SandBlast Mobile

3.5

Release Notes
Important Information

**Latest Software**
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

**Check Point SandBlast Mobile 3.5**
For more about this product, see the SandBlast Mobile Product Page
https://www.checkpoint.com/products/sandblast-mobile/

**More Information**

### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 September 2019</td>
<td>Added support for iOS 13</td>
</tr>
<tr>
<td></td>
<td>Improved document layout</td>
</tr>
<tr>
<td>August 2019</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Version 3.5 Updates

Policy: On-device Network Protection (ONP) suspend abuse detection

ONP is one of the most powerful features of SBM yet to maintain user flexibility and interoperability with 3rd party/enterprise VPNs installed on user devices. ONP automatically detects 3rd party/enterprise VPNs and suspends ONP operation until the 3rd party/enterprise VPN becomes inactive.

To avoid scenarios of 3rd party/enterprise VPN misconfigurations which may compromise your organization’s security, SBM will notify if ONP is suspended due to 3rd party/enterprise VPN for a long period (suspended over 20 hours in a sliding time window of 24 hours). This capability is controlled using a new ONP configuration parameter.
**ONP Support for Enterprise VPNs** (available from version 3.4): Co-existence of multiple VPNs on a single mobile device is a common scenario. In some cases more than one VPN can be operational, but in other cases only a single VPN can operate at a single point of time. This depends on the OS (iOS, Android) and the VPN type and configuration.

Prior to version 3.4, SandBlast Mobile had a simplified control over ONP. In cases of collision between On-device Network Protection and other VPNs, users could turn off ONP or the other VPN.

From version 3.4, users can configure how SandBlast Mobile reacts in presence of additional VPNs:

- Keep ONP active unconditionally
- Suspend ONP if any other VPN is detected
- Suspend ONP only if another VPN is connected to user’s specified URL which represents enterprise resource (i.e. other VPN is used to access end-user corporate resources)

**On-device Client: Offline Detection**

While almost all attacks on mobile devices originate and require network access, there are some instances where they may occur while the device is offline. In order to provide better coverage for such scenarios, we’ve expanded our offline capabilities with new detection engines on-device. With offline detection you will be notified when a malware, profile, or a malicious device setting has been detected on the device while it is offline. When the device is back online, the admin will receive an alert as well.

**On-device Client: New App Analysis Notification**

To improve ease of deployment, user education, and user engagement, the SandBlast Mobile Protect App will display a notification each time a new app has been installed. To learn more on the newly installed App, user can click directly from the notification and switch into the App Analysis Report.
Events & Alerts: New Filter in Events and Alerts screen

The Events & Alerts tab is designed to supply an audit trail of incidents and actions that occurred on devices, such as new detected threats, risky application installation, Profiles detected on devices, etc.

To reduce administrative overhead, a new filter based on the property “Group” has been added to the Events & Alerts tab.

Device Risk: New filter for Threat Factor

The Device Risk tab allows the SandBlast Mobile administrator to view the various causes for devices to be at risk state. To reduce administrative overhead, a new filter based on the property “Threat Factor” has been added to the Device Risk tab.
Settings: Granular Admin Notifications

Now admins will be able to get focused notifications about the things they care about the most.
Settings: New admin roles

New admin roles have been added: ‘Group Admin Manager’ and ‘Group Admin Manager Viewer’. Those new roles allow organizations to further protect user privacy by allowing an admin to only manage and see specific devices pertaining to a specific device group and specific Policy Profiles.

On-device Client: Ongoing Improvements

As part of our ongoing efforts to maintain the SandBlast Mobile advantage and customer satisfaction, version 3.5 includes stability, battery and performance improvements.
Supported Mobile Client Versions

**iOS**: SandBlast Mobile Protect 2.60* and higher  
**Android**: SandBlast Mobile Protect 2.60* and higher  
(*) Devices running an older version will continue to be protected, but will not receive policy changes.

**Supported Mobile Client Platforms**

**iOS**: 8.x*, 9.x*, 10.x, 11.x, 12.x, 13.x  
**Android**: 4.x*, 5.x, 6.x, 7.x, 8.x, 9.x  
(*) Does not support On-device Network Protection.

To learn more about SandBlast Mobile's capabilities, visit the [SandBlast Mobile website](#). To make sure you know how to take full advantage of all the security capabilities of the solution, please refer to the [SandBlast Mobile Dashboard Admin Guide](#).