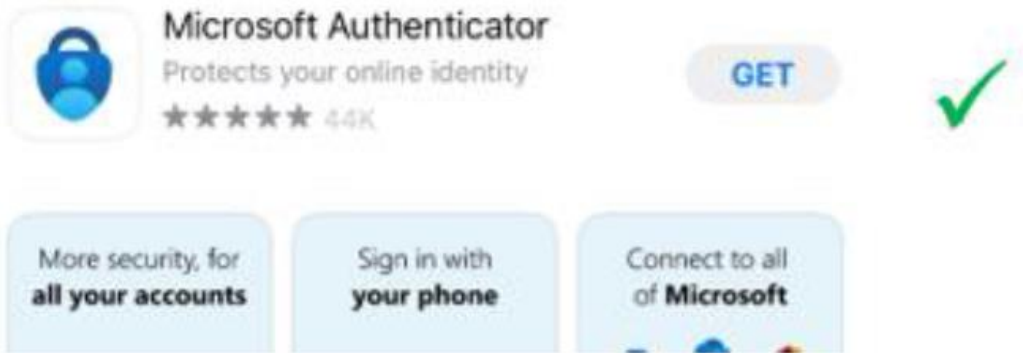
- You are now logged in to SYNERGY



Authenticator Apps

As stated above, you will need to use a 2FA app in order to access Synergy. Microsoft Authenticator can be downloaded to your mobile phone and used to set up 2FA. The information below tells you how to set up the app.

When selecting a 2FA App please ensure you are selecting one of the following ticked below as multiple apps may be offered, some of which are chargeable.



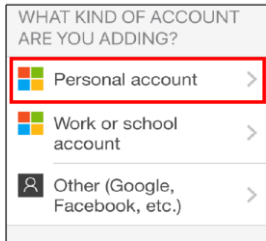
Microsoft Authenticator

- Download the app to your mobile phone
- Open the app

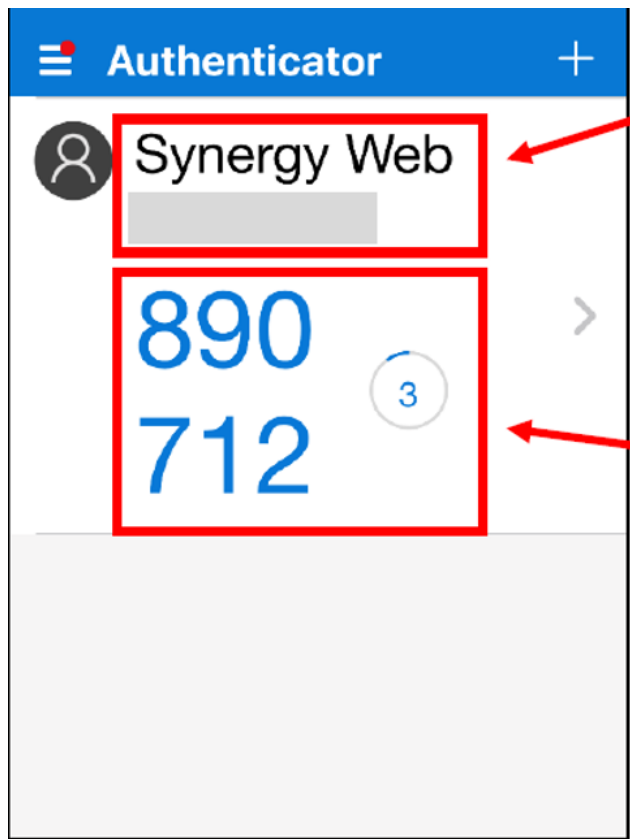


Select the **Add account** button. If you already use Microsoft Authenticator select the plus button to add a new account.

- Select **Personal account**.



- Use your phone camera to scan the QR Code displayed on the SAM webpage.

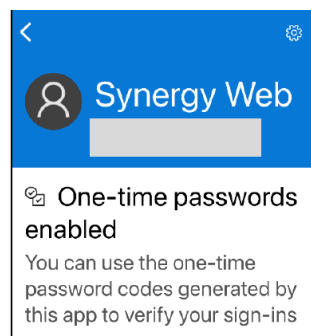


Scanning the QR code will add the Synergy Web account and will display your username (greyed out on this image).

Enter this code into the **2FA Enrolment** field on Synergy when prompted. This will complete the configuration process.

The 6 digit code displayed will need to be entered each time you sign in to SYNERGY. This is a random number and regenerates every 30 seconds

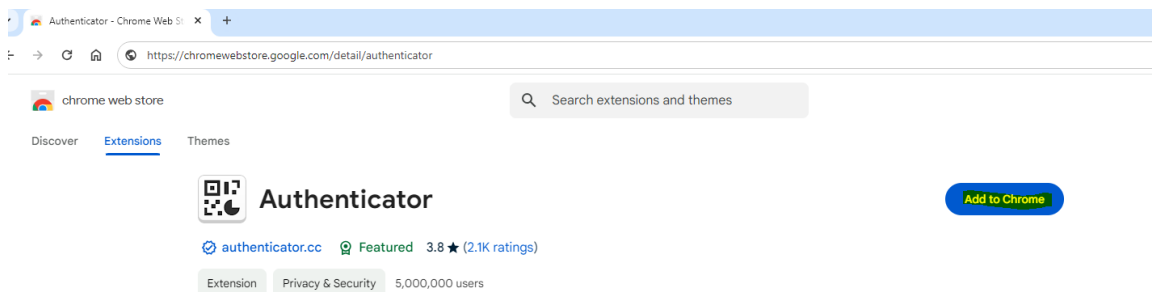
- Your account set up is now complete and you can use the app to generate one-time codes each time you access Synergy



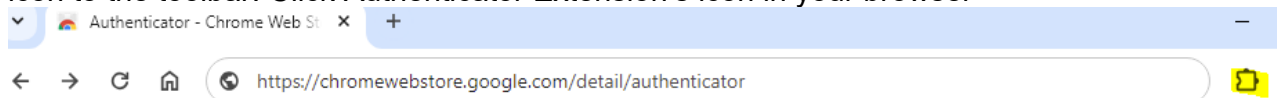
Google Authenticator to your web browser

If you do not have a mobile phone google authenticator generates two-factor authentication (2FA) codes in your web browser (Chrome, Firefox, Edge).

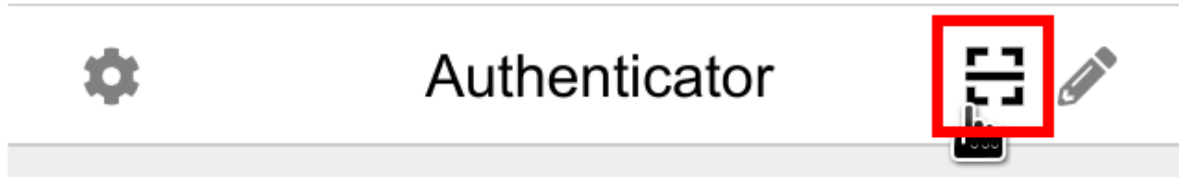
Download the authenticator app



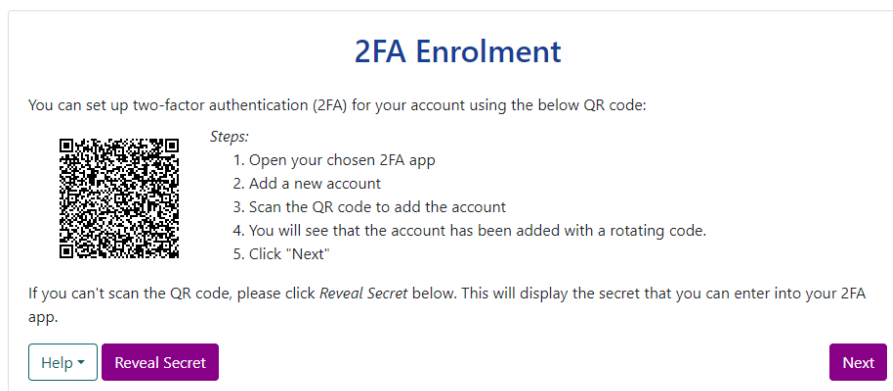
When you first install Authenticator Extension in Chrome you should PIN the authentication icon to the toolbar. Click Authenticator Extension's icon in your browser



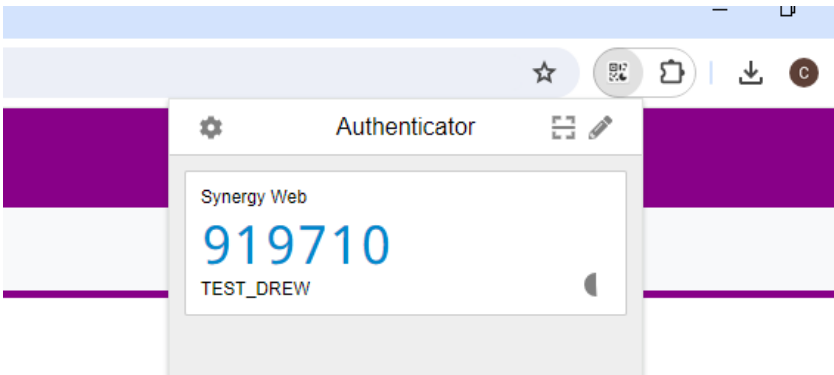
Click the scan icon at the top right corner of the window.



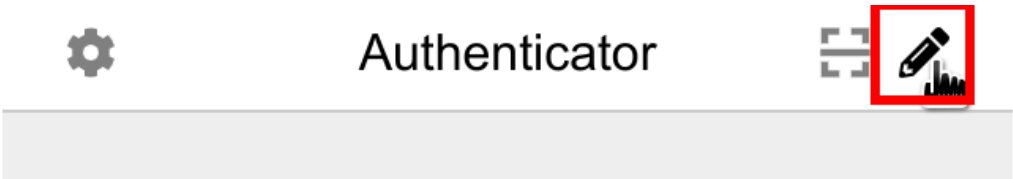
Click and drag to draw a square that completely covers the QR code. You will then see a prompt confirming the account has been added



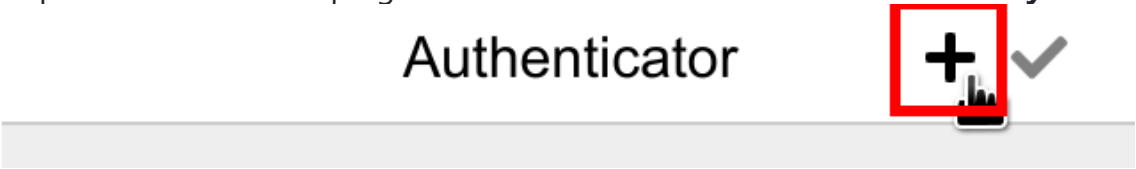
After the new account is added, you will see a new entry in the window. The 6-digit number is your current one-time password, circle at bottom right corner tells you how much time left for the current password.



If you do want to add an account without scanning the QR code then click Authenticator Extension's icon in your browser and then click the pencil icon at the top right corner of the window.



Click the plus button at the top right corner of the window. Select **Manual Entry**.



Input "SYNERGY WEB" in the **Issuer** field, the account secret given to you in the **Secret** field (found by clicking reveal secret in SYNERGY 2FA enrolment screen), and finally click **OK**.

A screenshot of the 'Manual Entry' form within the Authenticator extension. It has two input fields: 'Issuer' with the text 'SYNERGY WEB' and 'Secret' with a masked value. Below these fields is an 'Advanced' section with a right-pointing arrow. At the bottom is an 'Ok' button.A screenshot of the '2FA Enrolment' screen. It features a QR code on the left and a list of steps on the right. Below the QR code is a 'Your secret is:' field with a masked value. At the bottom are three buttons: 'Help', 'Hide Secret' (highlighted with a yellow border), and 'Next'.