University of Vermont
Larner College of Medicine

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is required to access various tech resources for the Larner College of Medicine.

Contents

Introduction to Multi-factor Authentication

Multi-factor authentication (MFA) is required when connecting to the LCOM Remote Gateway, VPN, and may be required to connect to other LCOM resources while traveling. The use of MFA protects the information within our environment, pairing typical credentials like email and password – which can be phished – with an additional verification method that is difficult to spoof (usually via an individual's phone).

Proceed to Registering Your Authentication Methods if you don't have a mobile device, or if you already have Microsoft Authenticator downloaded.

If you have a new phone number, proceed to Configuring a New Phone Number or Device.

Microsoft Authenticator

Both the Larner College of Medicine and the UVM Health Network use Microsoft Authenticator, a mobile device app, as part of the authentication process. Once credentials are entered, the system will prompt the user to approve (or deny) the sign-in on the app.

Downloading Authenticator

Ensure your mobile device is connected to Wifi or has a strong cell signal before proceeding.

STEP 1: Open the App Store (Apple devices) or the Play Store (Android devices) and search for "Microsoft Authenticator".

STEP 2: Verify you have found the correct app. The icon should match this:

STEP 3: Download the app. You may be asked for your Apple ID or Play Store password. If you have forgotten it, follow the link below for assistance in recovering it:

- Apple App Store Password Recovery
- Android Play Store Password Recovery

STEP 4: Once the application is downloaded, proceed to Signing In.

Registering Your Authentication Methods

COMTS recommends that you set up two methods of authentication, ensuring you can still easily access your account if you get a new device or change phone numbers.

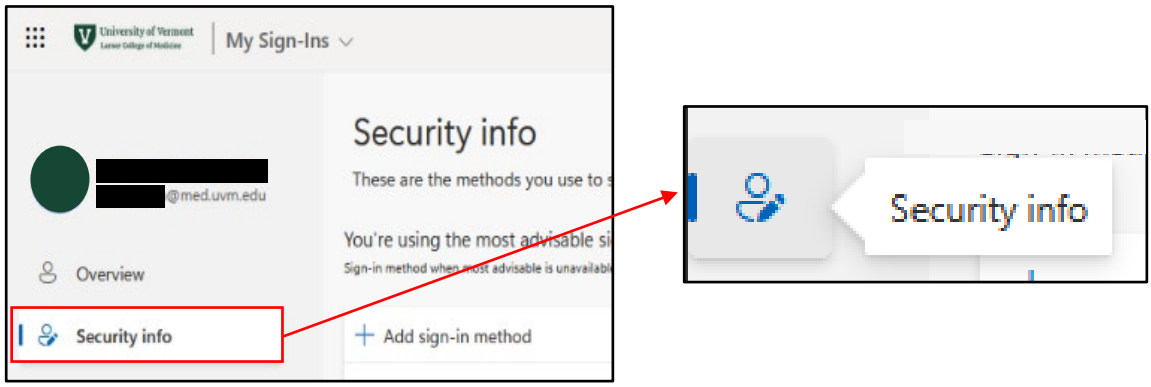
Signing In

STEP 1: Open a web browser on your computer and navigate to https://mysignins.microsoft.com/

STEP 2: Sign in with your LCOM email (*firstname.lastname@med.uvm.edu* or *comid@med.uvm.edu*) and password.

If you are prompted to approve your sign-in request and are unable to do so, contact the COMTS Help Desk at 802-488-5553

STEP 3: Click "Security info" on the left side of the page. Please note that you may only see icons without labels, based on the size of your browser window; hover your cursor over the icons to see their labels:



Registering Your Phone Number

STEP 1: Click "+ Add sign-in method" and choose "Phone".
STEP 2: Enter your phone number then click "Next". The number you choose should be for a phone you usually have access to, such as your cell or work phone.
STEP 3: Answer your phone and follow the instructions.
STEP 4: Click "Done" on your computer screen.

If you do not have a mobile device on which to install Authenticator, you must complete these steps again using another phone number you can access during work hours. If you are going to install Authenticator, you can proceed to the next step.

Registering Microsoft Authenticator

STEP 1: Click "+ Add sign-in method" and choose "Microsoft Authenticator".
STEP 2: Click "Next" until a QR code appears.
STEP 3: On your mobile device, open the Microsoft Authenticator app. Click the **. . .** or **+** in the upper-right corner of the screen and select "Work or school account", then click "Sign-in" and use your LCOM email.
STEP 4: If prompted, allow the app to use your camera and send notifications.
STEP 5: With your device, scan the QR code that is displayed on your computer. Click "Next" on the computer.
STEP 6: Approve the notification that will be sent to your Authenticator app to complete the set-up.

Setting Your Default Method

STEP 1: When you have set-up multiple authentication methods, you will see the option to "Set default sign-in method" which can be changed at any point in the future.

STEP 2: Click "Set default sign-in method" and use the pulldown menu for your selection:

- **App based authentication – notification** will prompt you to interact with the Authenticator app any time verification is required.
- **Phone – call** and **Phone – text** will require that you have access (and cell service, if mobile) to the number you select. If you work in a building with spotty service, using a landline or your Cisco Jabber line will be the more reliable options.

STEP 3: If your default method is not working at any point, Microsoft usually provides the option to select another method when you are signing in. See **STEP 3** of Configuring a New Phone Number or Device for further information.

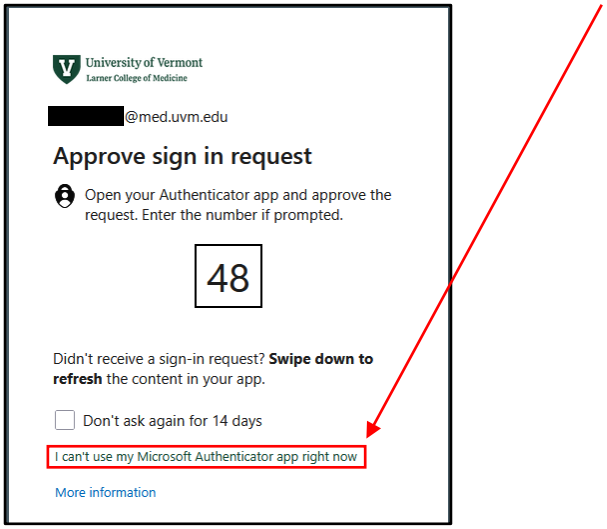
Configuring a New Phone Number or Device

If you change mobile devices or your phone number, you will need to remove the old information from your account and add the new device or number.

STEP 1: Open a web browser on your computer and navigate to https://mysignins.microsoft.com/

STEP 2: Sign in with your LCOM email (*firstname.lastname@med.uvm.edu* or *comid@med.uvm.edu*) and password.

STEP 3: When prompted to authenticate your sign in, look for the link near the bottom of the window with wording such as "I can't use my Microsoft Authenticator app right now"



STEP 4: Click the link and select an alternative sign-in method.

If there is no alternative method available to you,
contact the COMTS Help Desk by calling 802-488-5553

STEP 5: Once signed in, click "Security Info" on the left-hand side. Reference **STEP 3** of Signing In above for screenshots if you don't see that option.

STEP 6: In the list of authentication methods, find your old device or phone number. Click "Delete" and confirm.

STEP 7: Add your new device or phone number using the instructions for Registering Your Authentication Methods above.