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
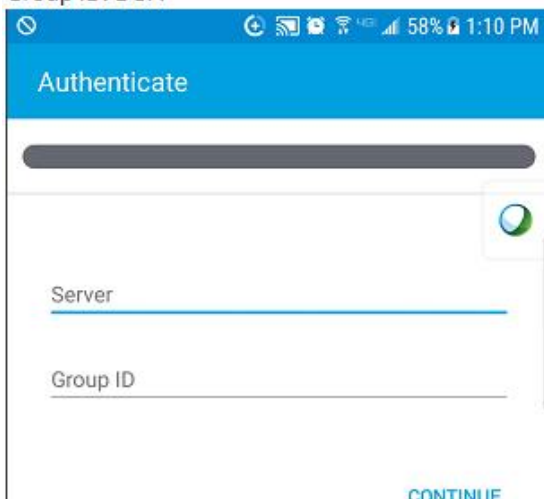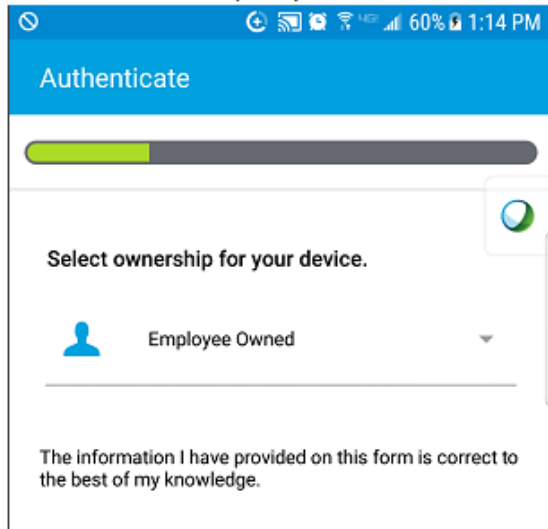
☰ SERVER DETAILS

▦ QR CODE

It is strongly suggested to stick to Server Details or QR Code for the authentication method.

Or via Server Details
Server: airds.mt.gov
Group ID: DOA

Authenticate

Server

Group ID

CONTINUE

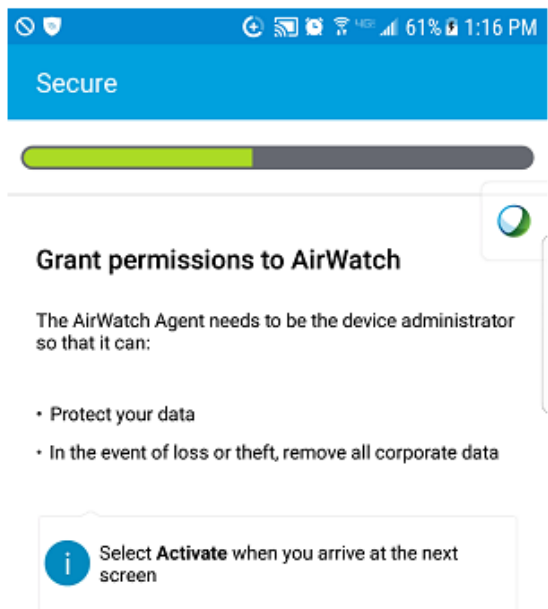On the next screen enter in your C# and password.
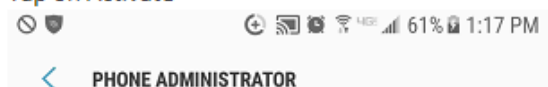
Then select ownership for your device:

Tap on continue

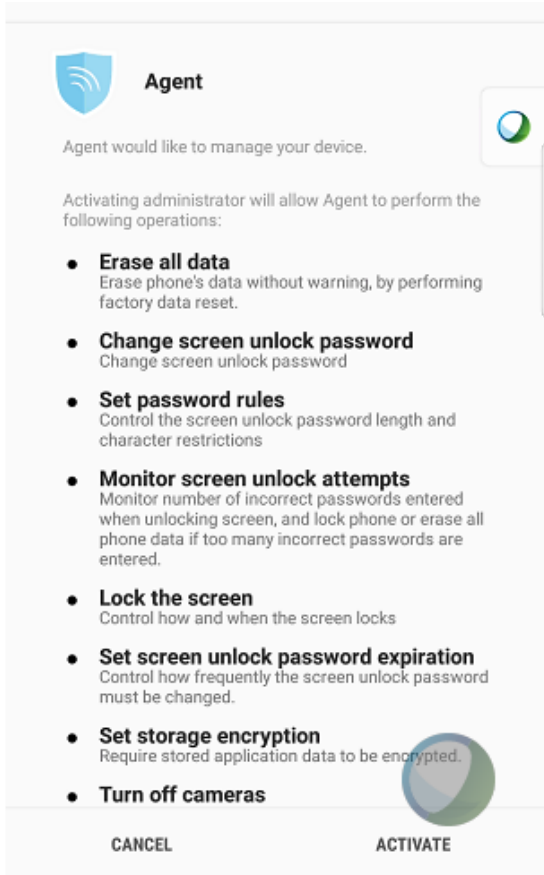Accept the terms of use.

Tap on continue

Tap on Activate

Agent

Agent would like to manage your device.

Activating administrator will allow Agent to perform the following operations:

- **Erase all data**
  Erase phone's data without warning, by performing factory data reset.

- **Change screen unlock password**
  Change screen unlock password

- **Set password rules**
  Control the screen unlock password length and character restrictions

- **Monitor screen unlock attempts**
  Monitor number of incorrect passwords entered when unlocking screen, and lock phone or erase all phone data if too many incorrect passwords are entered.

- **Lock the screen**
  Control how and when the screen locks

- **Set screen unlock password expiration**
  Control how frequently the screen unlock password must be changed.

- **Set storage encryption**
  Require stored application data to be encrypted.

- **Turn off cameras**

CANCEL   ACTIVATE

Tap on continue to get past the Allow non-Play Store apps page

Secure

Allow non-Play Store apps

Enable installation of enterprise apps not available in the Play Store

ℹ️ You will leave this app. Check **Unknown sources** when you arrive at the next screen. Please **return by relaunching the Agent** to continue.
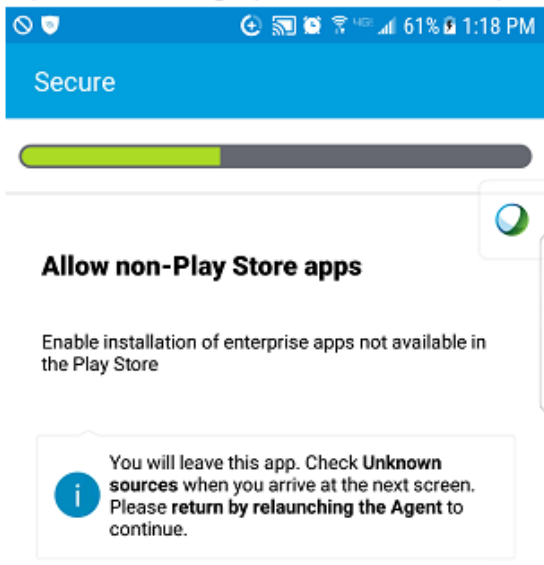
Your screen might look different but mine looks like this.
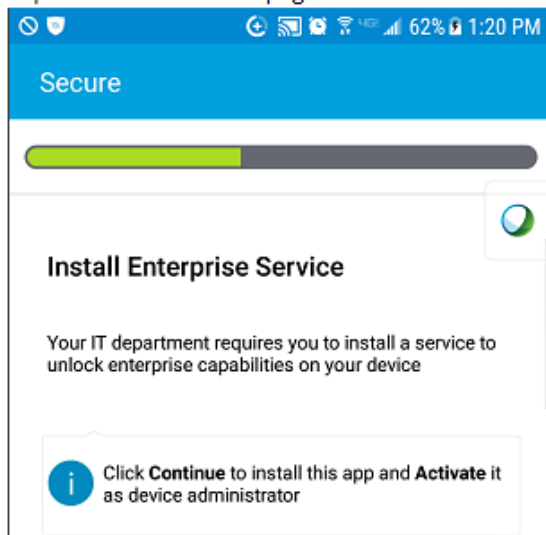Change Unknown sources so that it is enabled

NOTE All Android devices will require that Unknown sources be checked.
This allows the installation of some of the additional services required for AirWatch to

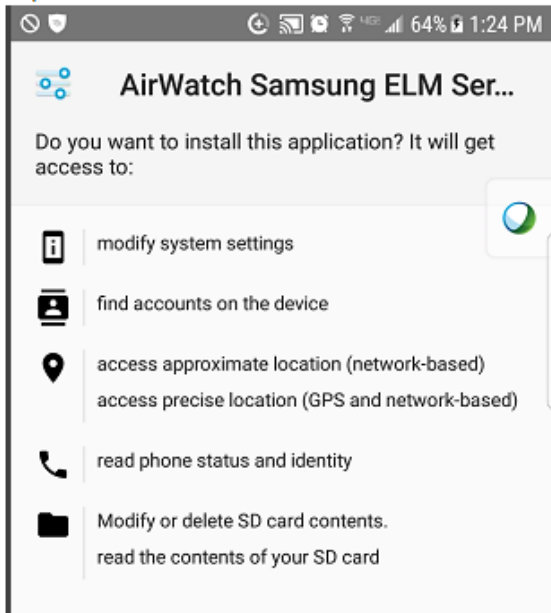**connect with our Exchange server.**
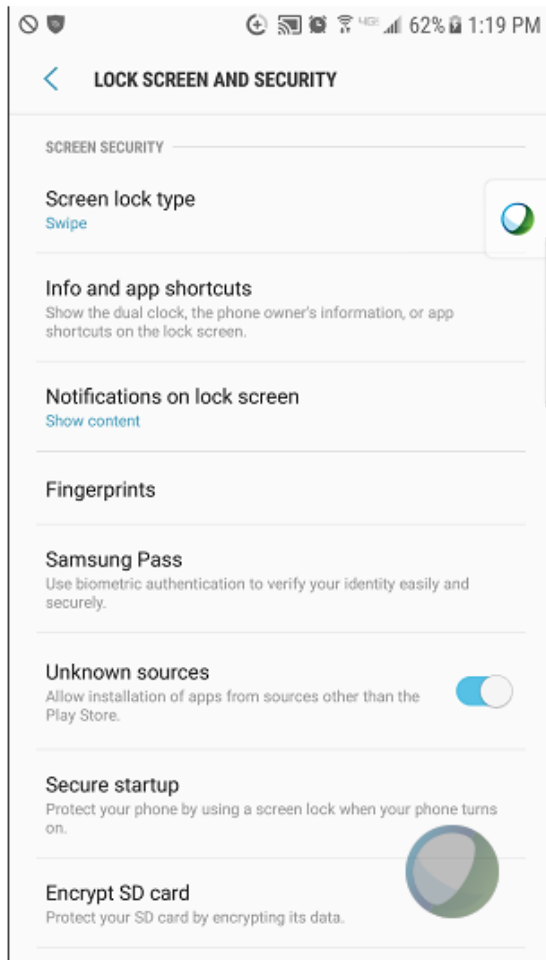
Then hit the back button on your phone.
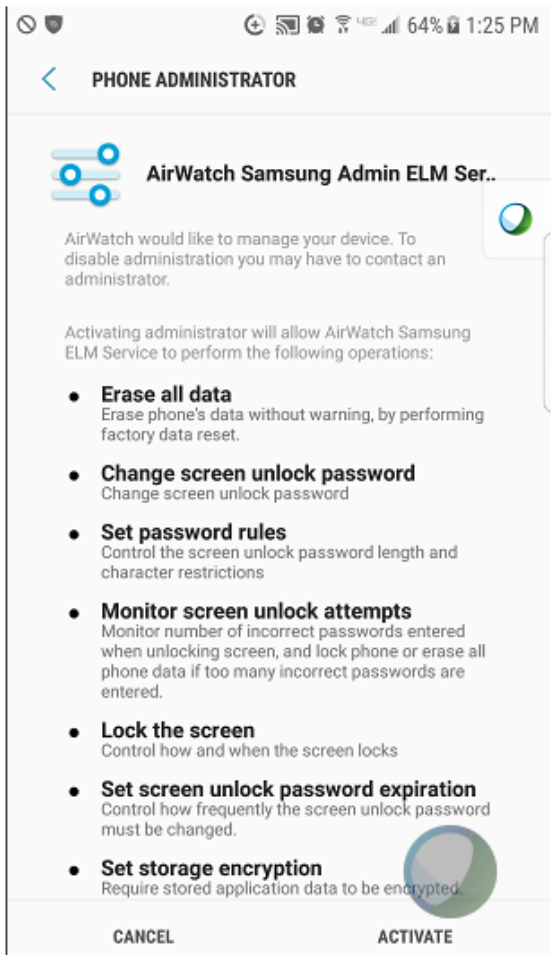
Tap on continue on this page

Each brand of phone will have different services. Samsung's looks like this.
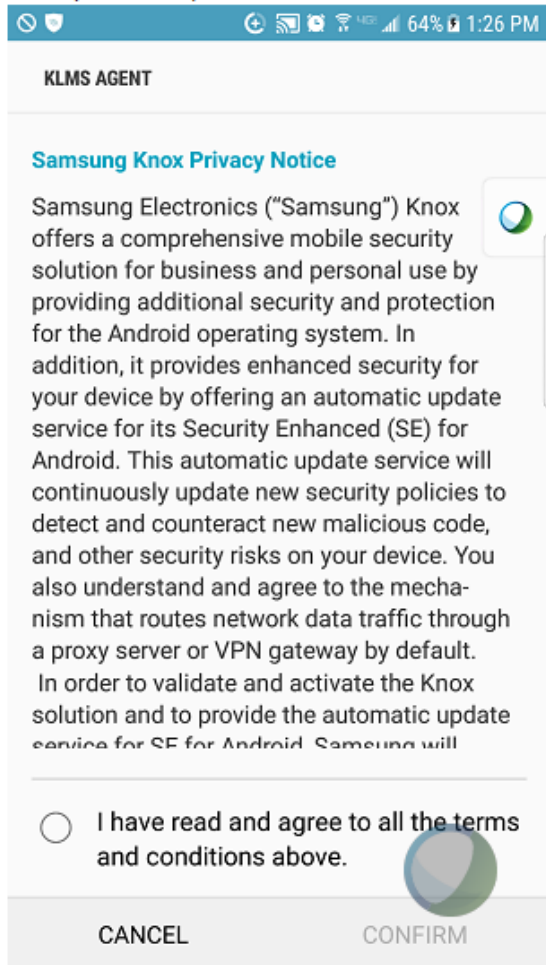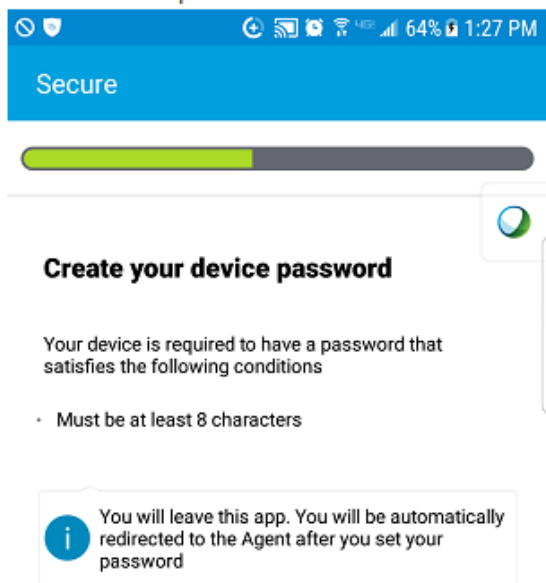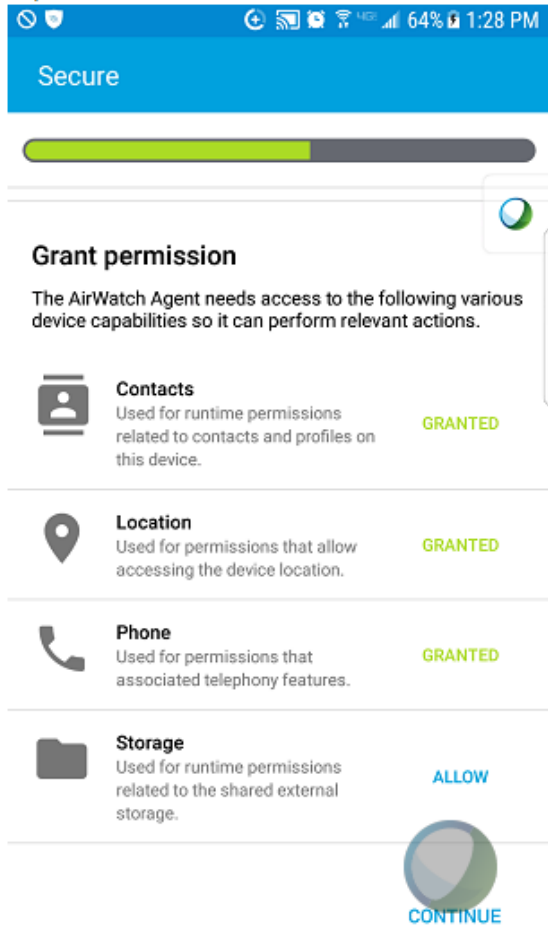Tap install

After installation it will need to be activated

Privacy notice, tap that it's been read. Feel free to read it, then confirm it.

KLMS AGENT

Samsung Knox Privacy Notice

Samsung Electronics ("Samsung") Knox offers a comprehensive mobile security solution for business and personal use by providing additional security and protection for the Android operating system. In addition, it provides enhanced security for your device by offering an automatic update service for its Security Enhanced (SE) for Android. This automatic update service will continuously update new security policies to detect and counteract new malicious code, and other security risks on your device. You also understand and agree to the mechanism that routes network data traffic through a proxy server or VPN gateway by default. In order to validate and activate the Knox solution and to provide the automatic update service for SE for Android. Samsung will

○ I have read and agree to all the terms and conditions above.

CANCEL   CONFIRM

Create a device password

Secure

Create your device password

Your device is required to have a password that satisfies the following conditions

· Must be at least 8 characters

ⓘ You will leave this app. You will be automatically redirected to the Agent after you set your password

Tap continue

Tap continue again
Tap continue again

Enter your email password twice

Should finish setup.