

Multi-Factor Authentication (MFA): Update Contact Methods

Introduction	1
Using the Authenticator App for MFA	2
Updating contact methods	4

Introduction

SCSU has enabled multi-factor authentication (also known as MFA) for all University accounts. This enhanced security feature will only occur when you are not connected to an SCSU network (computer lab, employee computer, SSL wireless network, eduroam wireless network). This two-step verification model is an effective measure in protecting your account from malicious hackers. When prompted for MFA verification, you will have the option to trust your device which will suppress this requirement for sixty days on that device.

Microsoft is phasing out native SMS and voice multi-factor authentication (MFA) in [Microsoft Entra ID](#) due to security vulnerabilities. Starting September 1, 2026, passkeys become the default and users on SMS/voice will be auto-enabled. On February 1, 2027, Microsoft-provided SMS delivery is fully retired unless organizations buy a customer-managed telecom add-on.

Key Timeline Dates

- **September 1, 2026:** Passkeys become the default sign-in method; users currently using SMS or voice are automatically enabled and prompted to register passkeys.
- **February 1, 2027:** Microsoft completely retires free, natively provided telecom SMS and voice delivery for MFA.

What This Means For You

- **Security Risk:** Microsoft considers SMS and voice texts weak and vulnerable to phishing and SIM-swapping attacks
- **No Free SMS After Feb 2027:** Standard tenants can no longer use Microsoft-provided SMS for MFA after February 1, 2027
- **Paid Workaround:** Organizations with strict regulatory or business needs for SMS must configure and pay for a customer-managed telecom provider via the Microsoft Security Store.
- **Required Action:** Users with only SMS/voice MFA will be forced to register a passkey or alternative secure method during sign-in to keep accessing their accounts.

The following steps will walk you through how to update your contact methods for Multi-factor Authentication (MFA). These instructions are intended for those who currently have access to their account. If you do not have access to your account, either due to a password issue or due to not being able to bypass the current MFA prompt in place, contact the Help Desk.

Using the Authenticator App for MFA

The [Microsoft Authenticator App](#) makes MFA an easy task. This application will generate the timed code needed for signing in and will also work without a network or data connection (after setup is completed).

Step 1. Select the Authenticator App and click **Confirm**. Then click **Next**.

Choose a different method

Which method would you like to use?

Authenticator app

Cancel

Confirm

Step 2. You will be prompted to setup the Authenticator App on your phone. Click **Next**.

- To begin: Download the Microsoft Authenticator app on your Android or iPhone device from the app store.
- Once the app is downloaded, open the app and sign in with your SCSU account.
 - Enter your full SCSU email address and password
- Once signed in, you will need to add an account. Tap the '+' (plus sign) to add an account.
 - Select work or school account.
- The QR code will now be available.

Step 3. Next, you will need to scan the QR code that appears on the webpage via the Authenticator App.

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?](#)

Back

Next

Step 4. Scan the code with your phone.

Step 5. The account will now appear in the Microsoft Authenticator app on a successful configuration.

Step 6. Click Next to complete.

(Image of Microsoft Authenticator screen)

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app.

Back

Next

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

Step 7. The system will send a notification to the app on your device, click **Approve** in the mobile app.

Step 8. On a successful approval, the following screen will show:

Microsoft Authenticator



✓ Notification approved

Back

Next

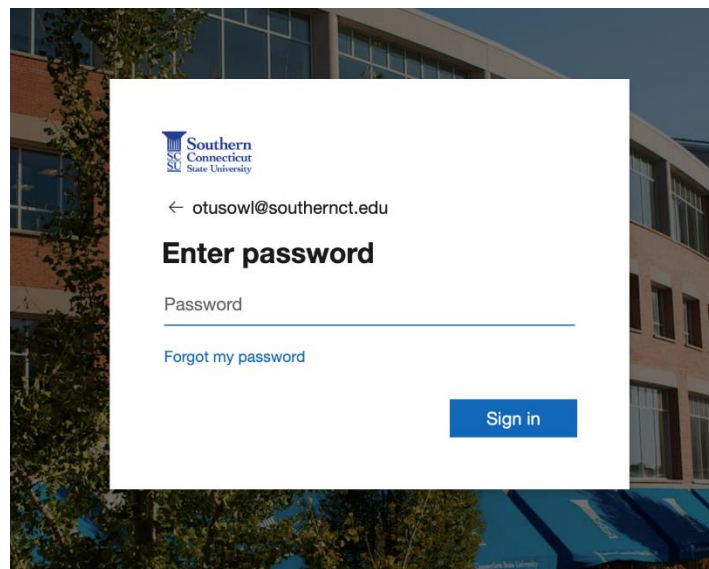
I want to set up a different method

Step 9. Click **Next** to complete the setup.

Step 10. A 'Success!' page should now be shown, click **Done**. MFA is now configured for the Microsoft Authenticator App.

Updating contact methods

1. Go to login.southernct.edu. Sign in using your full SCSU email address and password.



2. Authenticate your account.


otusowl@southernct.edu

Enter code

☐ We texted your phone +X XXXXXXXX91. Please enter the code to sign in.

Code

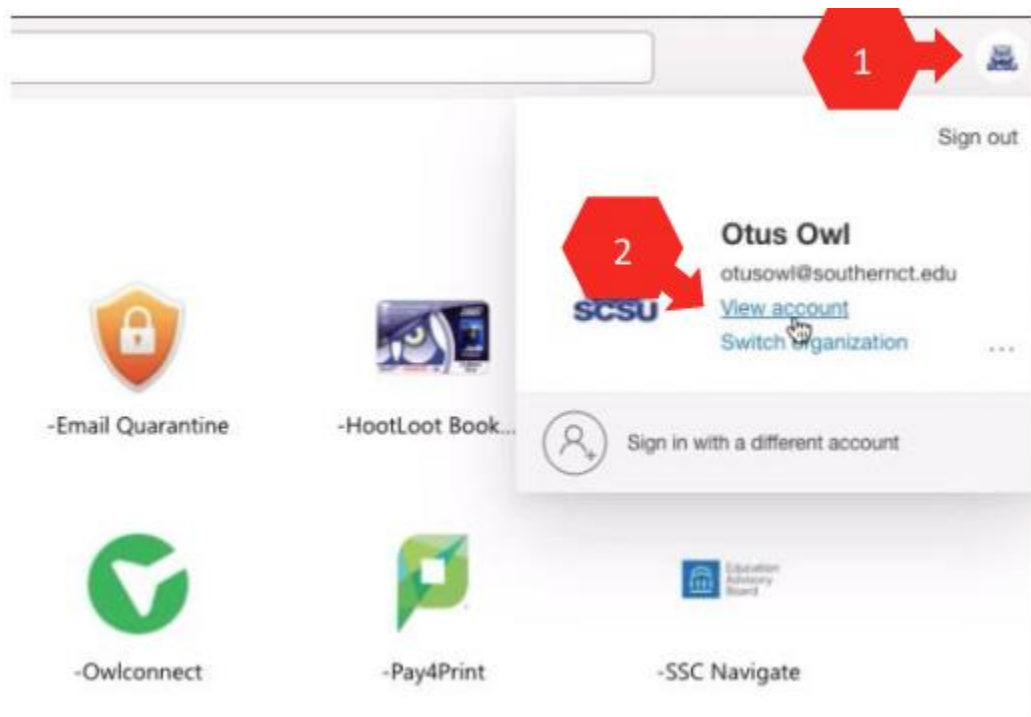
☐ Don't ask again for 60 days

Having trouble? [Sign in another way](#)

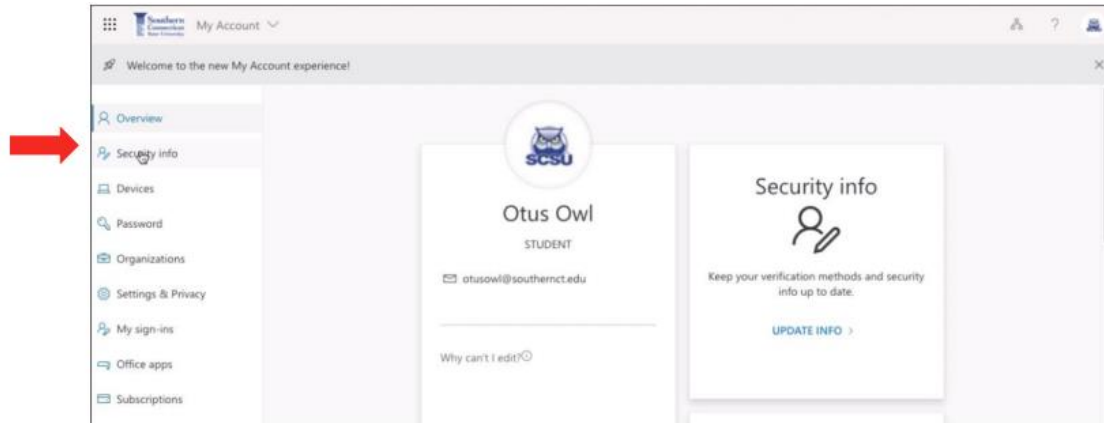
[More information](#)

[Verify](#)

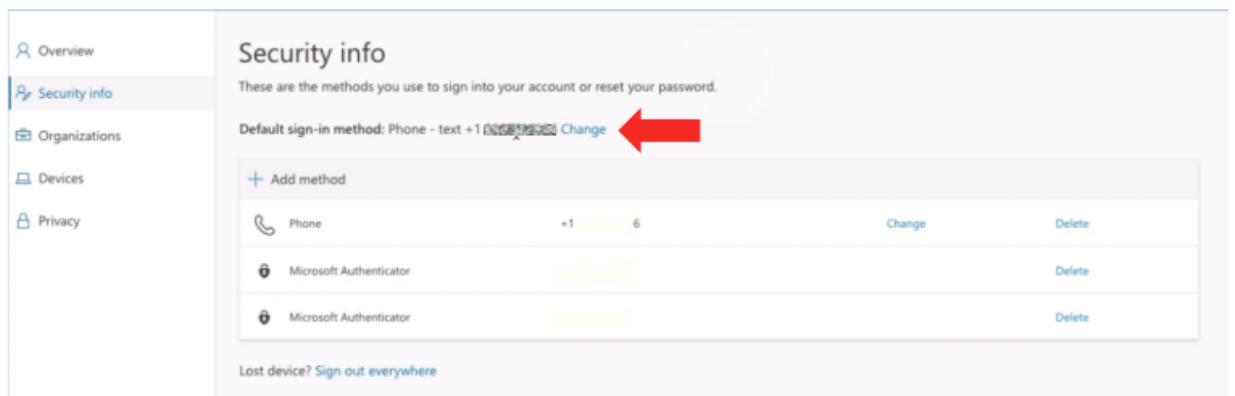
3. Select the profile icon in the upper, right-hand corner, then “View account”.



4. Select “Security info” from the left menu:



5. Select “Change” next to the piece of information you wish to update. You may also “Add method” or “Delete” if needed. Here, we will be updating our current phone number being used for MFA.



6. After selecting “Change”, enter the new information and desired contact method (**Please remember that text or call will be fully retired in the coming months. Taking that into account, it is highly advised that if the current default sign-in method is either SMS or voice delivery for MFA, please Change the method to reflect the Microsoft Authenticator**), and select “Next” once finished.
7. After verifying your information, you are all set to use this as your new MFA method.