Check Point SandBlast Mobile

SandBlast Mobile Connector
Installation Guide
# Table of Contents

**About this Guide** ........................................................................................................................................... 4  
  Solution Architecture ....................................................................................................................................... 4  
**Prerequisites** .................................................................................................................................................. 6  
**Step-by-Step Guide** ........................................................................................................................................ 7  
  Install Gaia ..................................................................................................................................................... 7  
  Install and Configure SandBlast Mobile Connector ...................................................................................... 8  
  Configure SandBlast Mobile dashboard. ......................................................................................................... 13  
**Advance Settings** .......................................................................................................................................... 16  
  Migrating from User and Device Management (UDM) .................................................................................. 16  
  Working with a Proxy ........................................................................................................................................ 16  
  Unified Endpoint Management (UEM) with a Self-Signed Certificate ....................................................... 17  
  High Availability .............................................................................................................................................. 18  
**Related Articles** .......................................................................................................................................... 19  
  BlackBerry UEM Integration Guide ................................................................................................................ 19  
  Citrix XenMobile Integration Guide .............................................................................................................. 19  
  MobileIron Cloud Integration Guide ............................................................................................................ 19  
  Airwatch Integration Guide ............................................................................................................................. 19
About this Guide

SandBlast Mobile Connector is a web-based application residing within the organization’s data center that provides a management integration interface between your SandBlast Mobile Dashboard and your on-prem Unified Endpoint Management (UEM) solution. SandBlast Mobile Connector keeps all user Personally Identifiable Information (PII) within your organization’s environment, by populating the SandBlast Mobile Dashboard with encrypted hash values instead of plain text for the device/user name, user’s email address, and device phone number.

This guide takes you step-by-step through the installation of SandBlast Mobile Connector as well as providing configuration instructions for a variety deployment scenarios.

Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>SandBlast Mobile Protect app</strong></td>
</tr>
<tr>
<td></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.</td>
</tr>
<tr>
<td></td>
<td>• To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.</td>
</tr>
<tr>
<td></td>
<td>• 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></td>
<td>• No Personal Information¹ is processed by or stored in the App.</td>
</tr>
<tr>
<td>2</td>
<td><strong>SandBlast Mobile Connector</strong></td>
</tr>
<tr>
<td></td>
<td>• SandBlast Mobile Connector is a web-based application residing within the organization’s data center that provides a management integration interface between your SandBlast Mobile Dashboard and your on-prem Unified Endpoint Management (UEM) solution.</td>
</tr>
<tr>
<td>3</td>
<td><strong>UEM</strong></td>
</tr>
<tr>
<td></td>
<td>• Unified Endpoint Management</td>
</tr>
<tr>
<td></td>
<td>• Device Management and Policy Enforcement System (generalized term replacing MDM/EMM)</td>
</tr>
</tbody>
</table>

¹ Personal Information is any information that can individually identify a person. Anonymous information connected or linked with any Personal Information shall be deemed as Personal Information so long as such a connection or linkage exists. Within the Solution, the user’s name, address, email address, and phone number, and linkage by way of unique identifier (Check Point device_id) to an IP address, unique device identifier (UDID/IMEI), etc. are considered to be Personal Information. See Section Error! Reference source not found. for additional details.
| 4 | SandBlast Mobile Gateway | - The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.  
- The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (“organization’s”) Dashboard instance.  
- No Personal Information\(^1\) is processed by or stored in the Gateway. |
| 5 | Management Dashboard | - The cloud-based web-GUI Check Point 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.  
- Personal Information\(^1\), such as a user’s name, email address, and phone number, is processed by and may be stored in the Dashboard. |
| 6 | Behavioral Risk Engine | - The cloud-based Check Point SandBlast Mobile Behavioral Risk Engine uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis.  
- The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.  
- The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.  
- No Personal Information\(^1\) is processed by or stored in the Engine. |
| 7 | ThreatCloud | - ThreatCloud powers the Anti-Phishing, Safe Browsing, and URL Filtering technologies for SandBlast Mobile. |
### Prerequisites

**For the SandBlast Mobile Connector Installation, prepare these in advance:**

1. Download the Check Point R80.10 (VM installation):  
   The Gaia Operating System is based on Linux Redhat 7 64-bit.

2. Download the SandBlast Mobile Connector installation file.  

3. Create a new Virtual Machine (VM) with these specifications:
   - Cores: 4
   - Memory: 4GB
   - Disk Space: 200GB

4. Required IPs and ports for SandBlast Mobile Connector:

<table>
<thead>
<tr>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>SandBlast dashboard URL*</td>
<td>443</td>
<td>US</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.87.59.245</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>SandBlast dashboard URL*</td>
<td>443</td>
<td>EU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.17.79.161</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>SandBlast dashboard URL*</td>
<td>443</td>
<td>AU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13.237.221.74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>Run nslookup to:</td>
<td>443</td>
<td>US</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-relay.locsec.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.87.59.245</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>Run nslookup to:</td>
<td>443</td>
<td>EU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eu-relay.locsec.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to SandBlast Mobile</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>Run nslookup to:</td>
<td>443</td>
<td>AU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>au-relay.locsec.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection to Customer UEM</td>
<td>Customer SandBlast Mobile Connector server</td>
<td>Customer UEM</td>
<td>443</td>
<td>ANY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BlackBerry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UEM only:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>18084</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step-by-Step Guide

Install Gaia

1. Install an R80.10 Virtual Machine (VM) with the instructions in these guides:
   a. Installing the Gaia Operating System on Open Servers
   b. Running the Gaia First Time Configuration Wizard

2. Change the admin user to use `bash`.
   a. Log in to Gaia with your initial credentials.
   b. On the left tool bar under User Management, click Users.
   c. Select your admin user and click Edit.
d. Change the Shell to /bin/bash

![Image of Shell Change](image.png)

e. Click Ok.

**Install and Configure SandBlast Mobile Connector**

1. Install SandBlast Mobile Connector package.

   a. Log in to Gaia with your initial credentials.

   ![Image of Gaia Login](image.png)

   b. On the left tool bar, under **Upgrade (CPUSE)** click **Status and Actions**.

   ![Image of Status and Actions](image.png)
c. Click **Import Package**.

![Import Package dialog box](image)

d. Browse for the SandBlast Mobile Connector package you downloaded earlier and click **Import**.

![Import Package dialog box](image)

e. Wait for the upload and import to finish.

![Import Package dialog box](image)
f. When the import is successful, look for a pop up message in the left bottom corner of the screen with the success message.

![Success Message](image1.png)

---

g. To see the imported package, select **All** under **Showing Recommended Packages**.

![Recommended Packages](image2.png)

---

h. Search for the imported SandBlast Mobile Connector package under **Minor Versions (HFAs)**.

The status should be **Downloaded Successfully**.

![Downloaded Successfully](image3.png)
i. Right click on the package to select **Install Update**.

j. When the installation finishes, the package shows as **Installed** and a pop up message says “Package installed successfully.”
k. Restart the VM with a click on **Shut Down** on the left bar and a click on **Reboot**.

2. Configure SandBlast Mobile Connector.

   a. Connect to the Virtual Machine (VM) with `ssh` and your initial credentials to expert mode.

   b. Create private and public keys.
      
         i. Run this command in expert mode:

            ```
            sbmc_create_keys
            ```

            The output looks like this:

            ```
            Started creating the SandBlast Connector keys
            '.'
            '.'
            SandBlast Connector keys creation finished successfully
            ```

         ii. Copy and save the public key to use in the dashboard configuration.

            ```
            cat /web/conf/sbmc_public_key.pub
            ```

3. Update the following settings:

   ```
   vi /opt/CPsbmc/components/api_dispatcher/application.yml
   ```

   Update this field:

   ```
   relay > task_info_key
   ```

   The URL of the SandBlast Mobile dashboard without https.

   ```
   task_info_key: “my.dashboard.locsec.net”
   ```

   Also update this field:
relay > url
The URL of Relay according to the region.

Example:
url: “https://us-relay.locsec.net”

4. Update the following settings:

```
vi /opt/CPsbmc/components/pii_protector/application.yml
```

Update these fields:

```
zuul routes proxy url - The url.
The URL of the SandBlast Mobile dashboard with https.
```

Example:
url: https://my.dashboard.locsec.net/

**Configure SandBlast Mobile dashboard.**

1. Configure the Privacy and Device Management settings in the SandBlast Mobile Dashboard
   a. Connect to the SandBlast Mobile dashboard.
   b. Go to the tab for **Settings > Device Management**.

Choose the **UEM type** in the **MDM service** drop down list.

![Device Management Settings](image-url)
c. Configure the UEM details.

Switch the **SandBlast Mobile Connector** to **On** and click **Configure**. For example in the BlackBerry UEM configuration:
d. Insert the created public key into the public key field.

Configure the SandBlast Mobile Connector Virtual Machine address in Server Address (and in High Availability Server address, if needed).

e. Press Ok in pop up window.

f. Click Verify and Save.

2. Verify SandBlast Mobile Connector integration.

   a. Verify UEM device sync.

   b. Verify devices do not show as encrypted when the browser is on the premises.
Advance Settings

Migrating from User and Device Management (UDM)

1. Follow the SandBlast Mobile Connector installation guide until the “Configure SandBlast Mobile dashboard” section.

2. Copy these files from the User and Device Management (UDM) server:

   /opt/CPudm-R77/conf/pii_encryption.iv
   /opt/CPudm-R77/conf/pii_encryption.key
   /opt/CPudm-R77/conf/pii_encryption_predefined.iv
   /opt/CPudm-R77/conf/pii_encryption_predefined.key

3. Copy the files to the SandBlast Mobile Connector:

   /opt/CPsbmc/components/pii_filter/conf/

4. Restart the SandBlast Mobile Connector:

   sbmc_stop
   sbmc_start

5. Continue with the SandBlast Mobile Connector installation guide.

Working with a Proxy

When a proxy must connect from the SandBlast Mobile Connector to the internet or to the Unified Endpoint Management (UEM):

1. Connect to the Virtual Machine (VM) by ssh with your initial credentials.

2. Update the settings to access the SandBlast Mobile dashboard through the proxy.

   a. Open this settings file for an update:

      vi /opt/CPsbmc/components/pii_protector/application.yml

   b. Update the relevant settings in the file (server > Proxy), for example:

      proxy:
      enabled: true
      host: “myproxy.mydomain.com”
      port: 8080
      authentication-required: true
      user: “proxy_user”
      password: “proxy_password”
3. Update settings for accessing SandBlast Mobile Connector cloud component through the proxy.

   a. Open this settings file to update:

```
vi /opt/CPsbmc/components/api_dispatcher/application.yml
```

   b. Update the relevant settings in the file:

   i. relay Proxy

   Example:

```
proxy:
  enable: true
  host: "myproxy.mydomain.com"
  port: 8080
  username: "proxy_user"
  password: "proxy_password"
```

   ii. MDM Proxy

   If there is a proxy to connect to the UEM. Example:

```
proxy:
  enable: true
  host: "myproxy.mydomain.com"
  port: 8080
  username: "proxy_user"
  password: "proxy_password"
```

---

**Unified Endpoint Management (UEM) with a Self-Signed Certificate**

Using an option when the UEM server has a self-signed certificate (not signed with a valid Certificate Authority):

1. Download the UEM certificate in a Privacy Enhanced Mail (PEM) format and copy it to the SandBlast Mobile Connector server.

2. Connect to the Virtual Machine (VM) by `ssh` with your initial credentials.

3. Update the settings file to use the self-signed certificate:

   a. Open the settings file to update.

```
vi /opt/CPsbmc/components/api_dispatcher/application.yml
```
b. Use self-signed certificate when connecting to the UEM.
   \texttt{mdm > ssl > use\_self\_sign\_certificate}

   Path to the UEM certificate.
   \texttt{mdm > ssl > certificate\_path}

   Example:
   \texttt{use\_self\_sign\_certificate: true}
   \texttt{certificate\_path: "/web/conf/my\_uem\_certificate.pem"}

   \textbf{Note} – There is an option to disable the SSL verification to the MSD
   \textbf{Use this option in Proof of Concept (POC) only and not in production.}

\section*{High Availability}

Creating a second SandBlast Mobile connector:

1. Duplicate the first working Virtual Machine (VM) with a SandBlast Mobile Connector.

2. Change the VM IP address (in Gaia).

   \textbf{In clish}:
   \begin{verbatim}
   show interface eth0
   set interface eth0 ipv4-address <ip> mask length <16/23>
   save config
   \end{verbatim}

3. Add the new IP to the Unified Endpoint Management (UEM) settings in the SandBlast Mobile dashboard.
Related Articles

BlackBerry UEM Integration Guide
http://downloads.checkpoint.com/dc/download.htm?ID=75248

Citrix XenMobile Integration Guide
http://downloads.checkpoint.com/dc/download.htm?ID=60203

MobileIron Cloud Integration Guide
http://downloads.checkpoint.com/dc/download.htm?ID=75249

Airwatch Integration Guide
http://downloads.checkpoint.com/dc/download.htm?ID=56770