Overview

What is AirWatch

AirWatch is the mobile device management (MDM) system provided by Michigan Medicine to ensure security for smart phones and tablets that connect to the Michigan Medicine environment. AirWatch provides service to its mobile device customers through the following:

- A user portal to self-manage devices in cases of theft, loss or a forgotten passcode.
- An enhanced security profile designed to ensure proper safeguards for protected information.
- The ability to publish applications to enrolled devices.
- Devices enroll in one of two different profiles, MiChart or UMHS, to access recommended applications such as Epic’s Haiku or Cisco’s AnyConnect VPN application.
- Rich reporting for asset tracking and compliance audits.

Requirements

Supported Platforms and Devices

There are limitations for certain mobile devices, and due to age, manufacturer-specific applications, or security features. Some devices will not function with AirWatch or have limited features.

This document provides directions for Android devices only; however, AirWatch is supported on the following platforms:

- Apple iOS 6.0 or higher. iOS 10.0 or higher for wireless.
- Android by HTC, Samsung, and LG running Android version 5.0 or higher for full function. Other Android models will have reduced features.
- Windows Phone 8.

Before You Begin

Make sure your device is fully charged and plugged into a charger.

- Remove existing UMHS Outlook connections.
- Back up your data. This process varies among devices and manufacturers. Please follow the manufacturer recommendations for data backup.
- Have a 6-digit alphanumeric or all numeric passcode ready for your device.
- Know your Michigan Medicine Uniqname and Level-2 password.
- Obtain a Google Play ID and password if you don’t already have one.
- Verify stable internet connectivity or join the Mwireless-UMHS network.

In order to access your Michigan Medicine Outlook email, calendar, contacts and Skype for Business Mobile on your mobile device, AirWatch enrollment is required. Otherwise, you may only access these services through Outlook Web Access.
Installation may take 30 minutes or more to complete.

Remove Existing UMHS Outlook Connections

This is only required if you currently access your Michigan Medicine outlook email on the device.

Before you enroll in AirWatch, you must start with a clean slate and you must remove any existing Outlook/Exchange connections already on your device – otherwise the new AirWatch connection to Outlook/Exchange will not work properly!

1. Tap Apps.
2. Tap Settings.
3. Scroll down and select Accounts.
4. Select the Microsoft Exchange ActiveSync account.
5. Select the UMHS Exchange mail address.
6. Access the Additional Options menu in Sync Settings.
7. Tap Remove Account.
8. Tap Remove Account again to delete all of the account’s content.
   - The existing UMHS Outlook account has been removed.
9. Return to the home screen.

The AirWatch enrollment process will restore your UMHS Exchange email connection. If existing connections are not removed prior to AirWatch installation, the enrollment process may generate an error or duplicate a connection to UMHS Exchange. If you forget this step and have a duplicate connection, un-enroll your Android device from AirWatch and delete any remaining UMHS Exchange connections, then re-enroll in AirWatch.
Join the MWireless Wi-Fi Network

It is preferred that you enroll in AirWatch while you are at a Michigan Medicine facility. Wi-Fi is available through the MWireless-UMHS network.

If you wish to enroll at home or outside the network, ensure you have a strong Internet connection before beginning. Go to Settings and connect to a Wi-Fi network.

1. While at a UMHS facility, select Settings from either the notification menu or the main application launcher.
2. Select Wi-Fi and verify it is set to On.
3. Select the MWireless-UMHS network from the list of available Wi-Fi networks.
4. Depending on your device, enter your Uniqname in either the User name or identity field, and your Level-1 password in the Password field.
5. Accept the certificate.

Some Android phones may need to reboot after the first connection to the MWireless-UMHS network to gain full network functionality.

Enroll your Device in AirWatch

Download the AirWatch MDM Agent

In order to download the AirWatch Agent, you must have a Google account and access to the Google Play Store. Be sure you have your Google Play Store user name/ID and password!

1. Tap to open the Google Play Store.

2. Enter AirWatch in the Search field and select the AirWatch MDM Agent app.
3. Tap Install.
4. Tap Accept.
   - The AirWatch agent is installed.
Enroll Your Android Device Using the AirWatch Agent

1. Tap Open to open the AirWatch MDM Agent app.

2. Select Email Address for the Authentication Method.

3. Enter your uniqname@med.umich.edu address.

4. Tap Continue.

5. Select either UMHS Standard or UMHS MiChart from the drop-down menu.

   A. Select UMHS Standard if you wish to access Exchange only.

   B. Select UMHS MiChart if you plan to access Exchange and MiChart using the Haiku or Canto apps.

6. Tap Continue.
Authentication, Device Details, and Terms of Use

1. Enter your **Uniqname** and **Level-2 password**.
2. Tap **Continue** to initiate the login process and complete authentication.
3. Select the **Device Ownership** setting that is appropriate for your device.
   - Corporate – Dedicated
   - Corporate – Shared
   - Employee Owned

These categories are only recorded in the AirWatch system and do not differentiate what services or policies apply to the device.

4. Review the **Terms of Use** and tap **Accept**.

Authentication is complete.

**Secure the Device**

When device authentication is completed, the device must be secured.

**Accept the Enrollment Policy**

1. Tap **Get Started**.
- The Grant permissions to AirWatch screen displays, requesting device administrator access.

Depending on your type of phone continue as instructed to activate the enrollment policy.

2. Tap Continue.

Along with AirWatch, additional related plug-ins or UMHS Apps may need to be installed. Depending on your device, you may need to enable the Unknown sources setting.

A. Tap Device Settings.

B. Select Unknown sources.

3. Tap Activate to activate the enrollment policy.
C. Tap OK.

D. Return to the AirWatch MDM Agent to Install Enterprise Service.

Install Enterprise Service

During the Configuration phase of the install process, you are prompted to Install Enterprise Service.

1. Tap Continue.

2. Tap Next to move to the next screen.

3. Tap Install.

The AirWatch Service for the device is installed. The next screen requests that you activate AirWatch as a device administrator.

Security Policies and Device Encryption

If the device is not encrypted in compliance with your organizations security policies, encryption needs to be set up.

Passcode and Related Security Policies

- Passcode length = 6 (this could be all numbers or alphanumeric)

UMHS and AirWatch will NOT and CANNOT collect any data related to phone calls, texts, installed applications, or web browsing. These capabilities have been disabled and there is NO remote management!
• Passcode history = 13 (this means each time you set a passcode it remembers the previous thirteen entries and will require a new, unique value)
• Passcode age = 365 days (after which you will be required to set a new passcode)
• Number of failed login attempts prior to device wipe = 10
• Auto Lock = at least 5 min (user can select more secure value)
• Grace period before lock = at least 5 min (user can select more secure value)

When you set your passcode, be sure it is something you’ll remember. 10 failed login attempts will result in the device being wiped as a security precaution!

Set Device Administrator
1. Tap Activate.

   ▪ A window appears requiring you to set a screen unlock PIN or password.

2. Tap OK.

3. Enter a password. Select a strong password at least 6 characters long.
4. Tap Continue.
5. Re-enter the password to confirm.
6. Tap OK to continue to Device Encryption.

**Device Encryption**

If your device is not already encrypted you will be required to perform that step now.

> This process can take an hour or more. If you have already elected to encrypt your device this step may not be necessary.

1. Tap **Device Settings**.

2. Tap **Encrypt Device**.

3. Enter your password.
4. Tap **Continue**.
5. Tap **Encrypt Device** to confirm encryption.
Configure Your Outlook Account

Once Encryption is completed, configure your Outlook account.

NOTE: If you do not want email setup or do not have an email supported device and are just enrolling for Skype for Business skip down to additional apps.

1. Tap Continue.

2. Tap Continue again.

3. Enter Your UMHS Level-2 password.

4. Confirm your password.

5. Tap OK. A screen indicating your device has been configured appears.

6. Tap Exit.
A. You are directed back to the AirWatch Agent where you can see your successful enrollment status. If you are not directed, tap the application to view your status.

2. View the available related apps.

With AnyConnect, you may access can access all UMHS resources, including the UMHS file servers and the internal web pages.

**Additional Apps**

Depending on your make and model, you may need to install a plug-in or it may have been installed automatically with the AirWatch MDM Agent. If a plug-in is needed, continue with these steps. If you omit this step, most (or all) functionality provided by AirWatch won’t be available.

1. Tap **App Catalog**.
Un-Enroll your Android Device from AirWatch

If you un-enroll from AirWatch you will not be able to access your Outlook Exchange email, calendar, or contacts. The only way you will access these services is via Outlook Web Access on a browser.

1. Open the AirWatch Agent app.
2. Tap your Menu button.
3. Tap Un-enroll.
4. Tap Yes to confirm you want to un-enroll.
   - If you select Yes, all AirWatch associated policies will be removed, the Exchange connection and its data will be removed, and any apps installed via AirWatch will be un-installed.
   - Manufacturer-specific plug-in software or downloaded applications are not be removed automatically.

Additional Resources

- HITS Customers: Service Desk at 734-936-8000