Overview

What is AirWatch for BYOD

AirWatch is the mobile device management (MDM) system provided by UMHS to ensure security for smartphones, tablets and computers that connect to the UMHS environment. BYOD (bring your own device) is defined as a device not owned by the corporation. 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.
- Utilize MiChart on a mobile device (Haiku or Canto), or on a personally owned laptop/desktop.
- Enable safeguards against data compromise, malware, ransomware, and the like.

In order to access internal secure wireless (UMHS-8021X) on your BYOD device, AirWatch enrollment is required for all personally owned devices. More information on Information Assurance here: https://goo.gl/QRu1wy

Requirements

Supported Platforms and Devices

Windows 10 Professional or Enterprise Editions are the only supported operating system.

This document provides directions for BYO (bring your own) Windows 10 Professional or Enterprise devices, with a TPM (Trusted Platform Module) to access privileged company information and networks only.

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 machine administrator Username and Password. (This password may have to be changed)
- Know your UMHS Uniqname and Level-2 password.
- The device itself does not need to be on UMHS network to be enrolled in Airwatch. The device can be enrolled using any network connection.

**NOTE:** Microsoft .NET Framework 4.0 full package or greater is required to be on the device. Microsoft Visual C++ 2013 is required as well. The .NET Framework is typically installed on most machines, the Visual C++ will be installed automatically if missing.
Enable your TPM (Trusted Platform Module)

**NOTE:** Do this before you start Enrollment to provide a consistent experience. Please follow the instructions for your device to enable the TPM in the BIO(s).

The BIO(s) steps will vary for each type of hardware. Please consult the product support site for enabling the TPM on your device. **Windows 10 Professional** or **Enterprise** will enable the rest automatically.

If this device has been enrolled in AirWatch before, make sure to delete it using the Console. A device cannot be enrolled twice in the system. Encryption keys cannot be stored/recovered if a machine name is duplicated in the system.

Enroll your Device in AirWatch

1. To do this, open the **Settings** app, click **Accounts**, and navigate to **Work access**.

2. Click on the + sign next to **Enroll in to device management**

3. In the **Connect to work or school** box please fill in your **Level 2** email address then click **Continue**

4. In the **Authenticate** box select by using the dropdown to the right of **Group ID**

5. Select the applicable **Group ID** from the dropdown arrow and click **Next**.
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. Enter your **Uniqname** and **Level-2 password** then
   click **Next** to initiate the login process and complete
   authentication.

7. Select **Employee Owned** in the **Device Ownership**
   dropdown then click **Next**.

8. Review the **Terms of Use** and click **Accept**.

9. Click **Skip** on the **Remember sign-in info?** screen.

   - Enter your Uniqname and password then click **Next**
     to initiate the login process and complete authentication.
   - Select **Employee Owned** in the **Device Ownership**
     dropdown then click **Next**.
   - Review the **Terms of Use** and click **Accept**.
   - Click **Skip** on the **Remember sign-in info?** screen.

10. **Well done!** The TPM is recognized and the device
    has a strong password, and registration is complete.

11. You can always check on your enrolled devices from
    the **AirWatch Self-Service Portal**.
    
    ![Screen shot showing AirWatch enrollment status](https://aw.med.umich.edu/MyDevice)

    **AirWatch will provide your device a Wi-Fi
     certificate and policy, but it will not auto-
     enroll you in UMHS-8021X. You will still need
     to join the wireless network separately.**