Android EMM Enrollment
Before starting the device enrollment procedure, make sure your device is disconnected from the “WUSM-Secure” wireless network. Use either the “Guest” wireless network, or your mobile data service if available on your device.

Locate the “Play Store” app on your home screen or within the app drawer.

Launch the “Play Store” app.
Tap the search box at top of the screen to search for the AirWatch app.
Using the on-screen keyboard, enter in “Airwatch Agent” into the search box.

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 app icon to view the app's information page.
Tap the “INSTALL” button to begin downloading and installing the AirWatch Agent from the app store.
Next tap the “OPEN” button to launch the AirWatch Agent app.
Once the app opens you should see a screen similar to the one on the right.

Welcome to AirWatch!

AirWatch helps your IT Department to provide your device with secure access to enterprise resources

You will be guided through a three part process to authenticate, secure and configure your device.

Choose Authentication Method:

- EMAIL ADDRESS
- SERVER DETAILS
- QR CODE
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 "CONTINUE" on the lower right to proceed.
Some devices may require an additional service app to be installed.

If required, the AirWatch Agent will redirect you back to the Play store if a service app is required.
The next screen prompts for your username and password.

The “Username” field doesn’t require you to use the “domain\username” combination used with some other applications. 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 “CONTINUE” in the lower right to proceed.
Select the appropriate ownership of the device from the pull-down menu.

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.

Press “CONTINUE” in the lower right to proceed
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.

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:

DECLINE  ACCEPT
The AirWatch Agent will acknowledge that your login information has been successfully authenticated.

Press “CONTINUE” in the lower right to proceed.

Part 2: Secure

You have completed Authentication

The following steps will ensure your device is compliant with your company policies
Next the AirWatch agent will prompt for permission to manage your device.

Press “CONTINUE” in the lower right to proceed.

Grant permissions to AirWatch

The AirWatch Agent needs to be the device administrator so that it can:

• Protect your data
• In the event of loss or theft, remove all corporate data

Select Activate when you arrive at the next screen

CONTINUE
The AirWatch Agent now prompts to be activated as a “Device Administrator”. This allows it to properly manage the device.

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

Press “ACTIVATE” in the lower right to proceed.
The AirWatch Agent now prompt for the permissions necessary to manage the device.

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

Press “ACTIVATE” in the lower right to proceed.
The Agent will inform you that 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.

Press “CONTINUE” in the lower right to proceed.

Part 3: Configure

You have successfully completed authentication and securing your device.

You will now configure enterprise resources assigned to your device by your IT department.
Next the AirWatch Agent app will declare the enrollment process has completed.

Press “EXIT” in the lower right to proceed.

You have completed the initial configuration for your device. You will receive a notification if further action is required.

You can now exit the wizard.
If the device is already encrypted and has a passcode, then you won’t have to do anything further.

If you have not setup a passcode, you’ll be prompted to set one up now.

Click “Device Settings” to continue.
You’ll be taken to the appropriate settings menu on the device.

Select “PIN” from the menu.
Enter a PIN with a minimum of 4 digits the click “Continue”.

Re-enter the PIN and click “Confirm” on the following screen.

If you’d prefer a more secure passcode, you may enter in a code longer than 4 digits and use letter characters.
After you’ve set your passcode, you must return to the AirWatch Agent app.

If your device’s storage is not already encrypted, the AirWatch Agent will now prompt to encrypt the device.

The device must be at least 80% charged before encryption will proceed.

Some devices may require being connected to a charger during the process.

Before proceeding with encryption, it is recommended you backup your device to another system, not just to your SIM or SD card.
The prompt will again open up the appropriate settings menu. Click “Encrypt device” to continue.

Enter the device’s PIN to continue with the encryption process.

The prompt will again open up the appropriate settings menu. Click “Encrypt device” to continue.

Enter the device’s PIN to continue with the encryption process.

*Some devices may take up to an hour to encrypt. While going through encryption process, other functions of the device will not be available.*
Once the device has finished encrypting and rebooted, return to the MDM agent.

The agent should inform you that your device has been successfully configured.
The screen should read that the enrollment process has been complete. Click the “Exit” button to leave the app.
After you have completed the steps above, you should now be able to access the WUSM-Secure wireless network form your Android device.

If you experience any problems with the network, you may see page similar to the one display when you browse the Internet.