iOS EMM Enrollment Process
Before starting the device enrollment procedure, make sure your device is disconnected from the “WUSM-Secure” wireless network.

Start by launching your device’s “Settings” app from your home screen.
Tap “Wi-Fi” in the left column to select your Wi-Fi settings.

Make sure you are either connected to the “Guest” wireless network, or your mobile data service if available on your device.
Now we can proceed with enrolling your device.

Return to your home screen and launch the “App Store”.
Tap the “Search” box in the upper right of the screen to search for the AirWatch app.

Using the on-screen keyboard, enter in “Airwatch Agent” into the search box. Then press the “Search” button from the on-screen keyboard.
The AirWatch Agent should be returned among the search results. The proper app can be located by the icon of a blue shield.

Tap the “Get” button to begin downloading the AirWatch Agent the app store.
Once installed, tap the “Get” button will change to an “Open” button.

Next tap the “Open” button to launch the AirWatch Agent app.
Once the app opens you should see a screen similar to the one above.
On the initial screen, select “Server Details” to continue.
The next screen should be prompting for Server Details.

Tap the white space beside each field and use the on-screen keyboard to enter in the appropriate information.

*Note: If your screen is not prompting for Server Details as depicted in the image above, return to the previous screen and ensure you selected the “Server Details” button.*
For the “Server” field, enter: *mdm.wusm.wustl.edu*

The “Group ID” is the same as your domain. (i.e. accounts, *medpriv, wudosis, dom, etc...*)

Press "Next" in the upper right to proceed.
The next screen prompts for your username and password.

The “Username” field doesn’t require you to use the “domain\username” combination. Your username by itself is sufficient.

You should use the same username and password you use to login to a WUSTL Windows computer

After you have filled in your username and password, press “Next” in the upper right to proceed.
Select the appropriate ownership of the device from the menu.

Then press “Next” in the upper right to continue.

Turn to the next page for an explanation of the available options.
Options are:

- **Corporate Dedicated** – A device purchased by Wash U, but used exclusively by one individual. An example would be a work provided mobile phone.
- **Corporate Shared** – A device purchased by Wash U and shared by multiple users. An example would be a tablet device that is shared across the department, or a mobile phone used for an on-call rotation.
- **Employee Owned** – A personal device purchased by an employee or student that would like to use it to access the WUSM-Secure network.
Terms of Use

WUSM-Airwatch Terms of Service

Mobile devices that connect to the School of Medicine secure wireless network (WUSM-secure) will be required to enroll that smartphone or tablet into a mobile device management solution called AirWatch.

By downloading the AirWatch App from your app store and registering it on our network, you will agree to allow information security policies to be enforced on your device to meet HIPAA requirements for protection.

These policies require:

- The device to have a pin or password set.
- The device to have its storage encrypted.
- Provide all WUSM Departments the ability to remotely wipe mobile devices.

These policies will not require:

- The tracking of the device.
- Inventory of applications installed.

If you have any questions concerning these policies please contact your respective support department.

You will now be prompted to accept the Terms of Service.

Please review the text displayed on your screen.
Then press “Accept” in the lower right of the screen to continue.
Enable Device Management

To enable your device, you will be redirected to Safari and Settings

Why?

• Access your company resource
• Remove company data in the event of loss or theft

The following screen is simply informational, letting us know a Device Management profile is about to be installed on the device.

Select “Redirect & Enable” at the bottom of the screen to continue.
Next you’ll be redirected to your Settings app and presented with an “Install Profile” prompt. Installation of management profiles are how iOS allows device management.

Tap “Install” in the upper right corner of the prompt to continue.
If your device already has a passcode enabled, you’ll be prompted for it at this time.

Enter your passcode to continue
Another prompt will display asking to confirm the installation of the profile.

Again tap “Install” to proceed.
At this point, iOS will display a prompt about the permissions being granted to manage the device.

**We are only using the permissions that allow us to ensure your device complies with existing Wash U Policy**

Tap “Install” in the upper right of the window.
Another prompt will display to confirm management of the device.
Tap “Trust” to continue.
The next dialog should inform you that the profile has been installed.

Tap “Done” in the upper right to continue
Next you’ll be redirected to your web browser very briefly and prompted to return to the “Agent”.

Tap “Open” to continue.
Next the AirWatch Agent app will declare the enrollment process has completed.

- You will receive company resources and settings assigned to your device by your IT department.
- You will receive a notification if further action is required.
The AirWatch Agent may prompt to be allowed access to post Notifications. Please select “Allow”

This not only allows IT services to determine what might be wrong if there is an issue with your device on AirWatch, but also allows us to push contact information if the device is lost and locked.
Once enrollment is complete, the device will start receiving profiles pushed to the device.

Presently the only profiles that are pushed across the entire Med School are for Passcode and Encryption. If the device does not yet have a passcode set for it, a dialog will pop-up stating that one is required.
If the iOS device already has a passcode, then nothing further should be required.

If the device does not have a passcode configured, one will need to be setup at this time. The passcode must be at least a 4 digit PIN.

You may also choose a longer more secure passcode with letters if desired.
After you have completed the steps above, you should now be able to access the WUSM-Secure wireless network form your iOS device.

If you experience any problems with the network, you may see page similar to the one display when you browse the Internet. If the message persists longer than 1 hour, contact your support department.