© 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 3.8
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>July 21, 2020</td>
<td>First release of this document</td>
</tr>
<tr>
<td>Aug 3rd, 2020</td>
<td>Updated version of this document</td>
</tr>
<tr>
<td>Sep 3rd, 2020</td>
<td>Final version of this document</td>
</tr>
</tbody>
</table>
Version 3.8 Updates

ZeroTouch Deployment with MDM/UEM

‘Zero-Touch Deployment’ enables automatic deployment of SandBlast Mobile Application on end-users’ mobile devices, both iOS and Android Enterprise. Zero-Touch requires the administrator to interconnect SandBlast Mobile with an MDM/UEM. MDM/UEM pushes and installs the SandBlast Mobile Protect App on the provisioned device with all the parameters required to register and run it. SandBlast Mobile immediately becomes active and protects the device without any user’s intervention. This functionality also includes ONP attack prevention.

For more information about configuration of Zero-Touch deployment refer to the SandBlast Mobile Release Notes and the MDM/UEM Zero-Touch Deployment Guide and MDM/UEM integration guides [here](#).

How it works

- SandBlast Mobile administrator must interconnect the SandBlast Mobile and the organization’s MDM/UEM through the SandBlast Mobile’s ‘System/Device Management/UEM Server’ setup menu.
- You choose and connect to the relevant MDM/UEM, then follow the instruction in your MDM’s Integration Guide to establish synchronization between SandBlast Mobile and the MDM/UEM.
- If you use Android Enterprise, follow the MDM/UEM Integration Guide to configure Android Enterprise according to the desired AE (Android Enterprise) management profile – Device Owner or Profile Owner.

Zero-Touch Deployment Compatibility Matrix:

<table>
<thead>
<tr>
<th></th>
<th>InTune</th>
<th>Workspace ONE</th>
<th>MobileIron Core</th>
<th>MobileIron Cloud</th>
<th>Maas360</th>
<th>XenMobile</th>
<th>BlackBerry UEM</th>
<th>Jamf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>X</td>
<td>V</td>
<td>X</td>
<td>N/A</td>
</tr>
<tr>
<td>iOS</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>

*If the device VPN is already in place, and you are installing the Zero-Touch Deployment for SandBlast Mobile, you must disable any other VPN throughout SandBlast Mobile Zero-Touch deployment process.

- Finally, to configure Zero-Touch deployment, follow the instruction of your relevant MDM/UEM in the ‘MDM/UEM Zero-Touch deployment configuration guide’ found [here](#).
Mobile Application Upload for Scanning

As part of SandBlast Mobile application analysis, SandBlast Mobile users can upload both iOS (IPA) and Android (APK) applications' binaries into SandBlast Mobile dashboard and receive a full app analysis report to their email box within few minutes. For more information, please refer to ‘SandBlast Mobile Admin Guide’.

How it works

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

- SandBlast Mobile App Analysis service scans 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 analysis is completed, administrator receives an email with the link to the full App analysis report.
  
  If the App is analyzed for first time, the process of the report creation take 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 is completed, administrators can make educated decisions based on the full App analysis before they distribute the App into the Mobile devices in their organization.
MITRE ATT&CK Matrix

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. With the release of SandBlast Mobile 3.8, malicious applications are now also analyzed and categorized using MITRE ATT&CK Tactics and Technics.

For more information about the MITRE ATT&CK matrix refer to the MITRE WEB site https://attack.mitre.org/techniques/mobile/

How it works

- If you click on any of the MITRE ATT&CK Technics (e.g. T1532: Data Encrypted) you launch a new tab on your browser that redirects you to a specific to Technic WEB page on the MITRE ATT&CK WEB site, where you receive the detailed description of that attack’s technic.

- You can also click the ‘Open MITRE ATT&CK full table’ option to view the full-size MITRE ATT&CK table on MITRE ATT&CK site, and from there you can browse to review any of the specific attack tactics and technics.
Generic MDMs Integration

This new capability enables customers to use MDMs that are officially not integrated with the SandBlast Mobile. These customers can use the SandBlast Mobile generic MDM integration API. MDMs, that implement this API, can integrate with the SandBlast Mobile and synchronize SandBlast Mobile with their mobile users and devices, and receive notifications from the SandBlast Mobile.

For more information refer to ‘SandBlast Mobile Admin Guide’

How it works

- The MDMs that are not officially supported by SandBlast Mobile, must implement the generic MDM API to enable the integration between the SandBlast Mobile and the designated MDM.

- One example for such MDM is ‘mdportsolution’ integrated now with the SandBlastMobile:
As soon as the SandBlast Mobile and MDM are synchronized, the SandBlast Mobile is updated with the list of users and devices from the MDM, and administrator can start inviting new users to register to SandBlast Mobile.

**Support MDM managed and unmanaged devices in a single dashboard**

With the SandBlast Mobile version 3.8, administrators can synchronize users and devices with an MDM and simultaneously manage the manually registered users and devices on the same SandBlast Mobile dashboard.

**How it works**

- Different device groups must be created for the 'Non-MDM managed Devices' and for the 'MDM Managed' devices.
- Manually registered devices must be labeled as 'Non-MDM managed Devices'. The MDM managed devices are synchronized to their relevant groups.
Support VMWARE Workspace ONE Intelligence

SandBlast Mobile version 3.8 supports integration with VMWARE Workspace ONE Intelligence. When connected to Workspace ONE Intelligence, the SandBlast Mobile sends the security event logs (syslog) messages. It allows security/SOC administrators to use other services that run over the Workspace ONE Intelligence. These additional services can use the advanced security indicators from the SandBlast Mobile that come from the organization’s mobile devices and create additional reports and insights.

For more information on Workspace ONE Intelligence refer to VMWARE Workspace ONE Intelligence WEB site.

How it works

- Before starting to integrate Workspace ONE Intelligence, SandBlast Mobile must be first integrated with Workspace ONE UEM.
- For more information on SandBlast Mobile integration with Workspace ONE Intelligence refer to Workspace ONE UEM integration https://downloads.checkpoint.com/dc/download.htm?ID=56770
- On the SandBlast Mobile Dashboard, go to ‘Settings/Syslog Settings’ and select the ‘Workspace ONE Intelligence’ option.

SandBlast Mobile sends Syslog messages to the Workspace ONE Intelligence service. You must configure the Workspace ONE Intelligence service details and verify the two systems are connected.
• When the connection is established, you can view the SandBlast Mobile threats insights on the Workspace ONE Intelligence dashboards and use the powerful Intelligence platform to automate the threats handling. For example, you can create a response to a new detected malware by sending a Slack message to the group of security analysts, or use a callback to any remote service that offers a web hook API.

Detection of Rogue Access Point on Corporate WI-FI

SandBlast Mobile version 3.8 detects and sends alerts about rogue WI-FI access points. These access points attempt to manipulate corporate end-users on their mobile devices and connect them to a fake access point disguised as a work place SSID. Furthermore, the hacker can perform a man-in-the-middle attack, reveal corporate credentials, steal sensitive data and more. Administrator can set the risk level and policy associated with this attack technique. Note: SandBlast Mobile currently supports this feature on iOS only.

How it works

• On the SandBlast Mobile Dashboard, go to ‘Policy>Policy-Name=WIFI Network’, click on the ‘Rogue Access Point on Corporate WI-FI Settings’ part and configure the settings for your corporate external IP and WiFi SSID. Also, set the desired risk level and associate it with the device exposed to a rogue corporate WIFI.
• When the SandBlast Mobile detects a rogue corporate WIFI on a mobile device, the device risk level changes to the one set in this policy. If the risk level is ‘Critical’ – and it is configured under the ‘Conditional Access’ then the access to the corporate resources is blocked immediately.
• Administrator will see both the events and the device risk level, and can further handle this threat.

Detection of Port Scanning

With this new capability, the SandBlast Mobile detects attempts to scan mobile device’s ports by an adversary in order to find open/vulnerable ports with known weaknesses, which can be used to initiate an attack on the mobile device. Administrator can set the risk level and policy associated with this attack technique. SandBlast Mobile currently supports this feature on iOS only.

How it works

• On the SandBlast Mobile Dashboard, go to ‘Policy->Policy-Name->WIFI Network’, and scroll to ‘Port Scan Settings’.
• In the ‘Port Scan Settings’ section, enable this feature and set the risk level and event severity level (or keep the default settings) for any attempt to scan the device that runs the SandBlast Mobile.
ONP Access Lists - New Formats

SandBlast Mobile version 3.8 supports new and unified location formats for all ONP access lists. The new formats include IPv4, IPv6, Domain Names, DomainName/URLs and Wildcards. All new formats can be used in any of ONP access lists.

For more information refer to ‘SandBlast Mobile Admin Guide’

How it works

**NOTE:** To use this new capability, you must upgrade all devices managed by a single Dashboard to the latest SandBlast Mobile App version - 3.8. If not all devices are upgraded, only older (“legacy”) formats can be used, each access list according to what was supported before 3.8.

- Option 1: Administrator configures any of SandBlast Mobile On-device Network Protection policy access lists, and can add any of the following formats: IPv4, IPv6, Domain Name or DomainName/URL. Each of these formats can be combined with wildcards.
- Option 2: Administrator imports a CSV file that contains a list of locations and comments with any of the allowed formats.

**Note:** An uploaded CSV file overrides any existing values in the relevant list.

ONP Allowed Android Apps

Administrators of the SandBlast Mobile On-device Network Protection use this new capability to specify Android applications that are allowed to access the Internet without considering their risk/maliciousness found by the SandBlast Mobile. It makes the administrators responsible for the security verdict. For more information please refer to ‘SandBlast Mobile Admin Guide’

How it works

- Option 1: On the SandBlast Mobile Dashboard, go to ‘Policy->policy-name->On-device Network Protection->Whitelisted Applications’ and add a new Android package name to the list.
- Option 2: Administrator can import a CSV file which contains a list of allowed Android apps with (or without) comments.
- **Note:** An uploaded CSV file overrides any existing values in the ‘Whitelisted Apps’ list.
Export InfinityPortal SandBlast Mobile logs to On-Premise SmartView

This new capability redirects the events generated by a SandBlast Mobile dashboard within the InfinityPortal to the on-premise SmartView server.

How it works

- Administrator that use SandBlast Mobile in the InfinityPortal, can redirect the SandBlast Mobile logs to an external (on-premise) SmartView server.

- In the InfinityPortal, go to 'Global Settings>Export Events' and connect the InfinityPortal exported logs to on premise SmartView. Follow the instructions under this section and configure the settings in the on-premise SmartView server to accept the incoming logs from the SandBlast Mobile in the InfinityPortal.

- **Note:** These settings apply to all the InfinityPortal applications (for example, SandBlast Mobile, CloudGuard SaaS, and more) that export logs to the InfinityPortal Events App (=cloud SmartView).
Protected DNS – Early Availability

This new capability of SandBlast Mobile On-device Network Protection, Administrators can use On-device Network Protection to centrally configure devices or group of devices with HTTPS protected DNS service from any third party provider of their choice. Protected DNS keeps end-users browsing information private, as well as prevents MiTM attacks and DNS Spoofing attacks which legacy clear text DNS is exposed to.

How it works

- Go to /Policy/Policy Profiles <policy-name>/On-Device Network Protection/Protected DNS
- Here administrator configures the different parameters of Protected DNS
- To enable the usage of Protected DNS, Administrator should set ‘Protected DNS Mode’ to ‘On’, this enforces the mobile device to use the DNS set by the administrator.
- Set the organization Compliancy policy risk level
- Set if using encryption protected DNS server, or legacy plain text DNS server.
- Verify the DNS server is reachable and save the settings
- With SandBlast Mobile Dashboard’s ‘granular policies’, administrator can manage ‘protected DNS’ centrally and per group.
- In any point of time administrator can turn off SandBlast Mobile Protected DNS server and make the device default DNS server to take over.

**Note:** We recommend customers who wish to experience Protected DNS to start using it with a selected group of devices, as this feature is still in its Early Availability stage for the next few weeks.

### Onboarding Dashboard (Quick Actions Menu)

This new capability of SandBlast Mobile allows new and experienced users to easily enroll new users and devices to SandBlast Mobile using three methods under ‘Quick Actions’ menu.

**How it works**

- Once logged to SandBlast Mobile Dashboard, go to ‘Overview’ tab and click ‘Quick Actions’ menu, a pop up window with 3 options will show up:
- Demo on Device – experience connecting a single end-user and device
- Invite by Email – with this option administrator can invite a single or multiple users, or groups to enroll to SandBlast Mobile, each will get an email with instructions and QR codes to ease the enrollment process
- Synch with MDM – with this option user administrators can connect SandBlast Mobile to any of their preferred MDMs and start synchronizing users and device to SandBlast Mobile.
Integration with Intune Mobile Application Management (MAM) – Early Availability

SandBlast Mobile version 3.8 integrates with Microsoft Intune Mobile Application Management (MAM). Using Intune MAM allows customers to manage enterprise applications on end-users devices.
without managing the mobile device itself. Intune MAM allows customers to install, update and remove applications and protect enterprise data used by those applications.
**Note:** Customers who wish to use Intune MAM with SandBlast Mobile should reach out to their local Check Point reseller or sales representative and ask for a trial.


**Integration with Google EMM – Early Availability**

SandBlast Mobile version 3.8 integrates with the upcoming Google EMM. Google EMM is in Beta phase and not generally available yet.

Integration of SandBlast Mobile with Google EMM allows synchronization of users and devices from Google EMM to SandBlast Mobile, and enforcement of policies from Google EMM on the mobile devices as a response to risk notifications raised by SandBlast Mobile to Google EMM.
**Note:** Customers who wish to use Google EMM with SandBlast Mobile should reach out to their local Check Point reseller or sales representative and ask for a trial.

**Mobile Client Supported Platforms**

- **iOS:** 10.x, 11.x, 12.x, 13.x, 14.x
- **Android:** 5.x, 6.x, 7.x, 8.x, 9.x, 10.x, 11.x