About This Guide

Check Point SandBlast Mobile 3.0 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.

Only SandBlast Mobile 3.0 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 WiFi 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 3.0 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

When used with an Unified Endpoint Management (UEM) system, such as BlackBerry UEM, SandBlast Mobile provides integral risk assessment of the device to which the UEM can use to quarantine or enforce a set of policies that are in effect until the device is no longer at 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 SandBlast Mobile Dashboard with BlackBerry UEM. It provides a quick tour through the interface of the BlackBerry UEM 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).
# 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                                                                                                                                                                    |
| 3 SandBlast Mobile Gateway | » The cloud-based 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) Dashboard instance.                                                                                     |
| 4 SandBlast Mobile Dashboard | » 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.  
» The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.  
» When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities.                                                                 |
| 5 Behavioral Risk Engine   | » The cloud-based 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.                                                                                                                                         |
## Contents

### Chapter 1 Preparing the UEM Platform for Integration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>BlackBerry UEM Console</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Creating an API Administrator Account (optional)</strong></td>
<td>2</td>
</tr>
<tr>
<td>Create a New Administrator User Account</td>
<td>3</td>
</tr>
<tr>
<td>Assign New User to Administrator Role</td>
<td>4</td>
</tr>
<tr>
<td><strong>Adding a User</strong></td>
<td>7</td>
</tr>
<tr>
<td>Adding a User from Corporate Directory</td>
<td>7</td>
</tr>
<tr>
<td>Adding a Local User</td>
<td>10</td>
</tr>
<tr>
<td>Adding a Device to an Existing User</td>
<td>12</td>
</tr>
<tr>
<td><strong>Creating User Provisioning Groups</strong></td>
<td>13</td>
</tr>
<tr>
<td>Information about Device Risk &amp; Status tags and BlackBerry UEM user groups</td>
<td>13</td>
</tr>
<tr>
<td>Creating a User Group based on Corporate User Directory</td>
<td>16</td>
</tr>
<tr>
<td>Creating Local User Group(s)</td>
<td>18</td>
</tr>
<tr>
<td>Adding an Existing User to the Local User Group</td>
<td>19</td>
</tr>
<tr>
<td>Adding a New User to an Existing Local User Group</td>
<td>21</td>
</tr>
<tr>
<td>Nesting User Groups (Optional)</td>
<td>23</td>
</tr>
<tr>
<td><strong>Enrolling Devices to BlackBerry UEM</strong></td>
<td>25</td>
</tr>
</tbody>
</table>

### Chapter 2 Configuring the SandBlast Mobile Dashboard UEM Integration Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td>27</td>
</tr>
<tr>
<td><strong>Configuring Device Management Settings</strong></td>
<td>28</td>
</tr>
<tr>
<td>Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM</td>
<td>31</td>
</tr>
<tr>
<td>Tag Device Status</td>
<td>31</td>
</tr>
<tr>
<td>Tag Device Risk</td>
<td>32</td>
</tr>
<tr>
<td>Mitigation Group</td>
<td>32</td>
</tr>
<tr>
<td>Controlling the Importing of Personally Identifiable Information (PII) from the UEM</td>
<td>32</td>
</tr>
<tr>
<td><strong>MDM Advanced Settings</strong></td>
<td>34</td>
</tr>
</tbody>
</table>

### Chapter 3 Configuring the UEM Platform

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisites</strong></td>
<td>35</td>
</tr>
<tr>
<td><strong>Configuring UEM to Deploy SandBlast Mobile Protect app</strong></td>
<td>36</td>
</tr>
<tr>
<td>Adding the SandBlast Mobile Protect App to Your App Catalog</td>
<td>36</td>
</tr>
<tr>
<td>AppStore iOS App – Add to Catalog</td>
<td>36</td>
</tr>
<tr>
<td>Android App – Add to Catalog</td>
<td>40</td>
</tr>
<tr>
<td>Creating an App Group (Optional)</td>
<td>44</td>
</tr>
<tr>
<td>Deploying SandBlast Mobile Protect app</td>
<td>47</td>
</tr>
<tr>
<td>Requiring the SandBlast Mobile Protect App to be Installed</td>
<td>48</td>
</tr>
<tr>
<td>Creating a Compliance Policy</td>
<td>48</td>
</tr>
<tr>
<td>Applying App Required Compliance Policy to User Provisioning Group</td>
<td>50</td>
</tr>
<tr>
<td>Device Out of Compliance – Missing SandBlast Mobile Protect App</td>
<td>52</td>
</tr>
<tr>
<td><strong>Creating a Mitigation Process</strong></td>
<td>55</td>
</tr>
<tr>
<td>Creating IT Policies</td>
<td>55</td>
</tr>
</tbody>
</table>
Applying the Policy to the User Mitigation Group ................................................................. 57

Chapter 4 Registering Devices to SandBlast Mobile .......................................................... 59
  Registration of an iOS Device ................................................................................................. 60
  Registration of an Android Device ......................................................................................... 62
  Redeployment of the SandBlast Mobile Protect App – iOS ................................................ 63
  Redeployment of the SandBlast Mobile Protect App - Android ............................................ 63
  Resending SandBlast Mobile Activation Code ....................................................................... 64

Chapter 5 Testing High Risk Activity Detection and Policy Enforcement ......................... 65
  Blacklisting a Test App ........................................................................................................... 66
  View of Non-Compliant Device ............................................................................................ 67
    SandBlast Mobile Protect App Notifications ...................................................................... 67
    UEM Client App Notifications ........................................................................................... 68
  Administrator View on the SandBlast Mobile Dashboard ..................................................... 68
  Administrator View on the BlackBerry UEM Console ......................................................... 69

Appendix .................................................................................................................................. 70
  Integration Information .......................................................................................................... 70
### Preparing the UEM Platform for Integration

This chapter discusses the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>1</td>
</tr>
<tr>
<td>BlackBerry UEM Console</td>
<td>2</td>
</tr>
<tr>
<td>Creating an API Administrator Account (optional)</td>
<td>2</td>
</tr>
<tr>
<td>Create a New Administrator User Account</td>
<td>3</td>
</tr>
<tr>
<td>Assign New User to Administrator Role</td>
<td>4</td>
</tr>
<tr>
<td>Adding a User</td>
<td>7</td>
</tr>
<tr>
<td>Adding a User from Corporate Directory</td>
<td>7</td>
</tr>
<tr>
<td>Adding a Local User</td>
<td>10</td>
</tr>
<tr>
<td>Adding a Device to an Existing User</td>
<td>12</td>
</tr>
<tr>
<td>Creating User Provisioning Groups</td>
<td>13</td>
</tr>
<tr>
<td>Information about Device Risk &amp; Status tags and BlackBerry UEM user groups</td>
<td>13</td>
</tr>
<tr>
<td>Creating a User Group based on Corporate User Directory</td>
<td>16</td>
</tr>
<tr>
<td>Creating Local User Group(s)</td>
<td>18</td>
</tr>
<tr>
<td>Adding an Existing User to the Local User Group</td>
<td>19</td>
</tr>
<tr>
<td>Adding a New User to an Existing Local User Group</td>
<td>21</td>
</tr>
<tr>
<td>Nesting User Groups (Optional)</td>
<td>23</td>
</tr>
<tr>
<td>Enrolling Devices to BlackBerry UEM</td>
<td>25</td>
</tr>
</tbody>
</table>

### Prerequisites

1. BlackBerry UEM 12.6 or higher.
2. For **on-premise BlackBerry UEM Deployments**, the port used for the UEM Web Services API (default: TCP 18084) must be accessible remotely by the SandBlast Mobile servers through your firewall before trying to connect.
1. Login to your BB Console.

**Note:** During the procedures in this document there are quite a few pieces of information that you will need to gather or create. There is a form in "Integration Information" on page 70 that you can record your settings for easy reference.

### Creating an API Administrator Account (optional)

For the interaction at the API, we will create an API admin user in the BlackBerry UEM Console that you use to limit the capability of the admin credentials used between the SandBlast Mobile Dashboard and the BlackBerry UEM system.

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

**Note:** Creating an administrator account and administrator role requires a "Security Administrator" level role.

To create an "API" Administrator Account, follow this process.
For more or updated information, please see BlackBerry’s documentation at http://help.blackberry.com/en/blackberry-uem/current/administration/create-administrator.html

Create a New Administrator User Account

1. Navigate to Users, click "Add user".

2. On the "Add a user" pop-up window "Local" tab, fill in the "Display name", "Username", and an "Email address" for the new user. In our example, we will create an admin username of "sbm_admin".
3. Enter in a temporary console password for this user. When you login the first time with these credentials, you will be prompted to set a new password.

4. Scroll down and deselect the "Enable user for device management" checkbox.

5. Click "Save".

Assign New User to Administrator Role

1. Navigate to Settings > Administrators > Users, click "Add Admin".
2. On the "Add an Administrator" pop-up window, search/select the user you created in "Create a New Administrator User Account" on page 3.

3. Click the user’s "Name".

4. Under "Assign a role" select the "Security Administrator" role.

5. Click "Save".
6. Finish the creation of the new admin account by logging out of the BlackBerry UEM Console, and then logging back in using the temporary credentials you assigned to this new admin, in our example "sbm_admin / T3mp0rary123!". This will force you to select a new unique password.

7. Click "Sign In".

8. On the "New password" pop-up window, enter in a new password.

9. Click "Submit".

10. On the "Find out about..." pop-up window, select "Do not show this again".

11. Click "Start".

12. Click "Log out".

**Note:** Log out and log back into the BlackBerry UEM Console with your original Admin credentials to continue with the configuration.
Adding a User

There are two ways to add a user, "Add a Local User", or sync with a corporate user directory.

Note: You can integrate with your Corporate User Directory to import group and associated user information. Imported information can be used for automatic provisioning of users, group based policy assignment and App distribution. Supported User Directories are Microsoft Active Directory and LDAP.

For more or updated information, please see BlackBerry’s documentation at http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/hse1372277059163.html

Adding a User from Corporate Directory

If you have configured your BlackBerry UEM Console to integrate with your company user directory, follow these steps to add a user to the BlackBerry UEM Console.

1. Navigate to Users, click "Add user".

© 2018 Check Point Software Technologies Ltd. All rights reserved. | P. 7
October 17, 2018
2. On the "Add a user" pop-up window "Company directory" tab, start typing the name of the user you want to add. When the name is displayed, select it from the drop-down list.
3. The required (*) user information such as Display Name, Username, and Email address will be filled in from the company directory entry.
4. Scroll down to the bottom on the pop-up window and set the "Device activation" settings as required for your company.

5. Click "Save".

Adding a Local User

We are going to show how to add a local user using the "Add User" method.

1. Navigate to Users, click "Add user".
2. On the "Add a user" pop-up window "Local" tab, fill in all the required (*) fields with the appropriate information, such as in the example below.

3. Enter in a temporary console password for this user and select "Send password to user".

![Add a user window with filled fields and console password option]
4. Scroll down to the bottom on the pop-up window and set the "Device activation" settings as required for your company.

Note: The user is already notified with device enrollment procedures upon the creation of the user.

Adding a Device to an Existing User

1. Navigate to Users, scroll to or search for the user, and select that user.
2. Click "Send activation email".
3. On the "Set device activation password" pop-up window, Set the "Device activation" settings as required for your company.

4. Click "Send".

**Note:** Repeat these steps to add another device.

---

**Creating User Provisioning Groups**

To create a group of users whose devices will be registered to the Check Point SandBlast Mobile solution, follow this procedure.

**Information about Device Risk & Status tags and BlackBerry UEM user groups**

User groups are how BlackBerry UEM applies policies and assigns/deploys apps.

For more or updated information about adding user groups, see BlackBerry’s documentation at:


SandBlast Mobile utilizes these groups to move devices in and out of 7 pre-defined groups, and one freeform mitigation group.

There are 3 pre-defined status groups:

- CHKP_Status_Provisioned
- CHKP_Status_Active
- CHKP_Status_Inactive

When a device is provisioned in SandBlast Mobile Dashboard, this device is placed in the CHKP_Status_Provisioned group.

After the user has installed and registered to SandBlast Mobile, this device is moved from the CHKP_Status_Provisioned group to the CHKP_Status_Active group.

If the device hasn’t checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin), then the device is moved from CHKP_Status_Active to CHKP_Status_Inactive.
There are 4 pre-defined risk groups:

- CHKP_Risk_None
- CHKP_Risk_Low
- CHKP_Risk_Medium
- CHKP_Risk_High

If a device is determined to be at High, Medium, or Low risk, the device is placed in the respective group. If the device has no risks, then it is placed in the CHKP_Risk_None group.

For example, if the device has a Low risk app and a High risk (malicious) SMS URL, then the device will appear in both the CHKP_Risk_Low and CHKP_Risk_High groups.

The freeform mitigation group is any unique name, such as "Users_At_High_Risk", that SandBlast Mobile will place only devices determined to be at High Risk. It does not provide the granularity of the different risk levels of the device, just high risk state. This method was the original way to group devices at high risk, and it is strongly recommended that you implement the CHKP Risk and Status groups instead of using the freeform group.

In "Creating Local User Group(s)" on page 18, we will create these pre-defined SandBlast Mobile groups and nest them according to how we want our corporate policies to be applied.

In our example, devices that are members of CHKP_Risk_High, CHKP_Risk_Medium, or CHKP_Status_Inactive will be considered to be "Users_At_Risk", and have the appropriate Mitigation Policies applied as defined later in "Creating a Mitigation Process" on page 55. Devices that are members of CHKP_Risk_None or CHKP_Risk_Low, will not have the mitigation policies applied.

See the following diagram on how polices and group nesting are applied.
Creating a User Group based on Corporate User Directory

In this section we will create a User Group that is tied to Active Directory.

1. Navigate to **Groups > User**, click "Add a directory-linked group" icon.

2. On the "Add directory-linked group" pop-up window, enter in a Group Name, such as "SBM_AD_Users", and, if desired, a Group Description.

3. Click "+" sign to add a Linked directory group.
4. On the "Search company directory" pop-up window, enter in the first few letters of the corporate directory group you want to link, and hit enter.

5. Click "Add".

6. We haven't created any IT policies and profiles or added Apps to our App Catalog as of yet, so we will add those in subsequent sections.

7. Click "Add".
Creating Local User Group(s)

In this section, we will create all of the User Groups we need for Provisioning, Monitoring, and Mitigation. These groups are:

- **Optional User Groups**, but recommended in order to simplify applying policies, deploying apps, and mitigating risks. Some of the required user groups will be nested under these groups as discussed further in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13 and in "Nesting User Groups (Optional)" on page 23.
  - SBM_Syncd_Users
  - Users_At_Risk

- **Required User Group** if not using AD User Group
  - SBM_Local_Users

- **Required User Groups for Integration** if using Tag Device Status and Tag Device Risk
  - CHKP_Status_Provisioned
  - CHKP_Status_Active
  - CHKP_Status_Inactive
  - CHKP_Risk_None
  - CHKP_Risk_Low
  - CHKP_Risk_Medium
  - CHKP_Risk_High

1. Navigate to Groups > User, click "Add a user group" icon.
2. On the "Add a user group" pop-up window, enter in a Group Name, such as "SBM_Local_Users", and, if desired, a Group Description.

3. We haven’t created any IT policies and profiles or added Apps to our App Catalog as of yet, so we will add those in subsequent sections.
4. Click "Add".

Note: Repeat these steps to add all the user groups listed above.

Adding an Existing User to the Local User Group

To add an existing user to the User Group we created in "Creating a User Group based on Corporate User Directory" on page 16 or "Creating Local User Group(s)" on the previous page, follow this procedure. Our example will be using the Local User group ("SBM_Local_Users").
1. Navigate to **Users**, scroll and select the user you want to add to the user group, and click the "Add to user groups" icon.

2. On the "Add to user groups" pop-up window, select the SBM_Local_Users from the "Available groups" list, can click right arrow.
3. Click "Save".

4. The User is now part of the User Group "SBM_Local_Users".

Adding a New User to an Existing Local User Group

Adding a new user to an existing user group is close to the same procedure in "Adding a User" on page 7.

1. Navigate to Users, click "Add user".
2. On the "Add a user" pop-up window "Local" tab, fill in all the required (*) fields with the appropriate information, such as in the example below.

3. Select the User Group from the "Available groups" list and click right arrow.
4. Scroll down to the bottom on the pop-up window, and enter in a temporary console password for this user and select "Send password to user".
5. Set the "Device activation" settings as required for your company.

![Image of pop-up window with console password and device activation settings]

6. Click "Save".

**Note:** The user is already notified with device enrollment procedures upon the creation of the user.

**Nesting User Groups (Optional)**

We will be nesting the user groups that we created in "Creating Local User Group(s)" on page 18 and as discussed in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13. This will simplify the policy enforcement.

**Note:** If you do not want to create nested user groups, then you must apply the appropriate policies, apps, etc to each group individually as inheritance only occurs from parent group to child group.

In our example, we will nest our groups as follows:

- SBM_Syncd_Users
  - CHKP_Status_Provisioned
  - CHKP_Status_Active
» CHKP_StatusInactive
» Users_At_Risk
« CHKP_Risk_High
« CHKP_Risk_Medium
« CHKP_StatusInactive

Also, if you want devices at Low Risk to be subject to the same Non-Compliant policies as those at High Risk, simply nest CHKP_Risk_Low under Users_At_Risk.

For more or updated information about nested groups in BlackBerry UEM, see http://help.blackberry.com/en/blackberry-uem/current/administration/jth1410530746516.html

1. Navigate to Groups > User, and select "Users_At_Risk" to edit it.
2. Select "Nested groups" tab, and click "+".

3. On the "Add a nested group" pop-up window, select CHKP_Status_Inactive, CHKP_Risk_Medium, and CHKP_Risk_High.

4. Click "Add".

Note: Repeat these steps for adding the appropriate nested groups for SBM_Syncd_Users.
Enrolling Devices to BlackBerry UEM


**Note:** At this point, we have all the information we will need to configure the UEM integration settings in the SandBlast Mobile Dashboard.

From Our Examples:

- **Server URL** = https://<FQDN of BlackBerry UEM Server>:<port to Web Services API>
  (ie. https://uem.acme.us:18084)
- **SandBlast Mobile API Admin Username/Password** = sbm_admin/<hidden>
- **User Provisioning Group(s)** = SBM_Local_Users; SBM_AD_Users
Configuring the SandBlast Mobile Dashboard UEM Integration Settings

This chapter discusses the following:

- Prerequisites ........................................................................................................... 27
- Configuring Device Management Settings ................................................................. 28
- Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM .................................. 31
  - Tag Device Status .................................................................................................... 31
  - Tag Device Risk ........................................................................................................ 32
  - Mitigation Group ...................................................................................................... 32
- Controlling the Importing of Personally Identifiable Information (PII) from the UEM .......................... 32
- MDM Advanced Settings ............................................................................................ 34

Prerequisites

You will need the following details from your BlackBerry UEM Deployment:

**Note:** There is a table in "Integration Information" on page 70 that you can record your settings for easy reference.

1. **Server:** The root URL to your BlackBerry UEM Web Services API including the leading https://, such as https://uem.acme.us:18084
2. **SRP ID:** This is the SRP ID from BlackBerry licensing registered to your instance, in the form of S12345678. This value can be found by going to BlackBerry UEM Console > Help > About BlackBerry UEM.
3. **BlackBerry UEM SandBlast Mobile Administrator Username and Password:** These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the UEM. You may have created a special API Admin account in "Creating an API Administrator Account (optional)" on page 2 for this purpose.
4. **Groups(s):** These are the BlackBerry UEM user provisioning groups to which the users/devices to be registered to SandBlast Mobile are grouped, and will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each group name separated with a semicolon (;). These are the User Provisioning Groups we created in "Creating User Provisioning Groups" on page 13 ("SBM_Local_Users; SBM_AD_Users").
5. **Mitigation Group:** This field will not be used as we will be using the CHKP Risk and Status tags, as defined in "Creating Local User Group(s)" on page 18.
6. **For on-premise UEM environments,** the BlackBerry UEM Web Services port (TCP 18084) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the UEM system before trying to connect.
7. **Delete any existing devices in the SandBlast Mobile Dashboard,** and ensure that any devices that are to be enrolled via BlackBerry UEM integration are removed from other SandBlast Mobile Dashboards.

**Note:** Only the devices are synchronized from BlackBerry UEM to the SandBlast Mobile Dashboard, not users. If a user doesn't have a device enrolled, their information will not be synchronized to the SandBlast Mobile Dashboard.
Configuring Device Management Settings

1. Navigate to **Settings > Device Management > Setting**.
2. Select "BlackBerry UEM" from the "MDM service" drop-down menu under the Device Management Settings area.

3. A pop-up window will open.
4. Configure the settings as are appropriate for your BlackBerry UEM Deployment, such as those you have created in "Preparing the UEM Platform for Integration" on page 1.
5. Turn ON the "Tag Device Status" and "Tag Device Risk" toggles. Additional information regarding these tags can be found in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 13 and in "Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM" on page 31.
6. If your organization does not want to import any of the Personally Identifiable Information (PII), these toggles can be turned OFF for Owner Name, Phone Number, and/or Owner Email address. See additional information in "Controlling the Importing of Personally Identifiable Information (PII) from the UEM" on page 32.
7. If the BlackBerry UEM instance is self-signed, you can upload the 64Base Certificate information to the SandBlast Mobile server by turning on "Advanced options", by click "Upload Certificate" and selecting the Base64 certificate you saved from your UEM instance’s Web Services page (i.e. https://uem.acmecorp.us:18084).

8. Click "Verify". If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the BlackBerry UEM system, you will be able to click "Save" to finish configuration.
9. After successful configuration and sync, the "Devices" tab will show the devices added to SandBlast Mobile and their status as "Provisioned" which indicates that they have not yet tried to register to the SandBlast Mobile Dashboard.

Multi-tags in SandBlast Mobile and Usage in BlackBerry UEM

Recently added to SandBlast Mobile Dashboard for UEM integrations is the concept of multi-tags.

The multi-tags are built-in tags that SandBlast Mobile will use to indicate the different registration states (CHKP_Status) and the different risk levels (CHKP_Risk) to which the devices can be marked. This allows the Administrators on the UEM to configure granular compliance policies based on device registration status or risk level. These tags are created as "user groups" in BlackBerry UEM.

There are 3 Status states:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHKP_Status_Provisioned</td>
<td>When a device is synchronized for the first time in SandBlast Mobile Dashboard</td>
</tr>
<tr>
<td>CHKP_Status_Active</td>
<td>After the user has installed and registered to SandBlast Mobile</td>
</tr>
<tr>
<td>CHKP_Status_Inactive</td>
<td>If the device hasn’t checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin)</td>
</tr>
</tbody>
</table>

There are 4 pre-defined Risk levels:

- CHKP_Risk_None
- CHKP_Risk_Low
- CHKP_Risk_Medium
- CHKP_Risk_High

For example, if the device has a Low risk app and a High risk (malicious) SMS URL, then the device will be marked as at High Risk (CHKP_Risk_High = 1) and at Low Risk (CHKP_Risk_Low = 1). Once the High Risk issue has been remediated (SMS deleted), then the CHKP_Risk_High will be set to 0. Once the Low Risk issue has been remediated, the CHKP_Risk_Low will be set to 0.

Tag Device Status

For integration with BlackBerry UEM, the Device Status Tag are interpreted as "user groups" of "CHKP_Status_Provisioned", "CHKP_Status_Active", or "CHKP_Status_Inactive" which will have an either "0" or "1" when set.

We will use the CHKP_Status user groups to determine when to prompt the user to install the SandBlast Mobile Protect app on their device. If the none of CHKP_Status user groups haven’t been set yet for a device, then the device has not been synced with SandBlast Mobile Dashboard.
Tag Device Risk

For integration with BlackBerry UEM, the Device Risk tags are interpreted as "user groups" of "CHKP_Risk_None", "CHKP_Risk_Low", "CHKP_Risk_Medium", and "CHKP_Risk_High" with the values of "0" or "1".

We will use the CHKP_Risk user groups to determine when to enact certain policies or actions on the device. As an example, if CHKP_Risk_High is set to "1", then the device will be sent an in-app notification and blocked from running corporate apps or connecting to corporate assets.

Mitigation Group

The free-form Mitigation group is any unique name, such as "SBM_HighRisk", that SandBlast Mobile will place only devices determined to be at High Risk.

Note: This mitigation group must be created as a "user group" in BlackBerry UEM prior to using.

Please note that the Mitigation group does not provide the granularity of the different risk levels of the device, just high risk.

This method was the original way to group devices at high risk, and it is strongly recommended that you implement the CHKP_Risk and CHKP_Status user groups instead of using the free-form Mitigation group.

Controlling the Importing of Personally Identifiable Information (PII) from the UEM

The PII for devices (users) can be limited from being imported to SandBlast Mobile by configuring the "Import Personally Identifiable Information (PII)" section.

If all entries are turned off, then a placeholder information set for the email address will be placed in the Device Owner's Email, in the form of "Device UDID@mdm_vendor", such as bb30f0ab-92dd-4b84-ba02-351bbaaacc22@uem.mdm.
1. PII Control is configured in the **Settings > Device Management > Setting > MDM** service pop-up window.

![UEM Configuration](image)

2. Turning off PII Import, will result in the following Devices display in SandBlast Mobile.

![Device Display](image)
MDM Advanced Settings

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

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

![MDM Advanced Settings](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices. Values: 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. 100% for no threshold</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync – device will not be deleted if it will be resync from UEM during the threshold interval. Values: 0-48 hours</td>
</tr>
<tr>
<td>App sync interval</td>
<td>Interval to connect with UEM to sync app list. Values: 10-1440 minutes, in 10 minute intervals</td>
</tr>
</tbody>
</table>

**Note:** If you make changes to the default settings, click "Save" to have changes take effect.
# Configuring the UEM Platform

Now the we have completed the integration steps, we can continue with the configuration of the UEM platform.

For this process we will return to the BlackBerry UEM Console to complete the configuration.

**This chapter discusses the following:**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>35</td>
</tr>
<tr>
<td>Configuring UEM to Deploy SandBlast Mobile Protect app</td>
<td>36</td>
</tr>
<tr>
<td>Adding the SandBlast Mobile Protect App to Your App Catalog</td>
<td>36</td>
</tr>
<tr>
<td>AppStore iOS App – Add to Catalog</td>
<td>36</td>
</tr>
<tr>
<td>Android App – Add to Catalog</td>
<td>40</td>
</tr>
<tr>
<td>Creating an App Group (Optional)</td>
<td>44</td>
</tr>
<tr>
<td>Deploying SandBlast Mobile Protect app</td>
<td>47</td>
</tr>
<tr>
<td>Requiring the SandBlast Mobile Protect App to be Installed</td>
<td>48</td>
</tr>
<tr>
<td>Creating a Compliance Policy</td>
<td>48</td>
</tr>
<tr>
<td>Applying App Required Compliance Policy to User Provisioning Group</td>
<td>50</td>
</tr>
<tr>
<td>Device Out of Compliance – Missing SandBlast Mobile Protect App</td>
<td>52</td>
</tr>
<tr>
<td>Creating a Mitigation Process</td>
<td>55</td>
</tr>
<tr>
<td>Creating IT Policies</td>
<td>55</td>
</tr>
<tr>
<td>Applying the Policy to the User Mitigation Group</td>
<td>57</td>
</tr>
</tbody>
</table>

**Prerequisites**

1. BlackBerry UEM 12.6 or higher.
2. For **on-premise BlackBerry UEM Deployments**, the port used for the UEM Web Services API (default: TCP 18084) must be accessible remotely by the SandBlast Mobile servers through your firewall before trying to connect.
Configuring UEM to Deploy SandBlast Mobile Protect app

For more or updated information, please see BlackBerry’s documentation at http://help.blackberry.com/en/blackberry-uem/current/getting-started-blackberry-uem-and-blackberry-dynamics/zfd1473950276026.html

Adding the SandBlast Mobile Protect App to Your App Catalog

Now that BlackBerry UEM and Check Point SandBlast Mobile Dashboard are communicating, we can now start deploying the SandBlast Mobile Protect app to those devices that will be protected by Check Point SandBlast Mobile.

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

AppStore iOS App – Add to Catalog

For the iOS app, BlackBerry UEM can automatically deploy and configure the SandBlast Mobile Protect app registration server and key on an iOS device. It does require the user to launch the SandBlast Mobile Protect app to finish device registration. There are two possible deployment scenarios for iOS, using the Apple App Store app or the Enterprise iOS app that has been signed by your organization. This procedure describes deploying the Apple App Store app.

1. Navigate to Apps > Apps, and click the icon.
2. Select "iTunes" from the Store List.

![App Store Selection]

3. In the "App" field, enter "SandBlast Mobile Protect", select the appropriate store for your country, and click "Search" to search the store.

4. Select SandBlast Mobile Protect app as indicated below by clicking the "Add".
5. A pop-up an App Configuration window for "SandBlast Mobile Protect" will open.
6. Scroll down to bottom of the screen, and click "+" on the right-hand side of the "App configuration" table.
7. Select "Configure manually" from the drop-down.
8. On the "SandBlast Mobile Protect" configuration pop-up window, enter an App configuration name.
9. Click "+" and select "String" twice.
10. Add the following Key/Value pairs:

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lacoon Server Address</td>
<td>string</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>string</td>
<td>%SerialNumber%</td>
</tr>
</tbody>
</table>

11. Click "Save".
12. Click "Add" to finish adding the app to the app catalog.

**Android App – Add to Catalog**

BlackBerry UEM can automatically deploy, but not configure the SandBlast Mobile Protect app registration server and key on an Android device. Completing deployment requires the user to launch the SandBlast Mobile Protect app to finish device registration, by entering the registration server and registration key the user received via email.
1. Navigate to **Apps > Apps**, and click the icon.

2. Select "Google Play App" from the Store List.
3. Click "Open Google Play" and search for the app that you want to add. You can then copy and paste information from Google Play in the following steps and also download icons and screen shots.

4. In the App name field, type the app name, "SandBlast Mobile Protect".
5. In the App description field, type a description for the app.
6. In the Vendor field, type the name of the app vendor, "Check Point Software Technologies, Ltd."
7. In the App icon field, click Browse. Locate and select an icon for the app. The supported formats are .png, .jpg, .jpeg, or .gif.

**Note:** Do not use Google Chrome to download the icon because an incompatible .webp image is downloaded.
8. In the App web address from Google Play field, type the web address of the app in Google Play.

9. Click "Add".
Creating an App Group (Optional)

This is an optional step, but does provide a method of organizing Apps.

1. Navigating to **Apps > App groups**, click the icon.
2. On the "Add app group" pop-up window, enter in a name for the App group.
3. Click "+" on the "Assigned apps" section.
4. Enter in SandBlast into the Search box, and select the Android and iOS versions of the SandBlast Mobile Protect app.

5. Set the App configuration to "iOS Protect" for the iOS app.

6. Click "Add".
Deploying SandBlast Mobile Protect app

To deploy the SandBlast Mobile Protect app to devices that will be registered to the Check Point SandBlast Mobile solution we need to link the SandBlast Mobile Protect app in our app catalog to the User Groups we created in "Creating User Provisioning Groups" on page 13.

1. Navigating to Groups > User, click name of the User Provisioning Group, in our example "SBM_Syndc_Users".
2. Click Settings tab.

3. Click "+" on the "Assigned apps" section.

4. On the "Assign app" pop-up window, select the App Group we created in "Creating an App Group (Optional)" on page 44. If you didn't create an App Group, you would select both SandBlast Mobile Protect apps and assign them directly, selecting the iOS Configuration.

5. Click "Next".
6. Set the "Disposition" to "Required" for the App Group.

![Assign apps](image)

7. Click "Assign".

**Note:** Repeat the steps in this section for "Users_At_Risk". This will prompt the users who belong to "SBM_Syncd_Users" to install the SandBlast Mobile Protect app. Also, those users who are in the "Users_At_Risk" who uninstall the SandBlast Mobile Protect app will be out of compliance.

**Note:** Repeat the steps in this section for "SBM_AD_Users" and "SBM_Local_Users", but change the "Disposition" to "Optional" instead of "Required".

### Requiring the SandBlast Mobile Protect App to be Installed

The SandBlast Mobile Protect app is required by creating a Compliance Policy for iOS and Android devices, then assigning this compliance policy to the User Provisioning Group we created in "Creating User Provisioning Groups" on page 13.

**Creating a Compliance Policy**

The policy will specify the actions taken on all SandBlast Mobile devices that do not have required apps, such as SandBlast Mobile Protect, installed.
1. Navigate to **Policies and profiles**, and click the "Add a profile" link under "Compliance".

![Policies and profiles](image1)

2. Enter a Name for the policy, such as "Missing Required Apps", enter a description, and select the "iOS" tab.

3. Select "Required app is not installed" and set appropriate actions to be taken if the user doesn’t install the app.

![Add a compliance profile](image2)
4. Select the "Android" tab.
5. Select "Required app is not installed" and set appropriate actions to be taken if the user doesn’t install the app.

6. Click "Add".

**Applying App Required Compliance Policy to User Provisioning Group**

The policies created in the previous section are assigned to the user provisioning group created in "Creating User Provisioning Groups" on page 13, in our example "SBM_AD_Users" and "SBM_Local_Users". Because the users will remain in the "SBM_AD_Users" or "SBM_Local_Users" group while their devices are synchronized with SandBlast Mobile, the policies will remain in effect for all other user groups they belong to as long as they are not removed from this group.
1. Navigate to **Groups > User**, locate the user provisioning group, click group’s name link.
2. Select the "Settings" tab, and click "+" in the "IT policy and profiles" section.
3. Select "Compliance" from the pop-up list.

4. On the "Assign a Compliance profile" pop-up window, select the "Compliance Policy" we created in the previous section.
5. Click "Assign".

**Note:** Repeat these steps for "SBM_Local_Users", if you are using it.
**Note:** Any device that belongs to the User Provisioning Group(s) which require the SandBlast Mobile Protect apps to be installed ("SBM_Syncd_Users" and "Users_At_Risk") that hasn't installed the SandBlast Mobile Protect app will be out of compliance.

**Device Out of Compliance – Missing SandBlast Mobile Protect App**

1. BlackBerry UEM Console Home Screen indicates an "Out of Compliance" issue.
2. Clicking on the "Non-compliant" pie piece, opens a reporting window.


3. Device Details View indicates an "Out of Compliance" issue.
4. The user will receive an alert email as well as an in-app notification.
Creating a Mitigation Process

In this procedure, you will create a mitigation policy set to enforce compliance and mitigation policies against those devices that belong to the Users_At_Risk group.


Creating IT Policies

We will create IT Policies that will be enforced on devices that are at risk. In this section, we will create an IT Policy that will be used to enforce restrict the At Risk device in some manner.

Note: We will show a example policy, 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 and IT policies according to their internal security policy.

The policy will specify the actions taken on At Risk devices. In our example, we will disable the camera, but you might create a policy that disables access to the corporate network or assets.

1. Navigate to Policies and profiles, and click the "Add an IT policy" link under "IT policies".

2. Enter a Name for the policy, such as "High Risk Device Policy", select the "iOS" tab.
3. Under "Device functionality", unselect "Allow use of camera".
4. Select the "Android" tab.
5. Under "Native OS > Device functionality", select "Disable camera".

6. Scroll to "KNOX MDM > Device functionality", unselect "Allow camera".

7. Scroll to "KNOX Premium – Workspace > Device functionality", unselect "Allow camera".

8. Scroll to the bottom of the screen and click "Add".
Applying the Policy to the User Mitigation Group

Now that we have created the policy ("High Risk Device Policy") we want to enforce, we need to link this policy to our User Mitigation Group ("Users_At_Risk") we created in "Creating Local User Group(s)" on page 18.

1. Navigate to **Groups > User groups**, find the user mitigation group you created in "Creating Local User Group(s)" on page 18, in our example "Users_At_Risk", and click group name link.
2. On the user mitigation group detailed view, click the "Settings" tab.
3. On the "Settings" tab, click "+" on the "IT policy and profiles" section.
4. Select "IT policy".

5. On the "Assign an IT policy" pop-up window, select the IT policy we created in "Creating IT Policies" on page 55, in our example "High Risk Device Policy".

6. Click "Assign".
Note: Now any device placed into the user groups, CHKP_Risk_High, CHKP_Risk_Medium or CHKP_Status_Inactive, which are nested under Users_At_Risk will have the policy actions in the IT Policy ("High Risk Device Policy") acted upon it.

7. When all of these steps have been completed, your User Groups will look something like this:
Registering Devices to SandBlast Mobile

In this chapter we will cover the user experience of device registration with SandBlast Mobile.

This chapter discusses the following:

- Registration of an iOS Device ................................................................. 60
- Registration of an Android Device ......................................................... 62
- Redeployment of the SandBlast Mobile Protect App – iOS ...................... 63
- Redeployment of the SandBlast Mobile Protect App - Android ................ 63
- Resending SandBlast Mobile Activation Code ........................................... 64
**Registration of an iOS Device**

After the device is registered to the BlackBerry UEM system and the SandBlast Mobile Protect app has been "Assigned" to the User Provisioning Group ("SBM_Syncd_Users"), the user will be prompted to install the SandBlast Mobile Protect App. Users will be automatically assigned to "SBM_Syncd_Users" when their device has been provisioned within SandBlast Mobile. This keeps the users of experiencing registration issues if there is a time lag between device enrollment to BlackBerry UEM and that device being synchronized to the SandBlast Mobile Dashboard.

1. The user is prompted to install SandBlast Mobile Protect.
2. The user taps "INSTALL".
3. After the App has been installed on the iOS Device, the user only needs to launch the App to finish the registration.

4. The user will be prompted to install the SandBlast Mobile Protect App. The user taps "INSTALL".
5. 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 BlackBerry UEM.
6. The user is prompted to enable Notifications, Location, and Network Security.

7. Continue with enabling Network Security, and tap "Allow" to allow SandBlast Mobile Protect to add the needed VPN Configuration profile.
8. The user is prompted to enable SMS Phishing Protection.

9. Continue through Settings > Messages > Unknown & Spam, and make sure that SMS Phishing > Protect is enabled.

10. Returning to SandBlast Mobile Protect, tap "Done" to initialize the scanning of the device.

11. 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.
Registration of an Android Device

After the device is registered to the BlackBerry UEM system and the SandBlast Mobile Protect app has been "Assigned" to the User Provisioning Group ("SBM_Syncd_Users"), the user will be prompted to install the SandBlast Mobile Protect App.

1. The user is prompted by the UEM client to install the SandBlast Mobile Protect app, tapping "OK".
2. The user taps the "INSTALL", and taps "ACCEPT" to accept the permissions of the App. The App installs.
3. After the App is installed, the user must launch the App to finish its deployment and registration to Check Point SandBlast Mobile.
4. The App will automatically register.

5. The user is prompted to allow SandBlast Mobile Protect to make and manage phone calls. Tap "Allow".
6. The user is prompted to turn on Location, SMS, and Network Protection features. Tap "Allow all required permissions".
7. Tap "OK" to allow SandBlast Mobile Protect to configure a VPN connection. This is necessary for the Network Security Protection features of Safe Browsing and Anti-Phishing to work.
8. Tap "Allow" to allow SandBlast Mobile Protect to access this device's location.
9. Tap "Allow" to allow SandBlast Mobile Protect to provide SMS protection.
10. Tap "Enable" to configure Accessibility permissions for SandBlast Mobile Protect.
11. Scroll down and tap "SandBlast Mobile" and tap the toggle to turn Accessibility ON.

12. Continue with configuring the Accessibility permissions for SandBlast Mobile Protect. Tap "OK".
13. Return to SandBlast Mobile Protect.
14. 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.

Redeployment of the SandBlast Mobile Protect App – iOS

If the user removes the SandBlast Mobile Protect app, the device will be out of compliance. Because the iOS app is auto-configured, the user only needs to open the BlackBerry UEM client App Catalog, and choose to install SandBlast Mobile Protect.

Note: The instructions for installing and registration of the SandBlast Mobile Protect app are described in "Registration of an iOS Device" on page 60.

Redeployment of the SandBlast Mobile Protect App - Android

If the user removes the SandBlast Mobile Protect app, the device will be out of compliance. Because the Android app is auto-configured, the user only needs to open the BlackBerry UEM client App Catalog, and choose to install SandBlast Mobile Protect.
Note: The instructions for installing and registration of the SandBlast Mobile Protect app are described in "Registration of an Android Device" on page 62.

Resending SandBlast Mobile Activation Code

If the user requires the activation registration email/SMS to be resent to them, the administrator will log into the SandBlast Mobile Dashboard.

1. Navigating to the Devices tab, select the device to which to send activation code, and click "Send activation".

2. On the pop-up "Send Activation Message" window, select the type of message, and click "Send". If the device has a phone number assigned, the message could be sent via SMS text message as well.
Chapter 5

Testing High Risk Activity Detection and Policy Enforcement

1 – SandBlast Mobile sends risk notification to User’s Device
2 – SandBlast Mobile sends the risk level for User’s Device to BlackBerry BES12/UEM
3 – BlackBerry BES12/UEM activates the appropriate compliance policy for User’s Device based on security risk level

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 to the BlackBerry UEM system for that device.

BlackBerry UEM receives the group assignment change, and applies any policies belonging to that group (either by direct or indirect assignment).

In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, all the devices with the app, "Dropbox", installed will be identified to be at High Risk (CHKP_Risk_High) due to the blacklisted app, "Dropbox". The SandBlast Mobile Dashboard will notify the user, and mark the device as belonging to the CHKP_Risk_High group to the BlackBerry UEM system. The BlackBerry UEM System will then enforce policy actions specified in the IT policy, in our example "High Risk Device Policy". This mitigation process was the one we created in "Creating a Mitigation Process" on page 55.

This chapter discusses the following:

- Blacklisting a Test App .......................................................... 66
- View of Non-Compliant Device ........................................... 67
- SandBlast Mobile Protect App Notifications .............................. 67
- UEM Client App Notifications ............................................. 68
- Administrator View on the SandBlast Mobile Dashboard .......... 68
- Administrator View on the BlackBerry UEM Console .......... 69
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.

1. Log into the SandBlast Mobile Dashboard.
2. Navigate to App Analysis tab, and search for the app you wish to blacklist, in our example "Dropbox".
3. Click "Policy" link of "Default".
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".

5. Click "OK".

**View of Non-Compliant Device**

**SandBlast Mobile Protect App Notifications**

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

2. Once the issue has been remediated by the user, the system will update the security posture.
UEM Client App Notifications

1. The user will not be able to use the device’s camera, as specified in the compliance actions (policy) we created in "Creating IT Policies" on page 55, in our example "High Risk Device Policy" until the user removes the blacklisted app.

2. Your policy will probably block the device’s access to corporate networks and data by disabling VPN profiles, connections to email, and/or connecting to the Corporate Wi-Fi, until the issue is remediated.

Administrator View on the SandBlast Mobile Dashboard

1. From the SandBlast Mobile Dashboard, the Administrator will see that there are devices at high risk.
2. Clicking the High Risk will display a list of devices at high risk.
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".

**Administrator View on the BlackBerry UEM Console**

1. In the BlackBerry UEM Console, in the User Device Detail screen the Administrator can see that the user is now a member of the "CHKP_Risk_High" group and indirectly a member of the "Users_At_Risk" group, and that the IT policy "High Risk Device Policy" has been assigned.
## Appendix

### Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Value</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 SRP ID</td>
<td></td>
</tr>
<tr>
<td>UEM SandBlast Mobile Admin Username</td>
<td></td>
</tr>
<tr>
<td>UEM SandBlast Mobile Admin 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 user groups in UEM</td>
<td>CHKP_Status_Provisioned, CHKP_Status_Active, CHKP_Status_Inactive</td>
</tr>
<tr>
<td>Tag Device Risk (Boolean tags) become user groups 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.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>