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 your C# and password.

Then select ownership for your device:

- Employee Owned

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

Tap on continue

Accept the terms of use.

Tap on continue

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

Tap on Activate

PHONE ADMINISTRATOR
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 looks

- **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**

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

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.

Install Enterprise Service

Your IT department requires you to install a service to unlock enterprise capabilities on your device.

Click Continue to install this app and Activate it as device administrator.
Each brand of phone will have different services. Samsung's looks like this.

Tap install

AirWatch Samsung ELM Ser..

Do you want to install this application? It will get access to:

- modify system settings
- find accounts on the device
- access approximate location (network-based)
  access precise location (GPS and network-based)
- read phone status and identity
- Modify or delete SD card contents.
- read the contents of your SD card

After installation it will need to be activated

PHONE ADMINISTRATOR

AirWatch Samsung Admin ELM Ser..

AirWatch would like to manage your device. To disable administration you may have to contact an administrator.

Activating administrator will allow AirWatch Samsung ELM Service 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.

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

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.
Grant permission

The AlWatch Agent needs access to the following various device capabilities so it can perform relevant actions.

- **Contacts**
  Used for runtime permissions related to contacts and profiles on this device.
  - GRANTED

- **Location**
  Used for permissions that allow accessing the device location.
  - GRANTED

- **Phone**
  Used for permissions that associated telephony features.
  - GRANTED

- **Storage**
  Used for runtime permissions related to the shared external storage.
  - ALLOW
  - CONTINUE

Tap continue again
Tap continue again

Enter your email password twice

Should finish setup.