Banner Health

CLINICAL CONNECTIVITY GETTING STARTED

Table of Contents

GETTING STARTED

Your healthcare office has identified a Clinical Connectivity Group Administrator to be the liaison for your group and Banner Health. The Group Administrator is your primary contact for Clinical Connectivity questions, problems, and/or issues. Please review the Clinical Connectivity Electronic Transmission Agreement with your Clinical Connectivity Group Administrator.

Browser, System and Connection Requirements

- Computer running Microsoft Windows 7, 8.1, 10, or 11 (Windows 7 and 8.1 will be discontinued in 2023)
    - Supported browsers: Microsoft Edge, Google Chrome, Internet Explorer (Explorer will also be discontinued)
- Computer running MAC OSx 10.15 and above
    - Supported browsers: Safari (7.0 and above), Chrome (28.x and later), Mozilla Firefox (22.x and later)
- Broadband internet access

Technical note: To install the required application versions below, you will need administrative access to your computer. If you do not have administrative rights on your computer, you will need assistance from your IT for application installation.

- Minimum .NET version is 4.8 (requires admin rights)
- Minimum VCRedist is 14.30.30704.0 (requires admin rights)
- Citrix Workspace 19.12 runs on Windows 10, 8.1, or 7 and will be discontinued in 2023
- Citrix Workspace 22.02 runs on Windows 11, 10, and 8.1

Login Credentials

Users will receive a LAN ID (Banner username) and temporary password via **two** secure email messages.
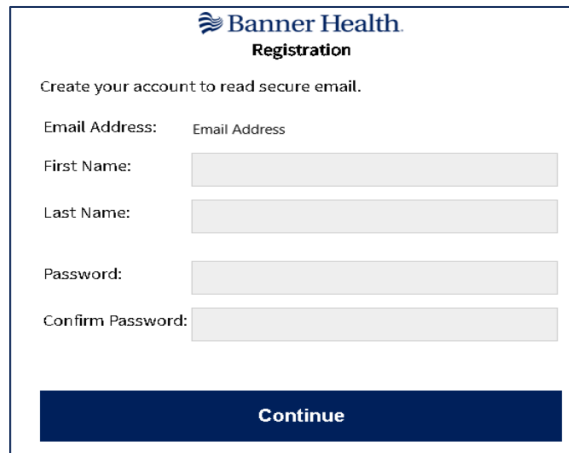
- If you did not receive the log in credentials, have them contact the Helpdesk at 602-747-4444 option 3

- If you had previous access to Banner systems and the account is active, only the username will be sent. Utilize your previous credentials. If you do not remember the credentials, contact the helpdesk at 602-747-4444 opt. 3 to request a password reset.
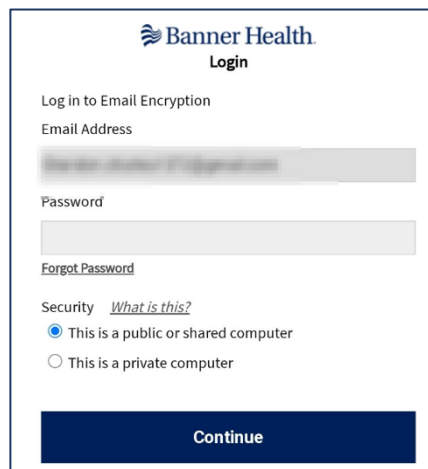
Encrypted Emails – Proofpoint

- Username and password will be sent via two Proofpoint encrypted emails.
- If this is the first time accessing Proofpoint encrypted emails, you will be prompted to set up an account with Proofpoint Encryption when you click on the "click here" link in the email.
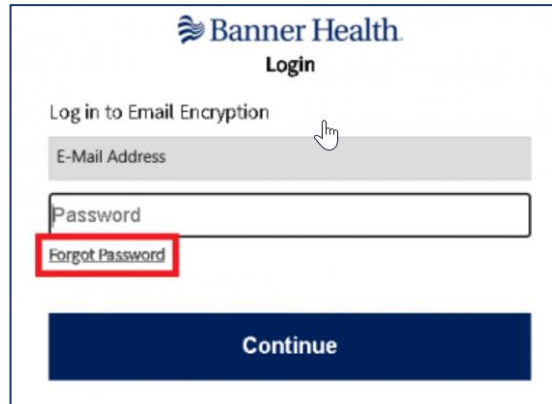

- When prompted for your email address, make sure to use the **same email address** with which you received the secure email notification.

- If you have already registered, or if your account already exists, you will be prompted to sign in and provide your password to decrypt the message. Click Continue.

- From this point on, log into to the Encrypted Email system with that login information. If you forget your password, use the "**Forgot Password**" link. <u>The Banner IT Service Desk **does not** have the ability to reset these passwords</u>.

Technical Support

- If you have urgent problems or questions, call the Service Desk at (602) 747-4444.
  - ➢ Press '3' for the Clinical Service Desk if you're having clinical application issues.
  - ➢ Press '2' for the Technical Service Desk if you're having computer-related access issues.
- For all other questions regarding Clinical Connectivity practice enrollment, enrollment status, or practice management, please contact the Clinical Connectivity Administrators at webconnect@bannerhealth.com

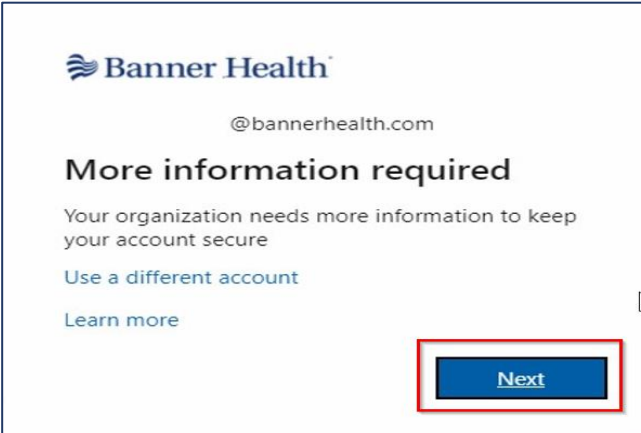## Azure MFA (Microsoft Authenticator) Mobile Phone or Tablet Enrollment

You are required to have **Microsoft Authenticator** installed on a mobile device. Microsoft Authenticator is a security tool used to generate a secondary random passcode on your mobile device that is required to log into Banner's remote applications.

➢ Alternatively, you can select to enroll via Phone Call Back, which **does not** require smartphone or software installation**. (Click Here for Phone Call Back Instructions).**

➢ If you already have the **Microsoft Authenticator** app downloaded on your mobile device and have a registered Banner account that you can add an existing method. **(Click Here for Adding Existing Method Enrollment Instructions).**

➢ For help with the Azure MFA enrollment process please contact the Banner Service Desk at **602-747-4444.**

1. From a Work or Personal Computer, go to **https://mysignins.microsoft.com/security-info**

2. Sign in using your **Microsoft Authenticator** username Example: (**ccTUser@bannerhealth.com**) and password.

a. You will be prompted for more information, click **Next**

3. You will then be prompted to download the app.
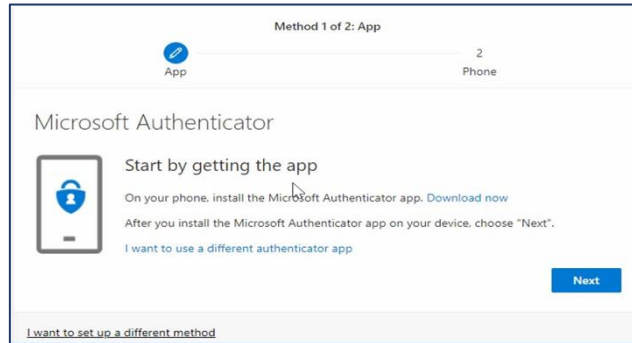
4. On your **mobile** device, download the **Microsoft Authenticator** app from the app store.
   a. For Android Devices - https://play.google.com/store/apps/details?id=com.azure.authenticator
   b. For iOS Devices - https://apps.apple.com/us/app/microsoft-authenticator/id983156458

5. After you download the app, press **Next** on your computer screen to begin the setup process
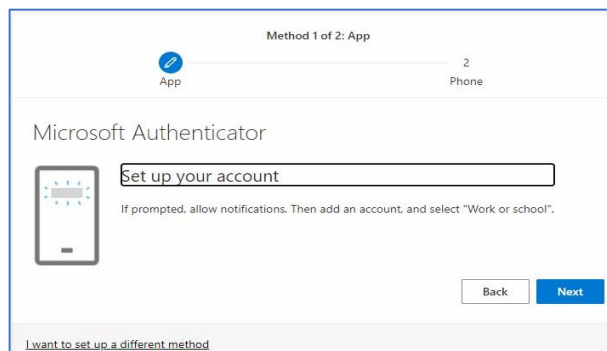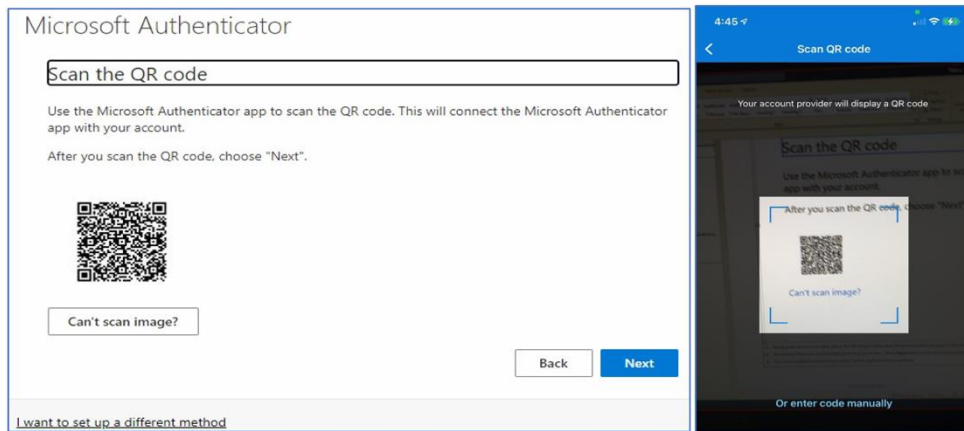

   a. In the Authenticator app, select **Add Account.** Press **Add New Account**.
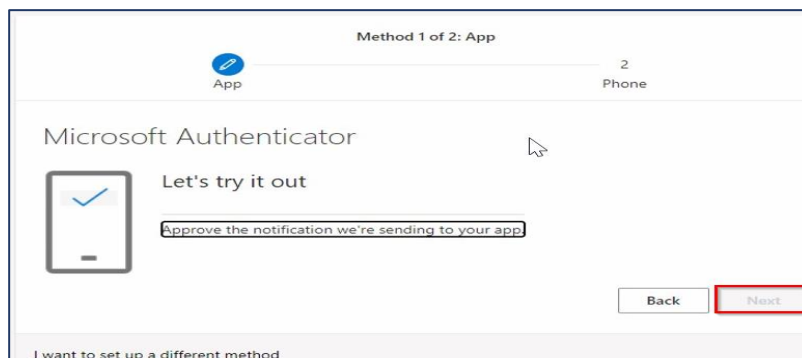   b. Select **Work or School Account**.
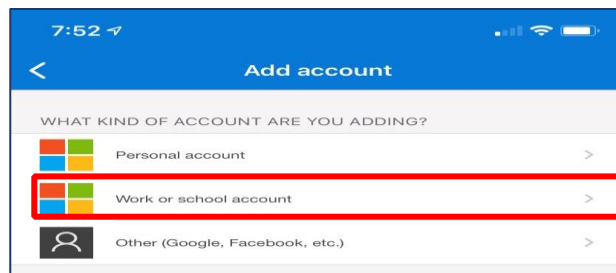

   c. Select **Scan QR code.**
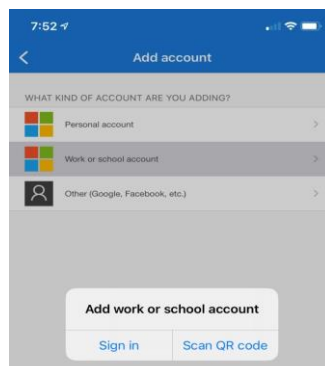
6. After clicking **NEXT** on your computer screen you will see the QR code unique to your registration.
7. Using your device's camera, place the QR image in the view finder to allow the app to scan the code.

8. Click **Next** on your **computer** after you scan the QR code, you'll get the verification screen.

9. A test notification will be sent to your personal device. Press **Approve** on your device to acknowledge the authentication test request.
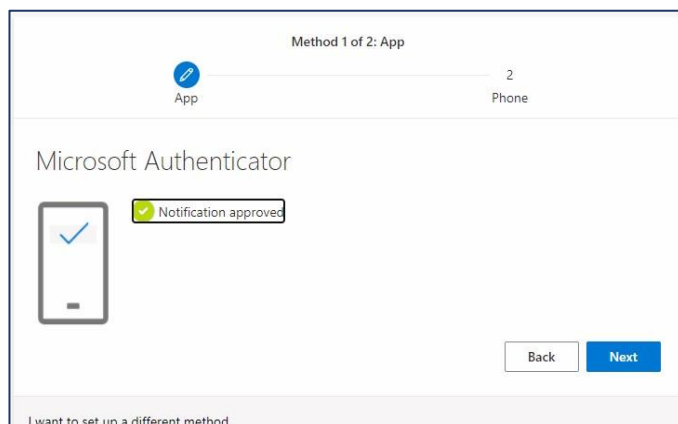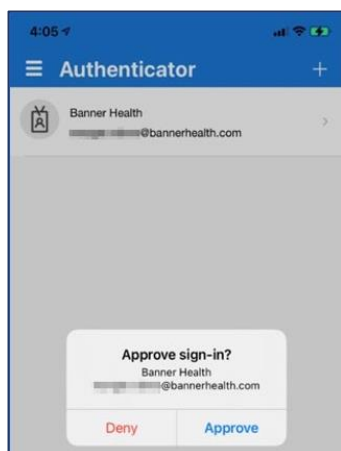
10. Click **Next** on your computer to continue the process and add a phone number as a **backup** option.

11. Once your phone number is entered and you click **Next**, you will be prompted to verify the phone number by entering the code you received on your mobile device.
12. Enter the code.

14. Click **Next**.

15. When you see the Success! Screen, Click **Done**.

16. Update Your Password, click **Sign In** when finished
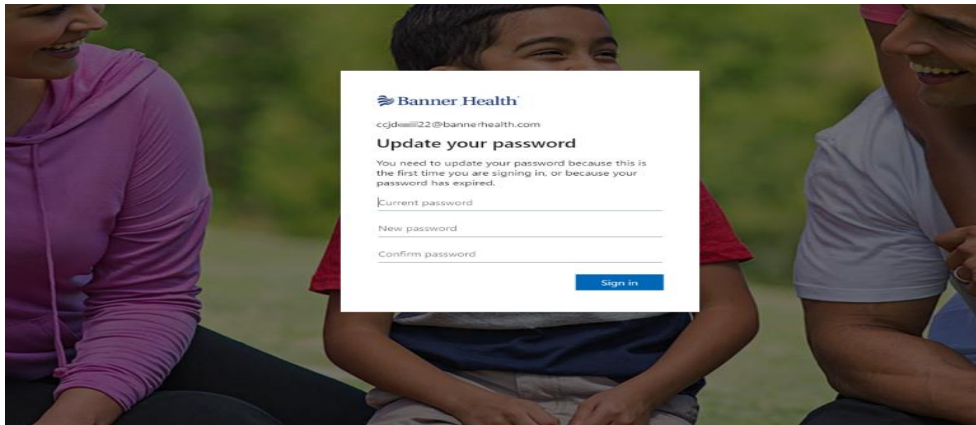
Note: The password you created will be the password used to access the Clinical Connectivity portal

HOW TO LOG INTO BANNER PORTAL
HTTPS://PORTAL.BANNERHEALTH.COM

1. Open your web browser and type https://portal.bannerhealth.com in the address bar. The BHS App Portal login screen displays. Note: Mark this page as a favorite for easier access by adding as a "Favorite" in your web browser.
2. There will be 3 fields of information to enter.
   1) Username
   2) Password
   3) Microsoft Verification Code (6-digit passcode)

3. Enter your network credentials under **User name** and **Password**. Click Log On.
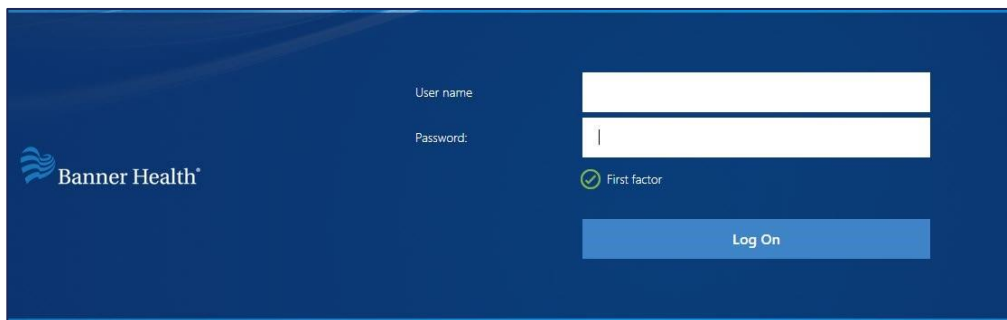
4. Open Microsoft Authenticator on your mobile device. Click **Continue** on your computer. A passcode will be generated on your phone app. This is your "Microsoft verification code." Note: The passcode can only be used one time. If you enter the wrong passcode, click **Generate Passcode** to create a new code.
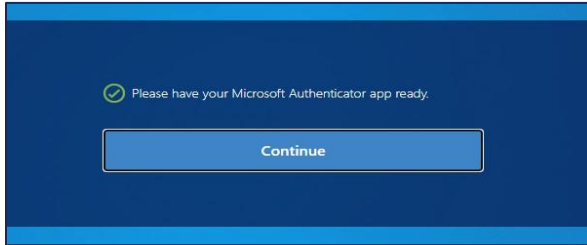
5. Enter the Microsoft verification code in the second Password field. Click **Submit**.
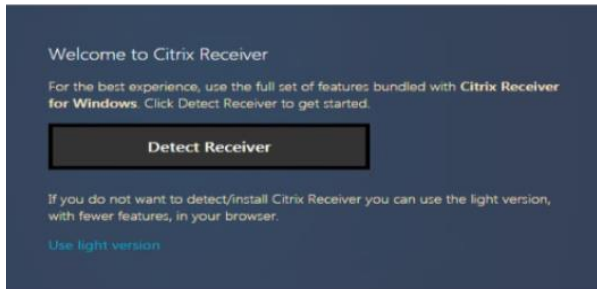
CITRIX APPLICATIONS DOWNLOAD & INSTALLATION

*Citrix application requires Citrix Receiver software installation. If you do not have administrative rights on your computer, please contact your practice admin or IT resource.
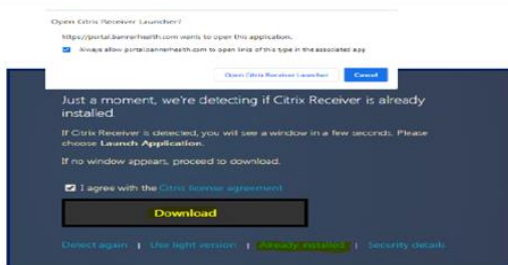
Step One

CITRIX RECEIVER DOWNLOAD
Download Citrix

1. Click Detect Receiver

2. Click "Always allow portal.bannerhealth.com to open" Click "Open Citrix Receiver Launcher".
Click I agree with the Citrix License Agreement, then click Download

3. File Download Will Appear, Click Run

4. Security Warning Will Be Presented, Click Run. This Will Launch the Installation
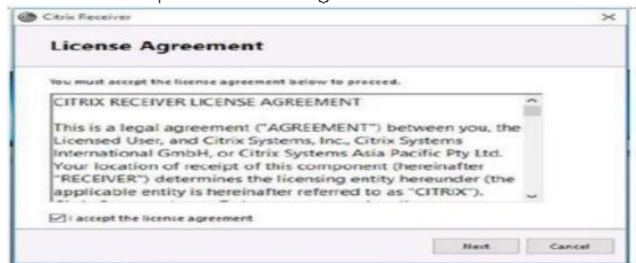

Step Two

CITRIX RECEIVER INSTALLATION
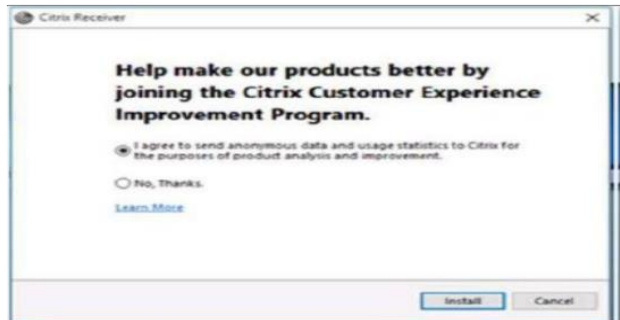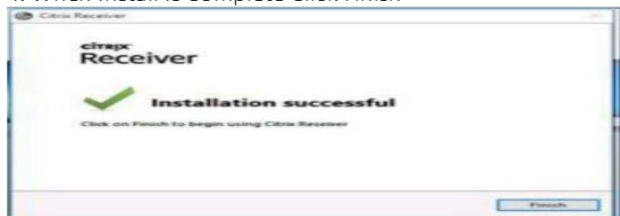### Install Citrix

1. Click Start

2. Click "I Accept the License Agreement" And Click Next

3. Click Install

4. When Install Is Complete Click Finish

ADDITIONAL INFORMATION

Azure MFA (Microsoft Authenticator) Phone Call Back Enrollment

These instructions will guide you through setting up the authenticator call back from your office desk or mobile phone option (**no software or smart phone required**) and enrolling in Azure Multifactor Authentication (MFA). For help with the Azure MFA enrollment process please contact the Banner Service Desk at **602-747-4444**.

1. Go to https://mysignins.microsoft.com/security-info on your computer.


2. Sign in using your @bannerhealth.com account and password. Your @bannerhealth.com account name is required for this process. **This is not a Banner email address**.
   Note: Sign in using your Clinical Connectivity portal username and adding @bannerhealth.com to the end of it. Example: ccTUser@bannerhealth.com. The password will be the same password as for your Clinical Connectivity portal login.

3. You will be prompted for more information, click Next.
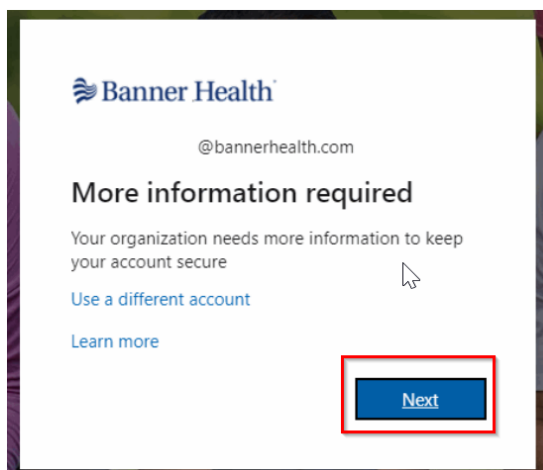
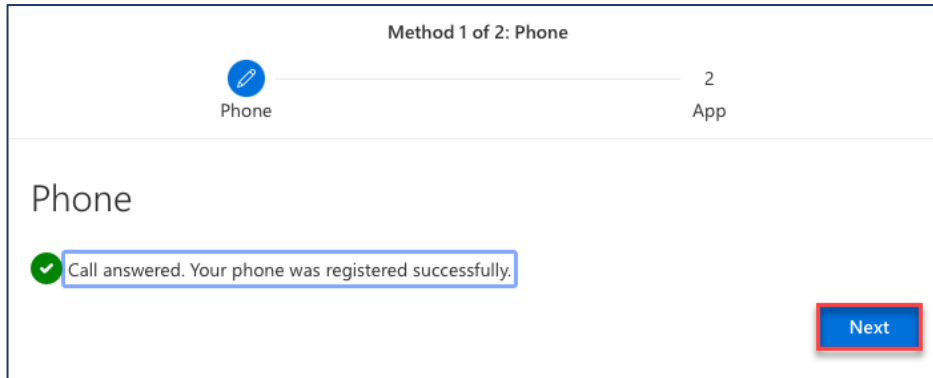4. Click **"I want to setup a different method**"
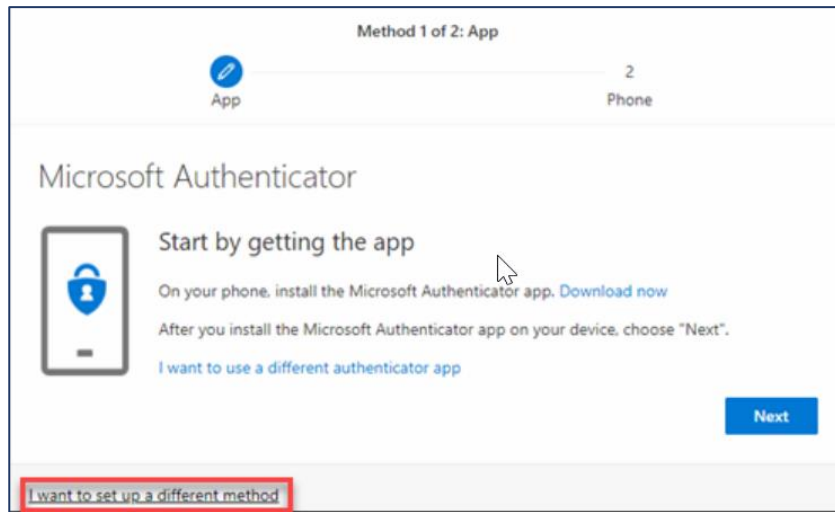
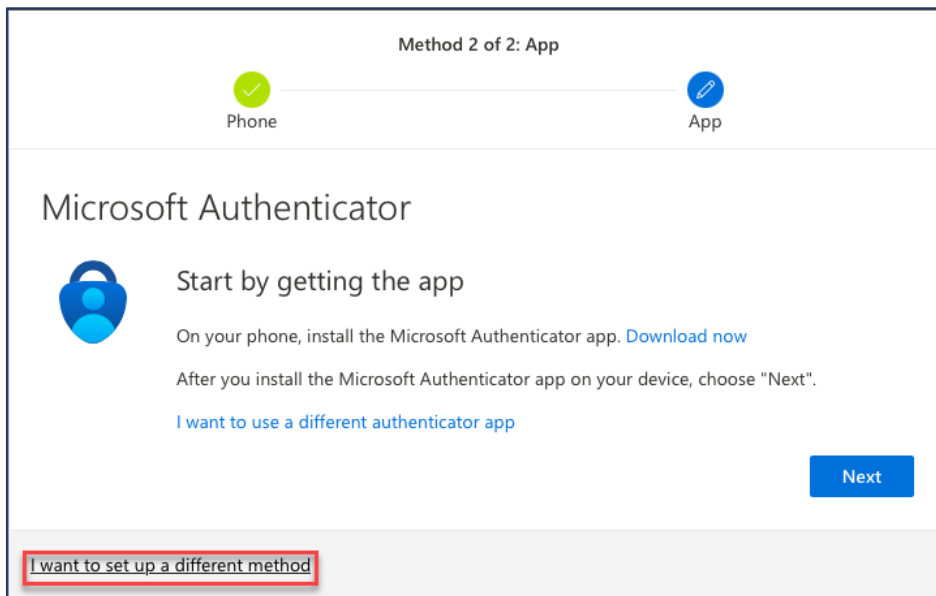5. Choose Phone in the drop-down list and click **Confirm**.
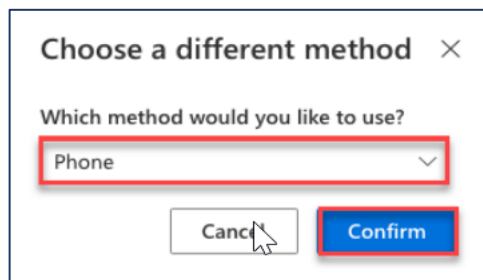
6. Enter your office desk or mobile phone number and select Call me. Note: Phones requiring an extension or international number dialing cannot be used for callback at this time.

7. Click **Next** to initiate the validation call and enter the phone number when prompted.
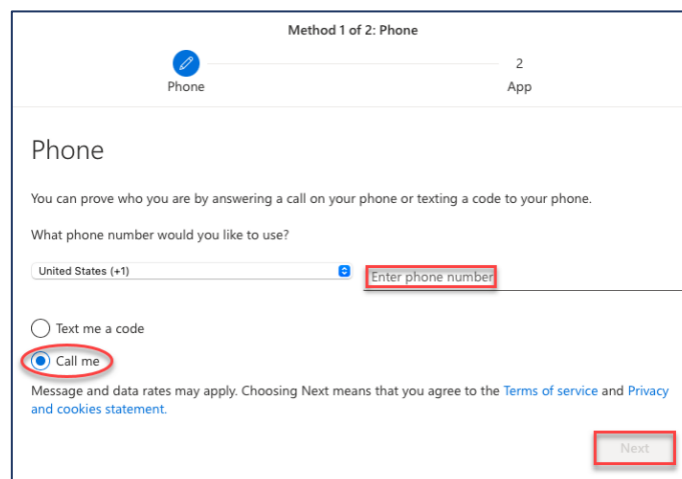
8. Once the call is verified, click Next to setup a backup method using your email address
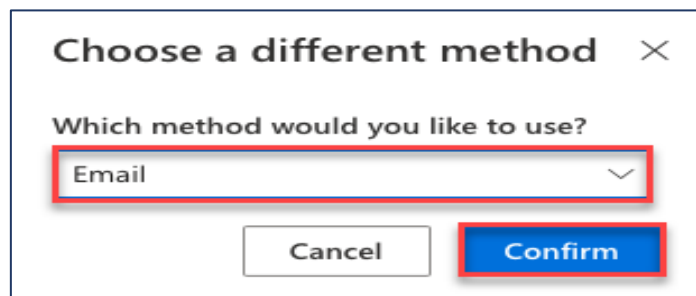

9. Click "**I want to setup a different method.**"

10. Select **Email** in the drop-down list and click **Confirm**.
Important: Email can only be used as a backup method to change authenticator settings (such as adding and removing authenticator types at https://mysignins.microsoft.com/security-info). Email cannot be used as an alternative MFA method.

11. Enter your email address in the **Email** field and click **Next** to have a 6-digit verification code sent to that email.

12. You will receive an email from "Microsoft on behalf of Banner Health." You may need to check your 'Junk' email folder if this is the first time you've received an email from Microsoft. Mark this type of email as 'Safe' to prevent login delays.
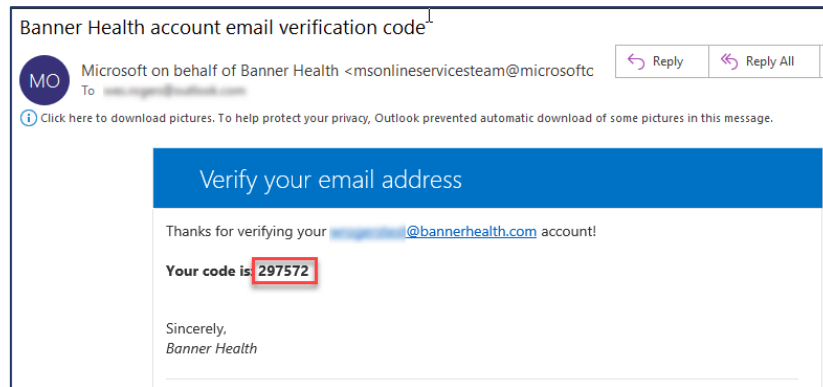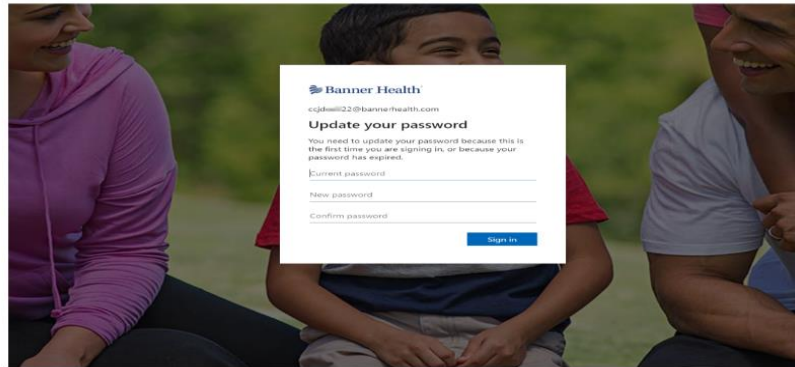

13. Enter the 6-digit code into the confirmation window and click Next.
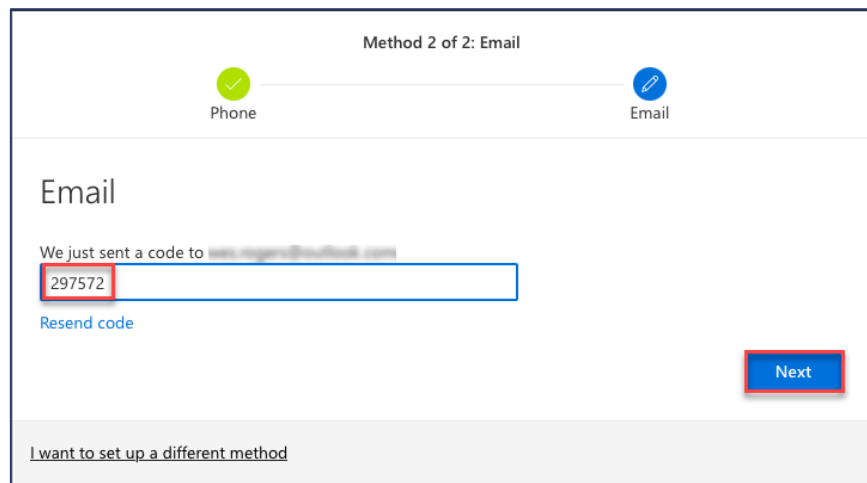
14. You will now see both authenticator methods setup, click **Done** to finish.
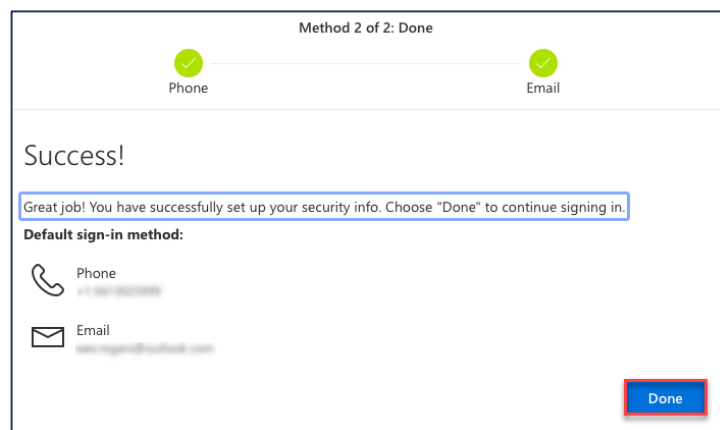
15. Update Your Password, click **Sign In** when finished

Note: The password you created will be the password used to access the Clinical Connectivity portal

16. Note: When you log in, you will receive a call back to your office desk or mobile phone. You will need to answer the call and press **#** at the prompt to verify your access.

Add Method to Existing Enrollment

If you already have the Microsoft Authenticator app downloaded on your mobile device and have a registered Banner account that you can access the Security Info with:
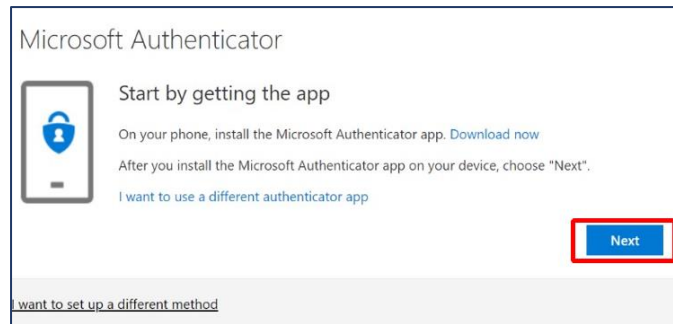
1. Go to https://mysignins.microsoft.com/security-info .
2. Sign in using your @bannerhealth.com account and password.
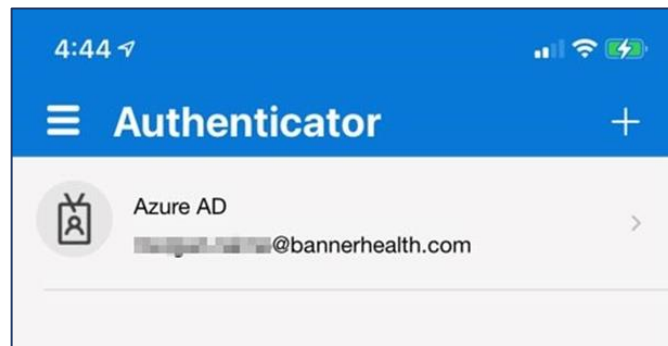3. Select **+ Add method**.

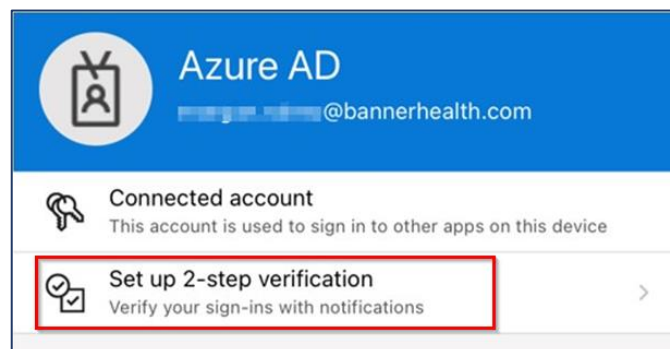4. Select **Authenticator App** from the drop-down menu
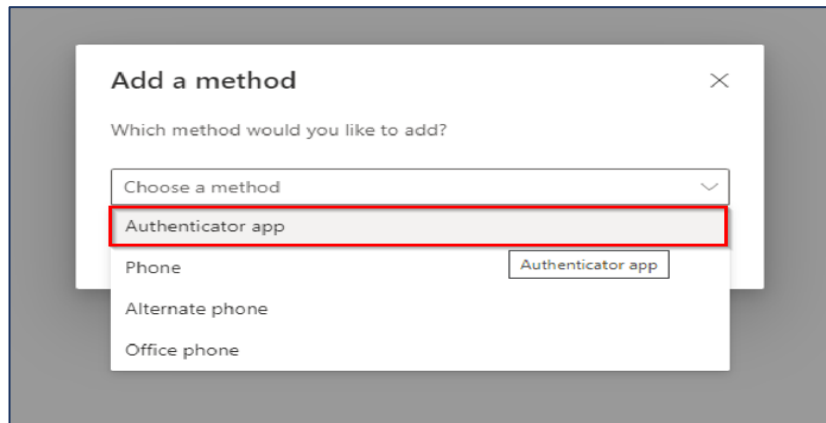
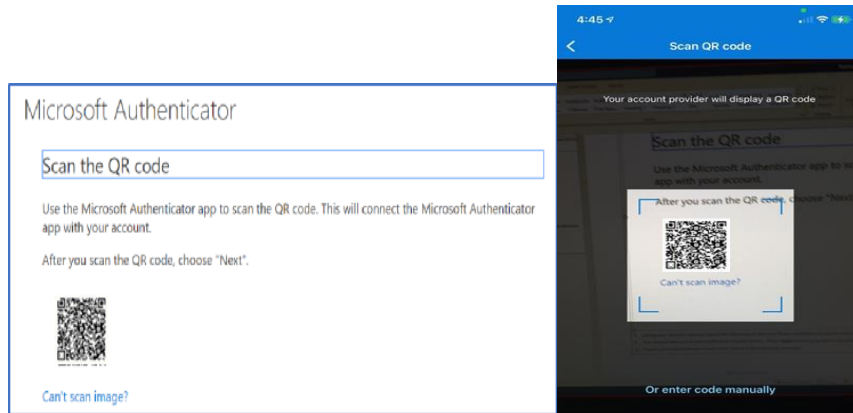5. Press **Next** on your computer screen.

6. Open the Microsoft Authenticator app.
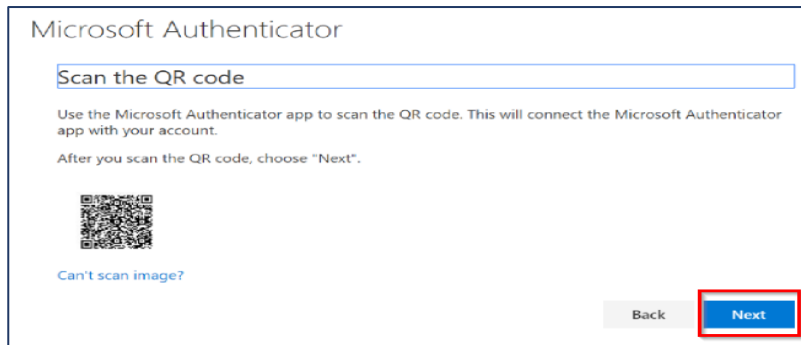7. Select your registered Banner account that ends in **@bannerhealth.com**

8. Select **Set up 2-step verification**

9. On your computer screen you will see the QR code unique to your registration.
10. Using your device's camera, place the QR image in the view finder to allow the app to scan the code.

11. After you scan the QR code, click **Next** on your computer.

12. A test notification will be sent to your mobile device. Press **Approve** on your device to acknowledge the authentication test request.
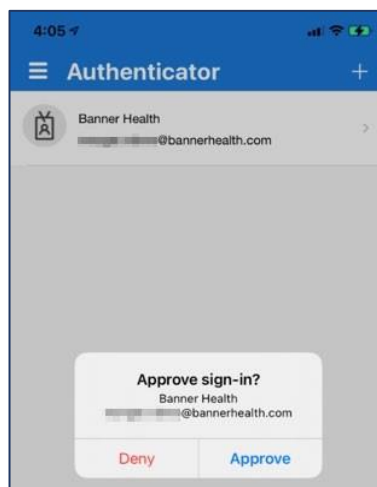
13. Click **Next** on your computer screen to complete the registration process.
14. The new Authenticator method has been added and you can close the app.