Microsoft MFA FAQ

What is Multifactor Authentication or MFA?

Multifactor authentication is a way to use a secondary means of identification, in addition to a network password, to confirm the identity of the person attempting to log into the Marshfield Clinic Health System computer network. To complete the login after entering the password, it is required to have access to a secondary device to acknowledge and approve the sign-in.

Who needs to enroll in MFA?

MFA is required for users that sign into any mobile device such as a laptop, convertible, or MCHS tower that connects to the Health System's network using Netmotion Mobility while on-campus or remote.

What will happen after I set up MFA?

If you are required to use MFA, you will be prompted to use MFA upon initial startup or restart of your device, or upon login to an MFA enabled device while working remotely or at a Marshfield Campus site. Devices that never leave the campus, like those in exam rooms, or on clinical floors, may not prompt for MFA.

You will also be prompted if you manually disconnect and reconnect NetMotion Mobility. If you use the app notification method, a pop-up notification will appear on your smartphone or tablet device (iPad, Samsung Galaxy Tab, etc.) to approve the sign in. You will generally have to re-enter your phone unlock password, or provide TouchID/FaceID to further prove it is you after you click "Approve" in the Microsoft Authenticator application.

Why do I have to use multi-factor authentication when signing into Netmotion on my Marshfield Clinic Health System mobile device?

It is required by our cybersecurity insurance. Most breaches related to remote access into corporate networks are mitigated by using MFA to add another level of security and verify the user’s identity when signing into the system. Passwords are simply not security enough by themselves. Passwords can be broken and or phished by bad actors who use various convincing methods to trick individuals into signing into sites that appear to be legitimate. By having MFA in place, even if someone with bad intentions has the password, they will not have the secondary sign-in method, like the user’s smartphone or landline phone. To complete the login after entering the password, it is required to have access to a secondary device to acknowledge and approve the sign-in.

How often and when will MFA occur?

After rebooting, after logging off Windows, or if you manually disconnect and then reconnect Netmotion. “Screen lock/unlock” will generally not cause an MFA prompt, nor will sleep/wake.

Significant or long-lived interruptions in network connectivity may require another MFA prompt when the cause of the connection issue finally resolves.

What if I forget or lose my phone or MFA Device? How can I sign in to my MCHS device?
Please contact the MCHS Help Desk directly at 715-389-3456 for assistance.

Can I use a phone or tablet device which does not have cell service?
Maybe. The device must be able to connect to wireless networks, and the operating system of the device must support downloading and running the current version of Microsoft Authenticator. Also, you must keep this device near you wherever you take your MCHS device.

Can I use an *older* phone or tablet device?
Maybe. It all depends on whether that device can connect to wireless networks wherever you are, and the operating system must be able to download and run the current version of Microsoft Authenticator. You must keep this device near you wherever you take your MCHS device.

How often do I need to set up MFA, once or on every device I use?
Setting up MFA once covers all the MCHS devices you use.

Will installing the Microsoft Authenticator App allow Microsoft to access the data on my phone, or will it give Microsoft or MCHS the ability to access my device?
The Microsoft Authenticator app does not give anyone the ability to access your device or the data on it; all we see is the model of your phone, and your phone number, if you provide it. It also allows us the ability to detect the country you are in so that in the future there are options for tighter control on attempts to access MCHS networks from certain countries.

When you install the application, it may prompt you to provide permission for the app to know your location for the reasons described above. It does request access to the camera for scanning QR codes to set up new connections. It also requests the ability to send you notifications so that you can get a pop-up asking you whether to approve the current login attempt.

Do I have any other options besides the Microsoft Authenticator app?
Absolutely! The other acceptable alternative is to provide a phone number Microsoft can use to call you with an automated message when you sign in to your MCHS device. However, please be sure to:

- Use a phone number that you can access wherever you are when signing in. The easiest option is generally to use a mobile device that can travel with you, but a "landline" will also work if you only work from one location and never go other places.

For example, if you configure your home phone for MFA calls and travel to an MCHS location, you may not be able to sign into your device without assistance from the MCHS Help Desk. Likewise, if you use an office desk phone and are at home trying to sign into your MCHS device, the phone call will go to your work phone.

- Only use a phone number that is your personally assigned phone number.
- Do not choose "Text Me," as it is not supported, and you will not be able to sign in.
- Use a phone number that's associated with a physical phone. If you use a soft-phone on your MCHS device (such as Cisco Jabber or IP Communicator), you **will not be able to receive the phone call** to sign in because you have to be already signed into your desktop to use those applications. Therefore, do NOT use an office phone number if it's used in conjunction with a soft-phone application on your MCHS device.

I am getting prompted by Microsoft Authenticator to Approve a connection or I'm getting a phone call to approve a connection into Marshfield Clinic, but I'm not signing in right now. What should I do?

DO NOT APPROVE the connection in the app or on the phone call. Click **Deny** within Microsoft Authenticator or simply hang up the phone without pressing the pound key if you chose **Voice phone call** as your verification method.

I keep getting prompted for approving sign-ins and I'm definitely not signing in right now. Wouldn't it be easier to just click approve so I can stop being bothered?

NO! Do not approve any connections if you are not signing in at this time. In rare instances, it could be an error, but most likely it's because someone else is attempting to sign-in as you. Do not simply approve the connection to stop being pestered, and report this immediately to the Helpline.

Self-Service HelpDesk

Help is available through My Solution Center, available from the intranet.

HelpLine Staff

Help is available through HelpLine, 715-389-3456 or extension 9-3456.