Multi-Factor Authentication

Introduction

Multi-Factor Authentication (MFA) provides an additional layer of security to your NHSmail account when signing in to NHSmail via a web browser. As a Local Administrator (LA) you will have MFA automatically enabled on your NHSmail account.

You will continue to sign in to NHSmail with your username and password. In addition to this, you will be required to authenticate your sign-on via a secondary method (for example, a text message code).

This guide provides guidance on registering for and signing in with MFA.

Why would a Local Administrator need MFA on their account?
MFA helps protect users by making it more difficult for someone else to sign in to their NHSmail account. It uses two different forms of identity: the user’s password, and a contact method. Even if someone else finds the user’s password, they will be prevented from gaining access to the NHSmail account if they do not also have access to the user’s preferred contact method.

Once MFA has been enabled on your account, two-step verification will help keep your NHSmail account secure: a security code will be sent to your mobile phone or generated via the Microsoft authenticator app every time you sign in.

Use of Office Phones for Authentication

Verification of your sign-in can be completed via the Microsoft authenticator app on your mobile device, a security code sent to your mobile device or a telephone call.

The use of the office phone option is not recommended or supported by NHSmail. This option is available to users as Multi-factor Authentication is an off-the-shelf feature that cannot be customised. The limitations observed of using this option are outlined on page 4 of this guide.

The recommended option for verification is to use the Microsoft authenticator app. Mobile phone numbers are stored for the sole purpose of supporting verification and will not be used for other purposes.
Once Multi-Factor Authentication (MFA) is enabled on your account, you will be taken through the set up process the next time you sign in.

Select ‘Click me for Phone Factor Authentication’ to proceed.

Security Notice

For security reasons your account has been identified as one that should use Multi-Factor Authentication, this help protect your account from Phishing attacks and other types of compromise.

You need to enrol into the additional authentication by clicking the link below, this will require you to set up a phone number to receive a call or SMS or use an app on your smartphone to generate a pin number.

Click me for Phone Factor Authentication

Note: After the registration, please close your browser session and re-launch the application.
Once redirected to this page, select ‘Next’ to start. The page below allows you to choose a preferred authentication method.

**Multi-Factor Authentication**

**Setting up Multi-Factor Authentication**

**Microsoft**

mfa.test01@nhs.net

**More information required**

Your organisation needs more information to keep your account secure

- Use a different account
- Learn more

---

**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?**

- **Authentication phone**
- **Select your country or region**

**Method**

- Send me a code by text message
- Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.
Multi-Factor Authentication

Setting up Multi-Factor Authentication

Additional information: choosing the authentication method

There are three options that you can choose from to authenticate your account: mobile app, authentication phone, office phone, or. It is recommended that you choose the mobile app option. The options are described below:

- The ‘Mobile app’ option requires you to download the Microsoft Authenticator app to your smartphone which will prompt you to verify your sign-in attempt. Going forward it will generate a verification code each time you sign in.
- The ‘Authentication phone’ option allows you to receive a text message containing a verification code to enter into the sign-on screen or receive a phone call to verify your sign-in attempt. Please note, the time taken to receive the text message containing your secure code may vary based on your mobile network provider.

The Mobile app and Authentication phone methods are covered in the following sections.

Use of Office Phones for Authentication

Verification of your sign-in can be completed via the Microsoft authenticator app on your mobile device, a security code sent to your mobile device or a telephone call.

The use of the office phone option is not recommended or supported by NHSmail. This option is available to users as Multi-factor Authentication is an off-the-shelf feature that cannot be customised.

Where users choose to use an office phone to verify their sign-in attempt, the following limitations have been observed:
- Office phones must support Dual Tone Multi-Frequency (DTMF).
- Users will require access to the specific office telephone number to verify their sign-in.
- MFA does not support routing of calls via switchboards or other telephony routing services. A direct dial telephone number is required.
- Office phone verification cannot be used by NHSmail Office 365 Hybrid users.

The recommended option for verification is to use the Microsoft authenticator app. Mobile phone numbers are stored for the sole purpose of supporting verification and will not be used for other purposes.
Select ‘Mobile app’ from the menu illustrated below. You will be prompted to choose whether to receive app notifications or a verification code. Click ‘Set up’ once you have made your choice.

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?
- Receive notifications for verification
- Use verification code

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

Set up Please configure the mobile app.

The **Configure mobile app** screen below will provide instructions on how to configure the mobile app. Follow the instructions shown, starting by downloading the **Microsoft Authenticator** app for the mobile device you have – the app can be downloaded onto Windows Phone, Android or iOS devices.
Following downloading the app, open it on your mobile device.

Tap the ‘+’ icon to add an account and select ‘work or school account’.

The Configure mobile app screen will display a QR code. You will be prompted by the Authenticator App to scan the QR code with your mobile device.
Once the app recognises the QR code it will generate a six-digit code (as shown below). This code expires in 30 seconds but a new one will be generated if it is not used in time.

On the Configure mobile app screen on your workstation, choose ‘Next’ to finish configuring the app.
After successful registration of your mobile app, you will receive acknowledgement that ‘mobile app has been configured for notifications and verification codes’. Select ‘Next’ as illustrated below.

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?

- [ ] Receive notifications for verification
- [ ] Use verification code

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

Set up

You will be directed to confirmation from the mobile app.

Additional security verification

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

Step 2: Let’s make sure that we can reach you on your Mobile App device

Please respond to the notification on your device.
On your mobile app, you will be prompted to ‘Approve’ sign-in as illustrated below.

You will be notified verification is successful.

Additional security verification

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

Step 2: Let’s make sure that we can reach you on your Mobile App device

Verification successful. Taking you to the next step...
Multi-Factor Authentication

Mobile App Method Verification

1. Sign-in to your NHSmail account via the NHSmail Portal. You will then be prompted to set up Multi-Factor Authentication.

2. You will be prompted for MFA. Select ‘Approve’ from your mobile app.

For security reasons, we require additional information to verify your account (xxxxx@nhs.net)

We’ve sent a notification to your mobile device. Please respond to continue.

Use a different verification option
Multi-Factor Authentication

Authenticating Phone Method

1. Enter phone details and choose whether to receive a text message with a verification code, or a phone call. This phone number is your preferred contact method, and is not linked to the number listed in your NHSmail Portal profile, i.e. it can be the same number, or you can opt for a different one.

Note:
• It is not expected that you will be charged to use this service as no outgoing calls or messages will be sent during 2-step verification.
• However, standard call and SMS charges may apply if you try to access your account from outside the UK (incurring roaming charges)
• These charges may also apply if your telecommunications provider has set charges for incoming calls or messages

2. Click on ‘Next’ to proceed with authentication. If you have chosen to receive a text, you will be redirected to a verification page – follow the prompt and enter the code. If ‘Call me’ is chosen instead, answer the call and follow the instructions to be verified.

3. You will be directed to further information on use of ‘app passwords’. Please refer to the App Passwords section of this guide for further guidance.
Following setup, you will be directed to a screen with further information on your app password. **Click ‘Finished’** once you have reviewed the information and password.

### Additional security verification

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

**Step 3: Keep using your existing applications**

In some apps, such as Outlook, Apple Mail and Microsoft Office, you can’t use a phone to secure your account. To use these apps, you’ll need to create a new “app password” to use in place of your work or school account password. **Learn more**

Get started with this app password:

[App password]

[Finished]

### Additional information: app passwords

App passwords can be used with legacy non-browser apps that do not support multi-factor authentication. This includes the Office 2010 app suite (or earlier) and Apple Mail.

It is not expected that you will need to use the app password for NHSmail sign-in on the majority of devices. Further information is available from the [Microsoft website on app passwords](#).
Multi-Factor Authentication

Changing authentication method after registration

This section of the guide provides information on how to change your authentication method, for example if your mobile number or your preferences change.


2. Select ‘Additional security verification’ to navigate to your current settings.
From the Additional Security Verification Screen, choose the settings that you wish to change or add.

Changing phone number or adding a secondary number

To change the primary phone number:

1. On the ‘Additional security verification’ page, select the text box with the current phone number and edit it with the new phone number.

2. Select Save. If this is the number used for the preferred verification method, the new number will need to be verified before it can be saved (this will be via text message verification code or phone call). This number is independent of the mobile number listed in your NHSmail Portal profile.
Multi-Factor Authentication

Changing authentication method after registration

To add a secondary phone number:

1. On the ‘Additional security verification’ page, check the box next to ‘Alternate authentication phone’. Enter a secondary phone number in the text box. Select Save and changes are complete.

Adding or switching to mobile app authentication

1. On the ‘Additional security verification’ page, check the box next to ‘Authenticator app’. Select Configure and follow the steps in the mobile app section of this guidance document.
Multi-Factor Authentication

Signing In

1. Following setup, visit [https://portal.nhs.net](https://portal.nhs.net) and select ‘Login’. Sign in with your NHSmail account on the screen below.

2. After entering your login details, the authentication process will default to the verification method you selected. You can also choose a different authentication method if needed.

3. Open the Authenticator app to access the verification code, or have it sent to you via text message or phone call. Once you have entered the code or approved the sign-in attempt you will be logged in.