Overview

What is AirWatch for Personally-owned macOS Devices?

AirWatch is the mobile device management (MDM) system provided by Michigan Medicine to ensure security for smartphones, tablets, and computers that connect to the Michigan Medicine environment. Personally-owned is defined as a device not owned by the Michigan Medicine institution. AirWatch provides service to its 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.
- Rich reporting for asset tracking and compliance audits.
- Certificate management which allows for access to the wireless network.
- Ability to utilize MiChart on a mobile device (Haiku or Canto), or on a personally-owned laptop or desktop
- Enables encryption and safeguards against data compromise, malware, ransomware, and the like

In order to access the internal secure wireless (UMHS-8021X) network on your personally-owned device, AirWatch enrollment is required effective April 27, 2017. More information on Network Admission Control here: [https://wiki.med.umich.edu/x/A4D3](https://wiki.med.umich.edu/x/A4D3)

Information on AirWatch is here: [https://wiki.med.umich.edu/x/HIoY](https://wiki.med.umich.edu/x/HIoY)

Supported Platforms and Devices

OS X 10.9 to current macOS 10.1x are supported. These devices are compliant and use FileVault 2 for encryption. [https://support.apple.com/en-us/HT204837](https://support.apple.com/en-us/HT204837)

Before You Begin

Make sure your device is fully charged or plugged into a charger (if applicable).

- **Back up your data.** This process varies among devices and manufacturers. Please follow the manufacturer recommendations for data backup.
- Know your device administrator Username and Password. (This password may have to be changed).
• Know your Michigan Medicine Uniqname and Level-2 password.

• The device itself does not need to be on the Michigan Medicine network to enroll; however, enrollment while on the network is recommended.

Encryption
PERSONALLY-OWNED devices must have encryption turned on before enrolling in AirWatch in order for them to receive policy that allows internal access. Note: For mac devices, you need to use FileVault to turn on encryption. Please review How to enable FileVault for instructions. Users are responsible for retaining and safeguarding their own encryption key which FileVault provides, as this information can only be retrieved by the original user!

Encryption prevents unauthorized access to data storage. This makes the data unreadable if the computer is lost or stolen, and is required by policy Standard Practice Guide UMHS Policy 01-04-507.

Enroll your Device in AirWatch
Personally-owned device instructions
1. Go to Safari, and navigate to awagent.com

2. Double click to open the AirWatchAgent.dmg

3. Double click Install AirWatch MDM Agent.pkg

4. Click Continue at the bottom right of the Introduction screen.

5. Click Continue on the License screen.

6. Please Agree to the software license.

7. Click Install to start the process.

8. Please provide your machine administrator Username and Password, and click Install Software.
9. Click **Email** at the bottom of the AirWatch screen.

10. Enter your Michigan Medicine email account information (**uniquname@med.umich.edu**), and click **Continue**.

11. Select **UMHS Standard** as your group, and click **Continue**.

12. Enter your **Level-2** credentials, and click **Continue**.

13. Select **Employee Owned** as your ownership, and click **Continue**.

14. Click **Accept** to the Terms of Use.
15. Click **Enable** to Enable Device Management.

16. Provide your machine administrator **Username and Password** to allow the change.

17. Congratulations! Click **Open Agent**.

18. You will see a Status box that gives you information about your enrollment status.

19. Click **Device Information** on the left side menu to see encryption status.

20. You can confirm that **AirWatch** is on, simply by the **shield** in the top right hand corner of your screen. The shield will blink from time to time, signifying the agent is syncing with the server.
UMHS-8021X wireless activation

If you have previously connected to the UMHS-8021X network, you need to remove this network before proceeding. Follow the instructions below to remove this network. If this is the FIRST time you are connecting to the 8021X network, then skip to the section on Page 6: ‘Join UMHS-8021X wireless connection’.

To remove UMHS-8021X wireless connection previously joined

1. Go to the Apple in the upper right hand corner, and select System Preferences
2. Double click Network.
3. Click Wi-Fi on the left, and click the Advanced button.
4. Click UMHS-8021X, and click the - (minus) symbol
To join UMHS-8021X wireless connection for the first time

1. At the top of the menu bar, click the wireless icon and select **UMHS-8021X**.

2. A new window will open:

3. Click the **Mode** dropdown menu and select **EAP-TLS**.

4. In the new window, click the **Identity** dropdown menu, and select your uniqname.

5. Leave the **Username** field empty, and click the **Join** button.

6. When prompted, type in the User Name and Password of an administrator of the machine to accept the changes.

Your WiFi connection to the Michigan Medicine UMHS-8021X wireless network should now be complete.