VPN

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 that 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></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 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.