GETS AIRWATCH MDM HANDBOOK

October 2014

Abstract

Using AirWatch, a mobile device management tool, within the public sector.

GTA Product and Services Group

Executive Summary

The mobile marketplace has expanded exponentially and quickly. Gone are the days of one-device-fits–all, replaced by a broad range of mobile device choices and the challenge of providing a secure mobile device management (MDM) platform to protect data.

AirWatch by VMware is an MDM tool that manages any mobile device. Using AirWatch, public and private entities can monitor which devices are authorized to access their email systems, as well as prevent access for unauthorized users. The tool does not monitor email messages but rather manages access to an email system.

The state of Georgia shifted from using BlackBerries to Android, iOS and Windows Phone devices. GTA implemented AirWatch as the enterprise MDM platform to manage these devices.

Key points:

- AirWatch is an industry-leading vendor, topping many consultants' "magic quadrant" lists.
- AirWatch manages devices and their access to email. It does not monitor or impact the flow of emails because email messages and message content do not pass through AirWatch.
- AirWatch allows state of Georgia agencies to create and enforce policies (PIN lock, for example) on devices enrolled in the MDM service. GTA is not enforcing any enterprise policies through AirWatch. Instead, GTA enables and administers the service while agencies manage their mobile environments.
- Each agency has been provided training for its AirWatch console administrators, and each agency administers its own console accounts.
- Because AirWatch is set up not to see agencies' message content, it should not create a compliance problem for agencies with regulated data.

Introduction to the GETS AirWatch MDM Service

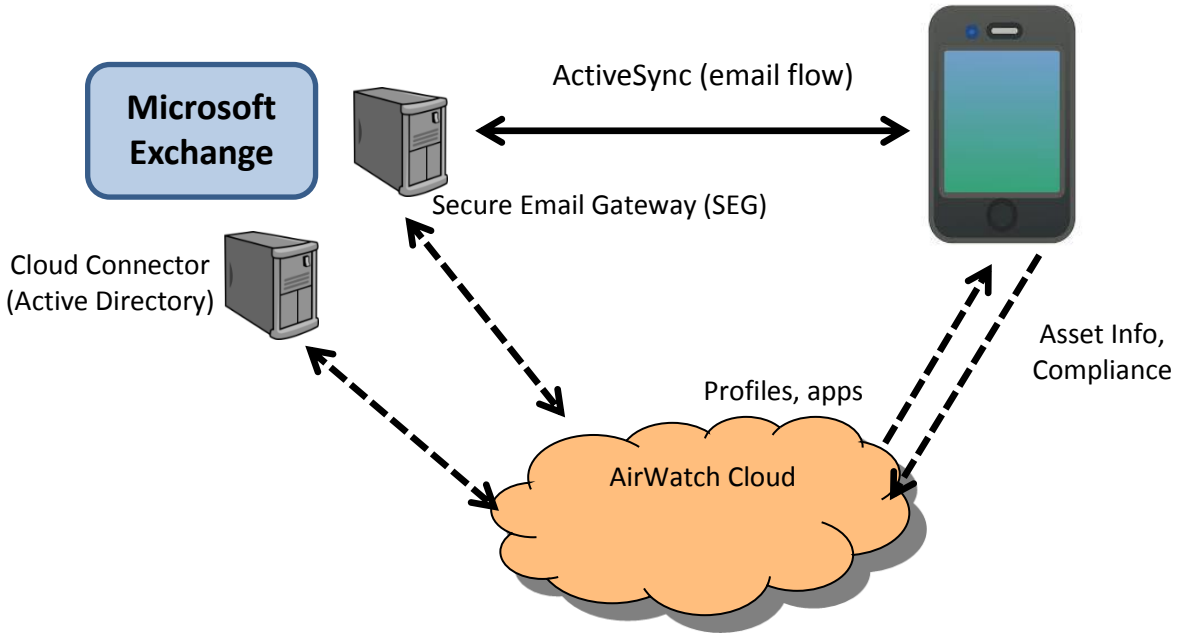
When the Georgia Enterprise Technology Services (GETS) program began in 2009, BlackBerry was the dominant enterprise smartphone manufacturer in the industry, and BlackBerry accounted for almost 100 percent of Georgia agencies' mobile device usage. Since that time, iOS and Android have become dominant for new deployments, and Microsoft's new Windows Mobile platform is growing as the number three market share player. The state's use of BlackBerry devices has been steadily declining, and in 2014 all of the GETS agencies are reporting plans to move away from BlackBerry.

As a result of migrating away from BlackBerry and its secure Blackberry Enterprise Server (BES), GTA sought out a solution for Apple, Android and Windows devices. AirWatch's mobile device management (http://www.air-watch.com; (https://sogconsole.awmdm.com/AirWatch/Loginservice) provides a way to manage and secure mobile devices, while giving the agencies the flexibility to use them in whatever ways they see fit. The tool offers, but is not limited to, numerous features such as wiping a device if lost

or stolen, implementing a PIN-lock standard, enforcing compliance policies on the devices, and managing mobile applications and content.

A common misunderstanding of what AirWatch MDM does is that it provides a "pathway" to transfer Microsoft Exchange email from the server to the device, similar to the way BlackBerry worked. Establishing a BlackBerry account on the BES was the only way a user could receive email access on a BlackBerry device. No BES account, no email. This is not the case with AirWatch.

So what does AirWatch do? It collects certain types of information from the device and enacts controls based on policies determined by each agency. Once a device is enrolled, AirWatch uses Application Programming Interfaces (APIs) provided by Apple, Google, and Microsoft to collect information and cause or prevent specific behaviors on the device.



Current mobile operating systems use a native **Microsoft Exchange Email** protocol called **Activesync** to synchronize email, calendar and contacts directly between the server and the device. Users have the ability to configure their mobile device's email app to do this on their own. The state uses AirWatch to manage the device, not the flow of email. Through rules and profiles, the **Secure Email Gateway (SEG**) prevents unauthorized, non-compliant devices from accessing email. (An agency's AirWatch console administrator provides enrollment instructions to unauthorized users once they're identified.) AirWatch does not actually transmit state of Georgia email through its servers or data center, nor does it have the ability to see the email content.

AirWatch **profiles** are also used to activate device features. For example, if agency policies require devices to have native encryption enabled, AirWatch can determine which devices are out of compliance and define an action for AirWatch to bring non-compliant devices into compliance.

The agency's console administrator chooses between setting up user accounts under "Basic" or "Active Directory." Basic accounts are created with a user name and password chosen by the admin. Active Directory accounts use the **Cloud Connector** to pull user data from Active Directory. The benefit to using Active Directory accounts is that an account is deleted automatically when a user is removed from the directory, as when an employee leaves an agency.

The administrator has the ability to view real-time data such as device type and serial numbers, amount of data transferred to and from the device and last synched events, OS levels and whether it has been compromised, and amount of data transferred. All of this is displayed to an agency console administrator through dashboards and reports. (See page 11 for examples.)

In addition to defining their own policies and controls, agencies have the ability to configure AirWatch *not* to collect certain types of information if they wish. This could be to extend privacy to "Bring Your Own Device" users, or it could be to avoid collecting information the agency does not want retained either by its own console admins or by AirWatch. Again, the MDM service is architected so that it cannot collect the contents of email or other information that could be deemed regulated content like Personal Health Information. The additional privacy controls are to avoid collecting non-content information like the names of the apps loaded on the device. Please refer to the spreadsheet on page 9 for a description of the privacy controls available to the agencies.

AirWatch Roles and Responsibilities

It is important to note some elements of the AirWatch MDM service that differ from other GETS services like BlackBerry support or email. The AirWatch implementation is designed to delegate control to each agency over its own settings and policies using AirWatch's web console. Download the Roles and Responsibilities document.

Highlights:

- By default, AirWatch does not change anything on the devices or add any security. Agencies must activate any of the controls they need in the AirWatch console.
- GTA will not enable or require any enterprise controls. Each agency is responsible for its own.
- As always, it is the agencies' responsibility to assure compliance with state policies and with their own unique regulatory requirements. AirWatch's ability to assure compliance will depend on the settings an agency enables. There may be a few agency use cases that require more security than AirWatch is designed to provide. In those cases, agencies should consult with GTA to determine what other kind of solution would be appropriate.
- GTA is making available to the agencies training, documentation and support resources to help assure effective use of AirWatch.

GTA Recommendations

GTA has developed the following recommendations from its initial experiences working with AirWatch and the agencies. Some training and familiarity with AirWatch basics will be needed to understand the recommendations. There are many different ways to do things in AirWatch, and these recommendations reflect what GTA has seen work best.

Summary:

- Enroll by email address, letting AirWatch automatically create the AirWatch user accounts.
- Install the AirWatch app on the devices, and enroll inside the app.
- For iOS users who don't have iTunes accounts, enroll using the website instead of the app.
- Avoid duplicating a Basic account with a Directory account for the same user.
- If using Basic accounts, when an employee turns in his/her device(s), delete the account from the AirWatch console.

User Accounts

New Accounts

There is no need to manually create user accounts in the AirWatch portal, if you enroll your devices using the end user's email account. This uses what AirWatch calls their Cloud Connector feature, which integrates with our Active Directory. When enrolling in that way, AirWatch will automatically create a Directory account for each user, with their email address as their AirWatch user name and their Exchange password as their AirWatch password. Later, if you un-enroll all of a user's devices, AirWatch will automatically delete that user account.

The only disadvantage of this method is that if you want to classify your users in groups (see next section), the console admin will need to log in after the user has enrolled and add the new user account to the relevant groups. Using Basic accounts requires more up-front work, but it lets you put the users in groups at the time you create them.

If you have already created some Basic user accounts, you do not need to change them to Directory accounts. However, GTA has found on occasion that it's best not to have duplicate accounts for the same user. So if you have users with Basic accounts who begin adding more devices using their email address (Directory Accounts), you will probably want to delete their Basic accounts.

Groups

Console admins can create user groups within AirWatch as needed to keep asset groups separately or to enforce different policies on different groups. Additionally, AirWatch can take advantage of any Active Directory groups you have set up. The benefit of using AD groups is that when users self-enroll they will automatically be placed into the correct groups. However, to be effective the use of AD groups requires

that newly hired employees get assigned properly to their groups. Most agencies expressed a preference for having direct control rather than relying on the new employee boarding process.

If an agency would like to use AD groups, it can submit a standard IMAC request identifying the name of the new group and specifying the users who should be placed in it. Then each time a new employee boarding request is submitted, the agency would specify in the OrderNow! request which AD groups the new employee should be assigned to.

Enrolling Devices

Some agencies will want to have mobile devices enrolled in AirWatch by central individuals with experience and training, while others will want to issue instructions and rely on each end user to self-enroll. GTA has created a set of end user instructions agencies can use if they wish.

While there are several ways to enroll devices, GTA recommends agencies choose one of two that seem to work the best. Both of these assume the agency is using Directory accounts automatically set up at the point of enrollment.

1) Download the app onto the device and enter the user's email address. The app will also request the user's Exchange user name and password, but no other information will be required.
2) From the AirWatch web console, the console admin can initiate an email to the end user that includes a link to a website. On the device, the user clicks the link in the email and is directed to a website where email address and Exchange credentials are entered. *Note that this only works if the user's email account is already set up on the device.*

Specifically for Apple iOS devices, you may have some users who do not wish to have an iTunes account. Those users will not have access to the App Store and will not be able to download the AirWatch app. Instead, they can navigate their mobile web browsers to sog.awmdm.com, enter their agency abbreviation as the Group Name, and then enroll using their Exchange user name and password.

Eliminating Devices

When you decommission a device, you should also un-enroll it from AirWatch. This removes it from the state's AirWatch billing and helps manage costs properly. GTA has created instructions for un-enrolling devices either at the device or using the AirWatch console. Un-enrolling a device does not wipe the data from it. It simply removes it from the AirWatch MDM service.

Adding Devices to AirWatch

These instructions apply to both Android and iOS devices. Because of the variety of Android handset manufacturers and different versions of the Android OS, Android phones behave slightly differently from each other, and you'll see that reflected in some of the steps.

1. In the Google Play store or Apple App store, find and install a free app called "AirWatch MDM Agent."
2. Launch the app.
3. For some Android devices, you may be asked to accept permissions to allow an application that's not from the Google Play store. This is fine, and you should allow the app to take you to the menu to accept the long list of permissions you're granting to AirWatch. If your Android device doesn't make this obvious, here's some help:
    - For Samsung devices, go to the home screen and press the Menu button at the bottom of the screen. Choose Settings, then Security, then Applications. There's a check box on the next menu for Allow 3rd Party Applications.
    - For Motorola devices, go to the home screen and press the Menu button at the bottom of the screen. Choose Settings, then Security. There's a check box on the next menu for Allow 3rd Party Applications.
4. Enter the following Device Services URL: https://sog.awmdm.com.
5. Enter your agency's Group ID: (Each agency has a unique Group ID, and these are kept by the Agency Mobility Focals who administer AirWatch.)
6. Click Enroll.
7. Next you will be asked to enter the following:
    - User Name = (see agency focal)
    - Password = (see agency focal)
8. You may (or may not) be prompted to press "Enroll" or "Activate," and that is fine.
9. When finished, you'll be left on the main screen of the AirWatch app, with no further prompts. You may return to your device's home screen and you're now enrolled in AirWatch.

Removing Devices from AirWatch

The instructions below will help you remove devices from AirWatch without wiping any email or other content from them. You may un-enroll either on the device or by using the AirWatch console, but you do not need to do both.

Google Android

GTA's experience with Android devices has been that you will need to install the AirWatch app in order to enroll. You may un-enroll a device by either removing the app or by using an un-enroll button inside the app. Also, note that there are some differences among Android OS versions and handset behaviors, so these instructions may not perfectly fit all devices.

Un-Enroll by removing the AirWatch App

1. Go into Settings
2. Go to Apps
3. Select AirWatch Agent and choose Uninstall

   If the app does not uninstall, please follow these additional steps, which some Android devices require:

4. Go to Settings
5. Go to Security
6. Go into Device Administrators
7. Deselect AirWatch
8. Then Apps (from Settings)

Un-Enroll inside the AirWatch app

This method will un-enroll the device from AirWatch but leave the app installed on the phone for future use.

1. Click on the AirWatch app (icon)
2. Depending on which Android version you are running, you may need to do either of the following:
   - Click on the page icon next to the home button on the Android (possible bottom left) – click un-enroll
   - Or click on the row of bullets (probably top right corner) and select UN-ENROLL

Apple iOS

Enrolling iOS devices can be accomplished with or without the AirWatch app. Deleting the AirWatch app does not un-enroll the device from AirWatch. To un-enroll a device:

1. From the iOS home screen, go to the Settings icon
2. Go to General
3. Go to Profiles
4. Select MDM Profile and click on Remove
5. If the AirWatch app is installed on the device, you may delete it from the home screen by pressing and holding the icon until it "wiggles." Then press the "x" on the icon to delete it. Note that deleting the app does *not* un-enroll the device.

Using the AirWatch Web Console to Un-Enroll a Device

1. Click on (User) Accounts
2. Click on List View

3. Select the user
4. Click on the drop down arrow (top right of the user) and select Deactivate
   (NOTE: To enroll this user again… this user must be re-activated.)

AirWatch Console Template

This spreadsheet is a planning document that describes all of the MDM controls available via AirWatch to each agency. GTA recommends that each agency go through the template and check the policies or controls it wants to activate. The agency's console admin can then use the document as a guide in setting up the agency's console. The spreadsheet can also serve as a reference document to inform other stakeholders of which controls are in place. Download the AirWatch Console Template.

AirWatch – Common Challenges

Users have been challenged by the following distinctions and procedures when using AirWatch:

1. What is the difference between Device Wipe and Enterprise Wipe?
   - Enterprise Wipe will remove everything that has to do with AirWatch from the device.
   - Device Wipe will automatically erase everything on the device, returning it to factory default settings.
     NOTE: The mobile device in the SOG AirWatch console must be set to corporate mode.

2. What is the difference between Basic Account and Directory Account when enrolling devices in AirWatch?
   - Directory accounts use the GETS Active Directory infrastructure and the user's email address to create accounts in AirWatch.
     These accounts are removed automatically from AirWatch when the user is no longer employed by the state.
   - Basic accounts have to be created and maintained manually by the agency AirWatch admin.

3. How can you check to see what devices are using state government email, but not currently enrolled in AirWatch?
   - This is a report that can only be generated by GTA at the enterprise level. Please send the request to Willie Phillips (willie.phillips@gta.ga.gov) and he will respond within one to two business days.

4. How do you resolve issues arising when a device has not checked in with the AirWatch Console for a number of days? For instance maybe 22 or 46 days for non-connectivity?
   - You may have to un-enroll the device from AirWatch, possibly even removing the app, then re-install the app and re-enroll the device.

Troubleshooting

End users should contact their agency's Mobility Focal for help with any issues with the mobile device itself. For assistance in resolving potential AirWatch issues or problems with the GETS email infrastructure, please contact GTA's Consolidated Service Desk at 877.GTA.3233 (877.482.3233.)

Ordering

All current GETS agencies have their own environments set up in AirWatch, and their console admins have been trained. There is no need to "order" AirWatch. Agency console admins will enroll devices as needed. For new agencies that might need to be set up for the first time, please contact your GTA Customer Relationship Manager (CRM) for assistance.

Pricing

The costs for AirWatch have been rolled into the GETS enterprise costs, which are spread across all GETS agencies. The costs are part of a Resource Unit on your bill called "LAN Attached Devices." That Resource Unit contains a number of other costs as well, and they're allocated based on the total employee count in your agency. As a result, agencies do not see a specific line item for AirWatch, and an agency's costs do not directly reflect the number of devices that agency enrolls. This is different from most other GETS services, which are more directly consumption-based. It was set up this way because it reflects the way we were already paying BlackBerry costs, and GTA is managing the costs downward as the newer technology replaces the old. GTA worked to avoid having budget constraints deter agencies' adoption of mobile device management. As of this writing, the LAN-Attached Devices rate is lower than it was before AirWatch implementation began. That could change over time with significant growth in the total number of mobile devices, but GTA anticipates having the chance to reevaluate the price model in the future.

Additional Documents

The following links take you to the AirWatch console (login credentials required).

Mobile Content Management (MCM) Guide
https://resources.air-watch.com/view/j5skz5nxsl79kmp3932d/en

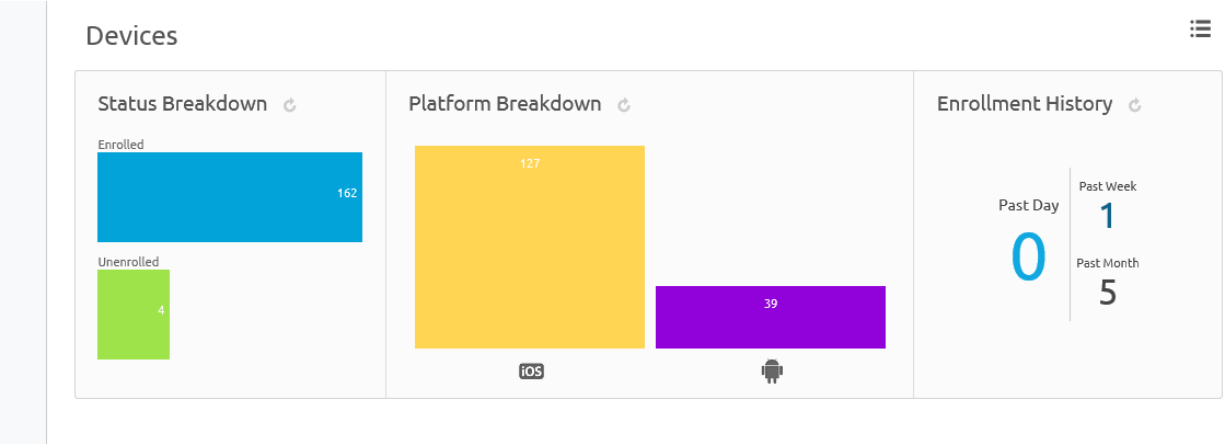
AirWatch Data Types Stored and Privacy Information
https://resources.air-watch.com/view/m38lm7tzvbfxjtv3kbc6/en

AirWatch Mobile Security and HIPPA Compliance
https://resources.air-watch.com/view/qv7tcyhfkq9b6zmtgm5q/en

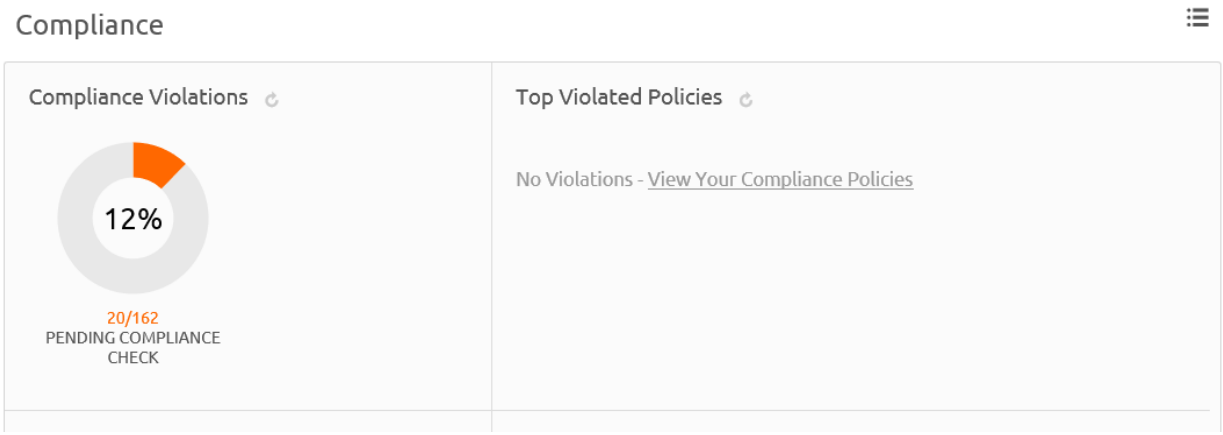
Sample AirWatch Data and Dashboards

The following screenshots provide a glimpse into the type of information AirWatch captures:

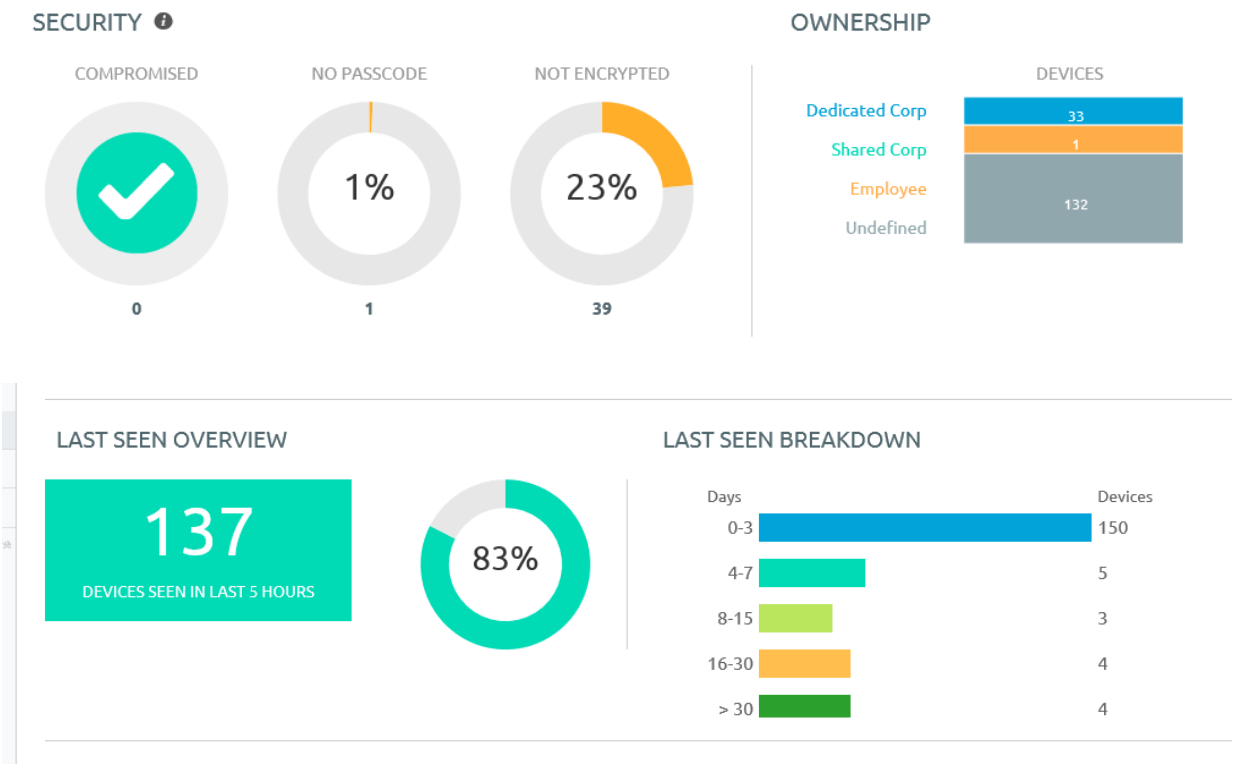
AirWatch Hub



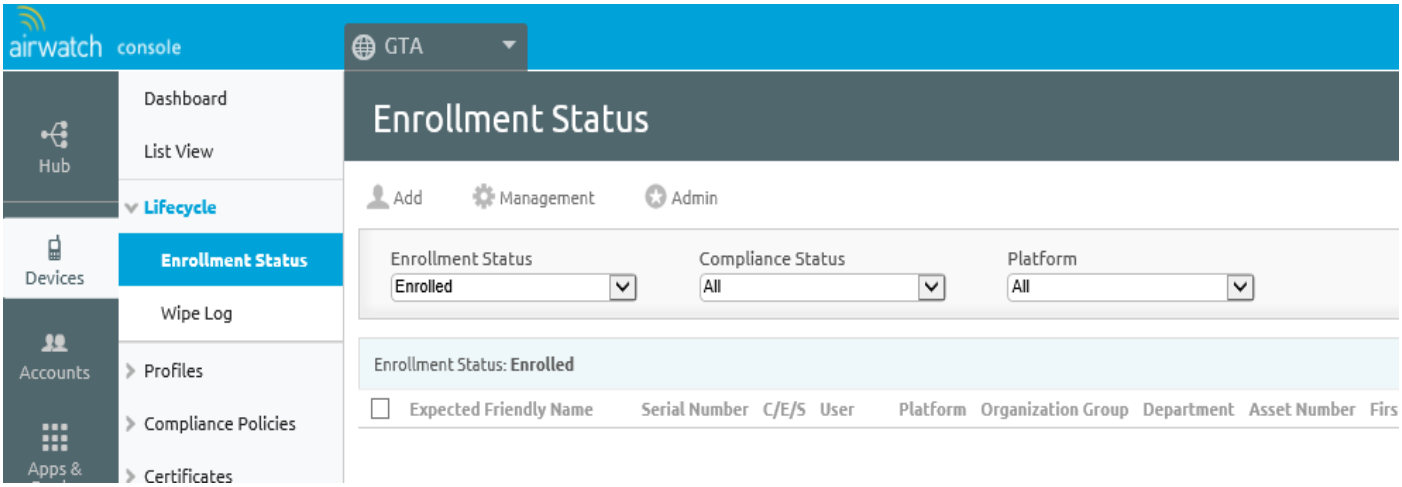
Compliance

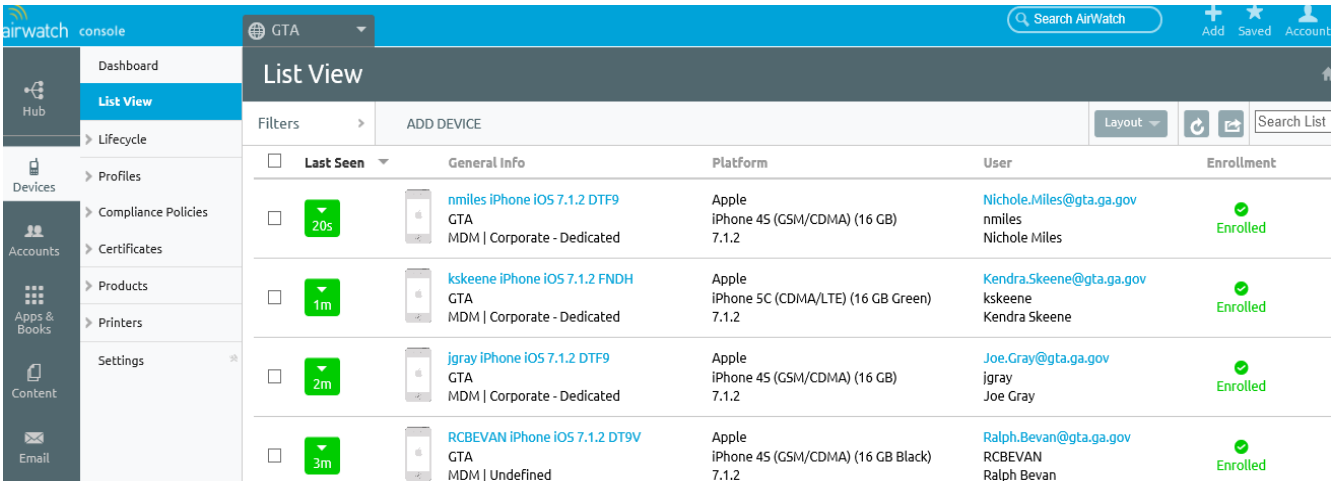


Dashboard



Devices


airwatch console
GTA
Dashboard
List View
Lifecycle
Enrollment Status
Wipe Log
Profiles
Compliance Policies
Certificates
Hub
Devices
Accounts
Apps &
Enrollment Status
Add
Management
Admin
Enrollment Status
Enrolled
Compliance Status
All
Platform
All
Enrollment Status: Enrolled
Expected Friendly Name
Serial Number
C/E/S
User
Platform
Organization Group
Department
Asset Number
Firs


airwatch console
GTA
Search AirWatch
Add
Saved
Account
Dashboard
List View
Lifecycle
Profiles
Compliance Policies
Certificates
Products
Printers
Settings
Hub
Devices
Accounts
Apps & Books
Content
Email
List View
Filters
ADD DEVICE
Layout
Search List
Last Seen
General Info
Platform
User
Enrollment
20s
nmiles iPhone iOS 7.1.2 DTF9
GTA
MDM | Corporate - Dedicated
Apple
iPhone 4S (GSM/CDMA) (16 GB)
7.1.2
Nichole.Miles@gta.ga.gov
nmiles
Nichole Miles
Enrolled
1m
kskeene iPhone iOS 7.1.2 FNDH
GTA
MDM | Corporate - Dedicated
Apple
iPhone 5C (CDMA/LTE) (16 GB Green)
7.1.2
Kendra.Skeene@gta.ga.gov
kskeene
Kendra Skeene
Enrolled
2m
jgray iPhone iOS 7.1.2 DTF9
GTA
MDM | Corporate - Dedicated
Apple
iPhone 4S (GSM/CDMA) (16 GB)
7.1.2
Joe.Gray@gta.ga.gov
jgray
Joe Gray
Enrolled
3m
RCBEVAN iPhone iOS 7.1.2 DT9V
GTA
MDM | Undefined
Apple
iPhone 4S (GSM/CDMA) (16 GB Black)
7.1.2
Ralph.Bevan@gta.ga.gov
RCBEVAN
Ralph Bevan
Enrolled