University of HUDDERSFIELD
Inspiring global professionals

HR Onboarding Portal

Multi-Factor Authentication User Guidance

Contents

What is Multi-Factor Authentication? 3

Authenticator App 3

- Installing an Authenticator App 3
- Registering for Multi-Factor Authentication (MFA) for the Onboarding Portal 4
  - Registering Using Microsoft Authenticator (Camera Method) 5
  - Registering Using Microsoft Authenticator (Manual Code Entry Method) 6
  - Registering Using Google Authenticator (Camera Method) 7
  - Registering Using Google Authenticator (Manual Code Entry Method) 7
- Signing in Using MFA with an Authenticator App 8

Email 9

- Requesting to use email for MFA 9
- Signing in Using MFA via Email 9

Recovering your Account (MFA Reset) 9

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) helps protect your account and personal information by adding an extra layer of security. Instead of relying only on a username and password, MFA asks you to confirm your identity using a second step that only you should have access to. For this system, that second step is a one-time code, which is generated by an authenticator app on your smart phone/tablet or sent to you via email when you try to sign in.

Many people already use MFA on other websites, such as Government Gateway/GOV.UK ONE or online banking, so you may find the process familiar.

To keep your information safe, MFA is required when using the HR onboarding portal. Using an authenticator app on a smartphone or tablet is the most secure option, but if that isn't convenient for you, you can choose to receive your code by email instead.

Authenticator App

The most secure form of MFA is to use an Authenticator App. These apps are available from the App Store on the majority of Apple and Android Devices. This section provides guidance on how to find and install an Authenticator App on your device and how to register to use this with our onboarding portal. If you already have an Authenticator App installed, you can skip the "Installing an Authenticator App" section and move on to the "Registering for Multi-Factor Authentication (MFA) for the Onboarding Portal" section.

Installing an Authenticator App

Installing an Authenticator App is quick and simple and can be done from your device's App store. This will be:

- App Store for Apple iPhone/iPad 
- Play Store for Android Devices 

Once the App Store is open, use the search box to search for "Authenticator".

There are several authenticator apps available, but we recommend either:

- Microsoft Authenticator
- Google Authenticator

Both are available on Apple and Android devices and have been confirmed to work with our onboarding portal.

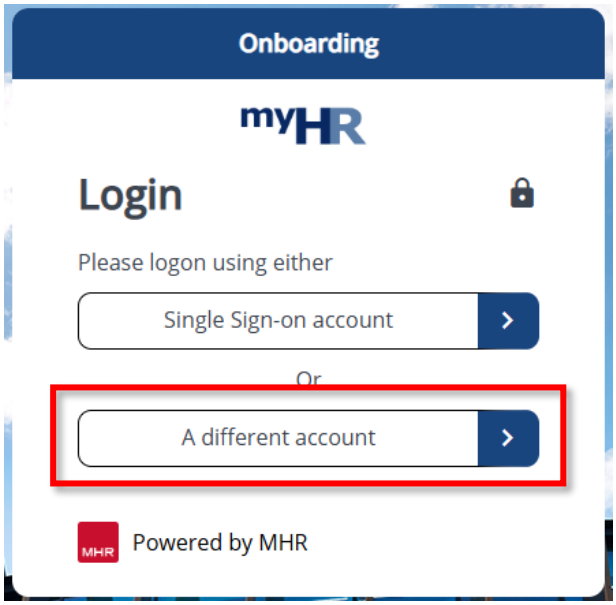
Tap Install, and the app will be downloaded to your device.

Once the installation is complete, you are ready to register for MFA.

Registering for Multi-Factor Authentication (MFA) for the Onboarding Portal

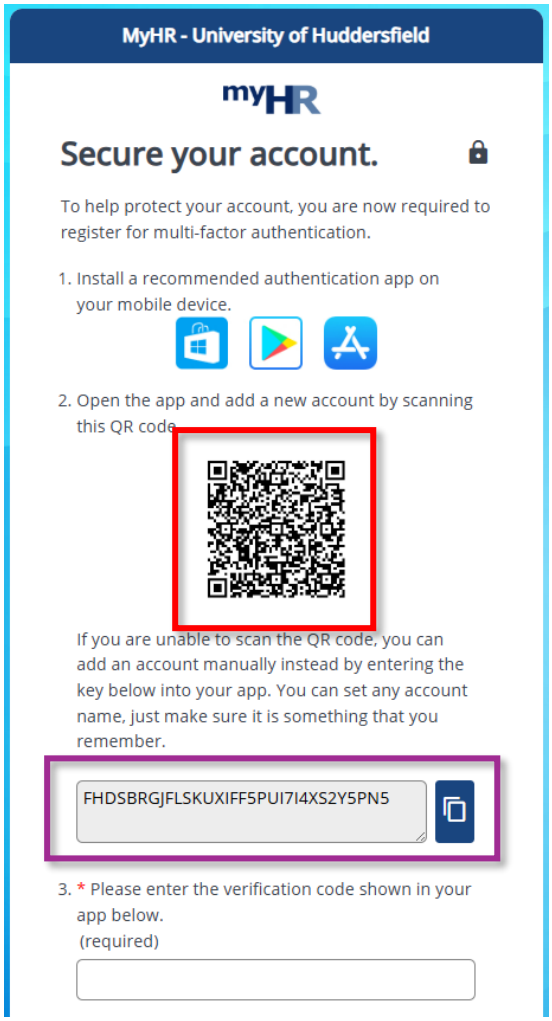
Registering your device for MFA is quick and simple and these steps are similar for both Microsoft and Google Authenticator.

When you click on the link for the onboarding portal in your email from HR select the “A different account” option:



Enter your username and password and click login.

You will then be asked to register for MFA. The screen will look like the below:



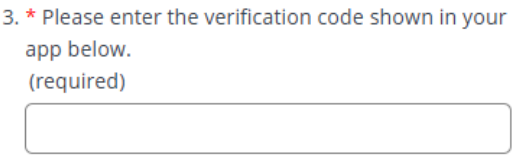
From this page, you can register to use MFA using the camera on your phone to scan the QR Code or use the Secret Key/Setup Code to manually add the onboarding page to your Authenticator App. If you will be registering for MFA using the Secret Key/Setup Code, you can click on the button next to the field to copy the code to your clipboard so you can paste it directly into your Authenticator App.

Registering Using Microsoft Authenticator (Camera Method)

To register for the onboarding portal using Microsoft Authenticator, follow the steps below:

1. Open Microsoft Authenticator and tap on the + button in the top right corner.
2. When asked what kind of account you are adding, select “Other (Google, Facebook, etc)”
3. The app will open your phone’s camera. If prompted, allow camera access.
4. Point your phone at the QR code on your computer screen so it fits inside the square on your screen.
5. You will be returned to the main Authenticator screen where your accounts are listed.

6. Find the new account. A six-digit code will be displayed next to it, along with a small timer.
    - The code changes every 30 seconds.
    - The timer shows when the next code will appear.
7. Enter the six-digit code into the field shown below on the Onboarding Portal page:

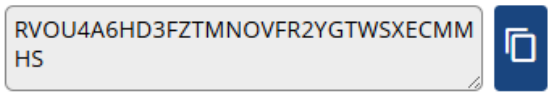


8. Click Continue. A recovery code will appear. Please record this code somewhere safe, it will make recovering your account easier if you lose access to your device.
9. Click continue again. You will now be signed in to the Onboarding Portal.

Registering Using Microsoft Authenticator (Manual Code Entry Method)

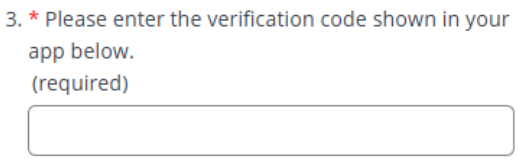
If the QR code does not work, or you would prefer to manually enter the code, follow the steps below:

1. Open Microsoft Authenticator and tap on the + button in the top right corner.
2. When asked what kind of account you are adding, select “Other (Google, Facebook, etc)”
3. When the camera opens, tap “Enter code manually”.
4. Enter an account name. Use something easy to recognise, such as “UoH Onboarding Portal”.
5. In the Secret key field, type the long code shown on the registration page. It will look like this:



6. Tap “Finish”.
10. You will be returned to the main Authenticator screen where your accounts are listed.
11. Find the new account. A six-digit code will be displayed next to it, along with a small timer.
    - The code changes every 30 seconds.
    - The timer shows when the next code will appear.

12. Enter the six-digit code into the field shown below on the Onboarding Portal page:

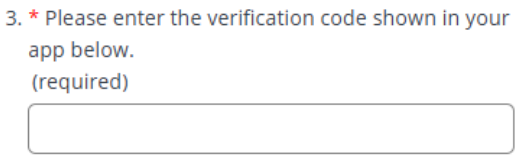


13. Click Continue. A recovery code will appear. Please record this code somewhere safe, it will make recovering your account easier if you lose access to your device.
14. Click continue again. You will now be signed in to the Onboarding Portal.

Registering Using Google Authenticator (Camera Method)

To register for the onboarding portal using Google Authenticator, follow the steps below:

1. Open Google Authenticator and tap on the + button in the bottom right corner.
2. Tap on "Scan a QR code" from the options
3. The app will open your phone's camera. If prompted, allow camera access.
4. Point your phone at the QR code on your computer screen so it fits inside the square on the screen.
5. You will be returned to the main Authenticator screen where your accounts are listed.
6. Find the new account. A six-digit code will be displayed for it, along with a small timer.
    - The code changes every 30 seconds.
    - The timer shows when the next code will appear.
7. Enter the six-digit code into the field shown below on the Onboarding Portal page:



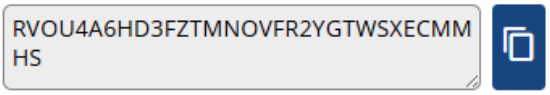
8. Click Continue. A recovery code will appear. Please record this code somewhere safe, it will make recovering your account easier if you lose access to your device.
9. Click continue again. You will now be signed in to the Onboarding Portal.

Registering Using Google Authenticator (Manual Code Entry Method)

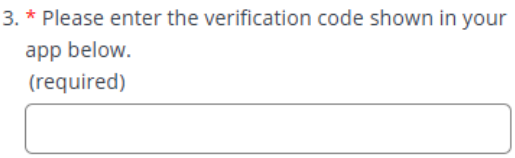
If the QR code does not work, or you would prefer to manually enter the code, follow the steps below:

1. Open Google Authenticator and tap on the + button in the bottom right corner.
2. Tap on "Enter a setup key" from the options

3. Enter an account name. Use something easy to recognise, such as “UoH Onboarding Portal”.
4. Enter the long code shown on the registration page into the “Your key” field. The code will look like this:



5. The type of key should default to “Time based”. Leave this value unchanged. If it is set to “Counter based” change this to “Timer based”.
6. Tap “Add”.
10. You will be returned to the main Authenticator screen where your accounts are listed.
11. Find the new account. A six-digit code will be displayed next to it, along with a small timer.
    - The code changes every 30 seconds.
    - The timer shows when the next code will appear.
12. Enter the six-digit code into the field shown below on the Onboarding Portal page:



13. Click Continue. A recovery code will appear. Please record this code somewhere safe, it will make recovering your account easier if you lose access to your device.
14. Click continue again. You will now be signed in to the Onboarding Portal.

Signing in Using MFA with an Authenticator App

Once you have registered for MFA, you will need to use this every time you sign in to the Onboarding portal.

The process to do so will be the same regardless which authenticator app you are using.

1. Navigate to the Onboarding portal.
2. Select the “A different account” option.
3. Enter your username and password and click login.
4. You will be asked to enter a verification code from your authenticator app.
5. Open your authenticator app on your device.
6. Find the account on the authenticator main page.
7. Enter the six-digit number into the field on the Onboarding portal login page.
8. If the code you have entered is correct, you will be signed in to the onboarding portal.

Email

Multi-factor Authentication by email works by sending an email containing a single use code to your registered email address, and does not require any installation of a third-party authenticator app.

Please note that while we provide the option to use email for MFA, we strongly recommend that you use an authenticator app as this offers the highest level of protection.

Requesting to use email for MFA

To request to use email for MFA, please contact the recruitment team at hr@hud.ac.uk and ask for this to be setup for you.

Once this has been done, the recruitment team will reply to your email to confirm this.

Signing in Using MFA via Email

Once you have received confirmation for the recruitment team that your account is set up to use MFA via email, you can sign in to the onboarding portal by following the steps below:

1. Navigate to the Onboarding portal.
2. Select the “A different account” option.
3. Enter your username and password and click login.
4. Check your email, you should receive an email from hr@hud.ac.uk with the subject “MFA Verification code”.
5. Open this email. You will see a six-digit code. This is your verification code and will remain valid for five minutes. If you do not use the code within this time, you will need to request a new code clicking on the “Resend email” button on the login page.
6. Enter the six-digit number into the field on the Onboarding portal login page.
7. If the code you have entered is correct, you will be signed in to the onboarding portal.

Recovering your Account (MFA Reset)

If you previously registered for Multi-Factor Authentication (MFA) but can no longer access your verification codes, for example, because you changed your device or removed the account from your Authenticator app, you can recover access using your MFA recovery code.

To do this, you will need to have the recovery code that you were given when you first registered for MFA. If you no longer have your recovery code, you will not be able to recover your account yourself and should contact the HR team at hr@hud.ac.uk for assistance.

To recover your account with your recovery code, follow the steps below:

1. Navigate to the Onboarding portal.
2. Select the "A different account" option.
3. Enter your username and password and click login.
4. When you are asked to enter your verification code, click on the option to "Re-register"

5. You will then be asked for your recovery code. Enter the recovery code and click continue.
6. You will then be taken to the MFA registration page where you can re-register. Guidance on how to register is available in the "Registering for Multi Factor Authentication (MFA) for the Onboarding Portal" section of this guide.