© 2020 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.
Important Information

Latest Software
We recommend you to 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 3.7
For more information 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>25th May 25, 2020</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Version 3.7 Updates

Android Enterprise

SandBlast Mobile now supports Android Enterprise with all the deployment modes – BYOD, COPE, COSU & COBO. It also supports integration with all the major MDMs/UEMs to enable and operate Android Enterprise.

Android Enterprise is a Google-led initiative that enables the operation of Android devices and apps in the workplace. The program offers APIs and other tools for developers to integrate support for Android into their enterprise mobility management (EMM) solutions. For example, through one or more API(s) your UEM platform can disable a camera, Bluetooth, or prevent an access to the system settings.

For information about configuring Android Enterprise on your device see [here](#).

How it works

- SandBlast Mobile administrator manages Android Enterprise modes and profiles through an MDM/UEM. For example, a COPE device (Company Owned, Personal Enabled) is seen as two devices managed by SandBlast Mobile, so that different policies can be applied to each profile, Work and Personal.
- SandBlast Mobile administrator is configured through MDM/UEM, gets synchronized with the SandBlast Mobile dashboard, and can view and manage every profile of every registered device, independently.
- SandBlast Mobile recognizes that these two profiles belong to a single device that consumes a single license for both profile instances of SandBlast Mobile.
- SandBlast Mobile administrator can set a policy to increase the risk level of the registered devices if the end user's choice was not to install the SandBlast Mobile protection on the Personal profile.

For more information about Android Enterprise and SandBlast Mobile refer to the SandBlast Mobile Admin Guide and to the latest version of MDM/UEM Integration guides [here](#).
MDM/UEM Integration - New Setup Menu

A new MDM integration setup menu and updated SandBlast Mobile MDM integration guides are now available for the SandBlast Mobile administrator here. They make the SBM-MDM interconnection configuration an easy and user-friendly task. Administrators understand the exact parameters required for each configuration phase and can monitor the status of the MDM integration at each phase.

How it works

- SandBlast Mobile supports all the major MDMs/UEMs available in the market, and also an integration with the non-officially integrated MDMs, and the MDMs that implement SandBlast Mobile MDM/UEM APIs.
- SandBlast Mobile new menu leads the administrator through the follow-up steps and phases of the interconnection between SBM and MDM.
- SandBlast Mobile administrators can view and manage all the registered MDM devices and users that appear under the SandBlast Mobile dashboard after their integration is successfully completed.

For more information refer to the new release MDM/UEM integration guides here.
MARS App Vetting

Mobile App Reputation Service (MARS) is a new application vetting service that allows SandBlast Mobile administrators to upload an APK (Android App format) file into SBM dashboard and receive a full app analysis report to their email box within few minutes. Future releases of MARS will add support for IPA (iOS App format).

How it works

- To learn about an application, administrator uploads the APK file into the SandBlast Mobile Dashboard under the App Analysis tab.

- The SandBlast Mobile MARS service analyzes the uploaded App in the background and generates a full analysis report. This report includes information about the App’s behavior, capabilities, permissions, risks, connections, cloud hosting services, and more.

- When the App analyze is finished, administrator receives an email with the link to the full App analysis report.

  If the App is analyzed for first time, the process of creating the report can last for several minutes. If the App was analyzed by SandBlast Mobile before, administrator can immediately download the full App analysis.

- After the study of the App analysis report administrators can make educated decisions based on the full App analysis before they distribute the App into their organization’s Mobile devices.
JAMF MDM Support

SandBlast Mobile now supports the interconnection with JAMF MDM. JAMF is a leading Apple solution (only for MDM devices).

How it works

- Administrator follows the instructions provided in the SandBlast Mobile user-friendly MDM setup menu and in the updated MDM integration guide for JAMF, and performs the interconnection between the SandBlast Mobile dashboard and a JAMF MDM.
Multiple Policy Enhancements

Copy Policy

With the **Copy Policy** function administrator can easily clone an existing Policy Profile on the SandBlast Mobile dashboard. The newly cloned Policy Profile inherits the exact definitions of the source Policy Profile. To make the newly cloned Policy Profile applicable, administrator must attach the newly cloned Policy Profile to the rule in the Rulebase.

Importing a List of Whitelisted/Blacklisted Domains

A domain name and location can be imported into **Whitelisted/Blacklisted Domain Names** list and into **Whitelisted/Blacklisted Download Prevention Locations** list.

**How it works**

- With the new **Import** feature SandBlast Mobile administrator can easily edit and manipulate a large list of Domain Names/Locations on any external 3rd party tool (for
example, text editor or Excel), then save it in CSV format. This CSV file is imported into the Whitelisted/Blacklisted Domain Names list and into the Whitelisted/Blacklisted Download Prevention Locations list on the SandBlast Mobile dashboard and replaces the existing list.

This feature allows administrators to import a list of Domain Names/Locations from other systems (for example, Firewall/Gateway) into the SandBlast Mobile On-device Network Protection (ONP) policy settings.

**URL Filter Categories – Show Events in Client**

This new capability allows SBM administrator to disable on-device notifications per URL Filter Category. On the way it allows the use of URL filtering based on web-site categories and minimizes the alerts and pop-ups on the end-user device.

**How it works**

- By default, the URL filtering action applies a client device pop-up notification with a new event card in the SandBlast Protect app **Events center**.

- If administrator unchecks the **Show events in client** option per specific category, only the blocked URL page is displayed to the end-user who accesses the browser.

- If administrator chooses to filter a URL category, both event on device (client) and events sent to the dashboard are visible, unless administrator chooses to disable it.
iOS Device Notification Permission Policy

This new device level policy allows administrators to set the risk level for end-users’ devices where the end-user did not approve, or removed, Protect App notifications permissions.

How it works

- During the installation of the SandBlast Mobile Protect App on an iOS device, the end-user is asked to grant Notification Permissions to the Protect App.
- If the end-user does not grant the permissions, or removes the granted permissions, the Protect App will not be able to use Notifications, which reduces some capabilities of the app.

For the SandBlast Mobile administrators who want to know about these cases and resolve them, Check Point added a new policy rule that allows SBM administrators to define the risk level of the associated device.

ONP Configuration – Change of Event Severity Level

By default, all the On-Device Protection (ONP) events sent from mobile devices to SandBlast Mobile dashboard are marked with the Critical severity level with no option to change the level.

This new feature allows administrators to change the severity level of the ONP events per the ONP policy. Now administrator can apply different ONP Events Severity Levels to different devices, basing on the policy applied to them.
Device Risk – Export CSV

This new option allows administrator to export data into a CSV file. The data is collected from all mobile devices that match the filter criteria of Device Risk tab.

Administrator sets multiple search criteria and then exports the list of matching devices with their associated details (for example, user name, email address, phone number, and more). Later administrator can use these details to approach the end-users and give them further instructions (for example, how to remove the risk off their mobile devices, and more).

Mobile Client Supported Platforms

iOS: 10.x, 11.x, 12.x, 13.x

Android: 5.x, 6.x, 7.x, 8.x, 9.x, 10.x