Check Point SandBlast Mobile

UEM Integration Guide with MobileIron Core
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 MobileIron Core, 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 MobileIron Core. It provides a quick tour through the interface of the MobileIron Core Admin Portal 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** .......................................................... 1
  **Prerequisites** .......................................................................................................................... 1
  **MobileIron Core Admin Portal** ............................................................................................. 2
  **Creating an API Administrator Account (optional)** ............................................................. 2
    Create a Local User Account .................................................................................................. 3
    Assign Local User to the "Global" Space & Assign Administrator "Roles" ............................. 3
  **Creating a Device Provisioning Group** ............................................................................... 8
    Creating a Static Device Provisioning Group ....................................................................... 8
    Creating a Dynamic Device Provisioning Group ................................................................. 9
    Creating a Secondary Device Provisioning Group ............................................................... 10
  **Adding a Local User** ........................................................................................................... 12
  **Adding a Device to a User** .................................................................................................. 13
    Adding the Devices to the Device Provisioning Group ....................................................... 14
    Enrolling a Device to MobileIron Core .............................................................................. 15

**Chapter 2 Configuring the SandBlast Mobile Dashboard UEM Integration Settings** ........... 17
  **Prerequisites** ...................................................................................................................... 17
  **Configuring Device Management Integration Settings** .................................................. 18
    Multi-tags in SandBlast Mobile and Usage in MobileIron Core ........................................ 21
      Tag Device Status ............................................................................................................. 21
      Tag Device Risk ............................................................................................................... 21
      Tag Device TF .................................................................................................................. 21
    Mitigation Group ............................................................................................................... 22
    Controlling the Importing of Personally Identifiable Information (PII) from the UEM ....... 22
    MDM Advanced Settings ................................................................................................. 24

**Chapter 3 Configuring the UEM Platform** ............................................................................. 25
  **App Collection** .................................................................................................................. 26
  **Configuring MobileIron Core to Deploy SandBlast Mobile Protect app** ......................... 28
    Prerequisites ....................................................................................................................... 28
    Add the SandBlast Mobile Protect App to Your App Catalog ........................................... 28
      Adding the Android App to the App Catalog .................................................................. 28
      Adding the iOS App to the App Catalog ......................................................................... 30
      iOS App Deployment Configuration .............................................................................. 33
    Adding the SandBlast Mobile Protect apps to the Device Provisioning Group ................. 35
    Requiring the SandBlast Mobile Protect app to be Installed ............................................ 36
      Creating an App Control Rule ......................................................................................... 36
    Creating Compliance Actions Policy ............................................................................... 37
    Creating Security Compliance Rule (Enforcement) ............................................................ 38
    Applying the MDM Security Policy to the Device Provisioning Group ......................... 41
      Applying the MDM Security Policy to the Secondary Device Provisioning Group .......... 41
      Applying the MDM Security Policy to the Primary Device Provisioning Group .......... 42
  **Creating a Mitigation Process** ............................................................................................ 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Compliance Policy</td>
<td>43</td>
</tr>
<tr>
<td>Creating a Compliance Policy Group</td>
<td>45</td>
</tr>
<tr>
<td>Applying the Compliance Policy Group to the Device Provisioning Group</td>
<td>46</td>
</tr>
<tr>
<td>Chapter 4 Registering Devices to SandBlast Mobile</td>
<td>47</td>
</tr>
<tr>
<td>Registration of an iOS Device</td>
<td>48</td>
</tr>
<tr>
<td>Registration of an Android Device</td>
<td>50</td>
</tr>
<tr>
<td>Chapter 5 Testing High Risk Activity Detection and Policy Enforcement</td>
<td>53</td>
</tr>
<tr>
<td>Blacklisting a Test App</td>
<td>54</td>
</tr>
<tr>
<td>View of Non-Compliant Device</td>
<td>55</td>
</tr>
<tr>
<td>SandBlast Mobile Protect App Notifications</td>
<td>55</td>
</tr>
<tr>
<td>Mobile@Work In-App Notifications</td>
<td>55</td>
</tr>
<tr>
<td>Administrator View on the SandBlast Mobile Dashboard</td>
<td>56</td>
</tr>
<tr>
<td>Administrator View on the MobileIron Portal</td>
<td>57</td>
</tr>
<tr>
<td>Appendix</td>
<td>59</td>
</tr>
<tr>
<td>Integration Information</td>
<td>59</td>
</tr>
<tr>
<td>Creating the ManagedAppConfig.plist File</td>
<td>60</td>
</tr>
</tbody>
</table>
## 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>MobileIron Core Admin Portal</td>
<td>2</td>
</tr>
<tr>
<td>Creating an API Administrator Account (optional)</td>
<td>2</td>
</tr>
<tr>
<td>Create a Local User Account</td>
<td>3</td>
</tr>
<tr>
<td>Assign Local User to the &quot;Global&quot; Space &amp; Assign Administrator &quot;Roles&quot;</td>
<td>3</td>
</tr>
<tr>
<td>Creating a Device Provisioning Group</td>
<td>8</td>
</tr>
<tr>
<td>Creating a Static Device Provisioning Group</td>
<td>8</td>
</tr>
<tr>
<td>Creating a Dynamic Device Provisioning Group</td>
<td>9</td>
</tr>
<tr>
<td>Creating a Secondary Device Provisioning Group</td>
<td>10</td>
</tr>
<tr>
<td>Adding a Local User</td>
<td>12</td>
</tr>
<tr>
<td>Adding a Device to a User</td>
<td>13</td>
</tr>
<tr>
<td>Adding the Devices to the Device Provisioning Group</td>
<td>14</td>
</tr>
<tr>
<td>Enrolling a Device to MobileIron Core</td>
<td>15</td>
</tr>
</tbody>
</table>

### Prerequisites

1. MobileIron On-Premise Core and MobileIron Connected Cloud version 8.0 or higher, but NOT MobileIron Cloud. Please see the Integration Guide for MobileIron Cloud for details on integrating with MobileIron Cloud.
2. MobileIron Privacy Policy needs to collect “All Apps” from devices enrolled to SandBlast Mobile. See “App Collection” on page 26 for details on how to create a privacy policy.
MobileIron Core Admin Portal

1. Login to your MobileIron Core Admin Portal.

Creating an API Administrator Account (optional)

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

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

To create an "API" Administrator Account, follow this process.
Create a Local User Account

1. Navigate to Devices & Users > Users, click "Add" drop-down menu, and select "Add Local User".

2. On the pop-up window, fill in all the required (__) fields with the appropriate information, such as in the example below.

   ![Add New User Window]

   - User ID: sbm_admin
   - First Name: SBM
   - Last Name: Admin
   - Display Name: 
   - Password: *********
   - Confirm Password: *********
   - Email: mis_admin@checkpoint.com

3. Click "Save".

Assign Local User to the "Global" Space & Assign Administrator "Roles".

1. Navigate to Admin > Admins, select the created user, i.e. "sbm_admin", then click "Actions" drop-down menu, and select "Assign to Space".

   ![Assign to Space]

© 2018 Check Point Software Technologies Ltd. All rights reserved. | P. 3

October 18, 2018
2. Select the "Global" Space from the "Select Space" drop-down menu.

3. The required Admin Roles are:
   - Device Management > View device page, device details
   - Device Management > Apply and remove device label
   - Device Management > Edit custom device attribute values
   - Device Management > View dashboard
   - Privacy Controls > View apps in device details
   - Label Management > View label
   - Other Roles > API
4. In the "Device Management" section, select:
   - Device Management > View device page, device details
   - Device Management > Apply and remove device label
   - Device Management > Edit custom device attribute values
   - Device Management > View dashboard
5. Scroll down to the "Privacy Control" section, and select "View apps and ibooks in device details" and under the "Label Management" section, and select "View label".
6. Scroll down to "Other Roles" section, and select "API", required to enable SandBlast Mobile to interact with MobileIron Core.

7. Click "Save".

8. Finish the creation of the new admin account by logging out of the MobileIron Core Admin Portal, and then logging back in using the credentials you created in "Create a Local User Account" on page 3.

Note: Log out and log back into the MobileIron Core Admin Portal with your Service Administrator credentials to continue with the configuration.
Creating a Device Provisioning Group

A device provisioning group is used to tie devices, apps, and app configurations together for deployment. MobileIron Core calls a device provisioning group a "device label". This label will also be used in the SandBlast Mobile Protect app deployment process discussed in "Configuring MobileIron Core to Deploy SandBlast Mobile Protect app" on page 28.

There are two types of Labels, manual (static) and filter (dynamic). For a manual label, you need to select the devices you want to add and "Apply to Label" manually. For a filter label, you define criteria, and if the device created adhere to that criterion, then the device will be added to the label automatically.

Creating a Static Device Provisioning Group

For the Device Provisioning Group, we will create a manual label.

1. Navigate to Devices & Users > Labels, click "Add Label".

2. Enter a Name, a Description, and set the "Type" to "Manual".

3. Click "Save".
Creating a Dynamic Device Provisioning Group

If you prefer a dynamic label to be used to group all iOS and Android devices, do the following.

1. Navigate to Devices & Users > Labels, click "Add Label".

2. Enter a Name, a Description, and set the "Type" to "Filter".

3. Under "Criteria" select "All" of the following rules are true, and select "User Fields > LDAP > Group > Name", select "Equals" from the drop-down choices, and enter in the AD Group Name.

4. If you want to exclude retired devices from search results, make sure that the checkbox is selected.

5. Click "Save".
Creating a Secondary Device Provisioning Group

**Note:** If all of the Android and iOS devices within your MobileIron Core environment will be registered to SandBlast Mobile, then it is recommended to create a second device provisioning group (label). Only devices in this group will be forced to install SandBlast Mobile Protect once their device has been synchronized with the SandBlast Mobile Dashboard. This will improve the user experience and avoid them trying to install SandBlast Mobile Protect app and register with SandBlast Mobile prior to their device being provisioned within SandBlast Mobile Dashboard.

1. Navigate to **Devices & Users > Labels**, click "Add Label".
2. Enter a Name, a Description, and set the "Type" to "Filter".
3. Under "Criteria" select "Any" of the following rules are true, and select:
   a. Custom Attributes > Device Attributes > CHKP_Status Equals Provisioned
   b. Click "+" icon at the end of the first rule
   c. Custom Attributes > Device Attributes > CHKP_Status Equals Active
   d. Click "+" icon at the end of the second rule
   e. Custom Attributes > Device Attributes > CHKP_Status Equals Inactive
   f. Check the "Exclude retired devices from search results" checkbox.

4. Click "Save".
Adding a Local User

There are two ways to add a user, "Add Local User", or "Resync With LDAP". We are going to show how to add a local user using the "Add Local User" method.

1. Navigate to Devices & Users > Users, click "Add" drop-down menu, and select "Add Local User".

2. On the pop-up window, fill in all the required fields with the appropriate information, such as in the example below.

3. Click "Save".
**Adding a Device to a User**

1. You can add a device to an existing user by navigating to **Devices & Users > Devices**, and clicking the **Add** drop-down menu, and select "Add Single Device".

![Device Management Interface](image)

2. On the "Add Single Device" pop-up window, fill in all the required (|) fields with the appropriate information, such as in the example below.
   a. In the "User" field, search for the user you want to add a device to by entering the first 3 characters, and select the user from the list.
   b. Select "Device Platform" of "Android" or "iOS".
   c. If this device doesn't have a phone number, check the "This device has no phone number." checkbox. Otherwise, fill in the appropriate "Country", "Operator", and "Mobile" number.
   d. Select the Ownership: "Corporate" or "Employee Owned".

![Add Single Device Window](image)

3. Click "Register".
4. The "Registration Instructions" that will be sent to the user.

**Note:** Repeat these steps to add another user and/or device.
Adding the Devices to the Device Provisioning Group

**Note:** This step is only required if you created a "manual" device provisioning group in "Creating a Device Provisioning Group" on page 8.

1. Navigate to **Devices & Users > Devices**, select the devices added in "Adding a Device to a User" on the previous page, and click "Actions" drop-down menu, and select "Apply to Label".

2. In the "Apply to Labels" pop-up window, select the provisioning label you created in "Creating a Device Provisioning Group" on page 8.

3. Click "Apply".
Enrolling a Device to MobileIron Core

1. Visit MobileIron Core documentation by navigating to your admin profile menu, and selecting "Help"

   ![MobileIron Core Admin Portal Screenshot]


   **Note:** At this point, we have all the information we will need to configure the Device Management Settings in the SandBlast Mobile Dashboard. We are going to do that and then return to the MobileIron Core Admin Portal to configure the SandBlast Mobile Protect app deployment settings as well as the mitigation policies.

   From Our Examples:
   - Server = https://m.mobileiron.net/cptme
   - API Admin Username/Password = sbm_admin\<hidden>\>
   - Device Provisioning Label(s) = CPTME_SBM
Configuring the SandBlast Mobile Dashboard UEM Integration Settings

This chapter discusses the following:

Prerequisites ........................................................................................................................................... 17
Configuring Device Management Integration Settings ................................................................. 18
Multi-tags in SandBlast Mobile and Usage in MobileIron Core ...................................................... 21
Tag Device Status ............................................................................................................................... 21
Tag Device Risk ................................................................................................................................. 21
Tag Device TF ...................................................................................................................................... 21
Mitigation Group ................................................................................................................................. 22
Controlling the Importing of Personally Identifiable Information (PII) from the UEM .................. 22
MDM Advanced Settings .................................................................................................................... 24

Prerequisites
You will need the following details from your MobileIron Core Deployment:

1. **Server**: The URL to your MobileIron Core, usually the same as the MobileIron Core Admin Portal URL.
2. **MobileIron API 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.
3. **Label(s)**: This is the MobileIron Core device provisioning group (label) to which the devices to be registered to SandBlast Mobile are linked, and will be integrated with the SandBlast Mobile Dashboard. This is the label we created in "Creating a Device Provisioning Group" on page 8. Multiple labels can be integrated with the one SandBlast Mobile Dashboard instance by entering each label name separated with a semicolon (;).
4. **For on-premise UEM environments**, port 443 (HTTPS) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the MobileIron Core system before trying to connect.
5. **Delete any existing devices in the SandBlast Mobile Dashboard**.

**Note**: Only the devices are synchronized from MobileIron Core 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.

**Note**: There is a table in "Integration Information" on page 59 that you can record your settings for easy reference.
Configuring Device Management Integration Settings

1. Navigate to Settings > Device Management > Setting.
2. Select "MobileIron Core" 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 MobileIron Core deployment, such as those you may have created in "Preparing the UEM Platform for Integration" on page 1.
5. There is no need to enter in the Mitigation label as this method has been replaced with the granular multi-tag capability.

6. Turn ON "Tag Device Status" and "Tag Device Risk". For our purposes, we are not enabling the "Tag Device TF", but it provides a list of threat factors associated with the Security Risk level, such as TF_BACKUP_TOOL, etc. A description of how these Tags work is provided in "Multi-tags in SandBlast Mobile and Usage in MobileIron Core" on page 21.

7. If you want to limit the type of Personally Identifiable Information (PII) from being imported from the MobileIron Core Admin Portal to SandBlast Mobile Dashboard, you can turn OFF "Import device name", "Import Device phone #", and/or "Device owner email". A description of what these settings do is provided in "Controlling the Importing of Personally Identifiable Information (PII) from the UEM" on page 22.
8. Click "VERIFY". If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the MobileIron Core system, you will be able to click "SAVE" to finish configuration.

![Mobile Iron Configuration Screen](image-url)
Multi-tags in SandBlast Mobile and Usage in MobileIron Core

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 "custom device attributes" in MobileIron Core.

The Multi-tags are automatically created in MobileIron Core Admin Portal when enabled during the Device Management Configuration process in SandBlast Mobile Dashboard.

There are 3 Status states:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioned</td>
<td>When a device is synchronized for the first time in SandBlast Mobile Dashboard</td>
</tr>
<tr>
<td>Active</td>
<td>After the user has installed and registered to SandBlast Mobile</td>
</tr>
<tr>
<td>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 level:

- None
- Low
- Medium
- 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). Once the High Risk issue has been remediated (SMS deleted), then the device will be marked as at Low Risk (CHKP_Risk = Low). Once the Low Risk issue has been remediated, the device will be marked as None (No Risk).

**Tag Device Status**

For integration with MobileIron Core, the Device Status tag is interpreted as a "custom device attribute" of "CHKP_Status" with the values of Provisioned, Active, or Inactive.

We will use the CHKP_Status custom device attribute to determine when to prompt the user to install the SandBlast Mobile Protect app on their device. If the CHKP_Status custom device attribute hasn’t been set yet, then the device has not been synced with SandBlast Mobile Dashboard.

**Tag Device Risk**

For integration with MobileIron Core, the Device Risk tag is interpreted as a "custom device attribute" of "CHKP_Risk" with the values of None, Low, Medium, or High.

We will use the CHKP_Risk custom device attribute to determine when to enact certain policies or actions on the device. If the CHKP_Risk is High or Medium, then the device will be sent an in-app notification and blocked from running corporate apps.

**Tag Device TF**

The Threat Factor tag (CHKP_TF) is a list of threat factors associated with the Security Risk level, such as TF_BACKUP_TOOL, etc. These threat factors can be used to provide additional detail and granularity of the current
Risk level, however, they are not necessarily appropriate for policy triggers. The CHKP_TF value is a sort of free-form comma separated string of threat factors from the BRE database.

**Mitigation Group**

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

**Note:** This group must be created as a "manual" label in MobileIron Core prior to configuring in SandBlast Mobile Dashboard.

Please note that the Mitigation Group does not provided 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 custom device attributes 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 "UEMDeviceUDID@mdm_vendor", such as bb30f0ab-92dd-4b84-ba02-351bbaaacc22@mobileiron.mdm.
1. PII Control is configured in the **Settings > Device Management > Setting > MDM service** pop-up window.

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

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

![Diagram of Device Management Advanced Settings]

<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 re-sync 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.
Chapter 3

Configuring the UEM Platform

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

For this process we will return to the MobileIron Core Admin Portal to complete the configuration.

This chapter discusses the following:

- **App Collection** ................................................. 26
- **Configuring MobileIron Core to Deploy SandBlast Mobile Protect app** ....................................................... 28
  - **Prerequisites** .................................................. 28
  - **Add the SandBlast Mobile Protect App to Your App Catalog** .............................................................. 28
    - Adding the Android App to the App Catalog .................................................................................. 28
    - Adding the iOS App to the App Catalog .................................................................................. 30
    - iOS App Deployment Configuration ....................................................................................... 33
  - **Adding the SandBlast Mobile Protect apps to the Device Provisioning Group** .............................. 35
- **Requiring the SandBlast Mobile Protect app to be Installed** .............................................................. 36
  - **Creating an App Control Rule** .................................................................................................. 36
  - **Creating Compliance Actions Policy** .......................................................................................... 37
  - **Creating Security Compliance Rule (Enforcement)** .............................................................................. 38
  - **Applying the MDM Security Policy to the Device Provisioning Group** ........................................ 41
    - Applying the MDM Security Policy to the Secondary Device Provisioning Group ........................ 41
    - Applying the MDM Security Policy to the Primary Device Provisioning Group .......................... 42
  - **Creating a Mitigation Process** .................................................................................................. 43
  - **Creating a Compliance Policy** .................................................................................................. 43
  - **Creating a Compliance Policy Group** ....................................................................................... 45
    - Applying the Compliance Policy Group to the Device Provisioning Group ............................... 46
**App Collection**

The application list needs to be collected by MobileIron Core Admin Portal from the devices to be enrolled to SandBlast Mobile. This can be accomplished by creating a specific Privacy Policy.

1. Navigate to **Policies & Configs > Policies**, click "Add New" drop-down menu, and select "Privacy".

![Add New Privacy Policy](image)

2. In the "New Privacy Policy" pop-up window, enter in a name and description.

3. Make sure that "Apps" is set to "All Apps" and "iOS Installed App Inventory" is set to "All Apps".

![New Privacy Policy](image)

4. Click "Save".
5. Now we want to apply this new privacy policy to the Device Provisioning Group we created earlier in this section, in our example "CPTME_SBM".

6. Select the Privacy Policy we just created, click "More Actions" drop-down menu, and select "Apply To Label".

7. On the "Apply To Label" pop-up window, search for and select the Device Provisioning Group name, in our example "CPTME_SBM".

8. Click "Apply".
Configuring MobileIron Core to Deploy SandBlast Mobile Protect app

Prerequisites

1. SandBlast Mobile Gateway/Server: Server name of the SandBlast Mobile gateway/server which is gw.locsec.net.

Add the SandBlast Mobile Protect App to Your App Catalog

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

Adding the Android App to the App Catalog

The Android SandBlast Mobile Protect App can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

1. Navigate to Apps > App Catalog, and select the "Add".

2. Select "Google Play" from the Store List.
3. In "Application Name" field, enter "SandBlast Mobile Protect", and click "Search". Select the "SandBlast Mobile Protect" app as indicated below.

4. Click "Next".

5. On the "Describe" pane, there are no changes needed.

6. Click "Next".
7. On the "App Store" pane, check only the "Feature this App in the Apps@Work catalog" checkbox.

8. Click "Finish".

Adding the iOS App to the App Catalog

1. Navigate to Apps > App Catalog, and select the "Add".

2. Select "iTunes" from the Store List.
3. In "Application Name" field, enter SandBlast Mobile Protect, select the appropriate "App Store", and click "Search". Select SandBlast Mobile Protect app as indicated below.

4. Click "Next".

5. On the "Describe" pane, there are no changes needed. click "Next".
6. On the "App Store" pane, check only the "This is a Free App", the "Allow conversion of apps from unmanaged to managed in Apps@Work (iOS 9 or later)", and the "Feature this App in the Apps@Work catalog" checkboxes.

7. Click "Next".

8. On the "App Configuration" pane, select the "Send installation request on device registration or sign-in", the "Remove app when MDM profile is removed", and the "Remove app when MDM profile is removed" checkboxes.

9. Click "Finish".
**iOS App Deployment Configuration**

The iOS SandBlast Mobile Protect App can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration. This process walks you through assigning configuration parameters to be used in configuring the app per user.

1. Before you can add a new configuration, you must create the ManagedAppConfig.plist file if you haven’t already using the instructions in “Creating the ManagedAppConfig.plist File” on page 60.
2. Navigate to **Policies & Configs > Configurations**, click "Add New" drop-down, selecting "iOS and OS X" > "Managed App Config".
3. On the resulting "New Managed App Config Setting" pop-up window, enter a Name, Description, "BundleId" of "com.checkpoint.capsuleprotect", and click "Choose File" and select the "ManagedAppConfig.plist" file you created at the beginning of this procedure.

4. Click "Save".

5. Select the just created Managed App Config, and click "More Actions" drop-down menu, and select "Apply To Label".

6. In the "Apply To Labels" pop-up window, select the primary or secondary device provisioning group (label) you created in "Creating a Device Provisioning Group" on page 8.

7. Click "Apply".
Adding the SandBlast Mobile Protect apps to the Device Provisioning Group

1. Navigating to Apps > App Catalog, select both the iOS and Android SandBlast Mobile Protect apps.

2. Then, click "Actions" drop-down, and select "Apply To Labels".

3. In the "Apply to Labels" pop-up window, select the provisioning label you created in "Creating a Device Provisioning Group" on page 8.

4. Click "Apply".
Requiring the SandBlast Mobile Protect app to be Installed

The SandBlast Mobile Protect app is required by creating an App Control policy which is referenced in a MDM Security Policy, creating a Compliance Actions Policy method which is referenced in the MDM Security Policy, and by applying the MDM Security Policy to the Device Provisioning Label we created in "Creating a Device Provisioning Group" on page 8.

Creating an App Control Rule

If we want to ensure that the SandBlast Mobile Protect app is installed on the iOS and Android devices, we need an App Control set to force the iOS and Android devices to have the SandBlast Mobile Protect app installed.

1. Navigate to **Apps > App Control**, click "Add".

2. On the "Add App Control Rule" pop-up window, configure a rule name, select the "Required" radio, and put in the following Rule Entries:
   a. App Identifier Equals > com.checkpoint.capsuleprotect > iOS
   b. App Identifier Equals > com.lacoon.security.fox > Android

3. Click "Save".
Creating Compliance Actions Policy

1. Navigate to Policies & Configs > Compliance Actions, and click "Add".

2. On the "Add Compliance Action" pop-up window, configure the policy name, in our example "Non-Compliant Device Actions", and select:
   a. "Enforce Compliance Actions Locally on Devices".
   b. "ALERT" > "Send a compliance notification or alert to the user",
   c. "BLOCK ACCESS" > "Block email access and AppConnect apps", and
   d. "QUARANTINE" > "Quarantine the device".

3. Click "Save".
Creating Security Compliance Rule (Enforcement)

Now that we have the compliance action set and an App Control Rule, we will link these to a new policy.

1. Navigate to Policies & Configs > Policies, click "Add New" drop-down menu, and select "Security".

![Policies & Configs](image1)

2. On the "New Security Policy" pop-up window, enter a policy name.

![New Security Policy](image2)
3. Scroll down to "Access Control > For All Platforms" section, and select the compliance action policy we created in "Creating Compliance Actions Policy" on page 37, in our example, "Non-Compliant Device Actions" when a device violates following App Control rules.

4. Move the App Control Rule we created in "Creating an App Control Rule" on page 36 from "Available" to "Enabled" in the "Required" Rule Type area.
5. Scroll down to "For iOS devices", and select the compliance action policy we created in "Creating Compliance Actions Policy" on page 37, in our example, "Non-Compliant Device Actions" "when device MDM is deactivated".
6. Scroll down to "For Android devices", and select the compliance action policy we created in "Creating Compliance Actions Policy" on page 37, in our example, "Non-Compliant Device Actions" "when device administrator is deactivated".

7. Click "Save".

**Applying the MDM Security Policy to the Device Provisioning Group**

**Applying the MDM Security Policy to the Secondary Device Provisioning Group**

**Note:** Skip this step if you are NOT using a Secondary Device Provisioning Group.

1. Navigate to Policies & Configs > Policies, select the Security Policy, click "More Actions" drop-down menu, and select "Apply To Label".
2. On the "Apply To Labels" pop-up window, select the Secondary Device Provisioning Label.

3. Click "Apply".

Applying the MDM Security Policy to the Primary Device Provisioning Group

Note: Skip this step if you used a Secondary Device Provisioning Group.

1. Navigate to Policies & Configs > Policies, select the Security Policy, click "More Actions" drop-down menu, and select "Apply To Label".

2. On the "Apply To Labels" pop-up window, select the Device Provisioning Label.

3. Click "Apply".
Creating a Mitigation Process

In this section, you will reference a custom device attribute (CHKP_Risk) SandBlast Mobile Dashboard will use to indicate the risk level of any device in High, Medium, or Low Risk, or None for device with No Risk as determined by the SandBlast Mobile Analysis. This custom device attribute, CHKP_Risk, will allow the MobileIron Core system to identify which devices are at risk and to enforce actions and policies based on risk level. To learn more about the CHKP_Risk multi-tag, please see "Tag Device Risk" on page 21 for more information.

In this procedure, you will create a Compliance Policy Rule, Compliance Policy Group and apply the Compliance Policy Group to the Device Provisioning Label.

Creating a Compliance Policy


2. Enter the Rule Name and a description.
3. Select Custom Attributes > Device Attributes > CHKP_Risk from the "Field" pulldown menu.
4. Select "Equals" from the "Operator" pulldown menu.
5. Enter in "High" in the "Value" field.
6. Make sure "Exclude retired devices from search results" is selected.
7. And select the Compliance Action you created in the "Creating Compliance Actions Policy" on page 37.

8. Click "Save".
9. If you want to apply the Compliance Action to devices whose CHKP_Risk level is set to High or Medium, do the following:
   a. Enter the Rule Name and a description.
   b. Select "Any" for the Condition.
   c. Select Custom Attributes > Device Attributes > CHKP_Risk from the "Field" pulldown menu.
   d. Select "Equals" from the "Operator" pulldown menu.
   e. Enter in "High" in the "Value" field.
   f. Click "+" icon at the end of the "Value" field to add another line.
   g. Select Custom Attributes > Device Attributes > CHKP_Risk from the "Field" pulldown menu.
   h. Select "Equals" from the "Operator" pulldown menu.
   i. Enter in "Medium" in the "Value" field.
   j. Make sure "Exclude retired devices from search results" is selected.
   k. And select the Compliance Action you created in the "Creating Compliance Actions Policy" on page 37.
Creating a Compliance Policy Group

Now that we have a Compliance Policy Rule, we can create Compliance Policy Group that will be applied to our Device Provisioning Group to enforce on devices that are at High or Medium Risk.

1. Navigate to Policies & Configs > Compliance Policies > Compliance Policy Group, and click "Add".

![Compliance Policy Group](image)

2. Enter in a Group Name and a description.
3. Select the Compliance Rule and click right arrow to select it.

![Select Compliance Rule](image)

4. Click Save.
Applying the Compliance Policy Group to the Device Provisioning Group

Once we have created the policies we want to enforce, we need to link those policies to our Device Provisioning Group we created in "Creating a Device Provisioning Group" on page 8.

1. Navigate to **Policies & Configs > Compliance Policies > Compliance Policy Group**, select the policy group you created in "Creating a Compliance Policy Group" on the previous page, click "Actions" drop-down menu, and select "Apply to Labels".

2. On the "Apply to Label" pop-up window, select the Device Provisioning Group label, in our example, CPTME_SBM.

3. Click "Apply".

**Note:** Now any device in the Device Provisioning Group ("CPTME_SBM") that has the "CHKP_Risk" custom attribute is set to "High" or "Medium" by the SandBlast Mobile system will be acted upon by the Compliance Policy Rules that are included in the Compliance Policy Group ("CPTME_SBM_AT_RISK_DEVICES").
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 ................................................. 48
- Registration of an Android Device ......................................... 50
Registration of an iOS Device

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

1. The user taps "INSTALL".
2. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration.

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

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

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

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

10. 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 synchronized to the SandBlast Mobile Dashboard, the user will navigate in the Mobile@Work app’s menu to "Apps@Work".

1. The user taps on the SandBlast Mobile Protect app to open the App Catalog.
2. The user taps the "INSTALL", and the user is taken to the Google Play Store.

3. The user taps the "INSTALL", and taps "ACCEPT" to accept the permissions of the App. The App installs.
4. After the App is installed, the user must launch the App to finish its deployment and registration to Check Point SandBlast Mobile.
5. The App will automatically register.
6. The user is prompted to allow SandBlast Mobile Protect to make and manage phone calls. Tap "Allow".
7. The user is prompted to turn on Location, SMS, and Network Protection features. Tap "Allow all required permissions".
8. 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.
9. Tap "Allow" to allow SandBlast Mobile Protect to access this device's location.
10. Tap "Allow" to allow SandBlast Mobile Protect to provide SMS protection.
11. Tap "Enable" to configure Accessibility permissions for SandBlast Mobile Protect.
12. Scroll down and tap "SandBlast Mobile", and tap the toggle to turn Accessibility ON.
13. Continue with configuring the Accessibility permissions for SandBlast Mobile Protect. Tap "OK".
14. Return to SandBlast Mobile Protect.
15. 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.
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 MobileIron Core
3 – MobileIron Core 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 CHKP_Risk custom attribute value to the MobileIron Core system for that device.

MobileIron Core receives the risk state change, and upon recognizing the CHKP_Risk value tied to a Compliance Policy Rule, enacts that policy.

In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, the user’s device will be identified to be at High Risk (CHKP_Risk = High) due to the blacklisted app, "Dropbox", being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device as High Risk (CHKP_Risk = High) to the MobileIron Core system. The MobileIron Core system will then enforce policy actions specified in the compliance policy. This mitigation process was the one we created in "Creating a Mitigation Process" on page 43.

This chapter discusses the following:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisting a Test App</td>
<td>54</td>
</tr>
<tr>
<td>View of Non-Compliant Device</td>
<td>55</td>
</tr>
<tr>
<td>SandBlast Mobile Protect App Notifications</td>
<td>55</td>
</tr>
<tr>
<td>Mobile@Work In-App Notifications</td>
<td>55</td>
</tr>
<tr>
<td>Administrator View on the SandBlast Mobile Dashboard</td>
<td>56</td>
</tr>
<tr>
<td>Administrator View on the MobileIron Portal</td>
<td>57</td>
</tr>
</tbody>
</table>
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 iOS will be blacklisted which will result in all Dropbox numbered release versions for iOS 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".

   ![Image]

2. The user will not be able to access their corporate data or networks from this device until they alleviate the risk level by uninstalling Dropbox.

Mobile@Work In-App Notifications

1. Checking the Mobile@Work app, the user can see that their device is out of compliance and that they will be unable to access corporate resources.

   ![Image]

2. The user will not be able to access their corporate data or networks from this device until they alleviate the risk level by uninstalling Dropbox.
**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 blacklisted app, "Dropbox".

---

© 2018 Check Point Software Technologies Ltd. All rights reserved. | P. 56

October 18, 2018
Administrator View on the MobileIron Portal

1. In the MobileIron Core Admin Portal from the Dashboard tab, the Administrator can see that one or more devices are "Out of Compliance".

2. The MobileIron Core Admin Portal shows that the device has its custom attribute "CHKP_Risk" set to "High" on the CUSTOM ATTRIBUTES tab.
3. Viewing the COMPLIANCE tab, the Administrator can see what Compliance Policy Rules are in violation and which Compliance Actions were applied.

4. The user will not be able to access their corporate data or networks from this device until they alleviate the risk level by uninstalling Dropbox.
# Appendix

## Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron Core Server/API URL</td>
<td></td>
</tr>
<tr>
<td>MobileIron Core API Admin Username</td>
<td></td>
</tr>
<tr>
<td>MobileIron Core API Admin Password</td>
<td></td>
</tr>
<tr>
<td>MobileIron Core Device Provisioning Group(s)</td>
<td></td>
</tr>
<tr>
<td>MobileIron Core Mitigation group (Device Group) (deprecated)</td>
<td></td>
</tr>
<tr>
<td>Tag Device Risk (CHKP_Risk)</td>
<td>None, Low, Medium, or High</td>
</tr>
<tr>
<td>Tag Device Status (CHKP_Status)</td>
<td>Provisioned, Active, or Inactive</td>
</tr>
<tr>
<td>Tag Device Threat Factor (CHKP_TP)</td>
<td>Free-form information provided by BRE</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>
Creating the ManagedAppConfig.plist File

Follow the steps below to create the plist file used for auto-deploy of the SandBlast Mobile Protect device to iOS devices.

1. Copy the following text to a text editor (e.g. Notepad)

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
   <plist version="1.0">
     <dict>
       <key>DEVICE_UDID</key>
       <string>$DEVICE_UDID$</string>
       <key>DEVICE_MAC</key>
       <string>$DEVICE_MAC$</string>
       <key>DISPLAY_NAME</key>
       <string>$DISPLAY_NAME$</string>
       <key>EMAIL</key>
       <string>$EMAIL$</string>
       <key>FIRST_NAME</key>
       <string>$FIRST_NAME$</string>
       <key>LAST_NAME</key>
       <string>$LAST_NAME$</string>
       <key>USERID</key>
       <string>$USERID$</string>
       <key>Lacoon Server Address</key>
       <string>gw.locsec.net</string>
     </dict>
   </plist>
   ```

2. Save As… Naming the file to "ManagedAppConfig.plist", and Exit the file.
3. Use this file in "iOS App Deployment Configuration" on page 33.