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 GETTING STARTED ............................................................................................................................. 6
3 CREATING AND LOGGING IN TO YOUR NEW INFINITY ACCOUNT ................................................. 8
4 NAVIGATING INTO SANDBLAST MOBILE DASHBOARD ............................................................... 11
5 SANDBLAST MOBILE DASHBOARD OVERVIEW ......................................................................... 11
6 PROVISIONING AND REGISTERING DEVICES ............................................................................. 15
1 Solution Architecture

1.1 Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mobile Device</td>
<td>▪ Customer’s end-user Mobile devices with SandBlast Mobile Application installed</td>
</tr>
</tbody>
</table>
| 2 SandBlast Mobile Connector | ▪ SandBlast Mobile Connector is an on-premise component of SandBlast Mobile  
 ▪ Connector encrypts all end-users’ PII (Personally Identifiable Information) with a key that stays on-premise and fully controlled by the customer.  
 ▪ End-user information goes encrypted to SandBlast Mobile cloud, using non-PII information to analyze and protect your mobile devices.                                                                                                                                   |
| 3 UEM/EMM/MDM             | ▪ Enterprise Mobility Management / Mobile Device Management  
 ▪ Device Management and Policy Enforcement System.                                                                                                                                                                                                                                                   |
| 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.                                                                                                                                                              |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5 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 SandBlast Mobile Dashboard can be integrated with an existing Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for automated policy enforcement on devices at risk.  
 ▪ When this integration is used, MDM/EMM serves as a repository with which the SandBlast Mobile Dashboard syncs enrolled devices and identities.  
 ▪ SandBlast Mobile dashboard is part of Check Point Infinity Portal, providing single pane of glass to all Check Point security applications and services. |
| 6 Behavioral Risk Engine | ▪ The cloud-based 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 is processed by or stored in the Engine. |
| 7 Check Point ThreatCloud | ▪ ThreatCloud is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to security services.  
 ▪ That intelligence is used to identify emerging outbreaks and threat trends.  
 ▪ ThreatCloud’s knowledge base is dynamically updated using feeds from a network of global threat sensors, attack information from gateways around the world, Check Point research labs and the industry’s best malware feeds. |
2 Getting Started

This guide describes how to launch the Check Point SandBlast Mobile from the Check Point Infinity Portal. It also describes the interface of the Check Point SandBlast Mobile, its main features and menus, and how to start a deployment. This includes activation and protection of a new device, malware detection and mitigation (including investigative flow).

2.1 General Workflow

   
   **Note** - Registration creates you an account on the Infinity Portal but does not automatically log you in to any specific security service. Use the "Try" function to log into the SandBlast Mobile service.

2. Enabling your user account on the Infinity Portal.
3. Navigating the screens, adding and activating new users, apps, policies, devices.
4. Updating and managing your Global Settings.

2.2 Launching the SandBlast Mobile

Your Check Point SandBlast Mobile is managed from the Check Point Infinity Portal.

Check Point Infinity Portal is a web-based interface for hosting the Check Point security SaaS services. For more information, see Check Point Infinity Portal Admin Guide.

**Note** - SandBlast Mobile is dependent on a purchased software license. For more information about licensing, contact your Check Point Sales representative, or check for updates at Check Point User Community.

To open your SandBlast Mobile service from the Infinity Portal window:

1. Click the Menu button in the top left corner of the Infinity Portal window.
2. Select the SandBlast Mobile service from the dropdown list:
<table>
<thead>
<tr>
<th>CLOUD PROTECTION</th>
<th>NETWORK PROTECTION</th>
<th>ENDPOINT PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudGuard SaaS</td>
<td>CloudGuard Connect</td>
<td>SandBlast Agent Management Platform</td>
</tr>
<tr>
<td>Infinity Next</td>
<td>Smart-1 Cloud</td>
<td>SandBlast Agent Cloud Management</td>
</tr>
<tr>
<td>CloudGuard Native</td>
<td>Data Tube</td>
<td>SandBlast Mobile</td>
</tr>
</tbody>
</table>
3 Creating and Logging in to your new Infinity Account

Create your new user in any Check Point Cloud security service to manage your Cloud protection services.

Example:

![Create User Account Form]

The Infinity Portal saves these credentials and uses them for any service on the portal.

**Note** - Account name cannot include special characters (!@#$%^&*, and so on).

**To create a new user in the Infinity Portal:**

1. Click [here](#) to receive the form to create a New User account.

Example:

![Create User Account Form]
2. Select the option **I accept the Infinity Portal terms of service and the privacy policy.**

3. Enter your company name and personal details.

4. Receive activation instructions to the email address that the administrator provides.

5. Go back to the Infinity Portal.

   Example:

   ![ACCOUNT CREATED SUCCESSFULLY](image)

   Back to sign in

   ![CHECK POINT INFINITY PORTAL](image)

   Unified security – delivered as a service

6. Click **Back to sign** into your newly created account.

   ✉️ **Note** - If you use SSO, you do no not need to provide a password.

7. In the **My Account** window, click **Next**.

8. In the Welcome screen, click **Let's Get Started**.

   ✉️ **Note** - Use the contract to associate your application User Account with the User Center. See **Contracts**.

You can at this time log in to any of the Infinity-based Cloud services from your active account.

Example:
To come back to an expired session:

When your work session ends, the **Session Expired** message shows.

Example:

To come back to your session, click **Back to Sign In**.

If you saved your password, click to re-start your session. It is not necessary to enter your credentials again.
4 Navigating into SandBlast Mobile Dashboard

Once logged into Infinity Portal, click on the left upper side MENU button, this will open the list of services on your Infinity Portal account, for that specific tenant. Clicking on SandBlast Mobile icon will take you to SandBlast Mobile Dashboard in Infinity Portal.

5 SandBlast Mobile Dashboard Overview

After logging into Infinity Portal chose SandBlast Mobile, you will be presented with the Dashboard view.
Navigating the Dashboard

The menu bar located on the left side of the page will be displayed on all of the dashboard pages and will help you navigate between the various screens. Each screen has tabs you can navigate to.

Menu Bar

The menu bar is permanently located on the left side of the SandBlast Mobile screen.

It displays the available options and menus on all of the dashboard pages and includes these options:
<table>
<thead>
<tr>
<th>Icon</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Menu</td>
<td>You can open the list of all Infinity Portal services available in your system. To work with the SandBlast Mobile, click the SandBlast Mobile icon on the list.</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>You can view both statistics and snapshot data based on information supplied by the enrolled devices.</td>
</tr>
<tr>
<td></td>
<td>Devices</td>
<td>You can view and manage the organization's devices.</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td>You can configure granular policies</td>
</tr>
<tr>
<td></td>
<td>Forensics</td>
<td>You can review the security forensic data, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Events &amp; Alerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Device Risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- App Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- iOS profiles</td>
</tr>
<tr>
<td></td>
<td>Settings</td>
<td>You can view and manage SandBlast Mobile specific settings.</td>
</tr>
</tbody>
</table>

The information in the **Global Settings** contains the initial default values of the administrators' profile settings that apply locally and impact the entire system.

**The Dashboard's Main Screen**

The Dashboard main screen displays 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 direct you to a query based page adapted to the state.

Example:

When you click on the event, you are redirected to the relevant window where you manage this event.

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Risk</td>
<td>Displays the number of devices in the organization that are currently at risk in these ways:</td>
</tr>
<tr>
<td></td>
<td>- Total number of devices at risk</td>
</tr>
<tr>
<td></td>
<td>- Number of devices at High risk</td>
</tr>
<tr>
<td></td>
<td>- Number of devices at Medium risk</td>
</tr>
<tr>
<td></td>
<td>- Number of devices at Low risk</td>
</tr>
<tr>
<td></td>
<td>- Device risk over time (last 7 days)</td>
</tr>
<tr>
<td>Device Status</td>
<td>Displays the number of devices registered in the dashboard and displayed in these ways:</td>
</tr>
<tr>
<td></td>
<td>- Total number of Devices</td>
</tr>
<tr>
<td></td>
<td>- Active Devices – devices that have installed and activated the App</td>
</tr>
<tr>
<td></td>
<td>- Provisioned &amp; User Notified – devices where the user has been notified on where and how to install and activate the App, or that the UEM has added to the System</td>
</tr>
<tr>
<td></td>
<td>- Disabled – devices that have uninstalled the App, or that the UEM has reported that the App is no longer installed</td>
</tr>
<tr>
<td></td>
<td>- Devices registered in the last day</td>
</tr>
<tr>
<td></td>
<td>- Devices registered in the last week</td>
</tr>
<tr>
<td></td>
<td>- Percent of devices on current agent version</td>
</tr>
<tr>
<td></td>
<td>- Percent of devices on older agent versions</td>
</tr>
</tbody>
</table>
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.

Dear Test Phone 1,

SandBlast Mobile Protect is a market-leading mobile threat defense solution that protects users from all mobile threats across apps, device and network. This one time setup takes approximately 2 minutes.

On your mobile device:

1) Install the SandBlast Mobile Protect app by clicking here or scanning the QR code below:

![QR Code]

2) Register by clicking here or scan the QR code below:

![QR Code]

3) Fill in the following information in case it is not yet populated:

   Server Address:
   Registration key:

   Press login.
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”.

![Google Play Store screenshot showing SandBlast Mobile app installation and access prompts.]
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 for download and registration.

Dear [Test Phone 1],

SandBlast Mobile Protect is a market-leading mobile threat defense solution that protects users from all mobile threats across apps, device and network. This one time setup takes approximately 2 minutes.

On your mobile device:

1) Install the SandBlast Mobile Protect app by clicking here or scanning the QR code below:

![QR Code](image)

2) Register by clicking here or scan the QR code below:

![QR Code](image)

3) Fill in the following information in case it is not yet populated:

Server Address: [Redacted]
Registration key: [Redacted]

Press login.
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.
# Modification History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modifications Made By</th>
<th>Modification Date</th>
<th>Description of Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>Hagay Sharon</td>
<td>20-Aug-2020</td>
<td>Updated new UI, Infinity Portal screenshots</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:hagays@checkpoint.com">hagays@checkpoint.com</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Pamela S. Lee</td>
<td>06-Dec-2017</td>
<td>Updated for New UI</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:pslee@checkpoint.com">pslee@checkpoint.com</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.2</td>
<td>Pamela S. Lee</td>
<td>17-May-2017</td>
<td>Updated with Yuval/Daniel feedback</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:pslee@checkpoint.com">pslee@checkpoint.com</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.1</td>
<td>Pamela S. Lee</td>
<td>04-May-2017</td>
<td>Updated with Yuval/Daniel feedback</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:pslee@checkpoint.com">pslee@checkpoint.com</a>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>Pamela S. Lee</td>
<td>03-May-2017</td>
<td>Initial Version</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:pslee@checkpoint.com">pslee@checkpoint.com</a>)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>