SandBlast Mobile for MobileIron Core

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 2021 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>3</td>
</tr>
<tr>
<td>About Check Point SandBlast Mobile</td>
<td>5</td>
</tr>
<tr>
<td>General Workflow</td>
<td>5</td>
</tr>
<tr>
<td>Introduction to the SandBlast Mobile Integration Guide</td>
<td>6</td>
</tr>
<tr>
<td>Solution Architecture</td>
<td>7</td>
</tr>
<tr>
<td>Preparing UEM Platform for Integration</td>
<td>9</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>9</td>
</tr>
<tr>
<td>General Workflow</td>
<td>10</td>
</tr>
<tr>
<td>Enabling the SandBlast Mobile Protect app on the MobileIron Core Devices</td>
<td>10</td>
</tr>
<tr>
<td>Creating API Account for Integration with the SandBlast Mobile</td>
<td>10</td>
</tr>
<tr>
<td>Creating a Local User Account</td>
<td>10</td>
</tr>
<tr>
<td>Assigning the SandBlast Mobile API Administrator to the Local User Account</td>
<td>11</td>
</tr>
<tr>
<td>Creating a Device Provisioning Group for SandBlast Mobile</td>
<td>15</td>
</tr>
<tr>
<td>Creating a Static Device Provisioning Group</td>
<td>16</td>
</tr>
<tr>
<td>Creating a Dynamic Device Provisioning Group (LDAP)</td>
<td>17</td>
</tr>
<tr>
<td>Creating a Secondary Device Provisioning Group (Optional)</td>
<td>19</td>
</tr>
<tr>
<td>Configuring Application Collection</td>
<td>21</td>
</tr>
<tr>
<td>To configure the UEM to collect the app lists</td>
<td>21</td>
</tr>
<tr>
<td>To apply the Application Collection Policy to the Device Provisioning Group</td>
<td>22</td>
</tr>
<tr>
<td>Setting Parameters for the Device Protection</td>
<td>24</td>
</tr>
<tr>
<td>Adding Local Users to the SandBlast Mobile Protect App</td>
<td>24</td>
</tr>
<tr>
<td>Adding a Device to a User</td>
<td>25</td>
</tr>
<tr>
<td>Adding Devices to the Device Provisioning Group</td>
<td>26</td>
</tr>
<tr>
<td>Enrolling a Device to MobileIron Core</td>
<td>27</td>
</tr>
<tr>
<td>Configuring the Check Point SandBlast Mobile Dashboard Integration Settings</td>
<td>28</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Integration Settings</td>
<td>28</td>
</tr>
<tr>
<td>Configuring UEM to Deploy the SandBlast Mobile Protect app</td>
<td>38</td>
</tr>
<tr>
<td>Adding the SandBlast Mobile Protect app to your App Catalog</td>
<td>38</td>
</tr>
<tr>
<td>iOS App Deployment Configuration</td>
<td>43</td>
</tr>
<tr>
<td>Automatic Activation of SandBlast Mobile: Prompt the Protect app installation</td>
<td>47</td>
</tr>
<tr>
<td>To prompt the SandBlast Mobile Protect app installation on your devices</td>
<td>47</td>
</tr>
<tr>
<td>Connecting the SandBlast Mobile Protect app to your Device</td>
<td>47</td>
</tr>
<tr>
<td>Creating a Protect app Group</td>
<td>48</td>
</tr>
<tr>
<td>Creating an App Control Rule</td>
<td>49</td>
</tr>
<tr>
<td>Creating a Compliance Actions Policy for the Organization Devices</td>
<td>50</td>
</tr>
<tr>
<td>Creating a Security Compliance Rule (Enforcement)</td>
<td>51</td>
</tr>
</tbody>
</table>
Applying the MDM Security Policy to the Device Provisioning Group........................................55
Creating a Mitigation Process ........................................................................................................57
Creating a Compliance Policy for the Devices at Risk ....................................................................57
Creating a Compliance Policy Group ...............................................................................................59
Applying the Compliance Policy Group to the Device Provisioning Group.....................................60

Deploying the SandBlast Mobile Protect app automatically (Zero Touch Deployment) [Optional] .61

Using Android Enterprise with SandBlast Mobile .............................................................................66
Profiles ..............................................................................................................................................66
Android Enterprise Deployment Scenarios ..........................................................................................66
Configuring SandBlast Mobile Protect app to Protect your Devices ..................................................67
Deploying Android Enterprise on your Devices ...................................................................................67
Policies ................................................................................................................................................69
Risk Handling ......................................................................................................................................69

Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement .......................72
Deploying the SandBlast Mobile Protect app on the Devices ...............................................................72

Testing High Risk Activity Detection and Policy Enforcement .........................................................75
Blacklisting a Test App ........................................................................................................................75
View of a Non-Compliant Device ......................................................................................................77
Administrator View on the SandBlast Mobile Dashboard ..................................................................78
Administrator View on the MobileIron Core Console ........................................................................79

Appendix .............................................................................................................................................81
Integration Information .........................................................................................................................81
About Check Point SandBlast Mobile

Check Point SandBlast Mobile is the most complete threat defense solution that prevents emerging fifth generation cyber attacks and allows workers to safely conduct their businesses. This technology prevents threats to the OS, apps, and network. It scores the highest threat catch rate in the industry and does not hit performance or user experience.

SandBlast Mobile delivers threat prevention technology that:

- Performs advanced app analysis to detect known and unknown threats.
- Prevents man-in-the-middle attacks on both cellular and Wi-Fi networks.
- Blocks phishing attacks on all apps: email, messaging, social media.
- Prevents sensitive data distribution from infected devices to botnets.
- Blocks infected devices from accessing corporate applications and data.
- Mitigates threats independently from user action or mobile management platforms.

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

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

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

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

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

General Workflow

1. Prepare your MobileIron Core UEM platform for the Check Point SandBlast Mobile Protect app integration. See Preparing UEM Platform for Integration.
2. Configure your MobileIron Core UEM to deploy the Check Point SandBlast Mobile Protect app. See Configuring UEM to Deploy the SandBlast Mobile Protect app.
3. Configure the Check Point SandBlast Mobile Dashboard for integration with the MobileIron Core. See Configuring the Check Point SandBlast Mobile Dashboard Integration Settings.
4. Apply the Check Point SandBlast Mobile Protect app configuration and policy enforcement to your MobileIron Core devices. See Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement.
5. Test the Check Point SandBlast Mobile Protect app on your protected MobileIron Core devices. See Testing High Risk Activity Detection and Policy Enforcement.
Introduction to the SandBlast Mobile Integration Guide

The SandBlast Mobile Protect app is an app for iOS® and Android™ that gathers data and helps analyze threats to mobile devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior.

To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.

The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience.

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| UEM | - Unified Endpoint Management (generalized term replacing MDM/EMM)  
- Device Management and Policy Enforcement System |
| SandBlast Mobile Gateway | - The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.  
- The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (organization’s) Dashboard instance.  
- No Personal Information is processed by or stored in the Gateway. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4 SandBlast Mobile Management 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 (BRE) uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis.  
- 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. |
| 6 ThreatCloud | - Check Point’s ThreatCloud is the world largest incidence of compromise database that incorporates real-time threat intelligence from hundreds of thousand Check Point gateways and from millions of endpoints across the globe.  
- ThreatCloud powers the Anti-Phishing, Safe Browsing, URL Filtering and Anti-bot technologies for SandBlast Mobile on-device Network Protection.  
- ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis. |
Preparing UEM Platform for Integration

MobileIron Core deploys SandBlast Mobile Protect app on a device.

Prerequisites

- SandBlast Mobile service integrates with MobileIron Core through the existing API. To enable integration, you must first create a MobileIron Core API account.

SandBlast Mobile integrates with MobileIron Core (On-Premise) and MobileIron Core is connected to MobileIron Cloud version 8.0 or later, through API access. SandBlast Mobile uses the API to synchronize the device records, to retrieve device apps list, and to report the device risk level to MobileIron Core.

**Note** - For more information about MobileIron Cloud see the online guide.

- You must configure your UEM to collect the app list from the devices enrolled to SandBlast Mobile. See Configuring Application Collection.

MobileIron Core Console (Example):
General Workflow

1. Enable the Check Point SandBlast Mobile Protect app on your MobileIron Core devices. See Enabling the SandBlast Mobile Protect app on the MobileIron Core Devices.
2. Create a Security Group for the Check Point SandBlast Mobile Protect app. See Creating Device Provisioning Group for SandBlast Mobile.
4. Create API Account for the Check Point SandBlast Mobile Protect app. See Creating API Account for Integration with the SandBlast Mobile.
5. Set SandBlast Mobile parameters for the device protection. See Setting Parameters for the Device Protection.

Enabling the SandBlast Mobile Protect app on the MobileIron Core Devices

To deliver content to devices, MobileIron Core identifies users and establishes permissions through Device Provisioning Groups.

Through your MobileIron Core Console, you can:

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

**Best Practice** - For integration with the Check Point SandBlast Mobile Protect app, use groups to set up the same UEM hierarchy as in your organization's internal hierarchy, or set up groups based on MobileIron Core features and content.

Creating API Account for Integration with the SandBlast Mobile

For the interaction with SandBlast Mobile and the MobileIron Core system, you must create a dedicated API account user in your MobileIron Core. This API account limits the capability of the admin credentials between the SandBlast Mobile Dashboard and the MobileIron Core system.

**Best Practice** - For the interaction at the API only, the MobileIron Core Console provides an "API Only" Admin Role. You can use this Administrator account between the SandBlast Mobile Dashboard and the MobileIron Core system. See Configuring the Check Point SandBlast Mobile Dashboard Integration Settings.

To create a “API Only” Administrator Account, create a dedicated Local User and assign it the Administrator Role.

Creating a Local User Account

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

**Assigning the SandBlast Mobile API Administrator to the Local User Account**

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

3. In the **Device Management** select:
   a. View device page, device details Device
   b. View device dashboard
   c. Apply and remove device label
   d. Edit custom device attribute values

![Assign to Space - admin](image)

4. 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**.
<table>
<thead>
<tr>
<th>Privacy Control</th>
<th>Selected Permissions</th>
<th>Available Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ View apps and ibooks in device details</td>
<td>• View device details</td>
<td>• View device IP and MAC address</td>
</tr>
<tr>
<td></td>
<td>• View device details</td>
<td>• Locate device</td>
</tr>
<tr>
<td></td>
<td>• View apps and ibooks in device details</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label Management</th>
<th>Selected Permissions</th>
<th>Available Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ View label</td>
<td>• View label</td>
<td>• View device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View device details</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit label</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Management</th>
<th>Selected Permissions</th>
<th>Available Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• View user</td>
<td>• View user</td>
</tr>
<tr>
<td></td>
<td>• Manage user</td>
<td>• Edit user</td>
</tr>
<tr>
<td></td>
<td>• Edit custom user attribute values</td>
<td>• Edit custom user attribute values</td>
</tr>
</tbody>
</table>
5. Scroll down to the Settings and Services Management section, and select **Manage custom attributes**.

6. Scroll down to **Other Role** 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.

**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 for SandBlast Mobile**

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.

There are two types of Labels, manual (static) and LDAP (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 (LDAP)

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**

4. Select **Equals** from the drop-down choices, and enter in the AD Group Name (in this example equals "Agents"): 

5. If you want to exclude retired devices from search results, make sure that the checkbox is selected
6. Click **Save**.
Creating a Secondary Device Provisioning Group (Optional)

**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.

A secondary group is essentially a filtered group or a sub-group of devices you can create only after connecting your UEM to SandBlast Mobile Dashboard. If you wish to create such group, prior to creating it, follow the steps of *Configuring the Check Point SandBlast Mobile Dashboard Integration Settings*.

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.
Configuring Application Collection

After the initial device sync, you must update the SandBlast Mobile Dashboard with the device app lists. The UEM must collect the app list from the devices enrolled to SandBlast Mobile.

To configure the UEM to collect the app lists

1. On the MobileIron Core Portal go to Policies & Configs > Policies, click Add New drop-down menu and select Privacy.

2. In the New Privacy Policy window enter a name and description.

3. Make sure to set these parameters:
   - Apps - to All Apps
   - iOS Installed App Inventory - to All Apps

   Example:
4. Click Save.
5. Apply this privacy policy to the SandBlast Mobile Device Provisioning Group that you created. For more information see Creating a Device Provisioning Group for SandBlast Mobile.

To apply the Application Collection Policy to the Device Provisioning Group:

1. On the MobileIron Core Portal go to Policies and select the Application Collection Policy.
2. Click More Actions drop-down menu and select Apply To Label.

Example:
3. In the **Apply to Label** pop-up window select the **Device Provisioning Group** name *(EXAMPLE_SBM)*.

Example:

4. Click **Apply**
Setting Parameters for the Device Protection

To protect your users, you must configure SandBlast Mobile Protect app to work on your user devices. Add users to the organization group for SandBlast Mobile protection. See Creating a Device Provisioning Group.

Repeat these steps to add more users and more devices.

Adding Local Users to the SandBlast Mobile Protect App

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 (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.

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: Company or Employee owned.

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 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*

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*.

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

To manage your devices and apps and their access to your company data you must enroll them in the MobileIron Core service.

For more information see the MobileIron Core online help:

1. On the MobileIron Core Portal go to the **Admin Profile** menu and click **Help**.

   Example:

   ![Admin Profile Menu](image)

2. Use your Support Account *at the MobileIron Core site*.

   **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://mobileiron.net
   API Admin Username/Password = sbm_admin/<******>
   Device Provisioning Label(s) = EXAMPLE_SBM
Configuring the Check Point SandBlast Mobile Dashboard Integration Settings

Assign the app to the selected groups of users or devices.

**Note** - For easy reference during configuration, you can record your settings in the special table (See Integration Information).

**Prerequisites**

You need these details from your MobileIron Core Deployment:

- **Server**: The URL of your MobileIron Core System. Usually - the same as the MobileIron Core Console.
  
  Example: $URL = https://m.mobileiron.net$

- **User name and Password**: Credentials of API Admin Account. See *Creating API Account for Integration with the SandBlast Mobile*

  Example: $API Admin Username/Password = sbm_admin/<******>

  The credentials that the SandBlast Mobile Dashboard uses to connect to MobileIron Core.

- **Group(s)**: The MobileIron Core mobile device / user groups to which the devices are registered and then integrated with the SandBlast Mobile Dashboard. You can integrate Multiple Device Provisioning Groups that use the same API in the same SandBlast Mobile Dashboard instance.

  Example: $Device Provisioning Label(s) = CPTME_SBM$

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

**Configuring Integration Settings**

After you complete the necessary steps, the Integrations pane shows the detailed status of the UEM settings integrated with the SandBlast Mobile dashboard.

**Procedure:**

1. Access your SandBlast Mobile Dashboard via the Infinity Portal. Go to Settings > Integration

   Click “+” to create a new integration setting.
The Integration Wizard opens.

Example:

2. Select **Assets**

3. Configure the settings for MobileIron Core UEM Deployment.
   
   **Server Setup**
   
   These are the UEM server settings used to synchronize devices into SandBlast Mobile:
   
   a. In **Server Setup** section, enter this information:
      
      - **UEM service** – MobileIron Core
      - **Display Name** – Enter displayed name or use default
      - **Server Address** – The full URL needed for the UEM service
      - **User name** – UEM Admin previously created
      - **Password**
      - **Connector Setup** (advanced)

      Example:
If the UEM server uses a self-signed certificate for external communication, check the relevant box to upload the certificate directly (use CER file format base64 [PEM] encoded) or just paste the certificate text directly in the box.

Connector Setup

(Optional) You can configure SandBlast Connector when the UEM is on-premises and has no direct access from the SandBlast Mobile cloud. For more information, see Sandblast Mobile Connector Integration Guide in the Check Point Support Download center.

b. Click Next.

Synchronization Configuration

Configure the Labels of devices that will synchronize with SandBlast Mobile Dashboard. The dropdown list will automatically populate all the labels in MobileIron Core.

Example:
a. In the **Label(s)** field:
   i. Click **Label(s)**. A dropdown with list of the available labels opens.
   ii. Select the label(s) you need for integration with MobileIron Core.

b. In the **Android Enterprise Deployment** field:

   If applicable for your implementation, select the groups for the deployed devices as part of the MobileIron UEM Android Enterprise deployment. See *Using Android Enterprise with SandBlast Mobile*.

Example:

![MOBILEIRON_Core_Integration](image)

c. In the **Advanced** section:

   Import Personally Identifiable Information (PII) and set the synchronization intervals.

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

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

Example:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
<tr>
<td>Device deletion</td>
<td>Percentage of devices allowed for deletion after UEM device sync (in %).</td>
<td>0-100% ; use 100% for no threshold *</td>
</tr>
<tr>
<td>Deletion delay after</td>
<td>Delay device deletion after several sync attempts – device is deleted after this amount of sync tries that confirmed deletion</td>
<td>1-100 sync tries.</td>
</tr>
<tr>
<td>App sync interval</td>
<td>Interval to connect with UEM to sync applications.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
</tbody>
</table>

* 100% value is recommended for evaluation/test usage – when you are adding a small amount of devices

d. Click Next
Tagging Configuration

Specify the information sent to MobileIron Core and the risk level of the device.

The tagging configuration will be synced to MobileIron Core and will be used in setting device risk status.

Please see: Creating a Secondary Device Provisioning Group (Optional), Creating a Mitigation Process, Creating a Compliance Policy for the Devices at Risk and Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement

Example:

a. In Tagging Section:
   Set Tag device status to ON.
   i. Create Mobile Device Extension Attribute and name it Status. See Connecting the SandBlast Mobile Protect app to your Device
   ii. Update each mobile device MobileIron Core with one of these Status values (see Creating a Device Provisioning Group for SandBlast Mobile):
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHKP_Status</td>
<td>During the first synchronization of a device in SandBlast Mobile Dashboard.</td>
</tr>
<tr>
<td>CHKP_Risk</td>
<td>After the user installs and registers to SandBlast Mobile.</td>
</tr>
<tr>
<td>CHKP_TF</td>
<td>If the device did not make contact with SandBlast Mobile for X number of days (that the SandBlast Mobile Admin configured).</td>
</tr>
</tbody>
</table>

iii. Set **Tag device risk** to **ON**.

- Create Mobile Device Extension Attribute and name it `risk_level`. See *Connecting the SandBlast Mobile Protect app to your Device*.
- Update each mobile device in MobileIron Core with one of these `risk_level` values:
  - None
  - Low
  - Medium
  - High

b. In **Advanced** section:

   The **Mitigation** tag is only applicable for the devices at High Risk. See *Connecting the SandBlast Mobile Protect app to your Device*

   **Note** - Create this User Group in MobileIron Core before you use it. See *Setting Parameters for the Device Protection*

c. Click **Next**

**Deployment**

a. Check the **“Allow auto device addition prior to device sync” option** in case you require a faster device enrollment (recommended). Without this option checked, the device will not be able to connect to the SandBlast Mobile Dashboard not until a complete sync step has created the device in the dashboard. This option generates a unique dashboard token to be used in the UEM configuration that will tell the device which dashboard it needs to register to.

**If you use SandBlast Mobile to manage the deployment:**

In this screen you’ll see the **Use token in application configuration settings**. Save this token for later as you will use it to manage the application in section *Adding the SandBlast Mobile Protect app to your App Catalog*

Example:
b. Advanced

Note – The Advanced section is optional, because MobileIron Core manages the deployment automatically.

In the Advanced section enable options to send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app. See Adding the SandBlast Mobile Protect app to your App Catalog
c. Click Finish.

4. View the **Integration Status** in **Settings > Integrations** menu.

   Select the integration you want to shows the information for and click the “i” icon on the top right:

   - **UEM Server** – The latest server configuration status.
   - **Synchronization** – The synchronized groups and the sync status.
     - **Device Sync** – The synchronized labels from MobileIron Core
     - **App Sync** – The last time applications were fetched from the UEM (applicable for iOS deployments only).
   - **Tagging** – Tagging Configuration and Tagging Status.
   - **Deployment** – Deployment Configuration and Deployment Status.
Example:

5. The 3 dots on the top of the integration settings will allow you to select extra functions:

Click **Edit /** (in each section) to edit the settings if needed.

Click **Sync Now** to force an immediate device sync call and not wait to the next auto sync cycle.

Click **Pause / Resume** to temporarily stop or resume the device sync process.

Click **Remove** to remove the integration settings altogether.

6. You can click again the “+” to add more integration settings from other different MDM/UEM solutions in case relevant for your deployment. SandBlast Mobile support integration of multiple MDM/UEM solutions from a single dashboard.
Configuring UEM to Deploy the SandBlast Mobile Protect app

Notes:

- If you configured MobileIron Core for Whitelisting Apps, you must add the SandBlast Mobile Protect app to the white list.
- For on-premise MobileIron Core UEM environments: Before you try to connect, make sure that you can remotely get access the TCP Web Services port (usually TCP port 443 (HTTPS) through your firewall from the SandBlast Mobile Dashboard to the UEM system.
- You can only synchronize devices from the UEM to the SandBlast Mobile Dashboard. You cannot synchronize users.
- Create the Check Point Statuses in the Device Provisioning Group.
- Mitigation tags, Smart Groups, and Compliance Policies are recursive. If you create them in the Device Provisioning Group, each Secondary Device Provisioning Group inherits and applies to the Device Provisioning Group devices that agree with the criteria.
- You must add the SandBlast Mobile Protect app for the two iOS and Android operating systems.

General Workflow:

1. Add the SandBlast Mobile Protect app to your App Catalog. See Adding the SandBlast Mobile Protect app to your App Catalog
2. Prompt the SandBlast Mobile Protect app installation on your devices. See Automatic Activation of SandBlast Mobile: Prompt the Protect app installation
3. Connect the app to your devices. See Connecting the SandBlast Mobile Protect app to your Device
4. Configure the Mitigation Process for the app (optional). See Connecting the SandBlast Mobile Protect app to your Device

Adding the SandBlast Mobile Protect app to your App Catalog

The SandBlast Mobile Protect app can be automatically configured and deployed. The user only needs to accept the installation and then launch the app to finish activation and registration. You assign configuration parameters for configuring the app per user.

Note - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

Use the CHKP Status Tags to deploy the SandBlast Mobile Protect app from the public stores to the devices that are protected by Check Point SandBlast Mobile. See Creating a Device Provisioning Group for SandBlast Mobile

You must add the Protect app for both iOS and Android operating systems.
To import the SandBlast Mobile Protect app:

1. Go to Apps -> App Catalog -> Add.

Example:

```
1. Go to Apps -> App Catalog -> Add.

Example:
```

2. Select and configure the SandBlast Mobile Protect app.

   a. For Android Enterprise Devices
      - Select Google Play > SandBlast Mobile Protect app.
      - In the Application Name field enter SandBlast Mobile Protect and click Search.

Example:

```
2. Select and configure the SandBlast Mobile Protect app.

   a. For Android Enterprise Devices
      - Select Google Play > SandBlast Mobile Protect app.
      - In the Application Name field enter SandBlast Mobile Protect and click Search.

Example:
```

   b. From the app list, select the SandBlast Mobile Protect app.

Example:
d. Click Next.

The **Describe** pane opens. No changes are required.

Example:

```
```

e. Click Next.

f. On the **App Store** pane go to **Apps@Work** catalog checkbox and select only the **Feature this App** option.

g. Select these options:

- Install the app for Android Enterprise
- Auto Update this App
- Silent Install for Mandatory Apps

Example:
h. Go to Configuration Choices and click Add.

i. In the Configuration Choices section configure these settings and assign to the label:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdm_uuid</td>
<td>String</td>
<td>$DEVICE_UUID$</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>hash_tenant_id**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The SHA-256 value of the Dashboard Management ID. You must use the token configured in the Deployment section. For more information see Configuring Integration Settings)</td>
</tr>
</tbody>
</table>

Example:

j. Click Finish

- **For iOS Devices**
  a. Go to Store List and select iTunes.
  b. In the Application Name field enter SandBlast Mobile Protect > App Store and click Search.
  c. Select the SandBlast Mobile Protect app

Example:
d. Click Next.

The Describe pane opens. No changes are required.

Example:

![Describe pane example]

---

e. On the App Store pane go to Apps@Work catalog and select these options:
   - This is a Free App
   - Allow conversion of apps from unmanaged to managed in Apps@Work (iOS 9 or later)
   - Feature this App in the Apps@Work catalog

Example:
f. Click Next.
g. On the App Configuration pane select these options:
   - Send installation request on device registration or sign-in
   - Remove app when MDM profile is removed

Example:

h. Click Finish.

Enable the automatic configuration and deployment of the app. See iOS App Deployment Configuration

iOS App Deployment Configuration

To enable the automatic configuration and deployment of the iOS SandBlast Mobile Protect app on your devices you must assign configuration parameters for configuring the app per user. Create the ManagedAppConfig.plist File and then use it for auto-deploy of the SandBlast Mobile Protect app on your devices.
To create the ManagedAppConfig.plist File:

1. **Copy this text to a text editor (for example, 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>
   <key>token</key>
   <string>hash_tenant_id</string>
   <key>mdm_device_id</key>
   <string>$DEVICE_UUID$</string>
   </dict>
   </plist>

2. **Change the `<string>hash_tenant_id</string>` content (i.e. instead of “hash_tenant_id” text) to the Token you saved from Deployment section in Configuring Integration Settings.

3. Click **Save As...** and save the file as **ManagedAppConfig.plist**

4. Exit the file.

5. Go to **Policies & Configs > Configurations** and click **Add New**.

6. From the drop-down list select **Apple > iOS / tvOS > Managed App Config**.

Example:
The **New Managed App Config Setting** window opens.

Example:

7. Enter these parameters:

   **Name**
Description

BundleId - Enter com.checkpoint.capsuleprotect

8. Click Choose File and select the ManagedAppConfig.plist file.

Example:

![New Managed App Config Setting](image)

9. Click Save.

10. Select this new Managed App Config and click More Actions drop-down menu

Example:

![More Actions Menu](image)

11. Select Apply To Label.

12. In the Apply To Labels window select the primary or secondary Device Provisioning group (label).

Example:
Automatic Activation of SandBlast Mobile: Prompt the Protect app installation

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

To prompt the SandBlast Mobile Protect app installation on your devices

1. Create a Protect app Application Group for both iOS and Android apps.
2. Assign this group to your organization.
3. Create a compliance policy that uninstalls and, or removes all corporate apps from the device until the user installs the SandBlast Mobile Protect app on the device.

Connecting the SandBlast Mobile Protect app to your Device

To install the SandBlast Mobile Protect app on your devices in your organization, you must first configure them to require the SandBlast Mobile Protect app. This is a dynamic group assignment according to the associated tag. MobileIron UEM calls these dynamic Assignment Groups “Smart Groups”.

Add all the devices marked with the Status tags to a group that indicates that the devices are registered in SandBlast Mobile Dashboard.
Optional: Create a mitigation process. See *Creating a Mitigation Process*

**General Workflow:**

1. Add SandBlast Mobile Protect apps to the Device Provisioning Group to create a Protect app group.
2. Create App Control Rule that prompts installation of the SandBlast Mobile Protect app on both the iOS and Android apps.
3. Assign the groups of the protected devices to the organization through the Status tags.
4. Create a Compliance policy to uninstall / remove corporate apps from the device until the user installs the required apps on the device.
5. Create a Mitigation Process for devices-at-risk through the Risk tags.

**Creating a Protect app Group**

Add the SandBlast Mobile Protect app group to your devices in the Device Provisioning group.

*Note* - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

**To add SandBlast Mobile Protect apps to the Device Provisioning Group:**

1. On the MobileIron Core Portal go to Apps > App Catalog, select SandBlast Mobile Protect app both the iOS and Android devices.

   Example:

   ![App Catalog](image.png)

   2. In the Actions drop-down menu select Apply To Labels.

   Example:
3. In the **Apply to Labels** window select the provisioning label you created for the Device Provisioning group. See *Creating a Device Provisioning Group for SandBlast Mobile*

4. Click **Apply**.

Example:

![Apply To Labels window](image)

### Creating an App Control Rule

**Procedure:**

1. Go to Apps > App Control click **Add**.

   App Control Rule prompts the iOS and Android devices to install the SandBlast Mobile Protect app.

   Example:

   ![App Control Rule](image)

2. In the Add App Control Rule window configure these parameters:
   - **Rule Name** - Select **Required** button.
   - Rule Entries:
     - **App Identifier Equals** - Select `com.checkpoint.capsuleprotect > iOS`
     - **App Identifier Equals** - Select `com.lacoon.security.fox > Android`
3. Click Save.

Creating a Compliance Actions Policy for the Organization Devices

The Compliance Policies are activated on the devices that did not install the required apps.

You must create separate compliance policies for specific OS types, such as iOS and Android.

**Note** - In every organization, the customer configures the compliance policies according to the production environment, needs, and the internal security policy.

To create a Compliance Policy:

1. Go to **Policies & Configs > Compliance Action** > and click **+ Add**.

   Example:

2. In the **Add Compliance Action** window configure these parameters:
Name - Enter Non-Compliant Device Actions (we recommend)
- Select these options:
  - Enforce Compliance Actions Locally on Devices
  - ALERT - Select Send a compliance notification or alert to the user
  - BLOCK ACCESS - Select Block email access and AppConnect apps
  - QUARANTINE - Select Quarantine the device

3. Click Save.

Example:

Creating a Security Compliance Rule (Enforcement)

Link the App Control Rule and Compliance Actions Policy to create the new Security Policy.

Procedure:


Example:
2. In the **New Security Policy** window enter a policy name.

Example:

![New Security Policy Window](image)

3. Scroll down to **Access Control > For All Platforms** section and select these options:
   - Option Non-Compliant Device Actions compliance action policy (see *Creating a Compliance Actions Policy for the Organization Devices*).
   - Option when a device violates following App Control rules (see *Creating an App Control Rule*).
   - Rule Type - Select Enabled > SBM_Required.
Example:

**For iOS Devices:**

Scroll down to *For iOS devices* section and select these options:

- **Non-Compliant Device Actions** Policy
- **when device MDM is deactivated**

Example:
For Android Devices

Scroll down to the For Android devices section and select these options:

- Non-Compliant Device Actions Policy
  - when device administrator is deactivated

Example:

5. Click Save.
Applying the MDM Security Policy to the Device Provisioning Group

Procedure:

1. Go to **Policies &Configs > Policies** and select the Security Policy.
2. Click **More Actions** drop-down menu and select **Apply To Label**.

Example:

Make sure the checkbox is checked:

And after that apply it to label:

3. In the **Apply To Labels** window select one of these options:
   - **If you created only a Primary Device Provisioning Group**
     - **Note** - Perform this step if you created a Primary Device Provisioning Group only.

     Select the **Device Provisioning Label**.
Example:

- If you created both a Device Provisioning Group and a Secondary Device Provisioning Group

  Note - Perform this step only if you created a Secondary Device Provisioning Group.

  Select the Secondary Device Provisioning Label.

Example:

4. Click Apply.
Creating a Mitigation Process

To let the MobileIron Core system identify the devices-at-risk and to enforce the configured compliance policies according to the risk level, you must apply the built-in Risk tags. The SandBlast Mobile Dashboard uses these tags (CHKP_Risk) to identify any device with the risk level that the SandBlast Mobile analysis determines.

For more information, see Configuring Integration Settings

To accomplish the policy enforcement on the devices, you must create Device Profiles and the Compliance Policy to apply these profiles to the devices. Create a Compliance Policy Rule, Compliance Policy Group and apply the Compliance Policy Group to the Device Provisioning Label.

Check Point recommends these names for the SandBlast Mobile Protect app attributes:

- Device Provisioning Group - CPTME_SBM
- Custom Attribute - CHKP_Risk (set to High or Medium)
- Compliance Policy Group - CPTME_SBM_AT_RISK_DEVICES

Creating a Compliance Policy for the Devices at Risk

The Compliance Policies are activated on the devices that are at high risk.

You must create separate compliance policies for specific OS types, such as iOS and Android.

Note - In every organization, the customer configures the compliance policies according to the production environment, needs, and the internal security policy.

To create a Compliance Policy for the Devices at Risk:


   Example:

   ![Compliance Policy Rule](image)

2. On the Compliance Policy Rule tab configure these parameters:
   - Rule Name - Enter the Rule Name.
   - Description - Enter a description.
   - Status - Check Enabled option.
   - Make sure Exclude retired devices from search results is selected.

3. From the Field menu select Custom Attributes > Device Attributes > CHKP_Risk.
4. From the **Operator** menu select **Equals**.
5. In the **Value** field enter **High**.
6. (Optional) To apply the Compliance Action to devices with **High or Medium** Risk level, click [+\] icon to add another line and enter **Medium** in the **Value** field.
7. From the Compliance Action menu select the Non-Compliant Device Action. See *Creating a Compliance Actions Policy for the Organization Devices*.
8. Click **Save**.

Example:
Creating a Compliance Policy Group

Compliance Policy Group uses the Compliance Policy Rules and applies to the Device Provisioning Group to enforce on devices that are at High or Medium Risk.

Procedure:


   Example:

   ![Image of Compliance Policy Group tab]

   2. On the Compliance Policy Group tab configure these parameters:

      - **Group Name** - Enter the Group Name.
      - **Status** - Check Enabled option.
      - Make sure Exclude retired devices from search results is selected.

3. In the Available Rules section, select the created Compliance Rule.
4. Click Save.

   Example:

   ![Image of Available Rules section]
Applying the Compliance Policy Group to the Device Provisioning Group

The Compliance Policy applies to the Device Provisioning Group (see Creating a Device Provisioning Group for SandBlast Mobile).

Procedure:

1. Go to Policies & Configs > Compliance Policies > Compliance Policy Group and select the Compliance Policy Group (see Creating a Compliance Policy Group)
2. Click Actions menu and select Apply to Labels.
   
   Example:
   
   ![Image of Compliance Policy Group]
   
3. In the Apply to Label window select the Device Provisioning Group label (for example, CPTME_SBM).
4. Click Apply.
   
   Example:
Deploying the SandBlast Mobile Protect app automatically (Zero Touch Deployment) [Optional]

UEM solutions traditionally prompt the mobile device user to install the application once it is registered. In addition, to get full protection, the user needs to approve the required permissions and profiles. Many users are vigilant about installing new mobile applications or granting different permissions, and as a Security company, Check Point even encourages that. Most of them don’t know that the SandBlast Mobile Protect app is focused on device characteristics and behaviors and not the content stored on or flowing through the device. Furthermore, some users are incompliant with the company’s security policy, especially when they use their own devices. Therefore, users often decide not to install the app or approve the required configuration. On top of that, users who do agree to install and accept the configuration will not often do it immediately and it will take time until the application is activated. As a result, many devices remain exposed to potential cyber-attacks.

SandBlast Mobile’s innovative zero-touch technology allows the Protect app to be installed and activated automatically without any user interaction. The solution leverages Check Point’s unique bootstrap technology to establish zero-touch activation.

Zero Touch deployment is optional, if the organization does not want to force SandBlast Mobile to activate itself automatically on employees’ devices, please skip this chapter.

1) Zero Touch Deployment in Android Enterprise devices

Note – The steps below are relevant when you want to apply Zero Touch to all devices. If this is not the case (e.g during evaluation/POC) you would need to change the labels criteria defined below to uniquely select the relevant devices you want to apply this on.

a. Create two new labels:
   Go to: Devices & Users > Labels > Add Label Type > Filter

1) Name: android_sbm_not_registered

Criteria (copy the following):
"custom.device.CHKP_Status" != "Active" AND "custom.device.CHKP_Status" != "Inactive" AND "common.platform" = "Android" AND "common.retired" = false
2) **Name**: *android_sbm_registered*

**Criteria (copy the following):**

"custom.device.CHKP_Status" = "Active" AND "common.retired" = false AND "common.platform" = "Android"

b. Create an Always-On VPN configuration

1) Create new **ANDROIDFORWORK** configuration, and apply Always-On VPN to SandBlast Mobile protect.

In this configuration, check:
- Enable Managed Device with Work Profile of the devices
- Auto update Mobile@Work app on the devices

In *For Android 7.0 and higher only* section, check Always-on VPN and select SandBlast Mobile Protect for the app identifier:
2) Click Save

c. Apply the configurations to your labels

1) Apply your Android Enterprise configuration (from type ANDROIDFORWORK) to android_sbm_registered label (the one you use to deploy the work profile to your Android devices).

2) Assign the configuration created in step 3 to the android_sbm_not_registered label.
2) Zero Touch Deployment in iOS devices

Create new VPN Profile. Go to Policies & Configs > Configurations > Add New > VPN

a. On VPN Settings fill in the following details:
   - **Connection Name:** Check Point Local Tunnel
   - **Connection Type:** Custom SSL
   - **Identifier:** com.checkpoint.capsuleprotect
   - **Server:** www.checkpoint.com
   - **User authentication type:** password
   - Enable VPN on Demand

b. Add On Demand Rules:

   Add two Connect rules, one for wifi and one for cellular.
c. On Custom Data > Add zero_touch=true

d. Click Save

e. Apply the configuration to your label.
Using Android Enterprise with SandBlast Mobile

Android Enterprise is a Google-led initiative that enables the operation of Android devices and apps in the workplace. The program offers APIs and other tools for developers to integrate support for Android into their enterprise mobility management (EMM) solutions.

For example, through one or more API(s) your UEM platform can disable a camera, Bluetooth, or prevent an access to system settings.

For information about configuring Android Enterprise on your device, see MobileIron Core AE guide online: here.

Profiles

Single profile configuration is supported out-of-the-box. No additional setup is needed.

In the Work / Personal Profile, the Administrator registers and sees the protected part of the device.

Note - If you protect only part(s) of the device, you must limit the SandBlast Mobile on your UEM to only Work or only Personal.

Android Enterprise Deployment Scenarios

Android Enterprise supports these deployment scenarios:

- Company-owned fully managed devices (COBO)
- Company-owned fully managed devices with a work profile (COPE)
- Company-owned devices for dedicated use (COSU)
- Employee-owned devices (BYOD)

COBO and COSU devices have a single profile. Follow integration guide instructions for Android Enterprise devices to deploy SandBlast Mobile Protect app on your devices. For more information, see the Android Enterprise online guide.

COPE and BYOD devices have Work and Personal profiles. With SandBlast Mobile Protect app you can protect one profile or both profiles.

For the highest protection level we recommend to protect both Work and Personal Profiles. See Configuring SandBlast Mobile Protect app to Protect your Devices.

Note - If you protect only the Work profile, skip the next section.
Configuring SandBlast Mobile Protect app to Protect your Devices

Note - The deployment of the SandBlast Mobile Protect app on the Personal profile of BYOD device cannot be automated by Android design (Personal profile of BYOD device is not managed).

With the Android Enterprise, you can protect the whole device or part(s) of it.

If you protect the whole device, install the SandBlast Mobile Protect app to both Work and Personal Profiles.

Note - If you protect only the Personal profile, skip this section.

Deploying Android Enterprise on your Devices

With the Android Enterprise, you can protect the whole device or part(s) of it.

If you protect the whole device, install the SandBlast Mobile Protect app to both Work and Personal Profiles.

To protect the whole device:

1. On the SandBlast Mobile Dashboard, go to Settings > Device Management.
2. Enable the SandBlast Mobile Protect app (for both profiles).
   - For a new UEM configuration:
     a. Go to Settings > Device Management > UEM service and select the UEM type.
     b. In the configuration prompt select the groups for synchronization.
     c. In the Android Enterprise Deployment section select and add the device groups for both profiles.
   - For existing UEM configurations:
     a. Go to Settings > Device Management > Edit Settings.
     b. In the Android Enterprise Deployment section select and add the device groups for both profiles.

Example:

<table>
<thead>
<tr>
<th>Android Enterprise Deployment</th>
<th>Work &amp; Personal deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select groups...</td>
<td></td>
</tr>
</tbody>
</table>
3. Click Verify.
4. Click Save.
5. (Optional) Send an email or SMS to all the users with installation instructions.
6. Click Sync Now to fetch the data from the UEM.

Note - If a device belongs to more than one group, one group selected in Android Enterprise deployment, and one group is not selected, the deployment is both Work and Personal.

General View on the Check Point Dashboard (Example):

To view and filter the devices:

1. On the SandBlast Mobile Dashboard, go to Devices > Groups >Devices.

   Example:

2. In the Device Type column, filter the devices in the list according to their protection profile.
### Policies

To change policy for inactive personal profile:

1. On the SandBlast Mobile Dashboard, go to **Policy > Global > Device > Android Enterprise Security Settings**.

   **Example:**

   ![Android Enterprise Security Settings](image)

2. From the drop-down list, select a policy.

   **Example:**

   ![Android Enterprise Security Settings](image)

   - **Change device risk level to:** High (Device Alert) if Sandblast Mobile on personal profile is not active

### Risk Handling

- If the SandBlast Mobile protection is inactive on the Personal profile, the risk level is raised to according to the Android Enterprise Security Settings policy on the Work profile (see **Policies**)

  **Example:**

  ![Risk Handling Example](image)
If the Personal profile has the High Risk status, the risk level is raised to **High** on the Work profile. The SandBlast Mobile informs the user that the personal profile is at risk.

Example:
You can enable mitigation by UEM on the personal profile, if you tag a risk on the work profile. To configure mitigation tags, see *Connecting the SandBlast Mobile Protect app to your Device.*
Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement

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

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

Deploying the SandBlast Mobile Protect app on the Devices

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section Configuring MobileIron UEM Integration Settings on the SandBlast Mobile, the App is automatically deployed to the devices that belong to the defined groups (see Configuring UEM to Deploy the SandBlast Mobile Protect app).

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

After you register your device in the MobileIron Core and attach it to the defined groups, the system prompts the user to install the SandBlast Mobile Protect app.

Procedure for the User:

1. Register your device.
   - iOS Device
     a. Tap INSTALL on the SandBlast Mobile Protect app.
       The Protect app is deployed on the iOS Device.
     b. Launch the Protect app to finish the registration.
MobileIron Core system automatically configures the registration server and the key in the Protect app.

c. Follow the on-screen instructions to enable Notifications, Location, and Network Security.

d. Tap **Allow** to allow SandBlast Mobile Protect app to add the needed VPN Configuration profile, when On-device Network protection is enabled.

e. The SandBlast Mobile Protect app scans the system. See the state of the device on the display.

### Android Device

a. Tap on the SandBlast Mobile Protect app in the managed Google Play Store.

b. Tap **INSTALL > ACCEPT** on the SandBlast Mobile Protect app to accept the permissions of the App.

The App is installed. Example:
c. Launch the App to finish its deployment and registration to Check Point SandBlast Mobile.

The SandBlast Mobile Protect app is automatically registered.

d. Follow the on-screen instructions to allow the SandBlast Mobile Protect app make these permissions on the device:
   - Turn on Location, Notifications, and Network Protection features.
   - Configure a VPN connection. This is necessary to enable the Network Security Protection features of Safe Browsing and Anti-Phishing.
   - The SandBlast Mobile Protect app scans the system. See the state of the device on the display.

Example:
Testing High Risk Activity Detection and Policy Enforcement

If the user’s device is determined to be at risk either due to a malicious app or malicious activity, the SandBlast Mobile system notifies the User through in-app notifications, and also updates the risk level custom attribute value to the MobileIron Core system for that device. MobileIron Core receives the risk state change, and upon recognizing the risk level value tied to a Configuration Profile, enacts that policy.

In this example, the Administrator blacklists an app, for example, "Waze". As a result, the user’s device is identified to be at High Risk (CHKP_Risk = High) due to the blacklisted app "Waze" installed on the device. The SandBlast Mobile Dashboard notifies the user, and mark the device as High Risk (CHKP_Risk = High) to the MobileIron Core system. The MobileIron Core system then enforces policy actions specified in the Compliance Policy Profile.

Example:

Blacklisting a Test App

1. Log into the SandBlast Mobile Dashboard.
2. Go to Forensics -> App Analysis tab and select for the app you wish to blacklist.

Example:
3. Go to Default and click Policy.

A Changing application policy pop-up window opens.

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

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

Example:

![Changing Application Policy - Global]

Changing the application policy will effect all of the devices it is installed on. This action might take some time to complete, check the dashboard audit trail for policy change event.

New policy: Black Listed

Audit Trail note: test compliance policy

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

**View of a Non-Compliant Device**

The device with the blacklisted app must be in one of the Smart Groups that you created for the Devices At Risk. See *Connecting the SandBlast Mobile Protect app to your Device.*

**To see the non-compliant device in the Smart Group for Mobile Devices:**

1. Go to **Devices > Smart Device Groups** and open your defined Smart Group for mobile devices.
2. Click **View**.

The device is displayed.

Example:

If you configured an email notification, you receive an email from MobileIron Core.

**Note** - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

The user is not allowed to use the app until the user removes the blacklisted app, or changes the compliance policy settings. See *Creating a Mitigation Process.*
SandBlast Mobile Protect app **Notifications**

The user receives SandBlast Mobile Protect app notifications in the Mobile@Work app.

Example:

![Notification Example](image)

**Administrator View on the SandBlast Mobile Dashboard**

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

1. On the Infinity Portal, go to **Device Risk > High Risk** section.
   
   A list of the Devices At Risk is displayed in the **Device Risk** section.

   Example:

   ![Dashboard Example](image)

2. Click **High Risk**.

   The list of devices at High Risk state is displayed.

3. Select the specified device on the left-side list.
You can see that the blacklisted app causes the High Risk state.

Example:

### Administrator View on the MobileIron Core Console

In the MobileIron Core Portal you can see these parameters:

- **Dashboard** tab: The devices in *Out of Compliance* status.

  Example:

  ![Dashboard Example]

- **Device & Users** tab:
  - Custom Attribute tab: **CHKP_Status** = Active
Example:

- Compliance tab: shows the violated Compliance Policy Rules and the applied Compliance Actions.

Example:
## Appendix

### Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Description</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)</td>
<td>(deprecated)</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>