SandBlast Mobile for Workspace ONE UEM

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** ....................................................... 9
  Prerequisites .................................................................................................. 9
  Creating a Child Organization Group for SandBlast Mobile ............................ 10
  Creating API Account for Integration with the SandBlast Mobile .................... 11
    Creating REST API Key ............................................................................. 12
    Creating an API Only Administrator Account ......................................... 12
  Configuring Application Collection ............................................................... 15
  Adding Users to the SandBlast Mobile Organization Group ............................ 15
    Adding a Device to a User ........................................................................ 17
    Connecting User Device to Workspace ONE UEM .................................. 18
  Creating a Mitigation Process ...................................................................... 18
  Creating Tags for Devices in Organization Group ....................................... 18
  Creating a Dynamic Assignment Group for Risk Tags ............................... 20
  Creating a Compliance Policy for the Devices at Risk .................................. 21

**Configuring the SandBlast Mobile Dashboard UEM Integration Settings** .......... 25
  Prerequisites ................................................................................................ 25
  Configuring UEM Integration Settings ......................................................... 26

**Configuring UEM to Deploy the SandBlast Mobile Protect app** ................. 35
  Adding the SandBlast Mobile Protect app to your App Catalog .................... 36
  Automatic Activation of SandBlast Mobile: Prompt the Protect app installation 45
  Creating app Group for required apps ......................................................... 45
  Creating Smart Groups for Required Apps .................................................. 47
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Compliance Policy for Required Apps</td>
<td>49</td>
</tr>
<tr>
<td>Deploying the SandBlast Mobile Protect app automatically (Zero Touch Deployment) [Optional]</td>
<td>53</td>
</tr>
<tr>
<td>Using Android Enterprise with SandBlast Mobile</td>
<td>61</td>
</tr>
<tr>
<td>Profiles</td>
<td>61</td>
</tr>
<tr>
<td>Android Enterprise Deployment Scenarios</td>
<td>61</td>
</tr>
<tr>
<td>Configuring SandBlast Mobile Protect app to Protect your Devices</td>
<td>62</td>
</tr>
<tr>
<td>Deploying Android Enterprise on your Devices</td>
<td>62</td>
</tr>
<tr>
<td>Policies</td>
<td>64</td>
</tr>
<tr>
<td>Risk Handling</td>
<td>64</td>
</tr>
<tr>
<td>SandBlast Mobile Protect app Deployment</td>
<td>66</td>
</tr>
<tr>
<td>Deploying the SandBlast Mobile Protect app on the Devices</td>
<td>66</td>
</tr>
<tr>
<td>Testing High Risk Activity Detection and Policy Enforcement</td>
<td>69</td>
</tr>
<tr>
<td>Blacklisting a Test App</td>
<td>69</td>
</tr>
<tr>
<td>View of a Non-Compliant Device</td>
<td>70</td>
</tr>
<tr>
<td>Administrator View on the SandBlast Mobile Dashboard</td>
<td>71</td>
</tr>
<tr>
<td>Administrator View on the Workspace ONE UEM Console</td>
<td>72</td>
</tr>
<tr>
<td>Appendix</td>
<td>76</td>
</tr>
<tr>
<td>Integration Information</td>
<td>76</td>
</tr>
</tbody>
</table>
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 with low impact on device performance and 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 machine learning algorithms and state-of-the-art 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 UEM. It provides a quick tour through the interface of the UEM and the SandBlast Mobile Dashboard to enable integration, alerting, and policy enforcement. This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).

General Workflow

2. Configure the Check Point SandBlast Mobile Dashboard for integration with the Workspace ONE UEM. See "Configuring the Check Point SandBlast Mobile Dashboard Integration Settings" on page 25.
3. Configure your Workspace ONE UEM to deploy the Check Point SandBlast Mobile Protect app. See "Configuring UEM to Deploy the SandBlast Mobile Protect app" on page 35.
4. Apply the Check Point SandBlast Mobile Protect app on the device. See "SandBlast Mobile Protect app deployment" on page 66.
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’s mobile device management systems.
# Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 SandBlast Mobile Protect app  | - The SandBlast Mobile Protect app is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior.  
  - To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.  
  - The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience. |
| 2 UEM               | - Unified Endpoint Management (generalized term replacing MDM/EMM)  
  - Device Management and Policy Enforcement System |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 SandBlast Mobile Gateway</td>
<td>• The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.</td>
</tr>
<tr>
<td></td>
<td>• The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (organization’s) Dashboard instance.</td>
</tr>
<tr>
<td></td>
<td>• No Personal Information is processed by or stored in the Gateway.</td>
</tr>
<tr>
<td>4 SandBlast Mobile Management Dashboard</td>
<td>• The cloud-based web-GUI SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance.</td>
</tr>
<tr>
<td></td>
<td>• The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.</td>
</tr>
<tr>
<td></td>
<td>• When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities.</td>
</tr>
<tr>
<td>5 Behavioral Risk Engine</td>
<td>• The cloud-based SandBlast Mobile Behavioral Risk Engine (BRE) uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis.</td>
</tr>
<tr>
<td></td>
<td>• The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.</td>
</tr>
<tr>
<td></td>
<td>• The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.</td>
</tr>
<tr>
<td></td>
<td>• No Personal Information is processed by or stored in the Engine.</td>
</tr>
<tr>
<td>6 ThreatCloud</td>
<td>• Check Point’s ThreatCloud is the world largest incidence of compromise database that incorporates real-time threat intelligence from hundreds of thousand Check Point gateways and from millions of endpoints across the globe.</td>
</tr>
<tr>
<td></td>
<td>• ThreatCloud powers the Anti-Phishing, Safe Browsing, URL Filtering and Anti-bot technologies for SandBlast Mobile on-device Network Protection.</td>
</tr>
<tr>
<td></td>
<td>• ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis.</td>
</tr>
</tbody>
</table>
Preparing UEM Platform for Integration

Workspace ONE UEM deploys SandBlast Mobile Protect app on a device.

Prerequisites

- SandBlast Mobile service integrates with Workspace ONE UEM through the existing API. To enable integration, you must first create a Workspace ONE UEM API account. You must enable Workspace ONE UEM version 7.0 or later with REST 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 Workspace ONE UEM.
- You must configure your UEM to collect the app list from the devices enrolled to SandBlast Mobile. See "Configuring Application Collection" on page 15.

Workspace ONE UEM Console (Example)

General Workflow

2. Create API Account for the Check Point SandBlast Mobile Protect app. See "Creating API Account for Integration with the SandBlast Mobile" on page 11.
4. Adding Users to the SandBlast Mobile Organization Group. See "Adding Users to SBM Group" on page 15
5. Adding actions and policies to mitigate risk. See "Creating a Mitigation Process" on Page 18
Creating a Child Organization Group for SandBlast Mobile

To deliver content to devices and manage them, Workspace ONE UEM identifies users and establishes permissions through organization groups (OG).

Through your Workspace ONE UEM Console, you can:

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

For more information, see Workspace ONE UEM Console Basics Guide: Organization Groups Overview.

**Best Practice** - For integration with the Check Point SandBlast Mobile, use organization groups to set up the same UEM hierarchy as in your organization’s internal hierarchy, or set up OGs based on Workspace ONE UEM features and content.

You can access your organization groups in these ways:

- Through the **Groups & Settings > Groups > Organization Groups > List View** menu.
- Through the **Organization Group** drop-down menu.

**Best Practice** - It is recommended to create a Child Organization Group to place all the SandBlast Mobile devices in it.

To create a Child Organization group for your devices:

1. Go to **Groups & Settings > Groups > Organization Groups > Details**.
2. On the **Add Child Organization Group** tab, enter information in all the required (*) fields.
   **Note** - Make sure you create a **Group ID**. You need it to add users to the groups.
Example:

3. Click **Save**.

   The new Child Organization group the active organization group shows as active in the organization group drop-down menu.

   Organization Group example name - **My Comp**.

Example:

This Organization Group will be used later on for integrating devices into SandBlast Mobile Dashboard

### Creating API Account for Integration with the SandBlast Mobile

For the interaction with SandBlast Mobile at the API level, you must create a dedicated API account user in your Workspace ONE UEM.
Creating REST API Key

SandBlast Mobile integration prompts you to retrieve the REST API Key from Workspace ONE. You can use the existing one or create one yourself as detailed below.

To create a dedicated REST API Key:

1. On the Workspace ONE UEM Console, go to Groups & Settings > All Settings > System > Advanced > API > REST API.

   Your API Key is in the API Key box list.

   To add a new REST API Key you must set the Organization Group to the top root hierarchy level.

Example:

2. Click Save.

   Note - Use this API Key and use when you configure the UEM Settings in the SandBlast Mobile Dashboard. See "Configuring the Check Point SandBlast Mobile Dashboard Integration Settings" on page 25.

Creating an API Only Administrator Account

Best Practice - For the interaction at the REST API only, the Workspace ONE UEM Console provides an "API Only" Admin Role. You can use this Administrator account between the SandBlast Mobile Dashboard and the Workspace ONE UEM system.

To create an “API Only” Administrator Account:

1. Configure the API Only Admin settings.
   a. On the Workspace ONE UEM Console go to Accounts > Administrators > Roles.
   b. From the Roles list select the Read Only role and click Copy.
c. In the **Copy Role** window enter a **Name** and **Description** for this new role.

**Name** - `api_admin_role` (recommended).

**Description** - *Role for SandBlast Mobile Integration* (recommended).

Example:

![Copy Role Window](image)

**Copy Role**

<table>
<thead>
<tr>
<th>Name</th>
<th>api_admin_role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Role for SandBlast Mobile Integration</td>
</tr>
</tbody>
</table>

**Categories** section go to these options and set them to **Edit**:

- API > REST > Devices.
- API > REST > Groups.
- Device Management > Bulk Management.
- Device Management > Compliance.
- Monitor > Reports > General.
- Settings > Tags > Tags.

e. Click Save.
2. Set a new Administrator account.
   a. Go to Accounts > Administrators > List View click Add and select Add Admin.

   Example:

   ![Add/Edit Admin window](image)

   The Add/Edit Admin window opens.

   b. On the Basic tab, enter applicable information in all the fields marked with (*).

   Example:

   ![Basic tab](image)

   c. On the Roles tab select the Child Organization group and the api_admin_role that you created previously. Example:
Configuring Application Collection

In order for the SandBlast Mobile Dashboard to be updated with device app lists after the initial device sync, the UEM must be configured to collect the app list from the devices enrolled to SandBlast Mobile. Without this setting in place SandBlast Mobile will not be able to get the app list from the iOS Devices and analyze application risk. To configure the UEM to collect the app lists:

1. Go to Groups & Settings > All Settings > Devices & Users > General > Privacy > Applications > Personal Application.
2. Make sure to set the parameters to Collect Do Not Display or Collect and Display for the all device ownership levels.

   ![Organizational Group](image)

   **Note** - If you do not want the Workspace ONE UEM Console interface to display the list of applications installed across all the devices, then you can change the privacy settings to Collect Do Not Display.

3. Click Save.

Adding Users to the SandBlast Mobile Organization Group

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 Child Organization Group for SandBlast Mobile" on page 10.

There are two ways to add a user to the organization group: You can use Add User option to add one user, or Batch Import option to upload more than one user at a time.
Procedure:

1. On the Workspace ONE UEM Console go to **Accounts > Users > List View** click **ADD** and select **Add User**.

   Example:

   ![Workspace ONE UEM Console screenshot](image)

2. In the **Add/Edit User** window, set these parameters:
   a. On the **General** tab, enter applicable information in all the fields marked with (*).

   Example:

   ![Add/Edit User window screenshot](image)

   b. Click **Save**.
Adding a Device to a User

You must assign the protected device to the user in your organization. Enter applicable information in all the fields marked with (*).

1. In the General section, enter the Friendly Name and Organization Group.
2. In the Device Ownership Type drop-down list, select the Ownership:
   - Corporate – Dedicated.
   - Corporate – Shared.
   - Employee Owned.
   - None.
3. Select the Message Type for example Email and enter the user email address.

   Example:

4. Click Save.
5. Make sure the device is ready and waits for enrollment: go to Devices > Lifecycle > Enrollment Status.
Example:

![Device Enrollment Status](image)

**Note** - The device will show in the Devices > List View only after the device completes the enrollment process.

Connecting User Device to Workspace ONE UEM

For information about connecting User Device to Workspace ONE UEM see the online guide - Device Enrollment.

Creating a Mitigation Process

To let Workspace ONE UEM identify the devices-at-risk and enforce compliance policies according to the risk level determined by SandBlast Mobile analysis, you can apply the built-in Risk tags. The SandBlast Mobile Dashboard uses tags to label the device with the risk level that the SandBlast Mobile analysis determines.

Creating Tags for Devices in Organization Group

Here below are the instruction on how to create the 7 tags manually in Workspace ONE UEM:

**Note** – The CHKP Tags must be created at the Customer Organization Group level, highest parent organization group. The tags name must match exactly as detailed in the tables below so please copy the exact text strings.

To create CHKP tags for Devices in the Customer Organization Group:

1. Go to Groups & Settings > All Settings > Settings > Devices & Users > Advanced > Tags.
2. Create CHKP Risk tags.

Click +Create Tag to create these tags (Copy & Paste from the table below):

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHKP_Risk_None</td>
<td>No risk detected by SandBlast Mobile</td>
</tr>
<tr>
<td>CHKP_Risk_Low</td>
<td>Low risk detected by SandBlast Mobile</td>
</tr>
<tr>
<td>CHKP_Risk_Medium</td>
<td>Medium risk detected by SandBlast Mobile</td>
</tr>
<tr>
<td>CHKP_Risk_High</td>
<td>High risk detected by SandBlast Mobile</td>
</tr>
</tbody>
</table>
3. Create CHKP Status Tags.

Click +Create Tag to create these tags (Copy & Paste from the table below):

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHKP_Status_Provisioned</td>
<td>During the first synchronization of a device in SandBlast Mobile Dashboard. Device created via the integration process but user have not installed the app yet.</td>
</tr>
<tr>
<td>CHKP_Status_Active</td>
<td>The user has installs and registers to SandBlast Mobile.</td>
</tr>
<tr>
<td>CHKP_Status_Inactive</td>
<td>In case the device did not make contact with SandBlast Mobile Dashboard for X number of days (that the SandBlast Mobile Admin configured).</td>
</tr>
</tbody>
</table>

Example:

4. Make sure that each mobile device in Workspace ONE UEM has one of these Status values and one of the Risk values. See example in "Admin view of the Workspace ONE UEM" on page 74.
Creating a Dynamic Assignment Group for Risk Tags

Create the Smart Group for the devices-at-risk.

Procedure:

1. Go to **Groups & Settings > Groups > Assignment Groups**.
2. Click **+Add Smart Group**.

Example:

```
1. Enter Tag name - Select these tags:
   - CHKP_Risk_High
   - CHKP_Risk_Medium
   - CHKP_Risk_Low
```
2. Click **Save**.

**Creating a Compliance Policy for the Devices at Risk**

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

To accomplish the policy enforcement on the devices, you must create Device Profiles and the Compliance Policy to apply these profiles to the devices.

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 their production environment, needs, and internal security policy.

**To create a Compliance Policy for the Devices at Risk:**

1. Go to **Devices > Profiles & Resources > Profiles**, click **Add > Add Profile**.

Example:
2. In the **Add Profile** window, select a platform to start.

   The **Add Profile** window opens.

   Example:

   ![Add Profile Window Example](image)

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

3. Configure the profile for Non-Compliant Devices Policy.
   a. Configure setting in the **Add a Profile** window:
      
      - **General Tab**
      
      - **Name** - Enter a unique Profile name (for example, *Non-Compliant iOS Devices Policy*).
      - **Description** - Enter short description (for example, *Non-Compliant iOS Devices Policy*).
      - **Assignment Type** - Select **Compliance**.
      - **Managed By** – Select the relevant OG under which the profile is managed

      Example for iOS:
- **Restrictions** Tab > click **Configure**.

Example for iOS:

By default, all the device functions are activated in **Device Functionality** section (for iOS devices), or in **Work Managed Device** (for Android devices). When you remove the check mark, you completely disable the function once the profile is applied.

Example for iOS:
b. Click Save and Publish.

4. Configure the compliance policy for the non-compliant devices.
   
   **Note** - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

   Preform steps 1-10 as in "Creating a Compliance Policy for the required app" on page 49.

   **Notes:**
   - On the **Rules** tab:
     - For iOS devices - Select **OS Version, Greater Than or Equal To, Apple - iOS 8.0.0**.
     - For Android devices - Select **OS Version, Greater Than or Equal To, Android - Android 5.0.0**.
   - On the **Assignment** tab, add the Assignment Group you created in "Creating a Dynamic Assignment Group for Risk Tags" on page 19.
   - On the **Summary** tab, enter a unique name for the **Compliance Policy**, and add the description of the policy, while both contain the words **Device At Risk**. Examples:
     - For iOS - Name this policy **iOS Devices At Risk**.
     - For Android - Name this policy **Android Devices At Risk**.

5. Click **Finish and Activate**.

   **Note** - Check Point recommends to create a separate Smart Group for each risk level and for each device status (active, inactive, and more).
Configuring the SandBlast Mobile Dashboard UEM Integration Settings

The following section includes all necessary configuration steps for SandBlast Mobile Dashboard that will enable the integration with Workspace ONE UEM.

**Note** - For easy reference during configuration, you can record your settings in the special table (see "Integration Information" Appendix on page 76).

**Prerequisites**

You need these details from your Workspace ONE UEM Deployment:

- **Server**: The URL of your Workspace ONE UEM System. Usually - the same as the Workspace ONE UEM Console URL.
- **User name and Password**: Credentials of API Account. See "Creating API Account for Integration with the SandBlast Mobile" on page 11.

  The credentials that the SandBlast Mobile Dashboard uses to connect to Workspace ONE UEM.

- **API Key**: use the API Key for the REST API Service. The key is located within your Workspace ONE UEM Console interface. See "Creating REST API Key" on page 11.
- **Group(s)**: The Workspace ONE UEM Organization groups or smart groups (Assignment Groups) to which the devices are registered and then integrated with the SandBlast Mobile Dashboard. You can integrate Multiple Groups. Selecting a parent group will not integrate devices from subsequent child groups.

  If a Parent Organization Group is integrated with a SandBlast Mobile Dashboard, then any child Organization Group of that Parent cannot be integrated with a different SandBlast Mobile Dashboard.

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

After you complete the necessary steps, the **Integrations** pane shows the detailed status of the all 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:

   ![Integration Wizard](image)

2. Configure the settings for Workspace ONE UEM Deployment.

   - **Server Setup**

     Configure your UEM to integrate with the created Workspace ONE UEM devices:

     a. In **Server Setup** section, enter this information:

        - **UEM service** - Workspace ONE
        - **Server Address** - The full URL needed for the UEM service
        - **User name**
        - **Password**
        - **API Key**
        - **Connector Setup** (advanced)
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**

You can configure SandBlast Connector when the UEM 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 groups of devices that will synchronize with SandBlast Mobile Dashboard. The dropdown list will automatically populate all the Organization Groups and Smart Groups the API user from previous step has access to.
Example:

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

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

   Select the groups for two deployed applications as part of the Workspace ONE UEM Android Enterprise deployment. See "Using Android Enterprise with SandBlast Mobile" on page 53.

   ![](attachment:image)

   **Note** – the list will populate only groups selected from previous step of synchronized groups

   Please make sure you select a group that include Android devices that are configured to have both personal and work profiles (iOS devices can be included in this group as well)

   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, by default it is set to ON.

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

Example:

![Workspace ONE Integration](image)

<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 threshold</td>
<td>Percentage of devices allowed for deletion after UEM device sync (in %).</td>
<td>0-100% : use 100% for no threshold *</td>
</tr>
<tr>
<td>Deletion delay 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>
</tbody>
</table>
App sync interval | Interval to connect with UEM to sync applications | 10-1440 minutes, in 10 minute intervals.

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

d. Click Next.

**Tagging Configuration**

Specify whether to send tag information to Workspace ONE UEM in order to communicate the deployment status of SandBlast Mobile Protect app and the risk level of the device.

Example:

a. In **Tagging Configuration** Section:

   i. Set all to **ON** (recommended) if you want to communicate the following characteristics of the device to the UEM:

   - **Tag device status** - the device status in SandBlast Mobile
   - **Tag device risk** - the device risk level in SandBlast Mobile
   - **Tag device TF** – the corresponding threat factors detected on the device by Sandblast mobile

   See "Creating Tags for Devices in Organization Group" on page 18.
b. In **Advanced** section:

The **Mitigation** tag is an additional tag value that is defined in Workspace ONE UEM and it will be set by SandBlast Mobile on the device only when the device is at High Risk.

![Mitigation Tag](image)

**Note** - If you are using the **Tag device risk** option from above you typically do not need to use this setting..


c. Click **Finish** to end the process or **Next** to continue to more advanced deployment options.

**Example:**

![Deployment](image)

- **Deployment**

  Check the “Allow auto device addition prior to device sync” option in case you require a faster device enrollment. 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.

![Dashboard Token](image)

**Note** - use the “copy to clipboard” button to set the Token value in the Application configuration step in the UEM. See section *Configuring the Application Configuration settings* Page 43
**Note** – The token is the hashed unique identifier of your dashboard. We will use it in a later step, when we will configure application configurations on Intune.

If you use SandBlast Mobile to manage the deployment and not the UEM:

In the **Advanced** section:

a. Enable options to have SandBlast Mobile Dashboard send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app. Usually when the UEM is configured it will notify the end user itself to install the app so this option is disabled by default.

b. Click **Finish**.
4. **View the Integration Status:** In **Settings > Integration** 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.
- **Device Sync Status** – The synchronized groups and the device sync status time stamp.
- **App Sync Status** – The last time applications were fetched from the UEM (Applicable for iOS deployment only).
- **Tagging** – Tagging Configuration and Tagging Status.
- **Deployment** – Deployment Configuration and Deployment Status.
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

In the following section, we will configure the Workspace ONE UEM to deploy the SandBlast Mobile Protect app to the managed devices.

Prerequisites

- The CHKP Status tags must be created at the customer Organization Group, highest parent organization group. See section "Creating Tags for Devices in Organization Group" on page 18
- Navigating to Groups & Settings > All Settings > Settings > Devices & Users > Advanced > Tags, the following tags should exist:
  - CHKP_Status_Provisioned
  - CHKP_Status_Active
  - CHKP_Status_Inactive

Notes:

- If you configured Workspace ONE UEM for Whitelisting Apps, you must add the SandBlast Mobile Protect app to the white list.
- You must add the SandBlast Mobile Protect app for both 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" on page 36.
2. Prompt the SandBlast Mobile Protect app installation on your devices. See "Automatic Activation of SandBlast Mobile: Prompt the Protect app installation" on page 45.
3. Connect the app to your devices. See "Deploying the SandBlast Mobile Protect app to your Device" on page 66.
Adding the SandBlast Mobile Protect app to your App Catalog

Using the CHKP Status Tags we can start deploying the SandBlast Mobile Protect app from the public stores to those devices that will be protected by Check Point SandBlast Mobile. We will do this to only require the Protect app when the device has the CHKP_Status of Provisioned, Active, or Inactive. If all of these tags are empty or 0, then the user will NOT be prompted to install the Protect app. This ensures that the devices are synchronized in the SandBlast Mobile Dashboard before asking the user to install the SandBlast Mobile Protect app.

Notes:
- As you add the SandBlast Mobile Protect app to your catalog, rename this New Mobile Device App to SandBlast Mobile Protect app.
- Approve the SandBlast Mobile Protect app in Work Google Play account.

Add SandBlast Mobile Protect app for iOS:

1. Go to Apps & Books > Applications > Native > Public.
2. Click +Add Application.

An Add Application window opens.

Example:
3. From the Managed By drop-down menu, select the proper Organization Group.
4. In Platform, select Apple iOS
5. Source should be “Search App Store”
6. Type “SandBlast Mobile Protect” into the Name field.

Example:

Add Application

<table>
<thead>
<tr>
<th>Managed By</th>
<th>My Comp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform *</td>
<td>Apple iOS</td>
</tr>
<tr>
<td>Source</td>
<td>[SEARCH APP STORE] ENTER URL</td>
</tr>
<tr>
<td>Name *</td>
<td>SandBlast Mobile Protect</td>
</tr>
</tbody>
</table>
5. Click **Next**.

The search result window shows the SandBlast Mobile Protect app.

6. Go to the SandBlast Mobile Protect app and click **Select**.

The **Add Application - SandBlast Mobile Protect** window opens.

Example:
8. Click **Save & Assign**.
9. The **SandBlast Mobile Protect - Assignment** window opens in the **Distribution** tab.
10. Give the assignment **Name** and select the **Assignment group**. This is the group of iOS devices that will be pushed with SandBlast Mobile Protect app.
11. Set the **App Delivery Method > Auto**.

Example:

For example, you can set the assignment group to a group that will include only devices that are tagged with `CHKP_Status_Provisioned (/Active/Inactive)`; this will prompt the user to install the SandBlast Mobile Protect app on the device only if it already synced into SandBlast Mobile Dashboard.

12. Click the **Restrictions** tab:
    - Turn **Managed Access** to **ON**,
    - **Remove On Unenroll** to **ON**,
    - **Prevent Application Backup** to **ON**

Example:

13. Click the **Application Configuration** tab

14. Turn **Send Configuration** to **ON**

15. Click **+Add** to insert rows in the Application Configuration table and enter the Key-Value information as detailed in the following table:
<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Value Type</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>{DeviceSerialNumber}</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 in the SandBlast Mobile Dashboard go to Settings &gt; Device Management. For more information see &quot;Configuring UEM Integration Settings on the SandBlast Mobile – Deployment Section&quot; on page 31.)</td>
</tr>
<tr>
<td>DEVICE_UDID</td>
<td>String</td>
<td>{DeviceUid}</td>
</tr>
</tbody>
</table>

Notes:
It is recommended to Copy & Paste the Configuration Key and Configuration Value directly from the table above.

Example:

16. Click Create
17. Examine the Assignment details if all looks good click Save
Example:

Add SandBlast Mobile Protect app for Android:

1. Go to Apps & Books > Applications > Native > Public.
2. Click +Add Application.

An Add Application window opens.

Select the Android Platform and search for “SandBlast Mobile Protect” app:

Notes:

Android EMM registration is required here – select the appropriate settings for your organization - Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration
Example:

Add Application

<table>
<thead>
<tr>
<th>Managed By</th>
<th>My Comp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform*</td>
<td>Android</td>
</tr>
<tr>
<td>Source</td>
<td></td>
</tr>
<tr>
<td>Name*</td>
<td>SandBlast Mobile Protect</td>
</tr>
</tbody>
</table>

3. Click Next.

4. Select “SandBlast Mobile Protect” and Click Select

Set the app Name “SandBlast Mobile Protect”.
Example:

5. Click **Save & Assign**.

6. The **SandBlast Mobile Protect - Assignment** window opens in the **Distribution** tab.

7. Give the assignment **Name** and select the **Assignment group**. This is the group of iOS devices that will be pushed with SandBlast Mobile Protect app.

8. Set the **App Delivery Method** > Auto.

9. In the **Restrictions** tab turn **Managed Access** > ON

10. In the **Application Configuration** tab turn **Send Configuration** > ON
Example:

<table>
<thead>
<tr>
<th>SandBlast Mobile Protect - Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Configuration</strong></td>
</tr>
<tr>
<td>EMM Managed Access</td>
</tr>
<tr>
<td>Only devices enrolled in EMM will be allowed to install the app and receive policies below:</td>
</tr>
<tr>
<td>Managed Access</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MDM UUID</td>
</tr>
<tr>
<td>{DeviceUid}</td>
</tr>
<tr>
<td>Token</td>
</tr>
<tr>
<td>hash_tenant_id**</td>
</tr>
<tr>
<td>(The SHA-256 value of the Dashboard Management ID. You must use the token configured in the Deployment section in the SandBlast Mobile Dashboard go to Settings &gt; Device Management. For more information see &quot;Configuring UEM Integration Settings on the SandBlast Mobile – Deployment Section&quot; on page 31.)</td>
</tr>
</tbody>
</table>

Enter the following Configurations:

<table>
<thead>
<tr>
<th>Item</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM UUID</td>
<td>{DeviceUid}</td>
</tr>
<tr>
<td>Token</td>
<td>hash_tenant_id**</td>
</tr>
</tbody>
</table>

11. Click Create
12. Examine the Assignment details if all looks good click Save
13. Click Publish
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 here are the steps to make SandBlast Mobile Protect app a required app on provisioned devices

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.

Creating app Group for required apps

Procedure:


2. In the Add Application Group window, on the List tab, configure these settings:
   - In the Type field, select Required.
   - In Application Name field, enter the name of the SandBlast Mobile Protect app ("SandBlast Mobile Protect").
Note - The data fields are similar for both iOS and Android users. The examples below are applicable for both platforms.

- **For iOS Apps**
  a. In the Platform field, select Apple iOS.
  b. In the Name field, enter a unique group name Required iOS Apps.
  c. Search the Apple AppStore for the SandBlast Mobile Protect app.

Search: sandblast mobile

The SandBlast Mobile Protect app ID shows in the Application ID field.

Example:

View Application Group

- **For Android Apps**
  a. In the Platform field, select Android.
  b. In the Name field, enter a unique group name (we recommend: Required Android Apps).
  c. Search the managed Google Play Store for the SandBlast Mobile Protect app. In the search result window select the SandBlast Mobile Protect app and click +Select link.

Search: SandBlast mobile
The SandBlast Mobile Protect app **ID** shows in the **Application ID field**.

Example:

3. Click **Add Application**.
4. Click **Enter**.
5. Click **Next**.
6. In the **Add Application** Group window, on the **Assignment** tab:
   a. In the **Description** field enter the device group description (for example, **Req. iOS devices** or **Req. Android devices**).
   b. Assign the Organization Group to the proper SandBlast Mobile Protect group. Enter applicable information in all the fields marked with (*).
8. Click **Finish**.

### Creating Smart Groups for Required Apps

**Procedure:**

1. Go to **Groups & Settings > Groups > Assignment Groups**.
2. Click **+Add Smart Group**.

   Example:
3. In the Create New Smart Group window, assign the tags for the dynamic group devices:
   - **Name** - Enter a unique Smart Group name. “
   - **Enter Tag name** - Select these tags:
     - CHKP_Status_Active
     - CHKP_Status_Inactive
     - CHKP_Status_Provisioned

   Example:
4. Click **Save**.

**Creating a Compliance Policy for Required Apps**

The Compliance Policy is activated on the devices that did not install the required apps.

You must create separate compliance policies for specific OS types: iOS and Android.

**Note** - In every organization, the customer configures the compliance policies according to the production environment needs, and the internal security policy. The policies and their Actions described below can serve as an example only.

**To create a Compliance Policy:**

1. Go to **Devices > Compliance Policies > List View**, and click **+ Add**.

Example:
2. In the **Add Compliance Policy** window, select a platform to start.

The **Add Compliance Policy** window opens.

Example:

![Add Compliance Policy Window](image)

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

3. On the **Rules** tab, select **Application List** and **Does Not Contain Required App(s)**.

Example:

![iOS Add Compliance Policy](image)

4. Click **Next**.

5. **On the Actions tab, add actions:**
- Enable the **Mark as Not Compliant** checkbox.
- Select and add the actions to your policy. For example, **Notify the user by email**, **Send Push Notification to Device**, and **Block/Remove All Managed Apps**.
- Use the [+ button to add a new action.

**Example for iOS:**

![Image of iOS configuration settings]

**Example for Android:**

![Image of Android configuration settings]

Here we are using the option **Disable All managed Apps** to block access to corporate data from the work profile in Android Enterprise

**Note** - If the User cannot resolve an issue, click + Add Escalation to add an escalation action. You can set these actions to repeat themselves over a specified number of times over a specified interval.

6. Click **Next**.
7. On the **Assignment** tab:

   In the Smart Groups field, select the dynamic Assignment Group you created in previous step "Creating a Dynamic Assignment Group" on page 19.

Example:
8. Click **Next**.
9. On the **Summary** tab:

Enter a unique name for the **Compliance Policy**, and add the description of the policy.

Example:

10. Click **Finish & Activate**.
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.

- **Zero Touch Deployment in Android Enterprise devices**
  1. Create new custom profile. Go to Devices > Profiles & Resources > Profiles > Add Profile.
  2. In "Add Profile" select the Android platform:
- Under General, select a name for the profile and assign to your Workspace ONE Smart Group.

- Excluded Groups > Create new Smart Group > sbm_registered.
- Exclude devices that have the CHKP_Status_Active or CHKP_Status_Inactive status Tag.
- Click Save.
3. Under Custom Settings click configure and Copy & Paste the following text - notice to replace the tenant token):

```xml
<characteristic uuid="9310785f-25a5-423e-b5e5-675100546e6e" type="com.airwatch.android.androidwork.app.com.lacoon.security.fox">
    <parm name="EnableAlwaysOnVPN" value="True" type="boolean" />
    <parm name="LockDown" value="False" type="boolean" />
    <parm name="token" value="your_tenant_token" type="string" />
    <parm name="mdm_uuid" value="{DeviceUid}" type="string" /></characteristic>
```

Use the token configured in the Deployment section in the SandBlast Mobile Dashboard go to Settings > Device Management. For more information, see "Configuring UEM Integration Settings on the SandBlast Mobile – Deployment Section" on page 31)
4. Save and Publish.
5. Create another custom profile. Go to Devices > Profiles & Resources > Profiles > Add Profile.
   - Under General, select a name for the profile and assign to your Workspace ONE Smart Group.
- Excluded Groups > Create new Smart Group > sbm_not_registered.
- Exclude devices that have the CHKP_Status_Provisioned status Tag.
- Click Save.
6. Under Custom Settings, Copy & Paste the following:

```xml
<characteristic uuid="9310785f-25a5-423e-b5e5-675100546e6e"
type="com.airwatch.android.androidwork.app.com.lacoon.security.fox">
  <parm name="EnableAlwaysOnVPN" value="False" type="boolean"/>
  <parm name="LockDown" value="False" type="boolean"/>
</characteristic>
```

7. Save and Publish.

- **Zero Touch Deployment in iOS devices**
  1. Create new Device profile. Go to Devices > Profiles & Resources > Profiles > Add Profile.

```
Profiles

Devices > Profiles & Resources > Profiles > Add Profile
```

2. In "Add Profile" select the iOS platform:
a. Select Device Profile in Context.

b. Under General, Name the profile and assign it to your Workspace ONE Smart Group.

c. Under the VPN tab:
   - **Connection Name**: Check Point Local Tunnel
   - **Connection Type**: Custom
   - **Identifier**: com.checkpoint.capsuleprotect
   - **Server**: www.checkpoint.com
- **Account:** {DeviceUuid}
- **Custom Data:** zero_touch=true
- **User Authentication:** Certificate
- **Identity Certificate:** None

d. Check the following boxes:
   - Enable VPN On Demand.
   - Use new on-demand keys.

e. Add the following On-Demand Rules:
   - Connect > Interface Match > Wi-Fi
   - Connect > Interface Match > Cellular
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 with Workspace ONE UEM, see 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” on page 62.

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 under “device sync status” section.
     b. In the Synchronization Configuration section select and add the device groups for both profiles under Android Enterprise Deployment.

Example:

![Android Enterprise Deployment Example](image)
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 Mobile Protect 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 solution will delete the Personal device record on every device in this group from SandBlast Mobile Dashboard.
- iOS devices are ignored in the Android Enterprise context even if they are part of the above group settings.

3. Click Finish.

4. 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.

To view and filter the devices:

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

   Example:

   ![SandBlast Mobile Dashboard](image)

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

<table>
<thead>
<tr>
<th>Profile</th>
<th>Icon</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>![icon]</td>
<td>Device Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OS - Android Enterprise</td>
</tr>
<tr>
<td>Personal</td>
<td>![icon]</td>
<td>Device Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OS - Android</td>
</tr>
</tbody>
</table>
Policies

To change policy for inactive personal profile:

   
   Example:

   ![Policy screenshot]

<table>
<thead>
<tr>
<th>#</th>
<th>Role Name</th>
<th>Groups</th>
<th>Policy Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Personal Side WGO</td>
<td>(Personal)</td>
<td>Personal Side Policy</td>
</tr>
<tr>
<td>2</td>
<td>Work Profile WGO</td>
<td>(Work)</td>
<td>Work Profile Policy</td>
</tr>
</tbody>
</table>

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

   ![Policy settings]

   **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:

![Risk handling screenshot]
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 work profile, if you tag a risk on the device. To configure mitigation tags, see *Creating a Mitigation Process* on page 18.
**SandBlast Mobile Protect app Deployment**

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

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section *Configuring Workspace ONE UEM Integration Settings on the SandBlast Mobile* on page 25, the App is automatically deployed to the devices that belong to the defined groups (see "*Configuring UEM to Deploy the SandBlast Mobile Protect app*" on page 35).

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

Note: This flow describes how to activate Sandblast Mobile application on your devices if you didn’t use the Zero Touch deployment described in the *Zero Touch Deployment* section on page 53. If you used the Zero Touch deployment you can skip this section. The devices will be automatically activated and your users will have to approve a few permissions, according to the policy defined for the user group in Sandblast Mobile dashboard, for example Location permission or Notification access.

Note that for Android devices, Android Enterprise is mandatory for the Zero Touch deployment process.

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

- **iOS Device Process**
  1. Tap INSTALL on the SandBlast Mobile Protect app.
  2. The Protect app is deployed the iOS Device.
  3. Launch the Protect app to finish the registration.
  4. Workspace ONE UEM system automatically configures the registration server and the key in the Protect app.
  5. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.

Example:
Android Enterprise Device Process

After the device is enrolled to Workspace ONE and the work profile is activated, SandBlast Mobile Protect app will be pushed and installed automatically since it is a managed and a required app.

1. When the user opens the app the app will register in the SandBlast Mobile Dashboard and become active.
2. According to the policy defined for the device the user might need to approve few permissions for example, allowing Notification access or Location permissions.
3. SandBlast Mobile Protect app might show the device at high risk because it is configured to alert when the personal side is not protected. See “Using Android Enterprise with SandBlast Mobile” on page 52.

4. Once the user installs the SandBlast Mobile Protect app on the personal side via his google play (relevant for COPE or BYOD modes) the app will automatically registers to the dashboard and becomes fully active.
The registration server and the key are automatically configured in the App by the Workspace ONE UEM system. See "Configuring UEM to Deploy the SandBlast Mobile Protect app" on page 35.
Testing High Risk Activity Detection and Policy Enforcement

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

In this example, the Administrator blacklists an app, for example, "Box". As a result, the user’s device is identified to be at High Risk due to the blacklisted app installed on the device. The SandBlast Mobile Dashboard notifies the UEM, and mark the device as High Risk (CHKP_Risk_High tag) to the Workspace ONE UEM system. The Workspace ONE UEM system then enforces policy actions specified in the Configuration Profile.

Blacklisting a Test App

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

Example:

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:

![Image](image)

6. Click **OK**.

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

**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 "**Deploying the SandBlast Mobile Protect app to your Device**" on page 66.

**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.

If you configured an email notification, you receive an email from Workspace ONE UEM.

**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**" on page 18.

**SandBlast Mobile Protect app Notifications**

The user receives SandBlast Mobile Protect app notifications.

Example:
Workspace ONE UEM Agent App Notifications

The user receives Workspace ONE UEM Agent notifications.

Example:

Workspace ONE UEM Agent App Notifications

The user receives an email from the Workspace ONE UEM system.

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:
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 Workspace ONE UEM Console**

On the Workspace ONE UEM Console:

1. Go to **Devices > Dashboard** view.
   You can see the devices that have compliance violations, or violate some policies, or both.
Example:

2. Go to **High Risk > List View**.

You can see the devices in the Out of Compliance state.

Example:

3. Click **Layout > Summary**, then click on the specified device with the Status **Non-Compliant**.

The **Details View** page opens.

- **Summary tab**

You can see the Smart Groups, the Status Tags, and the Risk Tags of the device. See "Creating Mitigation a Process - Tags" on page 18.
Example:

- **Compliance tab**

  You can see that the device is out of compliance, and the policy that applies to the device.

Example:

- **Profiles tab**

  You can see that the device has the **Non-Compliant Android Device Policy** profile.

Example:

- **Click More > Status History.**
  
  **Status History tab**
You can see the status history, and see when the device was non-compliant.

Example:
## Appendix

### Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEM/ Server URL</td>
<td></td>
</tr>
<tr>
<td>UEM Web Services URL</td>
<td></td>
</tr>
<tr>
<td>UEM API Account Username</td>
<td></td>
</tr>
<tr>
<td>UEM API Account Password</td>
<td></td>
</tr>
<tr>
<td>UEM Organization Group(s)</td>
<td></td>
</tr>
<tr>
<td>UEM Mitigation Group</td>
<td></td>
</tr>
<tr>
<td>Tag Device Status (Boolean tags)</td>
<td>CHKP_Status_Provisioned</td>
</tr>
<tr>
<td></td>
<td>CHKP_Status_Active</td>
</tr>
<tr>
<td></td>
<td>CHKP_Status_Inactive</td>
</tr>
<tr>
<td>Tag Device Risk (Boolean tags)</td>
<td>CHKP_Risk_None</td>
</tr>
<tr>
<td></td>
<td>CHKP_Risk_Low</td>
</tr>
<tr>
<td></td>
<td>CHKP_Risk_Medium</td>
</tr>
<tr>
<td></td>
<td>CHKP_Risk_High</td>
</tr>
<tr>
<td>SandBlast Mobile Gateway</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>SandBlast Mobile App Name (iOS / Android)</td>
<td>SandBlast Mobile Protect</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (iOS)</td>
<td>com.checkpoint.capsuleprotect</td>
</tr>
<tr>
<td>Information Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (Android)</td>
<td>com.lacoon.security.fox</td>
</tr>
</tbody>
</table>