

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.**

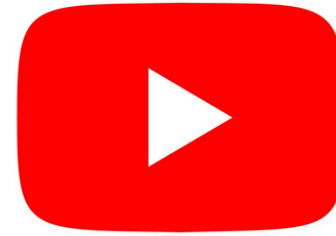
MFA will be enforced for student email and Office365 on January 22, 2024.

- 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.](#)



YouTube

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

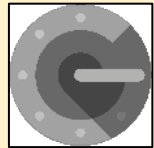
- Phone Number: (714) 628-5086
- Email: studenthelpdesk@sccollege.edu
- Website: [Select this link for the SCC Student Help Desk website.](#)
- Physical Location: SCC Building E-101

[\(Select this link to return to the list of Approved Methods for MFA\)](#)

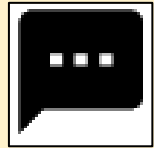
Approved Methods for MFA:



[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.

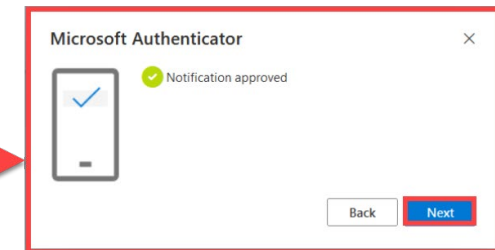
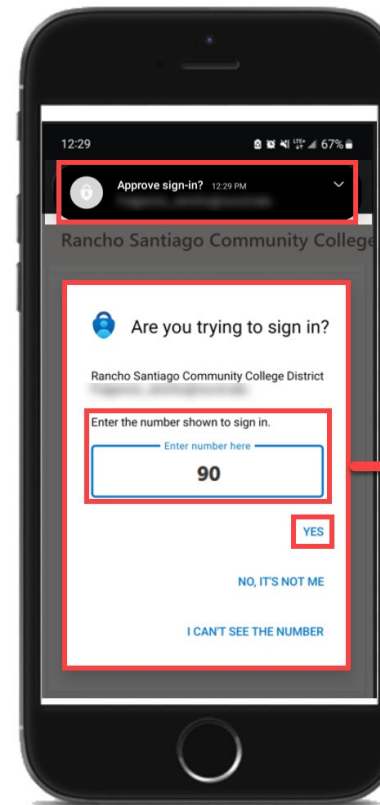
STEP 3 – Follow the instructions on the website. You'll be shown a unique picture known as a QR code. **When you see this QR code, open the MS Authenticator app on your phone, tap "Add work or school account," and then tap "Scan a QR code" to scan the code with your phone's camera.**

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.



[\(Select this link to return to the list of Approved Methods for MFA\)](#)

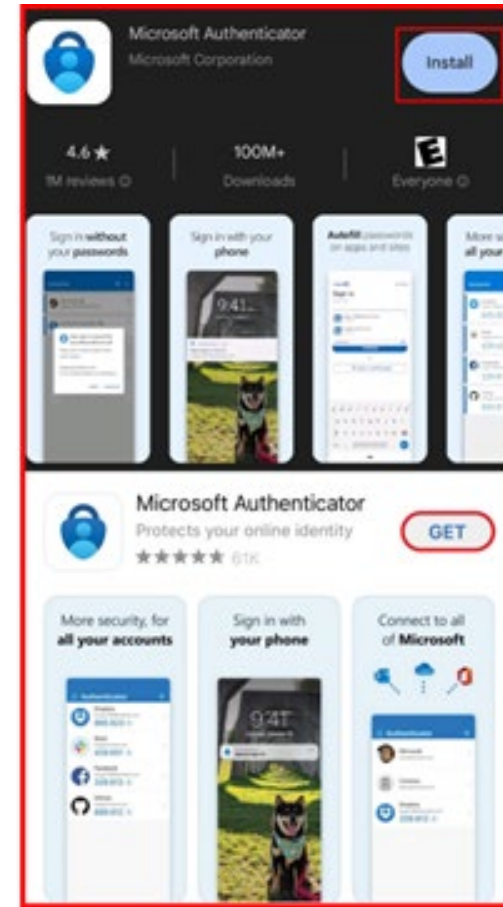


Microsoft Authenticator – Step 1

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.”

Sign in with your organizational account

studenttestuser@student.sac.edu

.....

Keep me signed in

Sign in

Learn More - Single Sign-On FAQ
Retrieve Username or Reset Password

For Students:

- SelfServiceID@student.sccollege.edu
- SelfServiceID@student.sac.edu
- Example: ab12345@student.sac.edu

For Employees:

- LastName_FirstName@sccollege.edu
- LastName_FirstName@sac.edu
- LastName_FirstName@rscsd.edu
- Example: Smith_John@rscsd.edu

Microsoft

studenttestuser@student.sac.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

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



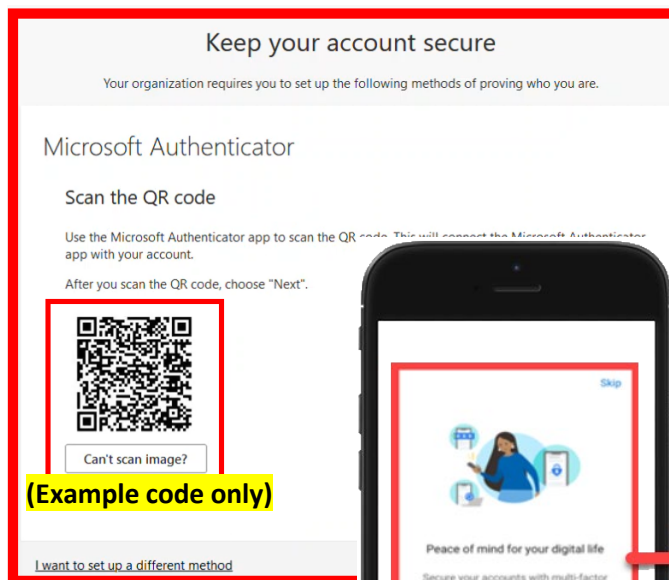
Microsoft Authenticator – Step 3

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.**



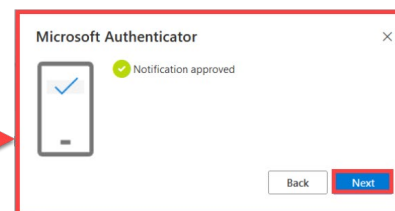
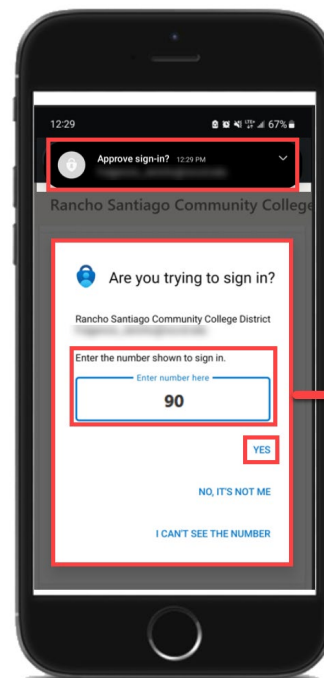
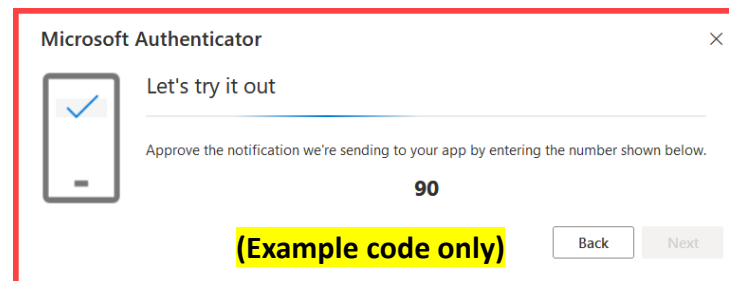
(Open MS Authenticator app > Add work or school account > Scan a QR code)



Microsoft Authenticator – Step 4

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

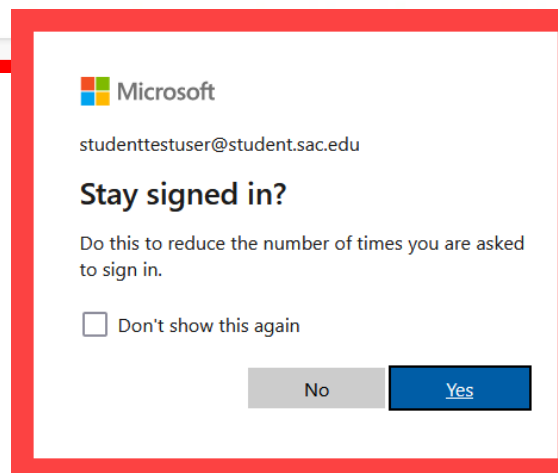
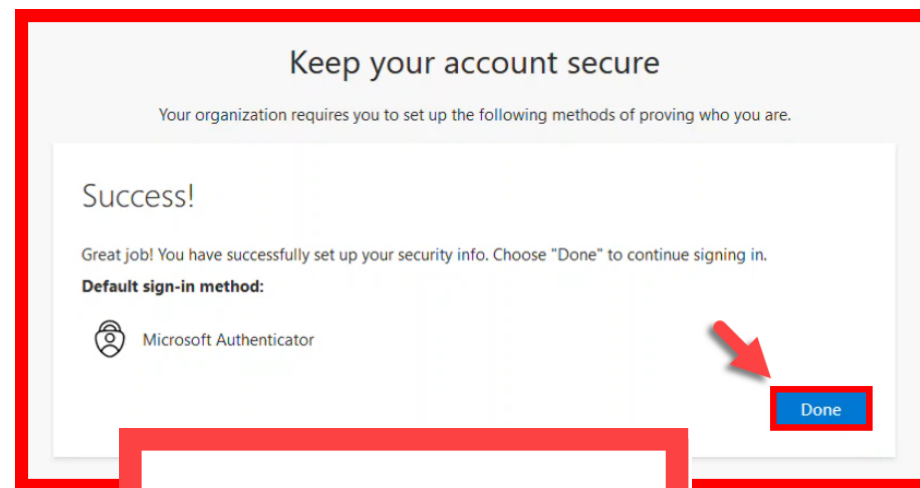
Enter that code where it asks you to on your phone.





Microsoft Authenticator – Step 5

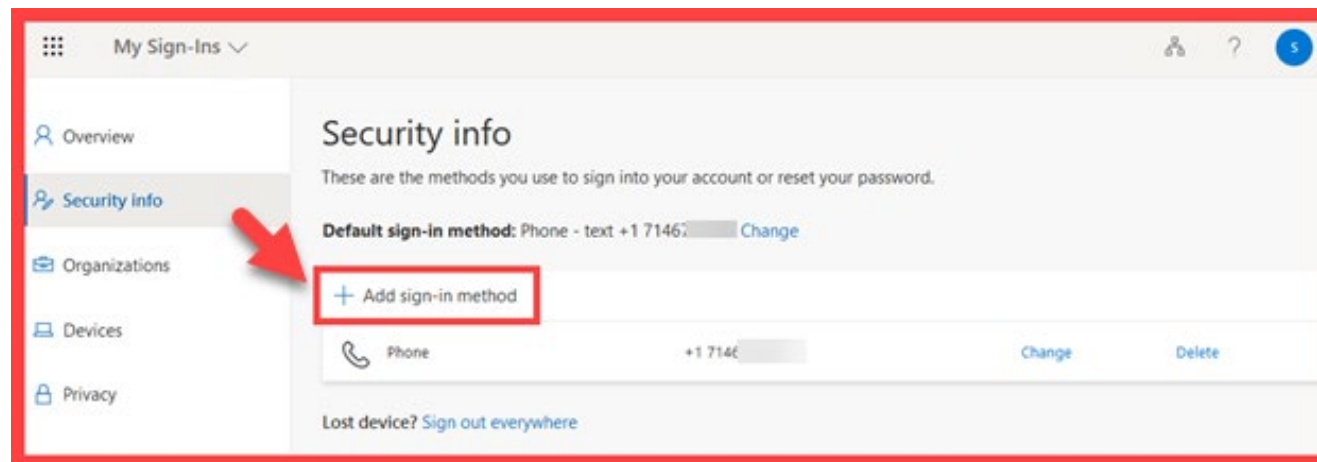
Finish the steps, and you'll be logged into the Security Info page at <https://aka.ms/mfasetup>.





Microsoft Authenticator – Step 6

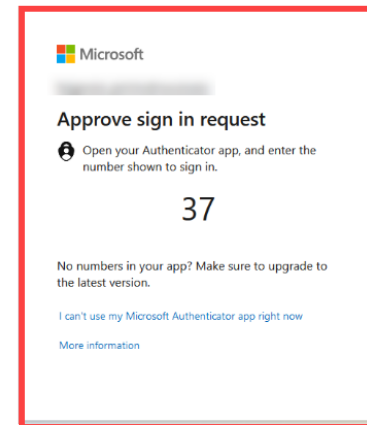
On the Security Info page, select **“Add sign-in method”** to set up a backup authentication method (such as Text or Phone).



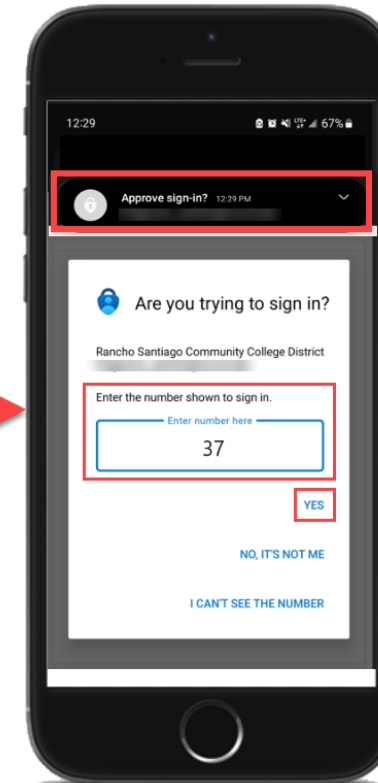


Microsoft Authenticator – Step 7

**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.

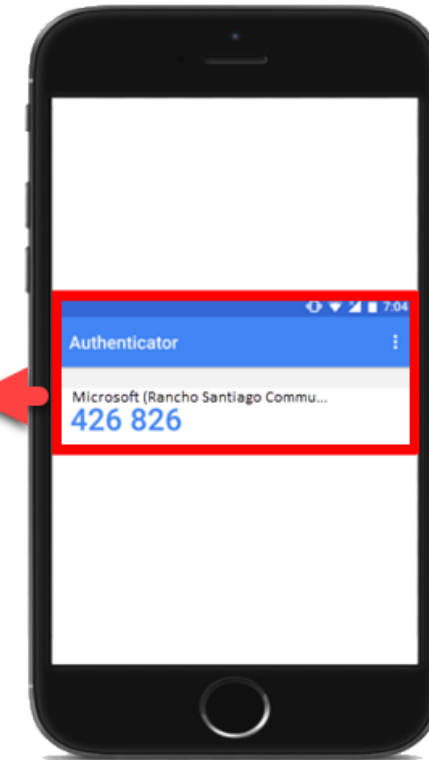
STEP 5 – Follow the steps on the website to check the Google Authenticator app is working correctly.

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!

Microsoft
studenttestuser@student.sac.edu
Enter code
Enter the code displayed in the authenticator app on your mobile device
426826
Having trouble? Sign in another way
More information
Verify



[\(Select this link to return to the list of Approved Methods for MFA\)](#)

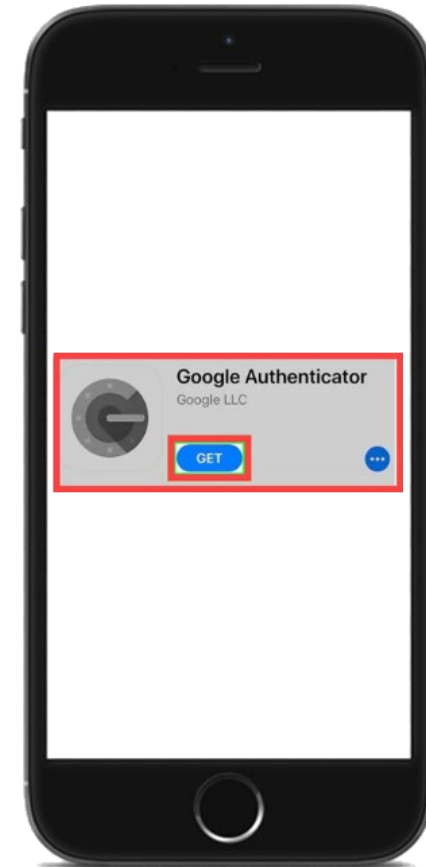
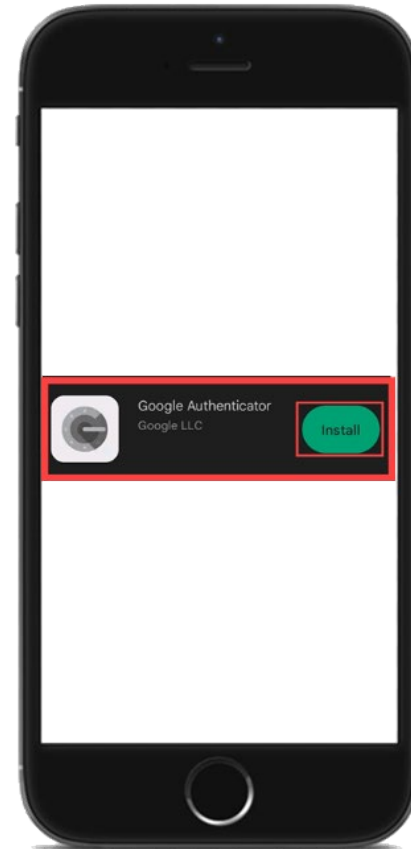


Google Authenticator – Step 1

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.”

The screenshot displays the Microsoft login interface for Santa Ana College. On the left, there are logos for Santiago Canyon College and Santa Ana College, along with a banner for Rancho Santiago Community College District. The main sign-in area includes the text 'Sign in with your organizational account', a text input field containing 'studenttestuser@student.sac.edu', a password field with masked characters, and a 'Keep me signed in' checkbox. A blue 'Sign in' button is visible. Below the sign-in area, there is a section for 'Login authentication' with links for 'Learn More - Single Sign-On' and 'Retrieve Username or Password'. It lists options for 'Students' and 'Employees' with example email addresses. A red box highlights the 'Sign in' button and the 'More information required' section. The 'More information required' section features the Microsoft logo, the email address 'studenttestuser@student.sac.edu', the heading 'More information required', and the message 'Your organization needs more information to keep your account secure'. It includes links for 'Use a different account' and 'Learn more', and a blue 'Next' button at the bottom right.

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.”**

Keep your account secure

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

Microsoft Authenticator

 Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

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



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.**

Keep your account secure

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

Authenticator app

Scan the QR code

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

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

Can't scan image?

(Example code only)

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

Stronger security with Google Authenticator

Get verification codes for all your accounts using 2-Step Verification

Get started

Setup your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to [g.co/2sv](#)

Scan a QR code

Enter a setup key

Place barcode within red lines

Secret saved

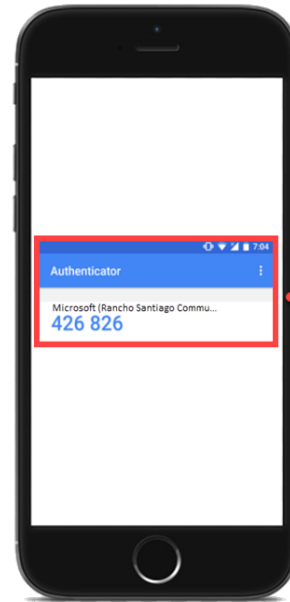


Google Authenticator – Step 5

**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.**



Keep your account secure

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

Authenticator app

Enter code

Enter the 6-digit code shown in the Authenticator app.

426826

(Example code only)

Back Next

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



Google Authenticator – Step 6

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

Keep your account secure


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

Success!

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

Default sign-in method:

Authenticator app

 Microsoft

studenttestuser@student.sac.edu

Stay signed in?

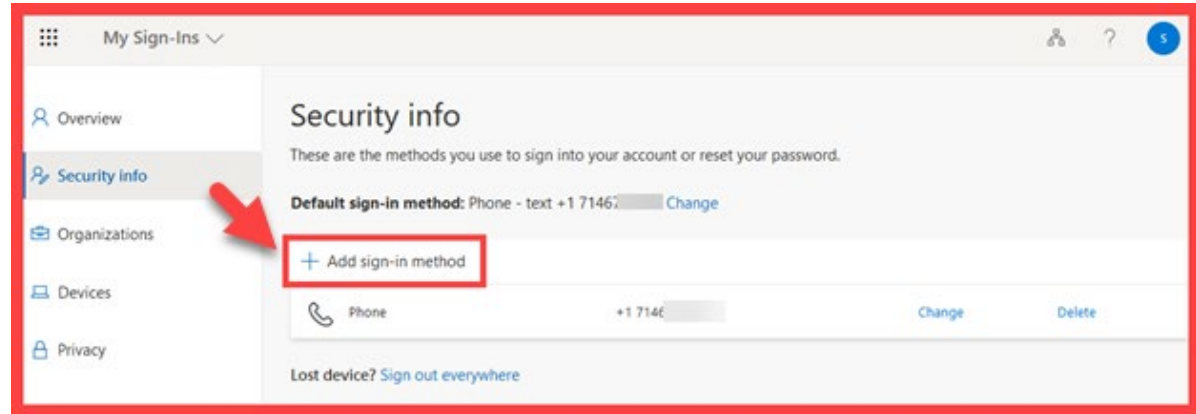
Do this to reduce the number of times you are asked to sign in.

Don't show this again



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](#)).

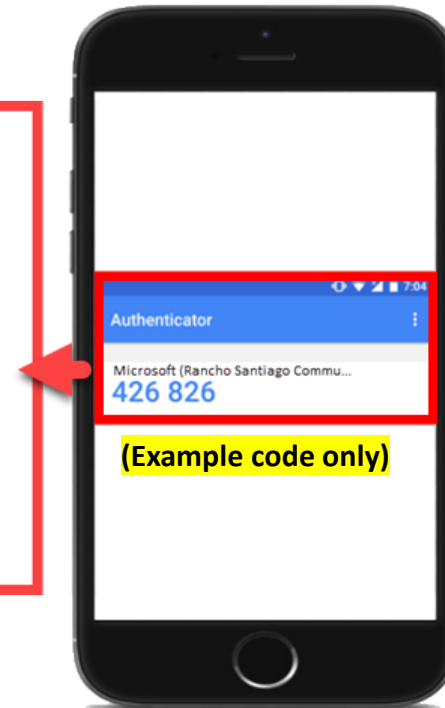




Google Authenticator – Step 8

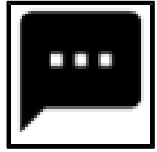
**The next time you log in, the Authenticator app will help make sure it's really you.
It's a way to keep your account safe!**

Microsoft
studenttestuser@student.sac.edu
Enter code
Enter the code displayed in the authenticator app on your mobile device
426826
Having trouble? [Sign in another way](#)
[More information](#)
Verify



[\(Select this link to return to the summary of steps for Google Authenticator\)](#)

[\(Select this link to return to the list of Approved Methods for MFA\)](#)



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.”**

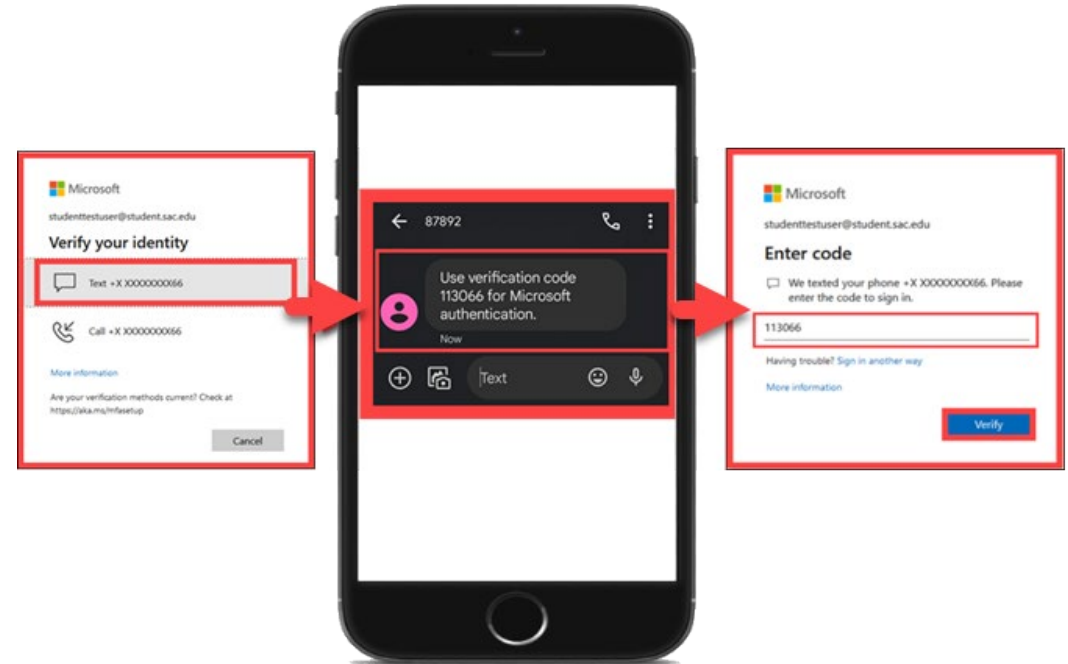
STEP 3 – Type in your phone number, then choose **“Text me a code.”**

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

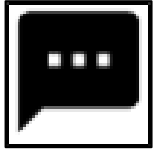
STEP 5 – Finish the steps, and you’ll be logged into the Security Info page at <https://aka.ms/mfasetup>.

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

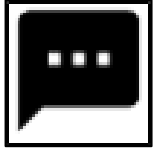
Go to <https://aka.ms/mfasetup> on a computer or tablet.

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

Select “Next” when it asks for “More Information Required.”

The screenshot shows a Microsoft login interface for a college account. On the left, there are logos for Santiago Canyon College and Rancho Santiago Community College District. The main area shows a sign-in prompt: "Sign in with your organizational account". Below this is a text input field containing "studenttestuser@student.sac.edu" and a password field with masked characters. There is a checkbox for "Keep me signed in" and a blue "Sign in" button. Below the sign-in options, there is a section for "Login authentication screen" with links for "Learn More - Single Sign-On" and "Retrieve Username or Reset Password". There are also instructions for students and employees with example email addresses. On the right, a red-bordered box highlights the "More information required" screen, which displays the Microsoft logo, the email address "studenttestuser@student.sac.edu", and the message "Your organization needs more information to keep your account secure". It includes a blue link for "Use a different account", a "Learn more" link, and a blue "Next" button at the bottom right.

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.”**

Keep your account secure

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

Microsoft Authenticator

 Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

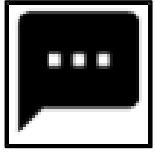
[I want to set up a different method](#)

Choose a different method ×

Which method would you like to use?

Phone

[Cancel](#) [Confirm](#)



SMS Text Message – Step 3

Type in your phone number,
then choose **“Text me a code”**.

Keep your account secure

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

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?

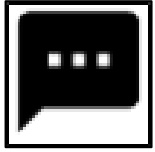
United States (+1) 7146

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](#).

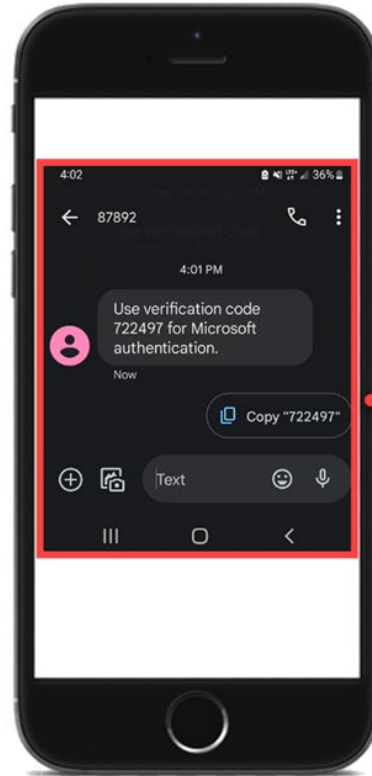
[Next](#)

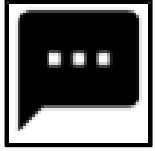
[I want to set up a different method](#)



SMS Text Message – Step 4

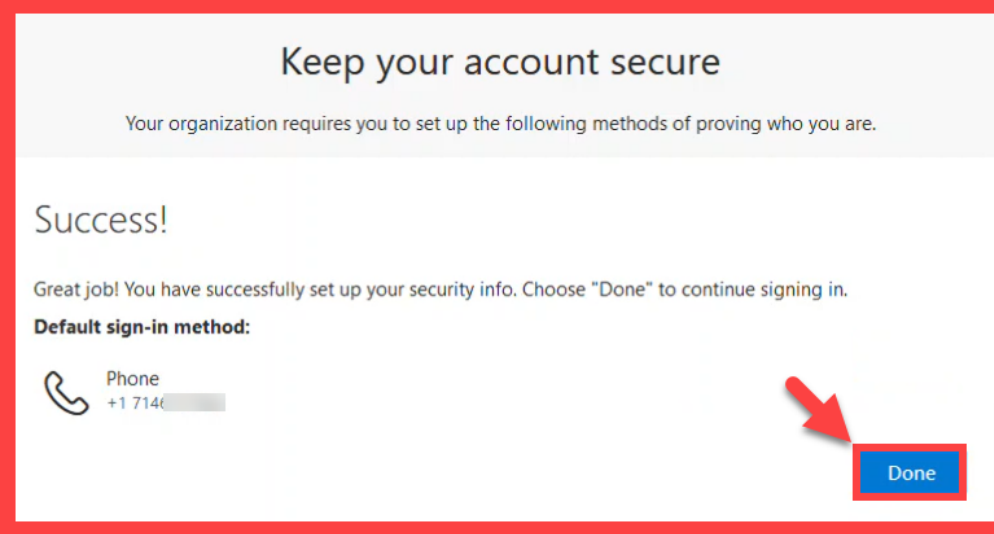
You'll get a code in a text message on your phone.
Enter that code where it asks you to.

A screenshot of a web page titled "Keep your account secure". Below the title is the text "Your organization requires you to set up the following methods of proving who you are." The page is for "Phone" authentication. It shows a text input field with the value "722497" and a "Resend code" link below it. A yellow box highlights the input field with the text "(Example code only)". At the bottom right, there are "Back" and "Next" buttons, with a red arrow pointing to the "Next" button. At the bottom left, there is a link that says "I want to set up a different method".



SMS Text Message – Step 5

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



Keep your account secure

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

Success!

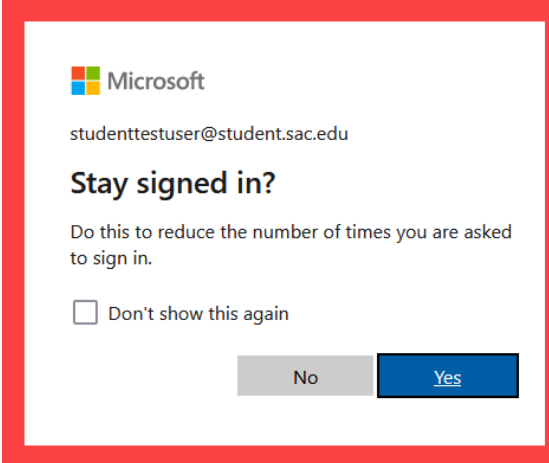
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Phone
+1 714[redacted]

Done

A red arrow points to the blue "Done" button.



Microsoft

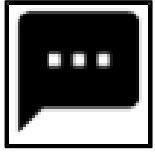
studenttestuser@student.sac.edu

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

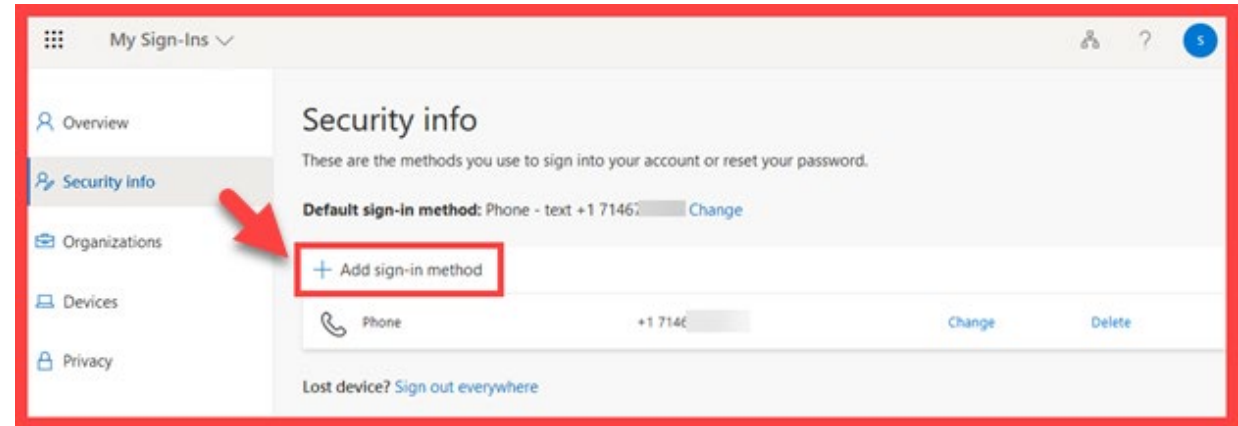
Don't show this again

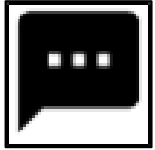
No Yes



SMS Text Message – Step 6

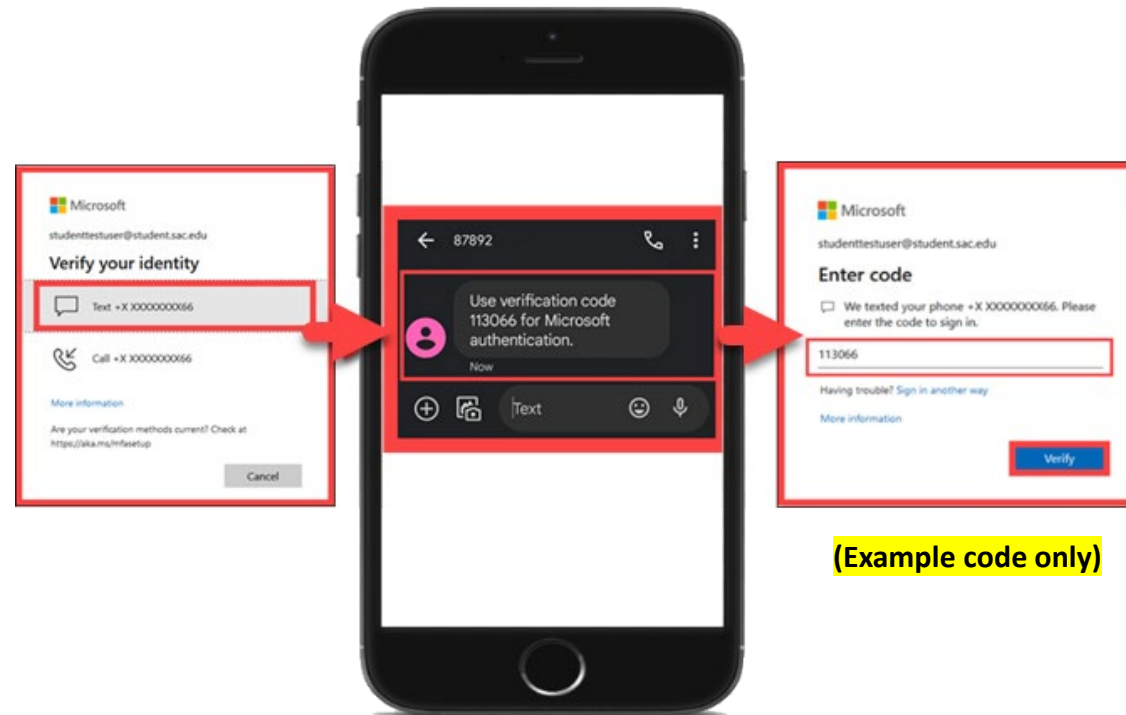
On the Security Info page, select **“Add sign-in method”** to set up a backup authentication method (such as [Microsoft Authenticator](#)).





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!



[\(Select this link to return to the summary of steps for SMS Text Message\)](#)

[\(Select this link to return to the list of Approved Methods for MFA\)](#)



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.”**

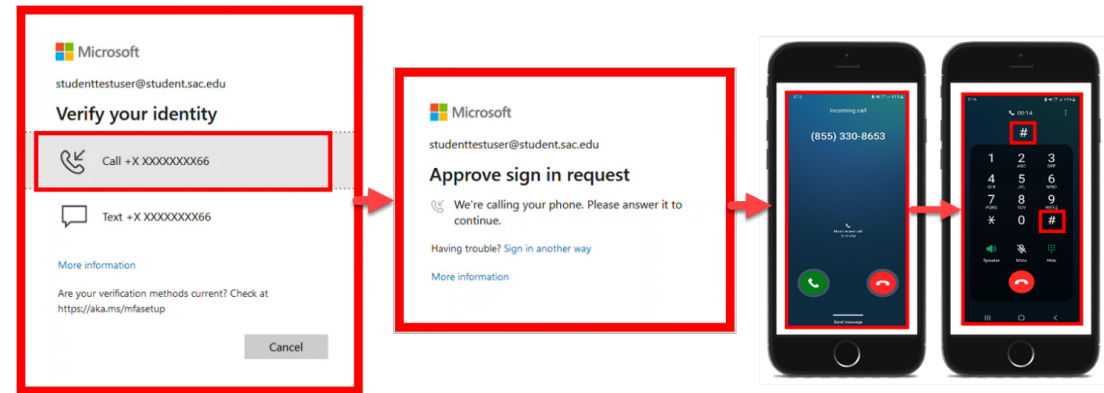
STEP 3 – Type in your phone number, then choose **“Call Me.”**

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.”

Santa Ana College
SANTA ANA COLLEGE
Sign in with your organizational account
studenttestuser@student.sac.edu
.....
 Keep me signed in
Sign in
Login authentication
Learn More - Single
Retrieve Username o
For Students:
• SelfServiceID@studen
• SelfServiceID@studen
Example: ab12345@st
For Employees:
• LastName_FirstName@
• LastName_FirstName@
• LastName_FirstName@
Example: Smith_John@

Microsoft
studenttestuser@student.sac.edu
More information
required
Your organization needs more
information to keep your account secure
Use a different account
Learn more
Next

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.”**

Keep your account secure

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

Microsoft Authenticator

 Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

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

Choose a different method ×

Which method would you like to use?

[Cancel](#) [Confirm](#)



Phone Call – Step 3

Type in your phone number,
then choose **“Call me.”**

Keep your account secure

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

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) 714

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](#).

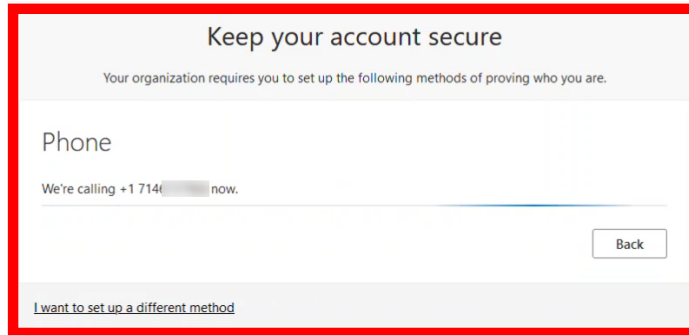
[Next](#)

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



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>.


Keep your account secure


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


Success!

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

Default sign-in method:

 Phone
+1 714 [redacted]

 [Done](#)

 Microsoft

studenttestuser@student.sac.edu

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

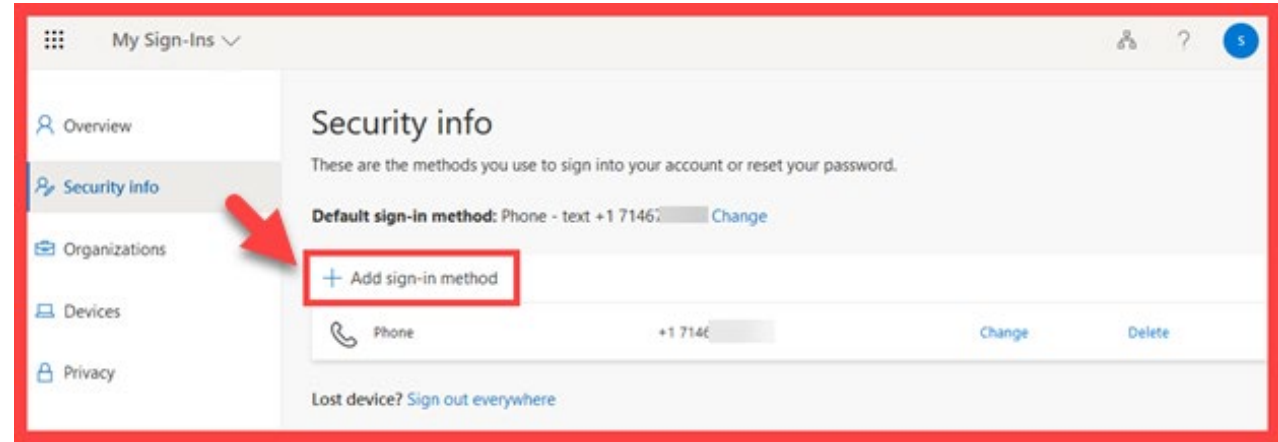
Don't show this again

[No](#) [Yes](#)



Phone Call – Step 6

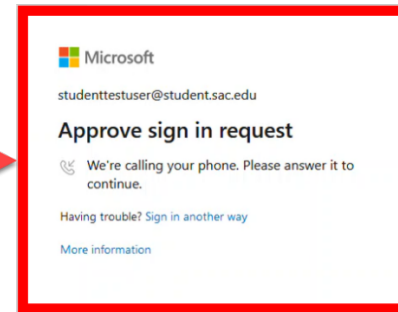
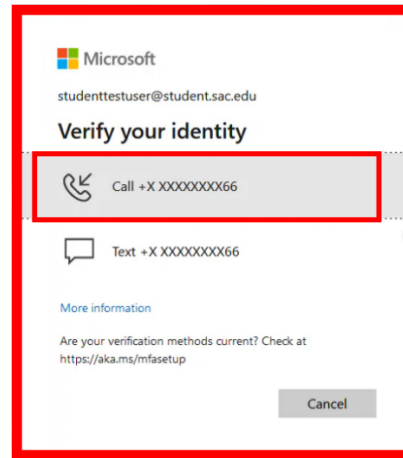
On the Security Info page, select **“Add sign-in method”** to set up a backup authentication method (such as [Microsoft Authenticator](#)).





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.

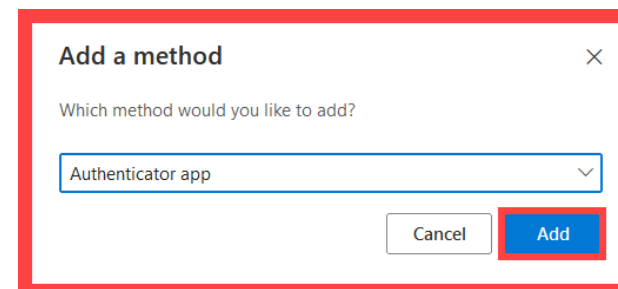
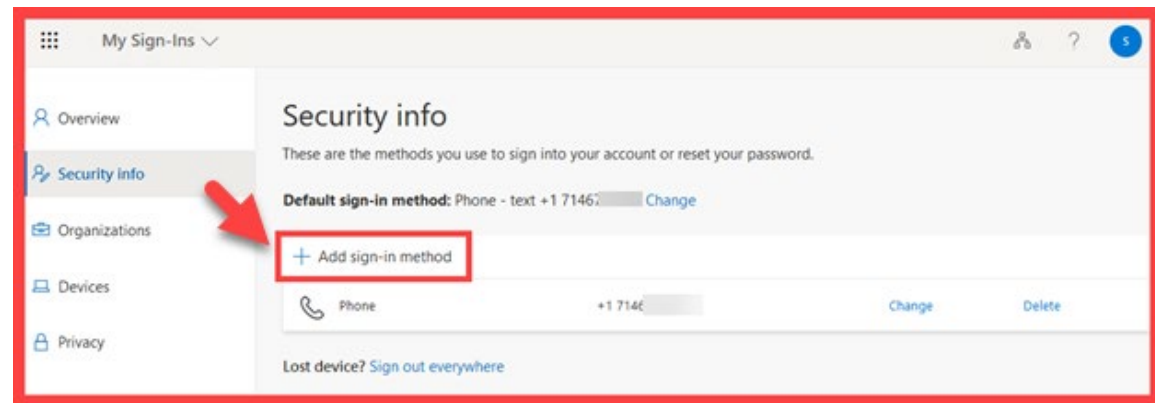
STEP 1

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.](#)