FAQ: Clinical Connectivity Access with Azure MFA

- **How do I know what my @Bannerhealth.com account name is?**
  - o Sign into the Clinical Connectivity portal the way you normally would. Then click on the WhoAmI icon.
 1. Sign into the portal

  2. Authenticate with YubiKey
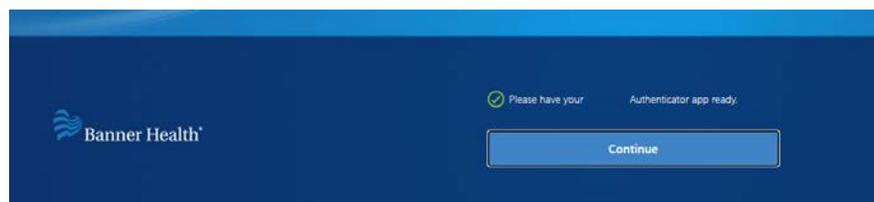
  3. On the Clinical Connectivity page, find the icon for WhoAMI.
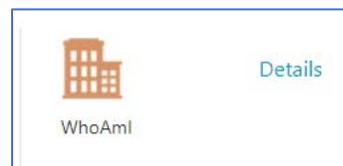
  4. Click on the Details link.
 5. Click on the Open button.

 6. Your @Bannerhealth.com account name will display.

- **What should I do if my cell phone is unavailable for MFA authentication on Clinical Connectivity?**
  - You can switch methods using MySignins on your desktop computer following the instructions below. If you're unable to access the MySignins page or having issues, call the Service Desk (602-747-4444) and ask them to switch your method to your backup.
  1. On your desktop computer, go to: https://mysignins.microsoft.com/security-info.
  2. The MFA prompt will pop up on the screen. Click the I can't use my Authenticator app right now link.
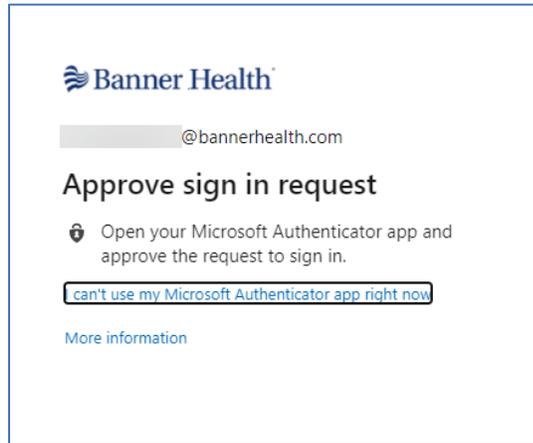
  3. Choose the alternate verification method from the list shown on Verify your identity.
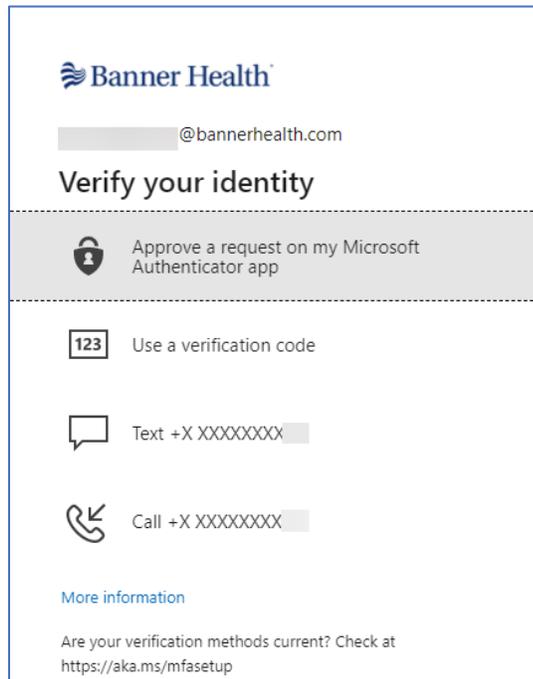
4. Approve the sign in request via whatever alternate method you selected.
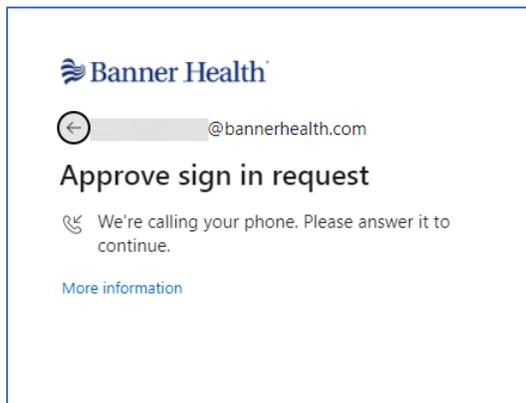
5. My Sign-Ins page will show the methods you have already set up.
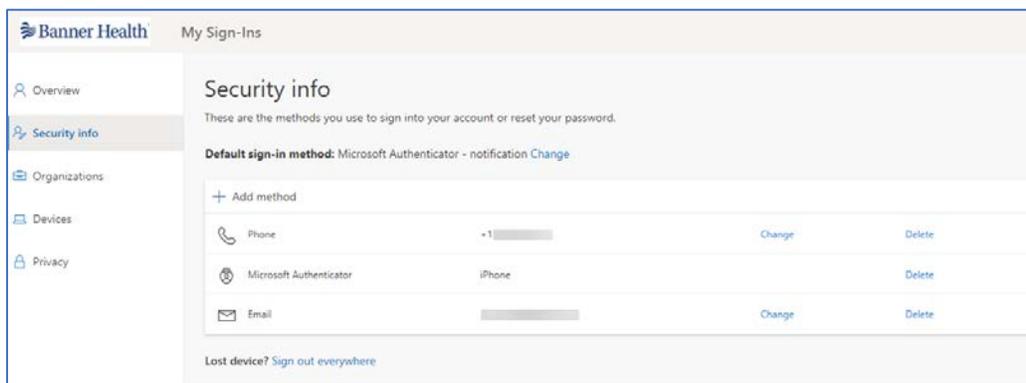
6. Click the blue Change link next to Default sign-in method.
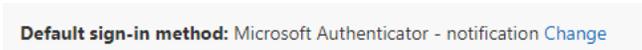
7. Select the method you want to use now from the dropdown list of your available methods. This will become your primary method unless or until you change it back. *Note: This requires that you have previously established more than one authentication method.*
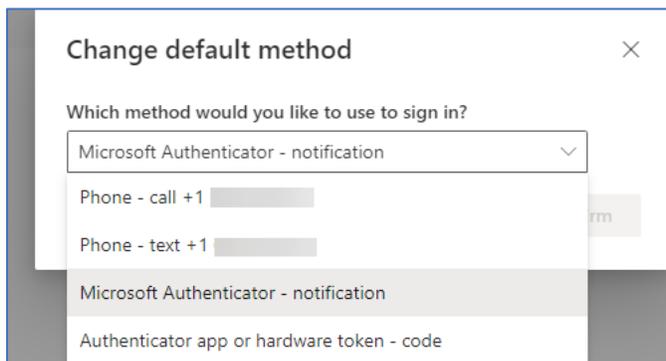
8. The selected method shows in a pop-up box. Click Confirm.
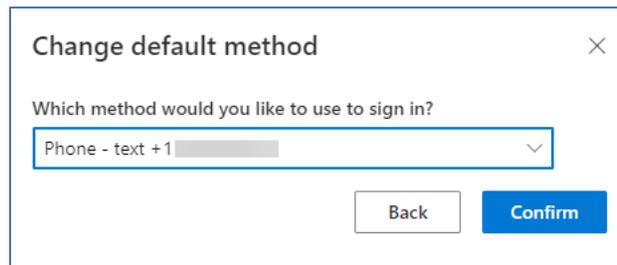
9. Exit out of My Sign-ins page.
10. Go back to the Citrix portal for Clinical Connectivity and sign in. You'll be asked to authenticate using your new default method.

- **Why do I need multiple authentication methods?**
  - Azure requires an alternative authentication method. It's also a good practice to have a backup in case your primary method is unavailable, for example when your cell phone has a dead battery.
- **Can I use my email as an authentication method?**
  - 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.
- **Dialing an extension is required to reach my phone line. How do I put the extension information into the phone number field for phone call back?**
  - The phone call back authentication method can't be used for phones with an extension or international number. You must have a number that can be directly dialed from outside your office.
- **Can I use the same call back phone number for more than one user in my office/location?**
  - No, this is not allowed. The intention of Azure MFA is to prove you are who you say you are by providing a unique second factor to authenticate you to Banner systems.
- **Can I access Azure MFA or Banner systems from outside the United States?**
  - No, this is not allowed as stated in the Data Access Agreement your entity signed with Banner.
  - Access to Banner systems is only allowed within the 50 United States or its territories.
- **Can I utilize any type of robotic process or other automation tools to accept the Azure MFA authentication on my behalf?**
  - No, automation of the Azure MFA authenticator is contrary to the principle of prove you are who you say you are, by allowing a "system or process" to accept that authentication request. By utilizing these tools you are "sharing" your login details which the Data Access Agreement prohibits.