© 2017 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and recompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:
Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:
Refer to the Copyright page http://www.checkpoint.com/copyright.html for a list of our trademarks.
Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

Check Point is a registered trademark of Check Point Software Technologies Ltd. All rights reserved. Android and Google Play are trademarks of Google, Inc. App Store is a registered trademark of Apple Inc. iOS is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. AirWatch is a registered trademark of AirWatch, LLC and/or its affiliates.
About This Guide

Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, in SMS messages, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Check Point SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

- Perform advanced app analysis to detect known and unknown threats
- Monitor network activity for suspicious or malicious behavior
- Monitor SMS messages received for malicious URLs
- Assess device-level (OS) vulnerabilities to reduce the attack surface

It uses a variety of patent-pending algorithms and detection techniques to identify mobile device risks, and triggers appropriate defense responses that protect business and personal data.

The Check Point SandBlast Mobile solution ("the Solution") includes the following components:

- Check Point SandBlast Mobile Behavioral Risk Engine ("the Engine")
- Check Point SandBlast Mobile Gateway ("the Gateway")
- Check Point SandBlast Mobile Management Dashboard ("the SandBlast Mobile Dashboard")
- SandBlast Mobile Protect app ("the App") for iOS and Android

In cooperation with an MDM, the SandBlast Mobile Solution provides integral risk assessment of the device to which the MDM can use to quarantine or enforce a set of policies that are in effect until the device is no longer at High Risk. Such policy enforcement could be to disable certain capabilities of a device, such as blocking access to corporate assets, such as email, internal websites, etc., thus, providing protection of the corporation’s network and data from mobile based threats.

This guide first describes how to integrate the Check Point SandBlast Mobile Dashboard with the AirWatch MDM. It provides a quick tour through the interface of the AirWatch Console and the SandBlast Mobile Dashboard in order enable integration, alerting, and policy enforcement.

This includes activation and protection of a new device, malware detection and mitigation (including mitigation flow).

Note: During the procedures in this this document there a quite a few pieces of information that you will need to gather or create. There is a table in Section 8.1 that you can record your settings for easy reference.
# Contents

1 SOLUTION ARCHITECTURE ......................................................................................................................... 5  
1.1 COMPONENTS ........................................................................................................................................... 5  

2 PREPARING MDM PLATFORM FOR INTEGRATION .......................................................................................... 6  
2.1 PREREQUISITES ........................................................................................................................................ 6  
2.2 AIRWATCH CONSOLE ............................................................................................................................... 6  
2.3 CREATING A CHILD ORGANIZATION GROUP (OPTIONAL) ................................................................. 7  
2.4 APP COLLECTION (REQUIRED) .................................................................................................................. 10  
2.5 CREATING AN API ONLY ADMINISTRATOR ACCOUNT (OPTIONAL) ......................................................... 11  
2.6 ADDING A USER TO AN ORGANIZATION GROUP ..................................................................................... 20  

3 CONFIGURING MDM TO DEPLOY SANDBLAST MOBILE PROTECT APP .......................................................... 23  
3.1 PREREQUISITES ...................................................................................................................................... 23  
3.2 ADD THE SANDBLAST MOBILE PROTECT APP TO YOUR APP CATALOG ............................................. 24  
3.3 REQUIRING THE SANDBLAST MOBILE PROTECT APP TO BE INSTALLED ........................................... 40  

4 CREATING A MITIGATION PROCESS .......................................................................................................... 58  
4.1 PREREQUISITES ...................................................................................................................................... 58  
4.2 CREATING A DYNAMIC ASSIGNMENT GROUP ....................................................................................... 59  
4.3 CREATING COMPLIANCE POLICIES FOR AT RISK DEVICES ................................................................. 61  

5 CONFIGURING THE CHECK POINT SANDBLAST MOBILE DASHBOARD MDM INTEGRATION SETTINGS .......... 78  
5.1 PREREQUISITES ...................................................................................................................................... 78  
5.2 CONFIGURING MDM INTEGRATION SETTINGS ....................................................................................... 79  

6 SANDBLAST MOBILE PROTECT APP DEPLOYMENT ..................................................................................... 84  
6.1 REGISTRATION OF AN IOS DEVICE ......................................................................................................... 84  
6.2 REGISTRATION OF AN ANDROID DEVICE ............................................................................................... 85  

7 TESTING HIGH RISK ACTIVITY DETECTION AND POLICY ENFORCEMENT .............................................. 86  
7.1 BLACKLISTING A TEST APP .................................................................................................................... 87  
7.2 VIEW OF NON-COMPLIANT DEVICE ....................................................................................................... 88  
7.3 ADMINISTRATOR VIEW ON THE SANDBLAST MOBILE DASHBOARD .................................................... 89  
7.4 ADMINISTRATOR VIEW ON THE AIRWATCH CONSOLE ....................................................................... 90  

8 APPENDICES ................................................................................................................................................ 93  
8.1 INTEGRATION INFORMATION .................................................................................................................. 93
1 Solution Architecture

1.1 Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 SandBlast Mobile Protect app | • The SandBlast Mobile Protect app is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior.  
  • To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.  
  • The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience. |
| 2 EMM/MDM                    | • Enterprise Mobility Management/Mobile Device Management  
  • Device Management and Policy Enforcement System.                                                                                                                                                                               |
| 3 SandBlast Mobile Gateway    | • The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.  
  • The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s ("organization’s") SandBlast Mobile Dashboard instance.                                                                 |
| 4 Dashboard                   | • The cloud-based web-GUI Check Point SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance.  
  • The SandBlast Mobile Dashboard can be integrated with an existing Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for automated policy enforcement on devices at risk.  
  • When using this integration, the MDM/EMM serves as a repository with which the SandBlast Mobile Dashboard syncs enrolled devices and identities.                                                             |
| 5 Behavioral Risk Engine      | • The cloud-based Check Point SandBlast Mobile Behavioral Risk Engine uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis.  
  • The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.  
  • The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.  
  • No Personal Information is processed by or stored in the Engine.                                                                                                                                                              |
2 Preparing MDM Platform for Integration

2.1 Prerequisites

2.1.1. AirWatch version 7.0 or higher with REST API access enabled.
2.1.2. AirWatch must be configured to “Collect” the app list from the devices. See Section 2.4 for instructions for this configuration.

2.2 AirWatch Console

2.2.1. Login to your AirWatch Console.
2.3 Creating a Child Organization Group (optional)

AirWatch identifies users and establishes permissions using organization groups. While any organization method will deliver content to devices, use organization groups (OG) to establish an MDM hierarchy identical to your organization's internal hierarchy or you may establish OGs based on AirWatch features and content.

You can access organization groups by navigating to Groups & Settings > Groups > Organization Groups > List View or through the organization group drop-down menu.

- Build groups for entities within your organization.
- Customize hierarchies with parent and child levels.
- Integrate with multiple internal infrastructures at the tier level.
- Delegate role-based access and management based on multi-tenant structure.¹

**Note:** It is not necessary to create a child organization group, however if you want to, for example, place all the SandBlast Mobile devices in a Child Organization Group, follow this process.

2.3.1. Navigate to Groups & Settings > Groups > Organization Groups > Organization Group Details.

---

¹ Airwatch Console Basics Guide: Organization Groups Overview
2.3.2. Select “Add Child Organization Group” tab, and fill in required (*) fields, such as in the example below. Also, make sure that you create a Group ID, otherwise you will have to edit this entry before you can add users.

![Add Child Organization Group](image)

2.3.3. Click the “Save” button.

**Note:** This will automatically select the new child organization group as the active organization group as indicated in the organization group drop-down menu.

![Save Button](image)
2.3.1 Determining the REST API Key for the Integration
SandBlast Mobile integration requires you to know the REST API Key.

2.3.1.1. Navigate to Groups & Settings > All Settings > System > Advanced > API > REST API.

2.3.1.2. Your API Key is listed in the box labeled API Key. This is the API Key that will be used when configuring the MDM Settings in the SandBlast Mobile Dashboard.

**Note:** This is the API Key that you will use in configuring the MDM Settings within the SandBlast Mobile Dashboard.
2.4 App Collection (Required)

In order for the SandBlast Mobile Dashboard to be updated with device app lists after the initial device sync, the MDM must be configured to collect the app list from the devices enrolled to SandBlast Mobile.

2.4.0.1. Navigate to Groups & Settings > All Settings > Devices & Users > General > Privacy > Applications > Personal Application and ensure that the setting is set to “Collect Do Not Display” or “Collect and Display” for the all device ownership levels.

2.4.0.2. If you do not want the AirWatch Console interface to display the list of applications installed across all the devices, you can change the privacy settings to “Collect Do Not Display”.

2.4.0.3. If necessary you can override these settings and make the appropriate changes.

2.4.0.4. Scroll to the bottom of the screen and click the “Save” button.
2.5 Creating an API Only Administrator Account (optional)

For the interaction at the REST API only, there is an Admin Role, “API Only”, provided in the AirWatch Console that you can use to create an account that you will use between the SandBlast Mobile Dashboard and the AirWatch system.

**Note:** It is a best practice to create such an admin account, but is optional.

To create an “API Only” Administrator Account, follow this process.

2.5.1 Create a New SandBlast Mobile API Only Administrator Role

2.5.1.1. Navigate to Accounts > Administrators > Roles, select the “Read Only” role, and click the “Copy” button.
2.5.1.2. On the “Copy Role” pop-up window, enter in a Name and Description for this new role.

2.5.1.3. In addition to the “Read Only” permissions, we are going to enable the following settings/capabilities for this role:

2.5.1.3.1. API > REST > Devices => Edit
2.5.1.3.2. API > REST > Groups => Edit
2.5.1.3.3. API > REST > Tags => Edit
2.5.1.3.4. Device Management > Bulk Management => Edit
2.5.1.3.5. Device Management > Compliance => Edit
2.5.1.3.6. Hub > Reports > Applications > ReportBlacklistedApplications => Read
2.5.1.3.7. Hub > Reports > Devices > ReportDeviceCompliance => Read
2.5.1.4. Navigate in the Categories Menu to API > REST
2.5.1.4.1. REST > Devices => Select Edit
2.5.1.4.2. REST > Groups => Select Edit
2.5.1.4.3. REST > Tags => Select Edit
2.5.1.5. Navigate in the Categories Menu to **Device Management**.

- **2.5.1.5.1.** Bulk Management => Select Edit
- **2.5.1.5.2.** Compliance => Select Edit

<table>
<thead>
<tr>
<th>Read</th>
<th>Edit</th>
<th>Category</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bulk Management</td>
<td>Perform bulk actions on devices from the device list view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificate Management</td>
<td>Certificate Management</td>
<td>View and manage certificates under device management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compliance</td>
<td>View and manage device compliance policies under device management.</td>
</tr>
</tbody>
</table>

- **Bulk Management**
  - **Dashboard**
    - Asset Tracking: Access to the asset tracking page under device management.
  - **Dashboard**
    - View Dashboard: View the device dashboard page within device management.

- **Certificate Management**
  - **Dashboard**
    - Android File Manager: Remotely managed android files and folders from the device details page.
  - **Dashboard**
    - Applications: Remotely install and removed applications from managed devices.

- **Compliance**
  - **Dashboard**
    - Attachments: Add and remove attachments from devices in device details.
  - **Dashboard**
    - ARMCM: Start and stop the AirWatch Cloud Manager connection from device details.
2.5.1.6. Navigate in the Categories Menu to **Hub**.
2.5.1.6.1. **Reports > Applications > ReportBlacklistedApplications** => Select **Read**
2.5.1.6.2. Scroll down to Reports > Devices > ReportDeviceCompliance => Select Read

2.5.1.7. Click the “Save” button.
2.5.2 Create a New Administrator Account

2.5.2.1. Navigate to Accounts > Administrators > List View, click the “Add” button, select “Add Admin”.

![AirWatch Console](image-url)
2.5.2.2. On the Basic tab, fill in all required (*) fields with appropriate information, such as in the example below.
2.5.2.3. On the Roles tab, select the Organization Group, i.e. CPTME Corp/SBM POC, and the Role of “sbm_admin_role” from their respective pull-downs.

2.5.2.4. Click the “Save” button.
2.6 Adding a User to an Organization Group

There are two ways to add a user to the organization group, one at a time, “Add User”, or in batch file upload, “Batch Import”. We are going to show how to add a user using the “Add User” method.

2.6.0.1. Navigate to Accounts > Users > List View, click the “ADD” drop-down menu, and select “Add User”.

![Image of AirWatch Console showing the Add User option]
2.6.0.2. On the Basic tab, fill in all the required (*) fields with the appropriate information, such as in the example below.

2.6.0.3. Click the “Save” button or click the “Save and Add Device” button, which will skip the navigation instruction in the next section and open a “Add Device” window.
2.6.1 Adding a Device to a User

2.6.1.0.1. You can alter the default “Expected Friendly Name”.
2.6.1.0.2. Select the Ownership: “Corporate – Dedicated”, “Corporate – Shared”, “Employee Owned”, or “None”.
2.6.1.0.3. Select the Message Type of “Email”, and enter the user’s email address.

2.6.1.0.4. Click the “Save” button.

**Note:** You will not see the device in the Devices > List View until the device completes the enrollment process. To see the device is indeed created and pending enrollment, navigate to Devices > Lifecycle > Enrollment Status.

**Note:** You can repeat the above steps to add another user and/or device.

2.6.1.1 Enrolling Devices to AirWatch

3 Configuring MDM to Deploy SandBlast Mobile Protect app

3.1 Prerequisites

3.1.2. If you have configured AirWatch for “Whitelisting Apps”, then you must add the SandBlast Mobile Protect apps to the white list.
3.1.3. The CHKP Status Tags must be created at the Customer Organization Group, highest parent organization group.
3.1.3.1. Navigating to Settings > Devices & Users > Advanced > Tags, the following tags should exist.
3.1.3.1.1. CHKP_Status_Provisioned
3.1.3.1.2. CHKP_Status_Active
3.1.3.1.3. CHKP_Status_Inactive
3.2 Add the SandBlast Mobile Protect App to Your App Catalog

Using the CHKP Status Tags we can start deploying the SandBlast Mobile Protect app from the public stores to those devices that will be protected by Check Point SandBlast Mobile. We will do this to only require the Protect app when the device has the CHKP_Status of Provisioned, Active, or Inactive. If all of these tags are empty or 0, then the user will NOT be prompted to install the Protect app. This ensures that the devices are synchronized in the SandBlast Mobile Dashboard before asking the user to install the SandBlast Mobile Protect app.

We will need to add the Protect App for both iOS and Android operating systems.

3.2.1 iOS App

3.2.1.1. Navigate to Apps & Books > Applications > Native > Public, and select the “+Add Application” button.

3.2.1.2. This will cause the “Add Application” pop-up window to open.
3.2.1.3. Select the appropriate Organization Group in the “Managed By” drop-down menu.
3.2.1.4. Select “Apple iOS” from the “Platform” drop-down menu.
3.2.1.5. “Source” should be “Search App Store”, and “SandBlast Mobile Protect” should be entered into the “Name” field.

3.2.1.6. Click the “Next” button to search the App Store for the SandBlast Mobile Protect app.
3.2.1.7. The search result window should show the SandBlast Mobile Protect app, such as in the example below.

3.2.1.8. Click the “+Select” button to the right.
3.2.1.9. This will continue with “Add Application” window where there are four tabs: Details, Terms of Use, and SDK.

3.2.1.10. Click the “Save & Assign” button.
3.2.1.11. On the “Update Assignment” pop-up, click the “Add Assignment” button.
3.2.1.12. On the “Add Assignment” pop-up window, select the appropriate “Assignment Group”.
3.2.1.12.1. Change the “App Delivery Method” from “On Demand” to “Auto” to prompt the user to install the SandBlast Mobile Protect app on the device.
3.2.1.12.2. Enable “Managed Access”.
3.2.1.12.3. Enable “Remove On Unenroll”.
3.2.1.12.4. Enable “Prevent Application Backup”.
3.2.1.12.5. Enable “Application Configuration”.
3.2.1.12.6. Scroll down to the Application Configuration Section.
3.2.1.12.6.1. Enter in the first row of the “Application Configuration” table:
3.2.1.12.6.1.1. “Configuration Key” = “Lacoon Server Address”
3.2.1.12.6.1.2. “Value Type” = “String”
3.2.1.12.6.1.3. “Configuration Value” = “gw.locsec.net”
3.2.1.12.6.2. Click the “+Add” button to add another row to the “Application Configuration” table.
3.2.1.12.6.3. Enter in the second row of the “Application Configuration” table:
3.2.1.12.6.3.1. “Configuration Key” = “Device Serial Number”
3.2.1.12.6.3.2. “Value Type” = “String”
3.2.1.12.6.3.3. “Configuration Value” = “{DeviceSerialNumber}”
3.2.1.13. Click the “Save & Publish” button.
3.2.1.14. Click the “Publish” button.
### 3.2.2 Android App

Just as with the iOS App, AirWatch can automatically configure the registration key for an android device. It does require the user to launch the SandBlast Mobile Protect app to finish device registration.

#### 3.2.2.1. Navigate to **Apps & Books > Applications > Native > Public**, and select the “+Add Application” button.

![AirWatch Console Screenshot]

This will cause an “Add Application” pop-up window to open.
3.2.2.3. Select the appropriate Organization Group in the “Managed By” drop-down menu.
3.2.2.4. Select “Android” from the “Platform” drop-down menu.
3.2.2.5. “Source” should be “Search App Store”, and “SandBlast Mobile Protect” should be entered into the “Name” field.
3.2.2.6. Click the “Next” button to search the App Store for the SandBlast Mobile Protect app.

3.2.2.7. The search result window should show the SandBlast Mobile Protect app, such as in the example below.

3.2.2.8. Click the “+Select” button to the right.
3.2.2.9. This will continue with “Add Application” window where there are four tabs: Details, Terms of Use, and SDK.

3.2.2.10. Click the “Save & Assign” button.
3.2.2.11. On the “Update Assignment pop-up, click the “Add Assignment” button.
3.2.2.12. On the “Add Assignment” pop-up window, select the appropriate “Assignment Group”.
3.2.2.12.1. Change the “App Delivery Method” from “On Demand” to “Auto” to prompt the user to install the SandBlast Mobile Protect app on the device.
3.2.2.12.2. Enable “Managed Access”.
3.2.2.12.3. Click the “Add” button.
3.2.2.13. Click the “Save & Publish” button.
3.2.2.14. Click the “Publish” button.
3.3 Requiring the SandBlast Mobile Protect app to be Installed

The SandBlast Mobile Protect app is required by creating an Application Group for both the iOS and Android apps, and assigning the group to the Organization, in our example “SBM POC”. Then, we can create a compliance policy to uninstall/remove corporate apps from the device until the user installs the required apps on the device.

3.3.1 Creating a Group of Required Apps

3.3.1.1 App Group for iOS Apps

3.3.1.1.1 Navigate to Apps & Books > Applications > Applications Settings > App Groups, and click the “+Add Group” button.
3.3.1.1.2. Set “Type” to “Required”, “Platform” to “Apple iOS”, and enter in a unique group name, such as “Required iOS Apps”.

3.3.1.1.3. Click the “Add Application” button.

3.3.1.1.4. Enter in “SandBlast Mobile Protect” into “Application Name” and click the enter button to search the Apple AppStore for the SandBlast Mobile Protect app.

3.3.1.1.5. In the search result window, click the “+Select” link for the proper app.
3.3.1.1.6. The search results will return the application ID from the store search.

3.3.1.1.7. Click the “Next” button.

3.3.1.1.8. On the “Assignment” tab, enter in a Description, and set the Organization Group to the appropriate group, in our example “SBM POC”.

3.3.1.1.9. Click the “Finish” button.
3.3.1.2  App Group for Android Apps

3.3.1.2.1. Navigate to Apps & Books > Applications > Applications Settings > App Groups, and click the “+Add Group” button.
3.3.1.2.2. Set “Type” to “Required”, “Platform” to “Android”, and enter in a unique group name, such as “Required Android Apps”.

3.3.1.2.3. Click the “Add Application” button.

3.3.1.2.4. Enter in “SandBlast Mobile Protect” into “Application Name” and click the enter button to search the Google Play Store for the SandBlast Mobile Protect app.

3.3.1.2.5. In the search result window, click the “+Select” link for the proper app.
3.3.1.2.6. The search results will return the application ID from the store search.

3.3.1.2.7. On the “Assignment” tab, enter in a Description, and set the Organization Group to the appropriate group, in our example “SBM POC”.

3.3.1.2.8. Click the “Finish” button.
3.3.2 Creating a Dynamic Assignment Group

Next we are going to group all devices using the tag from the previous section. This is a dynamic group assignment based on the associated tag. AirWatch calls these dynamic Assignment Groups “Smart Groups”.

3.3.2.1 Navigate to Groups & Settings > Groups > Assignment Groups.

3.3.2.2 Click “+ADD SMART GROUP”.

![AirWatch Console](Image)
3.3.2.3. Configure the Tags that will be used to dynamically group devices.
3.3.2.3.1. In the Name field, enter a unique Smart Group name.
3.3.2.3.2. Click in the “Enter Tag name” field, and select the desired tags from the resulting drop-down menu. Click the “Add” button.
3.3.2.3.2.1. In our example, we are looking for devices that have been marked with CHKP_Status_Provisioned, CHKP_Status_Active, and CHKP_Status_Inactive which indicates the devices registration status within SandBlast Mobile Dashboard.

3.3.2.4. Click the “Save” button.
3.3.3 Creating a Compliance Policy for Required Apps

Now that we have a Smart Group, we can create Compliance Policies that will be enforced on devices that have not installed the required apps. In order to take appropriate action on devices correctly, you have to create separate compliance policies that are for specific OS types, such as iOS and Android.

**Note:** We will show a couple of different compliance policies, but these enforcement policies are something that the customer should create for their environment and needs. In a production environment, the customer should configure the compliance policies according to their internal security policy.

3.3.3.1 Compliance Policy for iOS Devices

3.3.3.1.1 Navigate to Devices > Compliance Policies > List View, and click “+ Add”.

![AirWatch Console](image)
3.3.3.1.2. Click “Apple iOS”.

3.3.3.1.3. The first tab is setting the “Rules”. Select “Application List” “Does Not Contain Required App(s)”.

3.3.3.1.4. Click the “Next” button.
3.3.3.1.5. This will take you to the “Actions” tab.

3.3.3.1.6. Make sure “Mark as Not Compliant” checkbox is checked. Add the Actions you want to be taken by this policy. In our example, we have chosen to Notify the user by email as well as a push notification, and “Application” “Block/Remove All Managed Apps”.

![iOS Add Compliance Policy](image)

3.3.3.1.6.1. To add additional actions click “+” at the end of the existing action.

3.3.3.1.6.1.1. Other actions can be:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Action</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Not Compliant</td>
<td>Marks the device as Not Compliant with Company Policy</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Block/Remove Managed App</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Managed Apps</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Request Device Check In</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Wipe</td>
<td></td>
</tr>
</tbody>
</table>
| | Change Roaming Settings (iOS 5+) | Enable Voice Roaming
Disable Voice Roaming
Enable Data Roaming
Disable Data Roaming |
| Email | Block Email | |
| Notify | Send Email to User | Use Default Template |
| | Send SMS to Device | Use Default Template |
| | Send Push Notification to Device | Use Default Template |
| | Send Email to Administrator | Use Default Template |
3.3.3.1.6.1.2. If issue is not resolved by the User, an escalation action set can be added using the ”+ Add Escalation” button. These actions can be repeated over a specified number of times over a specified interval.

3.3.3.1.7. When done with configuring the Actions, click the “Next” button.

3.3.3.1.8. This will take you to the “Assignment” tab. Add the “Assignment Group” you created in Section 3.3.2.

3.3.3.1.9. Click the “Next” button.
3.3.3.1.10. This will bring you to the “Summary” tab where you must provide a unique name for the Compliance Policy, and a Description of policy.

3.3.3.1.11. Click the “Finish & Activate” button.
3.3.3.2 Compliance Policy for Android Devices

3.3.3.2.1. Navigate to Devices > Compliance Policies > List View, and click “+ Add”.

3.3.3.2.2. Click “Android”.
3.3.3.2.3. The first tab is setting the “Rules”. Select “Application List” “Does Not Contain Required App(s)”.

3.3.3.2.4. Click the “Next” button.

3.3.3.2.5. This will take you to the “Actions” tab.
3.3.3.2.6. Make sure “Mark as Not Compliant” checkbox is checked. Add the Actions you want to be taken by this policy. In our example, we have chosen to Notify the user by email as well as a push notification, and “Install Compliance Profile” of “Non-Compliant Android Device Policy” that disables the camera.

![Add Compliance Policy screenshot]

3.3.3.2.6.1. To add additional actions click “+” at the end of the existing action.

3.3.3.2.6.1.1. Other actions can be:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Action</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Not Compliant</td>
<td>Marks the device as Not Compliant with Company Policy</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Block/Remove Managed App</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Managed Apps</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Enterprise Wipe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Reset</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Block Email</td>
<td></td>
</tr>
<tr>
<td>Notify</td>
<td>Send Email to User</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send SMS to Device</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send Push Notification to Device</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send Email to Administrator</td>
<td>Use Default Template</td>
</tr>
<tr>
<td>Profile</td>
<td>Install Compliance Profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove Profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove Profile Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Profiles</td>
<td></td>
</tr>
</tbody>
</table>
3.3.3.2.6.2. If action is not taken by the User to correct the issue, an escalation action can be added using the "+ Add Escalation" button.

3.3.3.2.7. When done with configuring the Actions, click the “Next” button.

3.3.3.2.8. This will take you to the "Assignment" tab. Add the "Assignment Group" you created in Section 3.3.2.

3.3.3.2.9. Click the “Next” button.
3.3.3.2.10. This will bring you to the “Summary” tab where you must provide a unique “Name” for the Compliance Policy, and a “Description” of policy.

3.3.3.2.11. Click the “Finish & Activate” button.
4 Creating a Mitigation Process

In this section, you will reference the built-in Risk Tags SandBlast Mobile Dashboard will use to label any device in High, Medium, Low, or No Risk as determined by the SandBlast Mobile Analysis. These tags will allow the AirWatch system to identify which devices are at risk and to enforce configured compliance policies based on risk level.

4.1 Prerequisites

4.1.1. The CHKP Risk Tags must be created at the Customer Organization Group, highest parent organization group.

4.1.1.1. Navigating to Settings > Devices & Users > Advanced > Tags, the following tags should exist.

4.1.1.1.1. CHKP_Risk_High
4.1.1.1.2. CHKP_Risk_Medium
4.1.1.1.3. CHKP_Risk_Low
4.1.1.1.4. CHKP_Risk_None
4.2 Creating a Dynamic Assignment Group

Next we are going to group all devices using the tag from the previous section. This is a dynamic group assignment based on the associated tag. AirWatch calls these dynamic Assignment Groups “Smart Groups”.

4.2.1. Navigate to Groups & Settings > Groups > Assignment Groups.

4.2.2. Click “+Add Smart Group”.

![AirWatch Console](image)
4.2.3. Configure the Tags that will be used to dynamically group devices.
4.2.3.1. In the Name field, enter a unique Smart Group name.
4.2.3.2. Click in the “Enter Tag name” field, and select the desired tag from the resulting drop-down menu. Click the “Add” button.
4.2.3.2.1. Select the Appropriate CHKP Tags to have this smart group to include those devices with the selected tags set by SandBlast Mobile.
4.2.3.2.2. Choices are:
4.2.3.2.2.1. CHKP_Risk_High
4.2.3.2.2.2. CHKP_Risk_Medium
4.2.3.2.2.3. CHKP_Risk_Low

4.2.4. Click the “Save” button.
4.3 Creating Compliance Policies for At Risk Devices

Now that we have a Smart Group, we can create Compliance Policies that will be enforced on devices that are at High Risk.

In order to take appropriate action on devices correctly, you have to create separate compliance policies that are for specific OS types, such as iOS and Android.

Note: We will show a couple of different compliance policies, but these enforcement policies are something that the customer should create for their environment and needs. In a production environment, the customer should configure the compliance policies according to their internal security policy.

4.3.1 Device Profiles for Non-Compliant Devices

We want to create demonstrable policy enforcement on the devices, this is accomplished by creating Device Profiles that are applied to the device by the Compliance Policy we will create in the next section.

4.3.1.1 iOS Device Profile

4.3.1.1.1 Navigate to Devices > Profiles & Resources > Profiles, click “ADD”, and select “Add Profile” from the drop-down menu.
4.3.1.1.2. On the “Add Profile” pop-up window, select “Apple iOS”.

4.3.1.1.3. Under the “General” section, enter in a Name and Description, and set “Assignment Type” to “Compliance”.
4.3.1.1.4. Select the “Restrictions” section, and click the “Configure” button.

4.3.1.1.5. Under the “Restrictions” section, under Device Functionality unselect “Allow use of camera”.

4.3.1.1.6. Click the “Save & Publish” button.
4.3.1.2 Android Device Profile

4.3.1.2.1. Navigate to Devices > Profiles & Resources > Profiles, click “ADD”, and select “Add Profile” from the drop-down menu.

4.3.1.2.2. On the “Add Profile” pop-up window, select “Android”.
4.3.1.2.3. Under the “General” section, enter in a Name and Description, and set “Assignment Type” to “Compliance”.

4.3.1.2.4. Select the “Restrictions” section, and click the “Configure” button.
4.3.1.2.5. Under the “Restrictions” section, under Device Functionality unselect “Allow Camera”.

4.3.1.2.6. Click the “Save & Publish” button.

4.3.2 Compliance Policy for iOS Devices
4.3.2.1. Navigate to Devices > Compliance Policies > List View, and click “+ Add”.
4.3.2.2. Click “Apple iOS”.

[Image of a screen with options to select a platform: Android, iOS, macOS, Chrome OS (Legacy), QNX, Windows Rugged, Windows.]
4.3.2.3. The first tab is setting the “Rules”. This is an iOS policy, so select “OS Version” is “Greater Than or Equal To” “Apple iOS – iOS 8.0.0”.

4.3.2.4. Click the “Next” button.
4.3.2.5. This will take you to the “Actions” tab.

4.3.2.6. Make sure “Mark as Not Compliant” checkbox is checked. Add the Actions you want to be taken by this policy. In our example, we have chosen to Notify the user by email as well as a push notification, and “Install Compliance Profile” of “Non-Compliant iOS Device Policy” that disables the camera.

4.3.2.6.1. To add additional actions click “+” at the end of the existing action.

4.3.2.6.1.1. Other actions can be:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Action</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Not Compliant</td>
<td>Marks the device as Not Compliant with Company Policy</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Block/Remove Managed App</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Managed Apps</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Request Device Check In</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Wipe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Roaming Settings (iOS 5+)</td>
<td>Enable Voice Roaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disable Voice Roaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Data Roaming</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disable Data Roaming</td>
</tr>
<tr>
<td>Email</td>
<td>Block Email</td>
<td></td>
</tr>
<tr>
<td>Notify</td>
<td>Send Email to User</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send SMS to Device</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send Push Notification to Device</td>
<td>Use Default Template</td>
</tr>
</tbody>
</table>
4.3.2.6.1.2. If issue is not resolved by the User, an escalation action set can be added using the "+ Add Escalation" button. These actions can be repeated over a specified number of times over a specified interval.

4.3.2.7. When done configuring the Actions, click the "Next" button.

4.3.2.8. This will take you to the "Assignment" tab. Add the "Assignment Group" you created in Section 4.2.

4.3.2.9. Click the "Next" button.
4.3.2.10. This will bring you to the “Summary” tab where you must provide a unique name for the Compliance Policy, and a Description of policy.

4.3.2.11. Click the “Finish & Activate” button.
4.3.3 Compliance Policy for Android Devices

4.3.3.1. Navigate to Devices > Compliance Policies > List View, and click “+ Add”.

![AirWatch Console Diagram]

- Blacklisted App Compliance
- Blacklisted App Compliance
- Required Apps Missing - Android
- Required Apps Missing - iOS
4.3.3.2. Click “Android”.

![Add Compliance Policy Screen](image-url)
4.3.3.3. The first tab is setting the “Rules”. This is an Android policy, so select “OS Version” is “Greater Than or Equal To” “Android – Android 4.0.1”.

<table>
<thead>
<tr>
<th>Add Compliance Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match: All</td>
</tr>
<tr>
<td>Of The Following Rules</td>
</tr>
<tr>
<td>OS Version</td>
</tr>
<tr>
<td>Greater Than or Equal To</td>
</tr>
<tr>
<td>Android – Android 4.0.1</td>
</tr>
</tbody>
</table>

4.3.3.4. Click the “Next” button.
4.3.3.5. This will take you to the “Actions” tab.

4.3.3.6. Make sure “Mark as Not Compliant” checkbox is checked. Add the Actions you want to be taken by this policy. In our example, we have chosen to Notify the user by email as well as a push notification, and “Install Compliance Profile” of “Non-Compliant Android Device Policy” that disables the camera.

4.3.3.7. To add additional actions click “+” at the end of the existing action.

4.3.3.7.1. Other actions can be:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>Action</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Not Compliant</td>
<td>Marks the device as Not Compliant with Company Policy</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Block/Remove Managed App</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Managed Apps</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Enterprise Wipe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Reset</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Block Email</td>
<td></td>
</tr>
<tr>
<td>Notify</td>
<td>Send Email to User</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send SMS to Device</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send Push Notification to Device</td>
<td>Use Default Template</td>
</tr>
<tr>
<td></td>
<td>Send Email to Administrator</td>
<td>Use Default Template</td>
</tr>
<tr>
<td>Profile</td>
<td>Install Compliance Profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove Profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove Profile Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block/Remove All Profiles</td>
<td></td>
</tr>
</tbody>
</table>
4.3.3.8. If action is not taken by the User to correct the issue, an escalation action can be added using the "+ Add Escalation" button.

4.3.3.9. When done with configuring the Actions, click the “Next” button.

4.3.3.10. This will take you to the "Assignment" tab. Add the "Assignment Group" you created in Section 4.2.

4.3.3.11. Click the “Next” button.
4.3.3.12. This will bring you to the “Summary” tab where you must provide a unique “Name” for the Compliance Policy, and a “Description” of policy.

4.3.3.13. Click the “Finish & Activate” button.

**Note:**
Now any device in the Device Provisioning Group (“SBM POC”) that has the Mitigation Tag (“CHKP_Risk_High” or “CHKP_Risk_Medium” or “CHKP_Risk_Low”) applied to it by the SandBlast Mobile system will be acted upon by the Security Policies which apply the actions specified in the policies:
- For iOS, this policy is named “iOS Devices At Risk”, and
- For Android, this policy is named “Android Devices At Risk”.

**Note:**
At this point, we have all the information we will need to configure the MDM integration settings in the SandBlast Mobile Dashboard. We are going to do that and then return to the AirWatch Console to configure the SandBlast Mobile Protect app deployment settings.
From Our Examples:
- Server = https://techp.awmdm.com
- API Admin Username/Password = sbm_admin/<hidden>
- Organization Group(s) = SBM POC
5 Configuring the Check Point SandBlast Mobile Dashboard

MDM Integration Settings

5.1 Prerequisites

5.1.1. You will need the following details from your AirWatch Deployment:

Note: There is a table in Section 8.1 that you can record your settings for easy reference.

5.1.1.1. Server: The URL to your AirWatch System, usually the same as the AirWatch Console URL.

5.1.1.2. AirWatch Administrative Username and Password: These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the MDM. You may have created a special API Only Admin account in Section 2.5 for this purpose.

5.1.1.3. API Key: This is the API Key for the REST API Service. Please see instructions in Section 2.3.1 for locating the REST API key within your AirWatch Console interface.

5.1.1.4. Organization Group(s): This is the AirWatch organization groups to which the devices are registered, and will be integrated with the SandBlast Mobile Dashboard. Multiple Organization Groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each Organization Group name separated with a semicolon (;), however, they MUST use the same REST API Key.

Note: This integration is hierarchical in that if a Parent Organization Group is integrated with a SandBlast Mobile Dashboard, then any child Organization Group of that Parent cannot be integrated with a different SandBlast Mobile Dashboard.

Note: Mitigation tags, Smart Groups, and Compliance Policies are recursive. If defined at the Parent Organization Group, any Child Organization Group will inherit and apply to Child Organization Group devices that match the criteria.

5.1.2. For on-premise MDM environments, the TCP Web Services port (usually TCP port 443 (HTTPS)) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the MDM system before trying to connect.

5.1.3. Delete any existing devices in the SandBlast Mobile Dashboard.

Note: Only the devices are synchronized from the MDM to the SandBlast Mobile Dashboard, not users.
5.2 Configuring MDM Integration Settings

5.2.0.1. Navigate to Settings > Device Management > Setting.
5.2.0.2. Select “AirWatch” from the “MDM service” drop-down menu under the Device Management Settings area.
5.2.0.3. A pop-up window will open. Configure the settings as are appropriate for your AirWatch Deployment, such as those you may have created in Section 2.

5.2.0.4. Click the “VERIFY” button. If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the AirWatch system, you will be able to click the “SAVE” button to finish configuration.
5.2.1 Registration Email and Registration Limit Settings

5.2.1.1. Navigate to Settings > Device Management > Setting, under the “Notify user when device was added by MDM” section, when a MDM Service is configured, these settings are configured automatically. Registration emails are turned off. Daily registration limit is set to 100. “Should install MDIS profile” is turned off.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration email (iOS)</td>
<td>Should the system send Registration email to iOS devices?</td>
</tr>
<tr>
<td>Registration email (Android)</td>
<td>Should the system send Registration email to Android devices?</td>
</tr>
<tr>
<td>Daily registration limit</td>
<td>The number of devices that can register within a 24 hour period.</td>
</tr>
</tbody>
</table>

5.2.1.2. If you make changes to the default settings, click the “Save” button to have changes take effect.
5.2.2 MDM Advanced Settings

When a MDM Service is configured, the Device Management Advanced Settings are automatically configured based on recommendations of the selected MDM provider, in this case from AirWatch.

5.2.2.1. Navigate to Settings > Device Management > Advanced, and make any appropriate changes.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with MDM to sync devices.</td>
</tr>
<tr>
<td>Device deletion threshold</td>
<td>Percentage of devices allowed for deletion after MDM device sync.</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync - device will not be deleted if it will be re-sync from MDM during the threshold interval.</td>
</tr>
</tbody>
</table>

5.2.2.2. If you make changes to the default settings, click the “Save” button to have changes take effect.
6 SandBlast Mobile Protect App Deployment

Based on the settings for the deployment of the SandBlast Mobile Protect app for iOS and Android configured in Section 3, the App will either be “Auto” or “On Demand” deployed. In the configuration above, we chose “Auto” for both iOS and Android deployment.

**Note:** It can take up to 10 minutes for the MDM to sync with the SandBlast Mobile Dashboard, and a few minutes for the MDM to push the App to the user’s device.

6.1 Registration of an iOS Device

After the device is registered to the AirWatch system, the user will be prompted to install the SandBlast Mobile Protect App.

6.1.1. The user taps “INSTALL”.

6.1.2. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration. The registration server and key are automatically configured in the App by the AirWatch system.

6.1.3. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.
### 6.2 Registration of an Android Device

After the device is registered to the AirWatch system, the user will be prompted to install the SandBlast Mobile Protect app. The user taps on the App to open the Google Play Store.

6.2.1. The user taps the “INSTALL” button, and taps “ACCEPT” to accept the permissions of the App. The App installs.

6.2.2. After the App is installed, the user must launch the App to finish its deployment and registration to Check Point SandBlast Mobile.

6.2.3. The App will automatically register, and the user must tap “Activate” to allow the SandBlast Mobile Protect app to be a device administrator.

6.2.4. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.
7 Testing High Risk Activity Detection and Policy Enforcement

If the user’s device is determined to be at risk either due to a malicious app or malicious activity, the SandBlast Mobile system notifies the User via in-app notifications as well as updates the risk state by setting the appropriate CHKP_Risk tag to the AirWatch system for that device. AirWatch receives the state change, and upon recognizing the set tag being tied to a Compliance Policy, enacts that policy.

In the following example, the Administrator will blacklist an app, such as in our example “Dropbox”. As a result, all devices with “Dropbox” installed will be identified to be at High Risk (CHKP_Risk_High=1) due to the blacklisted app being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device with CHKP_Risk_High set to 1 to the AirWatch system. The AirWatch system will then enforce policy actions specified in the compliance policy. This mitigation process was the one we created in Section 4.
7.1 Blacklisting a Test App

The first step is to blacklist an app, in our example “Dropbox”. By blacklisting this app, all release version and OS types will also be blacklisted. In our example, Dropbox for Android will be blacklisted which will result in all Dropbox numbered release versions for Android to be blacklisted as well, unless the “Apply only to this version” checkbox is selected.

7.1.1. Log into the SandBlast Mobile Dashboard.
7.1.2. Navigate to App Analysis tab, and search for the app you wish to blacklist, in our example “Dropbox”.

7.1.3. Click the “Policy” link of “Default”.

7.1.4. On the “Changing application policy” pop-up window, select “Black Listed” from the “New policy” drop-down menu, and enter a reason for this change in the “Audit Trail note”.

7.1.5. Click the “OK” button.
7.2 View of Non-Compliant Device

7.2.1 SandBlast Mobile Protect App Notifications

7.2.1.1. The user receives a SandBlast Mobile Protect notification indicating that the blacklisted app is not allowed by Corporate Policy, in our example “Dropbox”.

7.2.1.2. The user will not be able to use the device’s camera, as specified in the compliance actions (policy) we created in Section 4.3, in our example “Android Devices At Risk” until the user removes the blacklisted app.

7.2.2 AirWatch Agent App Notifications

7.2.2.1. The user receives an AirWatch Agent notification as specified in the “Android Devices At Risk” policy.
7.2.3 AirWatch Email Notification

7.2.3.1 The user receives an email from the AirWatch system, as specified in the “Android Devices At Risk” policy.

7.3 Administrator View on the SandBlast Mobile Dashboard

7.3.1 From the SandBlast Mobile Dashboard, the Administrator will see that there are devices at high risk.
7.3.2. Clicking the High Risk will display a list of devices at high risk.
7.3.3. Selecting the desired device from the left-side list, the Administrator can see that the high risk state is caused by the existence of the blacklisted app, “Dropbox”.

7.4 Administrator View on the AirWatch Console

7.4.1. In the AirWatch Console on the Devices > Dashboard view, the Administrator can see that one or more devices are have compliance violations and/or violate certain policies.

7.4.2. In the AirWatch Console from the Devices > List View, the Administrator can see that one or more devices are “Out of Compliance”.

7.4.3. Clicking the device’s name, the Administrator is presented with the device details view.
7.4.4. On the Summary tab, the Administrator can see that the device is out of compliance, and to which smart groups the device belongs.

7.4.5. On the “Compliance” tab, the Administrator can see that the device is out of compliance and that the Policy Name applied, in our example “High Risk Android Devices”.

7.4.6. On the “Profiles” tab, the Administrator can see that the “Non-Compliant Android Device Policy” profile has been applied to the device.
7.4.7. Clicking on the “More” drop-down menu, the Administrator can choose “Status History”. The Administrator can see the Status History, and notice that the device was Non-Compliant.
8 Appendices

8.1 Integration Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Server URL</td>
<td></td>
</tr>
<tr>
<td>AirWatch API Admin Username</td>
<td></td>
</tr>
<tr>
<td>AirWatch API Admin Password</td>
<td></td>
</tr>
<tr>
<td>AirWatch API Key</td>
<td></td>
</tr>
<tr>
<td>AirWatch Organization Group(s)</td>
<td></td>
</tr>
<tr>
<td>AirWatch Mitigation Label (Tag)</td>
<td></td>
</tr>
<tr>
<td>Tag Device Status (Boolean tags)</td>
<td>CHKP_Status_Provisioned, CHKP_Status_Active, CHKP_Status_Inactive</td>
</tr>
<tr>
<td>Tag Device Risk (Boolean tags)</td>
<td>CHKP_Risk_None, CHKP_Risk_Low, CHKP_Risk_Medium, CHKP_Risk_High</td>
</tr>
<tr>
<td>SandBlast Mobile Gateway</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>SandBlast Mobile App Name (iOS)</td>
<td>SandBlast Mobile Protect</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (iOS)</td>
<td>com.checkpoint.capsuleprotect</td>
</tr>
<tr>
<td>SandBlast Mobile App Name (Android)</td>
<td>SandBlast Mobile Protect</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (Android)</td>
<td>com.lacoon.security.fox</td>
</tr>
</tbody>
</table>