Check Point SandBlast Mobile

UEM Integration Guide with Citrix XenMobile

Version: 3.0
About This Guide

Check Point SandBlast Mobile 3.0 is the most complete threat defense solution designed to prevent emerging fifth generation cyber attacks and allow workers to safely conduct business. Its technology protects against threats to the OS, apps, and network, scoring the industry’s highest threat catch rate without impacting performance or user experience.

Only SandBlast Mobile 3.0 delivers threat prevention technology that:

- Performs advanced app analysis to detect known and unknown threats
- Prevents man-in-the-middle attacks on both cellular and WiFi networks
- Blocks phishing attacks on all apps: email, messaging, social media
- Prevents infected devices from sending sensitive data to botnets
- Blocks infected devices from accessing corporate applications and data
- Mitigates threats without relying on user action or mobile management platforms

SandBlast Mobile 3.0 uses a variety of patent-pending algorithms and detection techniques to identify mobile device risks, and triggers appropriate defense responses that protect business and personal data.

The SandBlast Mobile solution ("the Solution") includes the following components:

- SandBlast Mobile Behavioral Risk Engine ("the Engine")
- SandBlast Mobile Gateway ("the Gateway")
- SandBlast Mobile Management Dashboard ("the Dashboard")
- SandBlast Mobile Protect app ("the App") for iOS and Android

When used with an Unified Endpoint Management (UEM) system, such as Citrix XenMobile, SandBlast Mobile provides integral risk assessment of the device to which the UEM can use to quarantine or enforce a set of policies that are in effect until the device is no longer at risk. Such policy enforcement could be to disable certain capabilities of a device, such as blocking access to corporate assets, such as email, internal websites, etc., thus, providing protection of the corporation’s network and data from mobile-based threats.

This guide first describes how to integrate the SandBlast Mobile Dashboard with Citrix XenMobile. It provides a quick tour through the interface of the XenMobile Console and the SandBlast Mobile Dashboard in order enable integration, alerting, and policy enforcement.

This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).
## Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 SandBlast Mobile Protect app | - The SandBlast Mobile Protect app is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior.  
- To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects.  
- The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience. |
| 2 UEM                         | - Unified Endpoint Management (generalized term replacing MDM/EMM)  
- Device Management and Policy Enforcement System                                                                                               |
| 3 SandBlast Mobile Gateway    | - The cloud-based SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered.  
- The Gateway handles all Solution communications with enrolled mobile devices and with the customer’s (organization’s) Dashboard instance. |
| 4 SandBlast Mobile Dashboard  | - The cloud-based web-GUI SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance.  
- The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.  
- When using this integration, the UEM serves as a repository with which the Dashboard syncs enrolled devices and identities. |
| 5 Behavioral Risk Engine      | - The cloud-based SandBlast Mobile Behavioral Risk Engine uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis.  
- The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity.  
- The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected.  
- No Personal Information is processed by or stored in the Engine. |
## Contents

### Chapter 1 Preparing the UEM Platform for Integration ........................................... 1  
**Prerequisites** ........................................... 1 
**Citrix XenMobile Console** ........................................... 2  
**Creating a Delivery Group** ........................................... 2  
**Sending Enrollment Invitations** ........................................... 4  
Enrolling Devices to Citrix XenMobile ........................................... 4  
**Creating Limited Administrator Account (optional)** ........................................... 5  
Create a New Administrator Role ........................................... 5  
Create a New Administrator Account ........................................... 6  

### Chapter 2 Configuring the SandBlast Mobile Dashboard UEM Integration Settings .... 9  
**Prerequisites** ........................................... 9 
**Configuring Device Management Integration Settings** ........................................... 10  
Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile ........................................... 13  
Tag Device Status ........................................... 13 
Tag Device Risk ........................................... 13 
Tag Device TF ........................................... 14 
Controlling the Importing of Personally Identifiable Information (PII) from the UEM ........................................... 14 
MDM Advanced Settings ........................................... 15  

### Chapter 3 Configuring the UEM Platform ........................................... 17  
**Configuring UEM to Deploy SandBlast Mobile Protect app** ........................................... 18  
Prerequisites ........................................... 18 
Adding the SandBlast Mobile Protect App to Your App Catalog ........................................... 18 
Adding an iOS Configuration Policy for SandBlast Mobile Protect ........................................... 26 
Collecting App List from iOS Devices ........................................... 29 
Requiring the SandBlast Mobile Protect app to be Installed ........................................... 31 
**Creating a Mitigation Process** ........................................... 34  
Creating Device Policies ........................................... 35 
Creating Actions for Devices at High Risk ........................................... 38  
Send Notification to User ........................................... 38 
Mark Devices at High Risk as Out of Compliance ........................................... 42 
Creating an AppLock Policy for Devices at High Risk ........................................... 45 
Creating Actions for Devices at Medium Risk ........................................... 48 
Creating Actions for Devices Not at Risk ........................................... 51  
Mark Devices at No Risk as Compliant ........................................... 51 
Mark Devices Not at High Risk as Compliant ........................................... 54  

### Chapter 4 Registering Devices to SandBlast Mobile ........................................... 59  
**Registration of an iOS Device** ........................................... 60 
**Registration of an Android Device** ........................................... 62  

### Chapter 5 Testing High Risk Activity Detection and Policy Enforcement .............. 65  
**Blacklisting a Test App** ........................................... 66
View of Device at Risk ................................................................. 67
SandBlast Mobile Protect App Notifications .......................... 67
Citrix XenMobile In-App Notification .................................... 67
Citrix XenMobile Email Notification ...................................... 68
Administrator View on the SandBlast Mobile Dashboard ........ 68
Administrator View on the Citrix XenMobile Console .......... 69
Appendix .................................................................................. 71
Integration Information .............................................................. 71
Preparing the UEM Platform for Integration

This chapter discusses the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>1</td>
</tr>
<tr>
<td>Citrix XenMobile Console</td>
<td>2</td>
</tr>
<tr>
<td>Creating a Delivery Group</td>
<td>2</td>
</tr>
<tr>
<td>Sending Enrollment Invitations</td>
<td>4</td>
</tr>
<tr>
<td>Enrolling Devices to Citrix XenMobile</td>
<td>4</td>
</tr>
<tr>
<td>Creating Limited Administrator Account (optional)</td>
<td>5</td>
</tr>
<tr>
<td>Create a New Administrator Role</td>
<td>5</td>
</tr>
<tr>
<td>Create a New Administrator Account</td>
<td>6</td>
</tr>
</tbody>
</table>

**Prerequisites**

1. Citrix XenMobile version 10.7 or higher.
2. Citrix XenMobile must be configured with an Apple Push Certificate (APNS) and Google Play Credentials.
3. The MDX app files for Citrix Mail and Citrix Web Browser have been added to the App Catalog.
4. For Active Directory integration, users to be registered to SandBlast Mobile must belong to Security Group(s) to be tied to SandBlast Mobile. See "Creating a Delivery Group" on the next page.
Citrix XenMobile Console

1. Login to your Citrix XenMobile Console.

Creating a Delivery Group

To deploy policies, configurations, apps, etc. in XenMobile, we must create a delivery group that will contain the users whose devices will be registered to SandBlast Mobile.

1. Navigate to **Configure > Delivery Groups**.
2. Click "Add", and on the "Delivery Group Info" tab, provide a unique name for the Delivery Group, such as in the example below.

3. Click "Next".

4. On the "User" tab, select whether this is an AD Domain user group or a local Citrix group.
   a. If an AD Domain group, select the domain, and then enter in a Security Group name to search the AD database for the group. Select the Security Group(s) to include.
   b. If a local group, select "local" from the Domain section and enter in a User Group if one exists. If a user group doesn't exist, you can skip selecting a group.

5. Click "Next".
6. Click "Next" through the remaining tabs until the final "Summary" tab, and then click "Save".
Sending Enrollment Invitations

This step isn’t absolutely required, but it is nice for the workflow for user engagement/enrollment into Citrix XenMobile. By sending enrollment invitations, the users are emailed enrollment instructions and any required authentication information.

1. Navigate to Manage > Enrollment Invitations, click "Add", and select "Add Invitation".

![Image of XenMobile interface for managing enrollment invitations]

2. On the "Enrollment Invitation" tab, select Recipient type, platform, and templates and other fields marked with (*).

![Image of XenMobile interface for configuring enrollment invitation details]

3. Click "Save & Send".

Enrolling Devices to Citrix XenMobile

Creating Limited Administrator Account (optional)

For integration from SandBlast Mobile to XenMobile, we will create an administrator role and account that limits the access of this admin to only those permissions necessary to provide integration.

**Note:** It is a best practice to create such an admin account, but is optional.

Create a New Administrator Role

1. Navigate to Settings > Role-Based Access Control, click "Add".

![Role-Based Access Control](https://example.com/role-based-access-control.png)
2. On the "Add Role" window, enter in a Name and select the following Authorized Access for this new role:
   a. Admin console access
   b. Remote Support access
   c. Public api access

3. In addition the Authorized Access permissions, we are going to select the following Console features for this role:
   a. Devices > Clear Restriction
   b. Devices > Edit device
   c. Devices > View software inventory
   d. Local Users and Groups > Edit Local User
   e. Local Users and Groups > Local User Groups

4. Click "Next".
5. Click "Save".

Create a New Administrator Account

1. Navigate to Manage > Users, click "Add Local User".
2. Add Local User screen, fill in all required (*) fields with appropriate information, such as in the example below. And select the Role we created in the previous step.

3. Click "Save".

**Note:** At this point, we have all the information we will need to configure the Device Management integration settings in the SandBlast Mobile Dashboard.

From Our Examples:

- Server = https://cxm.cptme.us:14443
- API Admin Username/Password = sbm_admin/<hidden>
- Organization AD Group(s) = Agents
Configuring the SandBlast Mobile Dashboard UEM Integration Settings

This chapter discusses the following:

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Configuring Device Management Integration Settings</th>
<th>Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile</th>
<th>Tag Device Status</th>
<th>Tag Device Risk</th>
<th>Tag Device TF</th>
<th>Controlling the Importing of Personally Identifiable Information (PII) from the UEM</th>
<th>MDM Advanced Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>10</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>14</td>
<td>14</td>
<td>15</td>
</tr>
</tbody>
</table>

Prerequisites

You will need the following details from your Citrix XenMobile Deployment:

**Note:** There is a table in "Integration Information" on page 1 that you can record your settings for easy reference.

1. **Server:** The URL to your Citrix XenMobile System, usually the same as the Citrix XenMobile Console URL. Such as https://cxms.example.com:4443.
2. **Citrix XenMobile Administrative Username and Password:** These are the Admin credentials that the SandBlast Mobile Dashboard will use to connect to the UEM. You may have created a special API Only Admin account in "Creating Limited Administrator Account (optional)" on page 5 for this purpose.
3. **Organization Local Group(s):** This is the Citrix XenMobile locally defined groups to which the users/devices are members, and whose devices will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each group name separated with a semicolon (;).
4. **Organization AD Group(s):** This is the Citrix XenMobile AD groups to which the users/devices are members, and whose devices will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each group name separated with a semicolon (;).
5. **Mitigation attribute:** This field will not be used as we will be using the CHKP Risk and Status tags.
6. **Tag Device Status:** Toggle ON to send preset mitigation tag CHKP_Status variable that can be set to Provisioned, Active, or Inactive by SandBlast Mobile to reflect the status of the device within SandBlast Mobile. This variable is interpreted as a "device property" of "CHKP_Status" by Citrix XenMobile.
7. **Tag Device Risk:** Toggle ON to send preset mitigation tag CHKP_Risk variable that can be set to High, Medium, Low, or None by SandBlast Mobile to reflect the status of the device within SandBlast Mobile. This variable is interpreted as a "device property" of "CHKP_Risk" by Citrix XenMobile.
8. **For on-premise UEM environments,** the TCP Web Services port (usually TCP port 4443 (HTTPS)) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the UEM system before trying to connect.

**Note:** Only the devices are synchronized from the UEM to the SandBlast Mobile Dashboard, not users.
Configuring Device Management Integration Settings

1. Navigate to **Settings > Device Management > Setting**.
2. Select "Citrix XenMobile" from the "MDM service" drop-down menu under the Device Management Settings area.
3. A pop-up window will open.
4. Configure the settings as are appropriate for your Citrix XenMobile Deployment, such as those you may have created in "Preparing the UEM Platform for Integration" on page 1.

5. Turn ON "Tag Device Status" and "Tag Device Risk". A description of how these Tags work is provided in "Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile" on the facing page.
   a. You can also turn on "Tag Device TF", which is also discussed further in "Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile" on the facing page.

6. If you want to limit the type of Personally Identifiable Information (PII) from being imported from the Citrix XenMobile Console to SandBlast Mobile Dashboard, you can turn OFF "Import device name", "Import Device phone #", and/or "Device owner email". A description of what these settings do is provided in "Controlling the Importing of Personally Identifiable Information (PII) from the UEM" on page 14.

7. Click "VERIFY". If the settings are correct, and the SandBlast Mobile Dashboard can communicate with the Citrix XenMobile system, you will be able to click "SAVE" to finish configuration.
Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile

Recently added to SandBlast Mobile Dashboard for UEM integrations is the concept of multi-tags. The multi-tags are built-in tags that SandBlast Mobile will use to indicate the different registration states (CHKP_Status) and the different risk levels (CHKP_Risk) to which the devices can be marked. This allows the Administrators on the UEM to configure granular compliance policies based on device registration status or risk level. These tags are created as "device properties" in Citrix XenMobile.

The Multi-tags are automatically created in XenMobile Console when enabled during the Device Management Configuration process in SandBlast Mobile Dashboard.

There are 3 Status states:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioned</td>
<td>When a device is synchronized for the first time in SandBlast Mobile Dashboard</td>
</tr>
<tr>
<td>Active</td>
<td>After the user has installed and registered to SandBlast Mobile</td>
</tr>
<tr>
<td>Inactive</td>
<td>If the device hasn’t checked-in with SandBlast Mobile for X number of days (configured by the SandBlast Mobile Admin)</td>
</tr>
</tbody>
</table>

There are 4 pre-defined Risk level:

» None
» Low
» Medium
» High

For example, if the device has a Low risk app and a High risk (malicious) SMS URL, then the device will be marked as at High Risk (CHKP_Risk = High). Once the High Risk issue has been remediated (SMS deleted), then the device will be marked as at Low Risk (CHKP_Risk = Low). Once the Low Risk issue has been remediated, the device will be marked as None (No Risk).

**Tag Device Status**

For integration with Citrix XenMobile, the Device Status tag is interpreted as a "device property" of "CHKP_Status" with the values of Provisioned, Active, or Inactive.

We will use the CHKP_Status device property to determine when to prompt the user to install the SandBlast Mobile Protect app on their device. If the CHKP_Status device property hasn’t been set yet, then the device has not been synced with SandBlast Mobile Dashboard.

**Tag Device Risk**

For integration with Citrix XenMobile, the Device Risk tag is interpreted as a "device property" of "CHKP_Risk" with the values of None, Low, Medium, or High.

We will use the CHKP_Risk device property to determine when to enact certain policies or actions on the device. If the CHKP_Risk is High or Medium, then the device will be sent an in-app notification and blocked from running corporate apps.

We will use these device property in the Mitigation Policies in "Creating a Mitigation Process" on page 34.
Tag Device TF

The Threat Factor tag (CHKP_TF) is a list of threat factors associated with the Security Risk level, such as TF_BACKUP_TOOL, etc. These threat factors can be used to provide additional detail and granularity of the current Risk level, however, they are not necessarily appropriate for policy triggers. The CHKP_TF value is a sort of free-form comma separated string of threat factors from the BRE database.

Controlling the Importing of Personally Identifiable Information (PII) from the UEM

The PII for devices (users) can be limited from being imported to SandBlast Mobile by configuring the "Import Personally Identifiable Information (PII)" section.

If all entries are turned off, then a placeholder information set for the email address will be placed in the Device Owner’s Email, in the form of "#@mdm_vendor", such as 3@xenmobile.mdm.

1. PII Control is configured in the Settings > Device Management > Setting > MDM service pop-up window.
2. Turning off PII Import, will result in the following Devices display in SandBlast Mobile.

MDM Advanced Settings

When a UEM Service is configured, the Device Management Advanced Settings are automatically configured based on recommendations of the selected UEM provider, in this case from Citrix XenMobile.

1. Navigate to Settings > Device Management > Advanced, and make any appropriate changes.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices. Values: 10-1440 minutes, in 10 minute intervals</td>
</tr>
<tr>
<td>Device deletion threshold</td>
<td>Percentage of devices allowed for deletion after UEM device sync. 100% for no threshold</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync – device will not be deleted if it will be re-sync from UEM during the threshold interval. Values: 0-48 hours</td>
</tr>
<tr>
<td>App sync interval</td>
<td>Interval to connect with UEM to sync app list. Values: 10-1440 minutes, in 10 minute intervals</td>
</tr>
</tbody>
</table>
Note: If you make changes to the default settings, click "Save" to have changes take effect.
Chapter 3

Configuring the UEM Platform

Now the we have completed the integration steps, we can continue with the configuration of the UEM platform.

For this process we will return to the XenMobile Console to complete the configuration.

This chapter discusses the following:

- Configuring UEM to Deploy SandBlast Mobile Protect app .......................................................... 18
  - Prerequisites ............................................................................................................................... 18
- Adding the SandBlast Mobile Protect App to Your App Catalog .................................................. 18
- Adding an iOS Configuration Policy for SandBlast Mobile Protect .............................................. 26
- Collecting App List from iOS Devices ....................................................................................... 29
- Requiring the SandBlast Mobile Protect app to be Installed ...................................................... 31
- Creating a Mitigation Process .................................................................................................... 34
- Creating Device Policies ............................................................................................................ 35
- Creating Actions for Devices at High Risk .................................................................................. 38
  - Send Notification to User .......................................................................................................... 38
  - Mark Devices at High Risk as Out of Compliance ................................................................... 42
  - Creating an AppLock Policy for Devices at High Risk ............................................................. 45
- Creating Actions for Devices at Medium Risk ............................................................................ 48
- Creating Actions for Devices Not at Risk .................................................................................... 51
  - Mark Devices at No Risk as Compliant .................................................................................... 51
  - Mark Devices Not at High Risk as Compliant ......................................................................... 54
Configuring UEM to Deploy SandBlast Mobile Protect app

Prerequisites


Adding the SandBlast Mobile Protect App to Your App Catalog

In this process we will be using the CHKP_Status tag, please see "Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile" on page 13 for more information.

Using the CHKP_Status Tag we can start deploying the SandBlast Mobile Protect app from the public stores to those devices that will be protected by Check Point SandBlast Mobile. We will do this to only require the Protect app when the device has the CHKP_Status of Provisioned, Active, or Inactive. If CHKP_Status device property has not been set, then the user will NOT be prompted to install the SandBlast Mobile Protect app. This ensures that the devices are synchronized in the SandBlast Mobile Dashboard before asking the user to install the SandBlast Mobile Protect app.

We will need to add the Protect App for both iOS and Android operating systems.

1. Navigate to Configure > Apps, and click "Add".
2. On the "Add App" pop-up window, select "Public App Store".

3. Enter a Name for the app.
4. Select only "iPhone", "iPad", and "Google Play" under Platforms.
5. Click "Next".
6. Enter in "SandBlast Mobile Protect" and click "Search".
7. The search result window should show the SandBlast Mobile Protect app, such as in the example below.
8. Click SandBlast Mobile Protect app.

9. Scroll down and Select "Deployment Rules".
10. Change "Deploy when" to "Any", and click "Advanced" tab.

11. Click "New Rule".
12. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Provisioned".
13. Click "+".

14. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Active".
   b. Click "+".
15. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Inactive".
   b. Click "+".

16. Once all the Deployment Rules are listed as they are below, click "Next".
17. On the iPad Platform tab, select the SandBlast Mobile Protect app, and scroll down to "Deployment Rules".

18. Change "Deploy when" to "Any", and click "Advanced" tab.

19. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Provisioned".
   b. Click "+".

20. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Active".
   b. Click "+".

21. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Inactive".
   b. Click "+".

© 2018 Check Point Software Technologies Ltd. All rights reserved. | P. 24
October 17, 2018
22. Once all the Deployment Rules are listed as they are above, click "Next".
23. On the Google Play Platform tab, select the SandBlast Mobile Protect app, and scroll down to "Deployment Rules".

24. Change "Deploy when" to "Any", and click "Advanced" tab.
25. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Provisioned".
   b. Click "+".
26. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Active".
   b. Click "+".
27. Click "New Rule".
   a. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Inactive".
   b. Click "+".
28. Once all the Deployment Rules are listed as they are above, click "Next".
29. Click "Next".
30. On the "Delivery Group Assignments" tab, select the Delivery Group you created in "Creating a Delivery Group" on page 2.

31. Click "Save".

Adding an iOS Configuration Policy for SandBlast Mobile Protect

To auto-register iOS devices to SandBlast Mobile, we need to configure an iOS Configuration Policy.

1. Navigate to Configure > Device Policies, and click "Add".
2. Select "Apps" > "App Configuration".
3. Enter in a Policy Name, select "iOS" only from Platforms, and click "Next".
4. On the Platforms: iOS tab, select "Add new" for "Identifier".
5. Enter "com.checkpoint.capsuleprotect".
6. Copy and Paste the following text into the "Dictionary content" field.

```
<dict>
  <key>Device Serial Number</key>
  <string>${device.serialnumber}</string>
  <key>DEVICE_MAC</key>
  <string>${DEVICE_MAC}</string>
  <key>DISPLAY_NAME</key>
  <string>${DISPLAY_NAME}</string>
  <key>EMAIL</key>
  <string>${EMAIL}</string>
  <key>FIRST_NAME</key>
  <string>${FIRST_NAME}</string>
  <key>LAST_NAME</key>
  <string>${LAST_NAME}</string>
  <key>USERID</key>
  <string>${USERID}</string>
  <key>Lacoon Server Address</key>
  <string>gw.locsec.net</string>
</dict>
```
7. Click "Check Dictionary" to make sure that there are no errors.
8. Click "Next".
9. On the Assignment tab, select the Delivery Group, and select "Deploy for always-on connections".

10. Click "Save".

Collecting App List from iOS Devices

This step is important to allow SandBlast Mobile to protect against malicious apps.

1. Navigate to Configure > Device Policies, and click "Add".
2. Select "Apps" > "App Inventory".
3. Enter a Policy Name.

4. Click "Next".

5. On the Platforms > iOS tab, make sure iOS is ON.
6. Click "Next".
7. On the Assignment tab, select the Delivery Group, and select "Deploy for always-on connections".

8. Click "Save".

**Requiring the SandBlast Mobile Protect app to be Installed**

The SandBlast Mobile Protect app is required by editing the Delivery Group Apps tab and moving the SandBlast Mobile Protect app from Optional to Required.

1. Navigate to Configure > Delivery Groups, select the Delivery Group, and click Edit.
2. Select the Apps tab.

3. Remove SandBlast Mobile Protect from the Optional Apps by clicking the "X".
4. **Drag "SandBlast Mobile Protect" to "Required Apps".**

5. **Select the Summary tab.**
6. On the Summary tab, make sure the apps show up correctly, and click "Save".

Creating a Mitigation Process

In this section, you will reference a device property (CHKP_Risk) SandBlast Mobile Dashboard will use to label any device in High, Medium, or Low Risk, or None for device with No Risk as determined by the SandBlast Mobile Analysis. This device property, CHKP_Risk, will allow the Citrix XenMobile system to identify which devices are at risk and to enforce actions and policies based on risk level. To learn more about the CHKP Risk tag, please see "Multi-tags in SandBlast Mobile and Usage in Citrix XenMobile" on page 13 for more information.

We will use the CHKP_Risk device property in several actions as a trigger that when met will enact the action described.

Important Note about Citrix XenMobile Device Properties:

Device Properties are controlled by the device in that if a device property is set/configured at the XenMobile Console, the device must sync to XenMobile in order for the device to receive this device property setting. This means that there is a delay between when a device is marked at risk, such that CHKP_Risk = High, and the device enacting the actions/policies sent to it during a previous sync (or during initial enrollment) to the XenMobile system. This is not a shortcoming of SandBlast Mobile; it is how XenMobile utilizes device properties. Because of this delay/operational requirement, there will be a delay between when a device is marked at risk and the policies/actions being enacted at the device to block access to corporate resources.

Note: We will show a couple of different Actions and Policies, but these enforcement policies are something that the customer should create for their environment and needs.

In a production environment, the customer should configure the policies according to their internal security policy.
Creating Device Policies

We will create a device policy to Lock certain apps while the device is at risk.

1. Navigate to **Configure > Device Policies**, and click "Add".

![Configure Device Policies]

2. On the pop-up window, select the type of Policy to create, in our example, we will create an App Lock policy by selecting "Security > App Lock".

![Add a New Policy]

© 2018 Check Point Software Technologies Ltd. All rights reserved.
3. On the "Policy Info" screen, enter in a unique name and, if desired, a description.

4. Click "Next".

5. On the iOS screen, Select "Add new" for App bundle ID, and enter in "com.citrix.mail.ios".

6. Set "Allow user to remove policy" to "Never".

7. Click "Next".
8. On the Android screen, enter in a Lock message that will be displayed to the user.
   a. Set "Prevent uninstall" to "ON".
   b. Enforce "Blacklist".
   c. Click "Add", and select "Add new".
   d. Enter in "com.citrix.mail.droid", and click "Save".

9. Click "Next".
10. On the Assignment screen, select the Delivery Group you created in "Creating a Delivery Group" on page 2, in our example "SBM_Users"

11. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

12. Click "Save".

Creating Actions for Devices at High Risk

Send Notification to User

1. Navigate to Configure > Actions, and click "Add".
2. On the Action Info screen, enter in a unique name, and if desired, a description.

3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter in "CHKP_Risk"
   d. Select "is"
   e. Enter in "High"

5. Select an Action as follows:
   a. Select "Send notification"
   b. Select "Non-Compliant Device"
   c. Set to "0" Hours (for immediately)
   d. Set to "1" Days for reminder

6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in "Creating a Delivery Group" on page 2, in our example "SBM_Users"

8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".

10. On the Summary screen, click "Save".
Mark Devices at High Risk as Out of Compliance

1. Navigate to Configure > Actions, and click "Add".

2. On the Action Info screen, enter in a unique name, and if desired, a description.
3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter in "CHKP_Risk"
   d. Select "is"
   e. Enter in "High"
5. Select an Action as follows:
   a. Select "Mark the device as out of compliance"
   b. Select "is"
   c. Select "True"
   d. Set to "0" Hours (for immediately)
6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in "Creating a Delivery Group" on page 2, in our example "SBM_Users".
8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".
10. On the Summary screen, click "Save".
Creating an AppLock Policy for Devices at High Risk

1. Navigate to Configure > Actions, and click "Add".

2. On the Action Info screen, enter a unique name, and if desired, a description.

3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter "CHKP_Risk"
   d. Select "is"
   e. Enter "High"

5. Select an Action as follows:
   a. Select "App Lock"
   b. Set to "0" Hours (for immediately)
6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in Section "Creating a Delivery Group" on page 2, in our example "SBM_Users"
8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".
10. On the Summary screen, click "Save".
Creating Actions for Devices at Medium Risk

1. Navigate to Configure > Actions, and click "Add".

2. On the Action Info screen, enter a unique name, and if desired, a description.
3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter in "CHKP_Risk"
   d. Select "is"
   e. Enter in "Medium"
5. Select an Action as follows:
   a. Select "Send notification"
   b. Select "Non-Compliant Device"
   c. Set to "0" Hours (for immediately)
   d. Set to "1" Days for Reminder
6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in "Creating a Delivery Group" on page 2, in our example "SBM_Users".
8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".
10. On the Summary screen, click "Save".
Creating Actions for Devices Not at Risk

Mark Devices at No Risk as Compliant

1. Navigate to Configure > Actions, and click "Add".

2. On the Action Info screen, enter in a unique name, and if desired, a description.

3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter in "CHKP_Risk"
   d. Select "is"
   e. Enter in "None"

5. Select an Action as follows:
   a. Select "Mark the device as out of compliance"
   b. Select "is"
   c. Select "False"
   d. Set to "0" Hours (for immediately)

6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in "Creating a Delivery Group” on page 2, in our example "SBM_Users"

8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".

10. On the Summary screen, click "Save".
Mark Devices Not at High Risk as Compliant

1. Navigate to Configure > Actions, and click "Add".

2. On the Action Info screen, enter in a unique name, and if desired, a description.

3. Click "Next".
4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. Select "Other"
   c. Enter in "CHKP_Risk"
   d. Select "Is Not"
   e. Enter in "High"

5. Select an Action as follows:
   a. Select "Mark the device as out of compliance"
   b. Select "is"
   c. Select "False"
   d. Set to "0" Hours (for immediately)

6. Click "Next".
7. On the "Assignment" screen, select the Delivery Group you created in "Creating a Delivery Group" on page 2, in our example "SBM_Users".
8. Also, under Deployment Schedule, turn ON "Deploy for always-on connections".

9. Click "Next".
10. On the Summary screen, click "Save".
11. The Actions screen will show something like this:

![Actions screen](image)

**Note:** Now any device in the Delivery Group ("SBM_Users") that has the Device Property "CHKP_Risk" "equal to" "High" or "Medium" set by the SandBlast Mobile system will be acted upon by the Actions and Policies.
Registering Devices to SandBlast Mobile

In this chapter we will cover the user experience of device registration with SandBlast Mobile.

This chapter discusses the following:

- Registration of an iOS Device ................................................................. 60
- Registration of an Android Device ......................................................... 62

Note: It can take up to 10 minutes for the UEM to sync with the SandBlast Mobile Dashboard, and a few minutes for the UEM to push the App to the user’s device.
Registration of an iOS Device

After the device is enrolled to the Citrix XenMobile and the device is synchronized to SandBlast Mobile, the CHKP_Status device property will be set to "Provisioned".

1. The user will be prompted to install the SandBlast Mobile Protect App. The user taps "INSTALL".
2. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration. The registration server and key are automatically configured in the App by the Citrix XenMobile system.

3. The user will be prompted to install the SandBlast Mobile Protect App. The user taps "INSTALL".
4. After the App has been deployed on the iOS Device, the user only needs to launch the App to finish the registration. The registration server and key are automatically configured in the App by Citrix XenMobile.
5. The user is prompted to enable Notifications, Location, and Network Security.

6. Continue with enabling Network Security, and tap "Allow" to allow SandBlast Mobile Protect to add the needed VPN Configuration profile.
7. The user is prompted to enable SMS Phishing Protection.

8. Continue through Settings > Messages > Unknown & Spam, and make sure that SMS Phishing > Protect is enabled.

9. Returning to SandBlast Mobile Protect, tap "Done" to initialize the scanning of the device.

10. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.
Registration of an Android Device

After the device is enrolled to the Citrix XenMobile and the device is synchronized to SandBlast Mobile, the CHKP_Status device property will be set to "Provisioned".

1. The user will be prompted to install the SandBlast Mobile Protect app. The user is automatically taken to the Google Play Store.

2. The user taps the "INSTALL", and taps "ACCEPT" to accept the permissions of the App. The App installs.

3. After the App is installed, the user must launch the App to finish its deployment and registration to Check Point SandBlast Mobile.

4. The App will automatically register.

5. The user is prompted to allow SandBlast Mobile Protect to make and manage phone calls. Tap "Allow".

6. The user is prompted to turn on Location, SMS, and Network Protection features. Tap "Allow all required permissions".

7. Tap "OK" to allow SandBlast Mobile Protect to configure a VPN connection. This is necessary for the Network Security Protection features of Safe Browsing and Anti-Phishing to work.

8. Tap "Allow" to allow SandBlast Mobile Protect to access this device's location.
9. Tap "Allow" to allow SandBlast Mobile Protect to provide SMS protection.
10. Tap "Enable" to configure Accessibility permissions for SandBlast Mobile Protect.
11. Scroll down and tap "SandBlast Mobile". and tap the toggle to turn Accessibility ON.

12. Continue with configuring the Accessibility permissions for SandBlast Mobile Protect. Tap "OK".
13. Return to SandBlast Mobile Protect.
14. Once the App is done scanning the system, it will display the state of the device. In this case, the device is without malicious or high risk apps, network and OS threats.
Testing High Risk Activity Detection and Policy Enforcement

1 – SandBlast Mobile sends risk notification to User’s Device
2 – SandBlast Mobile sends the risk level for User’s Device to Citrix XenMobile
3 – Citrix XenMobile activates the appropriate compliance policy for User’s Device based on security risk level

If the user’s device is determined to be at risk either due to a malicious app or malicious activity, the SandBlast Mobile system notifies the User via in-app notifications as well as updates the risk state by setting the appropriate CHKPRisk tag to the Citrix XenMobile system for that device.

Citrix XenMobile receives the state change, and upon recognizing the set Device Property being tied to Policies/Actions, enacts those policies/actions.

In the following example, the Administrator will blacklist an app, such as in our example "Dropbox". As a result, all devices with "Dropbox" installed will be identified to be at High Risk (CHKP_Risk = High) due to the blacklisted app being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device with CHKPRisk to High to the Citrix XenMobile system. The Citrix XenMobile system will then enforce policy actions specified in the policies/actions. This mitigation process was the one we created in "Creating a Mitigation Process" on page 34.

This chapter discusses the following:

- Blacklisting a Test App ................................................................. 66
- View of Device at Risk ............................................................... 67
- SandBlast Mobile Protect App Notifications .............................. 67
- Citrix XenMobile In-App Notification ......................................... 67
- Citrix XenMobile Email Notification .......................................... 68
- Administrator View on the SandBlast Mobile Dashboard ............ 68
- Administrator View on the Citrix XenMobile Console ................. 69
**Blacklisting a Test App**

The first step is to blacklist an app, in our example "Dropbox". By blacklisting this app, all release version and OS types will also be blacklisted. In our example, Dropbox for Android will be blacklisted which will result in all Dropbox numbered release versions for Android to be blacklisted as well, unless the "Apply only to this version" checkbox is selected.

1. Log into the SandBlast Mobile Dashboard.
2. Navigate to **App Analysis** tab, and search for the app you wish to blacklist, in our example "Dropbox".
3. Click "Policy" link of "Default".
4. On the "Changing application policy" pop-up window, select "Black Listed" from the "New policy" drop-down menu, and enter a reason for this change in the "Audit Trail note".
5. Click "OK".
**View of Device at Risk**

**SandBlast Mobile Protect App Notifications**

1. The user receives a SandBlast Mobile Protect notification indicating that the blacklisted app is not allowed by Corporate Policy, in our example “Dropbox”.

**Citrix XenMobile In-App Notification**

1. The user will not be to open the Citrix Mail app as specified in the AppLock device policy.
Citrix XenMobile Email Notification

1. The user receives an email from the Citrix XenMobile system, as specified in the "SBM_HighRisk" Actions policy.

Administrator View on the SandBlast Mobile Dashboard

1. From the SandBlast Mobile Dashboard, the Administrator will see that there are devices at high risk.
2. Clicking the High Risk will display a list of devices at high risk.
3. Selecting the desired device from the left-side list, the Administrator can see that the high risk state is caused by the existence of the blacklisted app, “Dropbox”.

**Administrator View on the Citrix XenMobile Console**

1. In the Citrix XenMobile Console on the Analyze view, the Administrator can see that one or more devices are Non-compliant.

2. In the Citrix XenMobile Console from the Devices View, the Administrator can see that Fox’s device is Out of Compliance and that the CHKP_Risk device property is equal to High.
3. Clicking the device’s name and selecting "Show more", the Administrator is presented with the device details view.

4. On the General tab, the Administrator can see that the device has been sent an AppLock Security profile.

5. On the "Properties" tab, the Administrator can see that the device has a CHKP_Risk value of High.
## Appendix

### Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenMobile Server/API URL</td>
<td></td>
</tr>
<tr>
<td>XenMobile API Admin Username</td>
<td></td>
</tr>
<tr>
<td>XenMobile API Admin Password</td>
<td></td>
</tr>
<tr>
<td>XenMobile Local Group(s)</td>
<td></td>
</tr>
<tr>
<td>XenMobile AD Group(s)</td>
<td></td>
</tr>
<tr>
<td>XenMobile Mitigation attribute (Device Property)</td>
<td></td>
</tr>
<tr>
<td>(deprecated)</td>
<td></td>
</tr>
<tr>
<td>Tag Device Risk (CHKP_Risk)</td>
<td>None, Low, Medium, or High</td>
</tr>
<tr>
<td>Tag Device Status (CHKP_Status)</td>
<td>Provisioned, Active, or Inactive</td>
</tr>
<tr>
<td>Tag Device Threat Factor (CHKP_TP)</td>
<td>Free-form information provided by BRE</td>
</tr>
<tr>
<td>SandBlast Mobile Gateway</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>SandBlast Mobile App Name (iOS)</td>
<td>SandBlast Mobile Protect</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (iOS)</td>
<td>com.checkpoint.capsuleprotect</td>
</tr>
<tr>
<td>SandBlast Mobile App Name (Android)</td>
<td>SandBlast Mobile Protect</td>
</tr>
<tr>
<td>SandBlast Mobile App ID (Android)</td>
<td>com.lacoon.security.fox</td>
</tr>
</tbody>
</table>