

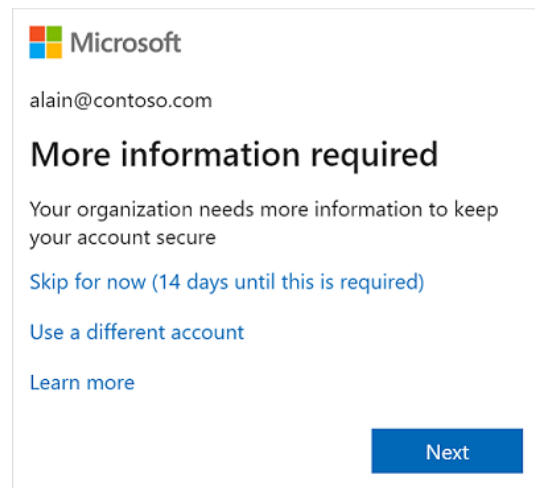
Securing your Office 365 account with Multi-Factor Authentication (MFA) & Self Service Password Reset (SSPR)

To ensure that your Office 365 account remains secure it will at times ask you to confirm your identity by using an app or inputting a code that will be sent to your phone. This is called Multi-Factor Authentication (MFA)

To make it easier for you to reset your password, you can do this yourself, rather than calling the Service Desk, by setting up Self Service Password Reset (SSPR). This guide will show you how to register for both.

Note: You will need to have your computer and mobile device to hand

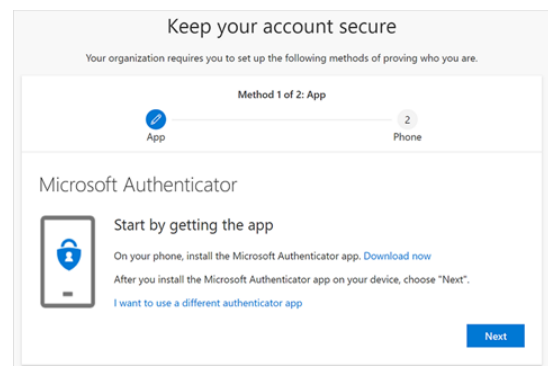
1. When you sign in to your NHS O365 account, you will be asked for your user ID and password. You will then see a prompt that asks you to provide more information before it lets you access your account. Select **Next**.



After you select Next from the prompt, a **Keep your account secure wizard** appears, showing the first method your administrator and organisation require you to set up.

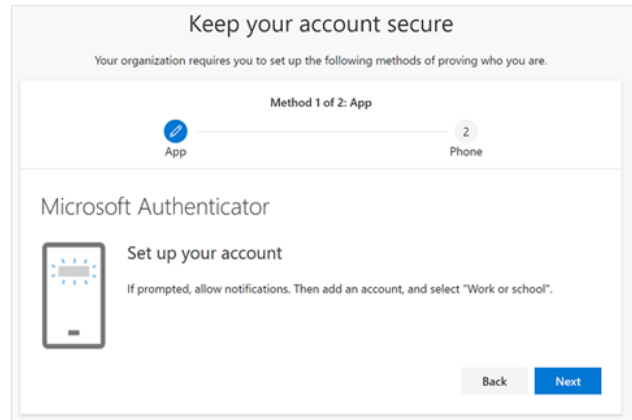
For this example, it is the Microsoft Authenticator app. If you want to choose a different method besides the authenticator app, select the *I want to set up a different method* link.

2. Select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**.

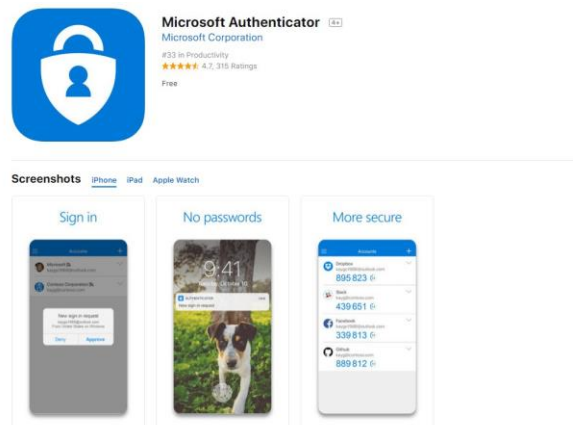


For more information about how to download and install the app, see [Download and install the Microsoft Authenticator app](#).

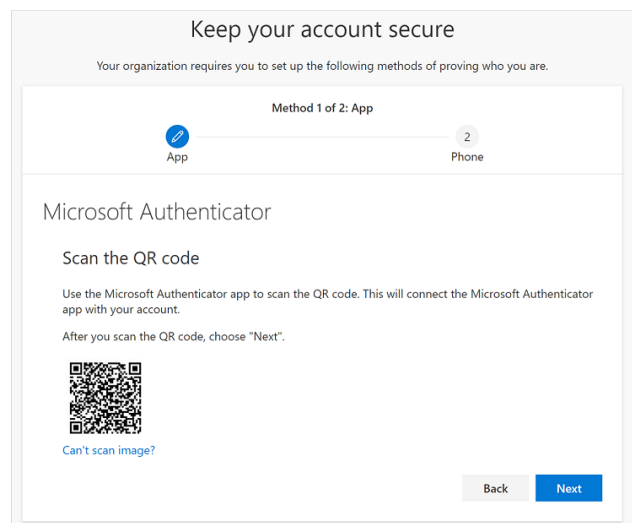
3. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device.



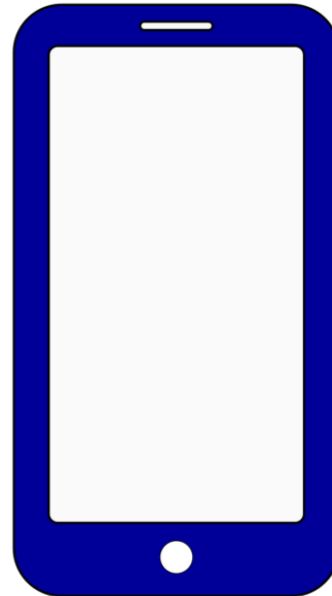
4. Set up Microsoft Authenticator on your mobile device.



5. Return to the **Set up your account** page on your computer, and then select **Next**. The **Scan the QR code** page appears.



6. On your mobile device, open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select **Work or school account**.
Note: If this is the first time you're setting up the Microsoft Authenticator app, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually. For information about how to add the code manually, see [Manually add an account to the app](#).



7. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your account in Step 4. The authenticator app should successfully add your NHSS account without requiring any additional information from you. However, if the QR code reader can't read the code, you can select the **Can't scan the QR image** and manually enter the code and URL into the Microsoft Authenticator app. For more information about manually adding a code, see [Manually add an account to the app](#).

8. Select **Next** on the **Scan the QR code** page on your computer. A notification is sent to the Microsoft Authenticator app on your mobile device, to test your account.

Keep your account secure

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

Method 1 of 2: App

2

App


Phone

Microsoft Authenticator

Scan the QR code

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

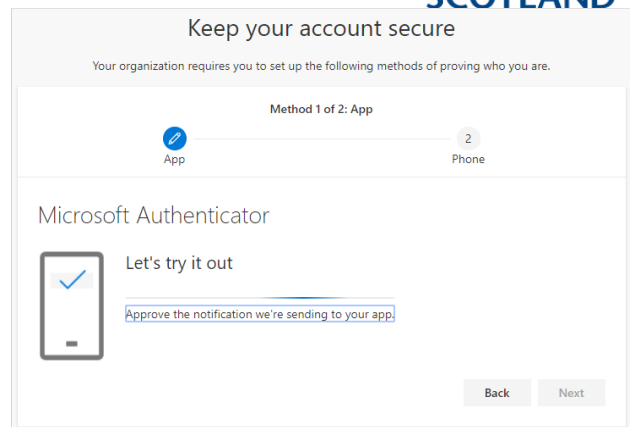
After you scan the QR code, choose "Next".



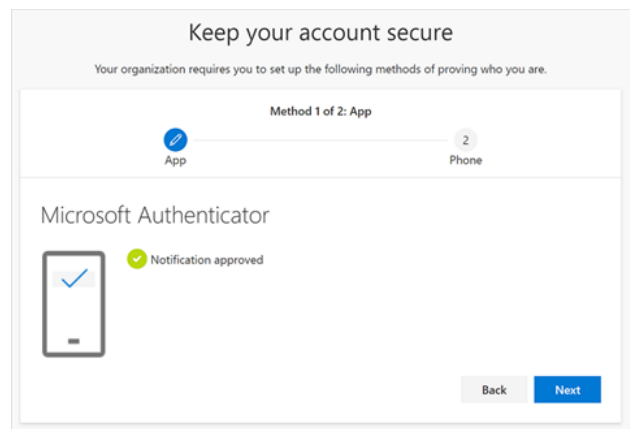
Can't scan image?

BackNext

9. Approve the notification in the Microsoft Authenticator app on your phone, and then select **Next**.

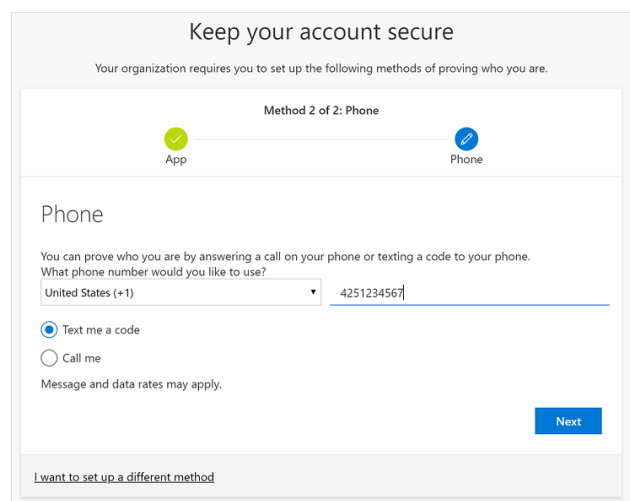


Your security info is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

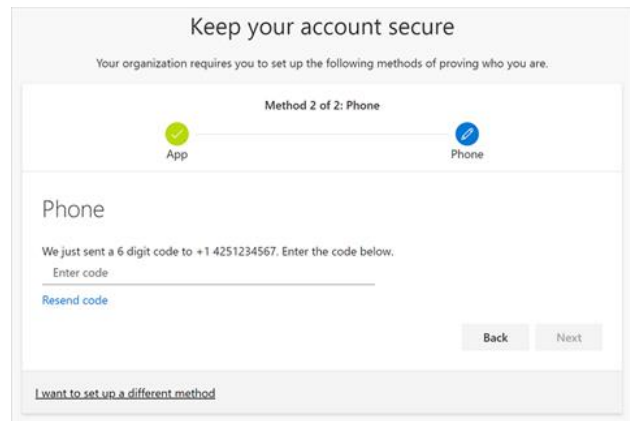


10. On the Phone set up page, choose whether you want to receive a text message or a phone call, and then select Next. For the purposes of this example, we're using text messages, so you must use a phone number for a device that can accept text messages.

A text message is sent to your phone number. If you would prefer to get a phone call, the process is the same. However, you'll receive a phone call with instructions, instead of a text message.



11. Enter the code provided by the text message sent to your mobile device, and then select **Next**. A text message is sent to your phone number. If you would prefer to get a phone call, the process is the same. However, you'll receive a phone call with instructions, instead of a text message.



Keep your account secure

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

Method 2 of 2: Phone

App Phone

Phone

We just sent a 6 digit code to +1 4251234567. Enter the code below.

Enter code

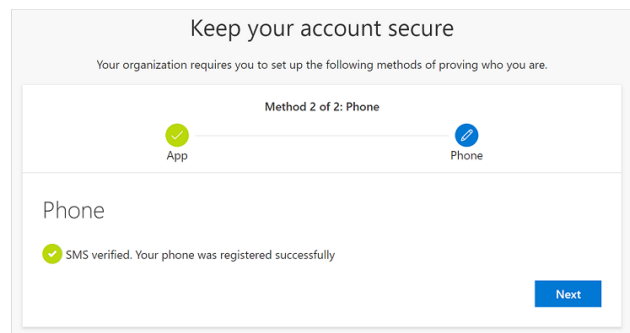
Resend code

Back Next

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

12. Review the success notification, and then select **Done**.

Your security info is updated to use text messaging as a backup method to verify your identity when using two-step verification or password reset.



Keep your account secure

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

Method 2 of 2: Phone

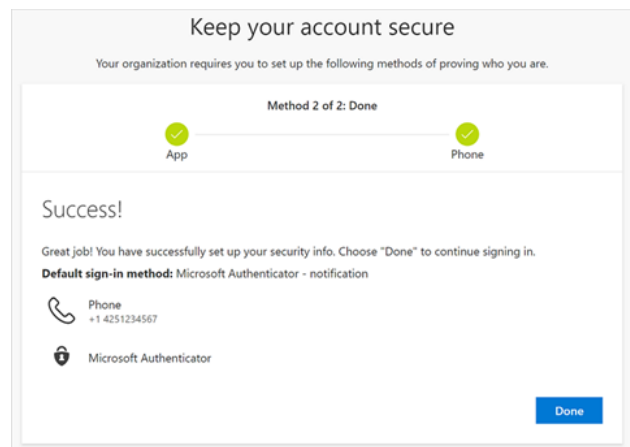
App Phone

Phone

SMS verified. Your phone was registered successfully

Next

13. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app and a phone (either text message or phone call) method for your security info, and then select **Done**.



Keep your account secure

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

Method 2 of 2: Done

App Phone

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Microsoft Authenticator - notification

Phone +1 4251234567

Microsoft Authenticator

Done

Note on Information Security & Governance.

The SSPR / MFA app will never ask you to allow it to:

- Read and write your files.
- Read your calendar.
- Sign you in and read your profile.

If you recognise this, or other unusual activity, do not continue and notify your local helpdesk.

Further information

- To change, delete, or update default security info methods, see:
 - [Set up security info for an authenticator app.](#)
 - [Set up security info for text messaging.](#)
 - [Set up security info to use phone calls.](#)
 - [Set up security info to use email.](#)
 - [Set up security info to use pre-defined security questions.](#)
- For information about how to sign in using your specified method, see [How to sign in.](#)
- Reset your password if you've lost or forgotten it, from the [Password reset portal](#) or follow the steps in the [Reset your work or school password](#) article.
- Get troubleshooting tips and help for sign-in problems in the [Can't sign in to your Microsoft account](#) article.