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 (1607 or Anniversary Edition) or Enterprise Editions are the only supported operating system.

This document provides directions for BYO (bring your own) Windows 10 Professional (1607 or Anniversary Edition) 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 for all personally owned devices. More information on Information Assurance here: https://goo.gl/QRu1wy
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. Navigate to [https://awagent.com](https://awagent.com) in your browser and it will direct you to the *Access work or school* section in *Settings*.

   ![](Welcome_to_AirWatch.png)

   **Welcome to AirWatch!**

   AirWatch helps your IT department to provide your device with secure access to resources.

   ![Connect to work or school account](Connect_to_work_or_school_account.png)

   **Connect to work or school account**

2. In Connect to work or school box you will choose *Enroll only in device management* at the bottom of

3. In *Set up a work or school account* box you will and then click *Next*, after entering your **Level 2** email address.

4. In the *Let’s get you signed in* box please fill in your **Level 2** credentials then click *Sign in*.
5. In the **Authenticate** box select the dropdown under *Group ID* to **UMHS Standard** and then click **Next**

**Authenticate**

Select your group from the list of available options below.

Group ID

UMHS Standard

6. In the subsequent **Authenticate** box please fill in your **Level 2** credentials then click **Next**

**Authenticate**

Enter your Username and Password

level2

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

**Authenticate**

Additional information is required to authenticate your device

Device Ownership

Employee Owned

The information I have provided on this form is correct to the best of my knowledge.

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

**Authenticate**

Terms of Use

I acknowledge that I have received and read the UMHS Policy 01-04-507 Mobile Device Security (only available while on UMHS internal networks). I understand that I must comply with this policy when accessing and using Mobile Device resources or those provided by UMHS. If I fail to comply with this policy, the UMHS reserves the right to revoke access to any services provided for Mobile Devices and pursue actions up to seeking administrative and legal actions for violations of the policies.

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

10. You're all set! Click **Finished**
11. Under the Access work or school settings under Connect to work or school you will see a confirmation of your enrollment.

![Connected to AirWatch MDM](https://aw.med.umich.edu/MyDevice)

12. You can always check on your enrolled devices from the AirWatch Self-Service Portal. [https://aw.med.umich.edu/MyDevice](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.