Computing Essentials for Michigan Medicine

**Introduction**

It's important to know your IT environment as effective members of Michigan Medicine. There are 3 essential basics that are necessary to understand to work effectively within your workplace IT environment. These basics are, **Accounts**, **Networks**, and **Security**

- **Accounts**: Level-1, Level-2
- **Networks**: MWireless, UMHS-8021x, VPN client.
- **Security**: AirWatch, Duo

Below are more detailed descriptions, and links to instructional pages for setup and configuration. The side bar has related topics, additional information, and a table of how this all fits together.

### Topics

- Introduction
- Wireless Networks
- Level-1 Password
- Level-2 Password
- DUO (Two Factor Authentication)
- Airwatch
- VPN
- Outlook Webmail
- Cloud Storage Options
- Quick Facts

### Wireless Networks

**MWireless** is available throughout the entire campus and you can connect to it with your Level-1 credentials. (Also sometimes named, “MWireless-UMHS”)

Read More...

**UMHS-8021x** is our Health system specific network and **AirWatch** is required in order to access it. The 8021x network grants access to our internal resources like vplaces.med.umich.edu, shared drives and the networked printers. All Core Image systems will have access to UMHS-8021x or MFleet which have the same access permissions for these networks.

Read More...

### Level-1 Password

Your Level-1 account is the standard-wide login information all University members have and use throughout the University. Other terms we would use to describe this would be “Kerberos” and/or “Umich”. The Level-1 account will allow you to use resources like Canvas, the UMMS Computer Lab Workstations (such as those located on the 5th and 6th floor of THSL) and Wolverine Access, our employee information page. These credentials will also allow you to login to the MWireless Wi-Fi, which is available for all students, faculty, and staff members.

Read More...
Level-2 Password

While the Level-1 Umich account is Universal, the Level-2 Michigan Medicine account is only provided to members that will need access to our medical resources. These resources include: Outlook for medical email, Our Michigan Medicine Core workstations (located in areas around the hospitals), MiChart access, and various websites that are not accessible outside of the Michigan Medicine Network (UMHS Domain). To learn more about requesting, to setup, or to reset and change your Level-2 account, click the link below.

Read More...

DUO (Two Factor Authentication)

Duo is the two-factor authentication practice we use as members of Michigan Medicine. It’s the extra layer of security in addition to our levels 1, and 2 passwords. Only required when using external Wi-Fi connections, once you are off the network (Not on campus) and connected to a home or public Wi-Fi like in a hotel or coffee shop, Duo will activate. This helps secure the clinical and medical resources we have available to us and when we need them while we are off campus or the hospitals.

Whether you need to check your OWA emails after hours or want to connect to the virtual private network (VPN) to access important documents. Duo is the application we use to get us working while we are away. Duo can be activated in two ways. The most popular way is by phone application and downloading from either Apple store or Google play store. Another way is by purchasing a hard token from the Computer Showcase. To learn more about DUO, and using DUO with EPCS.

Read More...

Airwatch

The AirWatch Mobile Device Management (MDM) system provides the required encryption and security protocols for mobile device customers to access internal Michigan Medicine resources. Other features include:

- Allows access to Michigan Medicine exclusive networks such as the 8021x wifi
- Automatic configuration for Outlook/Exchange emails and calendars
- A user Self-service Portal to self-manage devices in cases of theft, loss, or a forgotten password
- Security profile to ensure your mobile device conforms to Michigan Medicine’s security policies (see the Smartphone/Mobile Device Security Policy Settings and Restrictions section for more information)
- The ability to publish clinical and other business applications to enrolled devices
- Access to MiChart mobile apps, Haiku/Canto, by enrolling in the MiChart profile.

If you would like to setup Airwatch on your mobile device please refer to the enrollment instructions page which contains detailed PDF instructions for all devices.

VPN

Many Michigan Medicine resources, such as shared network drives and internal websites, are not available to the general public. To access these resources while off-campus, and outside of our network, Michigan Medicine members will need to use the Cisco AnyConnect Secure Mobility Client. This Virtual Private Network (VPN) application will establish an encrypted “tunnel” that allows members to securely connect to internal resources as if they were on campus. (It is possible to access some internal resources, such as MiChart, using Citrix Receiver with its separate, built-in VPN client, but this access is more limited in scope.)
The Cisco VPN software can be downloaded from the website https://vpn.med.umich.edu/level1. Logging in to this site requires that the member sign in using their Level-1 password and two-factor authentication (DUO). Once the member is authenticated, a webpage will open with downloads and instructions on how to proceed. When Cisco AnyConnect Secure Mobility Client is installed and launched, it will prompt for a server address. The server address is vpn.med.umich.edu. When it prompts for user name and password, the user name is the member's uniqname and Level-1 password. Two-factor authentication through DUO will also be required. The Level-2 password is not required to sign in, but the VPN will fail to connect if the member does not also have an active Level-2 account. For more information about the Cisco AnyConnect Secure Mobility Client, click here. For more general info about VPN use by members of Michigan Medicine,

Read More...

Outlook Webmail

Error rendering macro 'excerpt-include' : User 'null' does not have permission to view the page 'Outlook Web App (OWA)'.

Read More...

Cloud Storage Options

**Shared Drives**. Some departments also make use of shared departmental drives called cores or maize storage. These are purchased by departments and their access is granted by the owners of the various drives. In order to access these drives you must be on our secure ethernet, UMHS-8021x/MFleet wireless network or connected to the VPN. When connecting to the drive you will have to type your uniqname as UMHS/Uniqname and the password will be your Level-2 password. For more details on how to map to these shared drives see this Knowledge Base Article. If you would like to request storage space see this article...

**MiShare** is a HIPAA compliant data transfer service used to send information to external collaborators in a secure manner. The service is not intended for storage, but simply for data transfer, as a file is purged after four days. It works similar to sending an email with an attachment, but unlike sending an attachment via normal email, MiShare has the attachment stored on our secure MiShare servers.

Read More...

**U-M Box** (sometimes called, M+Box) can be used to store information and sync it across devices as well as edit them online. Everyone with either an active Level-1 or Level-2 account can access to M+Box. There are special parameters involving using M+Box with sensitive data such as patient health information so please refer to the information below:

Read More...
U-M Box HIPAA Compliance Policies

As of September 2014, U-M Box has been approved for the storage of Protected Health Information (PHI) and electronic Protected Health Information (ePHI) with the following caveats:

- Only **shared** Box accounts that have been setup by ITS are HIPAA compliant, you can request one to be created at this link. For further information please read the Box page on the Safe Computing Website.
- Box Apps are downloadable applications available from Box (a non-university service) that can be used with U-M Box (a U-M contracted-for service).
  - Only the listed **U-M Box Core Apps** provide a secure environment in which to maintain or share the university's sensitive unregulated data as well as some kinds of sensitive regulated data, including PHI.
  - While **Additional/Non-Core Apps** are also available, these applications are **not approved** for the storage of PHI.
- While storing PHI in U-M Box is permitted, individuals must still follow the protocols and procedures of the university and their unit in regard to handling and sharing protected health data. For more information, see the **Using ITS HIPAA-Aligned Services: What U-M Units Need to Know** page.
- HIPAA regulations only allow for the use of **#Box Sync** when syncing to an encrypted machine (such as CoreImage (Windows) or CoreMac machine). Syncing to a home computer or other non-encrypted device, it is **not approved** by HIPAA.
- Do not share folders that contain HIPAA information to collaborators outside of the University of Michigan (collaborators that do not have a @umich.edu or @med.umich.edu email address).

## Service Desk Information

<table>
<thead>
<tr>
<th>HITS Resources</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Help Knowledgebase</td>
<td>wiki.med.umich.edu</td>
</tr>
<tr>
<td>Service Portal</td>
<td>help.medicine.umich.edu</td>
</tr>
<tr>
<td>Help Me Now</td>
<td>Walk in Locations</td>
</tr>
</tbody>
</table>

For Urgent Issues and Immediate Concerns please contact the HITS Service Desk at 734-936-8000. We’re available 24 hours a day 7 days a week.
### Quick Facts

<table>
<thead>
<tr>
<th></th>
<th>U of M - Main Campus</th>
<th>Michigan Medicine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Level-1 / UMICH / (formerly Kerberos)</td>
<td>Level-2</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>@umich.edu</td>
<td>@med.umich.edu</td>
</tr>
<tr>
<td><strong>WiFi Networks</strong></td>
<td>MWireless</td>
<td>UMHS-8021x / MFleet</td>
</tr>
<tr>
<td><strong>Domains</strong></td>
<td>UMROOT/ADS ROOT</td>
<td>UMHS</td>
</tr>
<tr>
<td><strong>Web Address</strong></td>
<td>umich.edu</td>
<td>med.umich.edu</td>
</tr>
<tr>
<td><strong>Example Sites</strong></td>
<td>password.it.umich.edu</td>
<td>idm.med.umich.edu</td>
</tr>
<tr>
<td></td>
<td>mail.umich.edu</td>
<td>email.med.umich.edu</td>
</tr>
<tr>
<td></td>
<td>wolverineaccess.umich.edu</td>
<td>med.umich.edu/i</td>
</tr>
</tbody>
</table>