Remote Work Documentation

This page collects information useful for users working from a remote location. Please note that most services require the remote user to establish a VPN Connection to the university.

<table>
<thead>
<tr>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness</td>
</tr>
<tr>
<td>VPN Connection</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>UMHS File Storage Connections (Mapping a Drive)</td>
</tr>
<tr>
<td>Xythos</td>
</tr>
<tr>
<td>Medical School Software Licensing</td>
</tr>
<tr>
<td>Confluence</td>
</tr>
</tbody>
</table>

Security Awareness

In this digital era, we must be even more vigilant about how we store and protect the confidential information with which we are entrusted. Always be aware that workstations, laptops, tablets, phones, and other mobile devices could be used by others to access confidential information.

Important policies and guidelines to avoid a security breach are available at the following link:
http://www.safecomputing.umich.edu/

VPN Connection

Access to Michigan Medicine protected resources is limited to users who have a Michigan Medicine (Level-2) or an "active Michigan Medicine VPN account" and are enrolled in Duo Two-Factor Authentication.

You will be unable to connect to the VPN unless you have set up your Duo Two-Factor Authentication.

A VPN (Virtual Private Network) client provides a secure computing experience when accessing a University of Michigan (U-M) resource from a remote location. The VPN clients provided by the university allow authentication by all U-M students, faculty, and staff who have a valid U-M uniqname and UMICH (Level-1) password.

The Michigan Medicine network has its own VPN server that specifically controls access to Michigan Medicine protected resources. Access to these protected resources is not available to users with only UMICH (Level-1) accounts. Remote/offsite VPN access to the health system network is limited to users who also have either a Michigan Medicine (Level-2) account or an "active Michigan Medicine VPN account" and are enrolled in Duo Two-Factor Authentication.

A "Michigan Medicine VPN account" is not a Michigan Medicine (Level-2) account and does not give access to other health system resources such as Outlook Exchange, CoreImage workstations, and NAS file share systems.
The university VPN uses Level-1 credentials and Duo Two-Factor Authentication for authentication.

### VPN Topics

- Michigan Medicine VPN Client Information
  - Cisco AnyConnect Secure Mobility Client
  - Clientless VPN
- MLearning Access
- Other VPN Clients
  - VPN Access to CCMB Network
  - VPN Access to va.gov

A single VPN solution is available to non-CoreImage devices for Michigan Medicine staff: the Cisco AnyConnect Secure Mobility Client client. Faculty and staff are encouraged to use the AnyConnect client and Level-1 (Kerberos) credentials with Duo Two-Factor Authentication to access all health system internal resources when off-site.

This change currently applies only to non-CoreImage machines.

### Michigan Medicine VPN Client Information

The health system offers two different options for connecting from a remote location: the full Cisco AnyConnect client and the Clientless VPN (Level-1 Page). These options provide two different methods for accessing health system resources remotely, so individuals do NOT need to perform steps for both methods in order to connect.

The main difference between the two options is the Clientless VPN only provides access to a small subset of applications, while the AnyConnect VPN client provides full access to Michigan Medicine resources.

<table>
<thead>
<tr>
<th>Feature</th>
<th>AnyConnect VPN Client</th>
<th>Clientless VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-speed Internet Connectivity Required</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Duo Two-Factor Authentication Required</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Full access to Michigan Medicine network</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Mobile Device Compatible</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Citrix installation required for MiChart access</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Cisco AnyConnect Secure Mobility Client**

Only the Cisco AnyConnect client is approved and supported by HITS for use in conjunction with clinical applications and the delivery of patient care. The AnyConnect client allows the user to access all health system internal resources.

Michigan Medicine staff are strongly encouraged to use the Cisco AnyConnect Secure Mobility Client client with iOS devices (iPad, iPhone, iPod Touch).
Cisco AnyConnect Instructions

- Windows
- Macintosh
- Linux (old Linux)

Mobile Devices

- Android devices
- iOS devices
  (iPad, iPhone, iPod Touch)

Clientless VPN

The Cisco Clientless VPN is an online authentication mechanism to access a small subset of web-based clinical applications (though not including MLearning) and also provide access to some resources from the Macintosh platform.

https://vpn.med.umich.edu/level1

After authenticating with a uniqname and Level-1 (UMICH) password and Duo Two-Factor Authentication, a list of available applications will appear. Note that not all applications will function properly when accessed via this method. Some have additional special instructions for Mac access.

MLearning Access

- MLearning users can access the MLearning website without establishing a VPN connection using the following link:
  https://trainingportal.med.umich.edu

Other VPN Clients

VPN Access to CCMB Network

Those who need access to the CCMB Clusters or Network use a different VPN than the usual UMHS VPN. Click the above link for more information.

VPN Access to va.gov

Staff members working in conjunction with the Veterans Affairs hospital (the VA) are required to access the VA systems securely in order to modify patient data. In order to establish a secure connection, the staff members must use the government's official VPN Server at va.gov site using the Rescue VPN client.

Email
Topics

- Email - Account Setup Pages
  - Mail - Secure Connections (Mac Only)
  - Outlook - Secure Connections
- Thunderbird - Secure Connections
- Email and IT Considerations for U-M Retirees, Alumni, and Employees Leaving U-M
- Email Clients
  - Mail
  - Outlook
  - Outlook - Web App (OWA)
  - Thunderbird
- Email - Directory Server for Address Books
- Email Etiquette
- Email - ITS (Main Campus) Google Accounts
- Phishing Scams - Email Requests for Personal Information
- Spam

Quick Info

- Clients Recommendations
  (Windows, Mobile, and Macintosh)
- Web Access to Email

Account Setup Pages

- Mail (Exchange) - Mac only
- Mail (IMAP) - Mac only
- Outlook
- Thunderbird

Clients

Windows

Michigan Medicine Exchange users are strongly encouraged to use the Outlook client. The recommended email client for all other users is Mozilla Thunderbird.

HITS Supported clients

- Outlook 2016
- OWA

Mobile

Michigan Medicine Exchange users are strongly encouraged to use Airwatch to sync their mail to the native email client on the mobile device.

HITS Supported clients
Native Email (iOS, Samsung, LG, HTC, Sony)
AirWatch Inbox (iOS / Android) (For now)
AirWatch Boxer (iOS / Android) (Going Forward)
OWA

**Macintosh**

Michigan Medicine Exchange users are strongly encouraged to use the Outlook client. The recommended email client for all other users is Mail (the Mac email program). Users may also use Mozilla Thunderbird.

HITS Supported clients

- Outlook 2016
- OWA

**For those users on BYOD devices that don't have Outlook you can get outlook via Office 365 here:** [http://computershowcase.umich.edu/item.php?cat=70&item=000365&id=3504](http://computershowcase.umich.edu/item.php?cat=70&item=000365&id=3504)

**Email via Web access (URLs)**

Users of the Outlook email application are likely have an account on one of the Exchange servers; Outlook users located in the Health System will have an account on the UMHS Exchange server.

**OWA (Outlook Web App)** is Microsoft's web-based Outlook 2016 client. Used on and off-campus, this web application can be accessed at [email.med.umich.edu](mailto:email.med.umich.edu). It is essential to members of Michigan Medicine by providing email access anytime and anywhere. In order to access this website off-campus and off the UMHS network, you will need two-factor authentication. Be sure to [enroll in Duo](http://computershowcase.umich.edu/item.php?cat=70&item=000365&id=3504) if you have not, already.

<table>
<thead>
<tr>
<th>Account</th>
<th>Web Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS Google Mail</td>
<td><a href="http://mail.umich.edu">http://mail.umich.edu</a></td>
</tr>
<tr>
<td>ITS Exchange</td>
<td><a href="http://exchange.umich.edu">http://exchange.umich.edu</a></td>
</tr>
<tr>
<td>Michigan Medicine Exchange</td>
<td><a href="http://email.med.umich.edu">http://email.med.umich.edu</a></td>
</tr>
</tbody>
</table>

To determine which mail server is associated with a IMAP account, look in the account settings under Thunderbird (or whichever IMAP-based email client is used).

In Thunderbird, go under the **Tools** menu and select **Account Settings**. The server is listed as the second option down on the left. Generally, typing the text in the **Server Name** field into a web browser will load the correct web access page.

If anything else is listed, contact MSIS and get help reconfiguring the email client.

The mail server information can also be found in the **Email Forwarding Address** field in the UM Online Directory.

**UMHS File Storage Connections (Mapping a Drive)**

Unable to render (include) The included page could not be found.
Xythos

Xythos is a web-based file sharing system, allowing its users to share files, with people outside of Xythos via the Ticket system. Xythos also contains auditing and file versioning features. It is mainly used for sharing files with people who do not have access to the Medical School file servers or by users who have advanced auditing needs for controlling access to their data.

Xythos should **never** be used, even temporarily, for storing ePHI and Sensitive Regulated Data.

### Topics

- Xythos Access
- Xythos - Basic Usage
- Xythos via WebDAV
- Xythos - Working with Audit Logs

**Xythos Access**

A unit supervisor must request access to Xythos. Once an account is created, the user can log into the system using the login window in the left frame of the Xythos site. The unit supervisor can grant additional access to files and folders within the Xythos system.

The Xythos file system is normally accessed using a web browser, but Windows machines can also mount Xythos as a share point using WebDAV. The following link will direct the web browser to the authentication level of the Xythos system. Authentication requires a U-M uniqname and Level-1 password.

https://files.umms.med.umich.edu/xythoswfs/webui

---

**Medical School Software Licensing**

### Medical School Software Eligibility

Currently, eligibility for Medical School applications is determined by appointment, not affiliation. In order to download software, software users must be members of UMMS Faculty or Staff. Generally, students are **NOT eligible to download software**. ITS disabled the ability to look up an individual’s group memberships in MCommunity because of privacy concerns, but individuals can determine their own group memberships, which determine eligibility for Medical School applications, in the following manner:

1. In a browser window, go to the MCommunity page: [http://mcommunity.umich.edu](http://mcommunity.umich.edu)
2. Search for your uniqname and then select your name from the Search Results list.
3. While viewing your entry, click the **Groups** tab. A list of all group memberships will appear.
4. At least one of the following groups must appear in the list for the individual to be eligible for Medical School software.
   - UMMS Medical School Faculty
   - UMMS Medical School Staff
   - UMMS Post-Doctoral Fellows

**House Officers** can also qualify for Medical Software, but may need to contact [msishelp@umich.edu](mailto:msishelp@umich.edu) to obtain access to the download page.

In order to install Medical School software on a workstation, the requester must be an administrator of the machine. Machines assigned a **TermID** number (CoreImage workstations) are managed by MCIT and generally users will not have the ability to install software. MCIT has packages of some Medical School applications that can be pushed to Core machines; a list is available in the **MCIT Packages for Core Workstations** section at the bottom of this page.

Applications are only available to individual users!
Medical School Software Usage

The applications offered by the Medical School are **keyed** unless otherwise indicated. The KeyClient software, listed at the top of the software list, must be downloaded and installed on the computer in addition to any application software (unless otherwise noted). The KeyClient establishes a connection with the KeyServer when the application is launched. If a license is available, the KeyServer releases a license to the KeyClient and the application will proceed to load. Note that this procedure **requires** keyed applications to have a network connection in order to launch. Please visit the KeyServer page for troubleshooting information.

Additionally, only machines on the greater University of Michigan campus network will be allowed to launch the software. If the user needs to use the software from offsite, a VPN client will also need to be installed on the machine. Additional information about VPN client software is available on the VPN page.

Confluence

Confluence pages can be accessed using the following link: https://wiki.umms.med.umich.edu/