

# SAS Azure MFA Setup Instructions

Last Updated: 9/8/2021

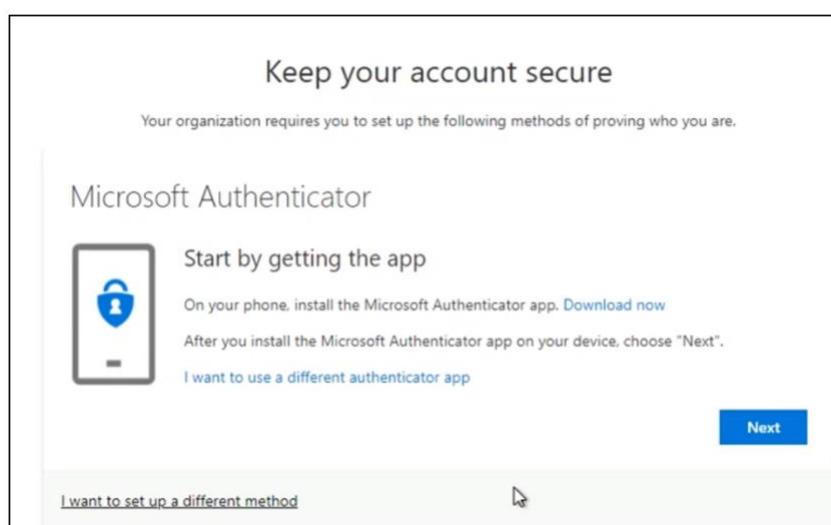
***This information applies to Employees and 3<sup>rd</sup> party contingent workers who have been provisioned a SAS account.***

You will need to use both your phone and a computer when following the instructions below. If you are setting up a new SAS machine, you will need to perform these tasks on two different devices other than the new machine – one to display the QR code, one to scan it. **You are required to set up two methods** as this process will be used to reset your SAS password if you forget it or need to reset it.

The **Microsoft Authenticator** App is the preferred option for MFA and will provide the best experience and may be required for future plans to changes in sign-in options. SMS text is the recommended second method. 3rd party authenticator applications are not recommended or supported by SAS but may be used in circumstances where mobile device access is unavailable.

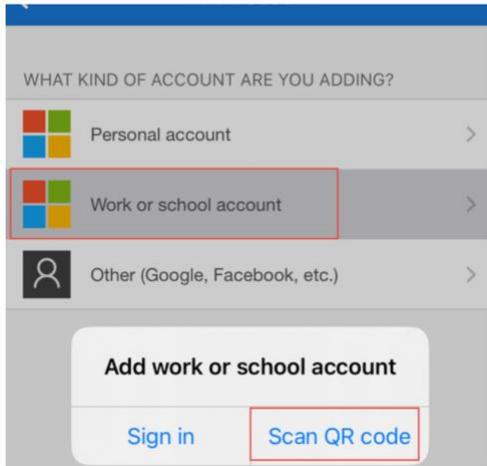
## Method 1: Microsoft Authenticator Mobile App

1. On any network-connected device, navigate to <https://aka.ms/mysecurityinfo>.
2. Click **Add Method** and choose the **Authenticator app** from the drop-down menu. Click **Add**.
3. Install the **Microsoft Authenticator** mobile app. If your mobile device is enrolled in SAS' Mobile Device Management solution, MobileIron, **you may already have the app installed**. Otherwise, install the app via your device's app store.

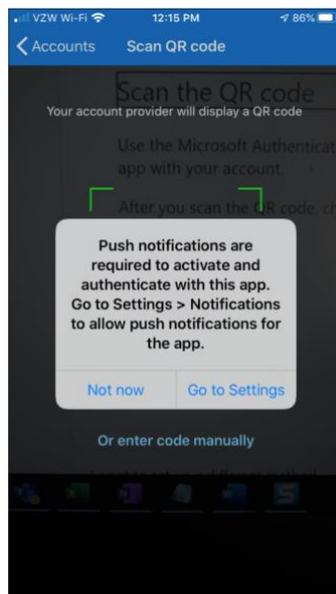


4. When the mobile app is installed, click **Next** on your computer screen.

5. Click **Next** when prompted to "Set up your account."
6. You will now see a QR Code appear on your computer screen.
7. Open the Microsoft Authenticator **mobile** app, click **Add account**. Choose **Work or school account**.

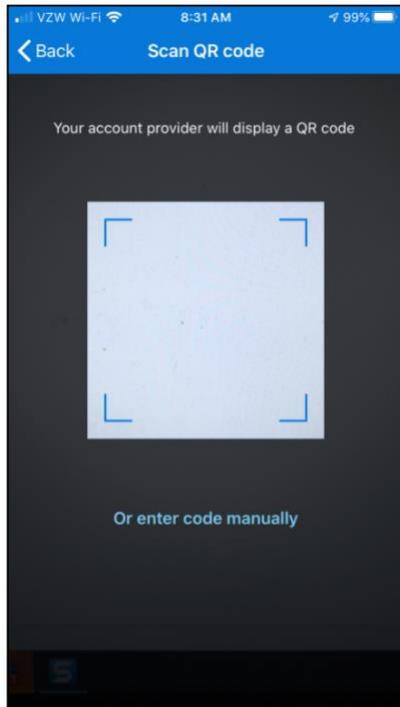


8. Tap **Scan QR code** (the QR code is displayed on your computer)
9. If prompted, allow push notifications.
  - a. If using an iPhone go to **Settings > Notifications** in iOS to allow push notifications for the Microsoft Authenticator app.



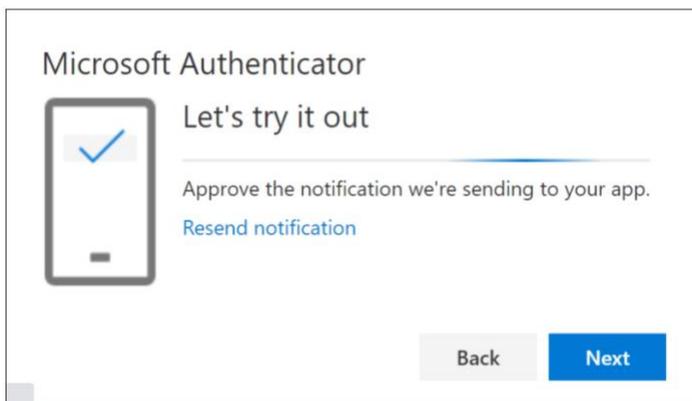
10. Scan the QR code *with the authenticator app*. **The QR code is displayed on your computer screen.** (Note: you may have to go into the settings for the Microsoft Authenticator app and enable camera access if it has been disabled.) If

the QR code reader can't read the code, select the **Can't scan the QR code link** on your computer and manually enter the code and URL into the Microsoft Authenticator app.

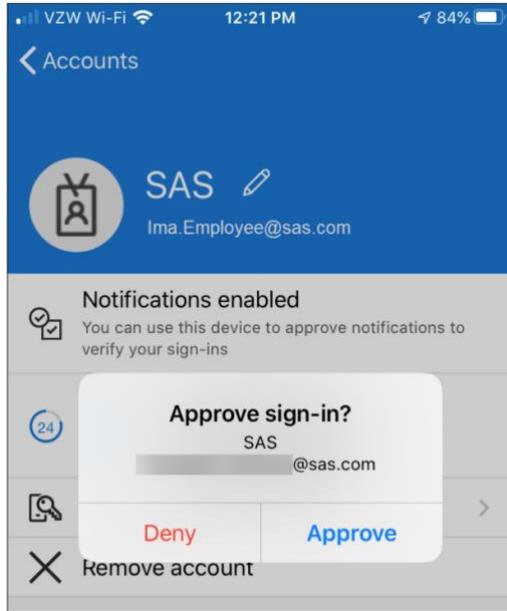


11. Click **Next** on the **Scan the QR code** page on your computer.

A notification is sent to the Microsoft Authenticator app on your mobile device to test your account.



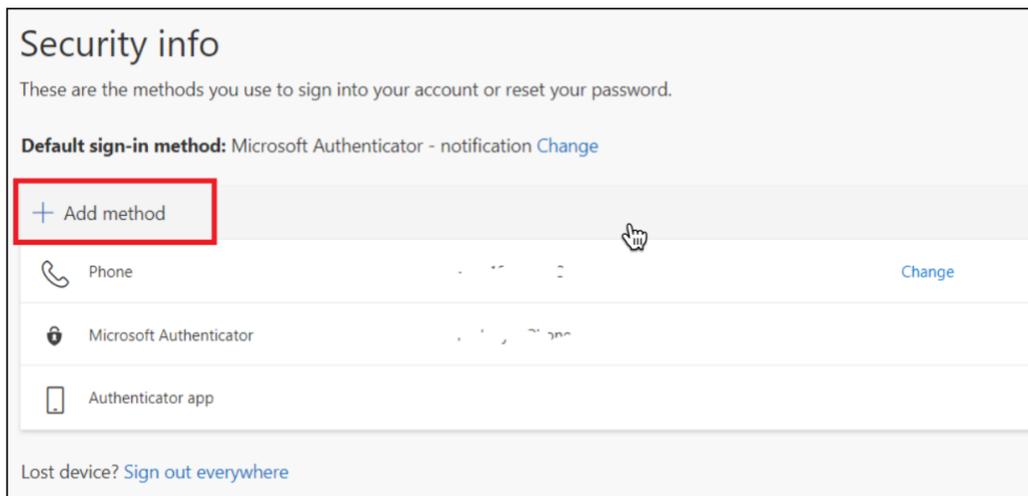
12. Approve the notification in the Microsoft Authenticator app and then click **Next**.



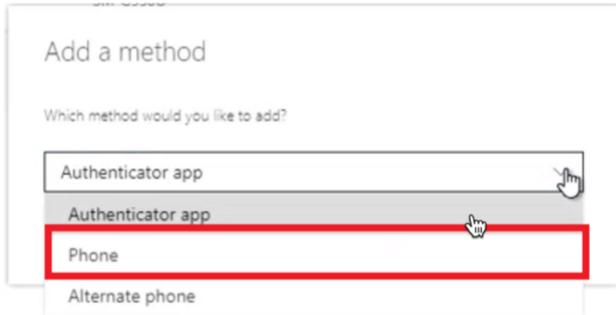
13. Success! The Authenticator mobile app is registered. Click **Next** to continue registration. You are required to register **two** methods of authentication.

### Method 2: Phone (SMS text)

1. From the main "Security info" menu on <https://aka.ms/mysecurityinfo>, click **+ Add Method**.



- From the drop-down menu, choose **Phone**.



Add a method

Which method would you like to add?

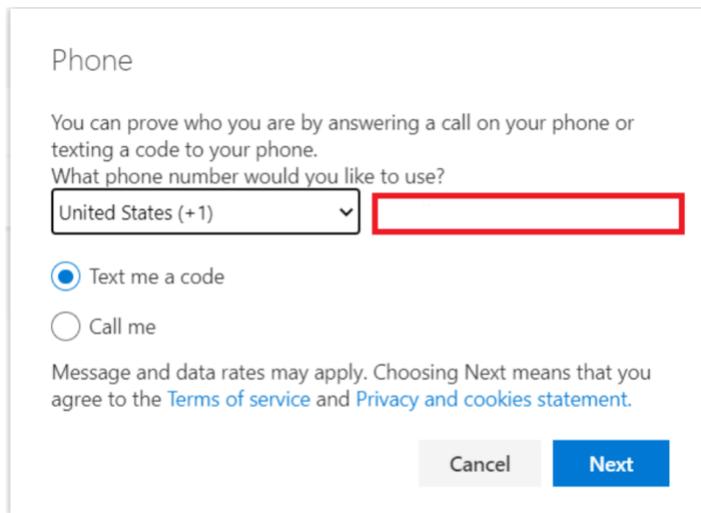
Authenticator app

Authenticator app

**Phone**

Alternate phone

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



Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1)

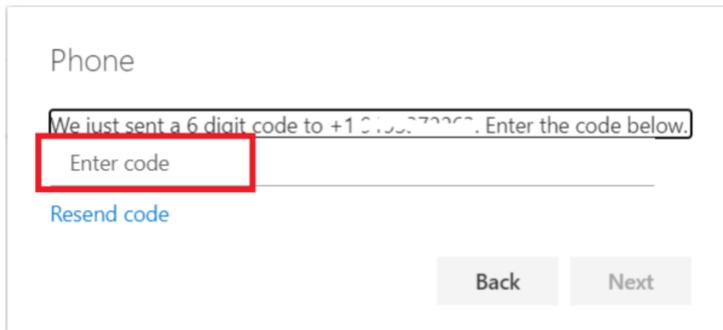
Text me a code

Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Cancel Next

- Enter the code you received via text message and click **Next**.



Phone

We just sent a 6 digit code to +1 212 273 2600. Enter the code below.

Enter code

[Resend code](#)

Back Next

- Success! Click **Done** to continue signing in.

### Method 3: Authenticator App (3rd party app for personal devices - not recommended or supported by SAS)

3<sup>rd</sup> party authenticator applications may be used on personal devices; however, you must agree that you are in control of that device from a security perspective. This means keeping the device up-to-date/patched, running anti-virus (where applicable) and applying a password or passcode to protect access to your device.

1. On any network-connected system, navigate to <https://aka.ms/mysecurityinfo>.
2. Click **Add Method** and choose the **Authenticator app** from the drop-down menu. Click **Add**.
3. Select **Configure App/Authenticator without Notifications**.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



4. Follow instructions within your 3rd party application to scan the QR code and finalize setup.

### Using Azure MFA

You may receive prompts from other apps, like Outlook and OneDrive, to log in and authenticate now that you are registered for multi-factor authentication. Simply sign into the apps with your SAS email address and password and accept the prompt to authenticate with MFA.

You may now change your default sign-in method directly from your [Microsoft account](#). To do this:

1. Go to your [Microsoft account](#).
  - a. To change your default sign-in method, click **Change**. (For example, 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.

**Security info**

These are the methods you use to sign into your account or reset your password.

**Default sign-in method:** Microsoft Authenticator - notification [Change](#) **a**

**+ Add method** **b**

Phone	+1 [redacted]	<a href="#">Change</a> <b>c</b> <a href="#">Delete</a>
Office phone	+1 [redacted]	<a href="#">Enable two-step verification</a>
Microsoft Authenticator	iPhone (5)	<a href="#">Delete</a>