26 May 2020

SandBlast Mobile for MobileIron Cloud

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 2020 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

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

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

About Check Point SandBlast Mobile ................................................................. 5  
General Workflow ......................................................................................... 5  

Introduction to the SandBlast Mobile Integration Guide ........................................... 6  

Solution Architecture .................................................................................. 7  

Preparing UEM Platform for Integration ......................................................... 7  
Prerequisites .................................................................................................. 9  
General Workflow ......................................................................................... 9  

Enabling the SandBlast Mobile Protect app on the MobileIron Cloud Devices .......... 10  
Creating API Account for Integration with the SandBlast Mobile ......................... 10  
Creating an API User Account ...................................................................... 10  
Assigning the SandBlast Mobile API Administrator Role to the API User .............. 12  
Creating a Device Provisioning Group ............................................................ 13  
Creating Custom Device Attributes ............................................................... 15  
Configuring Application Collection ................................................................ 17  
Setting Parameters for the Device Protection .................................................. 19  
Adding Local Users to the SandBlast Mobile Protect app .................................. 19  
Enrolling a Device to MobileIron Cloud .......................................................... 21  

Configuring the Check Point SandBlast Mobile Dashboard Integration Settings .......... 22  
Prerequisites .................................................................................................. 22  
Configuring Integration Settings ................................................................... 23  

Configuring UEM to Deploy the SandBlast Mobile Protect app .......................... 33  
Prerequisites .................................................................................................. 33  
Adding the SandBlast Mobile Protect app to your App Catalog .......................... 34  
Automatic Activation of SandBlast Mobile ....................................................... 44  
Creating an App Control Policy ..................................................................... 44  
Configuring Email Notifications .................................................................... 46  
Connecting the SandBlast Mobile Protect app to your Device ............................. 47
Creating a Protect app Group ........................................................................................................................................ 48
Assigning the Protect app Group to your Organization .................................................................................................. 48
Creating a Mitigation Process ............................................................................................................................................ 50
Creating a Compliance Policy for the Devices at Risk ........................................................................................................ 50
Creating a Compliance Policy Group .................................................................................................................................. 52
Applying the Compliance Policy Group to the Device Provisioning Group .............................................................. 53

Using Android Enterprise with SandBlast Mobile .................................................................................................................. 55
Profiles .................................................................................................................................................................................. 55
Android Enterprise Deployment Scenarios .............................................................................................................................. 55
Configuring SandBlast Mobile Protect app to Protect your Devices .................................................................................. 56
Deploying Android Enterprise on your Devices .................................................................................................................... 56
Policies .................................................................................................................................................................................. 58
Risk Handling ....................................................................................................................................................................... 58

Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement ........................................... 61
Deploying the SandBlast Mobile Protect app on the Devices ............................................................................................... 61

Testing High Risk Activity Detection and Policy Enforcement ....................................................................................... 64
Blacklisting a Test App .......................................................................................................................................................... 64
View of a Non-Compliant Device ......................................................................................................................................... 65
Administrator View on the SandBlast Mobile Dashboard .................................................................................................... 66
Administrator View on the MobileIron Cloud Console ....................................................................................................... 67

Appendix ................................................................................................................................................................................. 69
Integration Information ............................................................................................................................................................ 69
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 Cloud. It provides a quick tour through the interface of the MobileIron Cloud 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 Cloud UEM platform for the Check Point SandBlast Mobile Protect app integration. See ""
<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 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.                                                                       |
| 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.                                                                       |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |

2. Preparing UEM Platform for Integration.  
3. Configure your MobileIron Cloud UEM to deploy the Check Point SandBlast Mobile Protect app. See "Configuring UEM to Deploy the SandBlast Mobile Protect app".  
4. Configure the Check Point SandBlast Mobile Dashboard for integration with the MobileIron Cloud. See "Configuring the Check Point SandBlast Mobile Dashboard Integration Settings".  
5. Apply the Check Point SandBlast Mobile Protect app configuration and policy enforcement to your MobileIron Cloud devices. See "Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement".  
6. Test the Check Point SandBlast Mobile Protect app on your protected MobileIron Cloud 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>
| 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 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

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

Through your MobileIron Cloud portal 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 Cloud features and content.

Prerequisites

1. MobileIron Cloud Instance and System Management Admin credentials.
2. An iOS MDM Certificate in MobileIron Cloud Portal. For more information see the online guide.

MobileIron Cloud Portal (Example):

![MobileIron Cloud Portal](image)

General Workflow

1. Enable the Check Point SandBlast Mobile Protect app on your MobileIron Cloud devices. See "0".
2. Create API Account for the Check Point SandBlast Mobile Protect app. See "Creating API Account for Integration with the SandBlast Mobile".
3. Create a User Provisioning Group for the Check Point SandBlast Mobile Protect app. See "Creating a Device Provisioning Group".
4. Configure application collection. See "Configuring Application Collection".
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 Cloud Devices

MobileIron Cloud deploys SandBlast Mobile Protect app on a device.

- SandBlast Mobile service integrates with MobileIron Cloud through the existing API. To enable integration, you must first create a MobileIron Cloud API account.
  
  SandBlast Mobile integrates with MobileIron On-Premise Core and MobileIron Connected Cloud version 8.0 or later, with 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 Cloud.

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

Creating API Account for Integration with the SandBlast Mobile

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

![Best Practice](image)

**Best Practice** - For the interaction at the API only, the MobileIron Cloud Console provides an "API Only" Admin Role.

You can use this Administrator account between the SandBlast Mobile Dashboard and the MobileIron Cloud system. See "Configuring the Check Point SandBlast Mobile Dashboard Integration Settings".

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

Creating an API User Account

To create a Local User account settings:

1. On the MobileIron Cloud Console go to Users > Users, click the +Add drop-down menu, and select API User.

   Example:
2. In the Add API User window enter all the required (|) fields with the applicable information.

Example:

- **Username** - *sbm_admin* (recommended)
  - *In our case we created a user "mdm.test"*
- **First Name**
- **Last Name**
- **Password**
- **Confirm Password**
- **Email**

3. In the API Management section:

Remove the selection mark from the **Cisco ISE Operations** option.

Example:

4. Click **Save**.
Assigning the SandBlast Mobile API Administrator Role to the API User

For more information see the online guide.

To set the new API Administrator account:

1. Go to Users > Users and select the new mdm.test user that you created.
2. From the Actions drop-down menu select Append Roles.

Example:

3. In the Select Role section select these settings:
   - System Read Only
   - User Read Only
   - Device Management
   - App & Content - Read Only

Example:
4. Click Next.
5. Click Done.
6. Log out and log in back with these new Admin credentials.

Example:

Creating a Device Provisioning Group

To configure your devices, apps, and app configurations for the SandBlast Mobile Protect app, you must add them to the Dynamically Managed Device Provisioning Group named cpuser_test_devices, and then synchronize them with the SandBlast Mobile Dashboard. They will be prompted to install the SandBlast Mobile Protect app after the synchronization.

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

These devices will be registered to SandBlast Mobile.

To create a Device Provisioning Group:

1. On the MobileIron Cloud Portal go to Devices > Device Groups and click Add+.

Example:
2. In the **Create Device Group** window enter these details:

   **Name** – `cpuser_test_devices`

   **Description**

   Select **Dynamically Managed**

   - In the **User Group** section:
     - Select **All of the following rules are true**
     - Set **User Group** is equal to `cptest_group`
   - In the **Platform** section:
     - Select **Any of the following rules are true** and click on **Add Group** button
     - Set **OS** is equal to `iOS`
     - Set **OS** is equal to `Android`

Example:

3. Click **Save**.

Example:
Creating Custom Device Attributes

To configure your devices and users for the SandBlast Mobile Protect app, you must add them to the device provisioning group that is registered with the SandBlast Mobile and integrated with the SandBlast Mobile Dashboard. Use tags to label these devices and users.

- **Status tags**

  SandBlast Mobile Dashboard uses labels to deploy the SandBlast Mobile Protect app from the public stores to the devices that Check Point SandBlast Mobile protects.

  The system prompts the user to install the Protect app only when the device has the CHKP_Status of **Provisioned**, **Active**, or **TF**. If all of these tags are empty or 0, then the system does NOT prompt the user to install the Protect app. In this way the devices first synchronize in the SandBlast Mobile Dashboard and then prompt the user to install the SandBlast Mobile Protect app.

  You must add the Protect app for both iOS and Android operating systems.

- **Risk Levels**

  SandBlast Mobile Dashboard uses the built-in Risk tags to identify any device as determined by the SandBlast Mobile Analysis.

  You must create special Mobile Device labels and name it **risk_level**. Each mobile device in MobileIron Cloud gets one of these risk level values:

  - None
  - Low
  - Medium
  - High
These tags allow the MobileIron Cloud system to identify the devices at risk and to enforce configured compliance policies based on their risk level.

**The complete Custom Attributes list (example):**

![Custom Attributes Table]

**To create Custom Device Attributes:**

1. On the MobileIron Cloud Portal go to **Admin > System > Attributes** and click **+Add New**.

   Example:

2. In the **Custom Attributes** window enter these settings:
   - **Attribute Name** - **CHKP_Risk**
   - **Set Attribute Type** - **Device**

3. Click **Add**.

   Example:
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 Cloud Portal go to **Configurations**, click +Add drop-down menu.

   Example:

   ![MobileIron Cloud Portal](image)

   - In the **Add Configuration** window select **Privacy**.

   Example:

   ![Add Configuration](image)

2. In the **Create Privacy Configuration** window configure these settings:
   - In the **Privacy Create Settings** section enter a Name and Description:
     **Name**: SBM_cmpm_privacy_policy
   - In the **Configuration Setup** section for **Collect App Inventory** section select **For Apps on the Device**
Example:

4. Click **Next**.
5. Click **Custom**.
6. Select the **Device Provisioning Group**. See "Creating a Device Provisioning Group".
7. Click **Done**.

Example:

8. Apply this privacy policy to the SandBlast Mobile Device Provisioning Group that you created. For more information see "Creating a Device Provisioning Group".
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

You can use Add Local User option to add one user, or Resync with DAPt option to upload more than one user at a time. Repeat this procedure for each new device that you add.

You can add a single user, multiple users, or invite users from LDAP.

To add a single user:

1. On the MobileIron Cloud Portal go to Users > Users and click the +Add.
2. Select Single User.
   
   Example:

   ![Image of MobileIron Cloud Portal with Users section highlighted]

   3. In the Add Single User window enter applicable information.
      
      Example:
4. Select the applicable User Group for integration with the SandBlast Mobile Protect app (See "Creating a Device Provisioning Group").
5. To invite the user to enroll a device to MobileIron Cloud, select the Send Invitation now option.
6. Click Done.

Example:
Enrolling a Device to MobileIron Cloud

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

For more information see the MobileIron Cloud online guide: Device Registration (iOS, macOS, and Android).
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 Cloud Deployment:

- **Server**: The URL of your MobileIron Cloud System. Usually - the same as the MobileIron Cloud Console.
  
  Example: \texttt{URL = https://eu1.mobileiron.com}

- **API Admin Username Password**: Credentials of API Admin Account. See "Creating API Account for Integration with the SandBlast Mobile".
  
  Example: \texttt{mdm_test@api.21db9a.checkpoint.com}

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

- **Group(s)**: The MobileIron Cloud 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: \texttt{cpuser_test_devices}

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

After you complete the necessary steps, the Device Management pane shows the detailed status of the settings.

Procedure:

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

   The Device Management page opens.

2. Click Edit.

   The Integration Wizard opens.

3. Configure the settings for your MobileIron Cloud Deployment.

   For information about the settings see ”
<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 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.                                                                                                                                         |
| 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.                                                                                                                                         |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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”.

**Server Setup**

Configure your UEM to integrate with the created MobileIron Cloud devices:

a. In **Server Setup** section, enter this information:
   - **UEM service** - MobileIron Cloud
   - **Server Address** - The full URL needed for the UEM service
   - **User name**
   - **Password**
   - **API Key**
   - **Connector Setup** (advanced)

b. Click **Next**.
**Synchronization Configuration**

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

a. In the **Group(s)** field:
   i. Click on the blank space and a drop down with list of the available groups opens.
   ii. Select the group(s) you need for integration with MobileIron Cloud.

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

   Select the groups for two deployed applications as part of the MobileIron Cloud Android Enterprise deployment. See "Using Android Enterprise with SandBlast Mobile".

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

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

d. Click **Next**.
Note - If all entries are OFF, the placeholder information set for the email address is placed in the Device Owner's Email, in form of "UEMDevice UDID@vendor.mdm".
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
<tr>
<td>Device deletion threshold</td>
<td>Devices for deletion after UEM device sync (in %).</td>
<td>100% for no threshold.</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync – device is not deleted if it is re-</td>
<td>0-48 hours.</td>
</tr>
<tr>
<td></td>
<td>synchronized from UEM during the threshold interval.</td>
<td></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>

- **Tagging Configuration**

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

  Example:
a. In **Tagging** Section:
   i. 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 Cloud with one of these **Status** values (See "Creating a Device Provisioning Group"): 
### Status | Description
--- | ---
CHKP_Status_Provisioned | During the first synchronization of a device in SandBlast Mobile Dashboard.
CHKP_Status_Active | After the user installs and registers to SandBlast Mobile.
CHKP_Status_Inactive | If the device did not make contact with SandBlast Mobile for X number of days (that the SandBlast Mobile Admin configured).

ii. Set **Tag device risk** to **ON**.
   i. Create Mobile Device Extension Attribute and name it `risk_level`. See "Connecting the SandBlast Mobile Protect app to your Device".
   ii. Update each mobile device in MobileIron Cloud 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 Cloud before you use it.
   See "Setting Parameters for the Device Protection".

c. Click **Finish**.

Example:
- **Deployment**

Specify the deployment status of a device.

**Note** - This section is optional, because MobileIron Cloud manages the deployment automatically.

Example:
4. View the **Integration Status**.

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

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

- **Server** – The latest server configuration status.
- **Synchronization** – The synchronized groups and the sync status.
- **App Sync** – The last type applications were fetched from the UEM (For iOS deployments only).
- **Tagging** – Tagging Configuration and Tagging Status.
- **Deployment** – Deployment Configuration and Deployment Status.

Example:
5. Click **Edit** in each section to edit the settings.
Configuring UEM to Deploy the SandBlast Mobile Protect app

Prerequisites

SandBlast Mobile Gateway / Server: gw.locsec.net

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".
3. Connect the app to your devices. See "Connecting the SandBlast Mobile Protect app to your Device".
4. Create the Mitigation Process for the app. See "Creating a Mitigation Process".
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".

You must add the Protect app for both iOS and Android operating systems.

To add the SandBlast Mobile Protect app to MobileIron Cloud:

1. Go to Apps > App Catalog > +Add and select the applicable App Store.

   Example:

   ![App Catalog](image)

   **Note:** As you add the SandBlast Mobile Protect app to your catalog,

   Rename this New Mobile Device App to SandBlast Mobile Protect app.

2. Enter SandBlast Mobile Protect to start searching the store.

   **Notes:**

   - For iOS App

   Select the Apple App Store

   Example:
For Android Enterprise App

Select Google Play Store.

Example:

4. In the Application Name field enter SandBlast Mobile Protect.
5. From the app list select the SandBlast Mobile Protect app.
6. Click Next.
7. On the Describe pane click Next.
8. On the Delegate pane click Next.

10. Select the User Provisioning Group: cpuser_test_group.
11. Click Add Distribution Filter.

12. Create a Distribution Filter.

Only the devices that are synchronized to the SandBlast Mobile Dashboard can install the application.

**Note** - For future reference, enter the name for this filter: cpuser_test_group.

a. In the Create Distribution Filter window enter a name and a description.
b. Select ANY and enter these parameters:
   - Custom Device Attribute > CHKP_Status is equal to Provisioned
   - Custom Device Attribute > CHKP_Status is equal to Active
   - Custom Device Attribute > CHKP_Status is equal to Inactive
c. Click Create Distribution Filter.
Example:

d. Click Next.

Example:
Note:
To select and apply an existing Distribution Filter:
  i. Go to Distribution Filter > Select below to distribute this app.
  ii. Select the cpuser_test_group option.
  iii. Click Next.
Example:

   e. Go to Configure pane and select the applicable option.
     - For iOS App
       Select iOS Managed App Configuration.
       Example:
        
        - For Android Enterprise App
          Select Manage Configuration for Android on the "+" button to the right.
13. On the **Configuration Setup** pane enter a name for this configuration.

14. Enter the configuration settings (a key/value pair and the key type).

15. Click **Next**.

**Get dashboard's token**

Go to your SandBlast Mobile dashboard > Settings > Device Management > Deployment > Edit:
Copy the token of your dashboard:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lacoon Server Address</td>
<td>String</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>String</td>
<td>${deviceSN}</td>
</tr>
<tr>
<td>DEVICE_UDID</td>
<td>String</td>
<td>${deviceUDID}</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>Take the copied value from the previous section</td>
</tr>
</tbody>
</table>
- For Android Enterprise Devices:

<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><code>${deviceGUID}</code></td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>Take the copied value from the previous section</td>
</tr>
</tbody>
</table>

16. Go to Configure pane and select the option Install on Device by clicking on the "+" button to the right. Example (this example is for an Android Device but applicable for both iOS and Android):

17. In the Configuration Setup enter a name and a description.
18. Toggle the button Install on Device – to be ON.
19. In the Distribute this App Config Configuration Setup section select Custom.
Example:

20. Select the User Group `cpuser_test_group` option and click “Next”.
21. Click Done.
Automatic Activation of SandBlast Mobile

If SandBlast Mobile Protect app is not installed or removed from device, then the device is marked as not protected. You must create a compliance policy that prompts the SandBlast Mobile Protect app installation on the device.

To prompt the SandBlast Mobile Protect app installation on your devices:

1. 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.
2. Connect the SandBlast Mobile Protect app to your organization.

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

Creating an App Control Policy

Procedure:

1. On the MobileIron Cloud portal go to Policies and click Add.

Example:

2. On the Choose Policy Type pane click on Allowed Apps section.

Example:

3. In the Add Policy window go to Required Apps > Policy and Compliance Setup and enter a name and a description.

4. Under the Add Apps tab from the pull-down menu select an applicable SandBlast Mobile Protect app.
Note - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

- **For iOS Apps:**

  Select Apple App Store > SandBlast Mobile.

  Example:

  ![iOS App Store Example](image)

- **For Android Enterprise Devices:**

  Select Google Play > SandBlast Mobile

  Example:

  ![Android Play Store Example](image)

5. Click **Next**.
6. On the **Whitelist / Blacklist Apps** pane click **Next**.
Configuring Email Notifications

1. On the Actions pane go to Allowed Apps and select Send Notification option from the menu.
2. Choose Send Both (Email and Push notifications).
3. Enter a subject and message body for the email message.
4. Enter a message for the push notification.

Example:

5. Click [+ ] to add more actions.
6. Select Block from the menu.

Example:
7. Select the checkbox to agree with statement and click "Next".

Example:

Connecting the SandBlast Mobile Protect app to your Device

To install the SandBlast Mobile Protect app on your devices in your organization, you must add them to the SandBlast Mobile Protect app group. This is a dynamic group assignment according to the associated tag.

Add all the devices marked with the Status tags to a group that indicates that the devices are registered in SandBlast Mobile Dashboard.

Create a mitigation process. See "Creating a Mitigation Process".
Creating a Protect app Group

Add the SandBlast Mobile Protect app group to your devices in the 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 Cloud portal, on **App Policy > Distribute** pane > select **Custom**.
   
   Example:

2. Click **Create new Device Group**.
   
   Example:

Assigning the Protect app Group to your Organization

1. In the Create **Device Group** window enter a name and description.
2. Select **Dynamically Managed**.
3. Enter a name and a description.
Configure Criteria 1 Section:

1. Select ALL of the following rules are true.
2. Set User Group is equal to cpuser_test_group.
3. Click the Group icon.

   The Group is added to your organization.

Configure Criteria 2 Section:

1. Select ANY of the following rules are true.
2. Set Criteria 1: Custom Device Attribute CHKP_Status is equal to Provisioned.
3. Set Criteria 2: Custom Device Attribute CHKP_Status is equal to Active.
4. Set Criteria 3: Custom Device Attribute CHKP_Status is equal to Inactive.
5. Click Save.

Example:

![Create Device Group](image)

6. Make sure the Protect App Group you created in the previous section is checked and click "Done".
Creating a Mitigation Process

To let the MobileIron Cloud 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 about tags 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 User and Device Provisioning group.

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

- Device Provisioning Group – cpuser_test_group.
- Custom Attribute - CHKP_Risk (set to High or Medium)
- Compliance Policy Group – SBM_cp_at_risk

The SBM_cp_at_risk Compliance policy applies to every device in the cpuser_test_group Provisioning Group has these parameters:

- CHKP_Risk custom attribute set to High or Medium
- Or
- CHKP_Status custom attribute set to Inactive

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:
2. On the Choose Policy Type pane click on **Compromised Devices** section.

   Example:

   ![Choose Policy Type](image)

3. In the **Settings** window enter a name and a description.

4. Select the applicable compliance actions and quarantine the device.
   i. Select **Block via Sentry**
   ii. Select **Send message to user (both email and push notification)**

5. Click **Next**.
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:

1. On the Distribute pane select Custom.
2. Click Create new Device Group.

Example:
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").

Procedure:

1. In the Create Device Group window enter a name and a description.
2. Select Dynamically Managed option.
3. For Criteria 1 set Select ALL of the following rules are true and set User Group is equal to cpuser_test_group.
4. For Criteria 2 select ANY and enter these parameters:
   - Custom Device Attribute > CHKP_Risk is equal to High
   - Custom Device Attribute > CHKP_Risk is equal to Medium
   - Custom Device Attribute > CHKP_Status is equal to Inactive
5. Click Save.
6. Make sure the Compliance Policy Group you created in the previous section is checked and click "Done".

Example:
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 Cloud for Android enterprise setup guide [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 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 BYUD 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:

```
Android Enterprise Deployment

Work & Personal deployment [Select groups...]
```
Notes:

- Only the synched groups in the upper groups’ section are available for Android Enterprise deployment.
- If one or more devices in the selected group have SandBlast MobileProtect app Version earlier than 3.6.4.4348, the operation stops until the devices are upgraded.
- If you add a group of devices for Android Enterprise deployment, make sure to configure the devices with both Personal and Work profiles.
- If you remove a group of devices from the Android Enterprise deployment, the SandBlast MobileProtect app deletes the Personal profile record on every device in this group.
- iOS devices are ignored in the Android Enterprise context.

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:

   ![Dashboard screenshot](image)

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

   Example:

   ```
   Android Enterprise Security Settings
   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:
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 Cloud for the device. This device must be added automatically to the Device Group with the criteria of an extension attribute. Also, MobileIron Cloud 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 Cloud. This adds the device to the Smart Mobile Device Group “CHKP_Risk_High”. Then the MobileIron Cloud system enforces policy actions specified in the Configuration Profile. This mitigation process is described in ”

<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 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” and in "Configuring Integration Settings".

**Deploying the SandBlast Mobile Protect app on the Devices**

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section "Configuring Integration Settings", 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 Cloud to sync with the SandBlast Mobile Dashboard, and several more minutes for MobileIron Cloud to push the App to the user device.
After you register your device in the MobileIron Cloud 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 Cloud 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.

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

   - **Android Device**
     a. Tap on the SandBlast Mobile Protect app in the Google Play Store.
     b. Tap **Install > Accept** on the SandBlast Mobile Protect app to accept the permissions of the App.
Example:

The App is installed.

c. Launch the App to finish its deployment and registration to Check Point SandBlast Mobile. The SandBlast Mobile Protect app is automatically registered.

2. The SandBlast Mobile Protect app scans the system.

d. Tap Continue

e. Enable security settings **Allow all required permissions**

f. Tap Enable

The registration server and the key are automatically configured in the App by the MobileIron Cloud system. See "Configuring UEM to Deploy the SandBlast Mobile Protect app".
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 Cloud system for that device. MobileIron Cloud 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 Cloud system. The MobileIron Cloud system then enforces policy actions specified in the Compliance Policy Profile.

Blacklisting a Test App

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

   Example:

   ![App Analysis Tab Example](image)

3. Go to **Default** and click **Policy**.

   A **Changing application policy** pop-up window opens.

4. From the **New Policy** drop-down menu, select **Black Listed**.
5. In the **Audit Trail note** field, enter a reason for this change.

   Example:
6. Click OK.

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

**View of a Non-Compliant Device**

The device with the blacklisted app 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".

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

**SandBlast Mobile Protect app Notifications**

You receive a SandBlast Mobile Protect notification that the blacklisted app is not allowed by Corporate Policy.

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

**Example:**

You are not allowed to use the app until you remove the blacklisted app or change the compliance policy settings. See "Creating a Mitigation Process".
Mobile@Work app Notifications

You receive SandBlast Mobile Protect app notifications in the Mobile@Work app.

You can see that the device is out of compliance and that it cannot access corporate resources.

Example:

![Notification Example]

You are not allowed to access your corporate data or network from this device until you uninstall this app to reduce the risk level.

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]

   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:

![Image of device details]

**Administrator View on the MobileIron Cloud Console**

In the MobileIron Cloud Portal, the Administrator can see that this device belongs to the "at risk" device group, in our example "CPTME_SBM_At_Risk".

- **Devices > Overview** tab:

  Example:

![Image of device overview]

- **Devices > Attributes** tab:

  The MobileIron Cloud Portal shows that the device has its custom device attribute “CHKP_Risk” set to
"High".

Example:

- **Devices > Policies** tab:

  The Administrator can see what Compliance Policy were applied, and we can see that the "at risk" policy was applied to this user's device.

  Example:

  The user cannot access their corporate data or networks from this device until they uninstall the blacklisted app and lower the risk.
Appendix

For more information see the online guide.

Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron Cloud Server/API URL</td>
<td></td>
</tr>
<tr>
<td>MobileIron Cloud API Admin Username</td>
<td></td>
</tr>
<tr>
<td>MobileIron Cloud API Admin Password</td>
<td></td>
</tr>
<tr>
<td>MobileIron Cloud Device Provisioning Group(s)</td>
<td></td>
</tr>
<tr>
<td>MobileIron Cloud 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 the SBM 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>