26 May 2020

SandBlast Mobile for Citrix Endpoint Management

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 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 for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.
# Table of Contents

About Check Point SandBlast Mobile .................................................................................. 6  
General Workflow .............................................................................................................. 6  

Introduction to the SandBlast Mobile Integration Guide ..................................................... 7  

Solution Architecture ......................................................................................................... 8  

Preparing UEM Platform for Integration ............................................................................ 10  
Prerequisites ....................................................................................................................... 10  
General Workflow .............................................................................................................. 11  
Creating a local users Group ............................................................................................. 11  
Creating a Delivery Group ................................................................................................ 12  
Sending Enrollment Invitations ........................................................................................ 15  
Enrolling Devices to Citrix Endpoint Management ............................................................. 16  
Creating Limited Administrator Account ........................................................................... 17  
(optional) ........................................................................................................................... 17  
Create a New Administrator Role ....................................................................................... 17  
Create a New Administrator Account .............................................................................. 20  

Configuring the Check Point SandBlast Mobile Dashboard Integration Settings ............... 22  
Prerequisites ....................................................................................................................... 22  
Configuring Integration Settings ....................................................................................... 24  
Procedure ........................................................................................................................... 24  

Configuring UEM to Deploy the SandBlast Mobile Protect app ....................................... 40  
General Workflow .............................................................................................................. 40  
Configuring UEM to Deploy SandBlast Mobile Protect app .............................................. 40  
Prerequisites ....................................................................................................................... 40  
Adding the SandBlast Mobile Protect App to Your App Catalog ....................................... 41  
Adding Android Enterprise Managed Configurations .......................................................... 56  
Adding an iOS Configuration Policy for SandBlast Mobile Protect ................................... 59  
Collecting App List from iOS Devices ................................................................................ 65
Testing High Risk Activity Detection and Policy Enforcement .................................................. 99

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requiring the SandBlast Mobile Protect app to be Installed</td>
<td>68</td>
</tr>
<tr>
<td>Creating a Mitigation Process</td>
<td>72</td>
</tr>
<tr>
<td>Creating Device Policies</td>
<td>72</td>
</tr>
<tr>
<td>Creating Actions for Devices at High Risk</td>
<td>77</td>
</tr>
<tr>
<td>Send Notification to User</td>
<td>77</td>
</tr>
<tr>
<td>Mark Devices at High Risk as Out of Compliance</td>
<td>80</td>
</tr>
<tr>
<td>Creating an AppLock Policy for Devices at High Risk</td>
<td>83</td>
</tr>
<tr>
<td>Creating Actions for Devices at Medium Risk</td>
<td>79</td>
</tr>
<tr>
<td>Creating Actions for Devices Not at Risk</td>
<td>82</td>
</tr>
<tr>
<td>Mark Devices at No Risk as Compliant</td>
<td>82</td>
</tr>
<tr>
<td>Mark Devices Not at High Risk as Compliant</td>
<td>85</td>
</tr>
<tr>
<td>Using Android Enterprise with SandBlast Mobile</td>
<td>89</td>
</tr>
<tr>
<td>Profiles</td>
<td>89</td>
</tr>
<tr>
<td>Android Enterprise Deployment Scenarios</td>
<td>89</td>
</tr>
<tr>
<td>Configuring SandBlast Mobile Protect app to Protect your Devices</td>
<td>90</td>
</tr>
<tr>
<td>Deploying Android Enterprise on your Devices</td>
<td>90</td>
</tr>
<tr>
<td>Policies</td>
<td>92</td>
</tr>
<tr>
<td>Risk Handling</td>
<td>93</td>
</tr>
<tr>
<td>Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement</td>
<td>95</td>
</tr>
<tr>
<td>Deploying the SandBlast Mobile Protect app on the Devices</td>
<td>95</td>
</tr>
<tr>
<td>Registration of an iOS Device</td>
<td>95</td>
</tr>
<tr>
<td>Registration of an Android Device</td>
<td>96</td>
</tr>
<tr>
<td>Testing High Risk Activity Detection and Policy Enforcement</td>
<td>99</td>
</tr>
<tr>
<td>Blacklisting a Test App</td>
<td>100</td>
</tr>
<tr>
<td>View of Device at Risk</td>
<td>101</td>
</tr>
<tr>
<td>SandBlast Mobile Protect App Notifications</td>
<td>101</td>
</tr>
<tr>
<td>Citrix Endpoint Management In-App Notification</td>
<td>101</td>
</tr>
<tr>
<td>Citrix Endpoint Management Email Notification</td>
<td>102</td>
</tr>
<tr>
<td>Administrator View on the SandBlast Mobile Dashboard</td>
<td>102</td>
</tr>
</tbody>
</table>
About Check Point SandBlast Mobile

Check Point SandBlast Mobile is the most complete threat defense solution that prevents emerging fifth generation cyber attacks and allows workers to safely conduct their businesses. This technology prevents threats to the OS, apps, and network. It scores the highest threat catch rate in the industry and does not hit performance or user experience.

SandBlast Mobile 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 Wi-Fi networks.
- Blocks phishing attacks on all apps: email, messaging, social media.
- Prevents sensitive data distribution from infected devices to botnets.
- Blocks infected devices from accessing corporate applications and data.
- Mitigates threats independently from user action or mobile management platforms.

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

- The SandBlast Mobile solution ("the Solution") includes these 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.

SandBlast Mobile integrates with UEM systems and provides integral risk assessment of the device which the UEM can use to quarantine, or activate a set of policies until the device is no longer at risk.

This policy enforcement can disable certain capabilities of a device, for example, block access to corporate assets, such as email, internal websites, and more. It provides protection of the corporation’s network and data from mobile-based threats.

This guide describes how to integrate the SandBlast Mobile Dashboard with your Citrix Endpoint Management. It provides a quick tour through the interface of the Citrix Endpoint Management and the SandBlast Mobile Dashboard to enable integration, alerting, and policy enforcement. This includes activation and protection of a new device, malware detection, and mitigation (including mitigation flow).

General Workflow

1. Prepare your Citrix Endpoint Management UEM platform for the Check Point SandBlast Mobile Protect app integration. See Preparing UEM Platform for Integration.
2. Configure your Citrix Endpoint Management UEM to deploy the Check Point SandBlast Mobile Protect app. See Configuring UEM to Deploy the SandBlast Mobile Protect app.
3. Configure the Check Point SandBlast Mobile Dashboard for integration with the Citrix Endpoint Management. See Configuring the Check Point SandBlast Mobile Dashboard Integration Settings.
4. Apply the Check Point SandBlast Mobile Protect app configuration and policy enforcement to your Citrix Endpoint Management devices. See Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement.
Introduction to the SandBlast Mobile Integration Guide

The SandBlast Mobile Protect app is an app for iOS® and Android™ that gathers data and helps analyze threats to mobile 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.

This Guide explains how to integrate the Check Point SandBlast Mobile Protect app with the company device managing systems.
## Solution Architecture

### 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 Check Point 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.
- No Personal Information is processed by or stored in the Gateway.
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SandBlast Mobile Management 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. |
| **Behavioral Risk Engine** | - The cloud-based SandBlast Mobile Behavioral Risk Engine (BRE) 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. |
| **ThreatCloud** | - Check Point’s ThreatCloud is the world largest incidence of compromise database that incorporates real-time threat intelligence from hundreds of thousand Check Point gateways and from millions of endpoints across the globe.  
- ThreatCloud powers the Anti-Phishing, Safe Browsing, URL Filtering and Anti-bot technologies for SandBlast Mobile on-device Network Protection.  
- ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis. |
Preparing UEM Platform for Integration

Citrix Endpoint Management deploys SandBlast Mobile Protect app on a device.

Prerequisites

- SandBlast Mobile service integrates with Citrix Endpoint Management through the existing API. To enable integration, you must first create a Citrix Endpoint Management API account.

  SandBlast Mobile integrates with **Citrix Endpoint Management** (On-Premise) and Citrix Endpoint Management is version 10.7 or later, through API access. SandBlast Mobile uses the API to synchronize the device records, to retrieve device apps list, and to report the device risk level to Citrix Endpoint Management.

- Citrix Endpoint Management must be configured with an Apple Push Certificate (APNS) and Google Play Credentials.

- The MDX app files for Citrix Mail and Citrix Web Browser have been added to the App Catalog.

- 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 Endpoint Management Console (Example):**
General Workflow

1. Create a Delivery Group for Check Point SandBlast Mobile. See "Creating a Delivery Group".
2. For user’s enrollment into Citrix Endpoint Management send an enrollment invitations. See "Sending Enrollment Invitations".
3. For integration from SandBlast Mobile to Endpoint Management create a limited administrator account (optional). See "Creating Limited Administrator Account (optional)".

Creating a local users Group

To include the delivery group, that will be created in the next step, in our own group, we must create a local group.

1. Navigate to Manage > Users and click on “Manage Local Groups” tab.
2. Enter a Local Group name as shown in the example below and click on the “+” sign to the right.

```
Manage Groups
```

```
SBM_local_group
```

Creating a Delivery Group

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

1. Navigate to **Configure > Delivery Group** and click “Add”.
2. On the "**Delivery Group Info**" tab, provide a unique name for the Delivery Group, such as in the example below.

![Delivery Group Info](image)

3. Click "**Next**".

4. On the "**Assignments**" tab, in **Mange user Assignment** section select whether it’s ‘’In Endpoint Management’’ or ‘’In Citrix Cloud’’.

5. In the **Select Domain** section 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.
c. If a local group, select "local" from the Domain section and enter in a User Group that you’ve created in the previous section.

d. Click "Next".
Sending Enrollment Invitations

This step isn’t absolutely required, but it is nice for the workflow for user engagement/enrollment into Citrix Endpoint Management. 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".

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

3. Toggle the “Send Invitation” button to be ON.
4. Click "Save & Send".

Enrolling Devices to Citrix Endpoint Management

Visit this guide for details on device enrollment to Citrix Endpoint Management.
Creating Limited Administrator Account (optional)

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

**Best Practice** - It is a best practice to create such an admin account, but is optional.

Create a New Administrator Role

1. Navigate to Settings > Server tab > find “Role-Based Access Control” in the list and click on it.

2. Click “Add”.
3. 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
4. In addition the Authorized Access permissions, we are going to select the following **Console features** for this role by scrolling to the desired features and selecting checkboxes as written below:

   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

5. Click "Next".

6. On the Assignment tab click "Save".
Create a New Administrator Account

1. Navigate to Manage > Users, click "Add Local User".

2. In Add Local User screen, fill in all required (*) fields with appropriate information, such as in the example below:
   a. Enter a valid name and password.
   b. In the Role field select the Role we created in the previous step above.
   c. In the Membership field select the local users group we created in the section above.

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://cpmobile.xm.cloud.com:4443/
API Admin Username/Password = Admin_User/<hidden>
Organization Local Group = SBM_local_group
Organization AD Group(s) = Users_Group_SBM
Configuring the Check Point SandBlast Mobile Dashboard Integration Settings

Assign the app to the selected groups of users or devices.

Note - For easy reference during configuration, you can record your settings in the special table (See Integration Information).

Prerequisites

You need these details from your Citrix Endpoint Management Deployment:

- **Server**: The URL of your Citrix Endpoint Management System. Usually the same as the Citrix Endpoint Management Console.
  

- **Citrix Endpoint Management 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)" for this purpose.

  Example: \textit{API Admin Username/Password = Admin_User/<hidden>}

  The credentials that the SandBlast Mobile Dashboard uses to connect to Citrix Endpoint Management.

- **Organization Local Group(s)**: This is the Citrix Endpoint Management locally defined groups where 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 (;).

  \textit{Example: Delivery Group = SBM\_local\_group}

- **Organization AD Group(s)**: This is the Citrix Endpoint Management AD groups where 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 (;).

  \textit{Example: Delivery Group = Users\_Group\_SBM}

- **Mittigation Attribute**: This field will not be used as we will be using the CHKP Risk and Status tags.
- **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 Endpoint Management.

- **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 Endpoint Management.

- **For On-Premise UEM Environment**, 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.

**Notes** - Before you start, delete any existing devices in the SandBlast Mobile Dashboard. Only the devices are synchronized from the UEM to the SandBlast Mobile Dashboard, not users.
Configuring Integration Settings

After you complete the necessary steps, the **Device Management** pane shows the detailed status of the settings.

**Procedure**

1. From the Infinity Portal, go to **Settings > Device Management**.

   The **Device Management** page opens.

2. Click **Edit** or “**No UEM configured, to start click here**”

   The Integration Wizard opens.

   Example:
Server Setup

Configure your UEM to integrate with the created Citrix Endpoint Management devices:

a. In Server Setup section, enter this information:
   - UEM service – Citrix Endpoint Management
   - Server Address - The full URL needed for the UEM service
   - User name
   - Password
   - Connector Setup (advanced)
Example:

![Citrix XenMobile INTEGRATION](image)

**Connector Setup**

You can configure SandBlast Connector when the UEM has no direct access from the SandBlast Mobile cloud. For more information see *Sandblast Mobile Connector Integration Guide* in the Check Point Support Download center.
Example:

![Citrix XenMobile Integration](image)

b. Click **Next**.

- **Synchronization Configuration**

  Configure the devices and groups that you synchronize with SandBlast Mobile Dashboard.

  a. In the **Group(s)** field:

     i. Click **Group(s)**.

     A dropdown with list of the available groups opens.

     ii. Select the group(s) you need for integration with Citrix Endpoint Management.
Example:

b. In the **Android Enterprise Deployment** field:

Select the groups for two deployed applications as part of the Citrix Endpoint Management Android Enterprise deployment. See *Using Android Enterprise with SandBlast Mobile*. 
Example:

**Citrix XenMobile INTEGRATION**

- **SERVER SETUP**
- **SYNCHRONIZATION CONFIGURATION**
- **TAGGING CONFIGURATION**
- **DEPLOYMENT**

**Synchronization Configuration**

- **Group(s)**
  - SBM_local_group

**Android Enterprise Deployment**

**Work & Personal deployment**

**Advanced**

- In the **Advanced** section:
  1. Import Personally Identifiable Information (PII) and set the synchronization intervals.

You can limit the import of the PII devices (users) to SandBlast Mobile.
d. Click Next.

![Example: Citrix XenMobile Integration](image)

**Note** - If all entries are OFF, the placeholder information set for the email address is placed in the Sandblast mobile dashboard’s Device Owner’s Email, in form of "UEMDevice UDID@vendor.mdm".
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device sync interval</td>
<td>Interval to connect with UEM to sync devices.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
<tr>
<td>Device deletion threshold</td>
<td>Devices for deletion after UEM device sync (in %).</td>
<td>100% for no threshold.</td>
</tr>
<tr>
<td>Deletion delay interval</td>
<td>Delay device deletion after sync – device is not deleted if it is re-synchronized from UEM during the threshold interval.</td>
<td></td>
</tr>
<tr>
<td>App sync interval</td>
<td>Interval to connect with UEM to sync applications.</td>
<td>10-1440 minutes, in 10 minute intervals.</td>
</tr>
</tbody>
</table>

- **Tagging Configuration**

Specify the information sent to Citrix Endpoint Management and the risk level of the device.

The tagging configuration will be synced to Citrix Endpoint Management and will be used in setting device risk status.

a. In **Tagging** Section:

   i. **Set Tag device status to ON.**
      For integration with Citrix Endpoint Management, 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.

   ii. **Set Tag device risk to ON.**
      For integration with Citrix Endpoint Management, 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.

   iii. **Set Tag device threat factor to ON.**
      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.
Example:

b. In **Advanced** section:

**Mitigation attribute**: This field will not be used as we will be using the CHKP_Risk and Status tags.

b. Click **Next**.
Example:

Citrix XenMobile | INTEGRATION

- Tagging Configuration
  - Tag device status
  - Tag device risk
  - Tag device TF

Advanced
Mitigation attribute

Next
Finish
- **Deployment**

  Specify the deployment status of a device.

  **Note** - This section is optional, because MobileIron Core manages the deployment automatically.

  Example:
If you use SandBlast Mobile to manage the deployment:

In the Advanced section:

a. Enable options to send email and/or SMS notification to the new users with instructions to download and install the SandBlast Mobile Protect app.
b. Click Finish.

Example:
View the **Integration Status** (In the Infinity Portal, **Settings > Device Management**).

The **Device Management** pane shows this information:

- **Server** – The latest server configuration status.
- **Synchronization** – The synchronized groups and the sync status.
  - **Device Sync** – The synced labels from MobileIron Core
  - **App Sync** – The last type applications were fetched from the UEM (For iOS deployments only).
- **Tagging** – Tagging Configuration and Tagging Status.
- **Deployment** – Deployment Configuration and Deployment Status.

Example:

![Integration Status Screenshot]

Click **Edit** in each section to edit the settings.
Configuring UEM to Deploy the SandBlast Mobile Protect app

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

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

General Workflow

1. Add the SandBlast Mobile Protect App to your App Catalog. See Adding the SandBlast Mobile Protect App to Your App Catalog.
2. Add an iOS Configuration Policy for SandBlast Mobile. See Adding an iOS Configuration Policy for SandBlast Mobile Protect.
4. Require the SandBlast Mobile Protect app to be installed on your mobile. See Requiring the SandBlast Mobile Protect app to be Installed”.

Configuring UEM to Deploy SandBlast Mobile Protect app

Prerequisites

SandBlast Mobile Gateway/Server – gw.locsec.net.
Adding the SandBlast Mobile Protect App to Your App Catalog

In this process we will be using the CHKP_Status tag.

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 in a Name for the app: "SandBlast Mobile Protect".

4. In the Platform pane select "iPhone", "iPad", "Android (legacy DA)" and "Android Enterprise".
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 on the "Advanced" tab.
11. Click on "New Rule" tab at the bottom.

12. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Provisioned".

13. Click "+" sign.

14. Click on the "OR" word and the "New Rule" button will be active again.
15. Click "New Rule".

16. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Active".

17. Click "+" sign.
18. Click "New Rule".

19. Select "Limit by raw device property name" with "CHKP_Status" is equal to "Inactive".

20. Click "+" sign.

21. Once all the Deployment Rules are listed as they are below, click "Next".
22. On the **iPad Platform** tab, select the SandBlast Mobile Protect app, and scroll down to "Deployment Rules".
23. Repeat the above steps as with the iPhone platform for the iPad platform as well as below:

![Deployment Rules](image1)

24. Once all the Deployment Rules are listed as they are above, click "Next".

25. On the **Android Enterprise Platform** tab, enter in "SandBlast Mobile Protect" and click **"Search"**.

26. Select the SandBlast Mobile Protect app shown in the search result window, such as in the example below:

![Managed Google Play Store](image2)
27. Click on the SandBlast Mobile Protect app.

28. Scroll down to "Deployment Rules".
29. Repeat the steps above for the **Android Enterprise Platform** as well and create 3 new rules as below.

30. Once all the Deployment Rules are listed as they are below, click "Next".

31. Repeat the steps above for the **Android (Legacy DA)** as well and create 3 new rules as below
32. Once all the Deployment Rules are listed as they are below, click "Next".

33. On the Approval (optional) tab click "Next".
34. On the "Delivery Group Assignments" tab, select the Delivery Group you created in "Creating a Delivery Group".

35. Click on the "Deployment Schedule" section toggle the "Deploy for always-on connection" button to be ON.

36. Click "Save".
Get dashboard's token
Go to your SandBlast Mobile dashboard > Settings > Device Management > Deployment > Edit:

Copy the token of your dashboard:
Adding Android Enterprise Managed Configurations

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


3. On the Security option choose "Android Enterprise Managed Configurations".

4. On the "Select Application ID" pop up window select the "SandBlast Mobile Protect" app and click "OK".
5. On the Policy Info pane enter in a policy name "AE Protect Configuration" and click "Next".
6. On the **Android Enterprise** pane enter in the configurations as described below (See example) and click "Next":

<table>
<thead>
<tr>
<th>Item</th>
<th>Value Type</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI</td>
<td>String</td>
<td>$device.imei</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>Take the copied value from the previous section</td>
</tr>
</tbody>
</table>

Example:
7. Under Assignment tab, assign the configuration to your group and 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. Scroll down to **Apps** section and select "**App Configuration**".

3. On the Policy Info nter in a Policy Name “iOS Protect Configuration" and click "Next".
4. Select "iOS" only from Platforms, and select "Add new" for "Identifier".
5. On the box appeared under the "Identifier" enter "com.checkpoint.capsuleprotect".

6. In the "Dictionary content" field copy and Paste the following text:

```xml
<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>USER_ID</key>
  <string>${USER_ID}</string>
  <key>Lacoon Server Address</key>
  <string>gw.locsec.net</string>
  <key>token</key>
  <string>hash_tenant_id</string>
  <key>DEVICE_UDID</key>
  <string>${device.id}</string>
</dict>
```
Change the `<string>hash_tenant_id</string>` content (i.e. instead of “hash_tenant_id” text) from the previous section.
7. Click "Check Dictionary" to make sure that there are no errors. If no error found a "Valid XML" label should appear.

8. Click "Next".

9. On the Assignment tab, select the Delivery Group you created in "Creating a Delivery Group".

10. In "Deployment Schedule" toggle the "Deploy for always-on connections" button to be ON.

11. 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. Scroll down to Apps section and select "App Inventory".
3. On the Policy Info pane enter a Policy Name "Collect iOS App Inventory" and Click "Next".

4. On the Platforms pane select "iOS" only and make sure the "iOS" button toggled to be ON.

5. Click "Next".
6. On the Assignment tab, select the Delivery Group you created in *Creating a Delivery Group*.

7. In the Deployment Schedule select "Deploy for always-on connections" button to be ON.

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**.

2. Select the Delivery Group you created in "Creating a Delivery Group" and click "Edit".
3. Select the **Apps** tab.

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

6. The app adds to the "Required Apps" list as below:

7. Scroll down to "Summary" tab.
8. On the **Summary** tab, make sure the app 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 Endpoint Management system to identify which devices are at risk and to enforce actions and policies based on risk level.

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

**Notes**

- Device Properties are controlled by the device in that if a device property is set/configured at the Citrix Endpoint Management Console, the device must sync to Citrix Endpoint Management 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 Citrix Endpoint Management system. This is not a shortcoming of SandBlast Mobile; it is how Citrix Endpoint Management 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.

- 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".

![Device Policies](image-url)
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.**

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. Scroll down to "Policy Settings" and set "Remove Policy" to "Select Date" and choose a date.

7. Click "Next".

8. On the Android screen, follow the instructions below:
   a. Enter in a Lock message that will be displayed to the user.
   b. Set "Prevent uninstall" to "ON".
c. Enforce "Blacklist".

d. On the "Apps" section click "Add", and select "Add new".

e. 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", in our example: **Users_Group_SBM**

11. Also, under Deployment Schedule, toggle the button **"Deploy for always-on connections"** to be **ON**.

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. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "is"
e. On "Enter a String" enter in "High".

5. Select an Action as follows:
   a. On "Select an action" select "Send notification"
   b. On "Select a template" 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",
in our example: Users_Group_SBM

8. Also, under Deployment Schedule, toggle the button "Deploy for always-on connections" to be **ON**.

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".

   ![Endpoint Management Configure Actions](image)

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

   ![Endpoint Management Configure Actions Action Info](image)

3. Click "Next".

4. On the Details screen, select a trigger as follows:
   a. Select "Device property"
   b. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "is"
e. On "Enter a String" 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", in our example: Users_Group_SBM

8. Also, under Deployment Schedule, toggle the button "Deploy for always-on connections" to be ON.
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 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. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "is"
   e. On "Enter a String" enter in "High".

2. Select an Action as follows:

   a. Select "App Lock"
   b. Set to "0" Hours (for immediately)

5. Click "**Next**".
6. On the Assignment screen, select the Delivery Group you created in "Creating a Delivery Group", in our example: Users_Group_SBM

7. Also, under Deployment Schedule, toggle the button "Deploy for always-on connections" to be ON.

8. Click "Next".

9. 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 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. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "is"
   e. On "Enter a String" enter in "High".
5. Select an Action as follows:
   
a. On "Select an action" select "Send notification"
b. On "Select a template" 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", in our example: Users_Group_SBM
8. Also, under Deployment Schedule, toggle the button "Deploy for always-on connections" to be **ON**.

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. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "is"
   e. On "Enter a String" 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", in our example: *Users_Group_SB*M

8. Also, under Deployment Schedule, toggle the button "**Deploy for always-on connections**" to be **ON**.

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. On "Select a Device Property" select "Other"
   c. On "Enter a property name" enter in "CHKP_Risk"
   d. Select "Is Not"
   e. On "Enter a String" 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", in our example: Users_Group_SBM

8. Also, under Deployment Schedule, toggle the button "Deploy for always-on connections" to be ON.

9. Click "Next".
10. On the Summary screen, click "Save"

11. The Actions screen will show something like this:

   ![Actions Screen Screenshot]

   **Note** - Now any device in the Delivery Group ("Users_Group_SBM") 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.
Using Android Enterprise with SandBlast Mobile

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 more information, see here.

For example, through one or more API(s) your UEM platform can disable a camera, Bluetooth, or prevent an access to system settings.

For information about configuring Android Enterprise on your device, see citrix AE guide here.

Profiles

Single profile configuration is supported out-of-the-box. No additional setup is needed.

In the Work / Personal Profile, the Administrator registers and sees the protected part of the device.

Note - If you protect only part(s) of the device, you must limit the SandBlast Mobile on your UEM to only Work or only Personal.

Android Enterprise Deployment Scenarios

Android Enterprise supports these deployment scenarios:

- Company-owned fully managed devices (COBO)
- Company-owned fully managed devices with a work profile (COPE)
- Company-owned devices for dedicated use (COSU)
- Employee-owned devices (BYOD)

COBO and COSU devices have a single profile. Follow integration guide instructions for Android Enterprise devices to deploy SandBlast Mobile Protect app on your devices. For more information, see the Android Enterprise online guide.

COPE and BYOD devices have Work and Personal profiles. With SandBlast Mobile Protect app you can protect one profile or both profiles.

For the highest protection level we recommend to protect both Work and Personal Profiles. See Configuring SandBlast Mobile Protect app to Protect your Devices.
Configuring SandBlast Mobile Protect app to Protect your Devices

Note - The deployment of the SandBlast Mobile Protect app on the Personal profile of BYOD device cannot be automated by Android design (Personal profile of BYUD device is not managed).

With the Android Enterprise, you can protect the whole device or part(s) of it.

If you protect the whole device, install the SandBlast Mobile Protect app to both Work and Personal Profiles.

Note - If you protect only the Personal profile, skip this section.

Deploying Android Enterprise on your Devices

With the Android Enterprise, you can protect the whole device or part(s) of it.

If you protect the whole device, install the SandBlast Mobile Protect app to both Work and Personal Profiles.

To protect the whole device:

1. On the SandBlast Mobile Dashboard, go to Settings > Device Management.
2. Enable the SandBlast Mobile Protect app (for both profiles).

   - For a new UEM configurations:
     a. Go to Settings > Device Management > UEM service and select the UEM type.
     b. In the configuration prompt select the groups for synchronization.
     c. In the Android Enterprise Deployment section select and add the device groups for both profiles.

   - For existing UEM configurations:
     a. Go to Settings > Device Management > Edit Settings.
b. In the **Android Enterprise Deployment** section select and add the device groups for both profiles.

Example:

![Android Enterprise Deployment](image)

- If you add a group of devices for Android Enterprise deployment, make sure to configure the devices with both Personal and Work profiles.
- If you remove a group of devices from the Android Enterprise deployment, the SandBlast Mobile Protect app deletes the Personal profile record on every device in this group.
- iOS devices are ignored in the Android Enterprise context.

**Note** - If a device belongs to more than one group, one group selected in Android Enterprise deployment, and one group is not selected, the deployment is both Work and Personal.

3. Click **Finish**.
4. (Optional) Send an email or SMS to all the users with installation instructions.
5. Click **Sync Now** to fetch the data from the UEM.

**General View on the Check Point Dashboard (Example):**

![Check Point Dashboard](image)
To view and filter the devices:

1. On the SandBlast Mobile Dashboard, go to Devices > Groups > Devices.

   Example:

   ![Device List](image)

2. In the **Device Type** column, filter the devices in the list according to their protection profile.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Icon</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>![Work Icon]</td>
<td>Device Type &lt;br&gt; OS - Android Enterprise</td>
</tr>
<tr>
<td>Personal</td>
<td>![Personal Icon]</td>
<td>Device Type &lt;br&gt; OS - Android</td>
</tr>
</tbody>
</table>

**Policies**

To change policy for inactive personal profile:


   Example:

   ![Policy Settings](image)
2. From the drop-down list, select a policy.

Example:

<table>
<thead>
<tr>
<th>Android Enterprise Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change device risk level to: <strong>High (Device Alert)</strong> - if Sandblast Mobile on personal profile is not active</td>
</tr>
</tbody>
</table>

**Risk Handling**

- If the SandBlast Mobile protection is inactive on the Personal profile, the risk level is raised according to the Android Enterprise Security Settings policy on the Work profile.

Example:

![Device Threat Notification](image)

- If the Personal profile has the High Risk status, the risk level is raised to **High** on the Work profile. The SandBlast Mobile informs the user that the personal profile is at risk.
Example:

- You can enable mitigation by UEM on the personal profile, if you tag a risk on the work profile.
Applying the SandBlast Mobile Protect app Configuration and Policy Enforcement

Deploying the SandBlast Mobile Protect app on the Devices

**Note** - It can take up to 10 minutes for MobileIron Core to sync with the SandBlast Mobile Dashboard, and several more minutes for MobileIron Core to push the App to the user device.

Registration of an iOS Device

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

**Procedure for the User:**

1. Register your device.
   a. Tap **INSTALL** on the SandBlast Mobile Protect app.

      The Protect app is deployed on the iOS Device.
   b. Launch the Protect app to finish the registration.

      MobileIron Core system automatically configures the registration server and the key in the Protect app.
   c. Follow the on-screen instructions to enable Notifications, Location, and Network Security.
Example:

d. Tap **Allow** to allow SandBlast Mobile Protect app to add the needed VPN Configuration profile, when On-device Network protection is enabled.

**Registration of an Android Device**

a. Tap on the SandBlast Mobile Protect app in the Google Play Store.

b. Tap **Install > Accept** on the SandBlast Mobile Protect app to accept the permissions of the App.

Example:
The App is installed.

c. Launch the App to finish its deployment and registration to Check Point SandBlast Mobile.

The SandBlast Mobile Protect app is automatically registered.

Example:

d. Tap Continue

e. Enable security settings **Allow all required permissions**

f. Tap **Enable**
2. The SandBlast Mobile Protect app scans the system. See the state of the device on the display.

Example:

**iOS Devices**

![iOS Device Screen](image1)

**Android Devices**

![Android Device Screen](image2)
Testing High Risk Activity Detection and Policy Enforcement

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 CHKP_Risk tag to the Citrix Endpoint Management system for that device.

Citrix Endpoint Management 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 CHKP_Risk to High to the Citrix Endpoint Management system. The Citrix Endpoint Management system will then enforce policy actions specified in the policies/actions. This mitigation process was the one we created in "Creating a Mitigation Process".
Blacklisting a Test App

1. Log into the SandBlast Mobile Dashboard.
2. Go to **App Analysis** tab and select for the app you wish to blacklist.
3. Select the app you wish to blacklist on the left-side list.
4. On the **Policy** section, click the **Edit** link.

5. On the **Changing Application Policy – Global** window, configure these settings:
   a. From the **New Policy** drop-down menu - select **Black Listed**.
   b. In the **Audit Trail note** field - enter a reason for this change.

   Example:
6. Click **OK**.

The user receives a SandBlast Mobile Protect app notification to indicate that the blacklisted app (for example, Waze) is not allowed by the Corporate Policy.

---

**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 "Waze".

---

**Citrix Endpoint Management In-App Notification**

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

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

Administrator View on the SandBlast Mobile Dashboard

On the SandBlast Mobile Dashboard the Administrator can see the devices at High Risk.

1. On the Infinity Portal, go to Device Risk > High Risk section.
A list of the Devices At Risk is displayed in the **Device Risk** section.

Example:

2. Click **High Risk**.
   
The list of devices at High Risk state is displayed.

3. Select the specified device on the left-side list.
   
You can see that the blacklisted app causes the High Risk state.

Example:
Administrator View on the Citrix Endpoint Management Console

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

2. In the Citrix Endpoint Management 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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Management Server/API URL</td>
<td></td>
</tr>
<tr>
<td>Endpoint Management API Admin Username</td>
<td></td>
</tr>
<tr>
<td>Endpoint Management API Admin Password</td>
<td></td>
</tr>
<tr>
<td>Endpoint Management Local Group(s)</td>
<td></td>
</tr>
<tr>
<td>Endpoint Management AD Group(s)</td>
<td></td>
</tr>
<tr>
<td>Endpoint Management Mitigation attribute (Device Property) (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>