





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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid  
© Centro Criptológico Nacional, 2022  
NIPO: 083-22-221-8

Fecha de Edición: septiembre 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## ÍNDICE

<b>1. INTRODUCCIÓN .....</b>	<b>5</b>
<b>2. OBJETO Y ALCANCE .....</b>	<b>7</b>
<b>3. ORGANIZACIÓN DEL DOCUMENTO .....</b>	<b>7</b>
<b>4. FASE PREVIA A LA INSTALACIÓN.....</b>	<b>8</b>
4.1 ENTREGA SEGURA DEL PRODUCTO .....	8
4.2 ENTORNO DE INSTALACIÓN SEGURO .....	8
4.3 REGISTRO Y LICENCIAS .....	8
4.4 CONSIDERACIONES PREVIAS.....	9
4.4.1. CONFIGURACIÓN DE LA POLÍTICA DE PRIVACIDAD .....	9
4.4.2. CREACIÓN DE UN ADMINISTRADOR DE MTD .....	10
4.4.3. HABILITACIÓN DE LA MENSAJERÍA CPS EN CORE.....	11
4.4.4. INTEGRACIÓN DE CORE COMO SERVIDOR MDM EN ZCONSOLE.....	12
4.4.5. PERMITIR ACCESO A APP GATEWAY .....	14
<b>5. FASE DE INSTALACIÓN.....</b>	<b>17</b>
5.1 HABILITACIÓN DE MTD PARA DISPOSITIVOS MOBILE@WORK .....	17
5.1.1. CREACIÓN DE UNA CONFIGURACIÓN DE ACTIVACIÓN DE MTD.....	17
5.1.2. DESACTIVACIÓN DE MTD EN CORE .....	18
5.1.3. COMPROBACIÓN FUNCIONAMIENTO MTD .....	18
<b>6. FASE DE CONFIGURACIÓN .....</b>	<b>20</b>
6.1 DEFINICIÓN DE POLÍTICAS.....	20
6.1.1. CONFIGURACIÓN DEL INTERVALO DE ACTIVACIÓN MTD PARA DISPOSITIVOS IOS 20	20
6.1.2. CONFIGURACIÓN DEL INTERVALO DE ACTIVACIÓN MTD PARA DISPOSITIVOS IOS 20	20
6.2 MITIGACIÓN Y CUMPLIMIENTO INICIADOS POR EL SERVIDOR .....	23
6.2.1. CREACIÓN Y APLICACIÓN DE ACCIONES DE CUMPLIMIENTO DE VARIOS NIVELES INICIADAS POR EL SERVIDOR.....	23
6.2.2. CREACIÓN DE ETIQUETAS MTD EN CORE PARA DISPOSITIVOS ANDROID Y IOS26	26
6.2.3. CONFIGURACIÓN DE LA POLÍTICA DE RESPUESTA A AMENAZAS DE ZCONSOLE27	27
6.2.4. ESTABLECER LA ACCIÓN DEL DISPOSITIVO.....	28
6.2.5. MEDIDAS DE MITIGACIÓN.....	30
6.2.6. NOTIFICACIONES .....	30
6.2.7. ACTUALIZACIÓN DE LA POLÍTICA DE SINCRONIZACIÓN PRINCIPAL.....	30
6.3 PROTECCIÓN CONTRA PHISHING PARA DISPOSITIVOS MTD.....	32
6.3.1. PROTECCIÓN AVANZADA CONTRA PHISING EN DISPOSITIVOS GESTIONADOS33	33
6.3.2. HABILITACIÓN ZCONSOLE ANTI-PHISING VPN .....	33
6.3.3. HABILITACIÓN DE PROTECCIÓN ADICIONAL CONTRA EL PHISING .....	35
6.3.4. USO DE UNA BASE DE DATOS REMOTA PARA VALIDAR DIRECCIONES URL.....	38
6.3.5. ANDROID ANTI-PHISING USANDO LA APLICACIÓN MI TUNNEL .....	38
6.3.6. CREACIÓN DE UNA CONFIGURACIÓN DE MI TUNNEL PARA DISPOSITIVOS ANDROID ENTERPRISE .....	39
6.3.7. DESCRIPCIÓN DEL CONTROLADOR DE URL.....	40
6.3.8. TAREAS DE CONFIGURACIÓN DE PHISING DE ANDROID HEREDADAS.....	43

6.3.9. USO DE LA PÁGINA DE DETALLES DEL DISPOSITIVO PARA VERIFICAR QUE EL ANTIPHISING ESTÁ HABILITADO .....	44
6.4 MITIGACIÓN Y CUMPLIMIENTO INICIADOS LOCALMENTE .....	45
6.4.1. CREACIÓN DE ACCIONES LOCALES MTD EN CORE .....	45
6.4.2. PERSONALIZACIÓN DEL TEXTO DE NOTIFICACIÓN DE AMENAZAS LOCALES....	47
6.4.3. NOMBRES DE CATEGORÍAS DE AMENAZAS Y AMENAZAS RELACIONADAS.....	49
6.4.4. AMENAZAS DE RED, DISPOSITIVOS Y APLICACIONES DISPONIBLES EN ACCIONES LOCALES.....	50
6.4.5. CREACIÓN DE GRUPOS Y REGLAS DE POLÍTICAS DE CUMPLIMIENTO .....	54
6.4.6. CONFIGURACIÓN DE LA ACCIÓN DE SINKHOLE EN DISPOSITIVOS IOS .....	57
6.4.7. COMPROBACIÓN DEL ESTADO DE MTD .....	61
6.5 CONFIGURACIÓN DE ADMINISTRADORES .....	64
6.5.1. USO DE ZCONSOLE .....	64
6.5.2. GESTIÓN DE LA PRIVACIDAD DEL USUARIO .....	71
6.5.3. ADMINISTRACIÓN DE MOBILE@WORK .....	74
<b>7. DOCUMENTACIÓN DE MOBILE THREAT DEFENSE.....</b>	<b>76</b>

## 1. INTRODUCCIÓN

1. La solución de defensa contra amenazas móviles Mobileiron Threat Defense (MTD) permite supervisar, administrar y securizar los dispositivos móviles frente a ciberataques en dispositivos, redes y aplicaciones. Detecta las amenazas tanto conocidas, como zero-day, incluso sin conectividad en red.
2. Los cuatro pilares que definen esta funcionalidad de seguridad son la detección proactiva de amenazas y ataques, la corrección puntual, una mayor visibilidad de los dispositivos y de la red y una fácil administración.
3. (MTD) consta de tres componentes, como se ilustra en la siguiente figura.
  - Servidor de administración de dispositivos móviles (MDM) (Core)
  - Aplicación cliente de Ivanti (Mobile@Work para iOS y Android)
  - Consola de administración (zConsole)

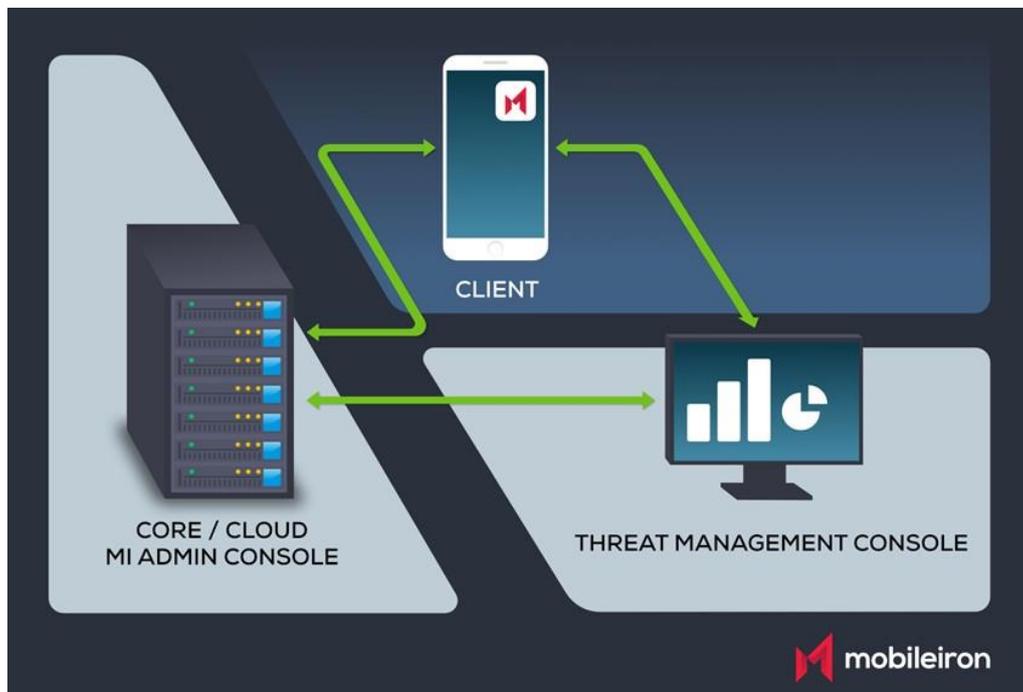


FIGURA 1. SOLUCIÓN MOBILE THREAT DEFENSE

4. El administrador de Mobile Device Management (MDM) puede configurar Core para instalar automáticamente la versión requerida de la aplicación cliente Ivanti, Mobile@Work para Android e iOS, implementar y habilitar un token de activación MTD en dispositivos seleccionados, y configurar los componentes para interoperar para proteger los dispositivos de las amenazas móviles.

5. Después de una incorporación inicial, la lista de flujos de trabajo necesarios para configurar la solución Mobile Threat Defense es:
  - Core proporciona un token de activación MTD para Mobile@Work clientes en dispositivos seleccionados.
  - La funcionalidad de defensa contra amenazas está habilitada en dispositivos seleccionados.
  - zConsole autentica y establece la comunicación con Core y sincroniza los parámetros del dispositivo.
  - El administrador define las políticas de defensa contra amenazas en la zConsole.
  - El administrador define las políticas de acciones locales de MTD en Core.
  - Habilitado para MTD Mobile@Work comienza a comunicarse con zConsole y con Core.
  - Mobile@Work habilitado para MTD analiza periódicamente el dispositivo en busca de amenazas y se toman medidas de acuerdo con las políticas de acción locales e iniciadas por el servidor definidas.
  
6. Las amenazas detectadas se pueden remediar mediante una combinación de acciones de mitigación y cumplimiento iniciadas localmente y por el servidor. Aplicados juntos, proporcionan la protección contra amenazas del cliente. Se realiza a través de la zConsole. La configuración de la mitigación y el cumplimiento iniciados localmente se realiza a través de Admin Console. El proceso funciona de esta manera:
  - Si la mitigación se implementa mediante Acciones locales, la amenaza se corrige en función de la configuración de Acciones locales y no necesita conexión a Core o zConsole.
  - Si el dispositivo está conectado a Core y zConsole (iniciado por el servidor), cualquier amenaza detectada en el dispositivo informa a zConsole del estado de la amenaza. zConsole indica a Core que se ha activado una infracción de la política. Core asigna el dispositivo comprometido a la etiqueta adecuada, lo que puede desencadenar un flujo de trabajo de aplicación de *custom*.
  - Cuando la amenaza se corrige en el dispositivo, el cliente pasa este cambio de estado a zConsole. zConsole indica a Core que se ha eliminado la infracción de política y elimina la etiqueta que desencadenó un flujo de trabajo de aplicación personalizado del dispositivo. A continuación, Core restaura el dispositivo a sus operaciones normales.

## 2. OBJETO Y ALCANCE

7. La presente guía aplica a la solución de Mobileiron 10.0.1 y posteriores.

## 3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento se compone de los siguientes apartados:

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

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

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.

Apartado **7**. En este apartado se recoge algunas referencias.

## 4. FASE PREVIA A LA INSTALACIÓN

### 4.1 ENTREGA SEGURA DEL PRODUCTO

9. Core incluye la capacidad de distribuir tokens de activación para habilitar la tecnología Mobile Threat Defense (MTD) integrada en Mobile@Work para clientes Android y iOS. Mobile Threat Defense protege los dispositivos administrados de amenazas y vulnerabilidades móviles que afectan a dispositivos, redes y aplicaciones.
10. Monitores de Mobile Threat Defense:
  - A nivel de dispositivo: parámetros del sistema, configuración, firmware y bibliotecas para identificar actividades sospechosas o maliciosas.
  - A nivel de red: tráfico de red y conexiones sospechosas hacia y desde dispositivos móviles.
11. A nivel de aplicación: aplicaciones con fugas (que potencialmente ponen en riesgo los datos empresariales) y aplicaciones de riesgo, a través de la evaluación de riesgos y el análisis de código.
12. Cuando esta configuración se habilita en Core y se aplica a los dispositivos, las bibliotecas MTD se habilitan en los clientes Mobile@Work. El servicio Mobile Threat Defense se puede desactivar en un dispositivo eliminando la etiqueta asociada a la configuración de la licencia MTD.
13. Aplicable a:
  - Mobile@Work para las versiones de cliente de iOS compatibles con Core.
  - Mobile@Work para las versiones de cliente de Android compatibles con Core.

**NOTA:** MTD actualmente **no** es compatible con dispositivos macOS y Windows.

### 4.2 ENTORNO DE INSTALACIÓN SEGURO

14. El producto debe instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa según la política de seguridad correspondiente al nivel de clasificación o categoría de la información manejada.

### 4.3 REGISTRO Y LICENCIAS

15. La licencia MTD determina la funcionalidad.
16. Mobile Threat Defense Solution tiene dos tipos de licencias, que determinan qué características están habilitadas y cuáles no. Si tiene una licencia MTD Plus, toda la funcionalidad MTD de Ivanti está habilitada, incluido el análisis avanzado de aplicaciones. Si necesita la funcionalidad MTD Plus debe ponerse en contacto con su representante de Ivanti.

## 4.4 CONSIDERACIONES PREVIAS

17. Antes de configurar Mobile Threat Defense, complete los siguientes requisitos previos:

- Configura Core para administrar dispositivos.
- Obtenga su licencia MTD.
- Obtenga las credenciales de Threat Management Console.
- Abra el puerto 8883 entrante desde zConsole a Core.
- Los clientes que utilizan las ACL de Portal para la lista blanca de IP para permitir conexiones desde zConsole a su Core para los puertos 443 u 8883 pueden usar esta información para acotar los direccionamientos permitidos:

TABLA 1. DIRECCIONAMIENTO PERMITIDO DESDE ZCONSOLE AL CORE

Region	VPC Name	IPs
North America	CORP	52.202.83.246, 3.210.62.246
North America	CORP2	129.146.150.66:443
North America	AMERICAS	51.143.17.112, 40.64.110.131, 20.59.42.144
North America	UAT	3.95.83.212, 34.237.18.172
EMEA	EMEA	3.121.90.14, 18.185.186.251
EMEA	EMEA2	18.157.59.24, 18.157.59.39
EMEA	EMEA UAT	3.121.251.110, 3.122.27.144
APJ	APJ	54.206.13.148, 13.237.19.174
APJ	India	54.206.13.148, 13.237.19.174

### 4.4.1. CONFIGURACIÓN DE LA POLÍTICA DE PRIVACIDAD

18. Puede modificar la Política de privacidad predeterminada para que se aplique a las aplicaciones o crear una nueva política si es necesario. Para configurar la Política de privacidad para que se aplique a las aplicaciones, siga estos pasos:

19. **Procedimiento:**

1. Vaya a **Políticas y configuraciones > políticas**.

2. Elija una de las siguientes opciones:

Seleccione la Política de privacidad predeterminada existente y haga clic en el botón **Editar** en la esquina superior derecha de la sección Detalles de la política. Se abrirá el menú **Modificar Privacy Policy**.

Haga clic en **Add New Policy >**. Se abrirá el menú **Privacy Policy**.

3. Introduzca el nombre de la política y una descripción si es necesario.

4. En la sección Apps, seleccione **All Apps**.

5. Haga clic para aplicar la etiqueta All Smartphones a la política de privacidad.

6. Haga clic en **Save**.

**CONSEJO:** La Política de privacidad predeterminada se puede modificar para recopilar todas las aplicaciones. Si detecta una conexión Wifi no segura, pero la

acción de cuarentena para eliminar las aplicaciones administradas no funciona, es posible que deba cambiar la configuración en el campo Aplicaciones desde Aplicaciones del catálogo de aplicaciones hasta Todas las aplicaciones.

#### 4.4.2. CREACIÓN DE UN ADMINISTRADOR DE MTD

20. Antes de configurar zConsole para su uso con Core, debe crear un usuario administrador de MTD, que se comunicará con Core a través de zConsole. Ivanti sugiere crear un nuevo usuario administrador para administrar MTD.

**NOTA:** se recomienda quitar el rol Portal de usuarios del administrador de MTD. Este rol se asigna automáticamente a cada usuario local.

#### 21. Procedimiento:

1. En el Portal de administración principal, seleccione **Dispositivos y usuarios > usuarios**.
  2. Haga clic en **Agregar > Agregar nuevo usuario**. Se abrirá el cuadro de diálogo Agregar nuevo usuario.
  3. Rellene los siguientes campos:
    - **ID de usuario:** Introduzca un ID de usuario significativo como "mtdadmin".
    - **Nombre:** Introduzca el nombre del usuario mtdadmin.
    - **Apellido:** Introduzca el apellido del usuario mtdadmin.
    - **Nombre para mostrar:** Introduzca un nombre que se mostrará.
    - **Contraseña:** Introduzca una contraseña.
    - **Confirmar contraseña:** Confirme la contraseña.
    - **Correo electrónico:** Introduzca la dirección de correo electrónico del usuario mtdadmin.
  4. Haga clic en **Guardar**.
22. Una vez que haya creado su usuario administrador mtd, debe asignar al administrador a un espacio de dispositivo, lo que limita su autoridad a ese espacio, y asignar al usuario los roles apropiados. Para obtener más información acerca de la asignación de espacios de dispositivos, consulte "Espacios de dispositivos" en la *Guía de administración delegada principal*.
23. Antes de empezar asegúrese de haber completado los pasos para "Crear un administrador de MTD" anteriores.

#### 24. Procedimiento:

1. En el portal de administración, vaya a la página **Administradores > Administradores**.

2. Seleccione el usuario administrador para que sea el administrador de MTD.
3. Haga clic en **Acciones > Asignar al espacio**.
4. En el menú desplegable **Seleccionar espacio**, seleccione el espacio que administrará el usuario local.

**NOTA:** Debe seleccionar un espacio para el administrador de MTD antes de que aparezcan los roles apropiados. El valor predeterminado es que no se ha seleccionado ningún espacio.

5. En la lista de **roles de administrador**, desplácese hacia abajo hasta:
  - a) **Administración de dispositivos** y seleccione **Aplicar y quitar etiqueta de dispositivo**.
  - b) **Control de privacidad** y seleccione **Ver aplicaciones e iBooks en detalles del dispositivo** y **Localizar dispositivo**.
  - c) **Administración de etiquetas** y seleccione **Ver etiqueta** y **Administrar etiqueta**.
  - d) **Administración de usuarios** y seleccione **Ver usuario** y **Administrar usuario**.
  - e) **Otros roles** y seleccione **Common Platform Services (CPS)**
6. Haga clic en **Guardar**.

#### 4.4.3. HABILITACIÓN DE LA MENSAJERÍA CPS EN CORE

25. El servidor zConsole se integra con MTD mediante el servicio de notificación de eventos, lo que requiere habilitar la mensajería CPS. La mensajería CPS hace posible que zConsole reciba notificaciones de cambios en los dispositivos en tiempo real, por ejemplo, para nuevos registros de dispositivos o nuevas instalaciones de aplicaciones, en lugar de confiando en el trabajo de sincronización que se ejecuta cada 1-4 horas. Estas notificaciones no serán recibidas por zConsole si la mensajería no está habilitada. Para obtener más información, consulte "Uso del servicio de notificación de eventos" en la *Guía de la API de Service y Common Platform Services*.
26. Puede ejecutar el programa Core CLI para habilitar la mensajería de Common Platform System (CPS). Este procedimiento invoca un agente de mensajes, habilita la característica de notificación de eventos del Servicio de notificación de eventos, reinicia el servidor Core y reinicia Apache Tomcat para volver a cargar las configuraciones.

**NOTA:** el puerto 8883 debe estar abierto de entrada desde zConsole a Core. Si Core se ejecuta en una configuración de alta disponibilidad, habilite la mensajería en los nodos principal y secundario.

**27. Procedimiento:**

Para habilitar o deshabilitar la mensajería CPS, ejecute los siguientes comandos en la CLI principal:

```
hostname> enable
hostname# configura terminal config#
activemq Warning: Maintenance mode commando.
El servicio del portal se detendrá durante esta operación. ¿Proceder? (y/n) y
Captura de métricas de tomcat: [ OK]
Detención de tomcat: [ OK] [ Aceptar]
```

**4.4.4. INTEGRACIÓN DE CORE COMO SERVIDOR MDM EN ZCONSOLE**

28. Debe agregar Core como servidor de administración de dispositivos móviles (MDM) en zConsole para habilitar Mobile Threat Defense. Después de introducir los detalles del núcleo, como la URL y el nombre de usuario y la contraseña del administrador, zConsole se sincroniza con Core. Puede seleccionar las etiquetas Core que desea usar en zConsole y los usuarios, dispositivos y aplicaciones relevantes de la pantalla Core en zConsole.

29. Antes de empezar:

- Busque el nombre de usuario y la contraseña del inquilino de zConsole que recibió de Ivanti después de comprar Mobile Threat Defense Solution.
- Asegúrese de haber completado "Asignación de un espacio y roles a un administrador de MTD" y Adición de roles de MTD al usuario administrador principal.

**30. Procedimiento:**

1. Inicie sesión en su tenant de zConsole con las credenciales proporcionadas por Ivanti. El nombre de usuario y la contraseña definidos para el administrador de MTD son necesarios para establecer comunicación con Core y sincronizar los dos servidores.
2. Vaya a **Administrar integraciones** de >> **Agregar MDM**.
3. Seleccione **Core** para agregarlo a zConsole como servidor MDM.
4. Cree su configuración utilizando la siguiente información requerida:

TABLA 2. REGLAS EXTERNAS E INTERNET

Artículo	Descripción
URL	Escriba el FQDN o la URL accesible externamente para su Core en el protocolo de hipertexto seguro (HTTPS). Por ejemplo: <a href="https://core.mydomain.com">https://core.mydomain.com</a>

Artículo	Descripción
Nombre de usuario/contraseña	Introduzca un nombre de usuario y una contraseña de administrador para Core. Al usuario administrador se le deben asignar varios roles, incluida la API, como se describe en Agregar roles al usuario administrador mtd.
Nombre de MDM	Introduzca un nombre para Core.
Lista blanca de aplicaciones administradas de MDM	Seleccione esta opción para agregar automáticamente aplicaciones iOS y Android administradas por MDM a la lista blanca. Las aplicaciones incluidas en la lista blanca no se informan como amenazas.
Sincronización en segundo plano	Seleccione esta opción para especificar que este proveedor de MDM (Core) debe sincronizar automáticamente usuarios, dispositivos, aplicaciones y perfiles periódicamente.
Información de usuario importada de máscaras	Seleccione esta opción para enmascarar la información de identificación personal (nombre, apellido y dirección de correo electrónico) de zConsole.
Envíe correo electrónico de activación de dispositivos a través de zConsole para dispositivos iOS.	Esta característica no es compatible con MTD en este momento.
Envíe correo electrónico de activación de dispositivos a través de zConsole para dispositivos Android.	Esta característica no es compatible con MTD en este momento.

5. Haga clic en **Siguiente**.
6. En la última ventana, seleccione las etiquetas Core que desea utilizar como grupos zConsole. La lista de grupos zConsole está organizada en orden de prioridad. Mueva el nombre de un grupo hacia arriba o hacia abajo para cambiar su prioridad.  
  
Ivanti recomienda crear nuevas etiquetas en el portal de administración de Core antes de sincronizar zConsole con Core, de lo contrario, las etiquetas no aparecerán cuando se realice este paso.
7. Haga clic en **Finalizar**.
8. Sincronice zConsole con Core. Asegúrese de que la sincronización se haya realizado correctamente.

**CONSEJO:** Cada vez que se elimina una configuración de MDM de zConsole, asegúrese de eliminar manualmente la etiqueta de token de activación MTD en Core. Si esto no se hace, el token de activación permanece asignado a una etiqueta en Core y Mobile@Work aún muestra "Habilitado".

#### 4.4.5. PERMITIR ACCESO A APP GATEWAY

31. Para crear una política de acción local MTD, debe conceder acceso Core a App Gateway para que pueda descargar definiciones de amenazas. Consulte la tabla siguiente para conocer la información sobre los puertos necesarios para registrarse en App Gateway.
32. Antes de empezar asegúrese de haber completado "Agregar Core como su servidor MDM en zConsole" en la página 11.
33. En la tabla siguiente se describen las reglas de firewall necesarias para el acceso a Internet/Externo para:
  - Ivanti Core Appliance (físico o virtual): todos los puertos (excepto UDP) deben ser "bidireccionales" para permitir el intercambio de información/datos entre sistemas.
  - Sentry Appliance (físico o virtual, ActiveSync/AppTunnel): el Sentry debe poder resolver el nombre de host Core (a través de la búsqueda DNS) o se debe agregar una entrada de archivo host.
34. Ivanti Core Appliance y los elementos de Sentry Appliance se comunican entre sí.

TABLA 3. REGLAS EXTERNAS E INTERNET

Requisito	Descripción	Puerto
<b>Tráfico de Internet/Exterior hacia CORE</b> CORE está en la DMZ		
Escaneo de Mobile Threat Defense en iOS	URL de la puerta de enlace del servicio de red de voz (VNS): URL de registro: <a href="https://appgw.mobileiron.com/api/v1/gateway/vns/organization:mobileiron.com/api/v1/gateway/vns/configurationde">https://appgw.mobileiron.com/api/v1/gateway/vns/organization:mobileiron.com/api/v1/gateway/vns/configurationde</a> <a href="https://appgw.mob">https://appgw.mob</a>	HTTPS 443
<b>Tráfico desde CORE a Internet / Exterior</b> CORE está en la DMZ		
Servicios APNS y MDM de Apple	Abra los puertos 443 (HTTPS) y 2195, 2196, 2197 (TCP) entre Core y la red Apple Push Notification Service (APNS) de Apple (17.0.0.0/8) para admitir APNS para dispositivos iOS. Si no está utilizando iOS MDM, entonces este puerto no es necesario. HTTPS 443: api.push.apple.com TCP 2195: gateway.push.apple.com TCP 2196: feedback.push.apple.com TCP 2197: api.push.apple.com (opcional, alternativa para	HTTPS 443 TCP 2195, 2196, 2197

Requisito	Descripción	Puerto
	HTTPS 443)	
Puerta de enlace principal	<p><b>support.mobileiron.com</b> (199.127.90.0/23) para el repositorio de actualizaciones de software y la carga del registro de showtech.</p> <p>Abra HTTPS 443 para <b>appgw.mobileiron.com</b>, <b>coresms.mobileiron.com</b>, <b>coreapns.mobileiron.com</b>, <b>clm.mobileiron.com</b>, <b>api.push.apple.com</b>, <b>supportcdn.mobileiron.com</b>, <b>coregcm.mobileiron.com</b> y <b>corefcm.mobileiron.com</b> (199.127.90.0/23) para datos de búsqueda de ubicación/número, registro en la aplicación, mensajería APNS/FCM/GCM, licencias, y soporte para el envío de SMS. <b>a.mobileiron.net</b> para la recopilación de estadísticas anónimas.</p> <p>Como el rango de IP para los sitios CDN (por ejemplo: supportcdn.mobileiron.com) puede cambiar de vez en cuando, incluya en la lista blanca el nombre de dominio en lugar de la IP en el firewall si hay una opción para hacerlo. De lo contrario, utilice support.mobileiron.com para descargar las actualizaciones en lugar de supportcdn.mobileiron.com.</p>	HTTPS 443
Repositorio de la comunidad AppConfig	<a href="https://appconfig.cdn.mobileiron.com">https://appconfig.cdn.mobileiron.com</a>	HTTPS 443

### Reglas de firewall adicionales

35. En la tabla siguiente se describen reglas de firewall adicionales desde la red corporativa interna hasta Internet.

- Las organizaciones con Wifi conectado a la red local deben reflejar la configuración del puerto del firewall externo en su firewall DMZ local para que los dispositivos conectados a Wifi se registren y funcionen el día a día.
- Ivanti Sentry no admite la agrupación de conexiones a través del equilibrador de carga. Desactive la agrupación de conexiones del equilibrador de carga antes de implementarla.

TABLA 4. REGLAS FIREWALL ADICIONALES

Requisito	Descripción	Puerto
Dispositivos iOS (solo Wifi)	<p>Abra TCP 5223 para abrir 17.0.0.0/8 y permitir que los dispositivos iOS que utilizan Wifi corporativo accedan al servicio APNS de Apple. Si no está utilizando iOS MDM, entonces este puerto no es necesario.</p> <p><b>Para dispositivos en redes cerradas:</b></p> <p><b>ax.init.itunes.apple.com:</b> Límite actual de tamaño de archivo para descargar aplicaciones a través de la red celular.</p> <p><b>ocsp.apple.com:</b> Estado del certificado de distribución utilizado para firmar el perfil de aprovisionamiento.</p>	TCP 5223
Dispositivos Android	<p><b>Para permitir el acceso al servicio FCM o GCM de Google:</b> abra los puertos TCP 5228, 5229 y 5230. FCM/GCM normalmente solo usa TCP 5228, pero a veces usa TCP 5229 y TCP 5230. FCM/GCM no proporciona IP específicas, por lo que debe permitir que su firewall acepte conexiones salientes a todas las direcciones IP contenidas en los bloques de IP enumerados en el ASN de Google de 15169. Para dispositivos más antiguos, considere abrir HTTPS 443, también.</p> <p>Para Android Enterprise: <a href="https://www.googleapis.com/Androidenterprise">https://www.googleapis.com/Androidenterprise</a> <a href="https://accounts.google.com/o/oauth2/token">https://accounts.google.com/o/oauth2/token</a></p> <p><b>Para Help@Work para Android:</b> En general, TeamViewer siempre funcionará si es posible el acceso a Internet. Como alternativa a HTTP 80, HTTPS 443 también está marcado. También es posible abrir solo TCP 5938 (necesario para conexiones móviles).</p>	TCP 5228 TCP 5229 TCP 5230 HTTPS 443

36. Para obtener la lista completa de puertos, consulte la *Guía de instalación de Ivanti Core On-Premise para Core y Enterprise Connector*.
37. Al registrar MTD por primera vez, aparece un mensaje de actualización de la configuración que solicita al usuario del dispositivo: "¿Acepta permitir que su empresa recopile la lista de aplicaciones en Este dispositivo para informe al servicio Mobile Threat Defense para proteger los datos de su empresa?" El dispositivo el usuario debe pulsar Aceptar. De lo contrario, el registro Mobile@Work no funcionará y el usuario del dispositivo lo hará.
38. Necesita volver a registrarse y estar de acuerdo.

## 5. FASE DE INSTALACIÓN

### 5.1 HABILITACIÓN DE MTD PARA DISPOSITIVOS MOBILE@WORK

39. Este procedimiento es aplicable tanto a dispositivos Android como iOS. Habilitar la defensa contra amenazas móviles implica:

- Completar los requisitos previos enumerados en "Requisitos previos de Mobile Threat Defense".
- Obtención de su token de activación MTD.
- Creación de una nueva configuración de activación de MTD.
- Aplique etiquetas a la configuración.

40. Una vez hecho esto, el token de activación MTD se entrega a los dispositivos.

41. Tenga en cuenta lo siguiente:

- Para obtener ayuda para activar MTD en los clientes inscritos en Apple Automated Device Enrollment o International Roaming Expert Group (IREG), consulta el artículo basado en conocimientos Permitir la activación de MTD de dispositivos mediante M@W cliente cuando la aplicación se ha suspendido o eliminado en el sitio web de soporte de Ivanti.
- Si tiene una configuración de activación de MTD existente, no la elimine. Instale primero el nuevo token de activación MTD y, a continuación, elimine opcionalmente el anterior.
- Para ser válida, la licencia MTD debe comprarse a Ivanti o a un socio con licencia.

#### 5.1.1. CREACIÓN DE UNA CONFIGURACIÓN DE ACTIVACIÓN DE MTD

42. Procedimiento:

1. Inicie sesión en zConsole y descargue el código de activación de Mobile Threat Defense.
2. En Core, vaya a **Políticas y configuraciones > Configuraciones**.
3. Haga clic en **Agregar nuevo > activación de MTD**. Se abrirá el cuadro de diálogo Agregar configuración de activación de MTD.
4. Introduzca un nombre y una descripción opcional para la configuración.
5. En la sección **Configuración**, realice las siguientes entradas:  
**Vendedor:** Zimperium  
**Clave de licencia:** introduzca su código de activación MTD.
6. Haga clic en **Guardar**. La página Configuraciones se actualiza con el nombre de la nueva configuración de activación de MTD.

7. Aplique una etiqueta a la configuración de activación de MTD. Tras el próximo check-in, la nueva configuración de activación se envía a los dispositivos. Consulte "Creación de etiquetas MTD en Core para dispositivos Android e iOS".

### 5.1.2. DESACTIVACIÓN DE MTD EN CORE

43. Puede deshabilitar MTD y eliminar la configuración de MTD de Mobile@Work dispositivos de varias maneras:

- Eliminar la configuración de las etiquetas del dispositivo
- Eliminar la configuración de MTD

44. **Procedimiento:**

1. Desde el núcleo, vaya a **Políticas y configuraciones >Configuraciones**.
2. Haga clic en la casilla de verificación de la configuración de Mobile Threat Defense.
  - Para **eliminar** la configuración, haga clic en el menú Acciones, seleccione **Eliminar** y confirme la eliminación.
  - Para **quitar** la configuración de los dispositivos, haga clic en el menú Acciones, seleccione **Quitar de la etiqueta**, seleccione las etiquetas de la lista y haga clic en **Quitar**.

### 5.1.3. COMPROBACIÓN FUNCIONAMIENTO MTD

45. Para comprobar que MobileIron Threat Detection funciona, los usuarios de dispositivos pueden revisar la pantalla Mobile@Work y los administradores pueden realizar una protección forzada de dispositivos. También puede utilizar zConsole para comprobar que los tokens de activación MTD se han distribuido a los dispositivos seleccionados mediante la aplicación de la etiqueta correcta.

46. Se puede verificar que MobileIron Threat Detection está funcionando comprobando Dispositivos en Core.

1. Desde MobileIron Core Admin Portal, vaya a **Dispositivos y usuarios > dispositivos**.
2. Seleccione el **icono ^** junto al nombre para mostrar del dispositivo que desea verificar. Se muestra la información del dispositivo.
3. En la pestaña Detalles del dispositivo, busque **Estado de MobileIron Threat Defense**:

TABLA 5. MENSAJE DE ESTADO DEL DISPOSITIVO

Tipo de dispositivo	Uso de la versión de cliente	Mensaje de estado del dispositivo
iOS	Mobile@Work cliente 10.2.0.0	"Activado"

Tipo de dispositivo	Uso de la versión de cliente	Mensaje de estado del dispositivo
	Mobile@Work cliente 10.4.0.0 a través de la versión más reciente admitida por MobileIron	"Protegido"
<b>Android</b>	Mobile@Work cliente 10.1.0.0	"Análisis de amenazas activado habilitado"
	Mobile@Work cliente 10.2.0.0 a través de la versión más reciente admitida por MobileIron	"Protegido"

47. Para comprobar que MTD funciona en todos los dispositivos, los administradores pueden realizar una comprobación forzada de dispositivos.

48. **Procedimiento:**

1. En el Portal de administración de Ivanti, haga clic en la pestaña **Dispositivos**.
2. Seleccione los dispositivos que desea registrar.
3. En el menú, seleccione **Forzar check-in**.

## 6. FASE DE CONFIGURACIÓN

### 6.1 DEFINICIÓN DE POLÍTICAS

49. Mobile Threat Defense utiliza políticas para regular el comportamiento de los dispositivos habilitados para MTD. Cada política consta de un conjunto de reglas. Puede crear varias políticas para cada tipo de política, pero solo se puede aplicar una política activa de cada tipo a un dispositivo específico.
50. Los tipos de políticas utilizadas por Mobile Threat Defense incluyen:
- Acciones de mitigación y cumplimiento de múltiples niveles. Consulte "Mitigación y cumplimiento iniciados por el servidor".
  - MTD Acciones locales políticas de defensa contra amenazas. Consulte "Mitigación y cumplimiento iniciados localmente".
  - Protección contra phishing. Consulte "Protección contra phishing para dispositivos MTD"
  - Políticas de sincronización. Consulte "Actualización de la política de sincronización principal".
  - Políticas de privacidad. Consulte "Configuración de la política de privacidad".

#### 6.1.1. CONFIGURACIÓN DEL INTERVALO DE ACTIVACIÓN MTD PARA DISPOSITIVOS IOS

51. Puede ajustar el intervalo de activación MTD predeterminado para dispositivos iOS desde el menú Política de **sincronización** de la página **Políticas y configuraciones** del portal de administración. Anteriormente, el intervalo de activación de MTD iOS predeterminado era de 15 minutos, lo que a veces resultaba en un uso excesivo de la batería para los clientes de iOS. Para la versión 10.7.0.0 y las versiones compatibles más recientes, el intervalo de activación predeterminado de MTD iOS es de 60 minutos, que se puede ajustar para su red. Para obtener instrucciones completas, consulte como **Sincronizar políticas** en el capítulo **Uso de políticas predeterminadas dentro de la guía de Introducción a Core (Getting Started with Core)** de la documentación principal de Ivanti.

#### 6.1.2. CONFIGURACIÓN DEL INTERVALO DE ACTIVACIÓN MTD PARA DISPOSITIVOS IOS

52. Puede crear notificaciones de eventos que el usuario verá en su dispositivo Android o iOS. Las notificaciones se envían a través de notificaciones push, SMS o correo electrónico, y solo se aplican a las infracciones de la política de cumplimiento de la aplicación.
53. En el contexto de la detección de amenazas de Ivanti, las notificaciones de eventos de cumplimiento iniciados por el servidor se rigen y controlan mediante zConsole. Cuando zConsole detecta un evento no conforme, genera una acción de

cumplimiento y envía un mensaje a los dispositivos afectados. Este es un proceso independiente de la notificación de cumplimiento para la política acciones locales.

54. Antes de empezar asegúrese de haber completado la definición de una política de seguridad MTD en Core.

55. **Procedimiento:**

1. En el Portal de administración principal, seleccione **Registros** > Configuración de **eventos**.
2. Seleccione **Agregar nuevo evento de** > de infracciones de políticas. Se abrirá el cuadro de diálogo Evento de nuevas infracciones de políticas.
3. Introduzca un nombre descriptivo en el campo Nombre, como MTD–ExploitDetected.
4. Desplácese hacia abajo hasta la sección Desencadenadores de políticas de seguridad. Seleccione los siguientes campos en el encabezado Control de aplicaciones - Todas las plataformas:
  - a) **Aplicación no permitida encontrada**
  - b) **Aplicación encontrada que no está en la lista Aplicaciones permitidas**
  - c) **Aplicación requerida no encontrada**
5. Para dispositivos iOS, desplácese hacia abajo hasta la sección iOS. Seleccione los siguientes campos:
  - a) **Se ha encontrado un modelo de iOS no permitido**
  - b) **Se ha encontrado una versión de iOS no permitida**
  - c) **Dispositivo iOS comprometido detectado**
  - d) **La configuración de iOS no es compatible**
  - e) **Dispositivo restaurado conectado al servidor**
  - f) **Activaciones basadas en la ubicación de iOS deshabilitadas por el usuario**
  - g) **MDM del dispositivo desactivado (iOS 5.0 o posterior)**
6. Para dispositivos Android, desplácese hacia abajo hasta la sección Android. Seleccione los siguientes campos:
  - a) **Se ha encontrado una versión no permitida del sistema operativo Android**
  - b) **Dispositivo Android comprometido detectado**
  - c) **Administración de dispositivos no activada para el cliente o agente de DM**
  - d) **Error de atestación**
7. Para dispositivos iOS y Android, desplácese hacia abajo hasta la sección Acciones. En el encabezado Configuración de alertas, configure las siguientes opciones:
  - a) Seleccione el botón de opción situado junto a **Limitado** en **Alertas máximas**.

- b) Seleccione el menú desplegable de **1 día** en **Alertar cada**.
  - c) Seleccione **Ninguno** o **Sólo usuario** para el campo **Enviar SMS**.
  - d) Seleccione **Solo usuario** o **Usuario + Administrador** para el campo **Enviar** a través de notificaciones push.
  - e) Mueva una etiqueta, como “MTD--ExploitedDetected”, de las columnas **Disponible** a seleccionado del campo **Aplicar a etiquetas**.
8. Haga clic en el botón Crear situado junto al campo Plantilla. Se abrirá el cuadro de diálogo Agregar nueva plantilla del Centro de eventos. Introduzca los siguientes campos:
- a) Escriba un nombre para la plantilla en el campo Nombre. Por ejemplo, use MTD-ExploitedDetected como nombre de plantilla.
  - b) Seleccione un idioma con el menú desplegable del campo **Editar plantilla para**.

FIGURA 2. AÑADIR NEW EVENT CENTER TEMPLATE

9. (Opcional) En el campo Mensaje, escriba el texto de las alertas generadas por infracciones de la regla de política de cumplimiento.

TABLA 6. EVENT CENTER VARIABLES SUPPORT

Tipo	Variables admitidas
Asunto del correo electrónico	<i>\$SEVERITY</i> : la gravedad definida del <b>evento</b> del sistema, por ejemplo, Información, Advertencia o Crítico.
Cuerpo del correo electrónico	<i>\$PHONE_NUMBER</i> - El número de teléfono utilizado por el dispositivo.
SMS	<i>\$USER_NAME</i> : el nombre para mostrar del usuario asociado al dispositivo.
APNS	<i>\$DEFAULT_POLICY_VIOLATION_MESSAGE</i> : el mensaje codificado de forma rígida asociado a la infracción de la política que desencadenó la alerta.

No se admiten sustituciones de variables de atributos personalizados

10. Haga clic en **Guardar** para guardar la plantilla. Aparece la página Evento de infracción de nueva política.

11. Haga clic en **Guardar**.

56. Próximos pasos, vaya a "Configuración de la política de respuesta a amenazas móviles de zConsole".

## 6.2 MITIGACIÓN Y CUMPLIMIENTO INICIADOS POR EL SERVIDOR

57. La configuración de la mitigación y el cumplimiento iniciados por el servidor para MTD requiere las siguientes tareas:

1. "Creación de etiquetas MTD en Core para dispositivos Android e iOS"
2. "Creación y aplicación de acciones de cumplimiento de varios niveles iniciadas por el servidor" a continuación
3. "Creación de reglas y grupos de políticas de cumplimiento"
4. "Configuración de la política de respuesta a amenazas móviles de zConsole"
5. "Actualización de la política de sincronización principal"

58. Tanto las acciones de cumplimiento locales como las iniciadas por el servidor pueden existir simultáneamente, no son mutuamente excluyentes.

### 6.2.1. CREACIÓN Y APLICACIÓN DE ACCIONES DE CUMPLIMIENTO DE VARIOS NIVELES INICIADAS POR EL SERVIDOR

59. En esta sección se describe cómo crear y aplicar acciones de cumplimiento iniciadas por la consola z (Por Acciones locales MTD, consulte "Creación de acciones locales MTD en Core").

60. Los dispositivos de usuario pueden activar un registro con zConsole, pero zConsole lo inicia en Core y, a continuación, Core envía un comando al dispositivo para realizar el registro. De esta manera, los dispositivos están protegidos contra amenazas de malware, dispositivos, redes y aplicaciones de día cero sin tener que esperar al próximo evento de registro programado.

61. Las acciones de cumplimiento se evalúan durante el evento de registro del cliente y core aplica las acciones de cumplimiento seleccionadas en el cliente, cuando se determina que el dispositivo no cumple con la política.

62. Para que la función de acciones de cumplimiento de varios niveles funcione, los usuarios del dispositivo deben tener instalada Mobile@Work 10.0.0.0 hasta la versión publicada más recientemente, según lo admita Ivanti.

63. Con acciones de cumplimiento personalizadas, puede crear acciones para administrar mejor el control de acceso. Con las acciones de cumplimiento en niveles, puede personalizarlas para incluir hasta 4 niveles de acción para administrar mejor las acciones de cumplimiento: **Crítico, Elevado, Normal y Bajo**.
64. De forma predeterminada, hay dos acciones de cumplimiento existentes disponibles: **Bloquear correo electrónico, Aplicaciones AppConnect y Enviar alerta**, y **Enviar alerta**. Es una práctica recomendada crear acciones de cumplimiento adicionales que se utilizarán específicamente para MTD, por ejemplo:
- **MTD – Notificar** (basado en la acción de cumplimiento "Enviar alerta")
  - **MTD – Bloquear** (basado en la acción de cumplimiento "Bloquear correo electrónico, aplicaciones app Connect y enviar alerta")
  - **MTD- Cuarentena** (consulte "Acción de cumplimiento de cuarentena" en la página siguiente)
  - **MTD- Cumplimiento** en niveles 4 horas (consulte "Acción de cumplimiento en niveles - 4 horas" en la página siguiente)
65. Antes de empezar, asegúrese de haber completado "Creación de etiquetas MTD en Core para dispositivos Android e iOS" en la página siguiente.
66. **Procedimiento para acción de cumplimiento de cuarentena:**
1. En el Portal de administración principal, seleccione **Políticas y configuraciones > Acciones de cumplimiento**.
  2. Haga clic en el **botón Agregar+**. Se abrirá el cuadro de diálogo Agregar acción de cumplimiento.
    - a. **Nombre:** Introduzca "Cuarentena".
    - b. **Aplicar acciones de cumplimiento localmente en dispositivos:** active la casilla de verificación para aplicar las acciones de cumplimiento en el dispositivo.
  3. En la sección Nivel 1, rellene los siguientes campos:
    - a. **Alerta:** Active la casilla de verificación para enviar una notificación o alerta de cumplimiento al usuario del dispositivo.
    - b. **Bloquear acceso:** seleccione la casilla de verificación para bloquear el acceso al correo electrónico y las aplicaciones AppConnect en el dispositivo. Esta selección no se aplica a los dispositivos macOS.
    - c. Seleccione **Poner en cuarentena el dispositivo** para ponerlo en cuarentena.
    - d. Seleccione **Eliminar todas las configuraciones** para eliminar todos los ajustes de configuración de un dispositivo Android o iOS.

- e. Seleccione **No eliminar** la configuración de **Wi-Fi** para todos los dispositivos (solo iOS, macOS y Android) para permitir que todos los dispositivos iOS y Android mantengan su conexión a Wi-Fi.
  - f. Seleccione **Eliminar iBooks, contenido, aplicaciones administradas y bloquear nuevas descargas** de aplicaciones para eliminar iBooks, contenido y aplicaciones administradas de estos dispositivos, así como para bloquear las descargas de nuevas aplicaciones.
4. Haga clic en **Guardar**.

#### 67. Procedimiento para acción de cumplimiento por niveles: 4 horas

1. Haga clic en el **botón Agregar+**. Se abrirá el cuadro de diálogo Agregar acción de cumplimiento.
2. **Nombre:** Introduzca "Cumplimiento por niveles 4 horas".
3. **Aplicar acciones de cumplimiento localmente en dispositivos:** active la casilla de verificación para aplicar las acciones de cumplimiento en el dispositivo.
4. En la sección Nivel 1, rellene los siguientes campos:
  - a. **Alerta:** Active la casilla de verificación para enviar una notificación o alerta de cumplimiento al usuario del dispositivo.
5. Haga clic en el botón **expandir (+)** en la parte inferior del cuadro de diálogo. Visualización de selecciones de nivel 2.
  - a. Establezca el tiempo de **espera** en 4 horas.
  - b. **Alerta:** Active la casilla de verificación para enviar una notificación o alerta de cumplimiento al usuario del dispositivo.
6. Haga clic en el botón **expandir (+)** en la parte inferior del cuadro de diálogo. Visualización de selecciones de nivel 3.
  - a. Establezca el tiempo de **espera** en 4 horas.
  - b. **Alerta:** Active la casilla de verificación para enviar una notificación o alerta de cumplimiento al usuario del dispositivo.
  - c. **Bloquear acceso:** seleccione la casilla de verificación para bloquear el acceso al correo electrónico y las aplicaciones AppConnect en el dispositivo. Esta selección no se aplica a los dispositivos macOS.
7. Haga clic en el botón **expandir (+)** en la parte inferior del cuadro de diálogo. Visualización de selecciones de nivel 4.
  - a. Establezca el tiempo de **espera** en 4 horas.
  - b. Seleccione **Poner en cuarentena el dispositivo** para ponerlo en cuarentena; la sección se expande.

- c. Seleccione **Eliminar todas las configuraciones** para eliminar todos los ajustes de configuración de un dispositivo Android o iOS.
  - d. Seleccione **No eliminar la configuración de Wi-Fi para todos los dispositivos (solo iOS, macOS y Android)** para permitir que todos los dispositivos iOS y Android mantengan su conexión a Wi-Fi.
  - e. Seleccione **Eliminar iBooks, contenido, aplicaciones administradas y bloquear nuevas descargas** de aplicaciones para eliminar iBooks, contenido y aplicaciones administradas de estos dispositivos, así como para bloquear las descargas de nuevas aplicaciones.
8. Haga clic en **Guardar**.

### 6.2.2. CREACIÓN DE ETIQUETAS MTD EN CORE PARA DISPOSITIVOS ANDROID Y IOS

68. Debe crear varias etiquetas que se aplicarán a dispositivos Android y iOS. En el siguiente procedimiento, cree etiquetas para etiquetas de malware infectado, exploit detectado y etiquetas de amenaza de red.
69. Si las etiquetas se crean después de configurar inicialmente zConsole y sincronizarla con Core, zConsole deberá sincronizarse con Core nuevamente antes de que las etiquetas aparezcan en zConsole.

#### 70. Procedimiento

1. En el Portal de administración principal, seleccione **Dispositivos y usuarios**.
2. Seleccione **Etiquetas > Agregar etiqueta**. Se abrirá el cuadro de diálogo Agregar etiqueta.
3. Asigne a la etiqueta el nombre "MTD-Block", agregue una descripción opcional.
4. En el campo Tipo, seleccione el botón de opción **Manual**. Esta etiqueta se puede aplicar a las amenazas de nivel de gravedad elevado o crítico dentro de las políticas de respuesta a amenazas móviles de zConsole.
5. Haga clic en **Guardar**.
6. Cree una segunda etiqueta "MTD-Notification" y haga clic en el botón de opción **Manual** en la sección Tipo. Esta etiqueta se puede aplicar a las amenazas de gravedad baja o normal dentro de las políticas mobile Threat Response dentro de zConsole.
7. Cree una tercera etiqueta "MTD-Quarantine" y haga clic en el botón de opción **Manual** en la sección Tipo. Esta etiqueta se puede aplicar a las amenazas de nivel de gravedad elevado o crítico dentro de las políticas de respuesta a amenazas móviles de zConsole.
8. Cree una cuarta etiqueta llamada "CUMPLIMIENTO POR NIVELES MTD 4 horas"

y haga clic en el botón de opción **Manual** en la sección Tipo. Esta etiqueta se puede aplicar a amenazas de nivel de gravedad bajo, normal, elevado o crítico dentro de las políticas de respuesta a amenazas móviles de zConsole.

### 6.2.3. CONFIGURACIÓN DE LA POLÍTICA DE RESPUESTA A AMENAZAS DE ZCONSOLE

71. La matriz de respuesta a amenazas (TRM) define las acciones que zConsole realiza al detectar un evento. Entre las opciones se encuentran:

- Habilitar o deshabilitar la detección de una clasificación de amenazas específica
- Alertar al administrador
- Cambiar la gravedad de una amenaza
- Establecer acciones de MDM y acciones de mitigación

72. Antes de empezar, si está configurando "Mitigación y cumplimiento iniciados por el servidor" asegúrese de haber completado los procedimientos enumerados en 6.4.5 CREACIÓN DE GRUPOS Y REGLAS DE POLÍTICAS DE CUMPLIMIENTO. Después de modificar estas opciones, haga clic en **Implementar** para enviar o sincronice el nuevo TRM con los dispositivos activados actualmente. Cuando se integra y sincroniza con Core, cada etiqueta utilizada para la integración se crea como un grupo con su propia política TRM. Consulte la política de TRM de ejemplo.

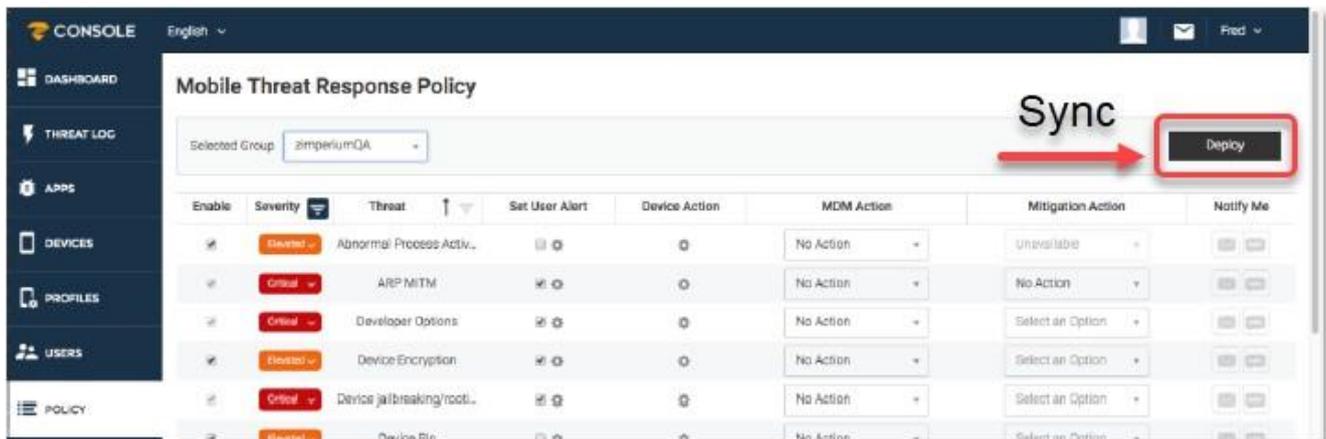


FIGURA 3. EJEMPLO DE MATRIZ DE RESPUESTA ANTE AMENAZAS

TABLA 7. POLITICA DE RESPUESTA ANTE AMENAZAS

Nombre	Descripción
<b>Habilitar</b>	El administrador de zConsole tiene la opción de deshabilitar ciertas detecciones de amenazas y, por lo tanto, la recopilación de análisis forenses asociados.

Nombre	Descripción
<b>Severidad</b>	El administrador tiene la opción de cambiar los niveles de gravedad de la amenaza. Esto es útil para diferentes casos de negocios. Las opciones son "Crítico", "Elevado", "Bajo" y "Normal".
<b>Amenaza</b>	Las amenazas enumeradas en la <b>columna Amenaza</b> representan las clases de amenazas que detecta Mobile Threat Defense. Las clases de amenaza son reconocidas por MTD, que es capaz de determinar cuándo está ocurriendo un evento malicioso.
<b>Establecer alertas de usuario</b>	Los administradores no pueden administrar alertas MTD a través de zConsole. Para implementar y localizar alertas MTD, utilice la política de acciones locales en Core. Consulte "Mitigación y cumplimiento iniciados localmente"
<b>Establecer acción de dispositivo</b>	Los administradores pueden implementar acciones de dispositivos para dispositivos Android e iOS en zConsole. Consulte "Establecer la acción del dispositivo" en la página siguiente.
<b>Acción mdm</b>	Los administradores pueden habilitar elementos de acción de administración de dispositivos móviles (MDM) impuestos por el servidor en la página de políticas de zConsole.  Después de implementar / sincronizar con Core, cuando se detecta una amenaza, zConsole indica a Core que mueva el dispositivo a la etiqueta elegida en la Política / Matriz de respuesta a amenazas. El flujo de trabajo asignado a esa etiqueta determina la acción que Core realiza en el dispositivo.  La comunicación de zConsole a Core se realiza de forma segura a través de una llamada a la API de Ivanti. Consulte "Acción MDM" en la página siguiente.
<b>Medidas de mitigación</b>	Cuando una amenaza detectada por zConsole se ha corregido y ya no representa una amenaza para el dispositivo, puede definir acciones específicas que se pueden realizar. Por ejemplo, cuando se determina que un dispositivo está bajo un ataque Man-in-the-Middle, se puede evitar que acceda a varios recursos corporativos. Cuando el dispositivo se mueve a una red limpia, puede permitir automáticamente que el dispositivo vuelva a acceder a esos recursos. Consulte "Acción de mitigación" en la página siguiente.
<b>Notificaciones</b>	Puede configurar un proceso de notificación por correo electrónico o SMS para cada amenaza específica. Las notificaciones por SMS requieren que la información telefónica del administrador se configura en la página <b>Usuario</b> de un administrador determinado. Cada correo electrónico o SMS contiene un resumen del evento y un enlace al evento real que se puede ver en un navegador después de iniciar sesión. Véase "Notificaciones"

#### 6.2.4. ESTABLECER LA ACCIÓN DEL DISPOSITIVO

73. Los administradores pueden implementar acciones de dispositivos para dispositivos Android e iOS en zConsole.

#### 74. Procedimiento

1. Desde MTD zConsole, vaya a la página **Policy > Threat Policy**.

- Utilice el menú desplegable del campo **Grupo seleccionado** para mostrar el grupo de configuración.
- Seleccione la política que desea modificar.
- En la columna Acción del dispositivo, haga clic en el icono de configuración de la fila seleccionada y seleccione una acción. zConsole se comunica de forma segura con Core



FIGURA 4. ACCIÓN DEL DISPOSITIVO

- Para quitar la acción del dispositivo, desmarque la acción y haga clic en **Aceptar**.
75. Los administradores pueden habilitar elementos de acción de administración de dispositivos móviles (MDM) impuestos por el servidor en la página de políticas de zConsole.
76. **Procedimiento**
- En zConsole, vaya a la página Política de > de amenazas.
  - Utilice el menú desplegable del campo **Grupo seleccionado** para mostrar el grupo de configuración Principal.
  - Seleccione la política que desea modificar.
  - En la columna **Acción de MDM**, haga clic en la flecha desplegable de la fila seleccionada y seleccione una acción. zConsole se comunica de forma segura con Core y aplica la acción.
  - Para quitar una acción de una clasificación de amenazas, cambie la amenaza **Acción mdm** a **Sin acción**.

### 6.2.5. MEDIDAS DE MITIGACIÓN

77. La columna Acción de mitigación se puede utilizar para asignar acciones. Para quitar la acción que se realizó como respuesta a una amenaza que ahora se ha mitigado, elija **Quitar**. Esta acción elimina el dispositivo del grupo al que se asignó cuando se detectó la amenaza.
78. Debido a la naturaleza de algunas amenazas, no todas las clasificaciones de amenazas se pueden mitigar. En la tabla siguiente se proporcionan posibles acciones de mitigación para una amenaza.

TABLA 8. POSIBLES RESPUESTAS DE MITIGACIÓN PARA AMENAZAS

Amenaza	Mitigación cuando se producen los siguientes eventos
Todas las amenazas man-in-the-middle (MITM)	Cuando el dispositivo se conecta a un identificador de conjunto de servicios básico (BSSID) diferente.
Root/Jailbreak	Cuando el indicador raíz de los dispositivos cambia de true a false
EOP, manipulación del sistema, actividad anormal del proceso	Sin mitigación, la única mitigación es flashear el dispositivo ya que se ha visto comprometido
Depuración USB	Cuando la depuración USB está habilitada

### 6.2.6. NOTIFICACIONES

79. En este procedimiento, se configuran las notificaciones y las acciones de mitigación que se aplican a los dispositivos iOS y Android.

80. **Procedimiento:**

1. En el portal zConsole, seleccione **Política**. Aparece la página Política de respuesta a amenazas móviles.
2. Utilice el menú desplegable del campo **Grupo seleccionado** para mostrar el grupo de configuración Principal.
3. Haga clic en el botón **Implementar** para implementar la política en sus dispositivos.
  - La columna **Amenaza** muestra la amenaza admitida que puede detectar el cliente.
  - La columna **Acción** del **dispositivo** muestra la acción realizada después de detectar una amenaza. Esta es una configuración opcional.

### 6.2.7. ACTUALIZACIÓN DE LA POLÍTICA DE SINCRONIZACIÓN PRINCIPAL

81. Un paso final para configurar la mitigación y el cumplimiento es asegurarse de que la política de sincronización esté actualizada.

82. Antes de empezar asegúrese de haber completado "Mitigación y cumplimiento iniciados por el servidor" o "Mitigación y cumplimiento iniciados localmente".
83. Puede establecer la frecuencia para despertar dispositivos iOS y ejecutar un análisis de amenazas.
84. **Procedimiento:**
1. En el portal core Admin, vaya a **Políticas y configuraciones > políticas**.
  2. Haga clic en **Agregar nuevo > Sincronización**. Se abrirá el cuadro de diálogo **Nueva política de sincronización**.  
Si ya existe una política de sincronización, se mostrará la pantalla **Modificar política de sincronización**.
  3. Introduzca el nombre de la política y una descripción si es necesario.
  4. (Solo iOS) Introduzca un **intervalo de activación MTD** en minutos. Este intervalo determina la frecuencia con la que Mobile@Work se despierta y realiza un escaneo MTD en dispositivos iOS. El intervalo de activación predeterminado es **de 15 minutos**. Establecer este valor en un intervalo bajo es más exigente para la batería del dispositivo que configurarlo en un intervalo más alto.
  5. Haga clic en **Guardar**.
  6. Aplique la etiqueta **Todos los teléfonos inteligentes** a la política.
85. La opción **Ciente siempre conectado** solo es aplicable para dispositivos Android y no se aplica a dispositivos iOS. Al seleccionar (habilitar) esta casilla de verificación, se garantiza el escaneo MTD continuo en Android.
86. **Temas relacionados:**
- Para obtener instrucciones generales sobre cómo crear una política de sincronización, consulte *Introducción a Core (Getting Started with Core)* de la documentación principal de Ivanti.
  - Para obtener instrucciones sobre la política de sincronización de iOS, consulta "Intervalo de activación basado en la ubicación de iOS y sincronización con Core" en la *Guía de administración de dispositivos principales para dispositivos iOS y macOS*.
  - Para obtener instrucciones sobre la política de sincronización de Android, consulte "Política de sincronización de notificaciones de Android" en la *Guía de administración de dispositivos principales para dispositivos Android y Android Enterprise*.

### 6.3 PROTECCIÓN CONTRA PHISHING PARA DISPOSITIVOS MTD

87. Mobile Threat Defense Solution detecta y previene los intentos de phishing en dispositivos iOS y Android habilitados para MTD utilizando un enfoque de múltiples capas. La siguiente tabla de referencia rápida identifica las principales opciones anti-phishing para dispositivos MTD en esta versión:

TABLA 9. MTD OPCIONES ANTI PHISING PARA CORE 11

Opción antiphishing	Plataformas soportadas	Características clave	Para más información
<b>Política de phishing de la consola de administración de amenazas</b>			
Habilite la protección contra phishing y habilite el uso compartido de URL	iOS y Android	Habilita las funciones de phishing de Threat Management Console y activa el uso compartido de URL.	Consulte "Habilitar zConsole ANTI-phishing VPN" en la página siguiente.
VPN local para phishing		Habilita la protección contra phishing a través de una VPN local y bloquea las URL de phishing detectadas.	
Habilitar la inspección de contenido en un servidor remoto		Comprueba los vínculos con una base de datos remota más grande.	
<b>Política de protección antiphishing de MTD</b>			
Bloqueador de contenido	iOS	Bloquea todo el tráfico de red cuando se detecta una amenaza de phishing. El usuario cliente de iOS debe habilitarlo.	Consulte "Habilitación de la protección adicional contra el phishing de EMTD"
Controlador de URL	Android	Intercepta la URL en el navegador predeterminado, la escanea y, si es maliciosa, la bloquea. El usuario cliente de Android debe habilitarlo.	
Usar VPN para analizar URL maliciosas	iOS	Comprueba los vínculos con una base de datos en el dispositivo.	
	Android	Comprueba los vínculos con una base de datos en el dispositivo. Requiere: Aplicación MI Tunnel	Consulte " <u>Habilitación de la protección adicional</u> contra el phishing <u>DE MTD</u> ", " <u>Android anti-phishing usando la</u> aplicación MI Tunnel"

Opción antiphishing	Plataformas soportadas	Características clave	Para más información
	Android Enterprise	Comprueba los vínculos con una base de datos en el dispositivo. Requiere: <ul style="list-style-type: none"> <li>• Aplicación MI Tunnel</li> <li>• Configuración de la aplicación para Tunnel.</li> </ul>	Consulte " <a href="#">Android anti-phishing using MI Tunnel app</a> " " <a href="#">Creación de una configuración de aplicación mi tunnel para dispositivos AE</a> "
<b>MTD general</b>			
Configuración de MobileIron Tunnel	Android	Enviado a los usuarios de Android según sea necesario. Configuración del sistema. No editable.	Consulte "Acerca de la configuración del Tunnel MI"

### 6.3.1. PROTECCIÓN AVANZADA CONTRA PHISHING EN DISPOSITIVOS GESTIONADOS

88. Desde Ivanti Core 10.8.0.0 hasta la versión lanzada más recientemente como compatible con MobileIron, puede habilitar la protección avanzada de phishing zConsole para dispositivos iOS y Android habilitados para MTD sin ninguna acción del usuario del cliente. Esta herramienta proporciona una cobertura completa contra URL riesgosas a través de una VPN habilitada automáticamente.

### 6.3.2. HABILITACIÓN ZCONSOLE ANTI-PHISHING VPN

#### 89. Procedimiento

1. Inicie sesión en zConsole.
2. Haga clic en **Política**.
3. En la página Política, haga clic en **Política de suplantación de identidad (phishing)**. Aparece la página de configuración de la política de suplantación de identidad (phishing).

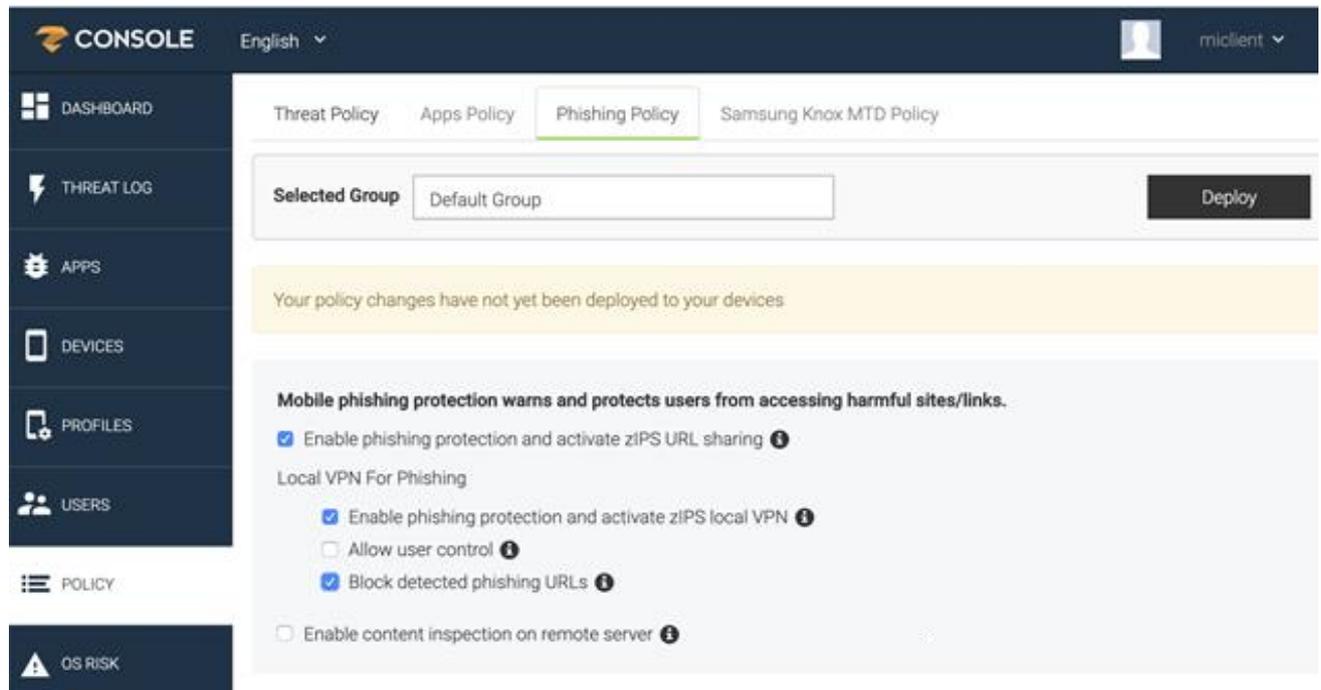


FIGURA 5. PAGINA DE POLITICA ANTI PHISING

4. En el **campo Grupo** seleccionado, seleccione el grupo para recibir protección contra suplantación de identidad (phishing).
5. Seleccione una de las siguientes opciones:
  - Habilite la protección contra phishing y active el uso compartido de URL zIPS: habilitado de forma predeterminada. Marque esta opción para habilitar la protección contra phishing en zConsole.

Los usuarios que inicien una aplicación VPN a nivel de dispositivo como PulseSecure o GlobalProtect desde su dispositivo desconectarán la VPN antiphishing de MobileIron, que deshabilita el anti-phishing en el dispositivo. El usuario del dispositivo debe volver a **Configuración > Configuración VPN** y volver a seleccionar **MobileIron ANTI-phishing VPN** para volver a habilitar la protección anti-phishing.

#### VPN local para-anti-phishing

- **Habilite la protección contra phishing y active iOS local VPN:** habilitado de forma predeterminada. Marque esta opción para habilitar una VPN de anti-phishing local.
- **Permitir control de usuario:** deshabilitado de forma predeterminada. Esta opción no se puede habilitar.
- **Bloquear URL de phishing detectadas:** habilitada de forma predeterminada. Marque esta opción para bloquear las URL de phishing cuando se detecten en un dispositivo.

No deshabilite la opción Política de phishing “Bloquear URL de phishing detectadas”. Si se deshabilita, los usuarios verán una notificación de que

no funciona.

- **Habilitar la inspección de contenido en el servidor** remoto: deshabilitado de forma predeterminada. Esta opción permite a zConsole acceder a una base de datos mucho más grande de sitios en la lista negra que los sitios disponibles en el dispositivo, proporcionando protección multinivel.

Haga clic en **Implementar** para distribuir la política de protección contra suplantación de identidad (phishing) al grupo de dispositivos seleccionado. Para los clientes de iOS, el antiphishing está habilitado.

90. Para los clientes de Android, ver el apartado [6.3.5 ANDROID ANTI-PHISING USANDO LA APLICACIÓN MI TUNNEL](#).

### 6.3.3. HABILITACIÓN DE PROTECCIÓN ADICIONAL CONTRA EL PHISING

91. Tiene la opción de habilitar protecciones antiphishing MTD adicionales para dispositivos Android e iOS administrados:

- **VPN en el dispositivo para analizar URL** maliciosas: esta opción utiliza VPN para proporcionar protección antiphishing sin necesidad de confirmación del usuario final. Los enlaces pulsados se comparan con una base de datos en el dispositivo de URL maliciosas.
- **Bloqueador de contenido:** (dispositivos iOS) Esta opción bloquea todo el tráfico de red cuando se detecta una amenaza de phishing. Una vez despejado, el tráfico de red se permite de nuevo. El usuario final debe habilitar esta característica.
- **Controlador de URL:** (dispositivos Android) Cuando el usuario del dispositivo pulsa una URL, la protección MTD phishing intercepta la URL en el navegador predeterminado, la escanea y, si es maliciosa, la bloquea. De lo contrario, se abrirá la URL. Consulte "Descripción del controlador de URL". Estas configuraciones antiphishing adicionales se pueden usar junto con las políticas antiphishing de Threat Management Console.

92. **Procedimiento:**

1. Inicie sesión en el portal de administración principal.
2. Vaya a **Políticas y configuraciones > políticas**.
3. Haga clic en **Agregar nuevo > MTD Anti-Phishing**. Se abrirá la página **Agregar política antiphishing de MTD**.

FIGURA 6. CREATING AN MTD ANTI-PHISHING POLICY

4. En el cuadro de diálogo **Agregar política antiphishing de MTD**, escriba un nombre para la política.
5. Para el estado, seleccione **Activo**. Esta es la configuración predeterminada.
6. Especifique una prioridad para esta política, en relación con las otras políticas personalizadas del mismo tipo. Seleccione **Superior o Inferior que**, a continuación, seleccione una política existente en la lista desplegable. Esta prioridad determina qué política se aplica si hay más de una política disponible. Solo se puede aplicar una política activa a un dispositivo.
7. (Opcional) Introduzca una descripción.
8. En la sección **iOS**, seleccione una de las siguientes opciones de política:

FIGURA 7. OPCIONES ANTI PHISING PARA IOS MTD

- a. Usar VPN en el dispositivo para analizar URL maliciosas.
  - b. Habilitar el bloqueo de contenido antiphishing.
9. En la sección **Android**, seleccione una de las siguientes opciones de política:

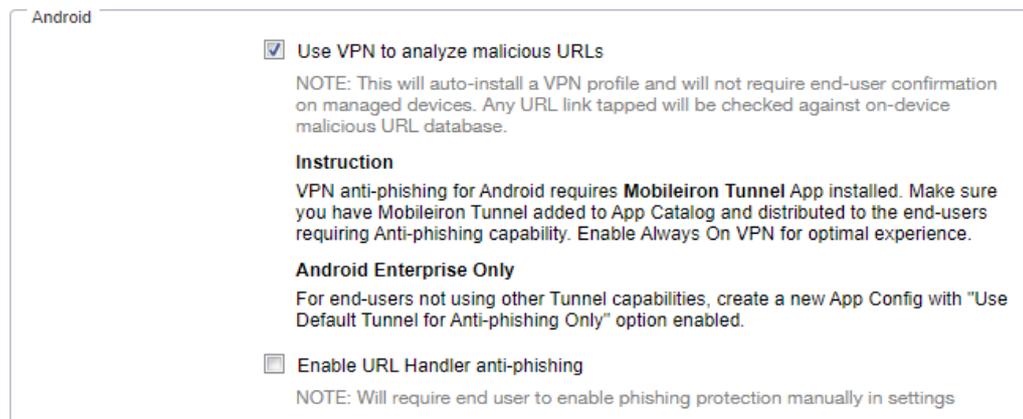


FIGURA 8. OPCIONES ANTI PHISING ANDROID MTD

- a) Usar VPN en el dispositivo para analizar URL maliciosas
  - b) Habilite el controlador de URL antiphishing. Consulte "Descripción del controlador de URL"
10. Haga clic en **Guardar**.
  11. Aplique una etiqueta a la política. Consulte "Creación de etiquetas MTD en Core para dispositivos Android e iOS".
  12. Cree una regla de política de cumplimiento para garantizar que los usuarios del dispositivo habiliten la protección antiphishing de Ivanti. Consulte [6.4.5 CREACIÓN DE GRUPOS Y REGLAS DE POLÍTICAS DE CUMPLIMIENTO](#). Asigne a la política la siguiente configuración:
    - a. **Condición:** MTD Anti-Phishing status / Equals / Not Enabled
    - b. **Expresión regular:**  
`"common.mtd_anti_phishing_status"="CLIENT_NOT_ENABLED"`  
 Esta expresión hace que los dispositivos no cumplan con las normas y desencadena una acción de cumplimiento que obliga a los usuarios de dispositivos a habilitar la protección contra phishing MTD
  13. Forzar el registro del dispositivo.
93. El antiphishing de Content Blocker no funcionará en dispositivos iOS que tengan habilitada la opción de "Bloquear ventanas Emergentes en Safari" en la configuración de su dispositivo iOS.
  94. Debe distribuir una configuración de restricción de iOS con la opción de "Bloquear ventanas emergentes" deshabilitada y compruebe que esta restricción está deshabilitada en los dispositivos cliente.

#### 6.3.4. USO DE UNA BASE DE DATOS REMOTA PARA VALIDAR DIRECCIONES URL

95. De forma predeterminada, la política de phishing está configurada para usar una base de datos en el dispositivo para detectar URL de phishing. Si prefiere que sus dispositivos tengan acceso a una base de datos mucho más grande y actualizada en tiempo real, puede configurarla a través de zConsole. También puede configurar esta opción al configurar PROTECCIÓN AVANZADA CONTRA PHISHING EN DISPOSITIVOS GESTIONADOS.

96. **Procedimiento:**

1. Inicie sesión en zConsole.
2. Vaya a **Policies > Anti-phishing Policy**.
3. Seleccione el grupo de dispositivos que desee en la política.
4. Seleccione estas opciones:
  - **Habilite la protección contra phishing y active el uso compartido de URL zIPS**
  - **Habilitar la inspección de contenido en un servidor remoto**

La opción para permitir el control del usuario de la VPN de phishing está deshabilitada.

5. Implemente los cambios.

#### 6.3.5. ANDROID ANTI-PHISHING USANDO LA APLICACIÓN MI TUNNEL

97. Una vez que tenga "Protección avanzada contra phishing para dispositivos administrados" para dispositivos Android a través de zConsole, deberá aprovisionar clientes Android con la aplicación MI Tunnel, para proporcionar una ruta VPN. Consulte "Implementación de la aplicación MI Tunnel en dispositivos Android y Android Enterprise" a continuación.

98. Los clientes de Android Enterprise (AE) necesitan una configuración de aplicación adicional con la opción "Usar Tunnel solo para antiphishing" habilitada. Esto permite el antiphishing para los usuarios finales que no utilizan otras capacidades de Tunnel. Consulte "Creación de una configuración de aplicación de MI TUNNEL para dispositivos AE" en la página siguiente.

99. Complete la siguiente tarea antes de comenzar: "Protección avanzada contra phishing para dispositivos gestionados"

100. **Procedimiento:**

1. En la **página Catálogo de aplicaciones > aplicaciones**, haga clic en **Agregar+**. Se abre una selección del catálogo de aplicaciones públicas.
2. Haz clic en **Google Play**.
3. En el campo **Nombre de la aplicación**, escriba la **aplicación MI TUNNEL** y haga

clic en **Buscar**.

4. En las opciones disponibles, haga clic en la **aplicación MI TUNNEL** y haga clic en **Siguiente**.
5. Haga clic en **Siguiente de nuevo**.
6. Haga clic en **Finalizar**.
7. En la página **Catálogo de aplicaciones**, seleccione la **aplicación MI TUNNEL**.
8. Haga clic en **Editar**.
9. En el campo Categoría, seleccione **Tunnel MI antiphishing**.
10. En la sección **catálogo Apps@Work**, seleccione si desea incluir la aplicación.
11. Haga clic en **Finalizar**. Aplique la aplicación MI Tunnel a las etiquetas para que esté disponible para los dispositivos con la etiqueta.

101. **Próximos pasos:** Para completar el antiphishing de Android para clientes Android Enterprise, continúe con "Creación de una configuración de aplicación de MI Tunnel para dispositivos AE" a continuación.

102. **Temas relacionados:** Para obtener más información sobre el Catálogo de aplicaciones, consulte "Administración de aplicaciones móviles para Android" en la Guía de *Apps@Work* principales. "Protección avanzada contra phishing para dispositivos gestionados"

### 6.3.6. CREACIÓN DE UNA CONFIGURACIÓN DE MI TUNNEL PARA DISPOSITIVOS ANDROID ENTERPRISE

103. El paso final para habilitar la protección antiphishing en dispositivos Android Enterprise (AE) es crear y enviar un archivo de configuración de la aplicación MI Tunnel a dispositivos AE.

104. Antes de empezar, complete las siguientes tareas:

- "Protección avanzada contra phishing para dispositivos gestionados"
- "Android anti-phishing usando la aplicación MI Tunnel" en la página anterior

105. **Procedimiento**

1. En la **página Catálogo de aplicaciones > aplicaciones**, haga clic en la aplicación MI TUNNEL que descargó anteriormente. Se abrirá la página Detalles globales.
2. Haga clic en **Editar**. Se abrirá la pantalla de edición de la aplicación MI Tunnel.
3. En el campo **Categoría**, seleccione o cree la categoría **MI Tunnel antiphishing**.
4. En la sección **catálogo Apps@Work**, seleccione si desea incluir la aplicación.

5. Seleccione Instalar esta aplicación para Android Enterprise.
6. Haga clic en **Usar Tunnel solo para antiphishing**.

Vpn anti-phishing requiere que la configuración de la aplicación MI Tunnel esté instalada en el dispositivo.

Seleccione esta opción si no se utiliza ninguna otra funcionalidad relacionada con el Tunnel y distribuya la aplicación a los usuarios que necesiten antiphishing.

7. Haga clic **en Finalizar**. Las aplicaciones se ponen a disposición de los dispositivos con la etiqueta. Dependiendo de cómo se haya configurado la etiqueta, la aplicación se instala de forma silenciosa (no se requiere ninguna acción por parte del usuario del dispositivo) y, en otros casos, está disponible, pero requiere que el usuario lo instale.

106.**Acerca de la configuración de MI Tunnel**, hay disponible una configuración de Tunnel predeterminada (configuración de MI Tunnel) para Core 11.0.0.0 y versiones posteriores. Si un dispositivo Android no tienen la configuración distribuida, el servidor enviará la configuración predeterminada MI Tunnel cuando sea necesario.

107.La configuración de MI Tunnel es generada por el sistema y siempre está disponible. No es editable.

### 6.3.7. DESCRIPCIÓN DEL CONTROLADOR DE URL

108.Puede configurar la protección antiphishing de URL Handler para dispositivos Android y Android Enterprise con o sin la opción VPN antiphishing. Ivanti intenta establecerse como el interceptor de URL predeterminado para proporcionar protección contra phishing, de modo que pueda escanear la URL y bloquear la URL si no es segura.

109.En los dispositivos Android administrados en Core, URL Handler no puede proporcionar protección antiphishing si el usuario final escribe la URL en un navegador manualmente.

110.Es necesario comprender los modelos y modos de implementación para dispositivos y modos Android. Para obtener información acerca de los dispositivos de implementación de Android, consulte "Modelos de implementación de Android" en la Guía de administración de dispositivos principales para dispositivos Android y Android Enterprise.

111.Para obtener información sobre los modos para dispositivos Android Enterprise, consulte "Información general de Android Enterprise" en la Guía de administración de dispositivos principales para dispositivos Android y Android Enterprise.

112. En el portal de administración, cree una política antiphishing MTD para garantizar que los usuarios del dispositivo se bloqueen de las URL maliciosas.
113. Los usuarios de dispositivos habilitan la protección contra phishing de Ivanti URL Handler.
114. Android nativo y Android Knox: se envía una notificación a los dispositivos de los usuarios indicando que se ha habilitado la protección contra phishing de Ivanti y se invita al usuario del dispositivo a activarla en el dispositivo. Durante este proceso, se solicita al usuario del dispositivo que seleccione un navegador predeterminado. Se recomienda que el usuario del dispositivo seleccione Mobile@Work como navegador predeterminado. La elección del navegador por parte del usuario se guarda en el dispositivo.
115. Si el usuario del dispositivo no habilita Ivanti Phishing Protection o el dispositivo se considera no compatible, no se le pedirá al usuario final que establezca Mobile@Work como predeterminado Explorador.
116. Android Enterprise: Ivanti Phishing Protection se habilita silenciosamente en el dispositivo del usuario con Mobile@Work como navegador predeterminado.
117. Para verificar si un usuario de dispositivo habilitó Ivanti Phishing Protection, consulte la página Detalles del dispositivo en Core.
118. Cuando el usuario del dispositivo pulsa una URL, se activa Ivanti Phishing Protection. El navegador predeterminado intercepta la URL, la escanea y, si es maliciosa, la bloquea. De lo contrario, la URL se abre en un navegador instalado. Mobile@Work lo pasa a un navegador instalado (si solo hay un navegador en el dispositivo) o a una lista de navegadores (si hay varios navegadores en el dispositivo). La elección del navegador por parte del usuario se guarda en el dispositivo.
119. Consulte la tabla para obtener una lista de las versiones de Android para el navegador predeterminado.

TABLA 10. ACCION POR DEFECTO DEL NAVEGADOR EN ANDROID

Modo de dispositivo	Cómo seleccionar el cliente Ivanti como navegador predeterminado
Modo de administración de dispositivos	<b>Android 7.0 a través de la última versión compatible con Ivanti:</b> Se guía al usuario para seleccionar el cliente Ivanti como la aplicación de navegador predeterminada desde la configuración predeterminada de las aplicaciones.
Perfil de trabajo (propietario del perfil) (Android 5.0 a través de la última versión compatible con Ivanti) Dispositivo administrado (propietario del dispositivo) (Android 5.0 a través de la última versión compatible con Ivanti)	<b>Android Enterprise:</b> El cliente Ivanti está configurado como el navegador predeterminado. Solo se solicita al usuario que establezca el cliente de MobileIron como navegador predeterminado si la configuración se deshabilita.

Modo de dispositivo	Cómo seleccionar el cliente Ivanti como navegador predeterminado
Dispositivo administrado con propietario de perfil (Android 8.0 a través de la última versión compatible con Ivanti)	<p>Tanto para el lado del dispositivo como para el lado del perfil, el cliente Ivanti se establecerá como el navegador predeterminado en Configuración, excepto en los dispositivos Samsung.</p> <p>En los dispositivos Samsung, el usuario debe elegir explícitamente el cliente Ivanti como el navegador predeterminado en la configuración del dispositivo y la configuración de trabajo. La configuración de trabajo y la configuración del dispositivo para la aplicación del navegador no se encuentran en la misma página configuración.</p>
AppConnect (Android 5.0 a través de la última versión compatible con Ivanti)	<p>Ivanti recomienda distribuir Ivanti Web@Work y habilitar lo siguiente en la política Global AppConnect para la protección antiphishing:</p> <ul style="list-style-type: none"> <li>• <b>Permitir web:</b> si está habilitado, un navegador no seguro puede intentar mostrar una página web cuando un usuario de dispositivo pulsa la URL de la página en una aplicación segura.</li> <li>• <b>Permitir que las aplicaciones que no son de AppConnect inicien la URL mediante Web@Work:</b> esto garantizará que en los clics de URL dentro y fuera del contenedor, el cliente de Ivanti pueda interceptar la URL para protección contra phishing y utilizar la Web@Work instalada para mostrar las URL seguras. Para obtener más información, consulte la sección <b>AppConnect</b> en la documentación del producto Ivanti en MobileIron Cloud.</li> </ul>

120.Consulte la tabla siguiente para conocer el comportamiento esperado después de que el cliente de Ivanti se haya establecido o seleccionado como el explorador predeterminado para proporcionar protección contra suplantación de identidad (phishing).

TABLA 11. COMPORTAMIENTO ESPERADO DEL CLIENTE ANDROID POR VERSION

Modo de dispositivo	Descripción	Comportamiento esperado
<b>Quiosco</b>	Dispositivos Samsung Android 5.0 a 8.0 y no Samsung Android 5.0 a 7.0.	<p>Cuando los clics de URL están dentro del quiosco, si la URL es segura, se mostrará con los navegadores disponibles en el modo de quiosco. El modo quiosco permanece activo y funcional si la protección contra phishing se habilitó fuera del quiosco y luego se eliminó mientras el dispositivo está en modo quiosco. Salir del modo de quiosco dentro y fuera del modo de quiosco mantiene la protección contra phishing funcional dentro y fuera del quiosco.</p> <p>Cuando un usuario pulsa una URL:</p> <ul style="list-style-type: none"> <li>• Si la URL no es segura, se bloqueará.</li> <li>• Si la URL es segura, el cliente de Ivanti representará la URL con el navegador disponible o mostrará una lista de navegadores para que el usuario final elija mostrar las URL "Solo una vez" o "Siempre".</li> </ul>

Modo de dispositivo	Descripción	Comportamiento esperado
		<ul style="list-style-type: none"> <li>◦ <b>Solo una vez:</b> Ivanti continuará mostrando una lista de navegadores si hay varios navegadores.</li> <li>◦ <b>Siempre</b> – El cliente de Ivanti guardará el navegador seleccionado. La próxima vez, el paquete de navegador guardado se utiliza para representar URL seguras.</li> </ul> <p>Una vez que el usuario selecciona "Siempre" a través de la lista de navegadores del cliente Ivanti, el usuario no puede cambiar el navegador predeterminado para representar URL seguras. Como solución alternativa, instale un nuevo explorador. Al hacer clic en la siguiente URL segura, se mostrará de nuevo al usuario una lista de navegadores, incluido el nuevo navegador.</p>
<b>Propietario del dispositivo Android Enterprise del quiosco</b>	Android 5.0 a través de la última versión según lo soportado por Ivanti.	

### 6.3.8. TAREAS DE CONFIGURACIÓN DE PHISHING DE ANDROID HEREDADAS

121. Estos clientes de Android heredados requieren que sus usuarios seleccionen el cliente MobileIron como navegador predeterminado y algunas tareas adicionales.

TABLA 12. TAREAS ADICIONALES DE CONFIGURACION ANTI PHISHING

Tarea	Descripción
<b>AppConnect</b> (Android 5.0+)	<p>En la configuración del contenedor Android AppConnect, los administradores deben distribuir Web@Work y habilitar los siguientes bloqueos para la protección contra phishing:</p> <ul style="list-style-type: none"> <li>• Permitir Web</li> <li>• Permitir que las aplicaciones que no son de AppConnect abran direcciones URL en Web@Work</li> </ul> <p>Esto asegurará que en los clics de URL dentro y fuera del contenedor, el cliente de Ivanti pueda interceptar la URL para la protección contra phishing y usar el Web@Work instalado para mostrar las URL seguras. Para obtener más información, consulte la sección <b>AppConnect</b> en la documentación del producto Ivanti en MobileIron Cloud.</p>

Tarea	Descripción
<b>Modo de administración de dispositivos de quiosco</b> (dispositivos Samsung de Android 5.x a 8.x y dispositivos que no son de Samsung de Android 5.x a 7.x) y <b>modo de propietario de dispositivos Android Enterprise de quiosco</b> (Android 5.0+)	Cuando los clics de URL están dentro del quiosco, si la URL es segura, se mostrará con los navegadores disponibles en el modo de quiosco. El modo quiosco permanece activo y funcional si la protección contra phishing se habilitó fuera del quiosco y luego se eliminó mientras el dispositivo está en modo quiosco. Salir del modo de quiosco dentro y fuera del modo de quiosco mantiene la protección contra phishing funcional dentro y fuera del quiosco.

122. Cuando un usuario hace clic en una URL:

- Si la URL no es segura, se bloqueará.
- Si la URL es segura, el cliente de Ivanti representará la URL con el navegador disponible o mostrará una lista de navegadores. Se pregunta al usuario final si desea utilizar este navegador **solo una vez** o **siempre**.
  - Para **Just Once**, Ivanti continuará mostrando una lista de navegadores, si hay varios navegadores.
  - Para **Always**, el cliente de Ivanti guardará el navegador seleccionado y lo usará para representar URL seguras en el futuro.

123. Una vez que el usuario selecciona "Siempre" a través de la lista de navegadores del cliente de MobileIron, el usuario no puede cambiar el navegador predeterminado para representar URL seguras. Como solución alternativa, instale un nuevo explorador. Al hacer clic en la siguiente URL segura, se mostrará de nuevo al usuario una lista de navegadores, incluido el nuevo navegador.

### 6.3.9. USO DE LA PÁGINA DE DETALLES DEL DISPOSITIVO PARA VERIFICAR QUE EL ANTIPHISHING ESTÁ HABILITADO

124. Después de elegir Forzar la protección del dispositivo, puede verificar que la configuración antiphishing esté habilitada en un dispositivo determinado comprobando los detalles del dispositivo para ese dispositivo.

125. **Procedimiento:**

1. En el Portal de administración principal, seleccione **Dispositivos y usuarios > dispositivos**.
2. Haga clic en el quilate (^) junto al dispositivo habilitado para MTD correspondiente.
3. En Detalles del dispositivo, **MTD Anti-Phishing Status** también mostrará el estado actual en uno de los siguientes valores:
  - **N/A** – La política de protección antiphishing de Ivanti no es distribuida por el

administrador o la política no se aplica.

- **Habilitado:** los usuarios del dispositivo recibieron una solicitud del administrador para activar manualmente la protección antiphishing de Ivanti y la han habilitado.
- **No habilitado:** los usuarios del dispositivo recibieron una solicitud del administrador para activar manualmente la protección antiphishing de Ivanti y NO la han habilitado.
- **Desconocido:** es probable que los usuarios del dispositivo no hayan configurado el navegador predeterminado del dispositivo para Mobile@Work y, por lo tanto, no hayan habilitado la protección antiphishing de Ivanti.

## 6.4 MITIGACIÓN Y CUMPLIMIENTO INICIADOS LOCALMENTE

126. Puede crear acciones de mitigación y cumplimiento mediante la política de defensa contra amenazas de acciones locales. Este método no requiere una conexión con el servidor. Las acciones se aplican localmente en el dispositivo.

127. Core recibe la lista de definiciones de amenazas de App Gateway. La lista de amenazas se actualiza periódicamente, cuando se identifican nuevas amenazas o se eliminan las amenazas existentes. Antes de comenzar, compruebe que Core puede comunicarse con App Gateway para obtener la lista de amenazas más reciente. El archivo de definiciones de amenazas cambia con poca frecuencia y se crea un registro de auditoría MTD cada vez que se dispone de una nueva versión del archivo.

128. Si desea configurar el cumplimiento iniciado por el servidor, consulte "Mitigación y cumplimiento iniciados por el servidor".

129. La mitigación y el cumplimiento iniciados localmente incluyen las siguientes tareas y opciones:

- "Creación de acciones locales mtd en Core"
- "Creación de reglas y grupos de políticas de cumplimiento"
- "Configuración de la acción del sinkhole en dispositivos iOS"
- "Comprobación del estado de Mobile Threat Defense"

### 6.4.1. CREACIÓN DE ACCIONES LOCALES MTD EN CORE

130. Mediante las políticas de acciones locales de Mobile Threat Defense, puede establecer acciones locales específicas que se tomarán en dispositivos iOS y Android compatibles cuando el cliente habilitado para MTD detecte una amenaza. La política de acciones locales MTD se aplica en los dispositivos, independientemente del dispositivo que se esté conectando y en comunicación

con Core o el servidor zConsole. En el dispositivo, Mobile@Work aplica la política localmente.

131. Antes de empezar asegúrese de haber completado "Requisitos previos de Mobile Threat Defense".

132. Procedimiento:

1. En el portal de administración principal, seleccione **Políticas y configuraciones > políticas > Agregar nuevas acciones locales de > MTD.**
2. Introduzca el nombre de la política en el campo Nombre y una descripción opcional.
3. En el campo Estado, seleccione **Activo** para habilitar la política. Seleccione **Inactivo** para deshabilitar la política.
4. Especifique la prioridad de esta política en relación con otras políticas personalizadas del mismo tipo, para determinar qué política se aplica Core si hay más de una política disponible. Seleccione **Superior o Inferior que** y, a continuación, seleccione una política existente en el menú desplegable. Por ejemplo, para dar a la "Política A" una prioridad más alta que a la "Política B", seleccione "Más alto que" y "Política B".
5. En la tabla "Nombres de categorías de amenazas y amenazas relacionadas", haga clic en ^ para expandir una categoría de amenazas, mostrando todas las amenazas contenidas en esa categoría. Esta selección controla qué notificaciones están habilitadas en el dispositivo y qué acciones de migración se realizan localmente en el dispositivo cuando se detecta una amenaza.
6. Haz tus selecciones.
7. Haga clic en **Guardar** para guardar la política.

133. Puede editar su política de acciones locales de Mobile Threat Defense para seleccionar defensas contra amenazas nuevas o alternativas.

134. Procedimiento

1. Seleccionar **políticas y configuraciones > políticas**
2. Active la casilla situada junto a la política MTD que desea editar. El panel Detalles de la política se muestra a la derecha de la página.
3. Haga clic en **Editar**. Se abrirá el cuadro de diálogo Editar política de acciones locales mtd.

Edit MTD Local Actions Policy X

Name

Status  Active  Inactive

Priority  Higher than  Lower than  v

Description

**⚠** 3 Threat(s) have been deleted since the last time this policy was saved. Please review the changes and resave this policy. Once saved, these threats will be removed from the policy.

Select the action to take for each of the threats below.

	THREAT CATEGORY NAME	NUMBER OF THREATS
^	Network Threats	4 / 18 Enabled (2 Removed)
^	Host Threats	24 / 26 Enabled
^	Malware Threats	1 / 4 Enabled (1 Removed)

FIGURA 9. EDITAR POLÍTICA DE ACCIONES LOCALES MTD

4. Introduzca los cambios.
5. Para elegir varias acciones de amenazas, active la casilla de verificación situada a la izquierda de la amenaza y, a continuación, utilice el botón **Menú** desplegable Acciones para seleccionar varias acciones para la amenaza.
6. Haga clic en **Guardar**.

#### 6.4.2. PERSONALIZACIÓN del texto de notificación de amenazas locales

135. Puede personalizar el texto de notificación de amenazas locales para dispositivos Mobile@Work a través de la página Política de amenazas de zConsole. También tiene la opción de deshabilitar o volver a habilitar la función en la configuración de Acciones locales de MTD.

136. Las notificaciones de amenazas locales personalizadas se habilitan y deshabilitan desde la página **Políticas principales**. Su función está habilitada de forma predeterminada.

137. Procedimiento:

1. En la página Políticas y configuraciones > **políticas**, cree o abra una política de acciones locales de MTD.
2. Haga clic en la casilla de verificación situada debajo de la Descripción: **Habilitar la capacidad de personalizar las notificaciones locales del usuario final**.
3. **Guarde** la política.

138. Una vez habilitadas las notificaciones locales personalizadas del usuario final, puede personalizar el texto de notificación que reciben los usuarios del dispositivo en cualquiera de los idiomas admitidos.

### 139. Procedimiento:

1. En zConsole, vaya a la página Política de > Políticas > **políticas de amenazas**.
2. En el menú desplegable **Grupo seleccionado**, seleccione el grupo para recibir el texto de notificación.
3. Desde cualquier amenaza habilitada, haga clic en la casilla de verificación **Establecer alerta de usuario** y haga clic en el icono Configuración para abrir el icono **Página Configuración de mensajes de usuario de alerta**.



FIGURA 10. ICONO DE CONFIGURACIÓN DE ALERTAS A USUARIOS

4. En la página Configuración de mensajes de usuario de alerta, desplácese hasta la amenaza habilitada e introduzca el texto, la etiqueta del botón y la información del vínculo del botón para la alerta que está personalizando.

Alert User Message Configuration English

Please set the language, text, button label and link for the alert to be displayed on the device when this threat occurs.

Threat Name	Text	Button Label	Button Link
Abnormal Process Activity	Detected abnormal activity. Your device is being m		
Always-on VPN App Set	An app, [app_name], has been configured as an alv		
Android Debug Bridge (ADB) Apps Not Verified	Apps installed via ADB are not required to be verifi		
Android Device - Compatibility Not Tested By Google	The profile of this Android device does not match t		
Android Device - Possible Tampering	This Android device may have been tampered with		
App Tampering	App tampering has been detected. Your data may		
ARP Scan	Detected a WiFi network scan on the network name		

FIGURA 11. CONFIGURACIÓN DE ALERTAS A USUARIOS

**Campo de texto de alerta:** introduzca el texto de alerta que desea que los usuarios de su dispositivo vean cuando se detecte una amenaza.

**Etiqueta de botón:** Esta opción no es compatible.

**Enlace de botón:** Esta opción no es compatible.

5. Haga clic en **Enviar**.
6. **Haga clic en Guardar e implementar.** La política se envía al grupo de clientes en el siguiente registro.

### 6.4.3. NOMBRES DE CATEGORÍAS DE AMENAZAS Y AMENAZAS RELACIONADAS

140. Para seleccionar y configurar una amenaza de red, dispositivo o aplicación desde la página Acciones locales de MTD, siga estos pasos generales:

1. Haga clic en **^** para expandir la categoría de amenazas, mostrando todas las amenazas contenidas en esa categoría. Esta selección controla qué notificaciones están habilitadas en el dispositivo y qué acciones de migración se realizan localmente en el dispositivo cuando se detecta una amenaza.
2. En **Acciones locales iOS**, seleccione **Bloquear aplicaciones AppConnect** o **Sinkhole de red**.

**NOTA:** Ivanti recomienda SELECCIONAR SOLO la acción Sinkhole de red para amenazas relacionadas con la red. El uso de la acción de sinkhole de red para amenazas de dispositivos y aplicaciones puede resultar en la desactivación de la conectividad de red al dispositivo sin la capacidad de restaurar la conectividad de red.

3. En **Acciones locales Android**, seleccione cualquiera de las siguientes opciones:
  - Borrar el dispositivo
  - Cuarentena: Quitar todas las configuraciones
  - Cuarentena: no elimine la configuración de Wifi para dispositivos solo con Wifi
  - Cuarentena: no elimine la configuración de Wifi para todos los dispositivos
  - Cuarentena: eliminar aplicaciones administradas y bloquear nuevas descargas
  - Deshabilitar Bluetooth
  - Desconectarse de Wifi
4. En **Notificaciones**, seleccione **Sí** y **No** para habilitar o deshabilitar las notificaciones, respectivamente.
5. Para elegir varias acciones de amenaza, active la casilla de verificación a la

izquierda de la amenaza. Haga clic en el menú desplegable **Acciones** para seleccionar varias acciones para la amenaza.

Por ejemplo, al expandir la sección **Amenazas de red** se muestran tres columnas: **Acciones locales IOS**, **Acciones locales Android** o **Mostrar columnas de notificación**. Estos se utilizan para seleccionar una acción que se aplica cuando se detecta una amenaza en un dispositivo. El siguiente ejemplo muestra **Amenazas de red** como expandidas, en la fila **Zona de peligro conectada**, iOS está configurado en **Bloquear aplicaciones conectadas** y la sección **Acciones locales de Android** está esTABLAcida en **Cuarentena: Eliminar aplicaciones administradas y bloquear nuevas descargas**.

THREAT CATEGORY NAME		NUMBER OF THREATS		
Network Threats		0 / 17 Enabled		
Set Multiple Local Actions				
NAME		LOCAL ACTION IOS	LOCAL ACTION ANDROID	SHOW NOTIFICATION
Captive Portal	<i>i</i>			Yes
Danger Zone Connected	<i>i</i>	Block AppConnect Apps	Quarantine: Remove Mana...	Yes
IP Scan	<i>i</i>			No

FIGURA 11. ICONO DE CONFIGURACIÓN DE ALERTAS A USUARIOS

#### 6.4.4. AMENAZAS DE RED, DISPOSITIVOS Y APLICACIONES DISPONIBLES EN ACCIONES LOCALES

141. Respecto a las Amenazas de red, dispositivos y aplicaciones disponibles en Acciones locales, para seleccionar todas las acciones, active la casilla situada junto al campo **Nombre**. Esta es una acción de una sola vez y no persiste después de guardar la política.

142. Las siguientes amenazas de red están disponibles en Mobile@Work Acciones locales:

TABLA 13. POLITICAS DE AMENAZAS DE RED

Amenaza	Mitigación cuando se producen los siguientes eventos
Escaneo ARP	Un análisis de reconocimiento utilizando el protocolo ARP que a menudo es un indicador de un atacante malintencionado que busca un dispositivo vulnerable para un ataque de red como man-in-the-middle (MITM).
Portal Cautivo	Se ha detectado que el dispositivo se conectaba a una red de portal cautivo.

Amenaza	Mitigación cuando se producen los siguientes eventos
Zona de peligro conectada	<p>Danger Zone Connected proporciona a los usuarios de dispositivos información sobre las redes Wifi cercanas y su riesgo potencial. Si un usuario de dispositivo iOS o Android se conecta a un punto de acceso Wifi malicioso, se notificará al usuario del dispositivo: "Este dispositivo se ha conectado a una red Wifi donde se han observado ataques maliciosos. Se recomienda desconectarse inmediatamente y utilizar una red alternativa".</p> <p>Para habilitar Danger Zone Connected, debe tener activada la casilla de verificación <i>Habilitar la función Danger Zone en zIPS</i> (ubicada en la <b>consola de administración &gt; administrar &gt; pestaña General</b>).</p> <p>Para Android versión 9.0 y versiones compatibles más recientes, si el desarrollador de la aplicación no agrega el permiso <code>Access_Coarse_Location</code>, la siguiente funcionalidad de zConsole no está habilitada:</p> <ul style="list-style-type: none"> <li>• Los campos Nombre de red y BSSID no están disponibles para la información forense de amenazas.</li> <li>• Las amenazas de red no se mitigan.</li> </ul> <p>Si zConsole no puede obtener el BSSID del dispositivo, entonces la amenaza de conexión de zona de peligro no funcionará.</p>
Escaneo de IP	Un análisis de reconocimiento utilizando el protocolo IP que a menudo es un indicador de un atacante malintencionado que busca un dispositivo vulnerable para un ataque de red como MITM.
Acceso a la red interna	Aplicación detectada que se conecta a servidores internos privados. Es poco común que las aplicaciones públicas se conecten a servidores internos. Las aplicaciones públicas que se conectan a servidores internos se consideran comportamiento sospechoso y deben investigarse inmediatamente para detectar la posible amenaza de malware instalado en el dispositivo y el riesgo de fuga de datos.
MITM	Ataque Man-in-the-Middle donde un atacante malicioso puede secuestrar tráfico y robar credenciales o entregar malware al dispositivo.
MITM-ARP	Ataque Man-in-the-Middle utilizando envenenamiento de tabla ARP donde un atacante malicioso puede secuestrar tráfico y robar credenciales o entregar malware al dispositivo.
Certificado SSL MITM-Fake	Ataque Man-in-the-Middle utilizando un certificado falso donde un atacante malicioso puede secuestrar tráfico y robar credenciales o entregar malware al dispositivo.
Redireccionamiento MITM-ICMP	Ataque Man-in-the-Middle utilizando el protocolo ICMP donde un atacante malicioso puede secuestrar tráfico y robar credenciales o entregar malware al dispositivo.
Tira MITM-SSL	Ataque Man-in-the-Middle utilizando SSL stripping que permite a un hacker cambiar el tráfico HTTPS a HTTP para que pueda secuestrar tráfico y robar credenciales o entregar malware al dispositivo.
Transferencia de red	La transferencia de red permite que un dispositivo altere el enrutamiento en una red, lo que potencialmente permite un ataque Man-in-the-Middle.

Amenaza	Mitigación cuando se producen los siguientes eventos
Punto de acceso no fiable	Rogue Access Point aprovecha una vulnerabilidad del dispositivo para conectarse a una red Wifi previamente conocida enmascarando las redes preferidas/conocidas.
Punto de acceso no autorizado: Cerca	Rogue Access Point aprovecha una vulnerabilidad del dispositivo para conectarse a una red Wifi previamente conocida enmascarando una red cercana.
Degradación de SSL/TLS	SSL/TLS Downgrade obliga a las aplicaciones a utilizar protocolos de cifrado antiguos. Estos protocolos pueden ser vulnerables a ataques que permiten a terceros ver información cifrada.
Análisis TCP	Un análisis de reconocimiento utilizando el protocolo TCP que a menudo es un indicador de un atacante malintencionado que busca un dispositivo vulnerable para un ataque de red como MITM.
Escaneo UDP	Un análisis de reconocimiento utilizando el protocolo UDP que a menudo es un indicador de un atacante malintencionado que busca un dispositivo vulnerable para un ataque de red como MITM.
Red Wifi no segura	Una red Wifi no segura es vulnerable a un ataque de red.
Cambio de proxy	Cambio de configuración de proxy en el dispositivo móvil que puede ser indicativo de enviar tráfico a un destino no previsto.
SELinux deshabilitado	Linux con seguridad mejorada (SELinux) es una característica de seguridad en la función operativa del sistema operativo que ayuda a mantener la integridad del sistema operativo. Si SELinux se ha deshabilitado, la integridad del sistema operativo puede verse comprometida y debe investigarse de inmediato.
Aplicaciones de prueba	Las aplicaciones de prueba se instalan independientemente de una tienda de aplicaciones oficial y pueden presentar un riesgo de seguridad.
Vulnerabilidad de Stagefright	La vulnerabilidad Stagefright indica que el dispositivo está en una versión de parche del sistema operativo susceptible de compromiso.
Manipulación del sistema	La manipulación del sistema es un proceso para eliminar las limitaciones de seguridad impuestas por el fabricante del dispositivo e indica que el dispositivo está completamente comprometido y ya no se puede confiar en él.
Modo de depuración USB	La depuración USB es una opción de configuración avanzada destinada únicamente a fines de desarrollo. Al habilitar la depuración USB, el dispositivo del usuario puede aceptar comandos de una computadora cuando está conectado a un Conexión USB.
Cambio de configuración de descarga de fuentes desconocidas	Permite al usuario descargar una aplicación que no está en Google Play Store.

Amenaza	Mitigación cuando se producen los siguientes eventos
Versión vulnerable de Android	Ivanti ha detectado que la versión de Android instalada en su dispositivo no está actualizada. El sistema operativo obsoleto expone el dispositivo a vulnerabilidades conocidas y la amenaza de ser explotado por actores maliciosos. Se recomienda actualizar el sistema operativo del dispositivo inmediatamente.
Versión vulnerable de iOS	Ivanti ha detectado que la versión de iOS instalada en su dispositivo no está actualizada. El sistema operativo obsoleto expone el dispositivo a vulnerabilidades conocidas y la amenaza de ser explotado por actores maliciosos. Se recomienda actualizar el sistema operativo del dispositivo inmediatamente.
Versión de Android vulnerable y no actualizable	Ivanti detectó un dispositivo que ejecutaba una versión vulnerable de Android. Sin embargo, el dispositivo no es elegible para una actualización del sistema operativo en este momento.
Versión de iOS vulnerable y no actualizable	Mobile Threat Defense detectó un dispositivo que ejecutaba una versión vulnerable de iOS. Sin embargo, el dispositivo no es elegible para una actualización del sistema operativo en este momento.

143.Las siguientes amenazas de aplicaciones están disponibles en Mobile@Work  
Acciones locales:

TABLA 14. POLITICAS DE AMENAZAS DE APLICACIONES

Amenaza	Mitigación cuando se producen los siguientes eventos
Aplicación sospechosa para Android	Una aplicación riesgosa conocida que intenta tomar el control del dispositivo del usuario de alguna manera (por ejemplo, elevar privilegios, spyware, etc.)
Perfil sospechoso	Un perfil sospechoso es un nuevo perfil introducido en el entorno y <b>no</b> es explícitamente de confianza o no es de confianza. Se recomienda que el administrador revise el perfil y marque el perfil como de confianza o no de confianza.
Aplicación iOS sospechosa	Una aplicación conocida y arriesgada que intenta tomar el control del dispositivo de alguna manera (por ejemplo, elevar privilegios, spyware, etc.)
Perfil que no es de confianza	Un perfil que no es de confianza es un nuevo perfil instalado en uno o más dispositivos y <b>se considera que no es seguro tenerlo instalado en los dispositivos de usuario</b> . Un perfil que no sea de confianza instalado en los dispositivos podría usarse para controlar dispositivos <b>de forma remota</b> , monitorear y manipular las actividades del usuario y / o secuestrar el tráfico de un usuario.

#### 6.4.5. CREACIÓN DE GRUPOS Y REGLAS DE POLÍTICAS DE CUMPLIMIENTO

144. Para la Creación de grupos y reglas de políticas de cumplimiento, antes de empezar, asegúrese de haber completado "Creación y aplicación de acciones de cumplimiento de varios niveles iniciadas por el servidor"

145. Dentro de Mobile Threat Defense, hay tres tipos de amenazas. Dentro de cada tipo hay niveles de gravedad: Crítico, Elevado, Normal y Bajo. En total, usted tiene:

- Dispositivo: niveles críticos, elevados, normales y de baja gravedad
- **Red:** niveles de gravedad críticos, elevados, normales y bajos
- Aplicación: niveles críticos, elevados, normales y de baja gravedad

146. Para cada tipo de amenaza, se crean reglas de política de cumplimiento basadas en la gravedad de la amenaza. Como práctica recomendada, debe tener las siguientes reglas de política de cumplimiento:

- Para los tipos de amenazas bajas y normales: use **Enviar alerta**
- Para el tipo de amenaza elevada: use **Bloquear acceso y/o Cuarentena**
- Para el tipo de amenaza crítica: use **Cuarentena** o **Cumplimiento de niveles:**
  - a. Bloquear – notificar
  - b. Notificación
  - c. Cuarentena – eliminar. Si es bajo, envíe una notificación y deje que el usuario decida qué acción tomar.
  - d. Cumplimiento por niveles 23 horas
  - e. Cumplimiento por niveles 4 horas

147. Ejemplo de implementación de tipo de amenaza: el usuario se conecta a la red Wifi del hotel

- Nivel 1 - Notificación - MTD alerta al usuario del dispositivo "Acaba de conectarse a Wifi no seguro"
- Nivel 2 - después de 4 horas, MTD bloquea el acceso del usuario al correo electrónico y a las aplicaciones AppConnect.
- Nivel 3 - MTD pone en cuarentena y bloquea el Wifi; quita el acceso del usuario a la red de la empresa.

148. Deberá crear reglas de política de cumplimiento basadas en el nivel de gravedad de la amenaza.

149. Procedimiento:

1. En el portal de administración principal, seleccione **Políticas y configuraciones > Políticas de cumplimiento**.
2. Haga clic en la ficha **Regla de política de cumplimiento** y, a continuación, haga clic en **Agregar+**.
3. Ingrese "Bloquear" en el campo Nombre de la regla.
4. Establezca el estado en **Habilitado**.
5. (Opcional) Introduzca una descripción de la regla, por ejemplo, "Regla de bloque MTD".
6. En el campo Expresión condición, escriba esta expresión:
 

```
(("common. platform" = "Android" O "common. platform" = "iOS") Y "common. retired" = false) Y "common.retired" = falso
```
7. En el campo Acciones de cumplimiento, seleccione en el menú desplegable: Bloquear correo electrónico, Aplicaciones AppConnect y Enviar alerta.
8. (Opcional) En el mensaje field, escriba el texto de las alertas generadas por infracciones de la regla de política.
9. Haga clic en **Guardar**. La regla Bloquear se muestra en la ficha Regla de política de cumplimiento.
10. Repita los pasos del 2 al 9 con los parámetros siguientes para crear reglas de política de cumplimiento adicionales.

TABLA 15. POLITICAS DE AMENAZAS DE APLICACIONES

Campo Nombre de regla	Campo de expresión de condición	Campo Acciones de cumplimiento
Notificación	(("common. platform" = "Android" O "common. platform" = "iOS") Y "common.retired" =false) Y "common.retired" = falso	Enviar alerta
Cuarentena	(("common. platform" = "Android" O "common. platform" = "iOS") Y "common.retired" =false) Y "common.retired" = falso	Cuarentena
Cumplimiento de normas escalonadas 23 horas	(("common. platform" = "Android" O "common. platform" = "iOS") Y "common.retired" =false) Y "common.retired" = falso	Cumplimiento por niveles 23 horas
Cumplimiento por niveles 4 horas	(("common. platform" = "Android" O "common. platform" = "iOS") Y "common.retired" =false) Y "common.retired" = falso	Cumplimiento por niveles 4 horas

11. Cuando haya terminado, debe tener cinco reglas de política de cumplimiento mostradas en la ficha Regla de política de cumplimiento.

RULE NAME	STATUS	CONDITION	ACTIONS
Block	Enabled	(("common.platform" = "Android" OR "common.platform" = "IO...)	Block Email, AppConnect apps, and Send Alert
Notification	Enabled	(("common.platform" = "Android" OR "common.platform" = "IO...)	Send Alert
Quarantine	Enabled	(("common.platform" = "Android" OR "common.platform" = "IO...)	Quarantine
TieredCompliance23hours	Enabled	(("common.platform" = "Android" OR "common.platform" = "IO...)	Tiered Compliance 23 hours
TieredComputer4hours	Enabled	(("common.platform" = "Android" OR "common.platform" = "IO...)	Tiered Compliance 4 hours

FIGURA 12. REGLAS DE POLÍTICA DE CUMPLIMIENTO

150. Los grupos de políticas de cumplimiento se utilizan para aplicar las reglas del grupo a los dispositivos que coinciden con la etiqueta.

#### 151. Procedimiento

1. Seleccione **Políticas y configuraciones > Políticas de cumplimiento**.
2. Haga clic en la ficha **Grupo de políticas de cumplimiento** y, a continuación, haga clic en **Agregar+**.
3. Introduzca "MTDBlock" en el campo Nombre del grupo.
4. Mantenga el estado predeterminado de **Habilitado**.
5. (Opcional) Introduzca una descripción del nombre del grupo, por ejemplo, "MTDBlock".
6. En el campo Reglas disponibles, mueva la regla "Bloquear" a la sección Reglas seleccionadas. (La acción es "Bloquear correo electrónico, aplicaciones AppConnect y enviar alerta").
7. Haga clic en **Guardar**. El grupo MTDBlock se muestra en la ficha Grupo de políticas de cumplimiento.
8. Repita los pasos del 2 al 7 con los parámetros siguientes para crear grupos de políticas de cumplimiento adicionales.

TABLA 16. GRUPOS DE POLITICAS DE CUMPLIENTO ADICIONALES

Campo Nombre de grupo	Estado	Nombre de la regla	Nombre de la acción
MTDNotificación	Habilitado	Notificación	Enviar alerta
MTDCuarentena	Habilitado	Cuarentena	Cuarentena

Campo Nombre de grupo	Estado	Nombre de la regla	Nombre de la acción
MTDTiered23 horas	Habilitado	TieredCompliance23 horas	Cumplimiento por niveles 23 horas
MTDTiered4hours	Habilitado	TieredCompliance4hours	Cumplimiento por niveles 4 horas

152. Cuando haya terminado, debe tener cinco reglas de política de cumplimiento mostradas en la pestaña Grupo de políticas de cumplimiento.

153. Los clientes de MTD Plus pueden configurar una política de cumplimiento de aplicaciones que proteja a los usuarios de clientes de la instalación de aplicaciones no aprobadas. Utilice esta tarea de ejemplo para crear una política de acciones locales fuera de cumplimiento y otras similares.

154. Antes de empezar, esta función solo está disponible con una licencia MTD Plus. Consulte a su representante de Ivanti para obtener más información.

155. Procedimiento:

1. Desde el portal de administración, vaya a la página **Políticas y configuraciones > políticas**
2. Haga clic en **Agregar nueva > acciones locales mtd**. Se abrirá la política Agregar acciones locales MTD.
3. Introduzca un nombre, un estado (activo o inactivo) y una descripción opcional.
4. Haga clic en el upcarat para **Amenazas de malware**.
5. En las opciones, haga clic en **Aplicación fuera de cumplimiento**
6. Seleccione las acciones y notificaciones locales para la política en las opciones desplegadas.
7. Haga clic en **Guardar**.

#### 6.4.6. CONFIGURACIÓN DE LA ACCIÓN DE SINKHOLE EN DISPOSITIVOS IOS

156. Puede configurar una opción de sinkhole de iOS para redirigir automáticamente el tráfico de Internet del cliente de riesgo fuera de su red.

157. El proceso funciona así:

1. Cuando se detecta una amenaza en el dispositivo y se asocia una acción de sinkhole de red con esta amenaza en la política MTD, la amenaza activa el perfil de VPN de Ivanti Defender para aislar el dispositivo de la red, bloqueando todo el tráfico de red. Véase.
2. Sin embargo, si la configuración del sinkhole de red en zConsole también se ha configurado para bloquear o permitir tráfico específico, el perfil del sinkhole vpn bloqueará o permitirá solo las direcciones IP, los grupos o

los países que especifique. Consulte "Mitigación de sinkholes por dirección IP, dominio o país" en la página siguiente.

- Después de que la amenaza se remedia en el dispositivo, el perfil vpn se deshabilita automáticamente y el tráfico de red ya no se ve afectado por el sinkhole. En este punto, el tráfico bloqueado del navegador ahora tiene éxito.

158. Mientras la acción Sinkhole de red está activa en el dispositivo, tenga en cuenta los siguientes problemas:

- Es posible que no se detecten y muestren otras amenazas hasta que se corrija la amenaza original que causó la acción de cumplimiento.
- Es posible que la lista completa de amenazas no se muestre en el dispositivo iOS.

159. Para habilitar la mitigación de VPN de sinkhole para dispositivos iOS, en la política de acciones locales de MTD, puede especificar opcionalmente direcciones IP, dominios y países específicos a través de zConsole. Consulte "Mitigación de sinkholes por dirección IP, dominio o país" en la página siguiente.

160. MobileIron recomienda seleccionar la acción Sinkhole de red SOLO para amenazas relacionadas con la red.

161. El uso de la acción de sinkhole de red para amenazas de dispositivos y aplicaciones puede resultar en la desactivación de la conectividad de red al dispositivo sin la capacidad de restaurar la conectividad de red.

162. Antes de empezar, asegúrese de haber revisado "Creación de acciones locales MTD en Core"

163. Procedimiento:

- En la página Políticas y configuraciones principales > políticas, cree o edite una política de acción local MTD.
- En una amenaza de la sección Amenazas de red, seleccione **Sinkhole de red** en la columna Acción local de iOS.



FIGURA 13. NETWORK SINKHOLE OPTION IN ACTIONS MENU.

- Finalice las opciones de configuración y haga clic en **Guardar**. Aparece la página Política, con la configuración actualizada.

**NOTA:** La política de VPN no se puede editar. Para quitar la configuración, quite las opciones de **Sinkhole de red** de la política.

- Para insertar esta política en los dispositivos, seleccione la política.
- Haga clic en **Acciones > Aplicar a la etiqueta**. Aparece el menú Aplicar a etiqueta.
- Seleccione las etiquetas de dispositivo que recibirán la política.
- Haga clic en **Aplicar**. La política se envía a los dispositivos etiquetados.

164. Si desea que la protección contra sinkholes se aplique a direcciones IP, dominios y/o países específicos, utilice la Configuración de sinkhole de red zConsole para definirlos.

165. Las acciones locales del sinkhole MTD deben estar habilitadas para implementar el sinkhole zConsole. Consulte "Habilitar la mitigación de VPN de sinkhole para dispositivos iOS" en la página anterior. La función The zConsole Sinkhole es opcional, y el sinkhole MTD continuará funcionando en cualquier caso.

166. Antes de empezar, complete "Habilitar la mitigación de VPN de sinkhole para dispositivos iOS" en la página anterior

167. Procedimiento:

- Inicie sesión en zConsole.
- Haga clic en la pestaña **Administrar**.

- Haga clic en Configuración **del sinkhole de red**. Aparece la página Configuración del sinkhole de red.

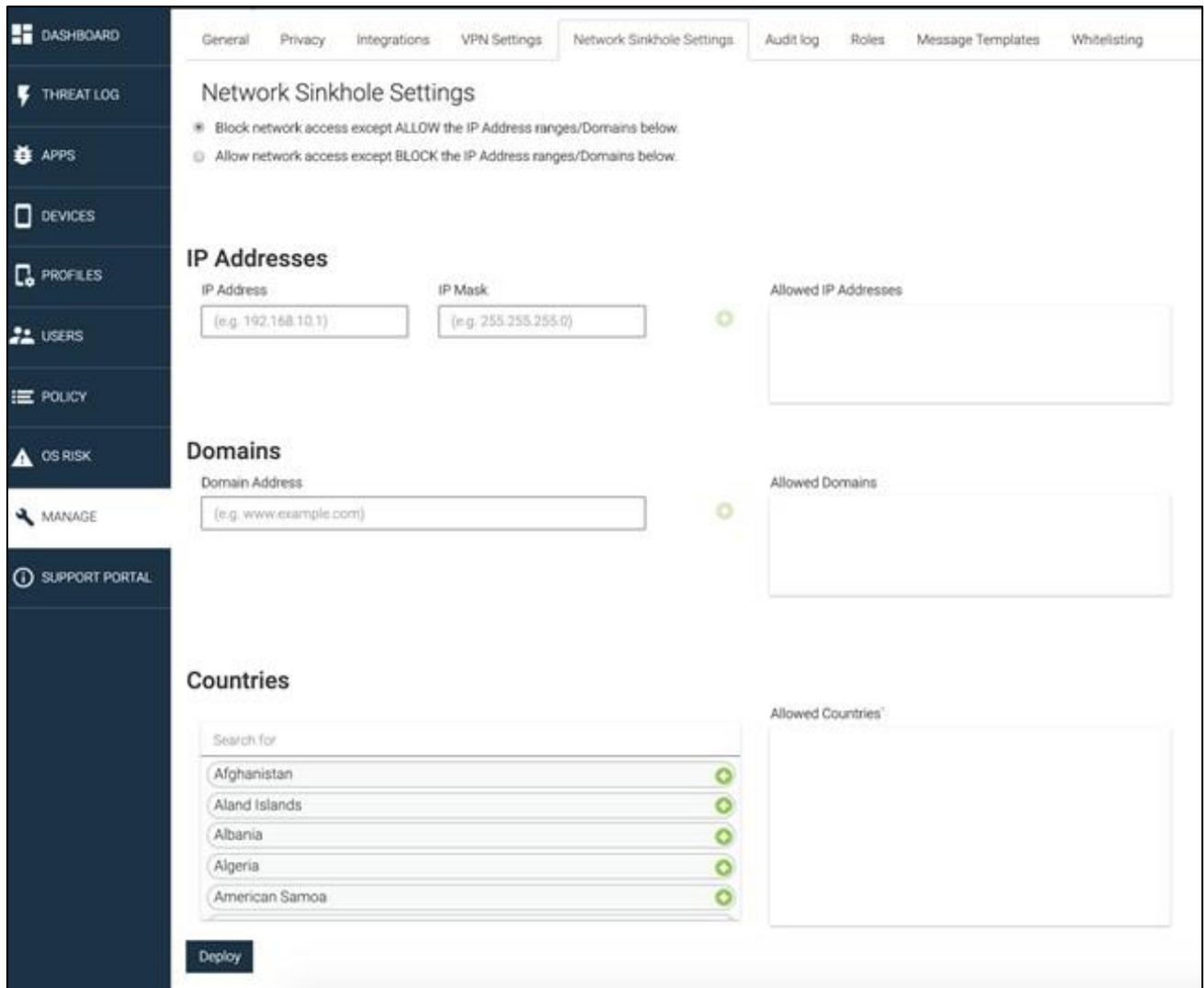


FIGURA 14. CONFIGURACION DE SINKHOLE DE RED EN zCONSOLE

- Elija si las direcciones enumeradas deben permitirse o bloquearse.
  - Marque **Bloquear el acceso a la red, excepto PERMITIR los rangos de direcciones IP / Dominios a continuación**, para permitir las direcciones enumeradas.
  - Marque **Permitir acceso a la red excepto BLOQUEAR los rangos de direcciones IP / Dominios a continuación**, para bloquear las direcciones enumeradas.
- Opcional. Introduzca una dirección IP válida y una máscara IP asociada en el campo Direcciones IP y haga clic en el icono verde más **+** para agregar la dirección a la lista **Direcciones IP permitidas/bloqueadas**.

6. Opcional. Introduzca una dirección de dominio válida (por ejemplo, www.example.com) y haga clic en el icono verde más  para agregar la dirección a la lista **Dominios permitidos/bloqueados**.
7. Opcional. Haga clic en el icono verde más  para cada país que desee agregar a la lista **Países permitidos/bloqueados**.
8. Haga clic en **Implementar** para aplicar las opciones de sinkhole a las entidades enumeradas.

#### 6.4.7. COMPROBACIÓN DEL ESTADO DE MTD

168. Para confirmar el estado de MTD desde el portal de administración principal para un dispositivo determinado, utilice una de las siguientes opciones:

- "Comprobación de dispositivos individuales" a continuación
- "Uso de la búsqueda avanzada"

169. Procedimiento de comprobación de dispositivos individuales

1. Seleccione **Dispositivos y usuarios > dispositivos** y haga clic en el quilate (^) junto al dispositivo correspondiente. Aparecerá la ficha **Detalles del dispositivo**.
2. Desplácese hasta que vea el campo Estado de Mobile Threat Defense y mire el valor (consulte la tabla a continuación).

TABLA 17. ESTADO DEL MTD EN LA PESTAÑA DE DETALLES DEL DISPOSITIVO

Nombre de error	Definición	Ubicación del mensaje de error
Error de conexión	Error de conexión. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido debido a un error de conexión".
Licencia caducada	La licencia ha caducado. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido porque la licencia ha caducado".
Licencia no válida	Clave de licencia no válida. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido porque la licencia no es válida".

Nombre de error	Definición	Ubicación del mensaje de error
Error de clave de licencia	Error de clave de licencia. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido debido a un error de clave de licencia".
Límite de licencia excedido	Se ha alcanzado el número máximo de licencias. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido porque se ha excedido el límite de licencia".
Licencia no activada	Error en la clave de licencia MTD de zConsole. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no lo es porque no se pudo activar la licencia".
Cierre de sesión	El dispositivo del usuario no está protegido debido a un cierre de sesión.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido debido a un cierre de sesión".
Inicio de sesión cancelado (Solo Android)	Demasiados inicios de sesión. El dispositivo del usuario no está protegido.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error")  Dispositivo del usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido debido a un inicio de sesión cancelado".
N/A	La configuración de activación de MTD no está asignada al dispositivo o MTD no se ha activado en el dispositivo	Dispositivos y usuarios > dispositivos > página detalles del dispositivo ("N/A")  Dispositivo de usuario: este valor no tiene equivalente en la aplicación cliente.
Pendiente	Se ha enviado la clave de licencia MTD, a la espera de la confirmación de zConsole.	Dispositivos y usuarios > dispositivos > página detalles del dispositivo ("Pendiente")  Dispositivo de usuario: este valor no tiene equivalente en la aplicación cliente.

Nombre de error	Definición	Ubicación del mensaje de error
Protegido	La activación de la licencia MTD se ha realizado correctamente. El dispositivo del usuario está protegido.	Dispositivos y usuarios > dispositivos > página detalles del dispositivo ("Protegido") Dispositivo del usuario – "Protegido"
Error del simulador	Error interno.	Dispositivos y usuarios > dispositivos > página Detalles del dispositivo ("Error") Dispositivo de usuario: "Mobile Threat Defense detectó que su dispositivo no está protegido debido a un error del simulador".

170.El uso de la búsqueda avanzada es útil para buscar a través de una gran cantidad de dispositivos.

171.Procedimiento:

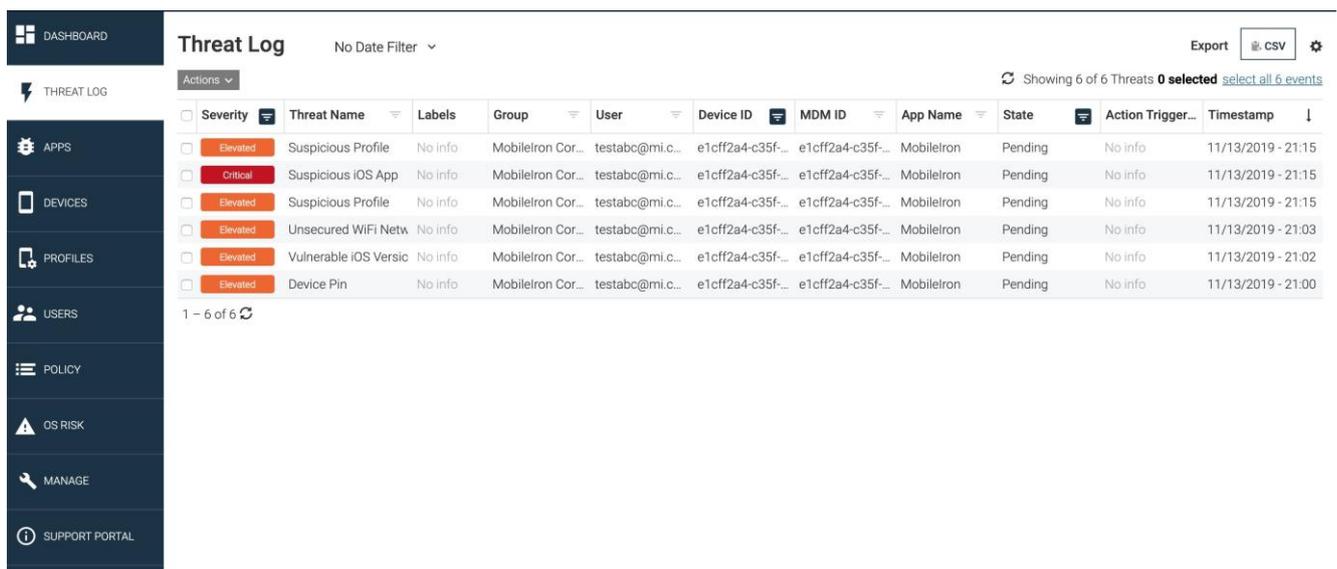
1. Seleccione **Dispositivos y usuarios > dispositivos** y haga clic en el quilate (^) junto al dispositivo correspondiente. Aparecerá la ficha **Detalles del dispositivo**.
2. Haga clic en **Todo** para combinar los criterios con un AND lógico. Haga clic en **Cualquiera** para combinar los criterios con OR.
3. En Campo, escriba Estado de defensa contra amenazas móviles o seleccione **Campos comunes > Estado de defensa contra amenazas de MobileIron**.
4. Seleccione un operador, como **Equals**.
5. En el campo Seleccionar tipo, elija el valor en el que desea buscar. Los valores predeterminados que puede seleccionar son:
  - **Protegido:** Indica que el token de activación MTD se ha enviado al dispositivo, el token es válido, MTD está activado y el escaneo está operando en el dispositivo.
  - **N/A:** Indica que no hay ninguna configuración de Mobile Threat Defense en el dispositivo.
  - **Error:** Indica que el token de activación de MTD se ha enviado al dispositivo, pero hubo errores. El análisis de amenazas no está habilitado. Consulte la tabla "Comprobación del estado de Mobile Threat Defense" en la página 70 para obtener definiciones de mensajes de error.
  - **Desconocido:** Indica que se acepta el token de activación de MTD, pero se desconoce el estado del análisis de MTD en el dispositivo. No se aplica a dispositivos iOS.

6. Haga clic en **Buscar**. Los resultados se muestran en la mitad inferior de la pantalla.

## 6.5 CONFIGURACIÓN DE ADMINISTRADORES

### 6.5.1. USO DE ZCONSOLE

172. En esta sección se describe cómo instalar, configurar y utilizar zConsole para las actividades compatibles de Mobile Threat Defense.



The screenshot shows the 'Threat Log' interface in ZConsole. The table displays the following data:

Severity	Threat Name	Labels	Group	User	Device ID	MDM ID	App Name	State	Action Trigger...	Timestamp
Elevated	Suspicious Profile	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:15
Critical	Suspicious iOS App	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:15
Elevated	Suspicious Profile	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:15
Elevated	Unsecured WiFi Netw	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:03
Elevated	Vulnerable iOS Versic	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:02
Elevated	Device Pin	No info	Mobileiron Cor...	testabc@mi.c...	e1cff2a4-c35f...	e1cff2a4-c35f...	Mobileiron	Pending	No info	11/13/2019 - 21:00

FIGURA 15. ZCONSOLE THREAT LOG

173. La página zConsole Manage proporciona una forma para que, actuando como administrador, configurar la privacidad y la configuración de VPN para el entorno, así como una vista de los registros de auditoría que recopilan toda la actividad en los dispositivos activos.

174. La ficha Administrar > General proporciona información básica sobre el entorno y una ubicación alternativa para modificar el idioma seleccionado. También proporciona la opción de cambiar la contraseña de administrador.

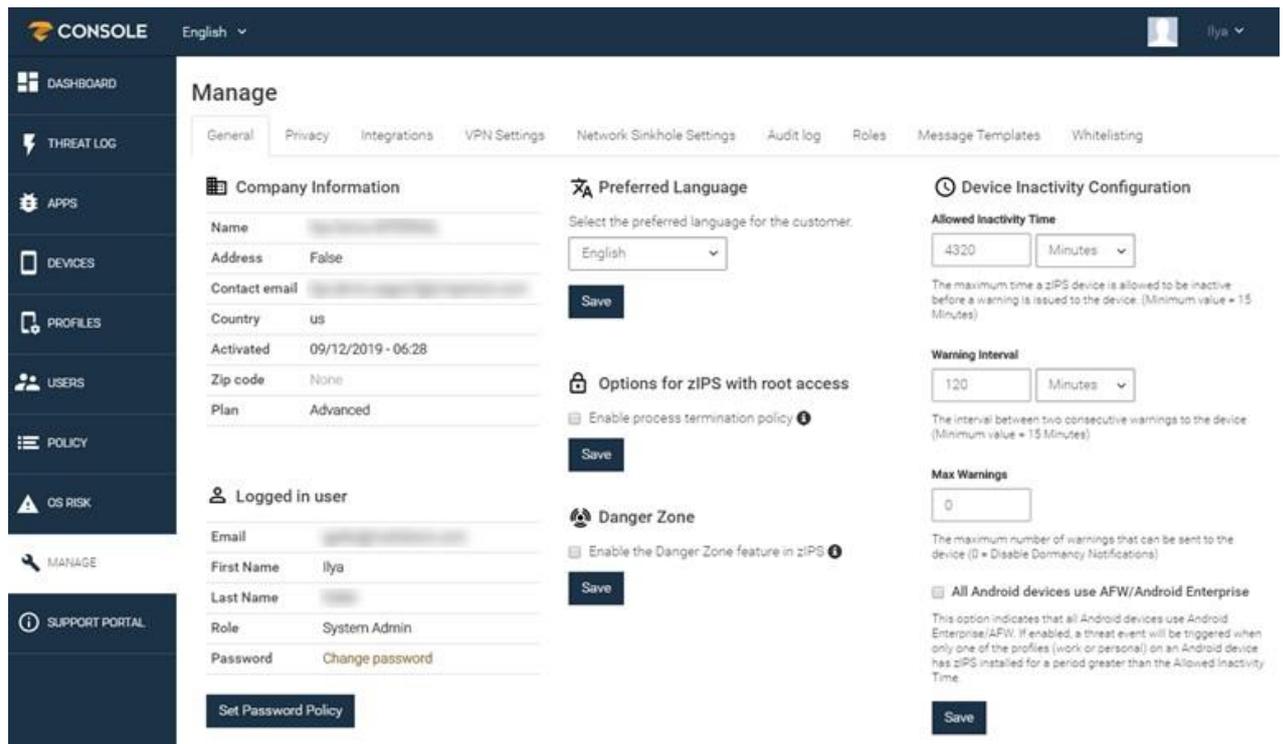


FIGURA 16. ZCONSOLE &gt; MANAGE &gt; GENERAL TAB

175. Estos son los elementos de configuración específicos para la ficha General:

TABLA 18. CONFIGURACIONES DE LA PESTAÑA GENERAL

Sección	Descripción y acciones
Información de la empresa	Ingrese la información de su empresa, incluido un correo electrónico de contacto. El tipo de plan y la fecha de activación se rellenan automáticamente.
Usuario que ha iniciado sesión	Escriba el nombre, la dirección de correo electrónico, el rol del sistema y la contraseña del usuario actual. Haga clic en <b>Cambiar contraseña</b> para abrir el menú establecer contraseña. Haga clic en Guardar para conservar los cambios.
Establecer política de contraseñas	<ol style="list-style-type: none"> <li>Haga clic en <b>establecer política de contraseñas</b> para abrir el menú de políticas de contraseñas.</li> <li>Defina los requisitos de contraseña para los usuarios de zConsole: <ul style="list-style-type: none"> <li>Longitud mínima de la contraseña</li> <li>Elementos de contraseña requeridos</li> <li>Máximo de caracteres repetidos</li> <li>Verifique que la nueva contraseña no se haya utilizado en el pasado "n" contraseñas</li> <li>Definir la frecuencia con la que se debe cambiar la contraseña</li> <li>Definir cuántos intentos fallidos antes de activar un bloqueo de cuenta</li> <li>Definir el tiempo de bloqueo de la cuenta en minutos</li> </ul> </li> </ol>

Sección	Descripción y acciones
	3. Haga clic en <b>Guardar</b> para conservar los cambios.
Idioma preferido	Elija el idioma para zConsole. Las opciones actuales son inglés, japonés o hebreo. Haga clic en <b>Guardar</b> para conservar los cambios.
Opciones para zIPS con acceso root	Esta característica no es compatible con los clientes MTD.
Zona de peligro	Cuando esta opción está habilitada, alerta al usuario de que se ha conectado a una red Wifi que se encuentra en la base de datos de Danger Zone de sitios web posiblemente maliciosos. Esta opción está deshabilitada de forma predeterminada. Haga clic en <b>Guardar</b> para conservar los cambios.
Configuración de inactividad del dispositivo	<p>Esta configuración controla cuánto tiempo espera el sistema antes de determinar que un dispositivo está inactivo:</p> <ol style="list-style-type: none"> <li>1. <b>Tiempo de inactividad</b> permitido: el tiempo máximo que un dispositivo puede estar inactivo antes de que el dispositivo se ingrese en el temporizador de advertencia, también conocido como Período de gracia. Escriba un número válido en el cuadro de la izquierda y elija Segundos, Minutos u Horas en el cuadro de la derecha.</li> <li>2. <b>Intervalo de advertencia (período de gracia)</b>: después de que el dispositivo excede el temporizador de inactividad permitido, entra en el período de gracia donde recibe una advertencia. Si se requiere más de una advertencia, escriba un número válido en el cuadro izquierdo para configurar el intervalo entre advertencias y elija Segundos, Minutos u Horas en el cuadro derecho.</li> <li>3. <b>Advertencias máximas</b>: el número de advertencias que se pueden enviar al dispositivo en el período de gracia. Una entrada de '0' desactiva el período de gracia.</li> <li>4. <b>Todos los dispositivos Android usan AFW/Enterprise</b>: Haga clic en este cuadro si todos sus dispositivos Android usan el modo Android Enterprise (AE) o AE Work Profile. Cuando está habilitado, desencadena un evento de amenaza si cualquiera de los perfiles de cliente (laboral o personal) supera el <b>tiempo de inactividad permitido</b>.</li> </ol> <p>Haga clic en <b>Guardar</b> para conservar los cambios.</p>

176.La página Dispositivos muestra la lista completa de dispositivos configurados en este entorno. Los dispositivos aparecen automáticamente en esta página porque un nuevo cliente habilitado para MTD se ha registrado. Además, esta página enumera los dispositivos que están sincronizados con Core. Los dispositivos atenuados en la lista son dispositivos que se han sincronizado con Core, pero que aún no se han registrado.

177.La información del dispositivo incluye lo siguiente:

- Postura de riesgo (por ejemplo, baja, elevada, crítica)
- Usuario
- Grupo
- SO (Versión del dispositivo)
- Sistema operativo actualizable (Sí, No o N/A)
- ID de dispositivo
- Modelo (por ejemplo, iPhone, Nexus 5)
- Versión de la aplicación (de Mobile@Work)
- Privilegios (por ejemplo, Rooteado, Jailbreak, No Jailbreak)
- Modo operativo (inactivo, activo)
- Visto por última vez (última fecha y hora en que el dispositivo fue visto por Mobile@Work, a través del check-in o de una comunicación de evento)

178. La postura de riesgo del dispositivo señala el nivel más alto de un evento pendiente visto para el dispositivo en el momento de la visualización. Si la Postura de Riesgo del dispositivo es Elevada y se detecta un evento Crítico, entonces el dispositivo tiene una nueva Postura de Riesgo de Crítico.

Risk Pos...	User	Group	OS	Upgrade...	Device ID	Model	App Vers...	Privileges	Operatio...	Last seen
Low	mostg2@z-com	Default Group	iOS 11.1	No	a95585b6-032...	iPhone	4.2.1	Not Jailbroken	Inactive	11/21/2017 1...
Low	mostg2@z-com	Default Group	iOS 11.1	No	649a19c7-903...	iPhone	4.1.33	Not Jailbroken	Inactive	11/21/2017 1...
Low	mostg2@z-com	Default Group	iOS 11.1	No	5e0cb6fc-086...	iPhone	4.1.33	Not Jailbroken	Inactive	11/21/2017 1...
Critical	mostg1@z-com	Default Group	iOS 7.1.1	N/A	358239068975...	Nexus 5	4.2.0	Rooted	Inactive	10/27/2017 1...
Disavowd	mostg2@z-com	Default Group	iOS 9.3.1	No	360506353346...	iPhone	3.0.86	Not Jailbroken	Inactive	10/17/2017 1...
Low	mostg2@z-com	Default Group	iOS 11.1	No	No Device ID	No Model	3.0.86	Not Jailbroken	Inactive	10/17/2017 1...
Low	mostg2@z-com	Default Group	iOS 9.3.1	No	116926212530...	iPhone	3.0.86	Not Jailbroken	Inactive	10/17/2017 1...
Critical	test_1507662458966@z-com	Default Group	iOS 8.0	N/A	922945969667...	SM-G900H	3.0.86	Not Rooted	Inactive	10/10/2017 1...

FIGURA 17. EXAMPLE OF RISK POSTURE ON DEVICES

179. A continuación, se muestra una lista de los filtros de visualización generales:

- **Perfiles:** Para mostrar una lista de dispositivos iOS que tienen perfiles específicos instalados, haga clic en la opción **Perfiles** cerca de la parte

superior de la pantalla y seleccione los perfiles de interés. Se muestra una lista de dispositivos que tienen instalados los perfiles seleccionados.

- **Aplicaciones:** Para mostrar una lista de dispositivos que tienen aplicaciones específicas instaladas, haga clic en la opción **Aplicaciones** cerca de la parte superior de la pantalla y seleccione las aplicaciones de interés. Se muestra una lista de dispositivos que tienen instaladas las aplicaciones seleccionadas.
- **Fecha del parche:** Para mostrar una lista de dispositivos que tienen una fecha de parche específica, haga clic en la opción **Fecha del parche** cerca de la parte superior de la pantalla y seleccione las opciones deseadas. Se muestra una lista de dispositivos que tienen la fecha de revisión seleccionada.

180. En la tabla siguiente se muestran las columnas incluidas en el filtro de página Dispositivos.

TABLA 19. DEVICES PAGE FILTER

Columna	Descripción
Postura de riesgo	Mostrar dispositivos que coincidan con la <b>postura</b> o posturas de riesgo seleccionadas
Usuario	Mostrar dispositivos que coincidan con el usuario o <b>usuarios</b> seleccionados
Grupo	Muestra los dispositivos que <b>coinciden</b> con los <b>grupos de consola de administración</b> seleccionados
SISTEMA OPERATIVO	Muestra dispositivos que <b>coinciden</b> con las versiones <b>del sistema operativo</b> seleccionadas
Actualizable	Muestra los dispositivos que coinciden con el valor de indicador actualizable seleccionado
ID de dispositivo	Muestra los dispositivos que coinciden con los <b>ID de dispositivo</b> seleccionados
Nombre de la aplicación	Muestra los dispositivos que ejecutan la aplicación <b>Mobile@Work</b> seleccionada
Versión de la aplicación	Muestra los dispositivos que ejecutan las versiones seleccionadas de la aplicación <b>Mobile@Work</b>
Privilegios	Muestra dispositivos que <b>están rotos o rooteados</b>

Columna	Descripción
Modo operativo	Esta columna muestra lo siguiente: <b>Activo:</b> describe los dispositivos que se comunican regularmente con la consola de administración <b>Inactivo:</b> describe los dispositivos que han estado activos pero que ahora no se comunican <b>Activación pendiente:</b> describe los dispositivos que se han sincronizado a través de Core, pero que aún no se han registrado.
Visto por última vez	Ordena por la fecha u hora en que se vieron por última vez los dispositivos filtrados

181. Puede exportar los listados con el icono de exportación. Esta exportación incluye solo la lista de dispositivos filtrados y se descarga como un archivo CSV a través de un enlace enviado a la dirección de correo electrónico del administrador.



FIGURA 18. ICONO PARA EXPORTAR EN .CSV

182. Al hacer clic en un dispositivo, se abre el panel **Detalles del dispositivo**. Se muestran detalles sobre el dispositivo, incluidos los elementos de configuración vulnerables y las alertas. En la parte inferior de la ventana hay algunas acciones y elementos que pueden mostrar información adicional sobre el dispositivo:

- Para mostrar las amenazas para este dispositivo de desarrollo, haga clic en el vínculo **Mostrar amenazas para este dispositivo**. Si no hay amenazas disponibles, aparece el mensaje "No se han detectado amenazas para este dispositivo".
- La función **Cerrar sesión** no es compatible con Ivanti y no funcionará con MTD.
- La opción **Información del dispositivo** proporciona información más específica sobre el dispositivo, como el teléfono celular, el operador y la información del país.

183. Después de configurar Core como servidor de administración de dispositivos móviles (MDM) en zConsole y distribuir Mobile@Work con MTD, puede usar zConsole para monitorear amenazas a redes, aplicaciones y dispositivos conectados.

184. Utilice zConsole para configurar las siguientes características de administración de amenazas MTD:

- Protección antiphishing avanzada para dispositivos gestionados. Consulte "Protección avanzada contra phishing para dispositivos

gestionados"

- Mitigación de sinkhole configurable para dispositivos iOS. Consulte "Mitigación de sinkholes por dirección IP, dominio o país"
- Lista blanca de aplicaciones de prueba para dispositivos Android. Consulte "Lista blanca de una aplicación de prueba para dispositivos Android" a continuación.

185. Puede ver estos elementos relacionados con MTD en zConsole:

- Dispositivos habilitados para MTD que están registrados con Core
- Aplicaciones administradas en dispositivos Core
- Redes
- Niveles de amenaza proyectados para dispositivos y aplicaciones

186. Si la amenaza de aplicación de prueba está habilitada a través de zConsole, cuando Mobile@Work para usuarios de Android instalan una aplicación en su teléfono que no se descargó de la Tienda de aplicaciones de Windows o Google Play Store (incluido Mobile@Work para Android), desencadena una amenaza de "aplicación de prueba". Si se aprueba una aplicación de prueba para su organización y desea incluirla en la lista blanca (permitirla), puede configurarla en zConsole antes o después de instalarla en un dispositivo.

187. Si decide no incluir en la lista blanca las aplicaciones administradas por UEM a través de zConsole, las amenazas de aplicaciones de prueba no deben estar vinculadas a ninguna acción de cumplimiento.

188. Procedimiento de inclusión en la lista blanca de una aplicación antes de la instalación:

1. En zConsole, haga clic en **APLICACIONES**.
2. Busca una aplicación que quieras incluir en la lista blanca.
3. Haga clic en el menú de tres puntos en el extremo derecho de la fila y seleccione **Permitir/Denegar**.
4. Desde el menú emergente **Permitir / Denegar**:
  - a. Seleccione **Todo el paquete de aplicaciones**, para evitar que las amenazas de aplicaciones de estas aplicaciones se muestren en las aplicaciones cliente y en zConsole.
  - b. Seleccione **PERMITIR** para incluir la aplicación en la lista blanca.
5. Haga clic en **Guardar** para aplicar los cambios.

189. Procedimiento de inclusión en la lista blanca de una aplicación después de la instalación

1. En zConsole, haga clic en **REGISTRO DE AMENAZAS**.

2. Seleccione la aplicación de prueba que desea incluir en la lista blanca.
3. En el menú Acciones, seleccione **Whitelist App Developer**. Su selección se guarda automáticamente.

### 6.5.2. GESTIÓN DE LA PRIVACIDAD DEL USUARIO

190. Mobile Threat Defense tiene políticas y herramientas para proporcionar niveles elevados de privacidad para los clientes de MTD que requieren estándares de privacidad de datos más altos.

191. Los miembros de la Unión Europea (UE) tienen derechos adicionales de protección de datos bajo el estándar del Reglamento General de Protección de Datos (GDPR). El perfil GDPR de Ivanti protege los datos de los miembros de la exposición a socios de integración, desarrolladores de API y administradores.

- "Habilitación del perfil GDPR" a continuación
- "Asignación de usuarios a un perfil GDPR" en la página siguiente

192. Antes de poder asignar el perfil gdpr a un usuario, debe habilitar la función en Core y seleccionar qué campos deben estar visibles y cuáles no.

193. Procedimiento

1. Desde el Portal de administración principal, vaya a **Configuración > usuarios y dispositivos > perfil GDPR**.
2. Haga clic en **Perfil GDPR**. Aparece la página Perfil del RGPD.
3. Haga clic en **Habilitar perfiles GDPR para asignarlos a los usuarios**. Se muestran las opciones Perfil **predeterminado** del RGPD. De forma predeterminada, todos los campos están seleccionados.
4. Haga clic en el lápiz azul en la esquina superior derecha para editar los valores predeterminados del perfil.
5. Deshabilite el RGPD para cualquier campo que **no** desee ocultar anulando la selección de la casilla de verificación del campo. Las opciones de campo incluyen:
  - ID de usuario
  - Nombre de la persona
  - Dirección de correo electrónico
  - Número de teléfono
  - Identidad Internacional de Equipos Móviles (IMEI)

- Número de serie
- ID de tarjeta de circuito integrado (ICCID)
- Identidad internacional de suscriptor móvil (IMSI)
- Identificador de equipo móvil (MEID)

6. Haga clic en **Guardar**.

194. Se muestran las elecciones de su perfil GDPR. En este ejemplo, el ID de usuario se mostrará en texto sin cifrar, pero los demás campos se ocultarán.

## GDPR Profile

Create profiles to restrict certain information from being accessed by users. The profiles will not be active until it has been assigned to a certain user.

Enable GDPR Profiles to be assigned to users

Note Disabling this will turn off all profile restrictions already assigned to users.

! To assign this profile to an user please select a user from the [Users](#) tab and use the action "Assign GDPR Profile".

**Default GDPR Profile** ✎

Fields shown below will be hidden. To add more fields use the edit icon on the right.

<input type="checkbox"/> User ID	<input type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Person Name	<input type="checkbox"/> ICCID
<input checked="" type="checkbox"/> Email Address	<input type="checkbox"/> IMSI
<input checked="" type="checkbox"/> Phone Number	<input type="checkbox"/> MEID
<input checked="" type="checkbox"/> IMEI	

FIGURA 19. PERFIL GDPR

195. Una vez que el perfil GDPR está habilitado, debe asignarle usuarios de API.

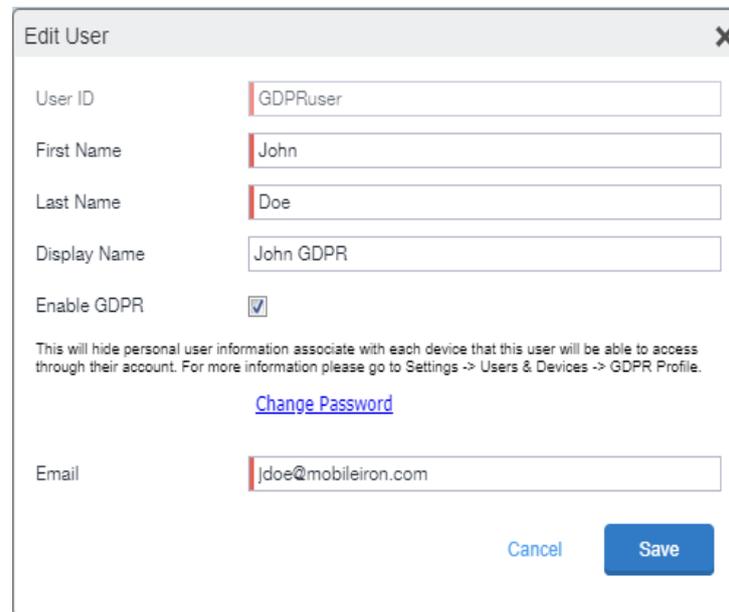
196. Cuando el perfil GDPR está habilitado para un usuario, se restringen algunas funciones y derechos de edición en las páginas Dispositivos principales y Usuarios. Los usuarios habilitados para GDPR verán un banner naranja en la parte superior de Core, recordándoles que estas restricciones están vigentes.

GDPR profile enabled - Some functionality and edit rights are restricted. Contact your Administrator for more information

FIGURA 20. MENSAJE DE RECORDATORIO GDPR

197. Procedimiento:

1. Desde el Portal de administración principal, vaya a **Dispositivos y usuarios > usuarios**. Aparecerá la página Usuarios.
2. Haga clic en el icono del lápiz a la izquierda del nombre de usuario para editar el perfil de usuario. Se abrirá el cuadro de diálogo Editar usuario.
3. Haga clic en **Habilitar GDPR** para asignar un usuario al perfil gdpr.



**Edit User**

User ID: GDPRuser

First Name: John

Last Name: Doe

Display Name: John GDPR

Enable GDPR:

This will hide personal user information associate with each device that this user will be able to access through their account. For more information please go to Settings -> Users & Devices -> GDPR Profile.

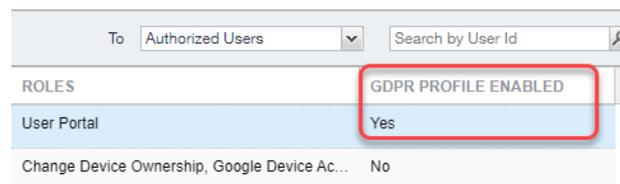
[Change Password](#)

Email: jdoe@mobileiron.com

Cancel Save

FIGURA 21. HABILITAR GDPR SOBRE UN USUARIO

4. Haga clic en **Guardar**. La página Usuarios ahora muestra **Sí** en la columna **Perfil gdpr habilitado** para los usuarios que ha habilitado.



To	Authorized Users	Search by User Id
ROLES		
User Portal	GDPR PROFILE ENABLED	Yes
Change Device Ownership, Google Device Ac...	No	

FIGURA 22. CONFIRMA QUE EL PERFIL GDPR HA SIDO

5. Una vez que se haya habilitado el RGPD para un administrador o usuario de API, no podrá ver la información del dispositivo y del usuario. Cuando navegan a **Dispositivos y usuarios > dispositivos**, los campos gdpr se muestran como asteriscos o un campo en blanco.

	DISPLAY NAME	CURRENT PHONE NUM...	MODEL	MANUFACTU...	PLATFORM N...
☐ ^	*****	*****	iPhone 6	Apple	iOS 9.3
☐ ^	*****	*****	iPhone 6	Apple	iOS 9.3
☐ ^	*****	*****	iPhone 6	Apple	iOS 9.3

FIGURA 23. DETALLES DE USUARIO Y DISPOSITIVO TRAS APLICAR PERFIL GDPR

### 6.5.3. ADMINISTRACIÓN DE MOBILE@WORK

198. Esta sección incluye información y tareas que los administradores de MTD pueden encontrar útiles para solucionar problemas de clientes Mobile@Work. Para obtener más documentación de MTD, artículos de la base de conocimientos, boletines de productos y grupos de foros, consulte la página de soporte técnico de Mobile Threat Defense.

199. Los usuarios de dispositivos iOS pueden reproducir el problema y enviar las trazas a su administrador.

200. Procedimiento:

1. Abra Mobile@Work.
2. Pulsa **Configuración**.
3. Para habilitar el registro cifrado a nivel de depuración de la información de tu teléfono, pulsa **Registro mejorado**. Si no necesita cifrado, asegúrese de que el **registro mejorado** esté desactivado.
4. Reproduzca el problema en el dispositivo.
5. Vuelva a Mobile@Work y toque Configuración > **Enviar registros**.  
 Seleccione un método para enviar la información de registro al soporte de Ivanti. Las opciones incluyen correo electrónico, SMS, AirDrop y otros.
6. Introduce una dirección de soporte y pulsa **Enviar**.

201. Mobile Threat Defense es compatible con el sistema operativo Android 10, con las siguientes advertencias de configuración:

- Los servicios de ubicación son necesarios para detectar amenazas de red: los dispositivos Android 10 requieren que los servicios de ubicación estén activados para configurar Wifi. Desactivar los servicios de ubicación afecta la capacidad del cliente para identificar amenazas de red, incluidos Wifi no seguro y puntos de acceso no fiables.

- Independientemente del estado de los permisos de ubicación en el dispositivo, las amenazas críticas basadas en la red como MiTM, MiTM Fake SSL Certy Internal Network Access aún se detectan.

202. Tenga en cuenta la ubicación esperada y el comportamiento de Wifi para los diferentes modos de Android, que se describen a continuación.

TABLA 20. COMPORTAMIENTO ESPERADO PARA NUEVAS INSTALACIONES DESDE ANDROID 10

Modo de implementación	Comportamiento esperado
<b>Todos los modos</b>	La acción local Desconectar <b>Wifi</b> está deshabilitada en todos los modos en dispositivos Android 10.
<b>Android Enterprise</b> (Propietario del perfil)	<p>Durante la instalación o actualización de MTD en Android 10, se solicita al usuario del dispositivo que habilite los servicios de ubicación tanto para el dispositivo como para el perfil.</p> <p>NOTA: Si <b>No permitir la ubicación compartida</b> está habilitada en la configuración de <b>bloqueo de PO</b>, esto bloqueará la capacidad del usuario para activar los servicios de ubicación. Desactive esta función para solicitar al usuario que habilite los servicios de ubicación.</p> <ul style="list-style-type: none"> <li>Si el usuario selecciona <b>IR A CONFIGURACIÓN</b>: el servicio de ubicación se inicia en Configuración. Cuando el usuario habilita ambas opciones de ubicación, se detectarán las amenazas de red configuradas.</li> </ul> <p>NOTA: Si los servicios de ubicación a nivel de dispositivo están activados, pero los servicios de perfiles están desactivados, MTD no puede abrirse directamente en el conmutador de Servicios de perfiles. El usuario tendrá que localizar el interruptor.</p> <ul style="list-style-type: none"> <li>Si el usuario selecciona <b>NO</b>: No se detectarán amenazas de red, aunque se aplique la configuración MTD.</li> </ul>
<b>Android Enterprise</b> (Propietario del dispositivo)	La configuración de ubicación está habilitada sin la acción del usuario, lo que permite configuraciones de Wifi y detección MTD de amenazas de red.
<b>Administrador de dispositivos</b> (DA) modo	Las API de Wifi no están disponibles para los modos DA y de administración de aplicaciones móviles (MAM), incluso si los servicios de ubicación están habilitados. Por lo tanto, MTD no puede detectar amenazas de red para estos dispositivos. Se detectarán todas las amenazas configuradas que no sean de red.
<b>Modo de propiedad corporativa, habilitado personalmente</b> (COPE)	MTD requiere que los dispositivos COPE que ejecutan Android 10 tengan la ubicación habilitada en todo momento, y actualmente no se pueden deshabilitar.

## 7. DOCUMENTACIÓN DE MOBILE THREAT DEFENSE

203.La siguiente es una lista de la documentación:

- *Guía de soluciones* MTD para [Mobileiron Cloud](#)

[https://help.ivanti.com/mi/help/en\\_us/mtd/8x/gdcl/Content/LandingPage.htm](https://help.ivanti.com/mi/help/en_us/mtd/8x/gdcl/Content/LandingPage.htm)

Contiene información sobre nuevas características y mejoras, problemas, instrucciones de configuración, administración en la nube y en la consola de administración de amenazas, descripciones de características, protección contra sinkholes y protección antiphishing.

- *Guía de soluciones* de MTD para [CORE](#)

[https://help.ivanti.com/mi/help/en\\_us/mtd/11.x/gdco/LandingPage.htm](https://help.ivanti.com/mi/help/en_us/mtd/11.x/gdco/LandingPage.htm)

Contiene información sobre nuevas características y mejoras, problemas, instrucciones de configuración, managing en Core y en la consola de administración de amenazas, descripciones de características, protección contra sinkholes y protección antiphishing.

