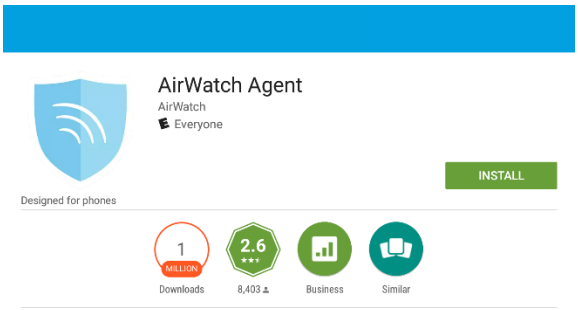
Android EMM Airwatch Enrollment

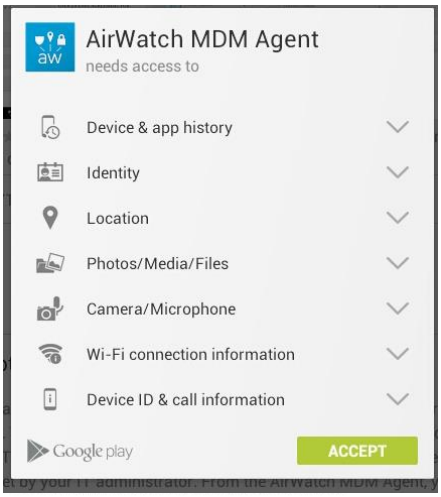
Connecting your Android mobile device to WUSM-secure WiFi requires that you enroll your device in AirWatch.

CAUTION

You **must be** connected to **Eduroam** or the **Guest** network, or your **cellular data** to download and install Airwatch



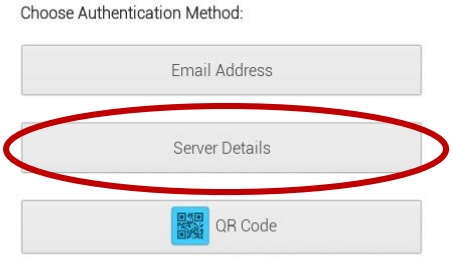
- **Download** the free **Airwatch Agent** from the Play store.



- The Google Play store may display a prompt about the permissions being granted to this application. These are required for AirWatch to securely manage your device.

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

- **Launch** the app once installed.

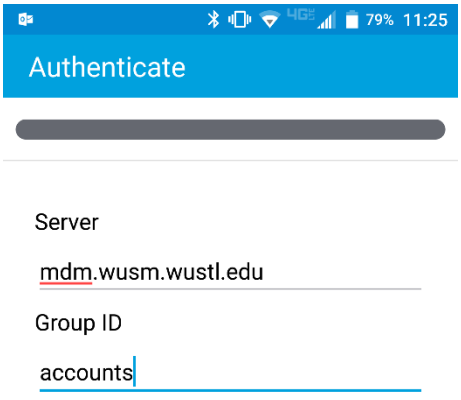


- You must choose **Server Details** as Authentication Method

- Enter

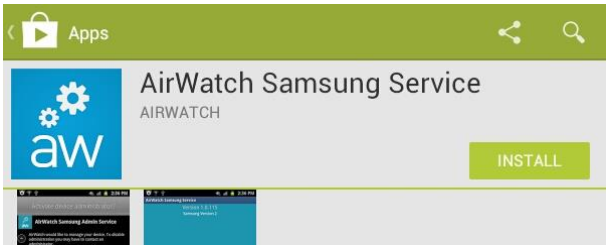
Server: **mdm.wusm.wustl.edu**

Group ID: **accounts**

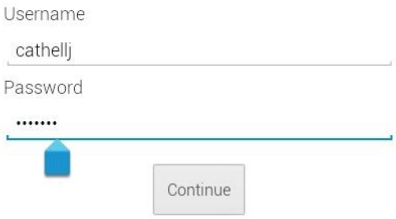


- Click **Continue** to proceed

Some devices may require an additional service app to be installed. You will be redirected to the Play store if your device requires another app.

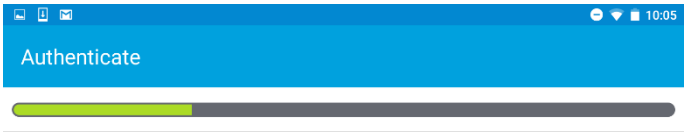


- Enter your **WUSTL Key** and password.

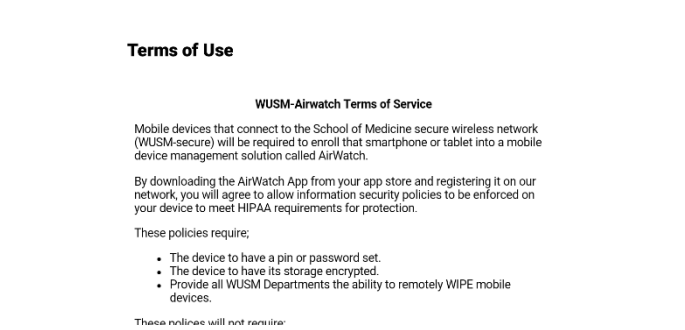


- Select **Continue**

- Select **ownership** from the pull-down menu.
  - Choose Employee Owned for personally owned devices.
  - Corporate Dedicated or Shared are for devices purchased by Wash U (Shared if used by more than one user).



- Next you'll see the Terms of Use. Read, and click Accept to continue or Decline to cancel installation.



- You may see several screens to let you know that your device is about to be secured with Airwatch. If so, click **Get Started** and/or **Continue**.

- The AirWatch Agent will prompt to be activated as a "**Device Administrator**".
-
- Read the Terms of Use, and click **Activate**. Or Cancel to stop installation

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

These policies require:

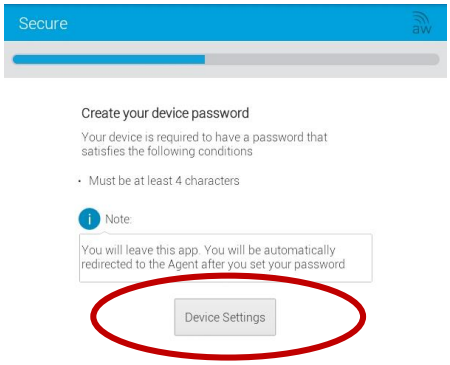
- The device to have a pin or password set.
- The device to have its storage encrypted.
- Provide all WUSM Departments the ability to remotely WIPE mobile devices (e.g. in case your phone containing confidential information is lost).

These polices will not require;

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

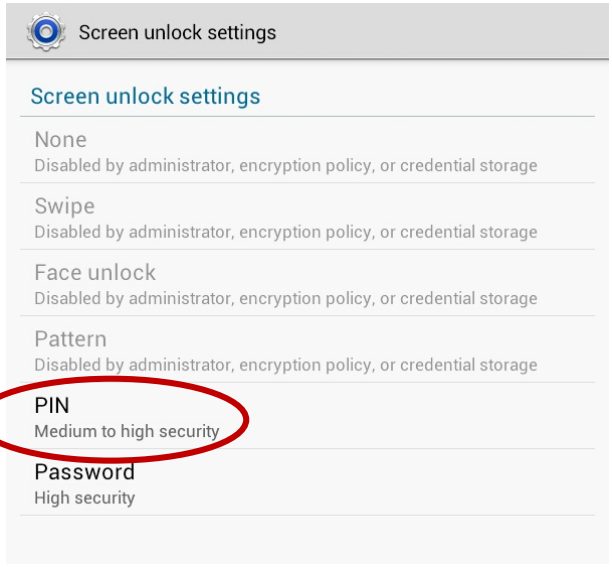
If you have any questions concerning these policies please contact the Information Security Office at infosec@wustl.edu or 314-747-2955.

If your 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 then click **Continue**.

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

- After you've set your passcode, you will need to return to the AirWatch Agent app.

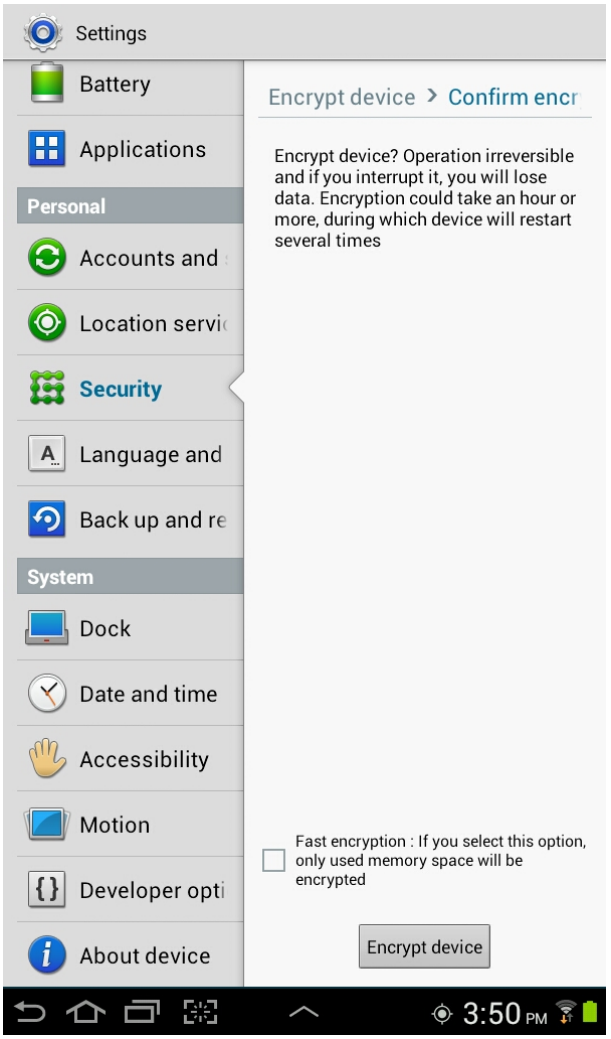
- If your device's storage is not already encrypted, the Airwatch agent will now prompt to encrypt the device.

The device must be at least 80% charged before encryption will proceed. Some devices may require it be connected to a charger.

<u>Before proceeding with encryption, it is recommended you backup your device to another system, not just to your SIM or SD card.</u>

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

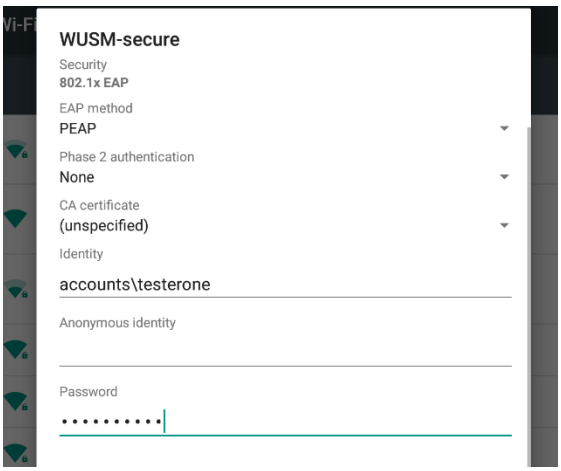
Enter the device's **PIN** to continue with the encryption process.



<u>Some devices may take up to an hour to encrypt. While going through encryption process, other functions of the device will not be available.</u>

- Once the device has finished encrypting and rebooted, return to the Airwatch agent app.
- The agent should inform you that your device has been successfully configured. – Click **Continue**. You may need to exit to your home screen.
- **Go to WiFi** under settings.
- Locate **WUSM-secure** in network listing**.**

.



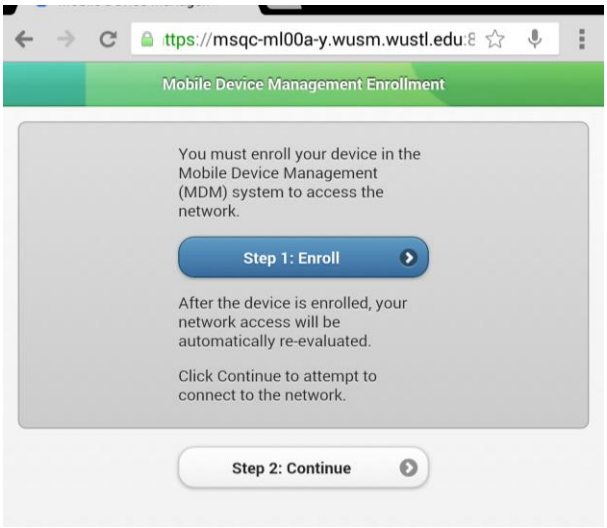
Identity : **accounts**\yourWUSTLkeyid.

Password: your WUSTL Key password

Once you have done this, **Join** the network. It may take a few minutes to connect. *

*If you have an older device, and are unable to join, be sure that your primary authentication is set to PEAP, and your phase2authication is set to MSCHAP/V2.

You should now be able to access the WUSM-Secure wireless network form your android device. You may see a page similar to the one shown at the right the first time you attempt to connect. Be sure you have waited long enough for your device to be fully enrolled, and then try to connect again.



If you have any issues with this process, please contact WashU IT at:

314-933-3333 (7am-5:30pm)

ithelp@wustl.edu

http://it.wustl.edu