2 April 2021

Harmony Mobile for Citrix Endpoint Management

Integration Guide

[Classification: None]
Check Point Copyright Notice

© 2021 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

Table of Contents........................................................................................................................................... 3

About Check Point Harmony Mobile .................................................................................................................. 6

General Workflow............................................................................................................................................. 6

Introduction to the Harmony 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....................................................................................................................... 14

Enrolling Devices to Citrix Endpoint Management........................................................................................ 15

Creating Limited Administrator Account ......................................................................................................... 16

(optional)......................................................................................................................................................... 16

Create a New Administrator Role .................................................................................................................. 16

Create a New Administrator Account ............................................................................................................ 18

Configuring the Check Point Harmony Mobile Dashboard Integration Settings ....................................... 20

Prerequisites ..................................................................................................................................................... 20

Configuring Integration Settings ..................................................................................................................... 22

Procedure......................................................................................................................................................... 22

Configuring UEM to Deploy the Harmony Mobile Protect app ................................................................. 32

General Workflow............................................................................................................................................. 32

Configuring UEM to Deploy Harmony Mobile Protect app .......................................................................... 33

Prerequisites ..................................................................................................................................................... 33

Adding the Harmony Mobile Protect App to Your App Catalog ............................................................ 33
Adding Android Enterprise Managed Configurations.......................................................... 44
Adding an iOS Configuration Policy for Harmony Mobile Protect...................................... 47
Collecting App List from iOS Devices .................................................................................. 52
Requiring the Harmony Mobile Protect app to be Installed.................................................. 55
Creating a Mitigation Process ............................................................................................... 57
Creating Actions for Devices at High Risk ........................................................................... 58
Send Notification to User ....................................................................................................... 58
Mark Devices at High Risk as Out of Compliance ................................................................. 61
Creating an AppLock Policy for Devices at High Risk ........................................................... 65
Creating Actions for Devices at Medium Risk ......................................................................... 79
Mark Devices Not at High Risk as Compliant ........................................................................ 82
Deploying the Harmony Mobile Protect app automatically (Zero Touch Deployment) [Optional] ........ 86
Using Android Enterprise with Harmony Mobile ................................................................. 92
Profiles ................................................................................................................................ 92
Android Enterprise Deployment Scenarios ............................................................................ 92
Configuring Harmony Mobile Protect app to Protect your Devices ......................................... 93
Deploying Android Enterprise on your Devices .................................................................... 93
Policies ................................................................................................................................. 96
Risk Handling ....................................................................................................................... 97
Applying the Harmony Mobile Protect app Configuration and Policy Enforcement .................. 100
Deploying the Harmony Mobile Protect app on the Devices ............................................... 100
Registration of an iOS Device ............................................................................................... 100
Registration of an Android Device ......................................................................................... 101
Testing High Risk Activity Detection and Policy Enforcement ............................................. 103
Blacklisting a Test App .......................................................................................................... 104
View of Device at Risk .......................................................................................................... 105
Harmony Mobile Protect App Notifications ......................................................................... 105
Citrix Endpoint Management In-App Notification ................................................................. 105
Citrix Endpoint Management Email Notification ................................................................. 106
Administrator View on the Harmony Mobile Dashboard ...................................................... 106
Administrator View on the Citrix Endpoint Management Console ..................................... 108
Appendix................................................................................................................................ 110
Integration Information ............................................................................................................ 110
About Check Point Harmony Mobile

Check Point Harmony 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.

Harmony 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 and more.
- 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.

Harmony 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 Harmony Mobile solution ("the Solution") includes these components:
  - Harmony Mobile Behavioral Risk Engine (BRE "the Engine").
  - Harmony Mobile Gateway ("the Gateway").
  - Harmony Mobile Management Dashboard ("the Dashboard").
  - Harmony Mobile Protect app ("the App") for iOS and Android.

Harmony 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 Harmony Mobile Dashboard with your Citrix Endpoint Management. It provides a quick tour through the interface of the Citrix Endpoint Management and the Harmony Mobile Dashboard to enable integration, alerting, policy enforcement and mitigation (including mitigation flow).

General Workflow

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

The Harmony 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 Harmony Mobile Protect app with the company device managing systems.
# Solution Architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 Harmony Mobile Protect app | - The Harmony 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 |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3 Harmony Mobile Gateway      | - The cloud-based Check Point Harmony 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.                                                                                                                                                                                                                                                                                      |
| 4 Harmony Mobile Management Dashboard | - The cloud-based web-GUI Harmony 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 Harmony 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 Harmony 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 Harmony Mobile Protect app on a device.

Prerequisites

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

  Harmony Mobile integrates with **Citrix Endpoint Management** (On-Premise) and Citrix Endpoint Management is version 10.7 or later, through API access. Harmony 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 Harmony Mobile must belong to Security Group(s) to be tied to Harmony 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 Harmony 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 Harmony 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.
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 Harmony 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.

3. Click "**Next**".

4. On the "**Assignments**" tab, in **Mange user Assignment** section select whether it is “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".

e. Click "Next" through the remaining tabs until the final "Summary" tab, and then click "Save".

Sending Enrollment Invitations

This step isn’t absolutely required, but it is nice for the workflow for user engagement/enrollment into Citrix 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 the following:

   a. Recipient Group

   b. Platform: Select Android and iOS

   c. Domain: local

   d. Group: Select the group you created in the previous step

   e. Enrollment mode: User name + Password

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 Harmony 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 Harmony 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 Harmony 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 Harmony 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: API Admin Username/Password = Admin_User/<hidden>

  The credentials that the Harmony 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 Harmony Mobile Dashboard. Multiple groups can be integrated with the one Harmony Mobile Dashboard instance by entering each group name separated with a semicolon (;).

  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 Harmony Mobile Dashboard. Multiple groups can be integrated with the one Harmony Mobile Dashboard instance by entering each group name separated with a semicolon (;).

  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 Harmony Mobile to reflect the status of the device within Harmony 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 Harmony Mobile to reflect the status of the device within Harmony 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 Harmony Mobile Dashboard to the UEM system before trying to connect.

Notes - Before you start, delete any existing devices in the Harmony Mobile Dashboard. Only the devices are synchronized from the UEM to the Harmony 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 > Integrations.

2. Click the “+” icon.

3. Select Assets
4. In UEM Service, select Citrix XenMobile

- **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:

**Connector Setup (Optional)**

You can configure Harmony Mobile Connector when the UEM in on-premises and has no direct access from the Harmony Mobile cloud. For more information, see *Sandblast Mobile Connector Integration Guide* in the Check Point Support Download center.

b. Click **Next**.

**Synchronization Configuration**

Configure the devices and groups that you synchronize with Harmony 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:

In case your Android Enterprise devices are deployed with two profiles (Work and Personal) it is recommended to protect both of them. Select the appropriate groups for deployed applications as part of the Citrix Endpoint Management Android Enterprise deployment. See *Using Android Enterprise with Harmony Mobile*. 
Example:

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

   You can limit the import of the PII devices (users) to Harmony Mobile.
Example:

![Citrix XenMobile Integration](image)

- Click **Next**.

**Note** - If all entries are OFF, the placeholder information set for the email address is placed in the Harmony 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>Percentage of devices allowed for deletion after UEM device sync (in %)</td>
<td>0-100% ; use 100% for no threshold *</td>
</tr>
<tr>
<td>Deletion delay after</td>
<td>Delay device deletion after several sync attempts – device is deleted after this amount of sync tries that confirmed deletion</td>
<td>1-100 sync tries</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>

* 100% value is recommended for evaluation/test usage – when you are adding a small amount of devices

### 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:

1. **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 Harmony 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 Harmony Mobile Dashboard.

2. **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.

3. **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**.
- **Deployment**

Specify the deployment status of a device.

**Note** - This section is optional, because Citrix Endpoint Management manages the deployment automatically.

**If you use Harmony Mobile to manage the deployment:**

In the **Advanced** section:

Enable options to send email and/or SMS notification to the new users with instructions to download and install the Harmony Mobile Protect app.

Example:

Click **Finish**.
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 Citrix Endpoint Management
  - **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:

![Citrix XenMobile Information](image)

---

Click **Edit** in each section to edit the settings.
Configuring UEM to Deploy the Harmony 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 Harmony Mobile Protect App to your App Catalog. See Adding the Harmony Mobile Protect App to Your App Catalog.
2. Add an iOS Configuration Policy for Harmony Mobile. See Adding an iOS Configuration Policy for Harmony Mobile Protect.
4. Require the Harmony Mobile Protect app to be installed on your mobile. See Requiring the Harmony Mobile Protect app to be Installed”.
Configuring UEM to Deploy Harmony Mobile Protect app

Prerequisites

Harmony Mobile Gateway/Server – gw.locsec.net.

Note – Harmony Mobile is the new brand-name that replaced “SandBlast Mobile” by the time of writing this document the SandBlast Mobile Protect App in the public stores (Apple & Google) wasn’t change yet to reflect the new logo and app name. In the following steps the instructions will address the old app name of “SandBlast Mobile Protect”.

Adding the Harmony 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 Harmony Mobile Protect app from the public stores to those devices that will be protected by Check Point Harmony 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 Harmony Mobile Protect app. This ensures that the devices are synchronized in the Harmony Mobile Dashboard before asking the user to install the Harmony 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. Click "Next".

5. In the **Platform** pane select "iPhone", "iPad" and "Android Enterprise".

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:

![iPad app settings](image)

- **Deployment Rules**
  - OR:
    - Limit by raw device property name CHKPS_Status is equal to Provisioned
    - Limit by raw device property name CHKPS_Status is equal to Inactive
    - Limit by raw device property name CHKPS_Status is equal to Active

- **Store Configuration**
- **Volume purchase**

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: approve it and click “Select”
27. Click on the Harmony 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. On the **Approvals (optional)** tab click "Next".
32. On the "Delivery Group Assignments" tab, select the Delivery Group you created in "Creating a Delivery Group".

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

34. Click "Save".

Get dashboard’s token
Go to your Harmony Mobile dashboard > Settings > Integrations > Select the three dots > Edit:
Go to Deployment and 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 "Harmony 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>MDM_UUID</td>
<td>String</td>
<td>${device.id}</td>
</tr>
<tr>
<td>Item</td>
<td>Value Type</td>
<td>Configuration Value</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>---------------------</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 Harmony Mobile Protect

To auto-register iOS devices to Harmony 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 enter 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:

   <dict>
   <key>Device Serial Number</key>
   <string>${device.serialnumber}</string>
   <key>DEVICE_MAC</key>
   <string>${DEVICE_MAC}</string>
   <key>DISPLAY_NAME</key>
   <string>${DISPLAY_NAME}</string>
   <key>EMAIL</key>
   <string>${EMAIL}</string>
   <key>FIRST_NAME</key>
   <string>${FIRST_NAME}</string>
   <key>LAST_NAME</key>
   <string>${LAST_NAME}</string>
   <key>USERID</key>
   <string>${USERID}</string>
   <key>Lacoon Server Address</key>
   <string>gw.locsec.net</string>
   <key>token</key>
   <string>hash_tenant_id</string>
   <key>DEVICE_UDID</key>
   <string>${device.id}</string>
   </dict>

Change the <string>hash_tenant_id</string> content to your token value that you copied from your Infinity Portal dashboard (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 Harmony 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 Harmony Mobile Protect app to be Installed

The Harmony Mobile Protect app is required by editing the Delivery Group Apps tab and moving the Harmony 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. Drag "Harmony Mobile Protect" to "Required Apps".

5. The app adds to the "Required Apps" list as below:
6. Scroll down to "Summary" tab.

7. On the Summary tab, make sure the app shows up correctly, and click "Save".
Creating a Mitigation Process

In this section, you will reference a device property (CHKP_Risk) Harmony 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 Harmony 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 Harmony 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 Actions for Devices at High Risk

Send Notification to User

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

![Configure Actions](image)

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".

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 "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".
### Summary

Review your settings, and then save or deploy this action.

<table>
<thead>
<tr>
<th>General</th>
<th>Name</th>
<th>Devices in High Risk Out of Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action details</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Assignment</td>
<td>If device property &quot;CHKP_Risk&quot; is &quot;High&quot;, then mark the device as out of compliance immediately.</td>
<td></td>
</tr>
<tr>
<td>Delivery groups</td>
<td>Users,Group,SBM</td>
<td></td>
</tr>
</tbody>
</table>
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".

   ![Trigger Screen](image)

2. Select an Action as follows:
   
   a. Select "App Lock"
   b. Set to "0" Hours (for immediately)

5. Click "Next".

   ![Action Screen](image)
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 "Medium".
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 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">

```
<table>
<thead>
<tr>
<th>Trigger *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device property</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>CHKP_Risk</td>
</tr>
<tr>
<td>Is Not</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>
```

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".

```
<table>
<thead>
<tr>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Action Info</td>
</tr>
<tr>
<td>2 Details</td>
</tr>
<tr>
<td>3 Assignment (optional)</td>
</tr>
<tr>
<td>4 Summary</td>
</tr>
</tbody>
</table>
```

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**".

1. On the Summary screen, click "**Save**".
Note - Now any device in the Delivery Group ("Users_Group_SBMs") that has the Device Property "CHKP_Risk" equal to "High" or "Medium" set by the Harmony Mobile system will be acted upon by the Actions and Policies.
Deploying the Harmony Mobile Protect app automatically (Zero Touch Deployment) [Optional]

UEM solutions traditionally prompt the mobile device user to install the application once it is registered. In addition, to get full protection, the user needs to approve the required permissions and profiles. Many users are vigilant about installing new mobile applications or granting different permissions, and as a Security company, Check Point even encourages that. Most of them don’t know that the Harmony Mobile Protect app is focused on device characteristics and behaviors and not the content stored on or flowing through the device. Furthermore, some users are incompliant with the company’s security policy, especially when they use their own devices. Therefore, users often decide not to install the app or approve the required configuration. On top of that, users who do agree to install and accept the configuration will not often do it immediately and it will take time until the application is activated. As a result, many devices remain exposed to potential cyber-attacks.

Harmony Mobile’s innovative zero-touch technology allows the Protect app to be installed and activated automatically without any user interaction. The solution leverages Check Point’s unique bootstrap technology to establish zero-touch activation.

It is important to note that the following steps of zero-touch deployment are optional. If the organization does not want to force Harmony Mobile to activate itself on employees devices, please skip this chapter.

- **Zero Touch Deployment in Android Enterprise devices**


  2. Select Endpoint Management Options.
3. Select a name for the policy and click “Next”.

4. In Platforms > leave only “Android Enterprise” > Select Enabled always-on VPN for VPN package: com.lacoon.security.fox
5. Deployment Rules > Advanced > New Rule: Limit by known device property name - CHKP_Status - isn't equal to – Active, and click the “+” sign:

6. Click on “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 “Save”: 
- **Zero Touch Deployment in iOS devices**


2. Select iOS > Policies most often used > VPN.

3. Leave only iOS checked and select a name for the policy.
4. Click “Next”.
5. Under iOS fill in the following:
   a. **Connection name**: Check Point Local Tunnel
   b. **Connection Type**: Custom SSL
   c. **Custom SSL Identifier**: com.checkpoint.capsuleprotect
   d. **Server name or IP address**: www.checkpoint.com
   e. **Authentication Type for the connection**: Password
   f. **Auth Password**: (type an optional authentication password)

6. On Custom XML > Add three rules:
   a. **Parameter name**: OnDemandRules
      **Value (copy-paste the below):**
      ```xml
      <array>
      <dict>
      <key>Action</key>
      <string>Connect</string>
      <key>InterfaceType-Match</key>
      <string>WiFi</string>
      </dict>
      <dict>
      <key>Action</key>
      <string>Connect</string>
      <key>InterfaceTypeMatch</key>
      <string>Cellular</string>
      </dict>
      </array>
      ```
   b. **Parameter name**: OnDemandEnabled
      **Value**: 1
c. **Parameter name:** zero_touch  
   **Value:** true

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnDemandRules</td>
<td></td>
</tr>
<tr>
<td>OnDemandEnabled</td>
<td></td>
</tr>
<tr>
<td>zero_touch</td>
<td>true</td>
</tr>
</tbody>
</table>

7. Click “Next”

8. On the Assignment screen, select the Delivery Group you created in ”Creating a Delivery Group”, in our example: Users_Group_SBM

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

10. Click “Save”: 
Using Android Enterprise with Harmony 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 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 Harmony 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 Harmony 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 Harmony 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 Harmony Mobile Protect app to Protect your Devices.

Note - If you protect only the Work profile, skip the next section.
Configuring Harmony Mobile Protect app to Protect your Devices

**Note** - The deployment of the Harmony 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 Harmony 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 Harmony Mobile Protect app to both Work and Personal Profiles.

**To protect the whole device:**

1. On the Harmony Mobile Dashboard, go to **Settings > Device Management**
2. Enable the Harmony 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 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 Harmony 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 Harmony 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.

**General View on the Check Point Dashboard (Example):**
To view and filter the devices:

1. On the Harmony 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>
<tbody>
<tr>
<td>Work</td>
<td><img src="image1.png" alt="Icon" /></td>
<td>Device Type&lt;br&gt;OS - Android Enterprise</td>
</tr>
<tr>
<td>Personal</td>
<td><img src="image2.png" alt="Icon" /></td>
<td>Device Type&lt;br&gt;OS - Android</td>
</tr>
</tbody>
</table>
Policies

Check Point recommends creating different policies for personal side and working profile of the device.

1. To create a new policy, go to Policy and click the + next to Policy Profiles

2. Create a policy called Policy-Personal side and a second one called Policy-Work Profile.

3. Then you have to apply these policies to the different groups.

4. At the top of the Rule-base click +New.

5. Give your new rule a name, choose the relevant group (work or personal), and select the relevant policy you just created.

6. Confirm your changes and click on Save.

Example:

To change policy for inactive personal profile:

You can raise the risk level of the Work Profile if the personal side of the device is not protected with Harmony mobile, or if Harmony Mobile on the personal side has detected a risk with a level of High:

1. On the Harmony Mobile Dashboard, go to Policy > The policy applied to the Work Profile, or the local one > Device

2. Go to Android Enterprise Security Settings. And select the risk level you want to give to the Work Profile is the personal side of the device is compromised or not protected:

Example:
Risk Handling

- If the Harmony 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:
- If the Personal profile has the High Risk status, the risk level is raised to **High** on the Work profile. The Harmony 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.

<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, 17:11:57</td>
<td>Low Information</td>
<td>Device</td>
<td>Personal profile compromised</td>
<td>Compliant</td>
<td></td>
<td></td>
<td>59052</td>
</tr>
<tr>
<td>Feb 09 2020, 17:11:57</td>
<td>Low Information</td>
<td>Application</td>
<td>Malware</td>
<td>Removed</td>
<td>Antivirus</td>
<td></td>
<td>59054</td>
</tr>
<tr>
<td>Feb 09 2020, 17:10:50</td>
<td>Critical</td>
<td>Device</td>
<td>Personal profile compromised</td>
<td>Noncompliant</td>
<td></td>
<td></td>
<td>59052</td>
</tr>
<tr>
<td>Feb 09 2020, 17:10:49</td>
<td>Critical</td>
<td>Application</td>
<td>Malware</td>
<td>Installed</td>
<td>Antivirus</td>
<td></td>
<td>59054</td>
</tr>
</tbody>
</table>
Applying the Harmony Mobile Protect app Configuration and Policy Enforcement

Deploying the Harmony Mobile Protect app on the Devices

Note - It can take up to 10 minutes for Citrix Endpoint Management to sync with the Harmony Mobile Dashboard, and several more minutes for Citrix Endpoint Management to push the App to the user device.

Note: This flow describes how to activate Harmony Mobile application on your devices if you didn’t use the Zero Touch deployment described in the Zero Touch Deployment section.

If you used the Zero Touch deployment you can skip this section. The devices will be automatically activated and your users will have to approve a few permissions, according to the policy defined for the user group in Harmony Mobile dashboard, for example Location permission or Notification access.

Note that for Android devices, Android Enterprise is mandatory for the Zero Touch deployment process.

Registration of an iOS Device

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

Procedure for the User:

1. Register your device.
   a. Tap INSTALL on the Harmony Mobile Protect app.
      The Protect app is deployed on the iOS Device.
   b. Launch the Protect app to finish the registration.
      Citrix Endpoint Management 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:

Example: 

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

Registration of an Android Device

a. Harmony Mobile Protect app is pushed and installed to the device by Citrix Endpoint Management

b. Launch the App to finish its deployment and registration to Check Point Harmony Mobile.

The Harmony Mobile Protect app is automatically registered.
Example:

c. Tap **Continue**
d. Enable security settings **Allow all required permissions**
f. Tap **Enable**

2. The Harmony Mobile Protect app scans the system. See the state of the device on the display.

Example:

**iOS Devices**

![iOS Devices](image)

**Android Devices**

![Android Devices](image)
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 Harmony 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 Harmony 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".

1. SandBlast Mobile sends risk notification to User’s device
2. SandBlast Mobile sends the risk level for User’s device to Citrix Endpoint Management
3. Citrix Endpoint Management activates the appropriate compliance policy for User’s device based on security risk level
Blacklisting a Test App

Note - When you blacklist an app, all release versions and OS types of this app are blacklisted. Select Apply only to this version option to blacklist the specified version only.

1. Log into the Harmony Mobile Dashboard.

2. Go to Forensics > App Risk tab and select for the app you wish to blacklist.

   Example:

   ![Harmony Mobile Dashboard with App Risk tab selected.]

3. Go to Global Policy and click Edit.

   A Changing application policy-Global window pops up.

4. From the New Policy drop-down menu, select Black Listed.

5. In the Audit Trail note field, enter a reason for this change.

6. Click OK.

   The user receives a Harmony Mobile Protect app notification to indicate that the blacklisted app (for example, Box) is not allowed by the Corporate Policy.
View of Device at Risk

Harmony Mobile Protect App Notifications

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

Citrix Endpoint Management In-App Notification

1. The user will not be able 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 Harmony Mobile Dashboard

On the Harmony 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 or Inactive.

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 "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>Harmony Mobile Gateway</td>
<td>gw.locsec.net</td>
</tr>
<tr>
<td>Harmony Mobile App Name (iOS)</td>
<td>Harmony Mobile Protect</td>
</tr>
<tr>
<td>Harmony Mobile App ID (iOS)</td>
<td>com.checkpoint.capsuleprotect</td>
</tr>
<tr>
<td>Harmony Mobile App Name (Android)</td>
<td>Harmony Mobile Protect</td>
</tr>
<tr>
<td>Harmony Mobile App ID (Android)</td>
<td>com.lacoon.security.fox</td>
</tr>
</tbody>
</table>