26 May 2020

SandBlast Mobile

Jamf

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 2020 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 decompilation. 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 for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.
# Table of Contents

About Check Point SandBlast Mobile ........................................................................................................... 4

Introduction to the SandBlast Mobile Integration Guide .................................................................................. 5

Solution Architecture ......................................................................................................................................... 6

Preparing the UEM Platform for Integration .................................................................................................... 8

Prerequisites ...................................................................................................................................................... 8

General Workflow ............................................................................................................................................ 8

Creating API Account ...................................................................................................................................... 8

Configuring Privileges for API Account ........................................................................................................... 10

Configuring Jamf to Deploy the SandBlast Mobile Protect app ........................................................................ 11

  Adding the SandBlast Mobile Protect App to your App Catalog ................................................................. 12

Setting Parameters for the SandBlast Mobile Protect in your App Catalog .................................................. 15

  Adding Configuration to SandBlast Mobile Application ............................................................................. 15

  Configuring Distribution Method .................................................................................................................. 17

  Assigning SandBlast Mobile Application to Groups of Users or Devices .................................................. 18

Configuring the SandBlast Mobile Dashboard Integration Settings ................................................................. 19

Prerequisites ...................................................................................................................................................... 19

Configuring Jamf Integration Settings ........................................................................................................... 20

Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement ........................................ 31

  Requiring the SandBlast Mobile Protect app to be Installed ..................................................................... 31

  Creating Smart Group for Devices with High Risk ..................................................................................... 32

  Creating Configuration Profile for Compromised Devices ......................................................................... 33

Testing High Risk Activity Detection and Policy Enforcement ........................................................................ 37

  Blacklisting a Test App ................................................................................................................................. 37

  View of a Non-Compliant Device .................................................................................................................. 38

  Administrator View on the SandBlast Mobile Dashboard ......................................................................... 40

SandBlast Mobile App Deployment on the Devices .......................................................................................... 41

Appendix .......................................................................................................................................................... 42

Integration Information .................................................................................................................................... 42
About Check Point SandBlast Mobile

Check Point SandBlast Mobile is the most complete threat defense solution designed to prevent emerging fifth generation cyber-attacks and allow workers to safely conduct business. Its technology protects against threats to the OS, apps, and network, scoring the industry’s highest threat catch rate without impacting performance or user experience.

- SandBlast Mobile delivers threat prevention technology that:
  - Performs advanced app analysis to detect known and unknown threats
  - Prevents man-in-the-middle attacks on both cellular and Wi-Fi networks
  - Blocks phishing attacks on all apps: email, messaging, social media
  - Prevents infected devices from sending sensitive data to botnets
  - Blocks infected devices from accessing corporate applications and data
  - Mitigates threats without relying on user action or mobile management platforms

SandBlast Mobile 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 SandBlast Mobile solution ("the Solution") includes the following components:
  - SandBlast Mobile Behavioral Risk Engine ("the Engine")
  - SandBlast Mobile Gateway ("the Gateway")
  - SandBlast Mobile Management Dashboard ("the Dashboard")
  - SandBlast Mobile Protect app ("the App") for iOS and Android

SandBlast Mobile integrates with UEM systems and provides integral risk assessment of the device which the UEM can use to quarantine, or activate a set of policies until the device is no longer at risk.

This policy enforcement can disable certain capabilities of a device, for example, block access to corporate assets, such as email, internal websites, and more. It provides protection of the corporation’s network and data from mobile-based threats.

This guide describes how to integrate the SandBlast Mobile Dashboard with your UEM. It provides a quick tour through the interface of the UEM and the SandBlast Mobile Dashboard to enable integration, alerting, and policy enforcement. This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).
Introduction to the SandBlast Mobile Integration Guide

The SandBlast Mobile Protect app is an app for iOS® and Android™ that gathers data and helps analyze threats to mobile 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.

This Guide explains how to integrate the Check Point SandBlast Mobile Protect app with the company device managing systems.
## Solution Architecture

<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** UEM | - Unified Endpoint Management (generalized term replacing MDM/EMM)  
- Device Management and Policy Enforcement System |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SandBlast Mobile Gateway</td>
<td>▪ The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.</td>
</tr>
<tr>
<td></td>
<td>▪ The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (organization’s) Dashboard instance.</td>
</tr>
<tr>
<td></td>
<td>▪ No Personal Information is processed by or stored in the Gateway.</td>
</tr>
<tr>
<td>SandBlast Mobile Dashboard</td>
<td>▪ The cloud-based web-GUI SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance.</td>
</tr>
<tr>
<td></td>
<td>▪ The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.</td>
</tr>
<tr>
<td></td>
<td>▪ When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities.</td>
</tr>
<tr>
<td>Behavioral Risk Engine</td>
<td>▪ The cloud-based SandBlast Mobile Behavioral Risk Engine (BRE) 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.</td>
</tr>
<tr>
<td></td>
<td>▪ The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.</td>
</tr>
<tr>
<td></td>
<td>▪ The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.</td>
</tr>
<tr>
<td></td>
<td>▪ No Personal Information is processed by or stored in the Engine.</td>
</tr>
<tr>
<td>ThreatCloud</td>
<td>▪ Check Point’s ThreatCloud is the world largest incidence of compromise database that incorporates real-time threat intelligence from hundreds of thousand Check Point gateways and from millions of endpoints across the globe.</td>
</tr>
<tr>
<td></td>
<td>▪ ThreatCloud powers the Anti-Phishing, Safe Browsing, URL Filtering and Anti-bot technologies for SandBlast Mobile on-device Network Protection.</td>
</tr>
<tr>
<td></td>
<td>▪ ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis.</td>
</tr>
</tbody>
</table>
Preparing the UEM Platform for Integration

Prerequisites

- SandBlast Mobile service integrates with Jamf through the existing API. To enable the integration, you must first create a Jamf API account.
- SandBlast Mobile will use API for the device records synchronization, device apps list retrieve, and for reporting device risk level to Jamf.
- Jamf will deploy SandBlast Mobile Protect app on a device to streamline the device enrollment.

General Workflow

2. Configure the account privileges. See "Configuring Privileges for API Account" on page 10.
3. Configuring Jamf to Deploy the SandBlast Mobile app. See "Configuring Jamf to Deploy the SandBlast Mobile Protect app" on page 11.

Creating API Account

For the interaction at the API, you must create a dedicated API account user in your Jamf.

Procedure:

1. Login to Jamf.
2. Go to Settings > System Settings -> Jamf Pro User Accounts & Groups.

Example:
3. Click **New**.
4. Go to **Choose an Action > Create Standard Account**.

Example:

5. Click **Next**.

New Account window opens.

6. Fill in all the required fields with the appropriate information.
Example:

Configuring Privileges for API Account

Note - For fast configuration of POC or demo, you can configure PRIVILEGE SET to Admin.

For production and testing environment, we highly recommend to use API account with limited permissions, as described below.

Procedure:

1. Go to the Account > Privileges section.
2. Verify that ACCESS STATUS is set to Enabled.
3. Configure API account.
   - Configure Basic Privileges.
In the **Jamf Pro Server Objects** section, check only **Read** option for all the settings.

Example:

<table>
<thead>
<tr>
<th>Jamf Pro Server Objects</th>
<th>CREATE</th>
<th>READ</th>
<th>UPDATE</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamp Pro User Accounts &amp; Groups</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Mobile Device Groups</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart User Groups</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Mobile Device Groups</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static User Groups</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Configure Mitigation Privileges.

   In the **Jamf Pro Server Objects** section, set a custom set of Mitigation Privileges for Mobile Device Extension Attributes and for Mobile Devices.

   Example:

<table>
<thead>
<tr>
<th>Jamf Pro Server Objects</th>
<th>CREATE</th>
<th>READ</th>
<th>UPDATE</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Extension Attributes</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **OK**.

### Configuring Jamf to Deploy the SandBlast Mobile Protect app

This configuration simplifies the SandBlast Mobile Protect app deployment and activation on managed devices.

**Notes:**

If you configured Jamf for **Whitelisting Apps**, you must add the SandBlast Mobile Protect apps to the white list.

**Procedure:**

1. Add the SandBlast Mobile Protect App to your App Catalog. See "**Adding the SandBlast Mobile Protect App to your App Catalog**" on page 12.
2. Connect the app to your devices. See "**Adding Configuration to SandBlast Mobile Application**" on page 15.
4. Assign the app to the selected groups of users or devices. See "Assigning SandBlast Mobile Application to Groups of Users or Devices" on page 18.

Adding the SandBlast Mobile Protect App to your App Catalog

**Note** - As you create the SandBlast Mobile Protect app for your catalog, rename this New Mobile Device App to SandBlast Mobile Protect app.

**Procedure:**

1. Go to Devices > Mobile Device Apps > New.

   Example:

   ![Device App Creation Example](image)

2. Select the type of the App:
   a. In **Choose an App Type** section, verify that **App Store app or apps purchased in volume** is selected.
   b. Click **Next**.

   Example:
3. Search for the SandBlast Mobile in App store:
   a. In the Search or Upload text field, enter the text SandBlast Mobile Protect.
   b. Select the app store in the relevant country.
   c. Click Next.

Example:

4. In the Add an App > iPhone & iPod touch Apps > SandBlast Mobile Protect row, click on Add.

Example:
5. Set the App Parameters in the next following section
6. Click **Save**.
Setting Parameters for the SandBlast Mobile Protect in your App Catalog

Adding Configuration to SandBlast Mobile Application

Connect the app to your devices.

Procedure:

1. In the Devices window, go to New Mobile Device App > App Configuration section.

   In the Preferences text field, add the following text:

   ```
   {{ hash_tenant_id }}
   ```

   (The SHA-256 value of the Dashboard Management ID. You must use the token configured in the Deployment section. For more information see "Configuring Jamf Integration Settings" on page 27.)

   ```
   <dict>
   <key>Lacoon Server Address</key>
   <string>gw</string>
   <key>Device Serial Number</key>
   <string>$SERIALNUMBER</string>
   <key>token</key>
   <string>{{ hash_tenant_id }}</string>
   </dict>
   ```

   Example:
2. Click **Done**.
Configuring Distribution Method

Procedure:

1. In the **Devices** window, go to the **SandBlast Mobile Protect app > General** section.
2. Go to **DISTRIBUTION METHOD** section and select **Install Automatically/Prompt Users to Install**.
3. Check **Schedule Jamf Pro to automatically check iTunes for app updates**.
4. Check **Automatically Force App Updates**.
5. Check **Make app managed if currently installed as unmanaged**.

Example:
Assigning SandBlast Mobile Application to Groups of Users or Devices

Procedure:

1. In the Devices window, go to the SandBlast Mobile Protect app > Scope section.
2. Under the Targets, click Add.

   Example:

3. Select the specific mobile device and/or specific user groups for deployment.
4. Click Done.
Configuring the SandBlast Mobile Dashboard Integration Settings

**Note** - For easy reference during configuration, you can record your settings in the special table (see "Integration Information" on page 42).

**Prerequisites**

You will need the following details from your Jamf Deployment:

- **Server**: The URL of your Jamf System. Usually - the same as the Jamf Console.
- **User name and Password**: Credentials of API Account. See "Creating API Account" on page 8.

  The credentials that the SandBlast Mobile Dashboard will use to connect to Jamf.

- **Group(s)**: This is the Jamf mobile device / user groups to which the devices are registered, and will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance.

- For on-premise Jamf environments: before you try to connect, make sure that the TCP Web Services port (usually TCP port 443 (HTTPS) is accessible remotely through your firewall from the SandBlast Mobile Dashboard to Jamf.

**Note** - Before you start, delete any existing devices in the SandBlast Mobile Dashboard.
Configuring Jamf Integration Settings

Procedure:

1. From the Infinity Portal, go to Settings > Device Management.

   The Device Management page opens.

2. Click Edit.

   The Integration Wizard opens.

   Example:

3. Configure the settings for your Jamf Deployment.

   - **Server Setup**

     Configure your UEM to integrate with the created Jamf devices:

     a. In Server Setup section, enter this information:

        - UEM service - Jamf
        - Server Address - The full URL needed for the UEM service
        - User name
        - Password
        - Connector Setup (advanced)
Example:
Connector Setup

You can configure SandBlast Connector when the UEM has no direct access from the SandBlast Mobile cloud. For more information see *Sandblast Mobile Connector Integration Guide* in the Check Point Support Download center.

Example:

b. Click **Next**.

- **Synchronization Configuration**

  Configure the devices and groups that you synchronize with SandBlast Mobile Dashboard.

Example:
a. In the **Group(s)** field:
   i. Click **Group(s)**.

   A dropdown with list of the available groups opens.

   ii. Select the group(s) you need for integration with Jamf.

b. In the **Advanced** section:
   i. Import Personally Identifiable Information (PII) and set the synchronization intervals.

   You can limit the import of the PII devices (users) to SandBlast Mobile.

   **Note** - If all entries are OFF, the placeholder information set for the email address is placed in the Device Owner’s Email, in form of "UEMDevice UDID@vendor.mdm".

Example:
**Tagging Configuration**

Specify the information sent to Jamf and the risk level of the device.

Example:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
<tr>
<td>Device deletion threshold</td>
<td>Percentage of devices allowed for deletion after UEM device sync (in %).</td>
<td>0-100% ; use 100% for no threshold.</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync – device is not deleted if it is re-synchronized from UEM during the threshold interval.</td>
<td>0-48 hours.</td>
</tr>
<tr>
<td>App sync interval</td>
<td>Interval to connect with UEM to sync applications.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
</tbody>
</table>

d. Click Next.
a. In **Tagging** Section:
   Create Mobile Device External Attribute and name it *status*. See "*Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement*" on page 30.
   i. Set **Tag device status** to ON.
   ii. Set **Tag device risk** to ON.

b. In **Advanced** section:
   **Mitigation tag**: This field will not be used as we will be using the CHKP Risk and Status tags.

   Click **Finish**.
Example:

Deployment

Specify the deployment status of a device.

Note - This section is optional, because Jamf manages the deployment automatically.
If you use SandBlast Mobile to manage the deployment:

In the **Advanced** section:

a. Enable options to send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app.

b. Click **Finish**.
4. View the **Integration Status**.
   a. View the **Integration Status**.

   In the Infinity Portal, go to **Settings > Device Management**.

   The **Device Management** pane shows this information:

   - **Server** – The latest server configuration status.
   - **Synchronization** – The synchronized groups and the sync status.
   - **App Sync** – The last type applications were fetched from the UEM (For iOS deployments only).
   - **Tagging** – Tagging Configuration and Tagging Status.
   - **Deployment** – Deployment Configuration and Deployment Status.
5. Click **Edit** in each section to edit the settings.
Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement

If the user’s device is determined to be at risk because of a malicious app or malicious activity, the SandBlast Mobile system notifies the User by sending the in-app notifications, and also updates the risk state by setting the appropriate risk_level extension attribute to Jamf for the device. This device must be added automatically to a Smart Mobile Device Group, with the criteria of an extension attribute. Also, Jamf must have a Configuration Profile that can apply a policy on a Mobile Device Group.

For example, an Administrator is blacklisting a Waze app. As a result, all the devices with Waze will be identified as devices at High Risk (“risk_level”="CHKP_Risk_High”). The SandBlast Mobile Dashboard will notify the user and mark the device with “risk_level” set to “CHKP_Risk_High” in Jamf. This will add the device to the Smart Mobile Device Group “CHKP_Risk_High”. Then the Jamf system will enforce policy actions specified in the Configuration Profile. This mitigation process is described in "Preparing the UEM Platform for Integration" on page 8 and in "Configuring Jamf Integration Settings" on page 20.

Requiring the SandBlast Mobile Protect app to be Installed

If SandBlast Mobile app is not installed or removed from device, the device is marked as not protected.

To configure the Required/Automatic Installation:

1. On Jamf, go to Devices > Smart Device Groups > New.

   Example:

   ![Jamf UI for Devices and Smart Device Groups]

2. Configure settings in Mobile Device Group Section:
   - In Display Name, enter the group name (recommended: “Not Protected Devices”).

3. Configure settings in Criteria Section:
   a. Click Add.
   b. Click Show Advanced Criteria.
c. Scroll down to the **App Name** option.
d. In this row, click **Choose**.
e. In the **Operator** field, select does not have.
f. Click (...) on right from **Value**.
g. Scroll to the **Protect**.
h. In this row click **Choose**.
i. Click **Save**.

4. Click **Done**.

Example:

![Smart Group Configuration](image)

**Creating Smart Group for Devices with High Risk**

1. Go to **Devices > Smart Device Groups > New**.

   Example:

   ![Smart Group Creation](image)

   2. Configure setting in the **Mobile Device Group** Section:
      a. In **Display Name**, enter the group name (recommended: “CHKP_Risk_High”).
b. Check the option Send email notification on membership change (recommended).

3. Configure setting in the Criteria Section:
   a. Click Add.
   b. Click Show Advanced Criteria.
   c. Scroll down to the risk_level option.
   d. In this row, click Choose.
   e. In the Operator field, select is.
   f. In the Value field, enter CHKP_Risk_High.
   g. Click Save.

4. Click Done.

Note - Check Point recommends to create a separate Smart Group for each risk level and for each device status (active, inactive, and more).

Creating Configuration Profile for Compromised Devices

For compromised and not protected devices, we must configure and apply a separate Configuration Profile.

1. Go to Devices > Configuration Profiles > New.

   Example:

   ![Configuration Profiles](image)

2. Configure setting in the Options section.

   Note - In this example, we will block the camera for the applied devices and use as a Test App. But you can select any other policy or restriction, for example, removing apps, etc.

   - On General Tab:
     - Enter the Profile name, for example, Non-Compliant Devices.

   - On Restrictions Tab:
Click on **Configure**.

Example:

**In iOS > Functionality section:**

Remove the check mark from the **Allow use of camera** option.

Example:

**In Scope > Targets section:**

a. In the **Selected Deployment Targets** row, click **Add**.

Example:
b. Click on **Mobile Device Groups** tab.

c. Click **Add** in the row of the **Smart Group** that you created for the devices at risk CHKP_Risk_High (see "Creating Smart Group for Devices with High Risk" on page 32).

d. Click **Add** in a row of the “**Not Protected Devices**” Smart Group.

e. Click **Save**.

3. Click **Done**.

Example:
Check Point SandBlast Mobile: UEM Integration Guide | Jamf

Add Deployment Targets

<table>
<thead>
<tr>
<th>Mobile Devices</th>
<th>Mobile Device Groups</th>
<th>Users</th>
<th>User Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All Managed iPads</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All Managed iPhones</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All Managed iPod touches</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHKP_Risk_High</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Done

©2020 Check Point Software Technologies Ltd. All rights reserved
May, 2020
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 through in-app notifications, and also updates the risk level custom attribute value to the Jamf system for that device. Jamf receives the risk state change, and upon recognizing the risk level value tied to a Configuration Profile, enacts that policy.

In the following example, the Administrator will blacklist an app, for example, "Waze". As a result, the user’s device will be identified to be at High Risk (CHKP_Risk_High) due to the blacklisted app "Waze" installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device as High Risk (CHKP_Risk_High) to the Jamf system. The Jamf system will then enforce policy actions specified in the Configuration Profile.

Blacklisting a Test App

1. Log into the SandBlast Mobile Dashboard.
2. Go to App Analysis tab and select for the app you wish to blacklist.
   Example:
   
   ![Screen shot of App Analysis tab]

   3. Go to Default and click Policy.

   A Changing application policy pop-up window opens.

   4. From the New Policy drop-down menu, select Black Listed.

   5. In the Audit Trail note field, enter a reason for this change.

   Example:
6. Click OK.

The user receives a SandBlast Mobile Protect app notification to indicate that the blacklisted app (for example, Waze) is not allowed by the Corporate Policy.

**View of a Non-Compliant Device**

The device with the blacklisted app (for example, Waze) must be added in the group you defined in section "Creating Smart Group for Devices with High Risk" on page 32.

To add the non-compliant device to the Smart Mobile Device Group:

1. Go to Devices > Smart Device Groups > Your defined Smart Mobile Device Group.

Example:
2. Click View.

The device is displayed.

Example:

Note - If you configured an email notification, you will receive an email from Jamf.
Administrator View on the SandBlast Mobile Dashboard

On the SandBlast Mobile Dashboard the Administrator can see the devices at High Risk.

1. Go to Device Risk > High Risk section.
   
   A list of the devices at high risk is displayed.

2. Select the specified device on the left-side list.
   
   You can see that the blacklisted app (for example, XYZ) causes the High Risk state.

Example:
SandBlast Mobile App Deployment on the Devices

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section "Configuring Jamf Integration Settings" on page 20, the App will be automatically deployed to the devices that belong to the defined groups (see "Configuring Jamf to Deploy the SandBlast Mobile Protect app" on page 11).

**Note** - It can take up to 10 minutes for Jamf to sync with the SandBlast Mobile Dashboard, and several more minutes to push the App to the user's device.

After the device is registered to the Jamf and attached to the defined groups, the user will be prompted to install the SandBlast Mobile Protect App.

**Procedure for the User:**

1. Tap **INSTALL** on your iOS Device.
   
   The App is deployed on the device.

2. Launch the App to finish the registration.
   
   The registration server and the key are automatically configured in the App by the Jamf system. See "Configuring Jamf to Deploy the SandBlast Mobile Protect app" on page 11

Example:

When the App finishes scanning the system, it displays the state of the device. In this case, the device has no malicious or high risk apps, network and OS threats.
## Appendix

### Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEM/ Server URL</td>
<td></td>
</tr>
<tr>
<td>UEM Web Services URL</td>
<td></td>
</tr>
<tr>
<td>UEM API Account Username</td>
<td></td>
</tr>
<tr>
<td>UEM API Account Password</td>
<td></td>
</tr>
<tr>
<td>UEM Group(s)</td>
<td></td>
</tr>
<tr>
<td>UEM Mitigation Group</td>
<td></td>
</tr>
<tr>
<td>Tag Device Status (Boolean tags) become (CP_Integrations.CHKPTag)s in UEM</td>
<td>CHKP_Status_Provisioned, CHKP_Status_Active, CHKP_Status_Inactive</td>
</tr>
<tr>
<td>Tag Device Risk (Boolean tags) become (CP_Integrations.CHKPTag)s in UEM</td>
<td>CHKP_Risk_None, CHKP_Risk_Low, CHKP_Risk_Medium, CHKP_Risk_High</td>
</tr>
<tr>
<td>SandBlast Mobile Gateway</td>
<td>gw</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>
</tbody>
</table>