The James Hutton Institute MFA User Guide

MFA for Guest Microsoft 365 users

Contents

This user guide is for External Guest users to help setup MFA (Multi-Factor Authentication)

This is required to access The James Hutton Institutes Microsoft 365 services such as Teams.

Background

Multi-Factor Authentication (MFA) is a layer of protection designed to help secure the data shared within The James Hutton Institutes Microsoft 365 service. The following steps may be the same or slightly different for setting up access within your own organisation if they use Microsoft 365.

The James Hutton Institutes requires all users to provide secondary authentication to gain access.

Am I a guest?

If you are outside of The James Hutton institute network, i.e. you don't have a **@hutton.ac.uk** email address then you are treated as a guest.

What do I have to do?

When a member of the institute shares a file, folder or invite to a Teams / SharePoint site with you, you are asked by Microsoft to verify your identity.

Guests will be asked to set up MFA for enhanced security and data protection.
Please use the instructions in this guide to help you set up MFA when prompted.

Setting up MFA as a Guest

When you are invited to collaborate with the institute an email will be sent from someone at the institute which will contain a link.

1. Depending on where the invitation was generated it will look like one of the following.
2. To start the process of setting up MFA, click on the link. "**Accept invitation**" or "**Open Microsoft Teams**".
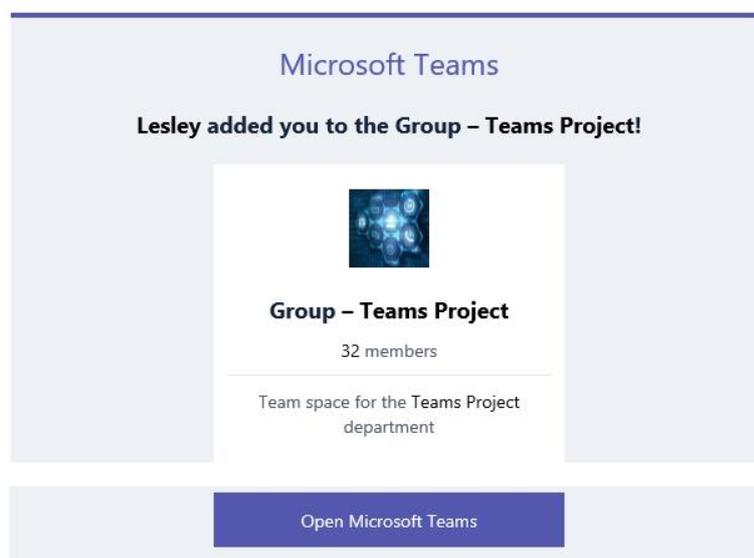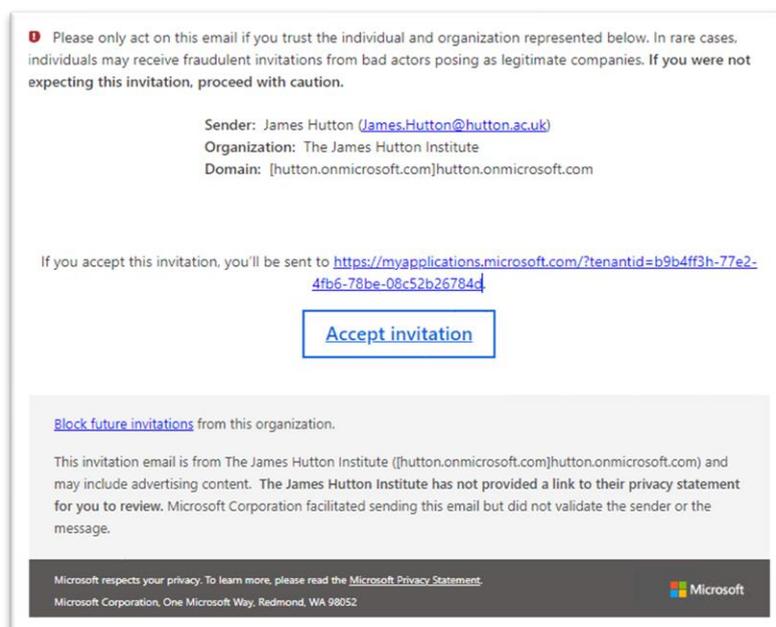
3. If you select "Open Microsoft Teams" you will be presented with the option to "**Download the Windows app**" or "**Use the web app instead**". Please proceed as you wish.

4. When we share this to your "Guest" email address, if your account is NOT a Microsoft account you will need to setup an "External Guest" account with us. If you have your own MFA enabled on this account (e.g gmail) you may be prompted to enter a code first.
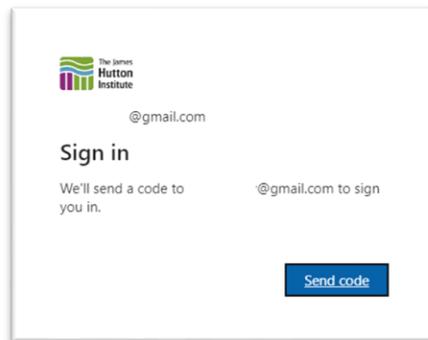
5. Once you have done this, or if your account is already a Microsoft 365 account, you will be asked to review permissions as shown below. Click **Accept**
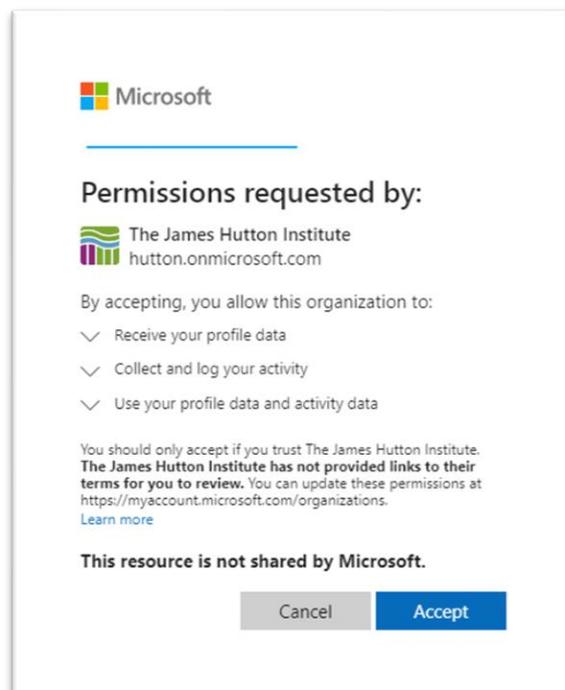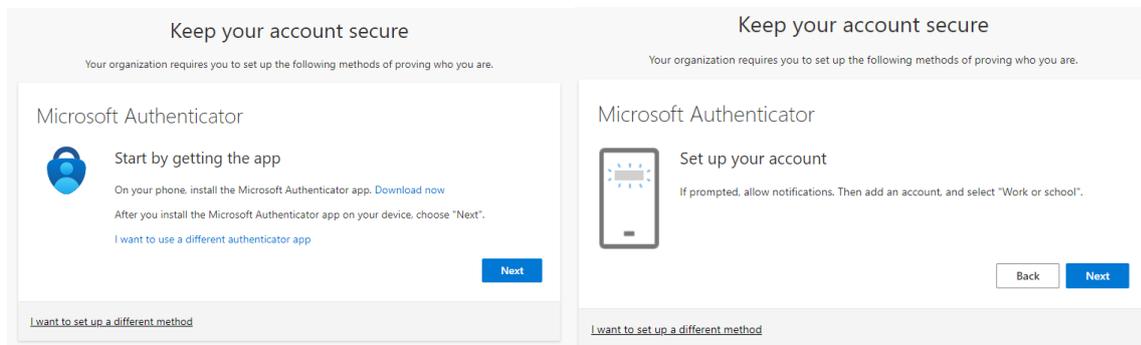
6. You should now be prompted with "**More information required**", Click **Next**
   You will be taken to the <u>**Keep your account secure**</u> page.
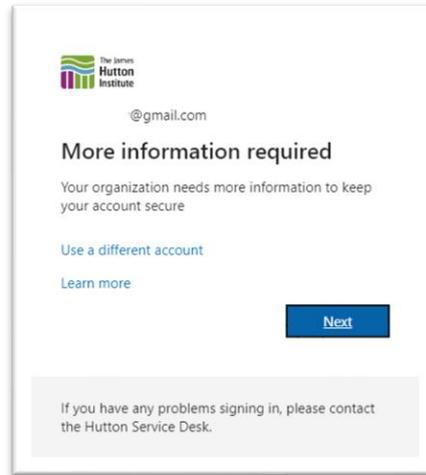

MFA Setup Instructions

1. Click **Next** on the following 2 pages:

Note: We recommend that all Hutton Guest users use the Microsoft Authenticator app.
This is the recommended method as it offers the best experience if using a smartphone.
The Microsoft Authenticator app can be downloaded from your smartphone's app store.

2. Once installed, open the app and press the **+** button at the top. Select "**Work or school account**" then select "**Scan a QR code**"
This will use the devices camera to help scan the QR code on the screen.
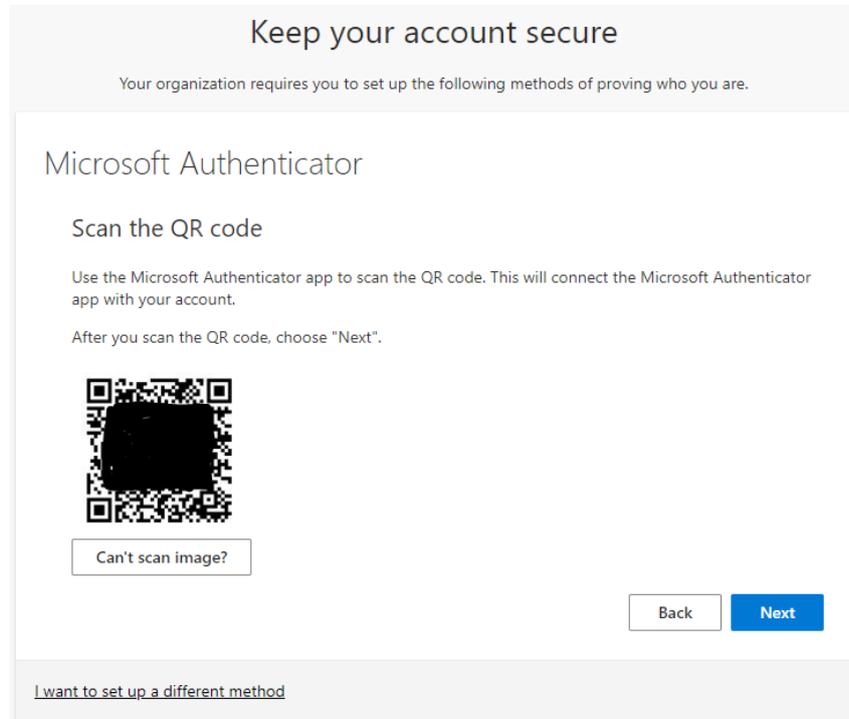
3. Clicking **Next** will generate a test code which you can enter in the Authenticator to ensure it is working correctly.
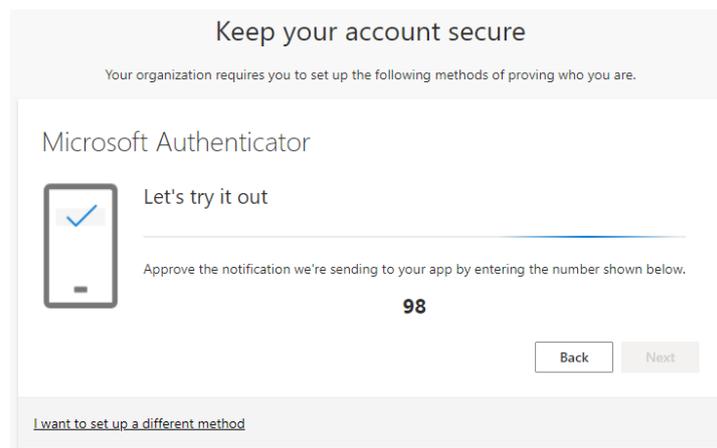
4. Click **Next** then **Done.**

All the steps above are part of the initial set up and once this has been completed, you won't be asked again.

Experiencing Issues?

All staff and students at The James Hutton Institute have been through the MFA set up.

process. In the first instance, please ask the person sharing information with you for support.

Additionally, many organisations and companies now use the same or similar two factor authentication methods, please ask your local IT team for support.

If you still require assistance, you can contact our IT Service Desk at **GuestAccess@hutton.ac.uk** Please note that we can only provide limited support.