Guía de configuración de Endpoint Manager for Mobile Devices

Contenido

Guía de configuración de IBM Endpoint Manager for Mobile Devices

La aplicación IBM Endpoint Manager for Mobile Device gestiona los teléfonos inteligentes y tabletas multimedia propiedad de la empresa y de los empleados que accedan a los recursos de la empresa. La aplicación se puede utilizar para gestionar la seguridad de dispositivos, el inventario de software y hardware y la gestión de aplicaciones.

Esta *Guía de configuración* proporciona instrucciones para los gestores de TI y administradores del sistema sobre cómo instalar y configurar la aplicación y cómo configurar los dispositivos móviles para integrarlos con la aplicación. Concretamente, incluye instrucciones de configuración para iOS, Android, Lotus Traveler y Microsoft Exchange. En esta guía además se incluyen los requisitos del sistema para cada componente de la aplicación y ofrece instrucciones de aplicación de la licencia y de instalación que le permiten desplegar Mobile Devices en su entorno.

Para obtener información sobre cómo utilizar Endpoint Manager for Mobile Devices, consulte la *Guía del usuario de Endpoint Manager for Mobile Devices*.

Componentes

La aplicación Mobile Devices incluye los siguientes componentes principales:

Servidor: El servidor de Endpoint Manager for Mobile Devices es una base de datos que se comunica con los retransmisores y la consola de Tivoli Endpoint Manager para gestionar los dispositivos de su implementación.

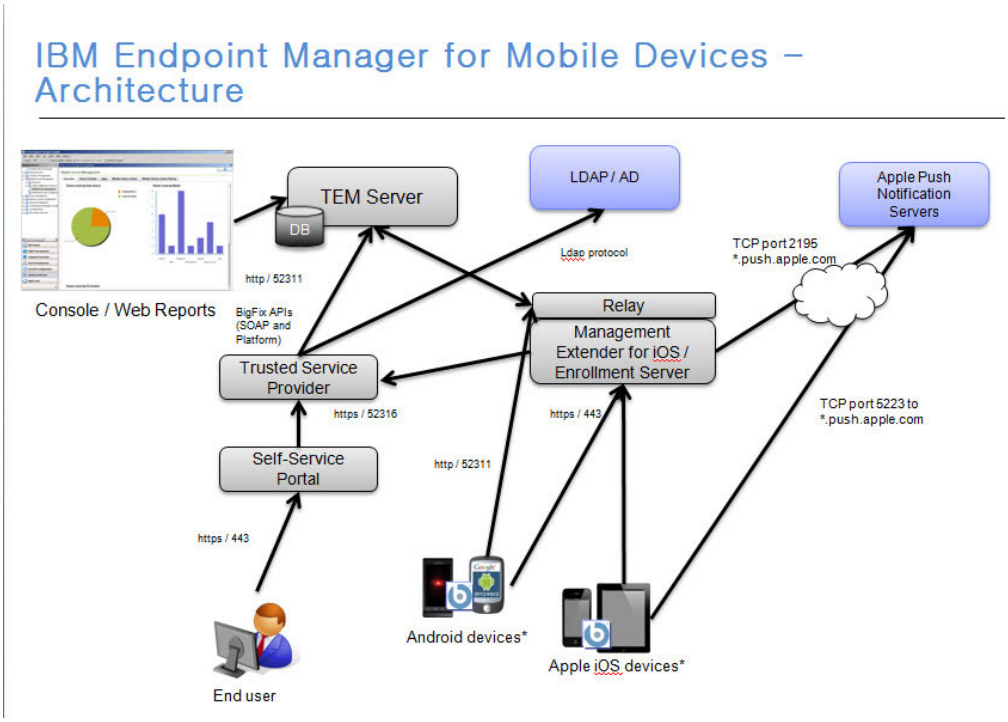
Retransmisores: Los retransmisores son componentes de red diseñados para distribuir la carga de descarga desde el servidor Tivoli Endpoint Manager y compilar y comprimir los datos recibidos desde clientes. En MDM, los retransmisores procesan la información de su dispositivos móviles y transmiten esa información al servidor de TEM.

Ampliadores de gestión: Los Ampliadores de gestión permiten gestionar los dispositivos sin un agente en el dispositivo.

Servidor de correo electrónico: Incluye los servidores Lotus Traveler y Microsoft Exchange.

Arquitectura

El diagrama que se muestra a continuación ilustra una representación visual de cómo Mobile Devices está diseñado para funcionar en el entorno.



Características principales

La siguiente es una lista de las características más importantes de Mobile Devices:

- Integración con la plataforma de Tivoli Endpoint Manager
- Capacidad para importar aplicaciones desde el servidor de Worklight
- Soporte para la gestión básica de dispositivos utilizando la gestión basada en el correo electrónico
- Soporte para la gestión avanzada de dispositivos utilizando la gestión basada en agentes
- Inventario de dispositivos
- Gestión de directivas de contraseñas y seguridad
- Mandatos de gestión como borrado de datos, bloqueo, borrado de contraseña, denegación de acceso al correo electrónico, envío y servicio itinerante de datos
- Gestión de aplicaciones
- Inscripción autenticada del acceso de usuario restringido
- Portal de autoservicio inteligente para gestionar dispositivos sin la necesidad de Tivoli Endpoint Manager o Web Reports.
- WiFi de Android
- Configuración de acceso a recursos empresariales, incluyendo correo electrónico, WiFi y VPN

Nota: El soporte para estas características varía según el dispositivo, sistema operativo y método de gestión.

Requisitos del sistema

General

A continuación se muestra una lista de requisitos del sistema general para utilizar la aplicación de MDM:

- Se debe utilizar Tivoli Endpoint Manager versión 8.2 o superior.
- Todos los ampliadores de gestión deben estar instalados en un sistema que ejecute Windows.
- Un retransmisor de Tivoli Endpoint Manager ya debe estar instalado en el sistema.

A continuación se listan los requisitos específicos para los servidores móviles.

Nota: Antes de utilizar esta aplicación, seleccione un puerto disponible para el Ampliador de gestión de iOS. El valor predeterminado es 443. Si desea utilizar un puerto diferente, especifique el puerto en el panel de control Configurar ampliador de gestión.

Para Lotus Traveler

Consulte los siguientes requisitos para utilizar el servidor de Traveler:

- El servidor de Domino debe ejecutar las tareas Traveler, DIIOP y HTTP.
- HTTP debe estar a la escucha en los puertos 80, 443 o ambos. El URL http(s)://<servidor>/diiop_ior.txt debe estar accesible de forma pública.
- DIIOP debe estar a la escucha en los puertos 63148, 63149 o ambos. En configuraciones que utilizan el puerto 63149, el certificado SSL debe ser válido y actual, y se debe haber generado un archivo *TrustedCerts.class* en la carpeta de datos de Domino.
- Cree un usuario administrativo. El usuario administrativo debe tener los permisos de *lectura* y *editar* en la ACL para LotusTraveler.nsf y debe poder ejecutar mandatos de Domino con y sin restricciones.

Consulte los siguientes requisitos para utilizar el ampliador de gestión del servidor de Lotus Traveler:

- El plugin debe ser capaz de contactar con el servidor en un puerto HTTP y uno DIIOP. Si DIIOP está a la escucha exclusivamente en el puerto 63149, el plugin requiere TrustedCerts.class específico del servidor en su ruta de clases. Para ello, incluya TrustedCerts.class en un archivo TrustedCerts.jar y despliéguelo mediante el panel de control Configurar ampliador de gestión.
- El usuario administrativo debe tener un nombre de usuario y contraseña. Las conexiones anónimas no están soportadas.

Para Microsoft Exchange

Consulte los siguientes requisitos para utilizar Exchange Server:

- Win 2008 Server
- Protocolo WS-Management

- WinRM
- Exchange Server 2007 o 2010

Consulte los siguientes requisitos para utilizar el ampliador de gestión del Exchange Server:

- Protocolo WS-Management
- WinRM
- Herramientas de administración de Exchange (solo Exchange 2007)

Nota: Si tiene la intención de utilizar esta Ampliador de gestión para conectarse a un servidor de Exchange 2007 remoto, primero debe instalar las Herramientas de administración de Exchange en el Ampliador de gestión de modo que se conecte correctamente con el servidor remoto.

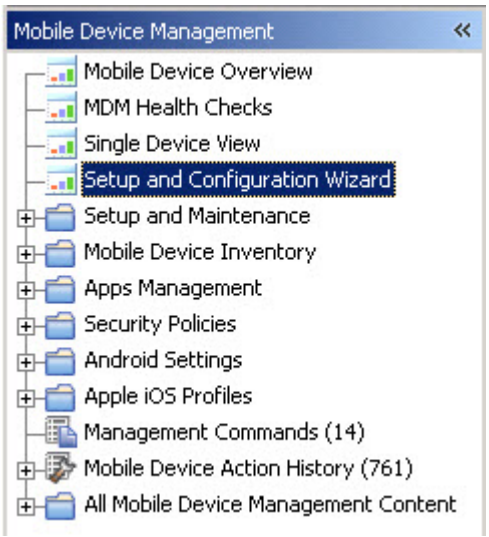
Para Android

Consulte los siguientes requisitos para utilizar Android:

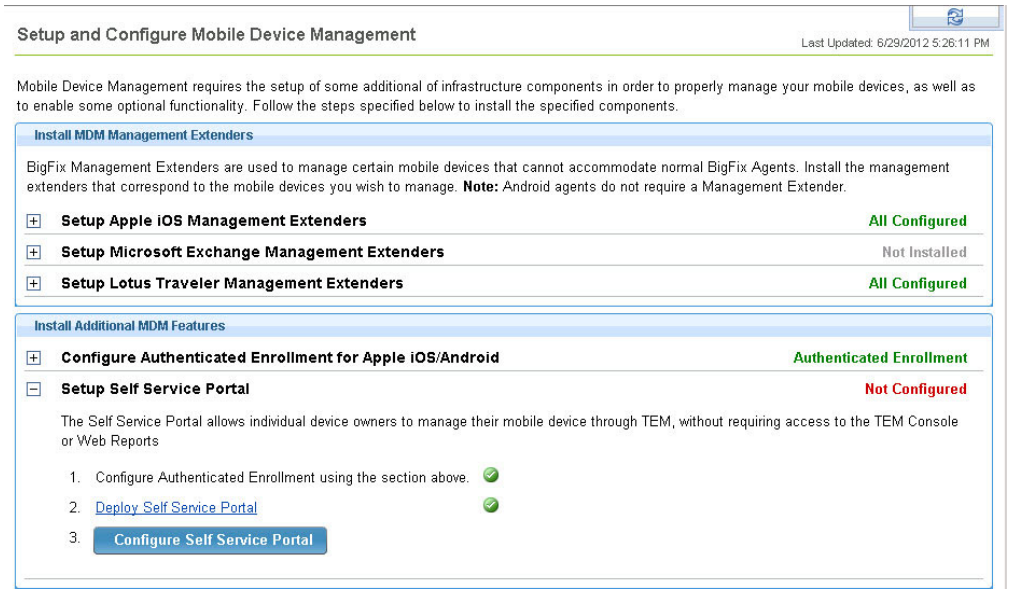
- Android 2.2+ (Froyo) en ejecución en procesadores ARM
- Capacidad para conectarse a un retransmisor o servidor de Tivoli Endpoint Manager

Asistente de instalación y configuración

El asistente de Instalación y configuración que está al inicio del árbol de navegación de MDM, configura los ampliadores de gestión para permitir que se conecten a servidores.



En el asistente Instalación y configuración, puede instalar ampliadores de gestión de iOS, Microsoft Exchange y Lotus Traveler y funciones adicionales de MDM como Inscripción autenticada y Portal autoservicio.

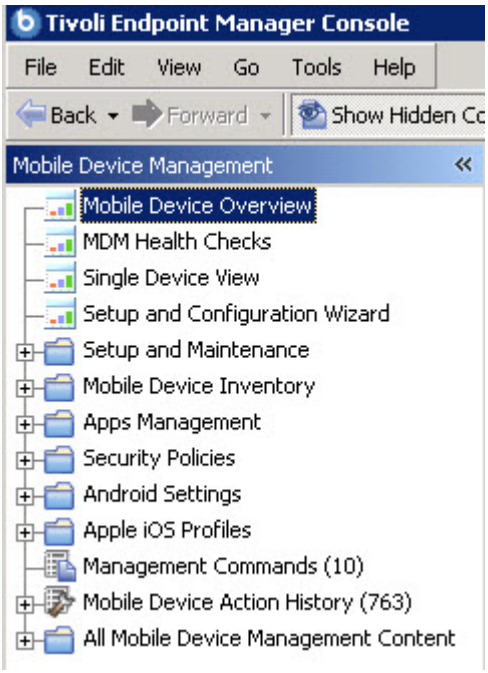


Haga clic en el signo más (+) que hay al lado de cada ampliador de gestión para expandir las opciones. A continuación, haga clic en *Configurar*. Se abrirá la ventana Configurar ampliador para cada tipo. En la ventana Configurar ampliador, puede definir los parámetros de la configuración.

Instalación y configuración

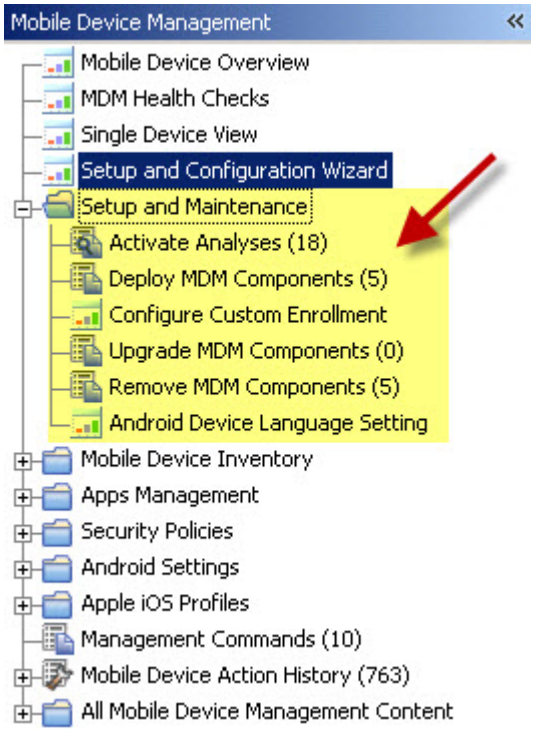
Antes de comenzar el proceso de instalación y configuración de Mobile Devices, debe familiarizarse con la consola de Tivoli Endpoint Manager y estar conectado al sistema. Para obtener más información sobre la consola, consulte la Guía del operador de la consola de Tivoli Endpoint Manager.

El árbol de navegación de Mobile Devices en la consola de Tivoli Endpoint Manager le servirá como un mando central para todas las tareas de instalación, configuración y gestión de Mobile Devices. El árbol de navegación le permite acceder fácilmente a todos los informes, asistentes, Fixlets, análisis y tareas relacionadas con la gestión de sus dispositivos. La parte superior del árbol de navegación contiene los cuatro paneles de control primarios: Visión general de dispositivos móviles, Comprobaciones de estado de MDM, Vista de dispositivo único y Asistente de instalación y configuración. El contenido primario de MDM se organiza en los siguientes nodos y categorías: Configuración y mantenimiento, Inventario de dispositivo móvil, Gestión de aplicaciones, Directivas de seguridad, Configuración de Android, Perfiles de Apple iOS e Historial de acciones de dispositivo móvil.



La configuración y la instalación de MDM en el despliegue utiliza el *Asistente de instalación y configuración* y el nodo *Configuración y mantenimiento* en el árbol de navegación. Ha utilizado el Asistente de instalación y configuración en la sección anterior para instalar y configurar los ampliadores de gestión. Ahora, puede utilizar el nodo Configuración y mantenimiento para activar análisis, desplegar o eliminar componentes, configurar una inscripción personalizada y configurar los valores de idioma del dispositivo Android

El nodo Configuración y mantenimiento del árbol de navegación muestra una lista de acciones preliminares que debe realizar antes de poder utilizar la aplicación Mobile Devices. Incluye activar análisis, desplegar o eliminar componentes, configurar una inscripción personalizada y configurar los valores de idioma del dispositivo Android.



El Ampliador de gestión proporciona un mecanismo para gestionar los dispositivos de su implementación mediante la interacción con su proceso de gestión existente.

Nota: No puede tener más de un ampliador de gestión para cada tipo.

Después de instalar y configurar todos los componentes MDM, los usuarios podrás descargar e instalar la aplicación de iOS desde Apple iTunes store y el agente de Android desde Google Play.

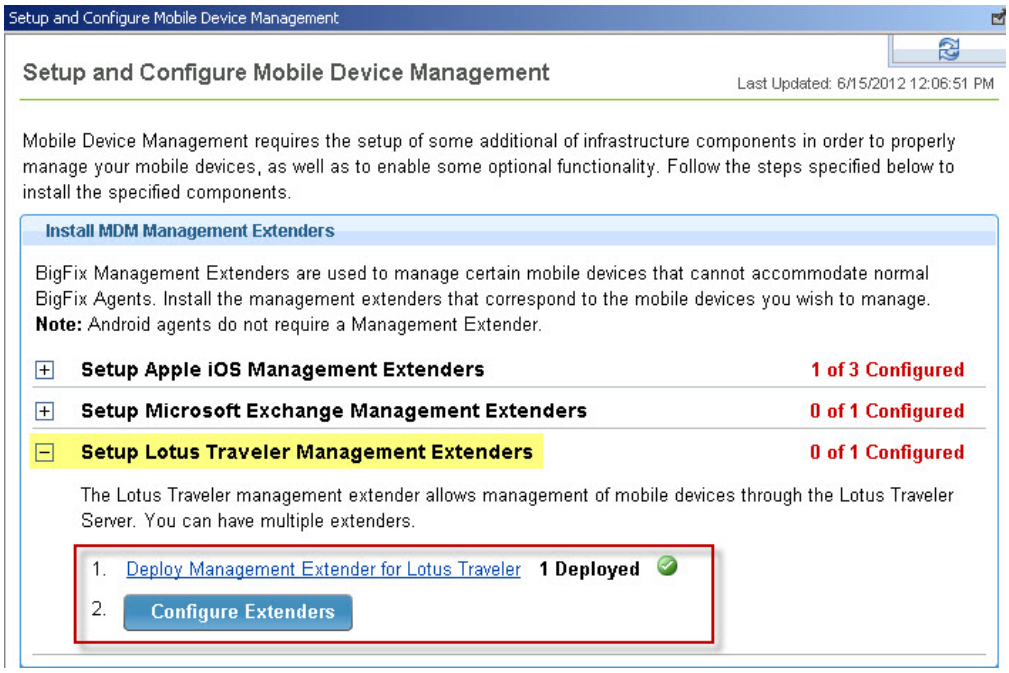
Activar Análisis necesarios

Empiece haciendo clic en el nodo Análisis necesarios en el árbol de navegación. Seleccione todos los análisis de la lista, haga clic con el botón derecho del ratón para mostrar el menú desplegable y haga clic en *Activar*. Después de activar todos los análisis, puede empezar a implementar sus ampliadores de gestión.

Ampliador de gestión para Lotus Traveler

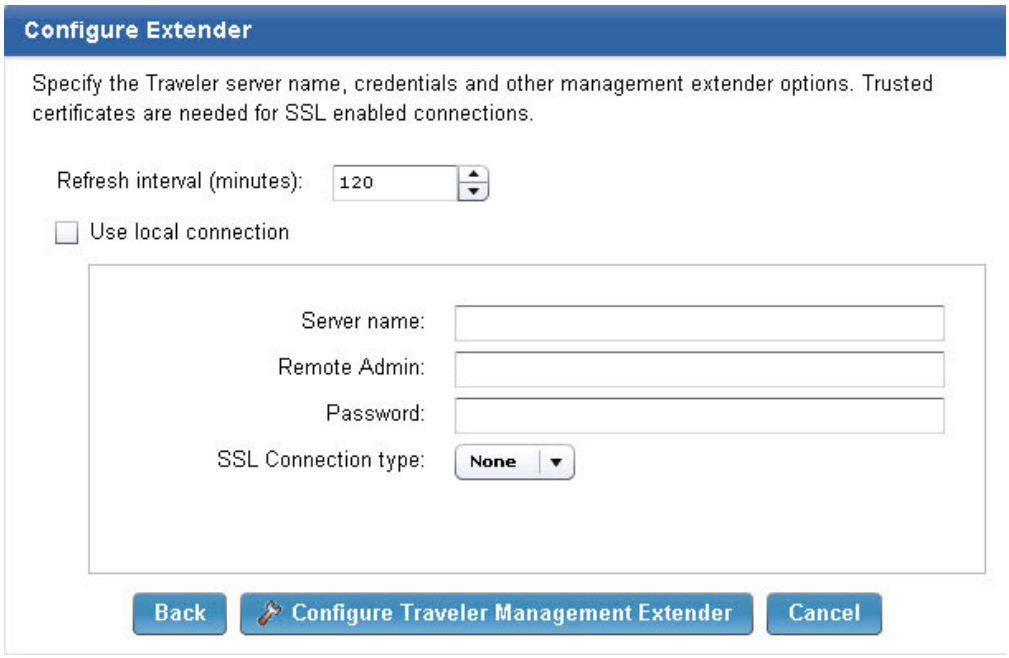
El Ampliador de gestión para Lotus Traveler debe estar instalado en el servidor de Tivoli Endpoint Manager o en un retransmisor. El Fixlet de implementación solo es relevante para los equipos con un agente de Tivoli Endpoint Manager y un retransmisor o servidor instalados.

Haga clic para expandir el Asistente de instalación y configuración del árbol de navegación. En la sección Instalar ampliadores de gestión MDM, haga clic en la sección *Configurar ampliadores de gestión de Lotus Traveler*.



Haga clic en el enlace para desplegar el Ampliador de gestión del fixlet de Lotus Travelers.

A continuación, haga clic en el asistente *Configurar ampliadores*. Haga clic en la línea correspondiente del ampliador que desea configurar y, a continuación, haga clic en Siguiente. En la siguiente pantalla, seleccione el nombre de servidor, credenciales y opciones del ampliador de gestión de Traveler. Haga clic en *Configurar Ampliador de gestión de Traveler* una vez configurados todos los parámetros.



Nota: Los Ampliadores de gestión deben conectarse a los servidores de correo electrónico, pero no hace falta que estén instalados en el mismo equipo.

Si está implementando el ampliador directamente en el servidor de Lotus Traveler, marque la casilla *Utilizar conexión local*. De lo contrario, especifique el servidor y las credenciales. También puede especificar un tipo de conexión SSL (HTTP, ORB, ninguno o ambos). Si selecciona ORB o ambos, debe proporcionar un archivo TrustedCerts.jar. Este archivo se genera en el servidor de Lotus Traveler.

Lotus Domino genera automáticamente el archivo TrustedCerts.class al habilitar la configuración de SSL. Este archivo normalmente está situado en la carpeta de datos de Domino y se regenera cuando se instalan o se modifican los certificados SSL del servidor de Domino. Un archivo TrustedCerts.class generado por un servidor solo es válido para ese servidor concreto. Al añadir o cambiar el certificado del servidor, se invalidarán todos los archivos TrustedCerts.class anteriores de ese servidor.

Un archivo TrustedCerts.class puede convertirse en un archivo TrustedCerts.jar utilizando este script ANT:

```
<project name="Convert" default="go" basedir=".">
<target name="go">
<jar destfile="TrustedCerts.jar" basedir="." compress="true">
<include name="TrustedCerts.class" />
</jar>
</target>
</project>
```

Este script generará un archivo TrustedCerts.jar que se puede desplegar en el plugin.

Cuando haya establecido todos los parámetros, haga clic en *Configurar Ampliador de gestión de Traveler.* Esta acción abre el diálogo Llevar a cabo acción, donde puede seleccionar el servidor que desea configurar. Haga clic en *Aceptar* para configurar los valores necesarios en el ampliador. Tras completar la acción, puede gestionar los dispositivos inscritos en el servidor de Traveler mediante IBM Endpoint Manager.

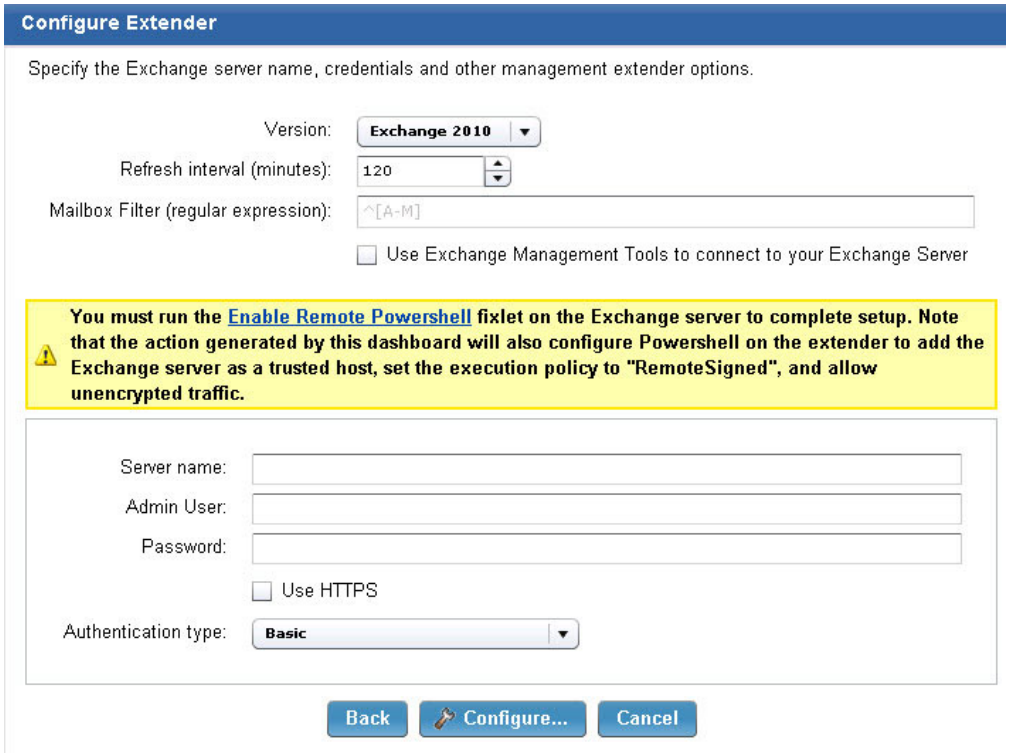
Ampliador de gestión para Microsoft Exchange

El Ampliador de gestión para Microsoft Exchange debe estar instalado en el servidor de Tivoli Endpoint Manager o en un retransmisor. El Fixlet de implementación solo es relevante para los equipos con un agente de Tivoli Endpoint Manager y un retransmisor o servidor instalados.

Haga clic para expandir el Asistente de instalación y configuración del árbol de navegación. En la sección Instalar ampliadores de gestión MDM, haga clic en la sección *Configurar ampliadores de gestión de Microsoft Exchange*.

Haga clic en el enlace para desplegar el Ampliador de gestión del fixlet de Microsoft Exchange.

A continuación, haga clic en el asistente *Configurar ampliadores*. Haga clic en la línea correspondiente del ampliador que desea configurar y, a continuación, haga clic en Siguiente. En la siguiente pantalla, seleccione el nombre de Exchange Server, credenciales y otras opciones del ampliador de gestión.



El Ampliador de gestión de Exchange admite ya conexiones para servidores de Exchange 2007, Exchange 2010 y Office 365.

El campo Filtros de buzón le permite seleccionar ampliadores de gestión en un pequeño subconjunto de cuentas de correo electrónico.

Acceso a Filtros de buzón desde el Asistente de instalación y configuración. Primero debe desplegar el fixlet. A continuación, haga clic en *Panel de control de Configuración de ampliadores* y busque el campo Filtros de buzón.

Los filtros se pueden introducir como una *expresión regular*. Por ejemplo,

```
^[A-K]
```

que incluiría todas las cuentas de correo electrónico que empiecen por la letra A hasta la K.

Nota: Como requisito previo, las Herramientas de administración de Exchange deben estar instaladas en los sistemas donde se implementarán los ampliadores.

Nota: Puede ejecutar el fixlet Habilitar Powershell remoto en el servidor de Exchange para finalizar la configuración. Si el aviso se muestra en la pantalla Configurar ampliador, haga clic en el enlace *Habilitar Powershell remoto* para desplegar el fixlet.

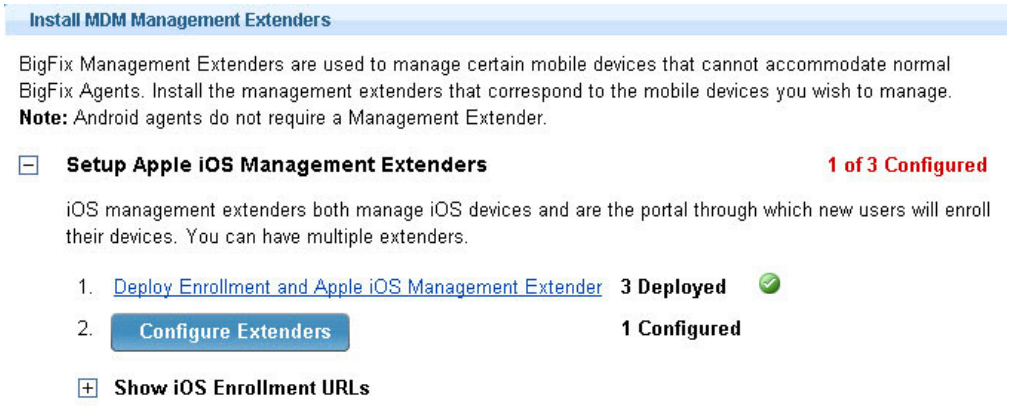
Tras especificar toda la información necesaria, haga clic en *Configurar*.

Ampliador de gestión para iOS

El Ampliador de gestión para Apple iOS debe estar instalado en el servidor de Tivoli Endpoint Manager o en un retransmisor. El Fixlet del ampliador de gestión solo es importante para los equipos con un agente de Tivoli Endpoint Manager y un retransmisor o servidor instalados.

Nota: Debe tener un ID de Apple para completar este proceso con una dirección de correo electrónico válida. Cree una cuenta que tenga una dirección de correo electrónico no personal y mantenga el acceso al portal de certificado Push en caso de que se vaya.

Haga clic en el Asistente de instalación y configuración desde el árbol de navegación. En la sección del asistente Instalar ampliadores de gestión MDM, haga clic en la cabecera *Configurar ampliadores de gestión de Apple iOS*.



Configure el ampliador de gestión de Apple iOS siguiendo estos pasos:

1. Despliegue el Fixlet del ampliador de gestión
2. Obtenga un certificado
3. Configure el ampliador de gestión

Desplegar Fixlet del ampliador de gestión

Haga clic en el enlace *Desplegar inscripción y ampliador de gestión de Apple iOS* en el panel de control para desplegar el fixlet.

Realice una copia de seguridad de la clave privada de notificación Push de Apple.

Tras implementar el Fixlet, realice una copia de seguridad de uno de los archivos en una ubicación segura. El archivo probablemente se encuentra en la ruta siguiente del ampliador de gestión:

C:\Archivos de programa (x86)\BigFix Enterprise\Management Extender\MDM Provider\private

Este archivo se denominará *push_key.pem*.

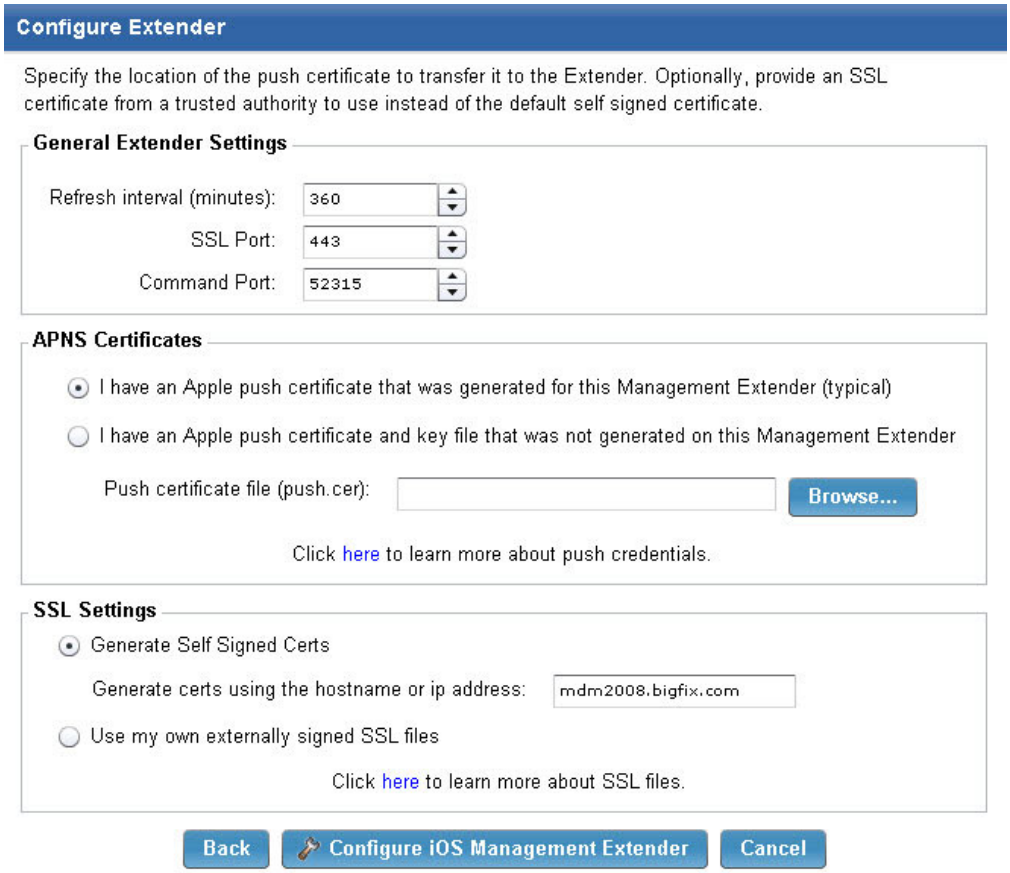
Esta clave está relacionada con su certificado push, de forma que si desea implementar diversos ampliadores de gestión con el mismo certificado, debe utilizar la misma clave para cada uno.

Obtener un certificado

1. Descargue el archivo CSR que se ha generado durante la instalación abriendo https://<dns o dirección IP>/csr. Guarde el archivo.
2. Envíe un mensaje de correo electrónico a iem-mdm-signup@wwpdl.vnet.ibm.com y adjunte el archivo push.csr. Escriba `MDM APNS CSR <nombre organización>` en la línea de asunto.
3. IBM responderá por correo electrónico con una solicitud de certificado firmada.
4. Vaya a https://identity.apple.com/pushcert/
5. Inicie la sesión con su ID de Apple. Considere la posibilidad de utilizar un ID que no sea personal para que otros miembros de la organización puedan utilizar el ID de Apple en el futuro.
6. Seleccione *Crear certificado*.
7. Lea y acepte los Términos y condiciones.
8. Siga las instrucciones para cargar el archivo de certificado que ha recibido de IBM.
9. Descargue el nuevo archivo de certificado push firmado "MDM_IBM Global Engineering Solutions_Certificate.pem".
10. Si abre el archivo .pem en un editor de texto, debería ver un certificado codificado en base64 que empieza por *BEGIN CERTIFICATE* y tiene varias líneas de caracteres aleatorios.
11. Cambie el nombre del archivo a *push.cer* y cree una copia de seguridad.

Configurar ampliadores

Haga clic en *Configurar ampliadores* en el panel de control.



En la ventana, seleccione las opciones de configuración.

No es común cambiar los números de puerto. El intervalo de actualización controla la frecuencia en que el ampliador de gestión enviará un mandato de actualización a los agentes. Si utiliza un intervalo de actualización más frecuente, podrá ver información actualizada de los dispositivos más rápido, pero potencialmente provoca que se utilicen más datos y batería en el dispositivo.

Seleccione el certificado que ha recibido de Apple en la sección anterior. Si tiene un archivo de clave push (porque ha generado manualmente el CSR y el par de claves), inclúyalo también en esta sección.

Si tiene una clave SSL y certificado de una fuente de confianza, puede incluirlos en esta sección. Esto sustituirá el certificado SSL autofirmado y evitará los avisos SSL en los dispositivos.

Ahora el Ampliador de gestión para Apple iOS está listo para gestionar dispositivos iOS (realizando la escucha en el puerto que ha especificado en el paso anterior). El puerto 443 es el puerto predeterminado. Puede probarlo abriendo el navegador y visitando https://<dns o dirección IP>.

Nota: El Ampliador de gestión de iOS requiere conexión directa al servidor de notificaciones Push de Apple. Esta interacción se produce mediante TCP/IP y no se puede utilizar ningún proxy HTTP.

Ampliadores de gestión de BlackBerry

Los ampliadores de gestión de BlackBerry son componentes en un despliegue de Mobile Device Management que gestionan un subconjunto de dispositivos BlackBerry. Los dispositivos BlackBerry que ejecutan las versiones del sistema operativo de BlackBerry 4.5, 4.6, 5.0, 6.0 y 7.0 están administrados por uno o varios BlackBerry Enterprise Servers. Los ampliadores de gestión de BlackBerry permiten la comunicación entre IBM Endpoint Manager Server y los BlackBerry Enterprise Servers de la red. Debe desplegarse y configurarse un ampliador de gestión de BlackBerry para cada BlackBerry Enterprise Server del despliegue.

Los dispositivos BlackBerry que ejecutan BlackBerry 10 o PlayBook no están gestionados por ampliadores de gestión de BlackBerry. En su lugar, estos dispositivos se comunican a través de ActiveSync y están gestionados por ampliadores de gestión de Microsoft Exchange. Si la red no incluye un BlackBerry Enterprise Server versión 4 o 5, no es necesario un ampliador de gestión de BlackBerry en el despliegue de Mobile Device Management.

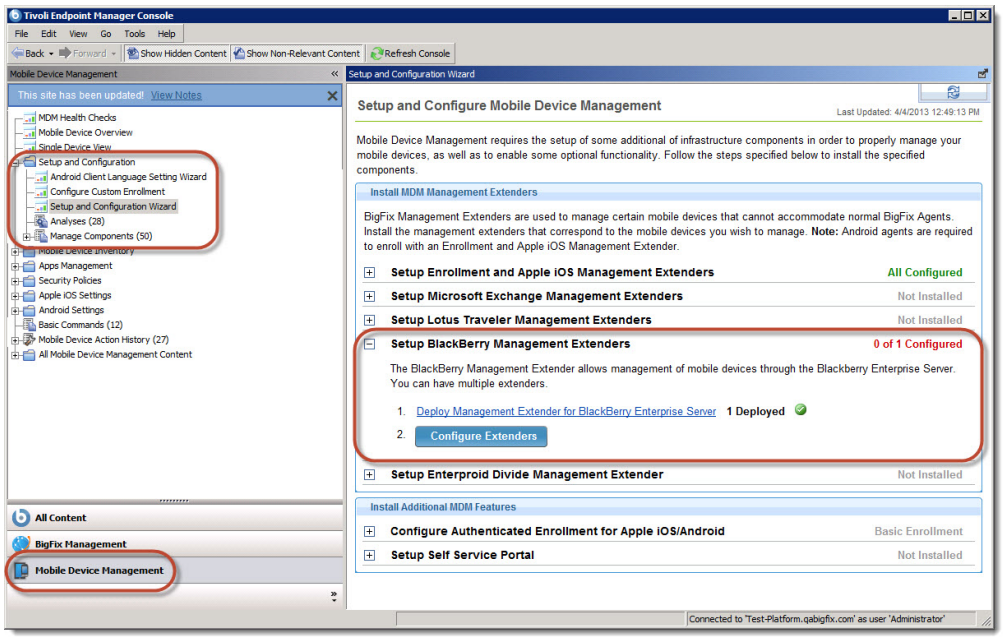
Los ampliadores de gestión deben desplegarse primero, que es el proceso de instalarlos en un equipo. Una vez desplegado un ampliador de gestión de BlackBerry, debe configurarlo para permitir que se comunique con un BlackBerry Enterprise Server en la red.

Despliegue de un ampliador de gestión de BlackBerry

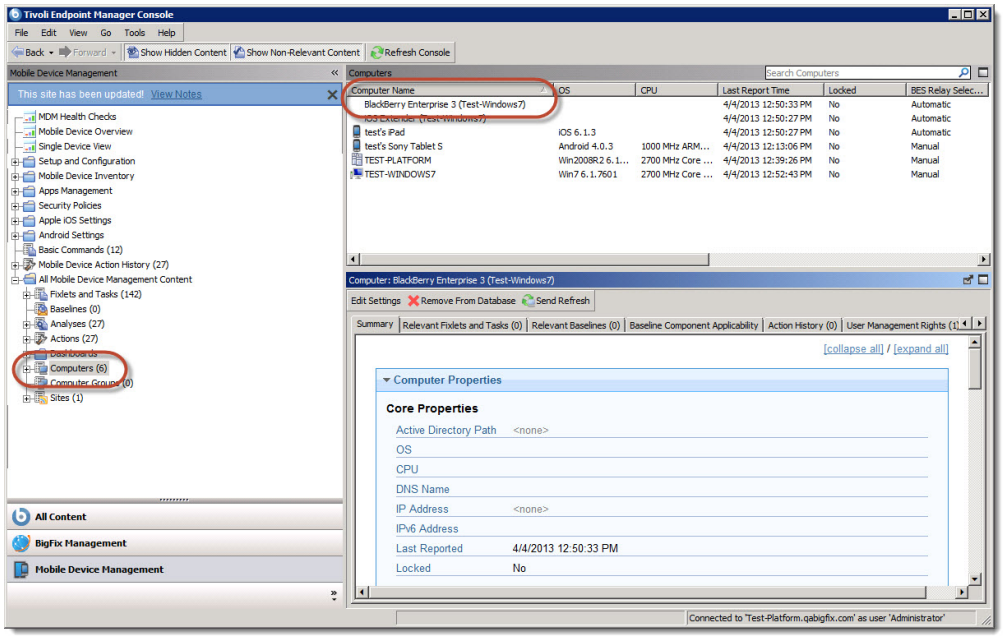
Para desplegar un ampliador de gestión de BlackBerry, siga estos pasos:

1. Seleccione el sitio Mobile Device Management y navegue a **Instalación y configuración > Asistente de instalación y configuración**. El panel de control aparece a la derecha. Debe activar los análisis relevantes si se le solicita.
2. En el campo **Instalar ampliadores de gestión de MDM**, expanda el nodo **Configurar ampliadores de gestión de BlackBerry**.
3. Seleccione la opción 2, **Desplegar ampliador de gestión para BlackBerry Enterprise Server**.
   a. Con la tarea de fixlet visualizada, seleccione **Llevar a cabo una acción**.
   b. Seleccione la primera opción, **Haga clic aquí para desplegar...**.
   c. Seleccione el equipo en el que desee desplegar el ampliador y haga clic en **Aceptar**.
   d. Espere a que finalice la tarea, que puede tardar varios minutos.
4. Vuelva al **Asistente de instalación y configuración** y asegúrese de que el despliegue haya sido satisfactorio con buscando las notificaciones **X desplegado** y **X de X configurados**.

Nota: Cuando ejecuta las tareas, puede haber un retardo entre una tarea que aparece como “Completada” y todos los elementos de las tareas que se están completando en el sistema host como, por ejemplo, la instalación de software.



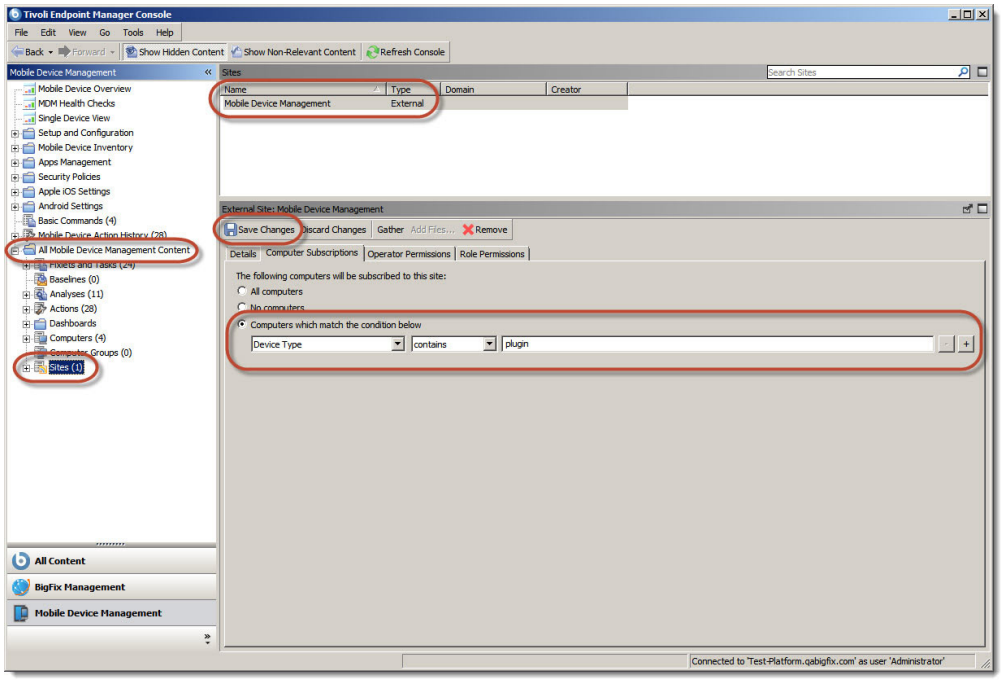
Una vez desplegado un ampliador de gestión de BlackBerry, aparece como un equipo individual con el nombre `BlackBerry Enterprise <##> <Nombre de retransmisor>`, donde `<##>` es el valor numérico del ampliador y `<Nombre de retransmisor>` es el nombre de host del retransmisor donde se instala el ampliador. Este comportamiento es distinto de otros ampliadores de gestión, ya que permite que los ampliadores de gestión de BlackBerry tengan una capacidad de varios inquilinos sin necesidad de configuración adicional.



Suscripción de un ampliador de gestión a Mobile Device Management

Los ampliadores de gestión deben suscribirse al sitio Mobile Device Management para realizar funciones de gestión. Asegúrese de que los ampliadores de gestión se suscriban al sitio Mobile Device Management realizando las siguientes tareas:

1. Navegue a **Mobile Device Management > Contenido de gestión de todos los dispositivos móviles > Sitios**.
2. Seleccione el sitio **Mobile Device Management**.
3. Seleccione la pestaña **Suscripciones del equipo**.
   - Si se selecciona **Todos los equipos**, el despliegue suscribe automáticamente los nuevos ampliadores de gestión al sitio; no continúe con estos pasos.
   - Si está suscribiendo sitios definiendo reglas con **Equipos que coinciden con las condiciones anteriores** seleccionado, continúe en el siguiente paso.
4. Cree una regla especificando los siguientes detalles para la regla:
   - `Device Type | contains | plugin`
5. Haga clic en **Guardar cambios** para guardar las nuevas reglas.



Configuración de un ampliador de gestión de BlackBerry

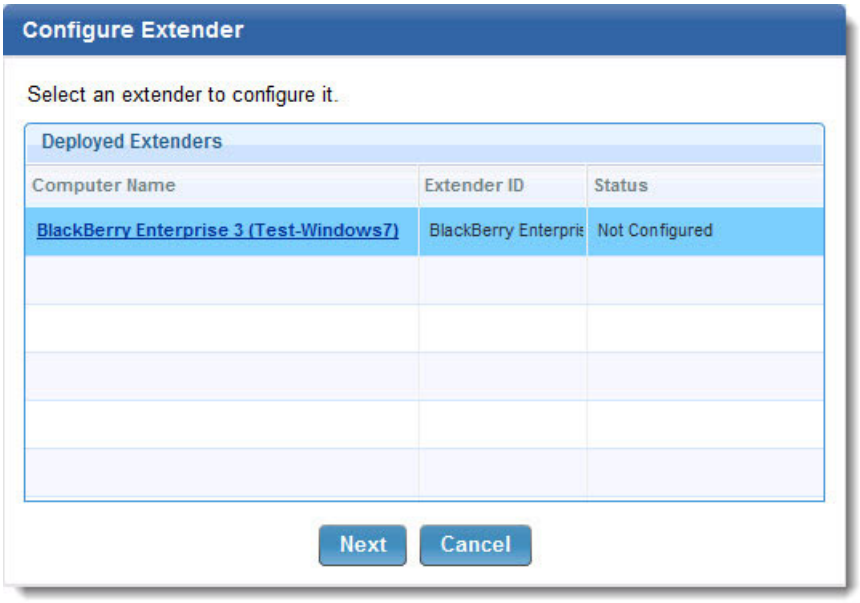
Una vez desplegado el ampliador de gestión de BlackBerry, debe configurarse. La configuración requiere valores del administrador de BlackBerry Enterprise Server. Durante la configuración, apunte el ampliador de gestión a un BlackBerry Enterprise Server. Las acciones ejecutadas en la consola de IBM Endpoint Manager se dirigen a BlackBerry Enterprise Server, que pasa los mandatos a los dispositivos BlackBerry gestionados por BlackBerry Enterprise Server.

Para configurar un ampliador de gestión de BlackBerry, realice estas tareas:

1. Navegue a **Mobile Device Management > Instalación y configuración > Asistente de instalación y configuración**.

2. Expanda el nodo **Configurar ampliadores de gestión de BlackBerry**. Esta área muestra cuántos de estos ampliadores de gestión específicos se despliegan y cuántos se configuran.
3. Haga clic en **Configurar ampliadores**. En la ventana que aparece, seleccione la fila que representa el ampliador que desea configurar y haga clic en **Siguiente**.

Nota: Si hace clic en el enlace de nombre de sistema subrayado, la consola muestra las propiedades de ese sistema. Haga clic en **Atrás** para volver a la ventana **Configurar ampliadores**.



La ventana **Configurar ampliador** contiene varios campos relacionados con el despliegue de BlackBerry Enterprise Server. El administrador de BlackBerry debe proporcionar los valores de estos campos. La excepción es el recuadro de selección **Etiqueta de inscripción para un entorno de varios inquilinos**, que sólo se utiliza en los entornos de varios inquilinos.

Para continuar configurando el ampliador de gestión, realice estas tareas:

1. Rellene los campos siguientes correspondientes al BlackBerry Enterprise Server:

   Método de inicio de sesión
   Elija el método de inicio de sesión adecuado en la lista desplegable. El valor adecuado viene determinado por el despliegue de BlackBerry Enterprise Server.

   Nombre de servidor
   Especifique el nombre de host del BlackBerry Enterprise Server que desee asociar con este ampliador de gestión de BlackBerry.

   Administrador remoto
   Especifique el nombre de usuario de la cuenta de administrador que se utiliza para acceder al BlackBerry Enterprise Server que se especifica en el campo **Nombre de servidor**.

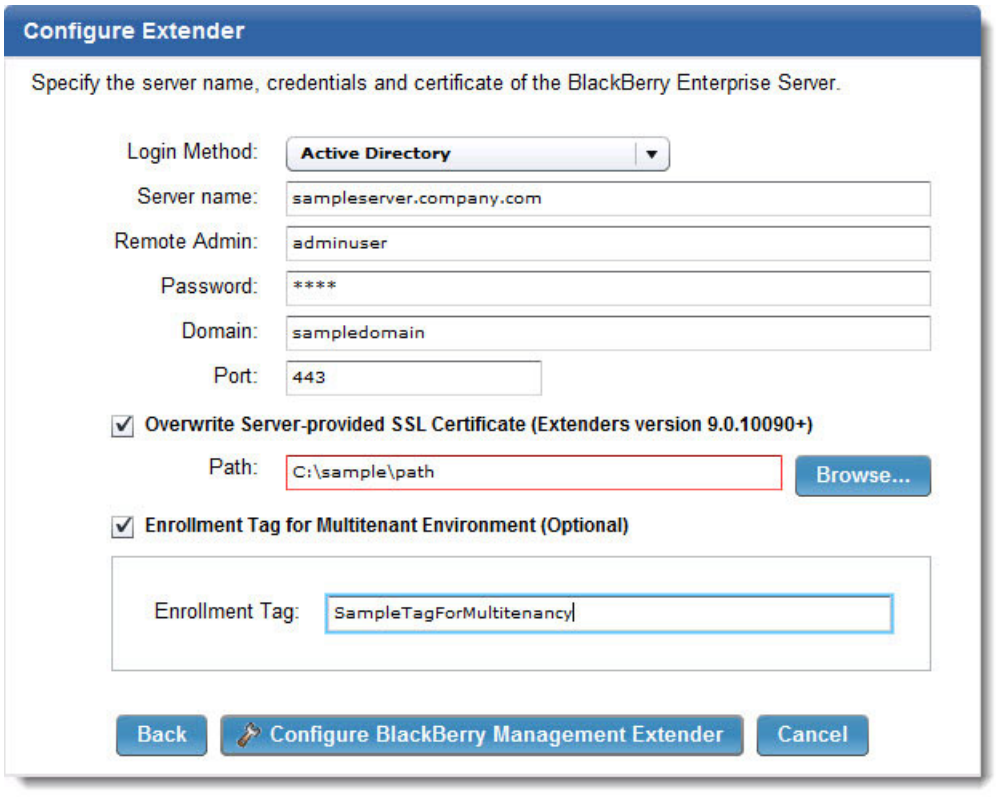
   Contraseña
   La contraseña de la cuenta de administrador que se especifica en el campo **Administración remota**.

Dominio
Este campo sólo aparece si el método de inicio de sesión elegido es "Active Directory". Especifique el dominio de BlackBerry Enterprise Server.

Puerto El puerto que se utiliza para comunicarse con BlackBerry Enterprise Server.

Sobrescribir certificado SSL proporcionado por el servidor
De forma predeterminada, el proceso de configuración importa el certificado SSL de BlackBerry Enterprise Server. Si selecciona esta opción, puede proporcionar manualmente el certificado SSL correspondiente especificando el nombre de ruta del archivo.

2. Si gestiona más de un BlackBerry Enterprise Server, seleccione **Etiqueta de inscripción para entornos de varios inquilinos** y especifique una etiqueta para asignársela a este ampliador de gestión de BlackBerry. Para obtener más información sobre esta opción, consulte "Etiqueta de inscripción para entornos de varios inquilinos".
3. Haga clic en **Configurar ampliador de gestión de BlackBerry**.
4. Seleccione el ampliador de gestión de BlackBerry correspondiente en el campo **Nombre del sistema** y haga clic en **Aceptar**.
5. Vuelva al **Asistente de instalación y configuración** y asegúrese de que aparezca una marca de selección verde para indicar que el ampliador de gestión se ha configurado. Este proceso puede tardar varios minutos.



Etiqueta de inscripción para entornos de varios inquilinos

Cuando configura un ampliador de gestión de BlackBerry, el recuadro de selección **Etiqueta de inscripción para entornos de varios inquilinos** sólo se utiliza si gestiona varios BlackBerry Enterprise Servers. La etiqueta de inscripción se utiliza para diferenciar este ampliador de gestión de BlackBerry de otros ampliadores

configurados para otros BlackBerry Enterprise Servers en la red. La utilización de una etiqueta de inscripción habilita un entorno de varios inquilinos que permite a los operadores de la consola de IBM Endpoint Manager seleccionar dispositivos específicos según el BlackBerry Enterprise Server que los gestione.

Seleccione **Etiqueta de inscripción para entornos de varios inquilinos** y especifique una etiqueta de inscripción para asignarla al ampliador de gestión de BlackBerry que está configurando. Debe desplegar y configurar un ampliador de gestión de BlackBerry aparte para cada BlackBerry Enterprise Server que desee incluir en el despliegue.

Nota: Cuando configura una etiqueta de inscripción en un ampliador de gestión de BlackBerry, se renombra el ampliador para que incluya la etiqueta de inscripción como parte del nombre. El convenio de denominación es `BlackBerry Enterprise <##> <NOMBRE_RETRANSMISOR>, <ETIQUETA DE INSCRIPCIÓN>`.

Configuración de aplicaciones de iOS

Para establecer el cliente móvil en el iPhone, siga los pasos siguientes:

1. Desde el iPhone, abra la App Store.
2. Seleccione *Buscar* y busque *IBM Mobile.*
3. Seleccione *IBM Endpoint Manager Mobile Client.*
4. Seleccione *Gratis* y, a continuación, *Instalar aplicación.*
5. En la pantalla *Entrar*, inicie la sesión utilizando su ID de Apple existente o cree un nuevo ID de Apple. Esto instalará el cliente móvil en el dispositivo.
6. Inicie la aplicación desde su dispositivo.
7. Especifique los campos dirección del servidor, correo electrónico del trabajo y propiedad del dispositivo.
8. Seleccione *Inscribir.*

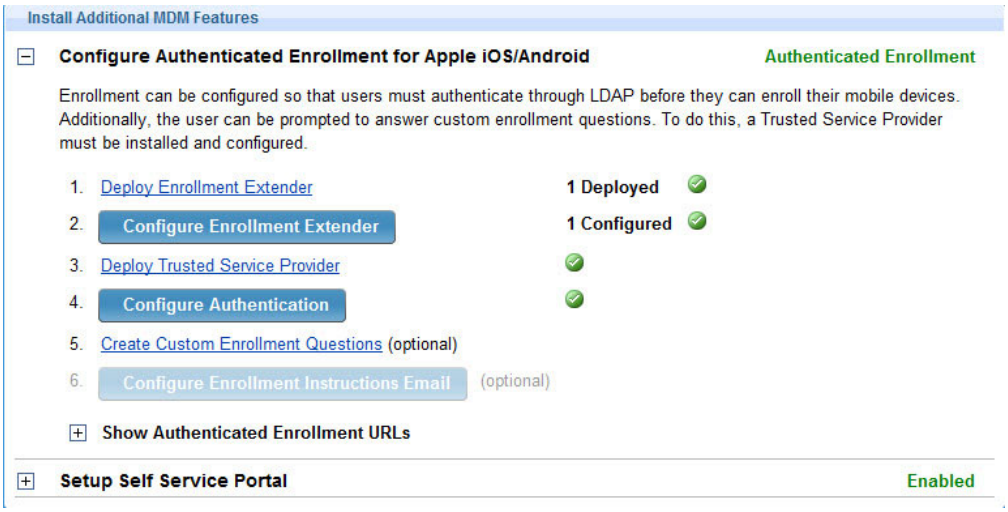
Inscripción autenticada

De forma predeterminada, MDM puede gestionar los dispositivos sin ninguna autenticación. Como novedad, puede restringir el acceso al despliegue de MDM para que accedan solo los usuarios autenticados que inicien sesión con un nombre de usuario y contraseña. La inscripción autenticada es una función opcional.

Para habilitar la inscripción autenticada, abra el Asistente de instalación y configuración desde el árbol de navegación y desplácese hacia abajo hasta la sección Configurar inscripción autenticada.

Para la configuración de las inscripciones autenticadas deberá seguir los siguientes pasos:

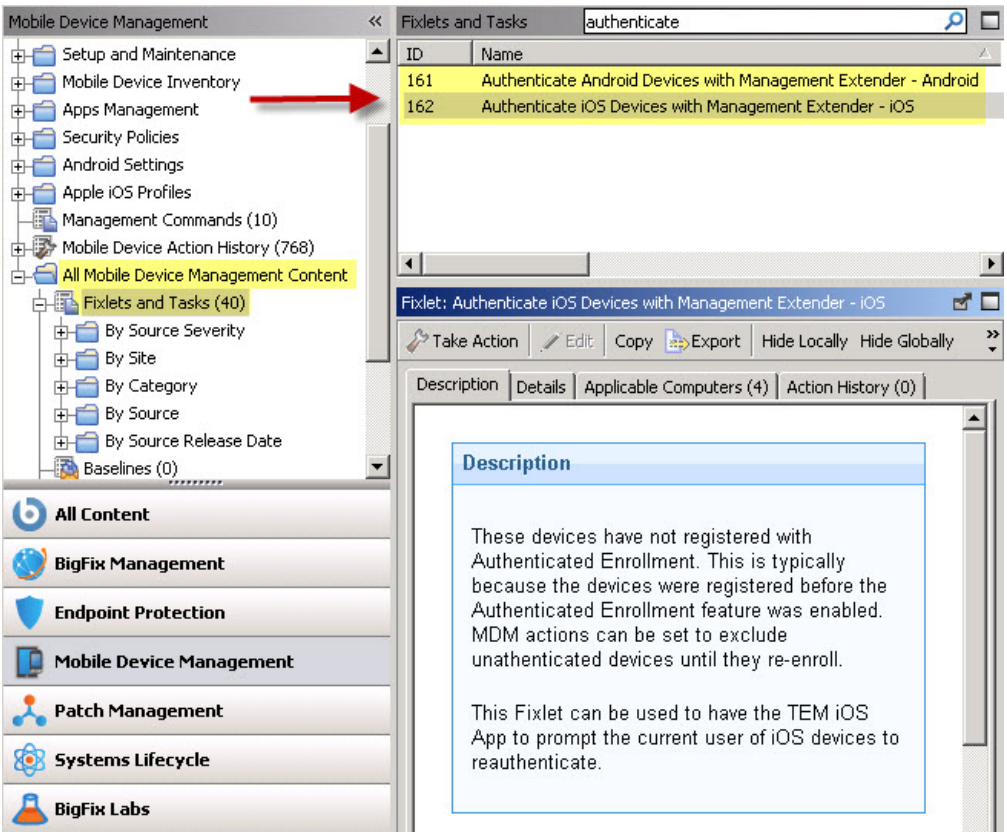
1. Desplegar el ampliador de inscripción.
2. Configurar el ampliador de inscripción.
3. Desplegar el proveedor de servicios de confianza.
4. Configurar Autenticación.
5. (Opcional) Crear preguntas de inscripción personalizada.
6. (Opcional) Configurar correo de instrucciones de inscripción.



Haga clic en cada paso y siga las indicaciones para completar el proceso.

Nota: A la terminación de cada paso, le seguirá un breve retraso.

Después de configurar el servidor de inscripción para su autenticación, utilice dos fixlets para iniciar una acción que les recuerde a los usuarios autenticar o volver a autenticar su dispositivo. Para acceder a los fixlets, haga clic en el nodo Contenido de gestión de todos los dispositivos móviles que hay en la parte final del árbol de navegación de MDM. Haga clic para ampliar el contenido, haga clic en Fixlets y tareas y, a continuación, muévase para ubicar los números 161 y 162 de los fixlets.

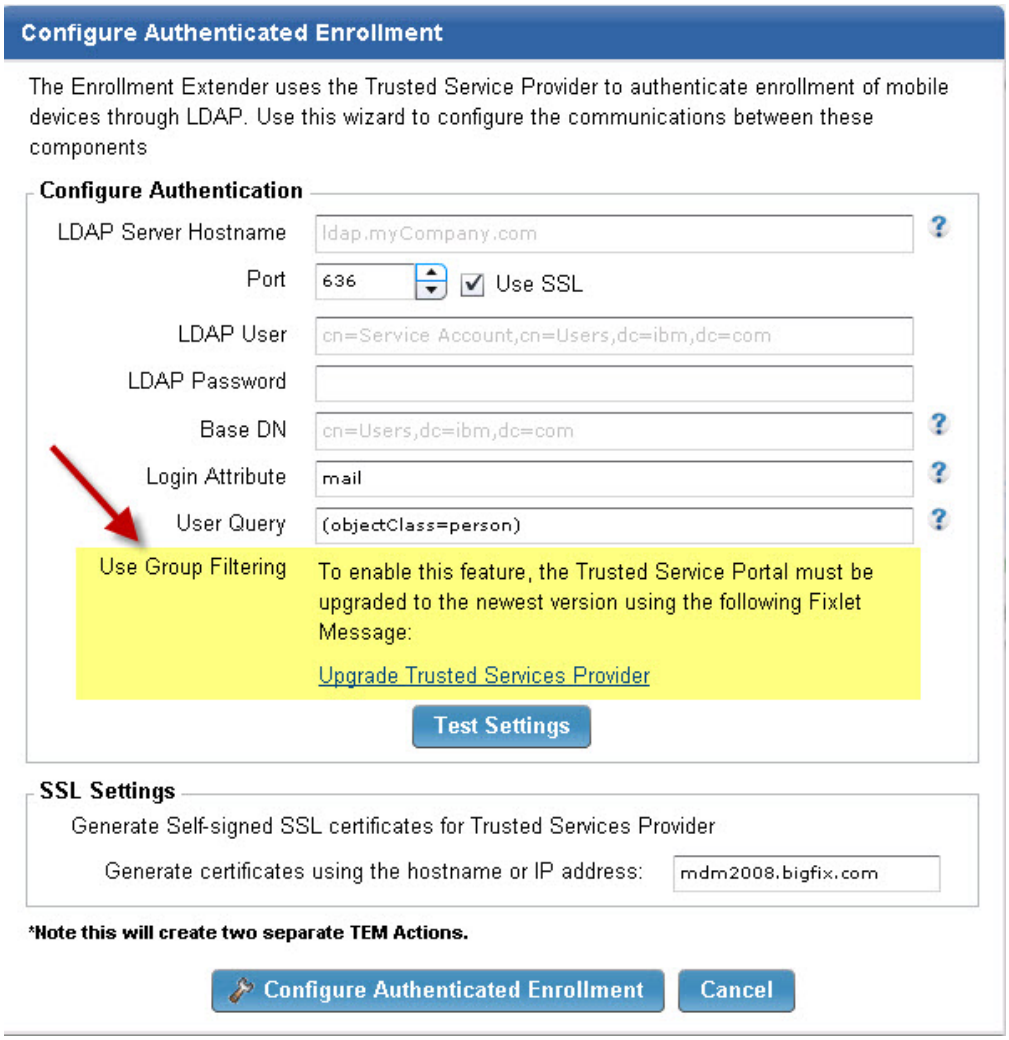


Inscripción restringida de dispositivos por Grupo LDAP

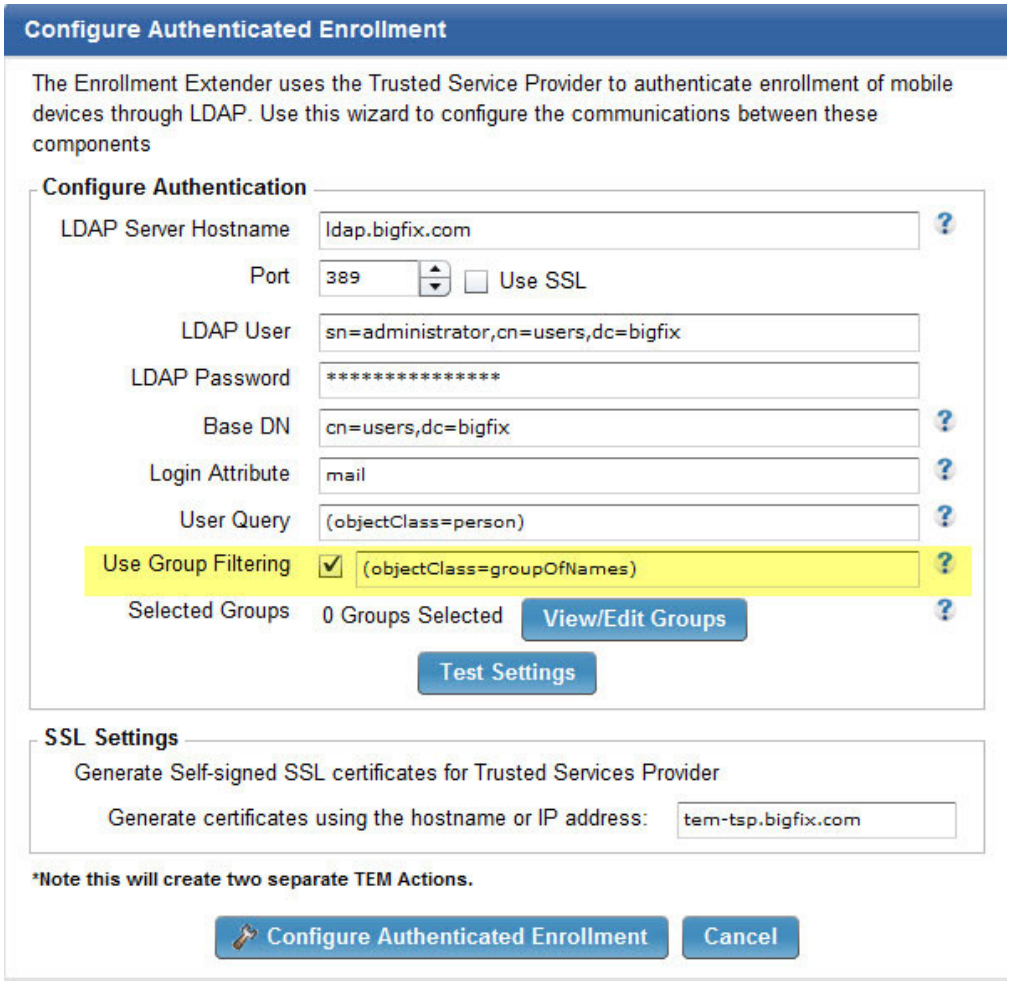
Ahora Endpoint Manager for Mobile Devices añade la función de inscripción restringida de dispositivos en un determinado conjunto de grupos LDAP utilizando TSP. Esta función opcional permite a los administradores del sistema seleccionar solo los grupos que pueden autenticar los ampliadores de gestión. La función proporciona control y seguridad adicional.

Al configurar la Inscripción autenticada en un despliegue de TSP, escriba los valores LDAP. Haga clic en el Asistente de instalación y configuración desde el árbol de navegación. Al instalar características adicionales de MDM, haga clic en Configurar autenticar.

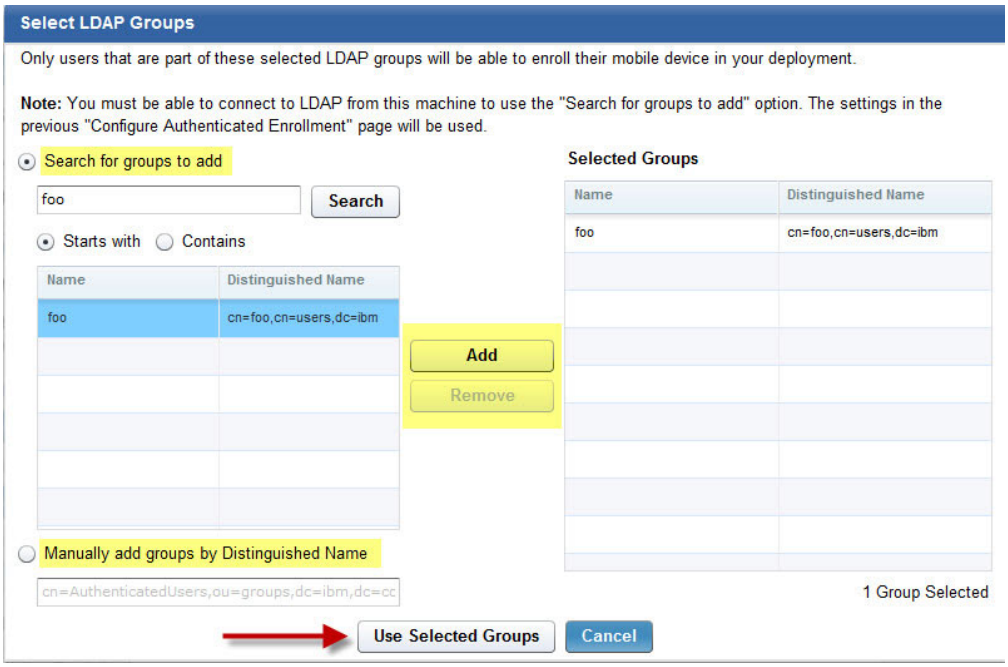
Si tiene un TSP desplegado, puede utilizar el enlace Actualizar Proveedor de servicios de confianza para actualizar su TSP a la versión más reciente.



Después de actualizar su TSP, haga clic en el recuadro de selección que hay al lado de Utilizar filtro de grupo para habilitar el botón Ver/Editar grupos.



Luego, haga clic en Ver/Editar grupos para abrir un nuevo diálogo "Seleccionar grupos LDAP", donde puede buscar grupos y seleccionar los grupos existentes o escribir manualmente el nombre distinguido de grupos LDAP. Utilice la opción manual si no puede establecer una conexión al servidor LDAP.



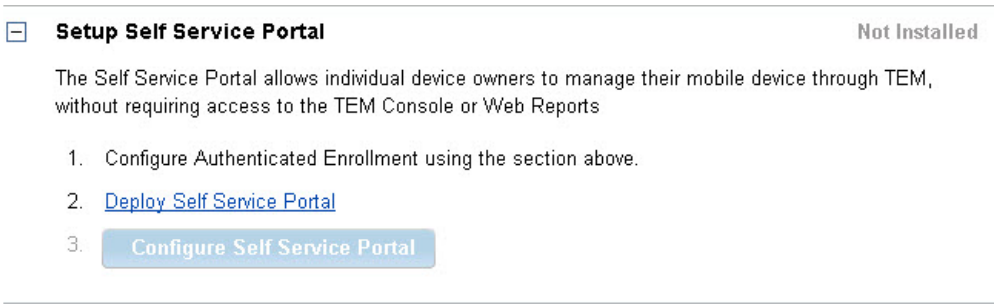
Puede buscar grupos con un nombre común que empiece o contenga una cadena determinada, utilizando credenciales LDAP desde el diálogo anterior. Los resultados se muestran en la tabla Seleccionar grupos. Después de localizar el grupo, selecciónelo en la tabla y haga clic en "Añadir". La acción añade el grupo a la tabla Grupos seleccionados que hay a la derecha. Puede escribir manualmente los grupos escribiendo el nombre distinguido del grupo en el recuadro de texto inferior y haga clic en "Añadir". Para eliminar un grupo, selecciónelo en la tabla Grupos seleccionados y haga clic en Eliminar. Haga clic en Utilizar grupos seleccionados para confirmar sus selecciones y vuelva al diálogo Configurar inscripción autenticada.

Portal de autoservicio

El Portal de autoservicio inteligente le permite gestionar dispositivos sin la necesidad de Tivoli Endpoint Manager o Web Reports.

Para acceder al Portal de autoservicio, abra el Asistente de instalación y configuración desde el árbol de navegación. Después de configurar la Inscripción autenticada, desplácese hacia la sección *Configurar Portal de autoservicio* del panel de control.

Despliegue el fixlet *Portal de autoservicio*, a continuación, haga clic en el asistente *Configurar Portal de autoservicio* y siga los pasos.



Configuración del agente de Android

Para configurar el agente de Android, utilice los pasos siguientes. Necesitará un retransmisor orientado a Internet para este proceso.

1. Inicie la aplicación Market de Android en el dispositivo y busque *IBM Endpoint Manager for Mobile Devices.* Seleccione la aplicación y haga clic en *Descargar.* Haga clic en *Aceptar y descargar.*
2. Después de instalar la aplicación, seleccione **Abrir**.
3. Haga clic en **Activar**.
4. Escriba la dirección del servidor TEM (o el retransmisor orientado a Internet) que ha obtenido del administrador y escriba la dirección de correo electrónico de su trabajo. Seleccione una de las dos opciones disponibles para indicar si el dispositivo es personal o de la empresa. Haga clic en **Incorporar**.
5. Si la conexión ha sido satisfactoria, aparecerá brevemente el mensaje *Configuración correcta del cliente móvil* y el estado del servicio indicará que el servicio está en ejecución.

Nota: Para desinstalar el agente de Android de TEM, deseleccione la opción Administrador de dispositivo bajo Configuración/Ubicación y seguridad en el dispositivo.

Nota: Para controlar la privacidad de la ubicación del dispositivo, implemente el Fixlet *Deshabilitar propiedades de ubicación de GPS* bajo Inventario de dispositivo móvil/Configuración de datos.

Samsung SAFE

Samsung Approved for Enterprise (Samsung SAFE) es un conjunto de características de gestión que están disponibles para usarlas en dispositivos móviles de Samsung. Después de instalar e inscribir el cliente móvil de IBM, un mensaje automático le solicitará que instale IBM Mobile Client para Samsung desde Google Play Store. Después de instalarlo, las funciones de Samsung se habilitarán automáticamente en el dispositivo.

Para obtener información sobre el flujo de trabajo para configurar SAFE en dispositivos móviles de Samsung, consulte la wiki Tivoli Endpoint Manager Developer Works:

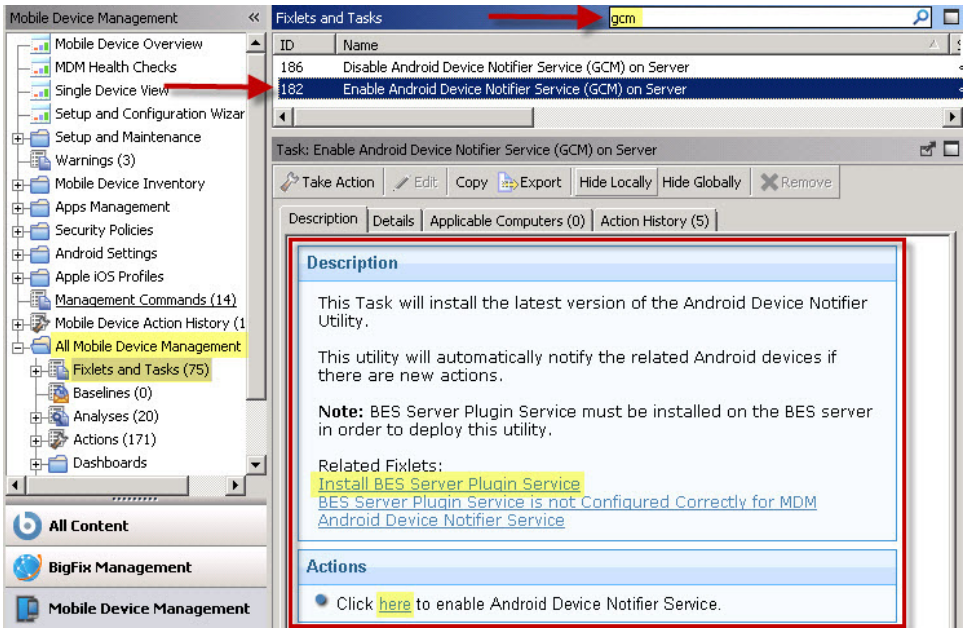
https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Mobile%20Device%20Management

Servicio de notificación del dispositivo Android

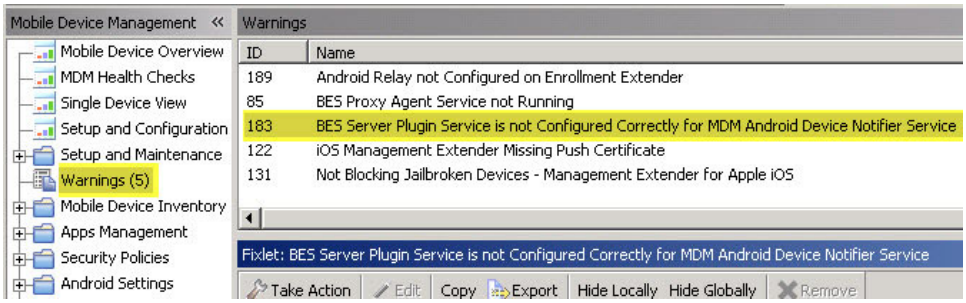
El Servicio de notificación del dispositivo Android es el equivalente de Android de Google Cloud Messaging. Para direccionar tiempos de respuesta lentos, puede utilizar el Servicio de notificación del dispositivo Android para cambiar tiempos de respuesta, por ejemplo, de cinco horas a varios minutos.

Para configurar el servicio en el servidor TEM del dispositivo Android, complete los siguientes pasos:

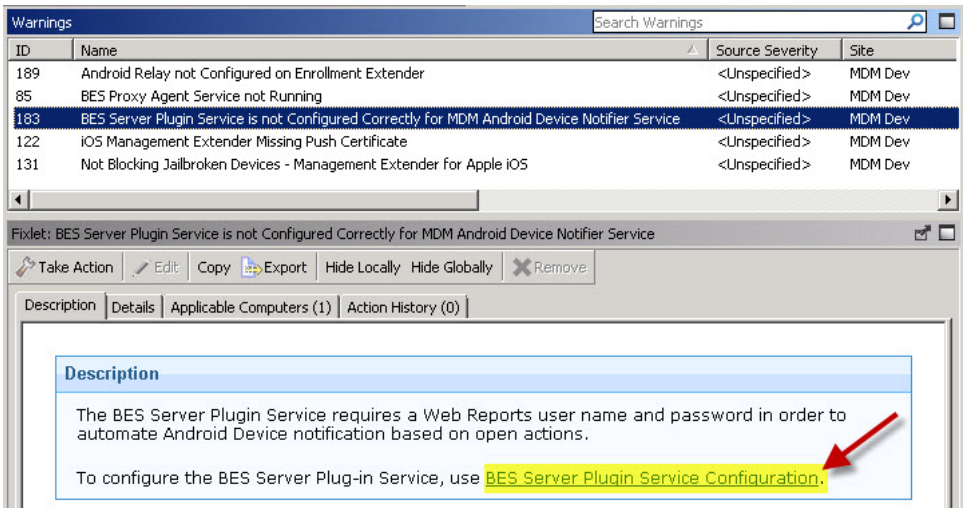
1. Instale el servicio de Plugin del servidor de BES en el servidor. Para hacerlo, haga clic en el árbol de navegación *Contenido de gestión de todos los dispositivos móviles* y seleccione *Fixlets y tareas*. En la lista, seleccione Habilitar notificador de dispositivo Android. Si no, puede escribir "GCM" en el recuadro de búsqueda de la parte superior. Haga clic en el enlace Instalación del servicio de Plugin del servidor de BES en la sección Descripción para instalar el servicio.



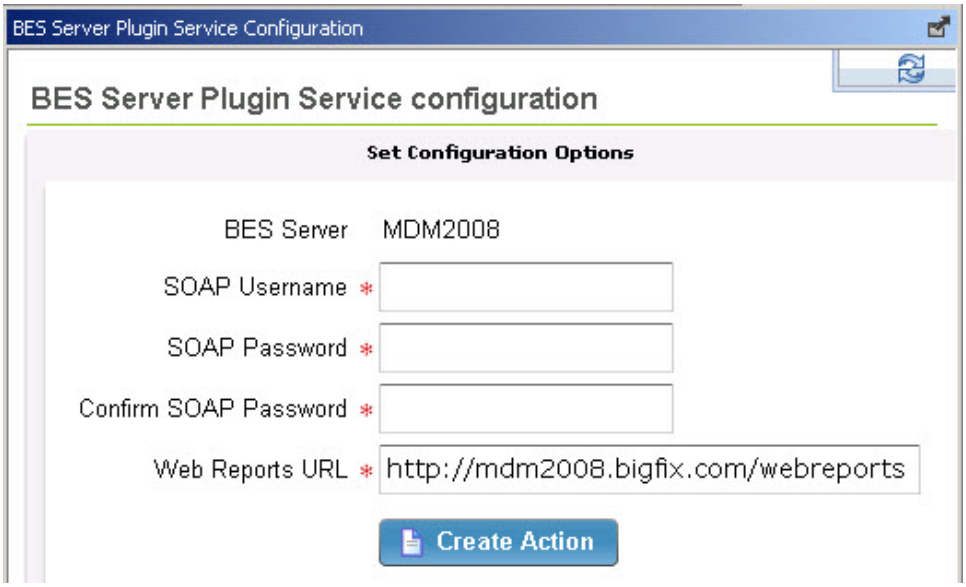
2. Utilice la configuración del Servicio de plugin del servidor BES para configurar el servicio de plugin. Haga clic en Avisos en el árbol de navegación y seleccione la Configuración del Servicio de plugin del servidor BES.



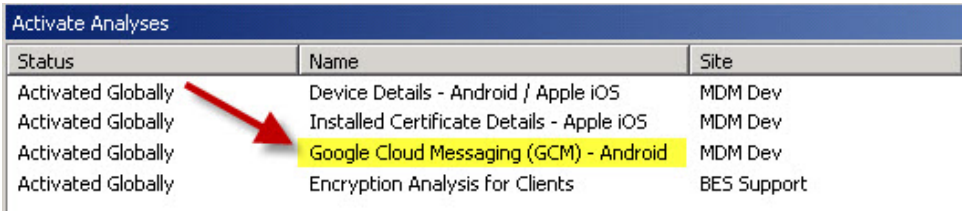
En la ventana del Fixlet, haga clic en el enlace Configuración del servicio de Plugin del servidor de BES.



Defina las opciones de configuración escribiendo el usuario y contraseña de Web Reports (SOAP) en los campos que se proporcionan. A continuación, haga clic en *Crear acción*.



3. Habilite el Servicio de notificador de dispositivo Android (GCM) en el servidor. Para hacerlo, vuelva al Contenido de gestión de todos los dispositivos móviles en el árbol de navegación y seleccione Fixlets y tareas. En la lista, seleccione Habilitar notificador de dispositivo Android. Haga clic en el enlace en el recuadro Acciones para habilitar el Servicio de notificador de dispositivo Android.
4. Active el análisis *Google Cloud Messaging (GCM) - Android* . Para ello, haga clic en el nodo Configuración y mantenimiento en el árbol de navegación y seleccione Activar análisis. Seleccione el análisis Google Cloud Messaging, haga clic con el botón derecho del ratón y seleccione Activar.



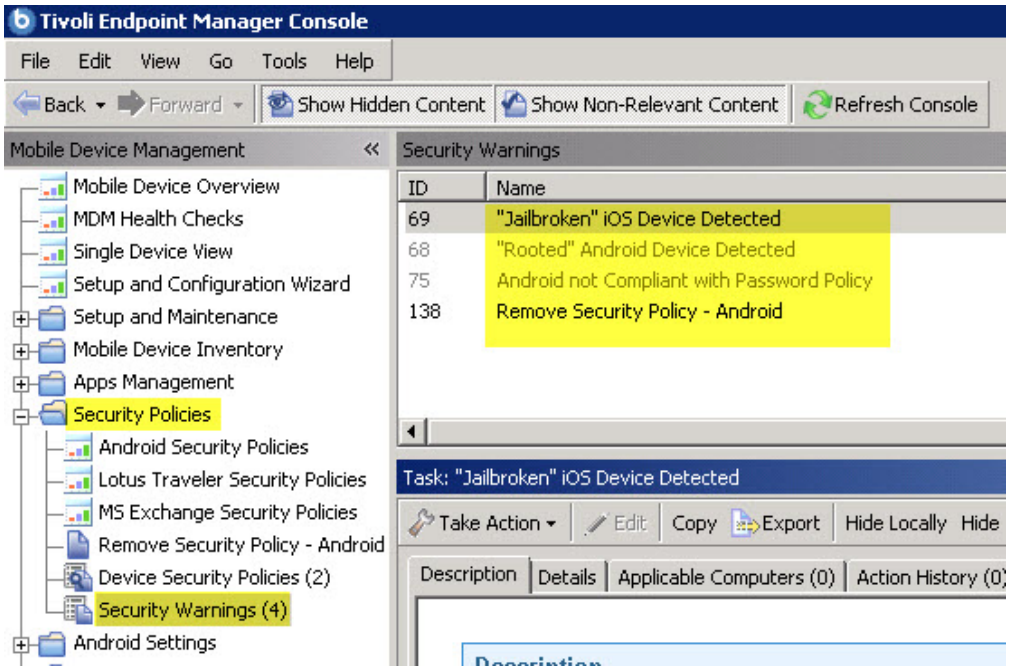
Al enviar mensajes de notificación, podría tener un retraso en la entrega en la aplicación Android de destino que se ejecuta en el dispositivo, según el volumen de mensaje y cómo se ponen en cola los mensajes.

Nota: El Servicio de notificación del dispositivo Android notifica todos los dispositivos Android si hay una nueva acción que no destina determinados dispositivos. Después, notifica los dispositivos de destino si la acción se destina por ID de sistemas.

Avisos

Se mostrarán cuatro posibles avisos en el panel de lista Avisos si son relevantes para su implementación:

- Dispositivo iOS manipulado (Jailbroken) detectado
- Dispositivo Android manipulado (Rooted) detectado
- Android no cumple la directiva de contraseñas
- Eliminar directiva de seguridad - Android



Para determinar qué avisos son relevantes para la implementación, acceda a ellos mediante el nodo Directivas de seguridad en el árbol de navegación.

Haga clic en cada aviso individualmente y despliéguelos haciendo clic en la sección Acciones que hay en la ventana Fixlet.

Preguntas más frecuentes

Utilice la siguiente lista de Preguntas más frecuentes para soporte de configuración general de MDM:

¿Cuál es la relación entre el Ampliador de gestión para iOS y la Inscripción autenticada?

El ampliador de iOS también es el servidor de inscripción que actúa como pasarela de los dispositivos que desea registrar en Mobile Device Management (MDM). Realiza todas las llamadas de fondo a LDAP para verificar que un usuario tiene permiso para registrarse o está verificado. Para iOS, descarga el perfil MDM que se instala en el dispositivo iOS que configura el teléfono que gestionará el servidor de MDM. Para Android, utiliza un retransmisor para realizar los otros procesos de inscripción.

¿Se pueden instalar dos ampliadores de gestión en el retransmisor?

Sí. Puede tener dos ampliadores diferentes en el mismo retransmisor pero no pueden ser del mismo tipo de ampliador. Por ejemplo, puede tener un ampliador de iOS y otro Lotus Traveler en el mismo retransmisor pero no dos ampliadores de iOS.

¿Qué credenciales necesito para utilizar MDM?

LDAP, Web Reports y credenciales para acceder a la consola de Tivoli Endpoint Manager.

¿Qué puertos debo habilitar para utilizar Mobile Device Management?

Debe tener habilitados los puertos 52315 y 52316 en un único sistema.

¿La versión del servidor de Mobile Device Management debe coincidir con la versión de mis aplicaciones?

Sí, se recomienda. Además, el servidor de MDM 1.1 se muestra con la versión 8.2.20000.0 y el servidor MDM 1.0 se muestra con 8.2.10000.0.

¿Dónde debo ubicar mi red en TSP (Proveedor de servicios de confianza) y SSP (Portal de autoservicio)?

Ubique el TSP en la red interna donde tiene acceso a LDAP, Tivoli Endpoint Manager y Web Reports. También debe ser accesible para el ampliador iOS. TSP sirve para proteger operaciones confidenciales que iOS o SSP realizan internamente. Se puede ubicar SSP externamente o internamente, según si desea ejecutar usuarios en VPN para poder acceder o permitir el uso desde el inicio.

¿Cómo actualizo a la versión más reciente de MDM?

Para actualizar los componentes del servidor, haga clic en *Actualizar componentes de MDM* desde el nodo Configuración y mantenimiento en el árbol de navegación. Después de la actualización, utilice el Asistente de instalación y configuración para asegurarse de que todos los componentes se configuran correctamente. Para

actualizar una aplicación de iOS, vaya a Apple iTunes Store desde su dispositivo. Para actualizar una aplicación de Android, vaya a Google Play desde su dispositivo de Android.

¿Cuántos sistemas admite el ampliador de iOS?

El ampliador de iOS normalmente admite hasta 5.000 sistemas.

¿Cómo habilito o inhabilito el rastreo del uso de datos en dispositivos iOS?

Puede utilizar los fixlets 195 y 196 para habilitar o inhabilitar el rastreo de uso de datos creando un valor de cliente en un dispositivo iOS de destino. Para acceder a los fixlets, haga clic en *Contenido de gestión de todos los dispositivos móviles* desde el árbol de navegación, luego haga clic en *Fixlets y tareas* y escriba el nombre de fixlet en el recuadro de búsqueda a la derecha. Nota: si inhabilita el rastreo de ubicación en una aplicación iOS, también se inhabilitará el rastreo de datos, es decir, que la aplicación iOS no rastreará el uso de ningún dato.

¿Cómo habilito o inhabilito el rastreo de ubicación de dispositivo?

Para poder habilitar el rastreo de ubicación de dispositivo deberá dar autorización al usuario de dispositivo y al administrador de TEM. El usuario de dispositivo debe alternar el valor adecuado en la configuración de aplicación de dispositivo. El administrador de TEM debe ejecutar la tarea "Habilitar propiedades de ubicación de GPS" en el árbol de navegación Asistente de instalación y configuración/ Configurar componentes de MDM y active el análisis "Información de ubicación - Android/Apple iOS" en Asistente de instalación y configuración/Activar análisis. Para inhabilitar el rastreo de ubicación, el usuario de dispositivo puede desactivar el valor en los valores de aplicación de dispositivo. El administrador de TEM puede desactivar el análisis o ejecutar la tarea "Inhabilitar propiedades de ubicación de GPS" que se lista en Configurar componentes de MDM, si anteriormente se ha habilitado el dispositivo. Por razones de privacidad, el administrador de TEM no puede sobrescribir el valor de autorización del usuario de dispositivo.

¿Por qué el nombre de la aplicación de instalación aparece en mi dispositivo de Android con caracteres ilegibles?

El agente de Android (aplicación de IBM Mobile Client) no tendrá conocimientos de la página de código (idioma) del despliegue de Tivoli Endpoint Manager, incluso después de que se registre. El valor actual del cliente IANA en dispositivos Android es Inglés (Windows-1252), a menos que esté configurado. Si este valor no es el mismo que el del despliegue de Tivoli Endpoint Manager, los datos que se envían desde los dispositivos Android podrían ser ilegibles incluso si los dispositivos tienen la misma página de códigos (idioma) como despliegue de Tivoli Endpoint Manager.

Para configurar el valor de cliente IANA automáticamente en todos los dispositivos tras la inscripción, cree la acción de directivas desde el asistente Configuración de idioma del dispositivo Android. Haga clic en *Crear acción de política*.

La siguiente lista muestra los valores IANA o idiomas admitidos:

- EN - windows-1252
- CH - gh2312 (simplificado)
- JA - Shift_JIS

- ES - windows-1252
- IT - windows-1252
- FR - windows-1252
- DE - windows-1252
- CH - big5 (tradicional)
- KO - ks_c_5601-1987

Asistencia

Para obtener más información sobre este producto, consulte los siguientes recursos:

- Sitio de soporte de IBM Endpoint Manager
- Wiki de IBM Endpoint Manager
- Base de conocimiento
- Foros y comunidades

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

Es posible que en otros países IBM® no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios disponibles actualmente en su localidad. Las referencias a programas, productos o servicios de IBM no pretenden establecer o implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que abarquen el tema descrito en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar sus consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

El siguiente párrafo no se aplica en el Reino Unido ni en ningún otro país en el que dichas disposiciones entren en conflicto con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRINGIMIENTO, COMERCIABILIDAD O ADECUACIÓN A UN PROPÓSITO DETERMINADO.

Algunos estados no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable en su caso.

Esta información podría contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. En cualquier momento, IBM puede realizar mejoras y/o cambios en el producto y/o programa descritos en esta publicación sin aviso previo.

Las referencias contenidas en esta información a sitios web no IBM se proporcionan únicamente para su comodidad y de ningún modo constituyen una recomendación de dichos sitios web. El material de esos sitios Web no forma parte del material para este producto IBM, por lo que el uso de esos sitios Web es a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el remitente.

Los propietarios de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluido, en algunos casos, el pago de una tarifa.

IBM suministra el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo, bajo los términos del Acuerdo de cliente de IBM, el Acuerdo internacional de licencias de programas de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos aquí se han determinado en un entorno controlado. Por consiguiente, los resultados obtenidos en otros entornos operativos pueden variar de manera significativa. Pueden haberse realizado algunas mediciones en sistemas en nivel de desarrollo y no existen garantías de que estas mediciones sean las mismas en sistemas disponibles para todos los usuarios. Además, algunas mediciones pueden haberse estimado por extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberán verificar los datos aplicables a su entorno específico.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de estos productos, sus anuncios publicados y otras fuentes

públicamente disponibles. IBM no ha probado dichos productos y no puede confirmar la precisión del rendimiento, compatibilidad u otra clase de afirmaciones relacionadas con los productos que no son de IBM. Las preguntas sobre las posibilidades de los productos no IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Todos los precios de IBM que se muestran son precios de distribuidor recomendados por IBM, corresponden al momento actual y están sujetos a cambios sin aviso previo. Los precios de los distribuidores pueden ser diferentes.

Esta información sólo se proporciona para facilitar la planificación. Dicha información está sujeta a cambios antes de que los productos descritos estén disponibles.

Este manual contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y las direcciones utilizados por una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin abonar ninguna cantidad a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se adecuen a la interfaz de programación de aplicaciones para el sistema operativo para la que se escriben los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por consiguiente, IBM no puede garantizar ni dar por implícito el servicio, la fiabilidad o la función de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantía de ningún tipo. IBM no se responsabilizará de daño alguno derivado del uso de los programas de ejemplo.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros productos y nombres de servicios pueden ser marcas registradas de IBM o de otras compañías. Para obtener una lista actualizada de las marcas registradas de IBM, consulte la sección “Copyright and trademark information” del sitio web www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript y todas las marcas registradas basadas en Adobe son marcas registradas o comerciales de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

IT Infrastructure Library es una marca registrada de la agencia Central Computer and Telecommunications Agency, que forma parte de la Office of Government Commerce británica.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o de sus filiales en Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos o en otros países.

ITIL es una marca registrada y una marca comunitaria de Office of Government Commerce, y está registrada en U.S. Patent and Trademark Office.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java™ y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus subsidiarias.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc. en Estados Unidos y/o en otros países, desde donde se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en Estados Unidos y en otros países.

Avisos legales de NitroDesk Touchdown

Si un cliente elige utilizar IBM Endpoint Manager for Mobile Devices para configurar y gestionar el software de NitroDesk TouchDown, IBM Endpoint Manager for Mobile Devices utilizará las API de NitroDesk TouchDown para comunicarse con el producto NitroDesk TouchDown. Los clientes son los responsables de adquirir de manera independiente el software NitroDesk TouchDown directamente de NitroDesk, Inc.

Las API de NitroDesk TouchDown se utilizan bajo licencia de NitroDesk, Inc. IBM puede actualizar las API de NitroDesk Touchdown cuando sea necesario y queda a su mera disposición. NitroDesk puede cambiar el software o API de NitroDesk Touchdown, de esta manera los cambios podrían provocar que la gestión de NitroDesk TouchDown mediante IBM Endpoint Manager for Mobile Devices deje de funcionar. IBM no tiene la obligación de dar soporte al software o API de NitroDesk TouchDown si estos dejan de funcionar.

Las API de NitroDesk Touchdown y su uso se proporcionan tal cual. SUJETO A CUALQUIER GARANTÍA ESTATUTARIA QUE NO SE PUEDA EXCLUIR, IBM NO OFRECE NINGUNA GARANTÍA NI CONDICIÓN, EXPLÍCITA O IMPLÍCITA, REFERENTE A LAS API O SOPORTE DE NITRODESK, EN EL CASO DE QUE HAYA, INCLUIDAS PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, IDONEIDAD PARA UN FIN DETERMINADO Y TÍTULO Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN.

LA EXCLUSIÓN DE GARANTÍAS EXPLÍCITAS O IMPLÍCITAS PUEDE NO ESTAR PERMITIDA POR ALGUNOS ESTADOS O JURISDICCIONES Y, POR TANTO, PUEDE QUE DICHA EXCLUSIÓN NO SEA APLICABLE AL LICENCIATARIO. EN ESE CASO, DICHAS GARANTÍAS ESTÁN LIMITADAS EN DURACIÓN AL PERIODO MÍNIMO DE GARANTÍA ESTABLECIDO POR LA LEY. NO SE APLICA NINGUNA GARANTÍA DESPUÉS DE DICHO PERIODO. ALGUNOS ESTADOS O JURISDICCIONES NO PERMITEN LIMITACIONES EN CUANTO A LA DURACIÓN DE UNA GARANTÍA IMPLÍCITA, POR LO PUEDE QUE LA LIMITACIÓN ANTERIOR NO SEA APLICABLE AL LICENCIATARIO. EL LICENCIATARIO PUEDE CONTAR CON OTROS DERECHOS QUE VARÍAN SEGÚN EL ESTADO O LA JURISDICCIÓN.