

Synergy Two factor Authentication

Contents

1. What is Two Factor Authentication	2
2. What's happening?	2
3. What does this mean for me?	2
4. First-time setup for Two Factor Authentication (2FA)	3
5. Logging in After Two-Factor Authentication Is Enabled.....	4

Version History

Version	Author	Date	Comments
1.0	Melissa Richings	29/04/2026	Document created

1. What is Two Factor Authentication

Two factor authentication is a security measure that requires two separate forms of identification to access an account. This typically includes a password (something you know) and a temporary code or biometric verification (something you have or are). This added layer of protection helps prevent unauthorised access, even if a password becomes compromised.

2. What's happening?

Before the end of May, we will be enabling Two Factor Authentication (2FA) for all users who access the SAM Portal. This includes anyone who uses the portal to view **Admissions information** or **Free School Meals reports**.

Some users also access the **Provider Portal** using the same login details as their SAM account. If this applies to you, you will also be asked to complete 2FA when signing into the Provider Portal.

Please note: This update only affects **SAM Portal users**. We are **not** rolling 2FA out to all providers at this time.

3. What does this mean for me?

After the change is applied, the next time you log in to the SAM Portal, you will be prompted to set up Two Factor Authentication.

To complete the setup, you will need to download the **Microsoft Authenticator App** from either the **Apple App Store** or the **Google Play Store**.

Search for *Microsoft Authenticator* and look for the icon shown below.



4. First-time setup for Two Factor Authentication (2FA)

Step 1:

Log in as you normally would by entering your usual username and password.

Step 2:

You will see a message explaining that 2FA is now required. This message will prompt you to download the **Microsoft Authenticator App** from the Apple App Store or Google Play Store. Once you have installed the app, click **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 must download the Microsoft Authenticator app from the App store or Play Store to your Work or Personal device.

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

Help ▾OK


Step 3:

You will then be taken to the **2FA Enrolment Screen**, which outlines the steps you need to follow.

As long as you have installed the Microsoft Authenticator App, you can scan the QR code displayed on the screen. This will automatically add your account to the Authenticator App.

2FA Enrolment

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



Steps:

1. Open the Microsoft Authenticator app (You will need to download this if you haven't already)
2. Add a new account (Choose work or School)
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"

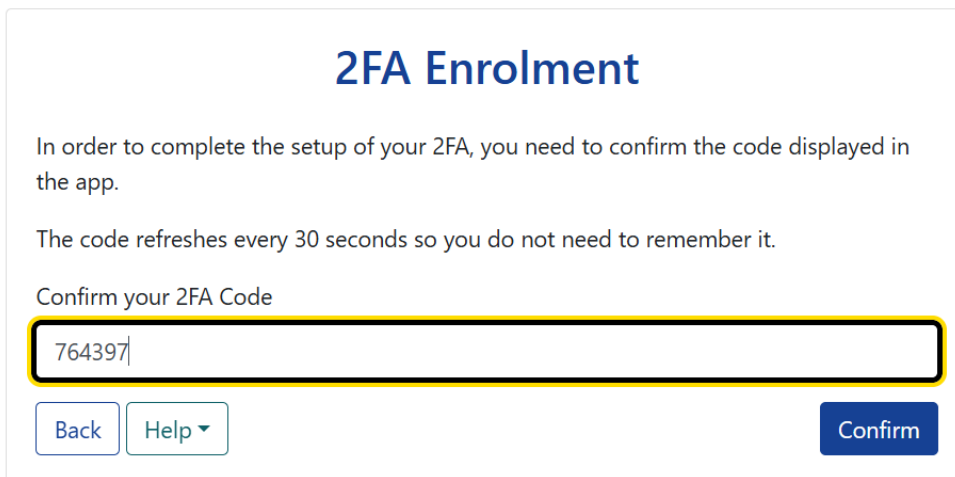
If you can't scan the QR code, please click *Reveal Secret* below. This will display the secret that you can enter into your 2FA app.

Help ▾Reveal SecretNext

In your Authenticator app, you should see an account named **Synergy Web**, showing your Synergy username and a verification code beneath it. Once you've located this, click **Next** on the screen.

Step 4:

A box will appear asking for the verification code from the Authenticator app. Enter the code, then click **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](#)

Step 5:

A confirmation message will appear to let you know that two-factor authentication has been successfully set up. Click **Finish** to complete the process.

5. Logging in after Two-Factor Authentication is enabled.

Once you have completed the initial setup for two-factor authentication, you will need to generate a new verification code each time you log in.

Step 1:

Enter your login credentials on the sign-in screen.

Step 2:

You will then be asked to enter a verification code. Open your Authenticator app and locate the account named **Synergy Web**. Enter the code displayed (before the timer expires) and click **Verify**.

Sign in

Enter your two-factor authentication code

Verify

Step 3:

Click **Accept** on the Access to Information Declaration, and you will be logged into your account.

If you experience any issues, you can log into your [Halo Portal for Schools](#) and locate the ticket titled “**Synergy - Two Factor Authentication Support**”. You can raise a ticket, detailing your issues and it will be sent directly to the Systems Support team, who will be able to assist you.