SandBlast Mobile

3.4

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 3.4**
For more about this product, see the SandBlast Mobile Product Page [https://www.checkpoint.com/products/sandblast-mobile/](https://www.checkpoint.com/products/sandblast-mobile/)

**More Information**
Visit the Check Point Support Center [http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2019</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
3.4 Updates

Policy: new On-device Network Protection (ONP) Configuration Parameters

On-device Network Protection (ONP) is one of four topics controlled per granular policy under the Policy tab. ONP Controls the Network layer protection provided by SandBlast Mobile. As part of SandBlast Mobile latest release, a new ONP Configuration screen is added to control the different parameters of ONP.

ONP can be configured to 3 states – Disabled, Always On, and Turn on when device is at HIGH risk. User can configure ONP parameters as described below.

Configure On-device Network Protection (ONP) Support for Enterprise VPNs:

Under policy tab, On-device Network Protection (ONP) section, user can push the ‘Configure’ button and use the pop-up screen to configure different ONP parameters. One of those parameters is the new ‘Suspend Policy’ feature. Suspend Policy allows the Administrator to decide, per Policy, if On-device Network Protection can be suspended manually, and whether ONP should be suspended when another VPN is detected on that device, any VPN or corporate resource related VPN. With this configuration user can practically enable ONP Support for Enterprise VPNs (aka Side-by-Side VPN) capability.
ONP Support for Enterprise VPNs – 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. With 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 Network Protection (ONP) Configuration General Settings:

On-device Network Protection (ONP) not installed Risk Level – with SandBlast Mobile version 3.4, under Policy/ONP/Configuration section, users can set the risk level of end user devices which did not install ONP or removed ONP.
Policy: Updated Policy Tab UI

Policy tab allows user to configure granular policies for different sections. To allow better user experience and easier navigation between the different Policies and their associated sections – an updated UI is presented.

As you can see in the upper screenshot, the 4 Policy sections (Device, Application, On-device Network Protection, WiFi Networks) move from a upper part of the screen to the policies list on the left side, under each and every policy.

Devices: New Search for Groups

Devices tab allows SandBlast Mobile users to configure logical groups and associate end-user devices to those logical groups. The groups can be nested (i.e. a tree or hierarchy – such as Sales – LATAM/EMEA/NAM/APAC …). A new Search facility is now available to allow SandBlast Mobile user to look for a specific group with its entire list of associated devices.
3.4 Updates

![Screen Shot of SandBlast Mobile dashboard with device information and options for adding and removing devices.](image_url)
App Analysis: New ‘Cloud Services’ report

A new capability under App analysis tab is available – Cloud Services report. This report lists all known cloud services used by the analyzed application. This capability gives users insights about other services used by this application and potentially involved risks or compliance issues.

App Analysis: New ‘Network Connections’ report

A new capability under App analysis tab is available – Network connections report. This report is applicable for Android app for now, it presents all App’s network connections, and it gives users insights about secured and non-secured connections as well as what services and backend servers the application uses. This can potentially unveil risks and compliance issues.

On-device Client - Application Analysis Report

SandBlast Mobile client now provides end-users with the ability to view an Application Analysis report which describes each Application installed on that device in terms of reputation, App Store Summary, Capabilities, overall risk and mitigation recommendations.
iOS Application Analysis:

High Risk
This application is a malware with dangerous capabilities, targeted to impact the device or exfiltrate sensitive data from the device. This app has access to calendar content on the device. It might modify or exfiltrate calendar data.

APP STORE SUMMARY
CAPABILITIES

(High exposure) **Uses Microphone** - This app has access to the device Microphone. It might perform surround recording without the user’s knowledge.

(High exposure) **Access Calendar** - This app has access to calendar content on the device. It might modify or exfiltrate calendar data.

(High exposure) **Access Contacts** - This app might access and read or update Contacts on the device.

BEHAVIORS
- **Contacts Collect** - This application sends your contacts to a remote server.
- **Calendar Collect** - This application sends the calendar events to a remote server.
- **Audio Recording Collect** - This application sends audio recording to a remote server.
On-device Client - On Going Improvements

As part of our ongoing efforts to maintain Sandblast Mobile advantage and customer satisfaction, version 3.4 includes bug fixes for stability and improved performance, as well as battery consumption 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.

Mobile Client Supported Platforms

**iOS:** 8.x*, 9.x*, 10.x, 11.x, 12.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, and 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.