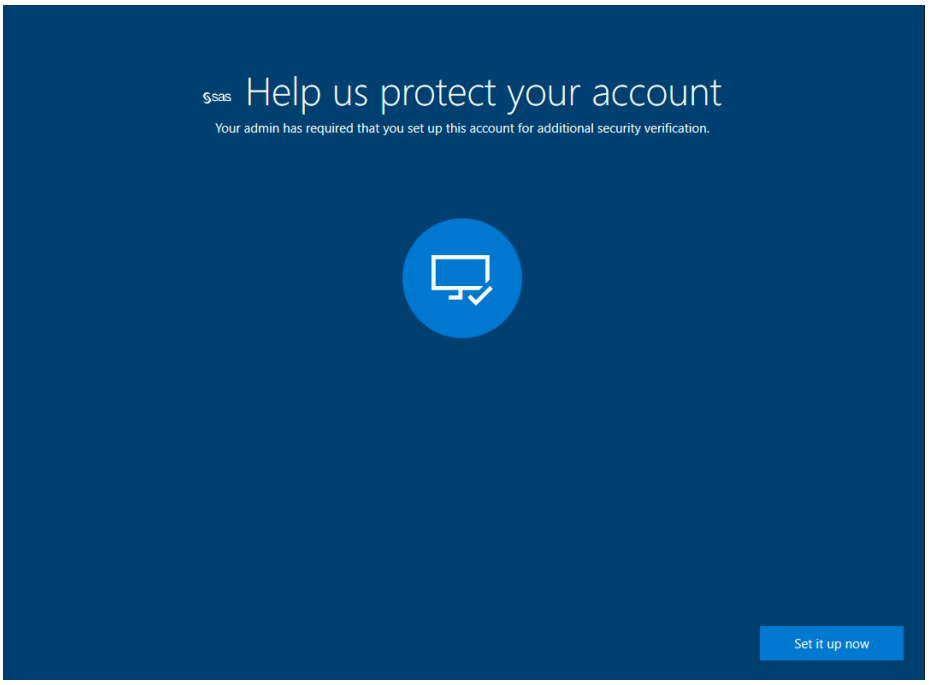
Windows Autopilot Enrollment — Azure MFA Setup

When provisioning your corporate owned Windows device, you will be required to have Multi-factor Authentication (MFA) set up in advance. MFA is an authentication process that is used to confirm a SAS employee's identify for a second time, and is required when accessing certain SAS resources and applications. If you have not configured MFA ahead of time, on-screen instructions are provided on your device to walk you through each step of the process.

You are required to **set up two methods** as this process is used to reset your SAS password in the instance that it is forgotten or needs to be reset. You will need to have either your corporate or personal phone present, as the Microsoft Authenticator mobile app is a preferred method.

MFA is typically sent via:

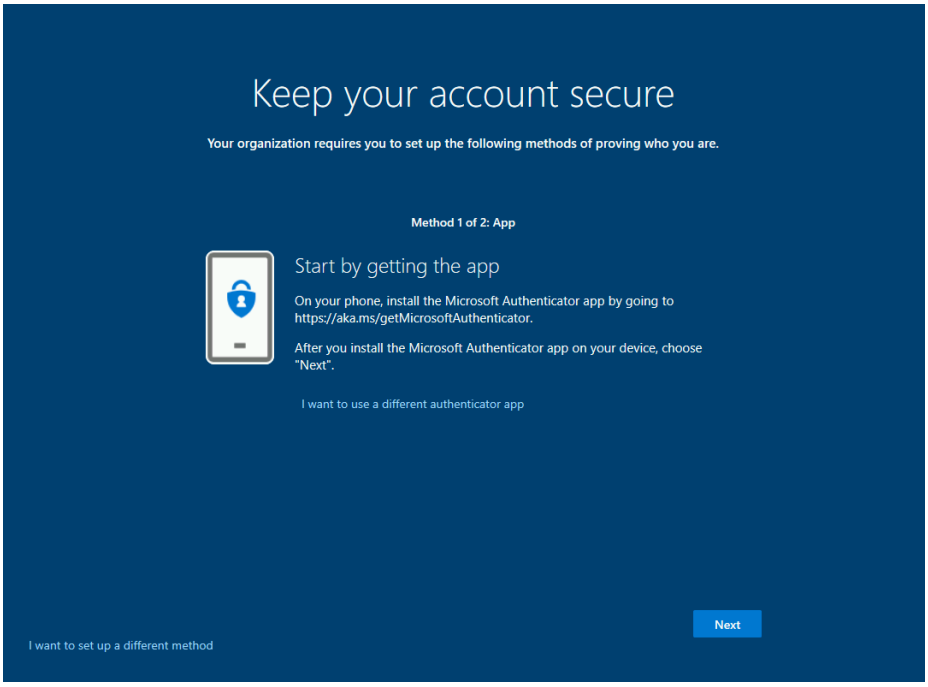
- a prompt sent through a mobile app for approval (Authenticator)
- a code texted to your personal or corporate mobile phone



Method 1: Microsoft Authenticator Mobile App

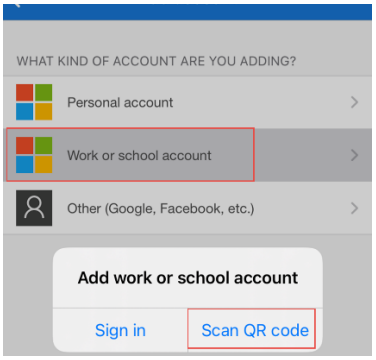
The Microsoft Authenticator app is the preferred option for MFA and will provide the best user experience. Third party authenticator applications are not supported by SAS but may be used on devices you control and are password/passcode protected.

1. On your mobile device, install the Microsoft Authenticator app by going to https://aka.ms/getMicrosoftAuthenticator

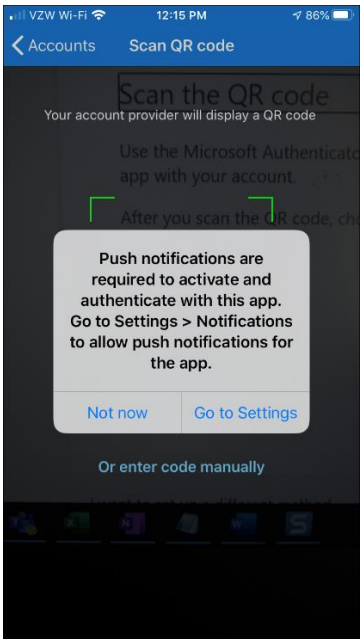


2. Once installed, select **Next** on your computer screen.

3. Open Authenticator on your mobile device. Select Add account (**+**) and choose **Work or school account**. Now, select **Scan QR code.**

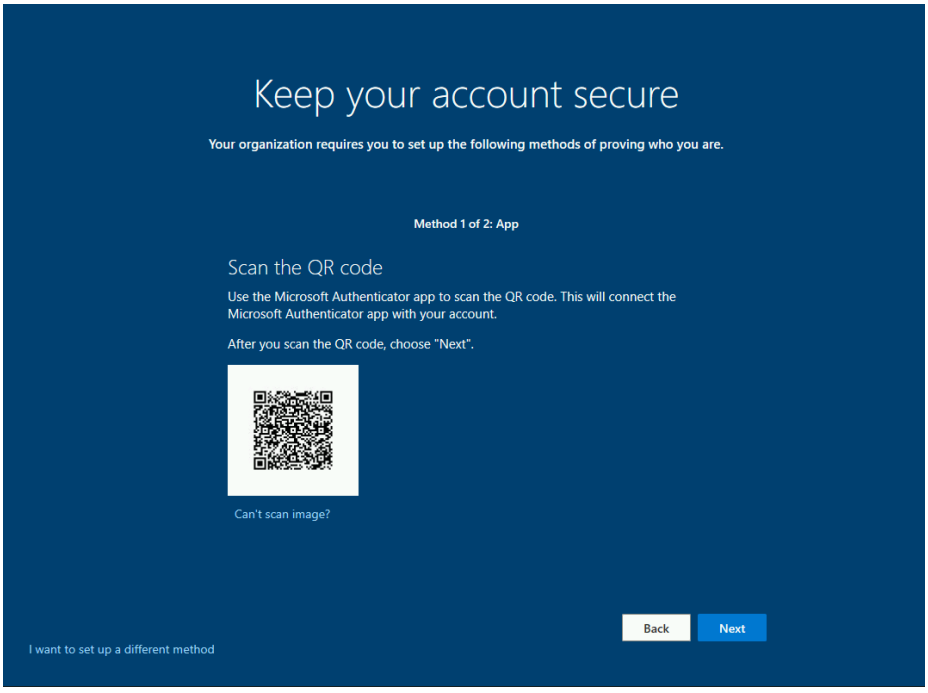


4. If prompted, allow push notifications. On an iPhone, push notifications for Authenticator can be managed within Settings > Notifications > Authenticator.

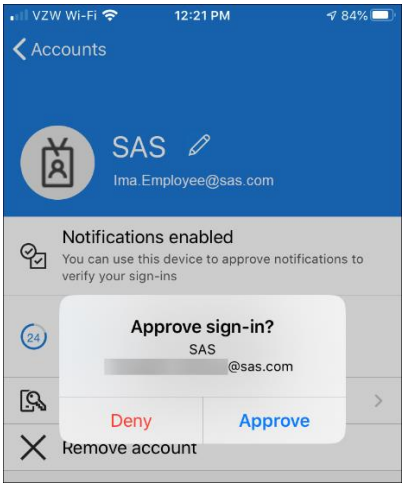


5. On the Authenticator app, scan the QR code that is currently displaying on your computer screen. (*Note: You may have to go into the Authenticator settings and enable camera access if it's currently disabled.*)

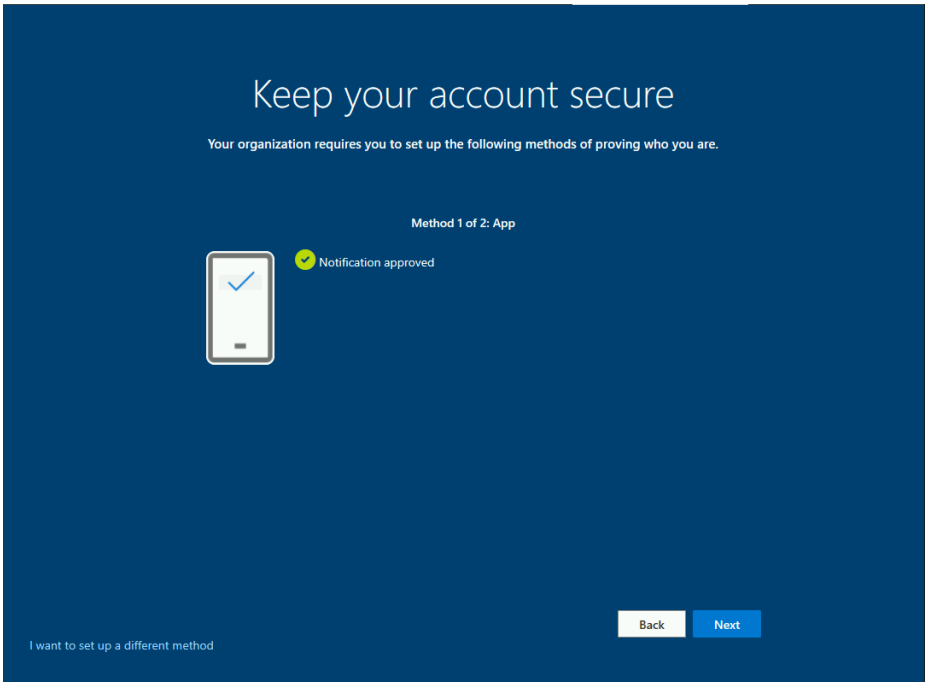
If the QR code reader is unable to read the code, select the **Can't scan image?** link displayed on your computer, and you can manually enter the code into the Authenticator app.



6. Once scanned or entered, a notification is sent to the Authenticator app on your mobile device to test your account. Select **Approve**.



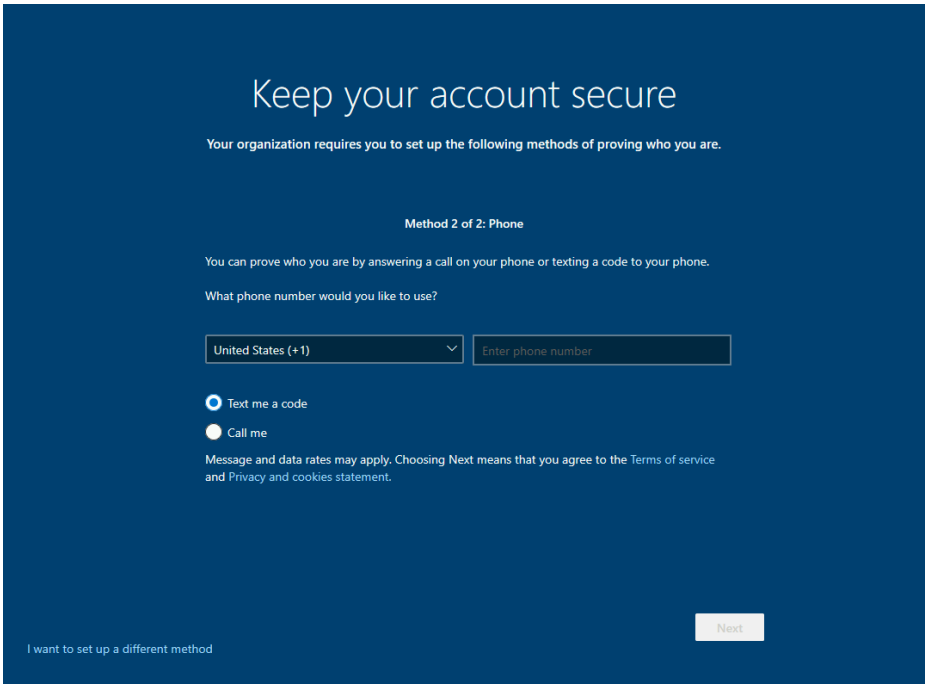
7. Success! The notification was approved and Authenticator is now registered. Select **Next** to continue. You are required to register **two** methods of authentication.



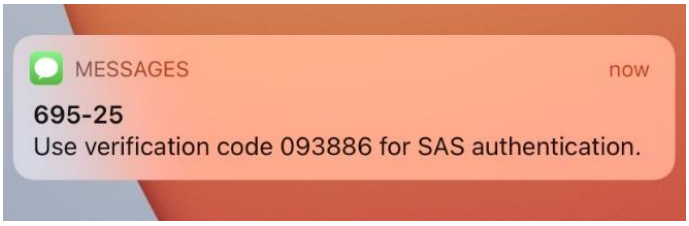
Method 2: Phone

To continue, you will need to set up a second form of authentication. You can choose between either SMS (text) or a phone call. Discussed below, are instructions to configure the SMS text option.

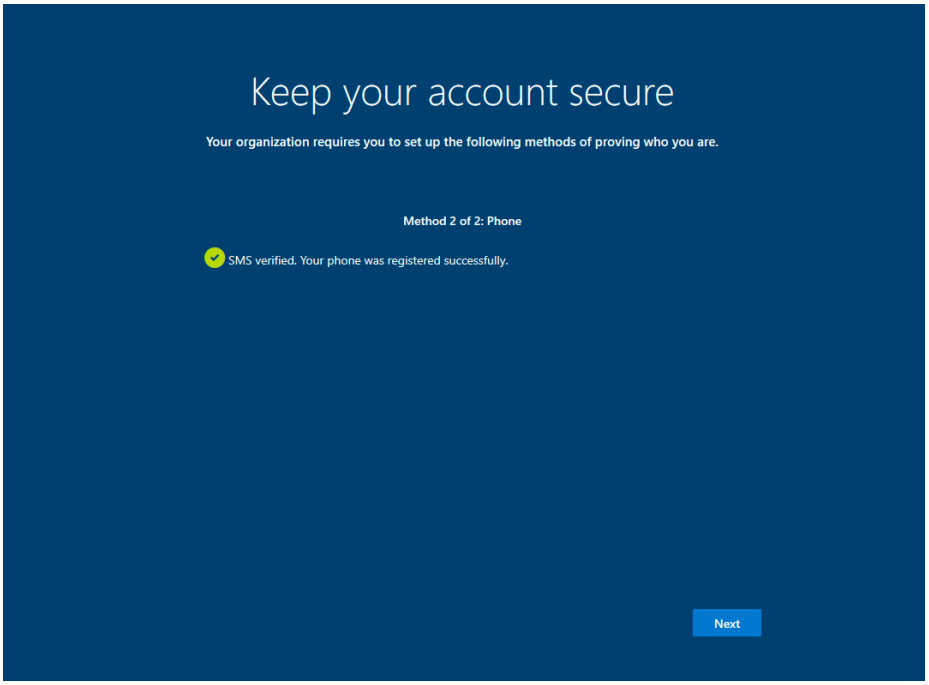
1. Enter your phone number and choose either the text or call option. Click **Next**.



2. Enter the code you received via text message. Click **Next**.

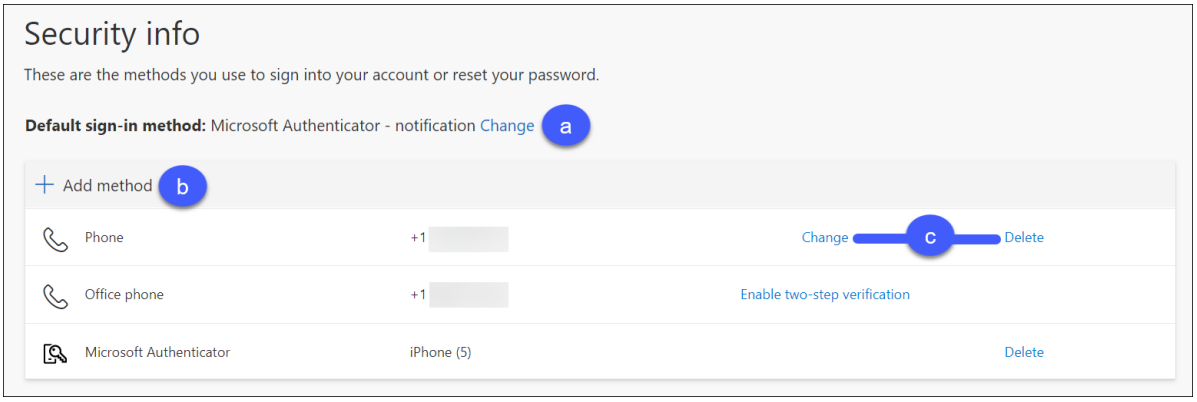


3. Success! SMS is verified and your mobile phone is now registered. Click **Next** to complete the MFA setup.



Manage MFA Default Sign-in Method and Devices

You may receive MFA prompts from other apps, like Outlook and OneDrive. Simply sign into the apps with your SAS email address and password and accept the prompt to authenticate with MFA. In the instance that you would like to manage your MFA sign-in methods and devices, go to https://mysignins.microsoft.com/security-info.



a. To change your default sign-in method, click **Change**. (Ex. change your sign-in method from SMS text to the Authenticator app.)
b. To add a new device or authentication method, click **Add method**. The setup wizard will walk you through the setup process.
c. To remove or edit a device or authentication method, click **Change** or **Delete** next to the option you want to change or remove.