Important Information

© 2019 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 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 3.3
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>20 February 2019</td>
<td>Updated Mobile Client Supported Platforms</td>
</tr>
<tr>
<td>3 February 2019</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
3.3 Updates

Granular Policies

Many organizations have a diverse set of users who in many cases require a different security policy. To support these organizations’ needs, we’ve introduced Granular Policies. Granular Policies allows an admin to configure a variety of security policies based on what’s best for the organization i.e. Device, Application, Network Protection, Wi-Fi Network Protection, and Cellular Network Protection. To accommodate this, the Policy setting will be moved to the Global policy profile so that you and your users will not have policy enforcement interruptions during the roll-out.

New Policy tab

When you navigate to the Policy tab, you are presented with a Rule Base list that has the default Global policy profile already listed.

Rule Base

As you add new policy profiles for different groups/users, you will add them to the Rule Base to assign them to the appropriate groups/users.

For more information, please refer to the CheckMates blog about Granular Policies and to the official SandBlast Mobile Admin Guide.
Deprecation of Android Legacy SMiShing Protection

Check Point has always been ahead of the curve in mobile security. SandBlast Mobile was the first mobile threat defense (MTD) product to introduce SMiShing (SMS Phishing) protection in general availability in the spring of 2017. Since then, the innovation has not slowed down, and in the summer of 2018, the broadest protection against phishing was made generally available as part of the SandBlast Mobile 3.0. It not only protects against SMiShing attacks, but attacks from all applications, including WhatsApp, Telegram, and Facebook Messenger. Coupled with Safe Browsing, Conditional Access, Anti-Bot, and URL Filtering, this provides customers with the most comprehensive mobile threat prevention capability in the industry.

Today, in order to comply with new industry-wide Google Play Store Guidelines, the legacy SMiShing protection will be removed from SandBlast Mobile, but the security protection offered by the solution is not decreased. SandBlast Mobile today provides better prevention and detection across Apps, Network, and Device attack vectors than it did two years ago, and is considered a leader in the industry.

To learn more about SandBlast Mobile’s Anti-Phishing capability, 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.

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.