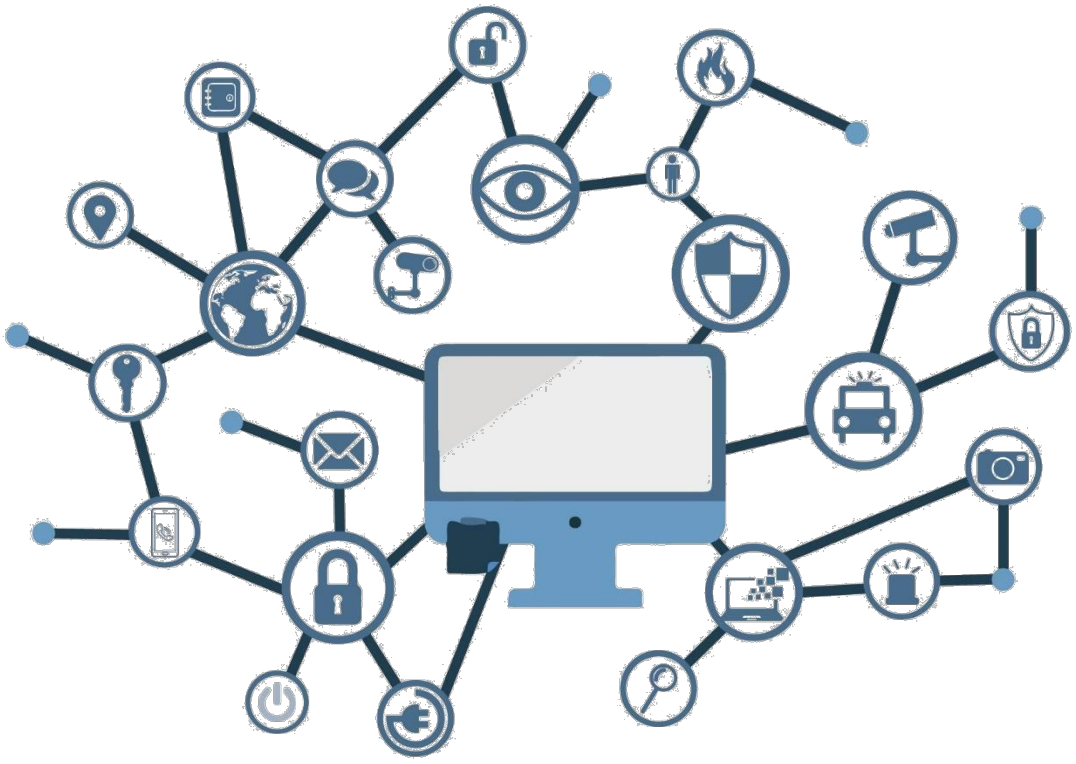
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1212

Procedimiento de Empleo Seguro
Harmony SandBlast Mobile



Marzo de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.17 13:21:03 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-095-6

Fecha de Edición: marzo de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN 4
2. OBJETO Y ALCANCE 5
3. ORGANIZACIÓN DEL DOCUMENTO 6
4. FASE PREVIA A LA INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 10
5. FASE DE DESPLIEGUE E INSTALACIÓN 14
5.1 CREACIÓN DE UNA CUENTA DE SEGURIDAD PARA HARMONY MOBILE EN INFINITY PORTAL 14
5.2 DESPLIEGUE DE HARMONY MOBILE 15
5.3 AÑADIR NUEVOS USUARIOS Y DISPOSITIVOS DESDE QUICK ACTIONS 17
5.4 AÑADIR UN NUEVO DISPOSITIVO 17
5.5 AÑADIR UN GRUPO DE DISPOSITIVOS 20
6. FASE DE CONFIGURACIÓN 21
6.1 MODO DE OPERACIÓN SEGURO 21
6.1.1. CREACIÓN DE PERFILES DE POLÍTICAS 21
6.1.2. BASE DE REGLAS (RULEBASE) 21
6.2 CONFIGURACIÓN DE POLÍTICAS 22
6.2.1. POLÍTICAS DE DISPOSITIVO 22
6.2.2. POLÍTICAS DE APLICACIONES 23
6.2.3. POLÍTICAS DE RED (ON-DEVICE NETWORK PROTECTION) 24
6.3 AUTENTICACIÓN 28
6.3.1. AUTENTICACIÓN DE DOBLE FACTOR (2FA) 28
6.4 ADMINITRACIÓN DEL PRODUCTO 29
6.4.1. ADMINISTRACIÓN LOCAL Y REMOTA 29
6.4.2. CONFIGURACIÓN DE ADMINISTRADORES 29
6.4.3. CONFIGURACIÓN DE ROLES DE ADMINISTRACIÓN GLOBALES 30
6.5 SERVIDORES DE AUTENTICACIÓN 33
6.5.1. AUTENTICACIÓN CON SINGLE SIGN-ON (SSO) 33
6.6 GESTIÓN DE CERTIFICADOS 36
6.7 AUDITORÍA 36
6.7.1. ALMACENAMIENTO REMOTO 37
6.8 FUNCIONES DE SEGURIDAD 39
6.8.1. ANTI-PHISHING 39
6.8.2. SAFE BROWSING 40
6.8.3. ANTI-BOT 40
6.8.4. ZERO-PHISHING PROTECTION 41
6.8.5. ACCESO CONDICIONAL 41
6.8.6. URL FILTERING 42

6.8.7. PREVENCIÓN DE DESCARGAS 47
6.8.8. PROTECCIÓN DE DNS 47
6.8.9. WIFI NETWORK 48
6.9 BUENAS PRÁCTICAS 53
6.9.1. BUENAS PRÁCTICAS PARA POLÍTICAS DE DISPOSITIVO 53
7. FASE DE OPERACIÓN 56
8. CHECKLIST 57
9. REFERENCIAS 59
10. ABREVIATURAS 61

1. INTRODUCCIÓN

1. **Harmony Mobile** es una solución de defensa contra amenazas móviles. Protege las aplicaciones, la red y el sistema operativo de todos los vectores de ataque. Se adapta al entorno móvil existente, se implementa y escala rápidamente, y protege los dispositivos sin afectar la experiencia ni la privacidad del usuario.
2. Los beneficios que aporta Harmony Mobile son:
    - Protección completa: protección de datos corporativos en todas las superficies de ataque móvil.
    - Gestión simple: seguridad escalable y fácil de administrar para cualquier tipo de recursos móviles.
    - Fácil de usar: adopción rápida con impacto mínimo en la experiencia o privacidad del usuario.
3. A continuación, se enumeran algunas de las funcionalidades de seguridad que proporciona el producto:
    - Evita la descarga de aplicaciones maliciosas.
    - Evita campañas de *phishing* a través de las aplicaciones instaladas en el dispositivo móvil.
    - Evita ataques de *Man-in-the-Middle*.
    - Proporciona la capacidad de bloquear dispositivos infectados, para que estos no puedan acceder a información sensible (por ejemplo, a aplicaciones corporativas).
    - Proporciona capacidades de detección de técnicas de *jailbreaking* **[REF6]** y *rooting* **[REF7]**, así como detección de vulnerabilidades del Sistema Operativo del dispositivo móvil.

2. OBJETO Y ALCANCE

4. El objeto de este documento es proporcionar un procedimiento de empleo seguro de los productos **Harmony Mobile para Android (versión 3.8.2.3023) y Harmony Mobile para iOS (versión 3.8.2.5594)** para pueda ser utilizado en los sistemas de información del sector público bajo el alcance del Esquema Nacional de Seguridad (ENS).

5. Dichos productos han sido cualificados e incluidos en el **Catálogo de Productos y Servicios STIC (CPSTIC) para categoría MEDIA, en la familia de EDR** (*Endpoint Detection and Response*).

3. ORGANIZACIÓN DEL DOCUMENTO

6. Se indica la estructura de capítulos del documento:

   a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

   b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   e) **Apartado 8.** En este apartado se incluye una *checklist* con las tareas a realizar, y el estado de cada una de ellas.

   f) **Apartado.9** Referencias empleadas en este documento.

   g) **Apartado 10**. Abreviaturas usadas en este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. La aplicación Harmony Mobile se trata de una aplicación para dispositivos móviles. Esta puede ser obtenida desde las plataformas de descarga oficiales: *Google Play* para el caso de dispositivos Android, y desde la *App Store* de Apple o el *Dashboard* de la solución para el caso de iOS.

8. Asimismo, el fabricante puede mandar un correo electrónico de invitación, para que el usuario descargue la aplicación. Este email de invitación se envía desde la dirección de correo *mtp-register@checkpoint.com*. Dicho mensaje de invitación puede ser enviado también vía SMS. El contenido del mensaje de invitación puede ser personalizado desde la plataforma de administración.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. La aplicación Harmony Mobile se trata de un producto *software* destinado a ser instalado en dispositivos móviles, por lo que no es necesario contar con un entorno de instalación seguro para su puesta en marcha.

4.3 REGISTRO Y LICENCIAS

10. Harmony Mobile emplea un sistema basado en licencias, es decir, requiere una licencia por cada dispositivo móvil que se desee proteger. Para más información acerca del proceso de licenciamiento, será necesario ponerse en contacto con el representante de ventas de CheckPoint, o comprobar las actualizaciones en la Comunidad de Usuarios de CheckPoint.

11. A través de *Infinity Portal*, desde la página *Contracts* se puede ver la información referente a las suscripciones a los diferentes servicios de seguridad.

12. Desde la opción *Global Settings > Contracts*, se pueden ver los servicios de seguridad para los que hay suscripción. Entre la información mostrada, se indica:

    - La fecha de expiración del contrato.
    - El número de contratos.
    - El número de “vacantes” asociadas al contrato que ya han sido ocupadas por dispositivos.

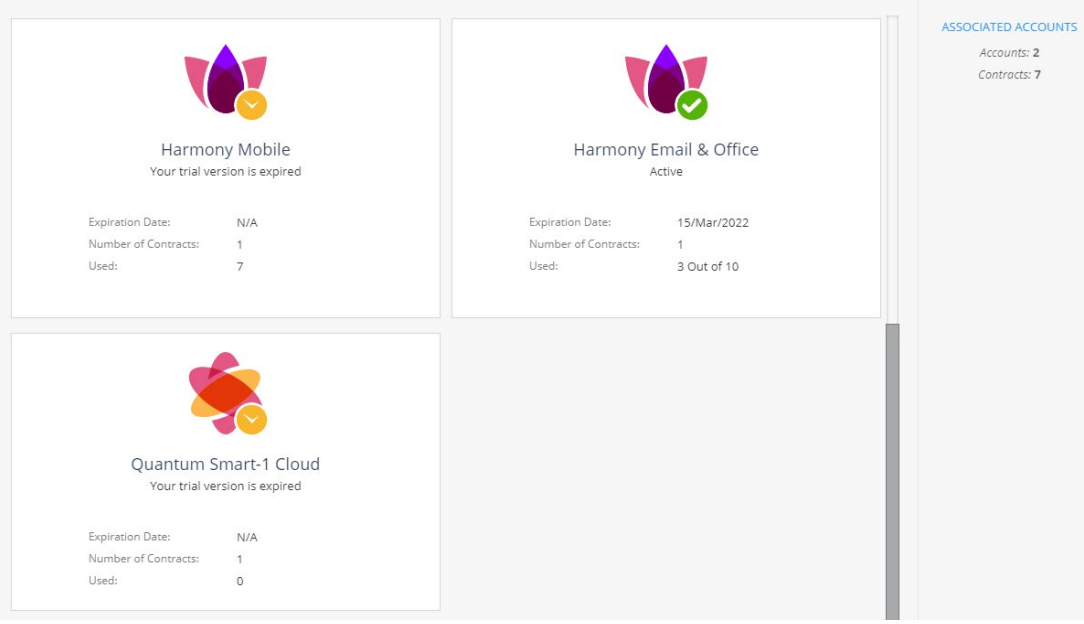


Figura 1: Detalles de contratos

13. Para más información, se recomienda consultar los apartados "*Contracts*" y "*Associated Accounts*", de la Guía de Administración de Infinity Portal **[REF3]**.

4.4 CONSIDERACIONES PREVIAS

14. Antes de empezar a gestionar los servicios ofrecidos en Infinity Portal, es necesario activar las licencias adquiridas. Para ello, se debe asociar las cuentas del Centro de Usuarios (*User Center*) a la cuenta de Infinity Portal. Para más información al respecto, consultar el siguiente enlace **[REF4]**:

    https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk144612

15. El panel *Contracts* muestra el listado de cuentas y licencias asociadas a la cuenta de *User Center*.

16. A continuación, se enumeran los pasos a seguir para asociar una cuenta al *User Center*:

    1) Hacer *login* en el *Infinity Portal*. Esta cuenta de *User Center* ya estará creada previamente por el equipo de ventas de CheckPoint. El número de esta cuenta (el *UserCenterID*) es transmitido al usuario por CheckPoint.

    2) Ir a *Global Settings* > *Contracts* > *Associated Accounts*. A continuación, se muestra una imagen de ejemplo:

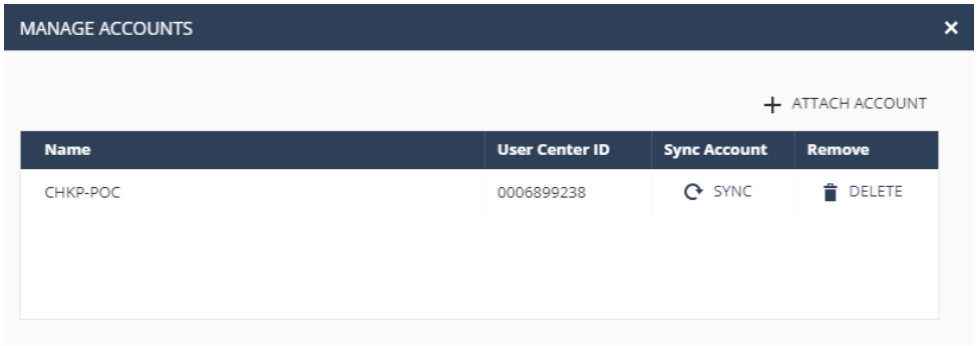


Figura 2: Cuentas asociadas de *User Center*

3) En la ventana *Manage Account*, hacer *click* en el botón [+] *Attach Account* (ver Figura 2) para asociar una nueva cuenta de *User Center* al *Infinity Portal.*

   Se abrirá la ventana correspondiente, en la que habrá que introducir las credenciales de la cuenta de *User Center*. A continuación, se incluye una imagen de ejemplo:

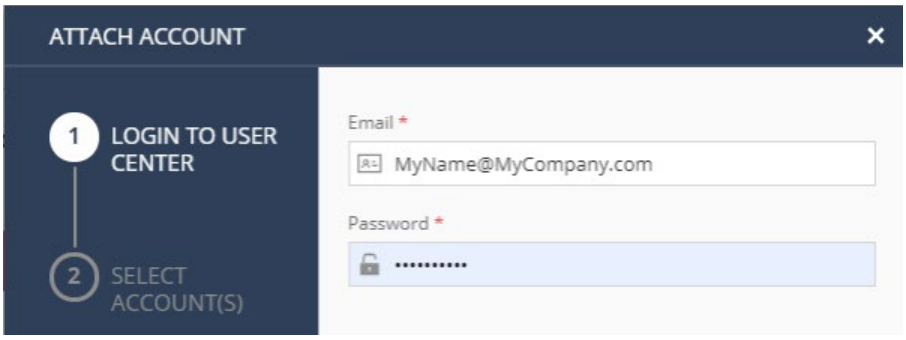


Figura 3: Ventana de asociación de cuenta

4) Hacer *click* en *Next*.

5) Una vez proporcionadas las credenciales, se producirá la conexión al *User Center*. A continuación, habrá que seleccionar la cuenta de *User Center* a las que están asociadas las licencias que se desea activar.

6) Una vez que se han activado las licencias seleccionadas, hacer *click* en *Finish*.

7) Volver a la página *Contracts*, y verificar que la/s licencia/s han sido asociadas a la cuenta de *Infinity Portal*. A continuación, se incluye una imagen de ejemplo:

Figura 4: Licencias asociadas en Infinity Portal

17. Si durante este proceso se diese algún tipo de confusión o contratiempo, se recomienda ponerse en contacto con la persona de contacto de CheckPoint.
18. A continuación, se indican los pasos a seguir para sincronizar las cuentas existentes con el *User Center*:
    1) Ir a *Contracts window > Associated Accounts.*
    2) Hacer click en el botón *Sync*.
19. A continuación, se indican los pasos a seguir para eliminar una cuenta existente:
    1) Ir a *Contract window > Associated Accounts > Manage Accounts.*
    2) Seleccionar una cuenta de la lista.
    3) En la columna *Remove*, hacer *click* en *Delete*.
    4) Hacer *click* en el botón *Sync*.
20. Para más información acerca del proceso a seguir para asociar cuentas del Centro de Usuarios con la cuenta de *Infinity* Portal, se recomienda consultar el apartado "*Associated Accounts*" de la Guía de Administración de *Infinity Portal* **[REF3]**.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

21. A continuación, se presenta el esquema de la arquitectura de la solución, así como una descripción de cada uno de los componentes de dicha arquitectura:

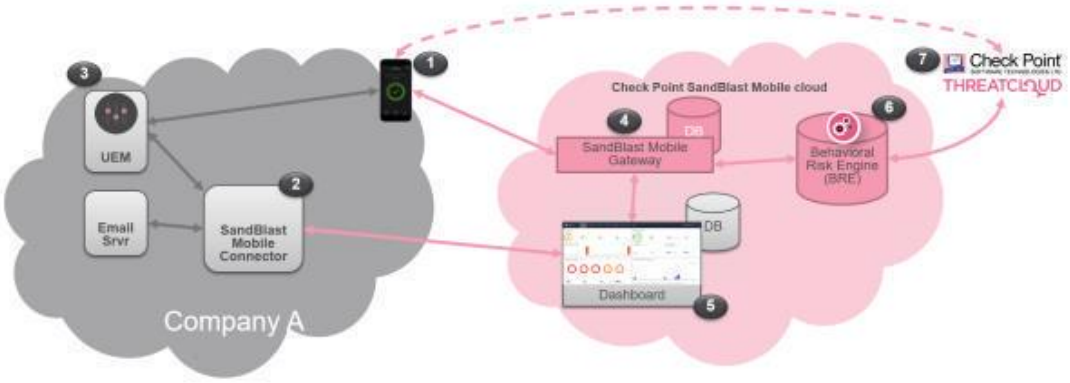


Figura 5: Arquitectura de Harmony Mobile

ITEM	COMPONENTE	DESCRIPCIÓN
1	**Dispositivo móvil**	Dispositivo móvil (Android o iOS) protegido por la solución *Harmony Mobile*
3	**UEM/EMM/MDM**	Gestión de movilidad empresarial / Gestión de dispositivos móviles Sistema de gestión de dispositivos y aplicación de políticas.

ITEM	COMPONENTE	DESCRIPCIÓN
4	***Harmony Mobile Gateway***	*Check Point Harmony Mobile Gateway* basado en la nube es una arquitectura de múltiples *tenants* en la que se registran los dispositivos móviles. *Gateway* maneja todas las comunicaciones de la Solución con los dispositivos móviles registrados y con la instancia del Panel de control del cliente (organización).
5	***Dashboard***	El panel de gestión de dispositivos móviles es gestionado a través de un navegador web basado en la nube, y permite la administración, el aprovisionamiento y la supervisión de dispositivos y políticas, y se configura como una instancia por cliente. *Harmony Mobile Dashboard* se puede integrar con una solución existente de Gestión de dispositivos móviles (MDM) / Gestión de movilidad empresarial (EMM) para la aplicación automatizada de políticas en dispositivos en riesgo. Cuando se utiliza esta integración, la solución existente de gestión de dispositivos móviles sirve como un repositorio con el que *Harmony Mobile Dashboard* sincroniza los dispositivos e identidades inscritos.
6	***Behavioral Risk Engine* (BRE)**	*Harmony Mobile Behavioral Risk Engine*, basado en la nube, utiliza los datos que recibe de la aplicación sobre la red, la configuración y los datos de integridad del Sistema Operativo del dispositivo móvil, así como información sobre las aplicaciones instaladas, para realizar un análisis de amenazas móviles en profundidad. El motor utiliza estos datos para detectar y analizar actividades sospechosas y genera una puntuación de riesgo basada en el tipo y la gravedad de la amenaza. El puntaje de riesgo determina si se necesita una acción de mitigación automática, y qué acción de mitigación automática se necesita para mantener un dispositivo y sus datos protegidos. El motor no procesa ni almacena información personal. Para más información al respecto, se recomienda consultar **[REF9].**

Tabla 1: Componentes de Harmony Mobile

- ***Aplicación Harmony Mobile Protect**:*

    - La aplicación protege al dispositivo móvil y ayuda a analizar amenazas para el mismo. Monitoriza las configuraciones del sistema operativo del dispositivo, así como el comportamiento de las aplicaciones instaladas en el mismo, y sus diferentes conexiones de red. Asimismo, recopila información, que será analizada para identificar comportamientos sospechosos o maliciosos, y analiza diferentes indicadores de riesgo detectados en la información recopilada.

      Nota: La aplicación realiza ciertos análisis sobre el dispositivo, mientras que un análisis en profundidad se lleva a cabo en la nube de CheckPoint **[REF5]**.

- ***UEM (Unified Endpoint Management):***

    - Desde este componente se lleva a cabo la gestión de dispositivos, así como la gestión y aplicación de políticas de seguridad sobre los mismos.

- ***Harmony Mobile Gateway:***

    - Arquitectura basada en la nube contra la que se registran los dispositivos móviles a ser protegidos.
    - El *Gateway* gestiona las comunicaciones con los dispositivos móviles registrados, así como con el *Dashboard* del cliente.

- ***Harmony Mobile Management Dashboard:***

    - Se trata de una interfaz web basada en la nube, y ubicada en el *CheckPoint Infinity Portal*.
    - Permite la administración, aprovisionamiento, así como la monitorización de los dispositivos, gestión de políticas de seguridad, eventos, alertas, y operaciones de tipo forense sobre los dispositivos.

- ***Behavioral Risk Engine:***

    - Servicio basado en la nube. Emplea la información recibida desde la aplicación sobre la red, configuraciones, integridad de los datos del sistema operativo, así como información sobre las aplicaciones instaladas en el dispositivo para llevar a cabo análisis de amenazas.
    - Analiza esta información para detectar y analizar actividades maliciosas, y proporciona una puntuación basada en los tipos de amenazas y su severidad. Esta puntuación determinará si se aplican acciones automáticas de mitigación para mantener el dispositivo protegido, así como el tipo de acciones a aplicar.

- ***ThreatCloud:***
    - Se trata de la base de datos de incidentes de compromiso de CheckPoint. Analiza la información sobre amenazas de los diferentes *endpoints* de *gateways* de CheckPoint.
    - Gestiona las funcionalidades de *Anti-Phishing*, navegación segura, filtrado de URLs, y tecnologías *Anti-Bot* asociadas a la protección de dispositivos conectados a la red de Harmony Mobile.

5. FASE DE DESPLIEGUE E INSTALACIÓN

5.1 CREACIÓN DE UNA CUENTA DE SEGURIDAD PARA HARMONY MOBILE EN INFINITY PORTAL

22. Para la creación de la cuenta de seguridad inicial, será necesario registrarse en el portal de CheckPoint Infinity **[REF8]**: https://portal.checkpoint.com/

    Nota: el registro crea una cuenta en el portal Infinity Portal, pero no registra automáticamente en ningún servicio de seguridad específico. Utilizar la función "*Probar*" para iniciar sesión en el servicio *Harmony Mobile*.

23. Habilitar la cuenta de usuario en Infinity Portal. En el caso de no disponer de cuenta de usuario en Infinity Portal, desde la web https://portal.checkpoint.com/, hacer *click* en "*Don't have an account? Register here*" o acceder directamente a https://portal.checkpoint.com/create-account.

24. En la ventana que se muestra, introducir los datos personales correspondientes.

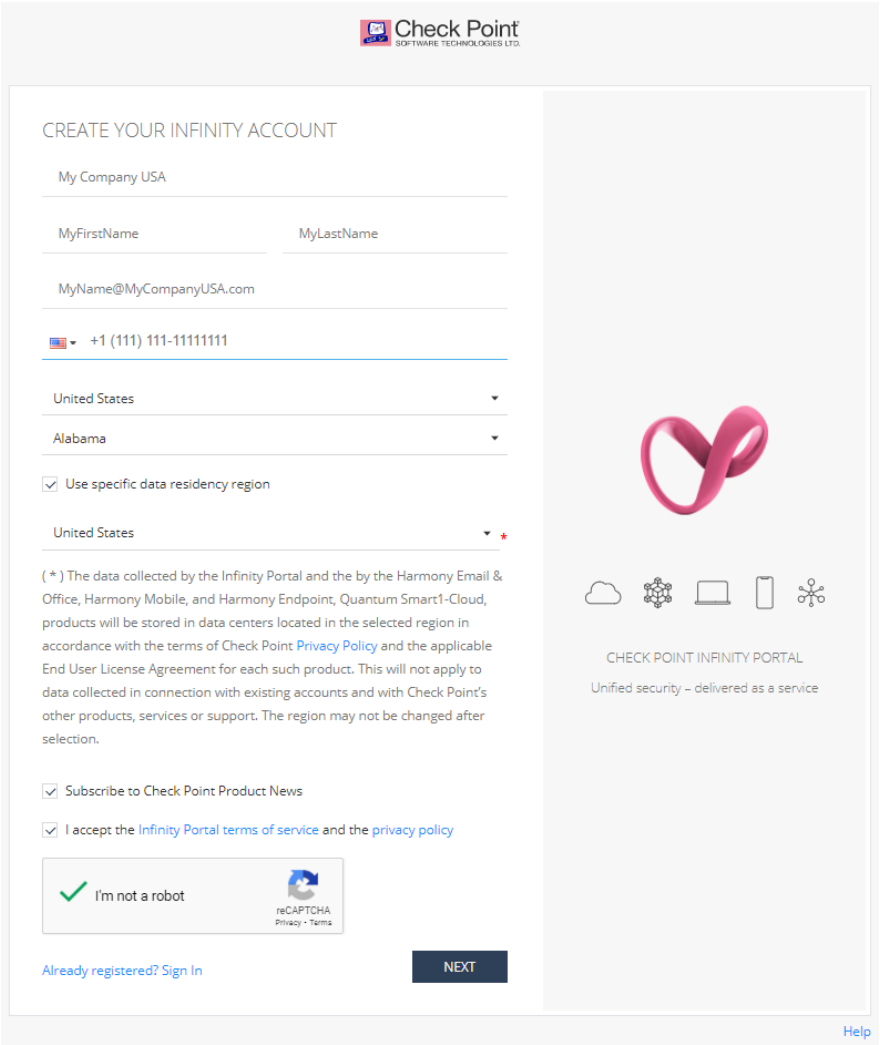


Figura 6: Creación de una cuenta en Infinity Portal

25. Hay una serie de datos a tener en cuenta:
    - *Company Name*: Nombre de la compañía, y será el nombre del Dashboard.
    - *Data Residency*: Ubicación de los datos. Se recomienda indicar "*Ireland*" para el cumplimiento del GDPR.
26. Se deben seguir los siguientes pasos:
    - Aceptar los términos de servicio y verificación del *Captcha*.
    - Hacer click en *Next*. Llegará un email de notificación referente a la confirmación de la creación de la cuenta de Infinity Portal que permitirá generar las credenciales asociadas a la cuenta (contraseña de acceso). Dicha contraseña de acceso sigue la política de complejidad de contraseñas reflejada en el punto 6.4.3.1 POLÍTICA DE CONTRASEÑAS de este documento.
    - Acceder a Infinity Portal (https://portal.checkpoint.com/) con las credenciales generadas en los pasos anteriores.
27. Para más información, consultar el apartado "*Creating an Logging in to your Infinity Account*", de la Guía de Administración de Infinity Portal **[REF3]**.

5.2 DESPLIEGUE DE HARMONY MOBILE

28. Check Point Harmony Mobile se administra desde el portal *Check Point Infinity Portal*. Check Point Infinity Portal es una interfaz basada en web empleada para alojar los servicios SaaS (*Software as a Service*) de seguridad de Check Point.
29. Para abrir el servicio Harmony Mobile desde *Infinity Portal*:
    1) Hacer click en el botón *Menú* en la esquina superior izquierda de la ventana de *Infinity Portal*.
    2) Seleccionar el servicio *Harmony Mobile* de la lista desplegable:

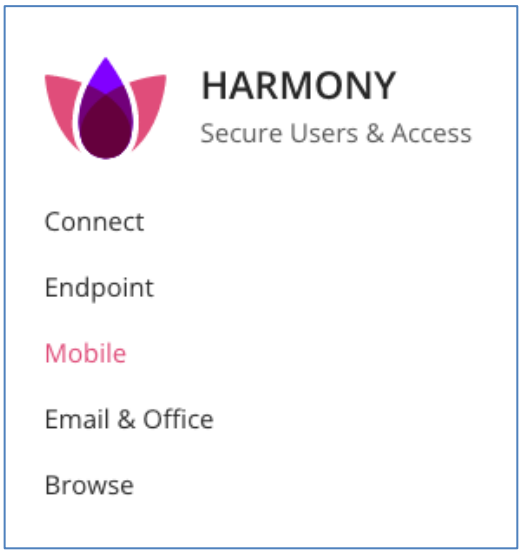


Figura 7: Menú Infinity Portal

30. La barra de menú está ubicada permanentemente en el lado izquierdo de la pantalla de Harmony Mobile.

31. A continuación, se enumeran las diferentes opciones que se incluyen en el menú lateral de Harmony Mobile:

Ítem	Descripción
Overview/ Dashboard	Ver estadísticas y datos capturados basados en la información proporcionada por los dispositivos inscritos.
Devices	Ver y administrar los dispositivos de la organización. La ventana de Dispositivos muestra una lista de todos los dispositivos protegidos por la organización. Desde esta pantalla, se puede Añadir, Eliminar, Editar Dispositivos, Importar y Exportar detalles referentes a dichos Dispositivos, y Activarlos. Desde esta pantalla, también se puede comprobar el estado en el que se encuentran los dispositivos: - ***Processing*****:** Un estado temporal, que tiene lugar entre el proceso de añadir un dispositivo de forma manual y el envío de la Invitación de Registro. - ***User Notified*****:** La Invitación de Registro ha sido enviada, pero el dispositivo no ha sido registrado todavía. - ***Provisioned*****:** el dispositivo ha sido añadido a través del UEM, pero aún no ha sido registrado. - ***Active*****:** La aplicación *Harmony Mobile* ha sido instalada, el dispositivo ha sido registrado con éxito, y ha sido escaneado con éxito. - ***Inactive*****:** La aplicación *Harmony Mobile* ha sido instalada, el dispositivo ha sido registrado, y posteriormente la aplicación ha sido eliminada del dispositivo, o bien el dispositivo no ha sido conectado al *Dashboard* durante un número determinado de días.
Policy	Configurar políticas granulares
Forensics	Permite revisar los datos forenses de seguridad, incluidos: - Eventos y alertas - Riesgo del dispositivo - Análisis de aplicaciones - Red - Perfiles de iOS
Settings	Ver y administrar la configuración del panel (*dashboard*).

Tabla 2: Menús de Harmony Mobile

32. La información en la pantalla de Parámetros Globales (*Global Settings*) contiene los valores predeterminados iniciales de la configuración de perfil de los administradores, que se aplican localmente y afectan a todo el sistema.

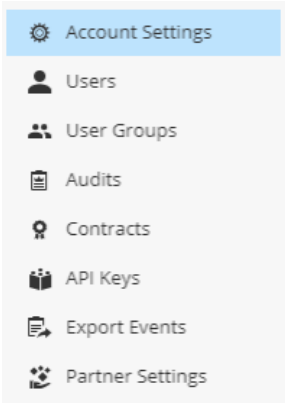


Figura 8: *Global Settings*

33. Para más información, consultar el apartado "*Global Settings*", de la Guía de Administración de Infinity Portal **[REF3]**.

5.3 AÑADIR NUEVOS USUARIOS Y DISPOSITIVOS DESDE QUICK ACTIONS

34. Desde el menú *Quick Actions (Dashboard > Overview > Quick Actions)*, los administradores pueden añadir nuevos usuarios y dispositivos a Harmony Mobile, empleando (3) tres opciones diferentes:

    1) *Demo on Device* – Permite experimentar el proceso de conexión de un único usuario y dispositivo.

    2) *Invite by Email* – Mediante esta opción, el administrador puede invitar a uno o múltiples usuarios o grupos a Harmony Mobile. Cada uno de los usuarios recibirá un correo electrónico con instrucciones y códigos QR, que permitirán llevar a cabo el proceso de registro.

    3) *Synch with MDM* - Mediante esta opción, los administradores de usuarios pueden conectar Harmony Mobile con otros sistemas de gestión de dispositivos móviles (*MDM*), y llevar a cabo el proceso de sincronización de usuarios y dispositivos a Harmony Mobile.

5.4 AÑADIR UN NUEVO DISPOSITIVO

35. Se invita a los dispositivos a instalar la aplicación Harmony Mobile y registrarse en el *Dashboard* a través de un correo electrónico de invitación generado desde el *Dashboard*, en la pestaña *Dispositivos*. También se pueden agregar dispositivos a través de la sincronización UEM. Para los clientes que utilizan soluciones UEM como *BlackBerry*, *AirWatch* o *MobileIron*, se recomienda consultar el documento *Harmony Mobile Integration Guide* **[REF2]**.

36. Para los clientes que usan dispositivos Android Enterprise, se debe consultar la mencionada guía de integración para obtener más orientación sobre cómo

configurar MDM para sincronizar dispositivos Android Enterprise con Harmony Mobile.

37. La invitación se envía a una dirección de correo electrónico que debe ser abierto desde el dispositivo. La primera parte del correo electrónico se puede personalizar con un mensaje específico del cliente desde *Settings > Email customization.*

    - Los dispositivos iOS se redirigen para instalar la aplicación desde la *App Store* de Apple. La instalación de iOS consta de dos (2) pasos posteriores a la instalación de la aplicación para su activación. Por una parte, se realiza la instalación de la aplicación y posteriormente se debe instalar, aceptar y marcar como perfil de confianza un *Perfil de Configuración* proporcionado directamente desde la aplicación. Todo el proceso es guiado mediante el propio sistema operativo iOS. Una vez completado el proceso de instalación, debe ingresar los detalles del servidor y el código de registro. Encontrará la información de registro y las instrucciones en el correo electrónico de registro.
    - Los dispositivos Android son redirigidos a *Google Play Store* para descargar la última versión de la aplicación Harmony Mobile disponible. Toda la información de registro será ingresada automáticamente por el sistema al usar el enlace de descarga en el correo electrónico desde el dispositivo durante el proceso de instalación.

38. A continuación, se enumeran los pasos a seguir para añadir un nuevo dispositivo:

    1) Ir a *Devices > New > Add new device*. A continuación, incluir la información necesaria.

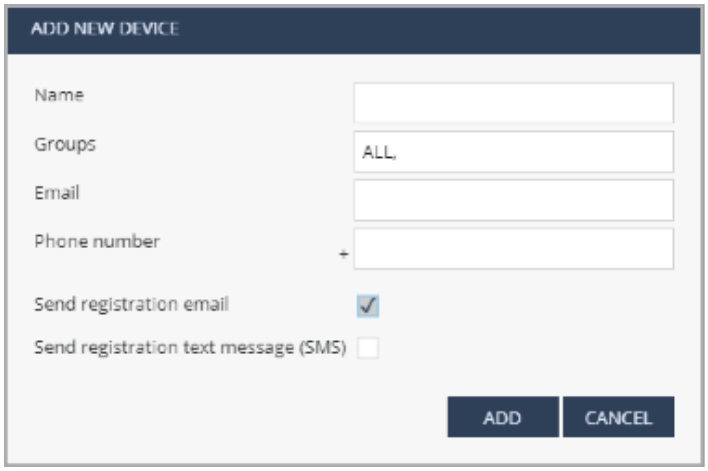
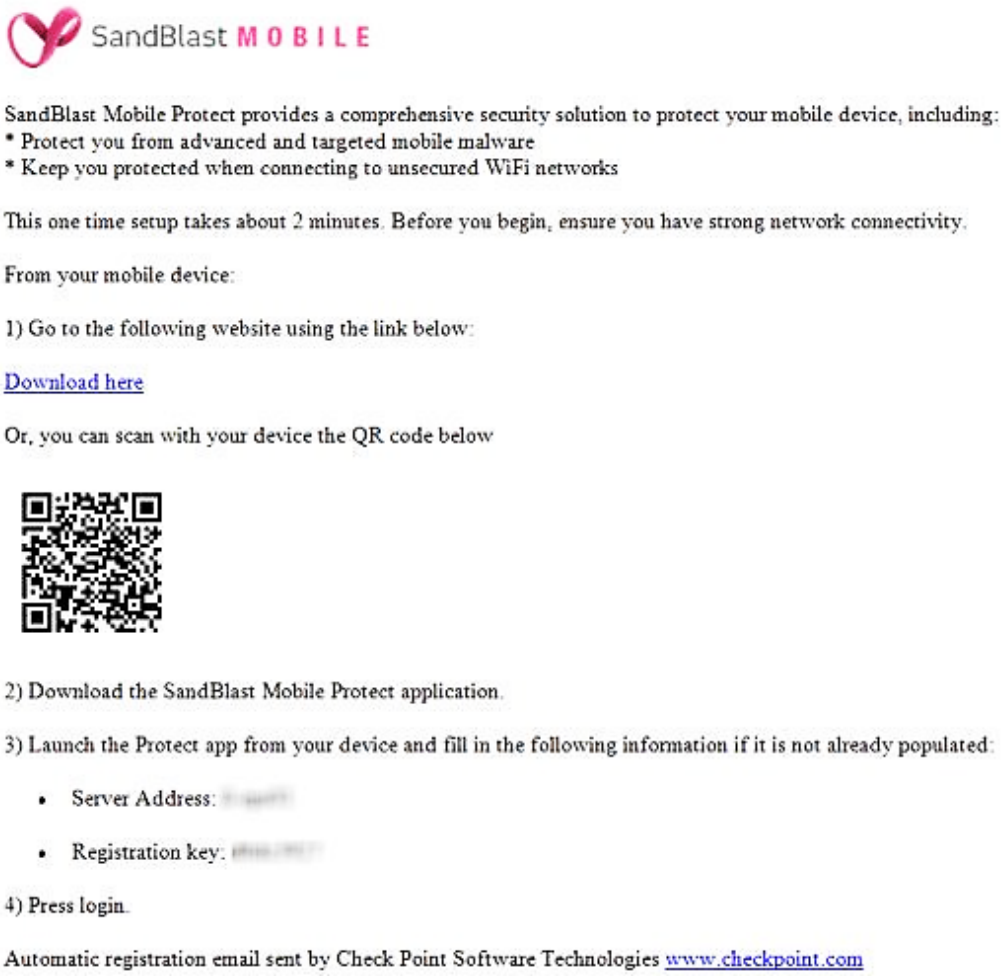


Figura 9: Añadir nuevo dispositivo

    2) Introducir el nombre, el grupo, la dirección de correo electrónico y el número de teléfono sencillos del dispositivo para el usuario en las propiedades de *Agregar nuevo dispositivo*.

    3) Hacer clic en *ADD*.

39. Se envía un correo electrónico desde el *Dashboard* con una breve descripción sobre la App de Harmony Mobile. El correo electrónico contiene un enlace para descargar la aplicación Harmony Mobile. A continuación, se muestra un ejemplo:


SandBlast MOBILE

SandBlast Mobile Protect provides a comprehensive security solution to protect your mobile device, including:
* Protect you from advanced and targeted mobile malware
* Keep you protected when connecting to unsecured WiFi networks

This one time setup takes about 2 minutes. Before you begin, ensure you have strong network connectivity.

From your mobile device:

1) Go to the following website using the link below:

Download here

Or, you can scan with your device the QR code below

2) Download the SandBlast Mobile Protect application.

3) Launch the Protect app from your device and fill in the following information if it is not already populated:

- Server Address:
- Registration key:

4) Press login.

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

Figura 10: Email de registro

40. Cuando el dispositivo añadido queda reflejado en el panel de control (*Dashboard*), aparece una entrada debajo de los dispositivos con un ID de dispositivo único. El estado del dispositivo se mostrará como *"User Notified"* hasta que se instale la aplicación Harmony Mobile y el dispositivo se haya comunicado con el panel de control (*Dashboard*).
41. Cuando la aplicación se instala y ejecuta correctamente desde el dispositivo, aparece la pantalla de registro. Para los dispositivos Android, el sistema ingresa la información automáticamente. En dispositivos iOS, debe ingresar la información manualmente.
42. Si el proceso de registro es exitoso, se realiza automáticamente un escaneo completo del dispositivo. Si no se encuentran *malware* o configuraciones maliciosas, el estado de la aplicación aparece en verde completo. Si la comunicación con el panel de control (*Dashboard*) es exitosa, la entrada del dispositivo cambia de "*User Notified*" a "*Active*" y los detalles del dispositivo se actualizarán.

5.5 AÑADIR UN GRUPO DE DISPOSITIVOS

43. Es posible asignar dispositivos a un grupo de dispositivos cuando estos son añadidos al sistema. También es posible asignar un dispositivo ya existente a un grupo de dispositivos.

44. A continuación, se enumeran los pasos a seguir para añadir un Grupo de Dispositivos:

    1) Ir a *Devices > Groups > ADD (*)*

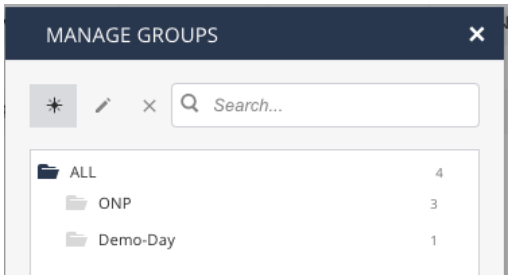


Figura 11: Añadir un grupo

    2) A continuación, ingresar un nombre para el nuevo grupo de dispositivos, y hacer *click* en Save.

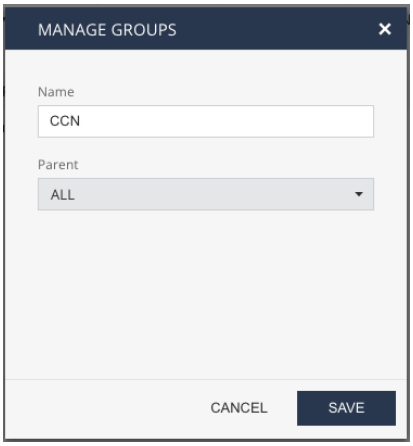


Figura 12: Añadir un grupo

45. Los dispositivos y grupos de dispositivos se importan desde la plataforma de Administración de Dispositivos Móviles (MDM) durante el proceso de integración con la misma. Las opciones *Agregar nuevo dispositivo* y *Agregar grupos* están deshabilitadas si se lleva a cabo la integración con un UEM/MDM. En caso de que no se haga uso de UEM/MDM, estas opciones estarán habilitadas para dar de alta dispositivos de forma local, tal y como se indica en el punto 5.4 AÑADIR UN NUEVO DISPOSITIVO.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

6.1.1. CREACIÓN DE PERFILES DE POLÍTICAS

46. Las políticas de seguridad permiten modelar el comportamiento típico de usuario y definir acciones que se consideran potencialmente peligrosas. La definición de políticas es un paso importante dado que estas determinan las alertas que van a ser generadas en el producto. Pueden ser de diferentes tipos, según el ámbito en el que apliquen. Harmony establece tres (3) grupos: políticas de dispositivo, políticas de aplicaciones y políticas de red.
47. **Como recomendación general de seguridad, se recomienda la creación de políticas lo más restrictivas posibles.**
48. Para crear un nuevo conjunto de políticas, se debe acceder a *Policy* > *Policy Profiles* y hacer *click* en AÑADIR (+). Se puede seleccionar *Crear una nueva política* o *Copiar* una existente (que no sea *Global Policy*). Finalmente, hacer *click* en *OK*.

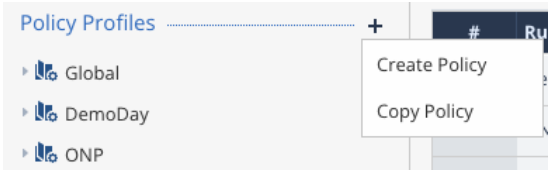


Figura 13: Crear una política

49. Una vez creada una política, esta puede ser editada desde la vista de edición de perfiles, o desde la lista de Perfiles de Políticas.
50. Para activar una política, ver el apartado siguiente.

6.1.2. BASE DE REGLAS (RULEBASE)

51. Cuando se accede por primera vez a la pestaña *Policy*, se puede ver una lista de reglas, asociadas al perfil de "*Política Global*".
52. A medida que se añaden nuevos perfiles de políticas (*Policy Profiles*), estos serán añadidos a la base de reglas, donde serán aplicados a los grupos de dispositivos adecuados.
53. Las reglas son procesadas en un orden de arriba hacia abajo. Una vez que hay una coincidencia en una regla, la política es aplicada al dispositivo. El resto de reglas serán ignoradas para ese dispositivo. **Se recomienda, por tanto, colocar las políticas más específicas en lo más alto de la lista, dejando la política más global en la base de la lista.**
54. Una vez creado el perfil (*Policy Profile*), se necesita crear una asociación entre Grupo y Política. Para ello, Ir a *Policy* > *Rulebase*. A continuación, se enumeran los pasos a seguir para activar una política y aplicarla a un grupo de dispositivos:

1) Hacer *click* en el botón "*+New*".
2) Introducir un nombre para la regla, seleccionar el dispositivo o grupo de dispositivos de la lista desplegable, seleccionar el perfil de política (*Policy Profile*), e introducir un comentario (si procede).
3) Hacer *click* en la marca al final de la regla para guardarla.
4) Para finalizar, hacer *click* en *Save*.
5) Para mover una regla, hacer *click* en el número de la regla, y arrastrarla hacia la posición adecuada.
6) Hacer *click* en *Save* para guardar los cambios o en *Discard* para deshacer los cambios.

55. Para más información, consultar el apartado "*Rulebase*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.2 CONFIGURACIÓN DE POLÍTICAS

6.2.1. POLÍTICAS DE DISPOSITIVO

56. En la pestaña *Device*, se puede establecer el nivel de riesgo y las condiciones de tiempo para políticas generales y específicas para Android e iOS.

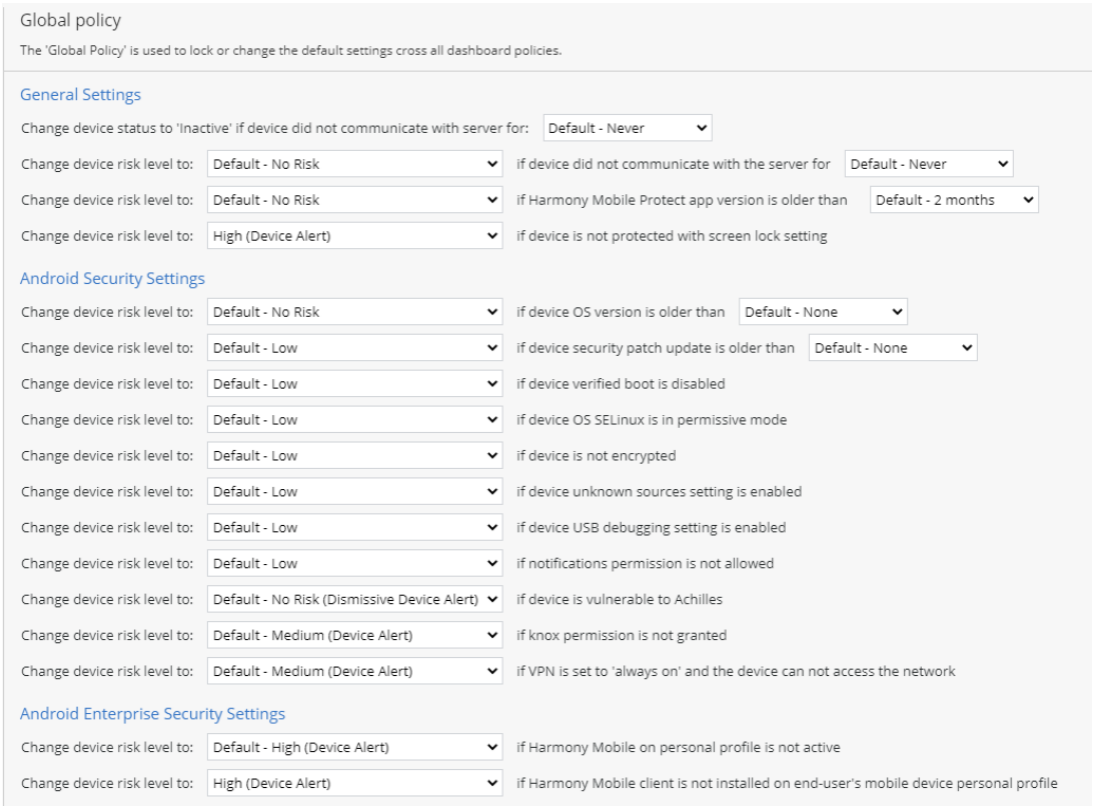


Figura 14: Políticas de dispositivo

57. Desde dicha pestaña, también es posible incluir en listas blancas las direcciones IP de servidores *proxy* asociados a la organización. Se muestra un ejemplo:

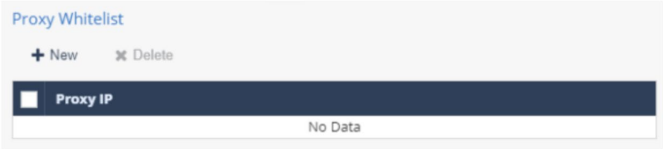


Figura 15: Lista blanca de Proxy

58. A continuación, se enumeran los pasos a seguir para añadir un nuevo *proxy* a la lista blanca:

    1) Hacer *click* en el botón [+].

    2) Una nueva ventana sobre la IP del proxy se abrirá:

Figura 16: Añadir dirección IP de Proxy

    3) Introducir la IP y hacer *click* en OK.

    4) Hacer *click* en *SAVE* para guardar los cambios en la política.

59. Para más información, consultar el apartado "*Device Policies*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.2.2. POLÍTICAS DE APLICACIONES

60. Las políticas de aplicaciones permiten establecer diferentes niveles de riesgos y clasificaciones entre las aplicaciones instaladas en dispositivos móviles. En la pestaña *Application*, se puede configurar el nivel de riesgo por aplicaciones.

61. Se puede obtener una descripción emergente de una aplicación seleccionada, dejando el cursor sobre [?]. A continuación, se enumeran los pasos a seguir para configurar el nivel de riesgo asociado a diferentes clasificaciones de aplicaciones:

    1) Seleccionar un nivel de riesgo de la ventana desplegable.

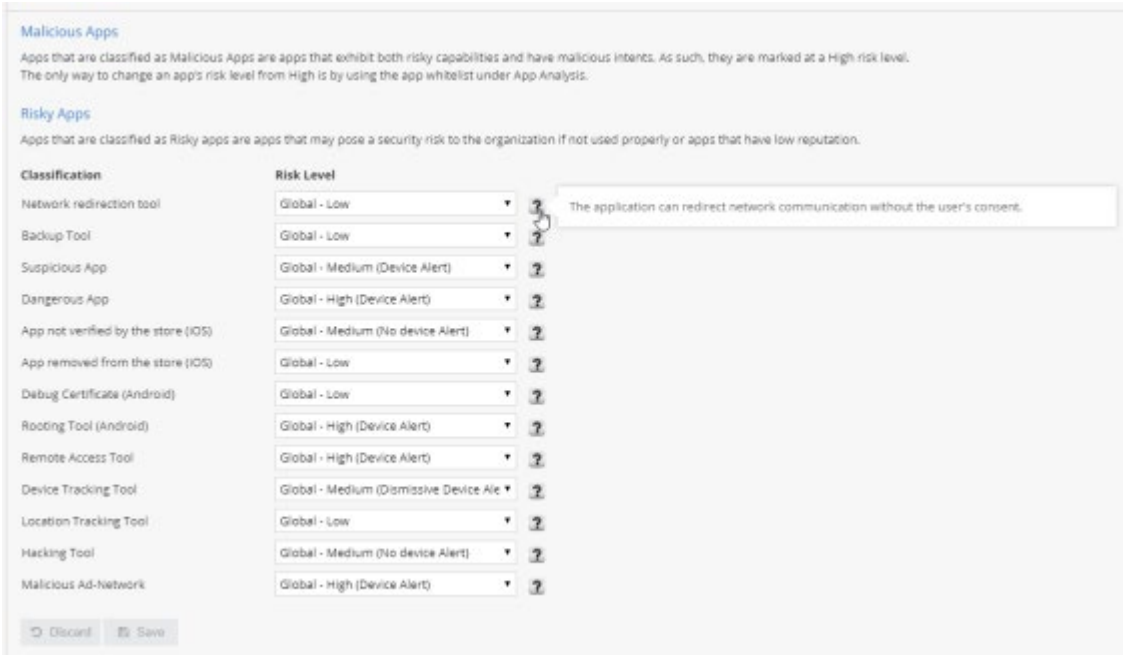


Figura 17: Políticas de Aplicaciones

2) Hacer *click* en *Save* para guardar los cambios en la política.

62. Para más información, consultar el apartado "*Application P*olicies", de la Guía de Administración de Harmony Mobile **[REF1]**.

63. Para editar la gestión de riesgos para una aplicación, seleccionar la opción *Edit* para la política que se desea editar.

64. A continuación, se enumera la lista de opciones para clasificar estas aplicaciones según el riesgo:

    a) *White Listed*: las aplicaciones incluidas en una lista blanca marcarán su nivel de riesgo como "*No Risk*". Dichas aplicaciones no activarán ninguna acción de mitigación ni avisos emergentes en el dispositivo.

    b) *Black Listed*: Las aplicaciones incluidas en listas negras pasarán a marcar su nivel de riesgo como "*High Risk*". Dichas aplicaciones activarán acciones de mitigación, así como avisos emergentes en el dispositivo

    c) *User Approval:* En este caso, tras la instalación de una aplicación, el usuario tendrá que introducir el nivel de riesgo de la misma, y podrá incluir dicha aplicación en una lista blanca o una lista negra para su dispositivo específico. La decisión tomada por el usuario no afectará a otros usuarios que instalen la misma aplicación.

6.2.3. POLÍTICAS DE RED (ON-DEVICE NETWORK PROTECTION)

65. En la pestaña *On-device Network Protection*, se puede mejorar la protección avanzada contra amenazas móviles de Harmony Mobile y establecer un nuevo paradigma de seguridad móvil para prevenir ataques emergentes a la red.

66. **Se deben configurar las protecciones avanzadas en el dispositivo de *Anti-Phishing*, Navegación segura, *Anti-Bot*, Acceso condicional y filtrado de URL.**

67. Se puede deshabilitar una política de protección, configurarla para que esté siempre activa (*Always ON*) o se active cuando el nivel de riesgo del dispositivo sea Alto (*Turn ON When a device is at HIGH risk*):

    - *Always ON*: La protección de red en el dispositivo está habilitada de forma predeterminada. La configuración avanzada en la ventana "*Configure*" dictará todo el comportamiento.
    - *Disabled*: Protección de red deshabilitada.
    - *Turn On when the device is at High Risk*: Cuando un dispositivo está en ALTO riesgo. En este estado, *ONP (On-device Network Protection)* se habilita automáticamente cuando el dispositivo entra en ALTO riesgo y se deshabilita automáticamente una vez que el dispositivo vuelve al estado normal.

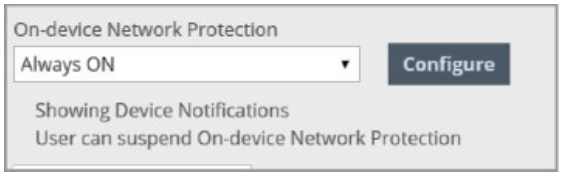


Figura 18: Configuración ONP

68. A continuación, se enumeran los pasos necesarios para aplicar el conjunto de condiciones que deben cumplirse para activar una política de protección:

    1) Seleccionar *Always O*n, o *Turn On when Device is at high Risk.*

    2) Hacer click en *Configure*. Se abrirá la ventana *Configure On-Device Network Protection*. Habrá que cubrir los parámetros que se presentan a continuación:

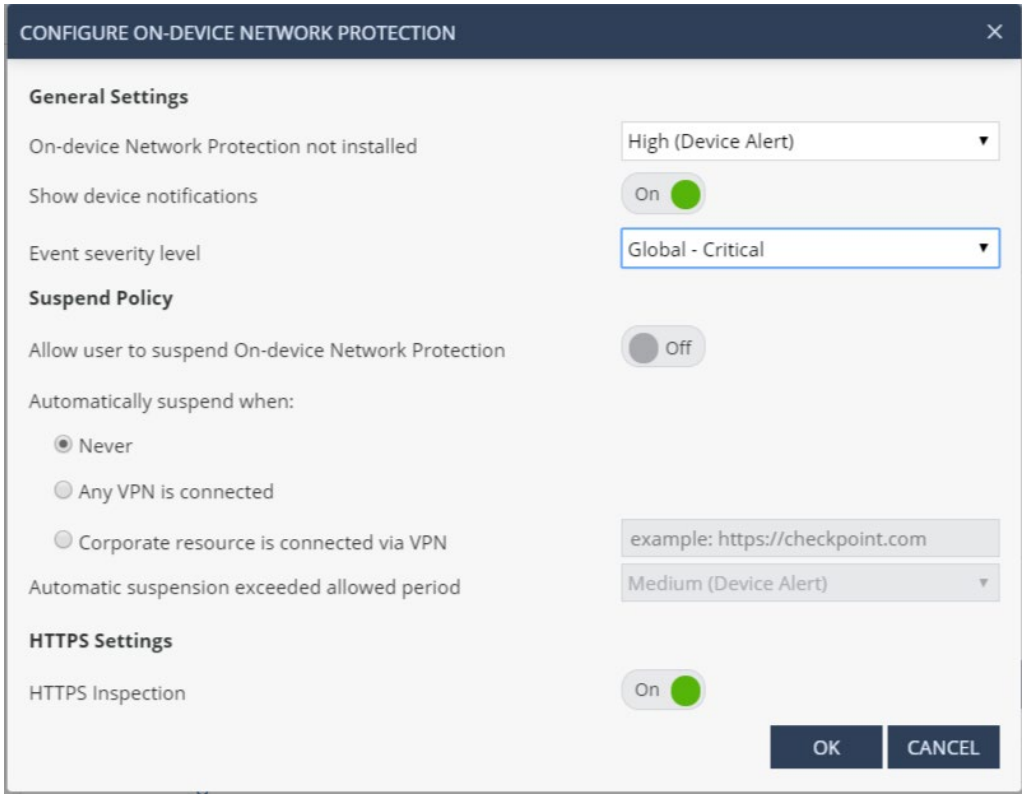


Figura 19: Configuración ONP

- *General Settings:*

OPCIÓN	DESCRIPCIÓN
On-Device Network Protection (ONP) not installed	Establecer el nivel de riesgo en caso de que se detecte que ONP no está instalado en el dispositivo: - Global - Medio (alerta de dispositivo) - Alto (alerta de dispositivo) - Medio (alerta de dispositivo) - Medio (sin alerta de dispositivo) - Medio (alerta de dispositivo despreciable) - Bajo - Sin riesgo
Show device notifications	Mostrar notificación en el dispositivo si un recurso de red está bloqueado (ON/OFF). Si el recurso de red está bloqueado, se mostrará una alerta/notificación en la App de Harmony Mobile indicando este bloqueo. Si esta opción está marcada como OFF, no se recibirá ninguna alerta/notificación en la App.

OPCIÓN	DESCRIPCIÓN
Event Severity Level	Configurar los niveles de riesgo de los eventos generados por la protección de red en el dispositivo: - Global – Crítico - Crítico - Advertencia - Información

Tabla 3: *General Settings* de ONP

- *Suspend Policy*

OPCIÓN	DESCRIPCIÓN
Allow user to suspend On - device Network Protection	La suspensión del servicio ONP por parte del usuario está deshabilitada cuando la protección de red en el dispositivo está configurada en ***Turn On when Device is at high Risk*:** On/Off
Automatically suspend when	- Nunca - Suspender ONP de forma automática cuando se detecta una VPN adicional. - Cuando se produce una conexión a un recurso corporativo: ONP se suspenderá si se detecta otra VPN, y a través de esta VPN se accede a un recurso corporativo.
Automatic suspension exceeded allowed period	Habilitado solo cuando la opción "*El recurso corporativo está conectado a través de VPN*" está habilitado por un tiempo excesivo, y se considera que el período de tiempo durante el cual ONP ha permanecido desconectado se considera un riesgo. Por defecto, ONP emite una alerta si ha permanecido desconectado durante 20 horas en una ventana de tiempo de 24 horas.

Tabla 4: Suspend Policy

- *HTTPS Settings*

OPCIÓN	DESCRIPCIÓN
HTTPS Inspection	Extiende las capacidades de protección de red en el dispositivo a las comunicaciones HTTPS.

Inspection CA	*On-Device Network Protection* necesita instalar un certificado de Autoridad de Certificación (CA) para inspeccionar el tráfico HTTPS. Esta instalación se puede realizar de forma manual por el usuario final, o a través de un gestor central de dispositivos móviles (MDM). La propia App proporciona los pasos a seguir para la instalación de dicho certificado.

Tabla 5: Opciones de HTTPS

69. Para más información, se recomienda consultar el apartado "*On-device Network Protection Policies*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.3 AUTENTICACIÓN

70. El producto implementa la autenticación de usuarios mediante usuario y contraseña.
71. Asimismo, el producto, a través del *Infinity Portal*, ofrece la posibilidad de establecer **autenticación de doble factor (2FA), opción recomendada**.
72. Adicionalmente, el producto ofrece la posibilidad de autenticación empleando proveedores de identidad externos.

6.3.1. AUTENTICACIÓN DE DOBLE FACTOR (2FA)

73. Para añadir una capa adicional de seguridad en el proceso de autenticación, se debe habilitar la autenticación de doble factor. Para ello, se emplea un *token* generado de 6 dígitos. Este *token* debe ser introducido junto con la contraseña para confirmar la identidad del usuario.
74. Es posible utilizar una de las siguientes aplicaciones, y escanear un código QR para enlazarlas con el *Check Point Infinity Portal*:
    a) *Google Authenticator*
    b) *Microsoft Authenticator*
    c) *Authy*
75. A continuación, se enumeran los pasos a seguir para habilitar la autenticación de doble factor:
    1) Ir a *Profile Settings > Two-factor Authentication*, y poner el botón en *ON*.

       Se abrirá la ventana de configuración.
    2) Seguir las instrucciones indicadas para conectar la aplicación de autenticación seleccionada con *Check Point Infinity Portal*.
    3) Hacer *click* en *Finish* para cerrar la ventana de configuración.

Nota: En caso de perder el acceso a la aplicación empleada para la autenticación de doble factor, será necesario ponerse en contacto con el *Centro de Soporte de Check Point*.

76. Para más información, se recomienda consultar el apartado "*Two-Factor Authentication"*, de la Guía de Administración de Infinity Portal **[REF3]**.

6.4 ADMINITRACIÓN DEL PRODUCTO

6.4.1. ADMINISTRACIÓN LOCAL Y REMOTA

77. La administración de la solución se lleva a cabo a través del *Harmony Mobile Management Dashboard*, una interfaz web basada en la nube, alojada en *Check Point Infinity Portal*.

78. Este panel de control permite la administración, aprovisionamiento y monitorización de dispositivos, políticas de seguridad, eventos, alertas y análisis forense de dispositivos móviles.

6.4.2. CONFIGURACIÓN DE ADMINISTRADORES

6.4.2.1. CONFIGURACIÓN DE ROLES DE ADMINISTRACIÓN ESPECÍFICOS

79. A continuación, se enumeran los pasos a seguir para la creación de roles de administración específicos para la aplicación Harmony Mobile, restringidos a grupos y perfiles de políticas específicos:

    1) Ir a *Settings > Administrators > Security Group Roles.*
    2) Hacer click en *+New* y seleccionar:
        a. Nombre del rol
        b. Seleccionar entre las opciones: *Group Security Manager* o *Group Security Manager Viewer.*
        c. Seleccionar los grupos de dispositivos a los que el administrador podrá acceder.
        d. Seleccionar los perfiles de políticas (*Policy Profiles*) a los que el administrador podrá acceder.

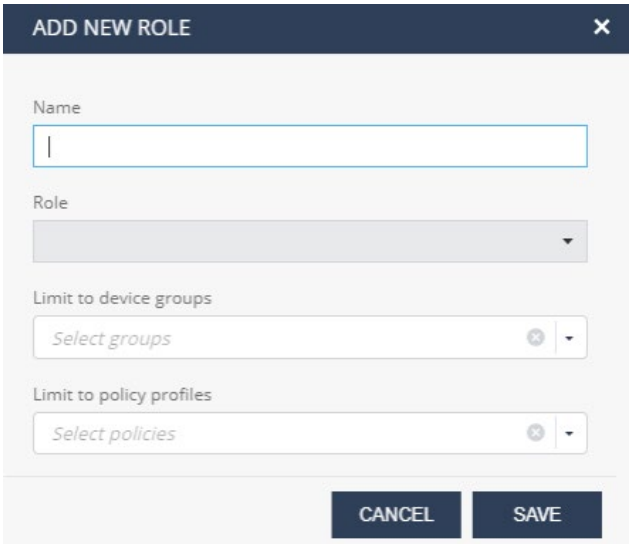


Figura 20: Añadir un nuevo rol

80. Una vez creado, este nuevo rol estará disponible desde la opción *Specific Harmony Mobile roles*, cuando se cree un nuevo usuario Administrador desde el *Infinity Portal*. Estos roles específicos solo estarán disponibles para realizar operaciones de gestión en el servicio Harmony Mobile.
81. Otros roles de administración están disponibles, como *Basic Support* o *Device Administrator*. Más información acerca de estos roles puede ser consultada en la pestaña *Settings > Administrators > Roles Definitions.*
82. Para más información, consultar el apartado "Administrators", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.4.3. CONFIGURACIÓN DE ROLES DE ADMINISTRACIÓN GLOBALES

83. Desde la página Users de la interfaz web de Infinity Portal, se puede ver un listado de todos los usuarios configurados en la cuenta de Infinity Portal.
84. Hay dos (2) tipos de roles de usuario en Infinity Portal: Roles Globales (*Global Roles*), y Roles de Servicios Específicos (*Specific Service Roles*):
    a) Roles Globales: estos roles aplican a la plataforma Infinity Portal, y a todos los servicios asociados a esta plataforma. No es posible asignar múltiples roles a un mismo usuario.
        i. *Admin*: otorga permisos de lectura y escritura sobre todos los servicios asociados a la cuenta de Infinity Portal. Cuando un nuevo servicio es activado en dicha cuenta, un usuario con Rol Global *Admin* adquiere automáticamente permisos de lectura y escritura para este servicio.
        ii. *Read-Only*: otorga permisos de solo-lectura para todos los servicios accesibles desde la cuenta de Infinity Portal. Cuando un nuevo servicio es activado en dicha cuenta, un usuario con Rol Global

Read-Only adquiere automáticamente permisos de lectura y escritura para este servicio.

iii. *User Admin*: permite la gestión de todos los aspectos relacionados con usuarios, grupos de usuarios y roles asociados a la cuenta de Infinity Portal. Únicamente administradores con Rol Global de *User Admin* pueden acceder a las pestañas Users y *User Groups*, así como asignar roles a usuarios y grupos de usuarios. Administradores con rol de *Admin*, pero no rol de *User Admin* no pueden acceder a dichas pestañas.

b) Roles de Servicios Específicos: Estos roles se aplican únicamente a un servicio específico. Hay dos (2) tipos de roles de servicio:

i. Roles de servicio por defecto: roles específicos de cada servicio. Estos roles forman parte de la configuración inicial del producto.

ii. Roles personalizados: estos roles son creados por el usuario a través de la interfaz gráfica (GUI). Estos roles solo son aplicables a la cuenta en la que han sido creados.

85. Algunos servicios soportan la asociación de múltiples roles a un mismo usuario, mientras que otros soportan únicamente la asociación de un único rol a un mismo usuario.

86. Para más información, se recomienda consultar el apartado "User Roles", de la Guía de Administración de Infinity Portal **[REF3]**.

6.4.3.1. POLÍTICA DE CONTRASEÑAS

87. A la hora de crear un nuevo usuario a través de *Infinity Portal*, se le debe asociar una **contraseña que cumpla con los siguientes requisitos**:

a) La contraseña debe tener una longitud mínima de 10 caracteres.

Nota: Por motivos de seguridad**, se recomienda emplear una longitud mínima de 12 caracteres.**

b) La contraseña debe tener, al menos, un carácter en minúscula.

c) La contraseña debe tener, al menos, un carácter en mayúscula.

d) La contraseña debe tener, al menos, un número.

e) La contraseña debe tener, al menos, un carácter especial.

88. Es necesario indicar que las contraseñas asociadas a usuarios locales de *Infinity Portal* no tienen fecha de expiración por caducidad. **Por ello, se debe establecer un procedimiento manual de actualización de contraseñas. Se recomienda que estas deben actualizarse, como mucho, cada 60 días.** En caso de que se haga uso de proveedores de identidad (IdP)/ *Single-Sign On (SSO),* la caducidad de las contraseñas estará sujeta a las configuraciones establecidas en dichos elementos.

89. A continuación, se enumeran los pasos a seguir para cambiar contraseñas de usuario, desde el contexto de Infinity Portal:

    a) En la página *Profile Settings*, ir a *Change Password > Change.*

    b) En la ventana *Change Password*, introducir la contraseña antigua.

    c) Introducir una contraseña nueva, y a continuación confirmar el cambio.

    Nota: La nueva contraseña debe respetar los parámetros definidos en la política de contraseñas.

    d) Hacer click en *Apply*.

    Nota: Esta contraseña es válida para todos los servicios accesibles desde el *Check Point Infinity Portal*.

90. Para más información, consultar el apartado "*User Password*", de la Guía de Administración de Infinity Portal **[REF3]**.

6.4.3.2. CONFIGURACIÓN DE PARÁMETROS DE SESIÓN

91. Desde la pantalla *Global Settings > Account Settings*, ubicada en el *Infinity Portal*, es posible configurar diferentes parámetros que afectan a las sesiones de los usuarios.

    - *Force Login After*: establece el tiempo de sesión tras el que el usuario debe identificarse de nuevo. Este tiempo de sesión es configurable, y puede establecerse a uno de los siguientes valores:
        - 12 horas
        - 1 día (valor por defecto)
        - 7 días
        - 1 mes

      Nota: Por motivos de seguridad**, se recomienda establecer el menor tiempo posible.**

    - *Idle Session Timeout After:* Establece el tiempo de inactividad del usuario tras el cual será necesario que este vuelva a autenticarse. Este valor es configurable, y puede establecerse a uno de los siguientes valores:
        - 5 minutos
        - 15 minutos
        - 30 minutos
        - 1 hora
        - 3 horas
        - 6 horas
        - 12 horas (valor por defecto)

Nota: Por motivos de seguridad**, se recomienda establecer el tiempo de inactividad en, como máximo, 5 minutos**.

92. Para más información, consultar el apartado "*Account Settings*", de la Guía de Administración de Infinity Portal **[REF3]**.

6.5 SERVIDORES DE AUTENTICACIÓN

6.5.1. AUTENTICACIÓN CON SINGLE SIGN-ON (SSO)

93. El producto ofrece la posibilidad de configurar la autenticación con *Single Sign-On* con proveedores de identidad conocidos, o integrarlos con *Duo*, que proporciona autenticación de doble factor.

6.5.1.1. CONFIGURACIÓN CON PROVEEDORES DE IDENTIDAD

94. A continuación, se enumeran los pasos a seguir para habilitar la configuración con *Single Sign-On:*

    1) Ir a *Global Settings > Account Settings*

    2) En *SSO Authentication*, hacer click en *Set up single sign-on.*

    Se abrirá la ventana de configuración.

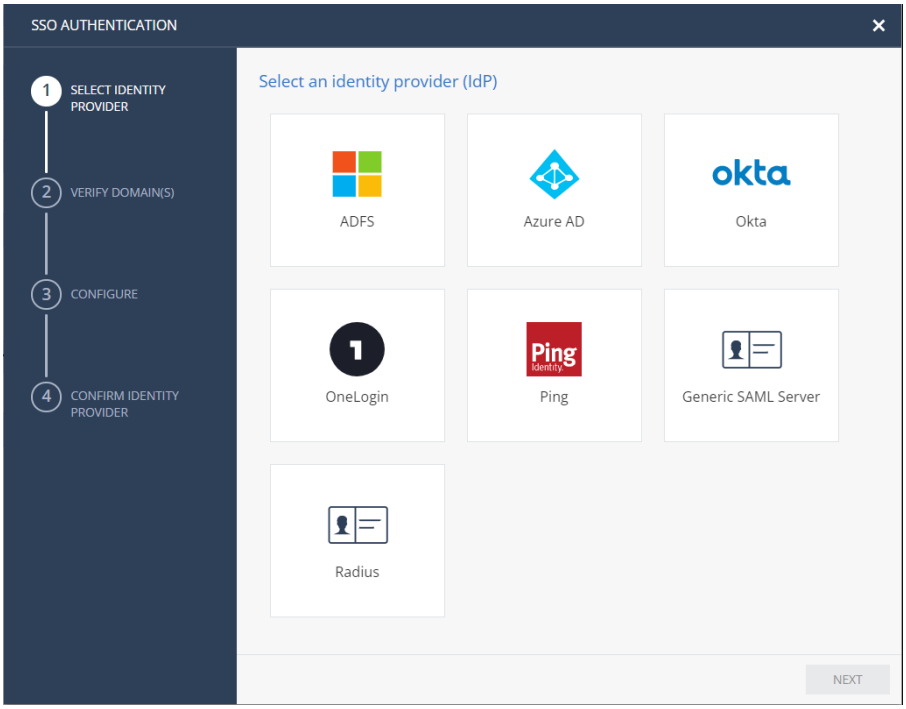


Figura 21: Ventana de selección de Proveedor de Identidad

    3) Seleccionar el proveedor de identidad deseado, y hacer *click* en *Next*.
    4) Seguir las instrucciones para completar la configuración.

95. Una vez completada la configuración, se podrá ver una "tarjeta" con el nombre del proveedor de identidad, el estado de autenticación, y el dominio.

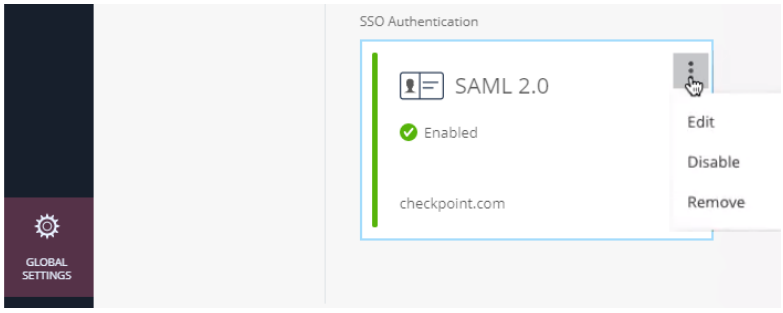


Figura 22: Tarjeta del proveedor de identidad

96. A continuación, se enumeran los pasos a seguir para modificar los datos existentes de autenticación con *Single Sign-On*:

    a) Seleccionar *Edit* para editar los detalles del proveedor de identidad.

    Nota: Cuando se modifica una configuración existente, *Infinity Portal* envía un aviso indicando que, tras aplicar los cambios, se desconectará a los usuarios conectados mediante acceso remoto.

    b) Seleccionar *Disable* para deshabilitar la autenticación con *Single Sign-On*. Los detalles de autenticación con SSO permanecerán en el sistema. Este tipo de autenticación podrá volver a ser habilitado en caso de ser necesario.

    c) Seleccionar *Remove* para eliminar una configuración con SSO existente. Si se lleva a cabo la configuración con otro proveedor de identidad, *Infinity Portal* no guardará la información del proveedor de identidad anterior.

97. En la Guía de Administración de Infinity Portal **[REF3]** se ofrece información sobre la configuración de autenticación con *Single Sign-On*, empleando diferentes proveedores de identidad:

    - *Microsoft AD FS*
    - *Microsoft Azure AD*
    - *Okta*
    - *OneLogin*
    - *Ping Identity*
    - *Generic SAML Server*
    - *RADIUS*

6.5.1.2. CONFIGURACIÓN DE AUTENTICACIÓN CON RADIUS

98. Antes de iniciar la configuración de autenticación SSO con RADIUS, es necesario asegurarse de llevar a cabo el *login* con el mismo usuario o email empleado para crear la cuenta. Esto permite la creación de un "usuario de fallback" que permite

llevar a cabo el proceso de *login*, independientemente de la disponibilidad de servidores RADIUS.

99. El usuario que creó la cuenta es denominado *Primary Administrator*. *Infinity Portal* nunca autentica a este usuario a través de RADIUS SSO. Esta medida se aplica para evitar que esta cuenta quede bloqueada para todos los usuarios debido a un fallo de los servidores RADIUS.

100. A continuación, se enumeran los pasos a seguir para configurar la autenticación SSO con RADIUS:

    1) Ir a Global Settings > Account Settings.
    2) En SSO Authentication, hacer *click* en *Set up single sign-on*.

       Se abrirá la pantalla de configuración de *SSO Authentication*.
    3) Seleccionar RADIUS y hacer click en *Next*.
    4) Seguir las instrucciones para completar la configuración.
    5) Verificar los dominios.

       Es necesario verificar la propiedad del dominio para asegurar la identificación exitosa para todos los usuarios que pertenecen a la organización.

        a) Copiar el valor de registro de DNS.
        b) Introducir el valor del servidor DNS como un registro de texto.
        c) En *Domain*(s), introducir uno o más dominios de correo electrónico empleados por la organización
        d) Cuando todos los dominios aparezcan en la lista, hacer *click* en *Next*.
    6) Configurar los servidores RADIUS.

        a) En la página *Configure Servers*, introducir los detalles de los servidores RADIUS:

            - *Primary Host IP*: introducir la dirección IP del servidor.
            - *Primary Host Secret*: Introducir el secreto del servidor.
            - *Port*: usar el puerto de RADIUS por defecto, o cambiar dicho valor de ser necesario.
            - *Add Another Host*: opcionalmente, es posible añadir un servidor RADIUS secundario para proveer una opción de alta disponibilidad, en caso de que el servidor primario no pueda ser alcanzado. Ambos servidores emplearán el mismo puerto. Introducir la dirección IP y el secreto de este servidor.

- *Connectivity Test*: opcionalmente, es posible comprobar la conexión con el servidor RADIUS:
  - Introducir el usuario
  - Introducir la contraseña del usuario
  - Hacer click en *Test connectivity*.

    Aparecerá un mensaje indicando la conexión exitosa con el servidor RADIUS.

b) Hacer click en *Next*.

7) Confirmar el Proveedor de Identidad.

Revisar los detalles de la configuración, y hacer click en *Submit*.

101. Para más información, consultar el apartado "*SSO Authentication*" de la Guía de Administración de Infinity Portal **[REF3]**.

6.5.1.3. INTEGRACIÓN SSO CON DUO

102. Duo proporciona un nivel adicional de seguridad a la autenticación *Single Sign-On* con proveedores de identidad.

103. Para más información sobre el proceso de integración, consultar el apartado *"SSO Integration with Duo*", de la Guía de Administración de Infinity Portal **[REF3]**.

6.6 GESTIÓN DE CERTIFICADOS

104. La aplicación se comunica con el servidor empleando el protocolo HTTPS, con un certificado de servidor firmado por una Autoridad de Certificación (CA). El certificado emplea claves RSA de longitud de 2048 bits para autenticación e intercambio de claves, para establecer una clave de sesión de 256 bits. La longitud de las claves RSA no puede ser modificada, al tratarse de una comunicación cifrada y encapsulada entre la aplicación y la plataforma Cloud de Check Point. Las sesiones HTTPS son cifradas empleando el algoritmo AES -256.

105. Para más información, se recomienda consultar el apartado "*Infrastructure – Infrastructure Security*", del documento "*Check Point SandBlast Mobile Data Privacy and Handling*" **[REF9].**

6.7 AUDITORÍA

106. **Los registros de auditoría deben ser configurados para que aporten la máxima información posible.** La configuración de la auditoría se realiza en la pestaña *Events & Alerts*, a la que se accede desde el panel principal de administración de Harmony Mobile. Muestra un registro de incidentes y acciones ocurridas en los dispositivos, por ejemplo, instalación de aplicaciones, perfiles detectados en los dispositivos, etc.

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

Figura 23: Panel de eventos y alertas

107. Para más información al respecto, consultar el apartado "*Events and Alerts*", de la Guía de Administración de Harmony Mobile **[REF1]**.

108. En la pestaña *Network* se muestran los eventos de red registrados. Esta pestaña proporciona una visión más granular de los eventos de la red. Se muestran los siguientes eventos de red:

a) *SSL Stripping*: Un agente de terceros ha interceptado el tráfico, y lo ha degradado de HTTPS a HTTP.

b) *SSL Interception (Basic):* Un agente de terceros ha interceptado el tráfico y se hizo pasar por el solicitante original hacia el servidor destino, mientras controla las respuestas enviadas al solicitante legítimo.

c) *SSL Interception (Advanced):* Similar al caso anterior, pero en este caso las respuestas del impostor fueron cifradas con un certificado SSL emitido por una Autoridad de Certificación que el dispositivo afectado considera como entidad de confianza.

d) *Captive Portal Redirection*: el tráfico del dispositivo es redirigido a un portal cautivo para su registro en la red.

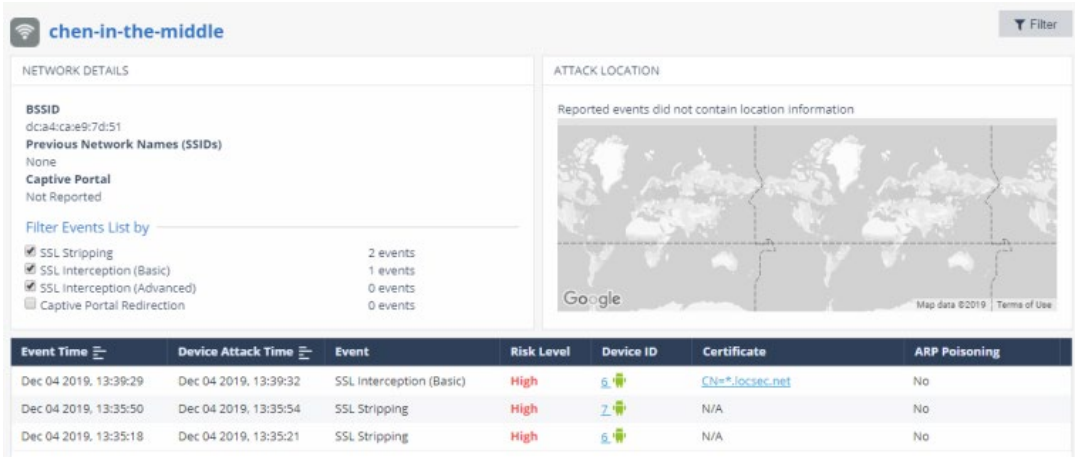


Figura 24: Eventos de red reportados

109. Para más información, consultar el apartado "*Network*" de la Guía de Administración de Harmony Mobile **[REF1]**.

6.7.1. ALMACENAMIENTO REMOTO

6.7.1.1. INTEGRACIÓN CON SYSLOG

110. **Se recomienda configurar Syslog para que el producto remita los logs a un servidor remoto.** El producto ofrece esta posibilidad a través del envío de logs desde el

dashboard. Este componente debe comunicarse con el servidor *Syslog* remoto a través del *firewall* de la organización. Las direcciones IP de origen pueden ser localizadas en el documento *Check Point SandBlast Mobile Communication Information Guide* **[REF10]**.

111. Se deben también introducir los siguientes valores:

a) *Host Name: Hostname* o dirección IP del servidor *Syslog*.

b) *Protocol*: UDP o TCP.

c) *Port*: El puerto en el que está escuchando el servidor *Syslog*.

d) *Syslog Level*: El nivel de severidad de los eventos a enviar al servidor remoto. Los valores aceptados son: *Info, Warn, Error* y *Debug*.

e) *Facility*: se emplea para especificar el tipo de programa que está logueando el mensaje.

112. Hacer click en *Apply*.

113. Para más información, se recomienda consultar el apartado "*Security Posture integration"*, de la Guía de Administración del producto **[REF1]**.

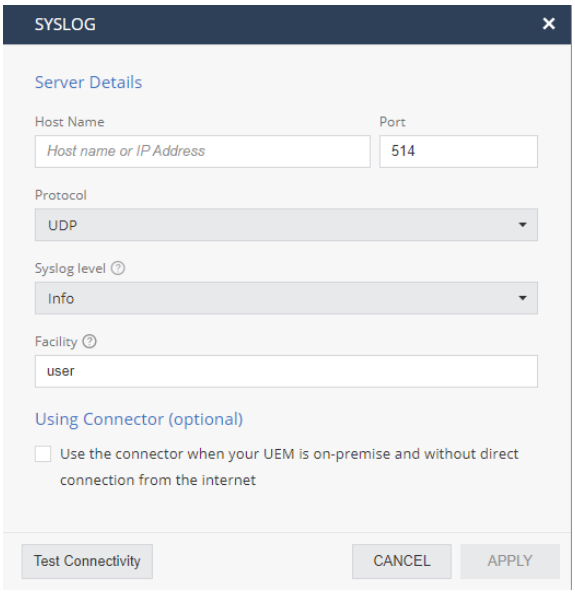


Figura 25: Integración con servidor Syslog remoto

114. Asimismo, desde *Infinity Portal*, desde la página "*Audits*", es posible rastrear las acciones llevadas a cabo por los usuarios con perfil de Administrador.

115. A continuación, se enumeran los pasos a seguir para ver la información de auditoría:

1) Ir a *Global Settings > Audits.*

2) Hacer click en el botón *Refresh* para ver los registros de auditoría actualizados:

- Severidad - Niveles de severidad: *Notice, Info, Warning, Critical*.
- Usuario – Descripción del usuario.

- Fecha – La fecha de creación del registro de auditoría.
- Servicio – El servicio de Infinity Portal en el que la acción se ha llevado a cabo.
- Categoría – Quien llevó a cabo la acción
- Tipo de acción.

116. Para más información, consultar el apartado "*Audits*", así como el apartado "*Syslog integration*", de la Guía de Administración de Infinity Portal **[REF3]**.

6.7.1.2. INTEGRACIÓN CON RSYSLOG

117. Para la integración con *Rsyslog*, se recomienda consultar el apartado "*RSyslog integration*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8 FUNCIONES DE SEGURIDAD

6.8.1. ANTI-PHISHING

118. *Harmony Mobile On-Device Network Protection* evita los ataques de *phishing* en cualquier aplicación de correo electrónico o mensajería instalada en el dispositivo móvil, al detectar y bloquear instantáneamente las URL maliciosas al hacer clic, sin importar cómo se entregó la URL.

119. La capacidad *Anti-Phishing* está impulsada por *ThreatCloud*, una red colaborativa y base de conocimiento que brinda inteligencia de seguridad dinámica en tiempo real.

120. Esta categoría incluye URLs que normalmente llegan en aplicaciones de mensajería o correo electrónico y se establecen para robar información de los usuarios.

121. ***La función de Anti-Phishing* debe habilitarse**. Para ello:

1) Ir a *Policy* y a continuación, seleccionar *Policy Profile > On-device Network Protection > Content Inspection*
2) En la sección *Block Connections to Phishing & Malicious Sites*, habilitar *Phishing*.

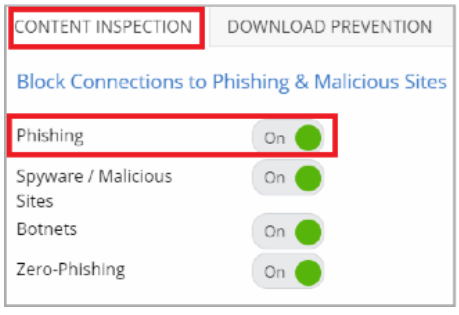


Figura 26: Habilitar *Anti-Phishing*

122. Para más información, consultar el apartado "*Content Inspection*", de la Guía de Administrador de Harmony Mobile **[REF1]**.

6.8.2. SAFE BROWSING

123. *Harmony Mobile On-device Network Protection* evita el acceso a sitios web maliciosos en cualquier aplicación de navegación, al bloquear el acceso a los sitios en función de la inteligencia de seguridad dinámica proporcionada por *ThreatCloud*.

124. Además, también evita que los usuarios visiten involuntariamente sitios web maliciosos en los que el dispositivo puede infectarse con malware no deseado.

125. Para que el usuario se beneficie de esta protección, debe habilitarse la funcionalidad de *Safe Browsing.* Para ello, se deben seguir los siguientes pasos:

    1) Ir a *Policy*, y a continuación seleccionar *Policy Profile > On-device Network Protection > Content Inspection*

    2) En la sección *Block Connections to Phishing & Malicious Sites,* habilitar *Spyware/Malicious Sites*.

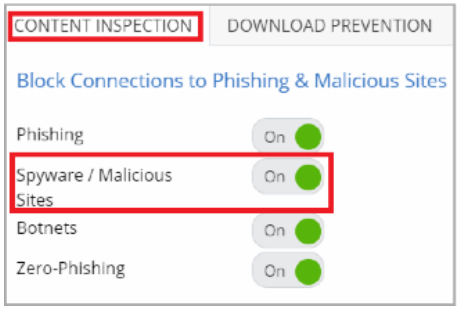


Figura 27: Habilitar *Safe Browsing*

126. Para más información, consultar el apartado "*Content Inspection*", de la Guía de Administrador de Harmony Mobile **[REF1]**.

6.8.3. ANTI-BOT

127. La función de Harmony Mobile, *Anti-Bot* extiende la tecnología Check Point Anti-Bot a los dispositivos móviles. Esta funcionalidad detecta dispositivos infectados por bots y bloquea automáticamente todas las comunicaciones con los servidores de comando y control (C&C) y otros servidores maliciosos, evitando de esta manera la filtración de datos confidenciales.

128. Esta categoría incluye URL, direcciones IP o nombres de dominio que usan bots, incluidos sitios de "*Comando y Control*" que facilitan el robo de información personal y corporativa en el dispositivo, grabar video o audio y / o instalar otro código malicioso.

129. La funcionalidad de anti-bot debe estar activada. Para ello:

    1) Ir a *Policy*, y a continuación, seleccionar *Policy Profile > On-device Network Protection > Content Inspection*

    2) En la sección *Block Connections to Phishing & Malicious Sites*, habilitar *Botnets*.

130. Para más información, se recomienda consultar el apartado "*Content Inspection*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8.4. ZERO-PHISHING PROTECTION

131. *Harmony Mobile On-Device Network Protection* evita los ataques de *phishing* en cualquier aplicación de correo electrónico o mensajería al detectar y bloquear instantáneamente las URL maliciosas al hacer clic, sin importar cómo se entregó la URL.

132. *Zero-Phishing* es una tecnología Check Point para identificar sitios web de *phishing* desconocidos, analizando cada uno de los elementos que componen el sitio web (Favicon, reputación de IP, reputación de dominio, similitud con otros sitios webs, etc) y prevenir ataques de *phishing*.

133. Esta funcionalidad *Zero-Phishing* debe estar habilitada para evitar estos ataques. Para ello:

    1) Ir a *Policy*, y a continuación, seleccionar *Policy Profile > On-device Network Protection > Content Inspection*

    2) En la sección *Block Connections to Phishing & Malicious Sites*, habilitar *Zero-Phishing*.

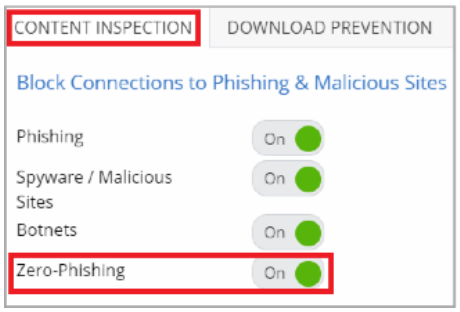


Figura 28: Habilitar *Zero-Phishing*

134. Para más información, consultar el apartado "*Content Inspection*", de la Guía de Administrador de Harmony Mobile **[REF1]**.

6.8.5. ACCESO CONDICIONAL

135. La función de Acceso Condicional permite que una organización controle automáticamente el acceso a los recursos corporativos, de forma que, si un dispositivo está expuesto a un ataque, se controlará el acceso a las redes corporativas o cualquier aplicación local o en la nube.

136. La aplicación de esta política es independiente de las soluciones *Unified Endpoint Management* (UEM).

137. Esta funcionalidad establece una lista de direcciones IP corporativas y/o nombres de host FQDN a los que un dispositivo de usuario con un nivel de riesgo alto no puede acceder.

138. A continuación, se enumeran los pasos a seguir para habilitar la funcionalidad de Acceso Condicional:

1) Ir a *Policy*, y a continuación seleccionar *Policy Profile > On-device Network Protection > Content Inspection > Conditional Access*.

Figura 29: Habilitar Acceso Condicional

2) Hacer click en *New* [+].

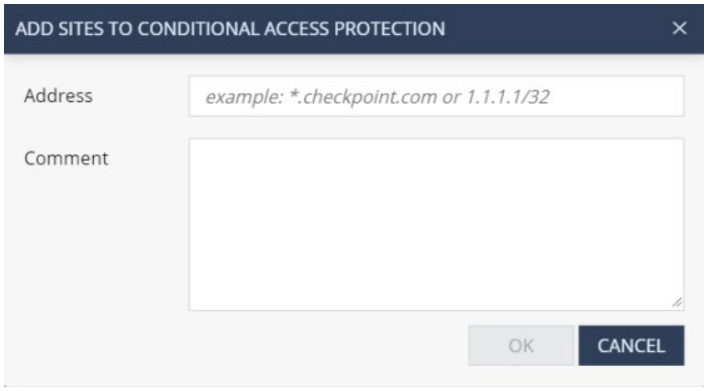


Figura 30: Habilitar Acceso Condicional

3) En la ventana emergente, indicar la IP o FQDN del recurso corporativo a bloquear cuando un dispositivo esté comprometido.

139. Para más información, consultar el apartado "*Content Inspection*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8.6. URL FILTERING

140. La función de filtrado de URL de Harmony Mobile evita el acceso a sitios web basados en categorías inapropiadas para las políticas corporativas de la organización. Esta categoría permite al administrador prohibir que los dispositivos accedan a URL particulares en una categoría temática específica, como juegos de azar, armas y violencia, etc. El filtrado de URL aplica políticas en los dispositivos móviles en todas las aplicaciones del navegador y en todas las aplicaciones que no son específicas del navegador, como Facebook Messenger, Slack, WhatsApp y otras.

141. La tecnología de filtrado URL de Harmony Mobile permite incluir dominios en listas negras y blancas. **Se recomienda la configuración del filtrado URL, a ser posible, a través de listas blancas. En caso de no resultar práctico, se recomienda la utilización de listas negras lo más restrictivas posibles.**

142. Cuando el filtrado URL se combina con *On-device Network Protection > Always ON > Allow user to suspend On-device Network Protection,* el usuario puede deshabilitar ONP durante un período de tiempo específico (tiempo configurable a 5 minutos, 30 minutos o 2 horas), para que pueda acceder a sitios web / categorías bloqueadas. Esta capacidad permite cierta flexibilidad en un entorno BYOD (*Bring Your Own Device*). Sin embargo, el usuario no puede suspender ONP si su dispositivo tiene un nivel de riesgo ALTO, y si durante la suspensión el dispositivo se mueve a riesgo ALTO, el acceso condicional aún se aplica.

143. A continuación, se enumeran los pasos a seguir para habilitar *URL Filtering*:

1) Ir a *Policy*, y a continuación seleccionar *Policy Profile > On-device Network Protection > URL Filter Categories*.

2) Hacer click en *Edit*.

Figura 31: Habilitar *URL Filtering*

3) En la ventana emergente, seleccionar las categorías a las que desea bloquear el acceso y hacer clic en ">" para mover las categorías seleccionadas a la lista de bloqueo en el lado derecho.

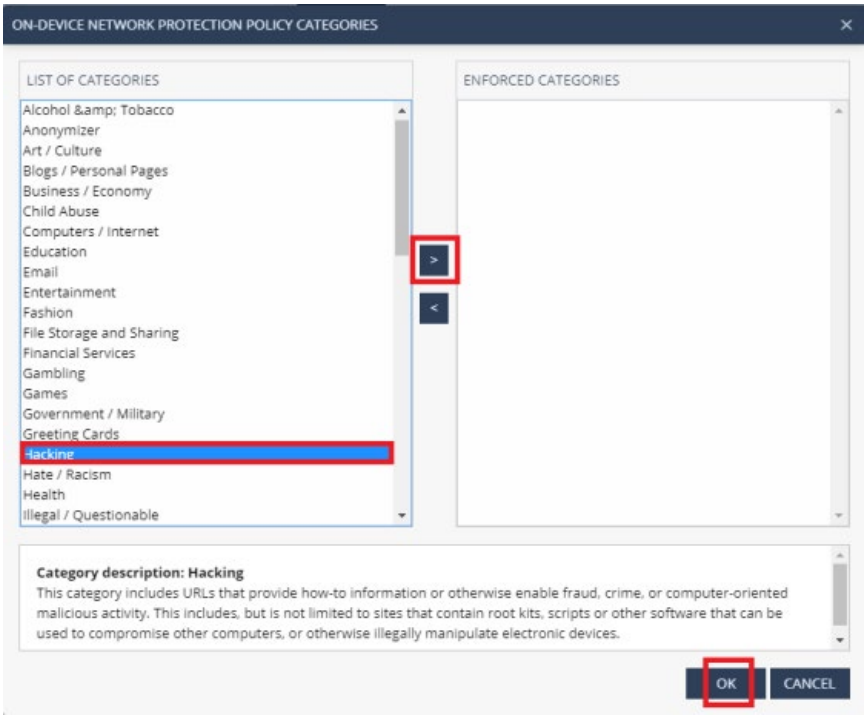


Figura 32: Añadir categorías a URL Filtering

Como se puede observar en la anterior figura, cada categoría tiene una descripción en la parte inferior de la pantalla.

4) Hacer click en *OK*.

144. El administrador puede decidir bloquear estas categorías, pero no rastrear cuándo ocurren tales eventos por categoría. Es posible decidir no realizar un seguimiento de dichos eventos por motivos de privacidad del usuario.

145. De forma predeterminada, la acción de filtrado de URL muestra una notificación emergente en el dispositivo cliente con una nueva tarjeta de evento en el "*Centro de eventos*" de la aplicación *Harmony Mobile Protect*. En caso de que el administrador desmarque la opción "Mostrar eventos en el cliente", el usuario final solo verá la URL de la página bloqueada dentro de un navegador cuando se acceda a ella.

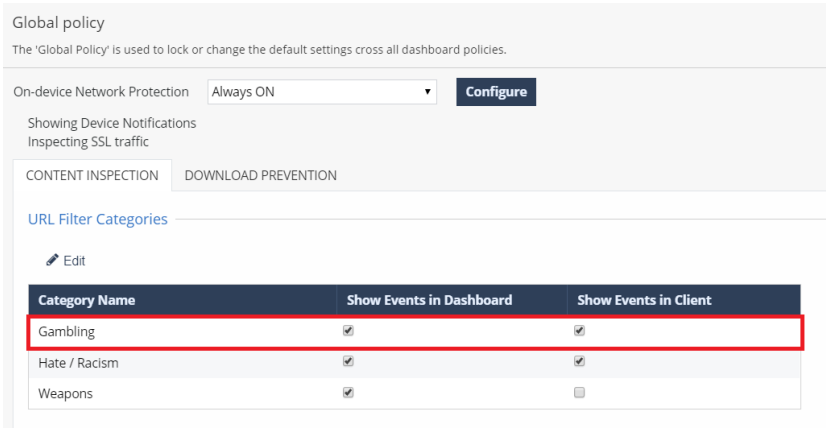


Figura 33: Seleccionar eventos de *URL Filtering*

6.8.6.1. LISTA NEGRA DE DOMINIOS

146. Esta categoría permite al administrador incluir dominios en la lista negra desde el dispositivo del usuario, sin importar la categoría temática o el nivel de riesgo del dispositivo.

147. Para añadir un dominio a la lista negra, ir a *Policy*, y a continuación ir a *Policy Profile > On-device Network Protection > Content Inspection > Blacklisted Domain Names > New*.

Figura 34: Lista Negra de Dominios

148. En la ventana emergente, en el campo *Domain*, introducir el dominio (O subdominio).

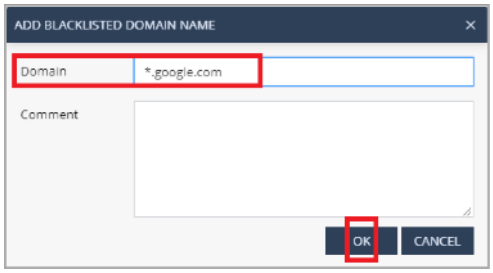


Figura 35: Añadir dominio a Lista Negra

149. Hacer click en *OK*.

150. Para eliminar un dominio de la lista, seleccionar el dominio y hacer click en *Delete*.

151. Para importar una lista de dominios, hacer click en *IMPORT* y cargar un fichero .CSV con la lista de Dominios que se desea bloquear.

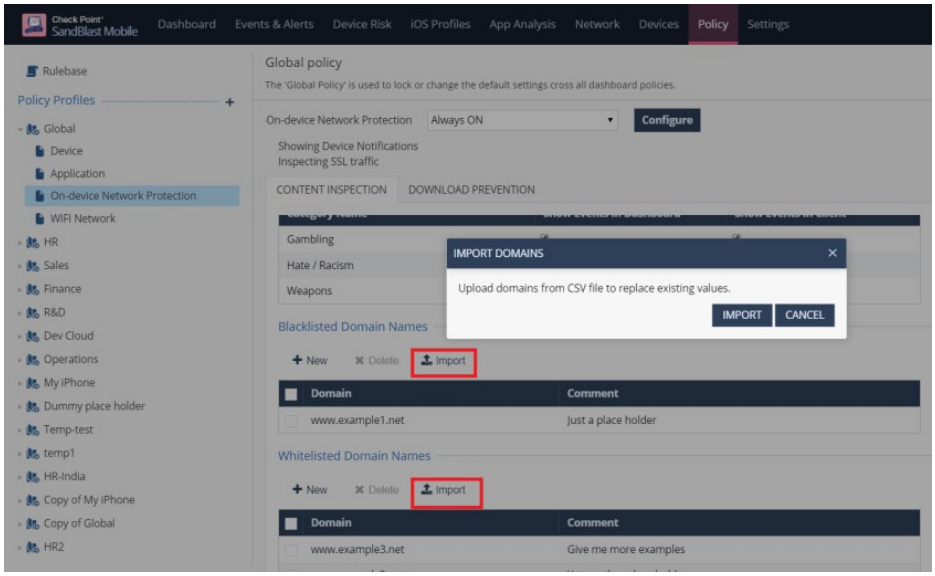


Figura 36: Añadir dominios a lista negra por CSV

Nota: Tanto si se añade una nueva lista de dominios de forma manual, como si se importa a través de un fichero en formato CSV, los dominios incluidos previamente en la lista no son eliminados de la misma. Esto permite a los administradores importar una lista de nombres de dominio/ubicaciones de otros sistemas, como *Firewall/Gateway*, a la configuración de la política de protección de red en el dispositivo (ONP) de Harmony Mobile.

6.8.6.2. LISTA BLANCA DE DOMINIOS

152. Esta categoría permite al administrador incluir en la lista blanca los dominios a los que siempre se puede acceder desde el dispositivo del usuario, sin importar la categoría temática o el nivel de riesgo del dispositivo.

153. Para añadir un dominio en lista blanca, ir a *Policy*, y a continuación, seleccionar *Policy Profile > On-device Network Protection > Content Inspection > Whitelisted Domain Names > New*.

Figura 37: Lista Blanca de Dominios

154. En la ventana emergente, en *Domain*, introducir el dominio (O subdominio).

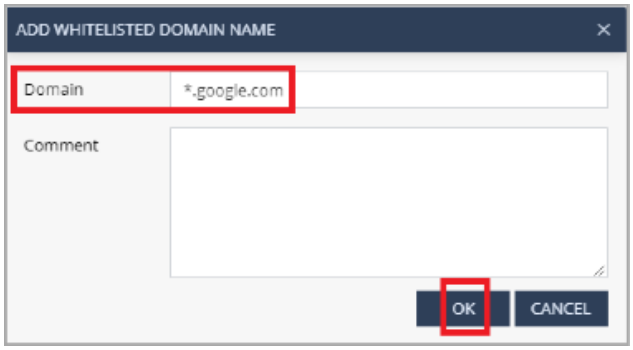


Figura 38: Añadir dominios en Lista Blanca

155. Hacer click en *OK*.

156. Para eliminar un dominio de la lista, seleccionar el dominio y hacer click en *Delete.*

157. Para importar una lista de dominios, hacer click en *IMPORT* y cargar un fichero .CSV con la lista de Dominios a añadir a la lista blanca.

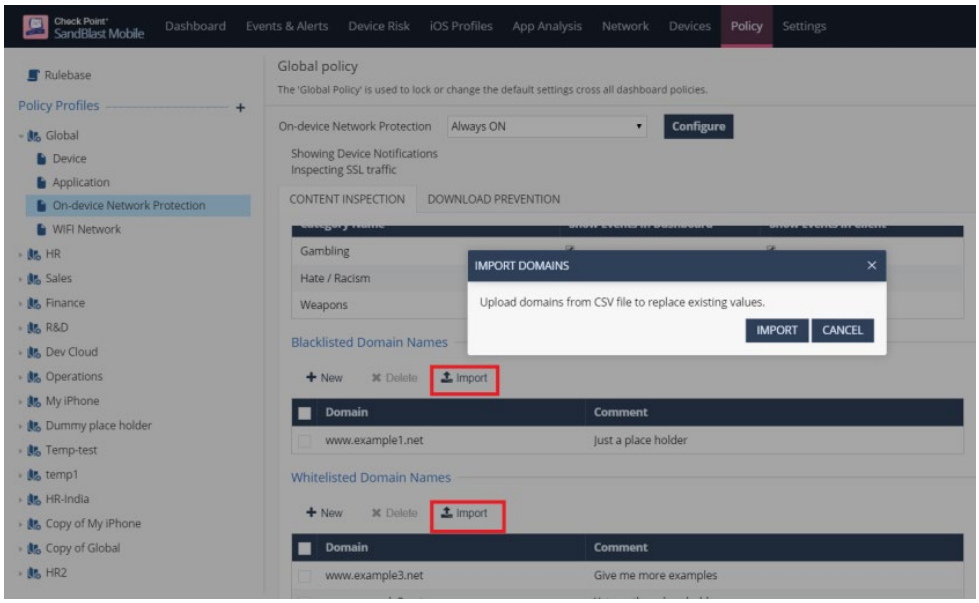


Figura 39: Añadir dominios en Lista Blanca por CSV

Nota: Tanto si se añade una nueva lista de dominios de forma manual, como si se importa a través de un fichero en formato CSV, los dominios incluidos previamente en la lista no son eliminados de la misma. Esto permite a los administradores importar una lista de nombres de dominio/ubicaciones de otros sistemas, como

Firewall/Gateway, a la configuración de la política de protección de red en el dispositivo (ONP) de SandBlast Mobile.

158. Para más información, se recomienda consultar el apartado "*Content Inspection*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8.7. PREVENCIÓN DE DESCARGAS

159. En la pestaña de *Download Prevention* se pueden configurar los siguientes parámetros:

Característica	Descripción	Opciones
Download Prevention Settings	Perfil de configuración de iOS: evita que los perfiles no autorizados y potencialmente maliciosos se descarguen e instalen en un dispositivo iOS. Aplicación iOS: Evita que aplicaciones no autorizadas y potencialmente maliciosas se descarguen e instalen en un dispositivo iOS. Aplicación de Android: evita que una aplicación de Android no autorizada y potencialmente maliciosa se descargue e instale en un dispositivo Android.	Off: No hay protección para descargas. *Allow only from Safe Domains*: Solo se permiten de dominios de confianza (*Google, Apple, Microsoft, etc…*) **Esta es la opción recomendada** *Block risky downloads*: Permite descargas de cualquier web que no contenga una mala reputación (*IP, dominio, etc…*)
Blacklisted Locations	Direcciones de red dónde los dispositivos no tendrán permitido realizar descargas de Apps/Perfiles de configuración.	
Whitelisted Locations	Direcciones de red dónde los dispositivos tendrán permitido realizar descargas de Apps/Perfiles de configuración.	

Tabla 6: Opciones de Prevención de Descargas

160. Para más información al respecto, se recomienda consultar el apartado *"Download Prevention"*, de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8.8. PROTECCIÓN DE DNS

161. *Protected DNS* proporciona servicios de DNS a través de la protección de red en el dispositivo de Harmony Mobile. Debe, por tanto, **habilitarse esta funcionalidad**, a través de las siguientes acciones:

1) Ir a *Policy > On-device Network Protection > Protected DNS* y *click* en *ON*.

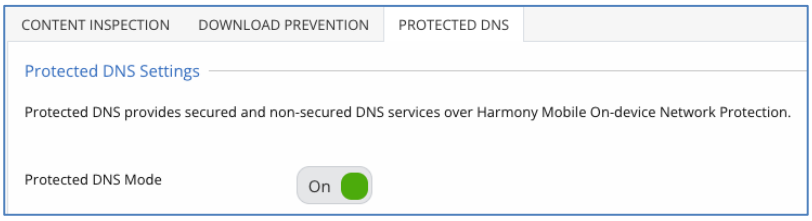


Figura 40: Habilitar Protected DNS

2) Seleccionar el riesgo del dispositivo cuando no pueda alcanzar al DNS protegido:

Figura 41: Riesgo de Protected DNS

3) Por último, indicar el/los servidor/es DNS protegido/s. Se pueden seleccionar dos (2) formas de indicar el DNS protegido:

- **Texto Plano:** Introducir IPv4 e IPv6 del servidor DNS.
- **Privado:** Introducir la dirección URL con la lista de DNS privados.

Figura 42: Introducir servidor DNS

162. Para más información, se recomienda consultar el apartado "*Protected DNS*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.8.9. WIFI NETWORK

163. En la pestaña *WiFi Network* **se debe hacer lo siguiente**:

- Establecer el nivel de riesgo para la configuración de protección de red Wi-Fi.
- Agregar servidores adicionales que se utilizarán para la detección de *Man-in-the-Middle* (*MitM)*.
- Habilitar la recopilación de datos de geolocalización.
- Configurar las URL de detección de MitM.
- Cargar certificados SSL para su lista blanca.

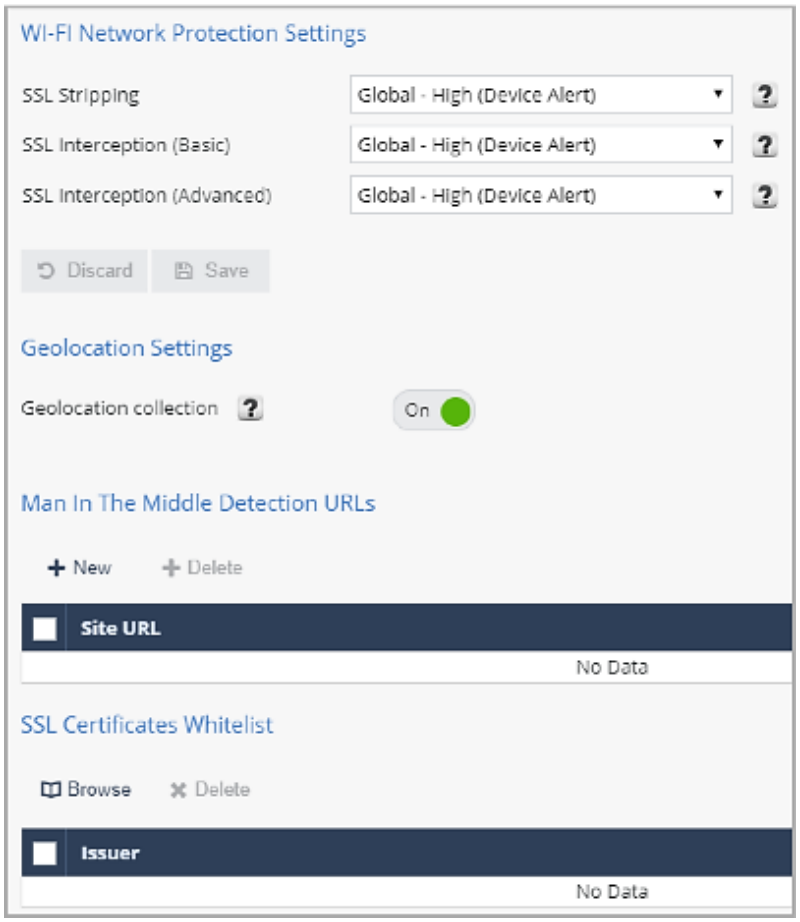


Figura 43: Opciones de WiFi Network

6.8.9.1. CONFIGURACIÓN DE MAN-IN-THE-MIDDLE

164. **Se debe configurar las URL para la detección de MITM, y seleccionar los niveles de riesgo adecuados** para la configuración de Protección de red Wi-Fi.

165. En la sección *Man-In-The-Middle*, hacer click en *[+ Nuevo]* para agregar la URL del sitio.

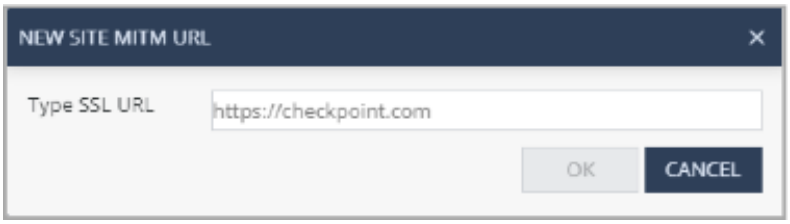


Figura 44: Añadir URL MiTM

166. Introducir la URL de SSL.

167. Hacer *click* en *OK*.

168. Para configurar la protección del dispositivo para varios ataques MITM, en la *Configuración de protección de red WI-FI* seleccionar un nivel de riesgo del dispositivo (de *Alto* a *Sin riesgo*) para evitar los siguientes ataques:

- Eliminación de SSL: se utiliza cuando el ataque *MITM* intercepta todo el redireccionamiento del tráfico de red de HTTP a HTTPS y "elimina" las llamadas HTTP dejando el tráfico como HTTP.
- Intercepción SSL (básica): se utiliza cuando el ataque *MITM* intercepta el tráfico HTTP mediante un certificado no válido que no existe en los certificados de confianza del dispositivo o no de confianza de una CA raíz.
- Intercepción SSL (avanzada): se utiliza cuando el ataque *MITM* intercepta el tráfico HTTP mediante un certificado válido que no coincide con el certificado del servidor.

6.8.9.2. HABILITAR GEOLOCALIZACIÓN

169. La funcionalidad de Geolocalización permite la recopilación de la ubicación GPS de un dispositivo si se detecta un ataque de red que afecte al dispositivo. Para habilitar la capacidad de geolocalización, en la sección *Geolocation Settings*, hacer click en *ON*.

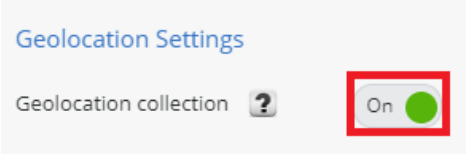


Figura 45: Habilitar Geolocation

170. Solo es posible habilitar la funcionalidad de Geolocalización desde el *Dashboard*. El usuario aún debe habilitar la aplicación *SandBlast Mobile Protect* para usar la ubicación en su dispositivo para que se recopile la información de ubicación geográfica.

171. Esta información se utiliza para proporcionar detalles del mapa en la pestaña *Network*.

6.8.9.3. LISTAS BLANCAS DE CERTIFICADOS

172. Al verificar los ataques de interceptación SSL (*SSL Bumping*), la solución verifica si el certificado SSL del sitio de destino es el esperado. Si no es así, la solución advierte que puede haber un ataque, incluso si el certificado recibido está en la lista de CA raíz del dispositivo.

173. Sin embargo, muchas organizaciones inspeccionan el tráfico de empleados y, para la solución, podría parecer que se trata de un ataque de interceptación SSL avanzado porque:

    1) La organización requiere que el certificado de la organización esté instalado en el dispositivo como una CA raíz.
    2) La interceptación SSL del tráfico en un proxy organizacional.

174. Para evitar recibir alertas sobre el propio certificado de la organización, la organización puede incluir sus propios certificados en una lista blanca (ver Figura

50). De esta forma, la solución no alertará de un "ataque" que involucre estos certificados.

175. Para añadir un certificado SSL a lista blanca, hacer click en *Browse* y seleccionar el certificado.

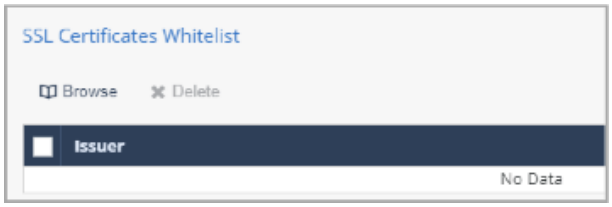


Figura 46: Lista blanca de certificados SSL

176. Hacer *click* en *OK*.

6.8.9.4. DETECCIÓN DE PUNTOS DE ACCESO FRAUDULENTOS QUE USAN IDENTIDADES DE WIFI CORPORATIVA

177. Harmony Mobile detecta y envía alertas acerca de puntos de acceso WiFi fraudulentos. Estos puntos de acceso intentan manipular a los usuarios de la empresa para que conecten sus dispositivos móviles, disfrazados como puntos de acceso legítimos que emplean SSIDs asociados a la organización. Mediante esta técnica, un atacante puede lanzar ataques de MitM, recolectar credenciales de usuarios, o hacerse con información sensible. Los administradores pueden establecer los niveles de riesgo y políticas asociadas a este tipo de técnica de ataque.

NOTA: Actualmente, la función de detección de puntos de acceso fraudulentos solo está disponible para IOS.

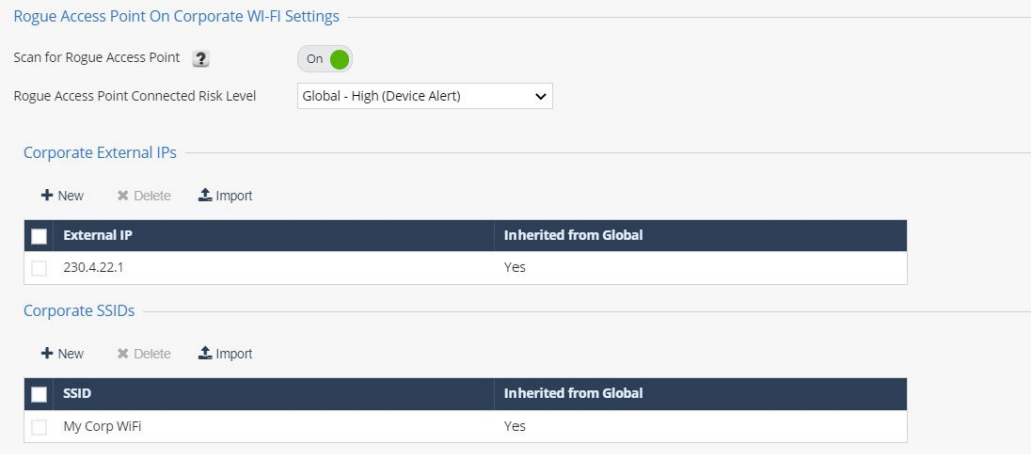


Figura 47: Detección de puntos de acceso WiFi fraudulentos

178. **Esta opción debe estar habilitada para detectar puntos de acceso fraudulentos y evitar así ataques de MitM.** Para ello:

1) Ir a *Policy > Policy Name > WiFi Network > Rogue Access Point On Corporate WiFi Settings.*

2) Habilitar *Scan for Rogue Access Point.*

3) Modificar la política de nivel de riesgo asociado a la conexión de un punto de acceso fraudulento, de acuerdo con el nivel de riesgo que se desea asociar a esta amenaza (el valor por defecto es '*Device Alert – High'*).

4) Configurar las direcciones IP externas corporativas.

5) Configurar los SSIDs corporativos.

179. Una vez completados estos pasos, la funcionalidad estará habilitada para los dispositivos móviles con sistema operativo IOS.

180. Cuando la aplicación detecte una conexión a una red WiFi fraudulenta por parte de un dispositivo, el nivel de riesgo asociado cambiará al establecido en la política correspondiente. Si el nivel de riesgo es '*High'* y las medidas de Acceso Condicional establecen que determinadas localizaciones deben ser bloqueadas, el acceso a dichas localizaciones es bloqueado de forma inmediata.

181. Los administradores podrán ver los eventos asociados a dichas conexiones, así como el nivel de riesgo asociado a las mismas, lo que permitirá manejar la situación de forma adecuada.

6.8.9.5. DETECCIÓN DE ESCANEO DE PUERTOS EN DISPOSITIVOS MÓVILES

182. La aplicación Harmony Mobile cuenta con capacidades de detección de intentos de escaneo de los puertos de dispositivos móviles de la organización por parte de agentes fraudulentos. Los administradores pueden establecer los niveles de riesgo y políticas asociadas a este tipo de técnica de ataque.

NOTA: Actualmente, esta función solo está disponible para IOS.

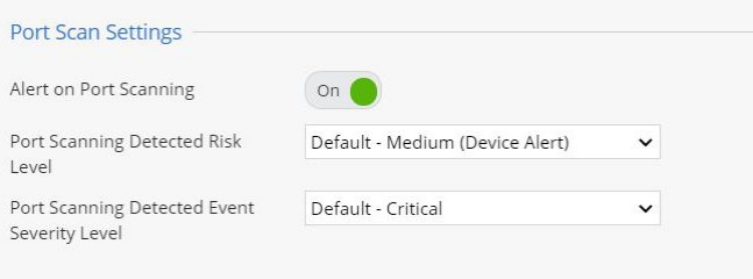


Figura 48: Configuración de escaneo de puertos

183. **Esta funcionalidad de detección de escaneo de puertos debe estar habilitada**. Se enumeran los pasos a seguir para detectar escaneos de puertos:

1) Ir a *Policy > Policy Name > WiFi Network > Port Scan Settings.*

2) Habilitar *Alert on Port Scanning.*

3) Modificar la política de nivel de riesgo asociado a la detección de un escaneo de puertos, de acuerdo con el nivel de riesgo que se desea asociar a esta amenaza (el valor por defecto es '*Device Alert – Medium'*).

4) Ajustar el nivel de severidad asociado a la política de detección de un evento de escaneo de puertos al nivel que se desee (el valor por defecto es '*Critical*').

184. Para más información, se recomienda consultar el apartado "*WiFi Network*", de la Guía de Administración de Harmony Mobile **[REF1]**.

6.9 BUENAS PRÁCTICAS

185. A continuación, se enumeran algunas configuraciones de buenas prácticas para tener un nivel de seguridad óptimo en los dispositivos móviles. Estas indicaciones son modificaciones a realizar sobre la política por defecto (*Global*) o a una nueva política.

186. **Estas buenas prácticas deben ser aplicadas para hacer uso del producto de la forma más segura posible.**

6.9.1. BUENAS PRÁCTICAS PARA POLÍTICAS DE DISPOSITIVO

187. A continuación, se introduce una serie de buenas prácticas, aplicables a políticas de dispositivo (*Device Policies*):

a) Configuraciones Generales (*General Settings*):

- **Cambiar el estado del dispositivo a "*Inactivo*" si el dispositivo no se ha comunicado con el servidor por 45 días.**
- **Cambiar el nivel de riesgo del dispositivo a *Medium (Device Alert)*, si el dispositivo no se ha comunicado con el servidor por 30 días.**
- Cambiar el nivel de riesgo del dispositivo a *Medium (Dismissive Device Alert)* si la versión de la aplicación Harmony Mobile Protect lleva *2 meses* sin actualizarse.

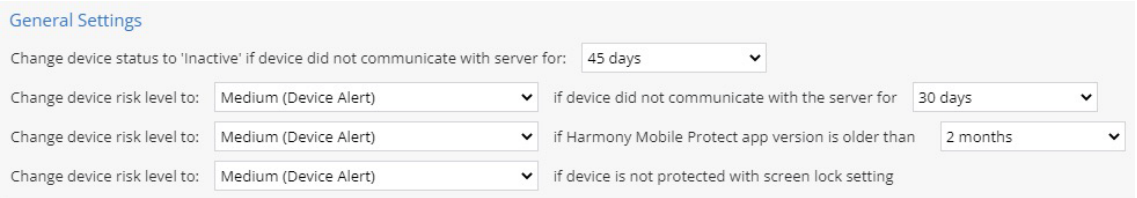


Figura 49: Buenas Prácticas – Configuraciones Generales

b) Configuraciones de Seguridad para Dispositivos Android:

- **Cambiar el nivel de riesgo del dispositivo a:*Medium (Device Alert)* si la versión del Sistema Operativo del dispositivo es más antigua que *10.0** (*API level 29*) [Se recomienda revisar el parque de dispositivos móviles para confirmar qué versión de Android es la más antigua y configurar la regla en base a dicha información.]
- **Cambiar el nivel de riesgo del dispositivo a *Medium (Device Alert)* si la última actualización de seguridad se instaló hace más de *2 meses*.**

- **Cambiar el nivel de riesgo del dispositivo a *Low* si el dispositivo es vulnerable a *Achilles*** [REF12].

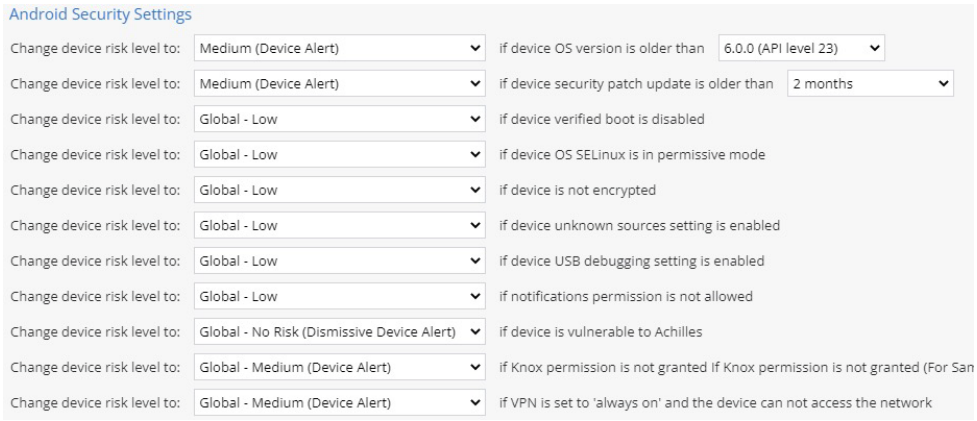


Figura 50: Buenas Prácticas – Configuraciones de Seguridad para Android

c) Configuraciones de Seguridad para IOS:

- **Cambiar el nivel de riesgo del dispositivo a *Medium (Device Alert)* si la versión del sistema operativo del dispositivo es inferior a *14.0.k*.**

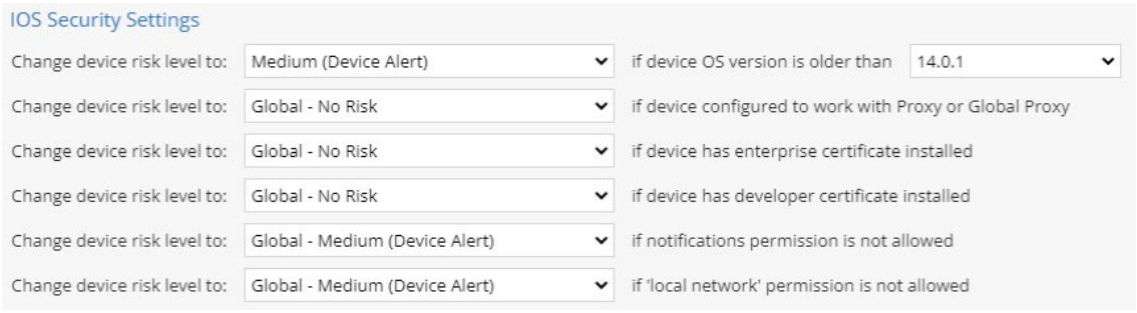


Figura 51: Buenas Prácticas – Configuraciones de Seguridad para iOS

d) Políticas de Red (Pestaña *On-device Network Protection*):

- ***On-device Network Protection: Always ON***
- Ir al botón *Configure* y seleccionar lo siguiente:
  - ***Show device notifications: ON***
  - ***Automatically suspend when: Any VPN is connected***
  - ***HTTPS Inspection: ON***

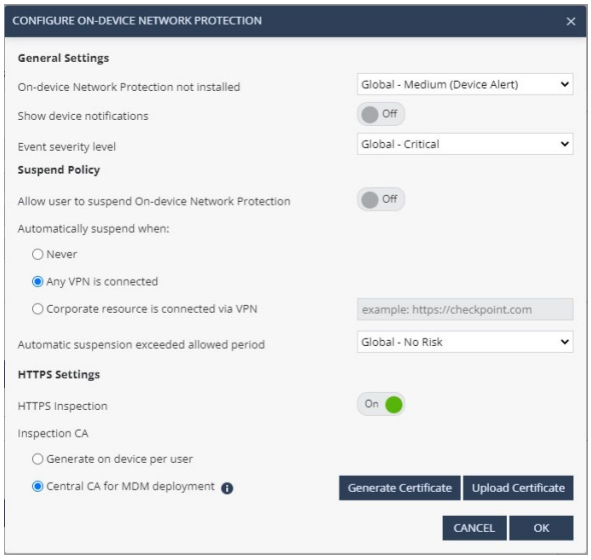


Figura 52: *On-Device Network Protection* – Opciones de configuración

e) Inspección de Contenido (*Content Inspection*):

- *Phishing:* ***ON***
- *Spyware / Malicious Sites:* ***ON***
- *Botnets:* ***ON***
- *Zero-Phishing:* ***ON***

Figura 53: Buenas Prácticas – Inspección de Contenido

f) Prevención de Descargas (*Download Prevention*):

- ***iOS Configuration Profile: Allow only from Safe Domains***
- ***iOS Application: Allow only from Safe Domains***
- ***Android Application: Allow only from Safe Domains***

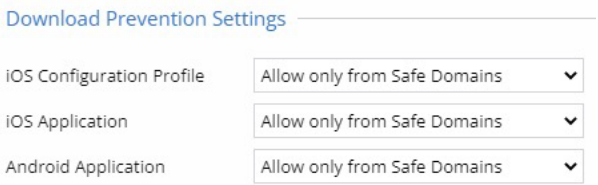


Figura 54: Buenas Prácticas – Download Prevention

188. Para más información sobre buenas prácticas, se recomienda consultar el documento "*Harmony Mobile – Recomendaciones de buenas prácticas*" [REF11].

7. FASE DE OPERACIÓN

189. Se recomienda que, durante la fase de operación y mantenimiento del producto, se sigan, al menos, los siguientes procedimientos operativos:

- **Comprobaciones periódicas del *hardware* y/o *software*** para asegurar que no se ha introducido hardware o software no autorizado.
- En caso de que aplique, deberá **verificarse el *firmware* activo y su integridad**, para comprobar que está libre de software malicioso.
- Aplicación regular de los **parches de seguridad**, con objeto de mantener una configuración segura.
- **Mantenimiento de los registros de auditoria**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará **en las condiciones y por el periodo establecido en la normativa de seguridad.**
- **Auditar, al menos, los eventos especificados en la normativa de referencia** y aquellos otros extraídos del análisis de riesgos.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Creación de *Infinity Portal*	☐	☐	
Activación del servicio *Harmony Mobile*	☐	☐	
Crear grupo de dispositivos	☐	☐	
Crear nuevo conjunto de política	☐	☐	
Asociar grupos y políticas en *Rulebase*	☐	☐	
CONFIGURACIÓN			
Utilización de 2MFA	☐	☐	
Integración con Syslog	☐	☐	
Aplicar la política de contraseñas	☐	☐	
Aplicación de políticas de Acceso Condicional	☐	☐	
Aplicación de políticas de *URL filtering*	☐	☐	
Activación de la protección de descargas	☐	☐	
Activación de la protección DNS	☐	☐	
Activación de políticas de protección de Redes WiFi	☐	☐	
Integración con MDM (*Si aplica*)	☐	☐	
Aplicación de buenas practicas (apartado 6.9)	☐	☐	
OPERACIÓN			
Comprobaciones periódicas del *hardware* y/o *software*	☐	☐	
Verificación del *firmware* activo y su integridad	☐	☐	
Instalación parches de seguridad	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Mantenimiento y almacenamiento seguro de logs	☐	☐	
Auditoría de logs	☐	☐	

9. REFERENCIAS

REF1 Guía de Administración de *Harmony Mobile*
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Mobile-Admin-Guide/Front-Matter/Front-Matter-How-to-Search-in-this-Book.htm

REF2 Guía de Integración con MDM
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Mobile-Admin-Guide/Topics-Admin-Guide/Navigating_the_Harmony_Mobile_Services.htm?tocpath=Navigating%20the%20Harmony%20Mobile%20Services%7CSettings%7C____4#Integrations_(Previously_%E2%80%98Device_Management%E2%80%99)

REF3 Guía de Administración de Infinity Portal
https://dl3.checkpoint.com/paid/ba/bab57dd88ae8654ced7285bf7ecdf93f/CP_Infinity_Portal_AdminGuide.pdf?HashKey=1643363643_e7eca45b62dc73b4069448db9eccb232&xtn=.pdf

REF4 *How to associate User Center acquired contracts with CloudGuard SaaS account*
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk144612

REF5 *Check Point Cloud Security Services*
https://cloud.checkpoint.com/_CP62979072C756/index.php

REF6 ¿Qué es el *jailbreak?*
https://opendatasecurity.io/que-es-el-jailbreak/

REF7 ¿Qué es el *Rooting*?
https://www.pandasecurity.com/es/security-info/root/#:~:text=es%20el%20Rooting%3F-,Rooting%20es%20una%20t%C3%A9cnica%20que%20permite%20a%20los%20usuarios%20de,da%20nombre%20a%20la%20t%C3%A9cnica)

REF8 Check Point Infinity Portal
https://portal.checkpoint.com/

REF9 *Check Point SandBlast Mobile Data Privacy and Handling*
https://dl3.checkpoint.com/paid/7c/7cb735ff2122a4f5ee12eb17dd58c89f/sandblast-mobile-data-privacy-handling-wp-us.pdf?HashKey=1646303569_4aea92754390c231610bd87c3c83186a&xtn=.pdf

REF10 Check Point SandBlast Mobile Communication Information Guide

REF11 Harmony Mobile – Recomendaciones de buenas prácticas
Este documento debe ser solicitado por el usuario final a Check Point España.

REF12 Over 400 vulnerabilities on Qualcomm's Snapdragon chip threaten mobile phones' usability worldwide
https://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/

10. ABREVIATURAS

ENS	Esquema Nacional de Seguridad.
ONP	*On-device Network Protection*
HM	*Harmony Mobile*
C&C	*Command and Control*
UEM	*Unified Endpoint Management*
MiTM	*Man-in-the-Middle*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL