Duo Two-Factor Security

Two-factor authentication is a second layer of security, keeping an individual's account secure even if their password is compromised. It requires two proofs of identity when logging in:

- Something you know, such as your Level-2 Password
- Something you have, such as a hardware token with passcodes or a mobile app

Duo provides a flexible two-factor authentication solution that allows us to extend security protection to more systems and individual accounts at U-M. With Duo, you’ll be alerted right away - on any phone or mobile device - if someone is trying to log in as you.

To use Duo Two-Factor Security, and anything it protects, you'll need to enroll first. Please see the information below for instructions.

### Duo Topics

- How Do I Enroll?
- Duo Self-management Options
  - Manage Duo Within the U-M Two-Factor Settings Drop-down Tool (the Michigan Medicine IT User Profile Page)
  - Navigate to the webpage: Michigan Medicine IT User Profile.
  - Manage Duo Within the U-M Hardware Token Drop-down Tool (Michigan Medicine IT User Profile Page)
- What Special Arrangements are Made for ePrescribing Controlled Substances?
- Learn More and Get Assistance
- Enroll a Device in Duo Mobile (PDF)
- Connect to VPN Using Two Factor (PDF)
- Connect to VPN Using Two-Factor (Video)
- Duo Two-Factor for Vendors (PDF)
- When you need to use AirWatch, Duo, and VPN (PDF)
- Traveling with Duo

### Duo-Protected Services of Note

- Wolverine Access
- Electronic Prescription of Controlled Substances
- UMHS VPN
- UMHS Exchange Outlook Web App
- ServiceNow

### How Do I Enroll?

Duo allows you to enroll multiple devices and telephone numbers, which allows you to have more flexibility on a daily basis. Learn more about each option and then use the table below to choose the enrollment that best fits your needs.

<table>
<thead>
<tr>
<th></th>
<th>Mobile Push</th>
<th>Mobile Passcode</th>
<th>Phone Call</th>
<th>SMS Text Message</th>
<th>Temporary Passcode</th>
<th>Hardware Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enroll a smartphone (recommended)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enroll a tablet</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enroll a basic cell phone</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enroll a landline phone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Additional Considerations for Selecting a Device

- The device you use for two-factor will need to be with you, each time you log in to a protected service.
- It’s recommended you enroll in a primary option plus at least one backup option.
- Where you are located while using two-factor may determine which device/options you use. The “Duo Mobile Passcode” option works without an Internet connection and/or cellular service.

If you are using two-factor for ePrescribing Controlled Substances (EPCS), see the next section for additional instructions.

Duo Self-management Options

There are a variety of features that allow you to manage your own device, authentication options, and overall Duo experience.

Manage Duo Within the U-M Two-Factor Settings Drop-down Tool (the Michigan Medicine IT User Profile Page)

1. Navigate to the webpage: Michigan Medicine IT User Profile.
2. Click Security Settings at the top of your User Profile.
3. Click U-M Duo Settings drop-down.

Verify Your Device is Connected to the Authentication Service

- Option 1: When you access the Security Settings tab, the system may automatically start testing the device/option you selected during the enrollment process. Click cancel at the below of the window, in order to exit the testing feature.
- Option 2: You can prompt it by clicking one of the options in the Duo account window.

Manage Your Duo U-M Two-Factor Account

This self-management Duo Two-Factor window allows you to update or change your Duo Two-Factor account settings.

- Add a New Smartphone (with New Phone Number) to Your 2FA Account
- Add Another Device & Select the Primary/Default Option in Your 2FA Account
- Change the Device's Name in Your 2FA Account
- Delete a Device Registered to Your 2FA Account
- Reactivate the Smartphone in Your 2FA Account
- Set the Primary/Default Device in Your 2FA Account

Turn On/Off the UMHS Global Default Override to Set Phone Call as Your Default

Some services cannot read the current authentication options selected during the Duo Registration Enrollment process. To overcome this limitation, you must select your primary authentication option here. When a service cannot read the option/device you selected, your default is set to the Duo Mobile Push option. To override this UMHS global setting, it requires you to complete a global setting override on your profile page by selecting the Phone Call (to put the override into effect) or the Duo Push (to remove the override) radio button.

Manage Duo Within the U-M Hardware Token Drop-down Tool (Michigan Medicine IT User Profile Page)

On this page, you can do the following:

- Add a Duo Hardware U-M Token

This process will link the token to you, which will allow it to generate a passcode when you need to use Duo.

- Resync Your U-M Token

Sometimes hardware tokens can become out of sync with the system. If this occurs, you will not be able to login. Resyncing your token is the first line of trouble shooting, similar to restarting a computer when it doesn’t work. This tool gives you the ability to resync your hardware token with the Duo Security System.

- Remove Your U-M Hardware Token

The U-M Device is no longer associated with your name in the system.
What Special Arrangements are Made for ePrescribing Controlled Substances?

Due to DEA regulations, EPCS uses its own Duo system that's separate from everything else. Only smartphone, tablet, and hard tokens are permitted (no call back, text messaging, or temporary passcodes).

To enroll in Duo Two-Factor Security as an EPCS provider:

- If you will be using a smartphone or tablet, make sure it is already enrolled in AirWatch as well as the normal Duo system. Click the appropriate link for instructions:
  - AirWatch enrollment instructions
  - Duo Two-Factor enrollment instructions
- If you will not be using a smartphone or tablet, meet with your EPCS Liaison to obtain an EPCS hardware token.

In either case, complete EPCS enrollment with your EPCS Liaison.

Learn More and Get Assistance

Help Me Now walk-in locations can answer your individual questions and provide you with hands on help with enrollment. (EPCS registration should be completed by the appropriate EPCS Liaison prior to visiting the Help Me Now location.) You may also return expired MTokens to any one of these locations.

The HITS Service Desk can be contacted at (734) 936-8000 for any additional assistance and questions.