Multi-factor Authentication

These instructions are intended for students, employees, and affiliates of the Larner College of Medicine at UVM. You must complete the following before connecting to the LCOM VPN. If you require assistance while completing these tasks, please contact COMTS Support by calling:

(802)488-5553

Or by submitting a Footprints request:

https://comis.med.uvm.edu/footprints/default.aspx

The College of Medicine uses Microsoft Multi-factor Authentication to protect your information. This is the same product used by our affiliate organization the UVM Medical Center and Health Network.

Make sure you are connected to WiFi (HSID or UVM) or have a strong cell signal before proceeding with the following steps.

Step 1: Install Microsoft Authenticator

If you have already completed the setup of multi-factor authentication with UVMMC / HN, you do not need to complete this step. Please continue to 'Step 2: Register your authentication method'.

Download **Microsoft Authenticator** on your mobile device from the App Store (Apple devices) or the Play Store (Android devices). You may be asked for your Apple ID or Play Store password. If you have forgotten it, follow the link below to attempt to recover it.

Apple App Store Password Recovery

Android Play Store Password Recovery

The University of Vermont
LARNER COLLEGE OF MEDICINE

Step 2: Register your authentication method

The College recommends that you set up two methods of authentication. Your primary authentication method will be the Microsoft Authenticator. If you don't have access to this app, we recommend using a SMS text message, explained in step **5** below.

1. Browse to **https://mysignins.microsoft.com/**.

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

3. Click **Security Info** from the left side of the page.

NOTE: *If you are prompted to **approve** your sign in request at this point, and you are unable to do so, submit a Footprints request so we can clear your previously configured methods.*

4. Set up **first method** for authentication.

    a. click **+ Add method**.
    b. Choose **Authenticator App** and click **Next** a couple times.
    c. Launch the Microsoft Authenticator app from your mobile device.
    d. If you have not used the app before, you will be prompted to **Add an account**. Otherwise, click the three dots icon in the upper right, then click **Add an account**.
    e. Choose **Work or school account.**
    f. You will now be prompted to scan the displayed QR code. Scan the code displayed on your computer screen. Once completed, click **Next**.
    g. Microsoft will now send your mobile device an authentication request. Please complete this process to verify and activate your Microsoft Authenticator.

5. Set up **second method** for authentication.

    a. On the Computer, click **+ Add method** again.
    b. Choose **Phone**.
    c. Type in your mobile phone number.
    d. Microsoft will now send you an SMS message. Please complete this process to verify and activate your phone authentication.

NOTE: *Step 5 is critical. If you skip this step and then later replace your cell phone, you will lose access.*

You have now successfully completed multi-factor authentication setup with Microsoft Authenticator. You will use this method for access to various LCOM resources, including the LCOM Virtual Private Network (VPN).

For additional assistance, please contact the COMTS Service Center by submitting a Footprints request at https://comis.med.uvm.edu/footprints or calling us at (802)488-5553.