

MFA user guide

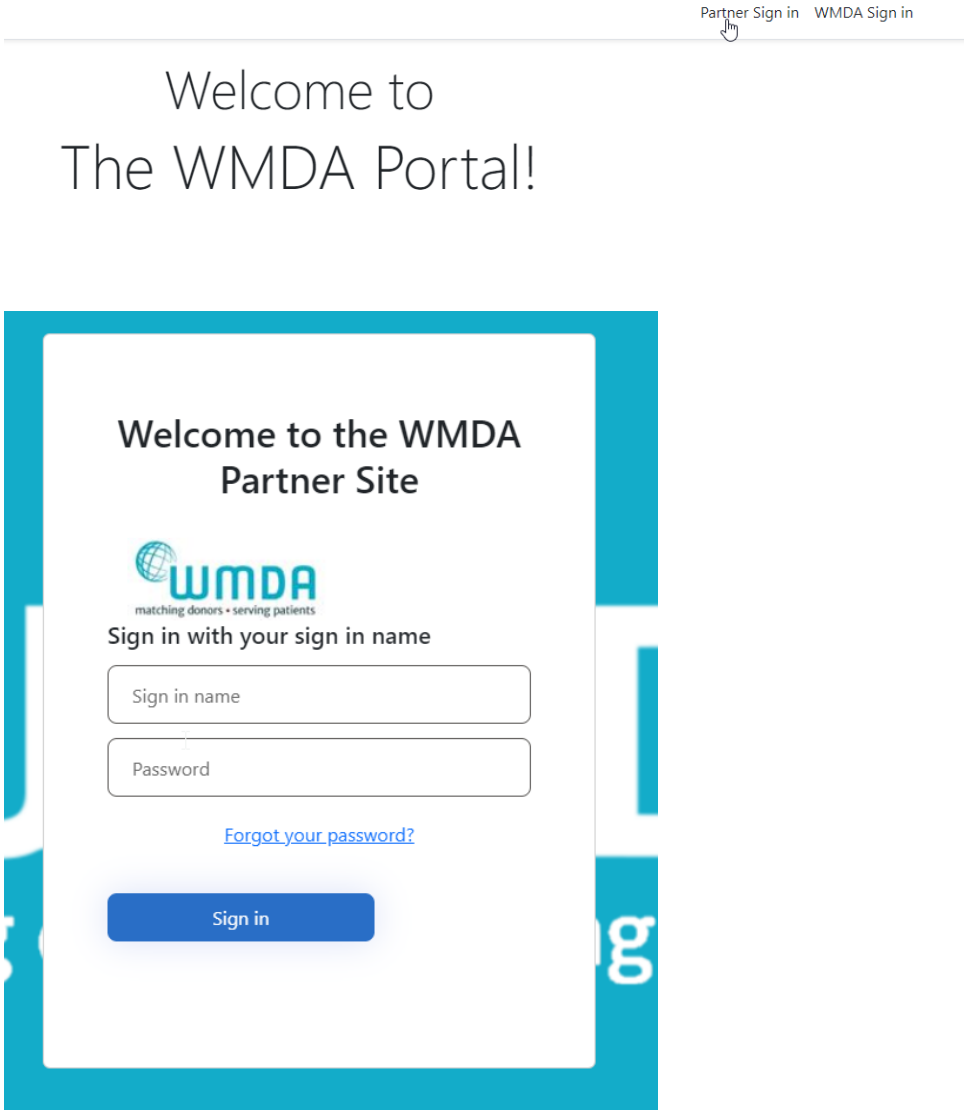
Multi-Factor Authentication (MFA) is a method which is used to strengthen the security of a file, website, etc, and adds extra protection to the sign in process.

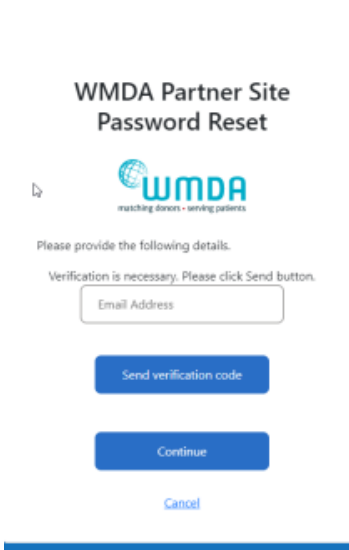

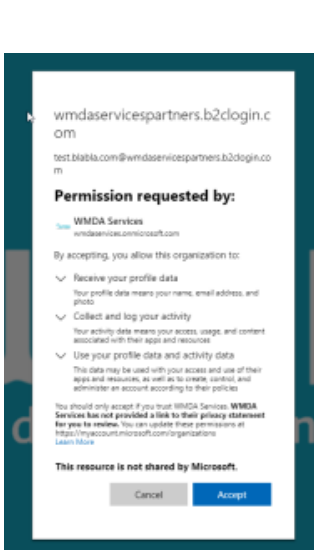
It is an authentication method which allows the user access to a website/application once the user has provided the two (or more) pieces of information to verify identity;

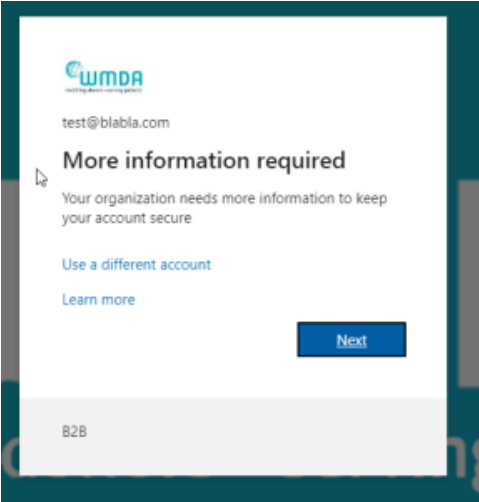
Valid authentication methods for WMDA services are passwords, authentication applications and hardware tokens.

This document is a guide to aid users to set up the required security verification methods to access the Search & Match Service.

Initial setup:

Step	Description	Image
1	<p>Please go to this web page. You can also go to https://portal.wmda.info/ and click on:</p> <p>"Login"</p> <p>followed by</p> <p>"Forgot your password?"</p>	

2	Follow the steps to verify your e-mail address and set up your initial password.	 <p>The screenshot shows the 'WMDA Partner Site Password Reset' page. At the top is the WMDA logo with the tagline 'matching donors • serving patients'. Below the logo, it says 'Please provide the following details.' and 'Verification is necessary. Please click Send button.' There is a text input field for 'Email Address', a blue 'Send verification code' button, a blue 'Continue' button, and a blue 'Cancel' link at the bottom.</p>
3	Enter a new password in the upper text box and confirm it in the lower text box	 <p>The screenshot shows the 'WMDA Partner Site Password Reset' page, similar to the previous one, but with two text input fields: 'New Password' and 'Confirm New Password'. Below these fields is a blue 'Continue' button and a blue 'Cancel' link. The entire screen is framed by a blue border.</p>
4	Please read the content and click "Accept" on the screen below.	 <p>The screenshot shows a Microsoft account permission screen. At the top, it says 'wmdaservicespartners.b2clogin.com' and 'test.b2bbl.com@wmdaservicespartners.b2clogin.com'. Below this, it says 'Permission requested by: WMDA Services' with a link to 'wmdaservices.onmicrosoft.com'. It then lists permissions: 'Receive your profile data', 'Collect and log your activity', and 'Use your profile data and activity data'. At the bottom, there are 'Cancel' and 'Accept' buttons.</p>

5	<p>Now, you will need to set up “Multi Factor Authentication”.</p> <p>Click Next.</p>	<p>Search & Match Front end</p>  <p>The screenshot shows a web browser window with a white background. At the top left is the WMDA logo with the tagline 'making defense training safer'. Below the logo is the email address 'test@blabla.com'. The main heading is 'More information required' in bold. Below this is the text 'Your organization needs more information to keep your account secure'. There are two links: 'Use a different account' and 'Learn more'. A blue 'Next' button is at the bottom right. A small number '828' is visible in the bottom left corner of the page.</p>
6	<p>Choose your MFA method. You may choose</p> <ul style="list-style-type: none"> • using an authenticator app on your smartphone • using a hardware token 	<ol style="list-style-type: none"> 1. We recommend Microsoft Authenticator if it is available in your region and on your smartphone /device if you have one. Download (from your smartphone/device) and install it if you don't already have it. It makes for the easiest MFA login experience. Alternative MFA tools are Authy or Google Authenticator, and there may be other options in your region <p><i>(Please let us know so we can add them to our documentation!)</i></p>

3. If you are not allowed to use a smartphone you may use hardware tokens that supports TOTP.
Hardware tokens are devices that work independently from a PC or Phone.

We recommend only to use only certified tokens, eg . from <https://token2.eu>

Tokens should minimally support **TOTP**, this is a single use six digit code that is uniquely bound to your account and changes every 30 seconds.

Examples of hardware tokens :



Example use : Token2 Molto

This type of device is programmed once. Once programmed they provide the TOTP code without the use of a PC or mobile phone.

You can program these devices with either a mobile phone that has NFC, or via USB, depending on the model.

Some models allow to store keys for up to 10 different accounts.

There are tokens that need a mobile phone with NFC and an companion app to generate the TOTP code. WMDA does not recommend these tokens. Contact support@wmda.info if you have questions selecting the correct token for your situation.

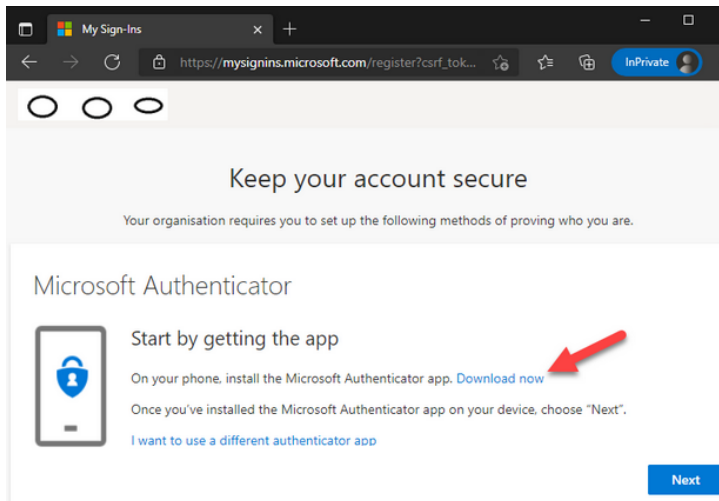
4. Software token on desktop. There are various desktop applications available for Windows and MAC that provide TOTP tokens. These include:
- Password managers such as Bitwarden, Lastpass and 1Password. In some cases you may need to have a paid subscription. Please check its documentation for instructions on how to set this up.
 - Standalone applications such as KeepassXC and Authy. Please check its documentation for instructions on how to set this up.
5. SMS is no longer a valid option as Microsoft will soon no longer allow this. Please see [Security improvements SMS MFA users WMDA services](#)

7

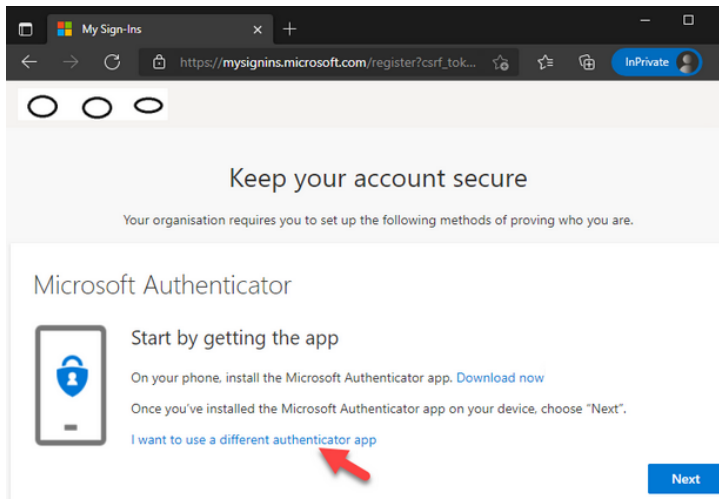
Proceed with setting up your second factor method:

- Microsoft Authenticator
- Other Authenticator app
 - Hardware Token
- Software Token on desktop OS

If you want to use Microsoft authenticator :

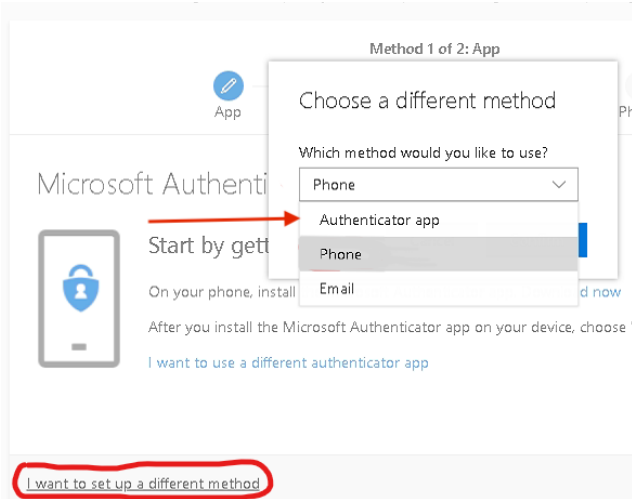


If you want to use another authentication app click the "I want to use a different authenticator app",

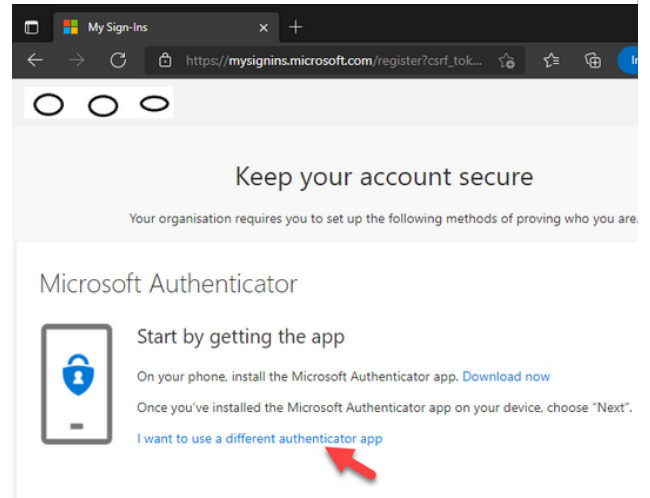


and then select "Authenticator app" from the drop down menu and follow the proceeding instructions.

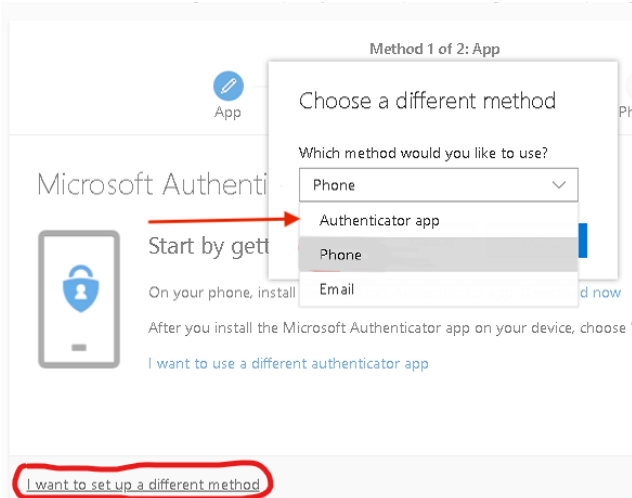
Any authenticator app that is TOTP compliant will be valid to generate codes. Some well known are Google Authenticator, Authy, Aegis



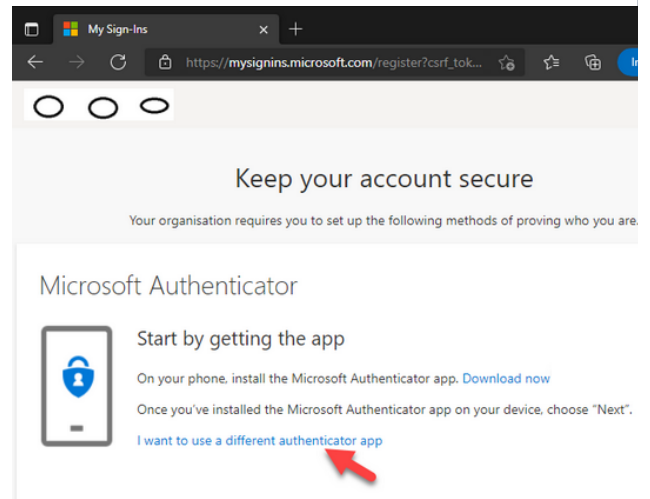
If you want to use a programmable TOTP token, click the "I want to use a different authenticator app"



and then select "Authenticator app" from the drop down menu and follow the proceeding instructions.



If you want to use a software based TOTP token on your desktop, click the "I want to use a different authenticator app"




and then click on "Next"

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Authenticator app



Set up your account

In your app, add a new account.

Back

Next

[I want to set up a different method](#)


You will then see a QR code. If your software is able to scan it, then do that. If not, then click "Can't scan image?"

Authenticator app

Scan the QR code

Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.

After you scan the QR code, choose "Next".



Can't scan image?

Back

Next

[I want to set up a different method](#)

You are then able to see the account name and the secret key. Copy the secret key to your desktop application.

Keep your account secure


Your organization requires you to set up the following methods of proving who you are.

Authenticator app

Scan the QR code

Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.


After you scan the QR code, choose "Next".




Can't scan image?

Enter the following into your app

Account name: WHCA
ServiceUser@whca.gemtrust.nhs.uk@wmdaaservices.onmicrosoft.com

Copy secret key to clipboard

Secret key: qh7m0d3l3ggm5h

Copy secret key to clipboard

Back

Next

[I want to set up a different method](#)

8

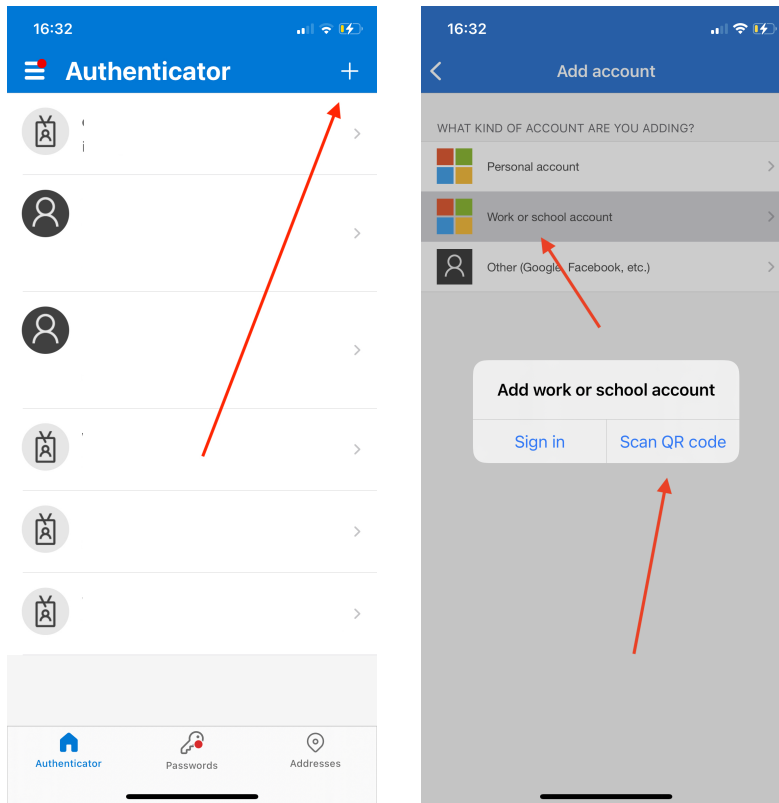
Continue set up:

There are a few more screens to work through, which will vary according to which MFA approach you use.

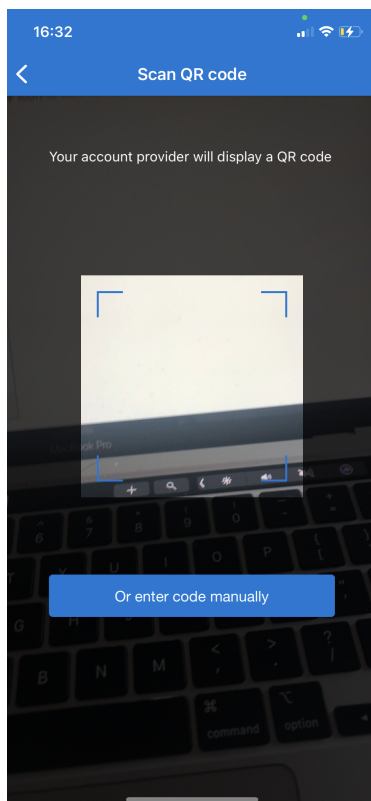
- [Microsoft Authenticator](#)
- [Other Authenticator Apps](#)
- [Hardware token](#)

Open the Microsoft Authenticator app and follow the instructions given.

Firstly click the "+" symbol to add the account and choose the "Work or school account" option, then choose the "Scan QR code" option.



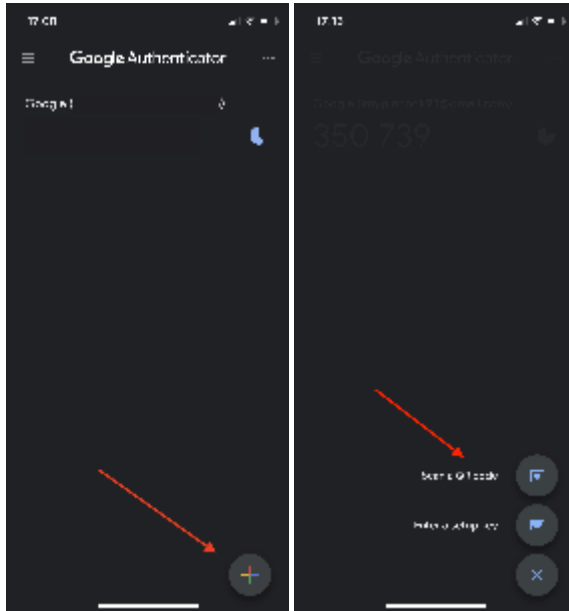
The app will then access your camera, allowing the user to scan the QR code displayed on the webpage on the computer (it is displayed once the user clicks "Next" on the webpage).



Now the authenticator has been set up, head back to the webpage on the computer for the final confirmation.

Example : Google Authenticator

Download the Google Authenticator app and open it up; click the multicoloured "+" and select "Scan a QR code".



The app will now ask for access to the phones camera to scan the QR code displayed on the webpage.

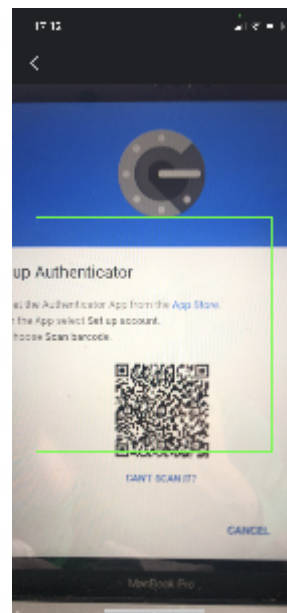
Set up authenticator app

- In the Google Authenticator app tap the +
- Choose Scan a QR code



Can't scan it?

Cancel Next



Hardware tokens will need to be set up, either using NFC or USB.

You need a helper application for that.

In short it works like this :

- 1) put the token in "programming mode"
- 2) approach the token to your phone, the burner app will start
- 3) select "add a profile" , and scan the QR code with your phone.
- 4) burn the code in the token

Due to the diversity of tokens you may want to ask assistance to your IT department.

A sample of a procedure of an NFC programmable token can be found here :

<https://www.token2.com/shop/page/hardware-tokens-for-azure-cloud-multi-factor-authentication>

Please contact us if you have problems setting up your token.

9

Check if the authenticator works

To ensure the MFA was set up correctly, the system will ask the user to verify the authenticator with a verification code, which is displayed on the next page of the app.

Once all complete, you should be brought back to the original home page, and it should show your email in the top right.

Set up authenticator app

Enter the six digit code you see in the app

Back

Cancel Verify

10

Logging in

When logging in, after having set up the MFA, the user will be prompted to approve the login, either by entering the code from your authenticator, or tapping the "Approve" pop up in your application (when using Microsoft authenticator)

The Microsoft Authenticator app will show a notification like the one below -

