Multi-Factor Authentication (MFA) for Students

Updated 01/25/24

Welcome to the Multi-Factor Authentication (MFA) guide for students at Rancho Santiago.

- By the end of this guide, you will learn:
  - What Multi-Factor Authentication (MFA) is.
  - How MFA is used at Rancho Santiago.
  - How to set up the Approved Methods for MFA, including backup methods.
  - How to contact the Student Help Desk for help with MFA.

What is Multi-Factor Authentication (MFA)?

- MFA is like an extra lock for your student login.
- It helps keep everyone at Rancho Santiago safe from hackers and other online threats.

Do I need to use MFA?

- MFA is only for your student email at **https://outlook.office.com** and when you log into Microsoft Office365 at **www.office.com**.
- **MFA doesn't change how you log into Canvas or Self-Service.**
  - **If you don’t use your student email address or Office365, you don’t need to set up MFA yet.**

MFA will be enforced for student email and Office365 on January 22, 2024.

- To start enrollment, use a desktop or laptop to open a web browser to **https://aka.ms/mfasetup**
- Then, follow the steps to set up the **Approved Methods for MFA**.

Do you learn better through video?

Select this link to view the video guide:

How to set up Microsoft Authenticator app and a backup method.

Do you have other questions?

Select this link to view our Frequently Asked Questions (FAQs)

Select this link for the contact information for Student Help Desk.

Student Help Desk – Contact Information

For Santa Ana College

- Phone Number: (714) 564-6123
- Email: studenthelpdesk@sac.edu
- Website: Select this link for the SAC Student Help Desk website.
- Physical Location: SAC Building A-106

For School of Continuing Education (SCE), also known as Centennial Education Center (CEC)

- Phone Number: (714) 480-7407
- Email: N/A
- Website: Select this link for the SCE Technology Support website.
- Physical Location: CEC Building F-101

For Santiago Canyon College

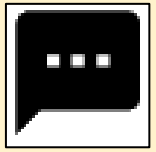
- Phone Number: (714) 628-5086
- Email: studenthelpdesk@sccollege.edu
- Website: Select this link for the SCC Student Help Desk website.
- Physical Location: SCC Building E-101

(Select this link to return to the list of Approved Methods for MFA)

Approved Methods for MFA:

Microsoft Authenticator (*Recommended)

Google Authenticator



SMS Text Message

Phone Call

Also see how to **Manage Your Backup Authentication Methods**.
Need help? **Select this link for Student Help Desk contact information.**

Microsoft Authenticator – Summary of Steps

Continue down this guide for step-by-step instructions with screenshots.

Summary of steps

STEP 1 – Get the Microsoft Authenticator app on your phone. You can find it in your phone's app store.

STEP 2 – Go to https://aka.ms/mfasetup and sign in with your Single sign-on account.

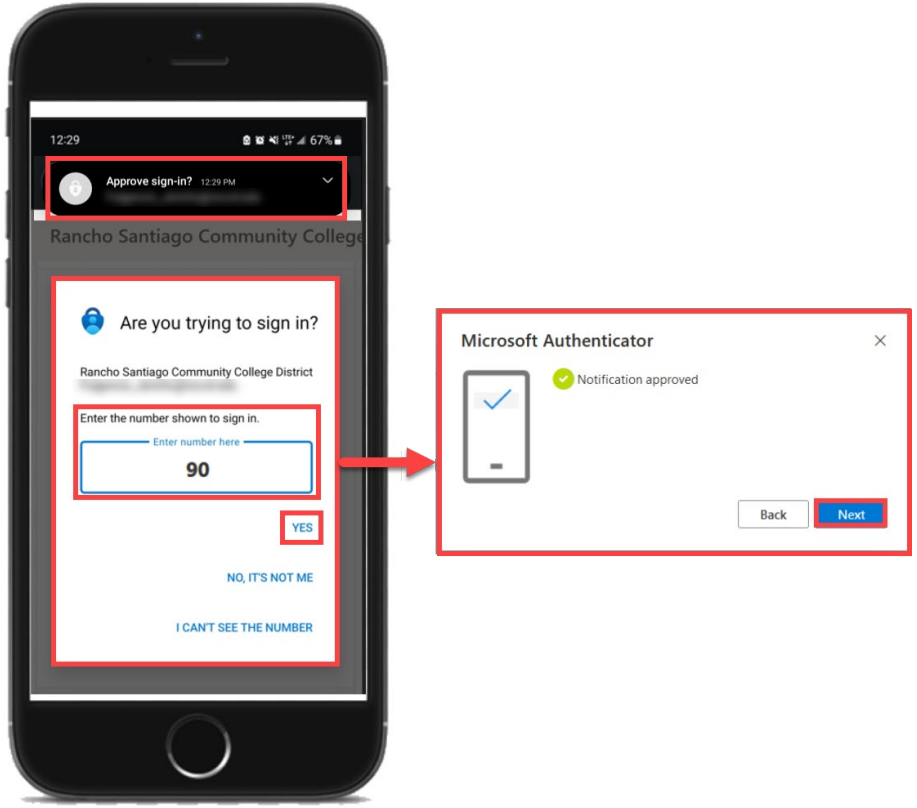
STEP 3 – Follow the instructions on the website. You'll be shown a unique picture known as a QR code. When you see this QR code, open the MS Authenticator app on your phone, tap "Add work or school account," and then tap "Scan a QR code" to scan the code with your phone's camera.

STEP 4 – You'll then get a code from the website to test that it's working. Enter that code where it asks you to on your phone.

STEP 5 – Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.

STEP 6 – On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Text or Phone).

STEP 7 – The next time you log in, the Authenticator app will help make sure it's really you.



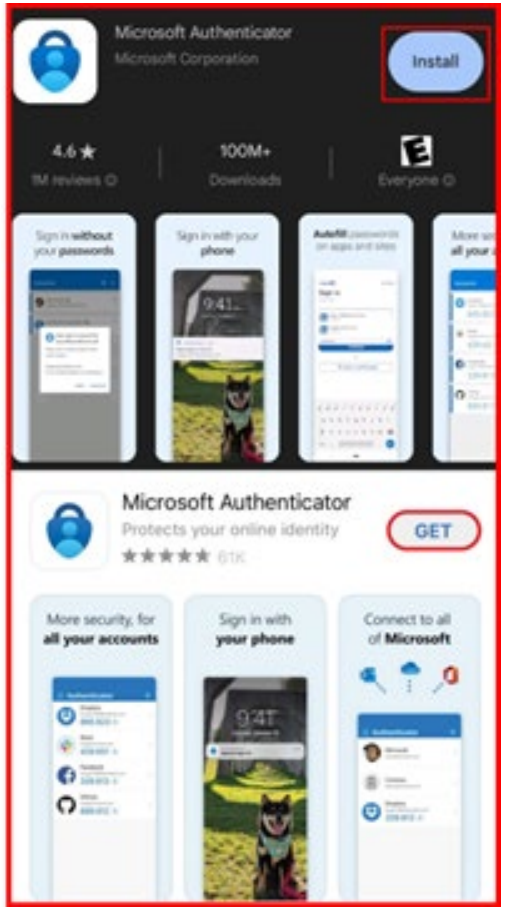
(Select this link to return to the list of Approved Methods for MFA)

Microsoft Authenticator – Step 1

Get the Microsoft Authenticator app on your phone.

You can find it in your phone's app store.

NOTE: The official app you need is from *Microsoft Corporation* and is free to download.

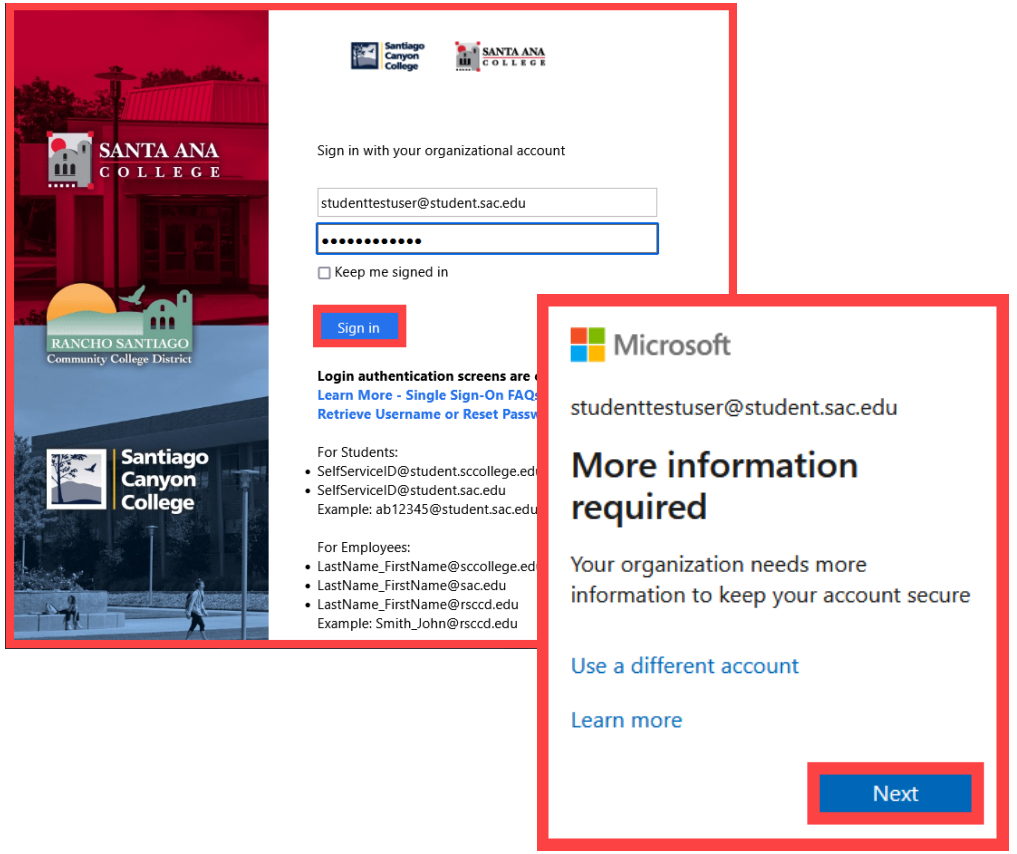


Microsoft Authenticator – Step 2

Next, go to https://aka.ms/mfasetup on a computer or tablet.

Use your Single Sign-On (SSO) credentials to log in.

Select "Next" when it asks for "More Information Required."



NOTE: You can also login to Self-Service > Navigation Menu > User Options > Select the link for Manage Multi-Factor Authentication (MFA)

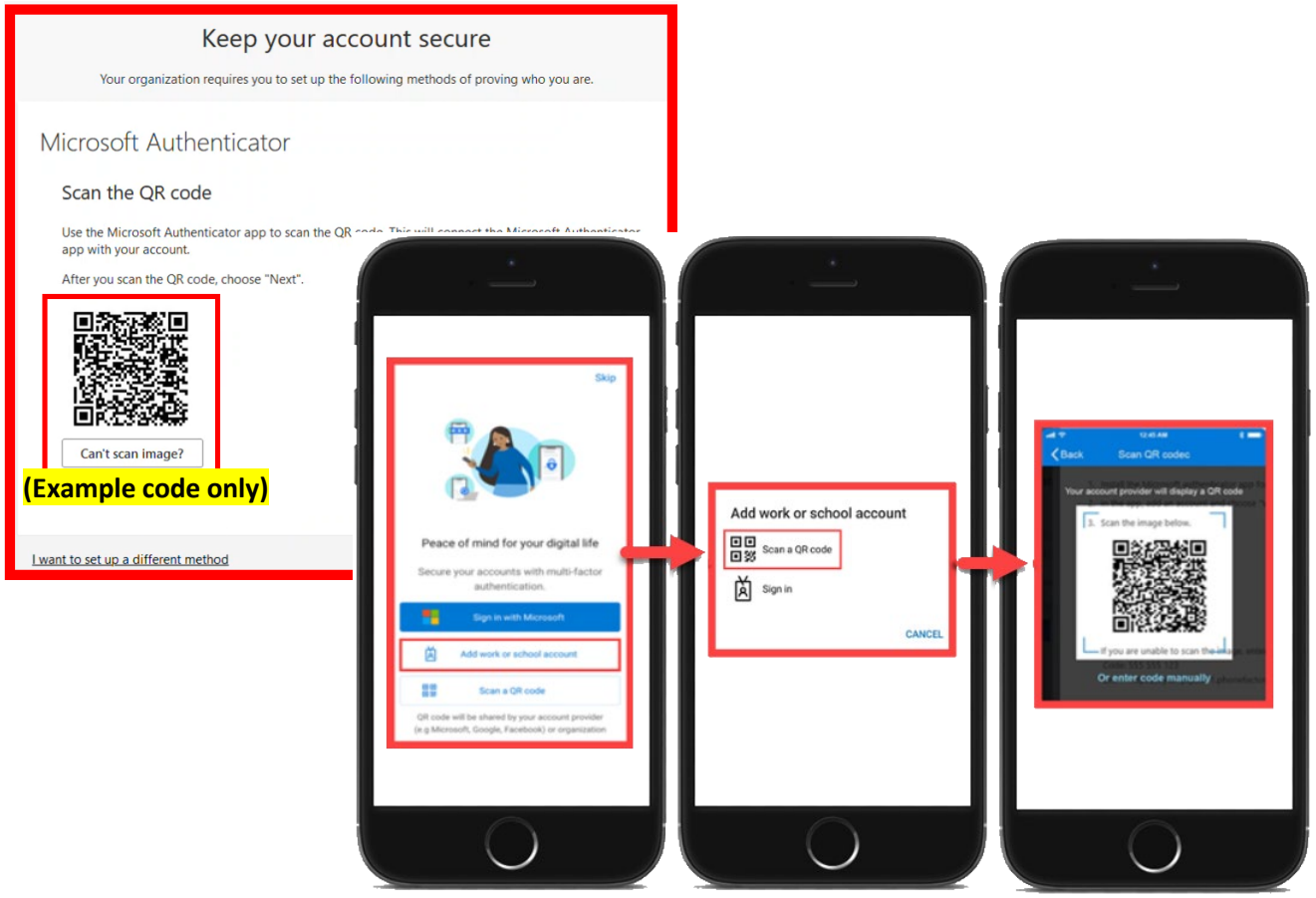
Microsoft Authenticator – Step 3

Follow the instructions on the website.

You'll be shown a unique picture known as a QR code.

When you see the QR code:

1. **Please open the MS Authenticator app on your phone.**
2. **Tap "Add work or school account."**
3. **Tap "Scan a QR code."**
4. **Then scan the code with your phone's camera.**



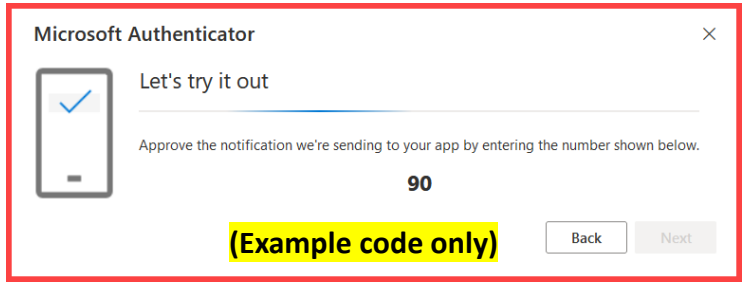
(Example code only)

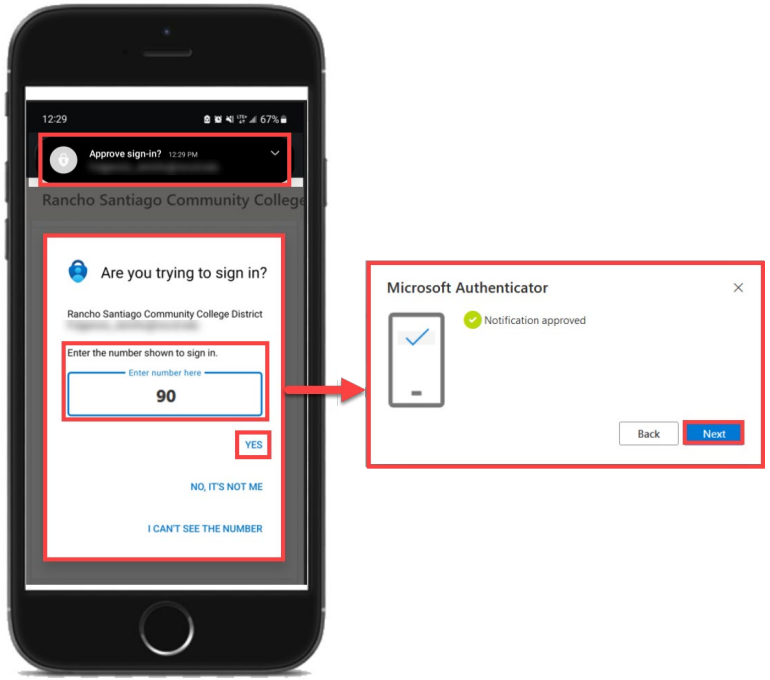
(Open MS Authenticator app > Add work or school account > Scan a QR code)

Microsoft Authenticator – Step 4

You'll then get a code from the website to test that it's working.

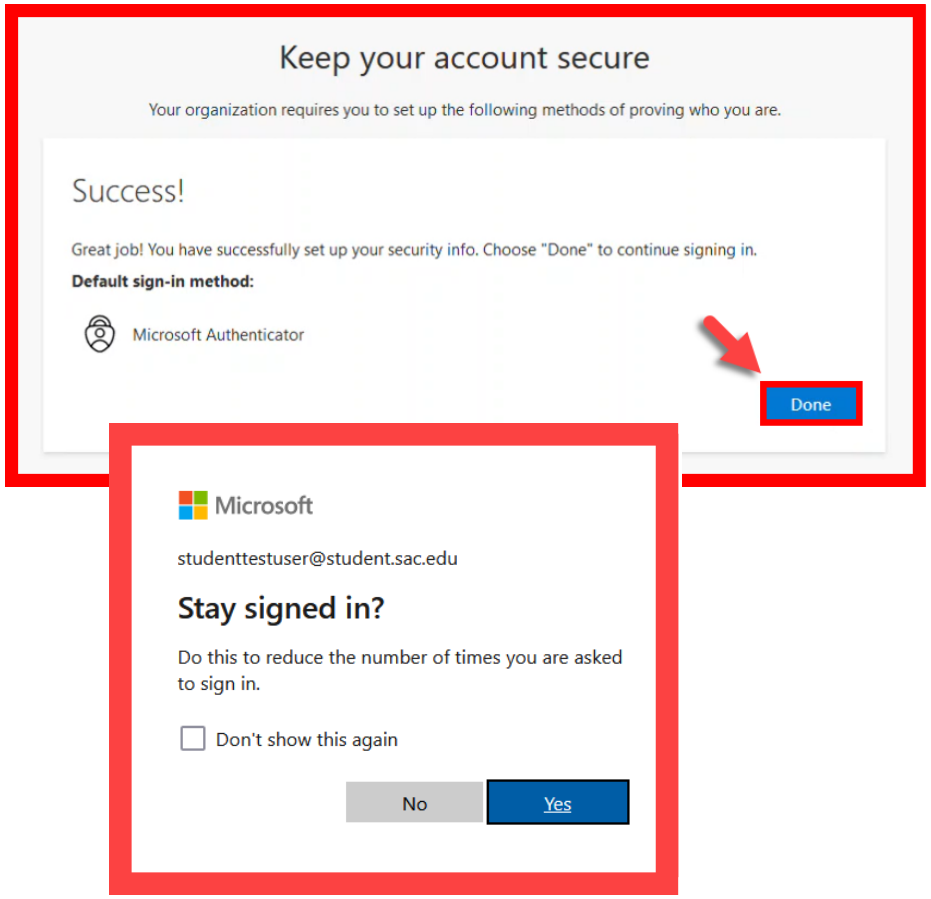
Enter that code where it asks you to on your phone.





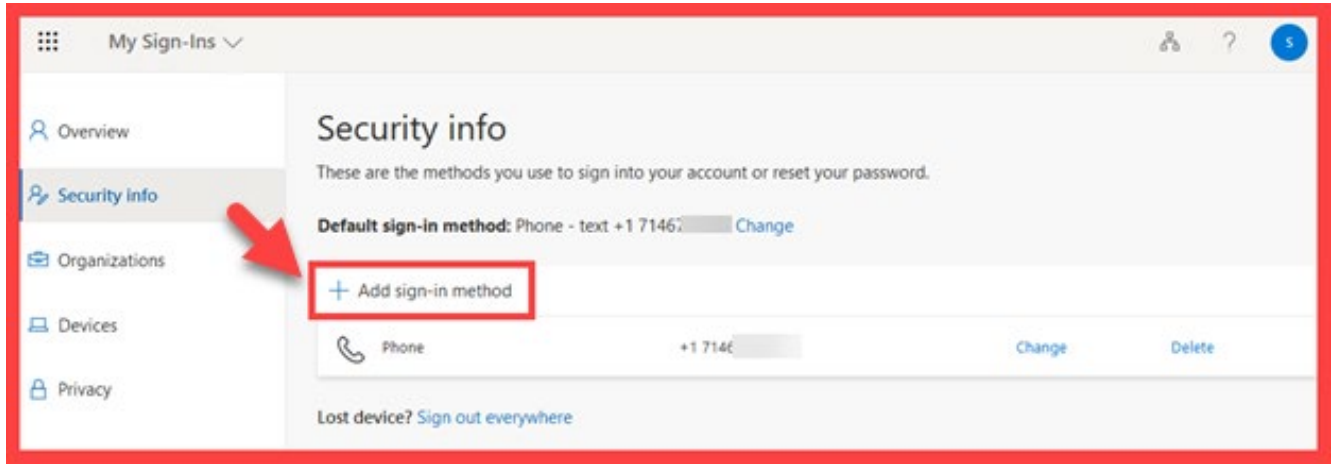
Microsoft Authenticator – Step 5

Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.



Microsoft Authenticator – Step 6

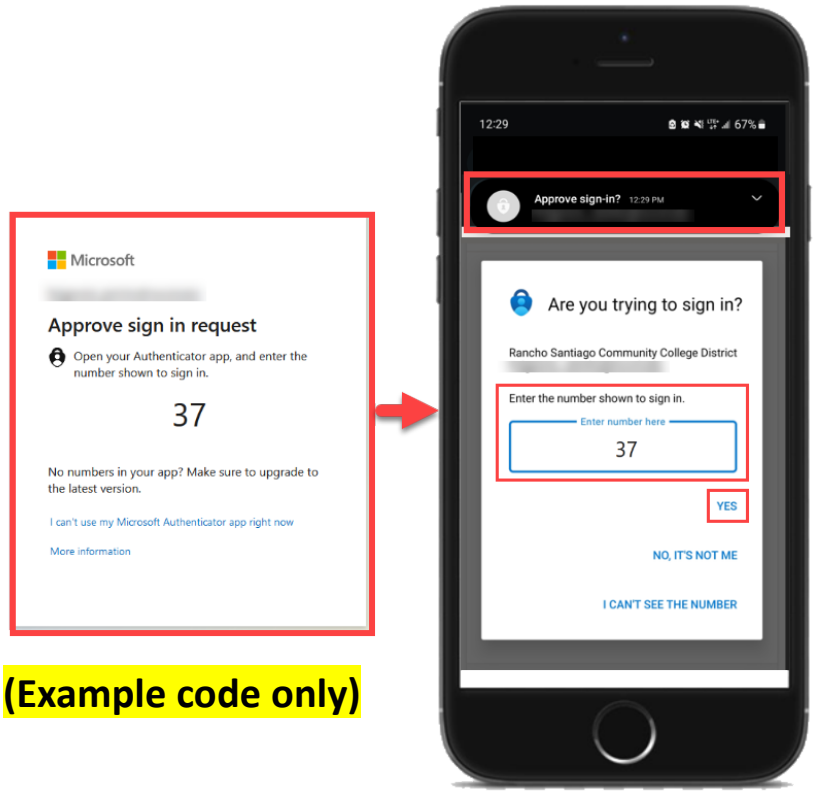
On the Security Info page, select “Add sign-in method” to set up a backup authentication method (such as Text or Phone).



Microsoft Authenticator – Step 7

The next time you log in, the Authenticator app will help make sure it's really you.

It's a way to keep your account safe!



(Example code only)

[(Select this link to return to the summary of steps for Microsoft Authenticator)]
[(Select this link to return to the list of Approved Methods for MFA)]

Google Authenticator – Summary of Steps

Continue down this guide for step-by-step instructions with screenshots.

STEP 1 – Get the Google Authenticator app on your phone. You can find it in your phone's app store.

STEP 2 – Go to https://aka.ms/mfasetup and sign in with your Single sign-on account.

STEP 3 – Choose the option that says, "I want to use a different authenticator app."

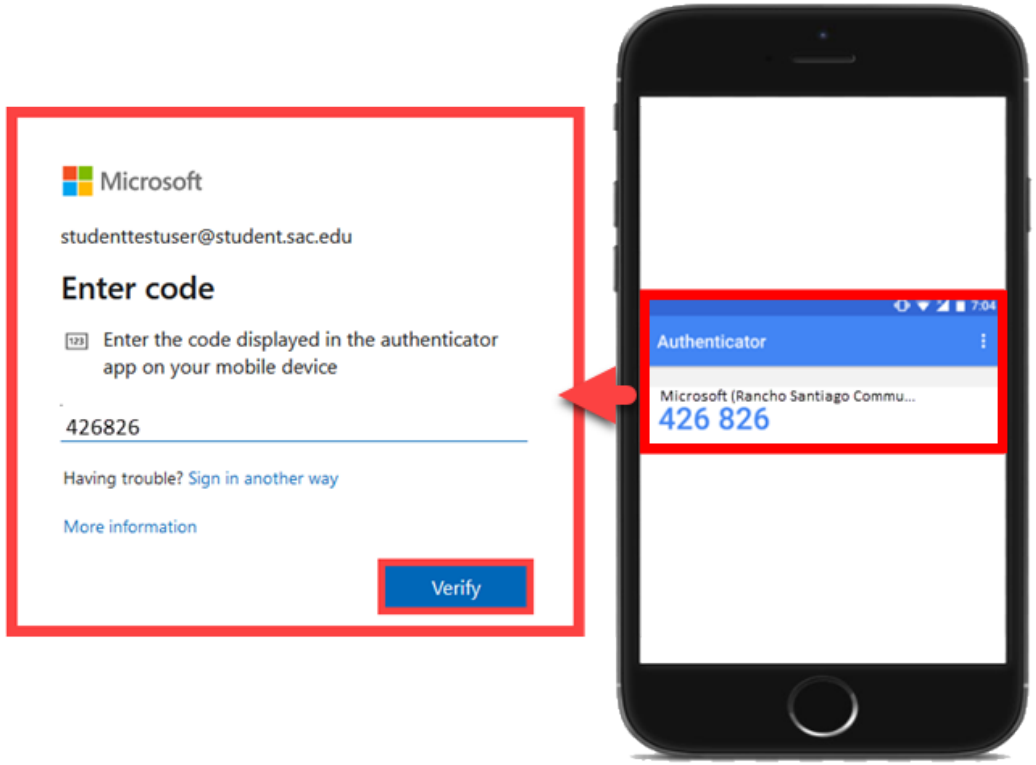
STEP 4 – Open the app, select "Scan a QR code," and scan the QR code that shows up on the website with your phone's camera.

STEP 5 – Follow the steps on the website to check the Google Authenticator app is working correctly.

STEP 6 – Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.

STEP 7 - On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Text or Phone).

STEP 8 - The next time you log in, the Authenticator app will help make sure it's really you. It's a way to keep your account safe!



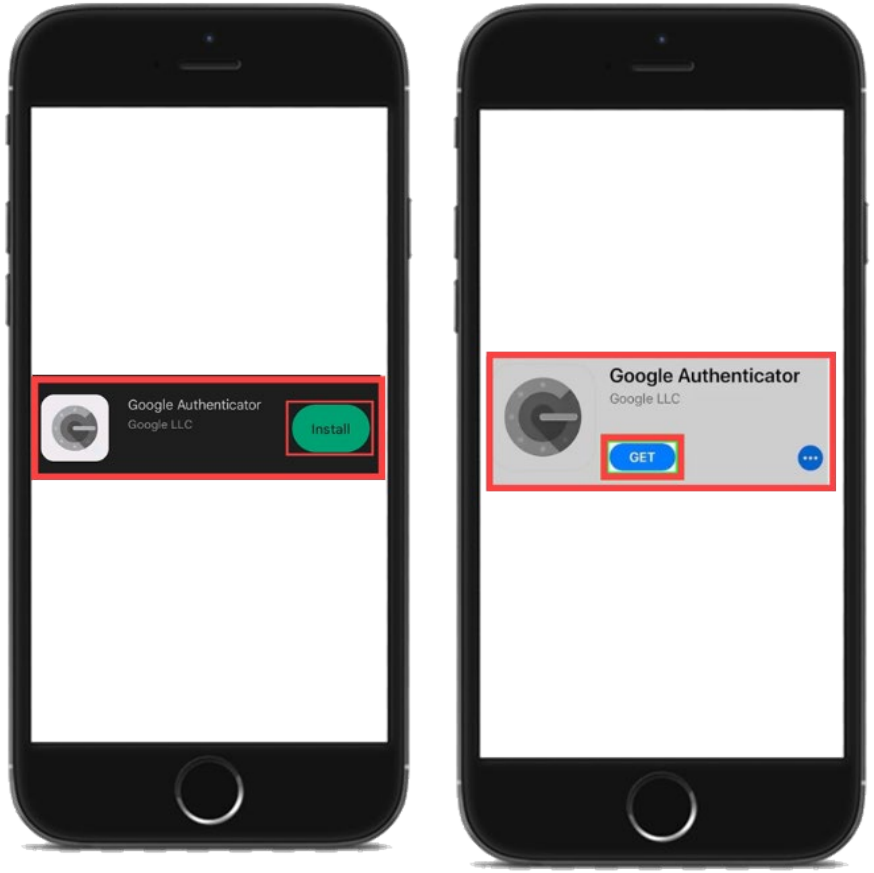
(Select this link to return to the list of Approved Methods for MFA)

Google Authenticator – Step 1

Get the Google Authenticator app on your phone.

You can find it in your phone's app store.

NOTE: The app you're looking for is *Google Authenticator* from *Google LLC* and is free to download.

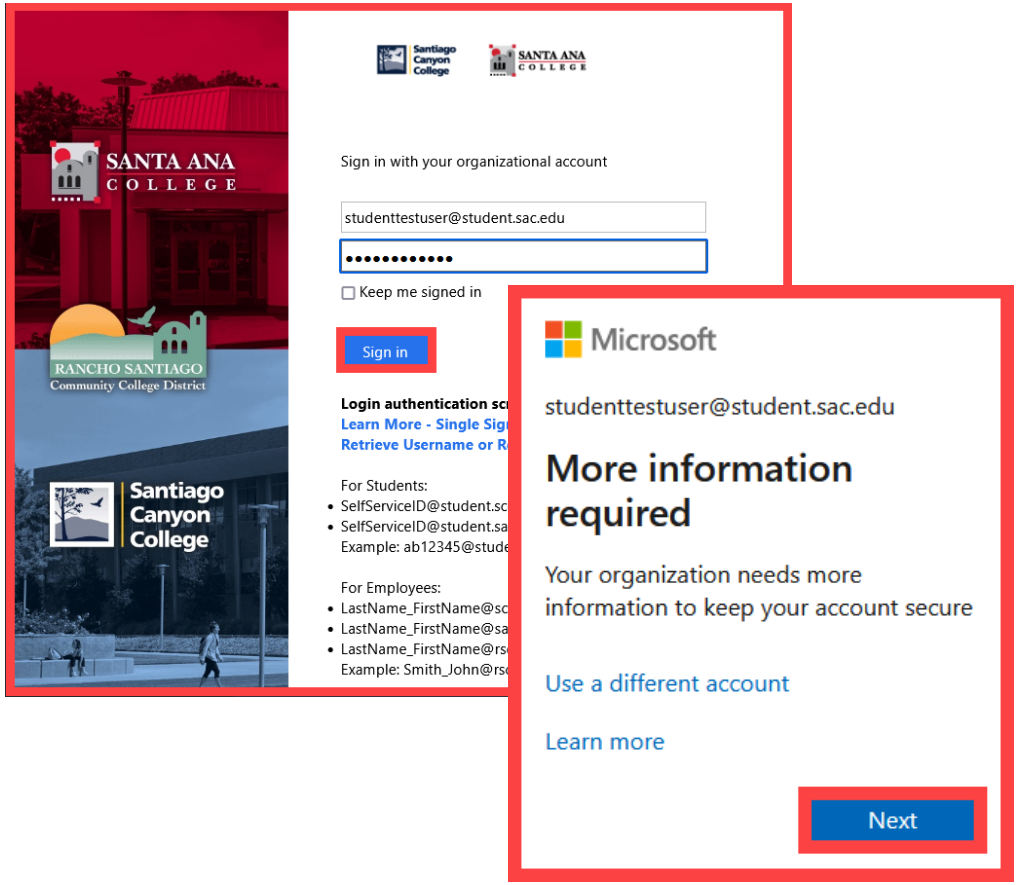


Google Authenticator – Step 2

Next, go to https://aka.ms/mfasetup on a computer or tablet.

Use your Single Sign-On (SSO) credentials to log in.

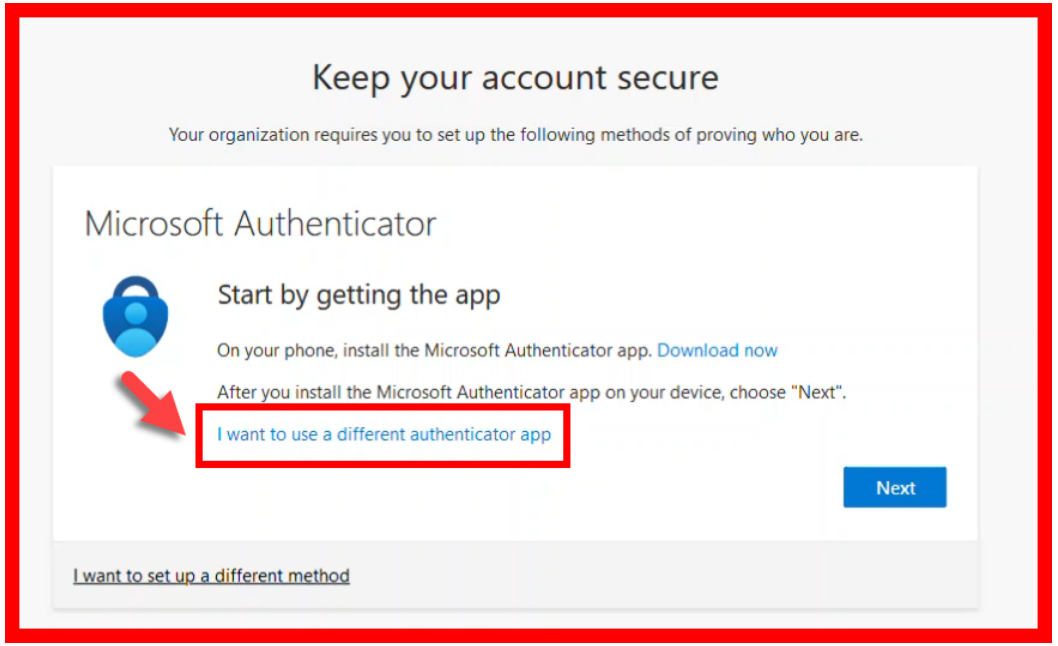
Select "Next" when it asks for "More Information Required."



NOTE: You can also login to Self-Service > Navigation Menu > User Options > Select the link for Manage Multi-Factor Authentication (MFA)

Google Authenticator – Step 3

Choose the option that says “I want to use a different authenticator app.”



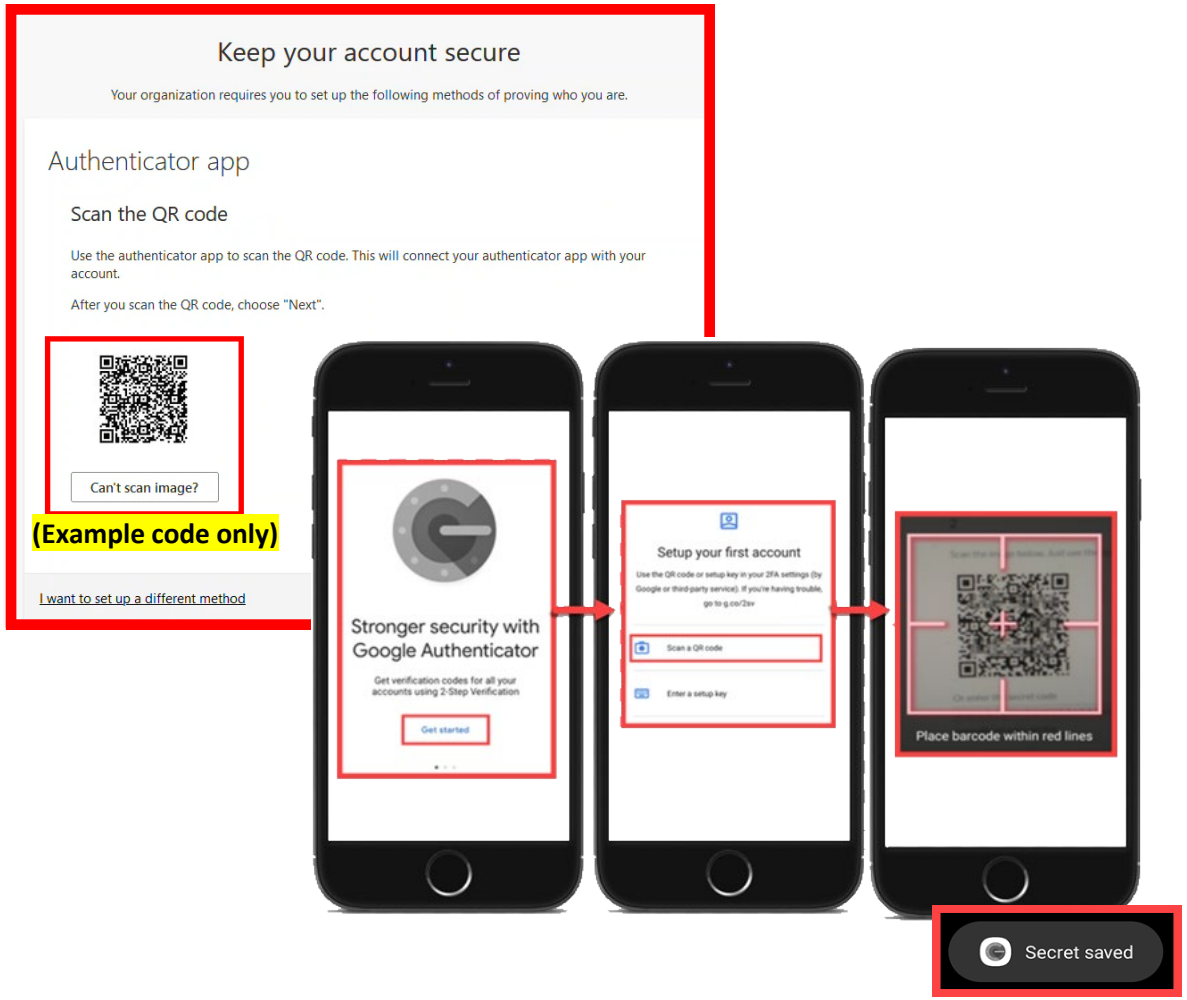
Google Authenticator – Step 4

Follow the instructions on the website.

You'll be shown a unique picture known as a QR code.

When you see the QR code:

1. **Please open the Google Authenticator app on your phone.**
2. **Select "Scan a QR Code."**
3. **Then scan the QR code that shows up on the website with your phone's camera.**

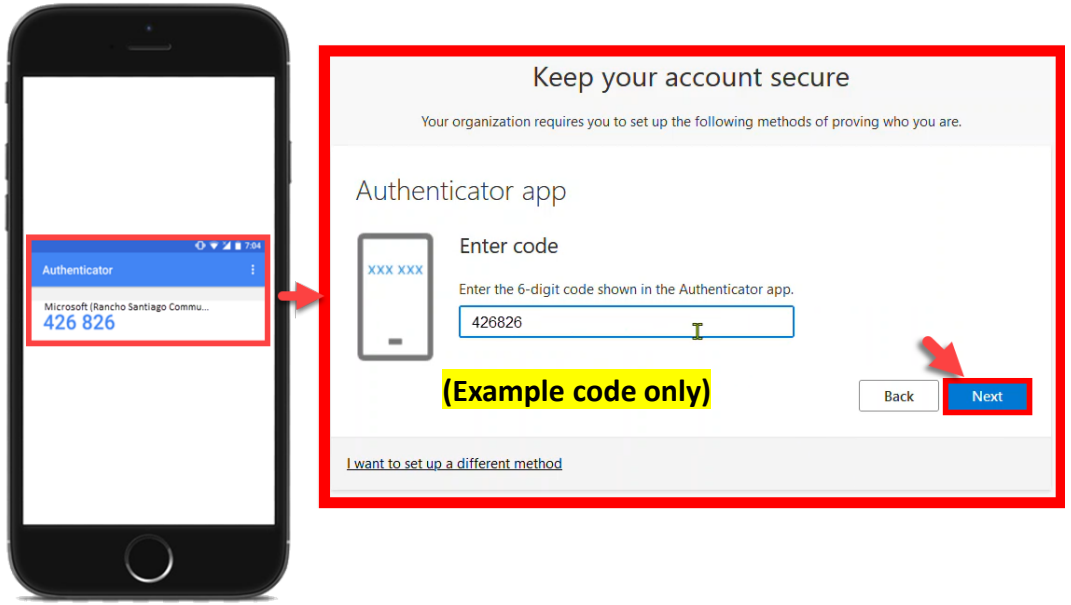


Google Authenticator – Step 5

Continue by selecting "Next."

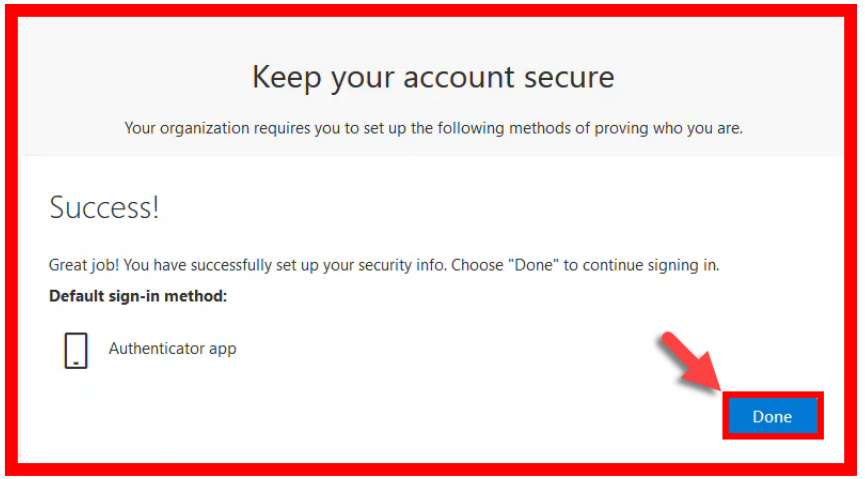
You'll then get a prompt from the website to enter a code shown on your Authenticator app.

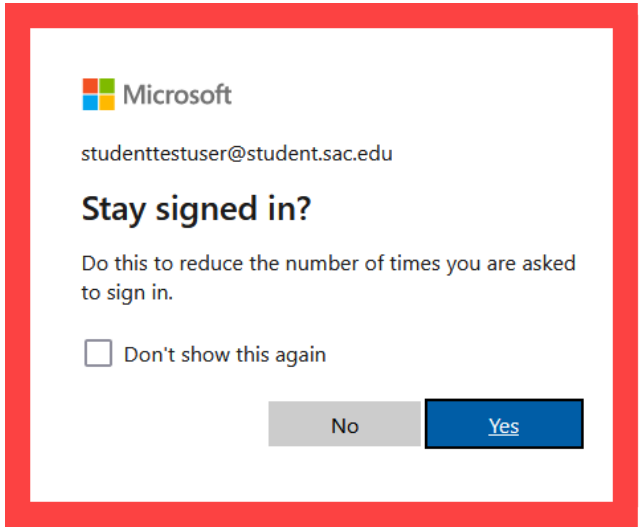
Enter that code where it asks you to on the website to make sure it's working.



Google Authenticator – Step 6

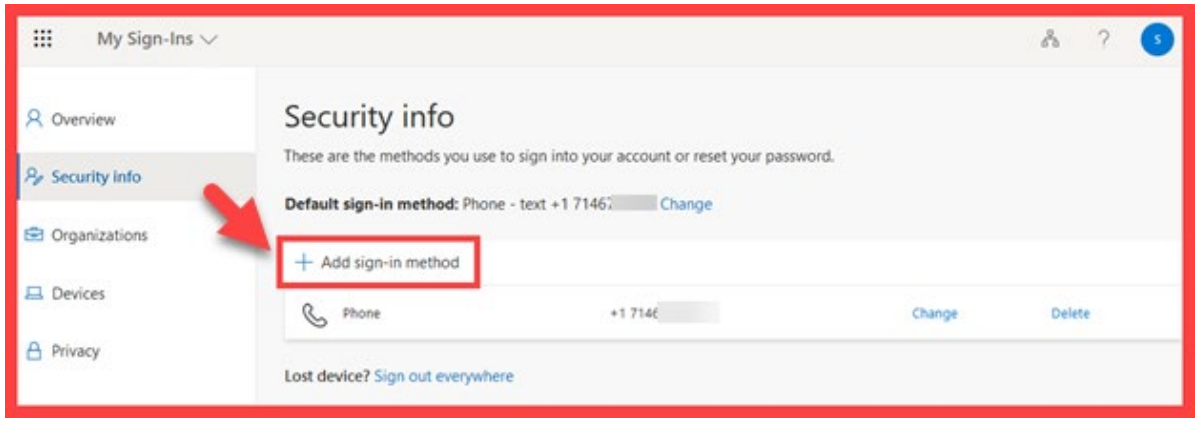
Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.





Google Authenticator – Step 7

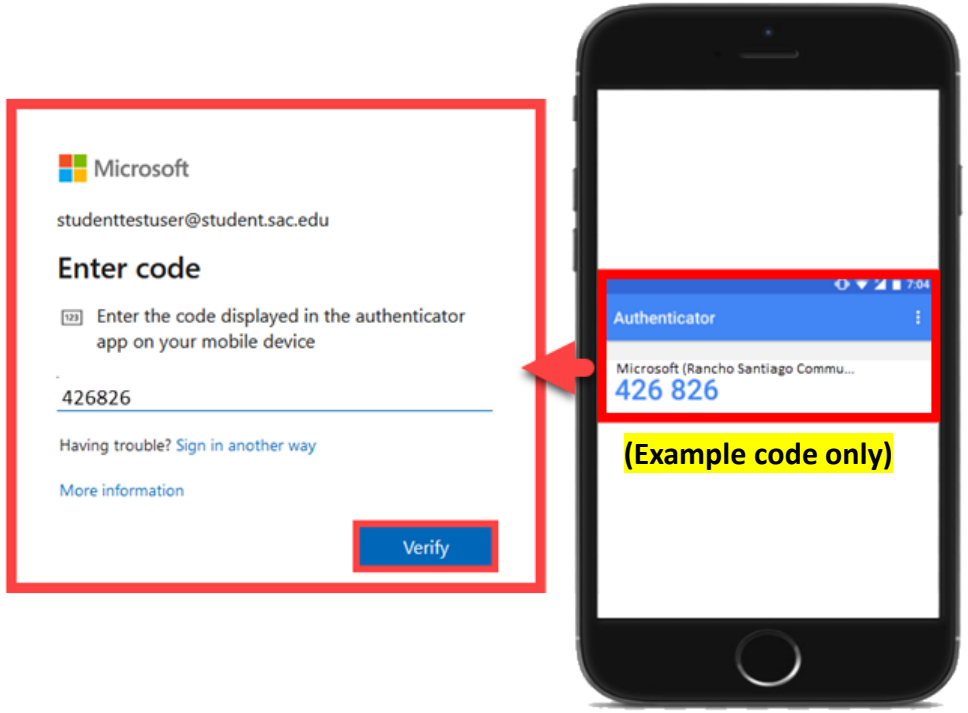
On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Text or Phone).



Google Authenticator – Step 8

The next time you log in, the Authenticator app will help make sure it's really you.

It's a way to keep your account safe!



(Select this link to return to the summary of steps for Google Authenticator)
(Select this link to return to the list of Approved Methods for MFA)

SMS Text Message – Summary of Steps

Continue down this guide for step-by-step instructions with screenshots.

STEP 1 – Go to https://aka.ms/mfasetup and sign in with your Single sign-on account.

STEP 2 – Choose "I want to set up a different method," then select "Phone."

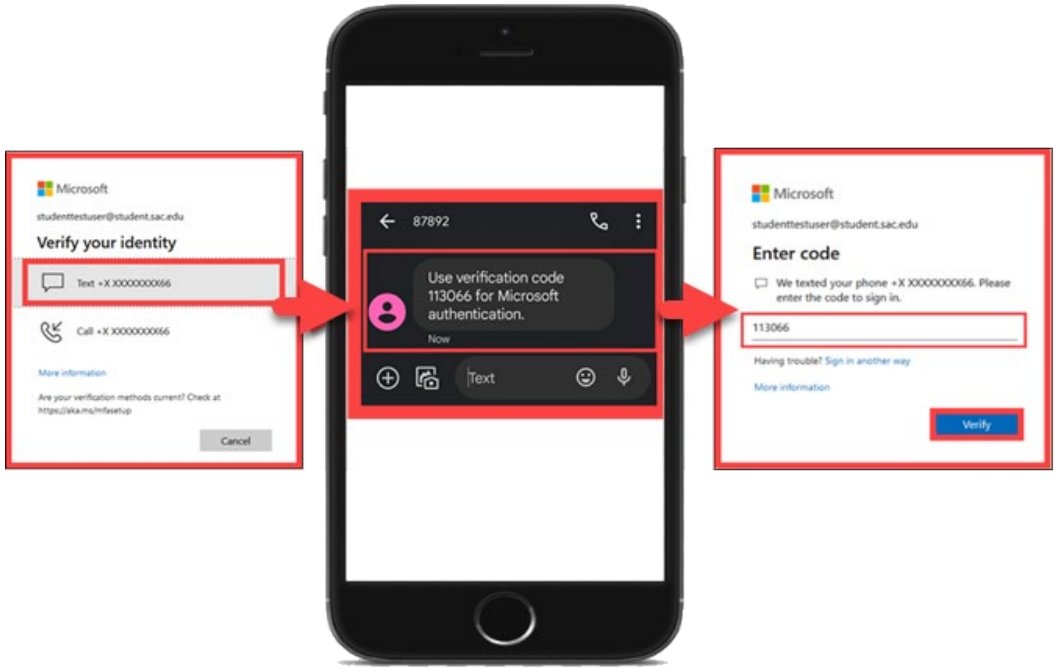
STEP 3 – Type in your phone number, then choose "Text me a code."

STEP 4 – You'll get a code in a text message on your phone. Enter that code where it asks you to.

STEP 5 – Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.

STEP 6 – On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Microsoft Authenticator).

STEP 7 – The next time you login, we'll check it's really you by sending a text message code again to your phone. It's a way to keep your account safe!



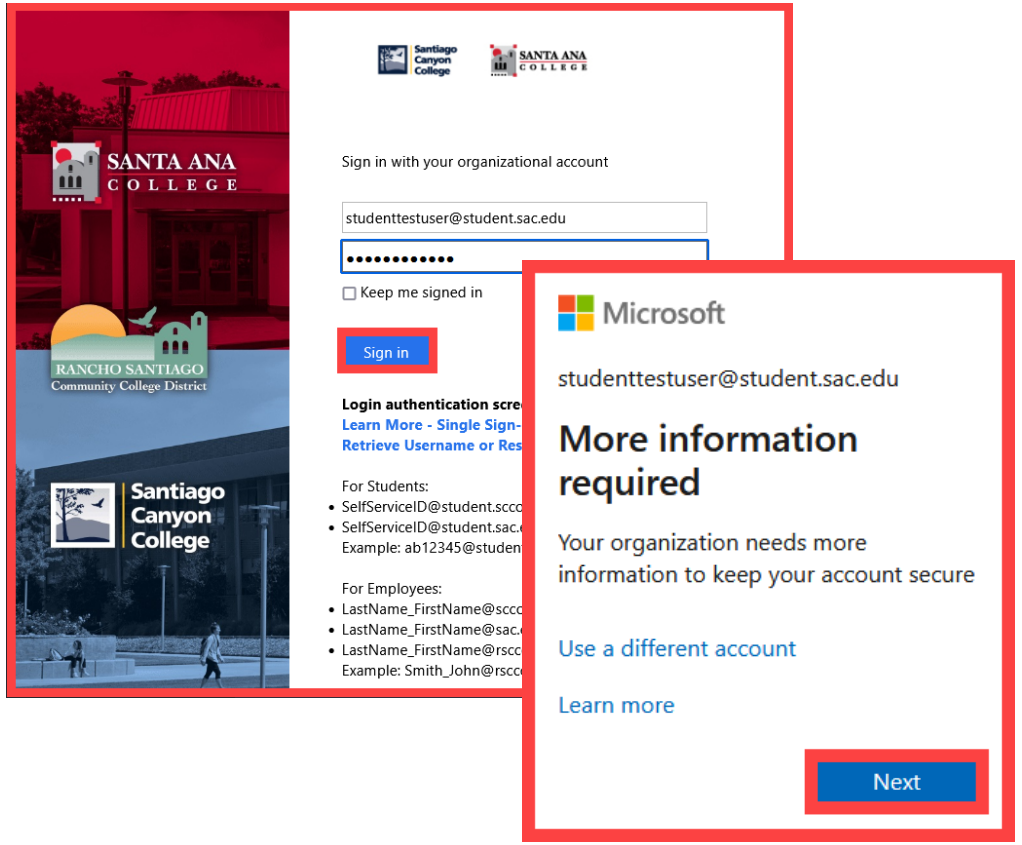
(Select this link to return to the list of Approved Methods for MFA)

SMS Text Message – Step 1

Go to https://aka.ms/mfasetup on a computer or tablet.

Use your Single Sign-On (SSO) credentials to log in.

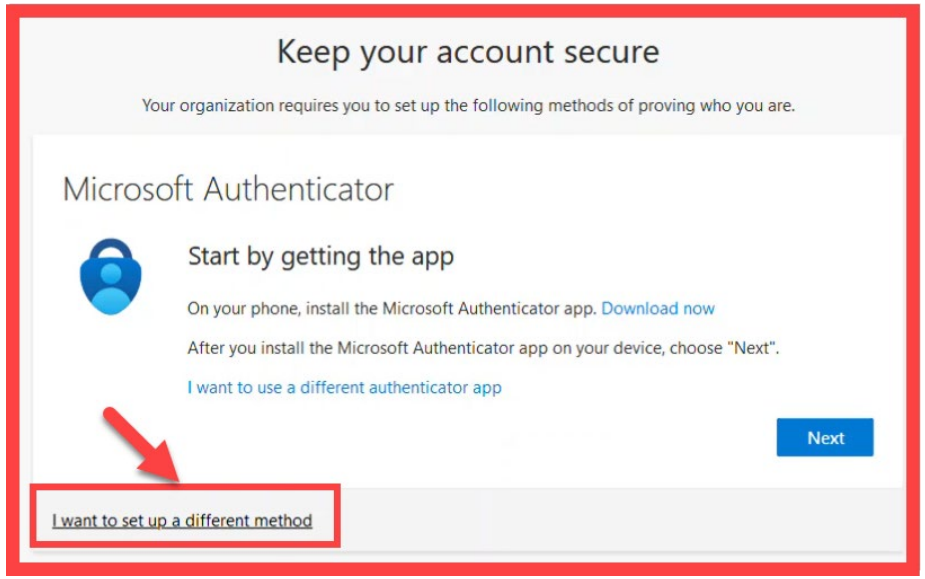
Select "Next" when it asks for "More Information Required."

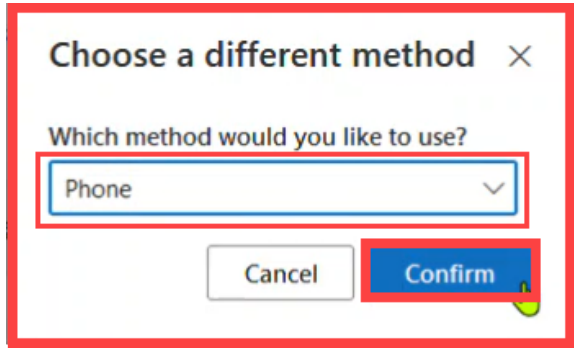


NOTE: You can also login to Self-Service > Navigation Menu > User Options > Select the link for Manage Multi-Factor Authentication (MFA)

SMS Text Message – Step 2

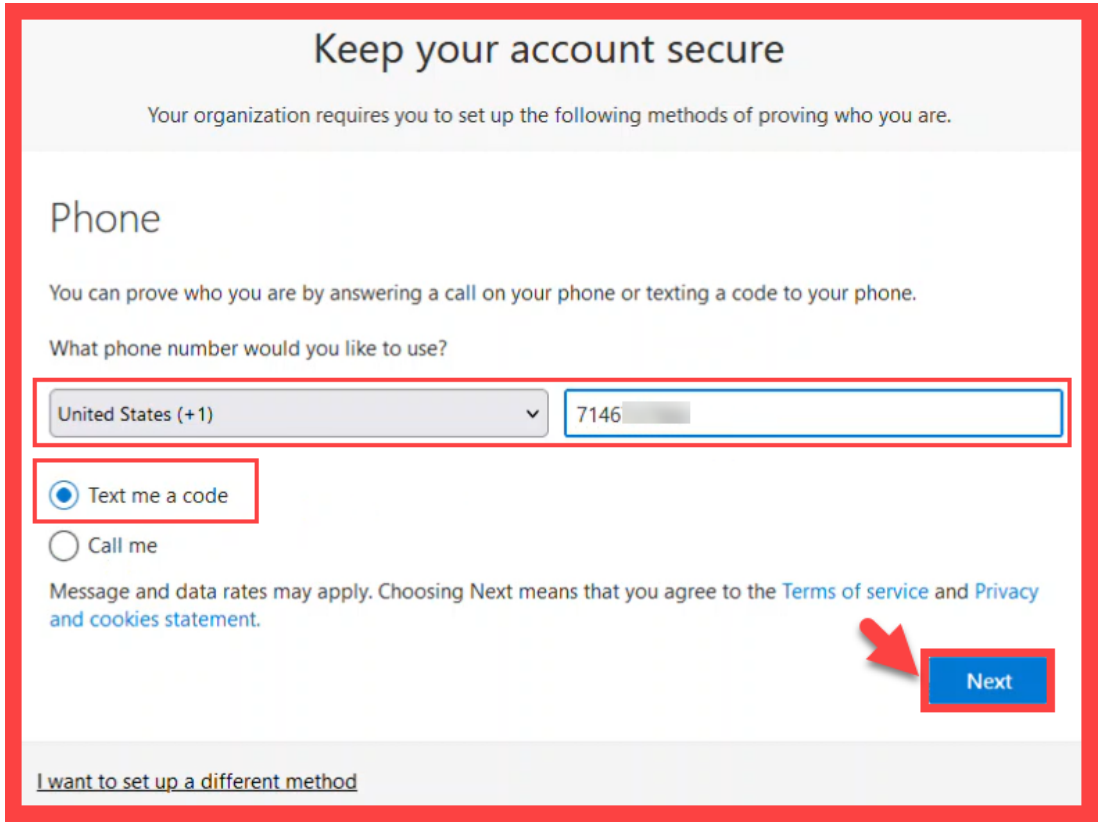
Choose “I want to set up a different method,” then select “Phone.”





SMS Text Message – Step 3

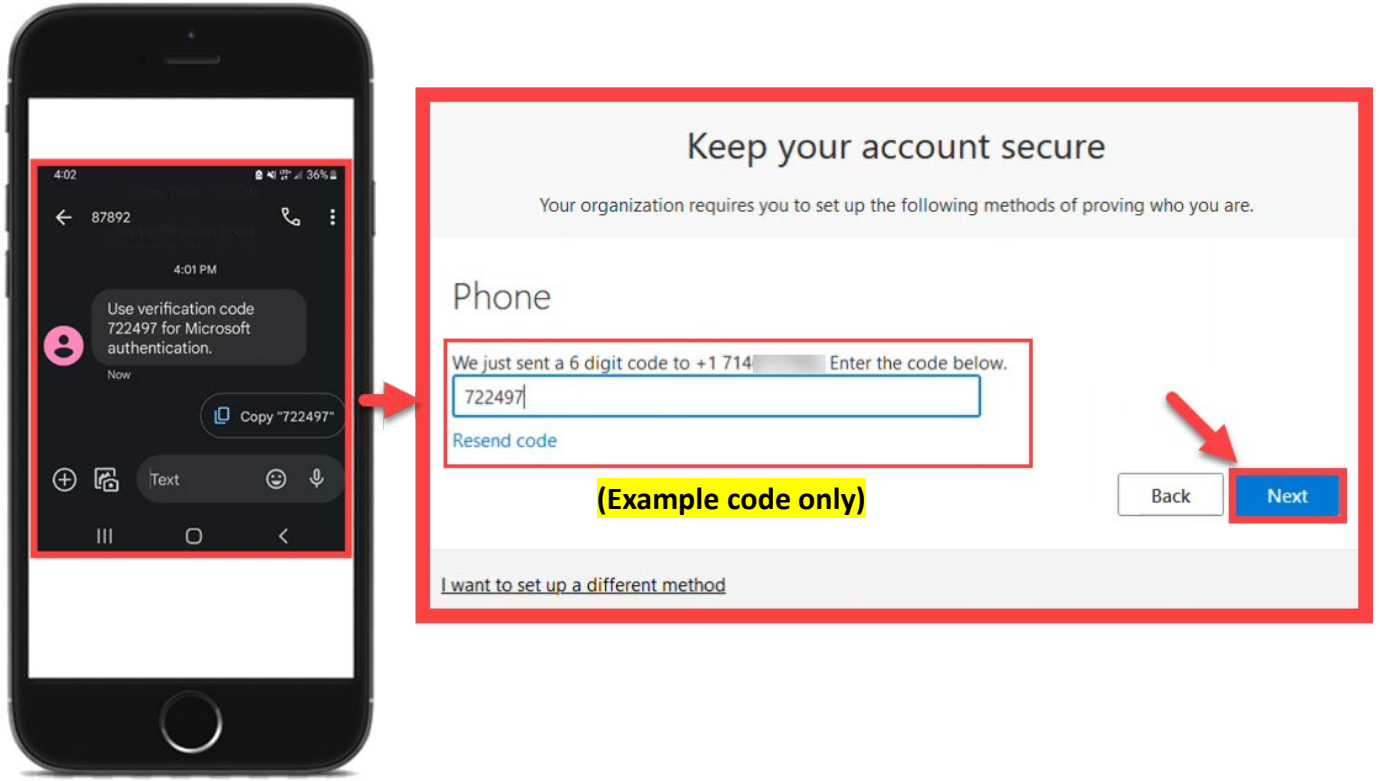
Type in your phone number, then choose "Text me a code".



SMS Text Message – Step 4

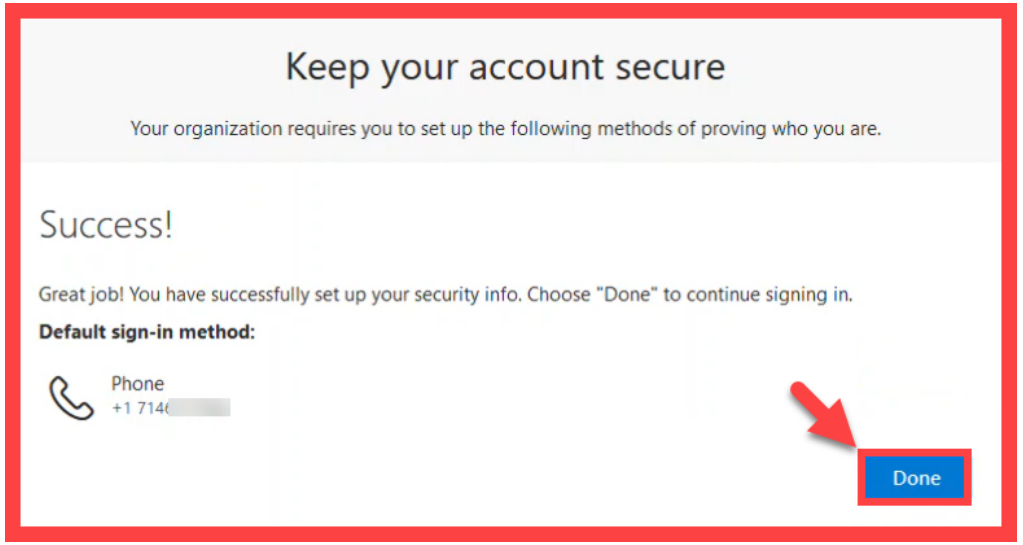
You'll get a code in a text message on your phone.

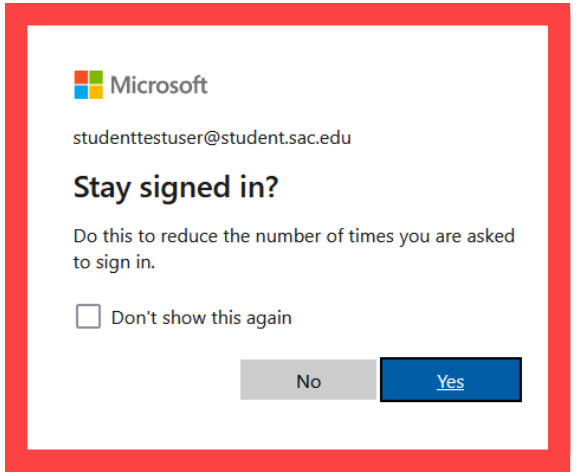
Enter that code where it asks you to.



SMS Text Message – Step 5

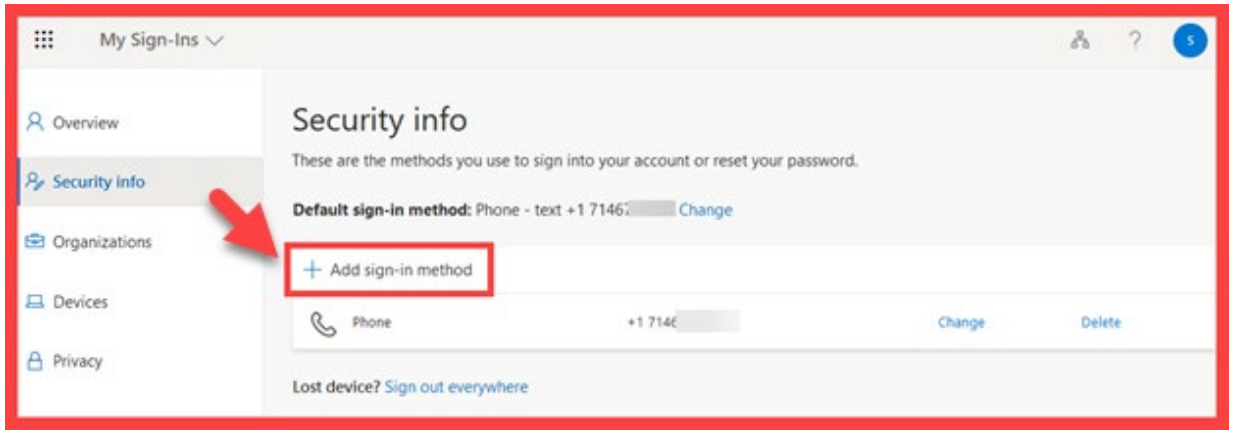
Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.





SMS Text Message – Step 6

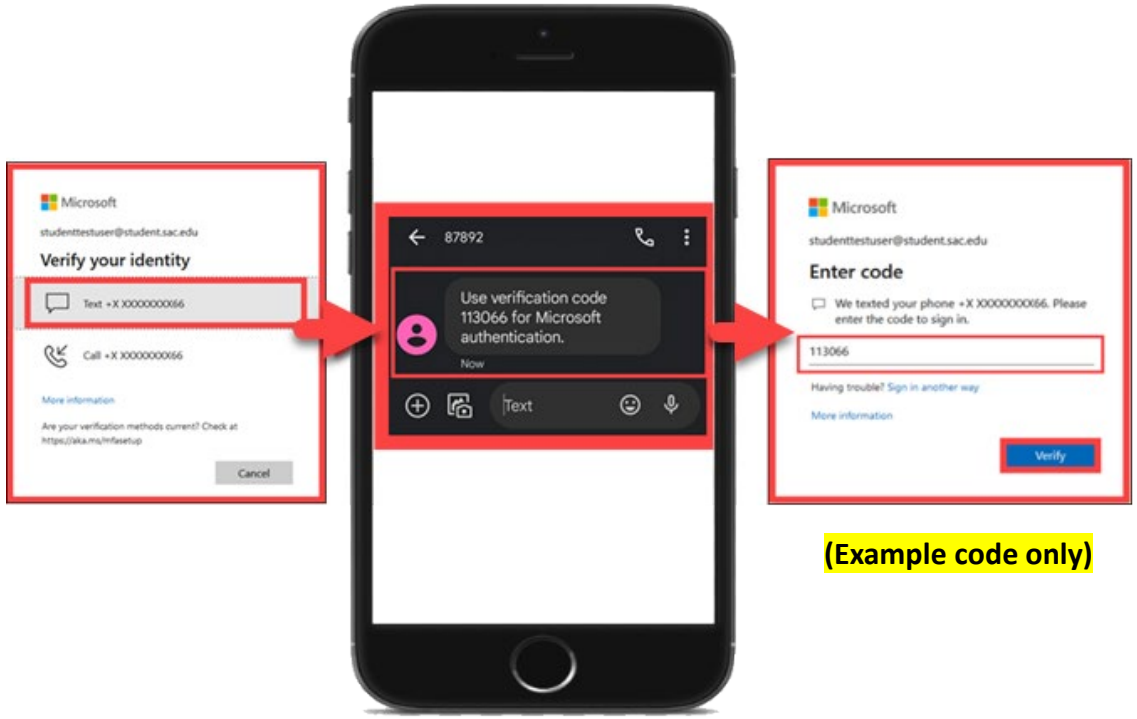
On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Microsoft Authenticator).



SMS Text Message – Step 7

The next time you login, we'll check it's really you by sending a text message code again to your phone.

It's a way to keep your account safe!



(Example code only)

[(Select this link to return to the summary of steps for SMS Text Message)]
[(Select this link to return to the list of Approved Methods for MFA)]

Phone Call – Summary of Steps

Continue down this guide for step-by-step instructions with screenshots.

STEP 1 – Go to https://aka.ms/mfasetup and sign in with your Single sign-on account.

STEP 2 – Choose "I want to set up a different method," then select "Phone."

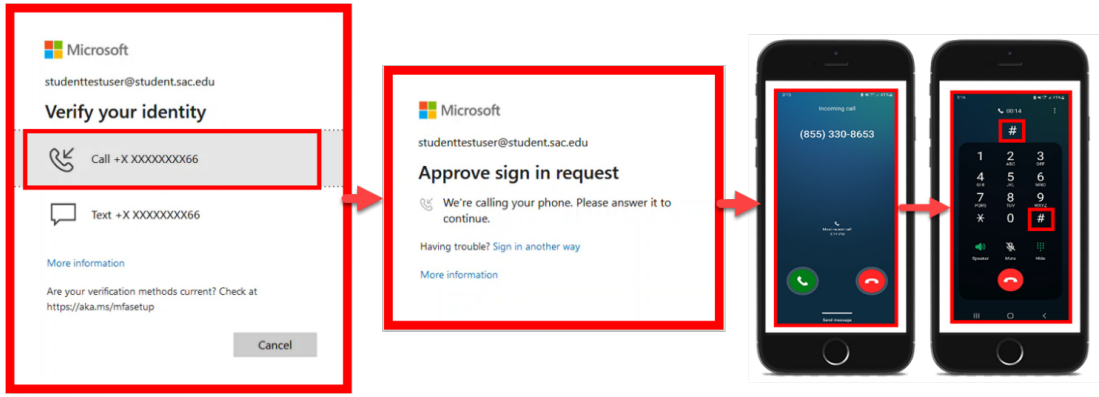
STEP 3 – Type in your phone number, then choose "Call Me."

STEP 4 – Answer the call from Microsoft and press the "#" key to confirm it's you.

STEP 5 – Finish the steps, and you'll be logged into the Security Info page at https://aka.ms/mfasetup.

STEP 6 – On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Microsoft Authenticator).

STEP 7 – The next time you login, you'll receive a phone call to verify it's really you.



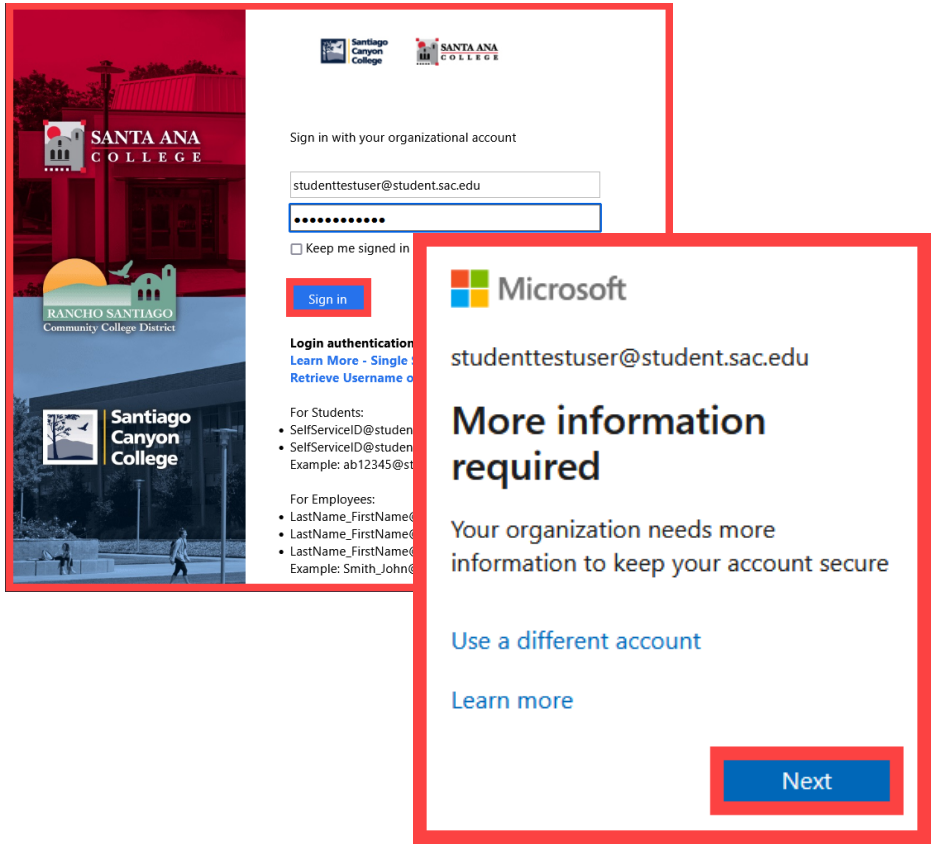
(Select this link to return to the list of Approved Methods for MFA)

Phone Call – Step 1

Go to https://aka.ms/mfasetup on a computer or tablet.

Use your Single Sign-On (SSO) credentials to log in.

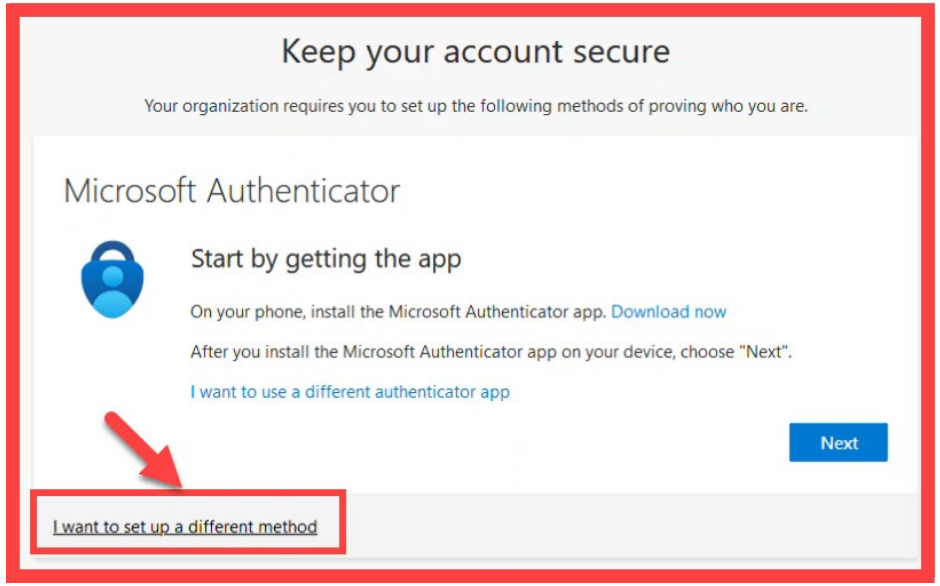
Select "Next" when it asks for "More Information Required."

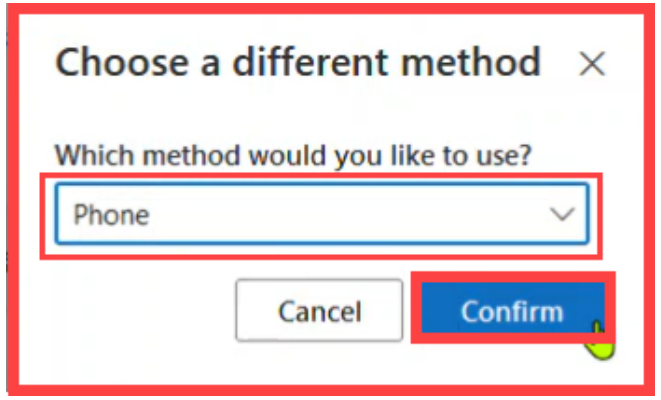


NOTE: You can also login to Self-Service > Navigation Menu > User Options > Select the link for Manage Multi-Factor Authentication (MFA)

Phone Call – Step 2

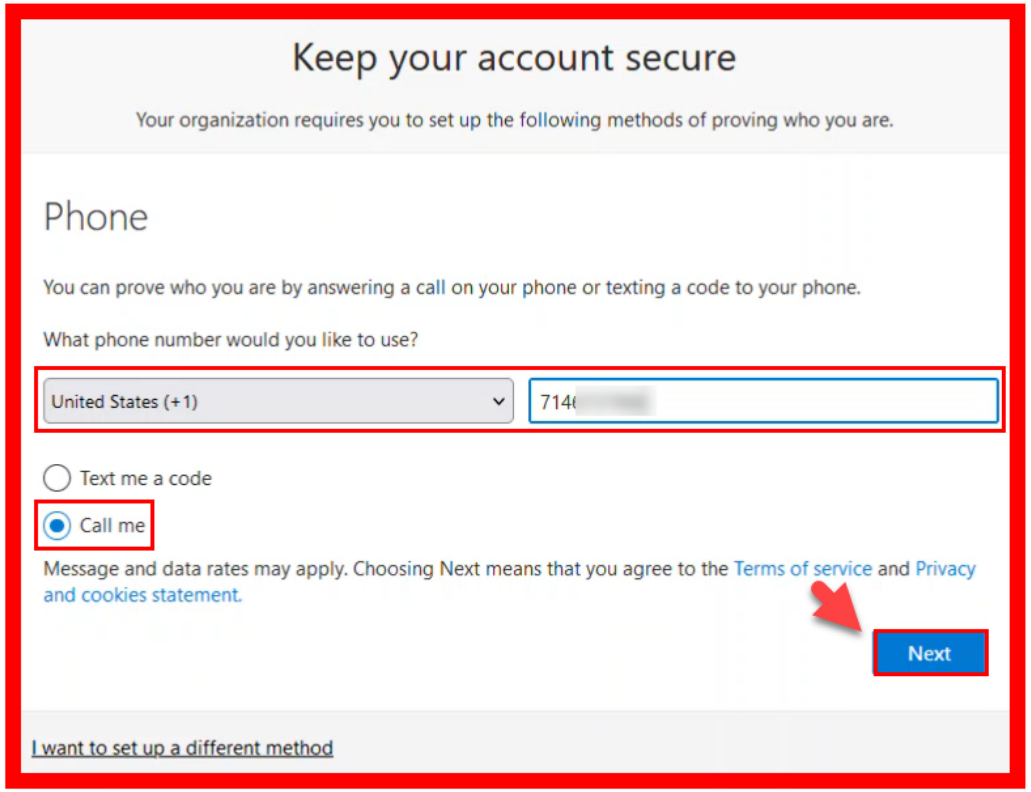
Choose “I want to set up a different method,” then pick “Phone.”





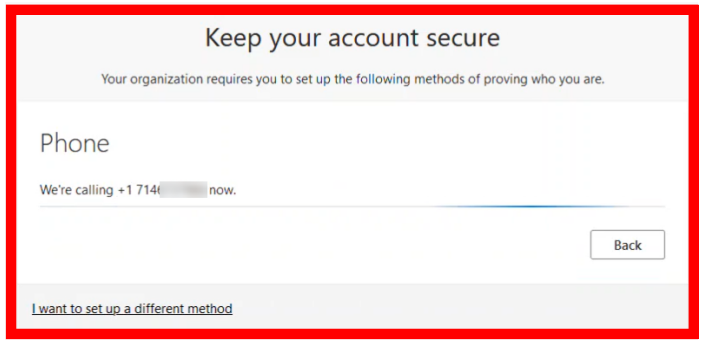
Phone Call – Step 3

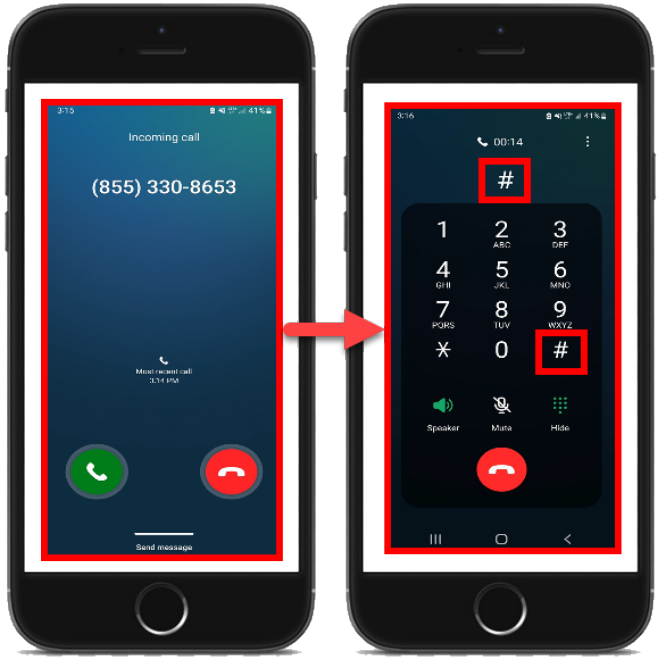
Type in your phone number, then choose "Call me."



Phone Call – Step 4

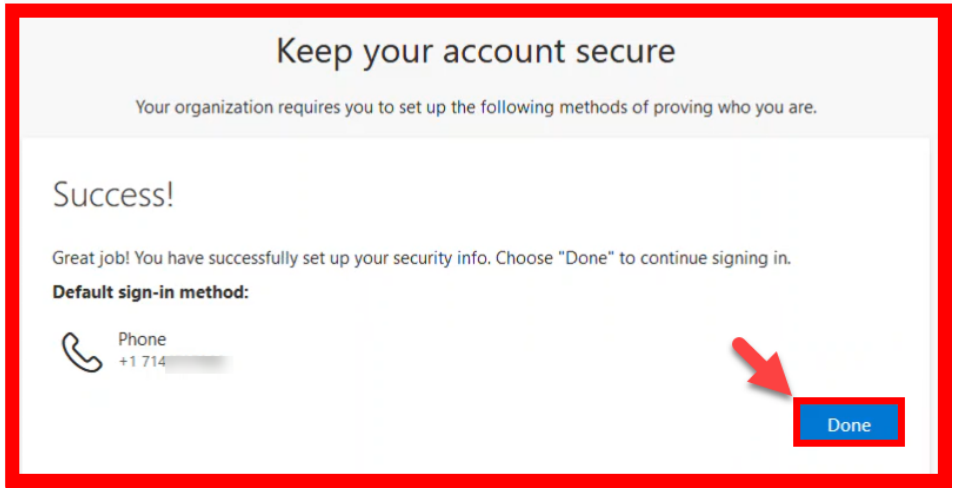
Answer the call from Microsoft and press the "#" key to confirm it's you.

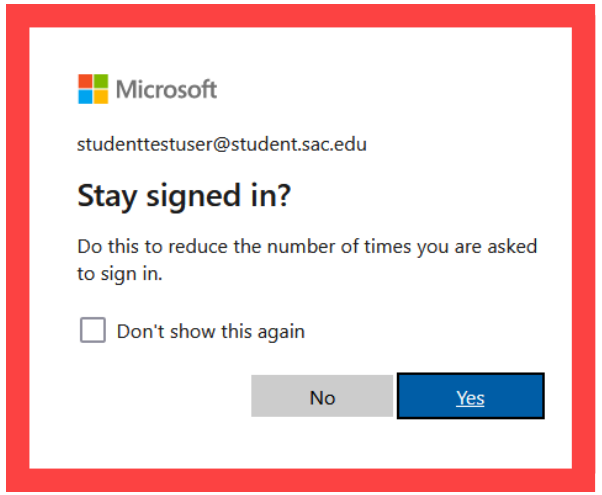




Phone Call – Step 5

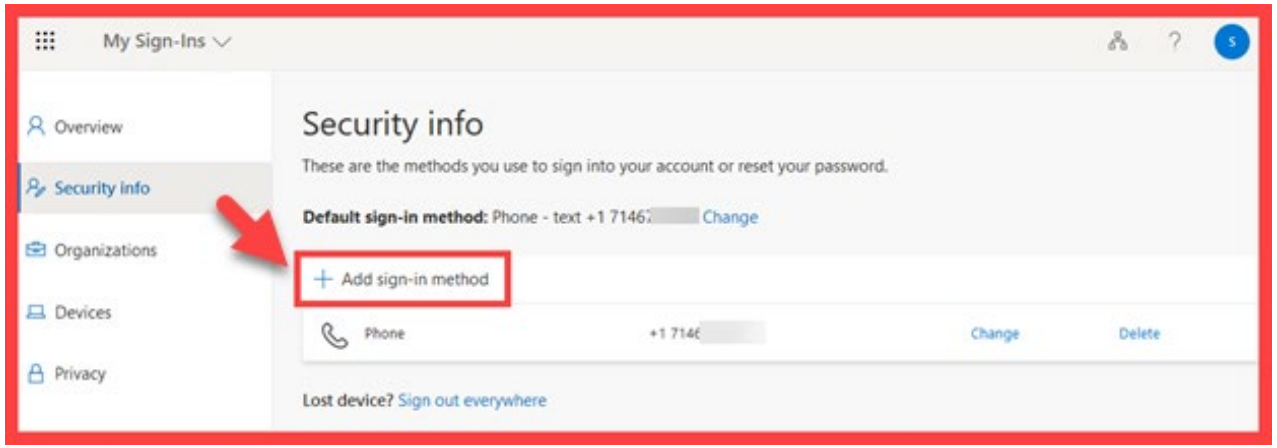
Finish the steps, and you'll be logged into the Security info page at https://aka.ms/mfasetup.





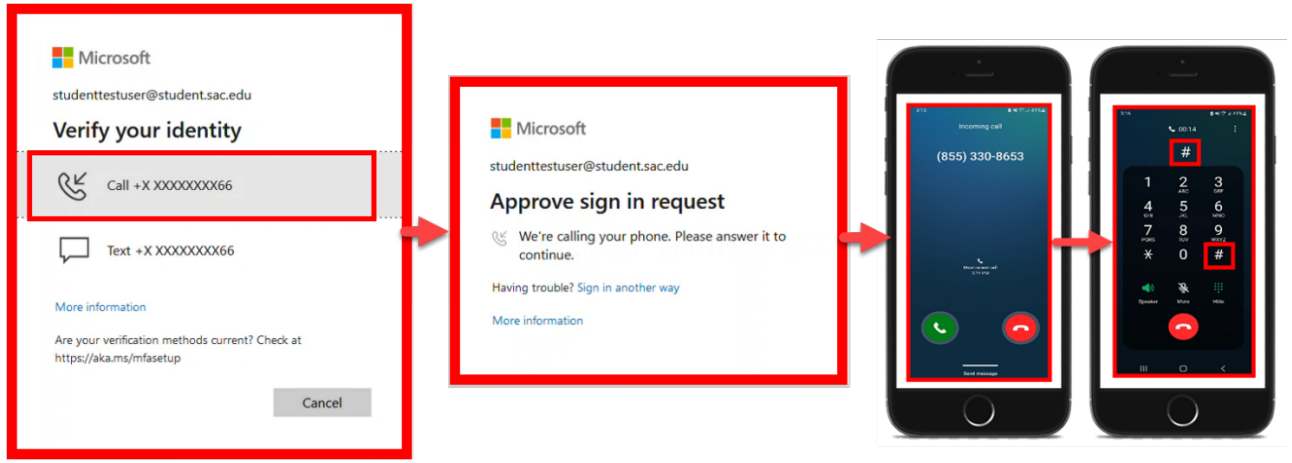
Phone Call – Step 6

On the Security Info page, select "Add sign-in method" to set up a backup authentication method (such as Microsoft Authenticator).



Phone Call – Step 7

The next time you login, you'll receive a phone call to verify it's really you. It's a way to keep your account safe!



(Select this link to return to the summary of steps for Phone Call)

(Select this link to return to the list of Approved Methods for MFA)

Manage Your Backup Authentication Methods

We strongly recommend setting up at least 2 different MFA Methods.
(If you lose access to one method, you can still sign in with the other.)

Follow these steps to access the **My Sign-ins > Security Info** page, where you can manage your MFA methods.

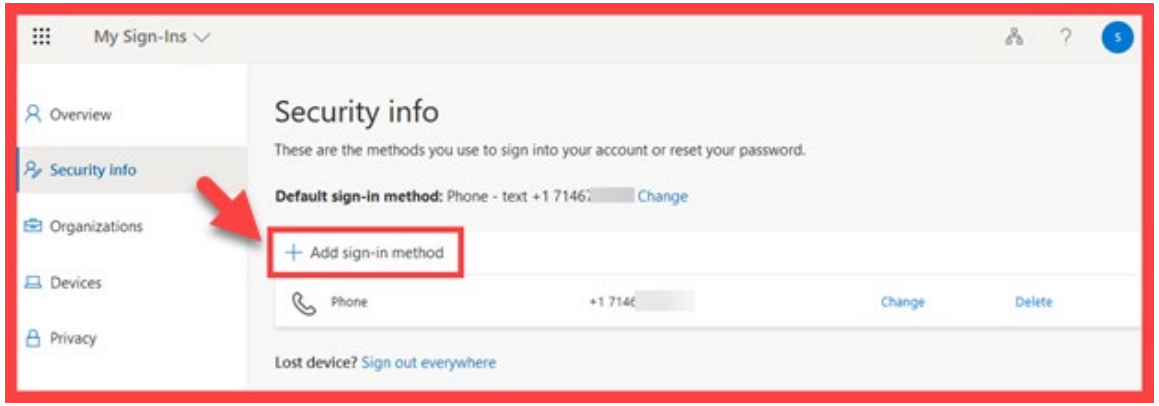
STEP 1

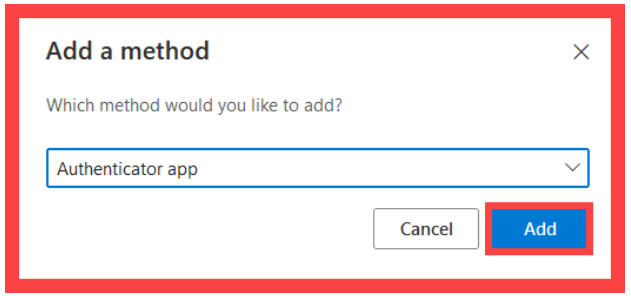
Go to https://aka.ms/mfasetup and login with your Single sign-on credentials.

Or, login to Self-Service > Navigation Menu > User Options > Select the link for Manage Multi-Factor Authentication (MFA)

STEP 2

Use this page to Add, Delete, or Change Your Sign-In Methods.





(Select this link to return to the list of Approved Methods for MFA)
Need help? Select this link for Student Help Desk contact information.