Workspace Security

30 April 2026

CHECK POINT MOBILE SECURITY

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point Check Point Mobile Security Administration Guide

For more about Mobile Security, see the home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Patent Notice

Mobile Security is protected by the following patents in the United States and elsewhere.
This page is intended to serve as notice under 35 U.S.C. § 287(a):
US9,319,427, US9,642,013, US9,935,903, US10,158,665, US10,230,758,US10,567,425, US10,645,074, US10,911,487, US11,489,811

Related Documents

Document Title	Description
Mobile Security UEM Integration Guide	Describes how to integrate Mobile Security with different mobile device Unified Endpoint Management (UEM) systems. The supported UEMs: ■ BlackBerry ■ Citrix Endpoint Management ■ Google UEM ■ IBM MaaS360 ■ Microsoft Intune ■ MobileIron Core ■ MobileIron Cloud ■ Samsung Knox Manage ■ Workspace ONE (Formerly AirWatch UEM)
Harmony Mobile Protect app for Android User Guide	Describes how to install and use Harmony Mobile Protect app on Android devices.
Harmony Mobile Protect app for iOS User Guide	Describes how to install and use Harmony Mobile Protect app on iOS devices.
Mobile Security Connector Installation Guide	Describes how to install Mobile Security Connector and provides the configuration instructions for different deployment scenarios.

Revision History

Date	Description
30 April 2026	Added *"Usage Report" on page 194* for MSPs.
27 March 2026	Updated product name and product grouping to align with the new Check Point strategic pillars and portal navigation. No functional changes were made. Harmony Mobile is now referred to as **Check Point Mobile Security**.
29 October 2025	Re-arranged HM Communication Matrix region-wise. See *"Appendix A - Mobile Security Communication Information" on page 198*.
1 August 2025	Added **Proxy mode** and **Next Generation ONP** options in *"Network Protection" on page 63*.
30 July 2025	Updated communication matrix in *"Appendix A - Mobile Security Communication Information" on page 198*.
21 July 2025	Added updates for Mobile Security 5.0 version release: ■ Added how to add HTTPS inspection exceptions. See *"HTTPS Exceptions" on page 121*. ■ Added how to add a **centralized CA certificate** and apply it to several policies. See *"Central HTTPS Inspection Root CA" on page 174*. ■ QRadar SIEM Integration - Added **Syslog event format for IBM QRadar SIEM** in *"Appendix B - Mobile Security Syslogs" on page 218*.
23 June 2025	Added the CSV file requirements while importing device information from a CSV file. See Importing device info from a CSV file.
6 May 2025	Updated that SMS sender name is no longer configurable. See *"SMS Sender Name" on page 190*.
26 March 2025	Added a new option **Always ON - Proxy mode** for ONP in *"Network Protection" on page 63*.
11 March 2025	Removed **Local Network Permission** for iOS devices. See *"Permissions for iOS Devices" on page 242*.
17 February 2025	Added *"Zero Touch Notification" on page 170* setting.

Date	Description
15 January 2025	Added *"Blocking Malicious URLs in SMS - ONP v/s SMS Phishing Protection" on page 130*.
11 December 2024	Updated the **Top Threats per device** widget in the *"Overview" on page 31* page.
9 December 2024	■ Added the procedure on how to send reminders for device registration. See *Registration Templates* > *"Sending Reminders for Device Registration" on page 172*. ■ Added downloading and scheduling of Mobile Security Report (Operational and Full report). See Mobile Security Reports.
7 October 2024	Added **Page texts** section to select the language of text to be displayed on the Block page. See *"Block Page" on page 165*.
18 September 2024	Added communication matrix information for UAE region. See *"Appendix A - Mobile Security Communication Information" on page 198*.
05 August 2024	Added: ■ *"Infinity AI Copilot" on page 197* ■ Export and import of policies. See *"Exporting and Importing a Policy" on page 58* ■ Procedure on how to send custom notifications to devices. See *Devices* > *"More Actions to Manage Devices" on page 44*. ■ Procedure on how to customize block pages. See *Customization* > *"Block Page" on page 165*.
17 July 2024	Added TLS certificate validity requirements for self-signed and third-party CA certificates. See Network Protection > *"HTTPS Settings" on page 69*.
10 July 2024	Added *"Supported Languages" on page 21*.
04 July 2024	Added the APK link to download Harmony Mobile Protect app. See *"Supported Operating Systems (OS)" on page 21*.

Date	Description
26 June 2024	Added support for Security Patch update: ■ Added **Installed Patch** version column in Devices table. See *"Devices" on page 36*. ■ Added new parameters to set risk level if the security patch is not installed or updated on the device. See Device policies > *"OS Vulnerabilities" on page 88*. ■ Added security patch information in OS CVE Assessment > *"View by Devices" on page 159*.
06 May 2024	Added: ■ **Jailbroken Device** setting in *"iOS Security Settings" on page 80*. ■ **Rooted Device** setting in *"Android Security Settings" on page 82*.
30 April 2024	Added the list of Android browsers that support SSL inspection in *"HTTPS Settings" on page 69*.
08 April 2024	Added information on support for Android tablets and iPads in *"Supported Operating Systems (OS)" on page 21*.
15 March 2024	Updated the procedure to attach a contract to the product in *"Accessing the Mobile Security Administrator Portal" on page 26*.
02 February 2024	Added a note on **Stolen Device Protection** in *"Mobile Device Integration Service (MDIS) Profile" on page 180*.
30 January 2024	Updated the descriptions for **Severity** and **Severity Level** filter in *"Application" on page 140*.
26 December 2023	Added *"Android SMS Phishing" on page 129*.
13 December 2023	Updated *"Installations" on page 147* in **Forensics > Application > Application Overview**.
06 December 2023	Added *"Supported Operating Systems (OS)" on page 21*.
11 November 2023	Added **SMS permission** in *"Permissions for Android Devices" on page 241*.

Date	Description
18 October 2023	Updated *"Networks - Blocked Locations" on page 116*.
11 October 2023	Updated *"Integration with Partner Supported UEMs" on page 179*.
03 October 2023	Added *"Connectivity Settings" on page 79* in Device Policy.
28 September 2023	Added these sections in **Devices**: ■ *"Viewing Connected UEMs" on page 43*. ■ *"More Actions to Manage Devices" on page 44*.
26 September 2023	■ Updated *"Devices" on page 36*: • Added PII Data Decryption Connector indication • Added **Policy** column in the Devices table • Added **UEM** column in the Devices table • Export of information for large number of devices. • How to add or remove multiple devices from or in a device group. See *"Adding a Device Group" on page 42*. ■ Updated these policies: • Added **Generative AI** category in *"Risky Applications" on page 93*. • Updated **Suspend ONP** description in *"Suspend Policy" on page 67*. • Added **Unsecure WiFi** setting in *"WiFi Network Protection Settings" on page 123*. ■ Updated **OS CVE Assessment**: • Added option to view OS CVE Assessment by Devices. See *"View by Devices" on page 159*. • Export of information for large number of CVEs.
25 July 2023	■ Updated **Inspection CA** in *"HTTPS Settings" on page 69*. ■ Added **HTTPS Inspection** checkbox in *"Advanced Network Protection Settings" on page 73*.
16 June 2023	Added *"API Reference" on page 22*.

Date	Description
31 May 2023	Added **Local Network** permission for iOS devices in *"Appendix D - Permissions for Harmony Mobile Protect app" on page 241*.
23 May 2023	Added *"Appendix D - Permissions for Harmony Mobile Protect app" on page 241*.
05 April 2023	Added a note for CVE information source in *"OS CVE Assessment" on page 157*.
14 March 2023	Added new steps in *"Getting Started" on page 26*.
7 March 2023	■ Added **Getting Started** section in *"Overview" on page 31*. ■ Updated *"Network Protection" on page 63*: • Added **Detect** mode in *"General Settings" on page 64*. • Added Fallback ONP DNS in *"Advanced Network Protection Settings" on page 73*. • Added *"Browser Only Settings" on page 74*. ■ Added *"Block Application Traffic" on page 99* in Application Policies. ■ Added File Download with Emulation in *"File Downloads" on page 109*.
30 January 2023	Added *"Specific Service Roles" on page 29*.
12 January 2023	Updated *"Application Exceptions" on page 102*.
27 December 2022	Updated *"Overview" on page 31*: Added **App Versions** and **License Info**.
27 October 2022	Updated **Security system configuration rules** table in *"Appendix A - Mobile Security Communication Information" on page 198*.
12 October 2022	Added *"SMS Sender Name" on page 190*.
23 September 2022	Replaced all MDM references with UEM.

Date	Description
16 September 2022	■ Added these appendices: • *"Appendix B - Mobile Security Syslogs" on page 218*. • *"Appendix C - Mobile Security ArcSight" on page 224*. ■ Added *"Related Documents" on page 4*. ■ Updated UEM information in *"Solution Architecture" on page 19*.
21 July 2022	Replaced all UDM references with Harmony Mobile Connector.
1 July 2022	Added a note in *"Overview" on page 31*.
20 Jun 2022	Added common Glossary for html version.
30 May 2022	■ Updated the path for MITRE ATT&CK Matrix in *"MITRE ATT&CK Matrix" on page 148*. ■ Updated security system configuration rules table in *"Appendix A - Mobile Security Communication Information" on page 198*. ■ Added Glossary. ■ Updated sub-sections in *"Getting Started" on page 26*.
20 May 2022	■ Added navigation steps to procedures in *"Network Protection" on page 63* and *"Policy Configuration" on page 54*. ■ Added details for default risk level in *"Policy Configuration" on page 54*.
11 May 2022	Updated these sections for UI enhancements: ■ *"Network Protection" on page 63* ■ *"Policy Configuration" on page 54* Added export and import of registration templates in *"Registration Templates" on page 171*.
01 February 2022	Removed App Category in *"Application Policies" on page 93*

Date	Description
26 January 2022	Added new features: ■ *"OS CVE Assessment" on page 157* ■ *"Campaign Detection" on page 161* ■ SMS messages configuration in *"Registration Templates" on page 171*. ■ Allow Apps from a Specific Developer Revised the *"Forensics" on page 132* screen section.
20 October 2021	First release of this document

Table of Contents

Introduction to Mobile Security

Check Point **Mobile Security** (formerly Harmony Mobile) is the most complete threat defense solution designed to prevent emerging fifth generation cyber-attacks and allows workers to safely conduct business. Its technology protects against threats to the OS, applications, and network, scoring the industry's highest threat catch rate without impacting performance or user experience.

Mobile Security delivers threat prevention technology that:

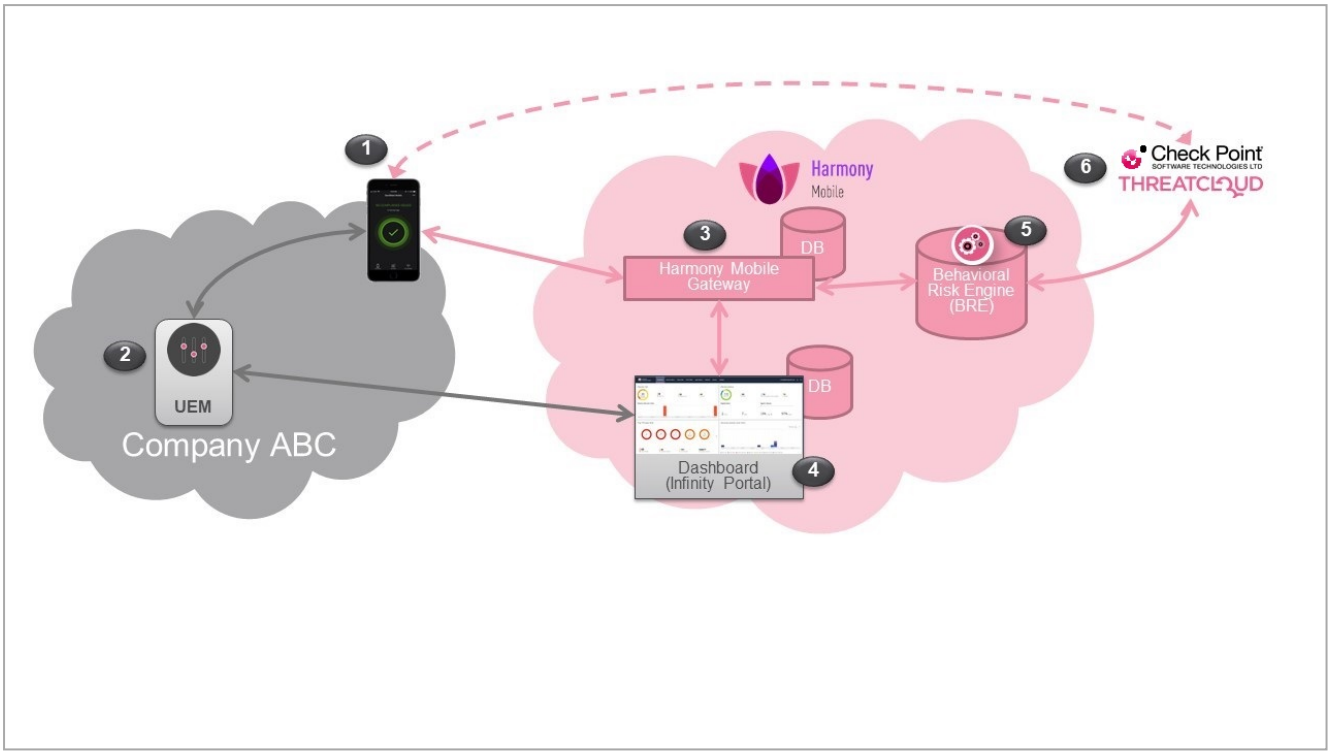
- Performs advanced app analysis to detect known and unknown threats
- Prevents man-in-the-middle attacks on both cellular and WiFi networks
- Blocks phishing attacks on all apps: email, messaging, social media
- Prevents infected devices from sending sensitive data to botnets
- Blocks infected devices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

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

The Mobile Security solution ("the Solution") includes these components:

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

Solution Architecture



	Component	Description
1	**Harmony Mobile Protect app**	■ The Harmony Mobile Protect app is a lightweight app for iOS® and Android™ that protects the device and helps analyze threats to devices in the Enterprise environment. It monitors operating systems device configurations, apps behavior 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.

	Component	Description
2	**UEM**	■ Unified Endpoint Management (generalized term replacing MDM/EMM). ■ Device Management and Policy Enforcement System. ■ The UEM option enables you to integrate Mobile Security to a generic unsupported UEM, or to any of these supported UEMs: • Workspace ONE (Formerly AirWatch UEM) • Microsoft Intune • MobileIron Core • IBM MaaS360 • Citrix Endpoint Management (Formerly XenMobile) • MobileIron Cloud • BlackBerry UEM On-Premises • Jamf Pro • Google Cloud • Samsung Knox Manage / Samsung SDS EMM • SOTI MobiControl • Applivery For more information on how to integrate the Mobile Security solution with different UEMs, see Mobile Security UEM Integration Guide.
3	**Mobile Security Gateway**	■ The cloud-based Check Point Mobile Security 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	**Mobile Security Management Dashboard**	■ The cloud-based web-UI Mobile Security Management Dashboard is hosted in the Check Point Portal and is configured as a per-customer instance. ■ It enables administration, provisioning, and monitoring of devices, security policies, events, alerts and mobile forensics ■ The Dashboard can be integrated with an existing Unified Endpoint Management (UEM) solution for automated policy enforcement on devices at risk.

	Component	Description
5	**Behavioral Risk Engine**	■ The cloud-based Mobile Security 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 Indicators of Compromise (IoC) 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 Mobile Security on-device Network Protection. ■ ThreatCloud exchanges threat intelligence with the Behavioral Risk Engine for app analysis.

Supported Operating Systems (OS)

Mobile Security is supported on these mobile OS versions:

- Android - Version 11.xor higher.
- iOS/iPadOS - Version 15.x or higher.

Notes:

- If the Harmony Mobile Protect app is not available in your local Google Play Store, you can download the APK from this link.
- Harmony Mobile Protect app is also supported on Android tablets and iPads but it cannot scan or share verdicts for applications exclusive to tablets/iPads.

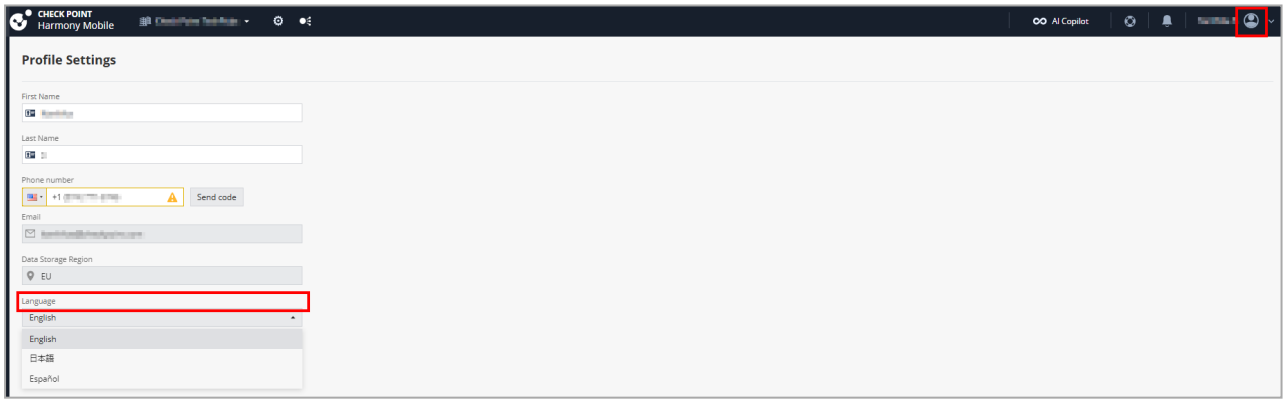
Supported Languages

Harmony Mobile Protect app supports the following languages:

- Simplified Chinese
- Traditional Chinese

- Dutch
- English
- Finnish (Android only)
- French
- German
- Italian
- Japanese
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazil)
- Russian
- Spanish
- Turkish

Note - To select the language in the Mobile Security Administrator Portal user interface, go to the user **Profile Settings**.



API Reference

Mobile Security API allows you to view and configure users, devices, device groups, connect to UEMs, retrieve security events from third-parties and so on, using REST API calls.

To access Mobile Security API:

1. Go to Check Point API Reference.
2. Click **Workspace Security**.
3. In the **Mobile Security API** widget, click **Open**.

Note - To view and configure your tenants, users, services and licenses in the Check Point Portal, go to Check Point Portal API.

Video Tutorials

1. How to send custom notifications to mobile devices

For relevant information, see *"Sending Notification to Devices" on page 50*.

2. How to customize block pages

For relevant information, see *"Block Page" on page 165*.

3. How to add exceptions for HTTPS Inspection

For relevant information, see *"HTTPS Exceptions" on page 121*.

4. How to generate a centralized CA certificate and apply it to several policies

For relevant information, see *"Central HTTPS Inspection Root CA" on page 174*.


CLICK HERE
TO START THE TUTORIAL

Getting Started

To get started with Mobile Security (formerly Harmony Mobile):

1. Create an account in Check Point Portal.
2. Access the Mobile Security Administrator Portal.
3. License the product.
4. Assign specific service roles to users.
5. Getting Started - If you have not added devices in the Mobile Security dashboard.
6. Overview - If you have added devices.

Creating an Account in the Check Point Portal

Check Point Portal is a web-based interface that hosts the Check Point security SaaS services.

With Check Point Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

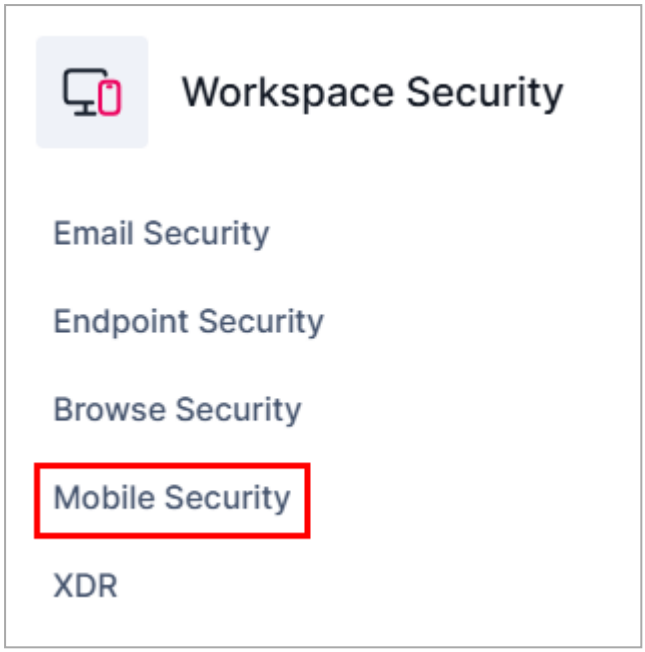
To create an Check Point Portal account, see the Check Point Portal Administration Guide.

Accessing the Mobile Security Administrator Portal

To access the Mobile Security Administrator Portal (formerly Harmony Mobile):

1. Sign in to *Check Point Portal*.
2. Click the **Menu** icon in the top left corner.

3. In the **Workspace Security** section, click **Mobile**.

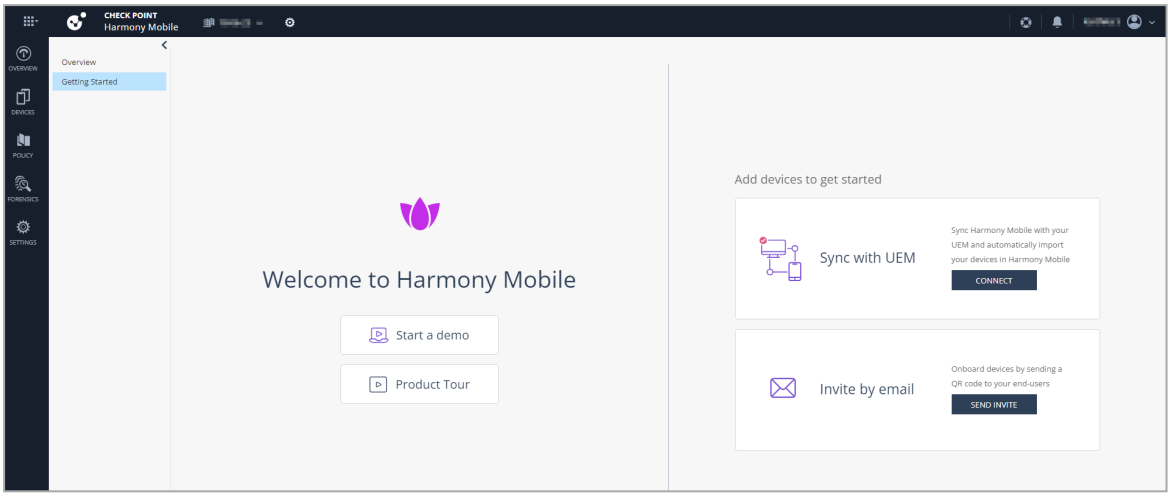


4. If you are accessing the portal for the first time, do one of these:

   - If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in the *Check Point Portal Administration Guide*.

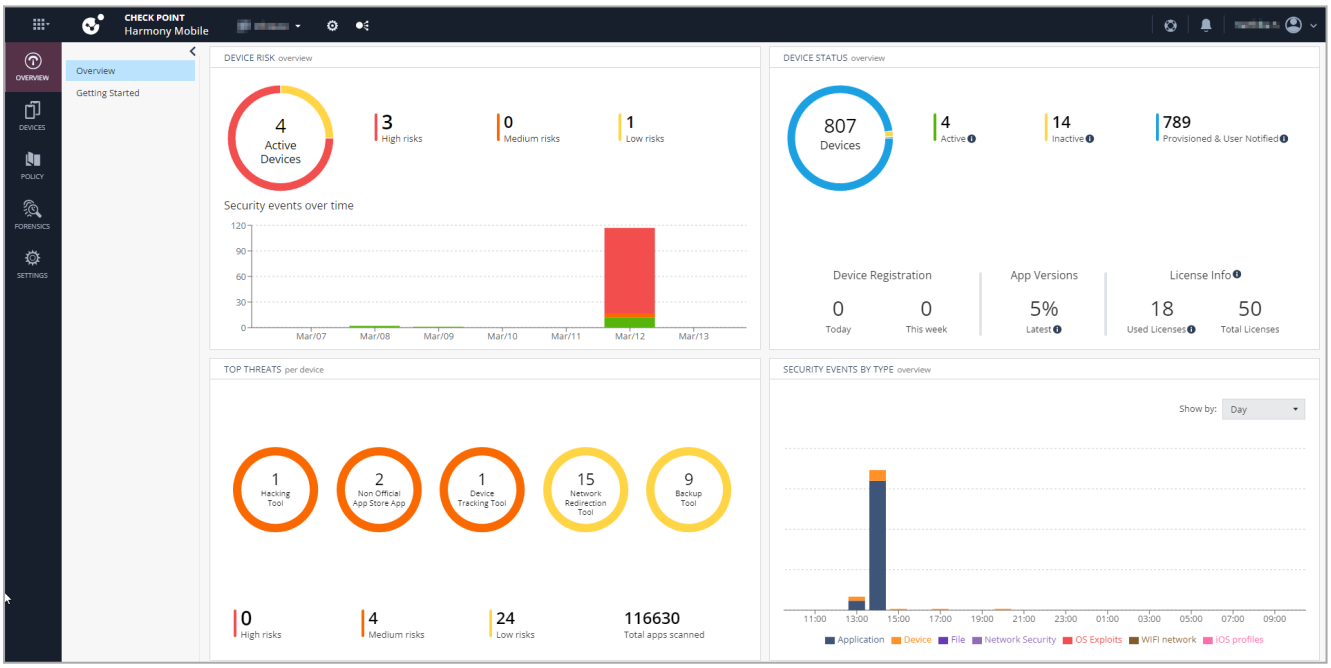
- If you want to trial the product, click **Start free trial**.

  The Mobile Security Getting Started page appears.



Note - This starts your Mobile Security trial. To use the service after 30 days, you must purchase a license. For more information, see *"Licensing the Product" below*.

If you have already attached the contract with the product, the Overview page appears.



Licensing the Product

When you create an account in the Check Point Portal and access the service, you get a free 30-day trial. After the 30-day trial period, you must purchase a software license to use the product. To purchase a license, you must create a Check Point User Center account. For instructions, see sk22716.

Once you create a User Center account, contact your Check Point sales representative to purchase a license.

When the customer moves to production (User Center account attached and production license activated):

- Trial (evaluation) licenses are no longer applicable.
- The device count on the **Overview** screen in the Mobile Security dashboard reflects only the devices covered by production licenses.

Policy behavior in production

- The system automatically updates the default values and settings in the **Global** policy to the recommended values. The custom changes remain unchanged.
- The custom policies automatically inherit the updates from the **Global** policy.
- All the policy changes are recorded in **Settings** > **Audit Trail**.

If you have already licensed the product, to view your current contract (license) information, go to **Check Point Portal** > **Global Settings** > **Contracts** page.

Specific Service Roles

Mobile Security supports specific service roles. For more information, see **Specific Service Roles** in the *Check Point Portal Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

The specific service roles supported in Mobile Security are:

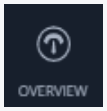
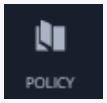
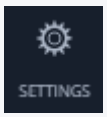
- Superuser
- Administrator
- Support
- Basic Support
- Device Administrator
- Security Manager
- Security Manager Viewer
- Basic Security Manager
- Group Security Manager
- Group Security Manager Viewer

To view permissions for each role, go to **Settings** > **Administrators** > **Roles Definitions**.

Menu Bar

The menu bar is located on the left side of the Mobile Security screen.

It displays the available options and menus on all of the dashboard pages and includes these options:

Icon	Item	Description
	Menu	You can open the list of all the CloudGuard services available in your system. To work with the Mobile Security, click the Mobile Security icon on the list.
	Dashboard	You can view both statistics and snapshot data based on information supplied by the enrolled devices.
	Devices	You can view and manage the organization’s devices.
	Policy	You can configure granular policies.
	Forensics	You can review the security forensic data for: ■ Events & Alerts ■ Application ■ Network ■ iOS profiles ■ OS CVE Assessment ■ Campaign Detection
	Settings	You can view and manage dashboard settings.

The information in the **Global Settings** contains the initial default values of the administrator's profile settings that apply locally and impact the entire system.

Overview

The **Overview** page shows these sub-menus:

- *"Overview" above*
- *"Getting Started" on page 34*

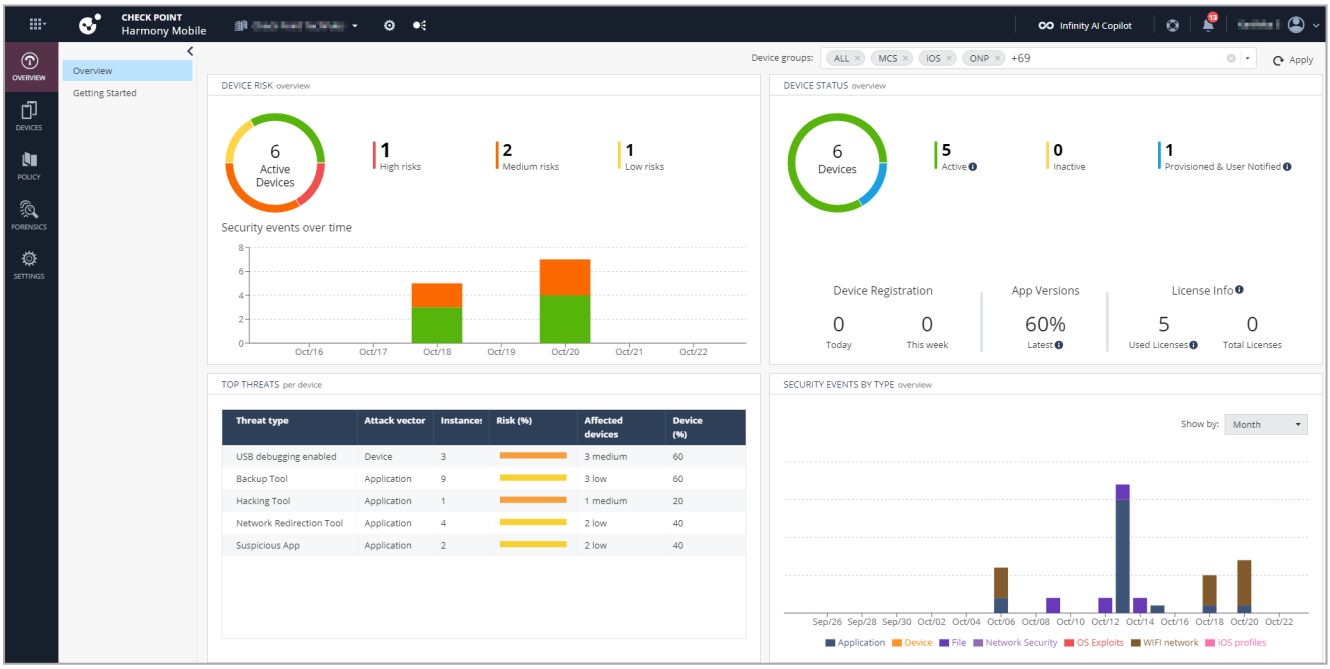
Overview

The **Overview** dashboard shows the statistics and snapshot data based on the information from the enrolled devices.

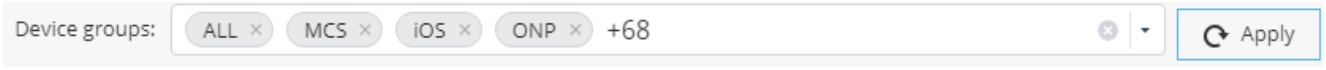
You can select specific device groups and view the statistics for:

- Device Risk
- Device Status
- Top Threats
- Security Events By Type

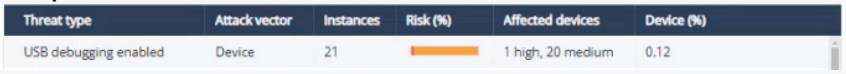
Click on each statistics value to view its related settings.



To view the overview statistics for specific device groups, select the groups from the **Device groups** list at the top-right corner, and click **Apply**.



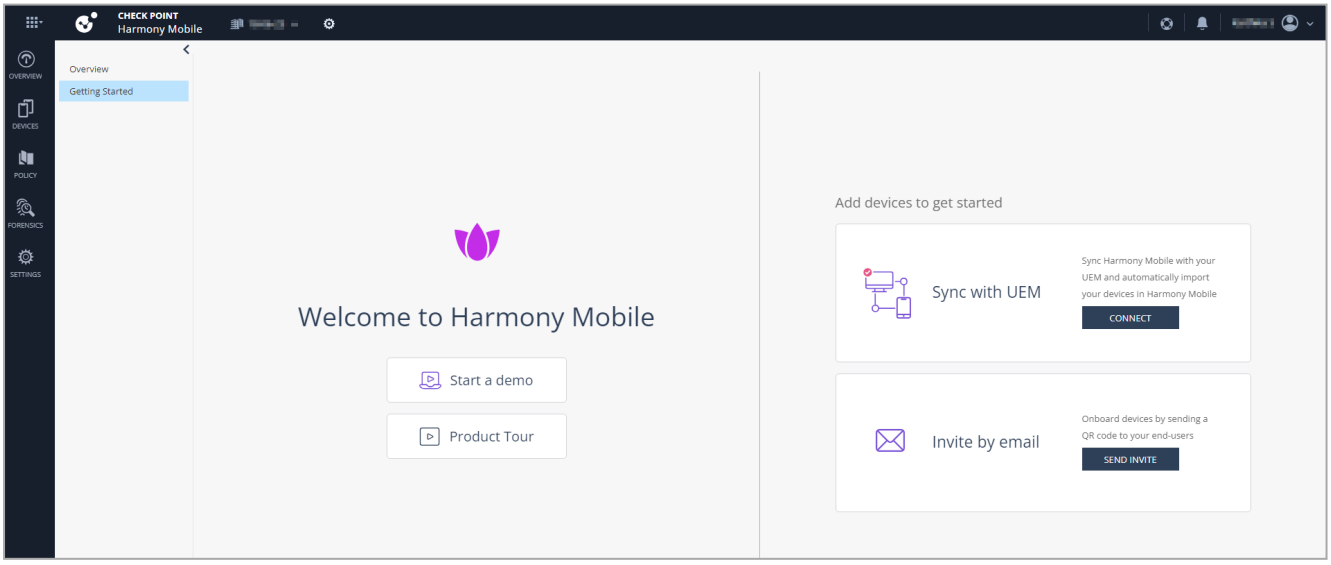
Widget	Description
Device Risk	Displays the number of devices in the organization that are currently at risk under these categories: ■ Total number of devices at risk ■ Number of devices at High risk ■ Number of devices at Medium risk ■ Number of devices at Low risk ■ Security events over time (last 7 days)
Device Status	Displays the number of devices registered in the dashboard under these categories: ■ Total number of devices ■ Active – Devices that have installed and activated the Harmony Mobile Protect app. **Note** - For an Android device, each profile (work and personal) is accounted as a device. For example, if an Android device has both work and personal profiles configured, and only the work profile is active, then the Devices Status shows 1 Active device and 1 Inactive device. ■ Inactive – Devices that have uninstalled the Harmony Mobile Protect app, or that the UEM has reported that the app is no longer installed. ■ Provisioned & User Notified – Devices where the user has been notified on where and how to install and activate the Harmony Mobile Protect app, or that the UEM has added the device to the system. ■ Device Registration - Devices registered in the last day and in the last week. ■ App Versions - Percentage of devices with the latest Mobile Security version installed. ■ License Info - Number of used licenses (includes active and inactive devices) and the total number of licenses available for your subscription. Each device consumes a license. **Notes** - ◦ An Android device with both work and personal profiles consumes a single license. For more information on how to account for licenses, see sk180953. ◦ To view the license information for Pay-as-you-go users, go to **Global Settings** > **Service & Contracts** > **Mobile Security**.

<table>
<tr><th>Widget</th><th>Description</th></tr>
<tr><td>Top Threats per device</td><td>Displays the top threats encountered by devices. The table shows:
<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Threat type</td><td>Type of threat factor that affected your devices.</td></tr>
<tr><td>Attack vector</td><td>Attack vector through which the threat factor affects the device:
Application
Device</td></tr>
<tr><td>Instances</td><td>Number of applications or devices affected by the specific threat type.
To view the security events details, click the instances count. The system displays the following:
For Device attack vector, the Forensics > Events & Alerts page appears and shows the list of devices with active events that have been reported, but not yet addressed.
For Application attack vector, the Forensics > Application page appears and shows the list of applications with the specific threat type.</td></tr>
<tr><td>Risk (%)</td><td>Percentage of the threat type determined by the risk levels assigned to it in the policies of affected devices, color-coded according to the risk levels.
In this example, the USB debugging enabled threat type is assigned High risk in one device policy and Medium risk in the policies of other devices.
 
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Widget</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Affected devices</td><td>Number of devices affected by the specific threat type and the corresponding risk level assigned to that threat type in the device policy.
For example, 2 mediumindicates that there are two devices affected with the specific threat type and that threat type is assigned Medium risk level in the device policy.
Note - This is the risk level caused by the specific threat type and not the overall device risk level.
To view the security events details, click the device count link. The Forensics > Events & Alerts page appears and shows the list of devices with active events that have been reported, but not yet addressed.</td></tr>
<tr><td>Devices (%)</td><td>The proportion of devices in your mobile fleet affected by the specific threat type.</td></tr>
</table>
</td></tr>
<tr><td>Security Events by Type</td><td>Displays the number of security events by their types (marked in colors) over time for last hour, day, or month and shows the total number of applications scanned from the devices enrolled to the dashboard.</td></tr>
</table>

Getting Started

If you have not added devices to the Mobile Security solution, then you are directed to the **Getting Started** page after you log in to the Mobile Security Administrator Portal.



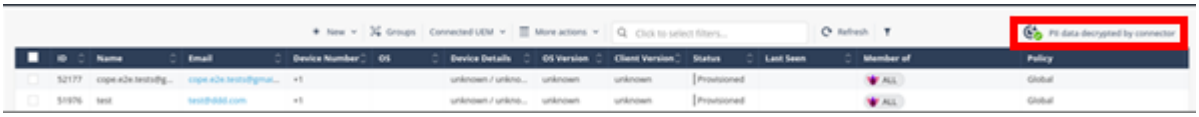
In this page, you can easily enroll new users and devices to Mobile Security using these methods:

- **Start a demo** – Experience connecting a single end-user and device.
- **Sync with UEM** – Connect Mobile Security to your preferred UEM and start synchronizing users and devices to Mobile Security.
- **Invite by email** – Invite a single or multiple users, or user groups to enroll to Mobile Security. Each user receives an email with the QR code and instructions for enrollment.

Devices

The **Devices** tab lists all organization-protected devices without filters. From this tab, you can add new devices, edit, import and export their details, and remove devices.

Note - For environments equipped with a Mobile Security Connector and with PII decryption enabled, an icon reflecting the status of the Connector appears on the top-right corner of the **Devices** screen.



The **Devices** table shows:

Item	Description
ID	A unique ID generated for each device upon installation of the Harmony Mobile Protect app. The system uses it as a reference to the device (instead of the device actual details for privacy). You can click device IDs that require attention to view the **Events & Alerts** page filtered for the device.
Name (Device Owner)	Device name given by the administrator when you send the registration link (or by UEM, if used for deployment).
Email	The email address registered to the device. When a new device is added, the system sends an email to the email address defined in the registration wizard. Any user logged in to a device using this email address receives a registration request and are directed to download the App from the **Google Play Store** (for Android) or the **Apple App Store** (for iOS). **Note** - The registration email is a one-time registration code. If the same email address is used for more than one device, only the first device that installs the App will be successfully registered. To register additional devices, you must send a new registration email to each one.

Item	Description
Device Number	The phone number of the device. It is configured by the administrator or set in UEM during the app installation link creation. This field is optional and is used only for identifying the device; it is not used by the system.
OS	The mobile device's operation system, based on the information received during Harmony Mobile Protect app installation. Values include: ■ iOS ■ Android ■ Android Enterprise
Device Details	Shows mobile device details such as device manufacturer and model, based on the information received post Harmony Mobile Protect app installation.
OS Version	OS Version on the mobile device, based on the information received post Harmony Mobile Protect installation.
Installed Patch	The security patch version installed on the Android device.
Client Version	The Harmony Mobile Protect app version currently installed on the mobile device.
Status	Displays the current status of the device: ■ **Processing** – A temporary state between manually adding the device and the Registration Invitation has been sent. ■ **User Notified** – The registration invitation has been sent, but the device is not yet registered. ■ **Provisioned** – The device was added via UEM but has not completed registration. ■ **Active** – Harmony Mobile Protect app is installed, the device was successfully registered and has been scanned. ■ **Inactive** – Harmony Mobile Protect app was installed and the device was registered, but the app was later removed, or the device has not connected to the dashboard for more than X days.

Item	Description
Last Seen	Indicates one of these: ■ Last time when the device contacted the Mobile Security server to check for updates. This occurs twice every 24 hours. ■ Last time when the user initiated a full scan from the Harmony Mobile Protect app on the device. **Notes** - ◦ Last time when the traffic, application, or a web page was blocked by the Harmony Mobile Protect app is not recorded under **Last Seen**. ◦ Devices with the **Last Seen** duration over two days require your attention.
Member of	The device groups to which the device is added. Device groups imported from UEM are labeled with the UEM logo.
Policy	Policy enforced on the device. **Note** - To verify whether the latest policy is enforced on the mobile device, check the time stamp of the last policy update on the Harmony Mobile Protect app: ■ In Android devices, tap the three dots ••• > **Settings** > **About**. ■ In iOS devices, tap the three dots ••• > **About** > **Policy**.
UEM	UEM that manages the device.

Adding a New Device

Overview

You can register devices in the dashboard by:

- Sending an invitation email from the **Devices** tab.

  The system sends the invitation to the registered email address that users must access from their device. To customize the email content, see *"Configuring Email and SMS Templates" on page 172*.

- **For iOS devices** - Users are redirected to install the Harmony Mobile Protect app from the App Store or to download the Enterprise signed App from the dashboard, based on the dashboard settings configured by Check Point. After installation, users must do the following to activate the app:

  a. Download iOS agent from the dashboard.

  b. Trust the Enterprise app.

  c. Enter the server details and registration code from the registration email.

  For more information, see Harmony Mobile Protect app for iOS User Guide.

- **For Android devices** - Users are redirected to Google Play Store to download the Harmony Mobile Protect app. The system automatically enters all registration information when using the download link in the email from the device.

  For more information, see Harmony Mobile Protect app for Android User Guide.

- Adding devices through UEMs. For more information, refer to the specific UEM in the Mobile Security UEM Integration Guide.

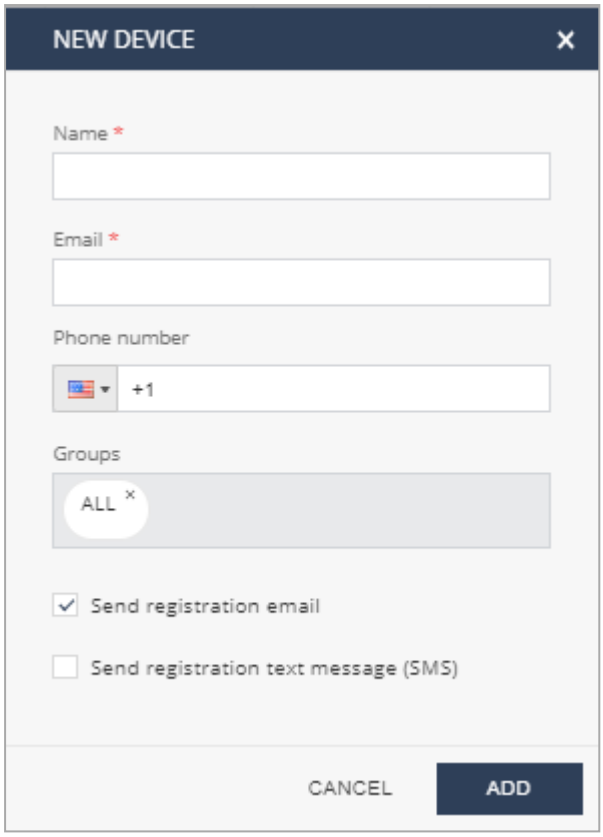
Note - Harmony Mobile Protect app requires certain permissions for the Mobile Security solution to operate on the end-user device. For more information, see *"Appendix D - Permissions for Harmony Mobile Protect app" on page 241*.

Procedure

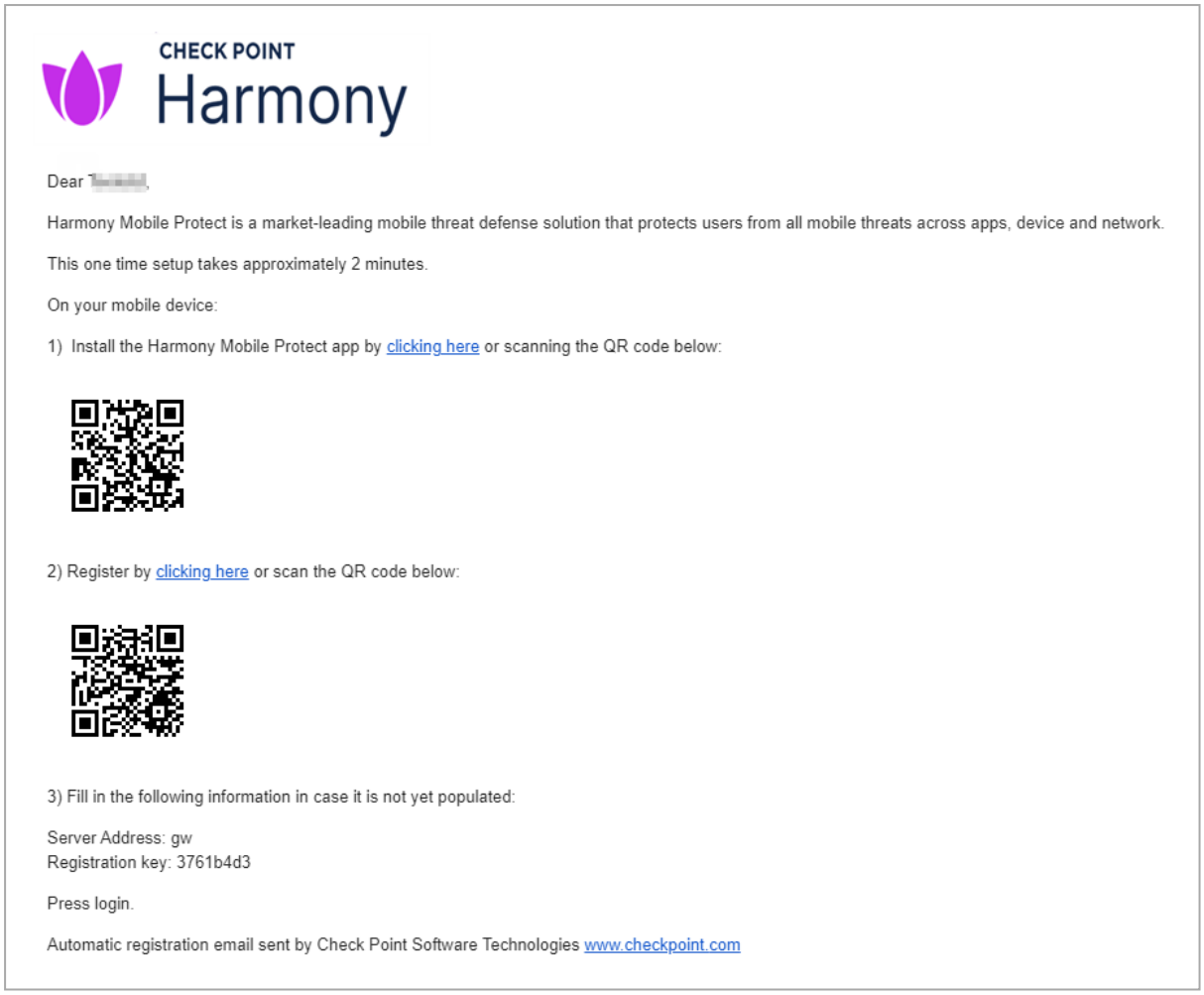
To add a new device:

1. Go to **Devices** > **New** and click **Add new device**.

   The **New Device** window appears.



2. Do these:
   - In the **Name** field, enter the device name.
   - In the **Email** field, enter the email address of the device owner.
   - In the **Phone number** field, enter the phone number of the device owner.
   - In the **Group** field, enter the device groups to which you want to add the device.
3. Click **Add**.
4. The system sends an email with the registration details and instructions to install the Harmony Mobile Protect app.



CHECK POINT
Harmony

Dear [redacted],

Harmony Mobile Protect is a market-leading mobile threat defense solution that protects users from all mobile threats across apps, device and network.

This one time setup takes approximately 2 minutes.

On your mobile device:

1) Install the Harmony Mobile Protect app by clicking here or scanning the QR code below:

2) Register by clicking here or scan the QR code below:

3) Fill in the following information in case it is not yet populated:

Server Address: gw
Registration key: 3761b4d3

Press login.

Automatic registration email sent by Check Point Software Technologies www.checkpoint.com

When the device is added to the dashboard, an entry appears in the Devices table with a unique device ID. The device status is displayed as **User Notified** until the Harmony Mobile Protect app is installed and the device has communicated with the dashboard.

ID	Name	Email	Device Number	OS	Device Details	OS Version	Client Version	Status
13333	Denis Diaz	denis@domain.com	+16548800064		unknown / unkn...	unknown	unknown	User Notified

When the App is successfully installed and run from the device, the registration screen appears.

If the registration is successful, the app performs a full device scan automatically. If no malware or malicious configurations are found, the app status appears in green. If the communication with the dashboard is successful, the device entry changes from **User Notified** to **Active**, and the device details gets updated.

ID	Name	Email	Device Number	OS	Device Details	OS Version	Client Version	Status
13333	Denis Diaz	denis@domain.com	+16548800064		OnePlus / HD1903	11	3.8.6.4611	Active

To import devices information from a CSV file:

1. To import devices in bulk from a CSV file, click **Import from file**.

   Important - CSV file format requirements:
   - The file must have a header row in this format:
     `name,email,number,group,send_reg_email,send_reg_sms`
   - Mandatory fields:
     - `name`
     - `email`
     - `send_reg_email`
     - `send_reg_sms`
   - If `send_reg_sms` is defined as TRUE, you must provide a phone number.
   - Use uppercase for TRUE/FALSE
   - For the `group` field, no need to add the **All** group in the CSV file as the system adds it automatically. Add only the required additional groups.

   Sample CSV template:
   ```
   name,email,number,group,send_reg_email,send_reg_sms
   John Smith,John@checkpoint.com,+123,,TRUE,TRUE
   Adam Smith,Adam@checkpoint.com,,Test-Group,TRUE,FALSE
   ```

2. Select the file and click **OK**.

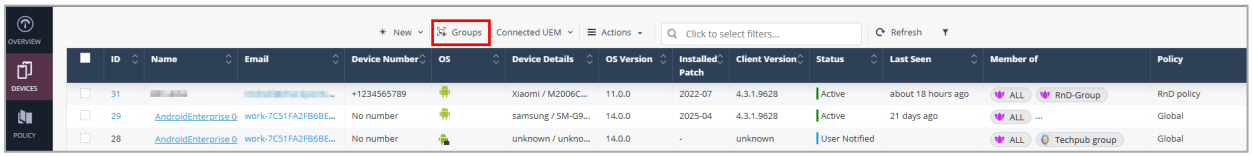
   The system imports the device details to the Devices table.

Adding a Device Group

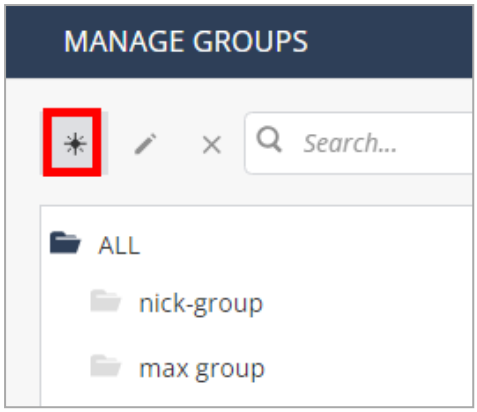
You can assign devices to appropriate device group when you add them to the system. You can also assign a group to the existing device.

To add a device group:

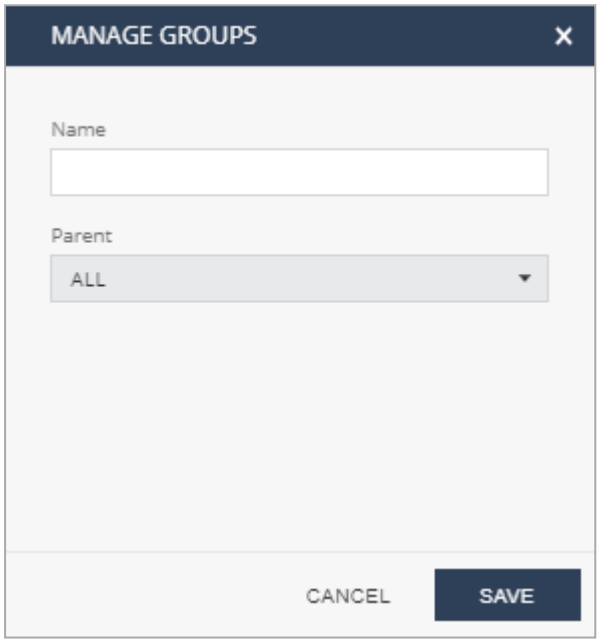
1. Go to **Devices** > **Groups**.



2. In the **Manage Groups** window, click ✳.



3. Enter the **Name** of the group and select the **Parent** group.



3. Click **Save**.

Devices and device groups are imported from the Device Management platform during the integration.

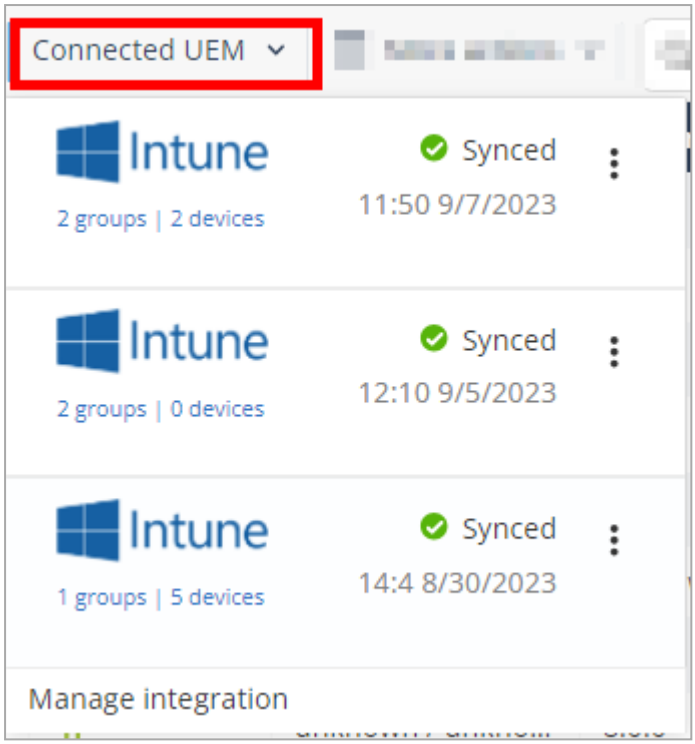
Viewing Connected UEMs

The **Connected UEMs** option allows you to view the sync status of the UEMs integrated with your tenant.

To view the connected UEMs:

1. Go to **Devices** > **Connected UEM**.

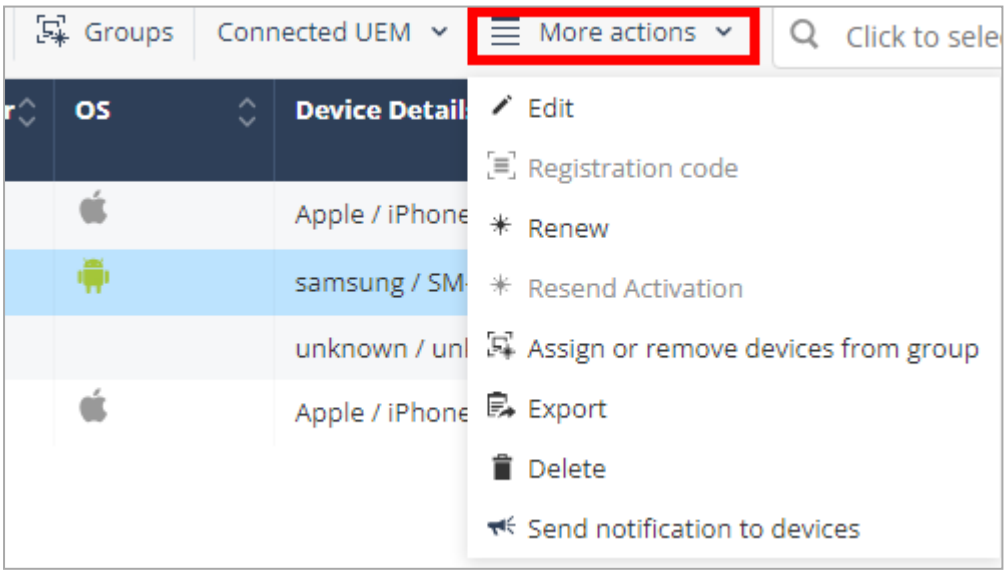
   The system shows a log of UEM syncs.



2. To force an immediate device sync without waiting for the next auto sync cycle, click ⋮ and then **Sync now**.
3. To temporarily stop or resume the device sync process, click ⋮ and then click **Pause** or **Resume**.

More Actions to Manage Devices

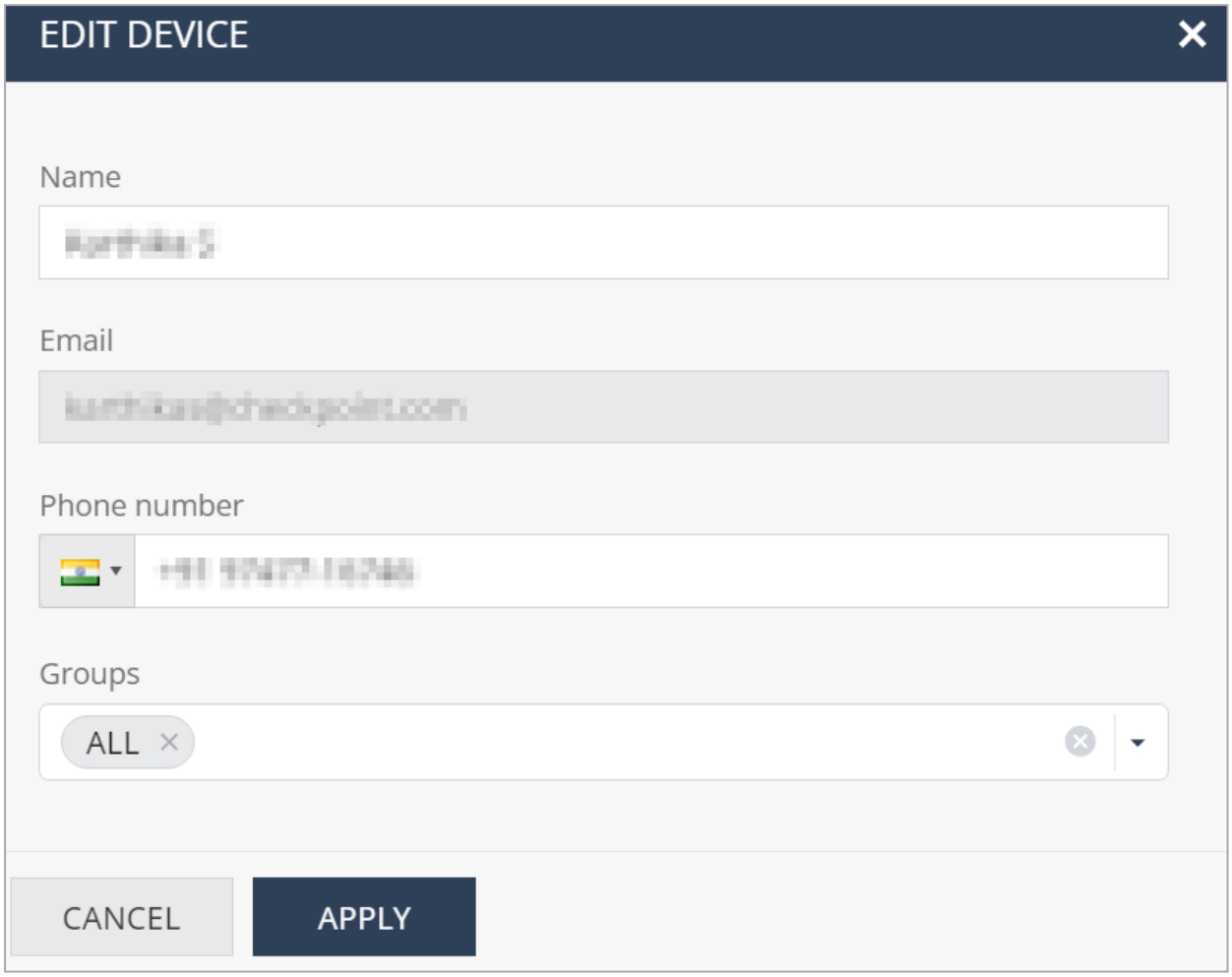
Go to **Devices** and click **More actions**.



Editing a Device

1. Select the device and click **More actions** > **Edit**.

   The **Edit Device** window appears.



2. Enter the required details and click **Apply**.

Generating a Registration Code to Enroll a New Device

1. Select the device and click **More actions** > **Registration code**.

   The **Registration Code** window appears.

2. Access the **Registration URL** or scan the QR code on your mobile device.
3. Click **OK**.

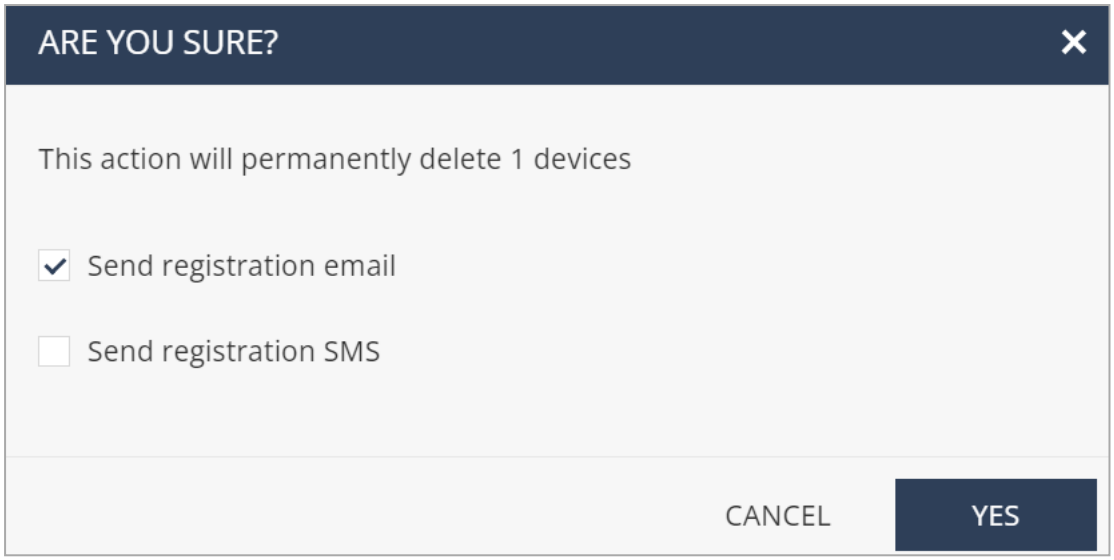
Renewing an Existing Device

The **Renew** option allows you to renew a device. It deletes a device, automatically adds the same device and send the registration information to the user, all in one click.

To renew a device:

1. Select the device and click **More actions** > **Renew**.

   The confirmation window appears.



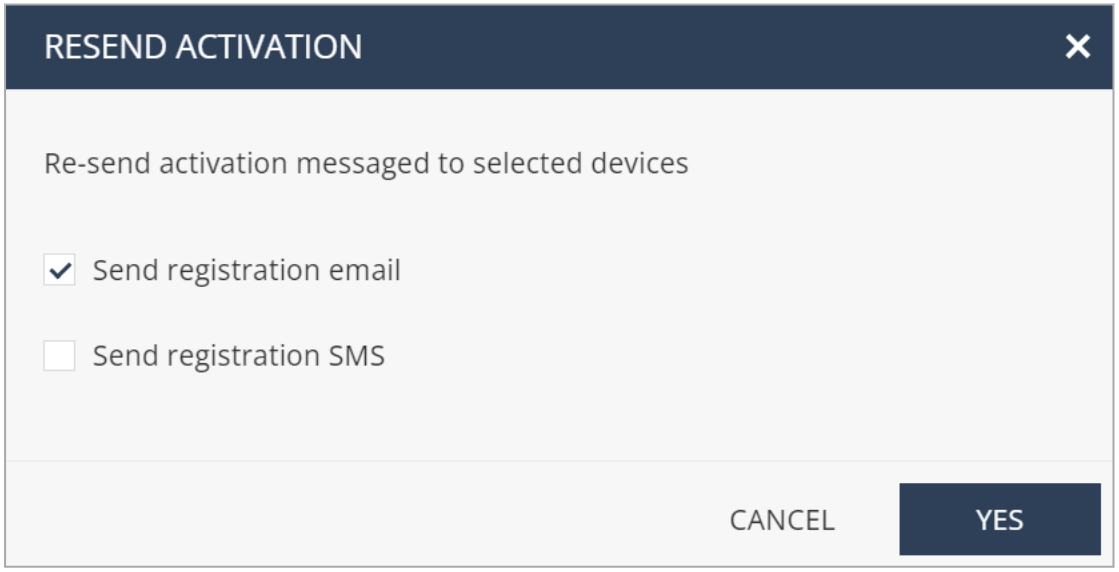
2. Select the method to send registration information to the user and then click **Yes**.

   The system deletes the device, automatically adds the device in the Mobile Security Administrator Portal with **Status** as **User Notified** and sends the registration information to the user.

Resending Activation Information to Provisioned Devices

1. Select the device and click **More actions** > **Resend Activation**.

   The **Resend Activation** window appears.



2. Select the method to send registration information to the user and then click **Yes**.

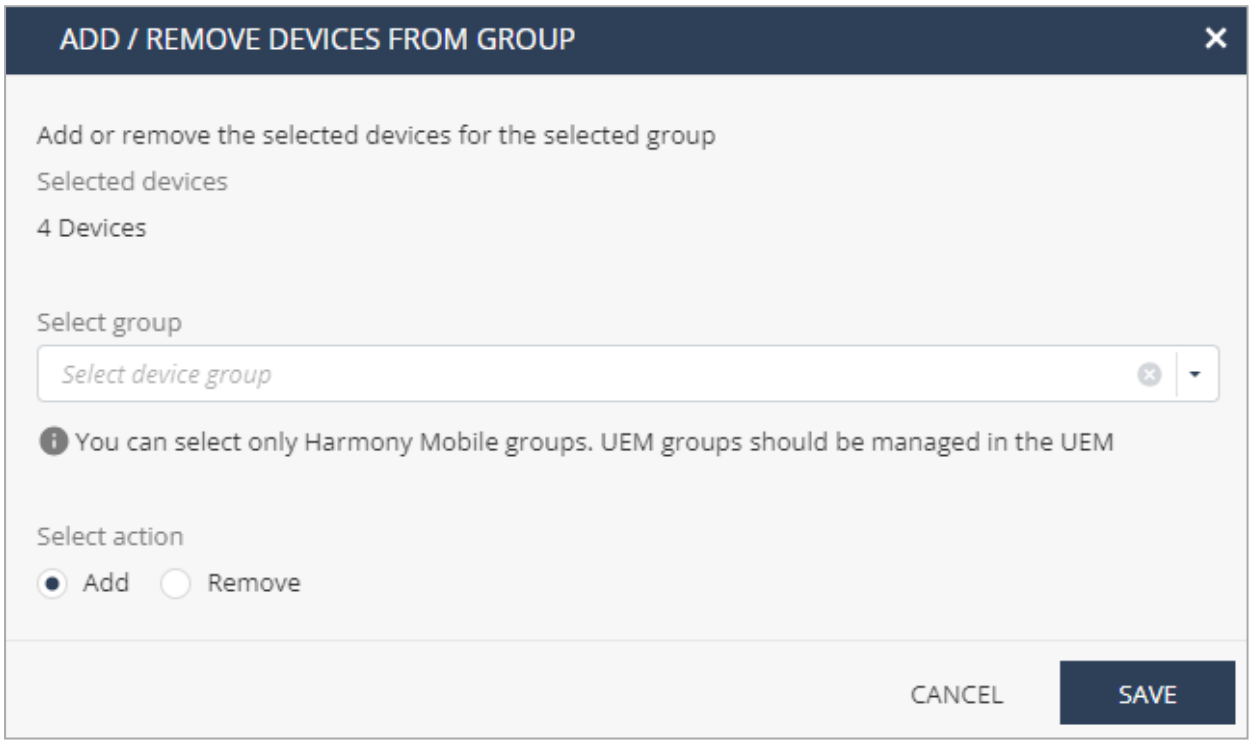
   The system sends the registration information to the user.

Adding/Removing Devices in a Device Group

Note - This procedure applies only to groups and devices added locally in the Mobile Security Administrator Portal.

1. In the Devices table, select the devices you want to add or remove.
2. Click **More actions** > **Assign or remove devices from group**.

   The **Add / Remove Devices From Group** window appears.

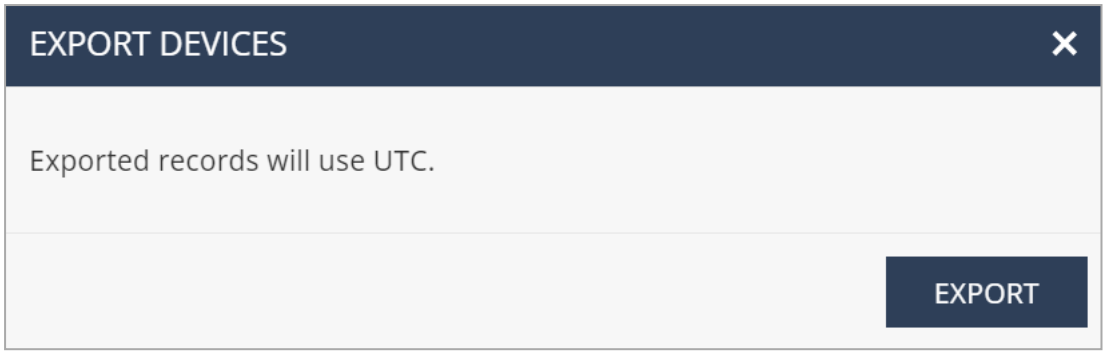


3. Select the device group and the required action.
4. Click **Save**.

Exporting Devices Information

1. In the Devices table, select the devices you want to export.
2. Click **More actions** > **Export**.

   The **Export Devices** window appears.



3. Click **Export**.

   The system generates and downloads a CSV file with the device information.

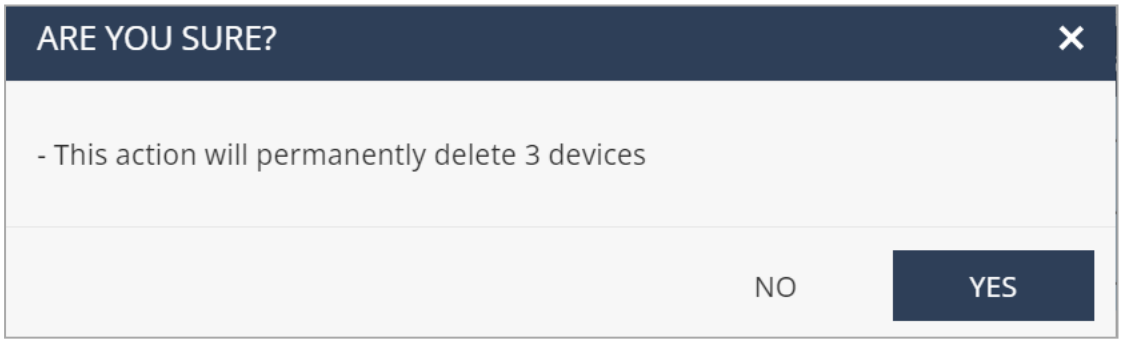
   If the number of devices exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days. For privacy reasons, PII data is obfuscated in the CSV file.

4. Click **Done**.

Deleting a Device

1. In the Devices table, select the devices you want to delete.
2. Click **More actions** > **Delete**.

   The confirmation window appears.



3. Click **Yes**.

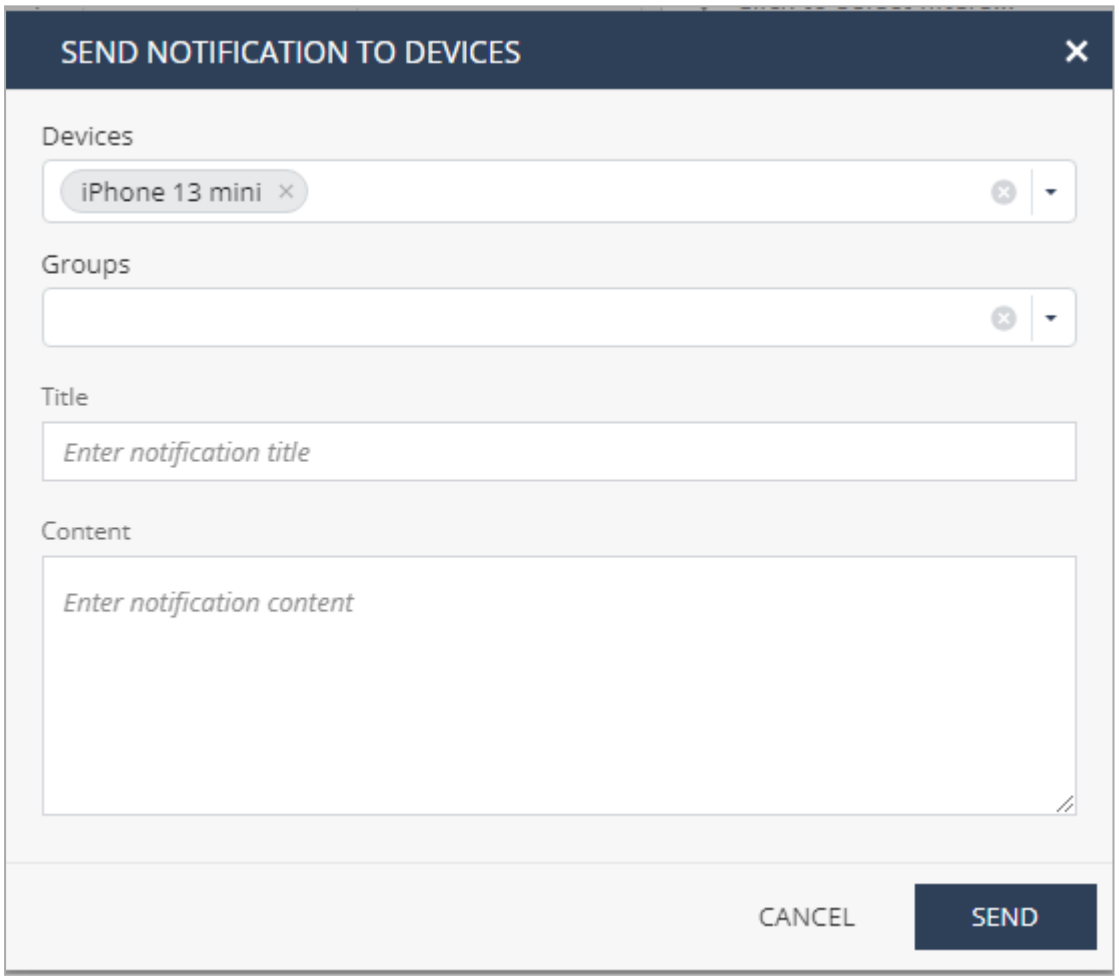
   The system deletes the devices from the Mobile Security Administrator Portal.

Sending Notification to Devices

Note - You can send notifications only to devices with **Status** as **Active**.

1. Select the devices from the **Devices** table.
2. Click **More actions** > **Send notification to devices**.

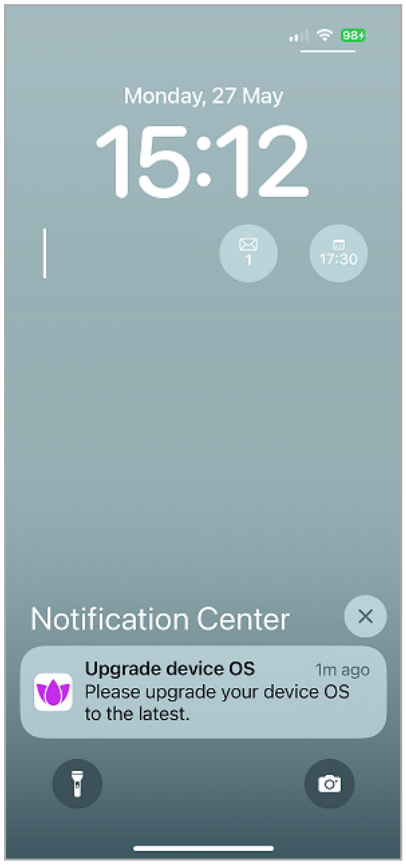
   The **Send Notification to Devices** window appears.



3. To send the notification to specific devices, from the **Devices** list, select the devices.

4. To send the notification to devices in a device group, from the **Groups** list, select the device group(s).
5. In the **Title** field, enter a title for the notification.
6. In the **Content** field, enter the message you want to notify the user.
7. Click **Send**.

   The system sends the notification to the selected device/device groups.



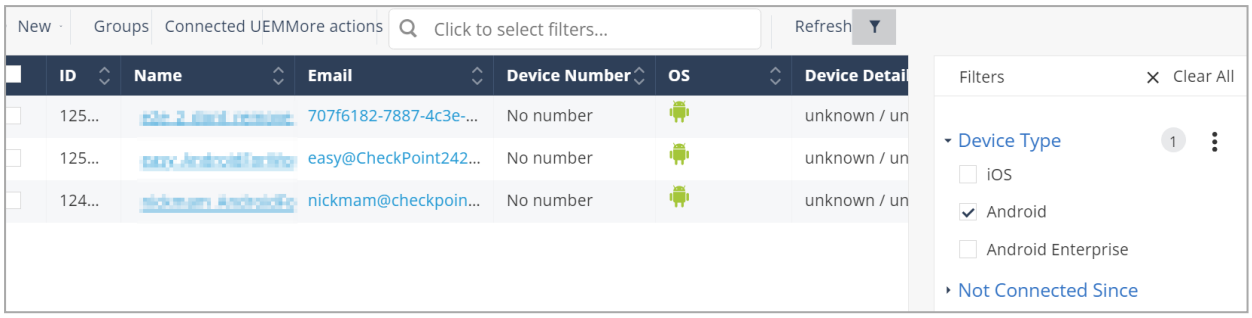
Note - Due to limitations with Android and iOS, Check Point cannot guarantee that notifications will be received or read on mobile devices.

Filtering Devices

To filter the Devices table:

1. Click above the Devices table.
2. On the **Filters** pane on the right side, select the required filters.

The Devices table shows information based on the selected filters.

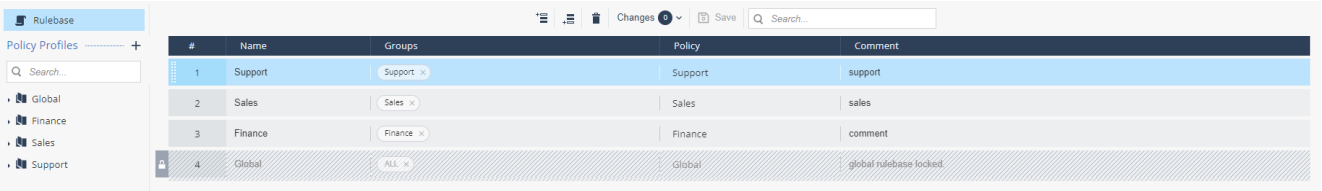


Policy

In the **Policy** tab, you can configure granular policies for different device groups. Granular policies let you apply stronger security controls to specific groups, for example, enable more security controls for your VIPs.

To create device groups, see *"Adding a Device Group" on page 42*. You can also apply policies to individual devices, but using groups allows better scalability.

To enforce the policy on the end-user device, the end-user or the UEM must grant the permissions listed in *"Permissions and Features Dependencies" on page 242*.



Note - To verify whether the latest policy is enforced on the mobile device, check the time stamp of the last policy update on the Harmony Mobile Protect app:

- In Android devices, tap the three dots ••• > **Settings** > **About**.
- In iOS devices, tap the three dots ••• > **About** > **Policy**.

Rulebase

When you open the **Policy** tab, the **Rulebase** displays a rulebase list with the **Global** policy profile as default.

When you add new policy profiles, they are added to the rulebase to apply them on the appropriate device groups.

The rules are processed in order from top to bottom (aka first-match). Once a match for the device is made, that policy is applied to the device. For example, if a device matches two policies, the highest-ranked matching policy is applied to the device.

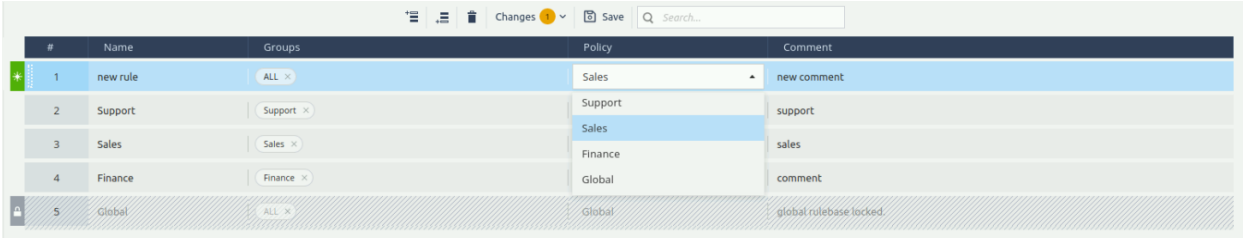
Best Practices:

- Place the most specific policies higher in the list.
- Keep the **Global** policy at the bottom of the list.
- To reorder policies, drag the rule number up or down.

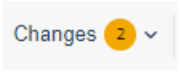
To activate a policy and apply it to a device group:

1. Click  or  .

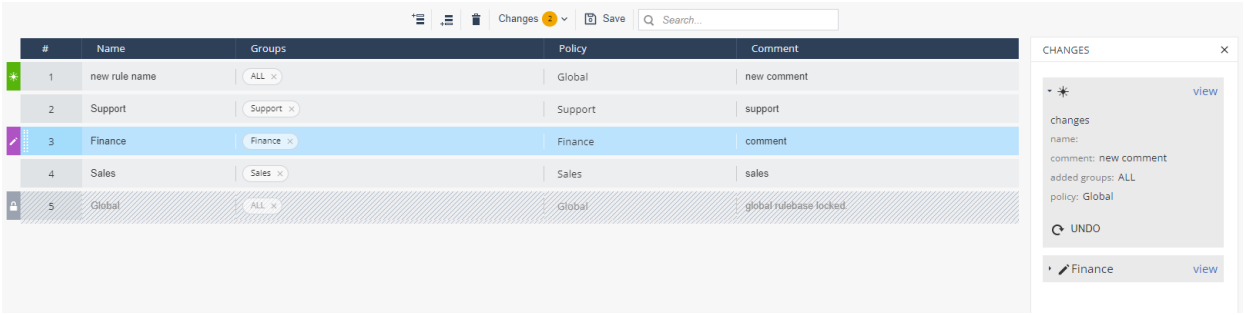
   A new line is added to the rulebase list.



2. Enter these:
   a. Rule Name
   b. Select the devices or device groups from the list.
   c. Select the policy profile from the list.

      For more information, see *"Policy Profiles" on page 56*.
   d. (Optional) Enter a comment.
3. Click **Save**.
4. To move a rule, click the rule # up or down, drag and drop as required.
5. To view all changes before you save them, click 

and then click **View Changes**.



6. Click **Save**.

Policy Configuration

You can set one of these risk levels to a device for a security event:

- Risk level (Default) - For example, **No Risk (Default)**.
- High (Device Alert)
- Medium (Device Alert)
- Medium (No Device Alert)
- Medium (Dismissive Device Alert)

- Low (No Device alert)
- No Risk

Notes:

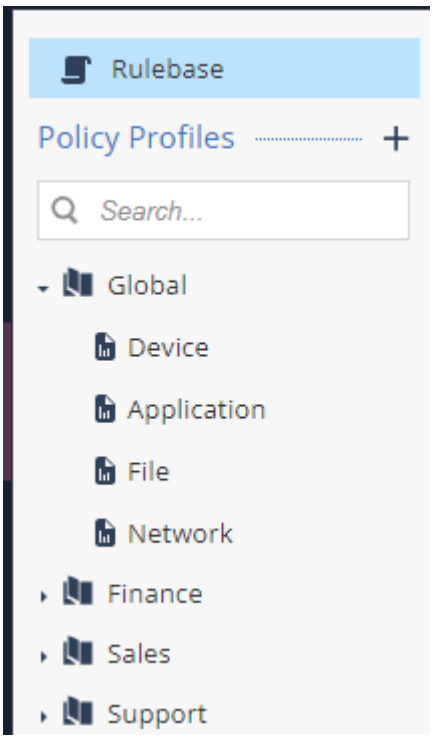
- **Risk level (Default)** – If you select a default risk level, the system automatically changes the default risk value based on its analysis.
- **Other risk values** - Administrator must set the value manually. The value does not change automatically by system detection.

Policy Profiles

Every policy profile that you create includes a pre-configured set of items to which the profiles apply:

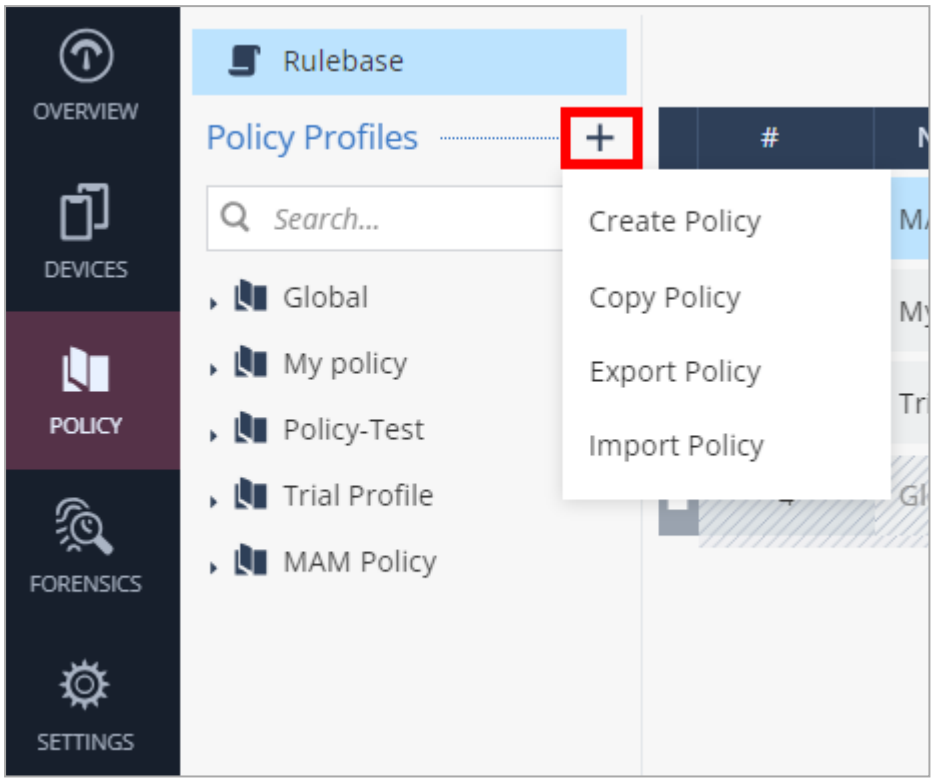
- Device. See *"Device Policies" on page 77*.
- Application. See *"Application Policies" on page 93*.
- File. See *"File Policies" on page 106*.
- Network Policies. See *"Network Policies" on page 113*.

Global policy profile is the default policy for all devices.



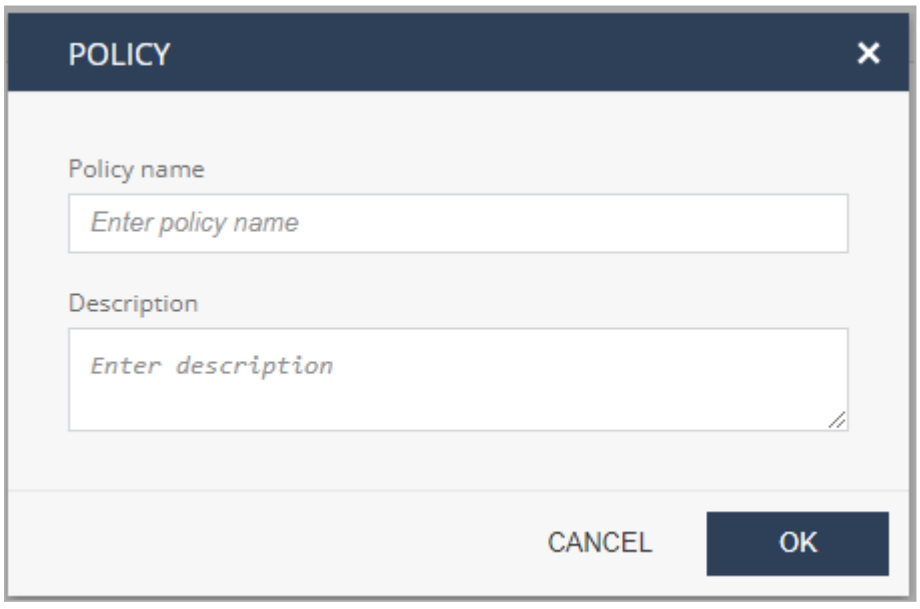
Creating a New Policy Profile

1. Go to **Policy** and click the **+** icon next to **Policy Profiles**.



2. Click **Create Policy**.

   The **Policy** window appears.



3. Enter a unique name and a description for the new policy.

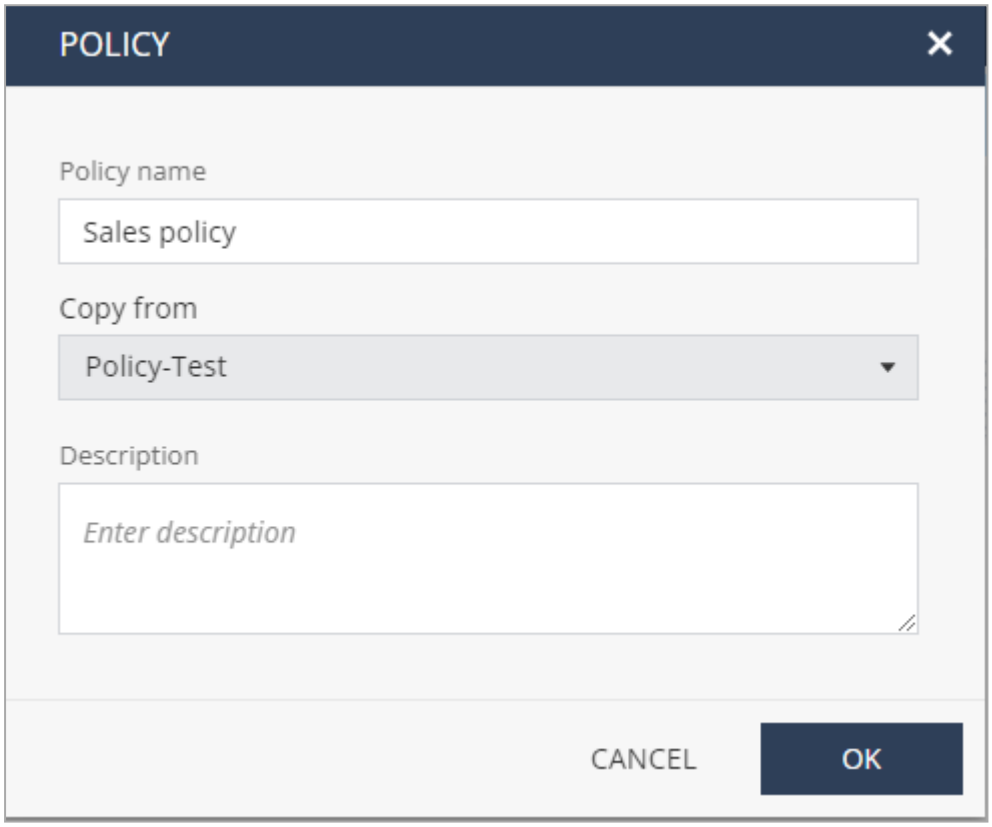
4. Click **OK**.

   The new policy is listed under **Policy Profiles**.

Copying an Existing Policy

1. Go to **Policy** and click the **+** icon next to **Policy Profiles**.
2. Click **Copy Policy**. Optionally, you can hover over the policy name and click the icon.

   The **Policy** window appears.



3. Enter a name for the new policy.
4. From the **Copy from** list, select the policy that you want to copy.
5. Enter a description.
6. Click **OK**.

You can edit the policy in the profile editing view, or edit it at any time on the **Policy Profiles** list.

To activate the policy, see *"Rulebase" on page 53*.

Exporting and Importing a Policy

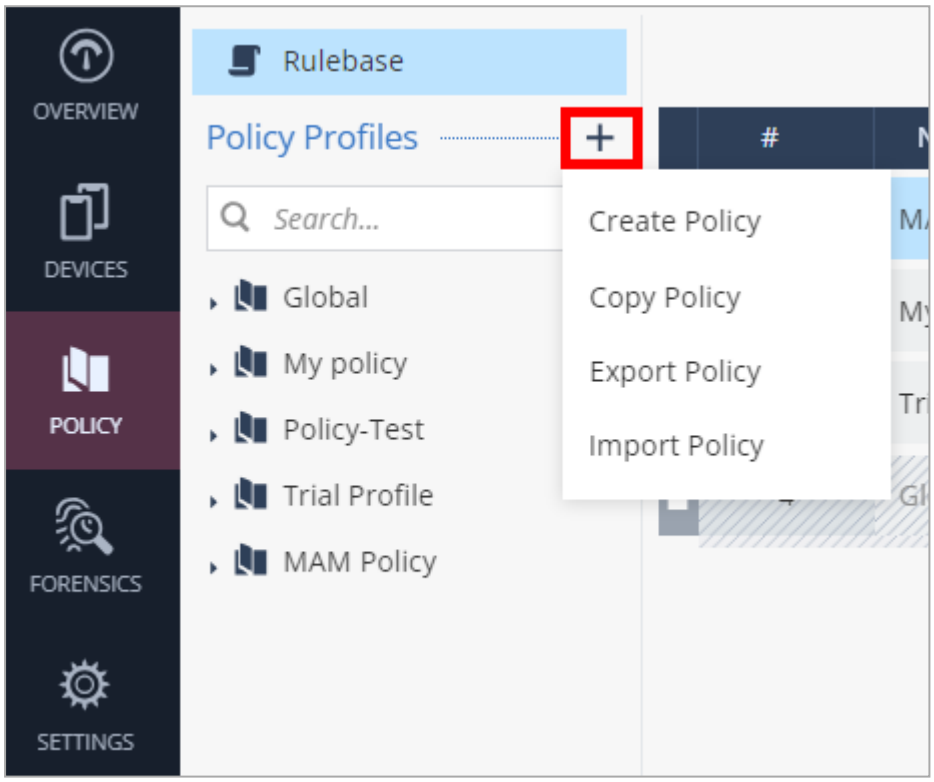
You can export a policy from one tenant and import it to another tenant, regardless of their data residency regions.

Use Cases

- You are a Managed Security Service Provider (MSSP) with multiple customers/tenants and want to use the same policy for all of them. You can configure the policy in one tenant, export it, customize (if required) and then import it to other tenants.
- Your organization has tenants in different data residency regions and wants to use the same policy for all of them.

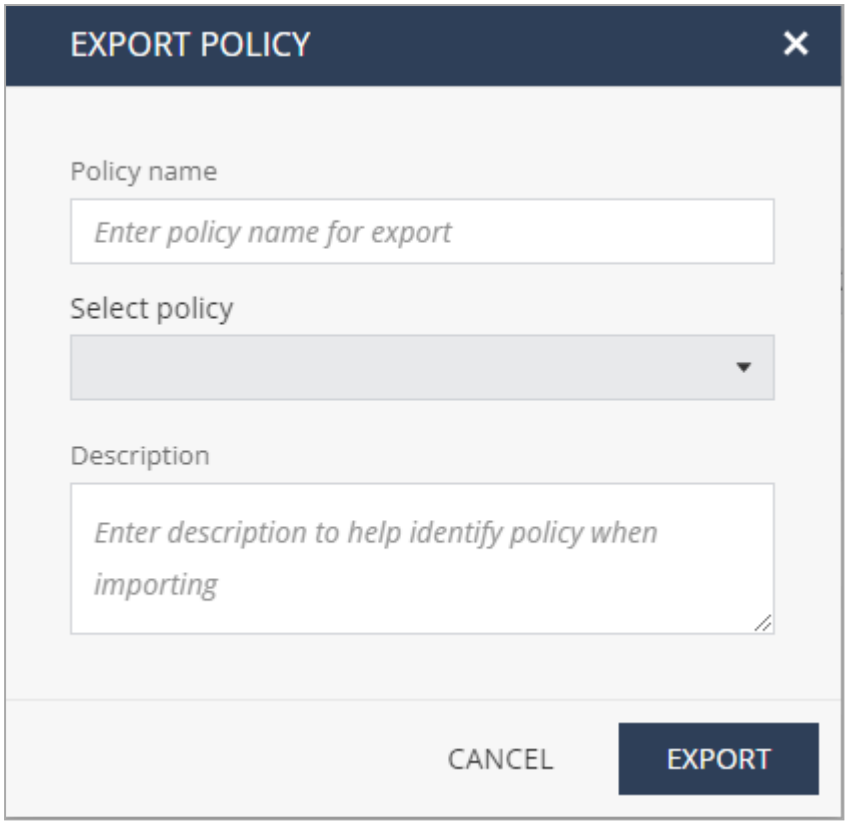
Exporting a Policy

1. Go to **Policy** and click the **+** icon next to **Policy Profiles**.



2. Click **Export Policy**.

   The **Export Policy** window appears.



3. In the **Policy name** field, enter a name to save the exported policy.

   Note - This is the name of the policy when it is imported to another tenant.

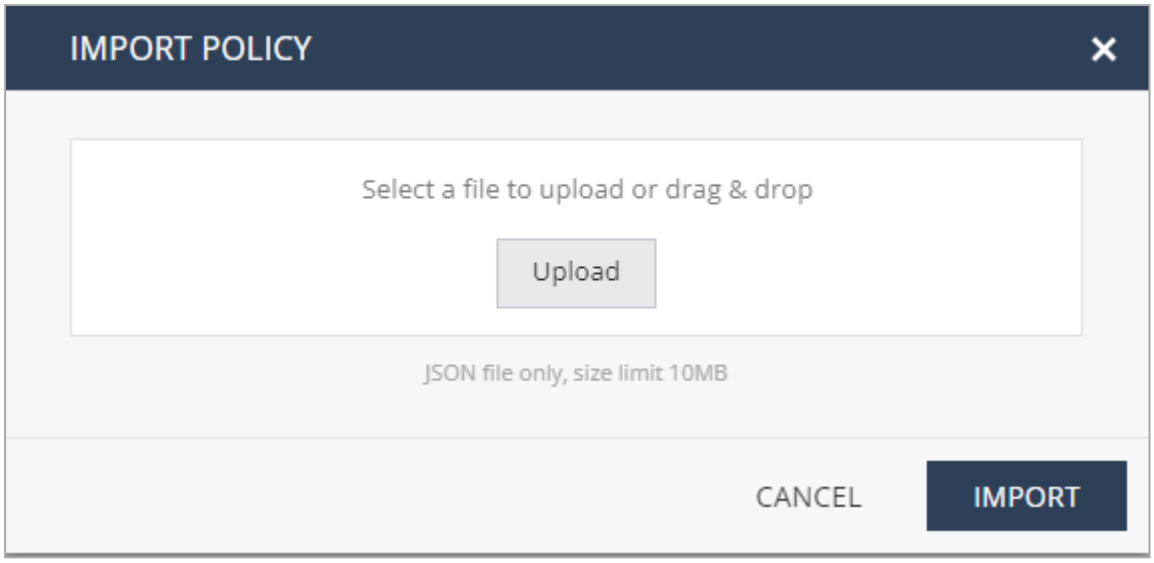
4. From the **Select policy** list, select the policy that you want to export.
5. In the **Description** field, enter a description to identify the policy.
6. Click **Export**.

   The system exports the policy and saves it as a JSON file on your computer.

Importing a Policy

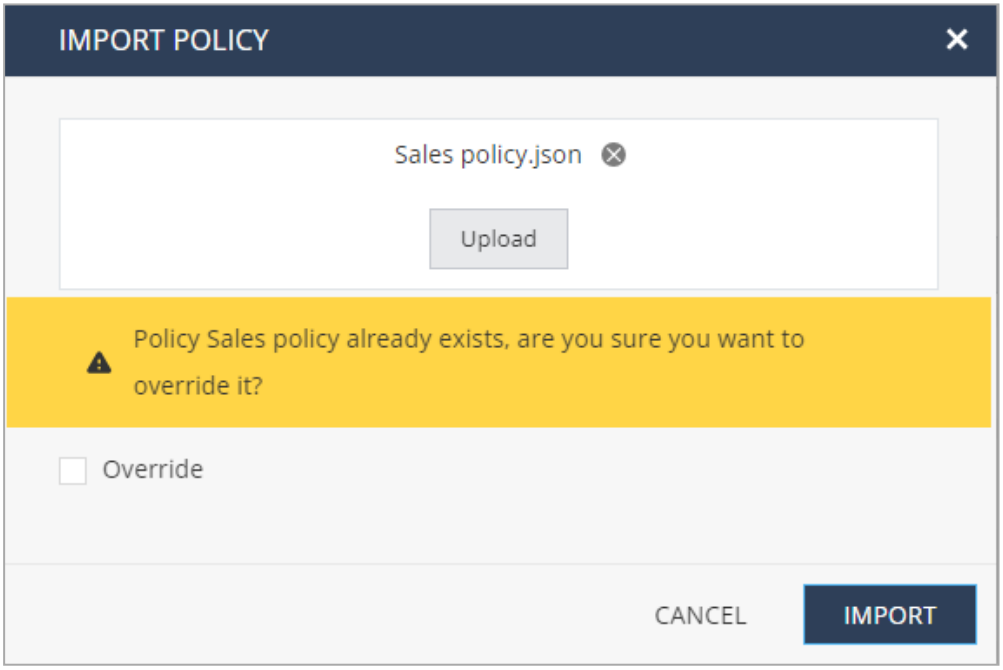
1. Go to **Policy** and click the **+** icon next to **Policy Profiles**.
2. Click **Import Policy**.

   The **Import Policy** window appears.



3. Click **Upload** and select the policy file. Optionally, you can drag and drop the file from its location.

   Notes:
   - The only supported file type is JSON, with maximum size of 10 MB.
   - If the same policy name exists in your tenant, the imported policy overrides it.

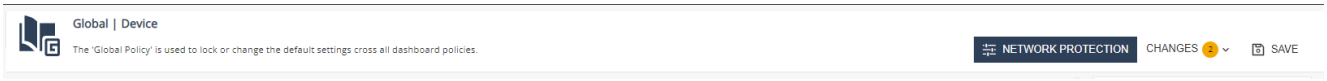
   

   To override the existing policy, select the **Override** checkbox.

4. Click **Import**.

   The system imports the policy to your tenant and lists it in the **Policy Profiles** section.

Policy Header



The policy header contains:

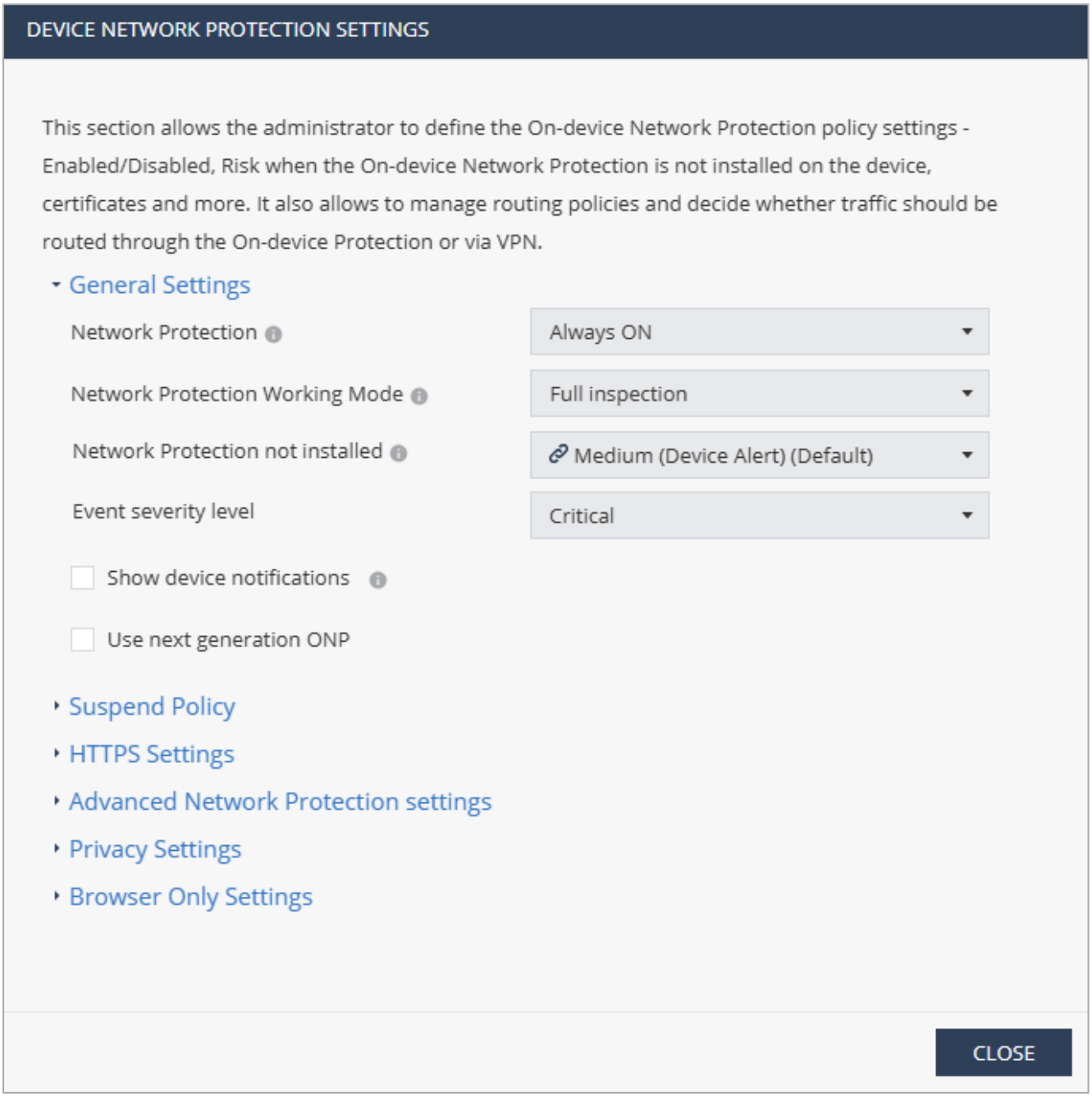
1. **Policy Name**
2. **Policy Description**
3. **Network Protection** - Allows to configure On-device Network Protection configurations
4. **Changes** - Display unsaved changes
5. **Save** - Saves all the new configurations the admin made

Network Protection

You can define the **On-device Network Protection** (ONP) policy settings to manage traffic routing policies and decide whether to route traffic through the On-device Protection or through a configured VPN.

Network protection settings are configured on policy profile level. One policy profile may have ONP enabled and another one may be configured without ONP.

Note - ONP cannot work when a proxy server is configured on the mobile device.



General Settings

To set general settings for network protection:

1. Go to **Policy** and expand a policy profile.
2. Click any one of these:
   - Device
   - Application
   - File
   - Network
3. Click **Network Protection** > **General Settings** and set these parameters:

Item	Description	Value
Network Protection	Enable or disable On-device Network Protection (ONP) through VPN.	■ **OFF** - Disables ONP. ■ **Always ON** - Enables ONP by default. To configure this behavior, go to **Configure** > **Advanced Configuration**. ■ **Turn ON when a device is at High risk** - Enables ONP automatically when the device's risk level changes to **High**. It is turned off automatically when the device's risk level is lowered to **Medium** or **Low**.

Item	Description	Value
Network Protection Working Mode	Set the ONP working mode. This setting is active only if the **Network Protection** is set to **Always ON** or **Turn ON when a device is at High risk**.	■ **Full inspection** (Default) - Enables ONP for the entire device network traffic. ■ **Browser only** - Enables ONP for specific browsers only. To select the browsers, go to *"Browser Only Settings" on page 74*. ■ **Detect mode** - Evaluates ONP before you enable it on the user device. Monitors the device traffic and does not block malicious traffic. If malicious traffic is detected, it is logged in **Forensics** > **Events & Alerts**. Detect Mode is not supported for Zero-day Phishing Detection and File Protection. ■ **Proxy mode** - Enables ONP for web traffic (example, HTTP and HTTPS). **Best Practice** - We recommend to use Detect mode for a certain period to only monitor traffic and identify malicious content. After this period, you must use the **Full inspection** or **Browser only** mode to block malicious traffic automatically.
Network Protection not installed	Set the device risk status when ONP is not installed.	■ Medium (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Event severity level	Set the risk level for ONP generated events.	■ Information (Default) ■ Critical ■ Warning ■ Information
Show device notifications	Indicates whether to show device notification if a network resource is blocked.	N/A

Item	Description	Value
Use next generation ONP	Enables the next generation ONP for iOS. For more information on the new ONP, see sk183634.	When you enable this option, the next generation ONP replaces the legacy ONP.

The table below lists the features available for the configured **Network Protection Working Mode**:

Feature	Network Protection Working Mode	
	Full inspection	Browser only
Anti-Bot	Yes	No
Phishing	Yes	Yes
Zero phishing	Yes	Yes
File download prevention	Yes	Yes (except Safari extension)
MiTM detection	Yes	Yes
Safe DNS (aka Protected DNS)	Yes	No
Block app traffic (on Android)	Yes	No
Content filtering (aka URLF)	Yes	Yes
Port scan detection	Yes	No

Feature	Network Protection Working Mode	
	Full inspection	Browser only
Zero-Touch support	Yes	Yes (except Safari extension)
Network Protection snooze by user	Yes	No
Conditional access	Yes	Applicable only to web traffic.

Suspend Policy

You can allow end-users to temporarily suspend ONP from the Harmony Mobile Protect app on their device for different periods of time. The options are 5 minutes, 30 minutes or 2 hours.

To allow users to suspend ONP:

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application
   - File
   - Network
3. Click **Network Protection** > **Suspend Policy** and set these parameters:

Item	Description	Value
Suspend severity level	Set the device risk level if the user suspends ONP on the device. **Note** - You cannot set the risk level to **High**. When a device moves to **High** risk, Mobile Security automatically restores ONP to enforce conditional access policy. This creates a conflict as ONP is restored automatically after the end-user suspends it.	■ No Risk (Default) ■ Medium (Device Alert) ■ Medium (Dismissive Device Alert) ■ Medium (No Device Alert) ■ Low ■ No Risk
Allow user to suspend On-device Network Protection	Select the checkbox to allow a user to suspend ONP on the device and set the duration for which the user can suspend ONP. When the user suspends ONP, the system reports an event in the **Events & Alerts** page.	■ 5 minutes ■ 24 hours ■ Unlimited

Item	Description	Value
Automatically suspend when	Set when to automatically suspend ONP.	Select one of these: ■ **Never** - Enables ONP even if other VPNs are detected. ■ **Any VPN is connected** - Automatically suspends ONP when VPN is detected. ONP resumes after 2 hours, or earlier if the VPN is disconnected within that time. ■ **Corporate resource is connected via VPN** - Suspends ONP only if VPN that allows access to corporate URLs (from the corporate resources table) is detected. ONP resumes when there is no traffic towards the corporate URL.

4. To save the policy changes, click **Save**.

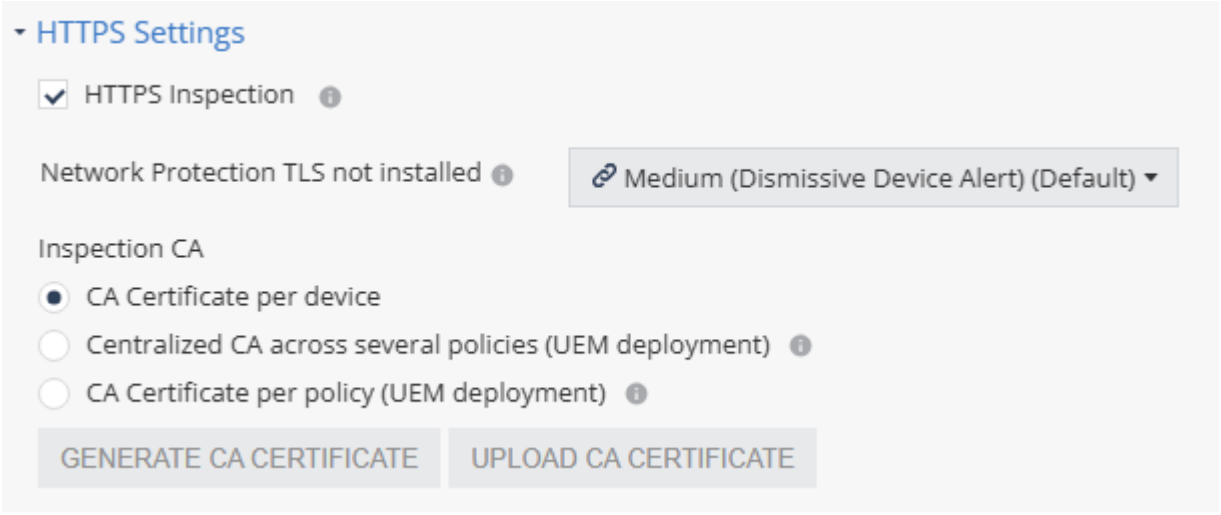
HTTPS Settings

Note - SSL inspection is not applied to sites:

- Categorized as *Finance* and *Health*, due to sensitive information.
- Listed in the Allowed Locations exception list. The system checks the Server Name Indication (SNI) to allow or block the traffic.

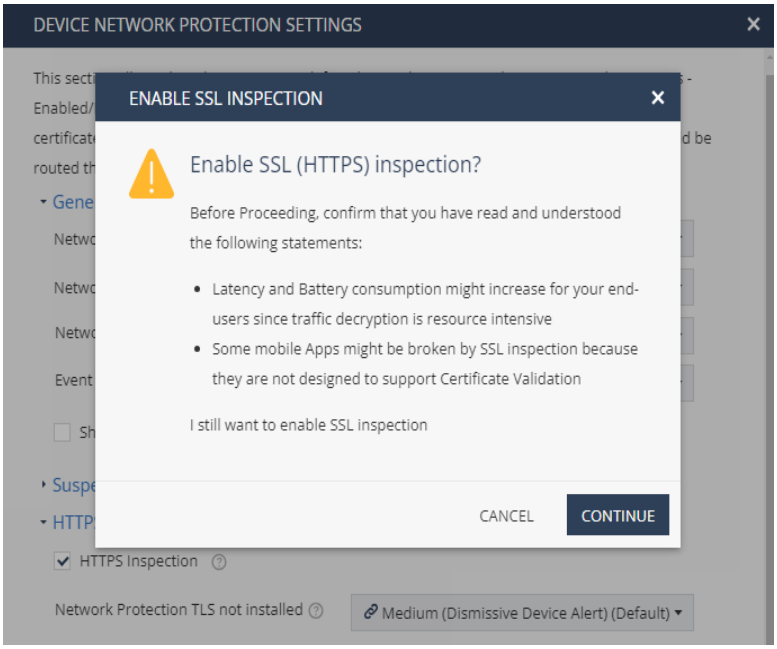
To configure HTTPS settings:

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application
   - File
   - Network
3. Click **Network Protection** > **HTTPS Settings**.



4. To enable SSL inspection, select the **HTTPS Inspection** checkbox.

   The **Enable SSL Inspection** window appears.



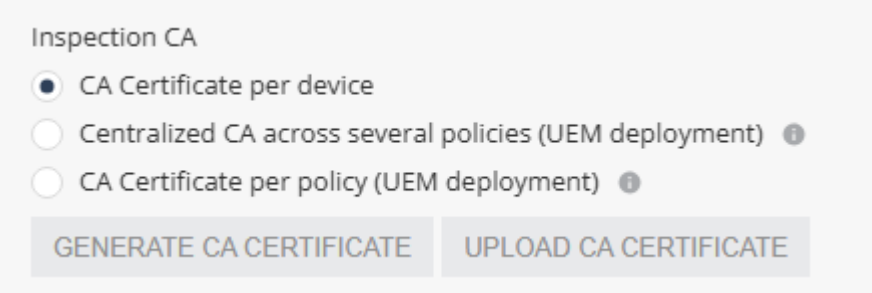
Notes -

- For Mobile Security/ONP to decrypt the HTTPS traffic, the mobile apps and browsers must support users' CA certificate.
- The browsers that support SSL inspection on Android are:

Browser Name	Package Name
Brave Browser	com.brave.browser
Bromite Browser	org.bromite.bromite
Chrome Beta	com.chrome.beta
Chrome Canary	com.chrome.canary
Chrome Dev	com.chrome.dev
Chromer	arun.com.chromer
Ecosia Browser	com.ecosia.android
Google Chrome	com.android.chrome
Huawei Browser	com.huawei.browser
Kiwi Browser	com.kiwibrowser.browser
Microsoft Edge	com.microsoft.emmx
Naked Browser	com.fevdev.nakedbrowser
Naked Browser LTS (Light)	com.fevdev.nakedbrowserlts
Opera Browser	com.opera.browser
Samsung Internet Browser	com.sec.android.app.sbrowser
Samsung Internet Browser Beta	com.sec.android.app.sbrowser.beta
Vivaldi Browser	com.vivaldi.browser
Yandex Browser	com.yandex.browser

5. Click **Continue**.
6. From the **Network Protection TLS not installed** list, select the risk level if CA certificate is not installed or not trusted on the device.

7. In the **Inspection CA** section, select the CA certificate that ONP will use to inspect HTTPS traffic on the end-user device.



Select one of these:

- **CA Certificate per device** - Allows you to generate a unique certificate for each device. The user must manually install the certificate on the device when installing the Harmony Mobile Protect app.
- **Centralized CA across several policies** - Allows you to use the centralized CA certificate across several policies. To generate the centralized CA certificate, go to **Settings** > *"Central HTTPS Inspection Root CA" on page 174*.

  Note - If you initially chose to use a centralized CA certificate but later changed to a different CA certificate option:
  - The current policy will no longer use the centralized certificate.
  - The centralized CA certificate remains active and continues to be associated with all other policies in your account.

- **CA Certificate per policy** - If your organization uses a UEM, you can generate a new CA certificate for each policy, download and deploy it on the end-user device through UEM.
  - To generate a CA certificate issued by Check Point, click **Generate CA Certificate**. The new certificate is valid for one year from the current date, as shown in **Expiration date**.
  - To use a self-signed or a third-party CA certificate, click **Upload CA Certificate**.

    For the Transport Layer Security (TLS) certificate to be valid:
    - The certificate must have a lifecycle of at least 30 days and not longer than 390 days.
    - The certificate must be valid for more than 30 days from the time it is uploaded to the Mobile Security Administrator Portal.

  Note - Check Point recommends you renew the CA certificate at least two weeks before the expiration date. To renew the CA certificate, see sk181288.

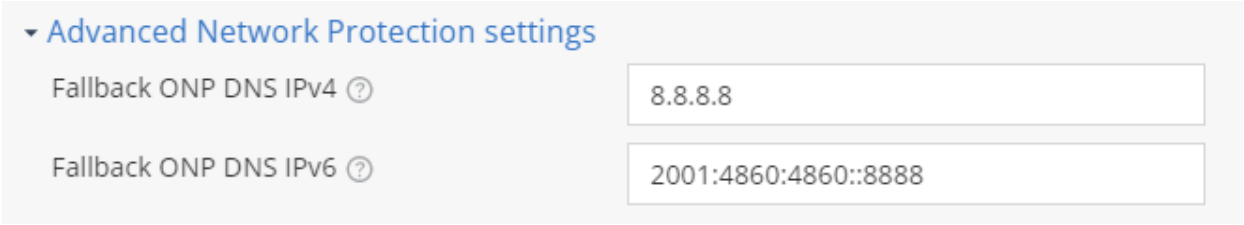
8. To save the policy changes, click **Save**.

Advanced Network Protection Settings

You can configure a fallback DNS server for ONP when the device's DNS server is not available.

To configure a fallback DNS server for ONP:

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application
   - File
   - Network
3. Click **Network Protection** > **Advanced Network Protection settings**.



   By default, the system uses a public DNS server IP address.
4. To use a private or a different public DNS server, modify the IP addresses in these fields:
   - **Fallback ONP DNS IPv4** - Fallback DNS server IP address in IPv4 format.
   - **Fallback ONP DNS IPv6** - Fallback DNS server IP address in IPv6 format.

     If the fallback DNS server address in IPv4 or IPv6 format is not available, the system uses the default public DNS server IP address.
5. To save the policy changes, click **Save**.

Privacy Settings

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application

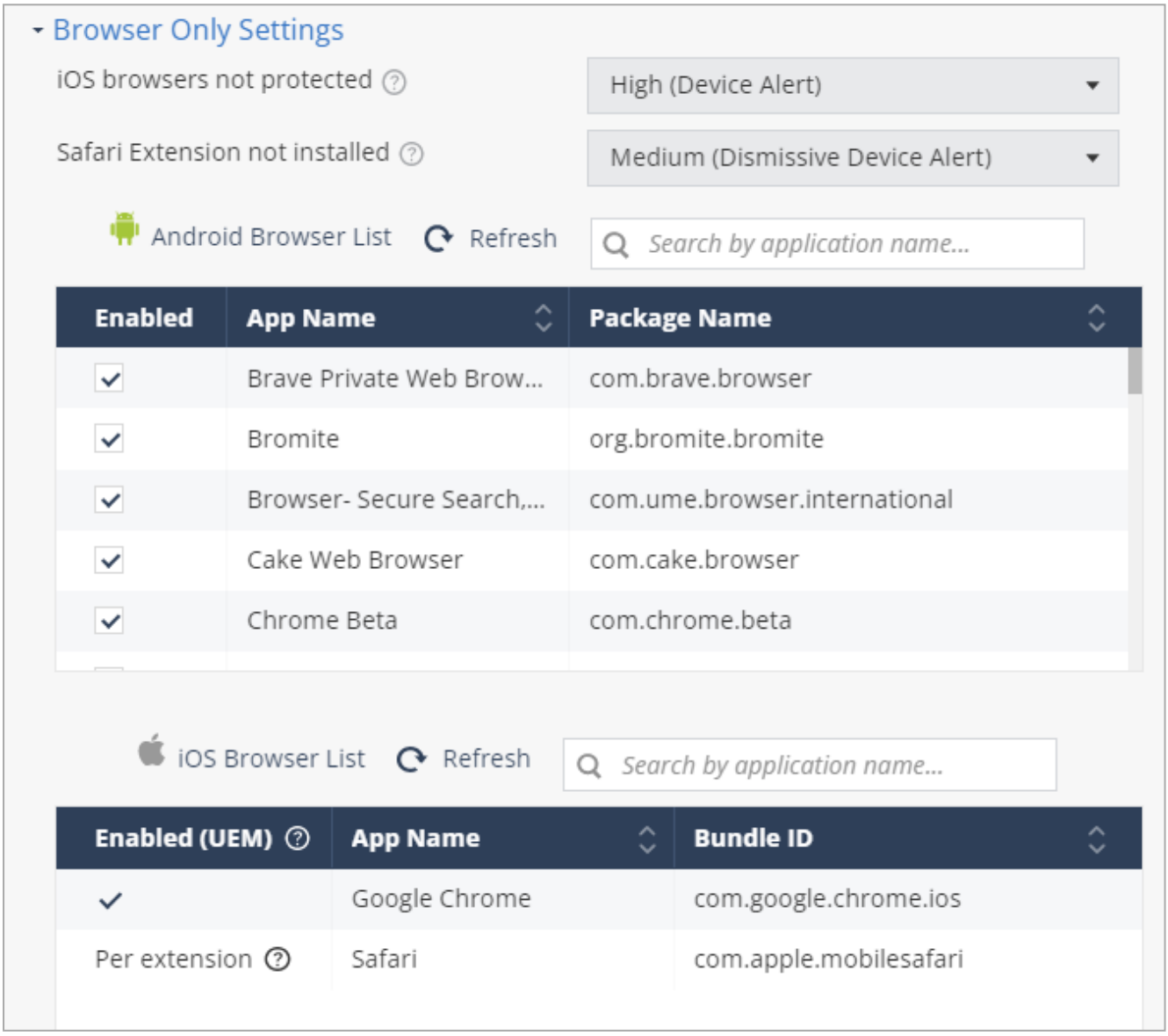
- File
- Network

3. Click **Network Protection** > **Privacy Settings**.
4. Select the **Hide browsing details** checkbox to hide device browsing details.
5. To save the policy changes, click **Save**.

Browser Only Settings

In this section, you can set the risk levels for iOS devices and enable or disable ONP for specific browsers. To enable these settings, you must set **Network Protection Working Mode** as **Browser only**. For more information, see *"General Settings" on page 64*.

For queries on operating your corporate VPN and **Browser only** VPN in tandem, contact Check Point support.



To set the risk level for iOS devices:

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application
   - File
   - Network
3. Go to **Network Protection** > **Browser Only Settings** and set these parameters:

Item	Description	Value
iOS browsers not protected	Set the risk level if the iOS browsers are not protected on the device.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Safari Extension not installed	Set the risk level if the Safari browser extension is not installed on the device.	

4. To save the policy changes, click **Save**.

Enabling ONP for Browsers Supported by Android Devices

For Android devices, the supported browsers are listed in the **Android Browser List** table. You can enable or disable ONP for these browsers from the Mobile Security dashboard.

1. Go to **Policy** and select a policy profile.
2. Click any one of these:
   - Device
   - Application

- File
- Network

3. Go to **Network Protection** > **Browser Only Settings**.

   By default, ONP is enabled for all the browsers.

4. To disable ONP for a browser, clear the checkbox. The system saves the changes automatically and applies them to the device immediately.

   When you disable ONP for a browser installed on any of the active devices, a warning message appears.

Note - To request ONP for a browser that is not in the **Android Browser List** table, contact Check Point Support.

Enabling ONP for Browsers Supported by iOS Devices

For iOS devices, the supported browsers are listed in **Policy** > **Network Protection** > **Browser Only Settings** > **iOS Browser List** table.

Use the **Per App VPN** setting in the UEM to enable or disable ONP for a browser. After you enable ONP for a browser in the UEM, it takes up to two hours for the system to add it in the **iOS Browser List** table.

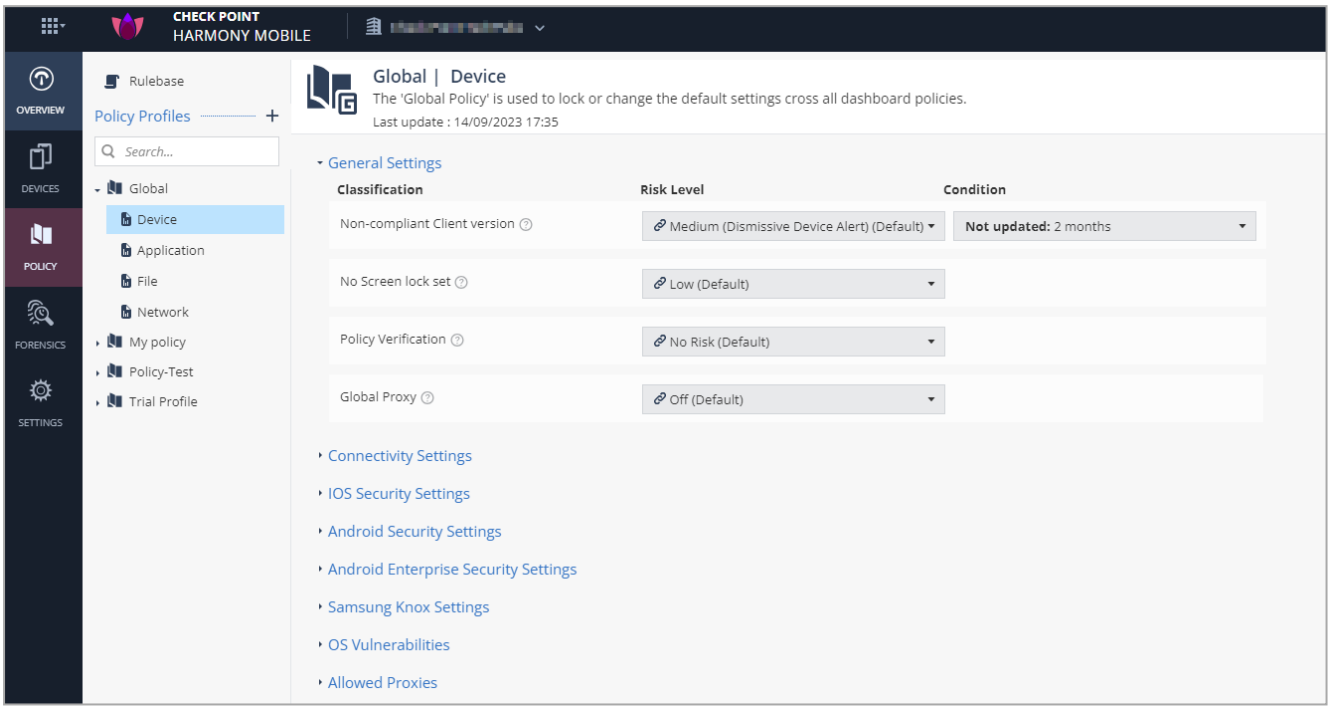
If the browser app configured for ONP in the UEM is not supported by Check Point, then it is not added in the **iOS Browser List** table. For assistance, contact Check Point Support.

For more information to configure the **Per App VPN** setting, see sk179387 or refer to your UEM documentation.

Note - To allow network protection for the traffic generated by Safari browser, the end-user need to enable Mobile Security Safari Extension in the mobile device. To enable the extension, see sk179966.

Device Policies

In this section, you can set the conditions and risk levels for general, iOS and Android specific policies.



General Settings

To configure the general settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **General Settings** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level	Condition
Non-compliant Client version	Set a **Risk Level** for the device if a non-compliant client version specified by the **Condition** is installed.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	Specify the non-compliant client version condition.
No Screen lock set	Set a **Risk Level** if no screen lock is set on the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	N/A
Policy Verification	Set a **Risk Level** if the device fails the policy compliance test.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	N/A

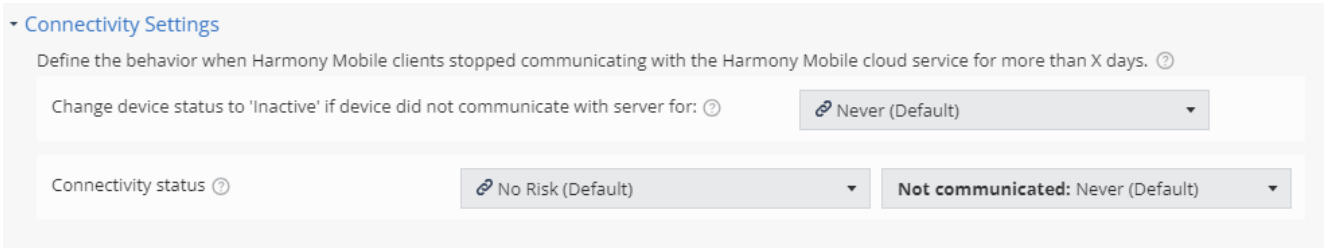
Classification	Description	Risk Level	Condition
Global Proxy	Set a **Risk Level** if the device is configured to work with a Global Proxy.	■ Off (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	N/A

3. To save the policy changes, click **Save**.

Connectivity Settings

If a user device does not communicate with the Mobile Security server for a specified number of days, you can change the device status to **Inactive** and set a risk level for the device.

Note - Mobile Security does not protect a device if its status is **Inactive**.



To change the status of the device to inactive:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **Connectivity Settings**.
3. From the **Change device status to 'Inactive' if device did not communicate with server for** drop-down list, select the number of days after which the system automatically changes the device status to **Inactive**.

4. In the **Connectivity status** section, select a risk level for the device if the device does not communicate with the Mobile Security server for the specified number of days.

   This must be less than the number of days you specify to change the device status to **Inactive** in step 3.

5. To save the policy changes, click **Save**.

iOS Security Settings

To configure the iOS security settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **iOS Security Settings** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level
Jailbroken Device	Set a **Risk Level** if the device is identified as a jailbroken device.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Notification Permission is set to OFF	Set a **Risk Level** if the user does not grant notification permission for the Harmony Mobile Protect app on the device. **Note** - Mobile Security triggers notifications in different scenarios. For example, when a new policy is set, or to announce detected risks for applications. We recommend that you allow notification permission for the Mobile Security application on the device.	▪ Medium (Device Alert) (Default) ▪ High (Device Alert) ▪ Medium (Device Alert) ▪ Medium (No Device Alert) ▪ Medium (Dismissive Device Alert) ▪ Low ▪ No Risk
Enterprise Certificate Profile	Set a **Risk Level** if an enterprise certificate profile is installed on the device.	▪ No Risk (Default) ▪ High (Device Alert) ▪ Medium (Device Alert) ▪ Medium (No Device Alert) ▪ Medium (Dismissive Device Alert) ▪ Low ▪ No Risk
Developer certificate profile	Set a **Risk Level** if a developer certificate profile is installed on the device.	▪ No Risk (Default) ▪ High (Device Alert) ▪ Medium (Device Alert) ▪ Medium (No Device Alert) ▪ Medium (Dismissive Device Alert) ▪ Low ▪ No Risk

Classification	Description	Risk Level
Location Permission is set to OFF	Set a **Risk Level** if the user does not grant location permission for the Harmony Mobile Protect app on the device. **Note** - If the location permission is turned on, Mobile Security application sends the device location if a Man-in-the-Middle attack occurs in the connected network. We recommend that you allow location permission for the Mobile Security application on the device.	▪ Low (Default) ▪ High (Device Alert) ▪ Medium (Device Alert) ▪ Medium (No Device Alert) ▪ Medium (Dismissive Device Alert) ▪ Low ▪ No Risk
Local Network Permission	Set a **Risk Level** if the user does not grant local network permissions for Harmony Mobile Protect app on the device. The system also sends an alert or notification to the user. This permission is required when **On-Device Network Protection** is enabled to use the local DNS server.	▪ Medium (Device Alert) (Default) ▪ High (Device Alert) ▪ Medium (Device Alert) ▪ Medium (No Device Alert) ▪ Medium (Dismissive Device Alert) ▪ Low ▪ No Risk

3. To save the policy changes, click **Save**.

Android Security Settings

To configure the Android security settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **Android Security Settings** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level
Rooted Device	Set a **Risk level** if the device is identified as a rooted device.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Verified boot is disabled	Set a **Risk Level** if the verified boot feature is disabled on the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
SELinux Permissive mode	Set a **Risk Level** if SELinux policy is not enabled on the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Device Encryption disabled	Set a **Risk Level** if device encryption is disabled.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Unknown Sources Enabled	Set a **Risk Level** if the device allows app installations from sources other than the play store.	■ Medium (No Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
USB debugging enabled	Set a **Risk Level** if the device allows USB debugging.	■ Medium (No Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Notification Permission is set to OFF	Set a **Risk Level** if notification permission is disabled for the Harmony Mobile Protect app on the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Location Permission is set to OFF	Set a **Risk Level** if device location permission is disabled for the Harmony Mobile application on the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Qualcomm Hexagon Vulnerability *	Set a **Risk Level** based on Qualcomm Hexagon vulnerability.	■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
VPN lock down	Set a **Risk Level** if the **Block connections without VPN** setting is disabled for the device.	■ Medium (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
MediaTek Audio DSP Vulnerability *	Set a **Risk Level** for the CVE-2021-0673 vulnerability. The system diverts the CVE MediaTek debugging framework for audio drivers to escalate local process privileges.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

** To view the setting, contact Check Point Support.*

3. To save the policy changes, click **Save**.

Android Enterprise Security Settings

Users may have both personal and work profile on an Android enterprise environment. The Harmony Mobile Protect app manages and protects only the work profile on the user device.

To protect the device's personal profile, you must install and activate Harmony Mobile Protect app manually. You can specify these settings to warn or enforce the user to install and activate Harmony Mobile Protect app to manage and protect the personal profile.

To configure the Android enterprise security settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **Android Enterprise Security Settings** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level
Personal Profile not Protected	Set a **Risk Level** when the Harmony Mobile Protect app is not activated for the personal profile.	■ High (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Mobile Security not installed on personal profile	Set a **Risk Level** when the Harmony Mobile Protect app is not installed for the personal profile.	■ Medium (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

3. To save the policy changes, click **Save**.

Samsung Knox Settings

Mobile Security integrates with the Samsung Knox framework to allow advanced security capabilities on Samsung devices. The user must grant the Samsung Knox permissions to enable these capabilities.

To configure the Samsung Knox settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **Samsung Knox Settings** and set the **Risk Level** for these classifications:

Setting	Description
Knox permission not granted	Select the device risk level if the Samsung Knox permissions are not granted. ■ Medium (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Block application until scan ended	Select this checkbox so that the application does not run until the scan is completed and the application is confirmed as legitimate.
Block application at risk	Select this checkbox to prevent the application from running based on the risk level selected in the drop-down list. Recommended threshold is **High**.

3. To save the policy changes, click **Save**.

OS Vulnerabilities

To configure the OS vulnerabilities settings:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **OS Vulnerabilities** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level	Condition
iOS OS Version	Select a **Risk Level** if the iOS version is older than the one specified in the **Condition**.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	Specify the condition for the iOS version.
Android OS Version	Select a **Risk Level** if the Android OS version is older than the one specified in the **Condition**.	■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	Specify the condition for the Android OS version.

Classification	Description	Risk Level	Condition
New Security Patch Available	Select a **Risk Level** if a new security patch update is available for the Android device but it is not installed for the duration specified in the **Condition**, after its release. **Note** - The availability of the patches depends on each Original Equipment Manufacturer (OEM). See https://source.android.com/docs/security/bulletin	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	Specify the duration. Default is one week.
Security Patch Not Updated	Select a **Risk Level** if the manufacturer has discontinued security patch updates or no security patch information available for the Android device since the duration specified in the **Condition**.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk	Specify the duration.

Classification	Description	Risk Level	Condition
CVEs detected on device OS	Set a **Risk Level** for the highest Common Vulnerability Scoring System (CVSS) V3 score of the CVEs detected on the device OS version, as specified in the **Condition**. **Note** - CVSS is a severity score of the vulnerability from 0.1 (lowest) to 10.0 (highest). Check the CVEs scores at: https://nvd.nist.gov/Vulnerability-Metrics/. For full visibility of the CVEs detected across your mobile device fleet, go to **Forensics** > **OS CVE Assessment**.	▪ High ▪ Medium ▪ Low ▪ No Risk	Specify the condition. For example, if the CVSS V3 score is above a certain range.

3. To save the policy changes, click **Save**.

To add CVEs that trigger a specific risk level on the user device:

1. In the **OS Vulnerabilities** section, click **Add**.
2. Enter the **CVE** and the **Risk Level**.
3. To save the policy changes, click **Save**.

Allowed Proxies

The **Allowed Proxies** table displays the allowed list of proxy server IP addresses that you can configure on the user's iOS device.

To add a new proxy to the allowed proxy list:

1. Go to **Policy** and select a policy profile.
2. Click **Device** > **Allowed Proxies**.
3. Click **Add**.

   The **Proxy IP** window appears.
4. Enter the **Proxy IP** and click **Add**.
5. To import a list of proxy IP address, click **Import** and upload the .CSV file with a list of addresses and comments.

6. To remove a proxy IP address from the list, select it and click **Delete**.
7. To save the policy changes, click **Save**.

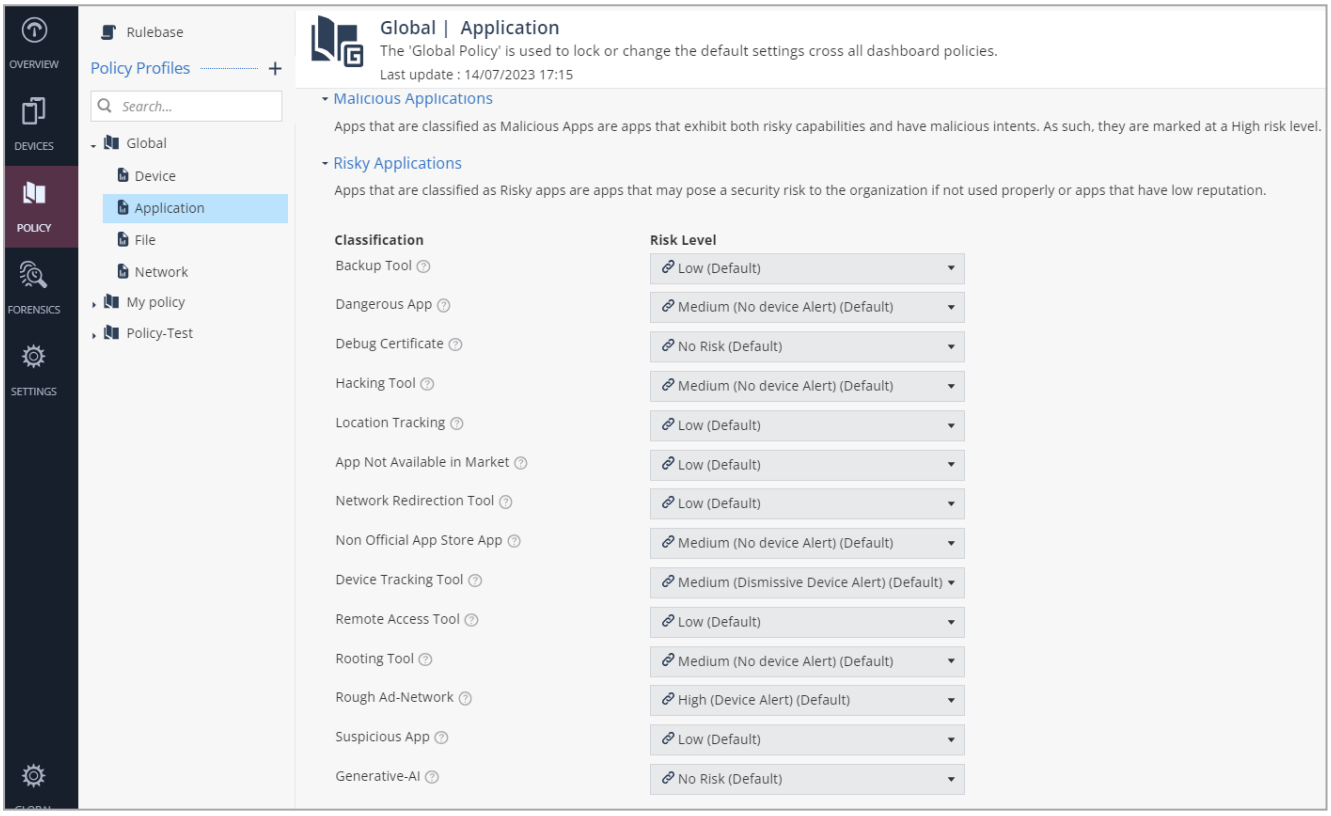
Application Policies

Malicious Applications

Applications that have both risky capabilities and have malicious intents are categorized as **malicious** applications by the Mobile Security Behavioral Risk Engine (BRE). Their risk level is always set to **High** and you cannot configure it.

Risky Applications

Applications that have bad reputation or that may pose a security risk to the organization are considered to be **risky** applications.



To set the risk level for these applications:

1. Go to **Policy** and select a policy profile.
2. Click **Application** > **Risky Applications** and set the **Risk Level** for these classifications:

Classification	Description	Risk Level
Backup Tool	Set the **Risk Level** if an application backs up sensitive information from the device.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Dangerous App	Set the **Risk Level** if a legitimate application can compromise the device, change configuration, or provide unauthorized access to corporate resources.	■ High (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Debug Certificate	Set the **Risk Level** if an application is signed by a debug certificate.	■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Hacking Tool	Set the **Risk Level** if an application compromises local network data, device data or application data (on either device or server).	■ Medium (No Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Location Tracking	Set the **Risk Level** if an application allows remote access to the device location without the user's consent.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
App Not Available in Market	Set the **Risk Level** if an application previously available in the app store is removed.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Network Redirection Tool	Set the **Risk Level** if an application redirects network communication without the user's consent.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Non Official App Store App	Set the **Risk Level** if an application is not verified by an official app store.	■ Medium (No Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

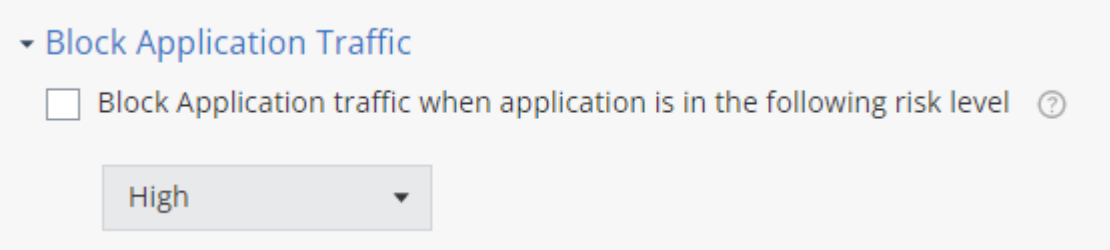
Classification	Description	Risk Level
Device Tracking Tool	Set the **Risk Level** if an application allows remote access to the device location without the user's consent.	■ Medium (Dismissive Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Remote Access Tool	Set the **Risk Level** if an application allows remote control of the device without the user's consent.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Rooting Tool	Set the **Risk Level** if an application is identified as a rooting or jailbreak tool.	■ Low (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

Classification	Description	Risk Level
Rough Ad-Network	Set the **Risk Level** if an application contains an ad-network and can leak sensitive data from the device and violates user privacy.	■ High (Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Suspicious App	Set the **Risk Level** if an application has suspicious capabilities.	■ Medium (No Device Alert) (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Generative-AI	Set the **Risk Level** if an application uses Artificial Intelligence (AI) services.	■ No Risk (Default) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk

3. To save the policy changes, click **Save**.

Block Application Traffic

You can block the traffic generated by or intended to a risky application based on the specified risk level. For example, if you specify the risk level as **Medium**, then the system blocks the traffic for all applications whose risk level is **Medium** or higher.



To block the application traffic, you must:

1. Set **On-device Network Protection** to **Always ON** or **Turn ON when device is at High risk**.
2. Set **Network Protection Working Mode** to **Full Inspection**.

   For more information, see *"Network Protection" on page 63*.

You can determine the risk level of an application from one of these:

- The **Severity** column in the **Application Risk** table:

  This table lists the risk level for each severity level. For more information, see *"View By Application Risk" on page 140*.

Severity Level	Risk Level
High	High
Medium	Medium
Low	Low
None	No risk

- *"Malicious Applications" on page 93*.
- *"Risky Applications" on page 93*.
- Applications allowed or blocked under *"Application Exceptions" on page 102*.

To block the application traffic:

1. Go to **Policy** and select a policy profile.
2. Click **Application** > **Block Application Traffic**.

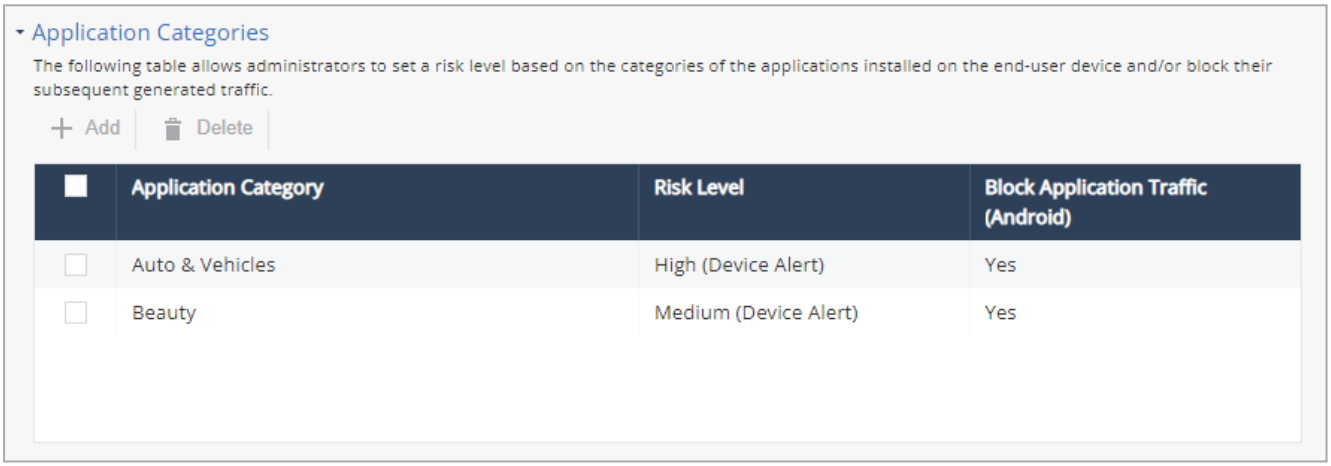
3. Select the **Block Application traffic when application is in the following risk level** checkbox.
4. From the drop-down list, select the risk level.

Notes :

- This option is supported only for Android devices where ONP is set to **Full Inspection**.
- Only the application's traffic is blocked, not the application.

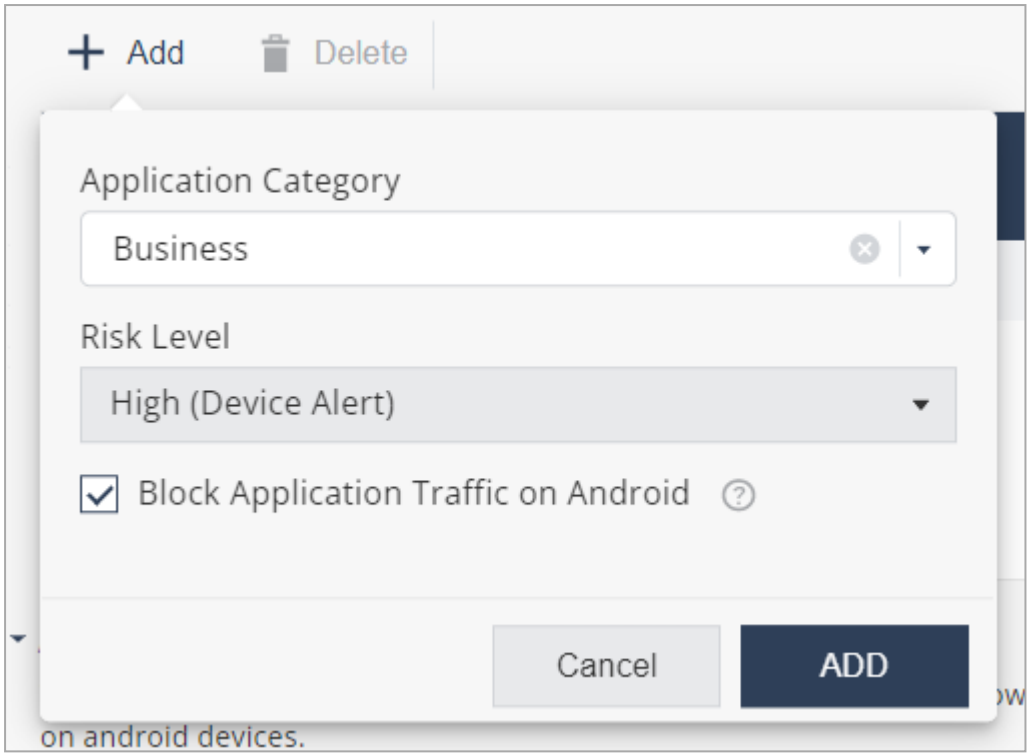
Application Categories

In this section, you can set risk level for the different application categories.



To add a new application category:

1. Go to **Policy** and select a policy profile.
2. Click **Application** > **Application Categories**.
3. In the table, click **Add**.
   A window appears.



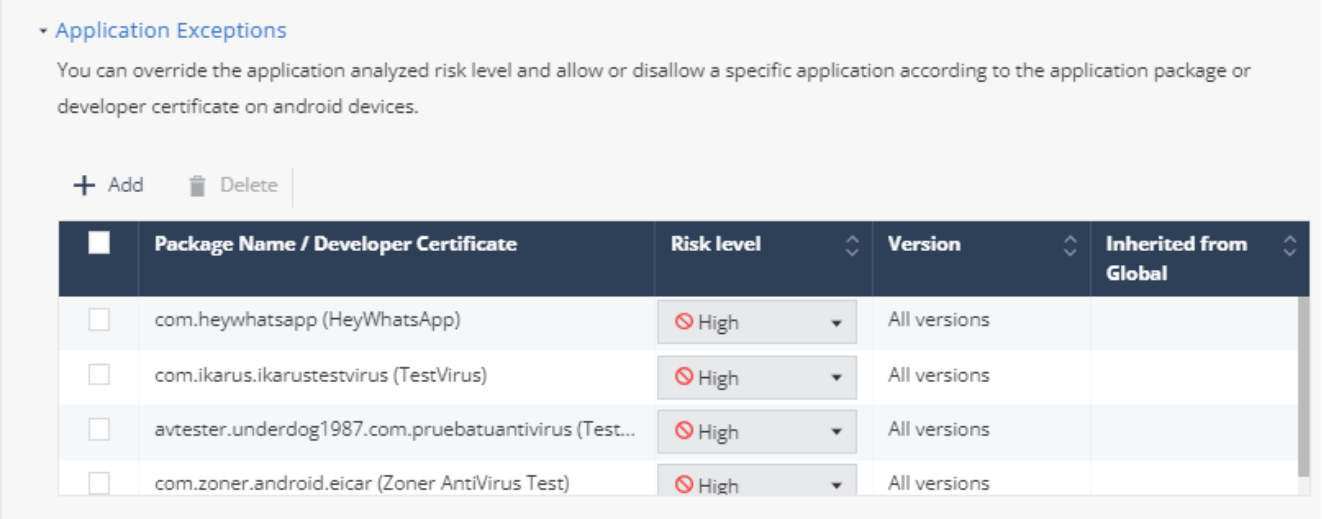
4. Set these parameters:

Item	Description
Application Category	Select the application category (Category obtained from Google Play (Android) and Play Store (iOS)).
Risk Level	Set the **Risk Level**: ■ No Risk (Default) ■ High (Device Alert) ■ Medium (Device Alert) ■ Medium (No Device Alert) ■ Medium (Dismissive Device Alert) ■ Low ■ No Risk
Block Application Traffic on Android	Select this checkbox to block application traffic on Android devices. The feature works only for Android devices that enable the **On Device Network Protection** feature.

5. To delete a category, select it and click **Delete**.
6. To save the policy changes, click **Save**.

Application Exceptions

You can override the application's analyzed risk level according to the application package or developer certificate on Android devices. By default, it inherits the settings from the **Global** policy.

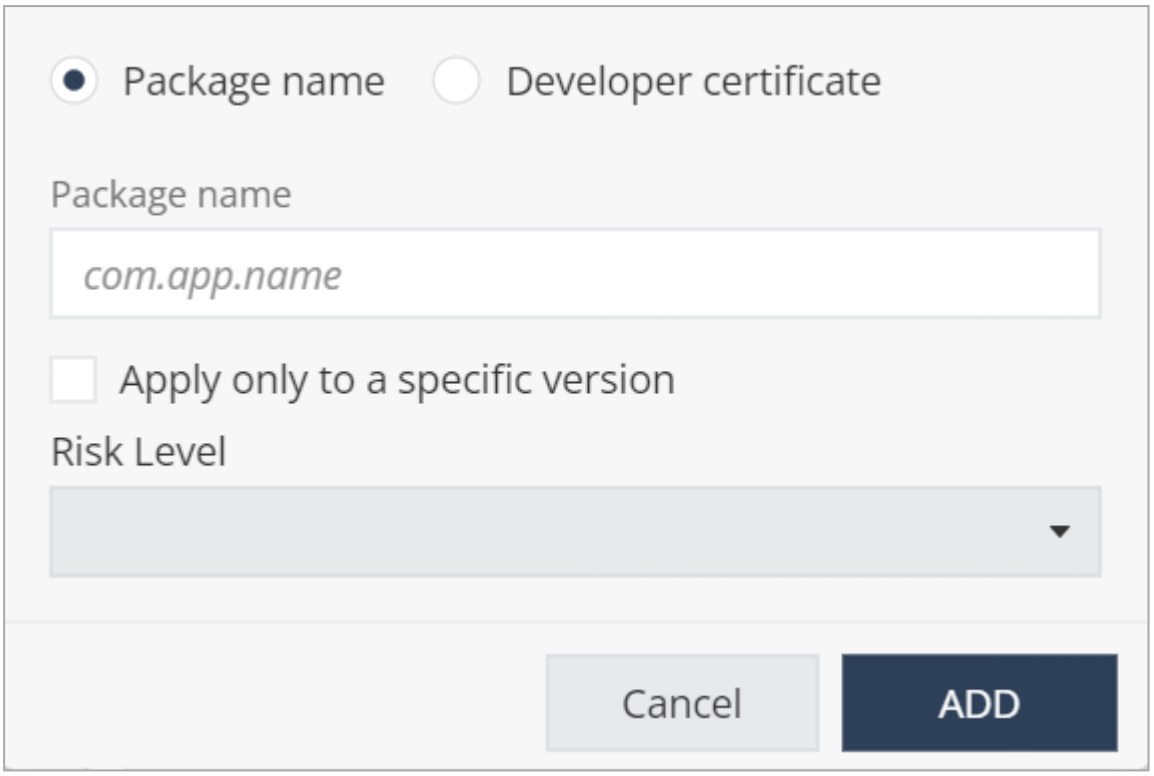


To add an exception to an application:

1. Go to **Policy** and select a policy profile.
2. Click **Application** > **Application Exceptions**.
3. In the table, click **Add**.

   A window appears.
4. Select one of these:

- **Package name**:



a. Enter the application **Package name**.

b. To apply the exception only to a specific version, select the **Apply only to specific version** checkbox.

c. In the **Version** field, enter the application package version number.

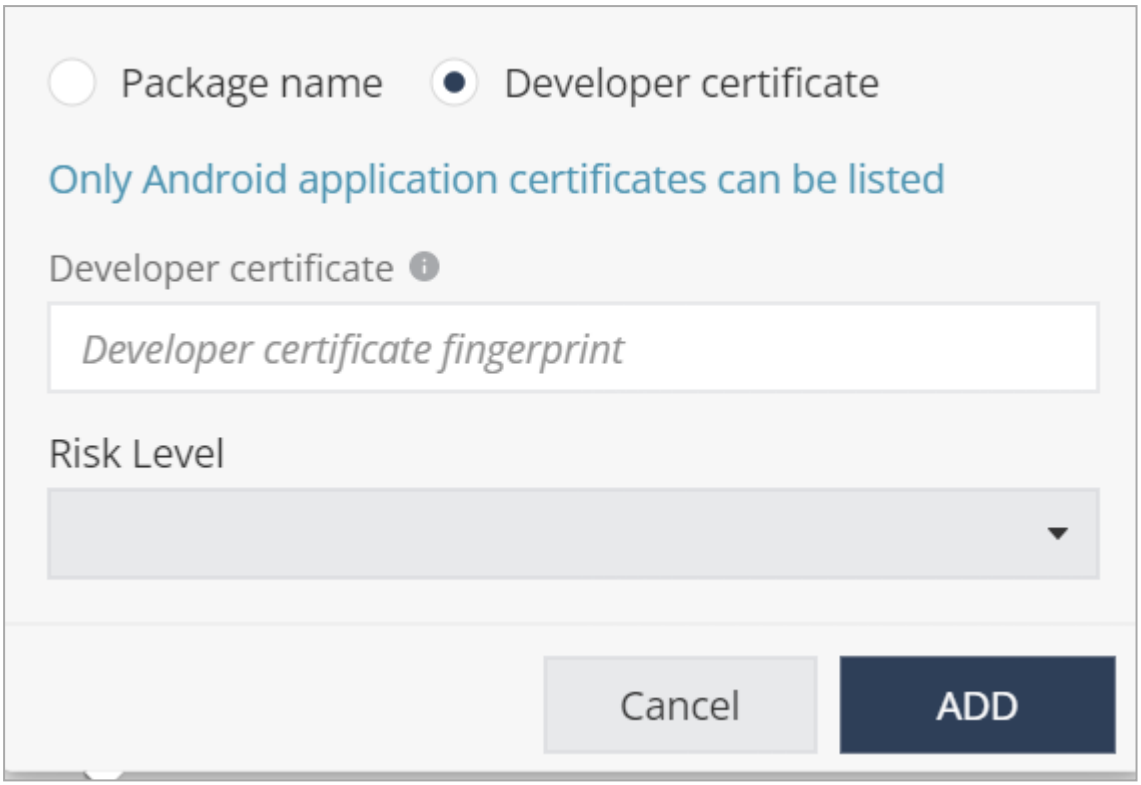
Note - Version field appears only if you select **Apply only to specific version** checkbox.

d. From the **Risk Level** drop-down list, select the risk level:

- **High** – The system changes the application's risk level to **High Risk**. As a result, the actual application triggers on-device mitigation and a pop-up event. This app triggers an increase in the risk level of the device.
- **No risk** – The system changes the application's risk level to **No Risk**. The application no longer triggers on-device mitigation or a pop-up event.
- **Ask for user approval** – When the user installs an app, the user is prompted about the risk and can allow or disallow the application.

e. Click **Add**.

- **Developer certificate** (applies only to Android applications):



  a. In the **Developer certificate** field, enter the certificate ID.

  b. From the **Risk Level** drop-down list, select the risk level:

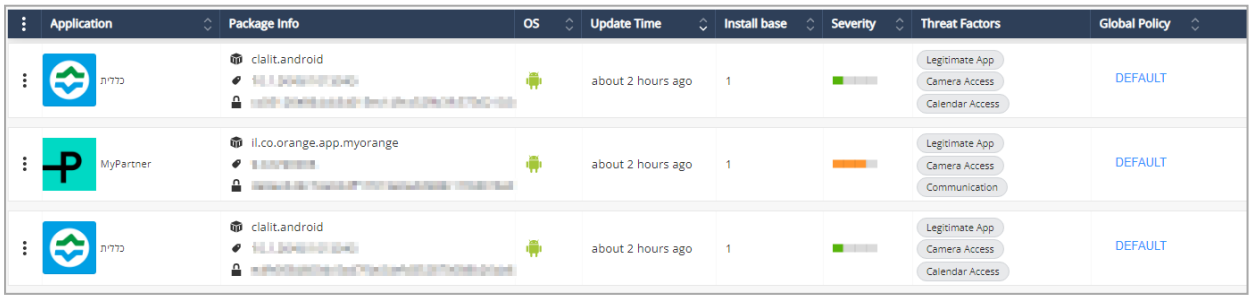
  - **High**
  - **No risk**
  - **Ask for user approval**

  c. Click **Add**.

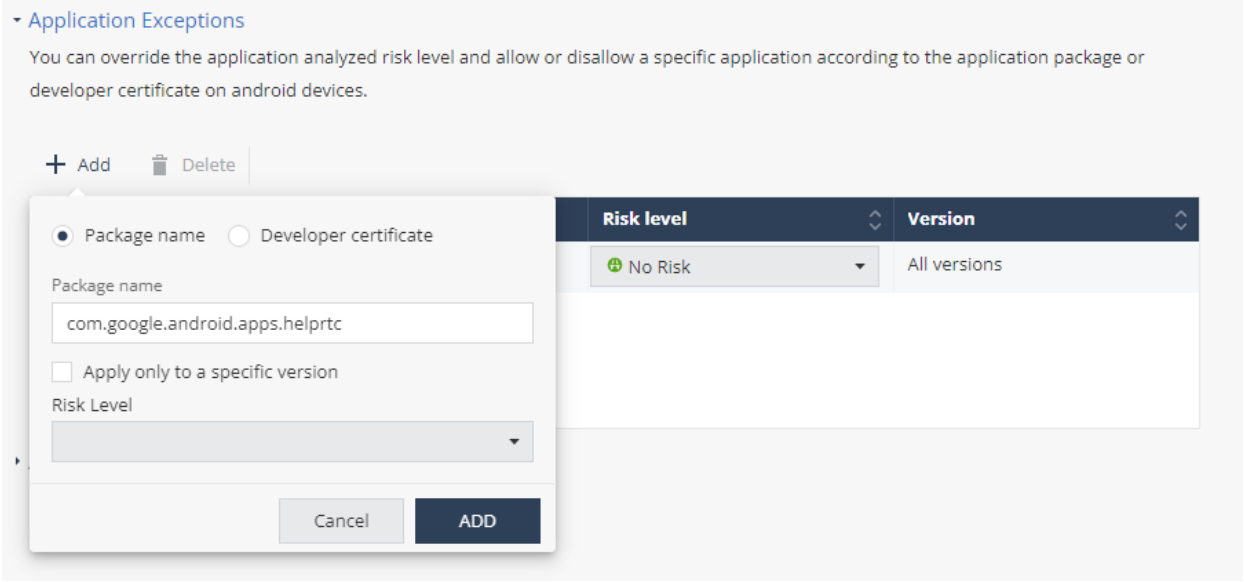
5. To save the policy changes, click **Save**.

If you do not know the applications details:

1. Go to **Forensics** > **Applications**.
2. Find the relevant application and click the **Global Policy** value.



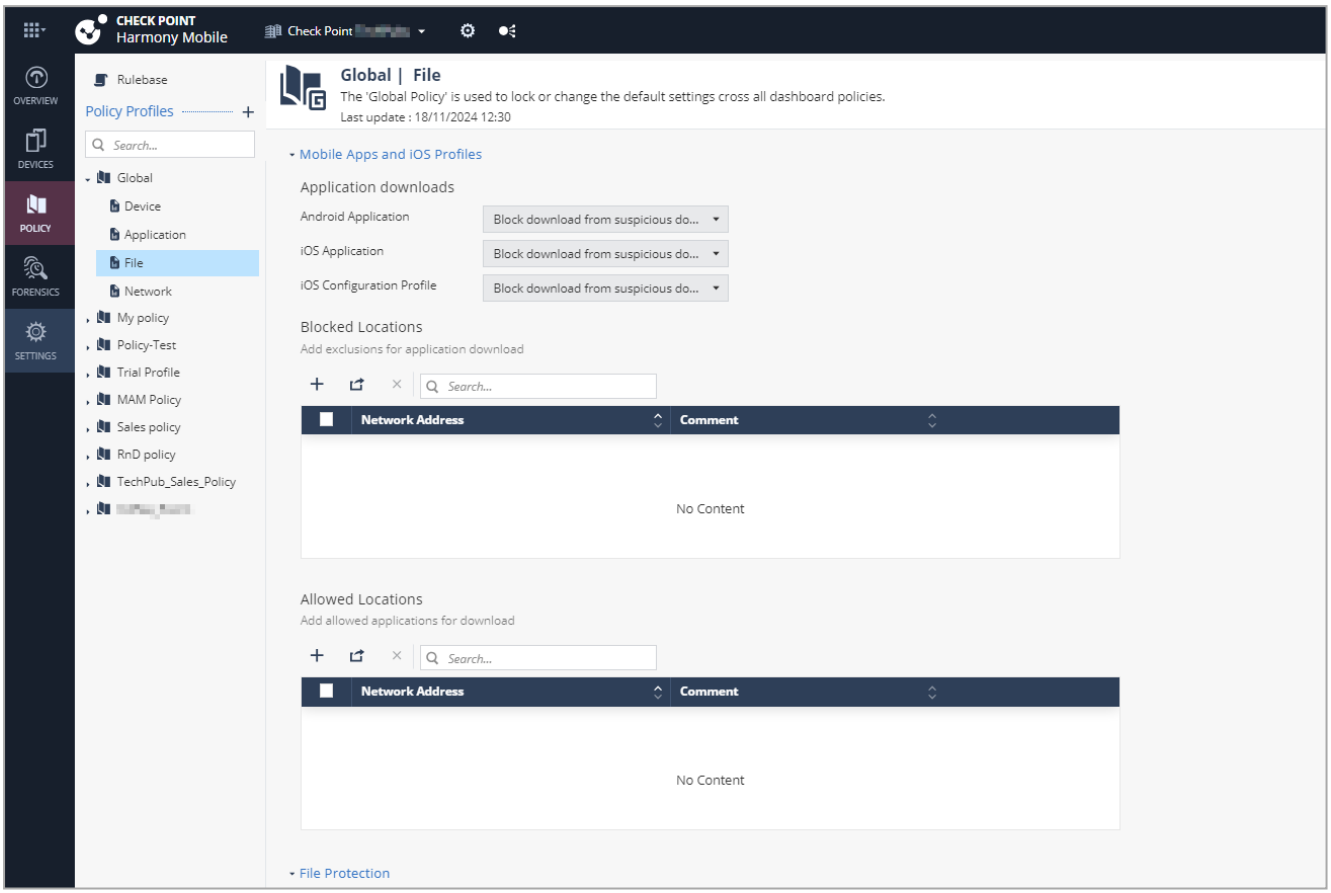
The **Application Exceptions** section appears with the chosen application details.



3. Select the **Risk Level** and click **Add**.
4. To save the policy changes, click **Save**.

File Policies

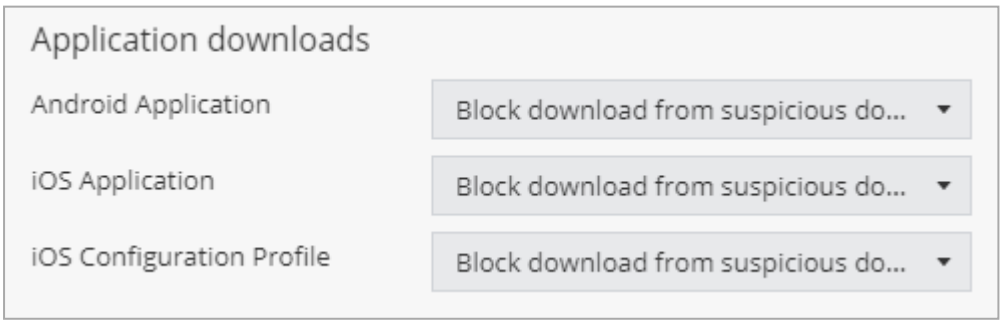
File policy settings:



Mobile Apps and iOS Profiles

Application Downloads

Prevents unauthorized download of applications on Android and iOS devices.



Important - To enable download protection, you must enable ONP. See *"Network Protection" on page 63*.

To enable download protection for applications:

1. Go to **Policy** and select a policy profile.
2. Click **File** > **Mobile Apps and iOS Profiles**.

   Under **Application downloads**, set these values:

Item	Description	Value
Android Application	Prevents download of unauthorized and malicious Android applications on Android devices based on domain reputation from ThreatCloud.	■ **Allow all** ■ **Block download from suspicious domains** (Default) ■ **Allow only from trusted domains**
iOS Application	Prevents download of unauthorized and malicious iOS applications on iOS devices based on domain reputation from ThreatCloud.	
iOS Configuration Profile	Prevents download of unauthorized and malicious profiles on iOS devices based on domain reputation from ThreatCloud. **Note** - To view the full list of profiles installed on the mobile devices in your organization, go to **Forensics** > **iOS Profiles**.	

3. To save the policy changes, click **Save**.

Files - Blocked / Allowed Locations

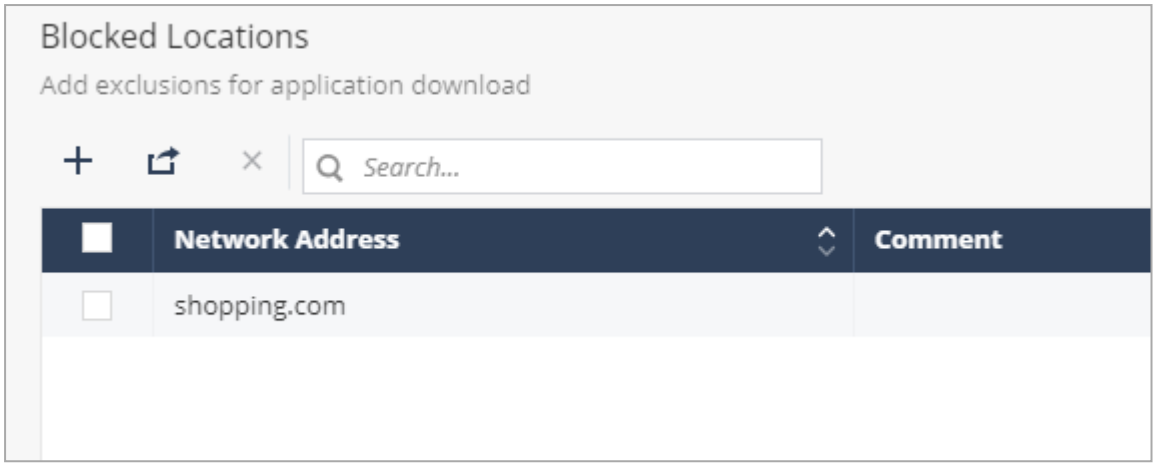
In this section, you can configure network locations that mobile devices use to **download apps** or **iOS management profiles**.

Note - You can add up to **100** entries to the Blocked/Allowed Locations list.

To block a network location:

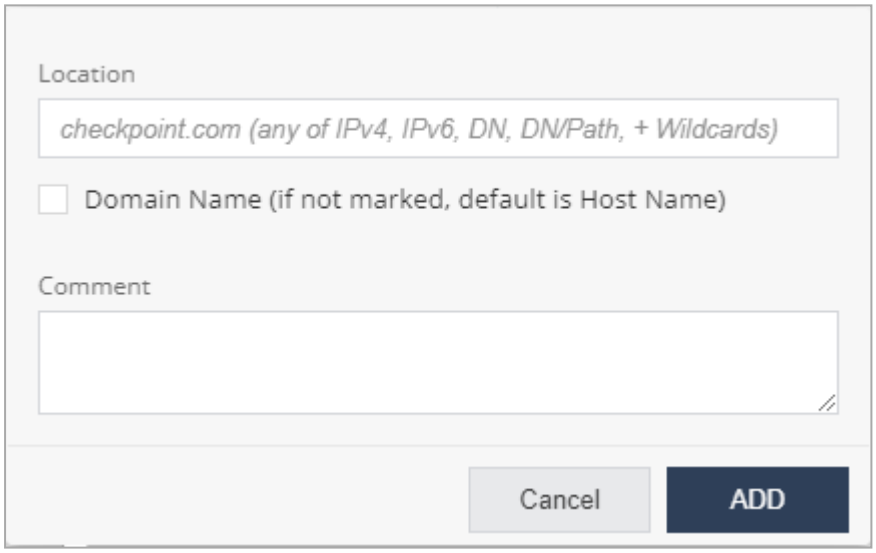
1. Go to **Policy** and select a policy profile.
2. Click **File** > **Mobile Apps and iOS Profiles** > **Blocked Locations**.
3. Click **Add**.

   The **Blocked Locations** table appears.



Note - To allow a network location, select **Policy Profile** > **File** > **Allowed Locations**, and click **Add**.

4. In the **Location** field, enter the network location to block in one of these formats: IPv4, IPv6, Domain Name (DN), DN/URL, + Wildcards.



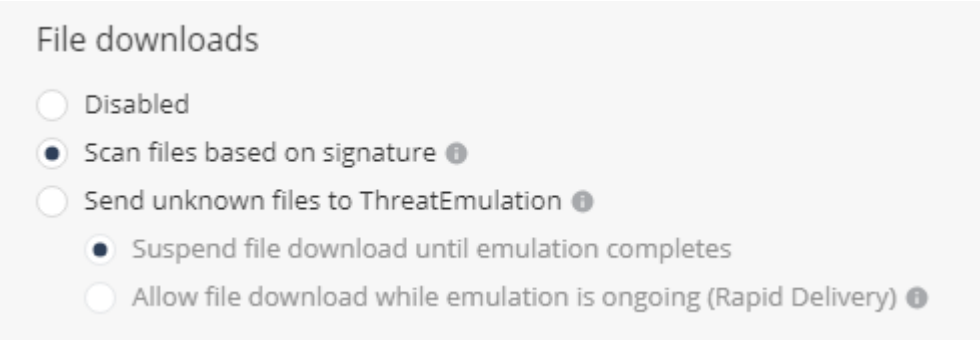
5. Click **Add**.
6. To import a list of locations, click **Import** and upload the .CSV file with a list of locations and comments.
7. To remove a network location from the list, select it and click **Delete**.
8. To save the policy changes, click **Save**.

Note - To allow or block device access to specific network locations, configure your **Network** policy. For more information, see *"Networks - Blocked Locations" on page 116* and *"Networks - Allowed Locations" on page 118*.

File Protection

File Downloads

Prevents the download of malicious files on Android and iOS devices. It checks the file reputation against the ThreatCloud before it is downloaded on the mobile device. When the file emulation option is enabled, if the file is unknown, it is sent for file emulation to ThreatCloud that provides a verdict whether the file is safe or not.



To enable download protection for files:

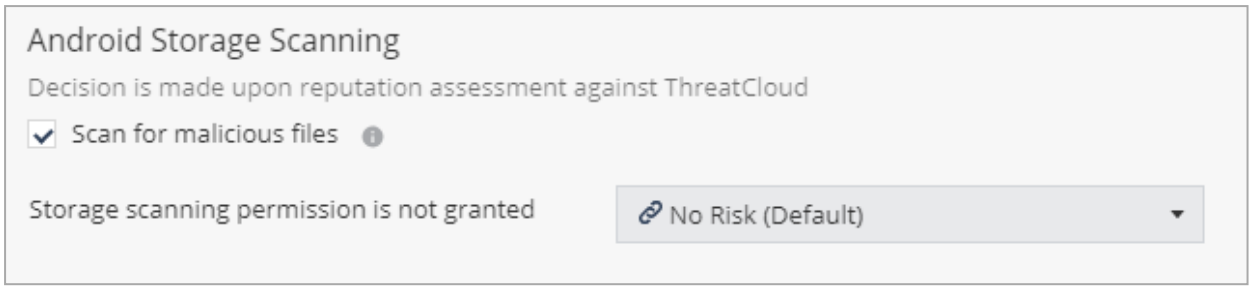
1. Go to **Policy** and select a policy profile.
2. Click **File** > **File Protection** > **File downloads**.
3. Select the file download method:
   - **Disabled** - File download is disabled.
   - **Scan files based on signature** - ThreatCloud assesses the file reputation based on the signature of the file.
   - **Send unknown files to ThreatEmulation** - Files unknown to ThreatCloud are uploaded for file emulation.
     - **Suspend file download until emulation completes** - Suspends download of unknown files until a verdict is available after emulation.
     - **Allow file download while emulation is ongoing (Rapid Delivery)** - Allows download of unknown files even if the verdict is not available.
4. To save the policy changes, click **Save**.

Android Storage Scanning

To scan the files stored on an Android device:

1. Go to **Policy** and select a policy profile.
2. Click **File** > **File Protection** > **Android Storage Scanning**.

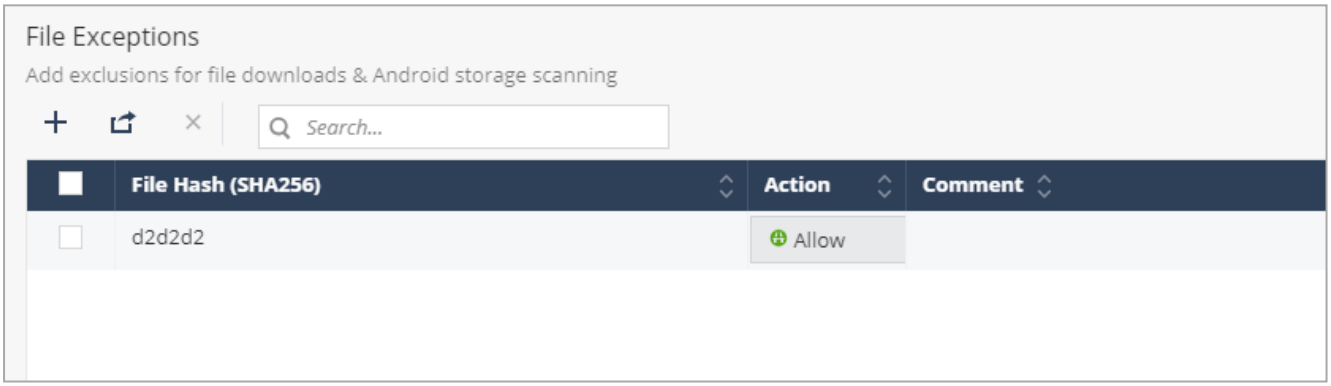
3. Select the **Scan for malicious files** checkbox.



4. Select the risk level if storage scanning permission is not granted.
5. To save the policy changes, click **Save**.

File Exceptions

You can create an exception to allow or block a hash or a file that was analyzed with a specific risk level.



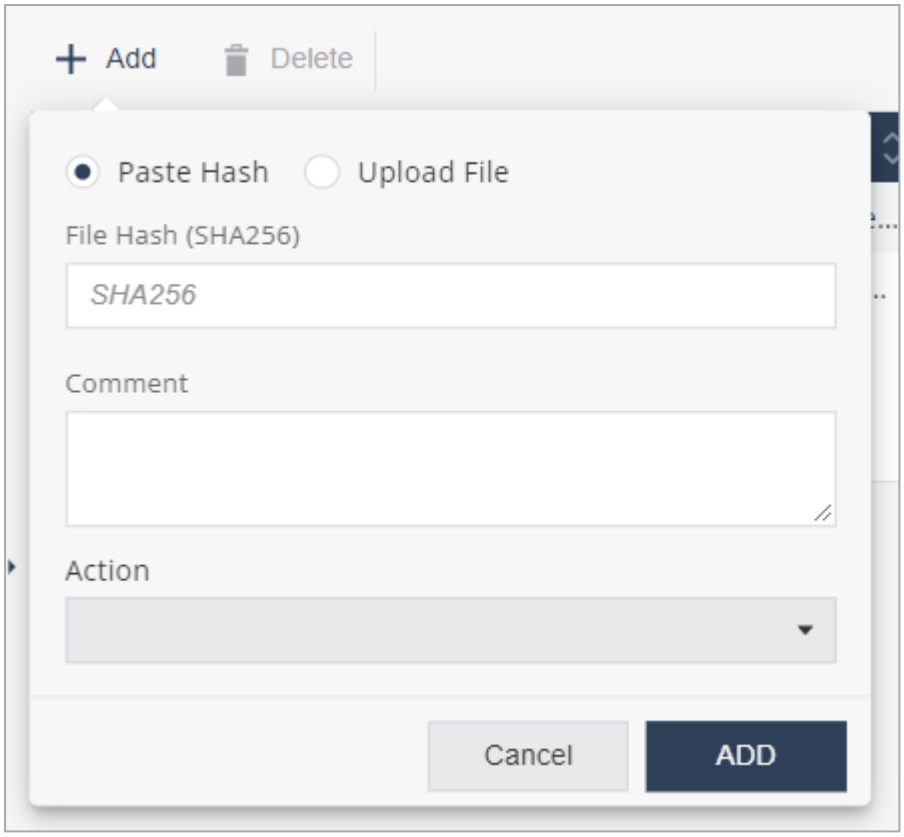
Notes:

- You can create a file exception to *allow* only if the file is known to the organization and you want to remove it from the dashboard alerts.
- You can create a file exception to *block* if you consider the file is malicious or banned by your organization even though it was determined as Low Risk by the ThreatCloud.
- You can add up to **100** entries to the **File Exceptions** list.

To add a file exception:

1. Go to **Policy** and select a policy profile.
2. Click **File** > **File Protection** > **File Exceptions**.
3. Click **Add**.

   A pop-up window appears.



4. Do one of these:
   - To add a file hash exception:
     a. Click **Paste Hash**.
     b. In the **File Hash** field, enter the file hash name. For example, SHA256.
   - To add a file exception:
     a. Click **Upload File**.
     b. Click **Upload** to upload the file.
5. (Optional) In the **Comment** field, add your comments.
6. From the **Action** drop-down list, select one of these:
   - **Block** - To block the file or file hash.
   - **Allow** - To allow the file or file hash.
7. To save the policy changes, click **Save**.

Note - You can also allow or block a file from the **Forensics** > **Events & Alerts** page.

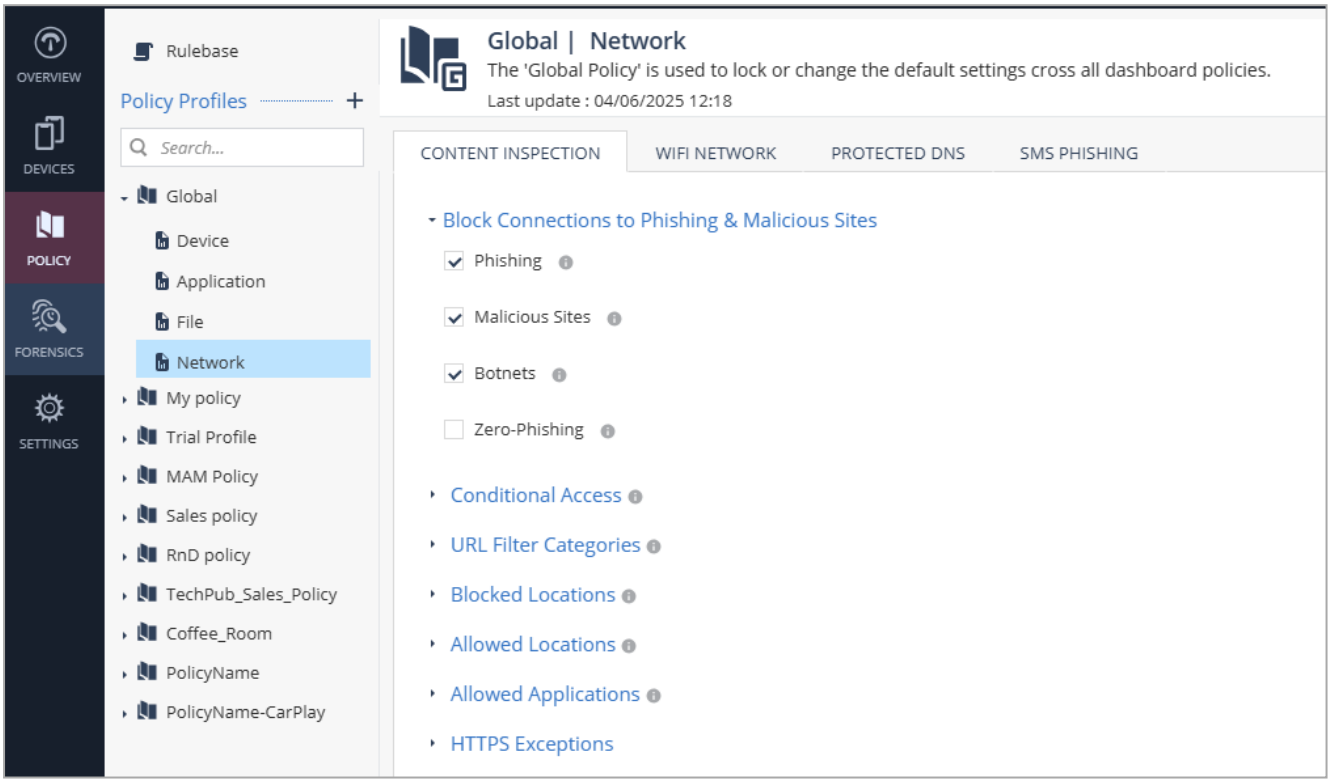
Select any one of these:

- **Allowed List** - The risk level of the file changes to **No Risk**.
- **Blocked List** - The risk level of the file changes to **High Risk**. A blocked file triggers on-device mitigation and user event notification.

Network Policies

Content Inspection

For Content Inspection configuration to work on the device, you must enable On-device Network Protection.



Set these parameters on the **Content Inspection** tab:

Block Connections to Phishing & Malicious Sites

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **Block Connections to Phishing & Malicious Sites** and set these parameters:

Item	Description
Phishing	Indicates whether to block connections to phishing URLs.
Spyware / Malicious Sites	Indicates whether to block connections to spyware or malicious sites.
Botnets	Indicates whether to block connections to sites that use bots.

Item	Description
Zero-Phishing	Indicates whether to enable zero-phishing (identify unknown phishing sites).

For an optimal browsing experience on the mobile device, Zero-Phishing technology is tuned, by default, not to scan all SSL locations but only domains not marked as safe (i.e. high confidence of no-risk).

3. To save the policy changes, click **Save**.

Conditional Access

The **Conditional Access** feature allows an organization to automatically control access to corporate resources from compromised devices (marked as **High Risk**).

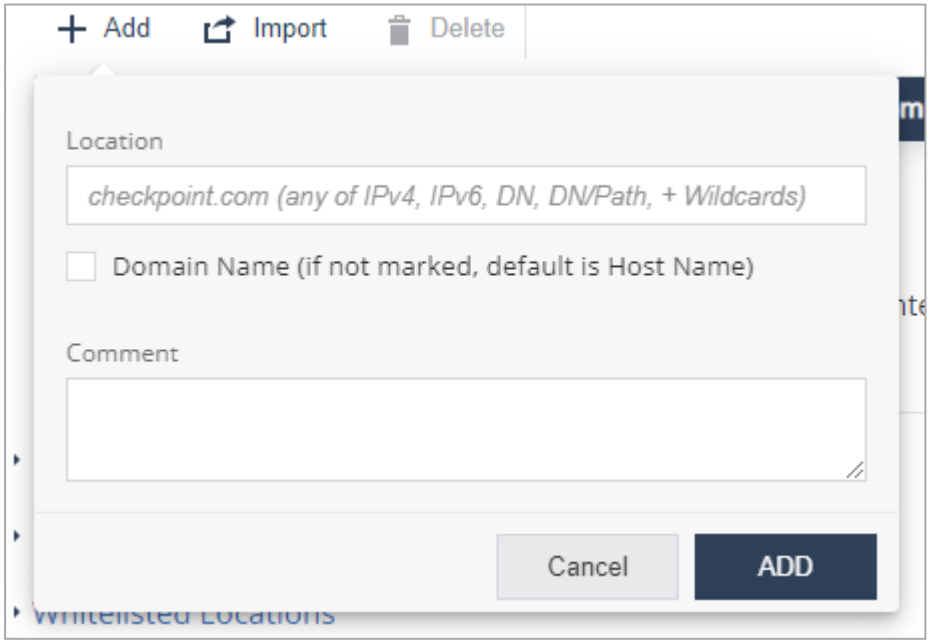
This policy enforcement is independent of Unified Endpoint Management (UEM) solutions.

This category is a list of corporate IP addresses and/or FQDN hostnames that a device at high risk cannot access.

To add conditional access to a specific network:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **Conditional Access**.
3. Click **Add**.

   A pop-up window appears.



4. In the **Location** field, enter the network location in one of these formats: IPv4, IPv6, Domain Name (DN), DN/URL, + Wildcards.
5. Select the **Domain Name** checkbox to enter location as domain name.
   For example, if you enter **Location** as google.com, and select this checkbox, it is interpreted as domain name and includes all URLs in *.google.com. If not set, location value is interpreted as host name (www.google.com).
6. (Optional) Add comments.
7. Click **Add**.
8. To import conditional access for a list of URLs, click **Import** and upload the .CSV file with URL names list and comments.
9. To delete a network location from the list, select it and click **Delete**.
10. To save the policy changes, click **Save**.

URL Filter Categories

The URL filtering feature prevents access to websites as per the organization's corporate policies. You can prohibit device access for URLs in a specific content category (for example, Gambling and Violence). You can enforce policies across all browser apps and non-browser specific apps, such as Facebook Messenger, Slack and WhatsApp.

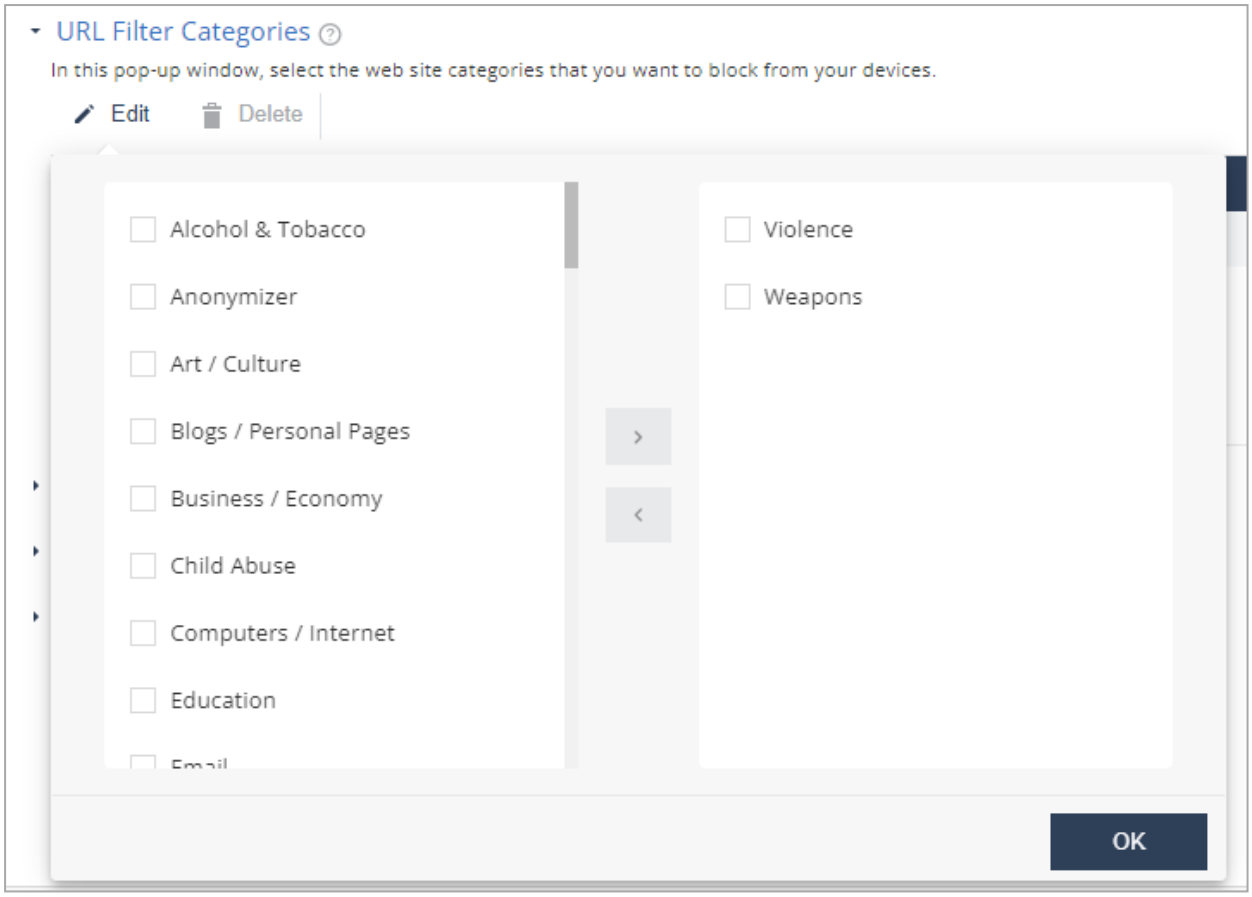
The URL Filtering technology also allows you to allow and block domains.

Note - When URL Filtering is coupled with **On-device Network Protection** > **Always ON** > **Allow user to suspend On-device Network Protection**, users can disable ONP for a specific amount of time (5 minutes, 30 minutes, or 2 hours), to access blocked websites or categories. This provides flexibility in a BYOD environment.
However, the user cannot suspend ONP if the device is at **High** risk. If the device moves to at **High** risk while in suspension, **Conditional Access** is enabled.

To edit URL filtering categories:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **URL Filter Categories**.
3. Click **Edit**.

   A pop-up windows appears.
4. In the left column, select the categories that you want to block access to, and click **>**.

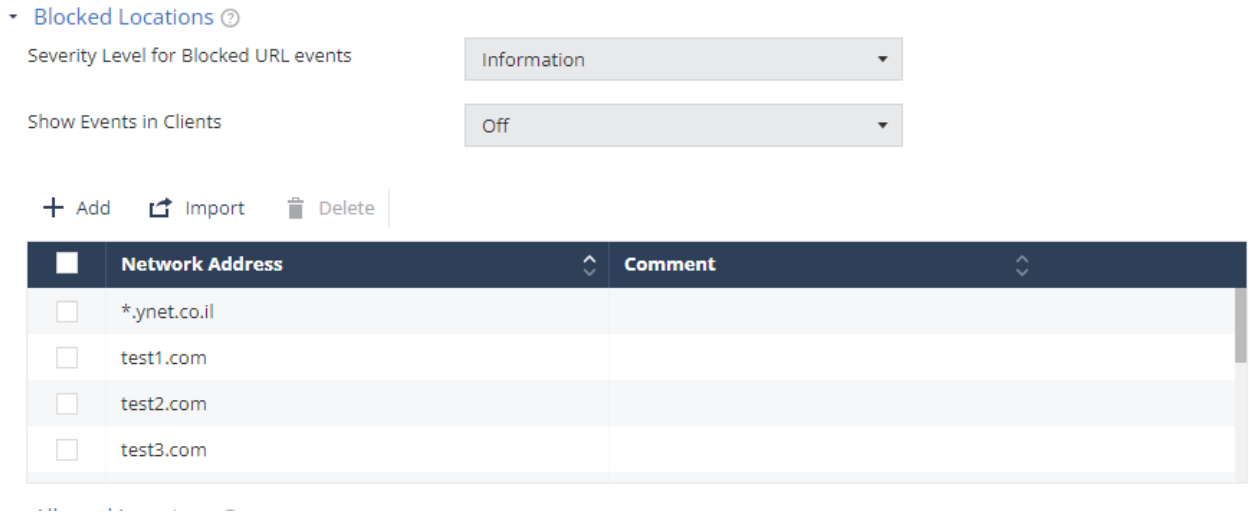


5. To undo a selection, in the right column, select the category and click **<**.
6. Click **OK**.
7. To save the policy changes, click **Save**.

The organization may decide not to track such events due to user privacy concerns. In that case, administrator can block these categories, but not track the events per category.

Networks - Blocked Locations

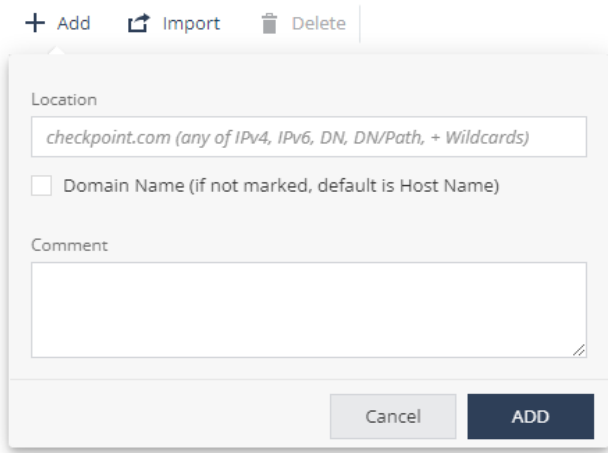
You can block the device access to specific network locations, regardless of the subject category or risk level of the device. In addition, you can also set the severity level for the events generated when Mobile Security blocks access to these network locations and configure whether to show the event notification in the Harmony Mobile Protect app.



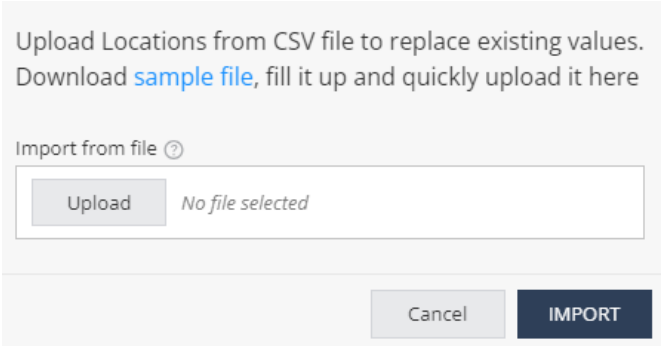
To add a network location to the Blocked Locations list:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **Blocked Locations**.
3. Click **Add**.

   A pop-up window appears.



4. In the **Location** field, enter the network location in one of these formats (IPv4, IPv6, Domain Name (DN), DN/URL, + Wildcards).
5. (Optional) Add your comments.
6. Click **Add**.
7. To import a list of network locations, click **Import** and upload the .CSV file with the locations list.



Note - The uploaded list replaces the existing list. This allows you to import a list of locations from other systems, such as Firewall and Gateway, into Mobile Security On-device Network Protection policy settings.

8. From the **Severity Level for Blocked URL events** drop-down list, select the severity level.
9. From the **Show Events in Clients** drop-down list, select one of these:
   - **Off** (Default) - The end-user does not receive the event notification in the Harmony Mobile Protect app, when Mobile Security blocks access to the network location.
   - **On** - The end-user receives an event notification in the Harmony Mobile Protect app, when Mobile Security blocks access to the network location.
10. To remove a network location from the list, select it and click **Delete**.
11. To save the policy changes, click **Save**.

Notes:

- You can add up to **100** entries to the **Blocked Locations** list.
- If a domain in the blocked location is still accessible by the device, then the domain is in the default allowed list. Collect the device logs (see sk179614) and contact Check Point Support.

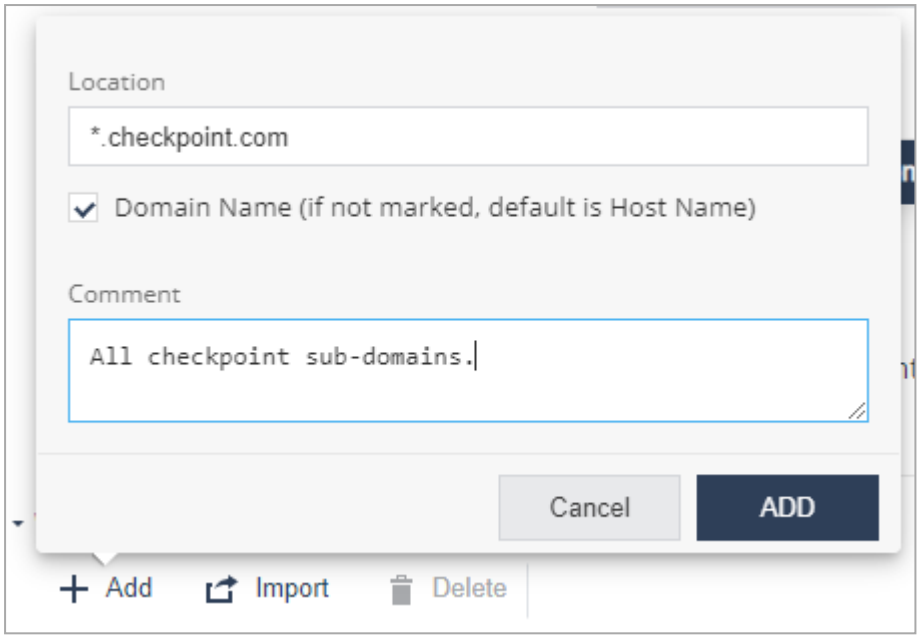
Networks - Allowed Locations

You can allow access to specific network locations or domains from the user device, regardless of the subject category or risk level of the device. For example, a self-service help desk site.

To add a network location to the allowed list:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **Allowed Locations**.
3. Click **Add**.

   A pop-up window appears.



4. In the **Location** field, enter a network location in one of these formats (IPv4, IPv6, Domain Name, DN/URL, +wildcards).
5. (Optional) In the **Comment** field, add your comments.
6. Click **Add**.
7. To import a list of locations, click **Import** and upload a .CSV file with a list of locations and comments.

   Note - The uploaded list replaces the existing list. This allows administrators to import a list of locations from other systems such as Firewall/Gateway into Mobile Security On-device Network Protection (ONP) policy settings.
8. To remove a network location from the list, select it and click **Delete**.
9. To save the policy changes, click **Save**.

Note - You can add up to **100** entries to the **Allowed Locations** list.

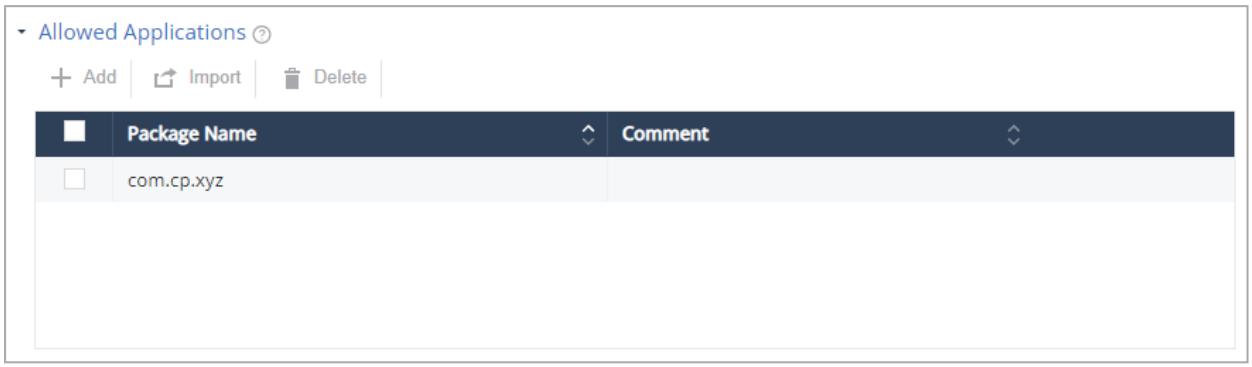
Allowed Applications

You can allow authorized **Android** applications to access the internet on the mobile device. You can configure the application list to ensure that a specific Android application can always access the internet from a user device, regardless of the device risk level.

Note - This setting impacts the traffic generated by the listed applications while the **Policy** > **Application** > **Application Exceptions** setting relates to the risk of the app.

To add an application to allowed list:

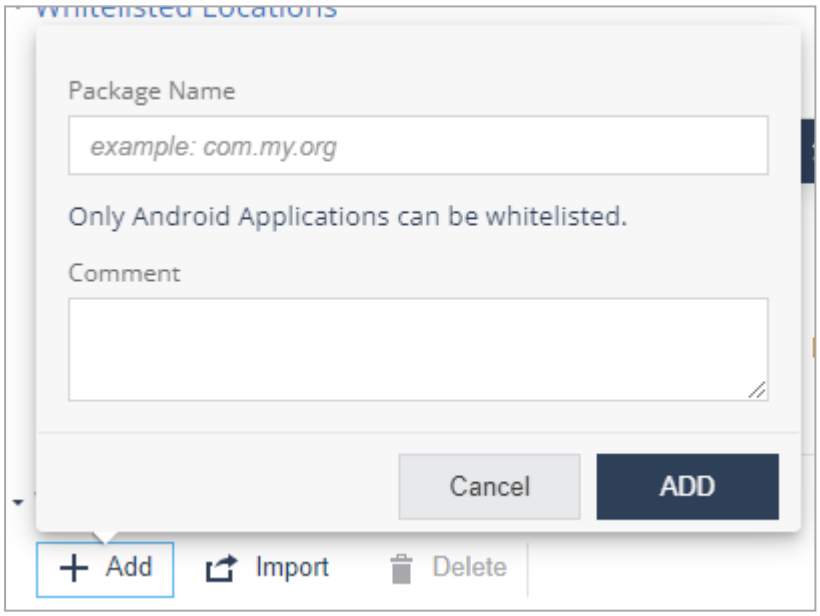
1. Go to **Policy** and select a policy profile.
2. Click **Network** > **Content Inspection** > **Allowed Applications**.



3. Click **Add**.

   A pop-up window appears.

4. In the **Package Name** field, enter the Android application Package Name (For example, com.cp.xyz).



5. (Optional) Add your comments.
6. Click **Add**.
7. To import a list of applications, click **Import** and upload a .CSV file with a list of applications' package names and comments.

   Note - The uploaded list replaces the existing list. This allows administrators to import a list of applications from other systems such as Firewall/Gateway into Mobile Security On-device Network Protection (ONP) policy settings.

8. To remove an item from the list, select it and click **Delete**.
9. To save the policy changes, click **Save**.

To summarize, Mobile Security blocks:

- Traffic from mobile apps flagged as malicious based on the BRE verdict.
- Traffic to malicious internet resources based on ThreatCloud reputation and risk score.
- Traffic to destinations marked as blocked locations (in **Mobile Security** or in **Infinity IOC Management** solution).
- Traffic which is not compliant with the corporate policy, such as URLs blocked in **URL Filter Categories**.
- Traffic from mobile apps in blocked categories (Android only)

Traffic that is safe (safe domains or not posing a security risk) and compliant with the corporate policy is allowed.

Note - To manage long IoC lists and feeds, use the **Infinity IOC Management** solution.

HTTPS Exceptions

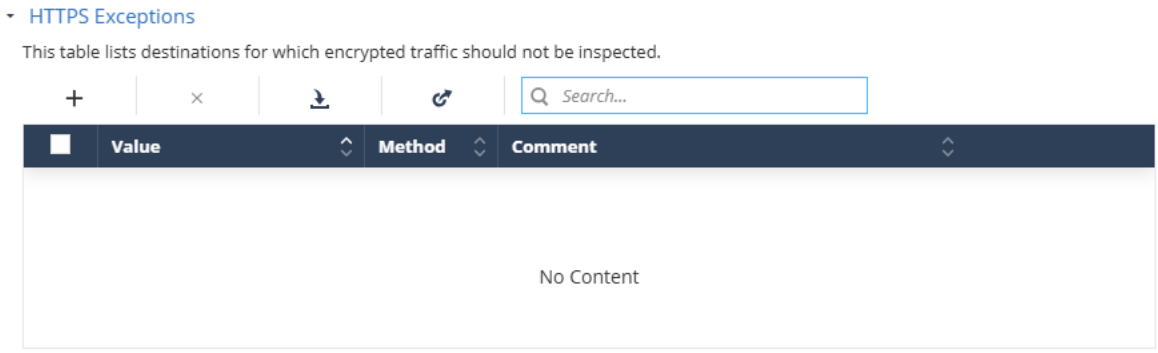
You can create an exception list for network locations that you want to exclude from HTTPS inspection, for specific sites or web categories for end-users' privacy.

Prerequisite

Before you add network locations to HTTPS exceptions, make sure that SSL inspection is enabled. For more information, see *"HTTPS Settings" on page 69*.

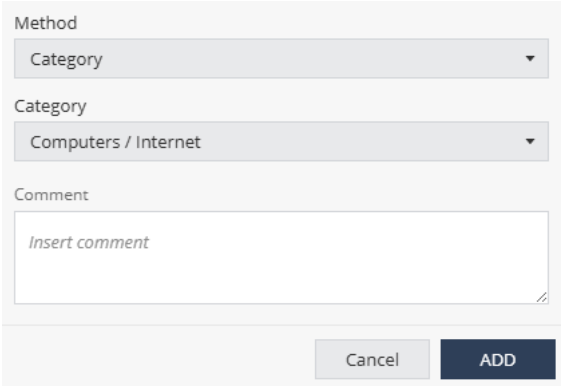
To add a network location to the HTTPS exception list:

1. Go to **Policy** and select a policy profile.
2. Go to **Network** > **Content Inspection** and click **HTTPS Exceptions**.



3. Click the **+** icon.

   A pop-up window appears.



4. From the **Method** list:
   - To exclude by category, select **Category** and select the category from the **Category** list.
   - To exclude a subnet, select **Subnet** and enter the subnet value in the **Subnet** field.
   - To exclude a domain, select **Domain** and enter the domain name in the **Domain** field.
5. (Optional) Enter your comments.
6. Click **Add**.
7. To import a list of exceptions from a JSON file:
   a. Click the icon.
   b. Click **Upload** and select the JSON file that contains the exception list.
   c. Click **Import**.

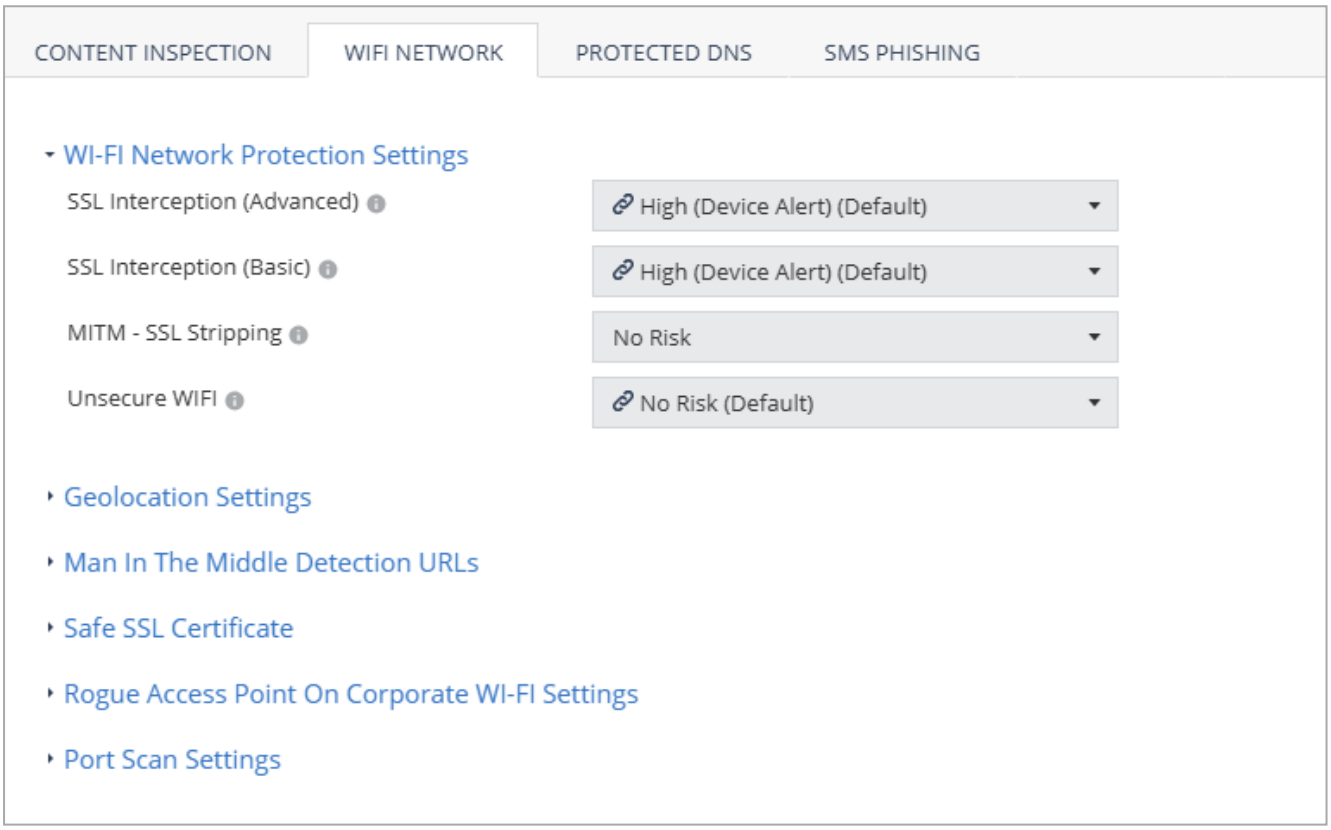
      The system appends the imported list to the existing list.
8. To export the HTTPS Exceptions list, click the icon and click **Export**.

The system exports the exception list as a JSON file and saves it on your computer. You can import this list to other policies.

9. To search for an exception, enter the value in the **Search** box.
10. To remove an item from the list, select it and click the × icon.
11. To save the policy changes, click **Save**.

WiFi Network

WiFi Network Protection Settings



To set the device protection for different MITM attacks:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network** and select the device risk level (from **High** to **No Risk**):

Setting	Description
SSL Interception (Advanced)	Set the risk level when MITM attack intercepts HTTP traffic by using a valid certificate that does not match the certificate of the server.

Setting	Description
SSL Interception (Basic)	Set the risk level when MITM attack intercepts HTTP traffic by using an invalid certificate that does not exist on the device trusted certificates, or is not trusted by a root CA.
MITM - SSL Stripping	Set the risk level when MITM attack intercepts all network traffic redirection from HTTP to HTTPS and strips the HTTP calls leaving the traffic as HTTP.
Unsecure WiFi	Set the risk level when the device connects to an unsecure WiFi network that is open or has no data encryption. For example, a public WiFi hotspot.

3. To save the policy changes, click **Save**.

Geolocation Settings

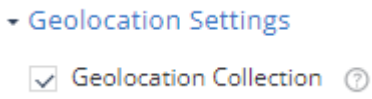
This setting enables collection of the device GPS location when a network attack is detected.

This information is used to provide map detail on the **Network** tab.

To enable geo location capability:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network**.
3. Select the **Geolocation Collection** checkbox.

   This enables it from the Dashboard side. The user must allow the Harmony Mobile Protect app to use the location on their device to collect geo location information.



4. To save the policy changes, click **Save**.

Man In The Middle Detection URLs

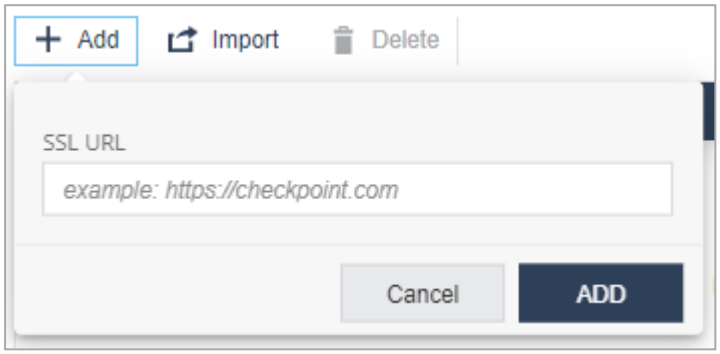
You can monitor suspicious URLs for Man-in-the-Middle (MITM) attacks. If Mobile Security detects any change in the SSL certificate used by the URL, it is categorized as a MITM attack and assigns a risk level for the device.

The risk level is the value set in **WiFi Network Protection Settings** > **MITM - SSL Stripping**.

To add the URLs for the MITM detection:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network** > **Man In The Middle Detection URLs**.
3. Click **Add**.

   A pop-up window appears.



4. In the **SSL URL** field, enter the URL.
5. Click **Add**.
6. To import a list of URLs, click **Import** and upload a .CSV file with URL names list and comments.
7. To remove a URL from the list, select it and click **Delete**.
8. To save the policy changes, click **Save**.

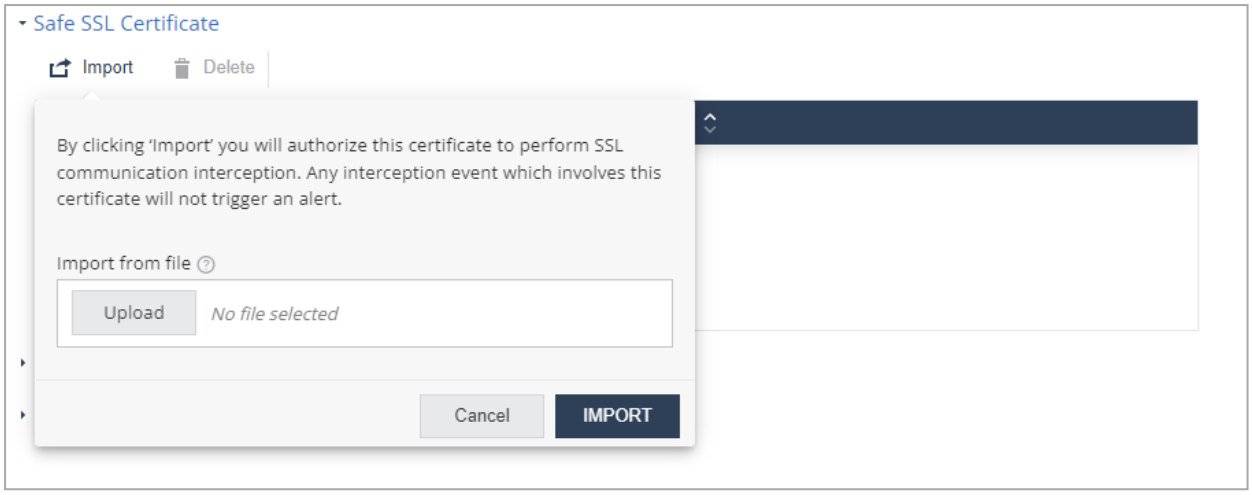
Safe SSL Certificate

You can import trusted SSL certificates and authorize them to intercept SSL traffic so that any change in the certificate is not interpreted as a MITM attack.

To import a SSL certificate:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network** > **Safe SSL Certificate**.
3. Click **Import** and upload the certificate in `.pem` format.

   Click **Import**.

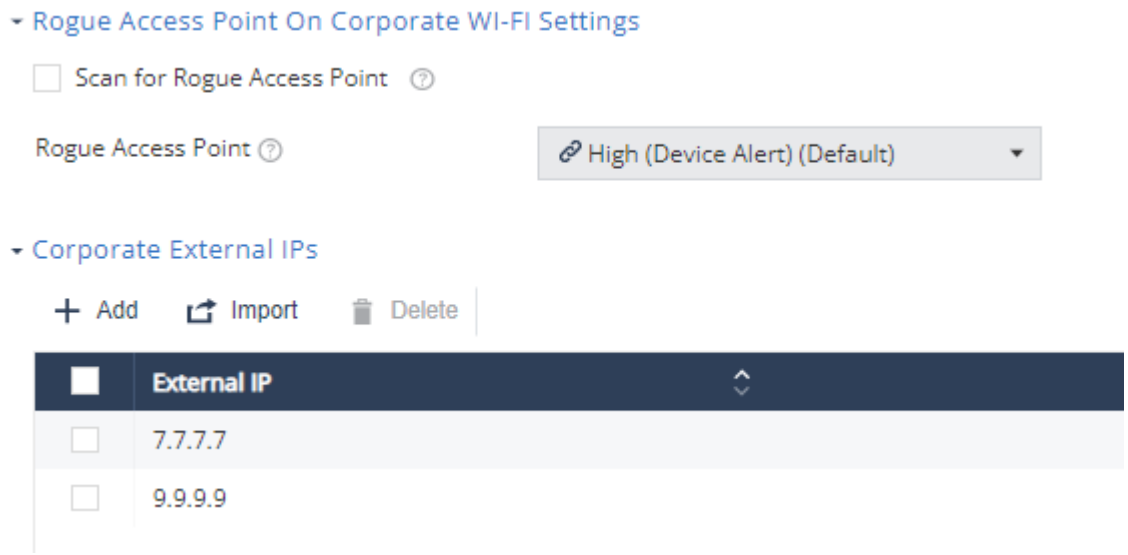


4. To delete a certificate, select it and click **Delete**.
5. To save the policy changes, click **Save**.

Rogue Access Point On Corporate Wi-Fi Settings

Mobile Security detects and sends alerts about rogue Wi-Fi access points. These access points attempt to manipulate corporate end-users on their mobile devices and connect them to a fake access point disguised as a workplace SSID. The hacker can also perform a man-in-the-middle attack, reveal corporate credentials or steal sensitive data. You can set the risk level and policy related to this attack technique in this section.

To detect rogue access point, you must add the corporate used SSIDs and the external IPs. Any access point that uses the corporate SSID but does not go to the internet through one of the corporate's external (public) IPs is not a corporate-owned access point and is therefore a suspected rogue access point.



To detect rogue access point using your corporate Wi-Fi identity:

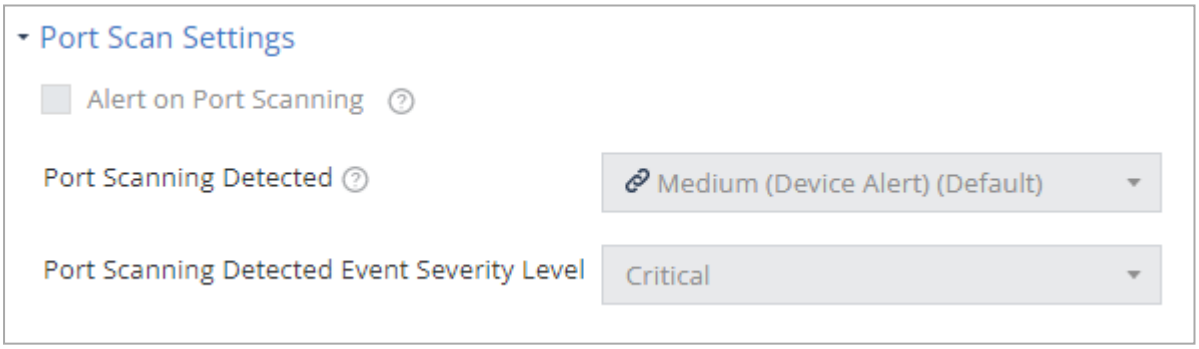
1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network** > **Rogue Access Point On Corporate Wi-Fi Settings**.
3. Select the **Scan for Rogue Access Point** checkbox.
4. From the **Rogue Access Point** drop-down list, select the device risk level (default is **High (Device Alert)**).
5. Configure the **Corporate External IPs**.
6. Configure the **Corporate SSIDs**.
7. To save the policy changes, click **Save**.

When Mobile Security detects a rogue corporate WiFi on a mobile device, the device risk level changes to the one set in this policy. If the risk level is **High** and **Conditional Access** is configured with locations to block, then the access to those corporate resources is blocked immediately.

You can monitor the events and device risk level to manage this threat.

Port Scan Settings

Mobile Security detects scan attempts for open ports on a mobile device. Set the risk level and the policy associated with this attack technique in this section.



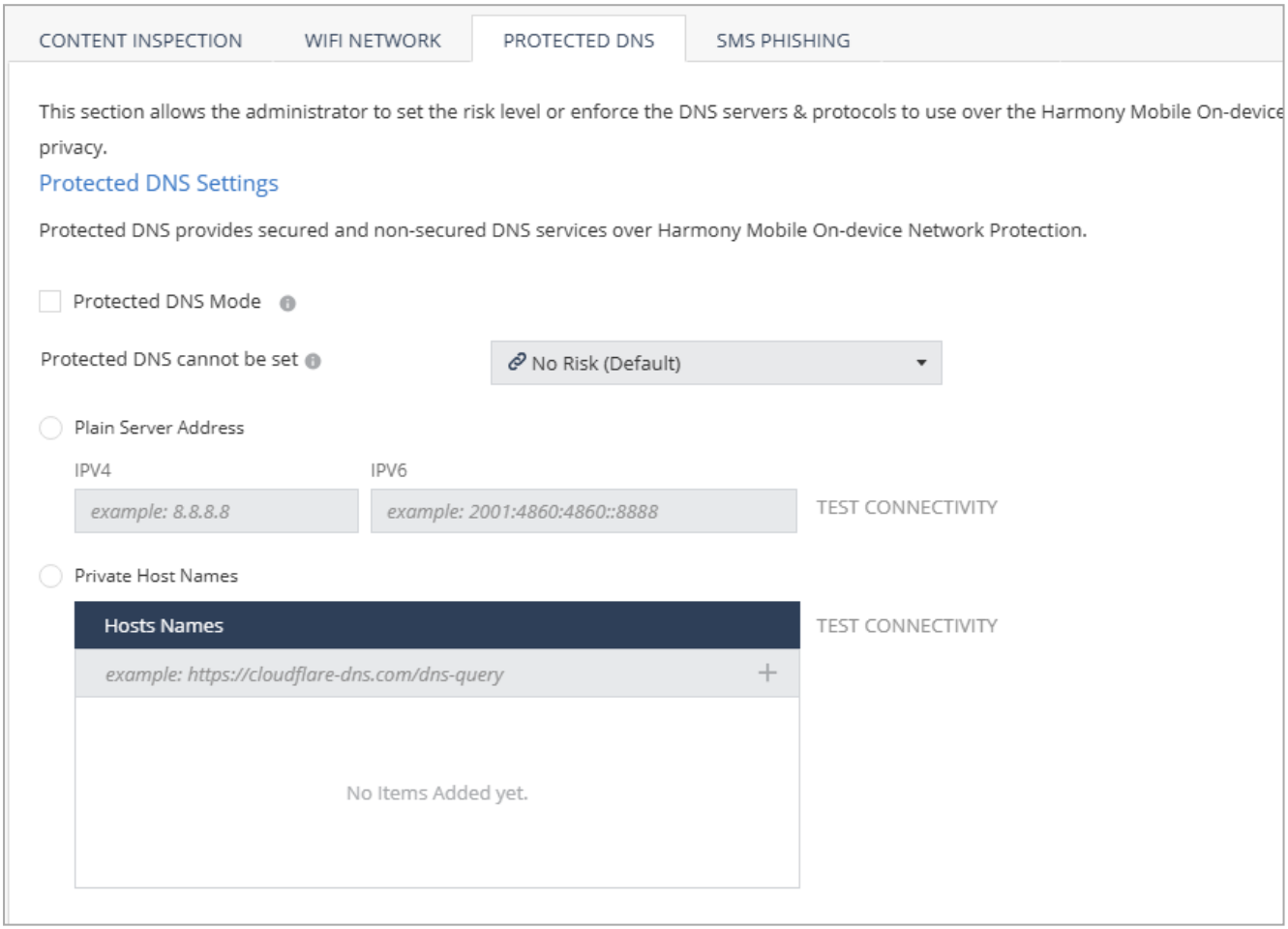
To detect port scan on your corporate mobile devices:

1. Go to **Policy** and select a policy profile.
2. Click **Network** > **WiFi Network** > **Port Scan Settings**.
3. Select the **Alert on Port Scanning** checkbox.
4. From the **Port Scanning Detected** drop-down list, select the device risk level (default is **Medium (Device Alert)**).

5. From the **Port Scanning Detected Event Severity Level** drop-down list, select the event severity level (default is **Critical**).
6. To save the policy changes, click **Save**.

Protected DNS

Protected DNS provides secured DNS services over Mobile Security On-device Network Protection.



A protected DNS service:

- Enhances user privacy and security.
- Ensures that users use their corporate DNS servers instead of the Internet Service Provider (ISP) servers, thereby preventing DNS-spoofing attacks.
- Enforces safe DNS protocols such as DNS over HTTPS (DoH) instead of the plain DNS requests (UDP/53) for end-user privacy.

To configure protected DNS policy settings:

1. Go to **Policy** and select a policy profile.
2. Go to **Network** > **Protected DNS** and set these parameters:

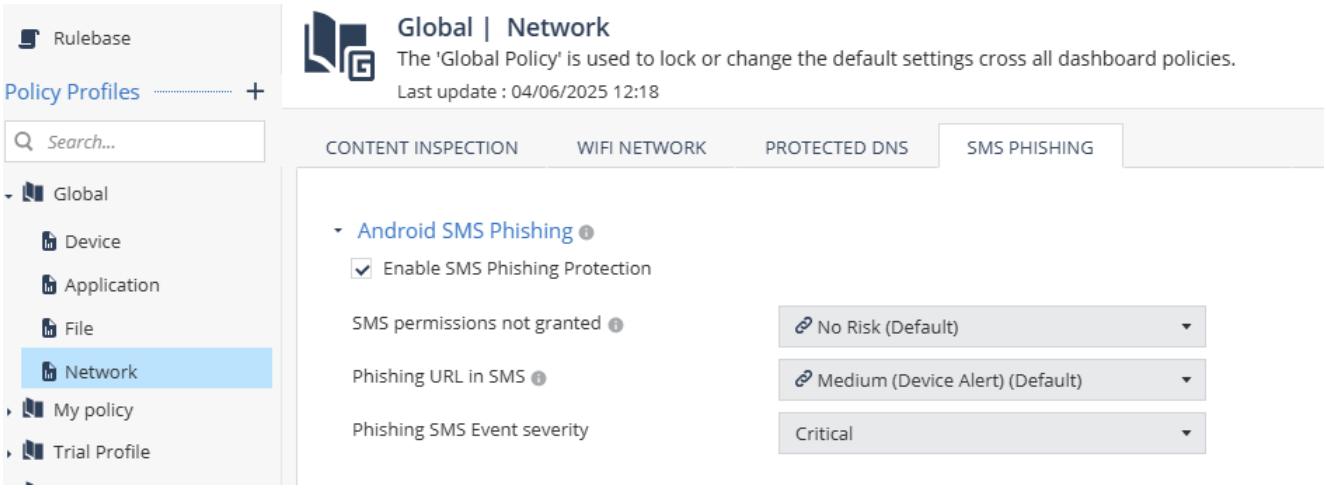
Item	Description
Protected DNS Mode	Indicates whether to enable the protected DNS feature. When it is enabled, Mobile Security on-device Protected DNS becomes the default DNS service for the mobile device.
Protected DNS cannot be set	Set the risk level if the protected DNS feature cannot be set on the device due to one of these reasons: ■ Device is already configured with Private DNS (Android). ■ DNS server is inactive. ■ DNS server does not support secure DNS (DoH/DoT).
Plain Server Address	Add the plain DNS service. Set the IPv4 and IPv6 server addresses for the plain DNS service.
Private Host Names	Add the HTTPS host name to add private (third-party) protected DNS service.

3. To save the policy changes, click **Save**.

SMS Phishing

Android SMS Phishing

The **Android SMS Phishing** setting allows you to enable SMS phishing protection on Android devices. Mobile Security blocks only the URLs categorized as *phishing* by ThreatCloud.



Important - For SMS phishing protection to work, the end-user must grant Mobile Security the permission to read SMS messages on the device.
To enable the SMS permission on the device, see Preventing SMS Phishing in Harmony Mobile Protect app for Android User Guide.

To enable SMS phishing protection:

1. Go to **Policy** and select a policy profile.
2. Go to **Network** > **SMS Phishing**.
3. Select the **Enable SMS Phishing Protection** checkbox.
4. From the **SMS permissions not granted** list, select the risk level if the user does not grant Mobile Security the SMS permission on the device.
5. From the **Phishing URL in SMS** list, select the risk level if Mobile Security detects a SMS with phishing URL.

   Mobile Security notifies the user to manually delete the message from the device. The device is set to **No Risk** after the user deletes the message.
6. Click **Save**.

Note - For iOS devices, the SMS phishing feature is enabled on the device. It blocks the URLs categorized as *malicious* by ThreatCloud.
To enable this feature on the device, see Preventing SMS Phishing in Harmony Mobile Protect app for iOS User Guide.

Blocking Malicious URLs in SMS - ONP v/s SMS Phishing Protection

The table below compares how the **SMS Phishing Protection** and **ONP** features block malicious URLs in SMS on iOS and Android platforms.

<table>
<tr><th>Feature</th><th>iOS</th><th>Android</th></tr>
<tr><td>SMS Phishing Protection</td><td>The feature can be enabled only by the mobile user (due to iOS policy). To enable, see Preventing SMS Phishing.
SMS from known contacts are not inspected.
Only URLs in SMS are inspected (context is not inspected for privacy reasons)
Malicious SMSes are silently quarantined to Junk inbox.
Admins or end-users are not updated about this due to Apple privacy policy.</td><td>The feature must be enabled by the admin in the Mobile Security Administrator Portal and the mobile user needs to grant the SMS permission to Mobile Security.
Only URLs in SMS are inspected.
The admin and the end-user are notified when a malicious URL is detected.
User needs to manually remove the SMS from the device as Mobile Security does not have the permission to remove SMS.
A risk level is raised for the device until the user deletes the malicious SMS.</td></tr>
<tr><td></td><td colspan="2">No user action is required to detect malicious links with SMS Phishing Protection (users do not need to open the SMS and tap the link).</td></tr>
<tr><td>ONP</td><td colspan="2">Feature is enabled by the admin in the Mobile Security Administrator Portal or by the UEM.
End-user accesses the SMS with malicious link.
When user taps the link, access is blocked.
User is redirected to blocking page.
Admin is notified about the access attempt.
Admin can also add the URL to the URL Filter Categories.
ONP protects users from malicious URLs from different sources (SMS, Email, WhatsApp). However, to detect the malicious link with ONP, the user need to open the SMS/message source and tap the link.</td></tr>
</table>

To ensure complete protection from malicious URLs in SMS, Check Point recommends to enable both **ONP** and **SMS Phishing Protection**.

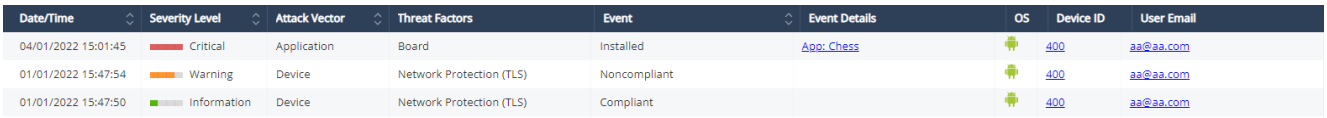
Forensics

In the **Forensics** tab, you can view all the security forensic data collected across the enterprise.

It has the following sub-sections:

Events and Alerts

The **Events & Alerts** tab shows an audit trail of incidents and actions that occurred on the devices, for example, Application installation and Profiles detected on devices.



Date/Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID	User Email
04/01/2022 15:01:45	Critical	Application	Board	Installed	App: Chess		400	aa@aa.com
01/01/2022 15:47:54	Warning	Device	Network Protection (TLS)	Noncompliant			400	aa@aa.com
01/01/2022 15:47:50	Information	Device	Network Protection (TLS)	Compliant			400	aa@aa.com

Events & Alerts table:

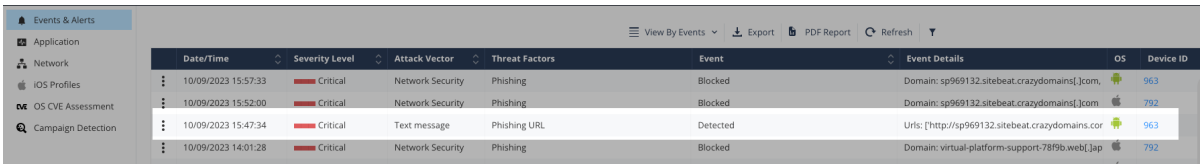
Item	Description
Date/Time	Displays the date and time when the event occurred.
Severity level	▪ **Critical**: • Indicates a malicious threat (such as a malware application) that has immediate impact on the device and sensitive corporate data. • Requires immediate action. • Triggers an alert on the user device to remediate the threat (for example, remove the malware, disconnect from the infected Wi-Fi network). • Sends an email/SMS alert to the administrators (if you define in the dashboard settings). ▪ **Warning**: Indicates a potential threat by a legitimate application, configuration or company policy violation. Examples: • Backup tools (Application) might be legitimate for personal use but will risk the organization if extracts information to unknown destinations. • **Enable USB Debugging** on Android might be legitimate for developers but is a potential risk for regular users. ▪ **Information** – Indicates that no further action is required. Appears most often when an Application is removed. **Note** - Low risk events do not trigger an alert on the end-user devices.

Item	Description
Attack Vector	Specifies the nature of the Event/Alert: ■ Application ■ Cellular network ■ Device ■ Network Security ■ OS Exploits ■ Text message ■ WiFi network ■ iOS profiles
Threat Factors	Specifies the threat factor for the event that occurred. Explains the reason for the severity level.
Event	Specifies the user or the action taken by the Mobile Security solution. ■ Noncompliant ■ Compliant ■ Policy changed ■ Active (Device is active) ■ Inactive (Device is inactive) ■ Disconnected ■ Detected ■ Ended ■ Installed ■ Removed ■ Blocked ■ Prevented ■ Deleted ■ Approved ■ Enabled ■ Disabled
Event Details	Additional details about the Event, such as name of application installed or removed Wi-Fi SSID or Identifying information, and so on. Event Details can link to an iOS Profile detail, Network detail, or App Analysis detail.
OS	Operating System of the device (iOS/Android). It is determined by the information received from the device when the application is installed.
Device ID	The device ID in the Mobile Security dashboard.
User email	Device user's email address. It is manually set by the Admin or automatically by UEM when the devices are provisioned.

Note - For Android devices, you get a **Phishing alert** on the dashboard when Mobile Security detects and blocks a SMS phishing attempt on the mobile device. This feature works only if the end-user has granted access to Harmony Mobile Protect app to scan the SMS received on the device.

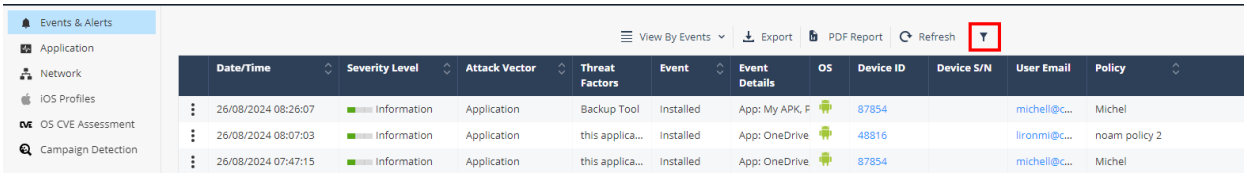
For more information on how to grant the access on the device:

- For Android devices, see Preventing SMS Phishing in Android.
- For iOS devices, see Preventing SMS Phishing in iOS.



Filtering the Events & Alerts Table

1. Click the  icon above the **Events & Alerts** table.

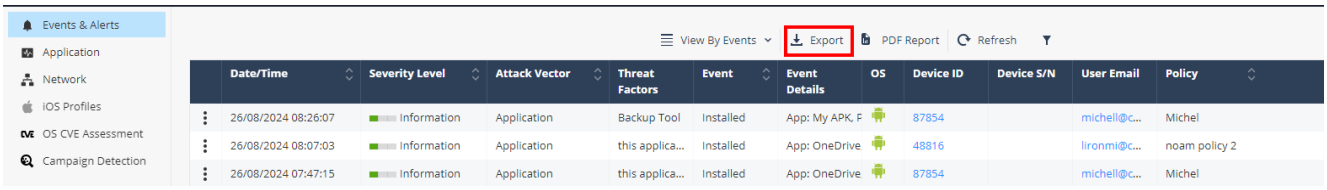


The **Filters** pane appears on the right side.

2. Expand the required category and select the filter.

Exporting Events Data to CSV File

To export Events data to a CSV file, click **Export** above the **Events & Alerts** table.



The system creates a comma separated values file that can be opened in spreadsheet applications such as Microsoft Excel. Use filter to select the required information for the file.

If the number of events exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days. For privacy reasons, PII data is obfuscated in the CSV file.

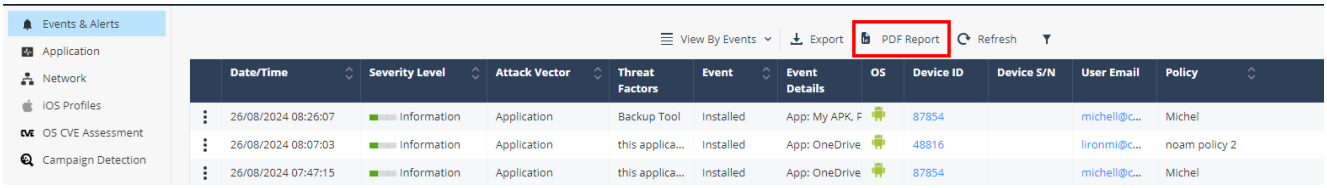
Generating Mobile Security Report

The **Mobile Security Report** provides an overview of the security status of all the mobile devices associated with your account. You can generate and download this report in PDF format whenever you need it, or set up a schedule to automatically generate and receive it on a weekly or monthly basis.

There are two types of security reports:

- **Operational report** - Contains the Operational Overview details such as **Device Status**, **Licensing Information**, **Mobile Models** and so on.
- **Full report** - Contains both the operational overview and the detailed security status of all mobile devices in your account. It provides full visibility to the Mobile Security usage.

To generate the report, click **PDF Report** above the **Events & Alerts** table.

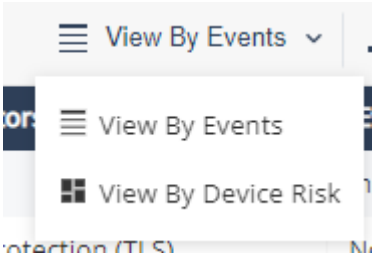


The system generates and downloads the report in this format:
mobile-security-report-yyyy-mm-dd-hh-mm

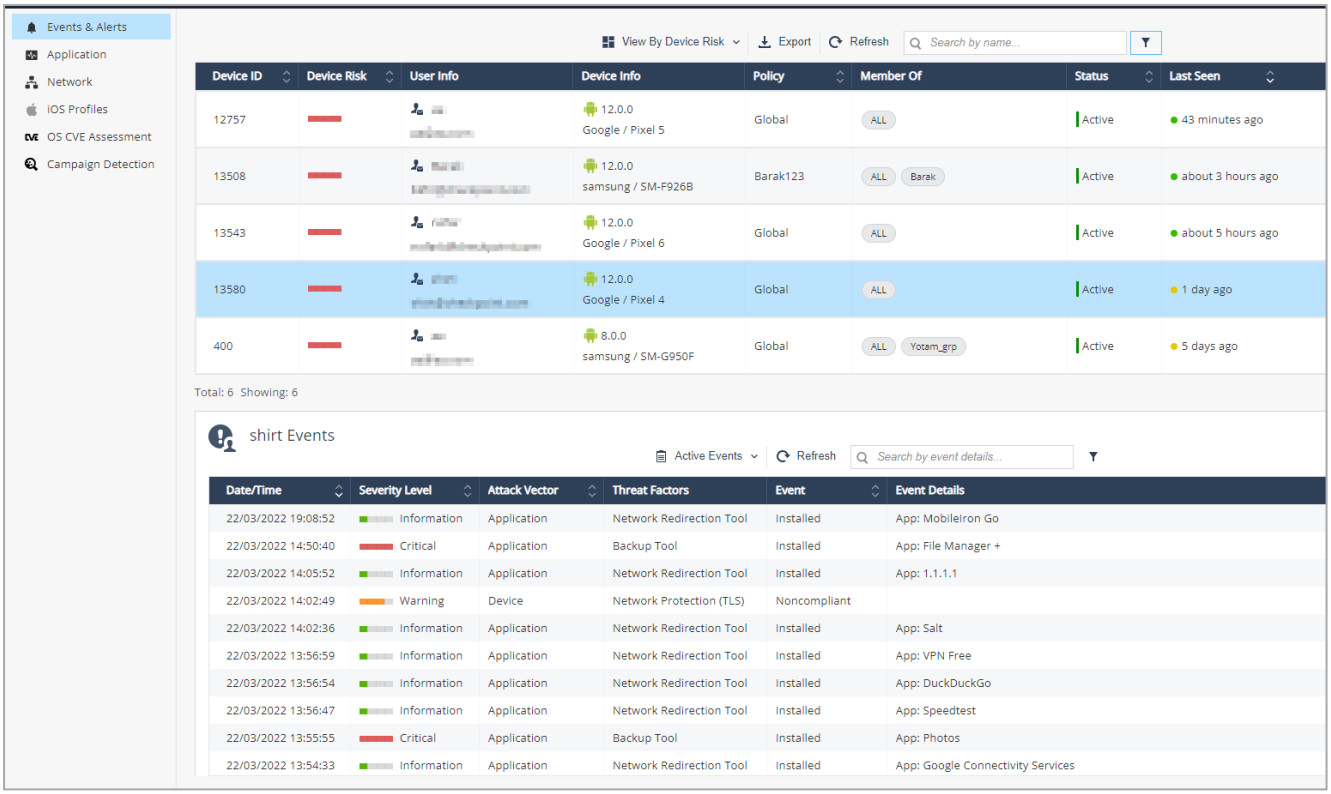
To select the report type and schedule the Mobile Security Report, go to **Settings** > **Administrators** > **Notifications**. See *"Scheduling Mobile Security Report" on page 192*.

Viewing Events by Device Risk

In addition to **Events** view, you can view the events according to device risk (not available when privacy mode is enabled):



This view shows all the necessary risk information per device in the system, and the number of the devices with a specific risk level.

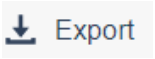


The top table shows the list of devices with their risk levels and the number of devices.

Item	Description
Device Risk	Device risk is determined by both the accumulative threats risk levels found on it and different settings present on the device. (Debugging tools, Jailbreak, Developer Tools, and so on). Risk levels: ■ **High** – Indicates a device is in a malicious state and an immediate action is needed. ■ **Medium** – Indicates a potential threat by a legitimate application or configuration which contradicts the company policy. ■ **Low** – Indicates a device might present potential risky behavior caused by a legitimate application or configuration. This might be caused by a legitimate application which uses an unusual ad network or an application which has access to the device contacts with no reasonable explanation but no potential risk is applied. ■ **None** – Indicates a device has zero risk.
User Info	User name and email as configured in the devices screen.

Item	Description
Device Info	Device Info determined by the information received from the device post the Protect installation: ■ Device type (OS) ■ OS Version ■ Device details
Policy	The device policy, determined according to the device group. Can be Global or custom.
Member Of	The device groups.
Status	Indicates the device current state: ■ Processing – A temporary state that occurs between adding the device manually and the Registration Invitation has been sent. ■ User Notified – A Registration Invitation was sent, device has not yet registered. ■ Provisioned – Device was added via UEM, device has not yet registered. ■ Active – Harmony Mobile Protect app is installed, the device was successfully registered, and the device was successfully scanned. ■ Inactive – Harmony Mobile Protect app was installed, the device was registered with Mobile Security dashboard, and then Harmony Mobile Protect app was removed, or the device has not connected to the Dashboard in more than X days.
Last Seen	Last seen field indicates the last time the device communicated with Mobile Security servers.

You can filter every column in the table:

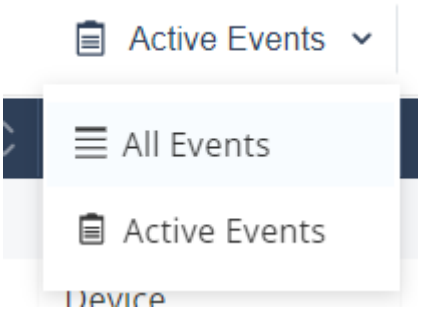
1. Click Filter  above the table.
2. On the **Filters** pane on the right side, select the information you want to view.
3. You can also export 

the mobile devices information from the table to CSV file, which creates a comma separated values file that can be opened in spreadsheet applications such as Microsoft Excel. Use filter to select the required information for the file. Later you can use those details to approach end-users and instruct them how to remove the risk off their mobile devices, or other related actions.

The lower table on the screen shows the chosen device row events details.

This table has two modes:

1. **Active Events** (default): Shows only the active events on the device.
2. **All Events**: Shows active and historic events.

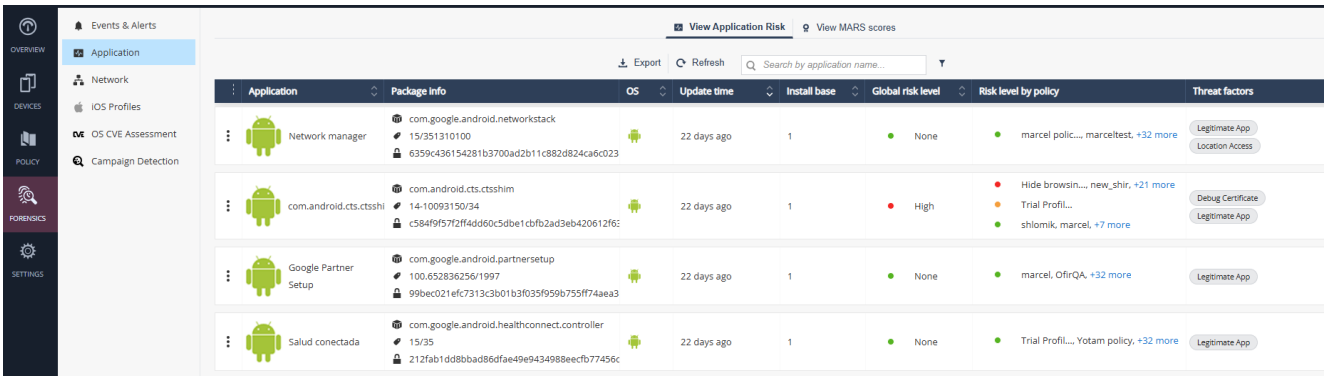


You can filter every column in the table:

1. Click Filter  above the table.
2. On the Filters pane on the right side, adjust information you want to view.

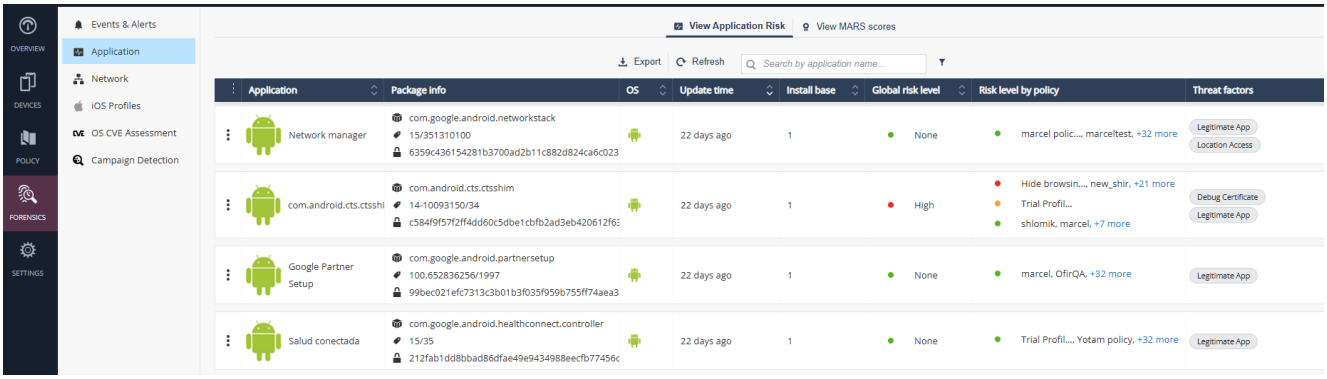
Application

You can view an application by **Application risk** or by **MARS score**.

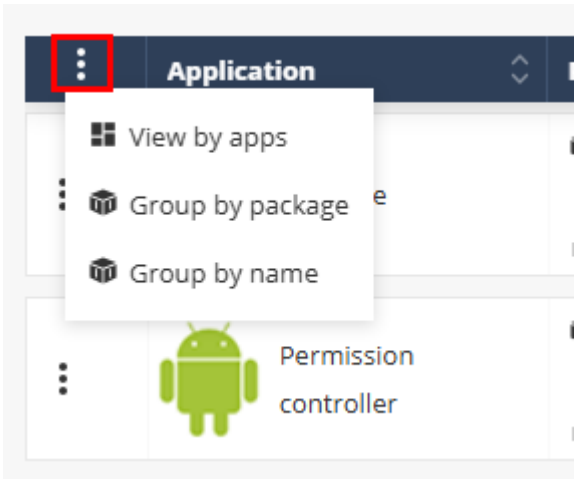


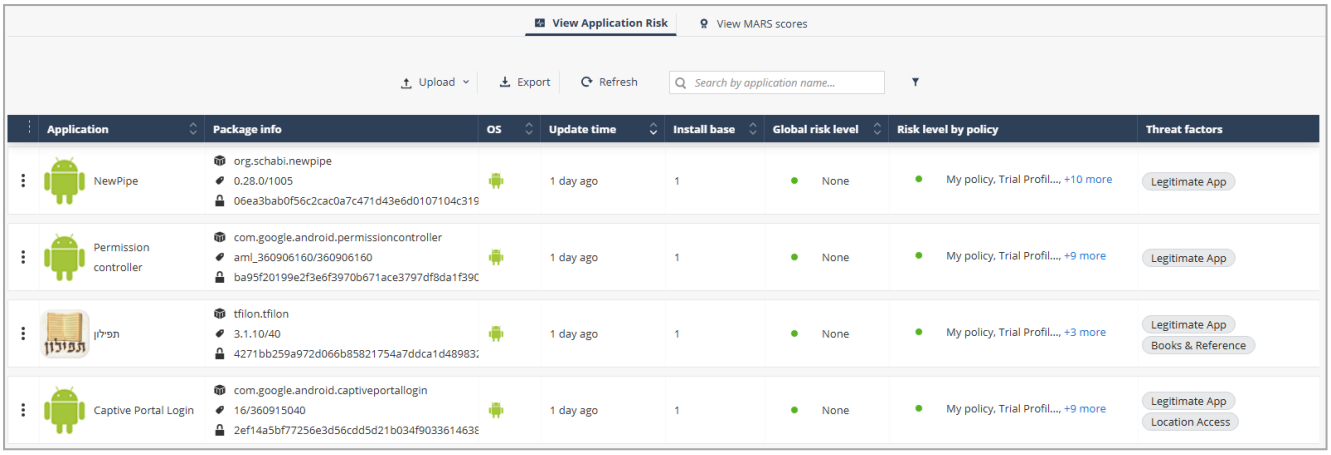
View By Application Risk

Applications Risk view is the main screen for risk analysis of different applications installed on the corporate devices. The applications are categorized to help the administrators understand the risk level. Click on each category to find the corresponding risk level.



You can arrange the application list according to package and name:





Application data:

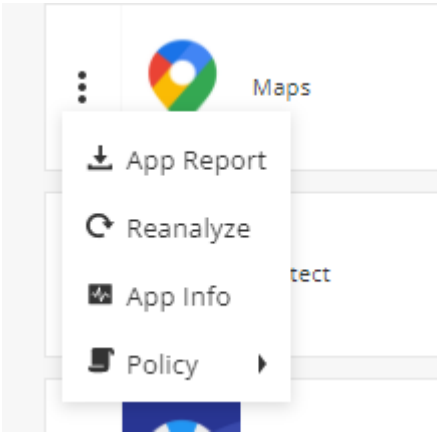
Item	Description
Application	Name of the application.
Package Info	■ Package name ■ Application version ■ SHA 256 of the application
OS	Application platform: ■ Android ■ iOS
Update Time	Indicates the last time the application was updated.
Install Base	The install base tells the administrators the current count of this app version that is currently installed within their environment.
Global risk level	Risk level of the application in the **Global** policy.
Risk level by policy	Risk level of the application in all other policies.

Item	Description
Severity	Highest risk level specified for the application in *"Application Exceptions" on page 102* across all the policies. For example, if the risk level of an application is **High** in policy 1, **Medium** in policy 2 and **Low** in policy 3, then the **Severity** is **High**. ■ **High** – Indicates a malicious application (such as a malware application) that has immediate impact on the device and sensitive corporate data, it requires immediate action. This will trigger an alert to the user on the device to remediate the threat (remove the malware, disconnect from the infected Wi-Fi network, and so on) as well as send an email/SMS alert to the administrators (if defined in the dashboard settings). ■ **Medium** – Indicates a potential threat by a legitimate application, configuration or company policy violation. For example, backup tools (Application) might be legitimate for personal use but will risk the organization by extracting information to unknown destinations. Enable USB Debugging on Android might also be legitimate for developers but is a potential risk for regular users. ■ **Low** – Indicates a legitimate application whose behavior might put the organization data at risk. This might be caused by a legitimate game which uses an unusual ad network or an application which has access to the device contacts with no reasonable explanation, but no potential risk is applied. ■ **None** – Indicates that no further action is needed.
Global Policy	The Global policy of the application: ■ Default ■ Blocked list ■ Allowed list ■ User Approval Click on the policy will direct to Application Policy section with the chosen application details.

- You can filter every column in the table:
  - Click Filter above the table.
  - On the **Filters** pane on the right side of the window, adjust information you want to view.

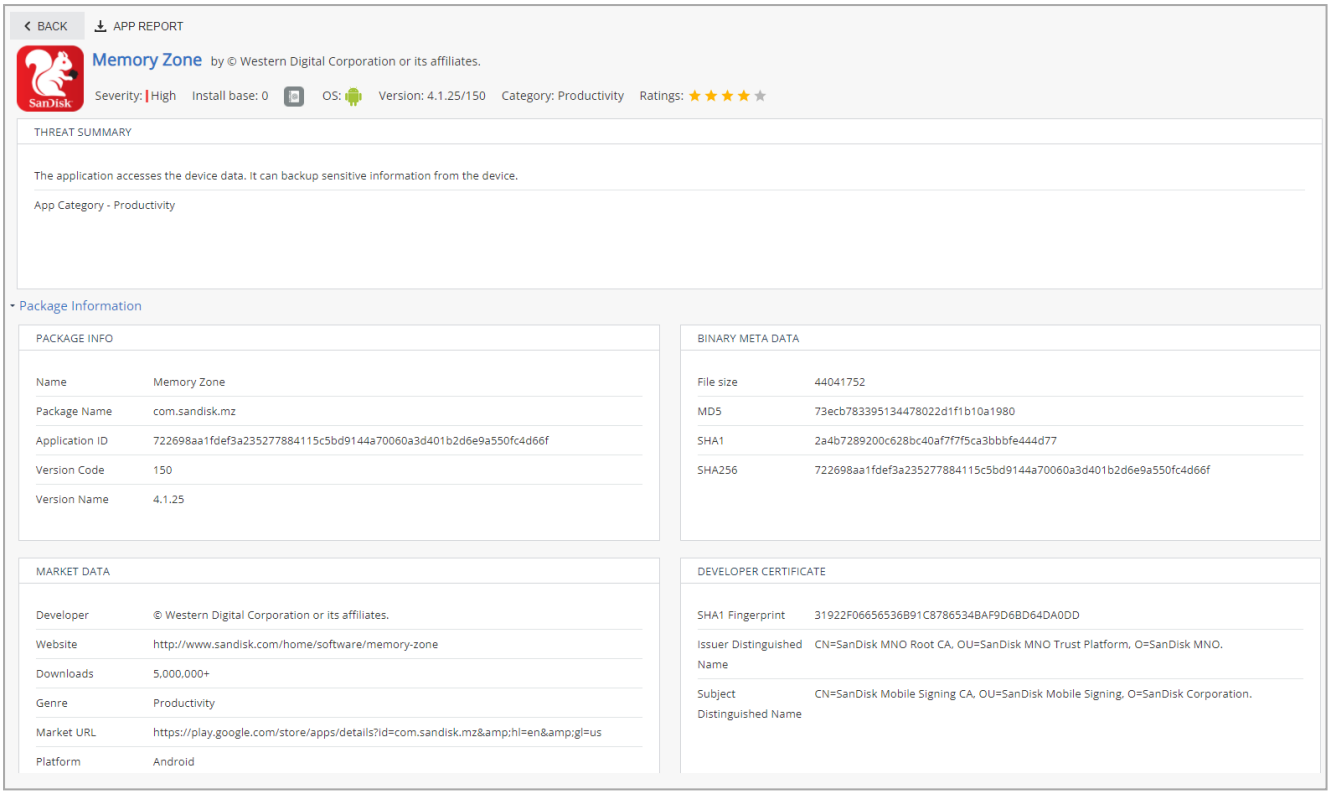
    Note - If you filter for a **Severity Level**, the **Severity** column may not match the specified filtered risk level. This is because the **Severity** column always shows the highest risk level specified for the application in *"Application Exceptions" on page 102* across all policies and at least one policy has the filtered risk level for the application.
    For example, if you filter for **None** and if the **Severity** column shows **High** for some applications, then it indicates that these applications' risk level is set to **None** in at least one of the policies.

- Click .
  - **App Report**: Generates application report
  - **Reanalyze**: Send application to reanalyzed
  - **App view**: Opens an extended application details view
  - **Policy**:Directs to the application policy section.



Application Overview

Click on the application row or on the **App View** option to open the application overview:



Severity

Severity indicates the risk level of the analyzed application. The possible values are:

- **High** – Indicates that the app is malicious or contradicts company policy.
- **Medium** – Indicates a potential threat by a legitimate application or configuration which contradicts the company policy.
- **Low** – Indicates the app might perform potentially risky behavior. This might be caused by a legitimate app which uses an unusual ad network or an app which has access to the device contacts with no reasonable explanation, but no potential risk is applied.
- **No Risk** – Indicates an app is legitimate or complies with company policy.

Install Base

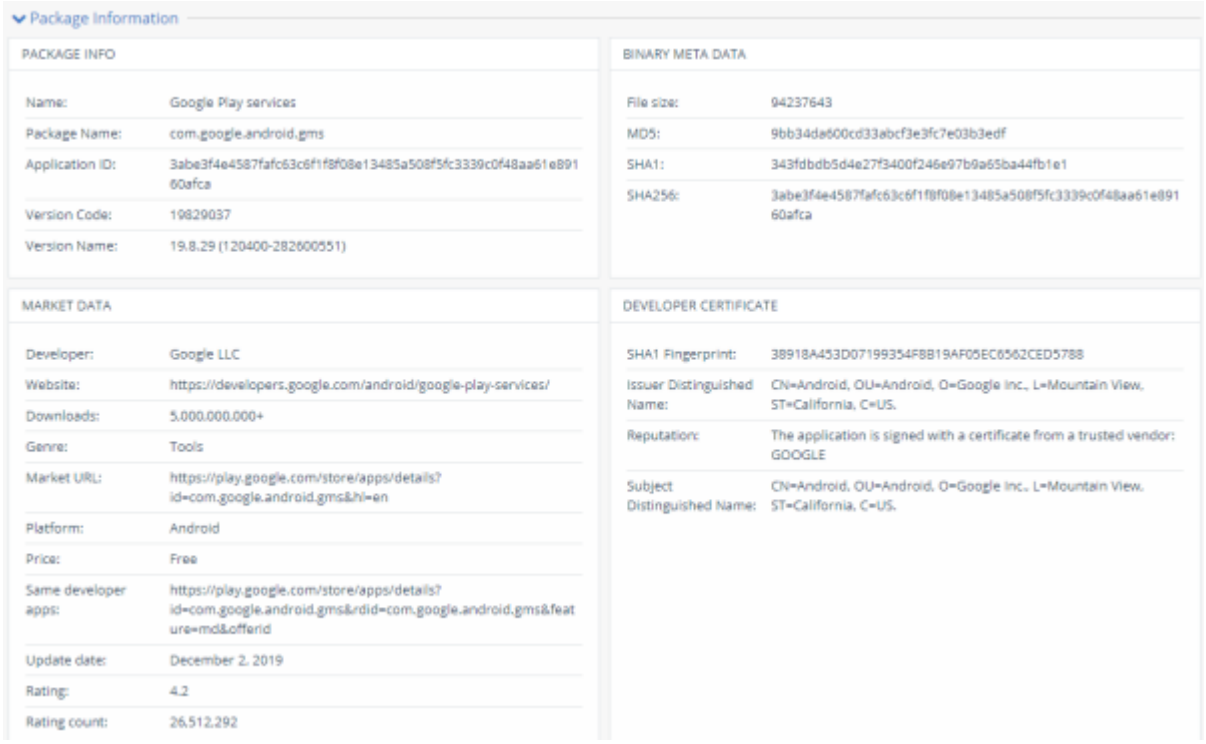
The install base tells the administrators the current count of this particular version of the app that is currently installed within their environment.

At the bottom of the page you can locate information of where this app is installed in the environment (only if the app presents a risk to your organization). See *"Installations" on page 147* for a list of devices on which the app is installed.

Package Information

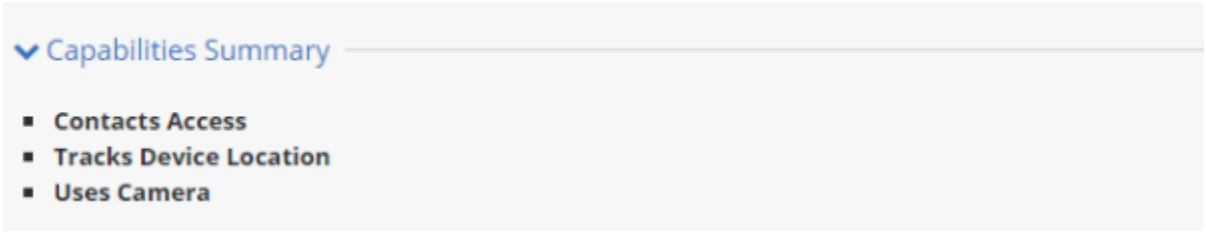
Package Information includes detailed information about these:

- Package Info
- Binary Meta-Data
- Market Data
- Developer Certificate Data



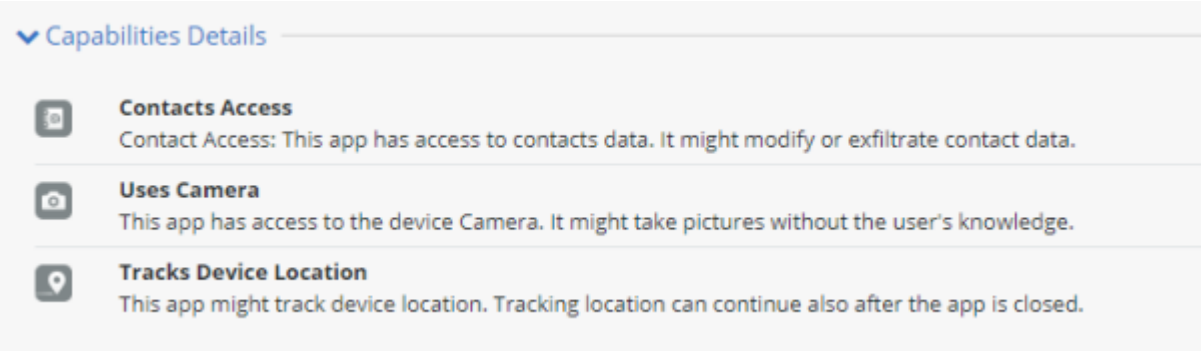
Capabilities Summary

This panel provides an overview of what this application can do.



Capabilities Details

This panel provides additional details about the capabilities of this application.

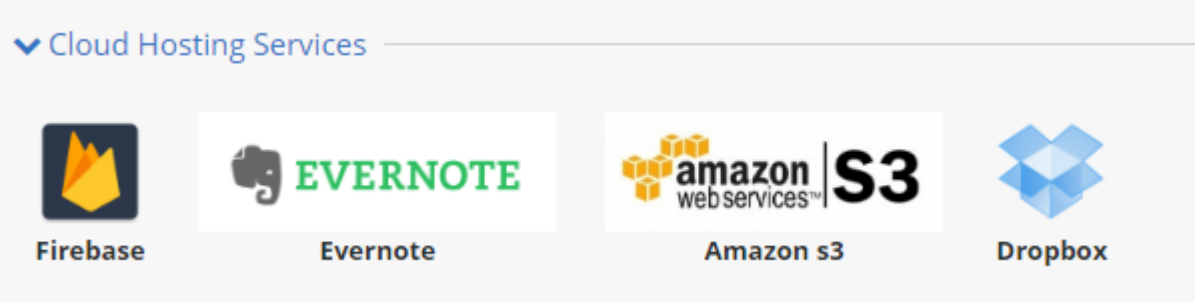


Exploits

Exploits panel appears only on malicious apps which use and exploit the OS vulnerability. It displays detailed information about the exploit and shows the risk level on a 1 to 10 scale.

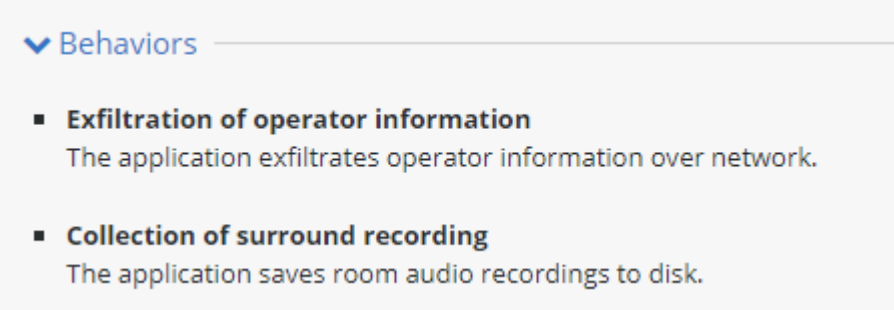
Cloud Hosting Services

This section displays a listing of any cloud services used by the app.



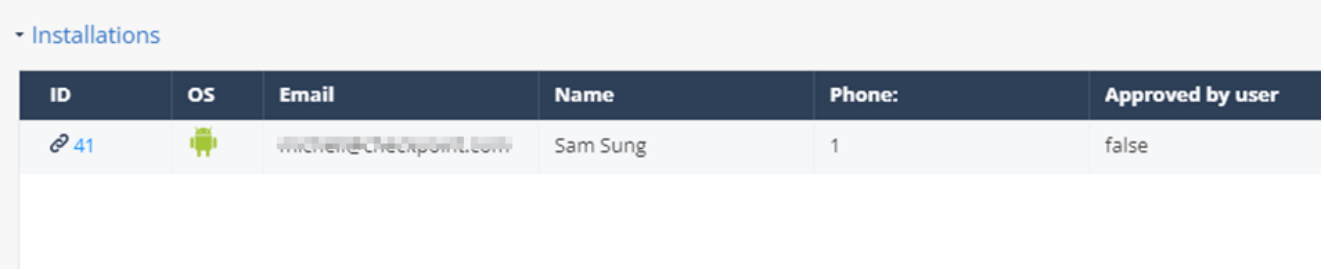
Behaviors

This section displays a collection of characteristics of the app called identifiers. Identifiers are used to declare the current risk level of the app.



Installations

The **Installations** table displays the list of devices where the selected application is currently installed.



Notes -

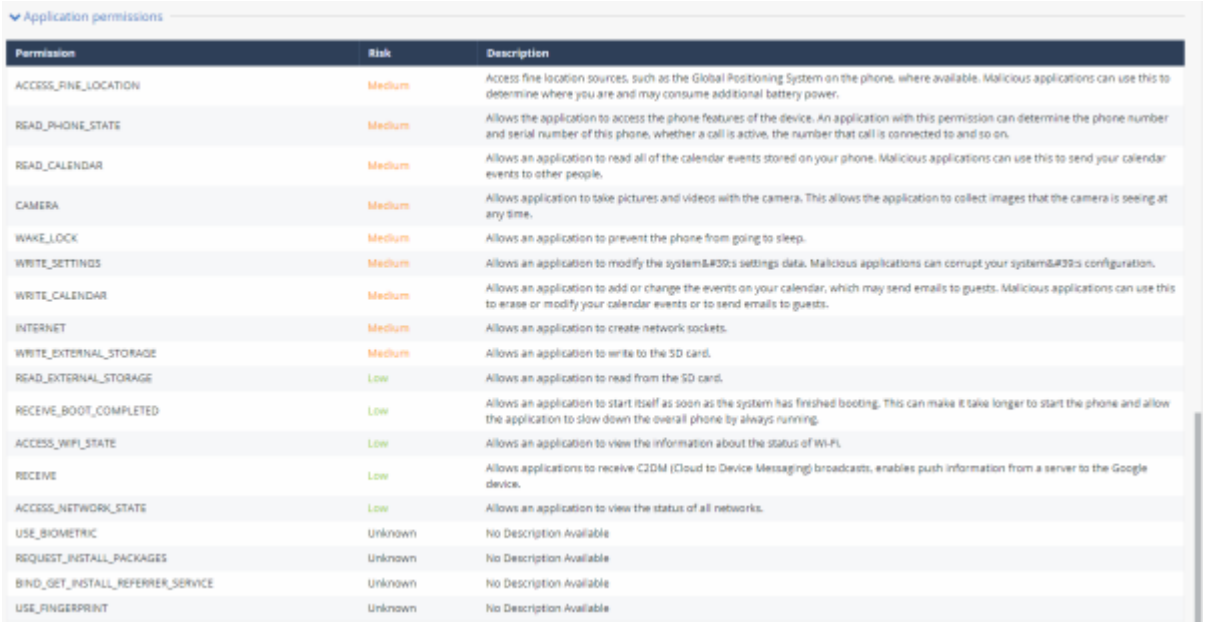
- You can view this list only when the severity of the application is **High**, **Medium** or **Low**.
- This list is not displayed if the application's severity is **None**.
  The list of legitimate apps installed on the user device is not displayed for privacy reasons.
- This list is not displayed when BYOD Privacy Mode is enabled. For more information, see *"BYOD Privacy Mode" on page 176*.

Network

If the app is designed to use the network for specific reason such as send information to a specific URL, this address will be shown in this section.

Application Permissions

The **Application permissions** panel displays the app permissions and the risk level it implies.

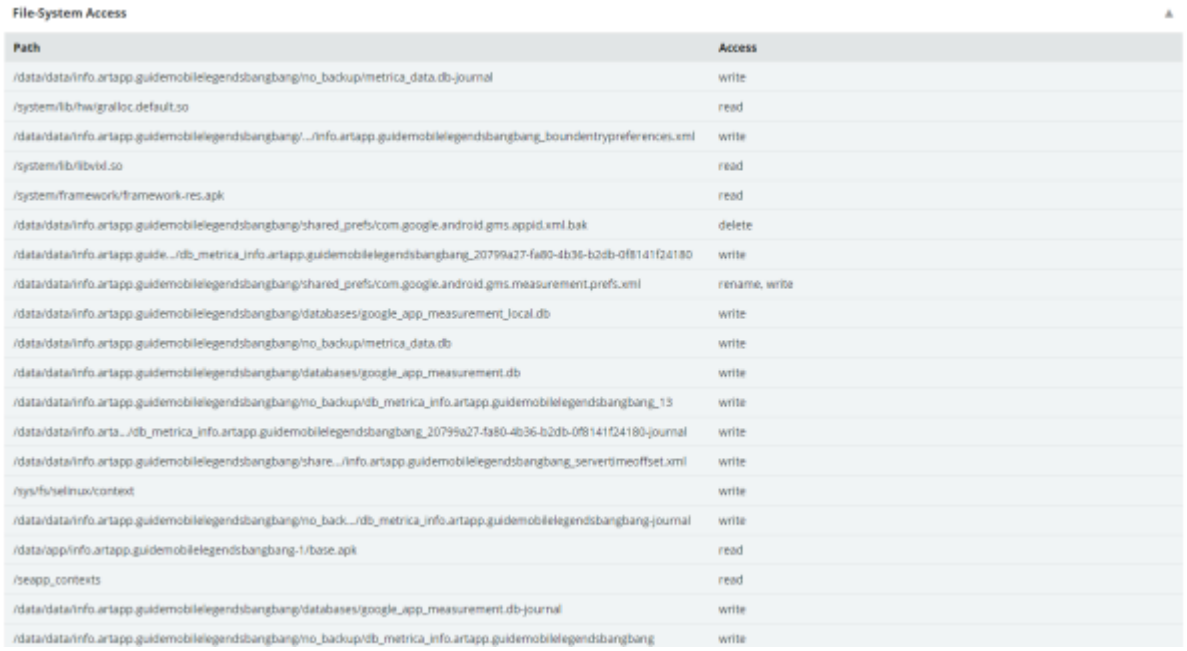


Application permissions

Permission	Risk	Description
ACCESS_FINE_LOCATION	Medium	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
READ_PHONE_STATE	Medium	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
READ_CALENDAR	Medium	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
CAMERA	Medium	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
WAKE_LOCK	Medium	Allows an application to prevent the phone from going to sleep.
WRITE_SETTINGS	Medium	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
WRITE_CALENDAR	Medium	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
INTERNET	Medium	Allows an application to create network sockets.
WRITE_EXTERNAL_STORAGE	Medium	Allows an application to write to the SD card.
READ_EXTERNAL_STORAGE	Low	Allows an application to read from the SD card.
RECEIVE_BOOT_COMPLETED	Low	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
ACCESS_WIFI_STATE	Low	Allows an application to view the information about the status of Wi-Fi.
RECEIVE	Low	Allows applications to receive C2DM (Cloud to Device Messaging) broadcasts. enables push information from a server to the Google device.
ACCESS_NETWORK_STATE	Low	Allows an application to view the status of all networks.
USE_BIOMETRIC	Unknown	No Description Available
REQUEST_INSTALL_PACKAGES	Unknown	No Description Available
BIND_GET_INSTALL_REFERRER_SERVICE	Unknown	No Description Available
USE_FINGERPRINT	Unknown	No Description Available

File System Access

This section displays all of the access permissions this app has to the device file system.



File-System Access

Path	Access
/data/data/info.artapp.guidemobilelegendsbangbang/no_backup/metrica_data.db-journal	write
/system/lib/hw/gralloc.default.so	read
/data/data/info.artapp.guidemobilelegendsbangbang/.../info.artapp.guidemobilelegendsbangbang_boundentrypreferences.xml	write
/system/lib/libvbd.so	read
/system/framework/framework-res.apk	read
/data/data/info.artapp.guidemobilelegendsbangbang/shared_prefs/com.google.android.gms.appid.xml.bak	delete
/data/data/info.artapp.guide.../db_metrica_info.artapp.guidemobilelegendsbangbang_20799a27-fa80-4b36-b2db-0f8141f24180	write
/data/data/info.artapp.guidemobilelegendsbangbang/shared_prefs/com.google.android.gms.measurement.prefs.xml	rename, write
/data/data/info.artapp.guidemobilelegendsbangbang/databases/google_app_measurement_local.db	write
/data/data/info.artapp.guidemobilelegendsbangbang/no_backup/metrica_data.db	write
/data/data/info.artapp.guidemobilelegendsbangbang/databases/google_app_measurement.db	write
/data/data/info.artapp.guidemobilelegendsbangbang/no_backup/db_metrica_info.artapp.guidemobilelegendsbangbang_13	write
/data/data/info.arta.../db_metrica_info.artapp.guidemobilelegendsbangbang_20799a27-fa80-4b36-b2db-0f8141f24180-journal	write
/data/data/info.artapp.guidemobilelegendsbangbang/share.../info.artapp.guidemobilelegendsbangbang_servertimeoffset.xml	write
/sys/fs/selinux/context	write
/data/data/info.artapp.guidemobilelegendsbangbang/no_back.../db_metrica_info.artapp.guidemobilelegendsbangbang-journal	write
/data/app/info.artapp.guidemobilelegendsbangbang-1/base.apk	read
/seapp_contexts	read
/data/data/info.artapp.guidemobilelegendsbangbang/databases/google_app_measurement.db-journal	write
/data/data/info.artapp.guidemobilelegendsbangbang/no_backup/db_metrica_info.artapp.guidemobilelegendsbangbang	write

MITRE ATT&CK Matrix

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. When Mobile Security detects a malicious application, it uses the MITRE ATT&CK tactics and techniques to categorize and represent the risks and damages that this application may cause.

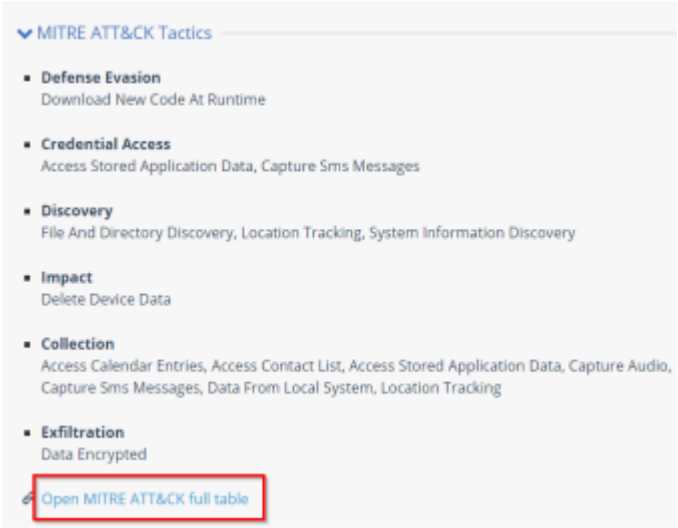
For more information about the MITRE ATT&CK Matrix, see https://attack.mitre.org/techniques/mobile/

Note - The MITRE ATT&CK Matrix is available only if the application contains malware.

To view the MITRE ATT&CK Matrix for an application:

1. Go to **Forensics** > **Application**.
2. Do one of these:
   - If the application was installed on the tenant device, click **View Application Risk**.
   - If the application file or URL was uploaded for analysis, click **View MARS scores**.
3. Click the application in the table to view its details.

   Note - If you selected **View MARS scores** in step 2, click the application and then click **App Info** to view the application details.
4. To view the attack technique description, click any of the **MITRE ATT&CK Tactics** (for example, T1532: Data Encrypted).
   The system opens a web page on the MITRE ATT&CK website that shows the description of the specific attack technique.
5. To view the complete MITRE ATT&CK Matrix for the application, click **Open MITRE ATT&CK full table**.
   This matrix highlights the tactics and techniques used for the application.

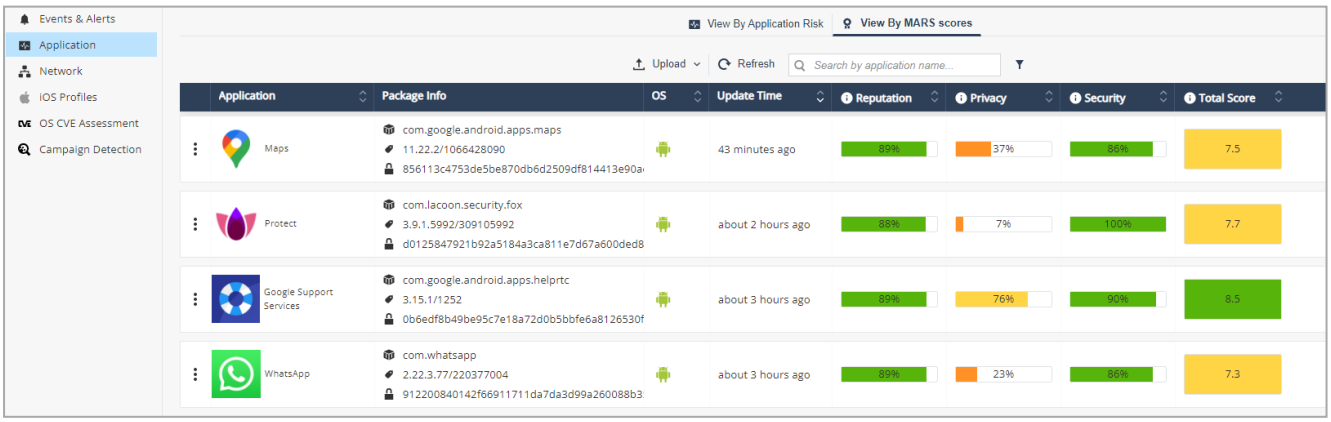


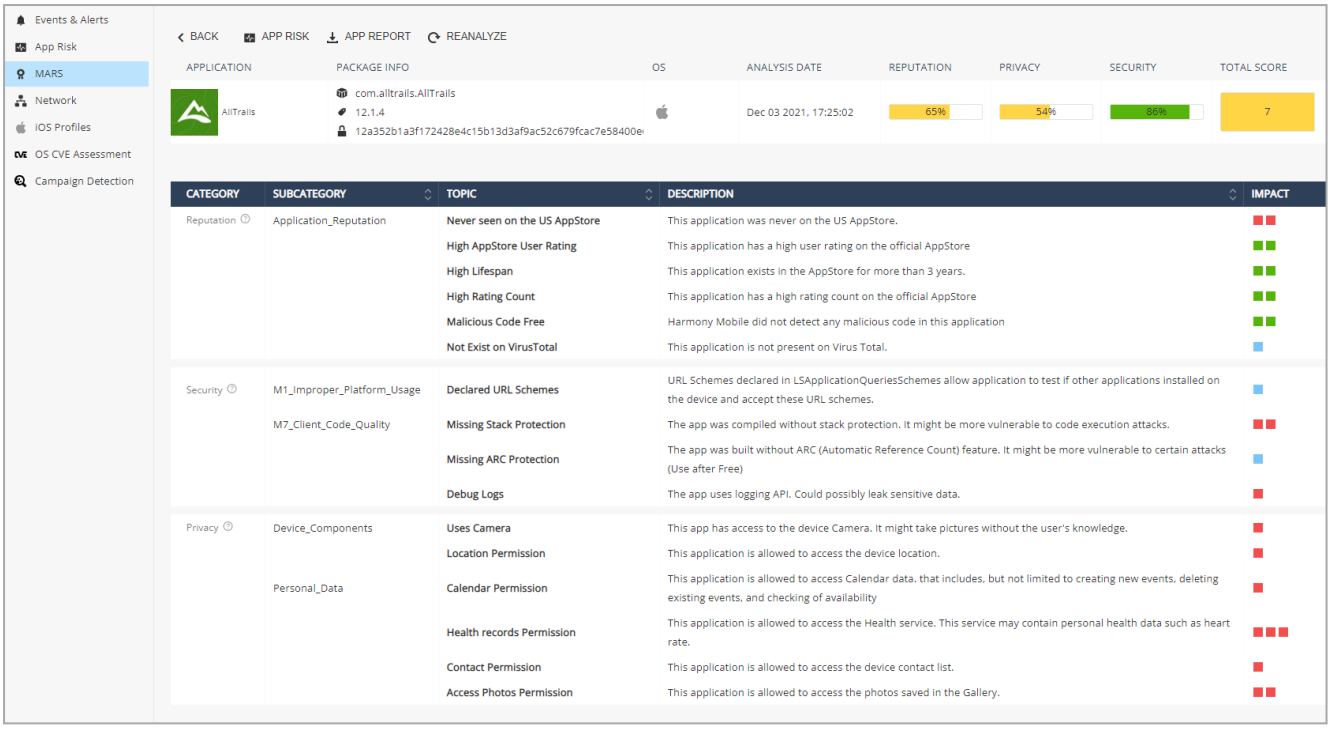
MARS – Mobile Application Reputation Service

MARS provides analysis of any mobile application that is uploaded to the service either as a binary file or a link to the official Apple App Store and Google Play. To view the MARS score of applications, go to **Application** and click the **View MARS scores** tab.

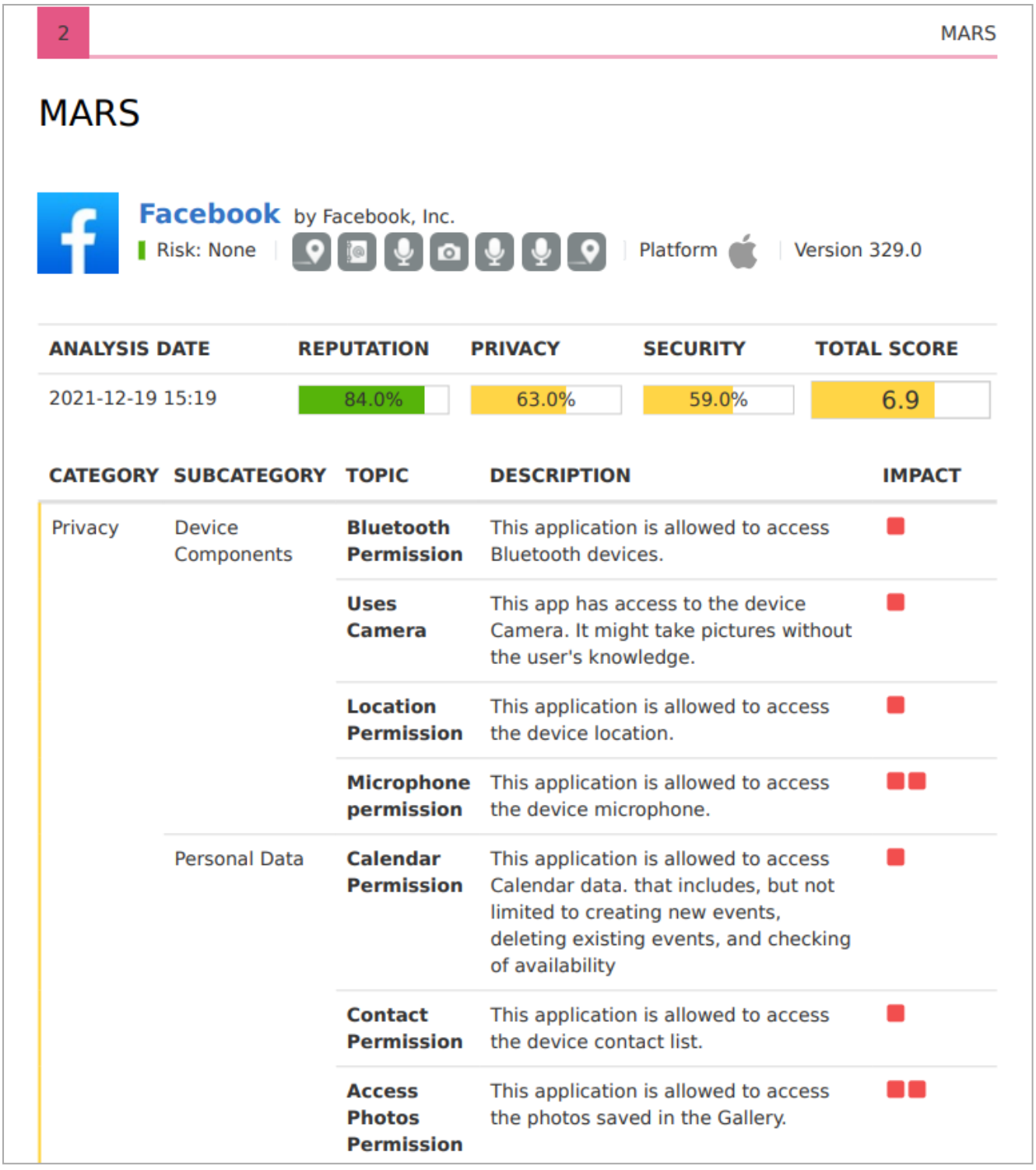
With MARS, administrators can upload an application either as a binary file (APK - Android App format or IPA - iOS App format) or a direct link to an application in the official store (Apple App Store or Google Play Store), once uploaded into Mobile Security Dashboard, administrator receives a full app analysis report after few minutes.

- To learn about an application, administrator should upload the APK/IPA file, iOS App Store link or Google Play Store link into Mobile Security Dashboard (under Forensics > MARS tab).
- If the App is analyzed for the first time, it may take few minutes for Mobile Security to analyze the App, when done - administrator receives an email with a link to MARS full App analysis report, at the same time MARS dashboard is updated with new report.
- MARS generates a report which analyses the application according to 3 categories: security (vulnerabilities), reputation and privacy. Each category consists of a list of findings, split into sub-categories and topics, with their associated impact on the category score.
- For each category a score is calculated according to MARS analysis findings, then, a weighted summary score is given to the application.
- If the App was already analyzed by Mobile Security, administrator can immediately view or download the full App analysis.
- After reading the App analysis report, administrators can make educated decisions based on full App analysis before they distribute an App into their organization's Mobile devices.
- The App analysis report consists of the data as described in 'App Analysis Overview' (p.62) plus the MARS analysis for the 3 categories – security, reputation and privacy.
- MARS detailed app report is linked to its App Risk analysis, clicking on 'App Risk' icon will take you directly to the App Risk analysis page.
- Administrator can also export a full app report (MARS + Risk Analysis) and ask to reanalyze the app if a new version is available on the Apple app store or Google Play.




Events & Alerts
App Risk
MARS
Network
iOS Profiles
OS CVE Assessment
Campaign Detection
BACK
APP RISK
APP REPORT
REANALYZE
APPLICATION
PACKAGE INFO
OS
ANALYSIS DATE
REPUTATION
PRIVACY
SECURITY
TOTAL SCORE
AllTrails
com.alltrails.AllTrails
12.1.4
Dec 03 2021, 17:25:02
65%
54%
86%
7
CATEGORY
SUBCATEGORY
TOPIC
DESCRIPTION
IMPACT
Reputation
Application_Reputation
Never seen on the US AppStore
This application was never on the US AppStore.
High AppStore User Rating
This application has a high user rating on the official AppStore
High Lifespan
This application exists in the AppStore for more than 3 years.
High Rating Count
This application has a high rating count on the official AppStore
Malicious Code Free
Harmony Mobile did not detect any malicious code in this application
Not Exist on VirusTotal
This application is not present on Virus Total.
Security
M1_Improper_Platform_Usage
Declared URL Schemes
URL Schemes declared in LSApplicationQueriesSchemes allow application to test if other applications installed on the device and accept these URL schemes.
M7_Client_Code_Quality
Missing Stack Protection
The app was compiled without stack protection. It might be more vulnerable to code execution attacks.
Missing ARC Protection
The app was built without ARC (Automatic Reference Count) feature. It might be more vulnerable to certain attacks (Use after Free)
Debug Logs
The app uses logging API. Could possibly leak sensitive data.
Privacy
Device_Components
Uses Camera
This app has access to the device Camera. It might take pictures without the user's knowledge.
Location Permission
This application is allowed to access the device location.
Personal_Data
Calendar Permission
This application is allowed to access Calendar data, that includes, but not limited to creating new events, deleting existing events, and checking of availability
Health records Permission
This application is allowed to access the Health service. This service may contain personal health data such as heart rate.
Contact Permission
This application is allowed to access the device contact list.
Access Photos Permission
This application is allowed to access the photos saved in the Gallery.

App report (MARS and Risk Analysis):



2 MARS

MARS

Facebook by Facebook, Inc.

Risk: None | Platform | Version 329.0

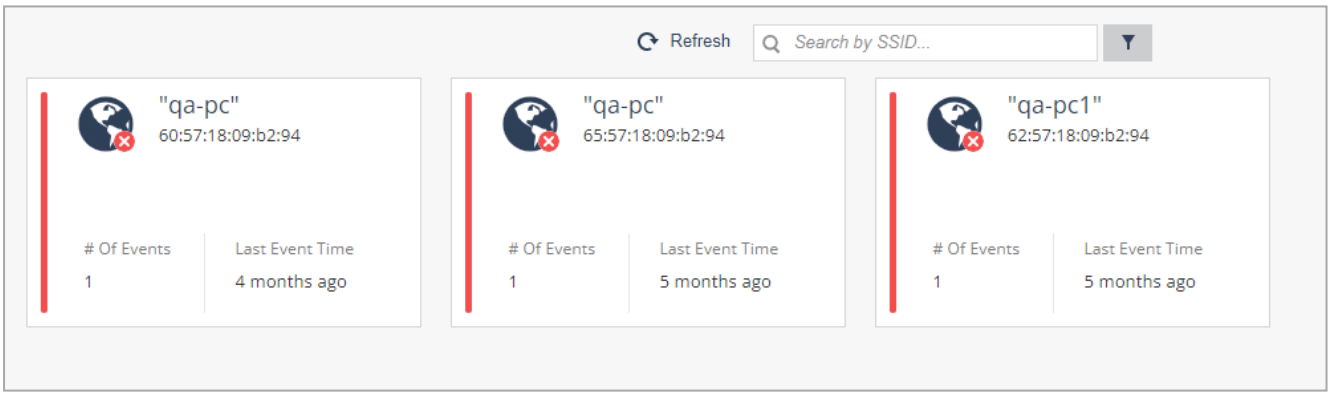
ANALYSIS DATE	REPUTATION	PRIVACY	SECURITY	TOTAL SCORE
2021-12-19 15:19	84.0%	63.0%	59.0%	6.9

CATEGORY	SUBCATEGORY	TOPIC	DESCRIPTION	IMPACT
Privacy	Device Components	**Bluetooth Permission**	This application is allowed to access Bluetooth devices.	
		Uses Camera	This app has access to the device Camera. It might take pictures without the user's knowledge.	
		Location Permission	This application is allowed to access the device location.	
		Microphone permission	This application is allowed to access the device microphone.	
	Personal Data	**Calendar Permission**	This application is allowed to access Calendar data. that includes, but not limited to creating new events, deleting existing events, and checking of availability	
		Contact Permission	This application is allowed to access the device contact list.	
		Access Photos Permission	This application is allowed to access the photos saved in the Gallery.	

Network

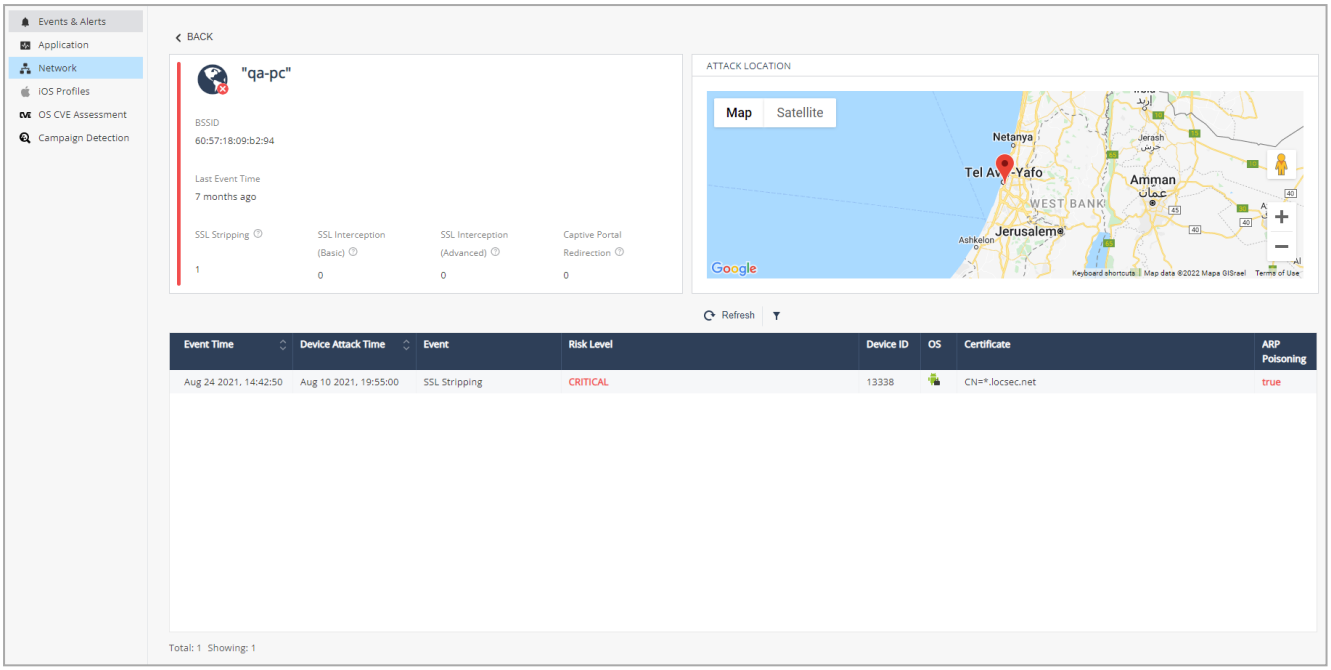
The **Network** tab displays any network event reported. It provides a more granular view of network events in the context of the network in which they occurred. The network events reported are:

- **SSL Stripping** – A third-party intercepted the traffic and downgraded it from HTTPS to HTTP.
- **SSL Interception (Basic)** – A third-party intercepted the traffic and posed as the original requester to the target server while controlling the responses back to the requester.
- **SSL Interception (Advanced)** – Similar to basic SSL Interception, however, in this case the perpetrator responses are encrypted with an SSL certificate issued by a certificate authority listed as trusted on the victim's device. This can be gained by either deceiving the certificate authority to issue an SSL certificate to the perpetrator or by injecting the perpetrator's certificate to the victim device's trusted list. This attack requires advanced skills and a higher level of sophistication.
- **Captive Portal Redirection** – The traffic from the device is redirected to the network portal for registration to the network. This is common with public networks, especially free networks, such as those in airports, hotels, and cafes.



You can click the  icon to filter the list of networks based on Network Name (SSID), BSSID, Device ID (affected device), and Network Status.

Clicking on one of the network card opens the network overview:



Information about reported events in the Network:

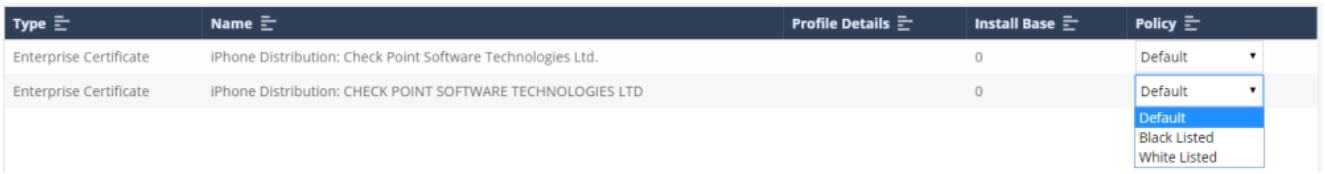
Item	Description
Network Details	
Network Name (SSID)	The name assigned in the access point as the wireless network name.
Occurrences	Number of times a network event was reported for a device in this organization's wireless network.
BSSID	The MAC address of the access point. It is used to identify the network, no matter if the Network Name was changed.
Previous Network Names (SSIDs)	If network name was changed, they are listed in this field.
Attack location	To receive Location, the user is required to enable location collection in the Dashboard Settings and to grant location collection permissions on their device. If the device has geo-location enabled for the Harmony Mobile Protect app, the location of the device is recorded when the device is connected to this network.
Event Summary	What type of Events were identified with this BSSID, such as SSL Stripping, SSL Interception, Captive Portal, etc.

Item	Description
Network Event Details	For each network event reported on this wireless network these details are provided: ■ Event Time – As recorded on the device. ■ Device Attack Time - When event was reported to the Dashboard ■ Event - SSL Stripping, SSL Interception, or Captive Portal Redirection ■ Risk Level – The determined risk level for the event. High, Medium, Low, No Risk. ■ Device ID – The ID in the Dashboard of the device that reported the attack. If the attack still exists in the Dashboard and has a risk associated with it, the Device ID links to the device risk details of the device. ■ Certificate – The SSL certificate of the designated page. Not applicable for SSL Stripping attacks. The value is the root authority at the root of the certificate chain. Clicking on the value will pop-up the entire certificate chain. ■ ARP Poisoning - Indicates if the attack utilized ARP Poisoning

Note - The networks in the list are identified by their BSSID, which is the unique network identifier. However, for readability purposes, the pronounced identifier is the network name (SSID). As a result, several networks of the same name may appear in the list next to each other. In such a case, please make sure to refer to the network of the desired BSSID.

iOS Profiles

iOS Profiles are unique to Apple iOS devices. To assist the mobile device admins, Apple developed a tool called **Profiles**, which includes Network Configuration Profiles, Provisioning Profiles, and Certificates. Network profiles are also used by the legitimate VPN applications. The shortcoming of iOS Profiles is that it opens a security hole where an attacker can create and install a malicious network configuration profile. It makes them act as a Man-In-The-Middle and collect all the information flowing from the device.



Information About iOS Profiles

The **iOS Profiles** tab shows the Network Configuration Profiles. It allows the administrator to get a clear view on the profiles installed on the devices in the organization.

Item	Description
Type	Displays the type of profile – Wi-Fi configuration, VPN, etc.
Name	Profile name as it appears on the iOS device.
Profile Details	Profile details indicated the information (properties) of the profile. Including remote address, IP and servers.
Install Base	Number of devices currently installed with this specific profile.
Policy	Policy drop down menu allows the Administrator to set the alert level of a specific profile in the dashboard.

The **iOS Profiles** tab also shows the Provisioning Profiles that are installed on the organization's iOS devices.

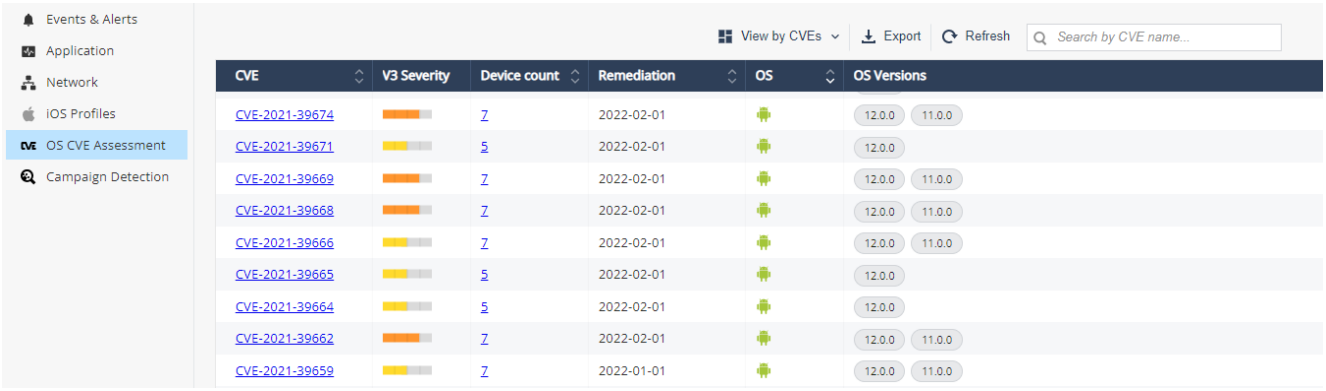
You can filter and select the profile information presented in the table. Filtering options include **Device Type**, **Device Name**, **Install Base**, and **Policy**.

OS CVE Assessment

The **OS CVE Assessment** tab shows the vulnerability status of the devices in the dashboard.

Note - The CVE information is derived from National Vulnerability Database. When the CVE information is updated in the National Vulnerability Database, Mobile Security automatically updates the dashboard.

View by CVEs

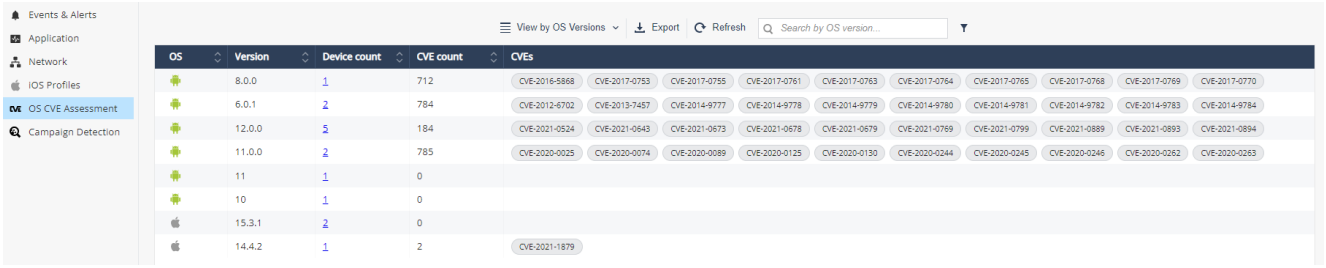


Item	Description
CVE	OS CVE name. Click on the name will direct to NVD for full description
V3 Severity	The Common Vulnerability Scoring System (CVSS) is a free and open industry standard to assess the severity of computer system security vulnerabilities. The scores displayed are as per CVSS version 3.x: ■ Low: 0.1 – 3.9 ■ Medium: 4- 6.9 ■ High: 7-9 ■ Critical: 9-10
Device Count	Number of devices that are exposed to the displayed CVE. Click on the number will direct you to the devices tab
Remediation	The release date of the security patch to the CVE
OS	Operating System (Android/iOS)
OS Version	List of OS Versions that contain the CVE

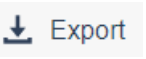
To export the CVEs information from the table to CSV file, click **Export**. It creates a comma separated values file that can be opened in spreadsheet applications such as Microsoft Excel. Use a filter to select the required information for the file.

If the number of CVEs exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days.

View by OS Versions



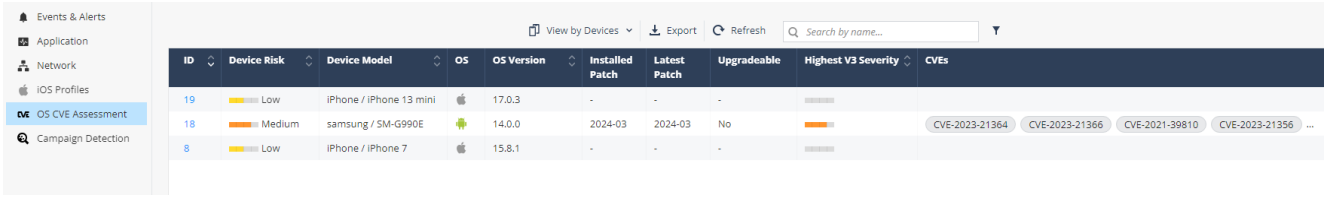
Item	Description
OS	Operating System (Android/iOS)
Version	OS Version
Device Count	Number of devices with the OS version
CVE Count	Number of CVEs that the OS version contains
CVEs	The first 10 CVEs the OS version contains

- You can filter by OS, OS version and CVE name in the table:
  - Click Filter  above the table.
  - On the **Filters** pane on the right side of the window, adjust information you want to view.
- You can also export 

the information from the table to CSV file, which creates a comma separated values file that can be opened in spreadsheet applications such as Microsoft Excel. Use filter to select the required information for the file.

  If the number of CVEs exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days.
- You can set policy according to the OS CVE under **Policy** > **Device** > **OS Vulnerabilities**.

View by Devices



Item	Description
ID	Device ID. To view the device details, click the ID link.
Device Risk	Risk level of the device
Device Model	Model of the device. For example, iPhone 13 Pro, Samsung SM-G998B
OS	Device Operating System ■ Android ■ iOS
OS Version	Device OS version
Installed Patch	The security patch version installed on the Android device.
Latest Patch	The latest security patch version available for the Android device OS version.
Upgradeable	Indicates whether the Android device can be upgraded to the latest security patch version: ■ **Yes** ■ **No**
Highest V3 Severity	Highest CVSS score of the device. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard to assess the severity of computer system security vulnerabilities. The scores displayed are as per CVSS version 3.x: ■ Low: 0.1 – 3.9 ■ Medium: 4- 6.9 ■ High: 7-9 ■ Critical: 9-10
CVEs	The CVEs detected on the device

- To filter the table, click  . You can filter by:
  - **OS**
  - **Device Risk**
  - **Highest CVSS greater than** - Shows the devices with **Highest V3 Severity** greater than the selected value.
  - **Not Connected Since** - Shows the devices not connected with the Mobile Security server since the selected date.
- To export the table to a CSV file, click **Export**.

  If the number of devices exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days.

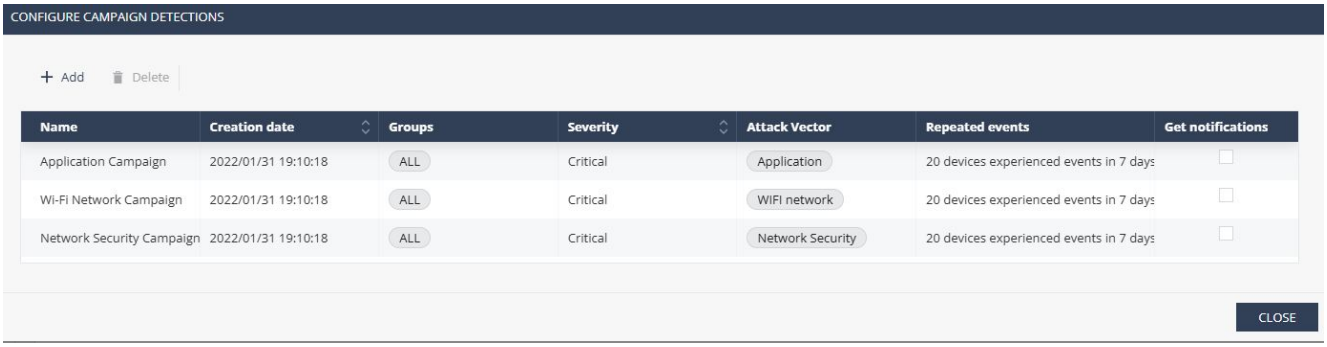
Campaign Detection

In the **Campaign Detection** tab, you can define attack campaigns you will be notified about.

A campaign is an attack using the same attack vector several times. For example, Network Security.

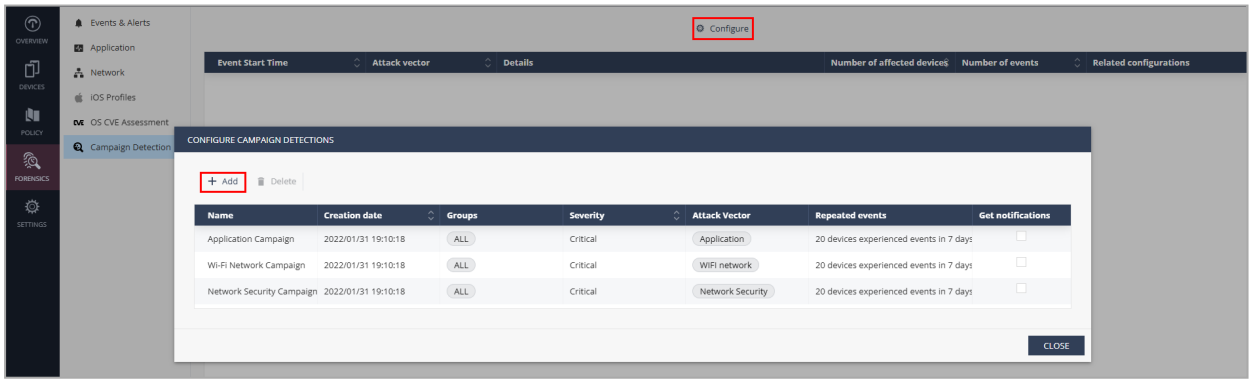
You can create pre-configured campaigns for:

- Applications
- Wifi
- Network security



To create a new campaign detection:

1. Go to **Forensics** > **Campaign Detection**.
2. Click **Configure** > **+Add**.



3. In the configuration window, enter:
   a. **Name** - Campaign name
   b. **Devices group** - Select the device groups to apply the campaign
   c. **Severity** - Severity level of the event

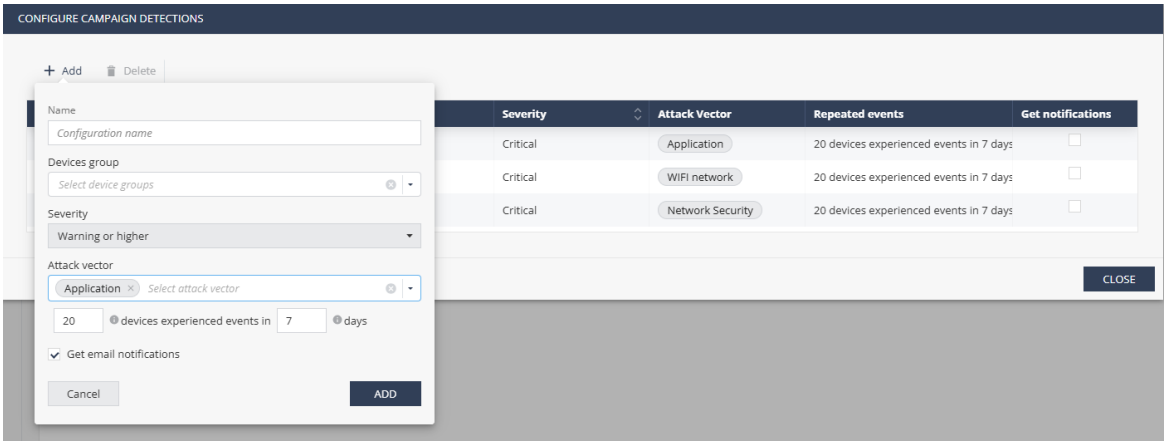
d. **Attack vector** - Select attack vectors

e. Select the number of devices and days.

   This count defines the scope of your campaign.

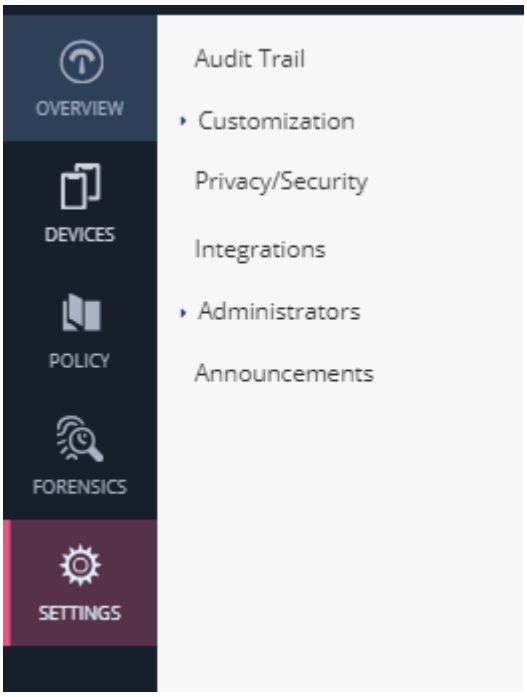
f. To receive email notification about the campaign, select the **Get email notifications** checkbox.

g. Click **Add**.



Settings

In the **Settings** tab, you can view and manage the dashboard settings, customize the detailed view of the private information for users, applications and devices.



The available settings are:

- *"Audit Trail" on page 164*
- *"Customization" on page 165*
- *"Privacy/Security" on page 174*
- *"Integrations" on page 178*
- *"Administrators" on page 191*
- *"Announcements" on page 196*

Audit Trail

The **Audit Trail** screen shows the logs for the system.

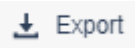
You can search the audit logs by **Time**, **Severity**, **Admin User**, **Module**, **Category**, **Event**, and **Event details**.

Severity	Date/Time	Admin User	Module	Category	Event	Event Details
Info	25/08/2021 15:5...	System	Device Manage...	MDM app sync	Succeed	UEM: None
Info	25/08/2021 15:5...	System	Device Manage...	MDM app sync	Started	UEM: None

Select one or more drop-down search options to produce a report of specific log entries.

- You can filter every column in the table:

  1. Click Filter  above the table.
  2. On the **Filters** pane on the right side of the window, adjust information you want to view.

- You can also export 

the information from the table to CSV file, which will create a comma separated values file that can be opened in spreadsheet applications such as Microsoft Excel. Use filter to select the required information for the file.

  If the number of audit logs exceeds 10,000, processing the data may take time. So the export is performed offline and an email is sent to the registered address with the link to download the CSV file. The link is valid for 7 days.

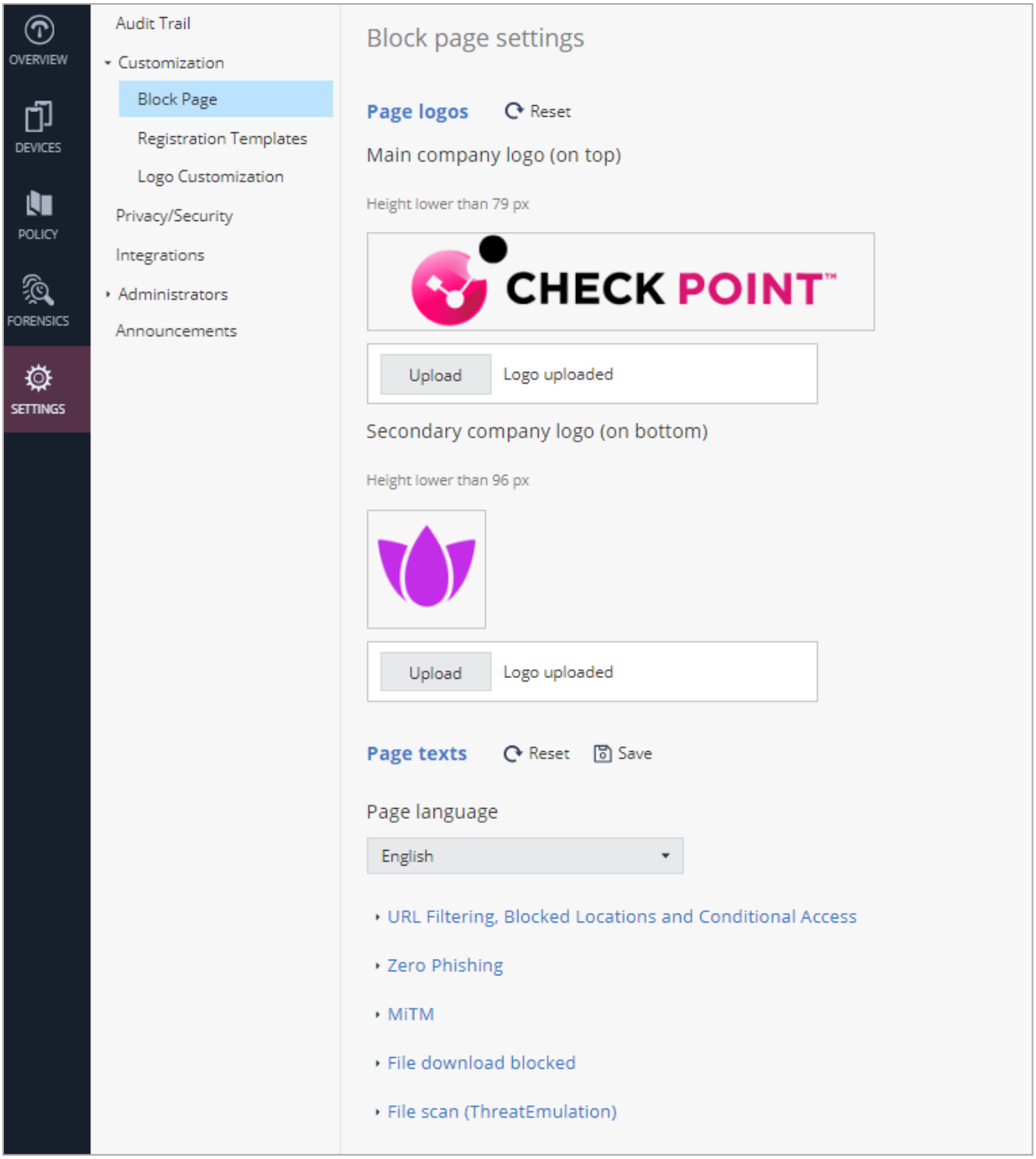
- You can set the number of the rows to list on the screen, and scroll to view previous items.

Customization

Block Page

The **Block Page** setting allows you to customize the content displayed on the block page that appears when a user accesses a web page blocked by the organization's security policy.

To customize, go to **Settings** > **Customization** > **Block Page**.

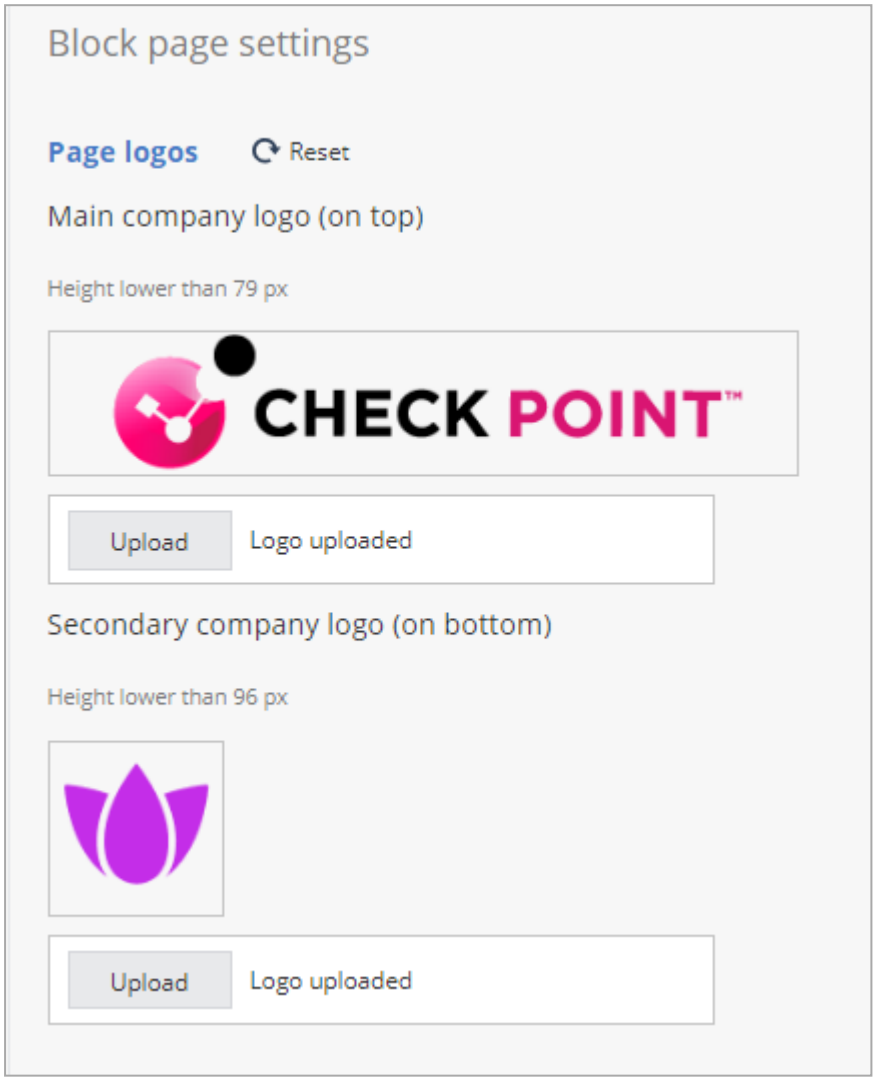


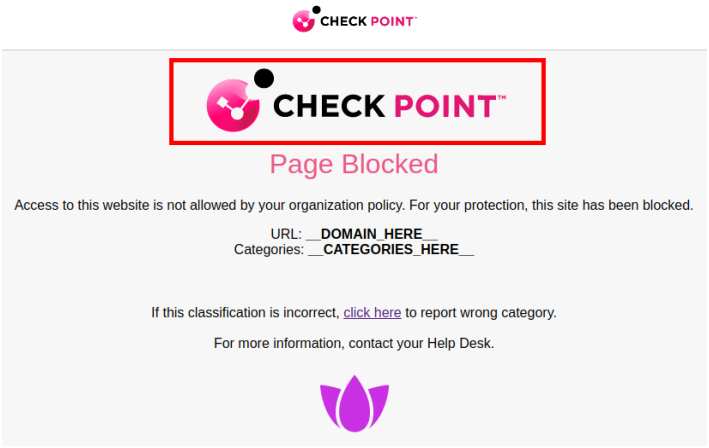
Note - To prevent Cross-Site Scripting (XSS) attacks, the text on the **Block Page** is always sanitized. Any hyperlinks or URLs added to this page are displayed as plain text on mobile devices.

To customize the block page:

1. To add the main logo, in the **Main company logo** section, click **Upload** and upload the image for the main logo. Check Point logo is the default.

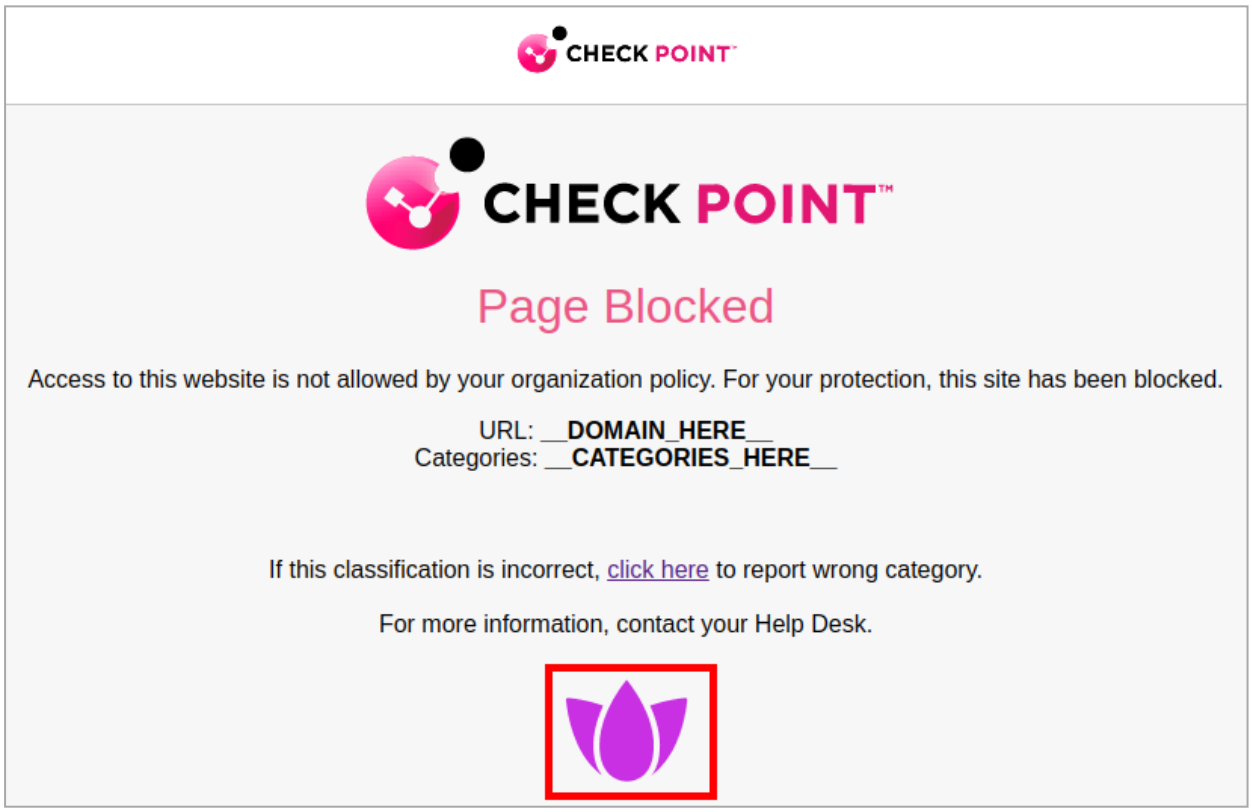
   Note - The height of the logo must be less than 79 pixels. Supported file types are .png and .jpeg, with a maximum size of 150KB.





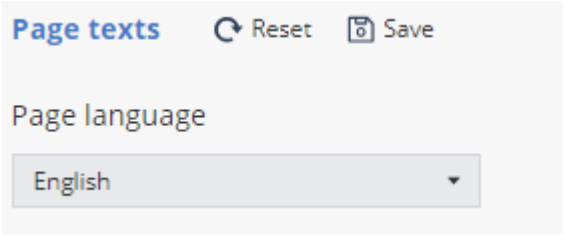
2. To add the secondary logo, in the **Secondary company logo** section, click **Upload** and upload the image for the secondary logo.

   Note - The height of the logo must be less than 96 pixels. Supported file types are .png and .jpeg, with a maximum size of 150KB.



3. In the **Page texts** section, select the language of text to be displayed on the block page and click **Save**.

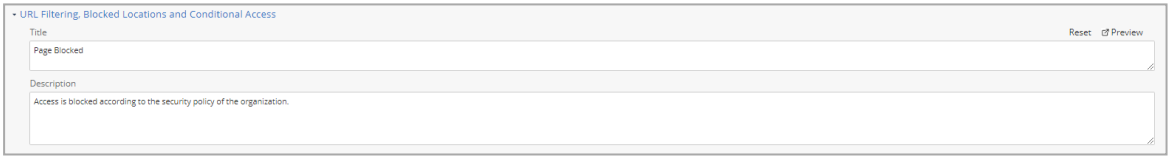
   The default language is English.



To reset to default language, click **Reset** and then **Save**.

Note - If the mobile OS is configured in an unsupported language, the block page is displayed in English.

4. Expand any of these:
   - URL Filtering, Blocked Locations and Conditional Access
   - Zero Phishing
   - MiTM
   - File download blocked
   - File scan (Threat Emulation)

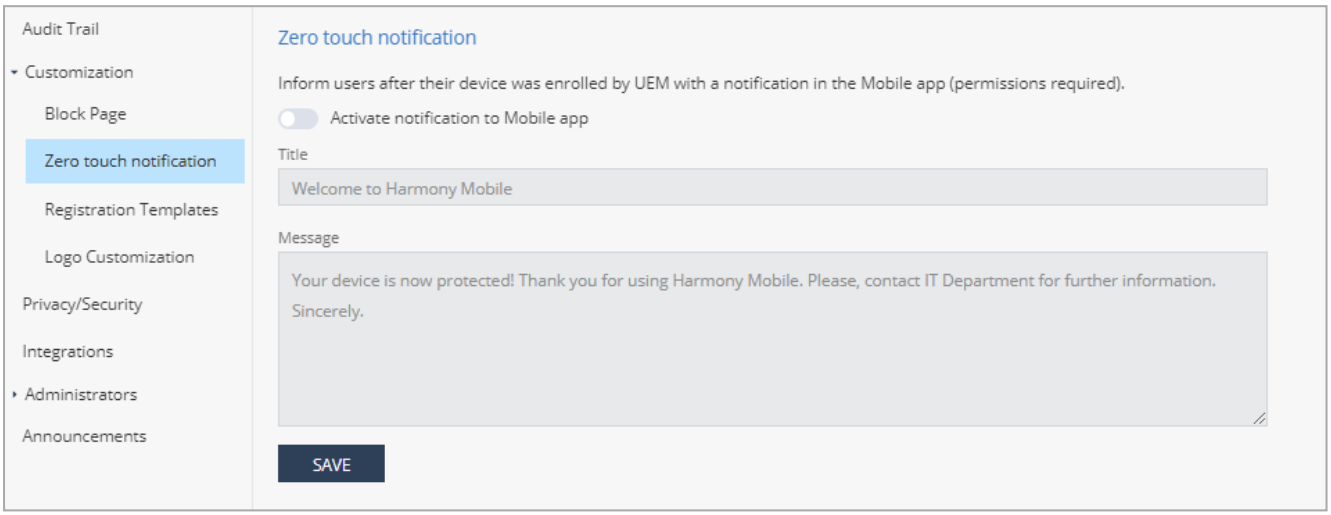


   a. In the **Title** field, enter the title for the block page.
   b. In the **Description** field, enter the reason for blocking the page.
   c. To preview the changes, click **Preview**.
   d. To reset the values to default, click **Reset**.
5. To save the page text in the current language, in the **Page texts** section, click **Save**.

Zero Touch Notification

The **Zero touch notification** setting allows you to notify users when Harmony Mobile Protect app is automatically installed on their device.

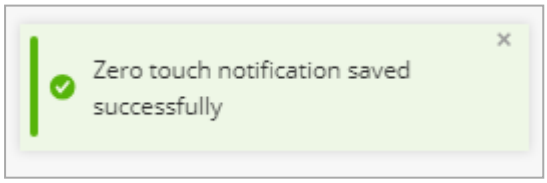
Note - The system sends a Zero Touch notification only if the UEM deployed the Harmony Mobile Protect app on devices through Zero Touch deployment.



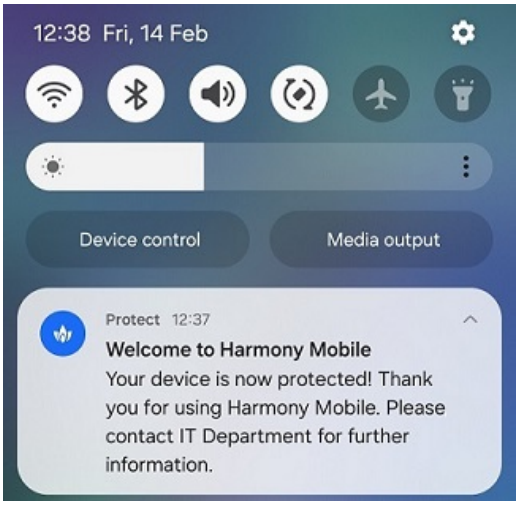
To enable Zero touch notification:

1. Go to **Settings** > **Customization** > **Zero touch notification**.
2. Turn on the **Activate notification to Mobile app** toggle button.
3. If required, customize the text in **Title** and **Message** fields.
4. Click **Save**.

   The system displays this message:

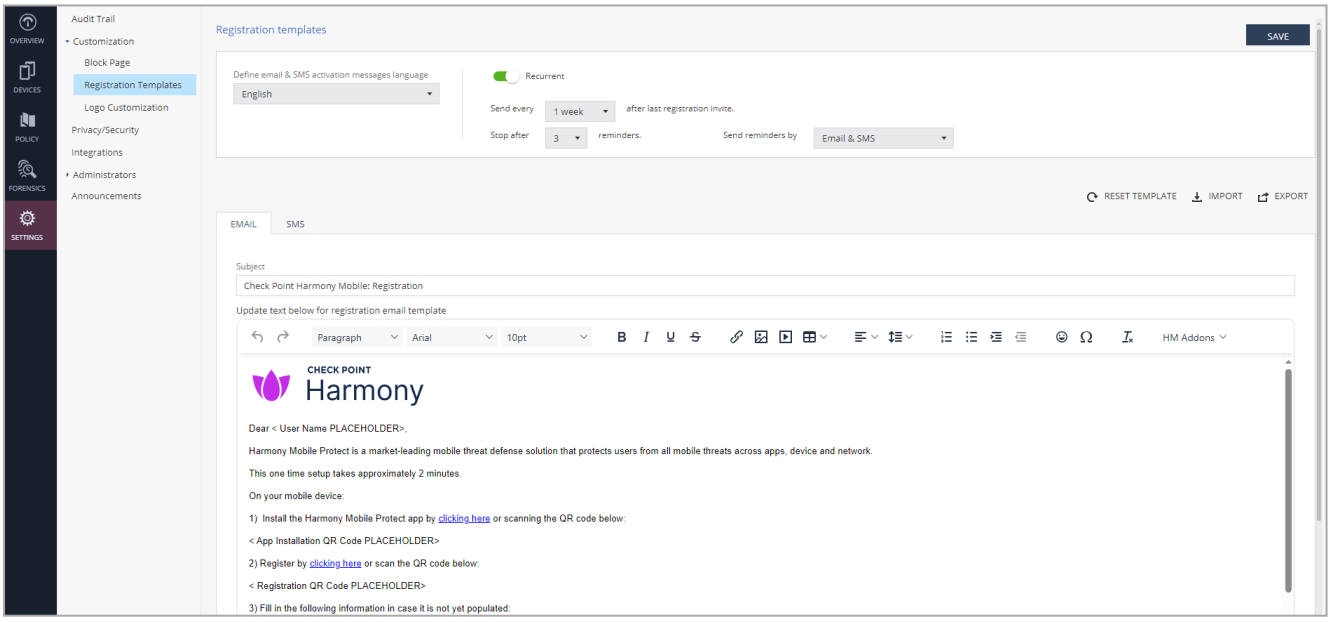
After the Harmony Mobile Protect app is installed and activated on the device, the user receives a notification from the Harmony Mobile Protect.



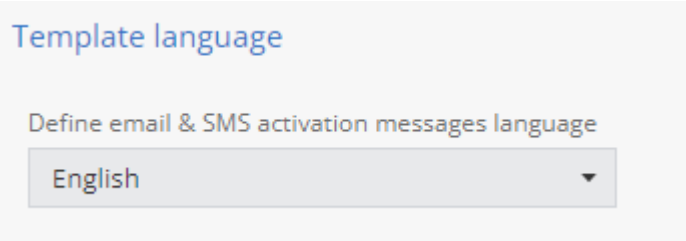
Registration Templates

Registration Templates allows you to customize the content of the registration email and SMS sent from the Check Point Portal to users when they register their mobile device to Mobile Security. This lets organizations to use their unique corporate message for device registration.

To configure the registration message templates, go to **Settings** > **Customization** > **Registration Templates**.

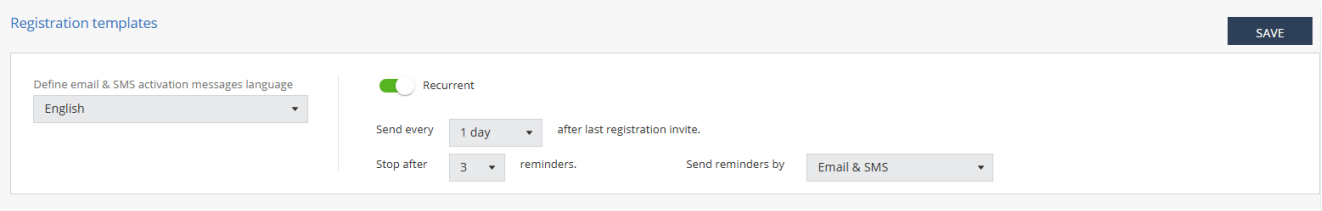


To change the default language of your email or SMS (English or Japanese), select the language from the list.



Sending Reminders for Device Registration

If users do not complete the Mobile Security registration on their devices, you can remind them by resending the registration invitation at specific intervals.



To send registration reminders to users:

1. In the **Registration templates** section, turn on the **Recurrent** toggle button.
2. From the **Send every** list, select the frequency to send the registration invitation.
3. From the **Stop after** list, select the number of times the invitation should be sent (maximum of 10).
4. From the **Send reminders by** list, select the method to send the registration invitation.
    - Email & SMS
    - Email
    - SMS
5. Click **Save**.

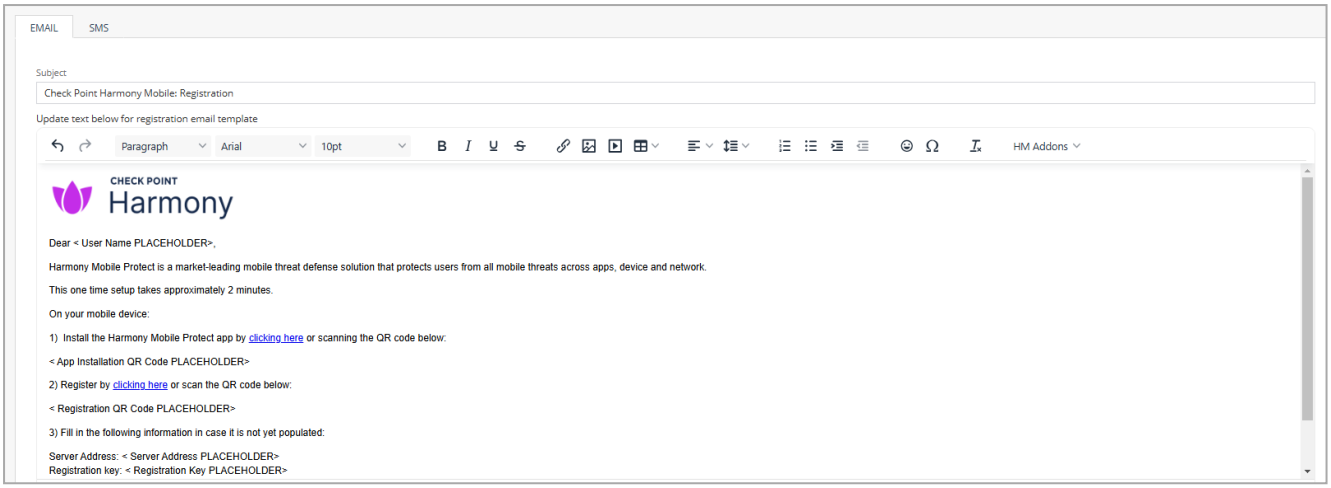
Configuring Email and SMS Templates

In the **EMAIL** and **SMS** tabs, you can view the default email and SMS templates. To customize the content, make the necessary changes and click **Save**.

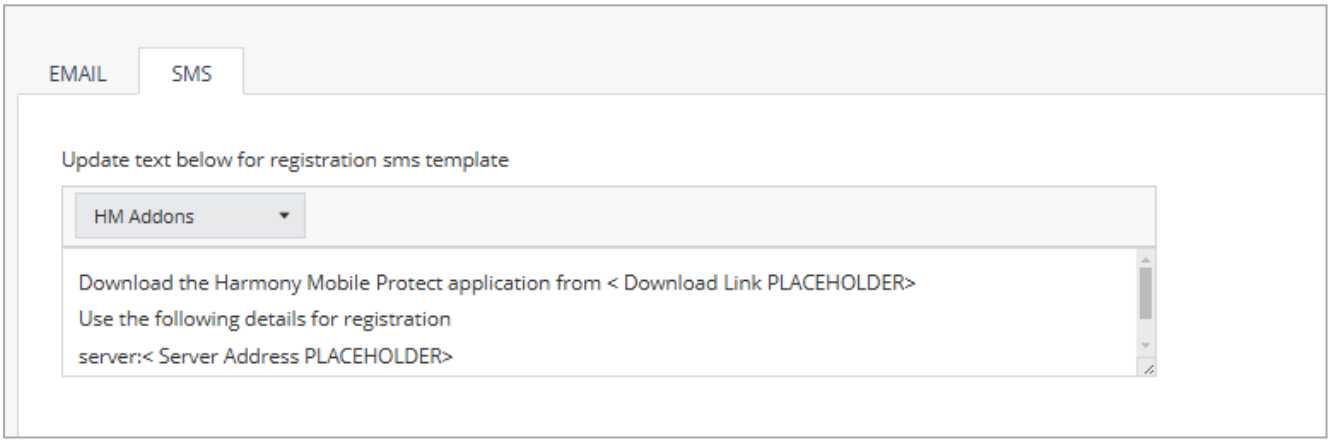
To reset to the default template, click **Reset Template**.

You can also export and import the registration templates.

Email template example:

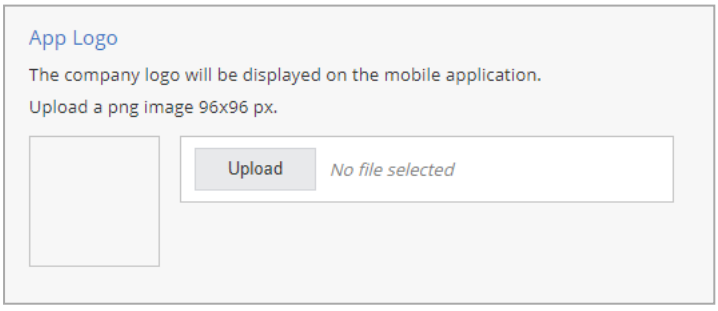


SMS template example:



Logo Customization

Go to **Settings** > **Customization** > **Logo Customization** to change the logo that appears in the upper left-hand corner of the Mobile SecurityHarmony Mobile Protect on user devices.



Privacy/Security

Central HTTPS Inspection Root CA

You can generate a centralized root CA certificate for HTTPS inspection to use across all policies in your account. Once generated, you can upload the certificate to your UEM for deployment to end-user devices.

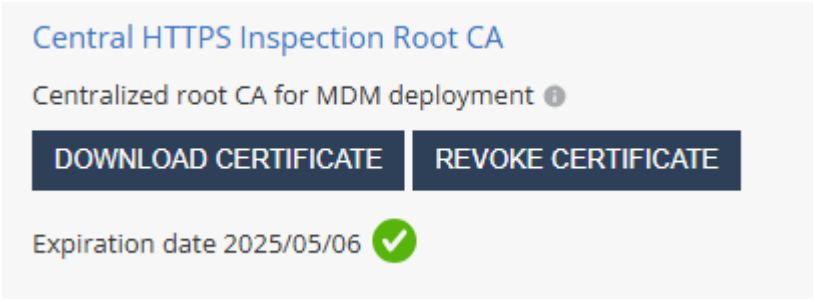
Prerequisite

To generate the centralized CA certificate, you must have one of these roles:

- **Admin** role in **Global Role**
- **Admin** or **Super User** role in **Specific Service Roles**

To generate a centralized root CA certificate:

1. Go to **Settings** > **Privacy/Security**.
2. In the **Central HTTPS Inspection Root CA** section, click **Generate Certificate**.



3. Do one of these:

- To generate a CA certificate issued by Check Point, click **Generate CA Certificate**.

  The system generates a certificate valid for one year from the generation date, as shown in **Expiration date**.

  Note - Check Point recommends you renew the CA certificate at least two weeks before the expiration date. To renew the CA certificate, see sk181288.

- To use a self-signed or a third-party CA certificate, click **Upload CA Certificate**.

  a. In the pop-up window, upload the certificate.

  Note -
  For the Transport Layer Security (TLS) certificate to be valid:
  - The certificate must have a lifecycle of at least 30 days and not longer than 390 days.
  - The certificate must be valid for more than 30 days from the time it is uploaded to the Mobile Security Administrator Portal.

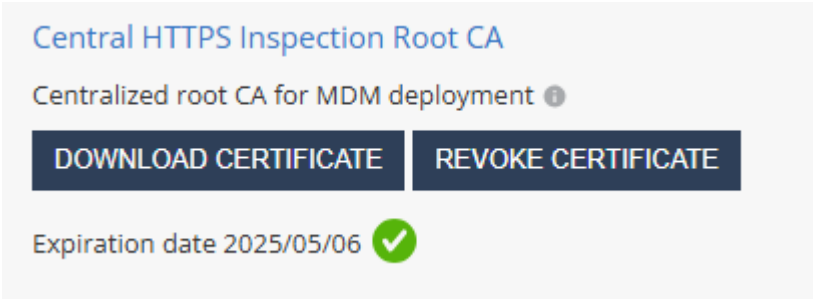
  b. Enter the certificate password.

  c. Click **Verify**.

  d. If there are no errors, click **Add**.

4. If you have generated a CA certificate by Check Point, click **Download Certificate**.

   The system downloads the certificate to your computer.



5. Upload the new certificate to the UEM.

   For more information, see **CA Certificate Deployment Using the UEM** section for the relevant UEM in *Mobile Security Integration Guide*.

6. To revoke the certificate, click **Revoke Certificate**.

   Important - Revoking the centralized certificate will remove it from all policies that use it.

To apply the centralized CA certificate to multiple policies in your tenant, go to *"HTTPS Settings" on page 69* in **Network Protection** settings.

Privacy/Security

BYOD Privacy Mode

When you enable BYOD Privacy Mode, administrators can only see that a malicious threat exists, but they cannot see the user affected by it. This ensures the highest user privacy when needed.

Example: Events & Alerts Tab

BYOD Privacy Mode Disabled:

When BYOD Privacy Mode is disabled, the Events & Alerts tab shows the Device Owner and Device Number fields as configured in the Devices tab.

Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID	User Email
Jun 03 2021, 12:08:27	Critical	Network Security	Application Download	Blocked	File name: AppTest.plist, File...		6779	
Jun 03 2021, 12:08:27	Critical	Network Security	Application Download	Blocked	File name: mobile_conf_ios.p...		6779	
Jun 03 2021, 11:18:50	Critical	Network Security	Configuration Profile	Blocked	File name: ibattle.mobilecon...		6779	
Jun 03 2021, 11:18:50	Critical	Network Security	Application Download	Blocked	File name: AppTest.plist, File...		6779	
Jun 03 2021, 11:18:49	Critical	Network Security	Application Download	Blocked	File name: AppTest.plist, File...		6779	

BYOD Privacy Mode Enabled:

When BYOD Privacy Mode is enabled, the Events & Alerts tab does not show the Device Owner and Device ID Number field.

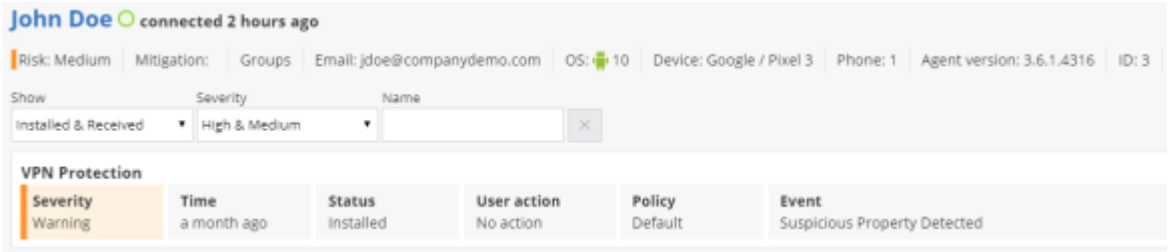
Example:

Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS
Jun 03 2021, 12:08:27	Critical	Network Security	Application Download	Blocked	File name: AppTest.plist, File type: plist,...	
Jun 03 2021, 12:08:27	Critical	Network Security	Application Download	Blocked	File name: mobile_conf_ios.plist, File ty...	
Jun 03 2021, 11:18:50	Critical	Network Security	Configuration Profile	Blocked	File name: ibattle.mobileconfig, File typ...	
Jun 03 2021, 11:18:50	Critical	Network Security	Application Download	Blocked	File name: AppTest.plist, File type: plist,...	

Example: Device Risk Tab

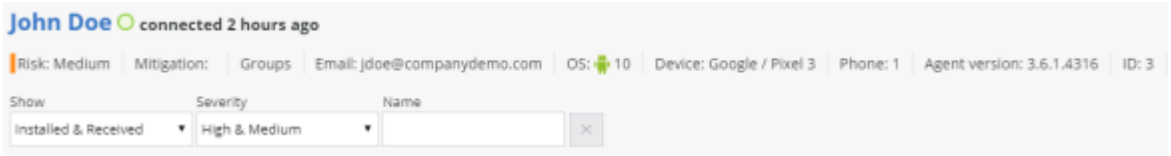
BYOD Privacy Mode Disabled:

When BYOD Privacy Mode is disabled, the Device Details show the app(s) that put this device at high risk.



BYOD Privacy Mode Enabled:

When BYOD Privacy Mode is enabled, the Device Details does not show the app(s) that put this device at high risk. The administrator will only see that the device is at risk, and its risk level, but not the reason.



Example: App Risk Tab

BYOD Privacy Mode Disabled:

When BYOD Privacy Mode is disabled, the drill-down into the App Analysis information about the App at Risk displays the app Owner Details.

BYOD Privacy Mode Enabled:

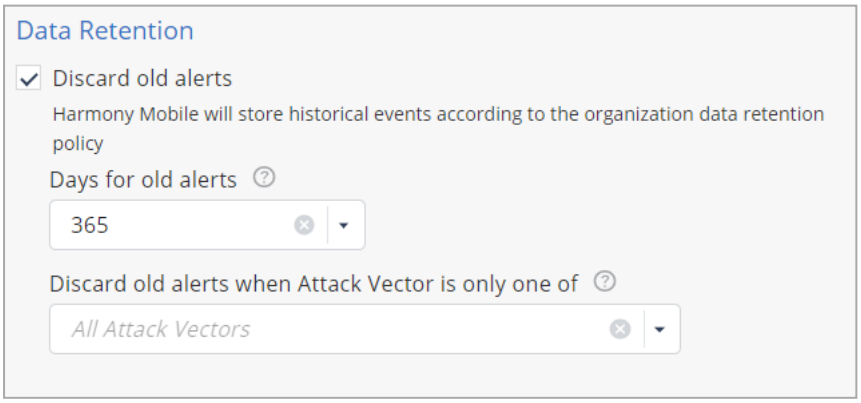
When BYOD Privacy Mode is enabled, the drill-down into the App Analysis information about the App at Risk does not display the app Owner Details.

Enable PII Decryption

Select this checkbox to enable the decryption of Personal Identifiable Information (PII) when you integrate with a Check PointMobile SecurityConnector installed on-premises. For more information on Mobile Security Connector installation, see Harmony Mobile Connector Installation Guide.

Data Retention

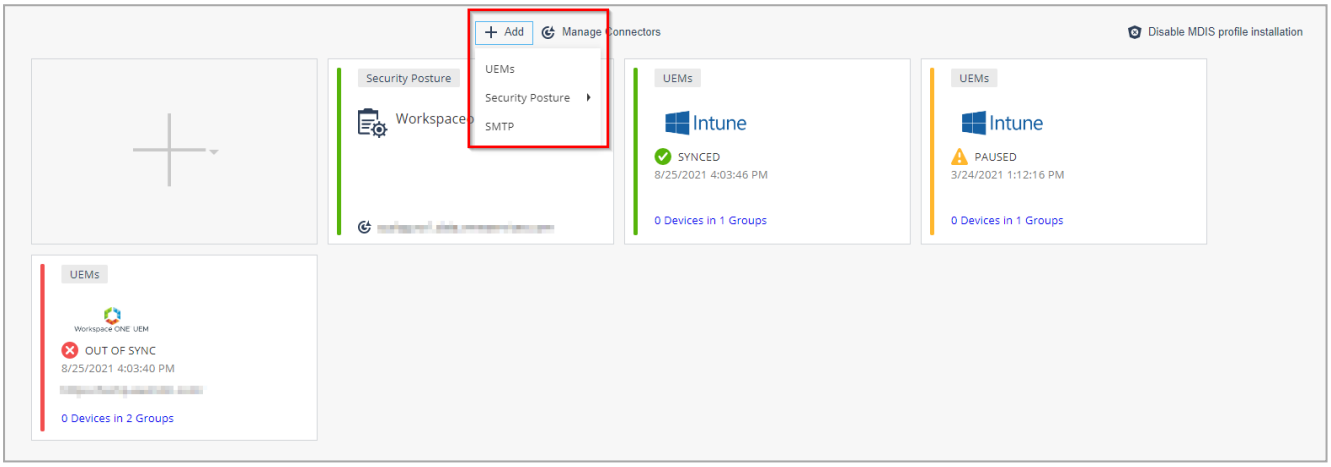
In this section, you can set the time period to discard old alerts. You can also configure it by attack vector.



Integrations

In the **Integrations** tab, you can manage your UEM integrations, other security posture systems such as Microsoft Defender ATP or Syslog, and SMTP servers. Mobile Security supports multiple integrations simultaneously. You can integrate Mobile Security to several UEMs in parallel, and to external security posture system such as Microsoft Defender ATP.

Click the **+Add** icon and choose to integrate Mobile Security with UEMs, with a Security Posture system, or with a SMTP server.



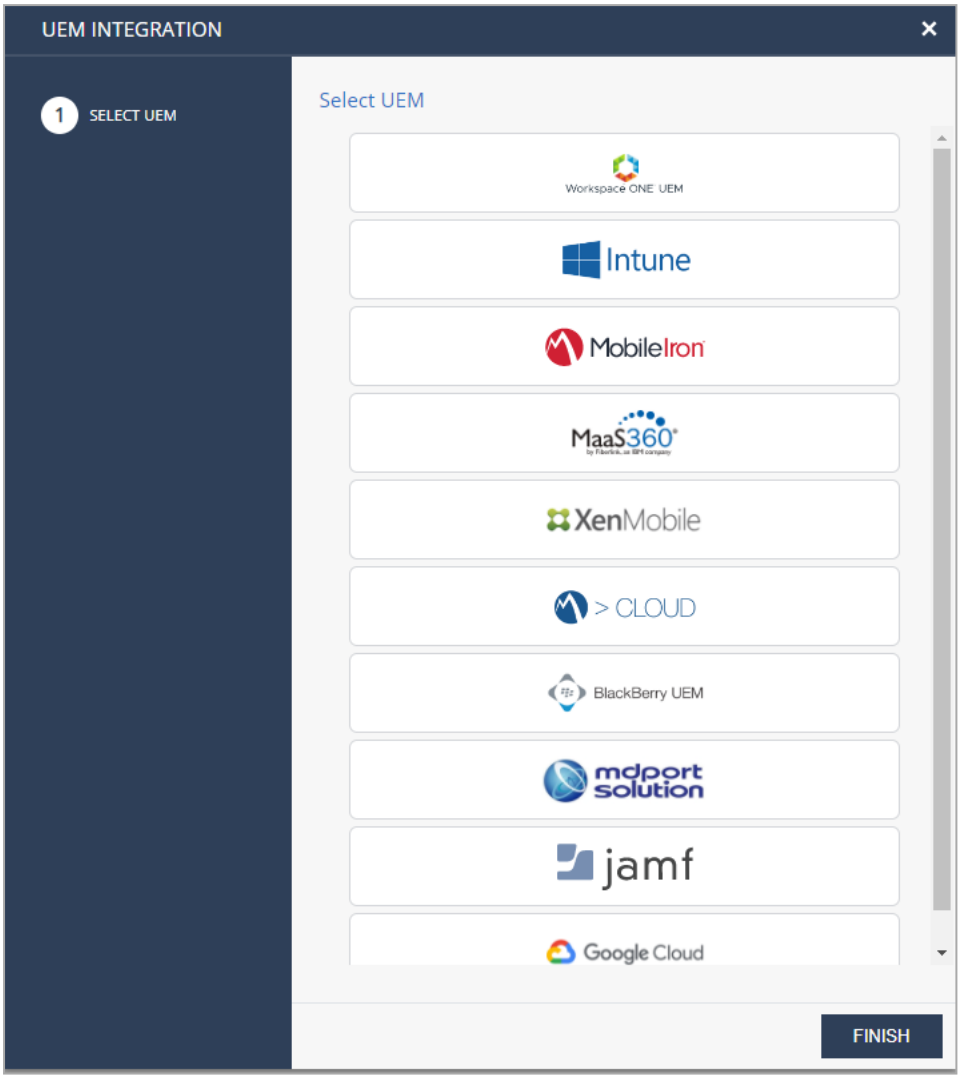
UEM Integration

Note - For more information on the integration procedure for different UEMs, see Harmony Mobile UEM Integration Guide.

Select the **UEMs** option to integrate Mobile Security to any of the below supported UEMs or partner supported UEMs.

- Workspace ONE (Formerly AirWatch UEM)
- Microsoft Intune
- MobileIron Core
- IBM MaaS360
- Citrix Endpoint Management (Formerly XenMobile)
- MobileIron Cloud
- BlackBerry UEM On-Premises
- Jamf Pro
- Google Cloud
- Samsung Knox Manage / Samsung SDS EMM

- SOTI MobiControl
- Applivery



Integration with Partner Supported UEMs

Partner supported UEMs are the UEMs that support integration with Mobile Security and tested by the partner.

The partner supported UEMs are:

- mdport solution
- SevenPrinciples (7P)
- Essentials MDM (Techstep/FAMOC)
- Hexnode
- ManageEngine

- Scalefusion
- Codeproof

For more information, see Integration with Partner Supported UEMs.

UEM Managed and Unmanaged Devices Management

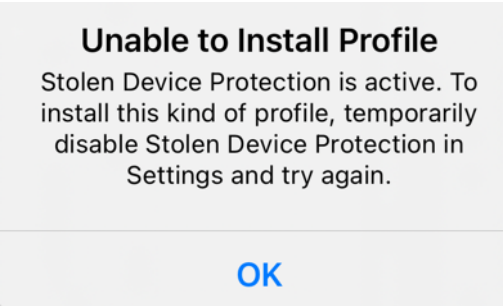
Mobile Security supports managing UEM managed devices and unmanaged devices on the same dashboard. You can synchronize users and devices with an UEM and simultaneously manage the manually registered users and devices on the same Mobile Security dashboard.

- Different device groups must be created for the 'Non-UEM managed Devices' and for the 'UEM Managed' devices.
- Manually registered devices must be labeled as 'Non-UEM managed Devices'. The UEM managed devices are synchronized to their relevant groups.

Mobile Device Integration Service (MDIS) Profile

Mobile Security's MDIS profile communicates with iOS devices that are not managed by a third-party UEM to retrieve the list of apps installed, certificates, profiles and so on. It is installed on the device with the Mobile SecurityHarmony Mobile Protect.

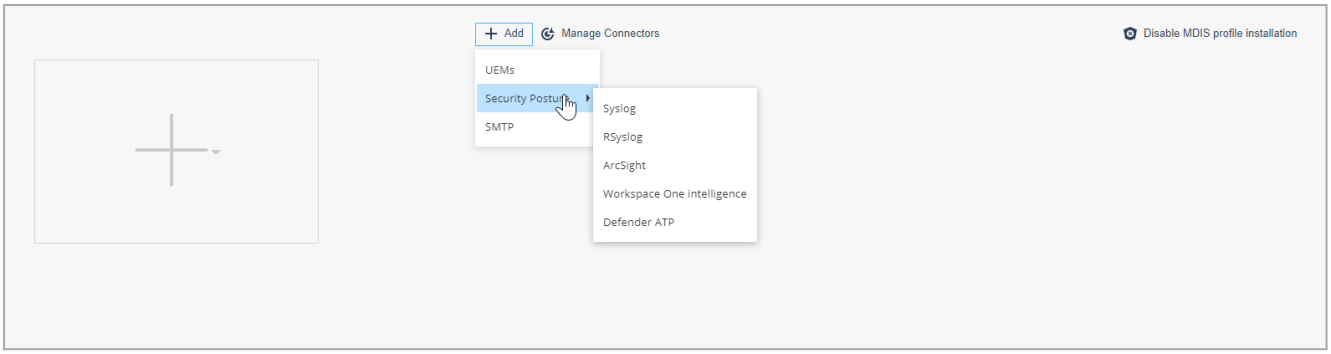
Note - For iOS 17.3 and higher, make sure to turn off **Stolen Device Protection** on the device before you install the Mobile SecurityHarmony Mobile Protect. You can turn it on after you install the app. Otherwise, **Unable to Install Profile** error appears.



Security Posture Integration

The **Security Posture** option allows you to integrate Mobile Security to an external security posture and management system.

Note - The Workspace One Intelligence Hub integration requires configuring both Syslog to Intelligence Hub and Workspace One UEM.



Syslog Integration

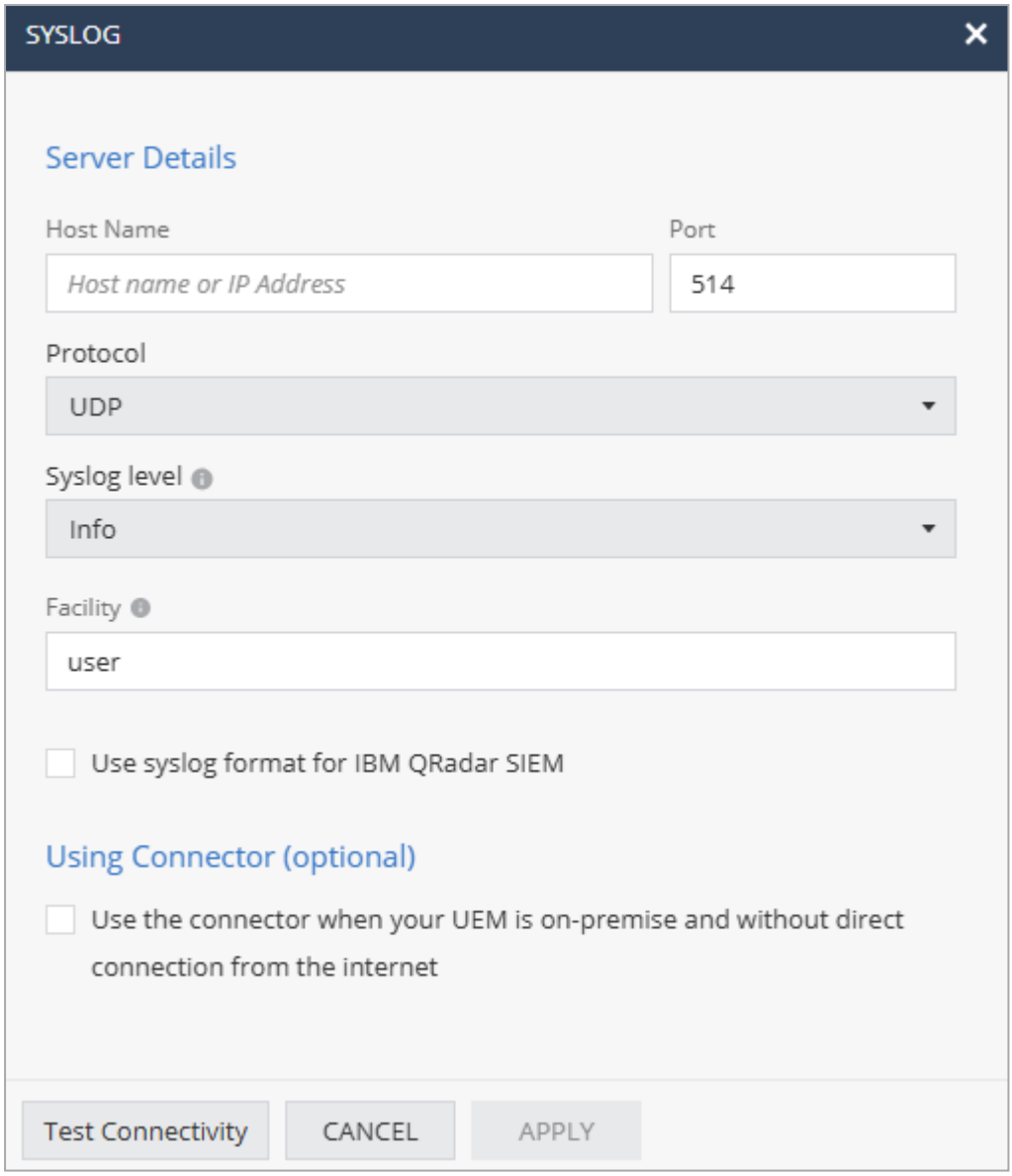
The administrator can set the dashboard to send Syslog events to a Syslog server. The Mobile Security dashboard must communicate to your Syslog server through your firewall.

To view the source IP addresses, see *"Appendix A - Mobile Security Communication Information" on page 198*.

To configure Syslog:

1. Go to **Settings** > **Integrations** and click **+Add**.
2. Click **Security Posture** > **Syslog**.

   The **Syslog** window appears.



3. Enter these:

Setting	Description
Host Name	Host name or IP Address of Syslog server
Protocol	UDP or TCP
Port	Port that the Syslog server is listening on.

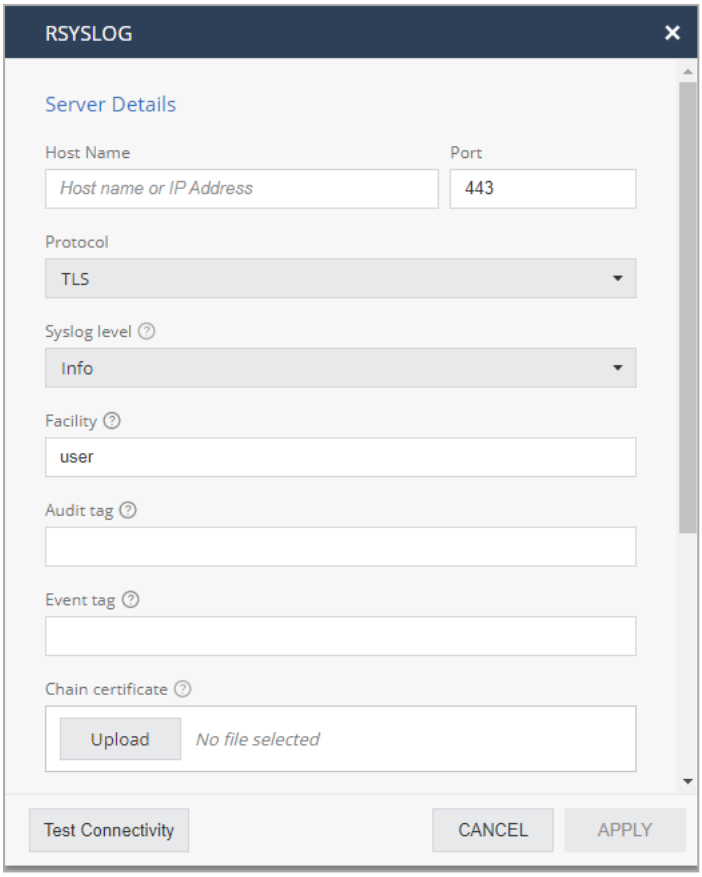
Setting	Description
Syslog level	Severity level of events to be sent to the server. Events with the selected severity level or higher will be sent. Supported values: ■ Info ■ Warn ■ Error ■ Debug
Facility	Type of program generating the log message. Messages from different facilities may be processed differently. Default value is **user**.

4. If you are using IBM QRadar SIEM, select the **Use syslog format for IBM QRadar SIEM** checkbox to format log messages according to QRadar's syslog requirements.
5. Click **Apply**.

For more information on the structure of the Syslog event sent by Mobile Security, see *"Appendix B - Mobile Security Syslogs" on page 218*.

Rsyslog Integration

Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds features such as using TCP for transport and SSL\TLS for encryption.


RSYSLOG
Server Details
Host Name
Host name or IP Address
Port
443
Protocol
TLS
Syslog level
Info
Facility
user
Audit tag
Event tag
Chain certificate
Upload
No file selected
Test Connectivity
CANCEL
APPLY

To configure Rsyslog:

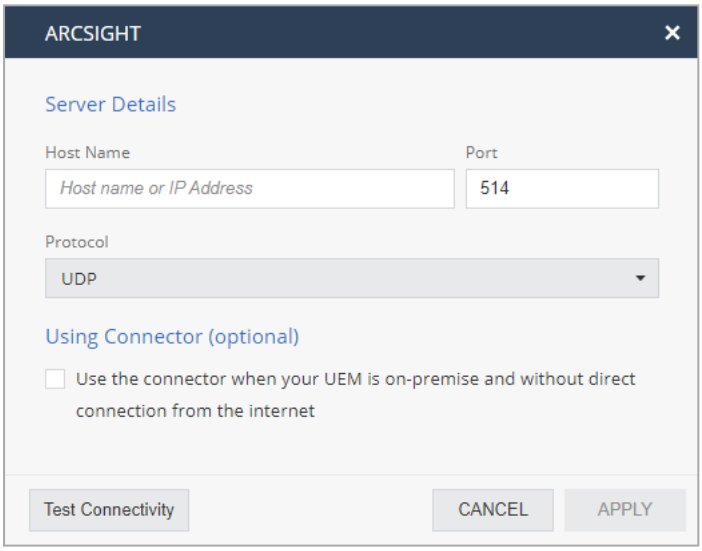
1. In the pop-up window, enter these values:

Setting	Description
Host Name	Host name or IP Address of rsyslog server
Protocol	TLS
Port	Port that the rsyslog server is listening on. Default SSL port: 443.
Syslog level	Severity level of events to send to the server. Acceptable Values are: ■ Info ■ Warn ■ Error ■ Debug
Facility	Facility is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently. Defaults to "user".
Audit TAG	Because Mobile Security can send 2 formats of logs, Event logs and Audit logs, the receiving rsyslog system publishes 2 parsers for these types. When Mobile Security sends an Event type it will add the Event Tag to the message. When Mobile Security sends an Audit type it will add the Audit Tag to the message.
Event TAG	Because Mobile Security can send 2 formats of logs, Event logs and Audit logs, the receiving rsyslog system publishes 2 parsers for these types. When Mobile Security sends an Event type it will add the Event Tag to the message. When Mobile Security sends an Audit type it will add the Audit Tag to the message.
Chain certificate	The rsyslog server needs to publish unique certificates to establish the secure connection from Mobile Security. The chain certificate is the X.509 certificate used to secure the rsyslog server. The root CA of the rsyslog system to which we are going to send logs.

Setting	Description
Certificate	The rsyslog server needs to publish unique certificates to establish the secure connection from Mobile Security. This is the certificate used for the TLS handshake. It is obtained from the rsyslog system that was generated specifically for the integration with Mobile Security.
Key certificate	The rsyslog server needs to publish unique certificates to establish the secure connection from Mobile Security. This the Private Key certificate used for the TLS handshake. It is obtained from the rsyslog system that was generated specifically for the integration with Mobile Security.

2. Click **Apply**.

ArcSight Integration



To configure ArcSight:

1. In the pop-up window, enter these values:

Setting	Description
Host Name	Host name or IP Address of ArcSight server
Protocol	UDP or TCP
Port	Port that the ArcSight server is listening on.

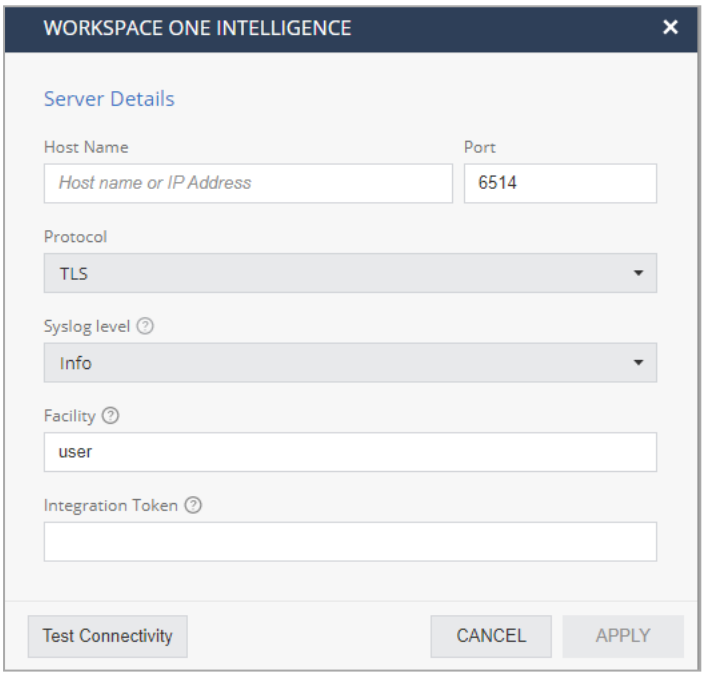
2. Click **Apply**.

For more information on the structure of the ArcSight event sent by Mobile Security, see *"Appendix C - Mobile Security ArcSight" on page 224*.

WorkSpace One Intelligence Integration

Mobile Security supports integration with VMWARE Workspace ONE Intelligence. When connected to Workspace ONE Intelligence, the Mobile Security sends the security event logs (syslog) messages. It allows security/SOC administrators to use other services that run over the Workspace ONE Intelligence. These additional services can use the advanced security indicators from the Mobile Security that come from the organization's mobile devices and create additional reports and insights.

For more information on Workspace ONE Intelligence refer to VMWARE Workspace ONE Intelligence WEB site.

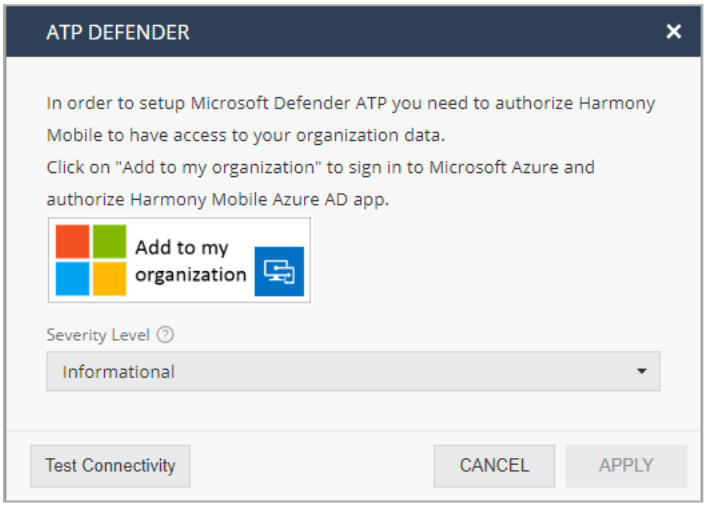


- Before starting to integrate Workspace ONE Intelligence, Mobile Security must be first integrated with Workspace ONE UEM.
- For more information on Mobile Security integration with Workspace ONE Intelligence, see Integration with Workspace ONE UEM.
- On the Mobile Security Dashboard, go to 'Settings/Syslog Settings' and select the 'Workspace ONE Intelligence' option.
- Mobile Security sends Syslog messages to the Workspace ONE Intelligence service. You must configure the Workspace ONE Intelligence service details and verify the two systems are connected

- When the connection is established, you can view the Mobile Security threats insights on the Workspace ONE Intelligence dashboards and use the powerful Intelligence platform to automate the threats handling. For example, you can create a response to a new detected malware by sending a Slack message to the group of security analysts, or use a callback to any remote service that offers a web hook API.

Microsoft Defender ATP Integration

Choosing to integrate with Microsoft Defender ATP, you will need to decide the minimum events severity to be sent to Microsoft Defender ATP and to log-in to your organization's account of Microsoft Defender ATP. Once connected – Mobile Security sends all events to Microsoft Defender ATP, both security events and device activation events.



To learn more about integration with each of the 3rd party systems – please read the relevant integration guide.

To adjust the default settings implemented for their UEM, see the integration guides dedicated for each UEM.

SMTP Integration

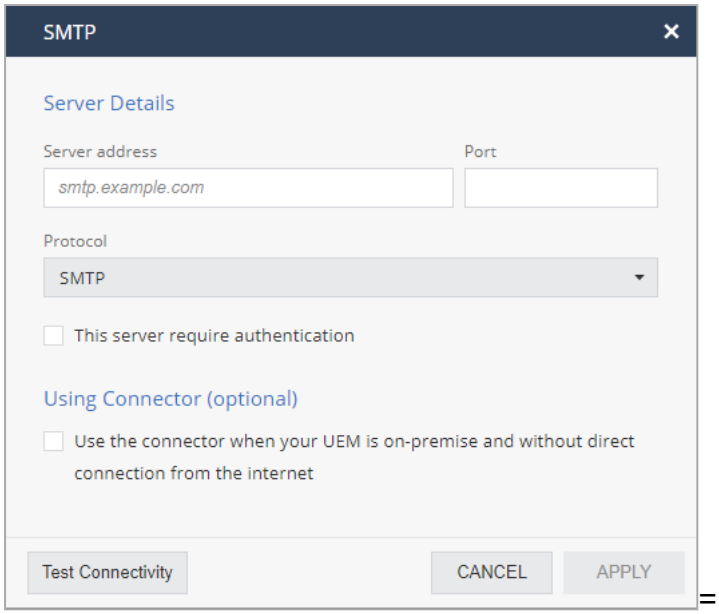
Go to **Settings** > **Integrations** > **+** > **SMTP** to configure the dashboard to send emails from the customer's local domain instead of using the Mobile Security email server.

There are two transport settings: SMTP and SMTPS.

To configure SMTP Settings:

1. Click **Add**.

   The SMTP Settings pop-up window appears.

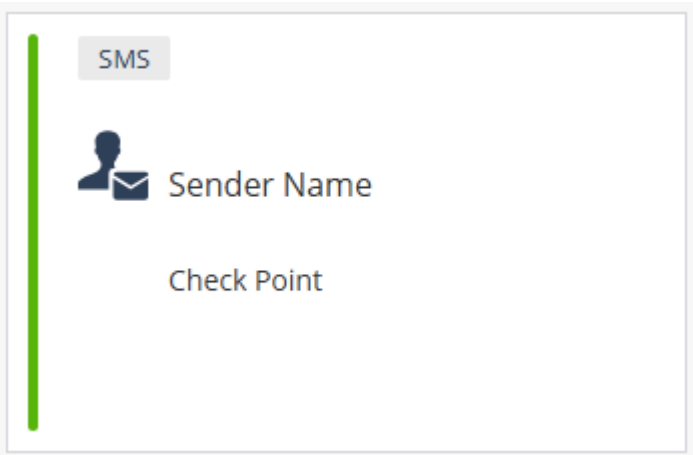


2. Select **SMTP** or **SMTPS**.
3. Enter the required information and click Save.

Note - You must configure the Firewall settings on the Enterprise's firewall to allow SMTP or SMTPS from Mobile Security to the enterprise's SMTP server. The allowed IP addresses are listed in Mobile Security Communication Information.

SMS Sender Name

You cannot configure the SMS sender name. If you previously configured a sender name, the SMS card may still appear in your dashboard; however, it can no longer be edited. To reset it to a default value based on your local regulation, contact *Check Point Support*.



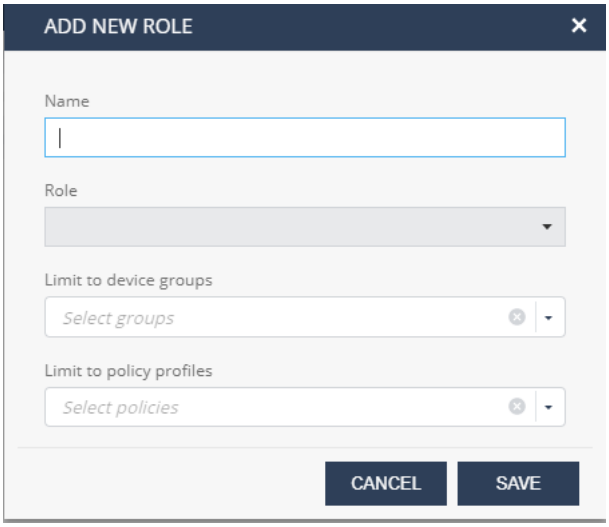
Administrators

Security Group Roles

Security Group Roles allows you to add, remove, or edit Administrator roles.

To create security group roles restricted to specific groups and policy profiles, click **+New** and select:

- Role Name
- Role between Group Security Manager and Group Security Manager Viewer
- Select the device groups the admin can access
- Select the policy profiles the admin can access



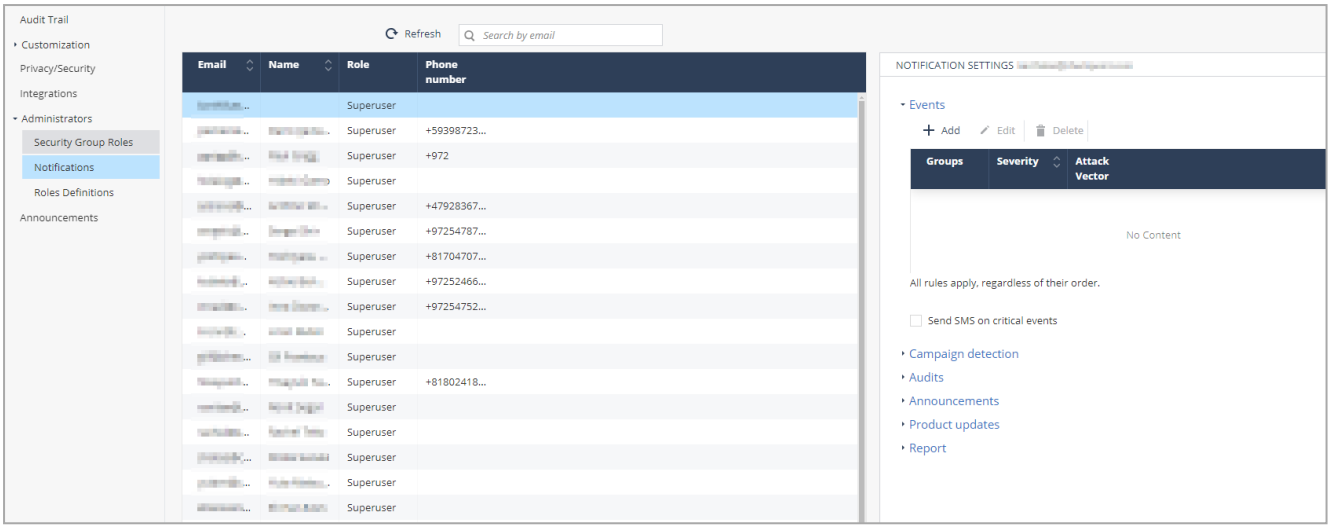
This new role will be available under Specific Mobile Security roles when creating a new Admin User in the Check Point Portal (under Global Settings).

Other admin roles are available such as Basic Support or Device Administrator. For more information about these roles, go to **Settings** > **Administrators** > **Roles Definitions**.

Notifications

In the **Notifications** tab, you can configure, how the administrator want to be alerted in case of security or audit events, dashboard announcements, product updates, scheduled mobile security reports and so on.

You can send Mobile Security notifications to a Microsoft Teams channel. For more information, see sk183491.



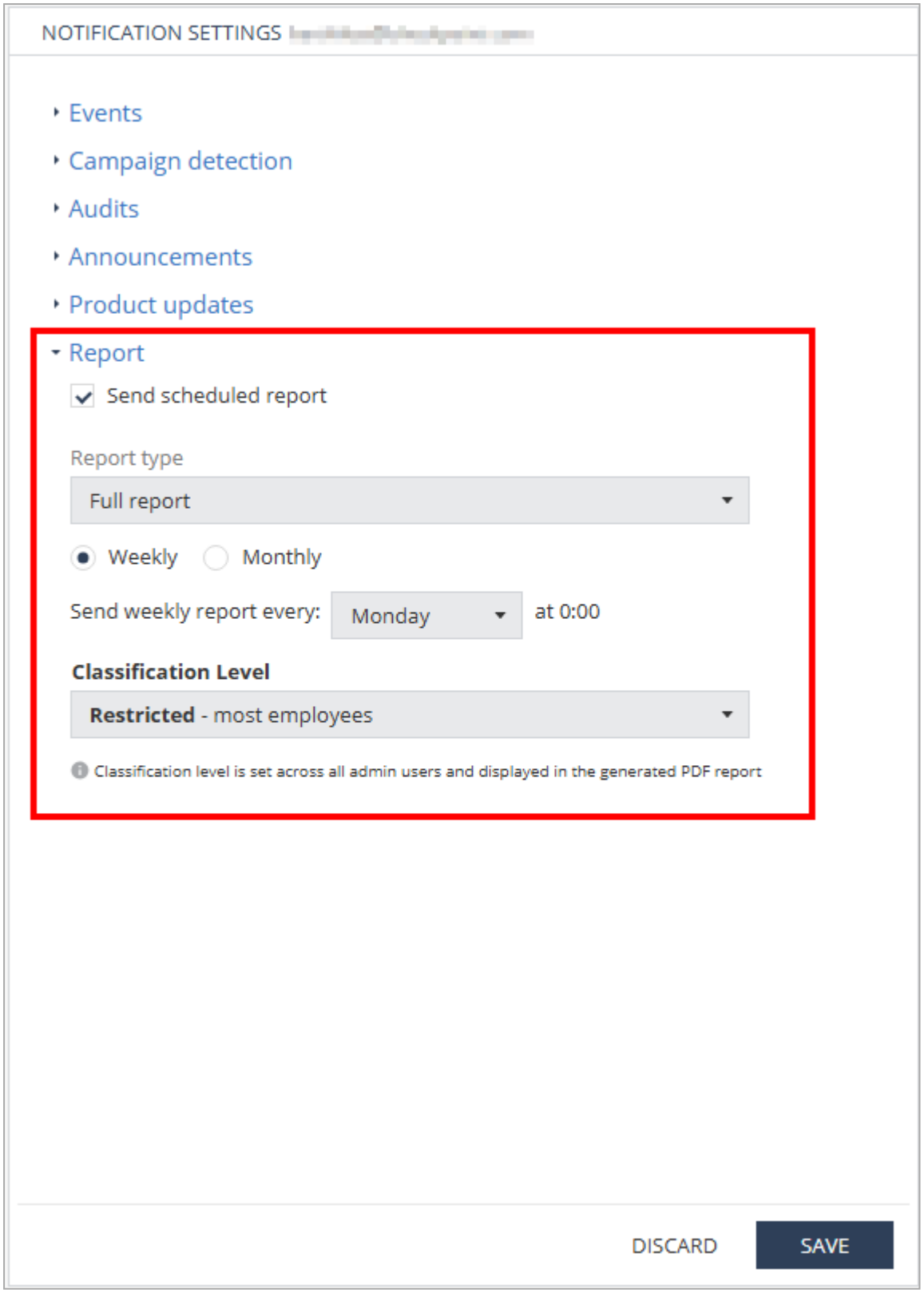
Scheduling Mobile Security Report

Note - You can also generate and download the Mobile Security report in PDF format whenever needed. To do that, go to **Forensics** > **Events & Alerts** and click **PDF Report** above the **Events & Alerts** table. For more information, see Generating Mobile Security Report.

To schedule a Mobile Security Report:

1. Go to **Settings** > **Administrators**.
2. Click **Notifications**.

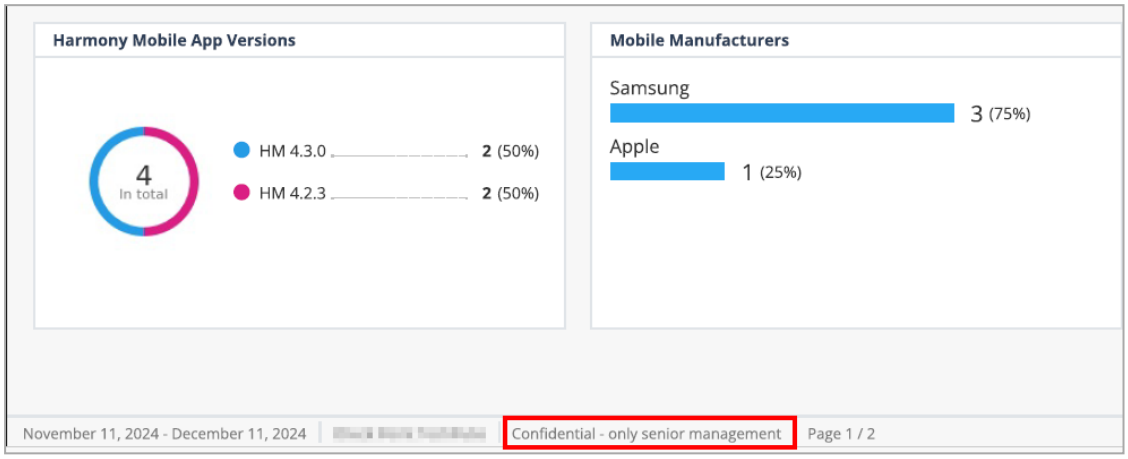
   The **Notification Settings** pane appears.
3. Expand **Report**.
4. Select the **Send scheduled report** checkbox.



5. From the **Report type** list, select one of these:
   - **Full report**
   - **Operational report**

6. Select the weekly or monthly option and set the day or date to generate the report.
7. From the **Classification Level** list, select the audience with whom you can share the report.

   Note - The **Classification Level** does not impact the content of the generated report. It is for informational purpose only and is displayed in the PDF report.



8. Click **Save**.

   The system generates the report at 00:00 UTC on the scheduled day and sends it through email to the administrator who set up the schedule.

Usage Report

Usage reports give Managed Security Service Providers (MSSPs) full visibility into the number of devices and license status across their child tenants. This helps them:

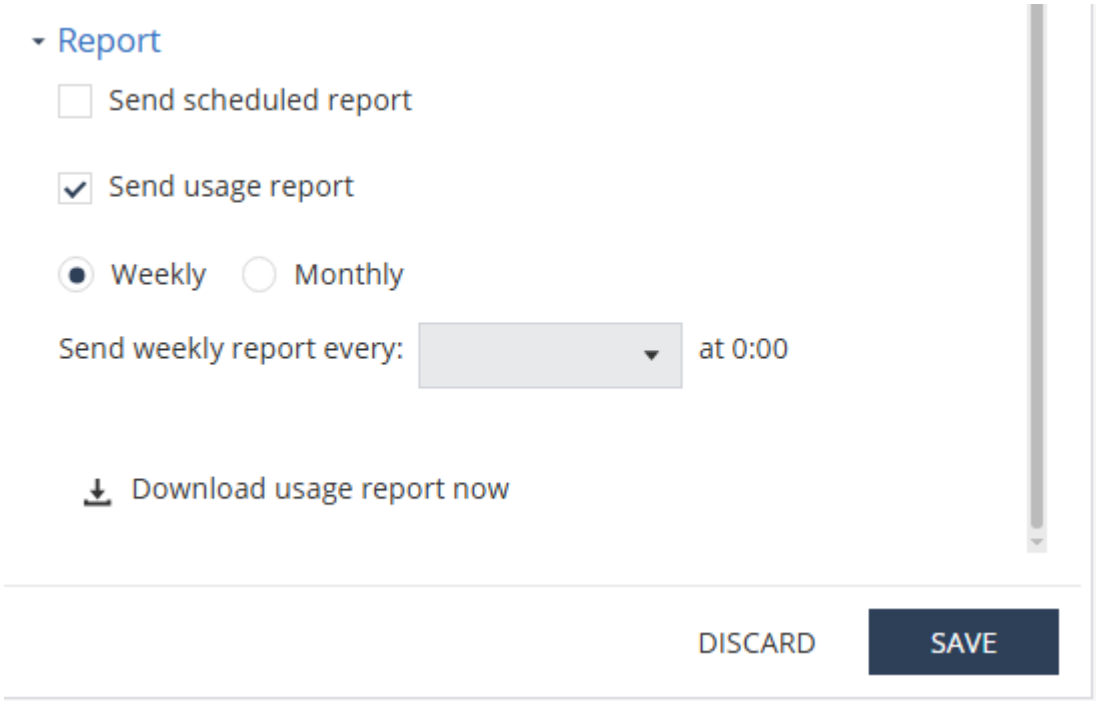
- Accurately bill customers based on active, inactive, or provisioned devices.
- Align their license usage (based on active and provisioned devices) to avoid unnecessary costs.

Admins can generate and download this report in CSV format whenever needed, or set up a schedule to automatically generate and receive it on a weekly or monthly basis.

To schedule or generate a Usage Report:

1. Go to **Settings** > **Administrators**.
2. Click **Notifications**.

   The **Notification Settings** pane appears.
3. Expand **Report**.
4. Select the **Send usage report** checkbox.



5. To schedule the report, select the weekly or monthly option and set the day or date to generate the report.

   The system generates the report at 00:00 UTC on the scheduled day and sends it through email to the administrator who set up the schedule.

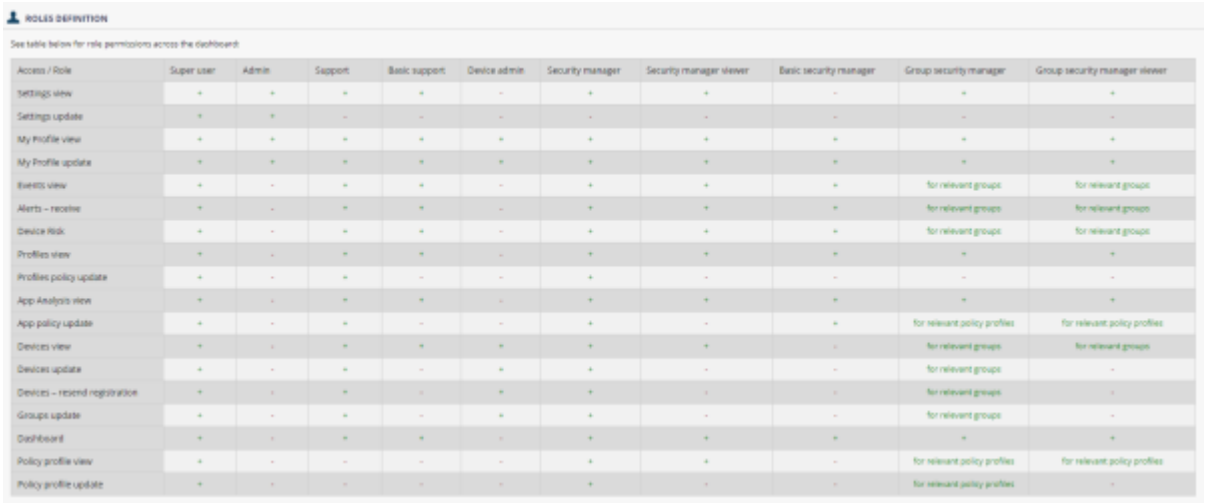
6. To generate and download the usage report instantly, click **Download usage report now**.

   The system generates and downloads the report in CSV format.

7. Click **Save**.

Roles Definitions

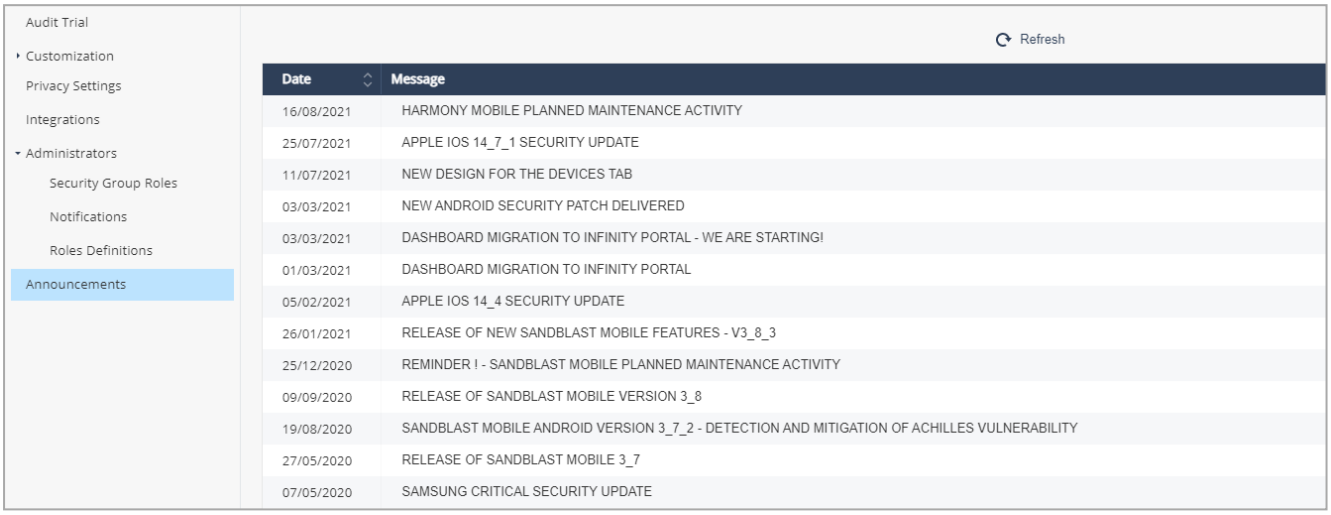
The **Roles Definitions** tab shows the different roles and their permissions in the Mobile Security Administrator Portal.



Announcements

The **Announcements** tab displays all system messages sent from Check Point.

To view, go to **Settings** > **Announcements**.



Infinity AI Copilot

Supported Capabilities for Mobile Security

AI Copilot can address questions for which the answer is available in Check Point Mobile Security documentation (Product guides, SK articles, CheckMates articles).

AI Copilot can also audit policies to improve the global mobile fleet security posture and analyze security events reported in Mobile Security as Early Availability (EA), available on demand. For more information, contact *Check Point Support*.

Appendix A - Mobile Security Communication Information

This appendix describes the networking rules required to configure your security systems in order to allow the solution's integration with your on-premises systems (UEMs, syslog, and so on).

If you do not know your dashboard's region, contact *Check Point Support*.

To prevent spam filters from blocking Harmony Mobile's emails, allow this IP address as a sender: 167.89.59.134.

For more information on how to integrate the Harmony Mobile Protect app with different UEMs, see Harmony Mobile UEM Integration Guide.

Best Practice - The best practice when enabling firewall access for Mobile Security is to use DNS based names. When it is not an option, use the IP addresses provided for the specified DNS in the table below.

Security System Configuration Rules

Regions:

- APAC

Region	Description	Source	Destination	Destination Port
APAC	Connection to customer's ArcSight/Syslog server	• 54.79.100.215 • 13.238.250.74 • 13.236.78.154 • 13.54.82.229 • 54.79.2.81 • 13.55.226.84 • 65.1.191.54	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
APAC	Connection to customer's UEM	• 54.79.100.215 • 13.238.250.74 • 13.236.78.154 • 13.54.82.229 • 54.79.2.81 • 13.55.226.84 • 65.1.191.54	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)
APAC	Mobile Security Connector to Mobile Security	Customer Mobile Security Connector server	Mobile Security Dashboard FQDN*	443

Region	Description	Source	Destination	Destination Port
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	au-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	ap.portal.checkpoint.com portal.checkpoint.com	443
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)

Region	Description	Source	Destination	Destination Port
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- CA

Region	Description	Source	Destination	Destination Port
CA	Connection to customer's ArcSight/Syslog server	• 35.182.193.41 • 35.182.219.40 • 99.79.19.121	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
CA	Connection to customer's UEM	• 35.182.193.41 • 35.182.219.40 • 99.79.19.121	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

Region	Description	Source	Destination	Destination Port
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	ca-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	ca.portal.checkpoint.com portal.checkpoint.com	443
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)

Region	Description	Source	Destination	Destination Port
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- EU

Region	Description	Source	Destination	Destination Port
EU	Connection to customer's ArcSight/Syslog server	• 52.49.95.252 • 34.251.122.117 • 52.30.229.13 • 52.31.98.20 • 18.200.64.57 • 108.129.52.172	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
EU	Connection to customer's UEM	• 52.49.95.252 • 34.251.122.117 • 52.30.229.13 • 52.31.98.20 • 18.200.64.57 • 108.129.52.172	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

Region	Description	Source	Destination	Destination Port
EU	Mobile Security Connector to Mobile Security	Customer Mobile Security Connector server	Mobile Security Dashboard FQDN*	443
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	eu-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	portal.checkpoint.com	443
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)

Region	Description	Source	Destination	Destination Port
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- IN

Region	Description	Source	Destination	Destination Port
IN	Connection to customer's ArcSight/Syslog server	• 65.2.156.71 • 65.1.191.54 • 65.0.210.5	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
IN	Connection to customer's UEM	• 65.2.156.71 • 65.1.191.54 • 65.0.210.5	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

Region	Description	Source	Destination	Destination Port
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	in-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	in.portal.checkpoint.com portal.checkpoint.com	443
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)

Region	Description	Source	Destination	Destination Port
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- UAE

Region	Description	Source	Destination	Destination Port
UAE	Connection to customer's ArcSight/Syslog server	• 3.29.188.5 • 3.29.9.81 • 3.29.120.64	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
UAE	Connection to customer's UEM	• 3.29.188.5 • 3.29.9.81 • 3.29.120.64	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

Region	Description	Source	Destination	Destination Port
UAE	Mobile Security Connector connection to Mobile Security	Customer Connector server	Mobile Security Dashboard FQDN*	443
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	uae-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	uae.portal.checkpoint.com portal.checkpoint.com	443

Region	Description	Source	Destination	Destination Port
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings).	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- UK

Region	Description	Source	Destination	Destination Port
UK	Connection to customer's ArcSight/Syslog server	• 18.135.91.41 • 35.178.23.186 • 3.8.43.176	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)
UK	Connection to customer's UEM	• 18.135.91.41 • 35.178.23.186 • 3.8.43.176	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)
UK	Mobile Security Connector connection to Mobile Security	Customer Connector server	Mobile Security Dashboard FQDN*	443
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	uk-gw.locsec.net bosko.locsec.net	443
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	uk.portal.checkpoint.com portal.checkpoint.com	443

Region	Description	Source	Destination	Destination Port
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- US

Region	Description	Source	Destination	Destination Port
US	Connection to customer's ArcSight/Syslog server	• 52.71.46.86 • 3.208.56.54 • 3.209.41.124 • 3.226.181.180 • 3.209.220.26 • 52.203.42.126 • 54.225.176.210 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 18.210.156.139 • 34.228.181.154	Customer ArcSight/Syslog server	Protocol and port as configured in the Dashboard (Settings > Syslog)

Region	Description	Source	Destination	Destination Port
US	Connection to customer's UEM	• 52.71.46.86 • 3.208.56.54 • 3.209.41.124 • 3.226.181.180 • 3.209.220.26 • 52.203.42.126 • 54.225.176.210 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 18.210.156.139 • 34.228.181.154	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)
US	Mobile Security Connector connection to Mobile Security	Customer Connector server	Mobile Security Dashboard FQDN*	443
ANY	Connection from **mobile devices** to Mobile Security from **corporate network**	Customer's internal network	gw.locsec.net bosko.locsec.net	443

Region	Description	Source	Destination	Destination Port
ANY	Tenant Admin to customer's Mobile Security dashboard	Customer's internal network	portal.checkpoint.com us.portal.checkpoint.com	443
ANY	Connection to the customer's SMTP server, if configured in dashboard (**Settings** > **Integrations** > **SMTP** settings)	• 54.225.176.210 • 52.203.42.126 • 3.219.149.71 • 52.202.175.192 • 54.162.65.19 • 3.209.220.26 • 18.210.156.139 • 3.226.181.180 • 3.209.41.124 • 3.208.56.54 • 52.71.46.86 • 34.228.181.154	Customer SMTP server	SMTP port configured in the dashboard (Settings > SMTP)
ANY	Mobile Security Connector to customer UEM	Customer Mobile Security Connector server	Customer UEM	443 BES UEM only: 18084 (default) Citrix XenMobile only: 4443 (default)

* Mobile Security Dashboard FQDN – The Fully Qualified Domain Name of your HM Dashboard, unique per customer (for example, sbm.mt2.locsec.net).

- **For customers using Mobile Security Connector**

Region	Description	Source	Destination	Destination Port
AU	Mobile Security Connector	Customer Mobile Security Connector server	au-relay.locsec.net	443
CA	Mobile Security Connector	Customer Mobile Security Connector server	ca-relay.locsec.net	443
EU	Mobile Security Connector	Customer Mobile Security Connector server	eu-relay.locsec.net	443
UAE	Mobile Security Connector	Customer Mobile Security Connector server	uae-relay.locsec.net	443
UK	Mobile Security Connector	Customer Mobile Security Connector server	uk-relay.locsec.net	443
US	Mobile Security Connector	Customer Mobile Security Connector server	us-relay.locsec.net	443

Notes -

- For more information on Mobile Security Connector installation, see Harmony Mobile Connector Installation Guide.
- For more information on the structure of the ArcSight and Syslog events sent by Mobile Security, see *"Appendix B - Mobile Security Syslogs" on page 218* and *"Appendix C - Mobile Security ArcSight" on page 224*.

Policy Profiles Description

Main features:

Feature	Description
Anti-Phishing (See Anti-Phishing).	■ This category includes URLs that typically arrive in email or messaging apps and are established to steal information from users. ■ These sites falsely represent themselves as legitimate websites to obtain users' account credentials or credit card information that can be used for fraudulent or illegal purposes.
Safe Browsing (See Safe Browsing).	■ This category includes URLs that may be reached during on-device browsing and are established to steal information from users or install drive-by malware. ■ These sites falsely represent themselves as legitimate websites to obtain users' account credentials or credit card information that can be used for fraudulent or illegal purposes. ■ These sites falsely represent themselves as legitimate websites to install malicious apps on the user's device to root/jailbreak the device, take command-and-control of the device, and steal on-device information.
Conditional Access (See Conditional Access).	■ This category is a list of corporate IP addresses and/or FQDN hostnames that the user's device cannot access while at high risk.
Anti-Bot (see Anti-Bot).	■ This category includes URLs, IP addresses, or domain names that use bots (zombies), including command-and-control sites facilitating stealing on-device personal and corporate information, record video or audio, and/or install other malicious code.
URL Filtering (See URL Filtering)	■ This category allows the administrator to prohibit devices from accessing particular URLs in a specific subject category, such as gambling, guns, and violence, etc. ■ This category also allows the administrator to block domain access from the user's device irrespective of the subject category or risk level of the device. ■ In addition, this category also allows the administrator to allow domains that are always accessible to the user's device irrespective of the subject category or risk level of the device.

Feature	Description
Parameter Configuration	■ This category allows users to configure the basic On-device Network Protection behavior (Disabled, Always on, Turn on when device is at risk.) ■ This category also includes a Configure pop-up window that allows to configure different parameters of On-device Network Protection (General settings and suspending policy for On-device Network Protection)

Appendix B - Mobile Security Syslogs

This appendix describes the structure of the Syslog event sent by Mobile Security.

Sample Mobile Security event:

```
May 15 11:24:26 dashboard-eu2-alerts HarmonyMobile: URL: dashboard-
url.locsec.net, Product: Harmony Mobile, AttackVector: Application,
DeviceAlert Event: Application, Product: Harmony Mobile, Threat
Factors: Backup Tool, EventType: Installed, Signature: app_hash\:
781938e38fea1ee520b8ebe2da5d5cdd28bfee5c51bcd8d4a36e4b063a676ddf,
RiskLevel: CRITICAL, DeviceID: 339, Client: Harmony Mobile Protect,
Device Client Version: 4.3.0.9307, DeviceOwner: testUser,
DeviceEmail: email@example.com, DeviceNumber: , DevicePolicy:
Global, DeviceGroups: ALL|hm-integrations-g, DeviceSerialNumber:
None, DeviceType: Android_work, DeviceOSLevel: 14, DeviceModel:
samsung / SM-S911B, DeviceRiskLevel: 1.0, Event ID: 78, Event
Timestamp: 1747297460000, Event Client Timestamp: 1747297457000,
Device Tracking ID:
5292f8dffd6b92f87a24fa32337fefbf200fe65e5c09fb2d48583c4cb89f2f99,
Host Type: Mobile, APP name: Smart Switch, APP package:
com.sec.android.easyMover, APP Threat summary: None, APP SHA256:
781938e38fea1ee520b8ebe2da5d5cdd28bfee5c51bcd8d4a36e4b063a676ddf,
App version: 3.7.62.1/376201130, App repackaged: False, APP
Developer: None, APP Developer Certificate: None, System APP: None,
APP Link: None, Network bssid: None, Device Location: None, Network
Certificate: None, NetworkArpPoisoning: None, sms_urls: None,
Sender: None, Location: None, ssid: None, Devicerootedjailbroken:
False, Network Resource: None#015
```

Syslog event format for IBM QRadar SIEM:

```
May 15 11:24:26 HarmonyMobile dashboard-eu2-alerts: URL: dashboard-
url.locsec.net, Product: Harmony Mobile, AttackVector: Application,
DeviceAlert Event: Application, Product: Harmony Mobile, Threat
Factors: Backup Tool, EventType: Installed, Signature: app_hash\:
781938e38fea1ee520b8ebe2da5d5cdd28bfee5c51bcd8d4a36e4b063a676ddf,
RiskLevel: CRITICAL, DeviceID: 339, Client: Harmony Mobile Protect,
Device Client Version: 4.3.0.9307, DeviceOwner: testUser,
DeviceEmail: email@example.com, DeviceNumber: , DevicePolicy:
Global, DeviceGroups: ALL|hm-integrations-g, DeviceSerialNumber:
None, DeviceType: Android_work, DeviceOSLevel: 14, DeviceModel:
samsung / SM-S911B, DeviceRiskLevel: 1.0, Event ID: 78, Event
Timestamp: 1747297460000, Event Client Timestamp: 1747297457000,
Device Tracking ID:
5292f8dffd6b92f87a24fa32337fefbf200fe65e5c09fb2d48583c4cb89f2f99,
Host Type: Mobile, APP name: Smart Switch, APP package:
com.sec.android.easyMover, APP Threat summary: None, APP SHA256:
781938e38fea1ee520b8ebe2da5d5cdd28bfee5c51bcd8d4a36e4b063a676ddf,
App version: 3.7.62.1/376201130, App repackaged: False, APP
Developer: None, APP Developer Certificate: None, System APP: None,
APP Link: None, Network bssid: None, Device Location: None, Network
Certificate: None, NetworkArpPoisoning: None, sms_urls: None,
Sender: None, Location: None, ssid: None, Devicerootedjailbroken:
False, Network Resource: None#015
```

Event Structure

Field	Description	Values	Sample Value
URL	Source tenant URL	HM tenant URL	dashboardurl.locsec.net
AttackVector	Attack vector	▪ Application ▪ Cellular network ▪ WIFI network ▪ Device OS ▪ Exploits iOS profiles ▪ Network Security	Application

Field	Description	Values	Sample Value
Product	Name of reporting product.	Harmony Mobile	Harmony Mobile
Threat Factors	Type of the threat.	See Threat Factor List.	Backup Tool
EventType	Type of the event.	▪ Non-compliant ▪ Compliant ▪ Policy changed ▪ Active ▪ Inactive ▪ Disconnected ▪ Detected ▪ Ended ▪ Installed ▪ Removed ▪ Blocked ▪ Prevented ▪ Enabled ▪ Disabled	Removed
RiskLevel	Risk level of the event.	▪ None ▪ Low ▪ Medium ▪ High ▪ Info	Info
DeviceID	Internal Mobile Security device ID.		1111
Client	Client application.	Harmony Mobile Protect	Harmony Mobile Protect
Device Client Version	Version of the client application.	M.m.mm.b	3.2.0.3986
DeviceOwner	Name of the device owner.		testUser

Field	Description	Values	Sample Value
DeviceEmail	Email of the device owner.		email@example.com
DeviceNumber	Phone number of the device.		9720000000
DeviceType	Device type.	Android_4_x, iPhone	Android_4_x
DeviceOSLevel	Device OS version.		6.0.1
DeviceModel	Model of the device.	Multiple	samsung / SM-G930F,
DeviceRiskLevel	Current device risk level.	▪ **Unknown** - cs6 = 0 ▪ **None** - cs6 = 0 ▪ **Low** - 0 < cs6 <= 0.3 ▪ **Medium** - 0.3 < cs6 <= 0.6 ▪ **High** - 0.6 < cs6 <= 1 cs6 is the custom string label for current device risk level.	0.0
Event ID	Internal ID of the event.		13
Event Timestamp	Event received timestamp.		1586078275000
Event Client Timestamp	Event occurred timestamp.		1586078274000
Device Tracking ID			3c55d882-f2c8-48ac-ba3a-91a1afab3f5e
Host Type	Type of the endpoint.	Mobile	Mobile

Field	Description	Values	Sample Value
APP name	Name of the application, if the Attack Vector is Application .		Photos
APP package	Application package name.		com.google.android.apps.photos
APP Threat summary	Description of the app threats.		The application accesses the device data. It can backup sensitive information from the device
APP SHA256	SHA256 identifier of the binary.		382c9be98a2e63539dc8....
App version	Application version.		1.1/24
App repackaged	App was repackaged or not.	▪ False ▪ True	False
APP Developer	Developer of the app.		None
APP Developer Certificate	Certificate of the app.		None
System APP	If system app or not.		None
APP Link	Link to the official app store.		None
Network bssid	BSSID of the attacking network.		None
Network Certificate	Certificate of the attacking network.		None

Field	Description	Values	Sample Value
sms_urls	DEPRECATED, URLs found in SMS.		None
Sender	DEPRECATED, SMS sender number.		None
Location	Geo location of attacking network.		None
ssid	SSID (name) of the attacking Wi-Fi network.		None
Devicerootedjailbroken	If the device is rooted or jailbroken.	▪ False ▪ True	False
Network Resource	Malicious URL blocked by Mobile Security.		None

Appendix C - Mobile Security ArcSight

This appendix describes the structure of the ArcSight event sent by Mobile Security.

Sample Mobile Security event:

```
<CEF:0|Check Point|SMB|4.0.2.9119|BACKUP_
TOOL|Application|3|act=Installed alert_details=app_hash:
9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232fa3a9a
app_name=Google Photos app_package=com.google.photos bssid=None
cat=Alert cnt=1234 cs1=IPhone cs1Label=DeviceType cs2=+44 7469
376815 cs2Label=Phone cs3=15.6.1 cs3Label=OSLevel cs4=iPhone /
iPhone 11 cs4Label=DeviceDetails cs5=None
cs5Label=NetworkCertificate cs6=0.6 cs6Label=Current Device Risk
deviceDirection=None deviceExternalId=971225
deviceInboundInterface=False device_client_version=4.0.2.9119
duid=AAA23C40-6577-4321-8B74-25454123457D duser= user@example.com
dvchost=example-tenant.locsec.net externalId= F112343S-4123-4b69-
90ff-0234DFHGHFY9
fileHash=9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232f
a3a9a fileId=6.4.469058872 filePermission=False fileType=The
application accesses the device data. It can backup sensitive
information from the device. App Category - Photography This app
might access and share your device unique identifier. This might be
used to track location, gather user behaviour and present targeted
advertisement msg=app_hash:
9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232fa3a9a
resource=None rt=1662318312000 sender=None sms_urls=None ssid=None
start=1662318312000 suid=None suser=Jhon's iPhone uuid=None
```

CEF Header

CEF Header	Description
CEF:0	Common Event Format (CEF) version.
Check Point	Vendor name.
SMB	Product name.
4.0.2.9119	Client version.

CEF Header	Description
BACKUP_ TOOL	Type of the threat, called as threat factor. To view the complete list of threat factors, see *"Threat Factor List" on page 231*.
Application	Attack vector.
10	Severity of the event (values are discrete). ■ Low - 3 ■ Medium - 7 ■ High - 10

CEF Extension

CEF Extension	Description	Values	Sample Value
act	Type of the event.	▪ Non-compliant ▪ Compliant ▪ Policy changed ▪ Active ▪ Inactive ▪ Disconnected ▪ Detected ▪ Ended ▪ Installed ▪ Removed ▪ Blocked ▪ Prevented ▪ Enabled ▪ Disabled	Installed
alert_details	Event details.		app_hash: 9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232fa3a9a
app_name	Related application name, if relevant.		Google Photos

CEF Extension	Description	Values	Sample Value
app_pacakge	Application package name, if relevant.		com.google.photos
bssid	BSSID of the attacking network.		None
cat	Mobile Security event category.		Alert
cnt	Mobile Security event ID.		1232
cs1	Device type.	▪ Android_4_x ▪ iPhone	iPhone
cs1Label	Custom string label Device Type.	DeviceType	DeviceType
cs2	Phone number of the device.		+44 7469 376815
cs2Label	Custom string label Phone.	Phone	Phone
cs3	Device OS version.		15.6.1

CEF Extension	Description	Values	Sample Value
cs3Label	Custom string label OS level.	OSLevel	OSLevel
cs4	Model of the device.	Multiple	iPhone / iPhone 11
cs4Label	Custom string label DeviceDetails.	DeviceDetails	DeviceDetails
cs5	Certificate of the attacking network.		
cs5Label	Custom string label NetworkCertificate	NetworkCertificate	NetworkCertificate

CEF Extension	Description	Values	Sample Value
cs6	Current device risk level.	▪ **Unknown** - cs6 = 0 ▪ **None** - cs6 = 0 ▪ **Low** - 0 < cs6 <= 0.3 ▪ **Medium** - 0.3 < cs6 <= 0.6 ▪ **High** - 0.6 < cs6 <= 1	0.6
cs6Label	Custom string label Current Device Risk.	Current device risk.	Custom string label
deviceDirection	Is ARP Poisoning network.	▪ None ▪ True ▪ False	None
deviceExternalId	Device UUID	Multiple	971225
deviceInboundInterface	If the device is rooted or jailbroken.	▪ True ▪ False	False

CEF Extension	Description	Values	Sample Value
device_ client_version	Version of the client app.	M.m.mm.b	4.0.2.9119
duid	Device Tracking ID.		AAA23C40-6577-4321-8B74-25454123457D
duser	User Email.		user@example.com
dvchost	Host		example-tenant.locsec.net
externalId	Device UUID.		F112343S-4123-4b69-90ff-0234DFHGHFY9
fileHash	SHA256 identifier of the binary.		9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232fa3a9a
fileId	Application version.		6.4.469058872
filePermission	Application was repackaged or not.	▪ False ▪ True	False
fileType	Description of the app threats.		The application accesses the device data. It can backup sensitive information from the device.
msg	Event details.		app_hash: 9061187fbd6aa0cf978bfe9928158cf41c53c70a884f9d8b279a52e232fa3a9a
resource	Malicious URL blocked by Mobile Security.		None

CEF Extension	Description	Values	Sample Value
rt	Event Client Timestamp.		1662318312000
sender	DEPRECATED, SMS sender number.		None
sms_urls	DEPRECATED, URLs found in SMS.		None
ssid	SSID (name) of the attacking Wi-Fi network.		None
start	Event Received timestamp.		1662318312000
suid	Network location.	▪ Latitude ▪ Longitude ▪ None	None
suser	Phone name.		Jhon's iPhone
uuid	Device UUID for Airwatch UEM.		None

Threat Factor List

Note - This list is dynamic, and the threat factors may be added or removed. The below list is as on March 2022.

Threat Factors
Accessibility permission
Account Info Access
Achilles vulnerability
Action
Admin Rights
Adventure
Alcohol & Tobacco
Anonymizer
App Not Available in Market
Application Download
Arcade
ARP Poisoning
Art & Design
Art / Culture
Auto & Vehicles
Background refresh permission
Backup Tool
Beauty
Blogs / Personal Pages
Bluetooth Access
Board
Books & Reference
Botnets
Business

Threat Factors
Business / Economy
Calendar Access
Call Log Access
Camera Access
Captive
Card
Casino
Casual
Cell Location Access
Child Abuse
Client version
Comics
Communication
Computers / Internet
Configuration Profile
Connectivity
Contacts Access
Dangerous App
Dating
Debug Certificate
Developer options
Dropper
Education
Educational

Threat Factors
Email
Entertainment
Fake App
Fake Corporate Wi-Fi
Fake Public Wi-Fi
Fashion
File Download
File Storage and Sharing
Finance
Financial Information Stealing App
Financial Services
Food & Drink
Gambling
Games
General
Government / Military
Greeting Cards
Hacking
Hacking Tool
Mobile Security not installed on personal profile
Hate / Racism
Health
Health & Fitness
Hidden Clicker

Threat Factors
History Bookmarks Access
House & Home
Illegal / Questionable
Illegal Drugs
Inactive Sites
Info Stealer
Instant Chat
Instant Messaging
Job Search / Careers
Keyboard Access
Knox permission not granted
Legitimate App
Libraries & Demo
Lifestyle
Lingerie and Swimsuit / Suggestive
Local Network Permission
Location Access
Location permission
Location Tracking
Malicious File
Malware
Man-In-The-Middle Attack App
Maps & Navigation
Marijuana

Threat Factors
Media Sharing
Media Streams
Mediatek vulnerability
Medical
Microphone Access
MITM Attack Prevention
Mobile Remote Access Tool
Music & Audio
Nature / Conservation
Network Protection
Network Protection (TLS)
Network Protection (VPN)
Network Redirection Tool
News & Magazines
News / Media
Newsgroups / Forums
Non Official App Store App
Non-profits & NGOs
Notification permission
Nudity
Open Wi-Fi
Optimizer Tool
OS patch level
OS Version

Threat Factors
P2P File Sharing
Parenting
Personal profile compromised
Personal profile inactive
Personalization
Personals / Dating
Phishing
Phishing App
Photography
Policy verification
Political / Legal
Pornography
Port Scanning Detected
Premium Dialer
Productivity
Protected DNS
Puzzle
Racing
Ransomware
Real Estate
Recreation
Religion
Remote Access Tool
Rogue Access Point Connected

Threat Factors
Role Playing
Rooting Management Tool
Rootkit
Rough Ad-Network
Safari is not installed
Samsung knox block application until scan ends
Samsung knox block risky application
Screen lock protection
SD card encryption
Search Engines / Portals
SELinux enforced
Sex
Sex Education
Shopping
Simulation
SMS Bot
Social
Social Networking
Software Downloads
Spam
Sports
Sports Game
Spyware / Malicious Sites
SSL Interception (Advanced)

Threat Factors
SSL Interception (Basic)
SSL Stripping
Storage encrypted
Storage permission not granted
Strategy
Suspecious app
Suspected Malware
Suspicious Content
Tasteless
This application was blacklisted
TLS/SSL Downgrade
Tools
Translation
Trivia
Uncategorized
USB debugging
Vehicles
Video Players & Editors
Violence
VPN lock down
Vulnerable app
Weapons
Weather
Web Advertisements

Threat Factors
Word
Zero-Phishing

Appendix D - Permissions for Harmony Mobile Protect app

This appendix describes the permissions required for Harmony Mobile Protect app in Android and iOS devices, to ensure that the Mobile Security solution operates as expected. The permissions required are based on commonly used policies and features activated for each tenant.

The permissions must be granted automatically by the UEM or by the end-users on the protected mobile devices.

Permissions for Android Devices

Permission	Description
Location Permission	Allows an application to access the device location. Mobile Security uses this permission to enrich the threat event reports with location.
Notification Permission	Allows an application to display notifications on the device. Mobile Security uses this permission to: ■ Notify mobile devices that a policy update is available so that the policy can be enforced in a timely manner, instead of waiting for the next policy polling time (occurs once per day/24 hours by default). ■ Notify any security event to the end-user and offering mitigation actions for events which require manual intervention from the end-user (For example, delete files, uninstall a malicious or risky mobile app, disconnect from an unsecure WiFi).
Network Permission	Allows an application to intersect the mobile device network traffic. Mobile Security uses this permission to bring up a local VPN to inspect the data traffic and mitigate any detected network threat.
Camera	Allows an application to use the device's camera. Mobile Security uses this permission to scan QR code in the on-boarding process.
Background Activity	Allows an application to run in the background without being killed by the OS to save battery.
Admin privileges	Required when Mobile Security is integrated with Knox Agent on Samsung Android devices.
External Storage	Required if the policy includes storage scan.

Permission	Description
SMS Permission	Allows Mobile Security to scan SMS messages for malicious URLs.

Permissions for iOS Devices

Permission	Description
Location Permission	Allows an application to access the device location. Mobile Security uses this permission to enrich threat event reports with the location.
Notification Permission	Allows an application to display notifications on the device. Mobile Security uses this permission to: ■ Notify mobile devices that a policy update is available so that the policy can be enforced in a timely manner, instead of waiting for the next policy polling time (occurs once per day/24 hours by default). ■ Wake-up the iOS.
VPN User Consent	Allows an application to intersect the mobile device network traffic. Mobile Security uses this permission to bring up a local VPN to inspect the data traffic and mitigate any detected network threat.
Camera	Allows an application to use the camera. Mobile Security uses this permission to scan QR code in the on-boarding process.
SMS Filtering	Allows Mobile Security to scan SMS messages for malicious URLs. To enable SMS filtering on the end-user device, see Preventing SMS Phishing in the Harmony Mobile Protect for iOS User Guide.

Permissions and Features Dependencies

The following table shows the permissions required to enforce the policy features in Android and iOS devices.

Permissions	Notification	Location (Android)	Network VPN (iOS)	Local Network (iOS)	Query Packages (Android)	Storage Access (Android)	Camera	Knox Agent (Android)	Ignore Battery Optimization
Features									

Permissions	Notification	Location (Android)	Network VPN (iOS)	Local Network (iOS)	Query Packages (Android)	Storage Access (Android)	Camera	Knox Agent (Android)	Ignore Battery Optimization
Application Malware and Side Loading detection	Mandatory				Mandatory				Mandatory
Application Malware and Side Loading detection and blocking	Mandatory							Mandatory	Mandatory
Malicious Process Control								Mandatory	
Risky Application Traffic Blocking (Android)	Mandatory		Mandatory	Mandatory					Mandatory

Permissions	Notification	Location (Android)	Network VPN (iOS)	Local Network (iOS)	Query Packages (Android)	Storage Access (Android)	Camera	Knox Agent (Android)	Ignore Battery Optimization
Malicious URL Access Blocking	Mandatory		Mandatory	Mandatory					Mandatory
Conditional Access	Mandatory		Mandatory	Mandatory					Mandatory
On-device File Download Prevention	Mandatory		Mandatory	Mandatory					Mandatory
File Protection – Storage Scan	Mandatory					Mandatory			Mandatory
URL Filtering	Mandatory		Mandatory	Mandatory					Mandatory
Application Category Based Blocking	Mandatory		Mandatory	Mandatory					Mandatory

Permissions	Notification	Location (Android)	Network VPN (iOS)	Local Network (iOS)	Query Packages (Android)	Storage Access (Android)	Camera	Knox Agent (Android)	Ignore Battery Optimization
QR code based On-Boarding	Mandatory						Mandatory		Mandatory
Unsecure WiFi *	Mandatory	Mandatory (For Android version lower than 13)							Mandatory
NEARBY_WIFI_DEVICES		Mandatory (For Android version 13 and above)							
MitM detection	Mandatory								Mandatory
Rogue Access Detection	Mandatory	Mandatory							Mandatory

Permissions	Notification	Location (Android)	Network VPN (iOS)	Local Network (iOS)	Query Packages (Android)	Storage Access (Android)	Camera	Knox Agent (Android)	Ignore Battery Optimization
Wake-up iOS devices	Mandatory								

* On Android, Mobile Security can report the SSID only if the Harmony Mobile Protect runs in foreground and is granted the required permissions.