AirWatch for Mobile Devices

AirWatch is the preferred method for e-mail access on all smartphones or mobile devices at Michigan Medicine. Click [here](#) for enrollment instructions.

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.

Visit the Customer Service Center's AirWatch Device Management System page for even more information on AirWatch. This page requires a Level-2 login and password. See below for what AirWatch can and cannot do.

**Supported Platforms for AirWatch**

AirWatch will support the following platforms, including personal laptops:

- Apple iPhone and iPad devices with iOS version 10.0 and above *(preferred devices)*
- Android devices with version 4.0 and above*
  
  Note: For Haiku and Canto access on Android platforms, devices by HTC, Samsung, and LG are required.
  - Due to some manufacturer-specific features, there are limitations for some mobile devices.
  - Nexus and Motorola phones are now compatible with AirWatch, but require a different set of instructions: AirWatch InBox
- Laptops and desktops running:
  - macOS 10.9 or higher (Apple)
  - Windows 10 Professional or Enterprise with TPM *(preferred operating system)*

  **NOTE:** Windows devices must have a Trusted Platform Module (TPM) version 1.2 or above. This is a hardware requirement to support device encryption on the PC. See the AirWatch - Enrollment Instructions page for more details.

Windows devices must have a Trusted Platform Module (TPM) version 1.2 or above. This is a hardware requirement to support device encryption on the PC.
### Smartphone/Mobile Device Security Policy Settings and Restrictions

UMHS has implemented the following guidelines to protect personal, corporate and sensitive data. Policies will be enforced once you have activated your device to a service, and prior to any data being downloaded. For example, you will be required to set up a device password prior to your mailbox getting synchronized to your smartphone or mobile device. The UMHS Passcode Security Requirements are as follows:

- Passcode length = 6 (this could be all numbers or alphanumeric)
- Passcode history = 13 (each time a passcode is set, the previous thirteen entries are recorded, so a new unique value must be used)
- Passcode age = 365 days (after which a new passcode must be set)
- Number of failed login attempts prior to device wipe = 10
- Auto lock = at least 5 minutes (user can select a more secure value)
- Grace period before lock = at least 5 minutes (user can select a more secure value)

### Self-Service Portal

Once enrolled, users may use the Self-Service Portal to self-manage their device in case of theft or to manage the device password. See the AirWatch Self-Service Portal Job Aid for instructions on how to perform some common functions.

Users who wish to enroll additional devices in AirWatch should go through the documented enrollment process and should not use the self-service portal to add devices.