26 May 2020

SandBlast Mobile for IBM MaaS360

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**

- General Workflow ................................................................. 5

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

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

**Preparing UEM Platform for Integration** .......................................................... 10

- Prerequisites ............................................................................. 10
- General Workflow .................................................................. 11
- Creating an API Only Administrator Account (optional) .................. 11
  - Create a New API Only Administrator Role ................................. 12
  - Create a New Administrator Account ........................................... 15
- Adding a User ........................................................................... 21
  - Adding a Device While Adding the User ................................... 23
- Creating a User Groups ................................................................. 25
  - Creating a User Group ............................................................... 25
  - Adding an Existing User to a User Group ................................... 26
  - Adding a New User to an Existing User Group ......................... 28
  - Adding a Device While Adding the User ................................... 30
- Creating a Device Provisioning Group .............................................. 31
  - Creating a Simple Device Provisioning Group ............................ 32
  - Creating a Specific Device Provisioning Group ........................... 34
- Adding a Device to an Existing User .............................................. 36
  - Enrolling an iOS Device to MaaS360 ........................................ 39
  - Enrolling an Android Device to MaaS360 ................................... 43
- Creating a Mitigation Process ......................................................... 45
  - Creating a Mitigation Label ....................................................... 45
  - Creating a Device Mitigation Group .......................................... 46
- Creating Compliance Policies .......................................................... 48
Creating Compliance Actions for iOS Devices (Policy) ........................................ 49
Creating Compliance Actions for Android Devices (Policy) ........................................ 53
Configuring the Check Point SandBlast Mobile Dashboard Integration Settings........ 63
Prerequisites ........................................................................................................ 63
Configuring UEM Integration Settings .................................................................. 65
Configuring UEM to Deploy SandBlast Mobile Protect app ............................... 75
Prerequisites ........................................................................................................ 75
Adding the SandBlast Mobile Protect App to Your App Catalog......................... 75
Get dashboard’s token .......................................................................................... 76
iOS App – Add to Catalog ...................................................................................... 78
Android Enterprise App – Add to Catalog ............................................................. 80
Deploying SandBlast Mobile Protect app ............................................................... 83
Setting Policy to Require SandBlast Mobile Protect to be installed ..................... 85
Creating Compliance Actions for iOS Devices (Policy) ........................................ 85
Creating Compliance Actions for Android Devices (Policy) ............................... 88
Applying App Required Policy to Device Provisioning Group ............................. 91
Using Android Enterprise with SandBlast Mobile ............................................. 94
Profiles ................................................................................................................ 94
Deploying Android Enterprise on your Devices ..................................................... 94
Policies ................................................................................................................ 96
Risk Handling ...................................................................................................... 97
Deploying SandBlast Mobile Protect App to the Devices ......................... 99
Registration of an iOS Device ............................................................................... 99
Registration of an Android Device ...................................................................... 100
Testing High Risk Activity Detection and Policy Enforcement ..................... 103
Blacklisting a Test App ......................................................................................... 104
View of Non-Compliant Device .......................................................................... 105
Administrator View on the SandBlast Mobile Dashboard .................................. 108
Administrator View on the MaaS360 Portal ...................................................... 109
Appendices ......................................................................................................... 113
Integration Information ......................................................................................... 113
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 IBM MaaS360 UEM. It provides a quick tour through the interface of the IBM MaaS360 Portal 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 IBM MaaS360 UEM platform for the Check Point SandBlast Mobile Protect app integration. See "Preparing UEM Platform for Integration".
2. Configure your IBM MaaS360 UEM to deploy the Check Point SandBlast Mobile Protect app. See "Configuring UEM to Deploy SandBlast Mobile Protect app".
3. Configure the Check Point SandBlast Mobile Dashboard for integration with the IBM MaaS360 UEM. 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 IBM MaaS360 devices. See "Deploying SandBlast Mobile Protect App to the Devices".
5. Test the Check Point SandBlast Mobile Protect app on your protected IBM MaaS360 devices. See "Testing High Risk Activity Detection 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

### Component Description

<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 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>
| **4** 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. |
| **5** 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. |
| **6** 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

IBM MaaS360 deploys SandBlast Mobile Protect app on a device.

Prerequisites

- SandBlast Mobile service integrates with IBM MaaS360 through the existing API. To enable integration, you must first create an IBM MaaS360 API account.

  SandBlast Mobile integrates with **IBM MaaS360** (On-Premise) and IBM MaaS360 is version 10.0 or later with REST API access enabled. For On-premise MaaS360 Deployments, the port used for the API must be accessible remotely through your firewall before trying to connect.

  SandBlast Mobile uses the API to synchronize the device records, to retrieve device apps list, and to report the device risk level to IBM MaaS360.

MaaS360 Portal (Example):

1. Login to your MaaS360 Portal:
Note - During the procedures in this document there are quite a few pieces of information that you will need to gather or create. There is a form in the section Integration Information that you can record your settings for easy reference.

General Workflow

1. Create an API Only Administrator Account (optional). See "Creating an API Only Administrator Account (optional)"
2. Add a new user. See "Adding a User"
3. Create a Security Group for Check Point SandBlast Mobile Protect app. See "Creating a Device Provisioning Group"
4. Add a device to an existing user. See "Adding a Device to an Existing User"
5. Create Mitigation Label and Compliance Policies that will be enforced on devices that are at High Risk. See "Creating a Mitigation Process"

Creating an API Only Administrator Account (optional)

For the interaction at the API, we will create an API admin user in the MaaS360 Portal that you use to limit the capability of the admin credentials used between the SandBlast Mobile Dashboard and the MaaS360 system.

Best Practice - It is a best practice to create such an admin account and highly recommended, but is optional. Creating an administrator account and administrator role requires a “Services Administrator” level role.

To create an “API” Administrator Account, follow the process below:
Create a New API Only Administrator Role

2. Navigate to Setup > Portal Administration > Roles.

3. Click “Add Role” button.

4. Enter in a Role Name, such as “Admin_Api”, and a description.

5. In “Select Mode Creation” select the “Create New” radio button.

6. Click Next.
7. On the “Grant Access Rights” screen, scroll down the list and select the following additional access rights for the new role:

   a) Device View – Read-only
   b) Device View – View All Devices
   c) Set Custom Attribute Value
8. Click **Save**.

9. Type your admin password, and then click the “**Confirm**” button.

10. A confirmation message is displayed as below:
Create a New Administrator Account

1. Navigate to **Setup > Portal Administration > Administrators**.

2. Click “Add Administrator”.

3. On the Administrator Details window, select Authenticate Using **"MaaS360 Local Credentials"**.
4. Fill in the email address and the user name for the new administrator.
5. If the user name is the same as the email address, select the **same as Corporate Email Address** checkbox. In our example, we will create an admin username of
6. Click **Next**.

7. On the **Assign Roles** window, select the Role created in the previous section (2.3.1), in our example “Admin_Api”.

8. Click on the arrow button to add the desired role and click **Next**.
9. On the “Review Details” window, review to ensure the configuration is appropriate.

10. Click Save.

11. Type your admin password, and then click the “Confirm” button.
12. A confirmation message is displayed:

13. Finish the creation of the new admin account by logging out of the MaaS360 portal, and then logging back in using the credentials sent to the email address used for mp_api_admin. This will force you to select a new unique password.

14. Log into MaaS360 Portal with the above credentials.
15. You are then prompted to select a new password. Enter a password that satisfies the password rules.

16. Click Save.

17. Enter in a First Name, Last Name, and Contact Phone Number in the “Add Personal Information” form.

18. Click Save.
**Note** - Log out and log back into the MaaS360 Portal with your Service Administrator credentials to continue with the configuration.
Adding a User

There are two ways to add a user, “Add User”, or sync with a corporate user directory.

**Note** - Use the Cloud Extender or Azure AD Integration to integrate with your Corporate User Directory to import group and associated user information. Cloud Extender is available for download on the Services enablement workflow. Azure AD Integration is available as part of Enterprise Integration. Imported information can be used for automatic provisioning of users, group based policy assignment and App & Doc distribution. Supported User Directories for Cloud Extender are Active Directory, OpenLDAP, Novell LDAP, IBM Domino LDAP and Oracle User Directory.

We are going to show how to add a local user using the “Add User” method:

1. Navigate to **Users > Directory**.

2. Click the **Add User** button.

3. On the **Add User** pop-up window, on the **Basic** tab, fill in all the required (*) fields with the appropriate information, such as in the example below.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>Dana Scully</td>
</tr>
<tr>
<td>Username</td>
<td>dscully</td>
</tr>
<tr>
<td>Domain</td>
<td>cptime.us</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:dscully@cptime.us">dscully@cptime.us</a></td>
</tr>
</tbody>
</table>

**Note** - You can either add a new device right now by following the instructions in the next section, or you can click the “Save” button now, and add a new device later using the instructions in section *Adding a Device to an Existing User.*
Adding a Device While Adding the User

1. To add a new device to this new user, select “Add New Device” checkbox, and select the “Notify User” method.

2. On the “Add User” pop-up window, click the “Advanced” tab.
3. On the “Advanced” tab, under “Platform”, select “iOS” or “Android”, and under the “Device Ownership”, select “Corporate” or “Employee Owned”.
4. Click Save.
5. Enter in your admin password and click "Confirm" button.

6. The system will pop-up a success message with the enrollment details sent to the user.

7. Click the “OK” button.
Creating a User Groups

To create a group of users whose devices will be registered to the SandBlast Mobile solution, follow this procedure. Although this can be an optional step, it is used in the creation of the dynamic Device Provisioning Group in the next section *Creating a Simple Device Provisioning Group*.

Creating a User Group

1. Navigate to **Users > Groups**.

2. Click the “Add” drop-down button, and select “Local User Group”.

3. On the “Add Local User Group” pop-up window, enter a Name, such as “MP_Users_Group”, and, if desired, a Description.
4. Click Save.

**Add Local User Group**

Note:
User Groups can be used for assigning policies and distributing Apps & Docs. To manage Groups and take actions on them, use the “Groups” workflow.

Name: MP_Users_Group

Usernames (or Email Addresses): Enter a few characters for username or email

Description: Check Point SandBlast Mobile users

User group to be available for:
- [ ] Security (Policies, Compliance Rules, Locations and Privacy Settings)
- [ ] App distribution
- [ ] Doc distribution
- [ ] Administrative access control

5. Click the “OK” button on the pop up window.

**Add Local User Group**

The User Group has been added successfully. You can manage this and issue Group Actions using the “Groups” workflow.

OK

Adding an Existing User to a User Group

To add an existing user to the User Group we created in the previous section *Creating a User Groups*, follow this procedure.

1. Navigate to Users > Directory, scroll to the user you want to add to a user group, and click the “View” link.
2. Click the “Add Group” button.

3. In the “Add Group” pop-up window, start typing the User Group you want to add the user to and select the appropriate group from the list, in our example “MP_Users_Group”.

4. Click the “Save” button.

5. Enter in your admin password, and click the “Confirm” button.

6. The User is now part of the User Group.
Adding a New User to an Existing User Group

Adding a new user to an existing user group is similar to the procedure in section Adding a User.

1. Navigate to Users > Groups, under the User Group you created in section Creating a User Groups, in our example “MP_Users_Group” click the “Users” link.

2. Click the “Add User” button.

3. On the “Add User” pop-up window “Basic” tab, fill in all the required (*) fields with the appropriate information, such as in the example below.
4. Also, enter in the user group in the “Users Groups” field, in our example “MP_Users_Group”
Adding a Device While Adding the User

1. To add a new device to this new user, select “Add New Device” checkbox, and select the “Notify User” method.

![Device Configuration Form]

2. On the “Add User” pop-up window, click the “Advanced” tab.

3. On the “Advanced” tab, under “Platform & MDM Policy”, select “iOS” or “Android”, and under the “Device Ownership” select “Corporate” or “Employee Owned”.

4. Click the “Save” button.
5. The system will pop-up a success message with the enrollment details sent to the user.
6. Click the “OK” button.

Creating a Device Provisioning Group

A device provisioning group is used to tie devices, apps, and app configurations together for deployment. Maas360 calls a device provisioning group a “device group”. This group will be used in the SandBlast Mobile Protect app deployment process discussed in Section "Configuring UEM to Deploy SandBlast Mobile Protect app".
Creating a Simple Device Provisioning Group

1. Navigate to Devices > Groups.

2. Click the “Add” drop-down button, and select “Device Group”.

3. On the “Advanced Search” screen, you will need to build a query that will group all devices matching the criteria into the device group.
   In our example, in “Condition 1” we will group all the devices assigned to all “Users” in the “Managed User Groups” that are “Equal To” the User Group we created in the previous section, in our example “MP_Users_Group”.

4. Click the “Search” button.
5. Click the “Create New Device Group” button.

6. On the “Device Group Details” pop-up window, enter a Group Name, such as “MP_Devices_Group”, and if desired, a Description.

7. Click the “Save” button.
Creating a Specific Device Provisioning Group

1. Navigate to **Devices > Groups**.

2. Click the “Add” drop-down button, and select “**Device Group**”.

3. On the “**Advanced Search**” screen, you will need to build a query that will group all devices matching the criteria into the device group. In our example, we will chose the following Conditions:
a. Change the “Search Criteria” to “Across Conditions (Advanced)” with the formula of “1 AND (2 OR 3)”

b. Users > Managed User Groups > Equal To > MP_Users_Group

c. Operating System > OS Name > Contains > iOS

d. Operating System > OS Name > Contains > Android

4. These criteria will match all iOS or Android devices belonging to the users that belong to the user group “MP_Users_Group”.

5. Click the “Search” button.

6. Click the “Create New Device Group” button.

7. On the “Device Group Details” pop-up window, enter a Group Name, such as “MP_Devices_Group”, and if desired, a Description.
8. Click the “Save” button.

Adding a Device to an Existing User

1. You can add a device to an existing user by navigating to Users > Directory.

2. Scroll to or search for the user to add a device to, and click the “Add Device” link.

3. On the “Add Device” pop-up window “Basic” tab, select the “Notify User” method.
4. Click the “Advanced” tab.

5. On the “Add Device” pop-up window “Advanced” tab, under “Platform & MDM Policy” select “iOS” or “Android”, and under “Device Ownership” select “Corporate” or “Employee Owned”.

6. Click the “Send Request” button.

7. Enter in your admin password and click "Confirm" button.
8. The system will pop-up a success message with the enrollment details sent to the user.

9. Click the “OK” button.

Note - Repeat these steps to add another device.
Enrolling an iOS Device to MaaS360

1. The user will receive an enrollment email from the MaaS360 system.

   ![Device Enrollment Request Image]

   - To ensure timely and successful delivery of email from MaaS360, add maas360@checkpoint.com to your address book.
   - Your IT administrator has requested you to enroll your iOS device with MaaS360. This will enable you to access the corporate resources from your iOS device. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.
   - To enroll your device, open the following URL in your iOS device browser and enter the enrollment passcode mentioned below.
   - Note: If you are enrolling an iOS device or Mac, use Safari browser to open the URL. If you are enrolling an Android device, use the OS native browser or Chrome. If you are enrolling a Windows Phone or Windows device, use IE or Edge browser.
   - [Device Enrollment URL]
     - Username: dosuly111
     - Password: n2567he
   - If prompted for your corporate identifier and email address, use the following:
     - Corporate Identifier: 123456789
     - Domain: example.com
     - Email Address: dosuly111@example.com
     - Platform: iOS
   - MaaS360 will guide you through the steps required to enroll your device.
   - [Enrollment Process Image]

   - If you haven’t received this email on your iOS device, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use your iOS device camera to capture the QR code displayed below and open the URL on your iOS device.

2. The user will open the “Device Enrollment URL” link in their device’s browser.
3. The user will be prompted to enter the passcode they received in the Device Enrollment Request email, and tapping the “Install” button.
4. The user will be prompted to continue with the steps by tapping the “Continue” button.
5. The user will be prompted to accept the “Terms of Use” by selecting the “I have read and accept the terms” checkbox, and tapping the “Continue” button.
6. The user is then prompted to continue with installing the MaaS360 UEM profile by downloading the profile.
Note - If there is already a device management profile installed, the user must uninstall the existing profile and then continue with the MaaS360 UEM profile installation.

7. The user must tap “Allow” through this procedure.
8. Once the profile is installed, the user will be prompted to install the MaaS360 app.

9. After the MaaS360 app is installed, the user must launch the app and "Agree and Continue" the enrollment process.
10. The device has been successfully enrolled to the MaaS360 system.
Enrolling an Android Device to MaaS360

1. The user will receive an enrollment email from the MaaS360 system.

2. The user will open the MaaS360 link in their device’s browser. This will prompt the user to go to the Google Play Store to download/install the MaaS360 app.
3. Once the MaaS360 app is installed, the user must launch the app to continue the enrollment process.

4. The user is prompted for the Corporate Identifier as provided in the email and their email address.

5. The user must accept the Terms of Use, and Activate the MaaS360 app to be a device administrator.

6. After the setup is finished, the device has been successfully enrolled to the MaaS360 system.
Creating a Mitigation Process

In this procedure, you will create a mitigation label that the SandBlast Mobile Dashboard will use to label any device in High Risk as determined by the SandBlast Mobile Analysis. This label will allow the MaaS360 system to identify which devices are at High Risk and to enforce configured compliance and mitigation policies against those devices.

Creating a Mitigation Label

In MaaS360 the mitigation label is called a custom device attribute. This section describes how to create the custom device attribute, and the next section Creating a Device Mitigation Group will use this custom attribute to create a device mitigation group on which compliance and mitigation policies can be applied.

1. Navigate to Devices > Device Attributes.

2. Click the “Manage Custom Attributes” button.

3. Click the “Add Custom Attribute” button.
4. On the “Add Custom Attribute” pop-up window, enter the “Attribute Name”, such as “MP_HighRisk”, with an “Attribute Type” of “Boolean”.

5. Click the "Add" button.

Add Custom Attribute

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>MP_HighRisk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
<td>Boolean</td>
</tr>
</tbody>
</table>

6. Enter in your admin password and click the "Confirm" button.

Creating a Device Mitigation Group

Now that we have a mitigation label (“MP_HighRisk”), we will create a Device Mitigation Group (device group) based on this custom attribute.

For this example, we will call this device mitigation group, “Devices_At_HighRisk”. This group will contain all the devices in which the custom attribute, for our example “MP_HighRisk”, is set to “Yes”.
1. Navigating to **Devices > Groups**.

![IBM MaaS360](https://via.placeholder.com/150)

2. Click the **“Add”** drop-down button, and select **“Device Group”**.

![IBM MaaS360](https://via.placeholder.com/150)

3. On the Advanced Search screen, configure the following settings:
   a. On the "Search Criteria" set "All Conditions (AND)".
   b. On the "Condition 1" set "Custom Attributes" and "MP_HighRisk", "Equal To" and "Yes".

4. Click the **"Search"** button.

![IBM MaaS360](https://via.placeholder.com/150)
5. Click the “Create New Device Group” button.

6. On the “Devices Group Details” pop-up window, enter the Group Name, such as in our example “Devices_At_HighRisk”, and a Description, if desired.

7. Click Save.

Creating Compliance Policies

Now that we have a Device Mitigation Group, we can create Compliance Policies that will be enforced on devices that are at High Risk using the Mitigation Label. In this section, we will create Security Policies and Compliance Rules that will be used to enforce these actions.

Note - We will show a couple of different compliance 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 compliance policies according to their internal security policy.
Security Policy (Examples)

Creating Compliance Actions for iOS Devices (Policy)

The policy will specify the actions taken on High Risk iOS devices. In our example, we will disable the camera and screen captures, but you might create a policy that disables access to the corporate network or assets.

1. Navigate to Security > Policies, and click the “Add Policy” button.

2. Make the policy available for "All".

3. Enter a Name for the policy, such as “MP_iOS_HighRisk”, and if desired, a description.

4. Select a “Type” of “iOS MDM”.

5. Select “Start From” equal to “Community Based Policy”.

6. Click the "Continue" button.

7. Select the Industry, Deployment Size and Region according to organization profile.
8. Click the “Continue” button.

9. Click the "Continue" button.

10. On the menu to the left select "Device Settings" pane. There are several options for policy sets, such as “Passcode”, "Restrictions", "Application Compliance", etc. We will make our modifications in the “Restrictions” section.

11. Select the “Restrictions” tab.
12. Click the “Edit” button.

13. Under the Restrictions > Device Functionality section, unselect “Allow Use of Camera” and “Allow Screen Capture”.

14. Under the Application Compliance section, select “Configure Required Applications”.
15. In the “Application Name” field, start typing “SandBlast Mobile Protect” and the app will pop-up, select SandBlast Mobile Protect.

16. Click the “Save and Publish” button.

17. Click the "Continue" button.
18. Enter in your admin password and click the "Confirm" button.

Creating Compliance Actions for Android Devices (Policy)

The policy will specify the actions taken on High Risk Android devices. In our example, we will disable the camera and screen captures, but you might create a policy that disables access to the corporate network or assets.

1. Navigate to Security > Policies, and click the “Add Policy” button.

2. Make the policy available for All.

3. Enter a Name for the policy, such as “MP_Android_HighRisk”.

4. Select a “Type” of “Android MDM”, and select “Start From” equal to “Community Based Policy”.
5. Click the "Continue" button.

6. Select the Industry, Deployment Size and Region according to organization profile.

7. Click the "Continue" button.
8. On the menu to the left select "Device Settings" pane. There are several options for policy sets, such as “Passcode”, "Security", "Application Compliance", etc. We will make our modifications in the "Security" section.

9. Click the “Edit” button.


11. Select the “Restrictions” tab.

12. Under the Restrictions > Device Feature Restrictions section, change Camera to “Disabled”.
13. Select the “Application Compliance” tab.

14. Under the Application Compliance section, select “Configure Required Applications”.
   
   a. In the “Application Name” field, enter “SandBlast Mobile Protect”
   
   b. In the “Application ID” field, enter “com.lacoon.security.fox”

<table>
<thead>
<tr>
<th>Application Name</th>
<th>SandBlast Mobile Protect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>com.lacoon.security.fox</td>
</tr>
</tbody>
</table>

[Image of the MaaS360 interface showing the Application Compliance section with the Application Name and Application ID fields highlighted.]
15. Click the “Save And Publish” button.

16. Click the "Continue" button.

17. Enter in your admin password and click the "Confirm" button.

Creating Security Compliance Rule (Enforcement)

This compliance rule will be used to enforce the policies created in the previous section.

1. Navigate to Security > Compliance Rules, and click the “Add Rule Set” button.
2. Make the rule available for the desired group.

3. Enter in a "Rule Set Name", such as “MP_HighRisk_Rules”, and if desired to "Copy From" an existing rule, such as “OS Version”.

4. Click the “Continue” button.
5. Because SandBlast Mobile supports iOS and Android only, under Basic Settings > Select Applicable Platforms section, we will unselect all OS’es other than “iOS” and “Android”.

6. Select “Group Based Rules” tab, and click the “Add a New Rule” button.

7. Enter in a Name, such as “MP_HighRisk”, select the Device Mitigation Group we created in section Creating a Device Mitigation Group to put all our SandBlast Mobile Devices into, in our example “Devices_At_HighRisk”.

8. Under Enforcement Action section, the first action “When detected in the group” is already set to “Alert”. Change “Alert” to “Change Policy” action. This will create additional fields for setting the policies to enforce on iOS, Android, and Windows Phone.
   a. Set iOS policy to the compliance policy we created in Section Creating Compliance Actions for iOS Devices (Policy), in our example “MP_iOS_HighRisk”.
   b. Set Android policy to the compliance policy we created in Section Creating Compliance Actions for Android Devices (Policy), in our example “MP_Android_HighRisk”.
9. Click the “Save” button.

10. Enter in your admin password, and then click the “Continue” button.
Applying the Compliance Policy to the Device Provisioning Group

Now that we have created the compliance rule (“MP_HighRisk_Rules”) we want to enforce, we need to link those rules to our Device Provisioning Group (“MP_Devices_Group”) we created in Section *Creating a Device Provisioning Group*.

Navigate to Security > Compliance Rules, find the rule you created in section *Creating Security Compliance Rule (Enforcement)*, our example is “MP_HighRisk_Rules”, and click the “Assign” link.

1. On the Assign Rule Set pop-up window, select the Device Provisioning Group we created in section *Creating a Device Provisioning Group*, in our example “MP_Devices_Group”.

2. Click the “Submit” button.

3. Click the "Continue" button.
4. Type your admin password, and then click the “Continue” button.

Note - Now any device in the Device Provisioning Group (“MP_Devices_Group”) that has their custom attribute (“MP_HighRisk”) set to “Yes” by the SandBlast Mobile system will be placed in the Device Mitigation Group (“Devices_At_HighRisk”), which in turn will have the compliance actions in the Compliance Rule (“MP_HighRisk_Rules”) acted upon it.

- For iOS, this policy is named “MP_iOS_HighRisk”, and
- For Android, this policy is named “MP_Android_HighRisk”.

Note - At this point, we have all the information we will need to configure the UEM integration settings in the SandBlast Mobile Dashboard. We are going to do that and then return to the MaaS360 Portal to configure the SandBlast Mobile Protect app deployment settings.

From Our Examples:

- **Server** = https://services.m3.maas360.com
- **API Admin Username/Password** = mp_api_admin/<hidden>
- **Device Provisioning Group(s)** = MP_Devices_Group.
- **Mitigation Label** = MP_HighRisk.
Configuring the Check Point SandBlast Mobile Dashboard Integration Settings

Prerequisites

1. You will need the following details from your MaaS360 Deployment:

   **Note** - There is a table in section *Integration Information* that you can record your settings for easy reference.

   a. Server: The root URL to your MaaS360 Web Services API including the leading https://, such as https://services.m3.maas360.com

   b. MaaS360 API Administrator 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 Admin account in section *Creating an API Only Administrator Account (optional)* for this purpose.

   c. Billing ID: This is the Corporate Identifier and can be located on Setup > Deployment Settings.

   d. API App ID: com.[Billing ID or Corporate Name].api (This information needs to be obtained from IBM MaaS360 Support)

   e. Access Key: This key needs to be obtained from IBM MaaS360 Support.

   **Note** - Multiple SandBlast Mobile Dashboards can be integrated to one MaaS360 instance by separating the devices into different “Device Provisioning Groups”, such as creating a device provisioning group for All EU Devices (i.e. “MTP_EU_Devices”) and a device provisioning group for All US Devices (i.e. “MTP_US_Devices”). Then, the SandBlast Mobile Dashboard in the EU would be integrated to “MTP_EU_Devices” and the SandBlast Mobile Dashboard in the US would be integrated to “MTP_US_Devices”.

   f. Organization Groups(s): This is the MaaS360 device provisioning group to which the devices to be registered to SandBlast Mobile are grouped, and will be integrated with the SandBlast Mobile Dashboard. Multiple groups can be integrated with the one SandBlast Mobile Dashboard instance by entering each label name separated with a semicolon (;). This is the Device Provisioning Group we created in section *Creating a Device*
**Provisioning Group** (“MP_Devices_Group”).

g. Mitigation Attribute: This is the custom attribute that will be set to “Yes” when the device is in High Risk. This is the custom attribute that you created in section *Creating a Mitigation Label* (“MP_HighRisk”).

2. For On-premise UEM environments, port 443 (HTTPS) must be remotely accessible through your firewall from the SandBlast Mobile Dashboard to the UEM system before trying to connect.

   a. See section *Integration Information* for the SandBlast Mobile Dashboard IP addresses for your region.

   b. If you do not know your SandBlast Mobile Dashboard’s region, follow the instructions in section *Integration Information* to find out.

3. Delete any existing devices in the SandBlast Mobile Dashboard.

**Note** - Only the devices are synchronized from the UEM to the SandBlast Mobile Dashboard, not users.
Configuring UEM 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. On Server Setup click Edit.
   The Integration Wizard opens.

Example:

3. Configure the settings for your MaaS360 Deployment.

Server Setup

Configure your UEM to integrate with the created MaaS360 devices:

a. In Server Setup section, enter this information:

- UEM service – MaaS360
- Server Address - The full URL needed for the UEM service
- User name
- Password
- Billing ID
- API app ID
- Access key
Example:

Synchronization Configuration

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

a. In the Group(s) field:

- Click Group(s). A dropdown with list of the available groups opens.
- Select the group(s) you need for integration with MaaS360.
Example:

b. In the Android Enterprise Deployment field:

Select the groups for two deployed applications as part of the MaaS360 Android Enterprise deployment.
c. In the Advanced section:

   Import Personally Identifiable Information (PII) and set the synchronization intervals.

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

   **Note** - If all entries are OFF, the placeholder information set for the email address is placed in the Device Owner’s Email, in form of "UEMDevice UDID@vendor.mdm".

Example:

Click Next.
Tagging Configuration

Specify the information sent to MaaS360 and the risk level of the device.

a. In Tagging Section:
   i. Set Tag device status to ON.
      o For integration with IBM MaaS360, the Device Status tag is interpreted as a "device attribute" of "CHKP_Status" with the values of Provisioned, Active, or Inactive.
      o 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.
      o For integration with IBM MaaS360, the Device Risk tag is interpreted as a "device attribute" of "CHKP_Risk" with the values of None, Low, Medium, or High.
      o 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:
The free-form Mitigation group is any unique name, such as "SBM_HighRisk", that SandBlast Mobile will place only devices determined to be at High Risk.

Click Next.
Example:

![Maas360 Integration](image)

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

Advanced

Mitigation attribute
Deployment

Specify the deployment status of a device.

Note - This section is optional, because MaaS360 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:

4. View the Integration Status.

The Device Management pane shows this information:

- **Server** – The latest server configuration status.
- **Synchronization** – The synchronized groups and the sync status.
- **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:

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

Prerequisites

SandBlast Mobile Gateway/Server – Server name of the SandBlast Mobile gateway/server, which should be us-gw01. If you don’t know your SandBlast Mobile server name, follow the instructions in section Integration Information to find out.

Adding the SandBlast Mobile Protect App to Your App Catalog

Now that the UEM and SandBlast Mobile Dashboard are communicating, we can now start deploying the SandBlast Mobile Protect app from the public stores to those devices that will be protected by SandBlast Mobile.

We will need to add the App for both iOS and Android operating systems.
Get dashboard’s token

1. Go to your SandBlast Mobile dashboard > **Settings** > **Device Management** > **Deployment** > **Edit**: 

![Dashboard Screenshot]

- **Server**
  - Last Connected: May 20, 2020, 21:20
  - UEM Service: MaaS360
  - Server Name: My_Ac_Admin

- **Synchronization**
  - Last Updated: May 20, 2020, 21:14
  - Groups: XP_Device_Group

- **Deployment**
  - Platforms: Deployment is managed by UEM console
3. Copy the token of your dashboard:
iOS App – Add to Catalog

The SandBlast Mobile Protect App for iOS can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.

1. Navigate to **APPS > Catalog**.

2. Click **"Add" > iOS > iTunes App Store App**.

3. In the **"App"** field, enter “SandBlast Mobile Protect” to start actively searching the store. Select the “SandBlast Mobile Protect” app as indicated below.
4. Navigate to the “Policies and Distribution” tab, and select “Distribute to” > select Group or "All Devices", and select Install Automatically.

5. Navigate to the “Configuration” tab, and select “App Config Source” of “Key/Value”.

6. Add the following Key/Value pairs:

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lacoon Server Address</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>%csn%</td>
</tr>
<tr>
<td>token</td>
<td>Take the copied value from section above</td>
</tr>
</tbody>
</table>
7. Click the “Add” button.

8. Enter in your admin password and click the "Confirm" button.

Android Enterprise App – Add to Catalog

The Android SandBlast Mobile Protect App can be automatically configured and deployed. The user only needs to accept the installation, and then launch the app once it is installed to finish activation and registration.
1. Navigate to **APPS > Catalog** and click "Add" > **Android** > **Google Play App**.

![App Catalog](image1)

2. In the Google Play search field, enter “SandBlast Mobile Protect” to start actively searching the store. Select the “SandBlast Mobile Protect” app as indicated below.

![Add Google Play App](image2)

![Apps](image3)
3. Navigate to the “Policies and Distribution” tab, and select “Distribute to” > Group or All Devices, and select Install Automatically.

![App Details and Policies and Distribution](image)


5. Add the following Key/Value pairs:

<table>
<thead>
<tr>
<th>Item</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM_UUID</td>
<td>%deviceid%</td>
</tr>
<tr>
<td>token</td>
<td>Take the copied value from section above</td>
</tr>
</tbody>
</table>

6. Click the "Add" button.
7. Enter in your admin password and click the "Confirm" button.

**Deploying SandBlast Mobile Protect app**

To deploy the SandBlast Mobile Protect app to devices that will be registered to the SandBlast Mobile solution we need to link the SandBlast Mobile Protect app in our app catalog to the Device Provisioning Group we created in section *Creating a Device Provisioning Group*.

1. Navigating to **Apps > App Catalog**, select both the iOS and Android SandBlast Mobile Protect apps.
2. Click the **Distribute** link.

3. On the **Distribute** pop-up window, set "Available for" equal to "All".

4. Set **Target** equal to “Group” and choose the device provisioning group you created in Section *Creating a Device Provisioning Group*, in our example “MP_Devices_Group”.

5. Select “Install Automatically” and “Send Email” checkboxes.

6. Click the **Distribute** button.
7. Enter your admin password, and click the “Continue” button.

Setting Policy to Require SandBlast Mobile Protect to be installed

The SandBlast Mobile Protect app is required by creating a Security Policy for iOS and Android devices, then creating a compliance rule set to the Device Provisioning Group we created in section Creating a Device Provisioning Group, and apply the compliance policy to the Device Provisioning Group.

Creating Compliance Actions for iOS Devices (Policy)

The policy will specify the actions taken on all SandBlast Mobile iOS devices.

Navigate to Security > Policies, and click the “Add Policy” button.
1. Enter a Name for the policy, such as “MP_App_iOS”, select a “Type” of “iOS MDM”, and select “Start From” equal to “My Existing Policies”. On "My Existing Policies” select "(def) Default iOS MDM Policy”.

2. Click the “Continue” button.

3. On the menu to the left, on the "Device Settings" pane there are several sections for policy sets, such as “Passcode, Restrictions, Application Compliance, etc. We will make our modifications in the "Application Compliance" section.

4. Click the “Edit” button.

5. Under the Application Compliance section, select “Configure Required Applications”.

6. In the “Application Name” field, start typing “SandBlast Mobile Protect” and the app will pop-up, select SandBlast Mobile Protect.
7. Click the “Save and Publish” button.

8. On the "Publish" pop up window click on "Continue".
Creating Compliance Actions for Android Devices (Policy)

The policy will specify the actions taken on all SandBlast Mobile Android devices.

1. Navigate to Security > Policies, and click the “Add Policy” button.

2. Enter a Name for the policy, such as “MP_App_Android”, select a “Type” of “Android MDM”, and select “Start From” equal to "My Existing Policies". On "My Existing Policies" select “Default Android MDM Policy”.

9. Enter in your admin password and click the "Confirm" button.
3. Click the "Continue" button.

4. On the menu to the left, on "Device Settings" there are several sections for policy sets, such as "Passcode", "Security", "Restrictions", "Application Compliance", etc. We will make our modifications in the “Application Compliance” section.

5. Click the “Edit” button.

6. Under the Application Compliance section, scroll down and select “Configure Required Applications”.

7. In the “Application Name” field, enter “SandBlast Mobile Protect”
8. In the “Application ID” field, enter “com.lacoon.security.fox”.

9. Click the “Save And Publish” button.

10. On the "Publish" pop up window click on "Continue".
11. Enter in your admin password and click the "Confirm" button.

Applying App Required Policy to Device Provisioning Group

The policies created in the previous section are assigned to the device provisioning group created in section **Creating a Device Provisioning Group**, in our example “MP_Devices_Group”.

1. Navigate to Devices > Groups, locate the device provisioning group, click the “More…” link, and select “Change Policy”.
2. Set iOS Policy to the compliance policy we created in Section 4.4.1, in our example “MP_App_iOS”.

3. Set Android Policy to the compliance policy we created in Section 4.4.2, in our example “MP_App_Android”.
4. Click the "Submit" button.

![Change Policy - MP_Devices_Group](image)

5. Enter in your admin password, and then click the "Confirm" button.

![Security Check](image)

6. The policies and the apps added to the "MP_Devices_Group".

![IBM MaaS360](image)

**Note** - Any device that belongs to the Device Provisioning Group ("MP_Devices_Group") that hasn’t installed the SandBlast Mobile Protect app will be out of compliance.
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.

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.

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. To enable the SandBlast Mobile Protect app (for both profiles):

   □ For a new UEM configurations:

   a. Go to UEM service and select the UEM type.
   b. In the configuration prompt, select the groups to synchronize.
   c. In the Android Enterprise Deployment section, select and add the device groups for both profiles.
For existing UEM configurations:

a. Go to Edit Settings.

b. In the Android Enterprise Deployment section, select and add the device groups for both profiles.

Example:

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

Notes:

- Only the synched groups in the upper groups section are available for Android Enterprise deployment
- If one or more devices in the selected group have SandBlast Mobile Protect app Version earlier than 3.6.4.4348, the operation stops until the devices are upgraded.
- 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.

To view and filter the devices:

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

Example:
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>
</table>
| Work          | ![Android Enterprise Icon] | Device Type  
OS - Android Enterprise |
| Personal      | ![Android Icon] | Device Type  
OS - Android |

Policies

To change policy for inactive personal profile:


   Example:

2. From the drop-down list, select a policy.

   Android Enterprise Security Settings
   
   Change device risk level to: High (Device Alert)  
   If Sandblast Mobile on personal profile is not active
Risk Handling

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

Example:

![Image showing device threat notification]

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity Level</th>
<th>Attack Vector</th>
<th>Threat Factors</th>
<th>Event</th>
<th>Event Details</th>
<th>OS</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 09 2020, 17:09:26</td>
<td>Information</td>
<td>Device</td>
<td>Personal profile inactive</td>
<td>Compliant</td>
<td></td>
<td></td>
<td>58052</td>
</tr>
<tr>
<td>Feb 09 2020, 17:09:26</td>
<td>Information</td>
<td>Device</td>
<td>Connectivity</td>
<td>Active</td>
<td></td>
<td></td>
<td>58054</td>
</tr>
<tr>
<td>Feb 09 2020, 17:08:14</td>
<td>Critical</td>
<td>Device</td>
<td>Personal profile inactive</td>
<td>Noncompliant</td>
<td></td>
<td></td>
<td>58052</td>
</tr>
</tbody>
</table>

- 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.
Deploying SandBlast Mobile Protect App to the Devices

This section describes the user experience during the deployment of the SandBlast Mobile Protect app.

Registration of an iOS Device

After the device is registered to the MaaS360 system and the SandBlast Mobile Protect app has been “Distributed” to the Device Provisioning Group (“MP_Devices_Group”), the user will be prompted to install the SandBlast Mobile Protect App.

1. The user taps “Install” on the device.

2. After the App has been installed on the iOS Device, the user only needs to launch the App to finish the registration.
3. After the overview, the App will automatically register. The registration server and key are automatically configured in the App by the MaaS360 system.

4. 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 registered to the MaaS360 system, the user will navigate in the MaaS360 App Catalog app or the user will receive a policy error.

SandBlast Mobile Protect Install Prompted by Compliance Violation

1. The user is prompted through notifications that their device is out of compliance. Clicking that notification will launch the MaaS360 app, opening the Compliance Status screen.

2. Clicking the “Install SandBlast Mobile Protect” button will launch the SandBlast Mobile Protect app in the Google Play Store.
SandBlast Mobile Protect Install Initiated by User in MaaS360 App Catalog

1. When the user opens the MaaS360 App Catalog, the app opens to the Apps list.
2. Clicking the “SandBlast Mobile Protect” app, the user then clicks the “Install” button.

Continuation of SandBlast Mobile Protect App

1. At the prompt to open within the Google Play Store, the user clicks the “Continue” button.
2. The user taps the “INSTALL” button, 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 SandBlast Mobile.

4. The user is prompted to allow the SandBlast Mobile Protect app to be a device administrator. They must tap “Install”.

5. 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

If the user’s device is determined to be at a High Risk state 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 High Risk state to the MaaS360 system for that device.

MaaS360 receives the state change, and upon recognizing the custom attribute being tied to a compliance policy, enacts the policy actions.

In the following example, the Administrator will blacklist an app, such as in our example “Dropbox”. As a result, the user’s device will be identified to be at High Risk due to the blacklisted app, “Dropbox”, being installed on the device. The SandBlast Mobile Dashboard will notify the user, and mark the device as High Risk to the MaaS360 system. The MaaS360 System will then enforce policy actions specified in the compliance policy, in our example “MP_Android_HighRisk” based on the compliance rules specifying that the custom attribute set to “yes” groups this device in the device mitigation group, “Devices_At_HighRisk”. This mitigation process was the one we created in section Creating a Mitigation Process.
Blacklisting a Test App

The first step is to blacklist an app, in our example “Dropbox”.

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 the “Policy” link of “Edit”.

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 the “OK” button.
View of Non-Compliant Device

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”.

2. The user will not be able to use the device’s camera, as specified in the compliance actions (policy) we created in section Creating Compliance Actions for iOS Devices (Policy), in our example “MP_iOS_HighRisk” until the user removes the blacklisted app.
MaaS360 App Notifications

1. The user receives a MaaS360 notification as specified in the “MP_HighRisk”.
MaaS360 Email Notification

1. The user receives an email from the MaaS360 system, as specified in the “MP_HighRisk_Rules”.

![MaaS360 Email Notification](image)

- **Device Name:** fmulder-SM-T567V
- **Username:** fmulder (fmulder@cptme.us)
- **Policy Violation:** Device is at High Risk

Review executed and planned enforcement actions below:

**Action(s) Performed:**
- Change Policy. MDM Policy will be changed on your device.

**Action(s) Planned:** None

**Instructions from Admin:** Your device has been flagged as High Risk. Please see the SandBlast Mobile Protect app and/or your email for further instructions to remediate the issues.
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:

   ![Device Risk 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:

   ![Device Details Example]
Administrator View on the MaaS360 Portal

In the MaaS360 Portal from the Home tab, the Administrator can that one or more devices are “Out of Compliance”.

1. Clicking the “Out of Compliance” button, the Administrator is presented with a list of the devices currently “Out of Compliance”.

![My Alert Center](image1)

<table>
<thead>
<tr>
<th>2 Recently Added</th>
<th>0 No Passcode</th>
<th>0 Jailbroken or Rooted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Out of Compliance</td>
<td>0 Roaming</td>
<td>46 Long Inactivity</td>
</tr>
</tbody>
</table>

![IBM MaaS360](image2)

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Username</th>
<th>Email Address</th>
<th>Model</th>
<th>Operating System</th>
<th>Last Reported</th>
<th>Platform Name</th>
<th>Managed Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscully111-HD1903</td>
<td>dscully111</td>
<td><a href="mailto:dscully@cptma.us">dscully@cptma.us</a></td>
<td>HD1903</td>
<td>Android 10 (GQ21 190716.003)</td>
<td>6/5/2020 23:11 IDT</td>
<td>Android</td>
<td>Enrolled</td>
</tr>
</tbody>
</table>
2. Clicking the “View” link under the device of interest will open the Device Details view displaying the “Summary” screen.

![Device Details View]

3. Clicking on the “Summary” drop-down menu, the Administrator can choose “Security & Compliance” details.

![Security & Compliance Details]

4. The Administrator can see that the device is “Out of Compliance” because of the device belongs to the “MP_Android_HighRisk” policy, with the compliance rule of “Device is at High Risk” under the compliance rule set “MP_HighRisk_Rules” being applied.
5. Clicking on the “Security & Compliance” drop-down menu, the Administrator can choose “Custom Attributes” details.

6. The Administrator can see which custom attributes are currently set. The device has the “MP_HighRisk” set to “Yes”.

7. Navigating to Security > Compliance Logs, the Administrator can view the active “Compliance Events”.
## Appendix

## Integration Information

<table>
<thead>
<tr>
<th>Information Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaaS360 API URL (Server)</td>
<td></td>
</tr>
<tr>
<td>MaaS360 API Admin Username</td>
<td></td>
</tr>
<tr>
<td>MaaS360 API Admin Password</td>
<td></td>
</tr>
<tr>
<td>MaaS360 Billing ID (Corporate Identifier)</td>
<td></td>
</tr>
<tr>
<td>MaaS360 API App ID (com.[Billing ID].api)</td>
<td>(such as com.3333300.api)</td>
</tr>
<tr>
<td>MaaS360 API Access Key</td>
<td></td>
</tr>
<tr>
<td>MaaS360 Device Group(s)</td>
<td></td>
</tr>
<tr>
<td>MaaS360 Device Custom Attribute</td>
<td></td>
</tr>
<tr>
<td>SandBlast Mobile Gateway</td>
<td></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>
</tbody>
</table>