07 January 2021

SandBlast Mobile for Blackberry UEM

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 2021 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and recompilation. 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
  - General Workflow .......................................................................................... 9

- **Creating API Account for Integration with the SandBlast Mobile** .................. 10

- **Adding a User** .............................................................................................. 14
  - Adding a User from Corporate Directory ...................................................... 15
  - Adding a local User ....................................................................................... 17
  - Adding a Device to an Existing User ............................................................. 18

- **Creating User Provisioning Groups** ................................................................ 20
  - Information about Device Risk & Status tags and BlackBerry UEM user groups .... 20
  - Creating a User Group based on Corporate User Directory ......................... 21
  - Creating Local User Group(s) ....................................................................... 23
  - Adding an Existing User to the Local User Group ......................................... 25
  - Adding a New User to an Existing Local User Group .................................... 26
  - Nesting User Groups (optional) .................................................................... 28

- **Enrolling Devices to BlackBerry UEM** ......................................................... 30

- **Configuring the Check Point SandBlast Mobile Dashboard Integration Settings** .................................................................................................................. 31
  - Prerequisites...................................................................................................... 31
  - Configuring BlackBerry UEM Integration Settings on the SandBlast Mobile ......... 32

- **Configuring UEM to Deploy the SandBlast Mobile Protect app** ....................... 42
  - Prerequisites...................................................................................................... 42
  - General Workflow .......................................................................................... 42
  - Adding the SandBlast Mobile Protect app to your App Catalog ...................... 43
Appendix

Testing High Risk Activity Detection and Applying the SandBlast Mobile Protect app on Devices

Using Android Enterprise with SandBlast Mobile

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

Using Android Enterprise with SandBlast Mobile

Deploying the SandBlast Mobile Protect app on Devices

Testing High Risk Activity Detection and Policy Enforcement

Integration Information
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 BlackBerry UEM. It provides a quick tour through the interface of the BlackBerry 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

1. Prepare your BlackBerry UEM platform for the Check Point SandBlast Mobile Protect app integration. See "Preparing UEM Platform for Integration" on page 9.
2. Configure the Check Point SandBlast Mobile Dashboard for integration with the BlackBerry UEM. See "Configuring the Check Point SandBlast Mobile Dashboard Integration Settings" on page 31.
3. Configure your BlackBerry UEM to deploy the Check Point SandBlast Mobile Protect app. See "Configuring UEM to Deploy the SandBlast Mobile Protect app" on page 42.
4. Apply the Check Point SandBlast Mobile Protect app on the device. See "Applying the SandBlast Mobile Protect app on Devices" on page 71.
Introduction to the SandBlast Mobile Integration Guide

The SandBlast MobileProtect 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 MobileProtect app with the company device managing systems.
# Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SandBlast Mobile Protect app</td>
<td>- 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.&lt;br&gt;- To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.&lt;br&gt;- 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.</td>
</tr>
<tr>
<td>2 UEM</td>
<td>- Unified Endpoint Management (generalized term replacing MDM/EMM)&lt;br&gt;- Device Management and Policy Enforcement System</td>
</tr>
<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.&lt;br&gt;- The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (organization’s) Dashboard instance.&lt;br&gt;- No Personal Information is processed by or stored in the Gateway.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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

Prerequisites

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

BlackBerry UEM Console (Example)

For more or updated information regarding BlackBerry UEM, please see BlackBerry UEM Docs.

Note - For easy reference during configuration, you can record your settings in the special table (see "Integration Information" on page 78).

General Workflow

1. Create API Account for the Check Point SandBlast Mobile Protect app. See "Creating API Account for Integration with the SandBlast Mobile" on page 10.
2. Add a user to BlackBerry UEM. See "Adding a User" on page 14.
3. Create a group of users whose devices will be registered to the Check Point SandBlast Mobile solution. See "Creating User Provisioning Groups" on page 18.
4. Enroll a device to BlackBerry UEM. See "Enrolling Devices to BlackBerry UEM" on page 30.
Creating API Account for Integration with the SandBlast Mobile

For the interaction with SandBlast Mobile at the API, you must create a dedicated API account user in your BlackBerry UEM.

For more or updated information, please see Create an Administrator guide.

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

To create a new administrator user account:

1. On the BlackBerry UEM Console, go to Users, click Add user.

   Example:

2. On the Add a user window, On the Local tab, configure these settings:
   a. In the Display name field - Enter a display name.
   b. In the Username field – Enter a username.
   c. In the Email address field – Enter an email address.

   Example:
3. Click **Save**.

d. In the **Console password** field – Enter a temporary password for this user. When you login the first time with these credentials, you will be prompted to set a new password.

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

Example:
To assign new user to administrator role:

1. On the BlackBerry UEM Console, go to Settings > Administrators > Users, click Add an administrator icon.

   Example:

2. On the Add an administrator window, search/select the user you created in “Creating API Account for Integration with the SandBlast Mobile” on page 10.

   Example:

3. Click the user’s Name.

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

   Example:
5. Click **Save**.

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

Example:

7. Click **Sign In**.

8. On the **New password** window, enter in a new password.

Example:
9. Click **Submit**.

10. On the “**Find out about...**” window, select **“Do not show this again”**.

    Example:

11. Click **Start**.

12. Click **Log out**.

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

**Adding a User**

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

For more or updated information see [Create a user account guide](#).

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

To add a user from corporate directory:

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

1. On the BlackBerry UEM Console, go to Users, click Add user.

Example:

![Add user interface](image)

2. On the Add a user window, On the Company directory tab, start typing the name of the user you want to add. When the name is displayed, select it from the drop-down list.

Example:

![Add a user interface](image)

3. The required (*) user information such as Display Name, Username, and Email address will be filled in from the company directory entry.

Example:
4. Scroll down to the bottom on the pop-up window and set the **Device activation** settings as required for your company.

Example:

5. Click **Save**.
Adding a local User

To add a local user:

1. On the BlackBerry UEM Console, go to Users, click Add user.

Example:

2. On the Add a user window, On the Local tab, configure these settings:
   a. In the First name field – Enter the user’s first name.
   b. In the Last name field – Enter the user’s last name.
   c. In the Display name field - Enter a display name.
   d. In the Username field – Enter a username.
   e. In the Email address field – Enter the user’s email address.
   f. In the Console password – Enter a temporary password for this user.
   g. Select Send password to user.

Example:
3. Scroll down to the bottom on the pop-up window and set the **Device activation** settings as required for your company.
   Example:
   ![Device activation settings](image)

4. Click **Save**.

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

### Adding a Device to an Existing User

**To add a device to an existing user:**

1. On the BlackBerry UEM Console, go to **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.

   Example:
4. In the **Activation details** pane, click **Set activation password**.

Example:

5. On the **Set device activation password** window, set the **Device activation** settings as required for your company.

Example:
6. Click Submit.

Creating User Provisioning Groups

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

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

User groups are how BlackBerry UEM applies policies and assigns/deploys apps. For more or updated information about adding user groups see Creating and managing user groups guide.

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

There are 3 pre-defined status groups:
- CHKP_Status_Provisioned
- CHKP_Status_Active
- CHKP_Status_Inactive

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

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

If the device hasn’t checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin), then the device is moved from CHKP_Status_Active to CHKP_Status_Inactive.

There are 4 pre-defined risk groups:
- CHKP_Risk_None
- CHKP_Risk_Low
- CHKP_Risk_Medium
If a device is determined to be at High, Medium, or Low risk, the device is placed in the respective group. If the device has no risks, then it is placed in the CHKP_Risk_None group.

For example, if the device has a Low risk app and a High risk device setting is enabled for example “unknown sources”, then the device will appear in both the CHKP_Risk_Low and CHKP_Risk_High groups.

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

In "Creating Local User Group(s)" on page 23, we will create these pre-defined SandBlast Mobile groups and nest them according to how we want our corporate policies to be applied.

In our example, devices that are members of CHKP_Risk_High, CHKP_Risk_Medium, or CHKP_Status_Inactive will be considered to be "Users_At_Risk", and have the appropriate Mitigation Policies applied as defined later in "Creating a Mitigation Process" on page 57. Devices that are members of CHKP_Risk_None or CHKP_Risk_Low, will not have the mitigation policies applied.

Creating a User Group based on Corporate User Directory

To create a user group that is tied to active directory:

1. On the BlackBerry UEM Console, go to Groups > User, click Add a directory-linked group icon.

   Example:

   ![Add a directory-linked group](image)

2. On the Add a directory-linked group window, configure these settings:
   a. In the Group name field – Enter a group name.
   b. In the Group Description field – Enter the group’s description (optional).

   Example:
3. Click + sign to add a Linked directory group.

4. On the **Search company directory** window, enter in the first few letters of the corporate directory group you want to link, and hit enter.

Example:

5. Click **Add**.

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

Example:
Creating Local User Group(s)

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

- **Optional User Groups**, but recommended in order to simplify applying policies, deploying apps, and mitigating risks. Some of the required user groups will be nested under these groups as discussed further in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 20 and in "Nesting User Groups (Optional)" on page 28.
  - SBM_Syncd_Users
  - Users_At_Risk
- **Required User Group** if not using AD User Group
  - SBM_Local_Users
- **Required User Groups for Integration** if using Tag Device Status and Tag Device Risk
  - CHKP_Status_Provisioned
  - CHKP_Status_Active
  - CHKP_Status_Inactive
  - CHKP_Risk_None
  - CHKP_Risk_Low
  - CHKP_Risk_Medium
  - CHKP_Risk_High

To add a user group:

1. On the BlackBerry UEM Console, go to **Groups > User**, click **Add a user group** icon.

   Example:
2. On the **Add a user group** window, configure these settings:
   a. In the **Group name** field – Enter a group name.
   b. In the **Group Description** field – Enter the group’s description (optional).

   Example:

   ![Add a user group](image)

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

4. Click **Add**.

   **Note** – Repeat these steps to add all the user groups listed above.
Adding an Existing User to the Local User Group

To add an existing user to the User Group we created in "Creating a User Group based on Corporate User Directory" on page 21 or "Creating Local User Group(s)" on page 23, follow this procedure. Our example will be using the Local User group ("SBM_Local_Users").

To add an existing user to the local user group:

1. On the BlackBerry UEM Console, go to Users > Managed devices, scroll and select the user you want to add to the user group, and click the Add to user groups icon.

Example:

2. On the Add to user groups window, select the SBM_Local_Users from the Available groups list, and click Right arrow.

Example:

3. Click Save.

Example:
4. The user is now part of the User Group **SBM_Local_Users**.

### Adding a New User to an Existing Local User Group

To add a new user to an existing local user group:

1. On the BlackBerry UEM Console, go to **Users**, click **Add user**.

   Example:

2. On the **Add a user** window, On the **Local** tab, configure these settings:
   
   a. In the **First name** field – Enter the user’s first name.
   b. In the **Last name** field – Enter the user’s last name.
   c. In the **Display name** field - Enter a display name.
   d. In the **Username** field – Enter a username.
   e. In the **Email address** field – Enter the user’s email address.

3. Select the User Group **SBM_Local_Users** from the **Available groups** list and click **Right arrow**.

   Example:
4. Scroll down to the bottom on the pop-up window, and enter in a temporary console password for this user and select **Send Password to user**.

5. Set the **Device activation** settings as required for your company.
   Example:
   ```
   [Diagram showing device activation settings]
   ```
   
   6. Click **Save**.

   **Note** - The user is already notified with device enrollment procedures upon the creation of the user.
Nesting User Groups (optional)

We will be nesting the user groups that we created in "Creating Local User Group(s)" on page 23 and as discussed in "Information about Device Risk & Status tags and BlackBerry UEM user groups" on page 20.

This will simplify the policy enforcement.

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

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

- **SBM_Syncd_Users**
  - CHKPI_Status_Provisioned
  - CHKPI_Status_Active
  - CHKPI_Status_Inactive

- **Users_At_Risk**
  - CHKPI_Risk_High
  - CHKPI_Risk_Medium
  - CHKPI_Status_Inactive

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

For more or updated information about nested groups see [Add nested groups to a user group guide](#).

To add a nested group:

1. On the BlackBerry UEM Console, go to **Groups > User**, and select **Users_At_Risk** to edit it.

2. Select **Nested groups** tab, and click +.

Example:

3. On the Add a nested group window, select CHKPI_Status_Inactive, CHKPI_Risk_Medium, and CHKPI_Risk_High.

Example:
4. Click **Add**.

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

For iOS device, see Activating iOS devices for more details. For Android device, see Activating Android devices for more details.

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

From Our Examples:

- **Server URL** = https://<FQDN of BlackBerry UEM Server>:<port to Web Services API> (ie. https://uem.acme.us:18084)
- **SandBlast Mobile API Admin Username/Password** = sbm_admin/<hidden>
- **User Provisioning Group(s)** = SBM_Local_Users; SBM_AD_Users
Configuring the 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" on page 78).

**Prerequisites**

You need the following details from your BlackBerry UEM Deployment:

- **Server**: The root URL to your BlackBerry UEM Web Services API including the leading https://, such as `https://uem.acme.us:18084`.

- **SRP ID**: This is the SRP ID from BlackBerry licensing registered to your instance, in the form of S12345678. This value can be found by going to BlackBerry UEM Console > Help > About BlackBerry UEM.

- **BlackBerry UEM SandBlast Mobile Administrator Username and Password**: These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the UEM. You may have created a special API Admin account, see "Creating API Account for Integration with the SandBlast Mobile" on page 10.

- **Groups(s)**: These are the BlackBerry UEM user provisioning groups to which the users/devices to be registered to SandBlast Mobile are grouped, and will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each group name separated with a semicolon (;). These are the User Provisioning Groups we created in "Creating User Provisioning Groups" on page 18 ("SBM_Local_Users; SBM_AD_Users").

- **Mitigation Group**: This field will not be used as we will be using the CHKP Risk and Status tags.

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

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

Procedure:

1. Access your SandBlast Mobile Dashboard via the Infinity Portal.
2. Go to Settings > Integration, Click “+” to create a new integration setting.
   The Integration Wizard opens.
   Example:

   1. Configure the settings for your – Blackberry UEM Deployment.
      • Server Setup

        Configure your UEM to integrate with the created BlackBerry UEM devices:

        a. In Server Setup section, enter this information:
           • UEM service - BlackBerry UEM
           • Display Name – UEM Default
           • Server Address - The full URL needed for the UEM service
           • User name
           • Password
           • SRF ID
           • Connector Setup (advanced)

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

**Connector Setup**

You can configure SandBlast Connector when the UEM in 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 User Groups the API user from previous step has access to.

  Example:
a. In the **Group(s)** field:
   i. Click **Group(s)**.

   A dropdown with list of the available groups opens.
   
   ii. Select the group(s) you need for integration with BlackBerry UEM.

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

   Select the groups for two deployed applications as part of the BlackBerry UEM Android Enterprise deployment. See "Using Android Enterprise with SandBlast Mobile" on page 65

   **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:

   ![BlackBerry UEM 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>
d. Click **Next**.

### Tagging Configuration

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

**Example:**

![Tagging Configuration Diagram]

a. In **Tagging** Section:
   1. Set **Tag device status** to **ON**.

For integration with BlackBerry UEM, the Device Status tags are interpreted as "user groups" of "CHKP_Status_Provisioned", "CHKP_Status_Active", or "CHKP_Status_Inactive" which will have an either "0" or "1" when set. We will use the CHKP_Status user groups to determine when to prompt the user to install the SandBlast Mobile Protect app on their device. If none of CHKP_Status user groups haven’t been set yet for a device, then the device has not been synced with SandBlast Mobile Dashboard.
ii. Set **Tag device risk** to **ON**.
   For integration with BlackBerry UEM, the Device Risk tags are interpreted as "user groups" of "CHKP_Risk_None", "CHKP_Risk_Low", "CHKP_Risk_Medium", and "CHKP_Risk_High" with the values of "0" or "1". We will use the CHKP_Risk user groups to determine when to enact certain policies or actions on the device. As an example, if CHKP_Risk_High is set to "1", then the device will be sent an in-app notification and blocked from running corporate apps or connecting to corporate assets.

b. In **Advanced** section:
   The free-form Mitigation group is any unique name, such as "SBM_HighRisk", that SandBlast Mobile will place only devices determined to be at High Risk. Note: This mitigation group must be created as a "user group" in BlackBerry UEM prior to using. Please note that the Mitigation group does not provided the granularity of the different risk levels of the device, just high risk. This method was the original way to group devices at high risk, and it is strongly recommended that you implement the CHKP_Risk and CHKP_Status user groups instead of using the free-form Mitigation group.

c. Click **Finish**.

- **Deployment**

Specify the deployment status of a device.

   **Note** - This section is optional, because Blackberry UEM manages the deployment automatically.

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

In this screen you will see the **Use token in application configuration settings**. Save this token for later as you will use it to manage the application in section "Adding the SandBlast Mobile Protect app to your App Catalog" on page 43.

In the **Advanced** section:

a. Enable options to send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app.

b. Click **Finish**.

Example:
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.
Example:

<table>
<thead>
<tr>
<th>BLACKBERRY UEM INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UEM Server</strong></td>
</tr>
<tr>
<td>Server status</td>
</tr>
<tr>
<td>UEM service: Blackberry UEM</td>
</tr>
<tr>
<td>Display Name: Blackberry UEM Default</td>
</tr>
<tr>
<td>Server: [URL]</td>
</tr>
<tr>
<td>User name: Nobody of UEM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device sync status</strong></td>
</tr>
<tr>
<td>(1 Groups) Jan 07 2021, 19:00</td>
</tr>
<tr>
<td>SBM_Local_Users</td>
</tr>
<tr>
<td><strong>App sync status</strong></td>
</tr>
<tr>
<td>Jan 07 2021, 19:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tagging status</strong></td>
</tr>
<tr>
<td>Device tags: Status, Risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment status</strong></td>
</tr>
<tr>
<td>Platforms: Deployment is managed by UEM console</td>
</tr>
</tbody>
</table>

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

Prerequisites

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

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 43.
2. Prompt the SandBlast Mobile Protect app installation on your devices. See "Automatic Activation of SandBlast Mobile: Prompt the Protect app installation" on page 50.
3. Connect the app to your devices. See "Connecting the SandBlast Mobile Protect app to your Device" on page 52.
Adding the SandBlast Mobile Protect app to your App Catalog

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

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

**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.

**Adding iOS Application to the Catalog**

1. On the BlackBerry UEM console, go to Apps > Apps, and click the icon.

2. Select App Store.
3. In the **App name** field, enter **SandBlast Mobile Protect** and select the appropriate store for your country.
4. Click **Search**.
   The search result window shows the SandBlast Mobile Protect app.
5. Click **Add**.

Example:

An App Configuration window shows the SandBlast Mobile Protect app.

6. In the **Category** drop-down, select **Business**.
7. Check **Remove the app from the device when the device is removed from BlackBerry UEM**.
8. In the **Default installation for required apps** drop-down, select **Prompt once**.
9. Scroll down to button of the screen

Example:
10. In the **App Configuration** table, click +.
11. Select **Configure manually**.

Example:

12. In the **App Configuration name** field, enter **Sandblast Mobile Protect**.
13. In the table, click + and select **String** thrice.
14. Add the following Key/Value pairs:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lacoon Server Address</td>
<td>String</td>
<td>gw.locsec.net</td>
</tr>
</tbody>
</table>
Check Point SandBlast Mobile: UEM Integration Guide | BlackBerry UEM

<table>
<thead>
<tr>
<th>Key</th>
<th>Value Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Serial Number</td>
<td>String</td>
<td>%SerialNumber%</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>hash_tenant_id**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(The SHA-256 value of the Dashboard Management ID. You must use the token configured in the Deployment section. For more information see &quot;Configuring the Check Point SandBlast Mobile Dashboard Integration Settings&quot; on page 31)</td>
</tr>
</tbody>
</table>

Example:

15. Click **Save**.
16. Click **Add** to finish adding the app to the app catalog.

**Adding Android Application to the Catalog**

1. On the BlackBerry UEM console, go to **Apps > Apps**, and click the **App** icon.
2. Select **Google Play**.

3. Click **Open Google Play** and search **SandBlast Mobile Protect**. You can then copy and paste information from Google Play in the following steps and also download icons and screen shots.

Example:

```plaintext
a. In the **App name** field, type the app name, "SandBlast Mobile Protect".
```
b. In the **App description** field, type a description for the app.

c. In the **Vendor** field, type the name of the app vendor, "Check Point Software Technologies, Ltd."

d. In the **App icon** field, click Browse. Locate and select an icon for the app.

e. In the **App web address from Google Play** field, type the web address of the app in Google Play. Example:

![Image of app configuration](image)

4. Under App configuration, Click **Add**.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI</td>
<td>String</td>
<td>%DeviceIMEI%</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>hash_tenant_id**</td>
</tr>
<tr>
<td>(Add this key if you use SandBlast Mobile to manage the deployment)</td>
<td></td>
<td>(The SHA-256 value of the Dashboard Management ID. You must use the token configured in the Deployment section. For more information see &quot;Configuring the Check Point SandBlast Mobile Dashboard Integration Settings&quot; on page 31)</td>
</tr>
</tbody>
</table>
5. Click **Save**.
Automatic Activation of SandBlast Mobile: Prompt the Protect app installation

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

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

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

Creating a Protect app Group

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

Procedure:

1. On BlackBerry UEM Console go to Apps > App Groups and click the icon.

2. In the Add app group window, configure these settings:
   a. In the App group Name field, enter the name of the app group (we recommend "SandBlast Mobile Protect").
   b. In the Assigned apps section, Click +.
   c. Enter Sandblast in the Search box and select Android and iOS versions of the Sandblast Mobile Protect app.
   d. Set the App Configuration for each app:
      - For iOS: SBM_iOS_Config
For Android: SBM_app_Config

1. Click **Add**.

- **Note** – The best practice is to create an app group and to apply the app configuration directly to it, 0.

### Connecting the SandBlast Mobile Protect app to your Device

To install the SandBlast Mobile Protect app on your devices in your organization, you must first configure them to require the SandBlast Mobile Protect app. For that, we need to link the Sandblast Mobile App in our catalog to the User Provisioning Groups we created in "Creating User Provisioning Groups" on page 18.
Optional: Create a mitigation process. See "Creating a Mitigation Process (Optional)" on page 58.

General Workflow:

1. Assign the App Groups to the User Provisioning Group.
2. Create a compliance policy to uninstall / remove corporate apps from the device until the user installs the required apps on the device.
3. Create a Mitigation Process for devices-at-risk through the User Provisioning Group Risk.

Assign App to User Provisioning Group

1. On the BlackBerry UEM console, go to Group > User.
2. Search for the Provisioning Group SBM_Syncd_Users and click it.
3. Click Settings tab.
4. In Assigned apps section, click +.
5. In the Assign apps window, select the App Group we created in “Creating a Protect app Group” on page 50.
6. Click Next.
5. In Disposition drop-down, select Required.
6. Click **Assign**.

![Assign apps screenshot]

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

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

### Creating a Compliance Policy for the Organization Devices

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

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

To **create a Compliance Policy**:

1. Go to **Policies and profiles > Managed devices > Compliance > Compliance**, and click +.

   Example:
2. On the **Add a compliance profile** window, configure these settings:
   a. In the **Name** field, enter a name for the policy, such as **Missing Required Apps**.
   b. In the **Description** field, enter a description.
   c. Select the **iOS** tab.
   d. Select **Required app is not installed** and set appropriate actions to be taken if the user doesn’t install the app.

   **Example:**

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

   **Example:**
Applying a Compliance Policy to User Provisioning Group

After creating a Compliance Policy, we need to assign it to User Provisioning Group.

1. Go to **Group > User**.
2. Search for the Provisioning Group **SBM_AD_Users** we created in "Creating User Provisioning Groups" on page 18 and Click it.
3. Click **Settings** tab.
4. In **Assigned profile**, Click +.
5. Select **Compliance** from pop-up list.
6. On the **Assign a Compliance profile** window, select the **Compliance Policy** we created in the previous section **Missing Required Apps**.

7. Click **Assign**.

Example:

![Assign a Compliance profile](image)

**Note** - Repeat these steps for "SBM_Local_Users", if you are using it.

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

**Note** - Any device that belongs to the User Provisioning Group(s) which require the SandBlast Mobile Protect apps to be installed ("SBM_Syncd_Users" and "Users_At_Risk") that hasn’t installed the SandBlast Mobile Protect app will be out of compliance.

Example:

2. Clicking on the “Non-compliant” pie piece, opens a reporting window.

3. Device Details View indicates an “Out of Compliance” issue.

4. The user will receive an alert email as well as an in-app notification.
Creating a Mitigation Process (optional)

To let the Blackberry UEM 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 to label any device with the risk level that the SandBlast Mobile analysis determines.

Creating IT Policies

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

Note - We will show an example policy, but these enforcement policies are something that the customer should create for their environment and needs. In a production environment, the customer should configure the compliance and IT policies according to their internal security policy.

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

To add an IT policy:
1. On the BlackBerry UEM console, go to Policies and profiles > Managed devices > Policy > IT policies and click +.
2. On the Add an IT Policy screen:
   a. In the Name field – enter a name for the policy. (We recommend “High Risk Device Policy”)
   b. For iOS:
      i. Select the iOS tab.
      ii. Under Device functionality, unselect Allow use of camera.
   c. For Android:
      i. Select the Android tab.
      ii. Under Global (all Android devices) > Device functionality, select Disable camera.
iii. Scroll to KNOX MDM > Device functionality, unselect Allow camera.

iv. Scroll to KNOX Premium – Workspace > Device functionality unselect Allow camera.

d. Scroll to the bottom of the screen and click Add.
Applying the Policy to the User Provisioning Group

Now that we have created the policy ("High Risk Device Policy") we want to enforce, we need to link this policy to our User Provisioning Group ("Users_At_Risk") we created in "Creating Local User Group(s)" on page 23.

To assign an IT policy to group:

1. On the BlackBerry UEM console, go to Groups > User, find the user mitigation group you created in "Creating Local User Group(s)" on page 23, in our example “Users_At_Risk”, and click group name link.
2. On the group detailed view, select the Settings tab.
3. On the Settings tab, Click + on the Assigned Profiles section.
4. Select IT policy.
5. On the Assign an IT policy window, select the IT policy we created in “Creating IT Polices” on page 59, in our example “High Risk Device Policy”.
6. Click Assign.

Note - Now any device placed into the user groups, CHKP_Risk_High, CHKP_Risk_Medium or CHKP_Status_Inactive, which are nested under Users_At_Risk will have the policy actions in the IT Policy ("High Risk Device Policy") acted upon it.
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**
  Zero-Touch Deployment for Android Enterprise devices is not available yet.

- **Zero Touch Deployment in iOS devices**
     Give it a name and choose Certification authority connection > Manually uploaded certificates > Add.

  2. Create a new VPN Profile. Go to Policies and Profiles > Networks and Connections > VPN > Add new.
- **Name**: Check Point Local Tunnel
- Chose only iOS.
- **Connection Type**: Custom
- **VPN bundle ID**: com.checkpoint.capsuleprotect
- **Server**: www.checkpoint.com
- **Authentication Type**: User Credentials
- **Associated user credential profile**: the profile we created in the previous section.
- Enabled VPN on demand.

**On demand rules:**

```
<array>
  <dict>
    <key>Action</key>
    <string>Connect</string>
    <key>InterfaceTypeMatch</key>
    <string>WiFi</string>
  </dict>
  <dict>
    <key>Action</key>
    <string>Connect</string>
    <key>InterfaceTypeMatch</key>
    <string>Cellular</string>
  </dict>
  <dict>
    <key>zero_touch</key>
    <string>true</string>
  </dict>
</array>
```

3. Assign the credentials profile and the VPN configuration to your devices group. Go to Groups > User > your_group
   Select both profiles we created in the previous sections by clicking the (+) button.

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 BlackBerry UEM AE 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" on page 66.

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 > Integrations.
2. Enable the SandBlast Mobile Protect app (for both profiles).
   - For a new UEM configuration: follow instructions in "Configuring UEM Integration on SandBlast Mobile Dashboard" page 32
   - For existing UEM configurations:
     a. Go to Settings > Integrations > Edit synchronization Settings
     b. In the Android Enterprise Deployment section select and add the device groups for both profiles.

Example:

<table>
<thead>
<tr>
<th>Android Enterprise Deployment</th>
<th>Work &amp; Personal deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select groups...</td>
</tr>
</tbody>
</table>
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 SandBlast Mobile Protect 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.

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

### Policies

**To change policy for inactive personal profile:**

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

   Example:

   ![Policy Settings](example.png)

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

   Example:

   ![Select Policy](example2.png)

   **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" on page 68).

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 group tags, see "Connecting the SandBlast Mobile Protect app to your Device" on page 52.
Applying the SandBlast Mobile Protect app on Devices

The following section describes the user experience of device install and registration process with SandBlast Mobile. After following all the configurations in previous chapters the registration process of the SandBlast Mobile Protect app with the SandBlast Mobile Dashboard is automatic using the UEM deployment.

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.

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.

Deploying the SandBlast Mobile Protect app on the iOS Devices

With the deployment settings for SandBlast Mobile Protect app for iOS configured in section Configuring BlackBerry UEM Integration Settings on the SandBlast Mobile, the App is automatically deployed to the devices that belong to the defined groups (see “Configuring UEM to Deploy the SandBlast Mobile Protect app” on page 42).

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

After you register your device in the BlackBerry UEM and attach it to the User Provisioning Group (“SBM_Syncd_Users”), 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 the iOS Device.
     b. Launch the Protect app to finish the registration.
        BlackBerry UEM 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:
Deploying the SandBlast Mobile Protect app on Android Devices

- **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.
d. Follow the on-screen instructions to enable Notifications, Location, and Network Security. Example:

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

Example:

iOS Devices

Android Devices

The registration server and the key are automatically configured in the App by the BlackBerry UEM system. See "Configuring UEM to Deploy the SandBlast Mobile Protect app" on page 42.
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 BlackBerry UEM system for that device. BlackBerry UEM 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 marks the device as High Risk (CHKP_Risk_High) to the BlackBerry UEM system. The BlackBerry UEM system then enforces policy actions specified in the IT policy.

Blacklisting a Test App

1. Log into the SandBlast Mobile Dashboard.
2. Go to App Risk tab.
3. Select the app you wish to blacklist on the left-side list.
4. On the Policy section, click the Edit link.
   Example:

5. On the Changing Application Policy – Global window, configure these settings:
   a. From the New Policy drop-down menu - select Black Listed.
   b. 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 User Provisioning Groups that you created for the Devices At Risk. See “Connecting the SandBlast Mobile Protect app to your Device” on page 52.

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

1. On the BlackBerry UEM console, go to **Group > User > Users** and open your defined Group for mobile devices (“Users_At_Risk”).

   The device is displayed.

   **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 (optional)” on page 58.

**SandBlast Mobile Protect app Notifications**

The user receives SandBlast Mobile Protect app notifications.

Example:

**BlackBerry UEM Agent App Notifications**

1. The user will not be able to use the device’s camera, as specified in the compliance actions (policy) we created in “Creating IT Policies” on page 59, in our example “High Risk Device Policy” until the user removes the blacklisted app.

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

Example:
Administrator View on the SandBlast Mobile Dashboard

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

1. On the SandBlast Mobile Dashboard, go to **Forensics**

   A list of the Devices at Risk is displayed in the **Device Risk** section.

2. 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 BlackBerry UEM Console

On the BlackBerry UEM Console:

1. Go to **Groups > User > Users** view.

   You can see the device is now a member of the "CHKP_Risk_High" group and indirectly a member of the "Users_At_Risk" group, and that the IT policy "High Risk Device Policy" has been assigned.

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 SRP ID</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>
</tbody>
</table>
| Tag Device Status (Boolean tags) become user groups in UEM | CHKP_Status_Provisioned  
CHKP_Status_Active  
CHKP_Status_Inactive |
| Tag Device Risk (Boolean tags) become user groups in UEM | CHKP_Risk_None  
CHKP_Risk_Low  
CHKP_Risk_Medium  
CHKP_Risk_High |
| SandBlast Mobile Gateway                 | gw.locsec.net                                  |
| SandBlast Mobile App Name (iOS / Android) | SandBlast Mobile Protect                       |
| SandBlast Mobile App ID (iOS)             | com.checkpoint.capsuleprotect                  |
| SandBlast Mobile App ID (Android)        | com.lacoon.security.fox                       |