Check Point SandBlast Mobile

Quick Start Guide
About This Guide

Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, in SMS messages, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Check Point SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

- Perform advanced app analysis to detect known and unknown threats
- Monitor network activity for suspicious or malicious behavior
- Monitor SMS messages received for malicious URLs
- Assess device-level (OS) vulnerabilities to reduce the attack surface

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

The Check Point SandBlast Mobile solution ("the Solution") includes the following components:

- Check Point SandBlast Mobile Behavioral Risk Engine ("the Engine")
- Check Point SandBlast Mobile Gateway ("the Gateway")
- Check Point SandBlast Mobile Management Dashboard ("the Dashboard")
- SandBlast Mobile Protect app ("the App") for iOS and Android

This guide describes how to quickly provision and deploy SandBlast Mobile to devices.

Note: If you use an MDM, such as AirWatch or IBM MaaS360, please use the Integration Guide appropriate for your MDM. This guide is for standalone deployment scenarios.

Contents

1 SOLUTION ARCHITECTURE ................................................................. 4
2 PREREQUISITES .................................................................................. 4
3 ACTIVATING ADMINISTRATOR ACCOUNT ............................................ 5
4 LOG INTO SANDBLAST MOBILE DASHBOARD .................................... 6
5 SANDBLAST MOBILE DASHBOARD OVERVIEW .................................... 6
6 PROVISIONING AND REGISTERING DEVICES .................................... 9
1 Solution Architecture

1.1 Components

<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.</td>
</tr>
<tr>
<td>2 EMM/MDM (optional)</td>
<td>Enterprise Mobility Management/Mobile Device Management</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. The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (“organization’s”) Dashboard instance.</td>
</tr>
<tr>
<td>4 Dashboard</td>
<td>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.</td>
</tr>
<tr>
<td>5 Behavioral Risk Engine</td>
<td>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.</td>
</tr>
</tbody>
</table>

2 Prerequisites

- SandBlast Mobile Dashboard Administrator Activation Email
- SandBlast Mobile Dashboard Administrator Account Credentials
- URL to your SandBlast Mobile Dashboard
3 Activating Administrator Account

You will receive an email with your new Check Point SandBlast Mobile Dashboard details and a link to activate your Administrator account.

By clicking the link, you will be directed to the User Activation page, where you will need to set your password for the Dashboard.

**Note:** The password must contain at least 8 characters, including one uppercase and one lowercase as well as one of the following special symbols: !@#$%^&*()_+?~{}[]:;<>,.

After you create a password, you will be re-directed to log into the Dashboard.
4 Log into SandBlast Mobile Dashboard
Navigate to the URL of the Dashboard and login with your Administrator credentials.

5 SandBlast Mobile Dashboard Overview
After logging into the Dashboard, you will be presented with the Dashboard view.
5.1 Navigating the Dashboard

The menu bar located on the top of the page will be displayed on all of the dashboard pages and will help you navigate between the various screens.

<table>
<thead>
<tr>
<th>Tabs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>The Dashboard’s main screen will display both statistics and snapshot data based on information supplied by the enrolled devices.</td>
</tr>
<tr>
<td>Events &amp; Alerts</td>
<td>The Events &amp; Alerts tab is designed to supply an audit trail of incidents and actions that occurred on the devices, such as Application installation, Profiles detected on devices, etc.</td>
</tr>
<tr>
<td>Device Risk</td>
<td>The Device risk tab is where all the necessary risk information is presented per device. If you want to access the risk coming from a specific device or view the number of the devices with a specific risk level, this is where you would go.</td>
</tr>
<tr>
<td>iOS Profiles</td>
<td>iOS Profiles are unique to Apple iOS devices. In order assist the mobile device admins, Apple has developed a tool called profiles, which include Network Configuration Profiles, Provisioning Profiles, and Certificates.</td>
</tr>
<tr>
<td>App Analysis</td>
<td>Apps Analysis tab is the main screen for viewing all apps that were installed across the Enterprise. The app analysis provides meta data and security data on the apps in a way that will help the administrators understand the risk level of a specific app.</td>
</tr>
<tr>
<td>Network</td>
<td>The Network tab is where any captive portal or suspicious network connectivity, such as SSL interception or possible network attack. This is a more granular Network view than shown in the Events &amp; Alerts tab.</td>
</tr>
<tr>
<td>Devices</td>
<td>The Devices tab is to view and manage the organization’s devices.</td>
</tr>
<tr>
<td>Settings</td>
<td>The Settings tab is to view and manage dashboard settings.</td>
</tr>
</tbody>
</table>
5.2 **The Dashboard’s Main Screen**

The Dashboard’s main screen will be shown each time you log into the Dashboard. The Dashboard’s main screen will display both statistics and snapshot data based on information supplied by the enrolled devices. Most of the graphical information presented on this screen has clickable items, which will direct you to a query based page adapted to the state when clicked on.

### The Dashboard’s Main Screen includes the following areas:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Menu Bar</strong></td>
<td>Displays the available options and menus. Will be displayed on all of the dashboard pages.</td>
</tr>
</tbody>
</table>
| **Device Risk**          | Displays the number of devices in the organization that are currently at risk in the following ways:  
  - Total number of devices at risk.  
  - Number of devices at High, Medium, and Low risk.  
  - Device risk over time (last 7 days). |
| **Device Status**        | Displays the number of devices registered in the dashboard and displayed in the following ways:  
  - Total number of Devices  
  - Active Devices – devices that have installed and activated the App  
  - Provisioned & User Notified – devices where the user has been notified on where and how to install and activate the App, or that the MDM has added to the System  
  - Inactive – devices that have uninstalled the App, or that the MDM has reported that the App is no longer installed  
  - Devices registered in the last day & in the last week  
  - Percent of devices running current agent version & older agent versions |
| **Security Events over time** | Displays the security events over time for the last hour, day or month, as well as the total number of applications that have been scanned from the devices that are attached to the dashboard. |
6 Provisioning and Registering Devices

This section describes the steps to add a device to the Dashboard and the user experience during the deployment of the SandBlast Mobile Protect app.

6.1. Navigate to Devices.

6.2. Click the “Add new device” button.

6.3. In the “Add New Device” pop-up window, enter in the Name, Groups, Email Address, and Phone Number of the User/Device.

6.4. Click the “ADD” button.

6.5. Repeat the procedure to add another device.
6.1 Registration of an Android Device

6.1.1. You should receive your email registration. This email contains several basic instructions and two important details for registration, the server address and the registration key. This email will also contain a link to download the App and a QR code, in case the email cannot be read on the device.

6.1.2. Tapping the “Download here” link or scanning the QR code will take you to the Google Play Store page for the SandBlast Mobile App.

6.1.3. Tap the “INSTALL” button and then tap “ACCEPT” to start the app installation.

6.1.4. Once the app has loaded, open the application.
6.1.5. The server address and registration key should already be auto-populated. If they are not, enter the Server Address and Registration Key that are contained in the registration email. Tap “Login”.

6.1.6. SandBlast Mobile Protect will perform an initial scan of your device.

6.1.7. Your device is now protected with Check Point SandBlast Mobile.
6.2 **Registration of an iOS Device**

6.2.1. You should receive your email registration. This email contains several basic instructions and two important details for registration, the server address and the registration key. This email will also contain a link to download the App and a QR code, in case the email cannot be read on the device.

1. Go to the following website using the link below:
   Download here
2. Download the SandBlast Mobile Protect application.
3. Launch the Protect app from your device and log in populated:
   - Server Address: gw
   - Registration key: 1356104c
4. Press login.

Automatic registration email sent by Check Point

6.2.2. When prompted, tap Open.
6.2.3. Tap the “Get” button to start the app installing.

6.2.4. Once the app has loaded, open the application, and allow the configuration profile to be installed. Tap “Allow”.

6.2.5. When prompted to install the Check Point Protect Profile, tap “Install” on the top right. This is essential for the App to perform its function.

6.2.6. You will be prompted to install a Mobile Device Management profile from SandBlast Mobile. This is to allow the App to function. Tap “Install” on the top right.

6.2.7. You will be prompted to trust the Profile for Remote Management. Tap “Trust”.
6.2.8. Once the profile, tap “Done” on the top right corner.
6.2.9. Once the process returns to Safari, it will prompt for you to continue to SandBlast Mobile Protect app. Tap “Open”.
6.2.10. Enter the Server Address and Registration Key that is contained in the email, tap the “Login” button.
6.2.11. You will now be prompted to enable Notifications, Location, and SMS Phishing Protection.

6.2.12. Enable as appropriate, but it is strongly recommended that you enable Notifications, Location, and SMS Phishing Protection.
6.2.13. You will now be prompted to enable SMS Phishing Protection.
6.2.14. Follow the instructions to enable SMS Phishing Protection.
6.2.15. Go to Settings > Messages > Unknown & Spam, and turn on SMS filtering for Protect.
6.2.16. SandBlast Mobile Protect will perform an initial scan of your device.

6.2.17. Your device is now protected with Check Point SandBlast Mobile.