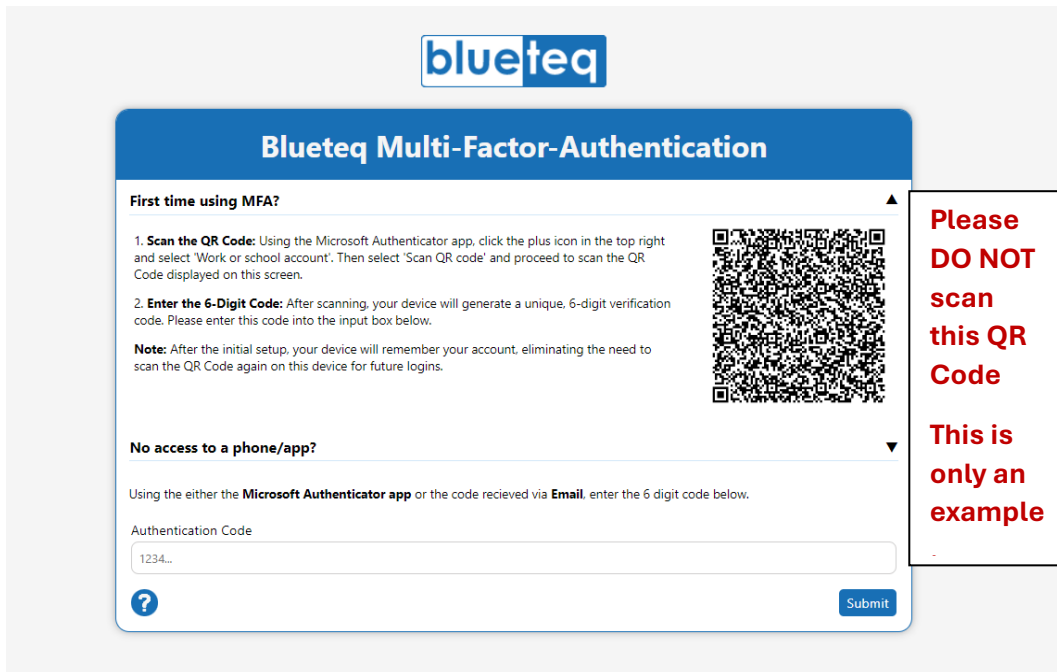


MFA (Multi-factor Authentication) Guide

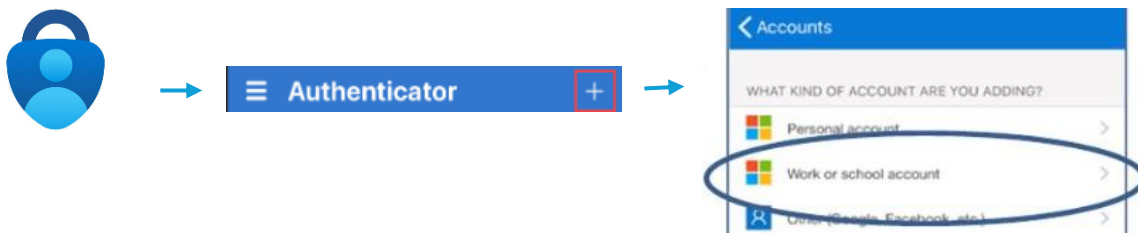
This guide will provide information about MFA and the required steps that you will need to follow for accessing a system using MFA. You will log in to the system in the normal way by entering your user name and password. The system will then display the following screen.



First time use of Multi Factor Authentication

The first time you use the system with MFA will require you to register the application in Microsoft Authenticator and then enter the six digit authorisation code as follows:

1. **Register system with Microsoft Authenticator app:** Using the Microsoft Authenticator app, click the plus icon in the top right and select 'Work or school account'. Then select 'Scan QR code' and proceed to scan the QR Code displayed on this screen.



Please **DO NOT** scan the QR code in this guide, this is only here as an example. Please scan the code which will be presented on your own screen.

2. **Enter the 6-Digit Code:** After scanning, your device will generate a unique, 6-digit verification code. Please enter this code into the input box "Authentication Code" below.

Please Note: The app will generate a new code every 30 seconds.

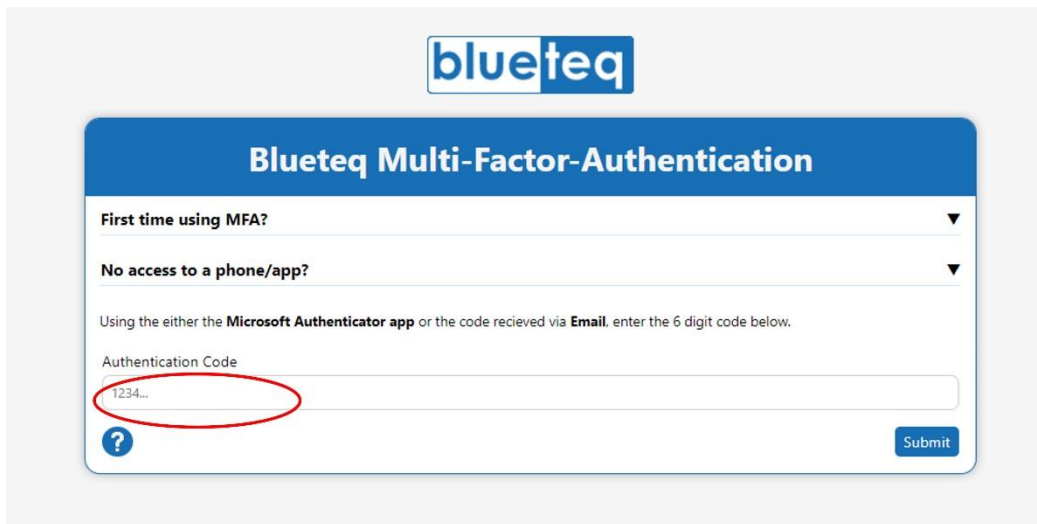
MFA (Multi-factor Authentication) Guide

Using Authenticator after initial Registration

By default the system will require you to enter a code each time you login. This policy may be amended by your organisation in line with their data security policies.

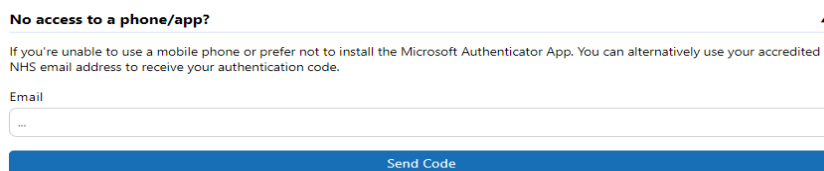
Once you have scanned the code (registered your account for this system) you will only need to:

- 1. Open Microsoft Authenticator**
- 2. Enter the 6-Digit Code:** Please enter the code for the Blueteq Multifactor Authentication into the input box "Authentication Code" below.



The screenshot shows the Blueteq Multi-Factor-Authentication login interface. At the top is the Blueteq logo. Below it is a blue header with the text "Blueteq Multi-Factor-Authentication". There are two dropdown menus: "First time using MFA?" and "No access to a phone/app?". Below these is a text prompt: "Using either the Microsoft Authenticator app or the code received via Email, enter the 6 digit code below." There is an input field labeled "Authentication Code" containing the text "1234...". A red oval highlights this input field. To the left of the input field is a question mark icon, and to the right is a "Submit" button.

No Access to phone/app: If you're unable to use a mobile phone or prefer not to install the Microsoft Authenticator App, you can receive the code via e-mail. The system will send the code to the e-mail address associated with your user account.



The screenshot shows the "No access to a phone/app?" form. It has a dropdown menu with an upward arrow. Below the dropdown is a text prompt: "If you're unable to use a mobile phone or prefer not to install the Microsoft Authenticator App. You can alternatively use your accredited NHS email address to receive your authentication code." There is an input field labeled "Email" containing the text "...". Below the input field is a blue button labeled "Send Code".

- Please make sure that the email address for your account is up to date and is on the NHS Digital accredited list:

<https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#list-of-accredited-organisations>

If you have any problems using the MFA service, please contact Blueteq at the following email address mfa@blueteq.co.uk.