Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Mobile Applications with MobileIron Virtual Smartphone Platform - Issue 1.0

Abstract

These application notes describe the steps required for Avaya Mobile Activity Assistant, Avaya Flare Communicator and various Avaya one-X Mobile clients installed on Apple iPad, Apple iPod touch and Samsung Galaxy Tab to be managed by MobileIron Virtual Smartphone Platform.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps required for Avaya Mobile Activity Assistant, Avaya Flare Communicator and various Avaya one-X Mobile clients installed on Apple iPad, Apple iPod touch and Samsung Galaxy Tab to be managed by MobileIron Virtual Smartphone Platform.

The MobileIron Connected Cloud solutions are a subscription-based SaaS (Software as a Service) where the MobileIron Virtual Smartphone Platform (VSP) is hosted on it. The MobileIron VSP is where the customer manages their devices.

The **MobileIron VSP** is the first solution to combine data-driven smartphone and tablet management with real-time wireless cost control. It provides visibility into what's on a smartphone and how it's being used, letting both IT and users better secure data and control costs without compromising privacy, even on employee-owned phones.

2. General Test Approach and Test Results

The general test approach was to verify interoperability between Avaya Mobile Applications and MobileIron VSP. Interoperability compliance testing was performed remotely between the Avaya DevConnect Lab and MobileIron VSP via the public internet. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

This section describes the interoperability compliance testing between Avaya Mobile Applications installed on Apple iPad, Apple iPod touch and Samsung Galaxy Tab and MobileIron Virtual Smartphone Platform. This section covers the general test approach and the test scenarios.

- Register to required Wi-Fi connections
- Acquire mandatory username and password credentials needed for MobileIron Portal
- Register each device with MobileIron Virtual Smartphone Platform (VSP)
- Install MobileIron MyPhone@Work Client
- Configure each device with login credential provided by MobileIron
- Verify devices are registered by logging into MobileIron Mobile Smartphone Manager Portal.
- Verify device and inventory information in the MobileIron Smartphone Manager Portal.

- In the MobileIron MyPhone@Work client, install mobile applications from App Storefront.
- Verify applications were installed on each device from the MobileIron Smartphone Manager Portal.
- Application Security Testing
    - Install application that violates security policy.
    - Application Control -Verify proper alerts and application removal from MobileIron
- Verify Avaya mobile application functionality.
    - Register applications to Avaya equipment
    - Perform inbound/outbound call testing where applicable
- Verify connectivity loss between devices and MobileIron has no impact on Avaya application functionality.

2.2. Test Results

Interoperability testing of MobileIron Virtual Smartphone Platform was completed with successful results for all test cases.

2.3. Support

or technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on MobileIron Virtual Smartphone Platform, contact MobileIron at www.mobileiron.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration where devices in the Avaya DevConnect Lab are connected over the public internet to the MobileIron VSP via a MobileIron Connected Cloud. Located at the DevConnect Lab were Apple iPad, Apple iPod touch and Samsung Galaxy Tab and Avaya network equipment.

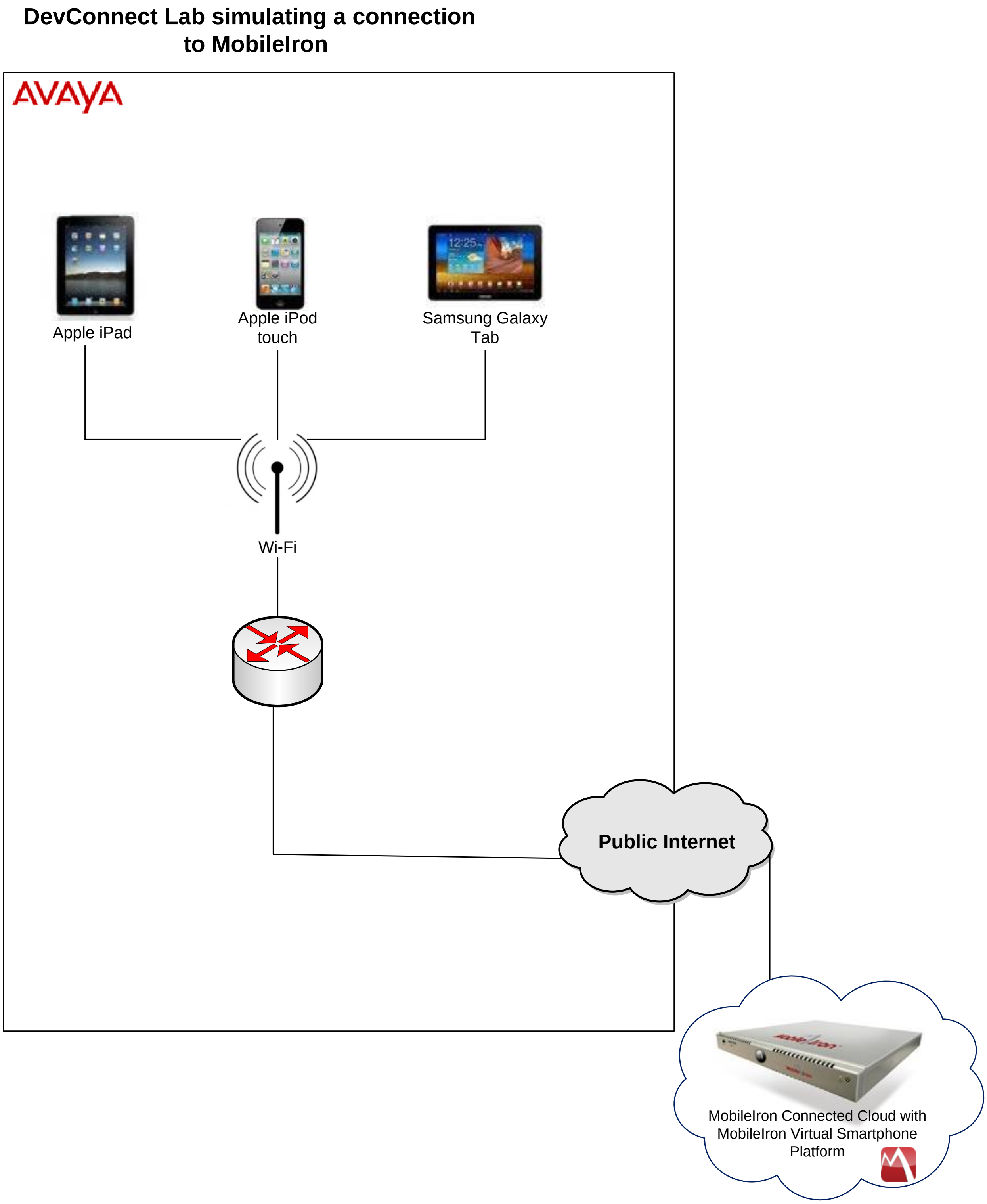

DevConnect Lab simulating a connection to MobileIron
AVAYA
Apple iPad
Apple iPod touch
Samsung Galaxy Tab
Wi-Fi
Public Internet
MobileIron Connected Cloud with MobileIron Virtual Smartphone Platform

Figure 1: Avaya DevConnect Network connected to MobileIron

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya one-X Mobile SIP	1.0.5
Avaya Mobile Activity Assistant	1.0.1
Avaya one-X Mobile 6.1 - iOS Avaya one-X Mobile 6.1 - Android	6.1.6.1.7 6.1.0.372
Avaya Flare Communicator	1.0.1
Avaya one-X Mobile for IPO	0.0.1
Mobile Devices • Apple iPod Touch • Apple iPad2 –MC916LL • Samsung Galaxy Tab- GT-P7510	 5.1 5.1 P7510UEKMP
MobileIron Solution Components	
MobileIron Virtual Smartphone Platform Installed on “off the shelf” high performance servers as a virtual machine utilizing VMWare ESXi	4.5.3 Build 98 (Branch r4.5.3)
MobileIron MyPhone@Work Client	4.5.12

Table 1: Equipment and Software

5. Configure devices to register with MobileIron Virtual Smartphone Platform

This section describes the configuration necessary to establish connectivity to MobileIron Virtual Smartphone Platform from mobile devices through MyPhone@Work Client. MyPhone@Work Client is the employee's interface to MobileIron, and operates in conjunction with the VSP.

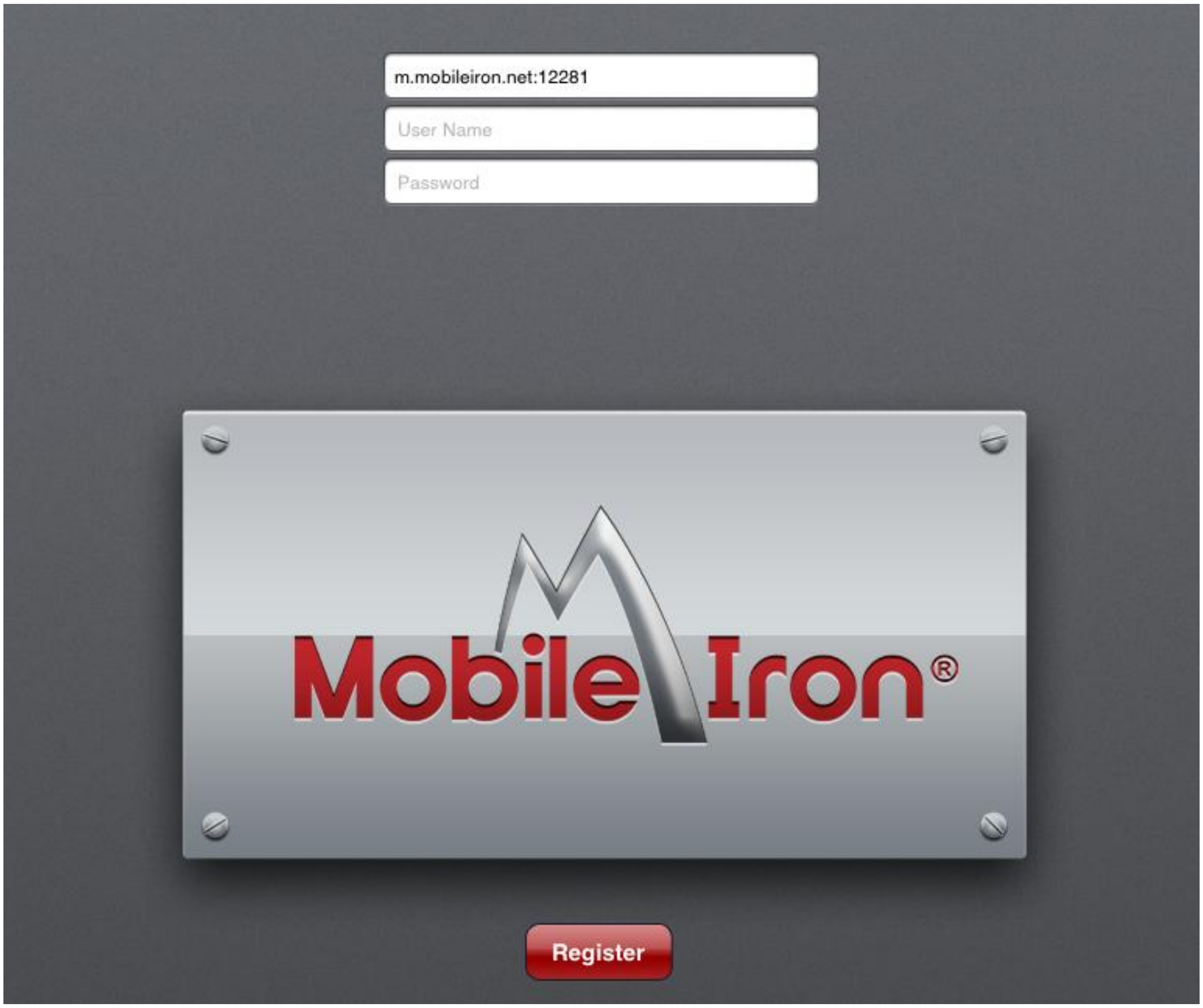
Prior to downloading MobileIron Client, establish internet access on each device via Wi-Fi connection. This connection must be able to access each network needed for testing. (e.g. Avaya, MobileIron and Public Internet)

5.1. Download & Install MobileIron Client

Each device must download and install MobileIron application, **MyPhone@Work Client**. Apple devices can download this application from the App Store and Samsung devices can download this application from the Android Market.

5.2. Registration

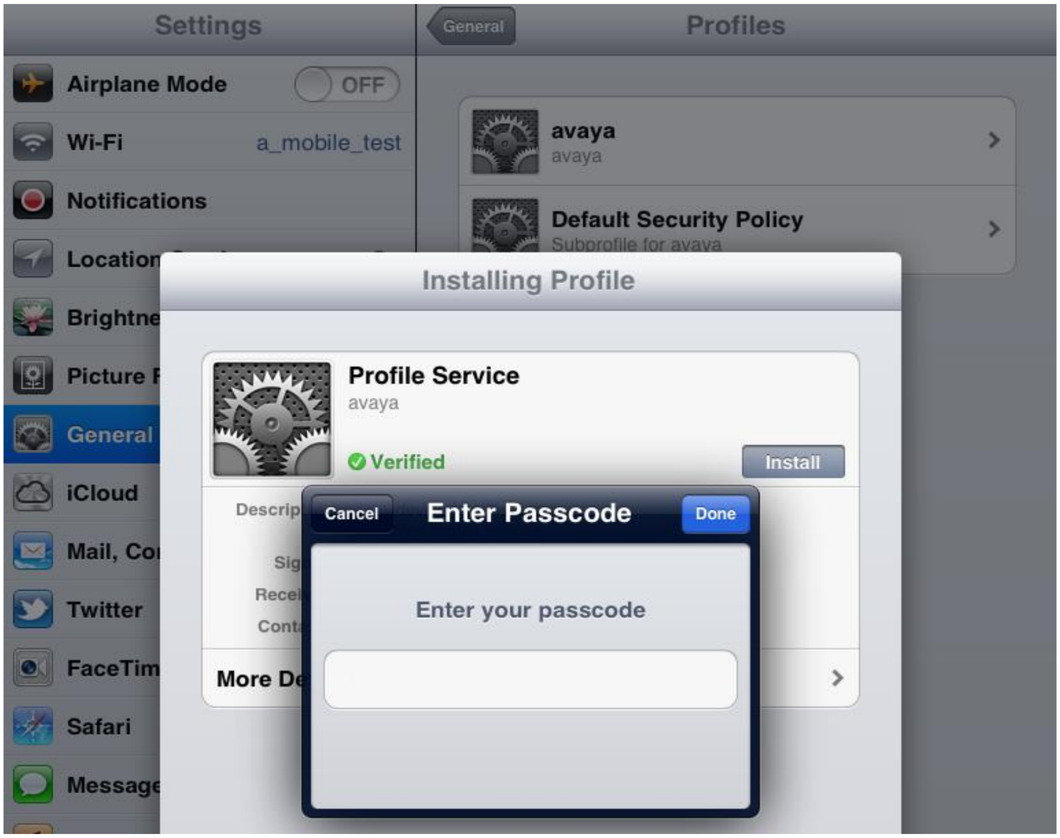
Launch MyPhone@WorkClient from the device. Enter **Server Address** (e.g., m.mobileiron.net:12281) of the Virtual Smartphone Platform provided by MobileIron, and then **User Name** and **Password** fields will appear. Enter in credentials and click on **Register**. See **Figure 2** as reference**.**



m.mobileiron.net:12281

Figure 2: MyPhone@Work Registration

After registering, a pop up window will be displayed advising there will be an update to the configuration. Select **OK**, then the **Installing Profile** screen will appear. Profile Service allows MobileIron VSP to control the smart device. Enter **passcode** to accept the profile service and settings.

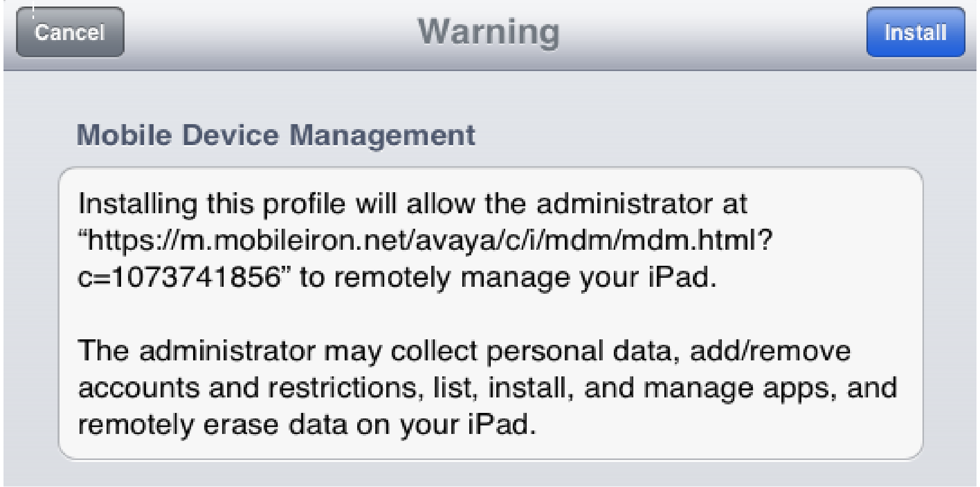


Airplane Mode OFF

Wi-Fi a_mobile_test

Figure 3: Profile Service

After entering the passcode a Warning Screen for Mobile Device Management will appear. Click **Install** and then **Done,** once it's completed.



Mobile Device Management

Installing this profile will allow the administrator at "https://m.mobileiron.net/avaya/c/i/mdm/mdm.html?c=1073741856" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.

Figure 4: Warning – Mobile Device Management

After entering the correct credentials and registering access to MobileIron, the device will now be secured and managed by MobileIron. Access to Camera and YouTube are disabled.

The following screen will be displayed. This will give you access into MobileIron App Storefront.

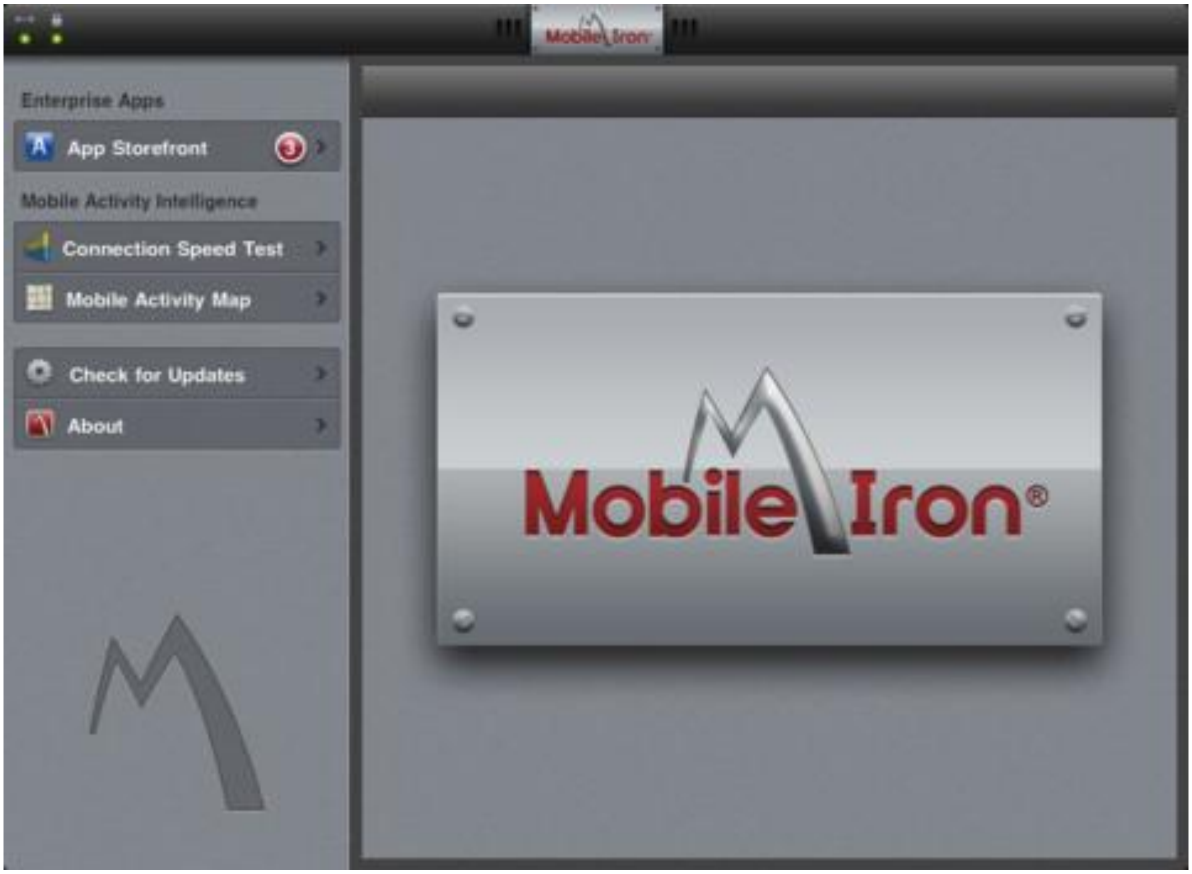


Figure 5: MobileIron Portal

6. Install Enterprise Recommended Applications

MobileIron's App Storefront has the applications an enterprise administrator has selected for each enterprise user to have access to. The applications listed are the enterprise recommended applications. An enterprise administrator has the ability to send remediation message via email and/or push to the smart device informing the user that they do not have a required application installed and what that application is. From the screen in **Figure 5** click on **App Storefront** on the top left.

The applications available for downloading and installing will be listed under Apps@Work. Click on the desired application. Once it opens, select install. See **Figure 6** below.

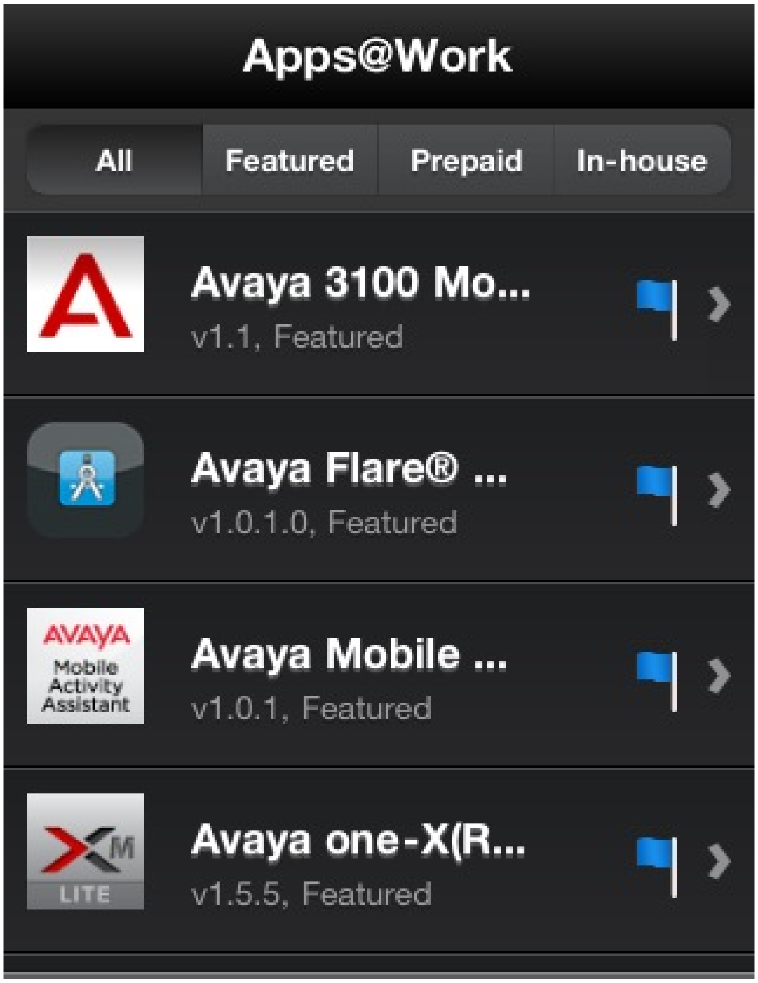


Figure 6: Apps@Work

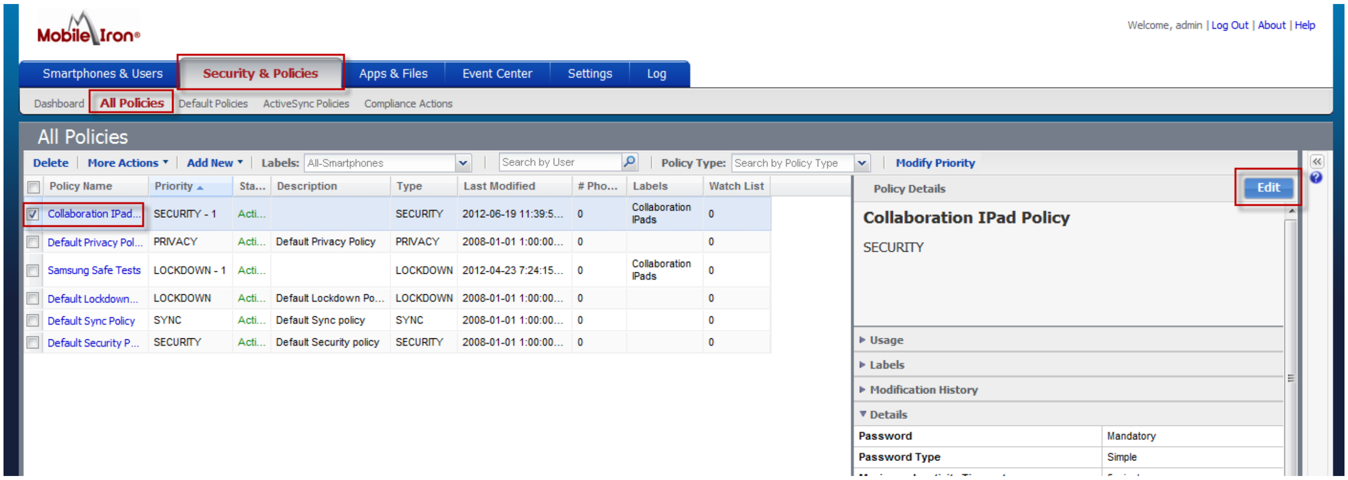
7. Configure MobileIron Smartphone Virtual Platform - Application Security

These Application notes do not provide steps to fully implement the MobileIron Virtual Smartphone Platform. In addition, there are different settings and configurations that can be used depending on the requirements. For complete installation information please contact MobileIron

7.1. Security Policy Configuration

An Administrator can set different levels of security for each user and device type. Navigate to **Security & Policies → All Policies.** Select **Collaboration IPad Policy**. Then click **Edit** on the right side menu.

Note: **Collaboration IPad Policy** was created for this compliance testing. To create a new policy select the **Add New** drop-down menu.



All Policies

Labels: All-Smartphones

Policy Type: Search by Policy Type

☐	Policy Name	Priority	Sta...	Description	Type	Last Modified	# Pho...	Labels	Watch List
☑	Collaboration IPad...	SECURITY - 1	Acti...		SECURITY	2012-06-19 11:39:5...	0	Collaboration IPads	0
☐	Default Privacy Pol...	PRIVACY	Acti...	Default Privacy Policy	PRIVACY	2008-01-01 1:00:00...	0		0
☐	Samsung Safe Tests	LOCKDOWN - 1	Acti...		LOCKDOWN	2012-04-23 7:24:15...	0	Collaboration IPads	0
☐	Default Lockdown...	LOCKDOWN	Acti...	Default Lockdown Po...	LOCKDOWN	2008-01-01 1:00:00...	0		0
☐	Default Sync Policy	SYNC	Acti...	Default Sync policy	SYNC	2008-01-01 1:00:00...	0		0
☐	Default Security P...	SECURITY	Acti...	Default Security policy	SECURITY	2008-01-01 1:00:00...	0		0

Policy Details

Collaboration IPad Policy

SECURITY

Password	Mandatory
Password Type	Simple

Figure 7: Collaboration IPad Policy

For compliance testing the following were selected or set:

Password:

- Password – **Mandatory**
- Minimum password length – **6**
- Maximum Inactivity Timeout – **5 minutes**

Data Encryption:

- Device Encryption – **On; ;l**
- Data Type – **All**
- File Type – **All**
- SD Card Encryption – **On**

Access Control:

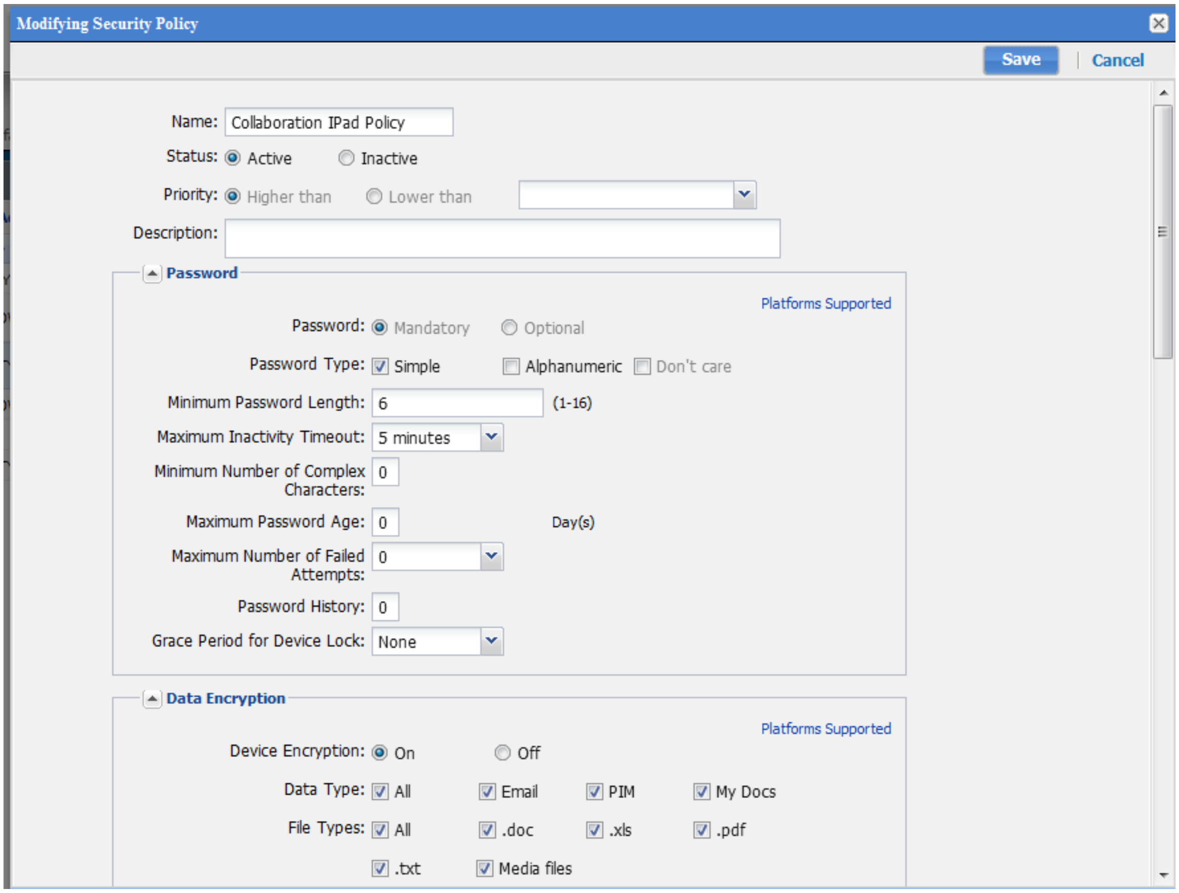
- **Send Alert** when device has not connected to MobileIron in **5** days
- **Block ActiveSync and Send Alert** when a policy has been out of date for **5** days.
- **Quarantine and Send Alert** when a device violates following App Control rules:
  - Rule Type: Required – Enabled: **Avaya Mobile Activity Assistant**
  - Rule Type: Disallowed – Enabled: **No Angry Birds**

For iOS Devices

- **Send Alert** when iOS version is less than **5.0**
- **Quarantine and Send Alert** when a compromised iOS device is detected
- **Send Alert** when device MDM is deactivated (iOS 5.0 or higher)

For Android devices

- **Send Alert** when Android version is less than **2.3**
- **Quarantine and Send Alert** when a compromised Android device is detected
- **Send Alert** when Data Encryption is disabled
- **Send Alert** when device administrator is deactivated



Name: Collaboration IPad Policy

Status: ● Active ○ Inactive

Priority: ● Higher than ○ Lower than

Description:

Password

Password: ● Mandatory ○ Optional

Password Type: ☑ Simple ☐ Alphanumeric ☐ Don't care

Minimum Password Length: 6 (1-16)

Maximum Inactivity Timeout: 5 minutes

Minimum Number of Complex Characters: 0

Maximum Password Age: 0 Day(s)

Maximum Number of Failed Attempts: 0

Password History: 0

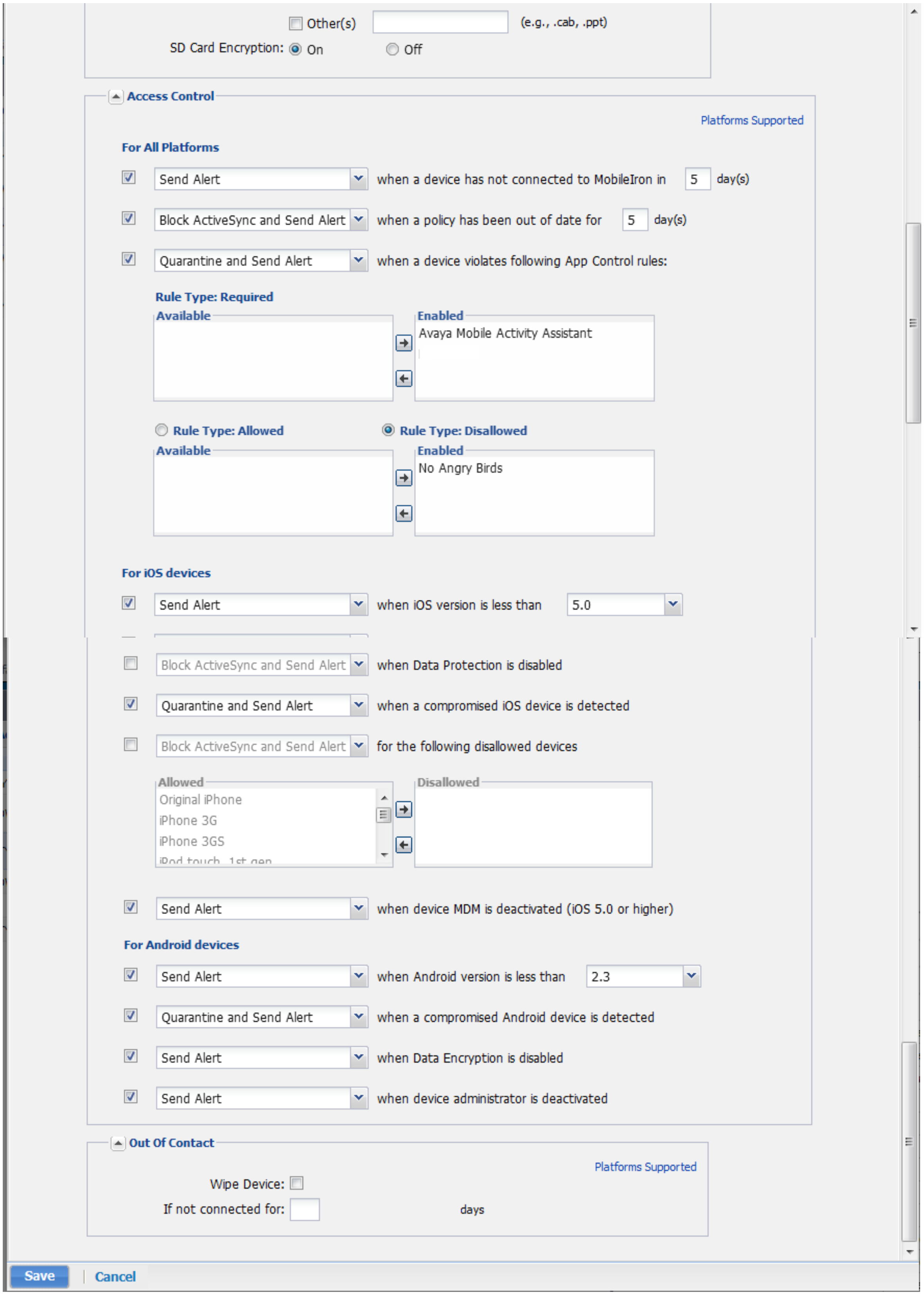
Grace Period for Device Lock: None

Data Encryption

Device Encryption: ● On ○ Off

Data Type: ☑ All ☑ Email ☑ PIM ☑ My Docs

File Types: ☑ All ☑ .doc ☑ .xls ☑ .pdf ☑ .txt ☑ Media files



□ Other(s) (e.g., .cab, .ppt)

SD Card Encryption: ● On ○ Off

Access Control

Platforms Supported

For All Platforms

☑ Send Alert when a device has not connected to MobileIron in 5 day(s)

☑ Block ActiveSync and Send Alert when a policy has been out of date for 5 day(s)

☑ Quarantine and Send Alert when a device violates following App Control rules:

Rule Type: Required

Available	Enabled
	Avaya Mobile Activity Assistant

○ **Rule Type: Allowed** ● **Rule Type: Disallowed**

Available	Enabled
	No Angry Birds

For iOS devices

☑ Send Alert when iOS version is less than 5.0

□ Block ActiveSync and Send Alert when Data Protection is disabled

☑ Quarantine and Send Alert when a compromised iOS device is detected

□ Block ActiveSync and Send Alert for the following disallowed devices

Allowed	Disallowed
Original iPhone iPhone 3G iPhone 3GS iPod touch 1st gen	

☑ Send Alert when device MDM is deactivated (iOS 5.0 or higher)

For Android devices

☑ Send Alert when Android version is less than 2.3

☑ Quarantine and Send Alert when a compromised Android device is detected

☑ Send Alert when Data Encryption is disabled

☑ Send Alert when device administrator is deactivated

Out Of Contact

Platforms Supported

Wipe Device: □

If not connected for: days

Figure 8: Security Policy

7.2. Notification of Violation of App Control Policy

When a device violates the App Control Security Policy, notifications and warnings are displayed and alerts are sent out. The Smartphone Virtual Platform displays the violation under the ‘All Smartphones’ section. Reference **Figure 9** below.

The Administrator receives an alert informing them the device has violated security and the end users receive an email and/or a text message to the device informing them they are violating security. An example could be having a disallowed application that needs to be removed. Access to the MobileIron Storefront is locked until the device is back into compliance.

The following is an example of email notifications sent to the end user:

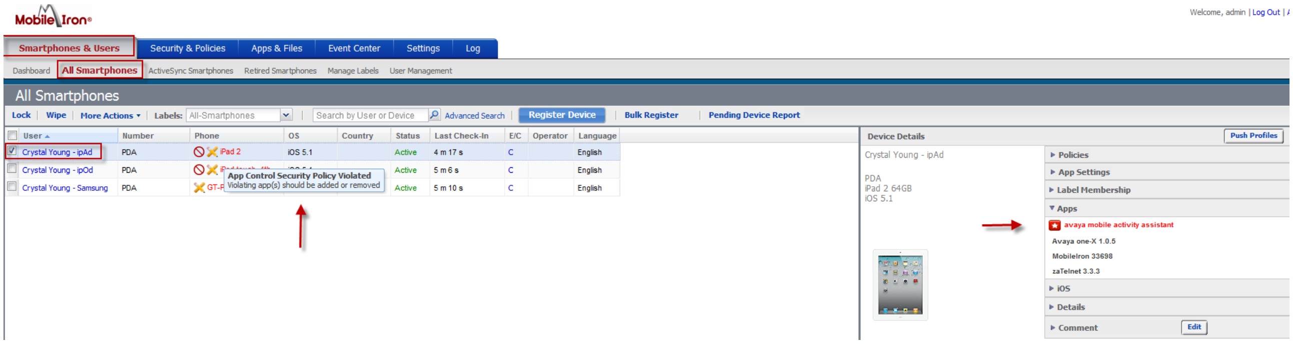
```
Email notifications sent:

WARNING::PDA (ipAd) Disallowed Application(s) found: No Angry Birds:Angry Birds
Please note that all required applications can be installed from the MobileIron
Client

WARNING::PDA (Samsung) Data protection/encryption disabled. Please note that all
required applications can be installed from the MobileIron Client

WARNING::PDA (ipOd) Required application(s) not found: Avaya Mobile Activity
Assistant:avaya mobile activity assistant; Please note that all required
applications can be installed from the MobileIron Client
```

Figure 9 below displays the warning for user **Crystal Young - ipAd**. A required application, **avaya mobile activity assistant** was un-installed. The Administrator can view this in the MobileIron Virtual Smartphone Platform by navigating to **Smartphone & Users → All Smartphones** and selecting **Crystal Young – ipAd**.



☐	User	Number	Phone	OS	Country	Status	Last Check-In	E/C	Operator	Language
☑	Crystal Young - ipAd	PDA	iPad 2	iOS 5.1		Active	4 m 17 s	C		English
☐	Crystal Young - ipOd	PDA	[illegible]	[illegible]		Active	5 m 6 s	C		English
☐	Crystal Young - Samsung	PDA	GT-P[illegible]			Active	5 m 10 s	C		English

App Control Security Policy Violated
Violating app(s) should be added or removed

Device Details

Crystal Young - ipAd

PDA
iPad 2 64GB
iOS 5.1

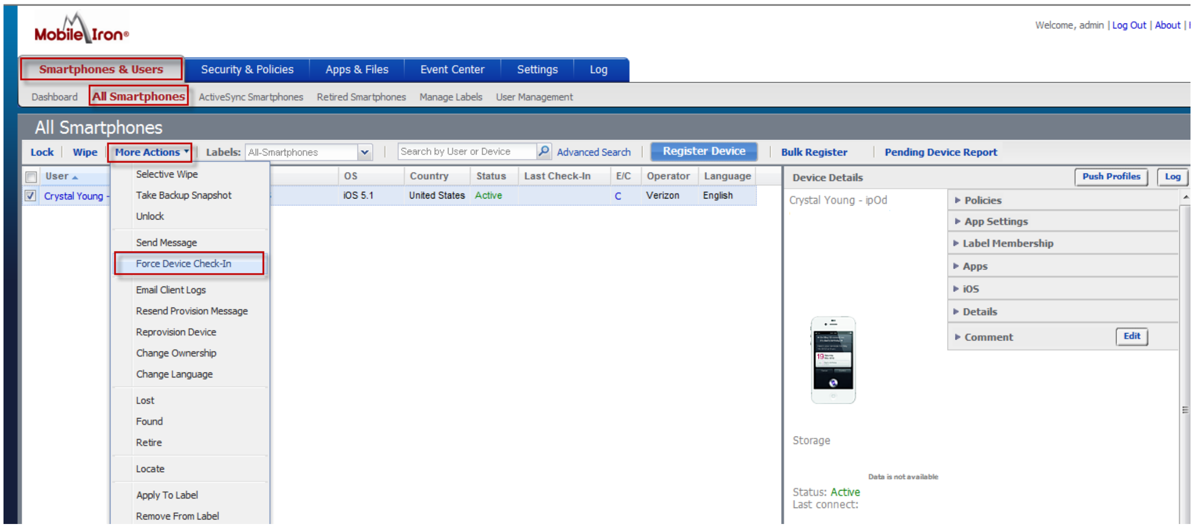
- ▸ Policies
- ▸ App Settings
- ▸ Label Membership
- ▾ Apps
  - avaya mobile activity assistant
  - Avaya one-X 1.0.5
  - MobileIron 33698
  - zaTelnet 3.3.3
- ▸ iOS
- ▸ Details
- ▸ Comment Edit

Figure 9: Security Violation

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

- Verify MobileIron Smartphone Virtual Platform shows each device registered and displays the correct device details.
- Verify MobileIron Smartphone Virtual Platform can sync to the device. Perform a **Force Device Check-In** on each device. Navigate to **Smartphone & Users** → **All Smartphones**. Select **Crystal Young ipOd** and click **More Actions** →**Force Device Check-In**.



User	OS	Country	Status	Last Check-In	E/C	Operator	Language
☑ Crystal Young -	iOS 5.1	United States	Active		C	Verizon	English

Device Details

Crystal Young - ipOd

Storage

Data is not available

Status: Active
Last connect:

Figure 10: Force Device Check-In

- Verify enterprise recommended applications are successfully downloaded.
- Verify correct actions are taken when device violates security policy.
  - MobileIron Storefront access is locked for violating device.
  - Avaya applications are automatically removed on the smart device via MobileIron VSP. Verify the required ones stay installed on the device.
  - Alerts are sent to Administrator and User
- Verify each application is functioning properly.
  - Use credentials to log into Avaya servers and place calls if applicable.
- Verify Avaya applications still function properly when connection to the MobileIron Network is lost.

9. Conclusion

These Application Notes describe the steps used to configure MobileIron Client and MobileIron Virtual Smartphone Platform for downloading Avaya Mobility Applications to various Smartphones and Tablets. Please refer to **Section 2.2** for Test Results.

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

(1) *Avaya one-X for Apple SIP Clients - Administrator guide – March 2012*
(2) *Avaya one-X for Mobile SIP for IOS – User guide – Release 1.0.2 December 2011*
(3) *Avaya one-X Mobile Integration, Administration and Maintenance Guide – Release 5.2 January 2010*
(4) *Avaya one-X Mobile Preferred for IP Office - Administration Guide - 01.02 March 2012*
(5) *Administering Avaya Flare Communicator for iPad Devices – 18-603949 Issue 1 January 2012*
(6) *Using Avaya Flare Communicator for iPad Devices*
(7) *MobileIron Administration Guide - Version 4.5 December 23, 2011*

Product documentation for Avaya products may be found at http://support.avaya.com
Product documentation for MobileIron Virtual Smartphone Platform is available at www.mobileiron.com

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.