XenMobile Server 10

Apr 15, 2016

Incorporación de aplicaciones

Vista general de las directivas MDX

Acciones automatizadas

Parámetros de cliente en XenMobile

Para crear marcas personalizadas de Worx Store en dispositivos iOS

Para crear opciones de asistencia de Worx Home y GoToAssist

Para agregar, modificar o eliminar propiedades de cliente

Referencia de propiedades del cliente

Parámetros de servidor en XenMobile

ActiveSync Gateway en XenMobile

Credenciales de Google Play

Programa de inscripción de dispositivos iOS

Programa VPP de iOS

Proveedor de servicios móviles

Control de acceso de red

Samsung KNOX

Propiedades de servidor

SysLog

Cómo configurar XenApp y XenDesktop

Asistencia técnica y mantenimiento

Comprobaciones de conectividad

Creación de paquetes de asistencia en XenMobile

Para ver el archivo del registro de depuración

Para configurar parámetros de registro

Cómo ver y analizar archivos de registros en XenMobile

Opciones de la interfaz de línea de comandos en XenMobile

Las API de XenMobile 10

XenMobile Mail Manager 10

Arquitectura

Requisitos del sistema y requisitos previos

Instalación y configuración

Aplicación de directivas de correo electrónico con los ID de ActiveSync

Reglas de control de acceso

Supervisión de dispositivos

Acerca de XenMobile 10

Oct 31, 2016

XenMobile 10 combina los componentes de App Controller y Device Manager de XenMobile 9 y versiones anteriores en una herramienta de administración unificada desde la que usted puede configurar y administrar dispositivos y aplicaciones de usuario.

Nota: El cliente Remote Support no está disponible en las versiones de XenMobile Cloud 10.x para dispositivos Windows CE y Samsung Android.

En la planificación de una implementación de XenMobile hay varios aspectos a tener en cuenta. Para ver recomendaciones, preguntas frecuentes y casos de uso de un entorno XenMobile de extremo a extremo, consulte XenMobile Deployment Handbook.

Novedades

Para ver la lista de problemas corregidos en esta versión, consulte http://support.citrix.com/article/CTX141722. . Para ver la lista de problemas conocidos para XenMobile 10.0, consulte Problemas conocidos.

- **Infraestructura unificada**. La administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM) están unificadas en una sola infraestructura de servidor.
  - Puede implementar XenMobile más rápidamente gracias a que ahora la configuración requiere menos pasos.
  - Puede administrar aplicaciones y dispositivos desde un solo servidor virtual.
- **Nueva consola de XenMobile unificada.**
  - Está diseñado con una interfaz de usuario muy fácil de usar que hace más sencillas tareas administrativas tales como inscribir, implementar, configurar y solucionar problemas en todo el entorno de movilidad.
  - Configuración simplificada de directivas de aplicaciones y dispositivos. Ahora puede configurar una directiva para todas las plataformas de dispositivos disponibles.
- **Integración con NetScaler Gateway desde la misma consola.** Puede administrar comprobaciones de conectividad automatizadas para varios sistemas que formen parte del entorno de movilidad.
- **Respaldo para balizas obsoleto.** Las balizas no reciben respaldo en XenMobile 10, aunque sus opciones siguen apareciendo en la consola de XenMobile. Citrix recomienda conectar con el servidor XenMobile a través de NetScaler Gateway o, si está dentro de su firewall, conectar directamente con el servidor XenMobile.
- **Respaldo mejorado para la autenticación de aplicaciones.** Ayuda a proteger el cifrado entre los dispositivos y la red interna, entre la red interna y el servidor XenMobile, y para las conexiones con la consola de XenMobile.
  - Autenticación adaptativa RSA
  - Respaldo para el cifrado avanzado FIPS 140.2

Introducción a XenMobile 10

Empiece por descargar e instalar la imagen virtual de XenMobile 10.0 Edition en un hipervisor como XenServer, VMware ESXi, o Hyper-V, y complete la configuración inicial de XenMobile en la consola de línea de comandos del hipervisor. Para obtener más información, consulte Requisitos del sistema, Lista de verificación de la instalación e Instalación de XenMobile.

A continuación, abra la consola Web de XenMobile usando la cuenta de administrador que definió durante la configuración inicial.

Para ayudarle a decidir a dónde ir ahora en la consola, consulte Introducción a la consola. El primer conjunto de recomendaciones cubre los parámetros iniciales que puede que haya omitido durante los pasos de instalación.

Descripción de la arquitectura

Oct 31, 2016

Los componentes de XenMobile de la arquitectura de referencia que usted elija para implementar deben basarse en los requisitos de administración de dispositivos o de aplicaciones de su organización. Los componentes de XenMobile son módulos y se construyen unos sobre otros. Por ejemplo, quiere conceder a los usuarios de la organización acceso remoto a las aplicaciones para móvil y necesita realizar un seguimiento de los tipos de dispositivos a los que se conectan los usuarios. En este caso, implementaría XenMobile con NetScaler Gateway. Con XenMobile puede administrar aplicaciones y dispositivos, mientras que NetScaler Gateway permite a los usuarios conectarse a la red.

Implementación de componentes de XenMobile. Puede implementar XenMobile para permitir que los usuarios se conecten a los recursos de la red interna de las siguientes maneras:

- Conexiones a la red interna. Si se trata de usuarios remotos, pueden conectarse mediante una conexión VPN o Micro VPN a través de NetScaler Gateway para acceder a aplicaciones y escritorios de la red interna.
- Inscripción de dispositivos. Los usuarios pueden inscribir dispositivos móviles en XenMobile para que estos se puedan administrar en la consola de XenMobile que se conecta a los recursos de red.
- Aplicaciones Web, SaaS y para móvil. Los usuarios pueden acceder a aplicaciones Web, SaaS y para móvil desde XenMobile mediante Worx Home.
- Escritorios virtuales y aplicaciones basados en Windows. Los usuarios pueden conectarse mediante Citrix Receiver o un explorador Web para acceder a escritorios virtuales y aplicaciones de Windows desde StoreFront o desde la Interfaz Web.

Para conseguir todas o algunas de estas funciones, Citrix recomienda implementar componentes de XenMobile en el siguiente orden:

- NetScaler Gateway. Puede configurar parámetros en NetScaler Gateway para habilitar la comunicación con XenMobile, StoreFront o la Interfaz Web mediante el asistente de configuración rápida. Antes de usar el asistente de configuración rápida en NetScaler Gateway, debe instalar XenMobile, StoreFront o la Interfaz Web para poder establecer la comunicación con él.
- XenMobile. Después de instalar XenMobile, puede configurar las directivas y los parámetros en la consola de XenMobile, lo que permite a los usuarios inscribir sus dispositivos móviles. También puede configurar aplicaciones Web, SaaS y para móvil. Las aplicaciones para móvil pueden incluir aplicaciones procedentes del App Store o de Google Play. Los usuarios también pueden conectarse a aplicaciones para móvil empaquetadas con MDX Toolkit y cargadas en la consola.
- MDX Toolkit. MDX Toolkit puede empaquetar de forma segura tanto una aplicación creada dentro de la organización como una aplicación para móvil creada fuera; por ejemplo, las aplicaciones de Citrix Worx. Después de empaquetar una aplicación, se utiliza la consola de XenMobile para agregarla a XenMobile y cambiar la configuración de directivas según sea necesario. También puede agregar categorías de aplicaciones, aplicar flujos de trabajo e implementar aplicaciones en grupos de entrega.
- StoreFront (optativo). Puede proporcionar acceso a aplicaciones y escritorios virtuales de Windows desde StoreFront a través de conexiones con Receiver.
- ShareFile Enterprise (optativo). Si implementa ShareFile, puede habilitar la integración de directorios de empresa a través de XenMobile, que actúa como un proveedor de identidad SAML (Security Assertion Markup Language). Para obtener más información acerca de la configuración de proveedor de identidades para ShareFile, visite el sitio Web de asistencia técnica de ShareFile.

En las siguientes secciones, se describen las diferentes arquitecturas de referencia para la implementación de XenMobile.

Para obtener más información acerca de los diagramas de arquitectura, consulte las secciones Reference Architecture for On-Premises Deployments y Reference Architecture for Cloud Deployments en "XenMobile Deployment Handbook". Para ver una lista completa de los puertos, consulte Requisitos de puertos para XenMobile.

En un entorno de producción, Citrix recomienda implementar la solución XenMobile en una configuración de clúster. Con ello, se obtiene escalabilidad y redundancia de servidores. Además, aprovechar la funcionalidad de la descarga de SSL de NetScaler puede reducir más la carga del servidor XenMobile y aumentar el rendimiento. Para obtener más información acerca de cómo hacer una instalación en clúster de XenMobile 10.x configurando dos direcciones IP virtuales de equilibrio de carga en NetScaler, consulte Configuración de la agrupación en clúster para XenMobile 10.

Modo de administración de dispositivos móviles (MDM)

XenMobile MDM Edition ofrece administración de dispositivos móviles para iOS, Android, Windows Phone y Amazon (consulte Plataformas de dispositivos respaldadas en XenMobile 10). Puede implementar XenMobile en modo MDM si solo va a utilizar las funcionalidades de MDM de XenMobile. Por ejemplo, puede utilizar el modo MDM cuando necesite administrar dispositivos entregados por la empresa para implementar directivas de dispositivo y aplicaciones y para obtener inventarios de activos y poder llevar a cabo acciones en los propios dispositivos, tales como, borrados selectivos.

En el modelo recomendado, el servidor XenMobile se encuentra en la zona desmilitarizada (DMZ) con un dispositivo NetScaler optativo en primer plano, lo que proporciona protección adicional para XenMobile.

Modo de administración de aplicaciones móviles (MAM)

MAM es compatible con dispositivos iOS y Android, pero no con dispositivos Windows Phone (consulte Plataformas de dispositivos respaldadas en XenMobile 10). Puede implementar XenMobile en modo MAM (también conocido como "modo solo MAM") si solo va a utilizar las funcionalidades de administración de aplicaciones móviles (MAM) de XenMobile, sin que los dispositivos se inscriban para MDM. Por ejemplo, puede utilizar el modo MAM si quiere proteger las aplicaciones y los datos en dispositivos móviles que pertenecen a sus empleados, o quiere entregar aplicaciones móviles de la empresa y poder bloquearlas o borrar sus datos. En este modo, los dispositivos no se pueden inscribir en MDM.

En este modelo de implementación, el servidor XenMobile se coloca con NetScaler Gateway en primer plano, lo que proporciona mayor protección para XenMobile.

Modo MDM+MAM

Con los modos MDM y MAM juntos, se puede llevar a cabo la administración de datos y de aplicaciones móviles, así como la administración de dispositivos móviles para iOS, Android, y Windows Phone (consulte Plataformas de dispositivo respaldadas en XenMobile 10). Puede implementar XenMobile en modo ENT (Enterprise) si va a utilizar las funcionalidades de MDM + MAM de XenMobile. Por ejemplo, elija este modo si quiere administrar dispositivos entregados por la empresa a través de MDM, quiere implementar directivas de dispositivos y aplicaciones, obtener un inventario de activos y poder borrar dispositivos. En este escenario, también quiere entregar aplicaciones móviles de la empresa y poder bloquear aplicaciones y borrar los datos en los dispositivos.

En el modelo de implementación recomendado, el servidor XenMobile se encuentra en la zona desmilitarizada (DMZ) con NetScaler Gateway en primer plano, lo que proporciona protección adicional para XenMobile.

Escalabilidad de XenMobile 10

Oct 31, 2016

Entender la escala que tendrá la infraestructura de XenMobile es vital para decidir cómo implementar y configurar XenMobile. En este artículo, se ofrecen respuestas a preguntas habituales formuladas para determinar los requisitos de las implementaciones empresariales a pequeña y gran escala.

Directrices de rendimiento y escalabilidad

Los datos de este artículo están pensados para guiarle a la hora de determinar el rendimiento y la escalabilidad de la infraestructura de XenMobile. Los dos factores clave para determinar cómo configurar el servidor y la base de datos son el índice de inicios de sesión y la escalabilidad (cantidad máxima de usuarios por dispositivo).

- La escalabilidad es la cantidad máxima de usuarios simultáneos que realizan una carga de trabajo definida. Para obtener más información acerca de los flujos de trabajo utilizados para cargar la infraestructura de XenMobile, consulte Cargas de trabajo.
- El índice de inicios de sesión es la integración de nuevos usuarios y a la autenticación de los usuarios existentes.
  - El índice de integración es la cantidad máxima de dispositivos que se pueden inscribir en el entorno por primera vez. Conocido como Primer uso o FTU (por las siglas en inglés de "First Time Use") en este artículo, este punto de datos es importante cuando se orquesta una estrategia de implementación.
  - El índice de usuarios existentes es la cantidad máxima de usuarios que se autentican en el entorno, que ya están inscritos y conectados a sus dispositivos. Estas pruebas incluían crear sesiones para usuarios ya inscritos y ejecutar aplicaciones WorxMail y WorxWeb.

En la siguiente tabla, se muestran las directrices de escalabilidad según los resultados de las pruebas en el entorno correspondiente de XenMobile.

Tabla 1. XenMobile Enterprise con inscripción

Escalabilidad	Hasta 100,000 dispositivos	
Índices de inicios de sesión	Integración (primer uso)	Un máximo de 2,777 dispositivos por hora
	Usuarios existentes	Un máximo de 16,667 dispositivos por hora
Configuración	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Clúster de 10 nodos del servidor XenMobile
	Base de datos	Base de datos externa de Microsoft SQL Server

Configuración del sistema y resultados de la prueba

En este apartado, se describen la configuración de hardware utilizada y los resultados de las pruebas de escalabilidad para cargas de trabajo de integración (primer uso) y cargas de trabajo de usuarios existentes.

En la siguiente tabla, se definen las recomendaciones de configuración y hardware para XenMobile cuando se amplía de 1000 a 100,000 dispositivos. Estas directrices se basan en los resultados de las pruebas y las cargas de trabajo asociadas. Las recomendaciones representan el margen de error aceptable, tal y como se define en Criterios de salida.

El análisis de los resultados de las pruebas llevó a las siguientes conclusiones:

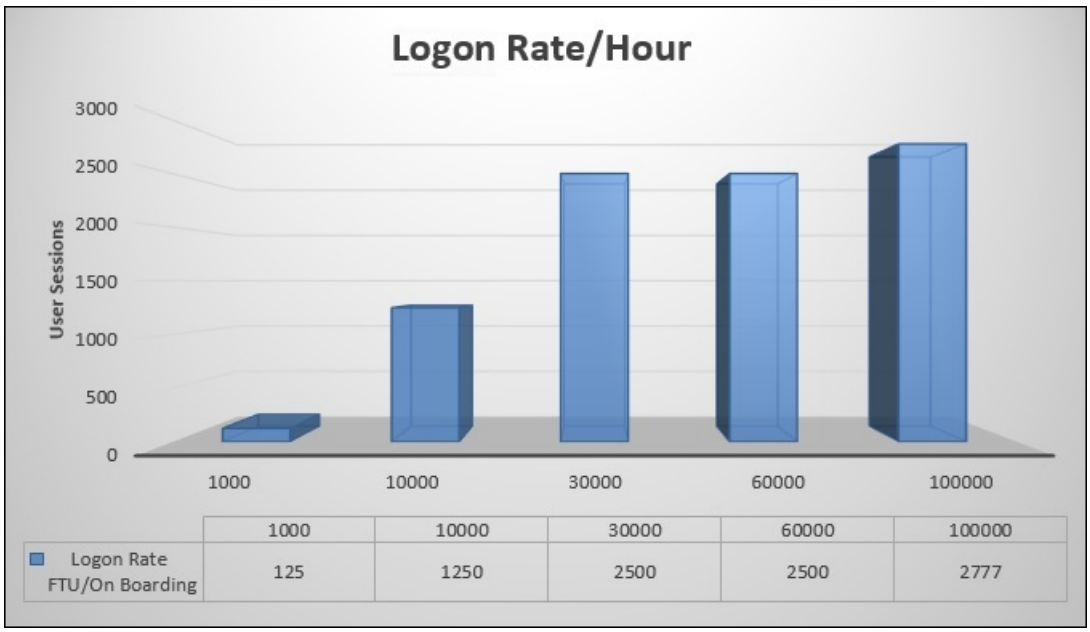
- El índice de inicios de sesión es un factor importante para determinar la escalabilidad de un sistema. Además del inicio de sesión inicial, el índice de inicios de sesión depende de los valores del tiempo de espera de autenticación configurado en el entorno. Por ejemplo, si el tiempo de espera de autenticación se establece en un valor demasiado bajo, los usuarios deben realizar solicitudes más frecuentes de inicio de sesión. Por lo tanto, es necesario comprender las consecuencias que tienen en su entorno los parámetros de tiempo de espera.
- Para las pruebas, se ha utilizado una base de datos externa (SQL Server) con 128 GB de RAM, 300 GB de espacio en disco y 24 CPU virtuales. Esto es lo que se recomienda para entornos de producción.
- Para lograr la máxima escalabilidad, los recursos de CPU y RAM se aumentaron en XenMobile.
- La configuración del clúster de 10 nodos es la configuración validada más grande. Aumentar la escalabilidad de más de 10 nodos requiere una implementación adicional de XenMobile.

Tabla 2. XenMobile Enterprise con resultados de escalabilidad de inscripciones

Cantidad de dispositivos	**1,000**	**10,000**	**30,000**	**60,000**	**100.000**
Índice de inicios de sesión					
Integración (primer uso)	125	1,250	2,500	2,500	2,777
Usuarios existentes	1,000	2,500	7,500	15,000	16,667
Configuración					
Entorno de referencia	VPX-XenMobile en modo autónomo	MPX-XenMobile en modo autónomo	MPX-XenMobile con clústeres (3)	MPX-XenMobile con clústeres (6)	MPX-XenMobile con clústeres (10)
NetScaler Gateway	VPX con 2 GB de RAM 2 CPU virtuales	MPX-10500		MPX-20500	
Modo de XenMobile	Autónomo	Autónomo	Clúster		
Clústeres de XenMobile	N/D	N/D	3	6	10
Dispositivo virtual de	8 GB de RAM y 4 CPU virtuales	8 GB de RAM y 4 CPU virtuales	8 GB de RAM y 4 CPU virtuales	16 GB de RAM y 4 CPU virtuales	16 GB de RAM y 4 CPU virtuales

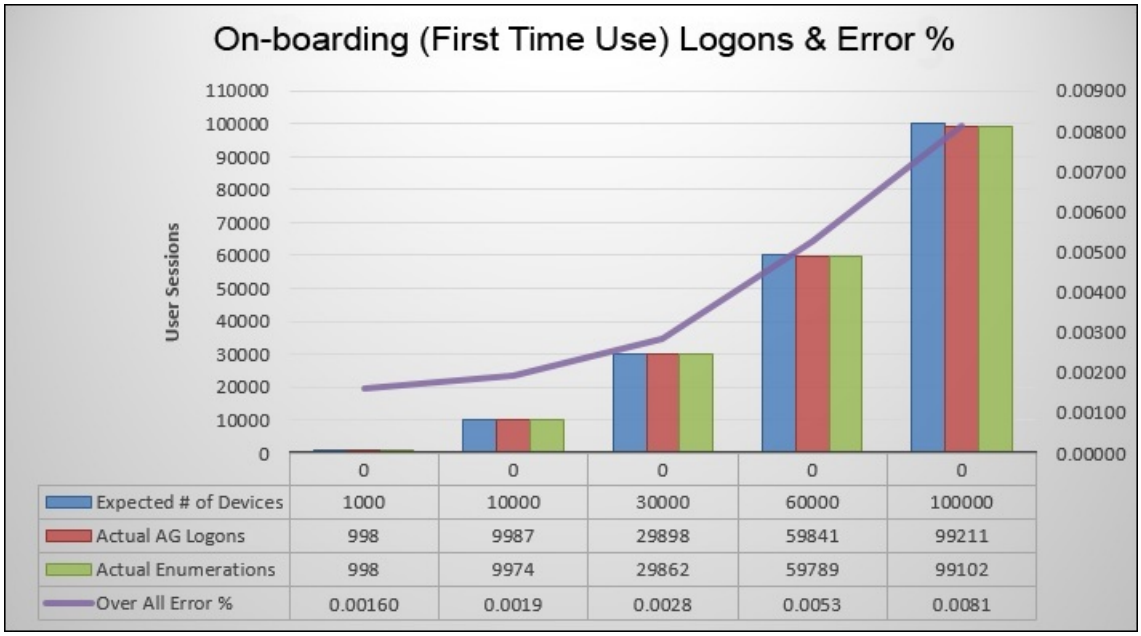
XenMobile					
Base de datos	Externa				

En la tabla anterior, se muestran los índices de inicios de sesión recomendados para usuarios existentes y nuevos. A su vez, esta recomendación se basa en la configuración de XenMobile, el dispositivo NetScaler Gateway, la configuración de clústeres y la base de datos. Puede utilizar los datos de esta tabla para crear una programación óptima de inscripciones de cara a las nuevas implementaciones y a los índices de usuario por dispositivo de las implementaciones existentes. La sección de configuración relaciona, por un lado, los datos de rendimiento en la inscripción y en los inicios de sesión y, por el otro, las recomendaciones del hardware apropiado.



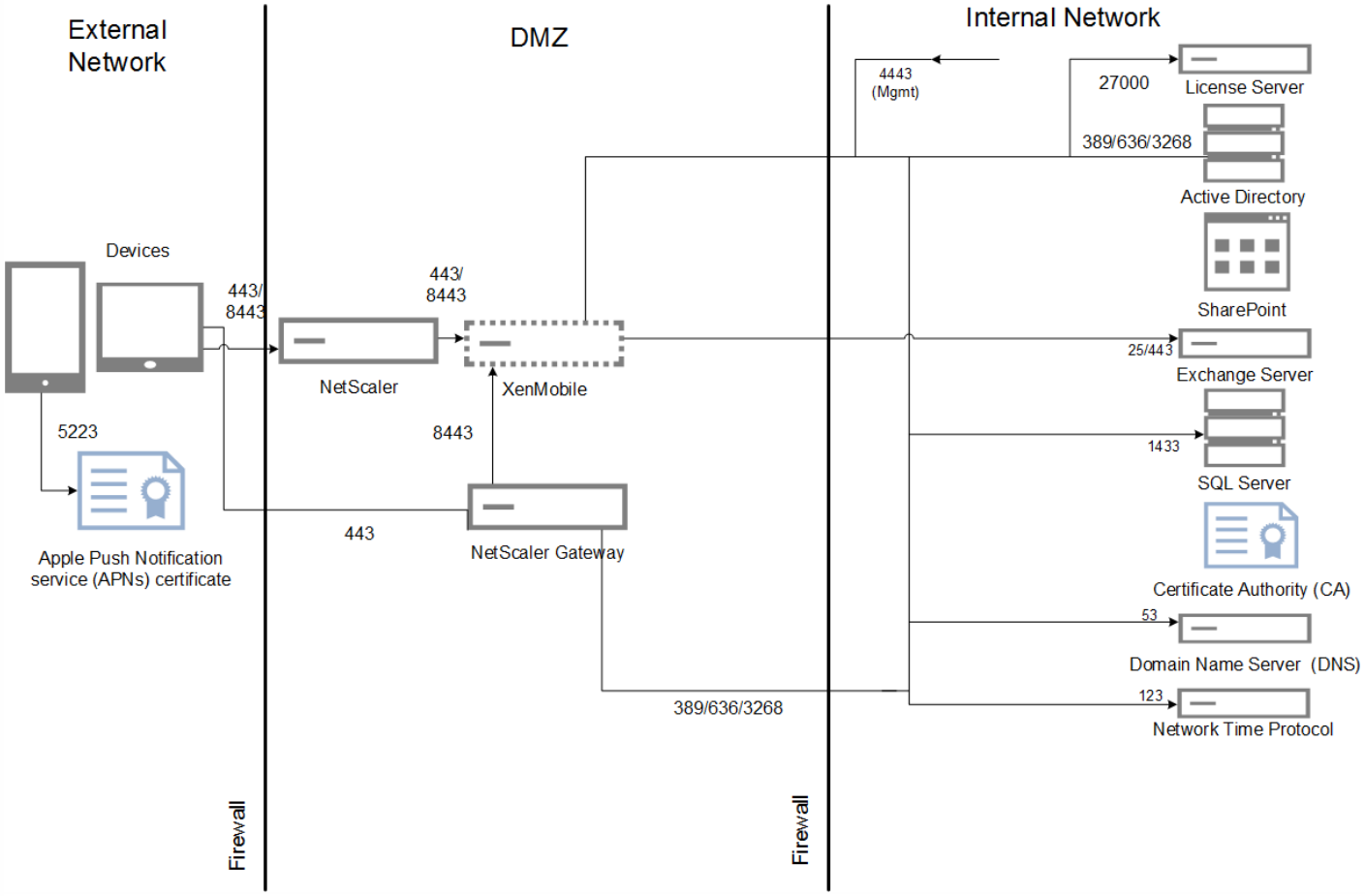
Nota: Experimentará lo siguiente si supera los índices recomendados o las recomendaciones de hardware al determinar el tamaño de su sistema.

- Latencia de inscripción o de inicio de sesión (tiempo de ida y vuelta)
  - Latencia media total: > 1,5 segundos
  - Latencia media de un inicio de sesión de NetScaler Gateway: > 440 milisegundos
  - Latencia media de una solicitud de Worx Store: > 3 segundos
- Se ha observado una degradación del rendimiento físico en los componentes de la infraestructura (por ejemplo, agotamiento de la memoria y la CPU) cuando se han alcanzado los límites de escalabilidad.
  - Respuestas no válidas en dispositivos NetScaler Gateway y XenMobile.
  - Tiempo largo de respuesta por parte de la consola de XenMobile.

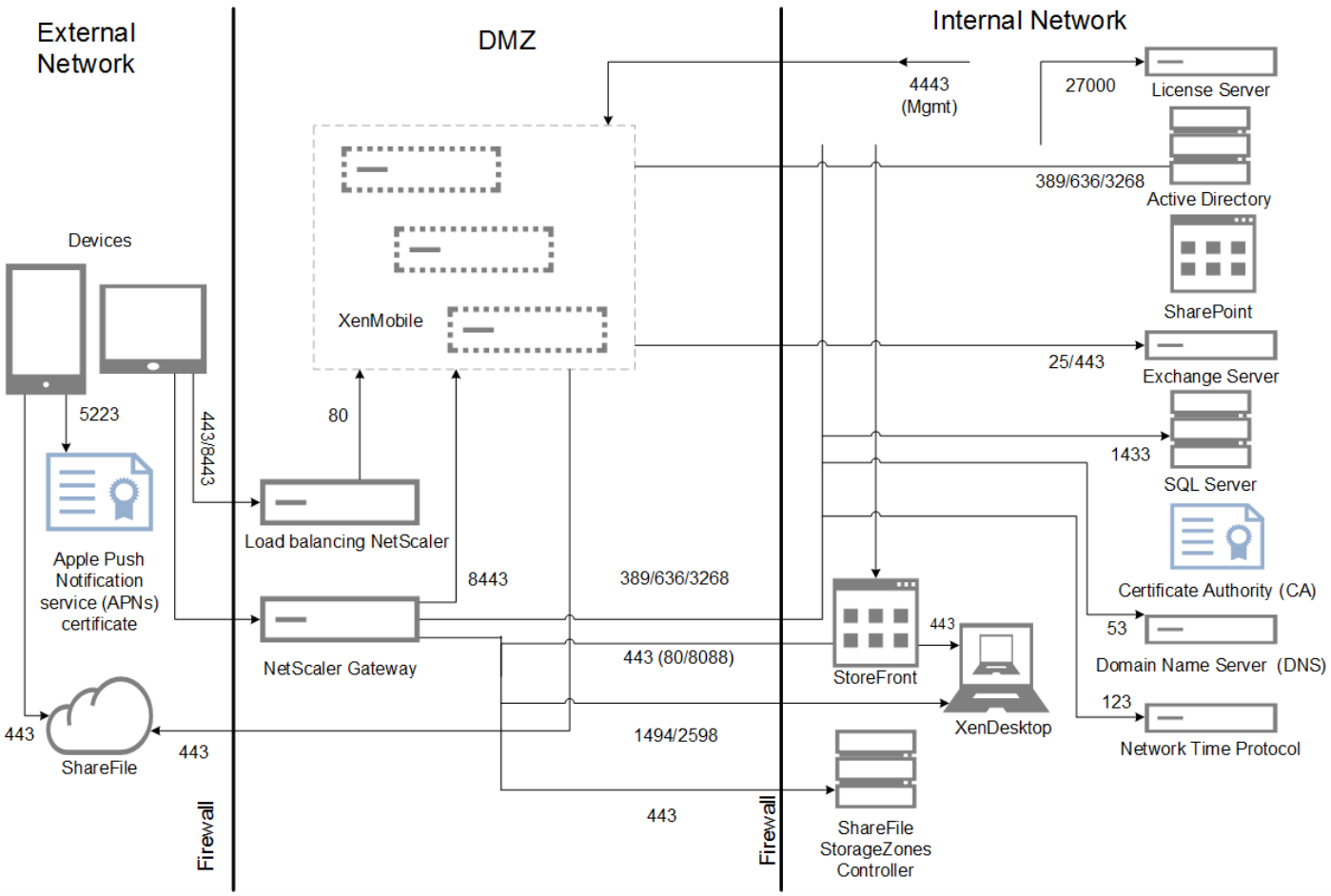


El porcentaje de error mostrado en la imagen anterior incluye errores generales obtenidos en solicitudes correspondientes a todas las operaciones, sin limitarse únicamente a los inicios de sesión. El porcentaje de error se encuentra dentro del límite aceptado para cada prueba realizada, tal y como se define en Criterios de salida.

En la siguiente imagen, se muestra la arquitectura de referencia para una implementación a pequeña escala. Es una arquitectura autónoma que admite un máximo de 10 000 dispositivos.



En la siguiente imagen, se muestra la arquitectura de referencia para una implementación empresarial. Se trata de una arquitectura en clúster con descarga de SSL para MDM a través de HTTP que admite 10 000 dispositivos o más.



Metodología de las pruebas

Las pruebas se realizaron con XenMobile Enterprise para establecer bancos de pruebas. Para ofrecer soluciones a implementaciones de tamaños múltiples, se han utilizado de 1000 a 10 0000 dispositivos en las mediciones.

Las cargas de trabajo se crearon para simular casos de uso reales. Esas cargas de trabajo se realizaron para cada prueba con el fin de examinar el efecto en los índices de inscripciones y de inicios de sesión. El objetivo de esas pruebas era obtener un índice óptimo de inicios de sesión que se encontrara dentro del margen de error aceptado, tal y como se describe en Criterios de salida. Los índices de inicios de sesión son un factor fundamental para determinar las recomendaciones de configuración de hardware para los componentes de la infraestructura.

Las solicitudes de inicio de sesión de integración (primer uso) de las cargas de trabajo incluían la detección automática, la autenticación y operaciones de registro de dispositivos. Las operaciones de suscripción, instalación e inicio de aplicaciones se distribuyeron de forma uniforme a lo largo del período de pruebas. Esto proporcionó la simulación más realista de las acciones de usuario. Al final de la prueba, se cerró la sesión. Las solicitudes de inicio de sesión de usuarios existentes de las cargas de trabajo solo incluían solicitudes de autenticación.

Cargas de trabajo

Las cargas de trabajo de usuario están definidas de la siguiente manera:

Tabla 3. Definiciones de las cargas de trabajo de usuario

Sesiones de usuario por dispositivo	Incluye los inicios de sesión, las enumeraciones y el registro de dispositivos de NetScaler Gateway, entre otros, para cada sesión.
Inicios de Worx Store	Los usuarios pueden iniciar Worx Store varias veces, y cada vez se suscriben a varias aplicaciones o se las instalan, independientemente de si se trata de una aplicación para móviles (Web, SaaS o MDX) o una aplicación Windows (HDX).
Single Sign-On para aplicaciones Web o SaaS por dispositivo	Representa la secuencia de inicio de las aplicaciones Web o SaaS hasta el momento en que XenMobile completa el inicio de sesión Single Sign-On y devuelve la URL real de la aplicación. No se envió ningún tráfico a aplicaciones reales.
Descargas de aplicaciones MDX por dispositivo	Recuentos del número de descargas de aplicaciones MDX (esto puede ocurrir en inicios de Worx Store). Para iOS, esto también incluye la automatización de la instalación de aplicaciones desde Apple ITMS, que utiliza las API nuevas de servicio TMS o de tokens en NetScaler Gateway.

Carga de trabajo de integración (primer uso)

Se conoce como carga de trabajo de integración (primer uso) la primera vez que un usuario accede al entorno de XenMobile. Las operaciones incluidas en esta carga de trabajo son:

- Detección automática
- Inscripción
- Autenticación
- Registro de dispositivos
- Entrega de aplicaciones (aplicaciones Web, SaaS y MDX para móvil)
  - Suscripción a aplicaciones (incluidas las descargas de imágenes e iconos)
  - Instalación de las aplicaciones MDX suscritas
- Inicio de aplicaciones (aplicaciones Web, SaaS y MDX para móvil)
- Conexiones mínimas a WorxMail y WorxWeb (túneles VPN): dos conexiones
- Instalación de las aplicaciones requeridas a través de XenMobile

Los parámetros de carga de trabajo incluyen:

- 1 registro de dispositivos por dispositivo
- 1 enumeración por dispositivo
- 14 aplicaciones enumeradas por dispositivo
- 4 inicios de Worx Store por dispositivo
- 4 inicios de sesión Single Sign-On a aplicaciones Web o SaaS por dispositivo
- 1 aplicación MDX descargada por dispositivo
- 2 descargas de aplicaciones requeridas

Carga de trabajo de los usuarios existentes

En la siguiente tabla, se muestra la carga de trabajo de usuarios existentes. Esta carga de trabajo simulaba un usuario que utiliza las aplicaciones WorxMail y WorxWeb. Esta simulación se utilizó para medir la escalabilidad del puerto de NetScaler

Gateway en la configuración de XenMobile. Para la aplicación WorxWeb, los usuarios accedían a sitios Web internos, que no activan el inicio de sesión Single Sign-On de XenMobile. Las operaciones en este modo son las siguientes:

- Autenticación (NetScaler Gateway y XenMobile)
- Conexiones a WorxMail y WorxWeb (túneles VPN): cuatro conexiones

Perfiles de conexión para WorxApps

En la siguiente tabla, se muestran los parámetros de carga de trabajo necesarios para los usuarios existentes.

Tabla 4. Perfiles de conexión para WorxApps

Conexión del dispositivo	Tipo de conexión	Datos enviados por sesión[1]	Datos recibidos por sesión[1]
WorxMail: Conexión 1	Tipo 1[2]	4,1 MB	4,1 MB
WorxMail: Conexión 2	Tipo 1	6,3 MB	12,5 MB
WorxWeb: Conexión 1	Tipo 2[3]	5,2 MB	15,7 MB
WorxWeb: Conexión 2	Tipo 2	4,1 MB	3,4 MB
Número total de bytes transferidos por sesión[1]		~19,7 MB	~ 40,7 MB

1. **Por sesión**: 8 horas.

2. **Tipo 1**: Envío y recepción asimétricos con conexiones de larga duración (es decir, WorxMail con una conexión de buzón dedicada de Microsoft Exchange).

3. **Tipo 2**: Envío y recepción asimétricos con conexiones que se cierran y se vuelven a abrir tras una demora (es decir, conexiones de WorxWeb).

Nota: Las modificaciones realizadas en los datos de conexión afectan los resultados de los análisis. Por ejemplo, si aumenta la cantidad de conexiones por usuario, la cantidad de sesiones respaldadas de NetScaler Gateway se puede reducir a su vez.

Perfiles de WorxMail y WorxWeb

En las siguientes tablas, se muestran los datos de perfil de WorxMail y WorxWeb.

Tabla 5. Perfil de WorxMail para una carga de trabajo media

Mensajes enviados al día	20
Mensajes recibidos al día	80

Mensajes leídos al día	80
Mensajes eliminados al día	20
Tamaño medio de mensaje (KB)	200

Tabla 6. Perfil de WorxWeb para una carga de trabajo media

Cantidad de aplicaciones Web iniciadas	10
Cantidad de páginas Web abiertas de forma manual	10
Cantidad media de pares de solicitud y respuesta por aplicación Web	100
Tamaño medio de la solicitud (bytes)	300
Tamaño medio de la respuesta (bytes)	1000

Configuración y parámetros

Se utilizaron las siguientes opciones de configuración al realizar las pruebas de escalabilidad:

- NetScaler Gateway y los servidores virtuales de equilibrio de carga (load balancing, LB) coexistieron en el mismo dispositivo NetScaler Gateway.
- Se utilizó una clave de 2048 bits en NetScaler Gateway para las transacciones SSL.

Criterios de salida

Los índices de inicios de sesión son la base de este análisis. Proporcionan la base de los componentes de infraestructura y sus respectivas configuraciones. Es importante saber que los índices de inicios de sesión tienen en cuenta un margen de error que consta de lo siguiente:

- Respuestas no válidas
  - No se considera válida una respuesta con el código de estado 401/404 en lugar de 200.
- Tiempos de espera de las solicitudes
  - Se esperan respuestas en 120 segundos.
- Errores de conexión
  - Se restablece la conexión.

- La conexión finaliza bruscamente.

El índice de inicios de sesión se acepta si el índice general de errores no llega al 1 % del total de solicitudes enviadas desde un dispositivo determinado. El índice de errores incluye los errores de cada operación individual de carga de trabajo, así como el rendimiento físico del componente de la infraestructura (como el agotamiento de la memoria y de la CPU).

Información detallada de software y hardware

En la tabla siguiente, se muestra el software de la infraestructura de XenMobile utilizado para las pruebas.

Tabla 7. Componentes de la infraestructura de XenMobile

Componente	Versión
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0.0.62300
Base de datos externa	Microsoft SQL Server 2008 R2 (128 GB de RAM, 300 GB de espacio en disco, 24 CPU virtuales)

Las pruebas de escalabilidad se realizaron en una plataforma XenServer, tal y como se describe en la siguiente tabla.

Tabla 8. Hardware de XenServer

Proveedor	GenuineIntel
Modelo	Intel Xeon CPU: E5645 @ 2,40 GHz (unidades CPU = 24)

Esto incluye los servicios centrales de la infraestructura. Por ejemplo, el servicio de nombres de dominio (DNS) de Windows, Active Directory, la entidad de certificación, Microsoft Exchange...), así como los componentes de XenMobile (el dispositivo virtual de XenMobile y el dispositivo virtual de NetScaler Gateway VPX, según corresponda).

Para obtener más información sobre el producto, si tiene dudas relacionadas con este artículo o los productos aquí mencionados, consulte Citrix.com. También puede consultar el sitio de la documentación de XenMobile para ver la última documentación del producto, o bien puede ponerse en contacto con su representante de Citrix.

Acerca de XenMobile Cloud

Oct 31, 2016

XenMobile Cloud es un servicio de producto que ofrece un entorno XenMobile de administración de movilidad empresarial (EMM) para administrar aplicaciones y dispositivos así como usuarios o grupos de usuarios. Con XenMobile Cloud, Citrix gestiona la configuración y el mantenimiento de la infraestructura local gracias al equipo de Citrix Cloud Operations. Esta separación permite centrarse exclusivamente en la experiencia de usuario y en la administración de dispositivos, directivas y aplicaciones. Asimismo, XenMobile Cloud elimina la necesidad de adquirir y administrar licencias con cuota de suscripción.

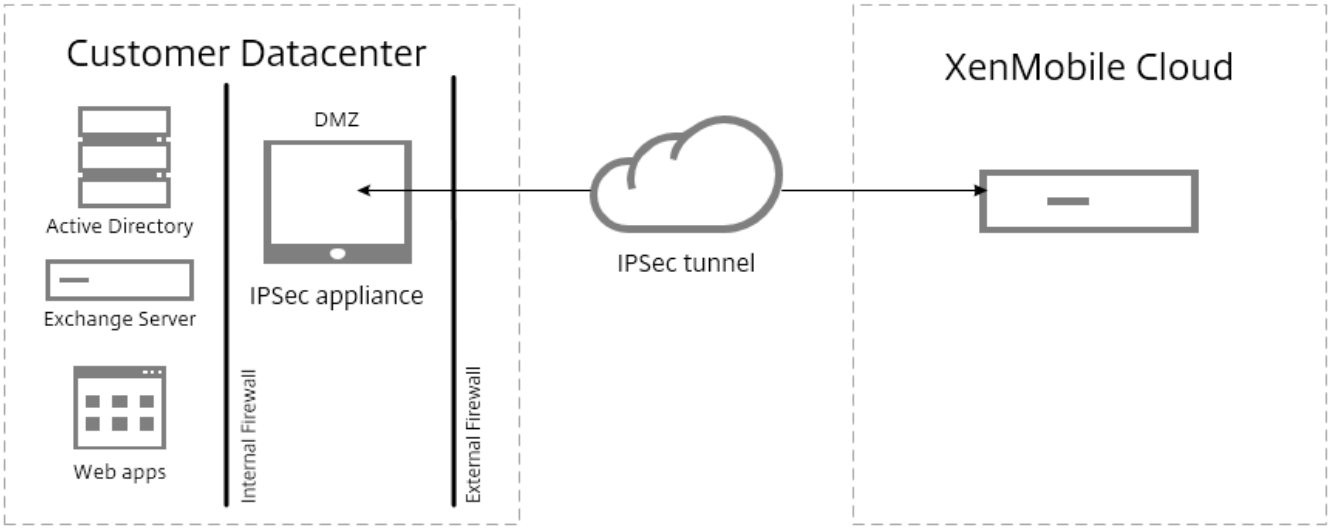
Los administradores de Cloud Operations se encargan del mantenimiento y la configuración de la conectividad de red, así como de la integración de productos Citrix como NetScaler, XenApp, XenDesktop, StoreFront y ShareFile. El entorno de Cloud se aloja en centros de datos de Amazon ubicados en todo el mundo para entregar un rendimiento eficaz, respuestas rápidas y un servicio de asistencia.

Para obtener más información sobre XenMobile Cloud, vaya a https://www.citrix.com/products/xenmobile/tech-info/cloud.html

Nota

- El cliente Remote Support no está disponible en las versiones de XenMobile Cloud 10.x para dispositivos Windows CE y Samsung Android.
- Los componentes del lado del servidor de XenMobile Cloud no cumplen el estándar FIPS 140-2.
- Citrix no respalda la integración de syslog en XenMobile Cloud con un servidor syslog ubicado en las instalaciones locales de la empresa. En su lugar, puede descargar los registros de la página Support de la consola de XenMobile. Al hacerlo, debe hacer clic en Descargar todo para poder obtener los registros del sistema. Para obtener información detallada, consulte Cómo ver y analizar archivos de registros en XenMobile.

La arquitectura básica de XenMobile Cloud se muestra en la siguiente imagen. Para ver diagramas de referencia de arquitectura en detalle, consulte la la sección "Reference Architecture for On-Premises Deployments" de la guía XenMobile Deployment Handbook.



Puede integrar la arquitectura de XenMobile Cloud en su infraestructura existente. Para ello, deberá instalar e implementar Citrix CloudBridge, o bien utilizar una puerta de enlace IPsec existente en su centro de datos.

Esta arquitectura permite beneficiarse del uso de NetScaler, ya sea en la nube, gestionado por el equipo de Cloud Operations o en su centro de datos. Cuando se usa en el centro de datos, NetScaler ofrece un único punto de administración para controlar el acceso y limitar las acciones que se pueden llevar a cabo en las sesiones en función de la identidad del usuario y el dispositivo de punto final. Esta implementación ofrece una mejor seguridad de aplicaciones, protección de datos y administración del cumplimiento normativo.

Para descargar e instalar Citrix CloudBridge, vaya a https://www.citrix.com/downloads/cloudbridge.html

Roles en XenMobile Cloud

XenMobile Cloud utiliza el mismo control de acceso basado en roles (RBAC) que una implementación local de XenMobile. La diferencia con XenMobile Cloud es que el equipo de Citrix Cloud Operations gestiona todos los roles, incluido el aprovisionamiento, relativos a la infraestructura.

En la siguiente imagen, se muestra la consola de RBAC para XenMobile Cloud.

XenMobile implementa cuatro roles de usuario predeterminados para separar de manera lógica el acceso a las funciones del sistema. Los roles predeterminados son los siguientes:

- **Administrator**. Concede acceso completo al sistema.
- **Support**. Concede acceso para la asistencia remota.
- **User**. Concede acceso a los usuarios para inscribir dispositivos y usar el portal Self Help Portal.
- **Provisioning**. Mediante la herramienta de aprovisionamiento de dispositivos, los administradores utilizan este rol para aprovisionar todos los dispositivos Windows Mobile o Windows CE como si se tratara de un grupo. El equipo de Cloud Operation gestiona este rol.

Asimismo, puede utilizar los roles predeterminados como plantillas para crear nuevos roles de usuario con permisos para acceder a funciones específicas del sistema, además de las funciones definidas para esos roles predeterminados.

Los roles se pueden asignar a usuarios locales (a nivel de usuario) o a grupos de Active Directory (todos los usuarios de ese grupo tendrán los mismos permisos). Si un usuario pertenece a varios grupos de Active Directory, todos los permisos se combinan entre sí para definir los permisos de ese usuario concreto. Por ejemplo: si los usuarios del grupo ADGroupA pueden ubicar los dispositivos de los administradores, y los usuarios del grupo ADGroupB pueden borrar los dispositivos de los empleados, entonces un usuario que pertenezca a ambos grupos podrá ubicar y borrar dispositivos de administradores y de empleados.

Nota: Los usuarios locales solo pueden tener un rol asignado.

En XenMobile, puede usar la función de control de acceso basado en roles (RBAC) para realizar las siguientes acciones:

- Crear un nuevo rol.
- Agregar grupos a un rol.
- Asociar usuarios locales a roles.

A continuación, se presentan los roles que se pueden asignar. El equipo de Citrix Cloud Operations gestiona los roles no incluidos en la lista.

Sección principal	Sección	Página	Página visible para
Panel de mandos	Todo	Todo	Administrador de TI
Administración	Dispositivos	Todo	Administrador de TI
Administración	Inscripción	Todo	Administrador de TI
Configuración	Directivas de dispositivo	Todo	Administrador de TI
Configuración	Apps	Todo	Administrador de TI
Configuración	Actions	Todo	Administrador de TI

Configuración	Delivery Groups	Todo	Administrador de TI
Configuración	Configuración	Certificados	Administrador de TI y Administrador de Cloud
Configuración	Configuración	Plantillas de notificaciones	Administrador de TI
Configuración	Configuración	Role Based Access Control	Administrador de TI y Administrador de Cloud
Configuración	Configuración	Inscripción	Administrador de TI
Configuración	Configuración	Grupos y usuarios locales	Administrador de TI y Administrador de Cloud
Configuración	Configuración	Administración de versiones	Administrador de TI y Administrador de Cloud
Configuración	Configuración	Flujos de trabajo	Administrador de TI
Configuración	Configuración	Proveedores de credenciales	Administrador de TI
Configuración	Configuración	Entidades de infraestructura PKI	Administrador de TI
Configuración	Configuración	Propiedades de cliente	Administrador de TI
Configuración	Configuración	NetScaler Gateway	Solo administrador de Cloud O solo administrador de TI
Configuración	Configuración	Puerta de enlace SMS de operador	Administrador de TI
Configuración	Configuración	Servidor de notificaciones	Administrador de TI y Administrador de Cloud
Configuración	Configuración	ActiveSync Gateway	Administrador de TI
Configuración	Configuración	Programa VPP de iOS	Administrador de TI
			Administrador de Cloud,

Asistencia técnica	Log Operations	Parámetros de registro	administrador de TI y equipo de asistencia técnica
Configuración	Configuración	Propiedades de servidor	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
Configuración	Configuración	Credenciales de Google Play	Administrador de TI
Configuración	Configuración	LDAP	Administrador de TI
Configuración	Configuración	Control de acceso de red	Administrador de TI
Asistencia técnica	Support Bundle	Crear paquetes de asistencia	Administrador de Cloud y equipo de asistencia técnica
Configuración	Configuración	iOS Device Enrollment Program	Administrador de TI
Configuración	Configuración	Proveedor de servicios móviles	Administrador de TI
Configuración	Configuración	Samsung KNOX	Administrador de TI
Configuración	Configuración	XenApp o XenDesktop	Administrador de TI
Configuración	Configuración	ShareFile	Administrador de TI
Asistencia técnica	Avanzado	Información de clústeres	Administrador de Cloud y equipo de asistencia técnica
Asistencia técnica	Avanzado	Recolección de elementos no utilizados	Administrador de Cloud y equipo de asistencia técnica
Asistencia técnica	Avanzado	Propiedades de memoria de Java	Administrador de Cloud y equipo de asistencia técnica
Asistencia técnica	Avanzado	Macros	Administrador de TI
FTU Wizard	Initial Configuration	NetScaler Gateway	Solo administrador de Cloud O solo administrador de TI

Configuración	Configuración	Worx Home Support	Administrador de TI
Configuración	Configuración	Worx Store Branding	Administrador de TI
Asistencia técnica	Diagnóstico	Comprobaciones de conectividad de NetScaler Gateway	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
Asistencia técnica	Diagnóstico	Comprobaciones de conectividad de XenMobile	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
Asistencia técnica	Log Operations	Registros	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
Asistencia técnica	Avanzado	Configuración de PKI	Administrador de TI y Administrador de Cloud
Asistencia técnica	Herramientas	Utilidad de firma APNS	Asistencia al cliente y asistencia técnica
Asistencia técnica	Herramientas	Citrix Insight Services	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
FTU Wizard	Initial Configuration	Certificado SSL	Administrador de TI y Administrador de Cloud
FTU Wizard	Initial Configuration	Configuración de LDAP	Administrador de TI
FTU Wizard	Initial Configuration	Servidor de notificaciones	Administrador de TI y Administrador de Cloud
FTU Wizard	Initial Configuration	Summary	Administrador de TI y Administrador de Cloud
Asistencia técnica	Enlaces	Citrix Knowledge Center	Administrador de Cloud, administrador de TI y equipo de asistencia técnica
		Estado de un dispositivo para	

Asistencia técnica	Herramientas	NetScaler Connector	Administrador de TI
Asistencia técnica	Log Operations	Configuración de registro -> Tamaño de registro	Administrador de Cloud y equipo de asistencia técnica

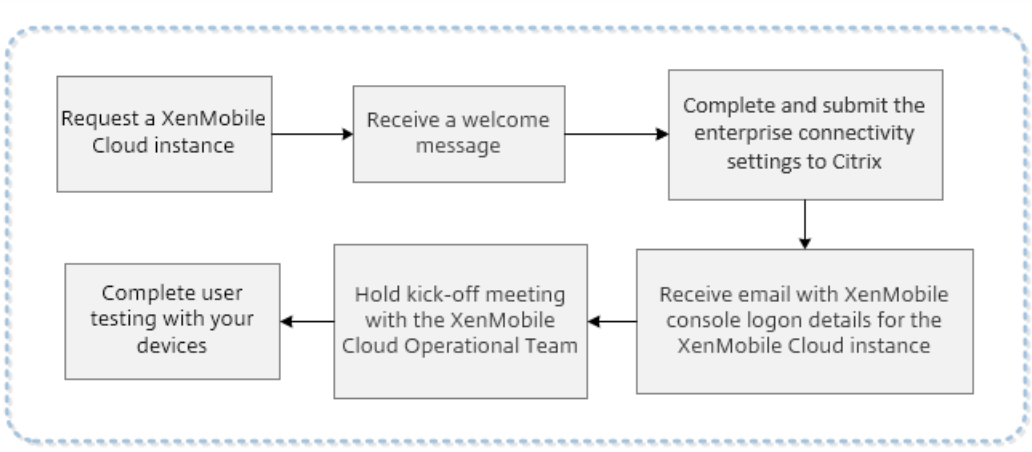
Para obtener instrucciones paso a paso acerca de la personalización de roles, consulte Configuración de roles con RBAC.

Para solicitar el reinicio de los nodos de servidor, póngase en contacto con el servicio de asistencia técnica en https://www.citrix.com/contact/technical-support.html.

Requisitos previos y administración de XenMobile Cloud

May 05, 2016

La siguiente ilustración muestra los pasos que conforman el proceso desde el momento en que se realiza una solicitud de una instancia de XenMobile Cloud hasta la prueba de usuario con los dispositivos de la organización. Al evaluar o adquirir XenMobile Cloud, el equipo de operaciones de XenMobile Cloud ofrece ayuda y comunicación continuas durante todo el proceso de incorporación, para asegurarse de que los servicios principales de XenMobile Cloud se ejecutan y se han configurado correctamente.



Citrix aloja y entrega la solución de XenMobile Cloud. No obstante, existen algunos requisitos de puertos y comunicaciones para conectar la infraestructura de XenMobile Cloud con los servicios de su empresa, tales como Active Directory. Consulte las secciones siguientes para preparar la implementación de XenMobile Cloud.

Puertas de enlace de túnel IPSec de XenMobile Cloud

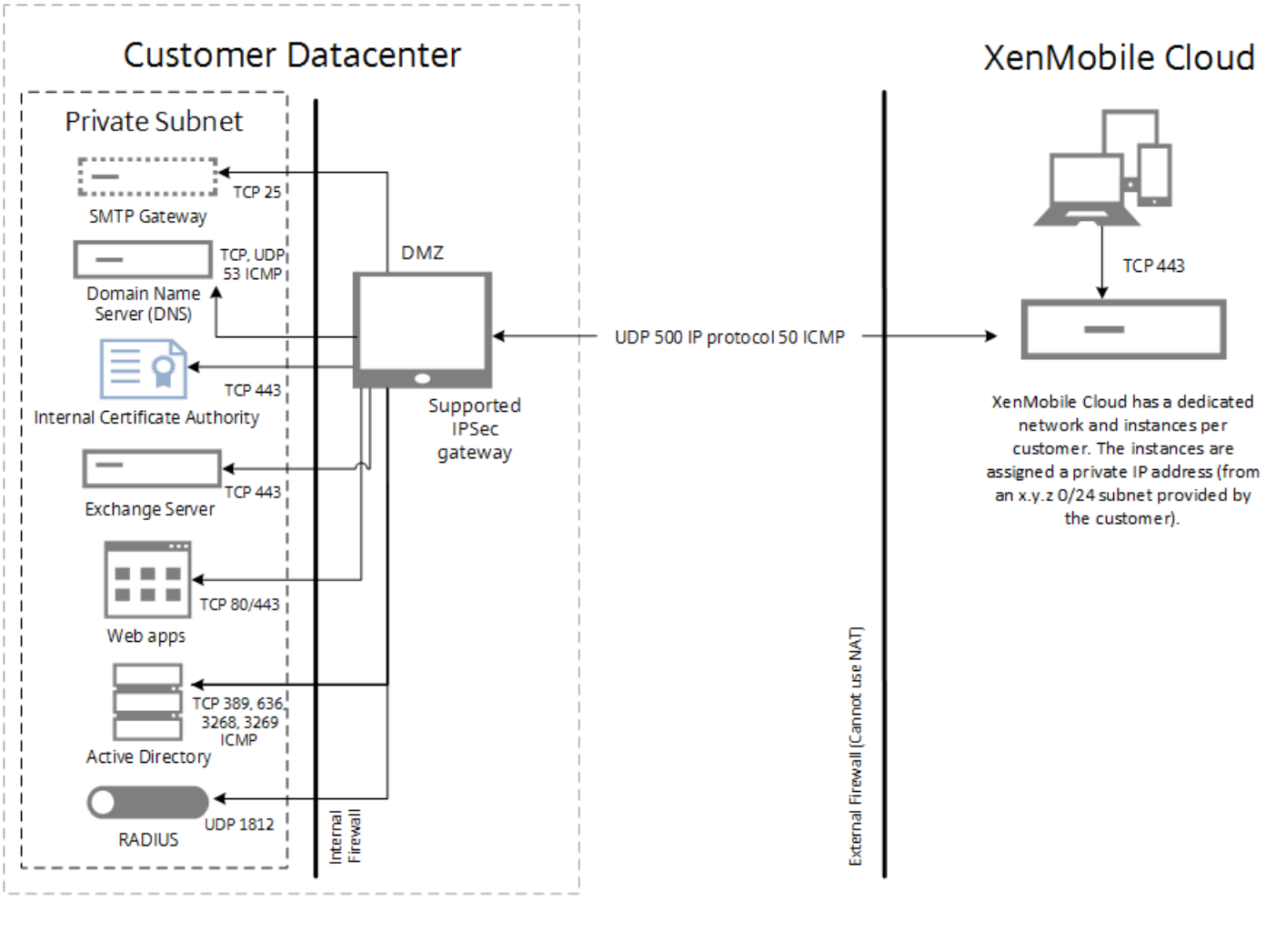
Puede usar un conector de XenMobile Enterprise, un túnel IPsec para conectar la infraestructura XenMobile Cloud con los servicios de la empresa, tales como Active Directory.

Las puertas de enlace IPsec enumeradas en este sitio Web de Amazon Web Services han sido probadas oficialmente y reciben respaldo en la solución de XenMobile Cloud: http://aws.amazon.com/vpc/faqs/. Consulte la sección "P. ¿Qué dispositivos de puerta de enlace de cliente funcionan con Amazon VPC?" para ver la lista de puertas de enlace.

> ## Nota
>
> Si su puerta de enlace IPsec no figura en la lista aprobada, es posible que funcione de todos modos con XenMobile Cloud, pero puede tardar más en configurarse. Asimismo, puede que sea necesario usar una de las puertas de enlace IPSec respaldadas oficialmente como plan de reserva.

Su puerta de enlace IPsec debe tener una dirección IP pública asignada directamente a ella y dicha dirección no puede usar la traducción de direcciones de red (NAT).

La siguiente ilustración muestra cómo se configura el túnel IPsec en XenMobile Cloud para conectarse a los servicios de la empresa a través de distintos puertos.



La siguiente tabla muestra los requisitos de comunicaciones y puertos para una implementación de XenMobile Cloud, incluidos los requisitos de túnel IPsec.

Origen	Destino	Protocolos	Puerto	Descripción
Firewall externo (perimetral): Reglas de entrada				
Direcciones IP públicas de VPN IPCSEC de XenMobile Cloud (AWS) [1]	Dispositivo IPSec del cliente	UPD	500	Configuración IKE de IPSec
Direcciones IP	Dispositivo IPSec del	ID de protocolo	50	Protocolo ESP de IPSec.

públicas de VPN IPCSEC de XenMobile Cloud (AWS) [1]	cliente	IP		
Direcciones IP públicas de VPN IPCSEC de XenMobile Cloud (AWS) [1]	Dispositivo IPSec del cliente	ICMP		Para la solución de problemas (puede quitarse después de la instalación).
Firewall externo (perimetral): Reglas de salida				
Subred DMZ del cliente	Direcciones IP públicas de VPN IPSec de XenMobile Cloud (AWS) [1]	UDP	500	Configuración IKE de IPSec
Subred DMZ del cliente	Direcciones IP públicas de VPN IPSec de XenMobile Cloud (AWS) [1]	ID de protocolo IP	50, 51	Protocolo ESP de IPSec.
Subred DMZ del cliente	Direcciones IP públicas de VPN IPSec de XenMobile Cloud (AWS) [1]	ICMP		Para la solución de problemas (puede quitarse después de la instalación).
Firewall interno: Reglas de entrada				
Subred /24 de cliente, no utilizada y enrutable [2]	Servidores DNS internos en el centro de datos del cliente	TCP, UPP, ICMP	53	Resolución DNS.
Subred /24 de cliente, no utilizada y enrutable [2]	Controladores de dominio de Active Directory en el centro de datos del cliente	LDAP(TCP)	389, 636 3268, 3269	Para la autenticación de usuarios en Active Directory y consultas de directorio a los controladores de dominio.
Subred /24 de cliente, no utilizada y enrutable [2]	Controladores de dominio de Active Directory en el centro de datos del	ICMP		Para la solución de problemas (puede quitarse después de completarse la instalación entera).

	cliente			
Subred /24 de cliente, no utilizada y enrutable [2]	Servidores Exchange Server en el centro de datos del cliente	SMTP (TCP)	25	Optativo: Para las notificaciones de XenMobile por correo electrónico.
Subred /24 de cliente, no utilizada y enrutable [2]	Servidores Exchange Server en el centro de datos del cliente	HTTP, HTTPS (TCP)	80, 443	Exchange ActiveSync, que es necesario si se envía tráfico de ActiveSync desde el dispositivo a la infraestructura de XenMobile Cloud (a través de un túnel IPsec) hacia los servidores Exchange Server. Esto NO es necesario si el dispositivo del usuario se comunicará con un nombre FQDN público de ActiveSync a través de Internet, sin necesidad de viajar a través del túnel IPsec de XenMobile hacia los servidores de Exchange.
Subred /24 de cliente, no utilizada y enrutable [2]	Servidores de aplicaciones, como servidores Web/de intranet, servidores SharePoint, etcétera.	HTTP, HTTPS (TCP)	80, 443	Acceso a servidores de intranet y de aplicaciones desde dispositivos móviles de usuario a través del túnel IPsec de XenMobile. Cada servidor de aplicaciones se debe agregar a las reglas de firewall con el número de puerto necesario para acceder a la aplicación (normalmente los puertos 80 y/o 443).
Subred /24 de cliente, no utilizada y enrutable [2]	Servidor PKI (si se usa una PKI local)	HTTPS (TCP)	443	Optativo (no utilizado para pruebas de concepto de XenMobile): Esto se puede aprovechar para establecer una integración entre la infraestructura de XenMobile Cloud y una infraestructura PKI local (tal como Microsoft CA) para establecer la autenticación basada en certificados dentro de la solución XenMobile.
Subred /24 de cliente,	Servidor RADIUS	UDP	1812	Optativo (no utilizado para pruebas

no utilizada y enrutable [2]				de concepto de XenMobile): Se puede usar para establecer la autenticación de dos factores en la solución XenMobile.
Firewall interno: Reglas de salida				
Subredes internas de cliente, desde donde tiene que estar disponible la consola de XenMobile	Subred /24 de cliente, no utilizada y enrutable [2]	TCP	4443	Consola XenMobile App Controller (MAM) en la infraestructura de XenMobile Cloud.

[1] Serán suministradas por el equipo de XenMobile Cloud cuando la instancia de XenMobile Cloud y los componentes de IPSec sean aprovisionados en la infraestructura de XenMobile Cloud.

[2] Una subred /24 sin utilizar, suministrada por el cliente como parte del proceso de aprovisionamiento, que no cree conflicto con subredes internas en el centro de datos del cliente, y que se pueda enrutar.

Si planea implementar XenMobile Mail Manager o XenMobile NetScaler Connector para el filtrado de correo electrónico nativo (por ejemplo, la posibilidad de bloquear o permitir la conectividad de correo desde los clientes de correo nativos en los dispositivos móviles de los usuarios), consulte los requisitos adicionales siguientes.

Certificado APNs de Apple de XenMobile

Si va a administrar dispositivos iOS con la implementación de XenMobile Cloud, necesitará un certificado APNs de Apple. Debe preparar el certificado antes de implementar la solución XenMobile Cloud. Para obtener más información, consulte Solicitud de un certificado APNs.

Certificado para notificaciones push de WorxMail para iOS

Si quiere usar notificaciones push en la implementación de WorxMail, debe preparar un certificado APNS de Apple para las notificaciones push de WorxMail para iOS. Para obtener información detallada, consulte Notificaciones push para WorxMail para iOS.

XenMobile MDX Toolkit

El MDX Toolkit es una tecnología de empaquetado de aplicaciones que prepara las aplicaciones para una implementación segura con XenMobile. Si quiere empaquetar aplicaciones, tales como Citrix WorxMail, WorxNotes, QuickEdit, etcétera, necesitará instalar el MDX Toolkit. Para obtener más información, consulte Acerca de MDX Toolkit.

Si va a empaquetar aplicaciones de iOS, necesitará una cuenta de desarrollador de Apple (Apple Developer) para crear los perfiles de distribución de Apple necesarios. Para obtener información detallada, consulte los Requisitos del sistema para el MDX Toolkit y el sitio Web de Apple Developer.

Si va a empaquetar aplicaciones para dispositivos Windows Phone 8.1, consulte los Requisitos del sistema.

Detección automática de XenMobile para la inscripción de Windows Phone

Si quiere utilizar la detección automática de XenMobile para la inscripción de dispositivos Windows Phone 8.1, asegúrese de que tiene un certificado SSL público disponible. Para obtener más información, consulte Para habilitar la detección automática en XenMobile para la inscripción de usuarios

La consola de XenMobile

La solución XenMobile Cloud utiliza la misma consola Web que una implementación local de XenMobile. De este modo, las tareas de administración diarias como la administración de directivas, aplicaciones y dispositivos, etcétera, en la nube, se realiza de manera muy parecida a cómo se hace en una implementación local de XenMobile. Para obtener información acerca de la administración de dispositivos y aplicaciones en la consola de XenMobile, consulte Introducción a la consola de XenMobile.

Inscripción de dispositivos en XenMobile

Para obtener información acerca de las opciones de inscripción de XenMobile para las distintas plataformas de dispositivos, consulte Inscripción de usuarios y dispositivos.

Asistencia para XenMobile

Para obtener más información sobre cómo obtener acceso a información relacionada y herramientas compatibles en la consola de XenMobile, consulte Mantenimiento y asistencia de XenMobile.

Respaldo de plataformas móviles en XenMobile Cloud

May 05, 2016

Después de solicitar una instancia de XenMobile Cloud, si quiere puede empezar a preparar el respaldo para plataformas Android, iOS y Windows. A medida que completa los pasos aplicables a su entorno, tenga esa información a mano para poder usarla al configurar parámetros en la consola de XenMobile.

Tenga en cuenta que estos requisitos son solo un subconjunto de todos los requisitos de puertos y comunicaciones que componen el proceso de incorporación de XenMobile Cloud. Para obtener más información, consulte Requisitos previos y administración de XenMobile Cloud.

Android

- Cree credenciales de Google Play. Para obtener más información, consulte Getting Started with Publishing en Google Play.
- Cree una cuenta de administrador de Android for Work. Para obtener más información, consulte Administración de dispositivos con Android for Work en XenMobile
- Verifique su nombre de dominio con Google. Para obtener más información, consulte Verify your domain for Google Apps
- Habilite las API y cree una cuenta de servicio para Android for Work. Para obtener más información, consulte Google for Work Android.

iOS

- Cree un ID de Apple y una cuenta de desarrollador. Para obtener más información, consulte el sitio Web de Apple Developer Program.
- Cree un certificado APNs (Apple Push Notification service) Para obtener más información, vaya a Apple Push Certificates Portal.
- Cree un token de empresa del programa de compras por volumen (VPP). Para obtener más información, consulte Apple Volume Purchasing Program.

Windows

- Cree una cuenta de desarrollador para la Tienda Windows de Microsoft. Para obtener más información, consulte Microsoft Windows Dev Center.
- Obtenga un ID de publicador para la Tienda Windows de Microsoft. Para obtener más información, consulte Microsoft Windows Dev Center.
- Adquiera un certificado de empresa de Symantec. Para obtener más información, consulte Microsoft Windows Dev Center.
- Cree un token de inscripción de la aplicación (AET). Para obtener más información, consulte Microsoft Windows Dev Center.

Requisitos del sistema

Oct 31, 2016

Para ejecutar XenMobile 10, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.2.x, 6.1.x o 6.0.x); para obtener más información, consulte XenServer
  - VMware (versiones compatibles: ESXi 5.5, ESXi 5.1, ESXi 4.1). Para obtener información más detallada, consulte VMware.
  - Hyper-V (versiones compatibles: Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2). Para obtener información más detallada, consulte Hyper-V.
- Procesador de doble núcleo
- Dos CPU virtuales
- 8 GB de RAM
- 50 GB de espacio en disco

La configuración recomendada para 10 000 dispositivos es la siguiente:

- Procesador de núcleo cuádruple
- 8 GB de RAM

Requisitos del sistema para NetScaler Gateway

Para ejecutar NetScaler Gateway con XenMobile 10, debe cumplir los siguientes requisitos mínimos:

- XenServer, VMware o Hyper-V
- Dos CPU virtuales
- 2 GB de RAM
- 20 GB de espacio en disco

También debe poder comunicarse con Active Directory, que requiere una cuenta de servicio. Solamente necesita acceso de lectura y consulta.

Requisitos de base de datos para XenMobile 10

El repositorio de XenMobile requiere una base de datos de Microsoft SQL Server que se ejecute en una de las siguientes versiones compatibles:

- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Citrix XenMobile respalda el grupo de disponibilidad de SQL Always On y SQL Clustering para una alta disponibilidad de las bases de datos. Citrix no respalda las bases de datos reflejadas para alta disponibilidad de bases de datos en XenMobile. Sí que se respalda la alta disponibilidad de bases de datos con el modo Active/Active o Active Passive con la implementación de MS SQL Cluster.

Nota: Si la base de datos está desconectada, el servidor XenMobile no dará servicio a conexiones desde dispositivos, ya que el servidor XenMobile también estará desconectado.

Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile y se debe utilizar de forma local o remota solo en entornos de prueba.

Nota: Compruebe que la cuenta de servicio de SQL Server que se va a usar en XenMobile tiene el permiso del rol DBcreator. Para obtener más información acerca de las cuentas de servicio de SQL Server, consulte las siguientes páginas del sitio de Microsoft Developer Network (estos enlaces hacen referencia a información acerca de SQL Server 2014; si su servidor es de otra versión, selecciónela en la lista "Otras versiones"):

- Configuración del servidor: cuentas de servicio
- Configurar los permisos y las cuentas de servicio de Windows
- Roles de nivel de servidor

Compatibilidad de XenMobile

Oct 31, 2016

> **Important**
>
> A partir de la versión 10.4, las aplicaciones móviles Worx pasan a llamarse aplicaciones XenMobile. La mayoría de las aplicaciones XenMobile también cambian de nombre, aunque no todas. Para obtener más información, consulte Acerca de aplicaciones XenMobile.

En este artículo, se ofrece un resumen de las versiones de los componentes de XenMobile respaldados que pueden integrarse, incluido NetScaler Gateway y la versión de MDX Toolkit necesaria para empaquetar, configurar y distribuir aplicaciones móviles Worx o XenMobile.

XenMobile 10.x

Versiones de NetScaler Gateway respaldadas:

- 11.1.x
- 11.0.x
- 10.5.x

Citrix respalda la versión actual de XenMobile y las dos anteriores. Por ejemplo, si la versión actual es XenMobile 10.4, Citrix también respalda XenMobile 10.3.6 (un Service Pack más que una versión completa) y XenMobile 10.3.5.

Los componentes de cliente de XenMobile cumplen los siguientes requisitos de compatibilidad:

- Las versiones más recientes de Secure Hub y del MDX Toolkit son compatibles con la versión más reciente del servidor XenMobile y con las dos versiones anteriores a esa.
- La versión más reciente de Secure Hub y la anterior son compatibles con las versiones más recientes de MDX Toolkit y las aplicaciones XenMobile.
- La versión más reciente de una de las aplicaciones XenMobile se ha probado con la versión más reciente de MDX Toolkit.

Para sacar partido a las ventajas que ofrecen las nuevas características, soluciones y actualizaciones de directivas, Citrix recomienda instalar la versión más reciente de MDX Toolkit, Secure Hub y las aplicaciones XenMobile.

Para aprovechar las ventajas de las nuevas funciones, soluciones y actualizaciones de directivas, Citrix recomienda instalar la versión más reciente del MDX Toolkit, Worx Home y las aplicaciones móviles

Versiones del MDX Toolkit para iOS y Android	**Versiones de Worx Home/Secure Hub**	
	Android	**iOS**
10.4	10.4	10.4
10.3.10	10.3.10	10.3.10
10.3.9	10.3.9	10.3.9
10.3.6	10.3.8	10.3.8
10.3.5	10.3.6	10.3.6
10.3.1	10.3.5	10.3.5
10.2.1	10.3.1	10.3.1
10.0.7	10.3	10.2.1
10.0.5	10.2.1	10.0.8
10.0.3	10.0.8	10.0.3
	10.0.3	

MDX Toolkit para Windows Phone	**Versiones de Worx Home compatibles***
10.0.7	10.0.3
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

* Las versiones de Worx Home anteriores a 10.0.3 son compatibles, pero no se respaldan.

> **Nota**
>
> Actualmente, Windows Phone 10 solo recibe respaldo en XenMobile 10 y 10.3.x. No recibe respaldo en XenMobile 10.1. Para XenMobile 9, se debe instalar una revisión para que las aplicaciones funcionen

correctamente. Para obtener más información, consulte CTX215497.

XenMobile 10.x respalda las versiones de aplicaciones XenMobile o aplicaciones móviles Worx que figuran en la siguiente tabla.

Aplicación	Android	iOS	Windows Phone 8.1/10[1]
Secure Hub	10.4	10.4	
Worx Home	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3.1 10.2.1 10.0.8 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
Secure Forms		10.4 10.3.10 10.3.9 10.3.8 10.3.6	
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
Worx Notes	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	

WorxTasks	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[2]	6.5	6.4	
ShareConnect	3.6	3.8	
ShareFile	4.9	4.7.1	

1 Windows Phone 10 no recibe respaldo en XenMobile 10.1.

2 Solo se respaldan las versiones más recientes de QuickEdit, ShareConnect y ShareFile.

Respaldo para exploradores Web

XenMobile 10.x admite los siguientes exploradores:

- Internet Explorer, no admite versiones 9 o anteriores
- Chrome
- Firefox
- Safari en dispositivos móviles para usrarlo con el Self Help Portal.

XenMobile 10.x es compatible con la versión más actualizada del explorador Web y con una versión anterior a la actual.

XenMobile 9

XenMobile 9 incluye Device Manager 9.0 y App Controller 9.0.

Versiones de NetScaler Gateway respaldadas:

- 11.0.64
- 10.5.x.e
- 10.5.x MR
- 10.1.x.e
- 10.1.x MR

Por lo general, los componentes de cliente de XenMobile respetan los siguientes requisitos de compatibilidad:

- La versión más reciente de Secure Hub y MDX Toolkit es compatible con las dos últimas versiones de XenMobile Server.
- La última versión de MDX Toolkit es compatible con la versión más reciente de aplicaciones XenMobile.
- Las últimas versiones de MDX Toolkit son compatibles con las siguientes versiones de Secure Hub:

	Versiones de Worx Home/Secure Hub*

Versiones del MDX Toolkit para iOS y Android	Android	iOS
10.4	10.4	10.4
10.3.6	10.3.6	10.3.6
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	
10.3	10.3	10.3
10.2.1	10.2.1	10.2.1
10.0.7	10.0.8	10.0.8
10.0.5	10.0.3	10.0.3
10.0.3		

MDX Toolkit para Windows Phone 10[1]	Versiones compatibles de Secure Hub -
10.4	10.4
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2	10.2

[1]En XenMobile 9, Windows 10 requiere la instalación de una revisión, disponible aquí.

MDX Toolkit para Windows Phone 8.1	Versiones compatibles de Secure Hub*
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2.1	10.2.1
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

* Las versiones de Secure Hub anteriores a 10.0.3 son compatibles, pero no se respaldan.

XenMobile 9 respalda las versiones de aplicaciones móviles Worx o aplicaciones XenMobile que figuran en la siguiente tabla.

Aplicación	Android	iOS	Windows Phone 8.1
Secure Hub	10.4	10.4	

Worx Home	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3.1 10.2.1 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
WorxNotes*	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	
WorxTasks	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	

		10.0.7	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[1]	6.0.2	6.3.10	
ShareConnect	3.2	3.6	
ShareFile	4.6.5	4.5	

[1] Solo se respaldan las versiones más recientes de QuickEdit, ShareConnect y ShareFile.

* MDX Toolkit 2.3 y 2.2.1 no respalda WorxNotes/Secure Notes.

Plataformas de dispositivos respaldados

Oct 31, 2016

XenMobile respalda dispositivos que ejecutan las siguientes plataformas para la administración de movilidad empresarial, incluida la administración de dispositivos y aplicaciones. Por motivos de seguridad y debido a restricciones de plataforma, no se respaldan todas las funciones en todas las plataformas.

Para dar respaldo a versiones más antiguas de sistemas operativos móviles, tales como Android 4.1 y iOS 7, consulte el artículo CTX204192 en Citrix Support Knowledge Center.

La información que se ofrece en este artículo acerca de las plataformas de dispositivo respaldadas también se aplica a XenMobile Mail Manager y XenMobile NetScaler Connector.

> ## Nota
>
> - Citrix respalda, como mínimo, la versión actual y la anterior de todas las plataformas de los sistemas operativos principales. No todas las características de la versión más reciente de XenMobile funcionarán en versiones más antiguas de las plataformas. En este artículo, se detalla lo que respalda Citrix actualmente de todos los sistemas operativos. En este artículo, también se incluyen los modelos de los dispositivos en los que Citrix ha llevado a cabo las pruebas. Si surgen problemas con otros modelos de dispositivos, póngase en contacto con la asistencia de Citrix.
> - A partir de la versión de la versión 10.4, las aplicaciones móviles Worx pasan a llamarse aplicaciones XenMobile. La mayoría de las aplicaciones XenMobile también cambian de nombre, aunque no todas. Para obtener más información, consulte Acerca de aplicaciones XenMobile.

Android

XenMobile 10.4 y 10.3.x

Sistemas operativos respaldados en todos los modos: Android 4.4.x, 5.x, 6.x, 7

Sistemas operativos respaldados solo en modo MDM: Android 4.1.x, 4.2.x, 4.3

Worx Home/Secure Hub se admite en dispositivos Android basados en x86 para la administración de dispositivos móviles.

Las aplicaciones XenMobile o las aplicaciones Worx empaquetadas con MDX se admiten en dispositivos Android basados en x64.

Algunos dispositivos Android utilizados para pruebas con XenMobile 10.3.x y 10.4 en la lista anterior de sistemas operativos son:

- Nexus 6, 7, 9, 10
- Samsung Galaxy S4 y Note 3, 4, 5
- Galaxy Tablet P750
- Galaxy Tab-A
- Galaxy Tab 2 - S3, S4, S5
- HTC One
- Samsung Tablet P750

- Samsung S6, S6 Edge y S7
- OnePlus X
- Xiaomi Mi 4
- Huawei Honor 6
- Huawei Ascend Mate 7
- HTC One M9
- Motorola Moto-X
- Sony Experia Z
- Note 2, 3, 4

XenMobile 10 y 10.1

Sistemas operativos respaldados en todos los modos: 4.4.x, 5.x, 6.x, 7

Sistemas operativos respaldados solo en modo MDM: 4.1.x

Android 4.2 y 4.3 no reciben respaldo.

Worx Home se admite en dispositivos Android basados en x86 para la administración de dispositivos móviles. La administración de aplicaciones solo está disponible en dispositivos Android con procesadores basados en ARM. Las aplicaciones empaquetadas con MDX no reciben respaldo en dispositivos Android basados en x86.

Las aplicaciones Worx empaquetadas con MDX se respaldan en dispositivos Android basados en x64.

Algunos dispositivos Android utilizados para pruebas con XenMobile 10 y 10.1 en los sistemas operativos indicados arriba son:

- Nexus 10, 7, 5, 9
- Galaxy S4 y Note 2, 3
- Galaxy Tablet 2, S3, S4, S5
- Moto X
- HTC One
- HTC Desire, LG
- Samsung Tablet P750

SAFE y KNOX

En dispositivos Samsung compatibles, XenMobile 10.x respalda y extiende directivas de Samsung for Enterprise (SAFE) y Samsung KNOX. Debe habilitar las API de la solución SAFE por medio de la implementación de la clave integrada de Samsung Enterprise License Management (ELM) a un dispositivo antes de implementar directivas y restricciones de la solución SAFE. Para habilitar la API de Samsung KNOX, además de implementar la clave ELM de Samsung, también deberá adquirir una licencia de Samsung KNOX mediante el sistema Samsung KNOX License Management System (KLMS).

En cuanto a directivas concretas de HTC, XenMobile respalda la versión 0.5.0 de la API de HTC. En el caso de directivas específicas de Sony, XenMobile respalda la versión 2.0 del SDK de Sony Enterprise.

iOS

Nota: Todas las aplicaciones Worx o XenMobile son compatibles con iOS 10 a partir de las versiones 10.3.10. Debe utilizar MDX Toolkit 10.3.10 o una versión posterior para empaquetar aplicación móviles o de empresa si quiere asegurar la compatibilidad con iOS 10. Para obtener información más detallada, consulte este artículo de asistencia de Knowledge Center.

XenMobile 10.3.x y 10.4

- iOS 10
- iOS 9.x
- iOS 8.x (Worx Home/Secure Hub solo en implementaciones en modo solo MDM)

Algunos dispositivos iOS respaldados en XenMobile 10.3.x y 10.4:

- iPhone 6, 6+, 6S, 6S+, 5s, 5, 5c
- iPad 2, 3
- iPad Air , iPad Air-2, iPad Mini-3, Mini-2
- iPad Pro
- Mac OS X
  - MacBook, Air, Mini, Mini Retina 10.9.5, 10.10, 10.11

XenMobile 10 y 10.1

- iOS 10
- iOS 9.x
- iOS 8.x (Worx Home solo en implementaciones en modo solo MDM)

Algunos dispositivos iOS respaldados en XenMobile 10 y 10.1:

- iPhone 5, 5s, 5c, 6, 6+
- iPad2, 3, Mini, Air, Air2, Mini Retina

Windows Phone y Tablet

XenMobile 10.3.x y 10.4

- Tableta Windows 10, 8.1
  - Windows 10 Tablet no recibe respaldo cuando XenMobile se encuentra solo en modo MAM.
- Windows Tablet Surface Pro 3, Surface 2, RT
- Windows Phone 10, 8.1
  - Para Windows Phone 10, debe instalar una revisión que se puede obtener en la página de descargas de XenMobile.
  - Windows 8.1 y 10 no reciben respaldo cuando XenMobile se encuentra solo en modo MAM.
- Compatibilidad de Windows Phone 8.1 con Worx Home:
  - Worx Home 10.0 cuando XenMobile está en modo Enterprise.
  - Worx Home 9.1.0 cuando XenMobile está solo en modo MDM.
- Windows 8.1 ediciones Pro y Enterprise (de 32 y 64 bits)
- Windows RT 8.1
- Windows Mobile/CE
  - Windows CE no recibe respaldo cuando XenMobile se encuentra solo en modo MAM.

Algunos dispositivos Windows respaldados en XenMobile 10.3:

- Windows Tablet 10, 8.1
- Windows Phone 10, 8.1
- HTC (Windows Phone 8.1)
- Nokia 920, 925, 1020, 1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3

- Windows Tablet Surface 2
- Windows Tablet RT

XenMobile 10 y 10.1

- Tableta Windows 10
- Windows Phone 8.1 / 10:
  - Windows Phone 8.1 no recibe respaldo cuando XenMobile se encuentra solo en modo de administración de aplicaciones móviles (MAM-only).
  - Windows Phone 10 recibe respaldo en XenMobile 10.3 y versiones posteriores.
  - Windows Phone 10 recibe respaldo en XenMobile 9, pero debe instalar una revisión de Device Manager, como se explica en este artículo de asistencia de Knowledge Center. Asimismo, tenga en cuenta la revisión de Windows 10 Anniversary Update 1607 si dispone de teléfonos Windows. Para obtener información más detallada, consulte este artículo de asistencia de Knowledge Center.
- Compatibilidad de Windows Phone 8.1 con Worx Home:
  - WorxHome 10.0 cuando XenMobile está en modo Enterprise
  - WorxHome 9.0.3 cuando XenMobile está en modo MDM-only
- Windows 8.1 ediciones Pro y Enterprise (de 32 y 64 bits)
- Windows RT 8.1
- Windows Mobile: XenMobile 10.1 no respalda dispositivos Windows Mobile. Los usuarios que tienen dispositivos que ejecutan Windows Mobile o Windows CE deben continuar usando XenMobile 9.

Algunos dispositivos Windows respaldados en XenMobile 10 y 10.1:

- Windows Tablet 8.1
- HTC (Windows Phone 8.1)
- Nokia 920, 925, 1020, 1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3
- Windows Tablet Surface 2
- Windows Tablet RT

La administración de dispositivos Windows Phone 7 se ofrece a través de XenMobile Mail Manager. Para obtener más información, consulte Instalación de XenMobile Mail Manager.

Symbian

XenMobile 10.3.x y 10.4

XenMobile 10.3.x y 10.4 no respaldan Symbian.

XenMobile 10 y 10.1

Estos son algunos de los dispositivos Symbian respaldados en XenMobile 10.1 y 10. En XenMobile 10, solo reciben respaldo para la administración de dispositivos:

- Symbian 3
- Symbian S60 5th Edition
- Symbian S60 3rd Edition, Feature Pack 2
- Symbian S60 3rd Edition, Feature Pack 1
- Symbian S60 3rd Edition

- Symbian S60 2nd Edition, Feature Pack 3
- Symbian S60 2nd Edition, Feature Pack 2

BlackBerry

La administración de dispositivos BlackBerry se ofrece a través de XenMobile Mail Manager. Para obtener más información, consulte Instalación de XenMobile Mail Manager.

Requisitos de puertos

Oct 31, 2016

Para habilitar la comunicación de dispositivos y aplicaciones con XenMobile, debe abrir puertos específicos en los firewalls. En la siguiente tabla se ofrece una lista de los puertos que se deben abrir.

Apertura de puertos de NetScaler Gateway y XenMobile para administrar aplicaciones

Debe abrir los siguientes puertos para permitir las conexiones de usuario desde Worx Home, Citrix Receiver y NetScaler Gateway Plug-in a través de NetScaler Gateway a XenMobile, StoreFront, XenDesktop, XenMobile NetScaler Connector y a otros recursos de la red interna, como los sitios Web de la intranet. Para obtener más información sobre NetScaler Gateway, consulte Configuración de parámetros para el entorno de XenMobile en la documentación de NetScaler Gateway. Para obtener más información acerca de las direcciones IP pertenecientes a NetScaler, tales como las direcciones IP de NetScaler (NSIP), las direcciones IP virtuales (VIP) y las direcciones IP de subred (SNIP), consulte Comunicación de dispositivos NetScaler con clientes y servidores en la documentación de NetScaler.

Puerto TCP	**Descripción**	**Origen**	**Destino**
21 ó 22	Se usa para enviar paquetes de asistencia a un servidor FTP o SCP.	XenMobile	Servidor SCP o FTP
53	Se utiliza para las conexiones DNS.	NetScaler Gateway XenMobile	Servidor DNS
80	NetScaler Gateway transfiere la conexión VPN al recurso de la red interna a través del segundo firewall. Normalmente, esto ocurre si los usuarios inician sesión con NetScaler Gateway Plug-in.	NetScaler Gateway	Sitios Web de la intranet
80 ó 8080 443	El puerto XML y Secure Ticket Authority (STA) se usa para la enumeración, la generación de tiquets y la autenticación. Citrix recomienda el uso del puerto 443.	Tráfico de red XML de StoreFront y de la Interfaz Web STA de NetScaler Gateway	XenDesktop o XenApp
123	Se usa para los servicios del protocolo de tiempo de red (NTP).	NetScaler Gateway	Servidor NTP

389	Se usa para conexiones de protocolo LDAP no seguras.	NetScaler Gateway XenMobile	Servidor de autenticación LDAP o Microsoft Active Directory
443	Se usa para las conexiones a StoreFront desde Citrix Receiver o desde Receiver para Web a XenApp y XenDesktop.	Internet	NetScaler Gateway
	Se utiliza para las conexiones a XenMobile con el objetivo de entregar aplicaciones Web, aplicaciones para móvil y aplicaciones SaaS.	Internet	NetScaler Gateway
	Se utiliza para la comunicación general del dispositivo con el servidor XenMobile	XenMobile	XenMobile
	Se usa para las conexiones desde dispositivos móviles hacia XenMobile para la inscripción.	Internet	XenMobile
	Se usa para las conexiones desde XenMobile a XenMobile NetScaler Connector.	XenMobile	XenMobile NetScaler Connector
	Se usa para las conexiones desde XenMobile NetScaler Connector a XenMobile.	XenMobile NetScaler Connector	XenMobile
	Se usa para la URL de respuesta en implementaciones sin la autenticación de certificado.	XenMobile	NetScaler Gateway
514	Se usa para las conexiones entre XenMobile y un servidor syslog.	XenMobile	Servidor syslog
636	Se usa para conexiones seguras de protocolo LDAP.	NetScaler Gateway XenMobile	Servidor de autenticación LDAP o Active Directory
1494	Se usa para las conexiones ICA a aplicaciones Windows en la red interna. Citrix recomienda mantener este puerto abierto.	NetScaler Gateway	XenApp o XenDesktop
1812	Se utiliza para las conexiones RADIUS.	NetScaler Gateway	Servidor de autenticación RADIUS

2598	Se utiliza para las conexiones a aplicaciones Windows en la red interna mediante la función de fiabilidad de la sesión. Citrix recomienda mantener este puerto abierto.	NetScaler Gateway	XenApp o XenDesktop
3268	Se usa para conexiones LDAP no seguras del catálogo global de Microsoft.	NetScaler Gateway XenMobile	Servidor de autenticación LDAP o Active Directory
3269	Se usa para conexiones seguras LDAP del catálogo global de Microsoft.	NetScaler Gateway XenMobile	Servidor de autenticación LDAP o Active Directory
9080	Se usa para el tráfico HTTP entre NetScaler y XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
9443	Se usa para el tráfico HTTPS entre NetScaler y XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
45000 80	Se utiliza para la comunicación entre dos máquinas virtuales de XenMobile cuando se implementan en un clúster.	XenMobile	XenMobile
8443	Se utiliza para la inscripción, XenMobile Store y la administración de aplicaciones para móvil (MAM).	XenMobile NetScaler Gateway Dispositivos Internet	XenMobile
4443	Se utiliza para que un administrador acceda a la consola de XenMobile a través del explorador.	Punto de acceso (explorador)	XenMobile
	Se utiliza para la descarga de registros y paquetes de asistencia de todos los nodos en clúster de XenMobile desde un nodo.	XenMobile	XenMobile
27000	Puerto predeterminado utilizado para acceder al servidor de licencias de Citrix externo.	XenMobile	Citrix License Server
7279	Puerto predeterminado utilizado para registrar	XenMobile	Demonio de proveedor de

	o anular licencias de Citrix.		Citrix

Apertura de puertos de XenMobile para administrar dispositivos

Debe abrir los siguientes puertos para permitir la comunicación de XenMobile en la red.

Puerto TCP	Descripción	Origen	Destino
25	El puerto SMTP predeterminado para el servicio de notificaciones de XenMobile. Si el servidor SMTP utiliza otro puerto, compruebe que el firewall no bloquea ese puerto.	XenMobile	Servidor SMTP
80 y 443	Conexión del almacén de aplicaciones empresariales al iTunes Store de Apple (ax.itunes.apple.com), a Google Play (se debe usar el puerto 80) o a la Tienda Windows Phone. Se utiliza para publicar aplicaciones de los almacenes de aplicaciones a través de Citrix Mobile Self-Serve en iOS, Worx Home para Android o Worx Home para Windows Phone.	XenMobile	iTunes App Store de Apple (ax.itunes.apple.com y *.mzstatic.com) Programa de compras por volumen de Apple (vpp.itunes.apple.com) Para Windows Phone: login.live.com y *.notify.windows.com Google Play (play.google.com)
80 ó 443	Se utiliza para las conexiones salientes entre XenMobile y la retransmisión de notificaciones SMS de Nexmo.	XenMobile	Servidor de retransmisión de SMS de Nexmo
443	Se usa para las conexiones salientes al servidor de detección automática (AutoDiscovery).	XenMobile	https://discovery.mdm.zenprise.com
443	Se usa para la inscripción y la instalación de agentes para Android y Windows Mobile.	Internet	XenMobile
	Se utiliza para la inscripción y la instalación de agentes en el caso de dispositivos Android y Windows, la consola Web de XenMobile y el cliente Remote Support para la administración MDM.	Wi-Fi o red LAN interna	
1433	Se utiliza para las conexiones a un servidor remoto de bases de datos (optativo).	XenMobile	Servidor SQL
2195	Se usa para las conexiones salientes del servicio de	XenMobile	Internet (hosts APNs con la

Puerto TCP	Descripción	Origen	Destino
	notificaciones push de Apple (APNs) a gateway.push.apple.com para notificaciones de dispositivos iOS y la inserción de directivas de dispositivo.		dirección IP pública 17.0.0.0/8)
2196	Se usa para las conexiones salientes APNs hacia feedback.push.apple.com para notificaciones de dispositivos iOS y la inserción de directivas de dispositivo.		
5223	Se usa para las conexiones salientes de APNs desde dispositivos iOS en redes Wi-Fi a *.push.apple.com.	Dispositivos iOS en redes Wi-Fi	Internet (hosts APNs con la dirección IP pública 17.0.0.0/8)
8443	Utilizado para la inscripción de dispositivos iOS y Windows Phone.	Internet	XenMobile
		Red LAN y Wi-Fi	

Requisito de puerto para la conectividad con el servicio de detección automática

Esta configuración de puerto garantiza que los dispositivos Android que se conectan desde Worx Home para Android 10.2 pueden acceder al servicio de detección automática de Citrix ADS (Auto Discovery Service) desde dentro de la red interna. La capacidad de acceder a ADS es importante en el momento de descargar las actualizaciones de seguridad que están disponibles a través de ADS.

Nota: Es posible que las conexiones ADS no funcionen con el servidor proxy. En este caso, permita que la conexión con el servicio ADS circunvale el servidor proxy.

Los clientes interesados en habilitar la fijación de certificados deben cumplir los siguientes requisitos previos:

- **Obtenga certificados para el servidor XenMobile y NetScaler**. Los certificados deben estar en formato PEM y deben ser un certificado público y no la clave privada.
- **Póngase en contacto con la asistencia técnica de Citrix y solicite la habilitación de la fijación de certificados**. Durante este proceso, se le pedirán los certificados.

Las nuevas mejoras para la fijación de certificados requieren que los dispositivos se conecten al servicio ADS antes de que el dispositivo se inscriba. Esto garantiza que la información de seguridad más actualizada esté disponible para Worx Home para el entorno en el que el dispositivo se va a inscribir. Worx Home no podrán inscribir un dispositivo si éste no puede contactar con el servicio ADS. Por lo tanto, la apertura del acceso al servicio ADS dentro de la red interna es vital para permitir la inscripción de dispositivos.

Para permitir el acceso al servicio ADS para Worx Home 10.2 para Android, abra el puerto 443 para el nombre de dominio completo (FQDN) y direcciones IP siguientes:

FQDN	Dirección IP
	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
discovery.mdm.zenprise.com	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

Cumplimiento del estándar FIPS 140-2

May 05, 2016

Los estándares Federal Information Processing Standard (estándares federales de procesamiento de la información, conocidos por sus siglas en inglés, FIPS), emitidos por el US National Institute of Standards and Technologies (Instituto nacional de estándares y tecnologías de EE. UU., NIST), especifican los requisitos de seguridad para los módulos de cifrado que se utilizan en los sistemas de seguridad. La publicación FIPS 140-2 es la segunda versión de este estándar. Para obtener más información acerca de los módulos de FIPS 140 validados por NIST, consulte http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf.

Importante: Solo puede habilitar el modo FIPS de XenMobile durante la instalación inicial.
Nota: Los modos de XenMobile de solo administración de dispositivos móviles (MDM) o de solo administración de aplicaciones para móvil (MAM), así como XenMobile Enterprise, cumplen el estándar FIPS mientras no se usen aplicaciones HDX.
En iOS, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" utilizan módulos de cifrado certificados por FIPS que proporcionan OpenSSL y Apple. En Android, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" desde el dispositivo móvil a NetScaler Gateway utilizan módulos de cifrado certificados por FIPS que proporciona OpenSSL.

En Windows RT, Microsoft Surface, Windows 8 Pro, y Windows Phone 8, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" para la administración de dispositivos móviles (MDM) utilizan módulos de cifrado certificados por FIPS que proporciona Microsoft.

En XenMobile Device Manager, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" utilizan módulos de cifrado certificados por FIPS que proporciona OpenSSL. Junto con las operaciones de cifrado descritas anteriormente para los dispositivos móviles, y entre los dispositivos móviles y NetScaler Gateway, todos los flujos de "Data in Transit" y de "Data at Rest" para la administración de dispositivos móviles utilizan módulos de cifrado compatibles con FIPS de punto a punto.

Todas las operaciones de cifrado de "Data in Transit" entre dispositivos móviles (ya sean iOS, Android o Windows Mobile) y NetScaler Gateway utilizan módulos de cifrado certificados por FIPS. XenMobile utiliza un dispositivo de FIPS NetScaler Edition, alojado en una zona DMZ y provisto de un módulo certificado por FIPS, para proteger esos datos. Para obtener más información, consulte la documentación de NetScaler FIPS.

Las aplicaciones MDX se admiten en Windows Phone 8.1 y usan bibliotecas de cifrado e interfaces API compatibles con FIPS en Windows Phone 8. Todos los "Data at Rest" de las aplicaciones MDX en Windows Phone 8.1, así como todos los "Data in Transit" entre el dispositivo Windows Phone 8.1 y NetScaler Gateway se cifran mediante esas bibliotecas e interfaces API.

El almacén MDX Vault cifra aplicaciones MDX empaquetadas y los datos "Data at Rest" asociados en dispositivos iOS y Android mediante módulos criptográficos certificados por FIPS proporcionados por OpenSSL.

Para obtener información completa acerca de la compatibilidad de XenMobile con FIPS 140-2, incluidos los módulos específicos utilizados en cada caso, póngase en contacto con su representante de Citrix.

Respaldo para idiomas en XenMobile

May 05, 2016

Las aplicaciones Worx de Citrix y la consola de XenMobile están adaptadas para poder utilizarse en otros idiomas además del inglés. Esto incluye respaldo para entradas de teclado y caracteres de idiomas no incluidos en el alfabeto inglés, incluso aunque la aplicación propiamente dicha no esté traducida al idioma preferido del usuario.

Respaldo para idiomas en las aplicaciones Worx

Esta tabla muestra los idiomas a los que se han traducido las aplicaciones Worx. La X indica que la aplicación recibe respaldo en ese idioma.

Idiomas de la interfaz de usuario	**Japonés**	**Chino simplificado**	**Alemán**	**Francés**	**Español**	**Coreano**	**Portugués**	**Neerlandés**	**Italiano**	**Danés**	**Sueco**	**Hebreo**
Apple iPhone/iPad												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Android Phone/Tablet												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Windows Phone												
Worx Home			X	X	X				X	X	X	
WorxMail			X	X	X				X	X	X	

WorxWeb	X	X	X		X	X	X

Para ver el estado de globalización de los productos Citrix al completo, consulte Citrix Knowledge Center.

Respaldo para idiomas en la consola de XenMobile

La tabla siguiente resume el estado de la traducción a otros idiomas de la consola de XenMobile. Una X indica que la consola está disponible en ese idioma.

Idiomas de la interfaz de usuario	**Chino simplificado**	**Alemán**	**Francés**	**Coreano**	**Portugués**
Consola de XenMobile	X	X	X	X	X

Respaldo para escritura de derecha a izquierda

La tabla siguiente resume el respaldo para texto de idiomas de Oriente Medio, para cada aplicación. La **X** indica que la función está disponible para esa plataforma.

App	**iOS**	**Android**	**Windows Phone**
Worx Home	X	X	
WorxMail	X	X	
WorxWeb	X	X	
WorxTasks	X	X	
WorxNotes	X	X	
QuickEdit	X	X	

Lista de verificación de la instalación

May 05, 2016

Puede usar esta lista de verificación para anotar los requisitos previos y los parámetros de la instalación de XenMobile 10. Cada tarea o nota incluye una columna que indica el componente o la función a los que se aplica el requisito. Para obtener los pasos de instalación, consulte Instalación de XenMobile.

Conectividad de red básica

A continuación, se presentan los parámetros de red que se necesitan para la solución XenMobile.

	Requisito previo o configuración	Componente o función	Escriba el parámetro
	Escriba el nombre de dominio completo (FQDN) al que se conectan los usuarios remotos.	XenMobile NetScaler Gateway	
	Escriba las direcciones IP local y pública. Necesita estas direcciones IP para configurar el firewall y la traducción de direcciones de red (NAT).	XenMobile NetScaler Gateway	
	Escriba la máscara de subred.	XenMobile NetScaler Gateway	
	Escriba las direcciones IP de DNS.	XenMobile NetScaler Gateway	
	Escriba las direcciones IP del servidor WINS (si corresponde).	NetScaler Gateway	
	Identifique y escriba el nombre de host de NetScaler Gateway. Nota: No se trata del FQDN. El FQDN se encuentra en el certificado de servidor firmado que está enlazado al servidor virtual al que se conectan los usuarios. Puede configurar el nombre de host mediante el Asistente para la instalación de NetScaler Gateway.	NetScaler Gateway	
	Escriba la dirección IP de XenMobile. Reserve una dirección IP si instala una instancia de XenMobile.	XenMobile	

	Requisito previo o configuración	Componente o función	Escriba el parámetro
	Si configura un clúster, escriba todas las direcciones IP que necesita.		
	• Una dirección IP pública configurada en NetScaler Gateway • Una entrada DNS externa para NetScaler Gateway	NetScaler Gateway	
	Escriba la dirección IP del servidor proxy Web, el puerto, la lista de hosts proxy y el nombre de usuario y la contraseña del administrador. Estos parámetros son opcionales si implementa un servidor proxy en la red (si corresponde). Nota: Puede utilizar el sAMAccountName o el nombre principal de usuario (UPN) al configurar el nombre de usuario para el proxy Web.	XenMobile NetScaler Gateway	
	Escriba la dirección IP de la puerta de enlace predeterminada.	XenMobile NetScaler Gateway	
	Escriba la dirección IP del sistema (NSIP) y la máscara de subred.	NetScaler Gateway	
	Escriba la dirección IP de subred (SNIP) y la máscara de subred.	NetScaler Gateway	
	Escriba la dirección IP del servidor virtual de NetScaler Gateway y el nombre de dominio completo (FQDN) del certificado. Si necesita configurar varios servidores virtuales, escriba todas las direcciones IP virtuales y los nombres FQDN de los certificados.	NetScaler Gateway	
	Escriba las redes internas a las que pueden acceder los usuarios a través de NetScaler Gateway. Ejemplo: 10.10.0.0/24. Introduzca todas las redes internas y los segmentos de red a los que deben acceder los usuarios cuando se conectan a Worx Home o NetScaler Gateway Plug-in si la opción de túnel dividido está en On.	NetScaler Gateway	
	Compruebe que la conectividad de red entre el servidor XenMobile, NetScaler Gateway, el servidor SQL Server externo de Microsoft y el servidor DNS está operativa.	XenMobile NetScaler Gateway	

Licencias

XenMobile requiere que adquiera opciones de licencias para NetScaler Gateway y XenMobile. Para obtener más información acerca de Citrix Licensing, consulte El sistema de licencias de Citrix.

•	Requisitos previos	Componente	Escriba la ubicación
	Obtenga licencias universales del sitio Web de Citrix. Para obtener más información, consulte la instalación de licencias de NetScaler Gateway.	NetScaler Gateway XenMobile Citrix License Server	

Certificados

XenMobile y NetScaler Gateway requieren certificados para habilitar las conexiones procedentes de dispositivos de usuario, así como las conexiones a otras aplicaciones y productos Citrix. Para obtener información más detallada, consulte Certificados en XenMobile.

✓	Requisitos previos	Componente	Notas
	Obtenga e instale los certificados necesarios.	XenMobile NetScaler Gateway	

Puertos

Debe abrir puertos para permitir la comunicación con los componentes de XenMobile. Para ver una lista completa de los puertos que se deben abrir, consulte Requisitos de puertos para XenMobile.

✓	Requisitos previos	Componente	Notas
	Puertos abiertos para XenMobile	XenMobile NetScaler Gateway	

Base de datos

Es necesario configurar una conexión de base de datos. El repositorio de XenMobile requiere una base de datos de Microsoft SQL Server con una de las siguientes versiones compatibles: Microsoft SQL Server 2014, SQL Server 2012, SQL Server 2008 R2 o SQL Server 2008. Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile y se debe utilizar de forma local o remota solo en entornos de prueba.

•	Requisitos previos	Componente	Escriba el parámetro
	Puerto y dirección IP de Microsoft SQL Server.	XenMobile	

	Requisitos previos	Componente	Escriba el parámetro
	Compruebe que la cuenta de servicio de SQL Server que se va a usar en XenMobile tiene el permiso del rol DBcreator.		

Parámetros de Active Directory

	Requisitos previos	Componente	Escriba el parámetro
	Escriba el puerto y la dirección IP de Active Directory de los servidores principales y secundarios. Si utiliza el puerto 636, instale un certificado raíz de una entidad de certificación en XenMobile y cambie la opción Use secure connections a Yes.	XenMobile NetScaler Gateway	
	Escriba el nombre de dominio de Active Directory.	XenMobile NetScaler Gateway	
	Escriba la cuenta de servicio de Active Directory, que requiere un ID de usuario, una contraseña y un alias de dominio. La cuenta de servicio de Active Directory es la cuenta que XenMobile utiliza para consultar a Active Directory.	XenMobile NetScaler Gateway	
	Escriba el DN base de usuario. Este es el nivel de directorio en el que se encuentran los usuarios; por ejemplo, cn=users, dc=ace, dc=com. NetScaler Gateway y XenMobile lo usan para enviar consultas a Active Directory.	XenMobile NetScaler Gateway	
	Escriba el DN base de grupo. Este es el nivel de directorio en el que se encuentran los grupos. NetScaler Gateway y XenMobile lo usan para enviar consultas a Active Directory.	XenMobile NetScaler Gateway	

Conexiones entre XenMobile y NetScaler Gateway

	Requisitos previos	Componente	Escriba el parámetro
	Escriba el nombre de host de XenMobile.	XenMobile	

Requisitos previos	Componente	Escriba el parámetro
Escriba el nombre de dominio completo (FQDN) o la dirección IP de XenMobile.	XenMobile	
Identifique las aplicaciones a las que pueden acceder los usuarios.	NetScaler Gateway	
Escriba la dirección URL de respuesta.	XenMobile	

Conexiones de usuario: acceso a XenDesktop, XenApp y Worx Home

Citrix recomienda usar el asistente de configuración rápida de NetScaler para configurar los parámetros de conexión entre XenMobile y NetScaler Gateway, así como entre XenMobile y Worx Home. Puede crear un segundo servidor virtual para habilitar las conexiones de usuario desde Receiver y exploradores Web con el objetivo de conectarse a escritorios virtuales y aplicaciones Windows de XenApp y XenDesktop. Citrix recomienda usar el asistente de configuración rápida en NetScaler para configurar también estos parámetros.

Requisitos previos	Componente	Escriba el parámetro
Escriba el nombre de host y la URL externa de NetScaler Gateway. La URL externa es la dirección Web a la que se conectan los usuarios.	XenMobile	
Escriba la URL de respuesta de NetScaler Gateway.	XenMobile	
Escriba las direcciones IP y las máscaras de subredes para el servidor virtual.	NetScaler Gateway	
Escriba la ruta para el Agente de Program Neighborhood o un sitio de servicios XenApp.	NetScaler Gateway XenMobile	
Escriba el nombre FQDN o la dirección IP del servidor XenApp o XenDesktop que ejecuta Secure Ticket Authority (STA) (solo para conexiones ICA).	NetScaler Gateway	
Escriba el nombre FQDN público de XenMobile.	NetScaler Gateway	
Escriba el nombre FQDN público para Worx Home.	NetScaler Gateway	

Problemas conocidos

May 05, 2016

A continuación, se describen los problemas conocidos de XenMobile 10.0.

Para ver la lista de problemas corregidos en esta versión, consulte http://support.citrix.com/article/CTX141722. .

- Es posible que en Worx Home se muestren marcadores de posición grises en lugar de iconos después de actualizar un dispositivo iOS de iOS 7 a iOS 8 y reiniciarlo. Este es un problema de terceros. [#502879]
- Durante la inscripción, es posible que los dispositivos iOS tengan errores durante o después de la instalación del perfil de administración de dispositivos móviles (MDM). Es posible que los usuarios vean "Cocoa error 4097" en los dispositivos con iOS 8.1 o "Profile cannot be decrypted" en los dispositivos con versiones anteriores de iOS. Si esto ocurre, los usuarios deben volver a llevar a cabo el proceso de inscripción. En algunos casos, es posible que haga falta más de un intento. [#507948]
- En XenMobile 10, no se pueden realizar llamadas SOAP de checkUserPassword y addGroup en la clase de grupo USER. Los cambios de la API de usuario aparecen en la base de datos, no en las interfaces de usuario de los dispositivos. [#511551, #511822]
- No está disponible la capacidad de cambiar el orden en que se implementan los recursos de los grupos de entrega desde la consola Web de XenMobile. Si quiere controlar el orden de la implementación, cambie el nombre de los recursos para seguir el protocolo de implementación que utiliza XenMobile: numérico (1, 2, 3...), alfabético con mayúsculas (A, B, C...) y alfabético con minúsculas (a, b, c...). Un recurso cuyo nombre empiece por "24" se implementará antes de un recurso cuyo nombre empiece por WM. Asimismo, ambos recursos se implementarán antes que un recurso cuyo nombre empiece por tw. [#512566]
- Si la restricción del filtro de contenido para adultos está habilitada, la búsqueda segura se inhabilita y se establece como moderada en dispositivos Windows Phone 8.1. [#513605]
- Cuando implemente directivas de dispositivos en tabletas Windows 8.1 y antes de que los dispositivos informen a XenMobile de que las directivas se han ejecutado, es posible que las vea en la ficha Deployed, en la sección Device Details de la consola de XenMobile. [#514749]
- Al volver a inscribir un dispositivo, la inscripción puede fallar si los usuarios lo reinscriben demasiado pronto después de desinscribirlo. [#516567]
- En ocasiones, cuando los usuarios se reinscriben en Worx Home, XenMobile presenta una sesión SSL almacenada en caché y los usuarios ven la pantalla de inscripción de nuevo. Cuando esto ocurra, los usuarios deben volver a llevar a cabo el proceso de inscripción. [#517301]
- La enumeración de aplicaciones falla cuando los grupos de entrega se definen con grupos de Active Directory que pertenecen a dominios principales y secundarios mediante el operador AND. Para evitar este problema, use el operador OR al definir los grupos de entrega. [#518084]
- Si configura una directiva o un parámetro en la consola de XenMobile en la que carga un archivo (certificado, PDF, fuente, etc.) y luego ve los detalles de dicha directiva o dicho parámetro, el nombre del archivo no aparece. [#519552]
- XenMobile no admite la autenticación con PIN en el modo de administración de aplicaciones móviles (MAM) en el caso de dispositivos iOS y Android. Si configura este modo como el predeterminado en la consola de XenMobile, los usuarios deben introducir sus credenciales dos veces en Worx Home. [#519572]
- Si inhabilita el grupo AllUsers como grupo de entrega en la consola de XenMobile, los usuarios que no pertenezcan a ningún grupo de entrega no podrán inscribir ningún dispositivo, pero podrán iniciar sesión en el portal Self Help Portal. [#521393]
- Worx Home para Windows Phone 8.x, en modo MDM (administración de dispositivos móviles), solo respalda aplicaciones de tiendas o almacenes públicos cuando se las implementa como optativas. Si estas aplicaciones se agregan al grupo de

entrega como aplicaciones obligatorias, no aparecen en Worx Home. [#521524]

- La página Role-Based Access Control (RBAC) Role Info parece permitir la modificación de la plantilla Admin predeterminada. Sin embargo, a pesar de hacer cambios en el campo RBAC de la plantilla y en otros lugares, estos cambios no se guardan en la plantilla Admin. La plantilla de administración está diseñada para que no se pueda modificar. [#521540]
- En dispositivos iOS, el aprovisionamiento del token de SAML cuando los usuarios se inscriben en Worx Home y configuran sus cuentas de ShareFile, puede no estar sincronizado. Como solución alternativa, los usuarios pueden cerrar y volver a entrar en Worx Home y luego iniciar una sesión en la aplicación de ShareFile para activar una nueva solicitud de token de SAML. [#521934]
- En la mayoría de los dispositivos, cuando los usuarios de dispositivos Android tocan el icono Menú, aparecen las opciones de menú Aceptar y Rechazar, lo que permite a los usuarios continuar el proceso de inscripción. Sin embargo, en algunos dispositivos con sistemas operativos anteriores a la versión 4.0 (como las tabletas Samsung GT-P7510), el icono Menú no aparece en la página de términos y condiciones en la vista predeterminada, y los usuarios no pueden completar el proceso de inscripción. Como solución alternativa, puede excluir los dispositivos de la implementación de términos y condiciones. [#524039]
- En dispositivos iOS, Worx Home no se puede conectar a Worx Store si se ha cambiado el nombre predeterminado del almacén en la página Beacons de la consola de XenMobile (Configure > Settings > More > Beacons). El valor predeterminado de este parámetro es Store. Si este parámetro se cambia, el servicio Discovery Service falla durante el inicio de sesión y no se puede encontrar Worx Store. Para evitar este fallo, deje el parámetro Store name en la página Beacons con el valor predeterminado Store. [#523306]
- En una configuración de XenMobile con equilibrio de carga y con descarga de SSL, cuando se configuran aplicaciones de SAML, para que funcione el Single Sign-on cuando los usuarios instalan WorxWeb y abren una aplicación iniciada por un proveedor de servicios, todas las referencias al servidor XenMobile deben apuntar al puerto 8443 en lugar del puerto 443. [528680]
- Al crear una directiva de códigos de acceso para Samsung KNOX y configurar la opción Lock device after (minutes of activity), el servidor aplica el bloqueo en segundos aunque esa opción en la consola muestre minutos como la unidad utilizada. [#531204]
- En XenMobile 10, no puede configurar su propio servicio y proveedor de identidades SAML para autenticar a los usuarios y sus dispositivos. [#530892]
- No se pueden agregar dispositivos BlackBerry o Windows de forma individual a la consola de XenMobile. [#532844]
- Si configura SAML con el signo de número (#) en el nombre, el inicio de sesión único (Single Sign-On) desde Worx Home no funciona y aparece un mensaje de error. [#533078]
- Cuando se agrega una entidad PKI genérica (GPKI) en la consola de XenMobile, no se puede probar la conexión de adaptador URL de Web Services Description Language (WSDL) durante la configuración. [#533871]
- Las directivas de contraseña de tabletas Windows no entran en vigor inmediatamente en los dispositivos y se producen algunas incoherencias en la aplicación de actualizaciones a la longitud mínima de la contraseña. Este es un problema de terceros. [#534088]
- Cuando los usuarios inscriben su dispositivo iOS en modo de administración de dispositivos móviles (MDM), las opciones de seguridad (Security) en la consola de XenMobile, en la página Manage > Devices, para ubicar y hacer un seguimiento del dispositivo, no aparecen inmediatamente. Después de una breve demora, esas opciones aparecen. [#534672]
- Si incluye un carácter especial (como un punto) en el nombre simplificado del Delivery Controller de StoreFront, los usuarios no pueden suscribirse y abrir aplicaciones con XenApp mediante Worx Home. Aparece el error: "Cannot complete your request". Como solución alternativa, quite los caracteres especiales del nombre. [#535497]
- Las aplicaciones no aparecen en Worx Store cuando se trata de dispositivos iOS anteriores a iOS 8 si se escribe un valor en el campo Excluded devices de la consola de XenMobile al agregar y configurar la aplicación. Como solución alternativa, puede definir una regla de implementación para especificar los dispositivos en los que puede instalarse la aplicación en

cuestión. [#537631]

- Al configurar las conexiones de NetScaler Gateway con XenMobile en un puerto que no es el predeterminado (443), la inscripción en el modo de administración de aplicaciones móviles (MAM) falla en dispositivos iOS, y en dispositivos Windows con Worx Home. [#537368]
- Los caracteres especiales como $, @ y " no se reconocen en las contraseñas para la línea de comandos al instalar XenMobile 10 y las asignadas a certificados; el carácter especial y los caracteres siguientes se ignoran y el inicio de sesión falla. Después de la instalación, la contraseña de la interfaz de línea de comandos no se puede cambiar para incluir caracteres especiales. [#541997] [#542436]
- Se produce un error de perfil no válido cuando se intenta configurar el programa de inscripción de dispositivos (DEP) de iOS en la consola de XenMobile. Este es un problema de terceros. [#608213]

A continuación, se describen los problemas conocidos de XenMobile Mail Manager 10.0.

- La versión instalada de XenMobile Mail Manager siempre muestra 8.5 durante la actualización a XenMobile Mail Manager 10; no obstante, la actualización tiene lugar. [539520]
- La notificación de "dispositivos encontrados" en la instantánea menor puede resultar confusa. Los mismos dispositivos pueden aparecer como "nuevos" en resúmenes de instantánea secundaria sucesivos si las instantáneas secundarias se ejecutan a continuación del inicio de una instantánea principal.

Instalación de XenMobile

Oct 31, 2016

La máquina virtual (VM) de XenMobile se ejecuta en Citrix XenServer, VMware ESXi o Microsoft Hyper-V. Puede utilizar las consolas de administración de XenCenter o vSphere para instalar XenMobile.

Antes de empezar: En la planificación de una implementación de XenMobile, hay varios aspectos a tener en cuenta. Para ver recomendaciones, preguntas frecuentes y casos de uso de un entorno XenMobile de extremo a extremo, consulte XenMobile Deployment Handbook. Asimismo, consulte Requisitos del sistema para XenMobile 10 y Lista de verificación previa a la instalación de XenMobile 10.

Nota: Compruebe que el hipervisor está configurado con la hora correcta porque XenMobile usa el mismo reloj.

Requisitos previos de XenServer o VMware ESXi. Antes de instalar XenMobile en XenServer o en VMware ESXi, debe seguir los siguientes pasos. Para obtener más información, consulte la documentación de XenServer o VMware.

- Instalar XenServer o VMware ESXi en un equipo con recursos de hardware adecuados.
- Instalar XenCenter o vSphere en un equipo separado. El equipo que aloja XenCenter o vSphere se conecta al host de XenServer o VMware ESXi mediante la red.

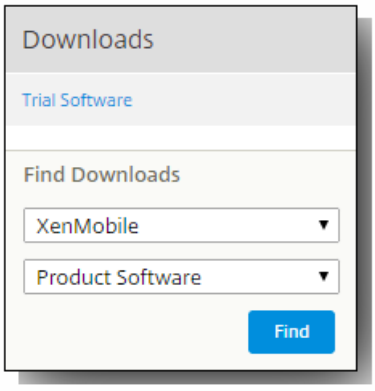
Requisitos previos de Hyper-V. Antes de instalar XenMobile en Hyper-V, debe seguir los siguientes pasos. Para obtener más información, consulte la documentación de Hyper-V.

- Instale Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2 con Hyper-V y sus roles habilitados en un equipo que disponga de los recursos de sistema adecuados. Cuando instale el rol Hyper-V, asegúrese de que especifica las tarjetas de interfaz de red (NIC) en el servidor que Hyper-V usará para crear las redes virtuales. Puede reservar algunas tarjetas para el host.

Modo FIPS 140-2: Si tiene pensado instalar el servidor XenMobile en modo FIPS, necesitará completar una serie de requisitos previos, según se describe en Configuración de FIPS con XenMobile.

Descarga del software del producto XenMobile

Puede descargar el software del producto desde el sitio Web de Citrix. Para ello, inicie una sesión en el sitio y haga clic en el enlace Descargas de la página Web de Citrix. Después puede seleccionar el producto y el tipo que quiere descargar. Por ejemplo, la siguiente ilustración muestra XenMobile y el software del producto seleccionado de las listas:



Cuando se hace clic en Buscar, aparece una página con la lista de las descargas disponibles, encabezadas por sus versiones más recientes. Puede seleccionar software en la lista de opciones disponibles.

Cómo descargar el software de XenMobile

1. Vaya al sitio Web de Citrix.
2. Haga clic en My Account (Iniciar sesión) e inicie una sesión.
3. Haga clic en Descargas.
4. En Find Downloads, en la lista de productos, haga clic en XenMobile.
5. En Find Downloads, en la lista de tipos de descarga, haga clic en Product Software y, a continuación, haga clic en Find.
6. En la página XenMobile Product Software, haga clic en la edición de XenMobile 10.0 que quiera descargar.
7. En la página XenMobile 10.0 Edition, haga clic en Download para descargar la imagen virtual correspondiente e instalar XenMobile en XenServer, VMware o Hyper-V.
8. Siga las instrucciones en pantalla para descargar el software.

Para descargar el software de NetScaler Gateway

Puede usar este procedimiento para descargar el dispositivo virtual NetScaler Gateway, para descargar actualizaciones de software para su dispositivo NetScaler Gateway actual.

1. Vaya al sitio Web de Citrix.
2. Haga clic en My Account (Iniciar sesión) e inicie una sesión.
3. Haga clic en Descargas.
4. En Find Downloads, en la lista de productos, haga clic en NetScaler Gateway.
5. En Find Downloads, en la lista de tipos de descarga, haga clic en Product Software y, a continuación, haga clic en Find. Nota: También puede hacer clic en Virtual Appliances para descargar NetScaler VPX. Cuando se selecciona esta opción, se recibe una lista de software para la máquina virtual para cada hipervisor.
6. En la página NetScaler Gateway, expanda 10.5(4).
7. Haga clic en la versión de software del dispositivo que desea descargar.
8. En la página de software del dispositivo correspondiente a la versión que quiere descargar, haga clic en Download para descargar el dispositivo virtual.
9. Siga las instrucciones en pantalla para descargar el software.

Configuración de XenMobile para el primer uso

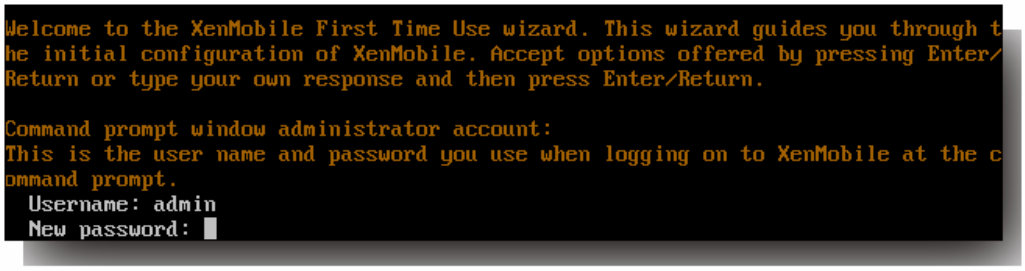
La configuración de XenMobile por primera vez es un proceso que consta de dos partes.

1. Configurar la dirección IP y la máscara de subred, la puerta de enlace predeterminada y los servidores DNS para XenMobile mediante la consola de línea de comandos de XenCenter o vSphere.
2. Iniciar sesión en la consola de administración de XenMobile y seguir los pasos indicados en las pantallas iniciales de inicio de sesión.

> **Nota**
>
> Al utilizar un cliente Web de vSphere, se recomienda no configurar las propiedades de conexión de red a la hora de implementar la plantilla OVF en la página **Customize template**. Con esto, en una configuración de alta disponibilidad, se evita el problema con la dirección IP que puede ocurrir al clonar y luego reiniciar la segunda máquina virtual de XenMobile.

Configuración de XenMobile en la ventana del símbolo del sistema

1. Importe la máquina virtual de XenMobile en Citrix XenServer, Microsoft Hyper-V o VMware ESXi. Para obtener información detallada, consulte la documentación de XenServer, Hyper-V o VMware.
2. En el hipervisor, seleccione la máquina virtual importada de XenMobile e inicie la vista del símbolo del sistema. Para obtener información más detallada, consulte la documentación de su hipervisor.
3. Desde la página de la consola del hipervisor, cree una cuenta de administrador para XenMobile en la ventana del símbolo del sistema.



Nota: No aparecerá ningún carácter (como, por ejemplo, asteriscos) cuando escriba la nueva contraseña. No aparece nada.

4. Proporcione la siguiente información:
   1. Dirección IP
   2. Máscara de red (Netmask)
   3. Puerta de enlace predeterminada
   4. Servidor DNS principal (Primary DNS server)
   5. Servidor DNS secundario (Secondary DNS server, si quiere)

Nota: Las direcciones que se muestran en esta imagen no son operativas; se proporcionan en calidad de ejemplos.

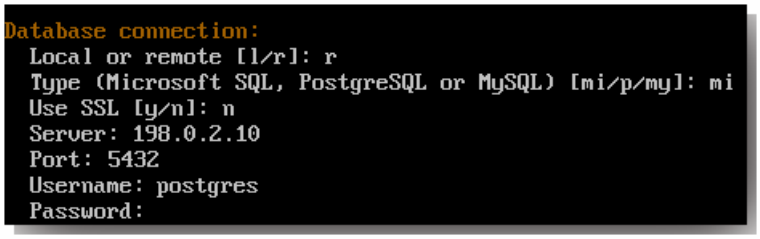
5. Escribay; para mejorar la seguridad, creando una frase secreta aleatoria on si quiere definir su propia frase secreta. Citrix recomienda escribiry; para generar una frase secreta aleatoria. La frase secreta se utiliza como parte de la protección de las claves de cifrado usadas para proteger información confidencial. Se usa un hash de la frase secreta, almacenada en el sistema de archivos del servidor, para recuperar las claves durante el cifrado y el descifrado de datos. El parámetro frase secreta no se puede ver.

Nota: Si va a ampliar el entorno y configurar servidores adicionales, debe definir su propia frase secreta. No se

puede ver la frase secreta si se ha seleccionado una frase secreta aleatoria.

6. Si quiere, puede habilitar el Estándar federal de procesamiento de información (FIPS). Para ver más información sobre FIPS, consulte Cumplimiento del estándar FIPS 140-2 de XenMobile. Además, asegúrese de completar los requisitos previos, según se describe en Configuración de FIPS con XenMobile.

7. Configure la conexión de la base de datos. La base de datos puede ser local o remota. Si se le solicita si es local o remota, escriba, según corresponda-r ol.
   Importante:
   - Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile y se debe utilizar de forma local o remota solo en entornos de prueba.
   - No se respalda la migración de la base de datos. Las bases de datos creadas en un entorno de prueba no se pueden mover a un entorno de producción.



   Importante: El puerto predeterminado para PostgreSQL es 5432.

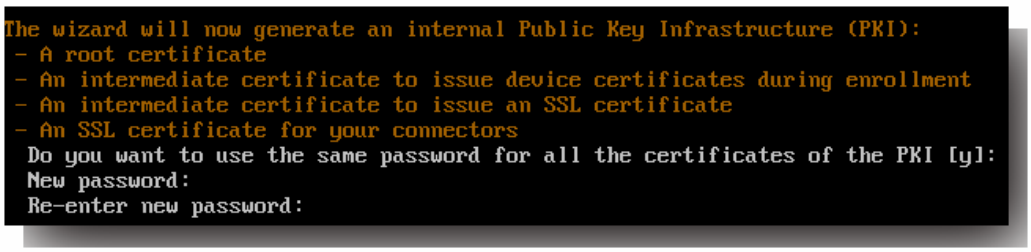
   Nota: Las direcciones que se muestran en esta imagen no son operativas; se proporcionan en calidad de ejemplos.
8. Proporcione el nombre de dominio completo (FQDN) del servidor que aloja XenMobile. Este servidor host proporciona servicios de administración de dispositivos y de administración de aplicaciones.

   Importante: No podrá cambiar el nombre FQDN sin reinstalar completamente el servidor.

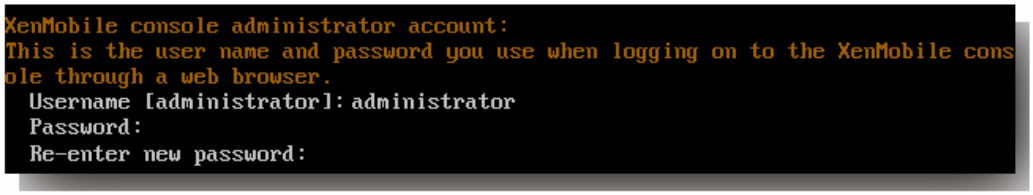
9. Identifique los puertos de comunicación. Para obtener información más detallada acerca de los puertos y sus usos,

consulte Requisitos de puertos para XenMobile.
Nota: Para aceptar los puertos predeterminados, presione Intro (Retorno en Mac).

10. Se le solicitará que proporcione las contraseñas para todos los certificados de servidor de la infraestructura de clave pública (PKI). Asimismo, se le ofrecerá la opción de utilizar la misma contraseña para cada certificado. Para obtener información más detallada acerca de la función PKI de XenMobile, consulte Carga de certificados en XenMobile.
Importante: Si va a agrupar nodos en clúster o instancias de XenMobile, deberá proporcionar contraseñas idénticas para los nodos subsiguientes.



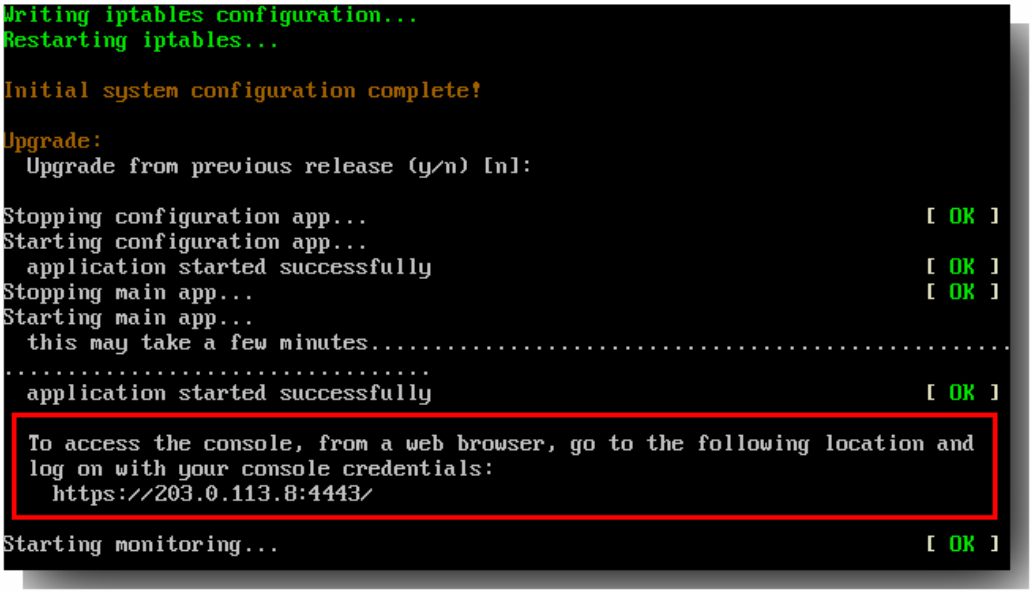
Nota: No aparecerá ningún carácter (como, por ejemplo, asteriscos) cuando escriba la nueva contraseña. No aparece nada.
11. Cree una cuenta de administrador para iniciar sesión en la consola de XenMobile con un explorador Web. Deberá recordar estas credenciales para usarlas más tarde.



Nota: No aparecerá ningún carácter (como, por ejemplo, asteriscos) cuando escriba la nueva contraseña. No aparece nada.
12. Cuando se le pregunte si se trata de una actualización, escriban ya que se trata de una nueva instalación.

13. Copie toda la URL que aparece en pantalla, y continúe la siguiente configuración inicial de XenMobile en el explorador

Web.



Configuración de XenMobile en un explorador Web

Después de completar la parte inicial de la configuración de XenMobile en la ventana del símbolo del sistema del hipervisor, complete el proceso en el explorador Web.

1. En el explorador Web, vaya a la ubicación proporcionada en la conclusión de la configuración de la ventana del símbolo del sistema.
2. Escriba el nombre de usuario y la contraseña correspondientes a la cuenta de administrador de la consola de XenMobile; los creó anteriormente en la ventana de símbolo del sistema.

3. En la página Get Started, haga clic en Start. Aparecerá la página Licensing.
4. Configure la licencia. XenMobile incluye una licencia de evaluación de 30 días. Para obtener información más detallada sobre cómo agregar y configurar licencias y notificaciones de caducidad, consulte Licencias de XenMobile.
   Importante: Si va a agrupar nodos en clúster o instancias de XenMobile, es necesario usar Citrix Licensing en un servidor remoto.

5. En la página Certificates, haga clic en Import. Aparecerá el cuadro de diálogo Import.
6. Importe los certificados APNs y el certificado de escucha de SSL. Para obtener más información sobre cómo trabajar con certificados, consulte Certificados en XenMobile.
   Nota: El certificado de escucha de SSL requiere reiniciar el servidor.
7. Si corresponde en función del entorno, configure NetScaler Gateway. Para obtener más información sobre cómo configurar NetScaler Gateway, consulte NetScaler Gateway y XenMobile y Configuración de parámetros para el entorno de XenMobile.
   Nota: Es posible implementar NetScaler Gateway en el perímetro de la red interna (o intranet) de la organización para proporcionar un único punto de acceso seguro a los servidores, las aplicaciones y otros recursos de red que residan en la red interna. En esta implementación, todos los usuarios remotos deben conectarse a NetScaler Gateway para poder acceder a los recursos de la red interna.
   Nota: Aunque configurar NetScaler Gateway sea optativo, después de escribir datos en la página, debe borrar o completar los campos obligatorios antes de salir de la página.
8. Complete la configuración del protocolo LDAP para acceder a usuarios y grupos de Active Directory. Para obtener información más detallada acerca de la configuración de la conexión LDAP, consulte Configuración de LDAP.
9. Configure el servidor de notificaciones para poder enviar mensajes a los usuarios. Para obtener información más detallada acerca de la configuración del servidor de notificaciones, consulte Notificaciones en XenMobile.

Configuración de FIPS con XenMobile

May 05, 2016

El modo FIPS (Federal Information Processing Standards) en XenMobile da respaldo a clientes pertenecientes a organismos del gobierno federal de los Estados Unidos, al configurar el servidor para utilizar bibliotecas de certificados FIPS 140-2 para todas las operaciones de cifrado. Mediante la instalación del servidor XenMobile con el modo FIPS, se asegura de que todos los datos, tanto en reposo como en tránsito, para el cliente y para el servidor XenMobile, cumplen los estándares de FIPS 140-2.

Antes de instalar un servidor XenMobile en modo FIPS, es necesario completar los siguientes requisitos previos.

- Debe usar un servidor SQL Server 2012 o SQL Server 2014 externo para la base de datos de XenMobile. El servidor SQL Server también debe configurarse para la comunicación SSL segura. Para ver instrucciones sobre cómo configurar la comunicación SSL segura con el servidor SQL Server, consulte los Manuales de SQL Server.
- Para la comunicación SSL segura se necesita instalar un certificado SSL en el servidor SQL Server. El certificado SSL puede ser un certificado público de una entidad de certificación (CA) comercial, o un certificado autofirmado de una CA interna. SQL Server 2014 no puede aceptar un certificado comodín. Por tanto, Citrix recomienda solicitar un certificado SSL con el nombre de dominio completo (FQDN) del servidor SQL Server.
- Si usa un certificado autofirmado para el servidor SQL Server, necesitará una copia del certificado raíz de la CA que emitió su certificado autofirmado. El certificado raíz de la CA debe importarse en el servidor XenMobile durante la instalación.

Configuración del modo FIPS

El modo FIPS solo puede habilitarse durante la instalación inicial del servidor XenMobile. No se puede habilitar FIPS una vez completada la instalación. Por lo tanto, si va a usar el modo FIPS, debe instalar el servidor XenMobile con el modo FIPS desde el principio. Además, si tiene un clúster de XenMobile, todos los nodos del mismo deben tener FIPS habilitado; no se puede tener una mezcla de servidores XenMobile con FIPS y sin FIPS en un mismo clúster.

Hay una opción **Toggle FIPS mode** en la interfaz de línea de comandos de XenMobile que no debe usarse en producción. Esta opción está pensada para usarse en entornos que no son de producción, con fines de diagnóstico, y no recibe respaldo en servidores XenMobile de producción.

1. Durante la instalación inicial, habilite **FIPS mode**.

2. Cargue el certificado raíz de la CA para el servidor SQL Server. Si usó un certificado SSL autofirmado en lugar de un certificado público en el servidor SQL Server, elija **Yes** para esta opción, y lleve a cabo una de las acciones siguientes:

    a. Copie y pegue el certificado de la CA.

    b. Importe el certificado de la CA. Para importar el certificado de la CA, debe publicar el certificado en un sitio Web que sea accesible desde el servidor XenMobile a través de una URL con HTTP. Para obtener más información, consulte la sección Importación de certificados más adelante en este artículo.

3. Especifique el nombre del servidor y el puerto del servidor SQL Server, las credenciales para iniciar sesión en SQL Server y el nombre de la base de datos que se debe crear para XenMobile.

Nota: Para acceder a SQL Server puede usar un inicio de sesión de SQL o una cuenta de Active Directory, pero el inicio de sesión que use debe tener el rol de creador de bases de datos (DBcreator).

4. Para usar una cuenta de Active Directory, introduzca las credenciales con el formato dominio\nombre-de-usuario.

5. Una vez completados estos pasos, continúe con la instalación inicial de XenMobile.

Para confirmar que la configuración de FIPS es correcta, inicie una sesión en la interfaz de línea de comandos de XenMobile. La frase **In FIPS Compliant Mode** aparecerá en el mensaje de inicio de sesión.

Importación de certificados

El siguiente procedimiento describe cómo configurar FIPS en XenMobile importando el certificado, lo cual es necesario cuando se usa un hipervisor VMWare.

Requisitos previos de SQL

1. La conexión con la instancia SQL desde XenMobile necesita ser segura y la versión debe ser SQL Server 2012 o SQL Server 2014. Para proteger la seguridad de la conexión, consulte Cómo habilitar el cifrado SSL para una instancia de SQL Server usando Microsoft Management Console.

2. Si el servicio no se reinicia correctamente, compruebe lo siguiente: Abra **Services.msc**.

   a. Copie la información de cuenta de inicio de sesión utilizada para el servicio SQL Server.

   b. Abra MMC.exe en SQL Server.

   c. Vaya a **Archivo** > **Agregar o quitar complemento** y luego haga doble clic en el elemento Certificados para agregar el complemento Certificados. Seleccione Cuenta de equipo y Equipo local en las dos páginas siguientes del asistente.

   d. Haga clic en **Aceptar**.

   e. Expanda **Certificados (Equipo local)** > **Personal** > **Certificados** y busque el certificado SSL importado.

   f. Haga clic con el botón secundario en el certificado importado (seleccionado en el Administrador de configuración de SQL Server) y haga clic en **Todas las tareas** > **Administrar claves privadas**.

   g. En **Nombres de grupos o usuarios**, haga clic en **Agregar**.

   h. Introduzca el nombre de la cuenta del servicio SQL que copió en uno de los pasos anteriores.

   i. Deje sin marcar la casilla de **Permitir control total**. De manera predeterminada, la cuenta del servicio recibe permisos de Control total y Leer, pero en realidad solo necesita leer la clave privada.

   j. Cierre **MMC** e inicie el servicio SQL.

3. Asegúrese de que el servicio SQL se inicia correctamente.

Requisitos previos de Internet Information Services (IIS)

1. Descargue el certificado raíz (base 64).

2. Copie el certificado raíz en el sitio Web predeterminado del servidor IIS, C:\inetpub\wwwroot.

3. Marque la casilla **Autenticación** para el sitio predeterminado.

4. Defina el parámetro **Anónimo** como **habilitado**.

5. Marque la casilla de reglas de **Seguimiento de solicitudes con error**.

6. Asegúrese de que .cer no esté bloqueado.

7. Busque la ubicación del archivo .cer en Internet Explorer desde el servidor local, http://localhost/nombre-certificado.cer. El texto de certificado raíz aparecerá en el explorador Web.

8. Si el certificado raíz no aparece en Internet Explorer, asegúrese de que ASP está habilitado en el servidor IIS, de este modo.

a. Abra Administrador del servidor**.**

b. Vaya al asistente **Administrar** > **Agregar roles y características**.

c. En los roles del servidor, expanda **Servidor web (IIS)**, expanda **Servidor web**, expanda **Desarrollo de aplicaciones** y después seleccione **ASP**.

d. Haga clic en **Siguiente** hasta que se complete la instalación.

9. Abra Internet Explorer y vaya a http://localhost/cert.cer.

Para obtener más información, consulte Internet Information Services (IIS) 8.5.

> **Nota**
>
> Puede usar la instancia de IIS de la CA para este procedimiento.

Importación del certificado raíz durante la configuración inicial de FIPS

Cuando complete los pasos para configurar XenMobile por primera vez en la consola de línea de comandos, debe completar estos parámetros para importar el certificado raíz. Para obtener información detallada sobre los pasos de instalación, consulte Instalación de XenMobile.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Enter HTTP URL to import: http://*Nombre FQDN del servidor IIS*/cert.cer
- Server: *Nombre FQDN del servidor SQL Server*
- Port: 1433
- User name: Cuenta del servicio con capacidad para crear la base de datos (dominio\nombre-de-usuario).
- Password: La contraseña de la cuenta del servicio.
- Database Name: Introduzca el nombre que desee para la base de datos.

Herramienta de actualización de XenMobile 10 MDM

May 05, 2016

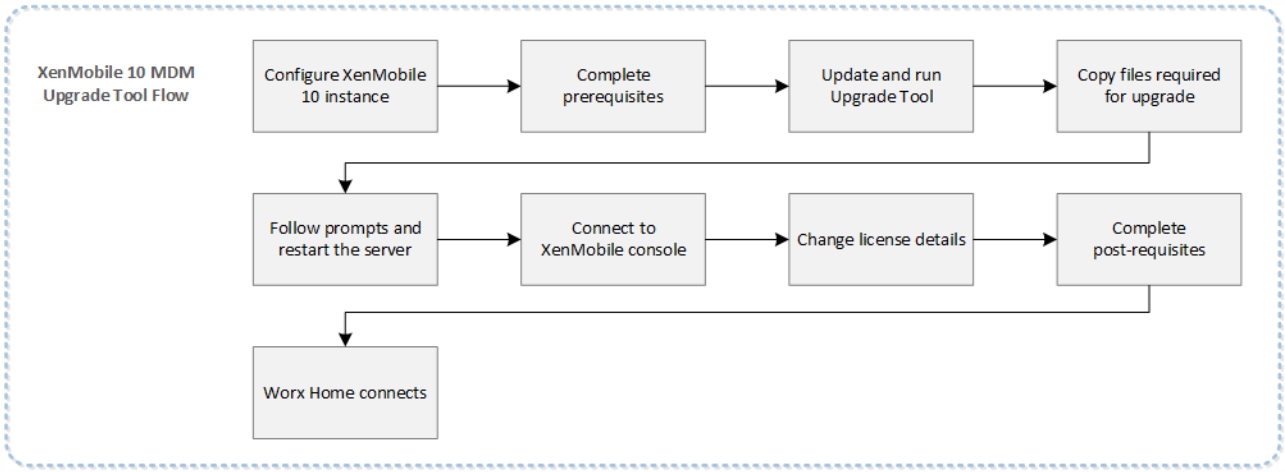
> **Nota**
>
> Citrix recomienda usar la versión más reciente de la herramienta de actualización (Upgrade Tool). Con la versión más reciente, podrá actualizar los modos MAM, MDM y Enterprise del entorno XenMobile 9.0 con una misma herramienta. La herramienta de actualización se encuentra en la página de descargas de Citrix.com.

Utilice la herramienta de actualización Upgrade Tool de XenMobile 10 MDM para actualizar XenMobile 9.0 a XenMobile 10. Esta herramienta se admite para actualizaciones desde implementaciones de la edición XenMobile MDM.

Importante: Esta herramienta no se admite para actualizar desde XenMobile App Edition o XenMobile Enterprise Edition. Asimismo, esta herramienta no se puede utilizar para actualizar XenMobile 8.6 o 8.7 a XenMobile 10. Además, si la consola Multi-Tenant Console (MTC) está habilitada en XenMobile 9.0, no se puede migrar a XenMobile 10.
Si su configuración de XenMobile 9.0 está basada en instancias SQL con nombre, necesita seguir unos pasos específicos. Para obtener más información, consulte Respaldo para instancias de SQL con nombre.

La herramienta de actualización está integrada en la máquina virtual de XenMobile 10. Puede habilitar el asistente de un solo uso mediante la consola de línea de comandos durante la instalación inicial de XenMobile 10.

El diagrama siguiente ilustra los pasos básicos necesarios para la actualización de XenMobile 9.0 a XenMobile 10.



Consulte los Requisitos previos y los Problemas conocidos, antes de iniciar la migración a XenMobile 10.

Acciones de la herramienta de actualización

La herramienta de actualización Upgrade Tool de XenMobile 10 MDM migra los datos de usuario y de configuración desde el servidor XenMobile 9.0 a una nueva instancia de XenMobile 10 con el mismo nombre de dominio completo (FQDN).

Puede optar por probar la actualización o por realizar una actualización completa de producción. Si elige Test Drive en la

herramienta, solo se migrarán los datos de configuración a XenMobile 10; no se migrará ningún dato de dispositivo o de usuario. Esta opción permite comparar XenMobile 9.0 y XenMobile 10 sin consecuencias para su entorno de producción.

Si selecciona Production Upgrade en la herramienta, se migrarán todos los datos de configuración, de dispositivo y de usuario. Al iniciar sesión en la consola de XenMobile 10 después de la actualización, verá todos los datos de usuario y de dispositivo que se han migrado desde XenMobile 9.

Nota: No se trata de una migración en contexto: los datos no se mueven, sino que se *copian* durante la migración a XenMobile 10. Todos los datos en XenMobile 9.0 permanecen intactos hasta que se mueve el servidor XenMobile 10 al entorno de producción. Si, por alguna razón quiere revertir a XenMobile 9.0, los usuarios que se conecten a XenMobile 10 en un entorno de producción deben inscribirse nuevamente en XenMobile 9.0.
Después de una actualización correcta del entorno de producción, para mover XenMobile 10 al entorno de producción en sí, debe llevar a cabo lo siguiente:

1. Actualice la entrada DNS para asignar el nombre de dominio completo (FQDN) de XenMobile 9.0 a la nueva IP del servidor XenMobile 10.
2. Si NetScaler está equilibrando la carga de los servidores XenMobile Device Manager, debe cambiar el servicio de XenMobile 9.0 al servicio de XenMobile 10.

Acciones que no realiza la herramienta de actualización

La siguiente información **no** se migra a XenMobile 10 cuando se usa la herramienta de actualización:

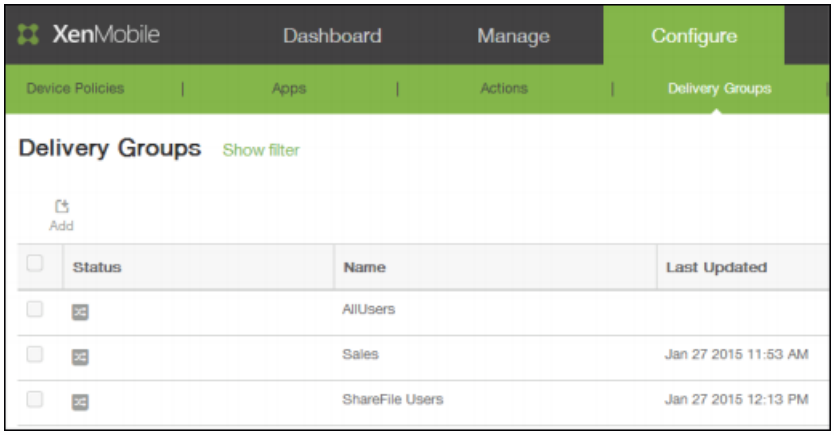
- Información acerca de licencias.
- Datos de informes.
- Acciones automatizadas.
- Directivas de grupo de servidores e implementaciones asociadas.
- Grupo de MSP.
- Directivas y paquetes relacionados con Windows CE y Windows 8.0.
- Paquetes de implementación que no se utilicen; por ejemplo, cuando no hay usuarios ni grupos asignados a un paquete de implementación.
- Cualquier otro dato de configuración o de usuario, según se describe en el archivo migration.log.
- CXM Web (reemplazado por Citrix WorxWeb).
- Directivas DLP (reemplazadas por Citrix ShareFile).
- Atributos personalizados de Active Directory.
- Si ha configurado varias directivas de personalización de marca, la directiva de personalización de marca no se migra. XenMobile 10 admite una directiva de personalización de marca; debe dejar una directiva de personalización de marca en XenMobile 9.0 para migrarla a XenMobile 10.
- Parámetros contenidos en el archivo auth.jsp de XenMobile 9.0 que se usan para restringir el acceso a la consola. En XenMobile 10, las restricciones de acceso a la consola son parámetros del firewall que se pueden configurar en la interfaz de línea de comandos.

Además, tenga en cuenta los cambios siguientes con XenMobile 10:

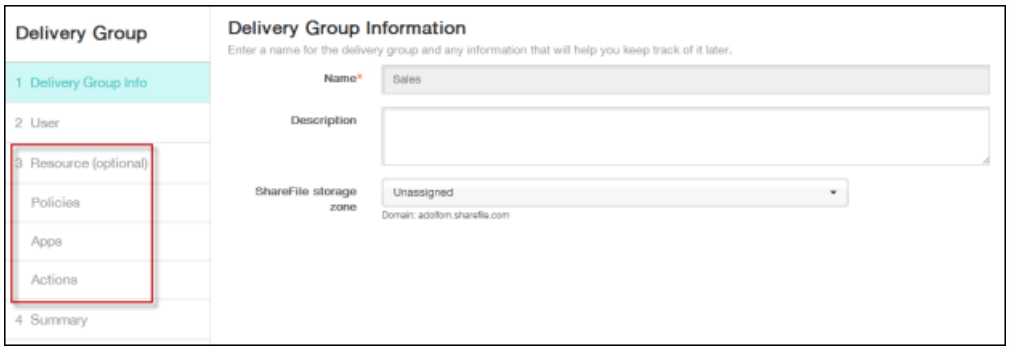
- XenMobile 10 no admite usuarios de Active Directory asignados a grupos locales.
- La jerarquía de los grupos locales se reduce.

Cambios terminológicos en XenMobile 10

Tenga en cuenta que, después de la actualización, los paquetes de implementación de Device Manager se conocen como grupos de entrega, como se muestra en la siguiente ilustración. Para obtener más información, consulte Administración de grupos de entrega.



En el grupo de entrega, puede ver directivas de MDM, acciones y aplicaciones necesarias para el grupo de usuarios que requieren los recursos.

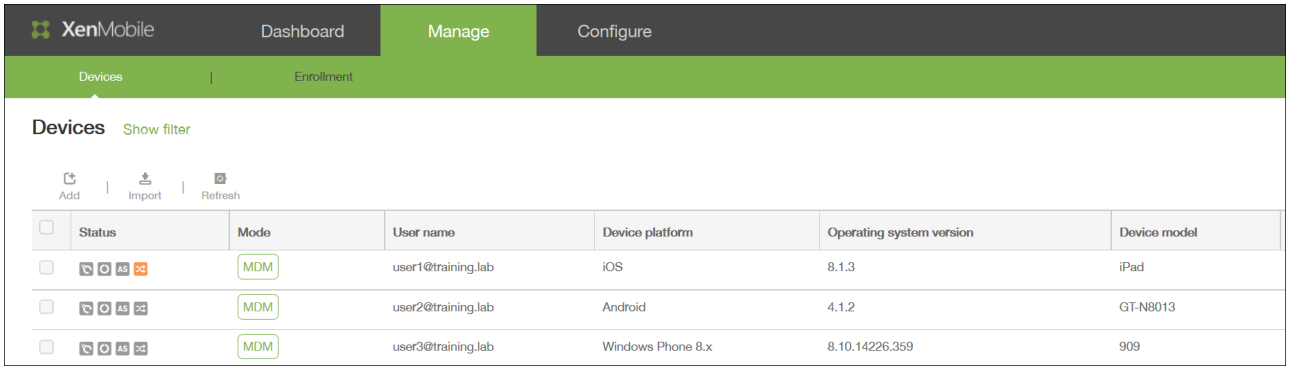


Inscripción de dispositivos después de la actualización

Los usuarios no necesitan volver a inscribir sus dispositivos después de actualizar a XenMobile 10. Los dispositivos deben poder conectar automáticamente con el servidor XenMobile 10 según el intervalo de latido.

Si quiere conectar un dispositivo a XenMobile 10 de forma inmediata, en el dispositivo, utilice WorxHome > Información del dispositivo > Actualizar directiva.

Una vez que los dispositivos de usuario se hayan conectado, compruebe que se ven en la consola de XenMobile, tal y como se muestra en la siguiente ilustración.



Requisitos previos

May 05, 2016

Debe cumplir los siguientes requisitos previos antes de ejecutar la herramienta de actualización Upgrade Tool de XenMobile 10 MDM.

Citrix License Server

Compruebe que se instala la versión 11.12.1 del servidor de licencias de Citrix (disponible en la página Citrix Licensing) y que configura el servidor con la licencia V6 pura de MDM más reciente. Compruebe que los puertos del servidor de licencias 27000 y 7279 están abiertos para el servidor. Este paso es fundamental para evitar la actualización accidental de los dispositivos de los usuarios al modo XenMobile Enterprise, lo que puede dar lugar a una infracción de licencias y obligar a los usuarios a volver a inscribir sus dispositivos.

Base de datos

La migración solo se puede realizar entre bases de datos del mismo tipo. Por ejemplo:
Respaldado

- De PostgreSQL a PostgreSQL
- De MSSQL a MSSQL

Sin respaldo

- De MSSQL a PostgreSQL
- De PostgreSQL a MSSQL

Durante el proceso de migración de datos, XenMobile necesita la capacidad de acceder a la solución de base de datos implementada en XenMobile 9.0 Device Manager. Por ejemplo, los siguientes puertos deben estar abiertos:

- Para Microsoft SQL Server, el puerto predeterminado es 1433.
- Para PostgreSQL, el puerto predeterminado es 5432.

Para permitir conexiones remotas a PostgreSQL, debe llevar a cabo los siguientes pasos:

1. Abra el archivo pg_hba.conf y busque la línea siguiente: "host all all 127.0.0.1/32 md5"
2. Añada una nueva línea de host all all [direcciónXMS/dirección externa]/32 md5
3. Guarde el archivo.
4. Detenga y vuelva a iniciar el servicio.
5. Busque y abra el archivo postgresql.conf y cambie la línea:
   "#listen_addresses = 'localhost'"

   por

   "listen_addresses = '*'"

   Nota: La línea debe figurar sin marca de comentario. Esto se puede restringir permitiendo que solo las direcciones IP de los servidores XenMobile 9.0 y XenMobile 10 puedan acceder a la base de datos PostgreSQL (listen_addresses = '10.x.x.1,10.x.x.2').
6. Detenga y reinicie el servicio de PostgreSQL para que los cambios surtan efecto.
7. Asegúrese de que XMS y la base de datos pueden comunicarse entre sí. (Esto también comprueba que la base de datos

puede aceptar conexiones remotas).

Si se ha asignado un puerto personalizado a la solución de base de datos, debe comprobar que ese puerto consta como permitido y abierto en el firewall que protege la versión 9.0 de XenMobile Device Manager. De esta manera, XenMobile 10 puede conectarse a la base de datos y migrar la información pertinente.

Certificado SSL externo

Los certificados SSL externos deben cumplir las condiciones que se describen en How to Configure an External SSL Certificate. No olvide consultar el archivo pki.xml antes de iniciar la migración para garantizar que el certificado SSL cumple esas condiciones.

Cuenta de administrador Nombre de usuario

La cuenta de administrador que se utiliza para iniciar sesión en la consola de XenMobile 10 solo puede contener letras en minúscula. Por tanto, no podrá iniciar sesión en la consola de XenMobile 10 después de la migración si la cuenta contiene letras en mayúscula. Cree una cuenta de usuario de administrador que contenga solo letras en minúscula y que tenga todos los permisos habilitados para que, después de la migración, pueda usar esa cuenta para iniciar sesión en la consola de XenMobile 10.

Nombres de paquetes de implementación con caracteres especiales

Los nombres de los paquetes de implementación presentes en XenMobile 9.0 que contienen caracteres especiales (!, $, (), #, % , +, *, ~, ?, |, {}, y []) se migran, pero los grupos de entrega en XenMobile 10 no se pueden modificar después de la migración. Además, los usuarios locales y los grupos locales creados en XenMobile 9.0 que contienen un corchete de apertura ([) causan problemas en XenMobile 10 cuando se crean invitaciones de inscripción. Antes de proceder a la migración, quite todos los caracteres especiales de los nombres de los paquetes de implementación, así como corchetes de apertura que estén presentes en los nombres de usuarios y grupos locales .

Copiar archivos de XenMobile 9.0 Device Manager

Si Device Manager está instalado en la ubicación predeterminada (C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager\tomcat), copie los siguientes archivos a una carpeta temporal:

De la carpeta C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager\tomcat\conf:

- server.xml
- https.p12
- cacerts.pem.jks
- pki-ca-root.p12
- pki-ca-devices.p12
- pki-ca-servers.p12

Nota: Si se han utilizado certificados SSL de servidor (.p12) personalizados en el servidor con Device Manager, compruebe que copia el certificado en lugar de https.p12 a la carpeta temporal.
Desde la carpeta C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager\tomcat\webapps\zdm\WEB-INF\classes\, copie los siguientes archivos a la misma carpeta temporal:

- ew-config.properties
- pki.xml
- variables.xml

Después de copiar todos los archivos mencionados, abra la carpeta temporal y comprímalos; no comprima la carpeta, solo

los archivos. Los archivos comprimidos se cargarán durante la actualización.

Tras familiarizarse con los problemas conocidos y cumplir todos los requisitos previos, inicie la actualización. Para obtener más información, consulte Cómo habilitar y ejecutar la herramienta de actualización Upgrade Tool de XenMobile 10 MDM

Problemas conocidos

May 05, 2016

A continuación, se describen los problemas conocidos de la herramienta de actualización de XenMobile 10 MDM:

- El valor del límite de bloqueo de XenMobile no se migra. Después de la migración, restablezca ese valor. [#545770]
- Las opciones de los roles relativos al control de acceso basado en roles (RBAC) no se migran correctamente. Después de la migración, revise los roles de RBAC y realice los ajustes necesarios. [#543183]
- Los parámetros de registro no se migran. Después de la migración, vuelva a configurar los parámetros de registro en la consola de XenMobile. [#541869]
- En una configuración con varias configuraciones de protocolos LDAP, de las cuales se migra solo una para respaldar grupos anidados, después de la migración, el respaldo a grupos anidados está habilitado en todos los protocolos LDAP configurados. Además, la sincronización de grupos se produce en todos los servidores LDAP durante el inicio de los servidores. [#540713]
- Cuando una directiva de filtro de contenidos Web contiene direcciones URL sin HTTP o HTTPS, la URL se elimina si los usuarios la modifican y, luego, cancelan la operación. Después de la migración, compruebe que todas las direcciones URL contengan HTTP o HTTPS para evitar su eliminación al cancelar una operación de modificación. [#540025]
- Si las directivas, aplicaciones o acciones están incluidas en varios paquetes con diferentes reglas, las reglas de implementación no se migran. Este comportamiento es el esperado. [#539517]
- El administrador de XenMobile 9.0 no puede iniciar sesión en la consola de XenMobile 10 después de la migración si el nombre de usuario del administrador contiene mayúsculas. Antes de la migración, cree una cuenta de usuario de administrador que contenga solo letras en minúscula y que tenga todos los permisos habilitados, para que después de la migración pueda usar esa cuenta para iniciar sesión en la consola de XenMobile 10. [#547422]
- Si la consola Multi-Tenant Console (MTC) está habilitada en XenMobile 9, no se puede migrar a XenMobile 10. [#549969]
- El rol de superadministrador creado en XenMobile 9.0 no migra varios permisos de configuración y asignación a XenMobile 10. Después de la migración, en la consola de XenMobile 10, vaya a Configure > Settings > Role Based Access Control y vuelva a crear el rol de superadministrador de XenMobile 9.0 con permisos del rol de administrador de XenMobile 10. [#553079]

- Los nombres de los paquetes de implementación creados en XenMobile 9.0 con caracteres especiales (:, !, $, (), #, % , +, *, ~, ?, |, {}, and []) no se pueden modificar después de la migración. Además, los usuarios locales y los grupos locales creados en XenMobile 9.0 que contienen un corchete de apertura ([) causan problemas en XenMobile 10 cuando se crean invitaciones de inscripción. Antes de proceder a la migración, quite todos los caracteres especiales de los nombres de los paquetes de implementación, así como corchetes de apertura que estén presentes en los nombres de usuarios locales y grupos locales. [#538639]

Cómo habilitar y ejecutar la herramienta de actualización Upgrade Tool de XenMobile 10 MDM

May 05, 2016

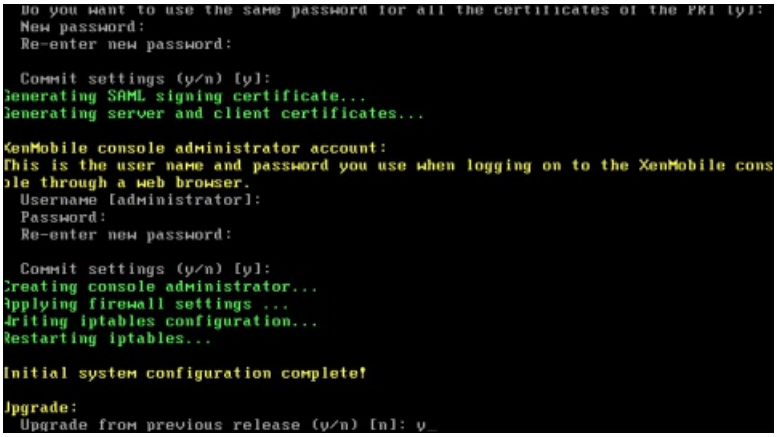
A continuación, se presentan los pasos básicos a seguir para actualizar XenMobile 9.0 a XenMobile 10:

1. Configure la instancia de XenMobile 10 mediante la consola de línea de comandos.
2. Cumpla todos los requisitos previos de la herramienta de actualización. Para obtener más información, consulte Prerequisites.
3. Actualice la herramienta de actualización a la versión más reciente.
   Importante: Borre la memoria caché del explorador Web tras reiniciar el sistema.
4. Inicie la herramienta de actualización en Firefox o Chrome.
5. Cargue los archivos copiados de XenMobile 9.0 en la herramienta de actualización.
6. Escriba la contraseña del certificado de XenMobile 9.0.
7. Permita la ejecución de la herramienta de actualización.
8. Reinicie el servidor XenMobile 10.
9. Inicie sesión en la consola de XenMobile 10.
10. Configure las licencias en XenMobile 10 para permitir las conexiones de los usuarios.
11. Para una actualización de producción, cambie el DNS externo para que XenMobile apunte al nuevo servidor XenMobile 10.
12. Para realizar una actualización de producción, si está utilizando un dispositivo NetScaler de equilibrio de carga, quite la dirección IP del servidor XenMobile 9.0 y agregue la dirección IP del servidor XenMobile 10.

Para instalar una instancia de XenMobile 10 y habilitar la herramienta de actualización Upgrade Tool

Puede habilitar la herramienta de actualización mediante la consola de línea de comandos durante la instalación inicial de XenMobile 10, como se muestra en la siguiente ilustración.

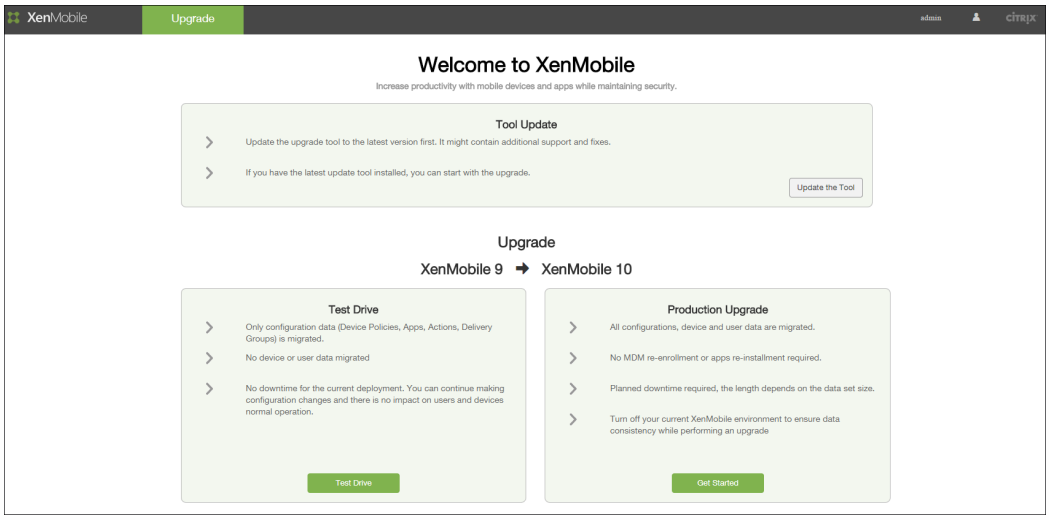
Importante: Si quiere tomar una instantánea del sistema, hágalo después de la configuración inicial de XenMobile 10 y *antes* de acceder a la herramienta de actualización.



Si escribe **y** para actualizar, XenMobile 10 habilita la herramienta de actualización de un solo uso. A continuación, puede acceder a la herramienta de actualización a través de https:///uw/.

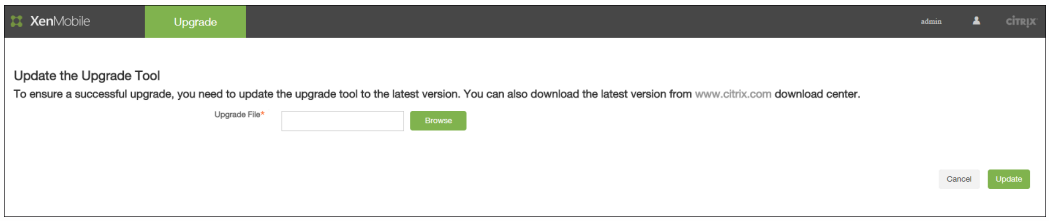
Sugerencia: Citrix recomienda utilizar Firefox o Chrome para acceder a la herramienta de actualización; Internet Explorer no

se recomienda.
Al migrar al nuevo servidor, compruebe que el nombre de host del nuevo servidor se corresponde con el nombre de host del servidor desde el que está migrando. Si se corresponden, Worx Home se puede conectar a XenMobile 10 con el mismo nombre de host que el que usaba para conectarse a XenMobile 9.0. De esta forma, los usuarios no necesitan volver a inscribirse en XenMobile 10.



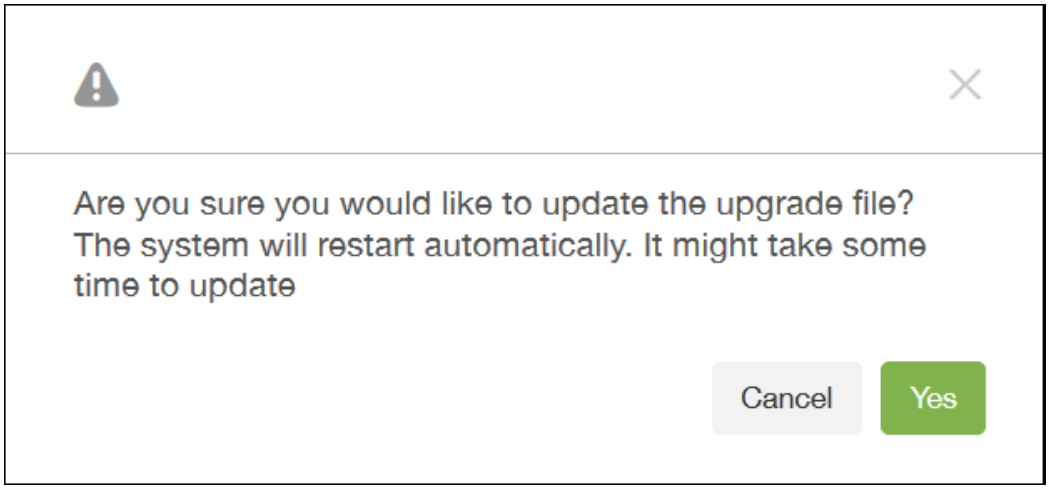
Para actualizar la herramienta de actualización e iniciar la migración

Las actualizaciones de la herramienta de actualización se encuentran en la página de descarga de XenMobile. Para las migraciones de MDM, debe usar la versión más reciente de la herramienta descargable de Citrix.com.



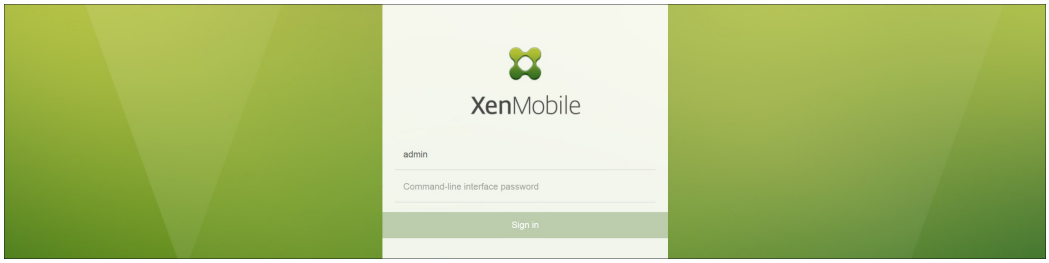
Aparecerá el siguiente mensaje para confirmar el inicio del proceso de actualización.

Nota: Después de hacer clic en Yes, no habrá ningún indicador visual del progreso, pero verá en la interfaz de línea de comandos cuándo se reiniciará el sistema. La actualización debería tardar aproximadamente 30 segundos.

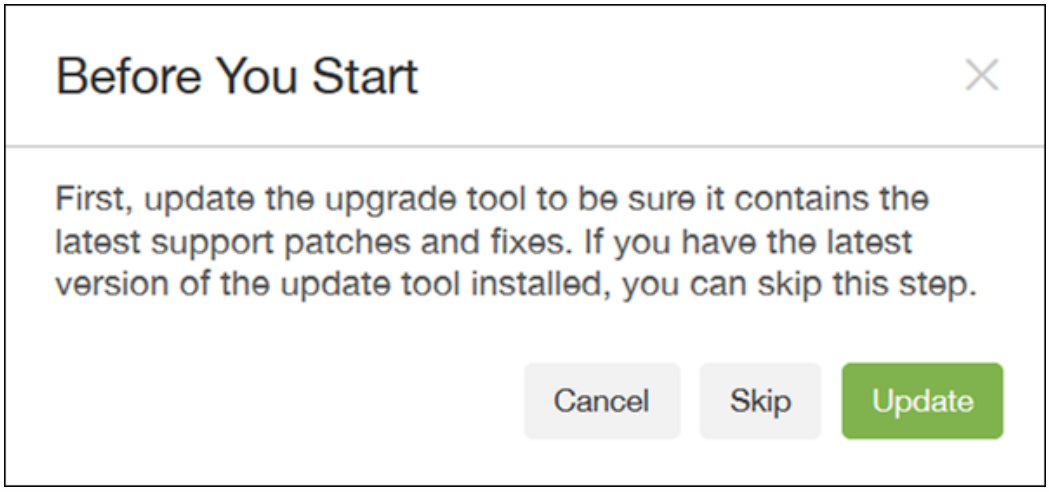


Nota:

- Tras reiniciarse el sistema, borre la memoria caché del explorador Web antes de acceder de nuevo a la URL de la herramienta de actualización: https:///uw.
- Si no utiliza el puerto predeterminado para la comunicación HTTPS (443), la URL de la herramienta de actualización es: https://:/uw.



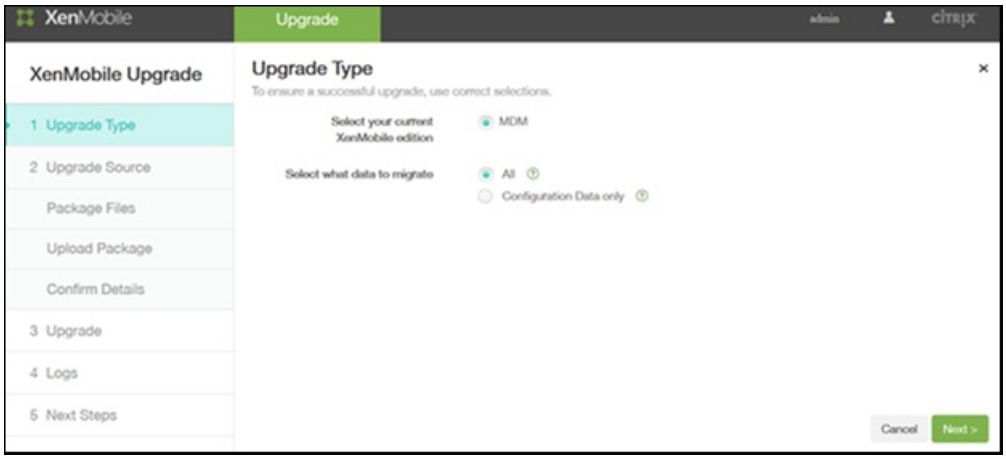
Después de iniciar sesión en la herramienta de actualización, en este caso, puede hacer clic en **Skip** porque ya habrá actualizado la herramienta de actualización.



Seleccione Test Drive o Production Upgrade y continúe con la migración.

Cuando la herramienta de actualización se inicie, puede optar por migrar todos los datos o solamente los datos de configuración. Si selecciona Configuration Data only, los usuarios deberán inscribir nuevamente sus dispositivos. Haga clic en

Next para cargar los archivos que ha copiado y comprimido como requisito previo en la carpeta temporal.

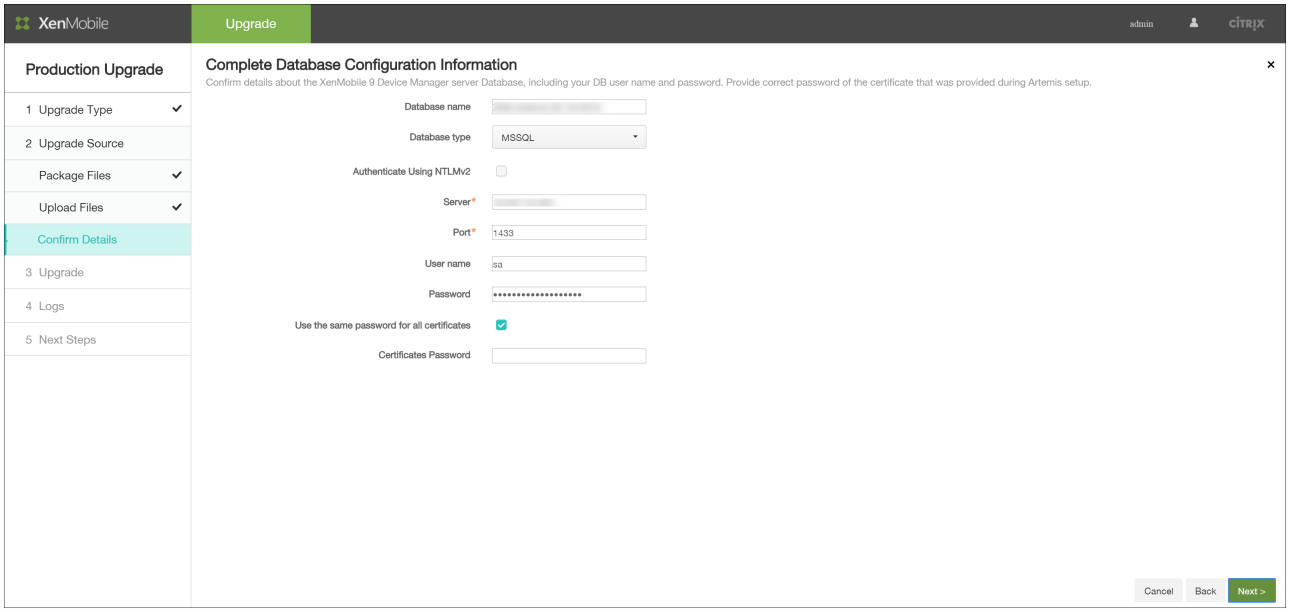


Haga clic en Next cuando se complete la carga.

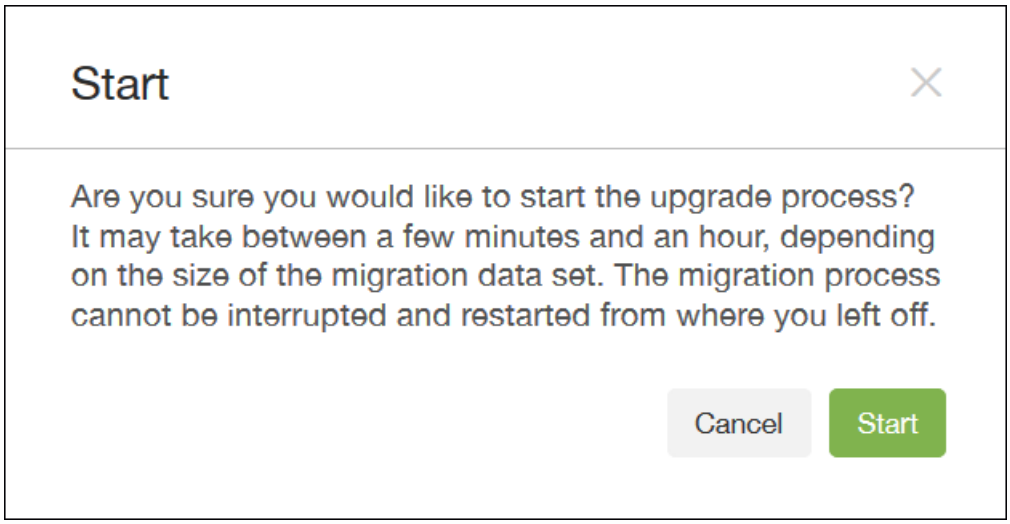
Al migrar una base de datos PostgreSQL, si el nombre del servidor es "localhost", debe cambiar "localhost" a la dirección IP del servidor.

Confirme que la información recopilada de XenMobile 9.0 Device Manager es correcta. También debe introducir la contraseña del certificado.

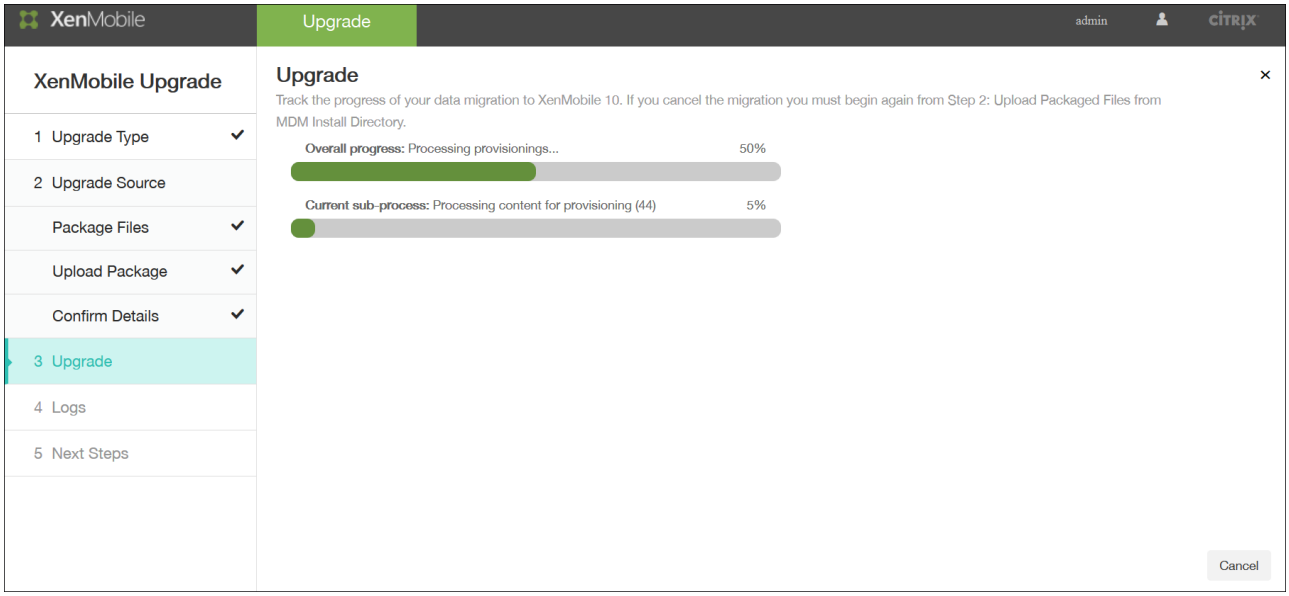
Importante: Todas las contraseñas de los certificados deben escribirse correctamente. De lo contrario, la migración no se producirá.

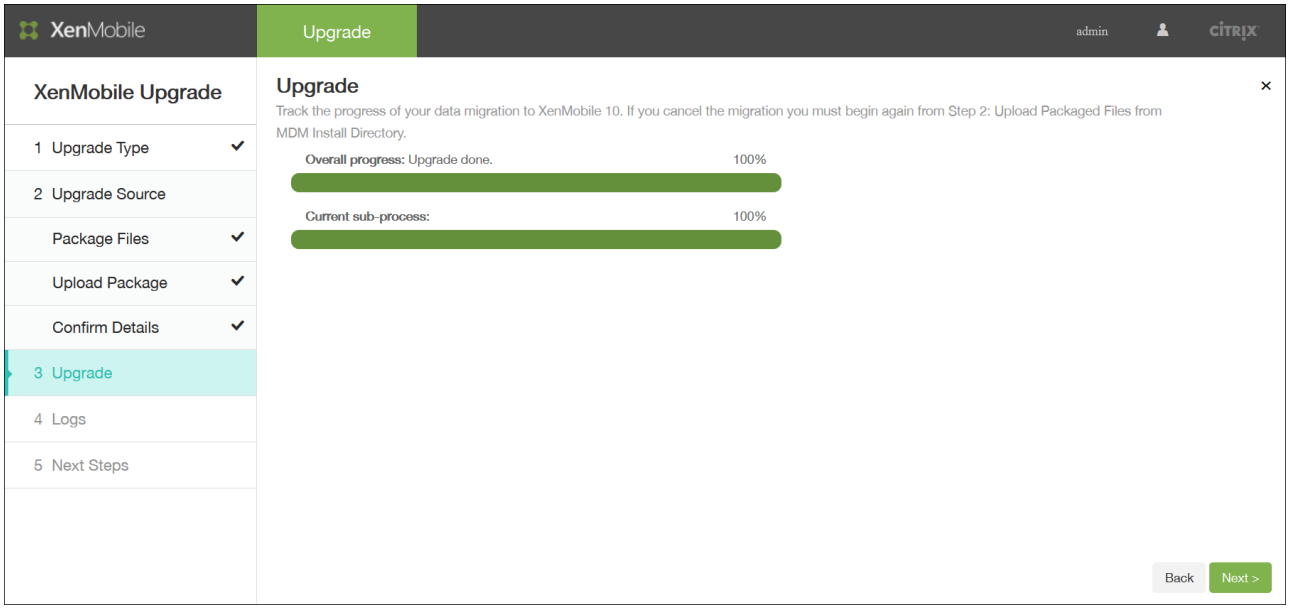


Al hacer clic en Next, aparecerá el siguiente mensaje de confirmación.



A continuación, la página Upgrade muestra indicadores de progreso para un seguimiento de la migración de datos desde XenMobile 9.0.



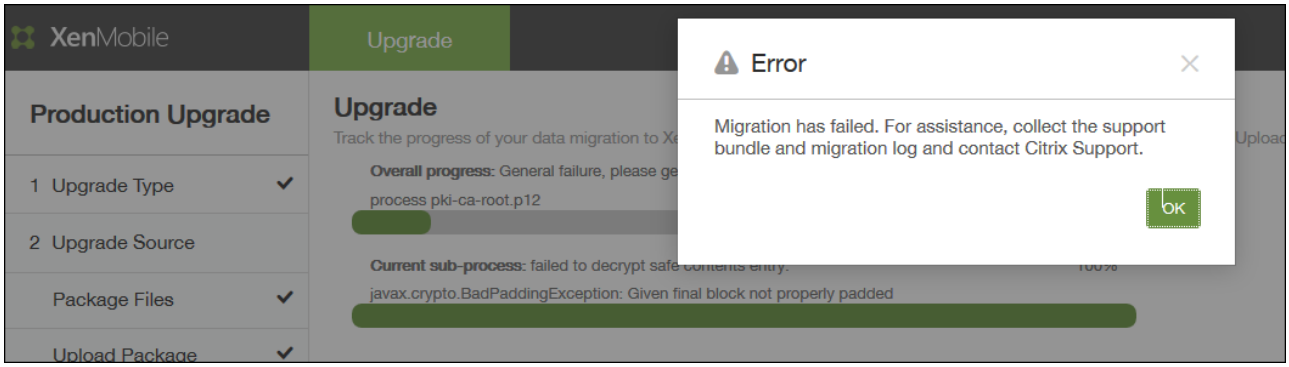


Si no ha copiado todos los archivos necesarios de Device Manager a la carpeta ZIP, la herramienta de actualización muestra los archivos que faltan. La herramienta reanuda el proceso después de agregar los archivos necesarios.

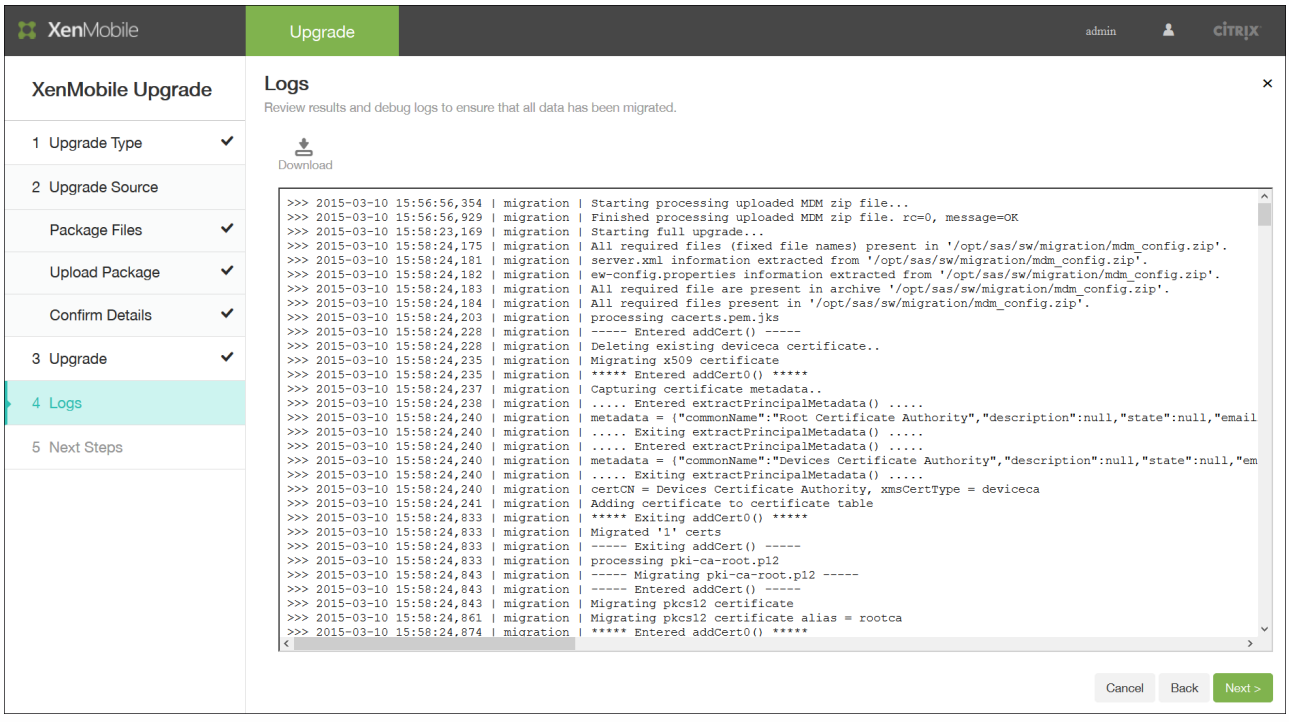
Si no puede resolver un problema que surja, aparecerá un mensaje de error que le pedirá generar un paquete de asistencia de XenMobile, recopilar el registro de migración y ponerse en contacto con el servicio de asistencia técnica de Citrix.

Nota:

- Si la migración falla, debe importar una nueva instancia de XenMobile 10 y, a continuación, reiniciar la migración.
- Una vez completada la migración (ya sea correcta o no), no podrá usar el botón Atrás para corregir la información. Deberá importar una nueva instancia de XenMobile 10 y reiniciar la migración.



Después de actualizar a XenMobile 10, la herramienta de actualización de XenMobile proporciona un archivo de registro (migration.log) para descargarlo y revisarlo, tal y como se muestra en la siguiente ilustración. Citrix recomienda que revise el archivo para determinar las directivas, las configuraciones y los datos de usuario, entre otros, que se han migrado o no a XenMobile 10.



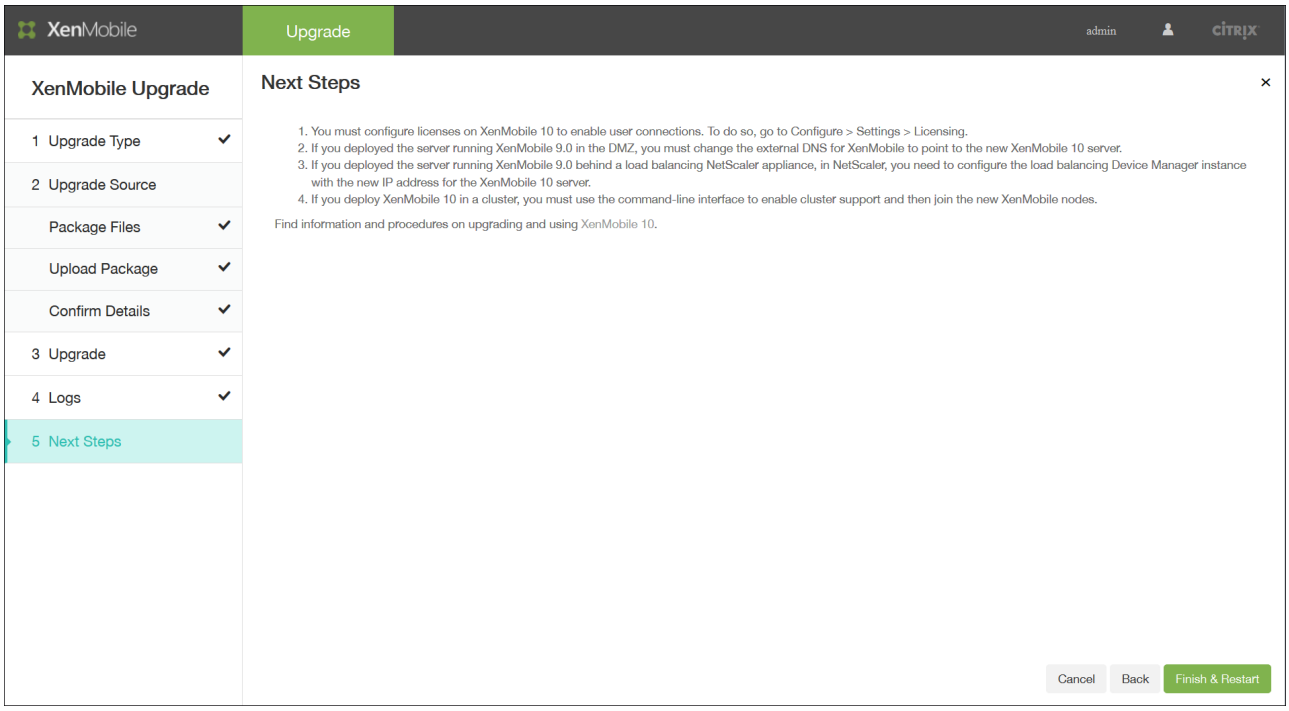
Después de descargar y revisar los registros de migración, haga clic en Next para ir a Next Steps. Para ver detalles, consulte Requisitos posteriores de la herramienta de actualización.

Requisitos posteriores de la herramienta de actualización

May 05, 2016

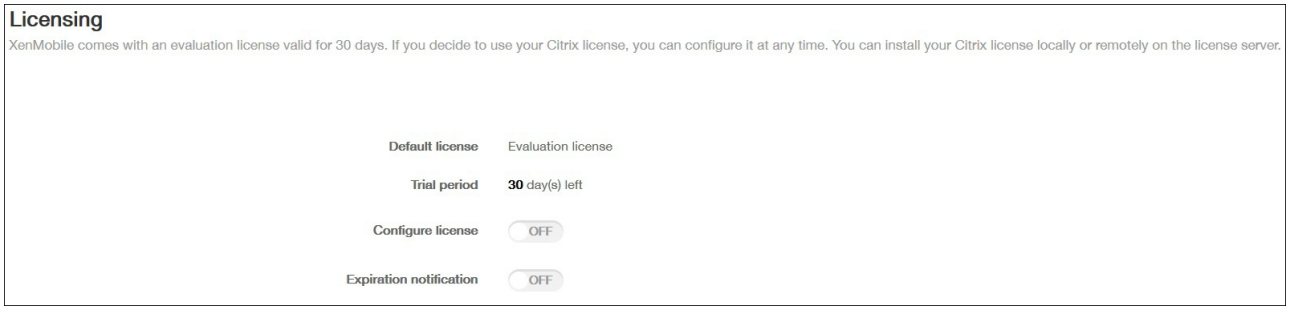
Después de la actualización, compruebe que se cumplen los siguientes requisitos posteriores; algunos de estos también aparecen en la última pantalla de la herramienta de actualización. Cuando haga clic en Finish & Restart, se reinicia el servidor.

Nota: Inicie sesión en la consola de XenMobile mediante https://:4443 con las credenciales de administrador.



Licencias

XenMobile 10 solo admite el sistema de licencias de Citrix V6. Defina la configuración de licencias locales o remotas en la consola de XenMobile como se muestra en la siguiente ilustración y descargue el archivo de licencia desde Citrix Licensing. Para obtener más información, consulte el apartado Licencias para XenMobile.



Debe configurar licencias en XenMobile 10 para habilitar las conexiones de usuario. Para ello, vaya a **Configure** > **Settings** > **Licensing**. En el caso de un servidor independiente con XenMobile 10, puede cargar la licencia pura de MDM en la consola de XenMobile.

DNS

Nota: Este requisito posterior es necesario para la actualización de producción. Si ha implementado el servidor con XenMobile 9.0 en la zona desmilitarizada (DMZ), debe cambiar el DNS externo para que XenMobile apunte al nuevo servidor XenMobile 10.

Dirección IP de NetScaler para el equilibrio de carga

Nota: Este requisito posterior es necesario para la actualización de producción. Si ha implementado el servidor con XenMobile 9.0 tras un dispositivo NetScaler de equilibrio de carga, debe configurar la instancia de Device Manager del equilibrio de carga en NetScaler con la nueva dirección IP para el servidor XenMobile 10.

Agrupación en clústeres

Si implementa XenMobile 10 en un clúster, debe usar la interfaz de línea de comandos para habilitar el respaldo de clústeres y unir los nuevos nodos de XenMobile. Puede volver a utilizar las direcciones IP de nodos de XenMobile 9.0 si configura la nueva instancia de XenMobile 10 con la misma dirección IP y la une al nodo Admin o al más antiguo.

Cómo actualizar información que no se ha migrado

Actualice lo siguiente según sea necesario:

- Acciones automatizadas
- Directivas de grupo de servidores e implementaciones asociadas
- Grupo de MSP
- Atributos personalizados de Active Directory
- Valor de límite de bloqueo de XenMobile
- Roles de RBAC
- Parámetros de registro
- Direcciones URL sin HTTP ni HTTPS
- Datos de configuración o de usuario que contenga el archivo migration.log

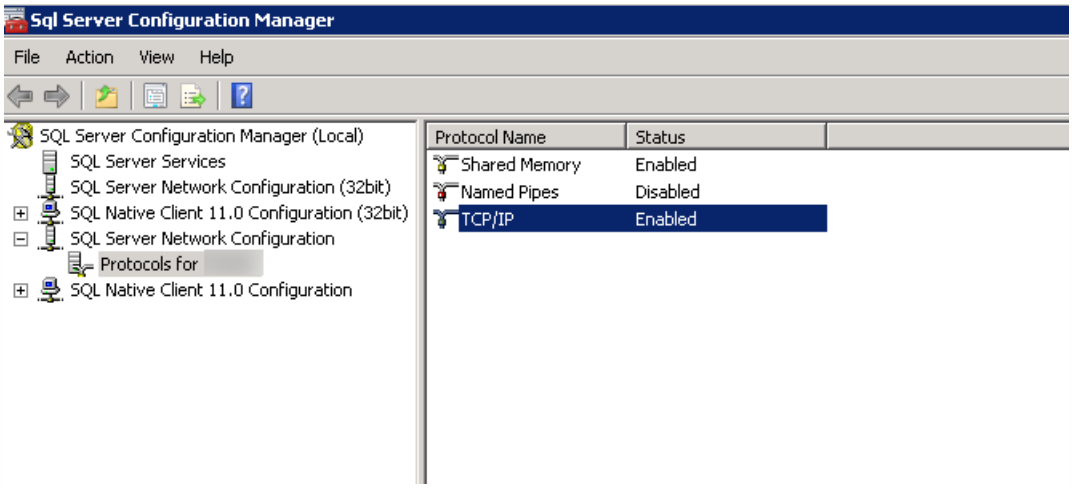
Respaldo para instancias de SQL con nombre

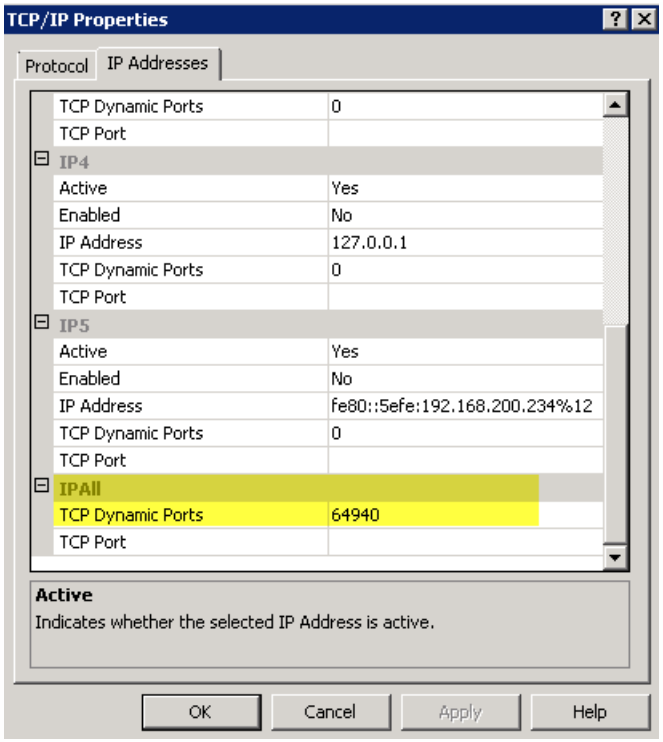
May 05, 2016

Puede usar Upgrade Tool para actualizar el producto desde XenMobile 9 a XenMobile 10 y desde XenMobile 9 a XenMobile 10.1. Si su configuración de XenMobile 9 está basada en instancias SQL con nombre, necesita seguir unos pasos específicos. Si el entorno de XenMobile 9 cumple los requisitos siguientes, siga los pasos indicados en este artículo para llevar a cabo la actualización.

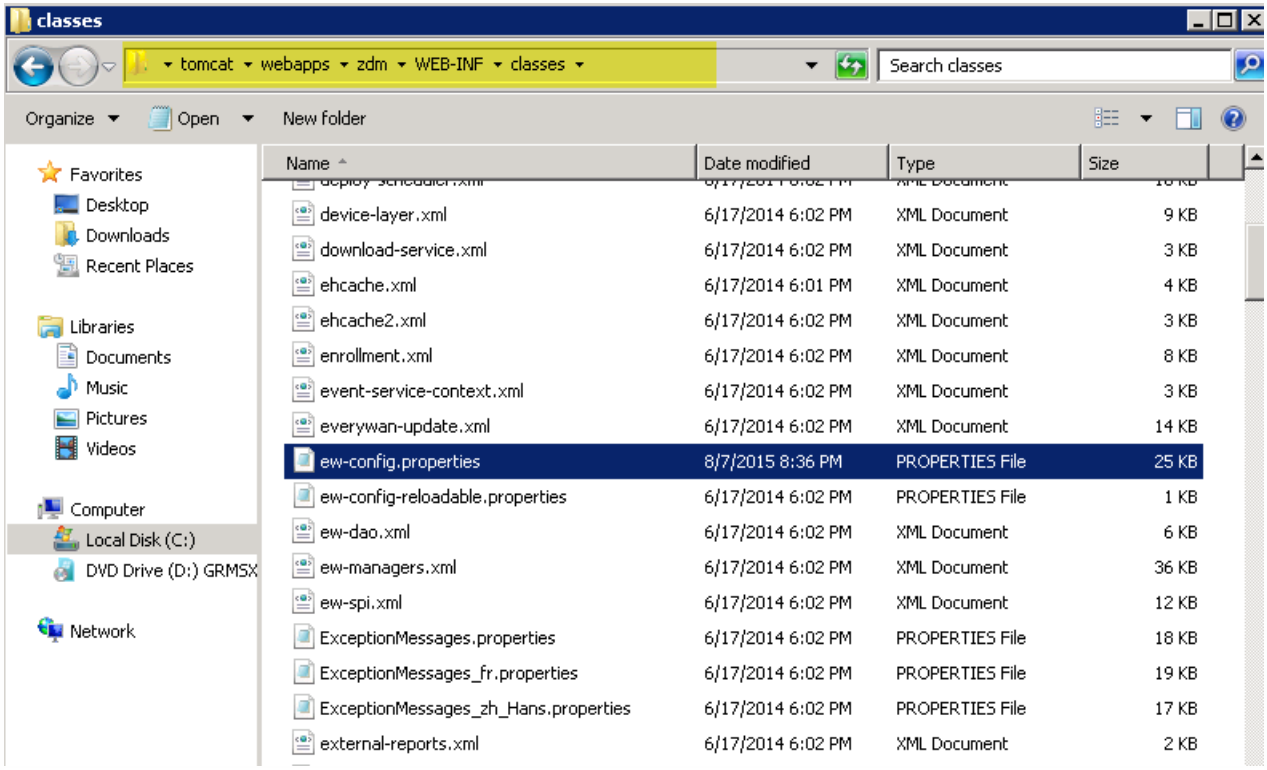
- XenMobile 9 MDM Edition o Enterprise Edition configurados con una base de datos SQL Server externa.
- Una base de datos SQL Server ejecutándose en una instancia no predeterminada con nombre.
- La instancia SQL Server con nombre escucha en un puerto TCP estático o dinámico. Puede verificar este requisito consultando las direcciones IP del protocolo TCP/IP de la instancia con nombre, como se ven en las siguientes imágenes.

> ## Nota
>
> Citrix recomienda que la instancia de la base de datos de SQL Server se ejecute siempre en un puerto estático, porque el servidor XenMobile necesita acceso continuo a la base de datos. Esta conexión, por lo general, atraviesa un firewall. Como resultado de ello, necesita abrir el puerto correspondiente en el firewall; por lo tanto, necesita tener la instancia de la base de datos ejecutándose en un puerto estático.





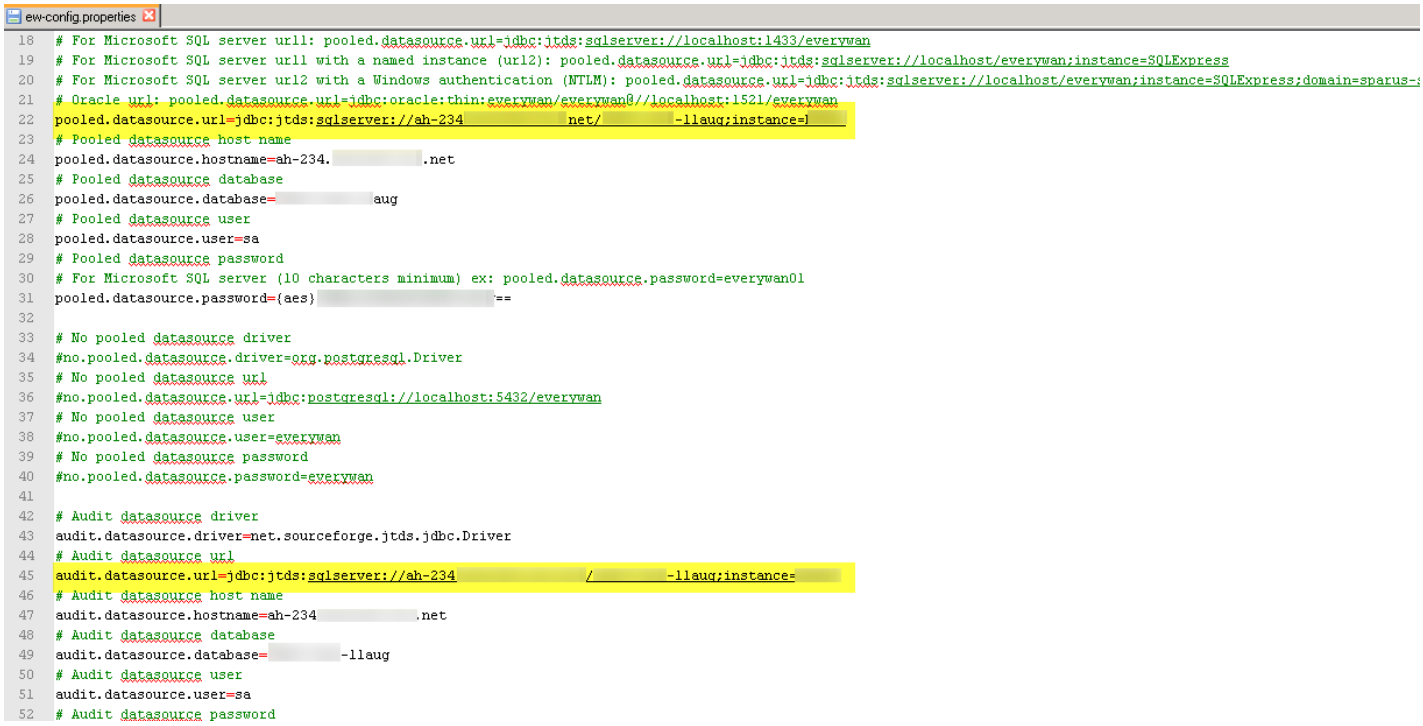
1. Vaya al directorio de instalación de Device Manager y abra el archivo ew-config.properties. Este se encuentra en tomcat\webapps\zdm\WEB-INF\classes.



2. En el archivo ew-config.properties, busque las siguientes URL en la sección DATASOURCE Configuration:

pooled.datasource.url= jdbc:jtds:sqlserver:///;instance=

audit.datasource.url= jdbc:jtds:sqlserver:///;instance=



3. Quite el nombre de la instancia en las direcciones URL anteriores y añada el puerto junto con el nombre de dominio completo (FQDN) del servidor SQL Server. En este caso, el puerto necesario es el 64940:

pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

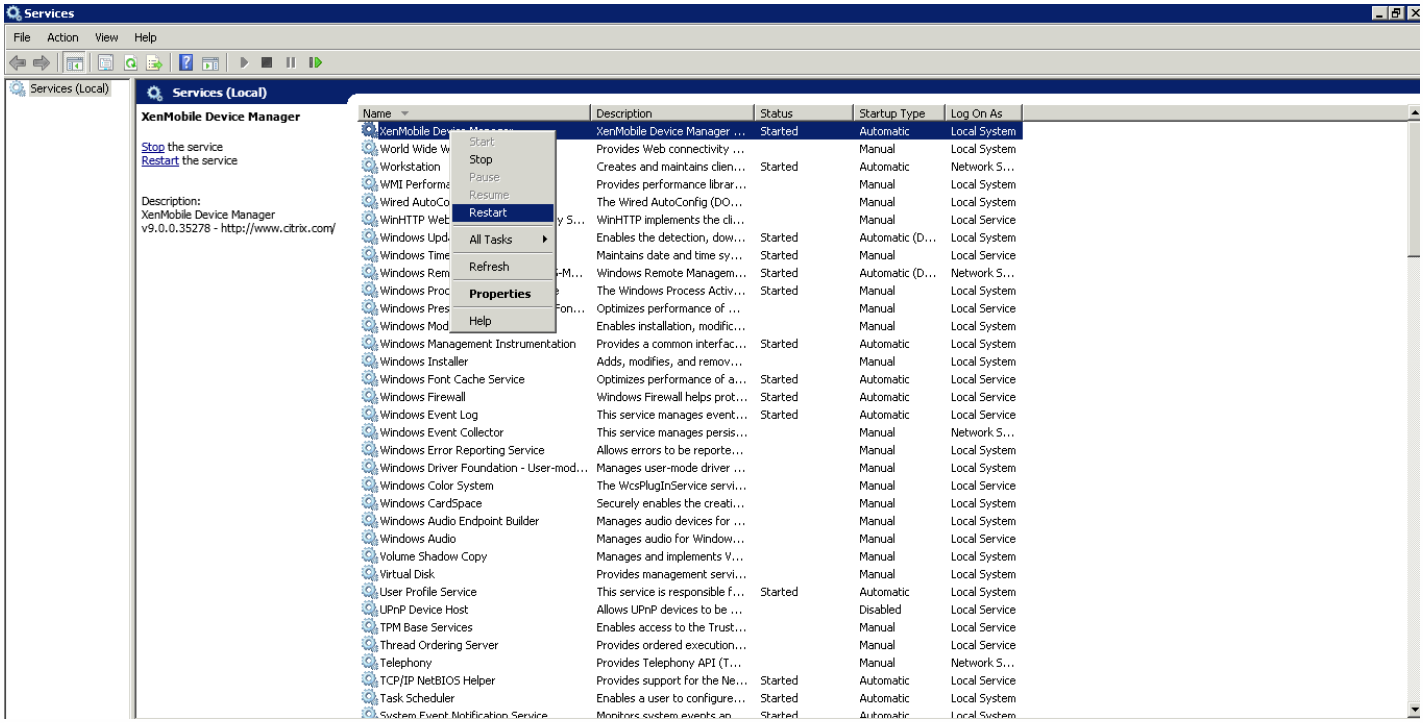
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

> ## Nota
>
> Citrix recomienda hacer una copia de seguridad, copiar, o tomar nota de los cambios realizados en el archivo ew-config.properties. Esta información puede servir de ayuda en caso de que falle la migración.

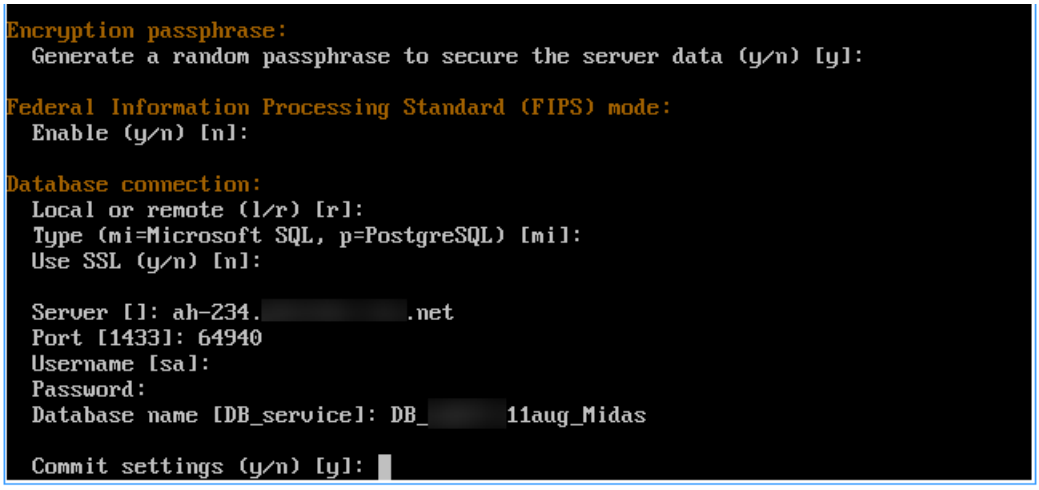
ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.                net:                -llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          -llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                    ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://                -inc.net:                -llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.          .net
# Audit datasource database
audit.datasource.database=          -llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

4. Reinicie el servicio de Device Manager. Actualice la vista de las conexiones de dispositivos cuando vuelva a la instancia de Device Manager.



5. Determine si el nuevo servidor XenMobile 10 también necesita funcionar con la instancia SQL con nombre. En ese caso, identifique el puerto en el que se está ejecutando la instancia con nombre. Si se trata de un puerto dinámico, Citrix recomienda convertirlo a un puerto estático; a continuación, configure el puerto estático en el nuevo servidor XenMobile durante la configuración de la base de datos.



6. Siga los pasos indicados en estos artículos para continuar la actualización del entorno de XenMobile:

- Para realizar una actualización desde XenMobile 9.0 App Edition o Enterprise Edition a XenMobile 10.1, utilice la herramienta de actualización Upgrade Tool de XenMobile Server App Edition y Enterprise Edition. Para obtener más información, consulte Cómo habilitar y ejecutar la herramienta de actualización Upgrade Tool de XenMobile 10.1
- Para actualizar solo desde XenMobile 9.0 MDM Edition a XenMobile 10.1, consulte Herramienta de actualización de XenMobile 10 MDM.

Actualización de XenMobile en la consola de XenMobile

May 05, 2016

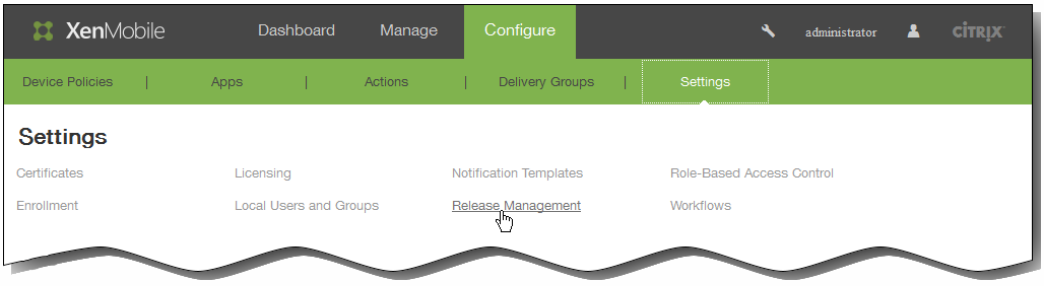
Cuando estén disponibles nuevas versiones del software de XenMobile, podrá realizarse la actualización a la nueva versión. En la consola de XenMobile, puede utilizar la página Release Management para instalar nuevos Service Packs, nuevas revisiones del sistema y nuevas versiones del software de XenMobile.

Nota: Cuando hay disponibles nuevas versiones o actualizaciones importantes, se publican en Citrix.com y se envía un aviso al contacto registrado de cada cliente.

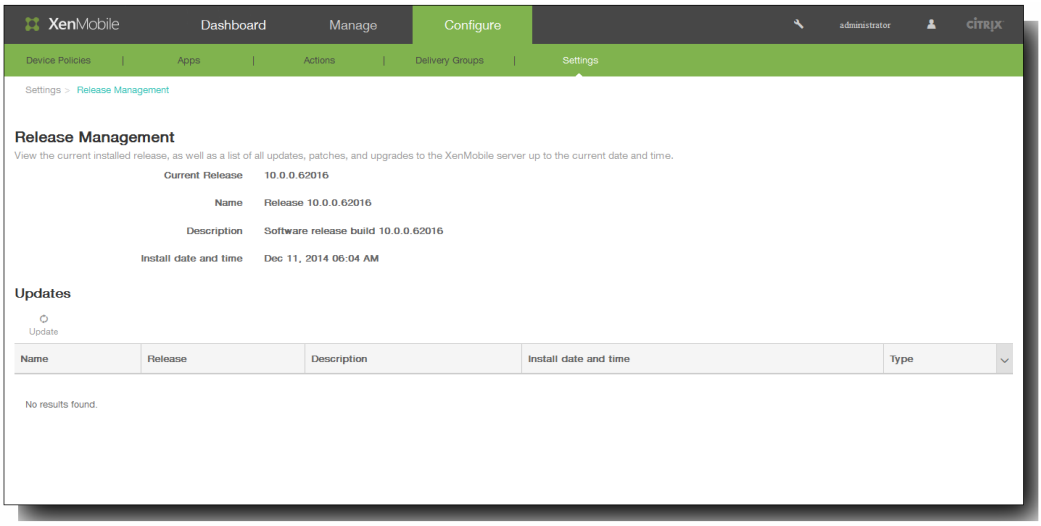
Importante:

- Antes de instalar una actualización de XenMobile, utilice las instalaciones de la máquina virtual (VM) para tomar una instantánea del sistema.
- Realice una copia de seguridad de la base de datos de configuración del sistema.
- Si ha habilitado la atestación de Samsung KNOX en el servidor de MDM y va a actualizar a XenMobile 10.0, debe agregar los nuevos dominios de atestación de KNOX personalizados antes de la actualización. Para obtener más información acerca de la habilitación de la atestación de Samsung KNOX, consulte Samsung KNOX. Los nuevos dominios de atestación son:
  - Región de China: china-attest-api.secb2b.com.cn
  - Región de Europa: eu-attest-api.secb2b.com
  - Región de EE. UU.: us-attest-api.secb2b.com

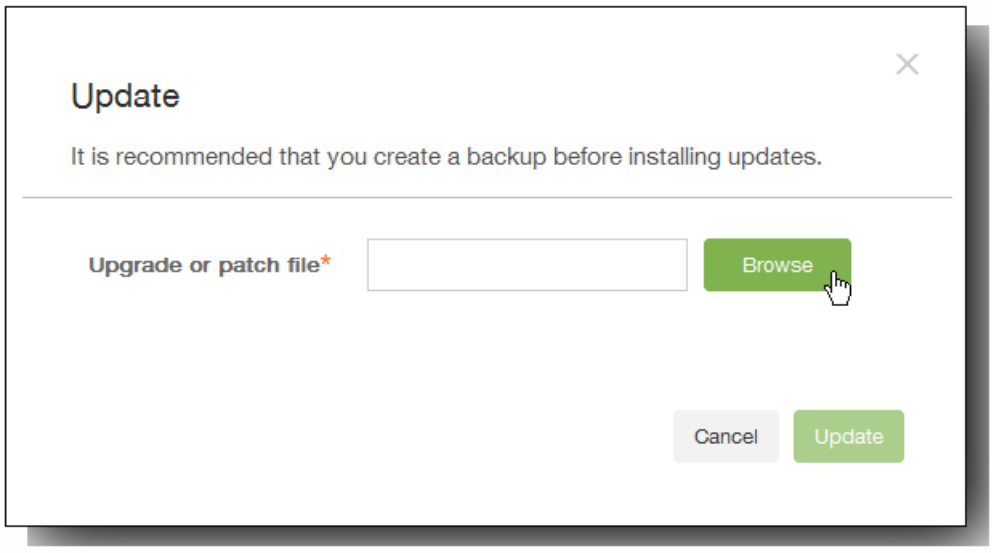
1. Inicie sesión con su cuenta en el sitio Web de Citrix y descargue el archivo de actualización (.bin) de XenMobile a una ubicación apropiada.
2. En la consola de XenMobile, haga clic en Configure > Settings > Release Management.



Aparecerá la página Release Management, que muestra la versión de software actualmente instalada, así como una lista de las revisiones, las mejoras y las actualizaciones que ya se han cargado.



3. En Updates, haga clic en Update. Aparecerá el cuadro de diálogo Update.



4. Haga clic en Browse, vaya a la ubicación en la que guardó el archivo de actualización de XenMobile que descargó de Citrix.com y, a continuación, seleccione el archivo.
5. Haga clic en Update y, a continuación, si el sistema se lo solicita, reinicie XenMobile.
   Nota: Es posible que no sea necesario reiniciar XenMobile una vez instalada la actualización. En este caso, un mensaje

indica que la instalación de la actualización se realizó correctamente. Si, sin embargo, XenMobile no necesita reiniciarse, debe usar la línea de comandos.

Importante: Si el sistema está configurado en modo de clúster, siga estos pasos para actualizar cada nodo:

- Apague todos los nodos menos uno.
- Actualice ese nodo.
- Compruebe que el servicio se está ejecutando antes de actualizar el siguiente nodo.

Si, por alguna razón, la actualización no se puede completar correctamente, aparece un mensaje de error que indica el problema. El sistema se revierte a un estado anterior al intento de actualización.

Configuración de clústeres en XenMobile 10

Oct 31, 2016

XenMobile 10 ha integrado Device Manager y App Controller de XenMobile 9. En versiones de XenMobile anteriores, se configuraba Device Manager como clúster y App Controller como par de alta disponibilidad. La alta disponibilidad no es aplicable en XenMobile 10. Por tanto, para configurar la agrupación en clústeres para XenMobile 10, deberá configurar las dos direcciones IP virtuales siguientes para el equilibrio de carga en NetScaler.

- **Dirección IP virtual de equilibrio de carga para la administración de dispositivos móviles (MDM)**. Se necesita una dirección IP virtual de equilibrio de carga para MDM para establecer la comunicación con los nodos de XenMobile configurados en clúster. Este equilibrio de carga se consigue en el modo de puente SSL.
- **Dirección IP virtual de equilibrio de carga para la administración de aplicaciones móviles (MAM)**. Se necesitan direcciones IP virtuales de equilibrio de carga para MAM para que NetScaler Gateway establezca conexión con los nodos de XenMobile configurados en clúster. De forma predeterminada, en XenMobile 10 todo tráfico proveniente de NetScaler Gateway se enruta a la dirección IP virtual de equilibrio de carga en el puerto 8443.

En los procedimientos de este artículo, se explica el proceso de creación de una nueva configuración en clúster, consistente en crear una nueva máquina virtual de XenMobile y unirla a una máquina virtual ya existente.

Requisitos previos

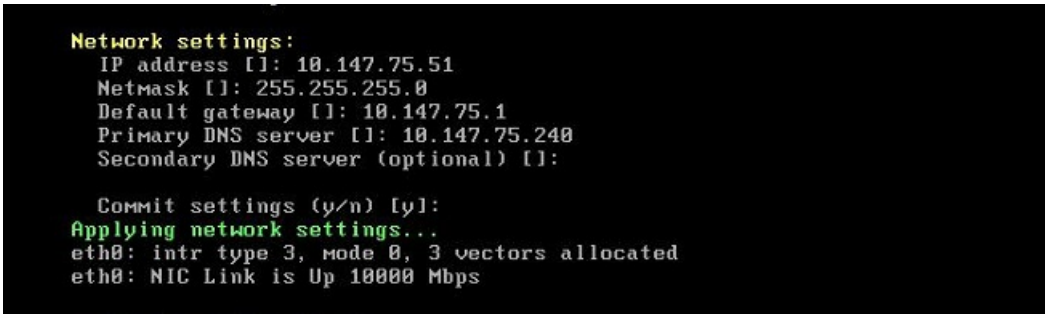
- Haber completado la configuración del nodo pertinente de XenMobile.
- Dos direcciones IP libres para usarlas como direcciones IP virtuales de equilibrio de carga.
- Certificados de servidor.
- Una dirección IP libre para la dirección IP virtual de NetScaler Gateway.

Para ver gráficos de referencia con las arquitecturas de XenMobile 10.x en configuraciones en clúster, consulte Descripción de la arquitectura.

Cree nuevas máquinas virtuales de XenMobile en función de la cantidad de nodos que necesite. Estas nuevas máquinas virtuales deberán apuntar a la misma base de datos, y deberá suministrar las mismas contraseñas de certificado PKI.

1. Abra la consola de línea de comandos de la nueva máquina virtual e introduzca la nueva contraseña de la cuenta de administrador.

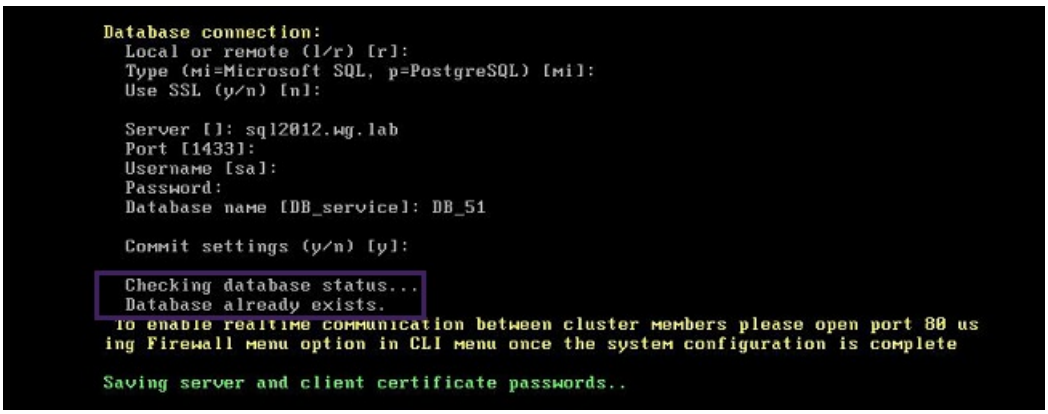
2. Facilite los datos de la configuración de red tal y como se muestra en la imagen siguiente.



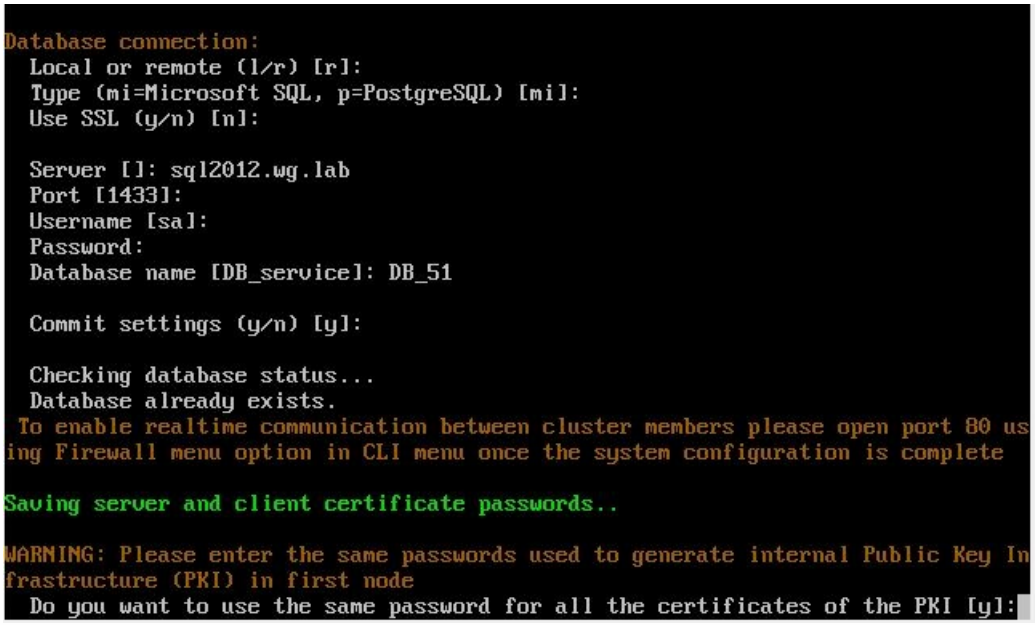
3. Si quiere usar la contraseña predeterminada para la protección de datos, escriba **y**; o escriba **n** y luego introduzca una nueva contraseña. **Nota:** Si tiene pensado agregar nodos adicionales al clúster manualmente y no va a clonar la VM inicial de XenMobile, debe introducir una nueva contraseña aquí. Los nodos secuenciales requieren una misma contraseña. Si no usa la misma contraseña para todos, cuando trate de unir el segundo nodo, el proceso fallará. Es posible clonar la VM cuando esto ocurre, pero si se introduce una nueva contraseña se evita el fallo.

4. Si quiere usar el estándar FIPS, escriba **y**; en caso contrario, escriba **n**.

5. Configure la base de datos de modo que apunte a la misma base a la que apuntaba la anterior máquina virtual completamente configurada. Verá el mensaje "Database already exists".

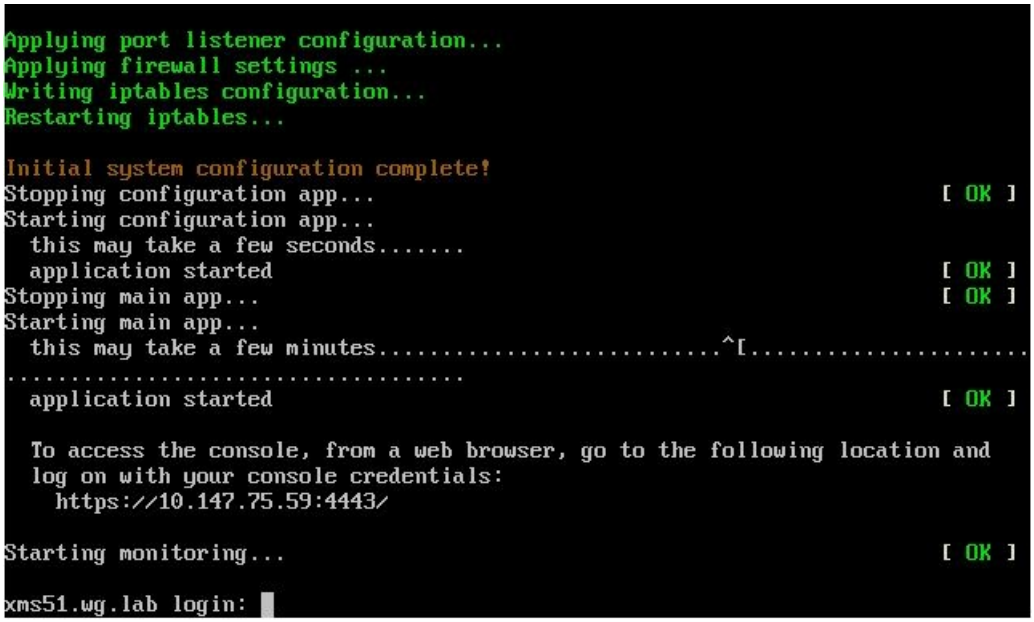


6. Introduzca las mismas contraseñas para los certificados proporcionados a la primera máquina virtual.



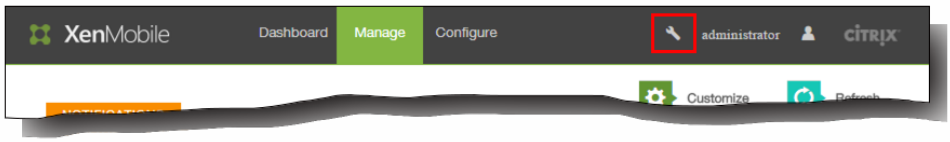
Una vez introducida la contraseña, se completará la configuración inicial del segundo nodo.

7. Cuando se complete la configuración, se reiniciará el servidor y aparecerá el cuadro de diálogo de inicio de sesión.

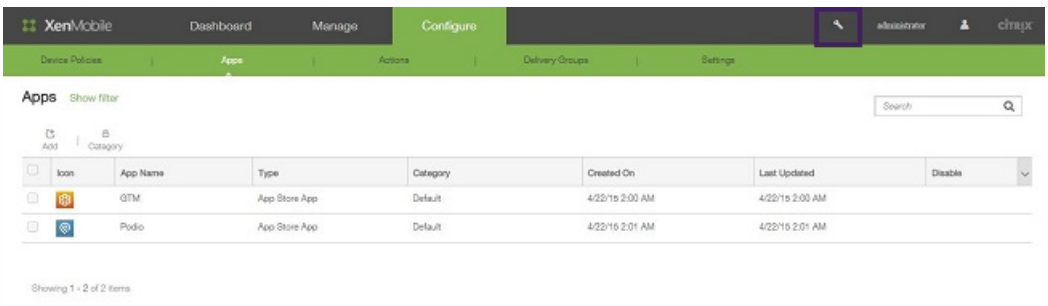


Nota: Este cuadro de diálogo de inicio de sesión es idéntico al cuadro de diálogo del inicio de sesión de la primera máquina virtual. Esta coincidencia sirve para confirmar que ambas máquinas virtuales utilizan el mismo servidor de base de datos.

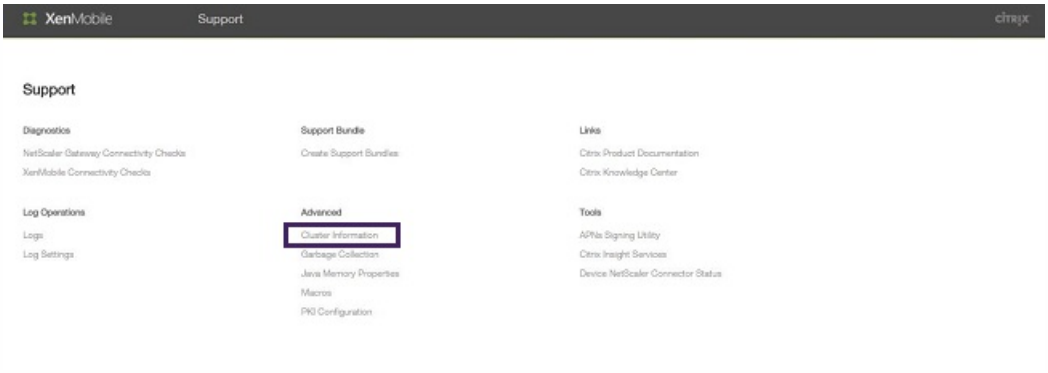
8. Use el nombre de dominio completo (FQDN) de XenMobile para abrir la consola de XenMobile en un explorador Web.
9. En el panel de mandos, haga clic en el icono de herramienta, situado en la parte superior derecha de la pantalla.



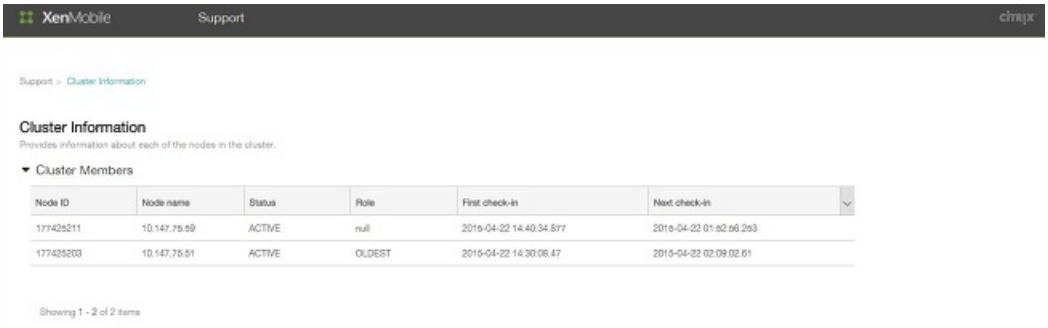
Se abrirá la página Support.



10. En Advanced, haga clic en Cluster Information.



Aparecerá toda la información relativa al clúster, incluida la información de sus miembros, de la conexión del dispositivo y las tareas, entre otros.

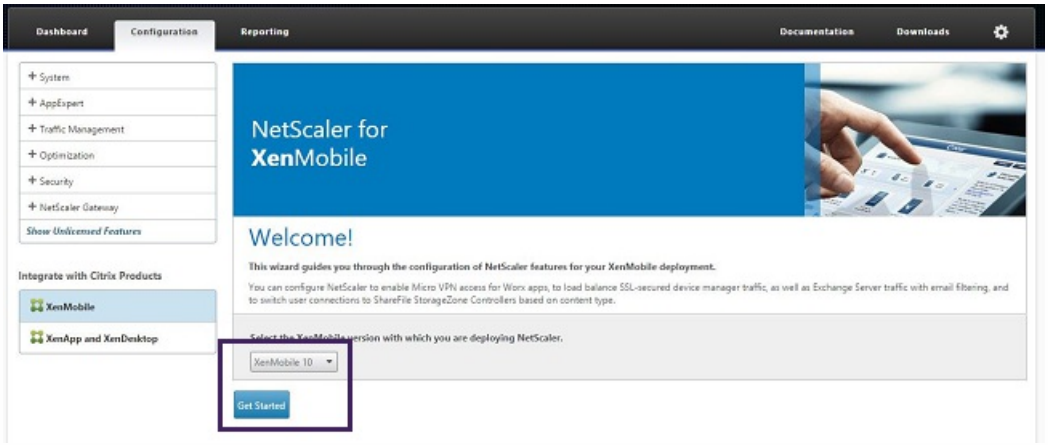


Ahora, el nuevo nodo es miembro del clúster. Puede agregar otros nodos siguiendo los mismos pasos.

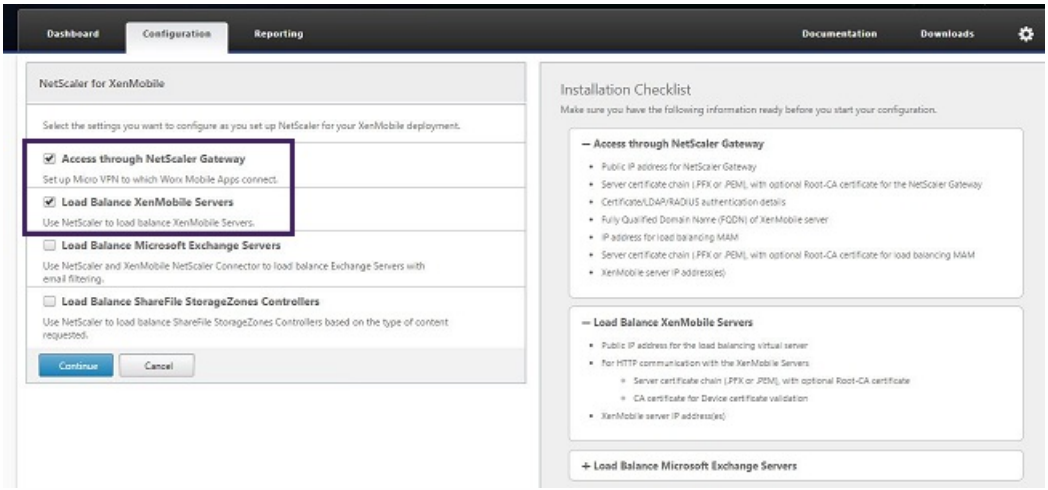
Después de agregar los nodos necesarios como miembros del clúster de XenMobile, deberá equilibrar la carga de esos nodos para poder acceder a los clústeres. La carga se equilibra mediante el asistente de XenMobile disponible en NetScaler 10.5.x. Siga los pasos de este procedimiento para equilibrar la carga de XenMobile con la ayuda del asistente.

1. Inicie sesión en NetScaler.

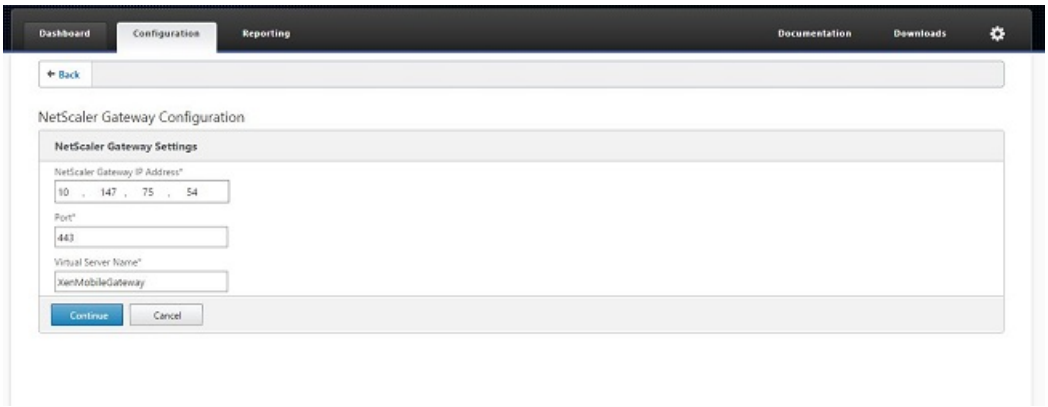
2. En la ficha Configuration, haga clic en XenMobile y en Get Started.



3. Marque las casillas Access through NetScaler Gateway y Load Balance XenMobile Servers. A continuación, haga clic en Continue.

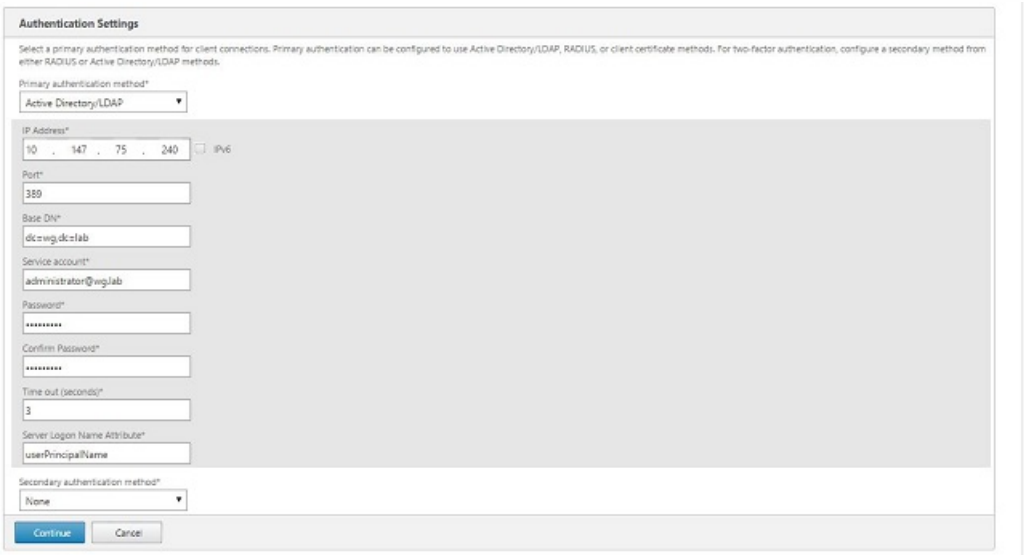


4. Introduzca la dirección IP de NetScaler Gateway y haga clic en Continue.



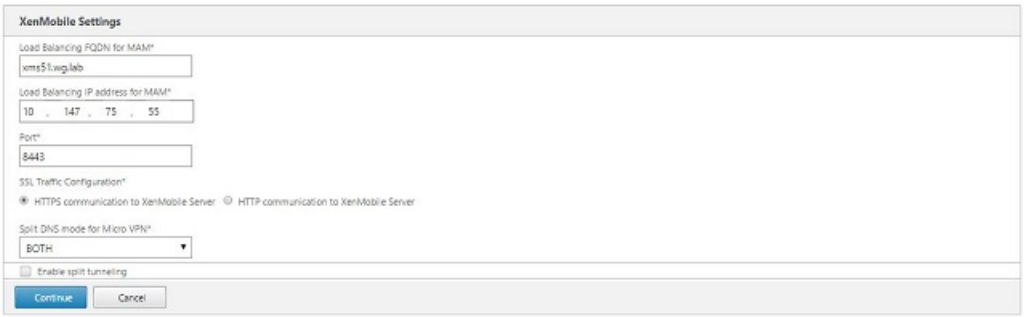
5. Vincule el certificado del servidor a la dirección IP virtual de NetScaler Gateway. Para ello, lleve a cabo una de las siguientes acciones y, a continuación, haga clic en Continue.
   - En Use existing certificate, elija el certificado del servidor de la lista.
   - Haga clic en la ficha Install Certificate para cargar un nuevo certificado de servidor.

6. Introduzca los datos del servidor de autenticación y, a continuación, haga clic en Continue.



Nota: Compruebe que el campo Server Logon Name Attribute es el mismo que el que facilitó en la configuración LDAP de XenMobile.

7. En XenMobile Settings, rellene el campo Load Balancing FQDN for MAM y, a continuación, haga clic en Continue.



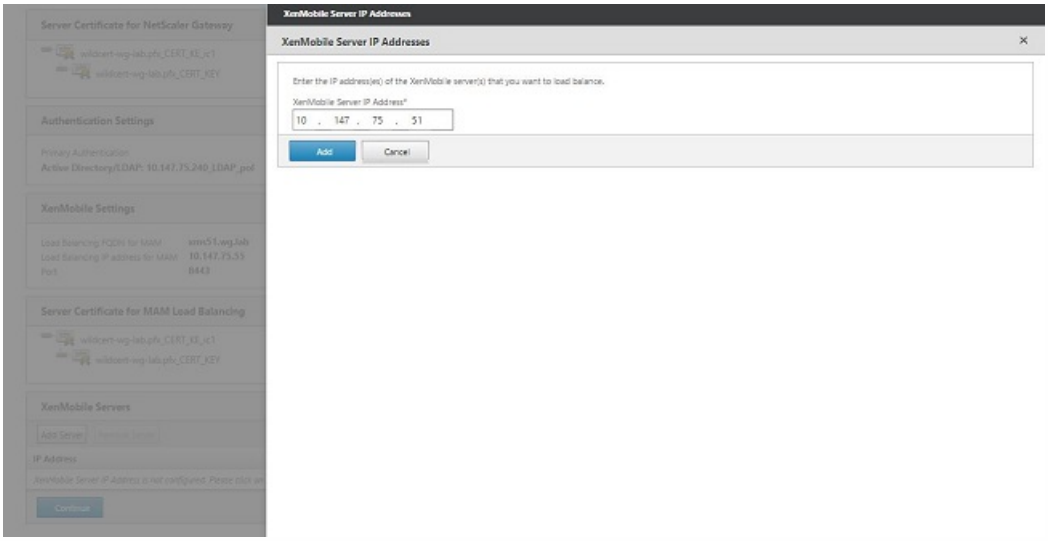
Nota: Compruebe que el nombre de dominio completo perteneciente a la dirección IP virtual de equilibrio de carga para MAM y el nombre de dominio completo de XenMobile coinciden.

8. Si quiere usar el modo de puente SSL (HTTPS), marque HTTPS communication to XenMobile Server. En cambio, si quiere usar la descarga de SSL, marque HTTP communication to XenMobile Server, como se muestra en la imagen anterior. Dada la finalidad de este artículo, se opta por el modo de puente SSL (HTTPS).
9. Vincule el certificado del servidor a la dirección IP virtual de equilibrio de carga para MAM. A continuación, haga clic en

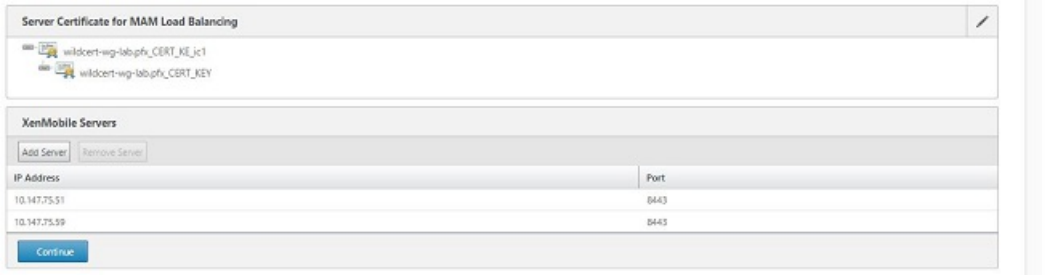
Continue.

10. En XenMobile Servers, haga clic en Add Server para agregar los nodos de XenMobile.

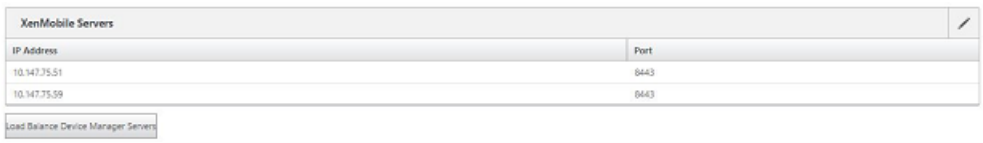
11. Introduzca la dirección IP del nodo de XenMobile y, a continuación, haga clic en Add.



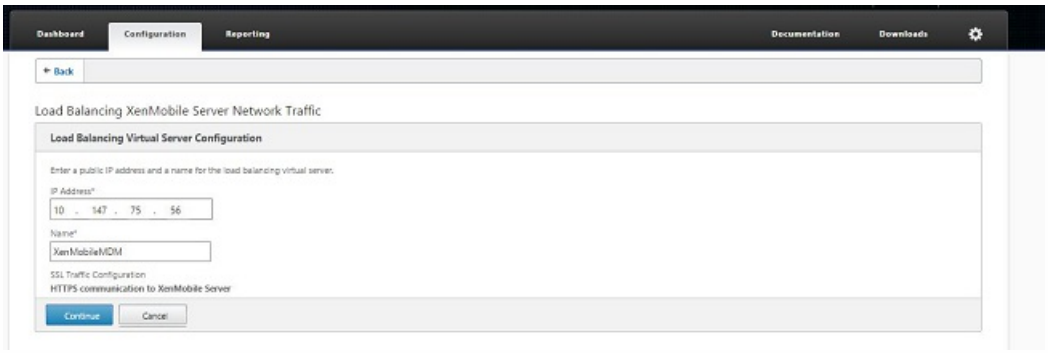
12. Repita los pasos 10 y 11 para agregar nodos de XenMobile adicionales que formen parte del clúster de XenMobile. Verá todos los nodos de XenMobile que haya agregado. Haga clic en Continuar.



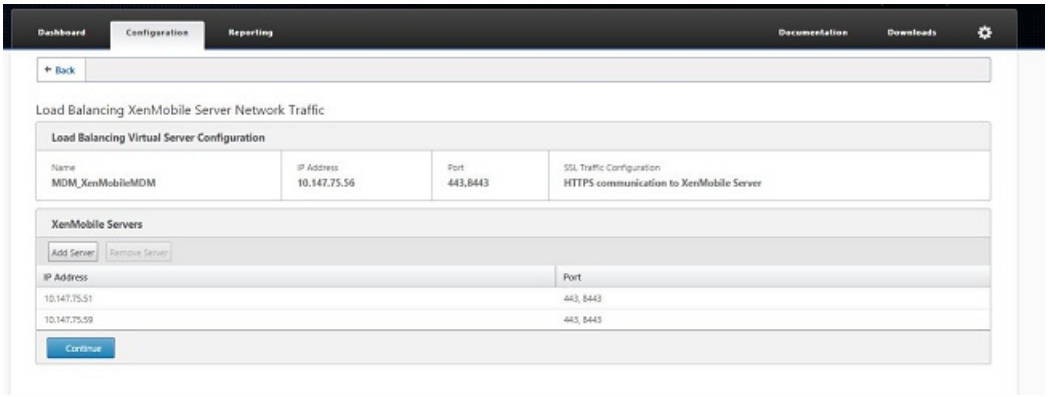
13. Haga clic en Load Balance Device Manager Servers para continuar con la configuración del equilibrio de carga para MDM.



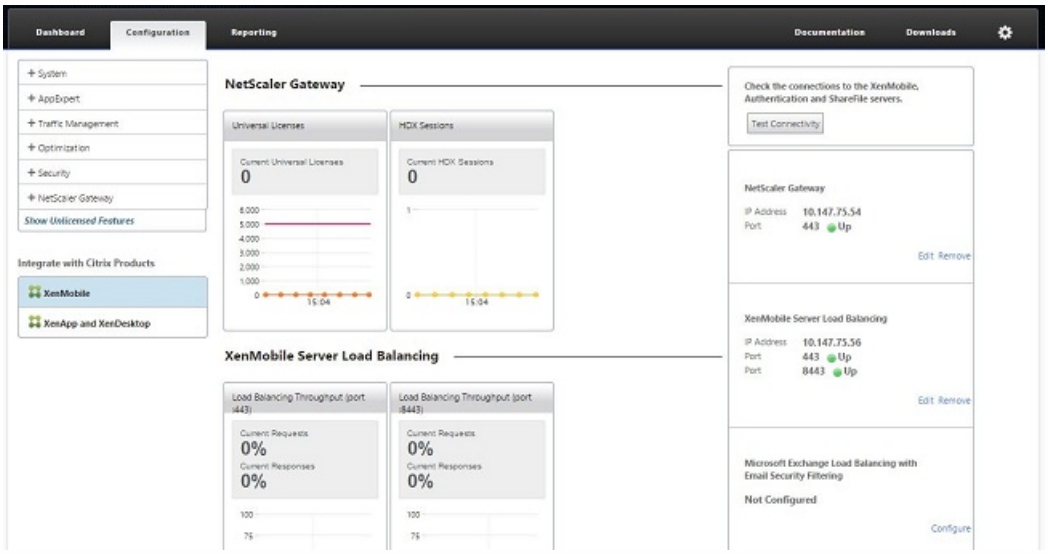
14. Introduzca la dirección IP que se utilizará como la IP de equilibrio de carga para MDM y, a continuación, haga clic en Continue.



15. Una vez que vea los nodos de XenMobile en la lista, haga clic en Continue y, a continuación, en Done para finalizar el proceso.

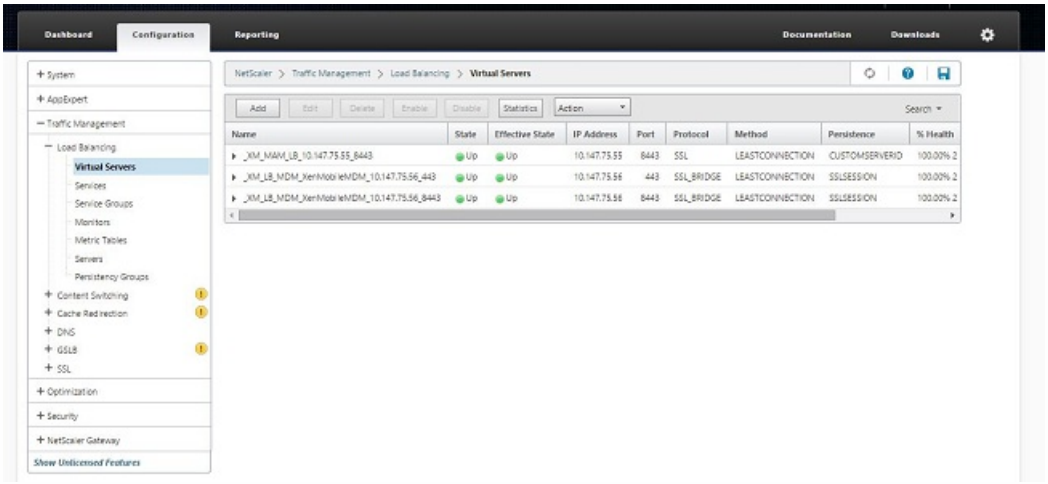


Verá el estado de la dirección IP virtual en la página XenMobile.

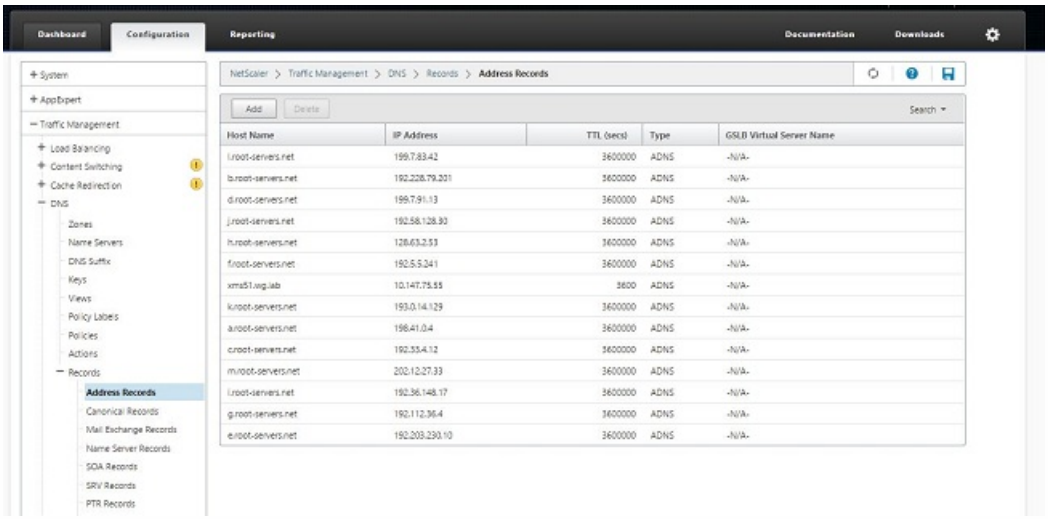


16. Para confirmar que las direcciones IP virtuales funcionan, haga clic en la ficha Configuration y vaya a Traffic

Management > Load Balancing > Virtual Servers.



También verá que la entrada DNS en NetScaler apunta a la dirección IP virtual de equilibrio de carga para MAM.

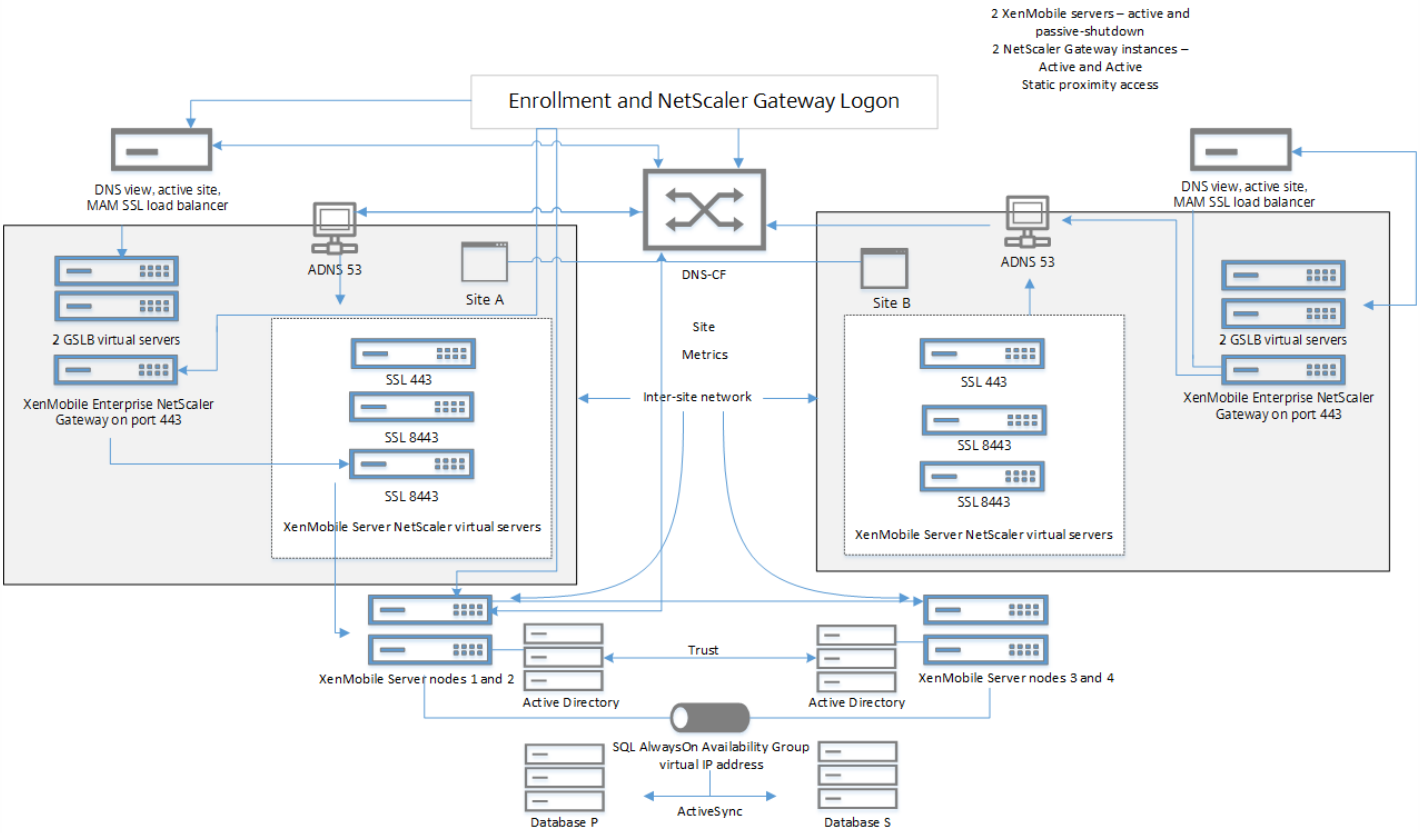


Guía de recuperación ante desastres de XenMobile

May 05, 2016

Esta guía, disponible como PDF, describe cómo configurar XenMobile 10 Enterprise Edition para una implementación de recuperación ante desastres.

La arquitectura para esta implementación se muestra en la figura siguiente y también está disponible para descargarla como PDF.



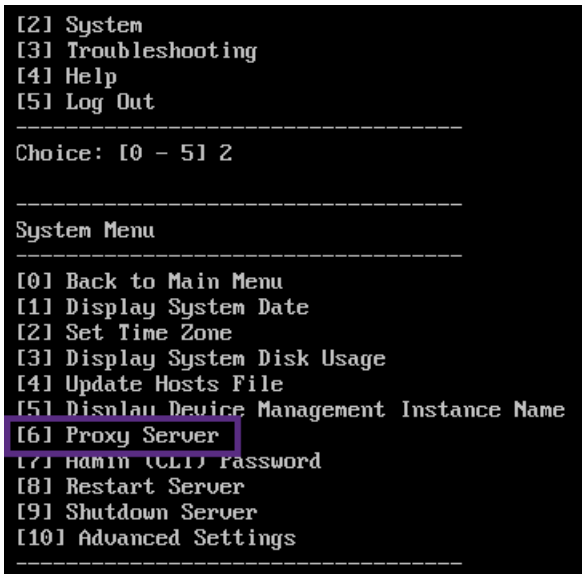
Habilitación de servidores proxy en XenMobile

May 05, 2016

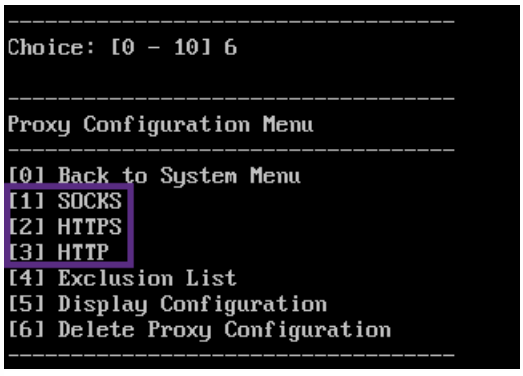
Si desea controlar el tráfico saliente a Internet, puede configurar un servidor proxy en XenMobile para transportar dicho tráfico. Para ello, debe configurar el servidor proxy mediante la interfaz de línea de comandos (CLI). Tenga en cuenta que la configuración del servidor proxy requiere reiniciar el sistema.

1. En el menú principal de la línea de comandos de XenMobile, introduzca **2** para seleccionar el menú de sistema.

2. En el menú de sistema, introduzca **6** para seleccionar el menú de servidor proxy.



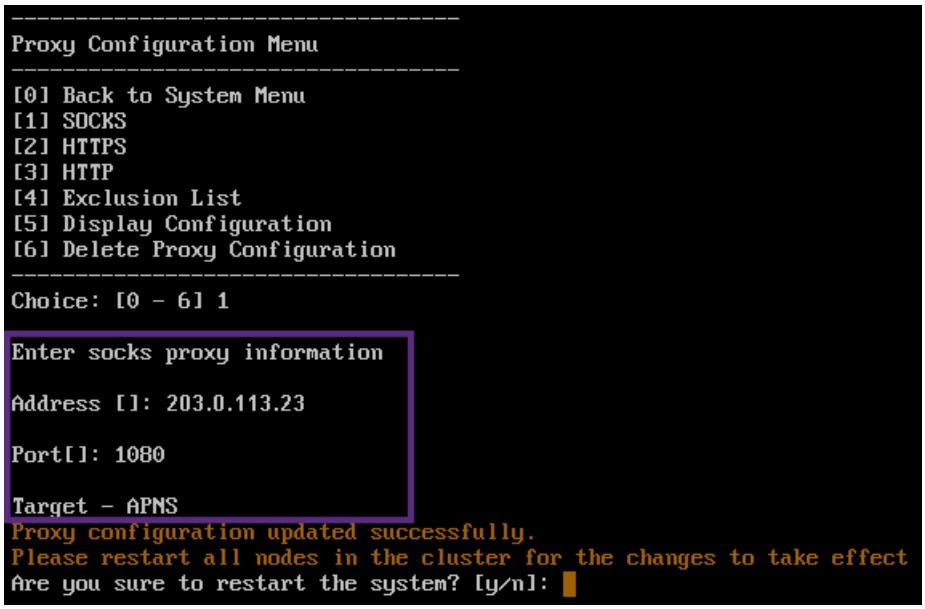
3. En el menú de configuración de proxy, introduzca **1** para seleccionar SOCKS, **2** para seleccionar HTTPS, o **3** para seleccionar HTTP.



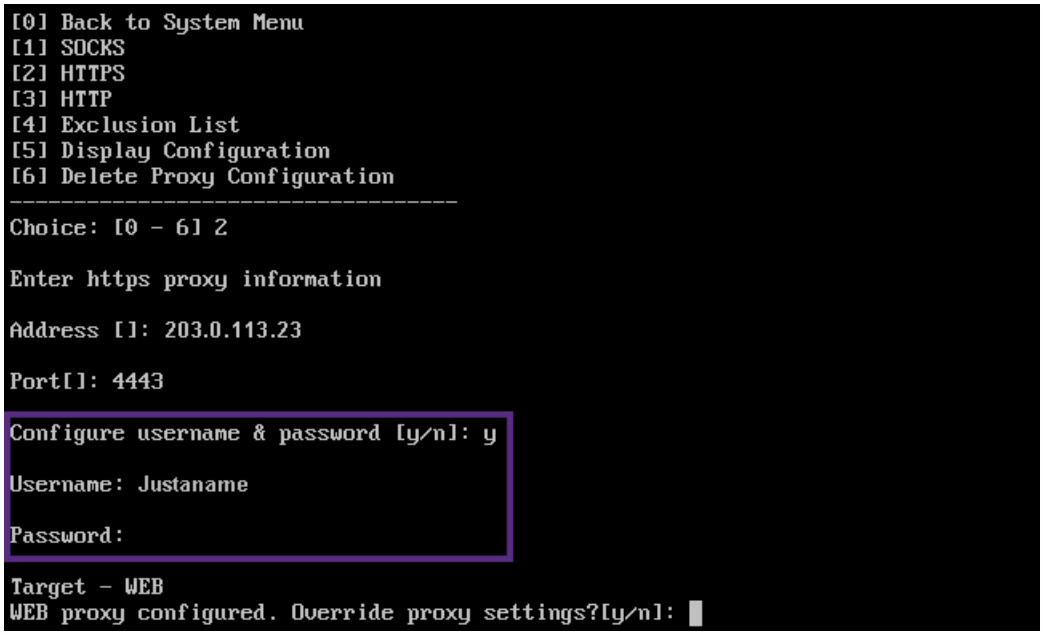
4. Introduzca la dirección IP del servidor proxy, el número de puerto y el destino. Consulte la tabla siguiente para ver los tipos de destino admitidos para cada tipo de servidor proxy.

Tipo de proxy	Destinos admitidos

SOCKS	APNS
HTTP	APNS, Web. PKI
HTTPS	Web, PKI
HTTP con autenticación	Web, PKI
HTTPS con autenticación	Web, PKI



5. Si elige configurar un nombre de usuario y una contraseña para la autenticación en el servidor proxy HTTP o HTTPS, introduzca **y** y, a continuación, escriba el nombre de usuario y la contraseña.



6. Introduzca **y** para finalizar la configuración del servidor proxy.

Licencias

May 05, 2016

XenMobile y NetScaler Gateway requieren licencias. Para obtener más información sobre el sistema de licencias de NetScaler Gateway, consulte Installing Licenses on NetScaler Gateway (en inglés).

XenMobile usa Citrix Licensing para administrar las licencias. Para obtener más información acerca de Citrix Licensing, consulte El sistema de licencias de Citrix.

Al adquirir XenMobile, recibirá un correo electrónico de confirmación del pedido con instrucciones para activar las licencias. Los clientes nuevos deben registrarse en un programa de licencias antes de realizar un pedido. Para obtener más información acerca de los programas y los modelos de licencia de XenMobile, consulte lLicencias de XenMobile.

Debe instalar Citrix Licensing antes de descargar las licencias de XenMobile. Se necesitará el nombre del servidor en el que instale Citrix Licensing para generar el archivo de licencias. Al instalar XenMobile, Citrix Licensing se instala en el servidor de forma predeterminada. También puede usar una implementación existente de Citrix Licensing para administrar las licencias de XenMobile. Para obtener más información sobre la instalación, la implementación y la administración de Citrix Licensing, consulte Licencias de productos.

Nota: XenMobile 10 requiere la versión 11.12.1 de Citrix License Server, o una versión posterior; las versiones anteriores del servidor de licencias no funcionan con XenMobile 10.

Importante: Si va a agrupar nodos en clúster o instancias de XenMobile, es necesario usar Citrix Licensing en un servidor remoto.

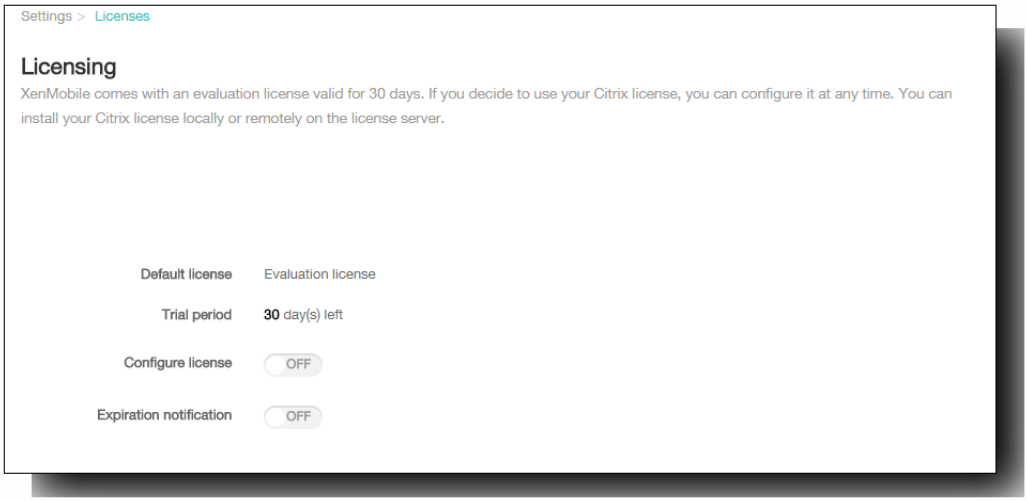
Citrix recomienda conservar copias locales de todos los archivos de licencias que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencias se incluyen en la copia de seguridad. Sin embargo, si vuelve a instalar XenMobile sin realizar antes una copia de seguridad del archivo de configuración, necesitará los archivos de licencia originales.

Si no dispone de licencia, XenMobile opera en modo de prueba con todas sus funcionalidades durante un período de gracia de 30 días. Este modo de prueba solo se puede usar una vez, y el período de 30 días comienza a partir de la instalación. El acceso a la consola Web de XenMobile no se bloquea nunca, independientemente de si hay disponible una licencia válida de XenMobile.

Aunque XenMobile permite cargar varias licencias, solo se puede activar una licencia en un momento dado.

Cuando caduca una licencia de XenMobile, todas las funciones de administración de dispositivos dejan de estar disponibles. Por ejemplo, no se pueden inscribir usuarios o dispositivos nuevos, además de que las configuraciones y las aplicaciones implementadas en los dispositivos inscritos no se pueden actualizar.

Cuando la página Licensing aparece por primera vez después de instalar XenMobile, la licencia aún no está configurada y funciona de forma predeterminada en el modo de prueba de 30 días. En esta página, puede agregar y definir licencias.

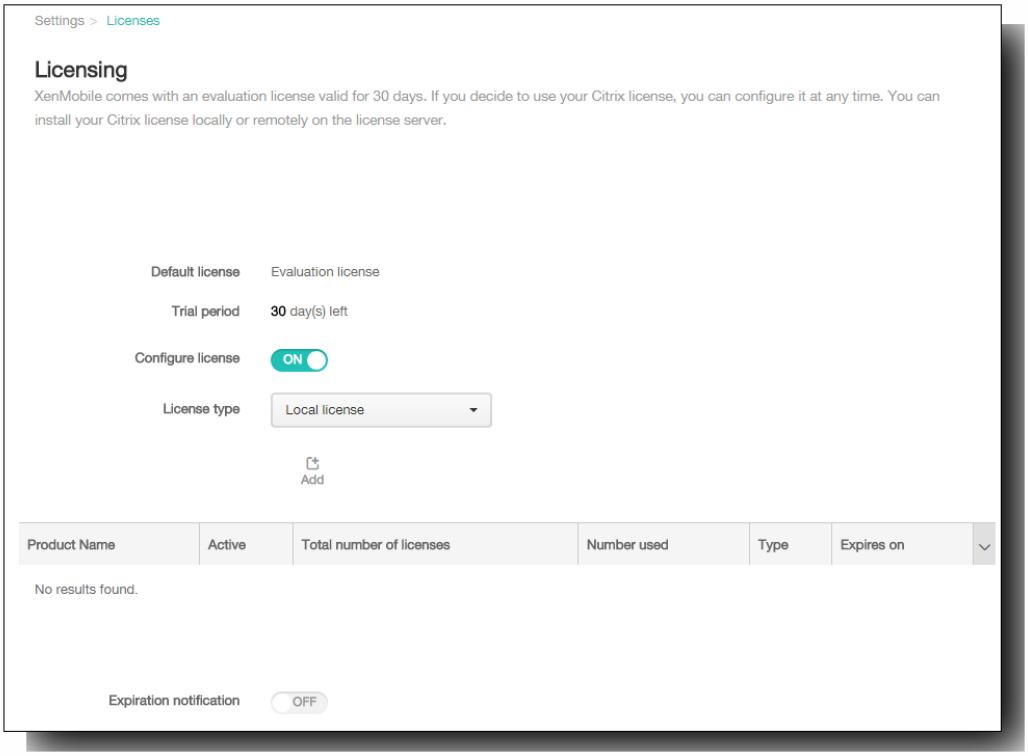


1. En la consola de XenMobile, haga clic en Configure > Settings.
2. Haga clic en Licensing. Aparecerá la página Licensing.

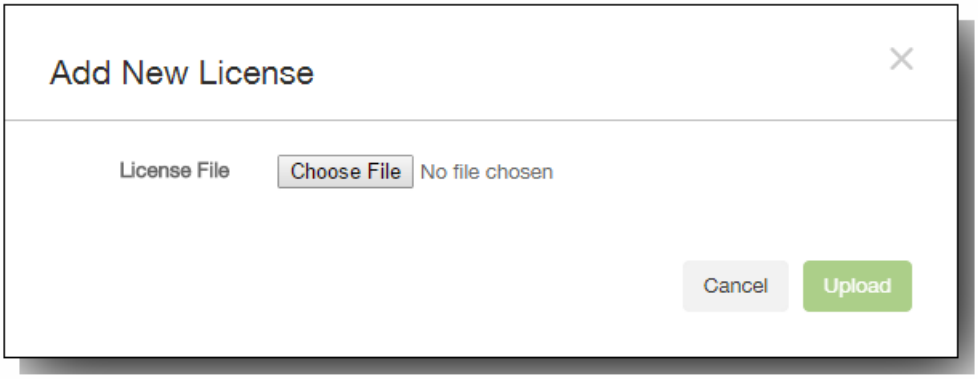
Al agregar nuevas licencias, estas aparecen en la tabla. La primera licencia agregada se activa automáticamente. Si agrega varias licencias de la misma categoría (por ejemplo, Enterprise) y del mismo tipo (por ejemplo, Device), dichas licencias aparecen en una sola fila de la tabla. En estos casos, Total number of license y Number used reflejan la cantidad total conjunta de licencias comunes. La fecha indicada en Expires on muestra la última fecha de caducidad de las licencias comunes.

Puede administrar todas las licencias locales a través de la consola de XenMobile.

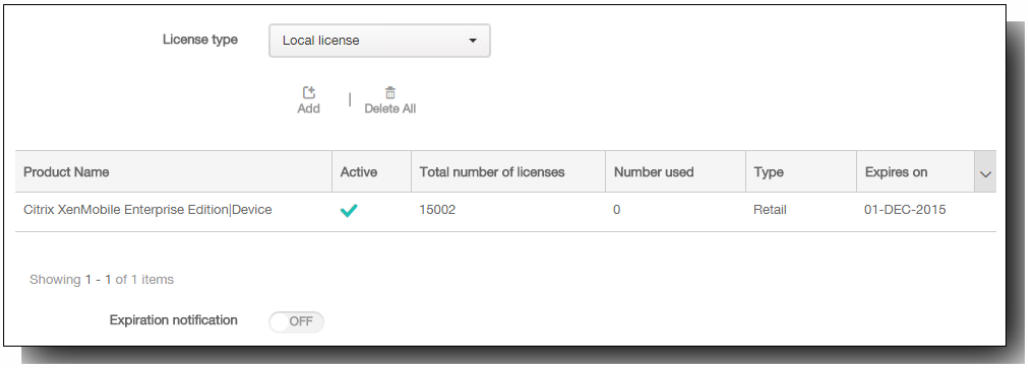
1. Los archivos de licencias pueden obtenerse del servicio Simple License Service mediante la consola License Administration Console o directamente desde su cuenta, en citrix.com. Para obtener información más detallada, consulte Obtención de archivos de licencias.
2. En la consola, haga clic en Configure > Settings > Licenses. Aparecerá la página Licensing.
3. Establezca Configure license en On. Aparecerán la lista License type, el botón Add y la tabla Licensing. La tabla Licensing contiene las licencias que haya usado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.



4. Compruebe que License type está establecido en Local license y, a continuación, haga clic en Add. Aparecerá el cuadro de diálogo Add New License.



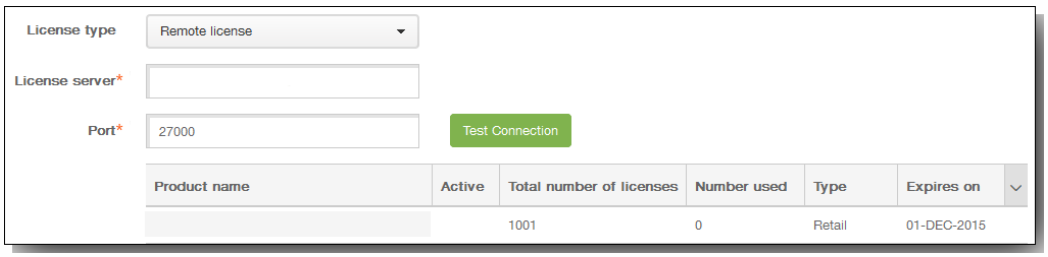
5. En el cuadro de diálogo Add New License, haga clic en Choose File y, a continuación, vaya a la ubicación de su licencia.
6. Haga clic en Upload. La licencia se cargará de forma local y aparecerá en la tabla.



7. Cuando la licencia aparezca en la tabla de la página License, actívela. Si se trata de la primera licencia de la tabla, la licencia se activa automáticamente.

Si utiliza el servidor remoto de Citrix Licensing, use ese servidor para administrar toda la actividad de las licencias. Para obtener más información, consulte Licencias de productos.

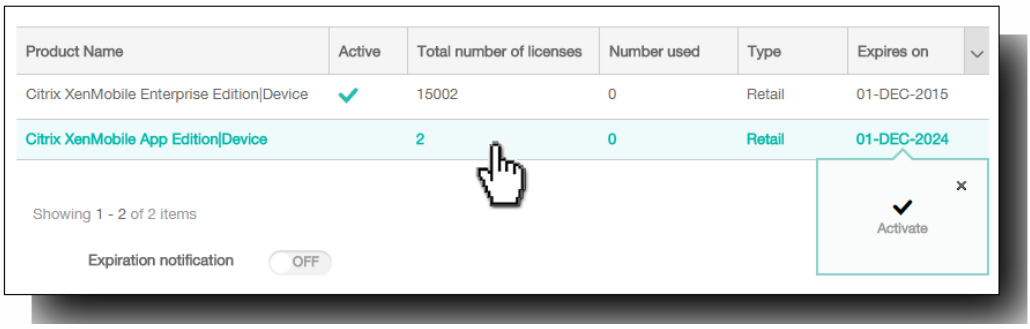
1. En la página Licensing, establezca Configure license en On. Aparecerán la lista License type, el botón Add y la tabla Licensing. La tabla Licensing contiene las licencias que haya usado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.
2. Establezca License type en Remote license. El botón Add se reemplaza por los campos License server y Port, así como el botón Test Connection.



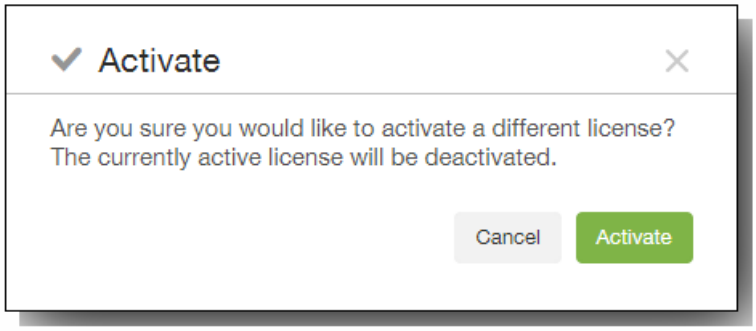
3. En License server, escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor de licencias remoto.
4. En el campo Port, acepte el puerto predeterminado o introduzca el número de puerto utilizado para comunicarse con el servidor de licencias.
5. Haga clic en Test Connection. Si la conexión es satisfactoria, XenMobile se conecta al servidor de Citrix Licensing, y la tabla Licensing se rellena con las licencias disponibles. Si la conexión no puede establecerse, compruebe que ha proporcionado la información correcta y que todas las conexiones están activas.
   Nota: Si solo hay una licencia, esta se activa automáticamente.

Si dispone de varias licencias, puede elegir la licencia a activar. Sin embargo, solo puede tener activa una licencia en un momento dado.

1. En la página Licensing, en la tabla Licensing, haga clic en la fila de la licencia a activar. Aparecerá el cuadro de confirmación Activate junto a la fila.



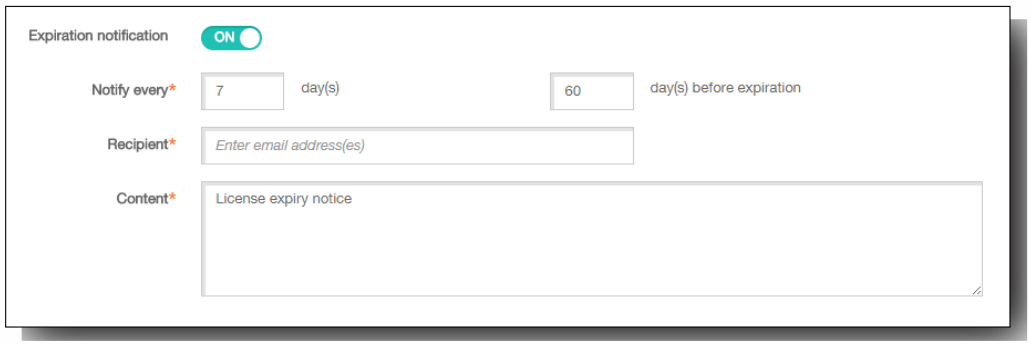
2. Haga clic en Activate. Aparecerá el cuadro de diálogo Activate.



3. Haga clic en Activate.
   Importante: Si activa la licencia seleccionada, la licencia actualmente activa se desactiva.
   Se activa la licencia seleccionada.

Después de activar las licencias locales o remotas, puede configurar XenMobile para enviarle automáticamente una notificación a usted o a la persona designada cuando se acerque la fecha de caducidad de la licencia.

1. En la página Licensing, establezca Expiration notification en On. Aparecerán nuevos campos relacionados con la notificación.



2. En Notify every, escriba:
   - La frecuencia con la que se enviarán las notificaciones; por ejemplo, cada 7 días.
   - Cuándo se comienza a enviar la notificación; por ejemplo, 60 días antes de que caduque la licencia.
3. En el campo Recipient, escriba su dirección de correo electrónico o la dirección de correo electrónico de la persona responsable de la licencia.
4. En el campo Content, escriba el mensaje de notificación de caducidad que el destinatario verá en la recepción.
5. Haga clic en Guardar. En la cantidad de días designados antes de la caducidad, XenMobile comienza a enviar mensajes de correo electrónico con el texto que haya proporcionado durante este proceso al destinatario que haya indicado. Las notificaciones se repiten con la frecuencia que haya establecido.

Introducción a la consola de XenMobile

May 05, 2016

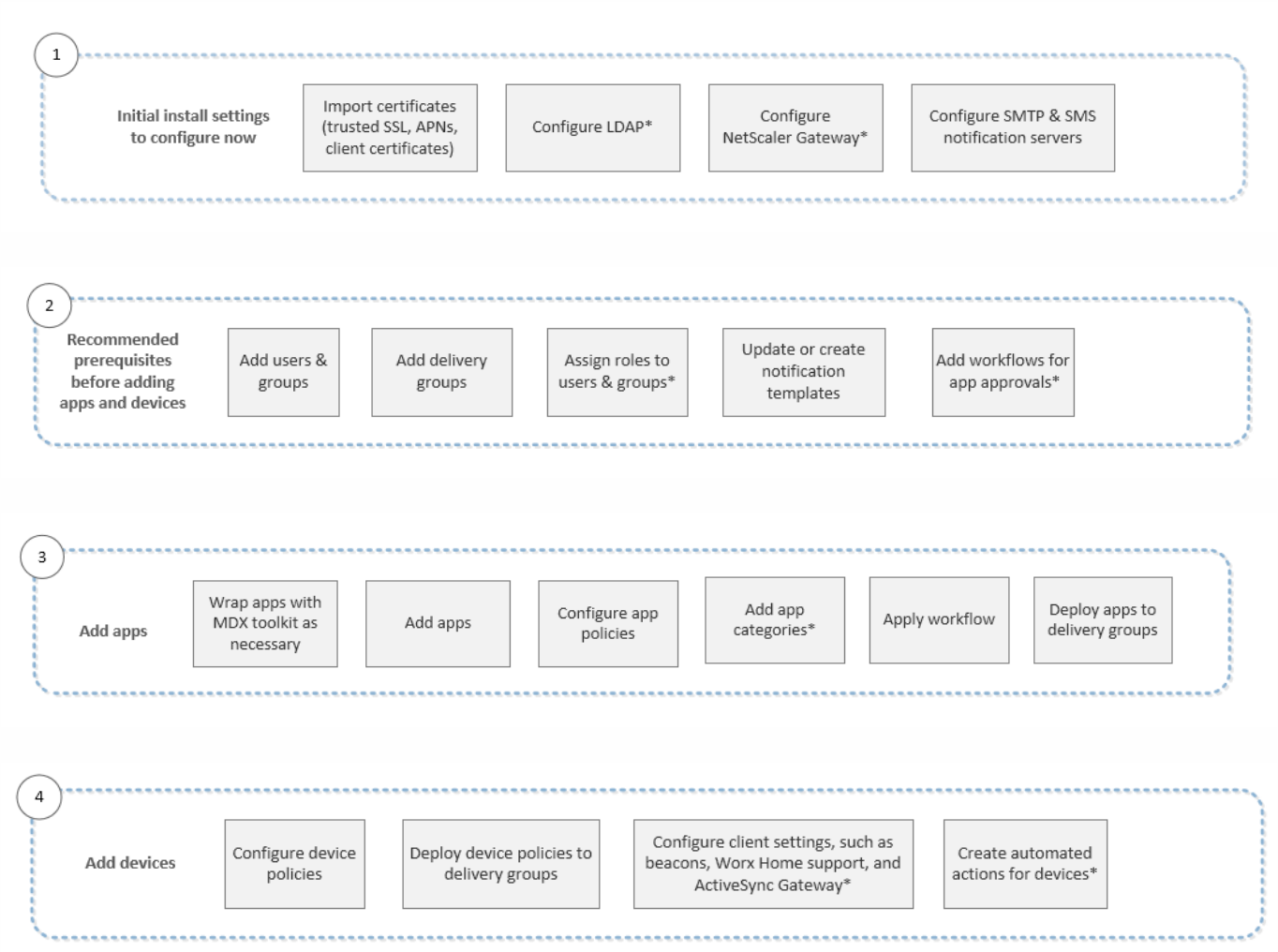
La consola de XenMobile es una herramienta de administración unificada en XenMobile 10 que combina los componentes de App Controller y Device Manager procedentes de XenMobile 9 y versiones anteriores. En este apartado, se da por hecho que XenMobile ya se ha instalado y está listo para su funcionamiento en la consola. Si necesita instalar XenMobile, consulte Instalación de XenMobile.

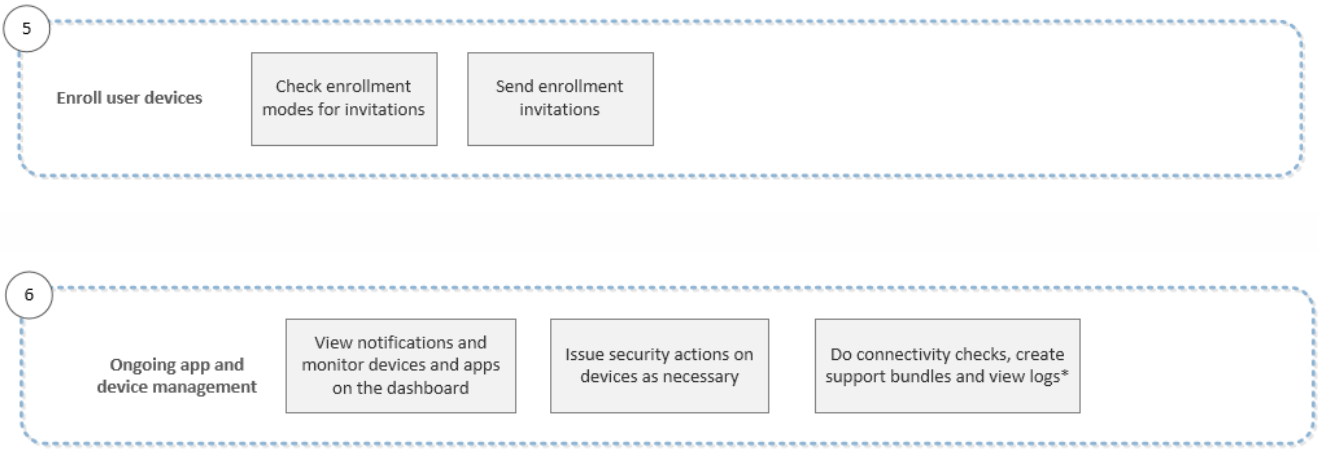
La consola de XenMobile está respaldada en las dos versiones más recientes de Firefox, Chrome e Internet Explorer.

Para ayudarle a decidir qué hacer en la consola, la siguiente ilustración muestra un flujo de trabajo recomendado para guiarle en la administración continua de dispositivos y aplicaciones. El primer conjunto de recomendaciones cubre los parámetros iniciales que puede que haya omitido durante los pasos de instalación.

Sugerencia: Haga clic en cada fila para abrir un apartado y, así, obtener información más detallada y enlaces a procedimientos.

Nota: Los elementos con un asterisco son optativos.



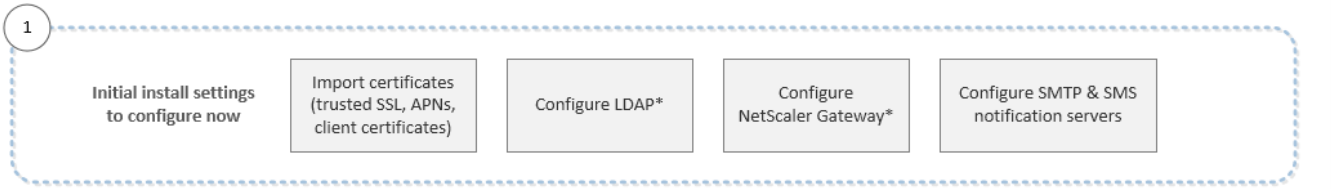


Flujo de trabajo para la configuración inicial

May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Como no se puede volver a las pantallas de configuración iniciales, si en ese momento omitió alguna configuración de instalación, puede establecer los siguientes parámetros en la consola. Antes de empezar a agregar usuarios, aplicaciones y dispositivos, debe plantearse completar estos parámetros de instalación. Para comenzar, haga clic en **Configure** > **Settings**. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

Nota: Los elementos con un asterisco son optativos.



Para obtener más información sobre cada parámetro, además de procedimientos paso a paso, consulte los siguientes apartados de eDocs:

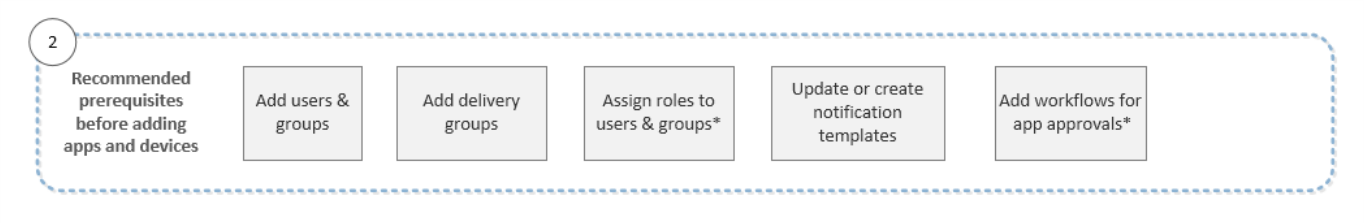
- Certificados en XenMobile
- Configuración de LDAP
- XenMobile y NetScaler Gateway
- Notificaciones en XenMobile

Flujo de trabajo para los requisitos previos de consola

May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Si en ese momento omitió alguna configuración de instalación, podrá ver la configuración inicial recomendada en Flujo de trabajo para la configuración inicial. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

En este flujo de trabajo se muestran los requisitos previos recomendados que puede configurar antes de agregar aplicaciones y dispositivos.
Nota: Los elementos con un asterisco son optativos.



Para obtener más información sobre cada parámetro, además de procedimientos paso a paso, consulte los siguientes apartados de eDocs:

- Configuración de cuentas de usuario, roles y parámetros de inscripción
- Administración de grupos de entrega en XenMobile
- Para crear o actualizar roles personalizados en XenMobile con RBAC
- Para crear o actualizar plantillas de notificaciones en XenMobile
- Para configurar modos de inscripción y habilitar el portal Self Help Portal
- Para crear y administrar flujos de trabajo

Flujo de trabajo para agregar aplicaciones

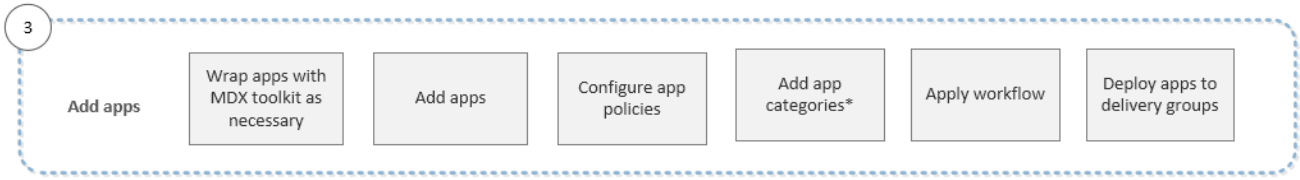
May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Si en ese momento omitió alguna configuración de instalación, podrá ver la configuración inicial recomendada en Flujo de trabajo para la configuración inicial.

A continuación, puede configurar algunos requisitos previos mediante Flujo de trabajo para los requisitos previos de consola antes de agregar aplicaciones y dispositivos. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

En este flujo de trabajo se muestra un orden recomendado a seguir en la incorporación de aplicaciones en XenMobile.

Nota: Los elementos con un asterisco son optativos.



Para obtener más información sobre cada parámetro, además de procedimientos paso a paso, consulte los siguientes apartados de eDocs:

- Empaquetado de aplicaciones con MDX Toolkit
- Incorporación de aplicaciones a XenMobile
- Directivas MDX para iOS, Android y Windows Phone 8.1
- Para agregar categorías de aplicaciones
- Para crear y administrar flujos de trabajo
- Administración de grupos de entrega en XenMobile

Flujo de trabajo para agregar dispositivos

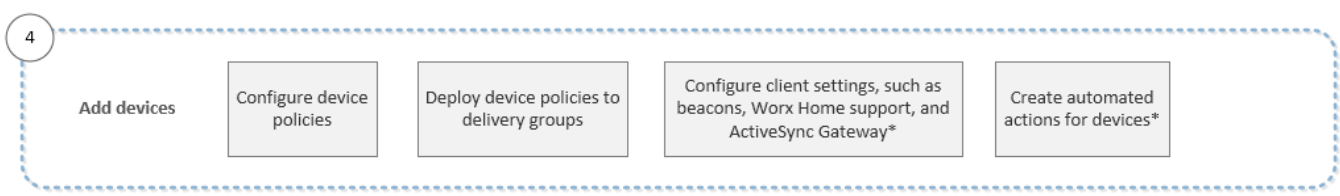
May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Si en ese momento omitió alguna configuración de instalación, podrá ver la configuración inicial recomendada en Flujo de trabajo para la configuración inicial.

A continuación, puede configurar algunos requisitos previos mediante Flujo de trabajo para los requisitos previos de consola antes de agregar aplicaciones y dispositivos. Luego, puede agregar aplicaciones mediante Flujo de trabajo para agregar aplicaciones. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

En este flujo de trabajo se muestra un orden recomendado a seguir en la incorporación y el registro de dispositivos en XenMobile.

Nota: Los elementos con un asterisco son optativos.



Para obtener más información sobre cada parámetro, además de procedimientos paso a paso, consulte los siguientes apartados de eDocs:

- Cómo agregar dispositivos y ver información de los mismos en XenMobile
- Directivas de dispositivos de XenMobile desglosadas por plataforma
- Administración de grupos de entrega en XenMobile
- Configuración de parámetros de cliente en XenMobile
- Creación de acciones automatizadas en XenMobile

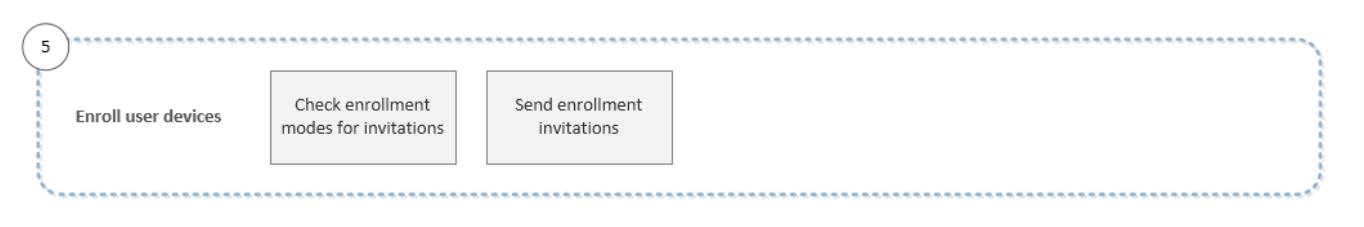
Flujo de trabajo para inscribir dispositivos de usuario

May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Si en ese momento omitió alguna configuración de instalación, podrá ver la configuración inicial recomendada en Flujo de trabajo para la configuración inicial.

A continuación, puede configurar algunos requisitos previos mediante Flujo de trabajo para los requisitos previos de consola antes de agregar aplicaciones y dispositivos. Luego, puede agregar aplicaciones mediante Flujo de trabajo para agregar aplicaciones, así como agregar y registrar dispositivos mediante Flujo de trabajo para agregar dispositivos. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

En este flujo de trabajo se muestra un orden recomendado a seguir en la inscripción en XenMobile de dispositivos de usuario.



Para obtener más información sobre cada parámetro, además de procedimientos paso a paso, consulte los siguientes apartados de eDocs:

- Configuración de cuentas de usuario, roles y parámetros de inscripción
- Para configurar modos de inscripción y habilitar el portal Self Help Portal

Flujo de trabajo para la administración continua de dispositivos y aplicaciones

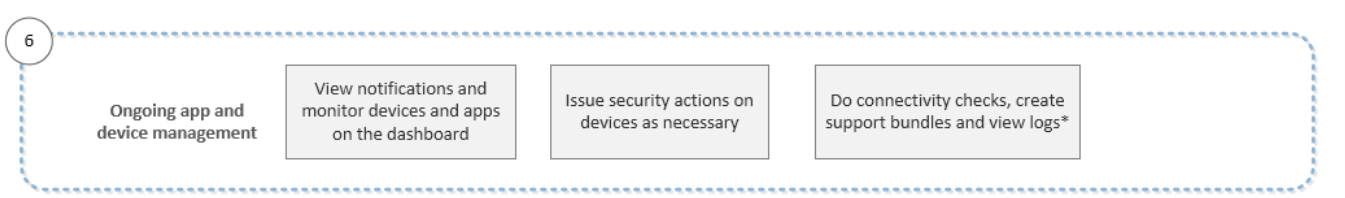
May 05, 2016

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. Si en ese momento omitió alguna configuración de instalación, podrá ver la configuración inicial recomendada en Flujo de trabajo para la configuración inicial.

A continuación, puede configurar algunos requisitos previos mediante Flujo de trabajo para los requisitos previos de consola antes de agregar aplicaciones y dispositivos. Luego, puede agregar aplicaciones mediante Flujo de trabajo para agregar aplicaciones, así como agregar y registrar dispositivos mediante Flujo de trabajo para agregar dispositivos. Después de completar los cuatro primeros flujos de trabajo, puede inscribir dispositivos de usuario mediante Flujo de trabajo para inscribir dispositivos de usuario. Para ver todo el flujo de trabajo, consulte Introducción a la consola de XenMobile.

El sexto flujo de trabajo y el último muestran las actividades recomendadas de la administración continua de dispositivos y aplicaciones que puede realizar en la consola.

Nota: Los elementos con un asterisco son optativos.



Para obtener más información acerca de las opciones de asistencia que aparecen tras hacer clic en el icono con forma de llave inglesa de la esquina superior derecha de la consola, consulte Mantenimiento y asistencia de XenMobile.

Filtros y tablas en la consola de XenMobile

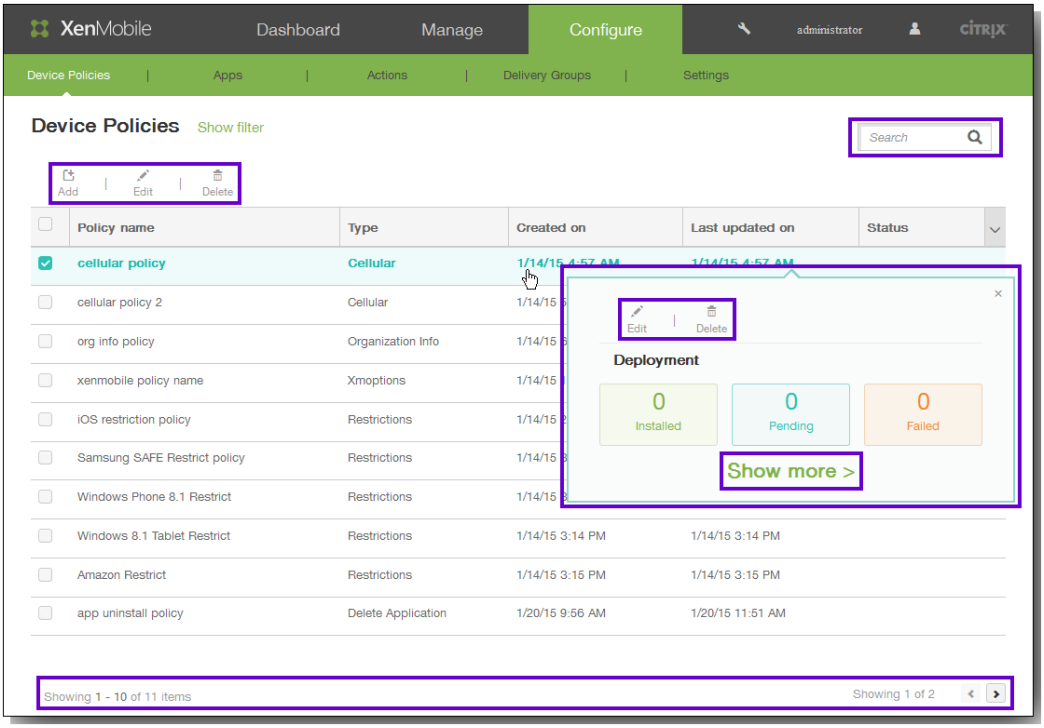
May 05, 2016

Puede encontrar los filtros y las tablas en la consola de XenMobile, en las pestañas Devices, Enrollment, Device Policies, Apps, Actions y Delivery Groups. Con los filtros, puede limitar la información de cualquiera de esas áreas de la consola para ubicar la información exacta que busca. Con las tablas, puede hacer clic en ellas para ver opciones y realizar acciones basadas en la información encontrada en dichas tablas.

A continuación, se presentan varias maneras de ver las distintas opciones disponibles de llevar a cabo acciones basadas en la información de las tablas de la consola:

- Puede marcar la casilla de verificación ubicada junto a una directiva para que el menú de opciones aparezca sobre la lista de directivas.
- Puede marcar las casillas de verificación de más de una directiva para eliminar todas las directivas seleccionadas al mismo tiempo.
- Puede hacer clic en una directiva de la lista para que el menú de opciones aparezca en el lado derecho de la lista. Cuando haga clic en Show More, verá una lista de los detalles de la configuración.
- Puede escribir el nombre completo o parcial de una directiva en el cuadro de búsqueda para limitar la cantidad de directivas de la lista.

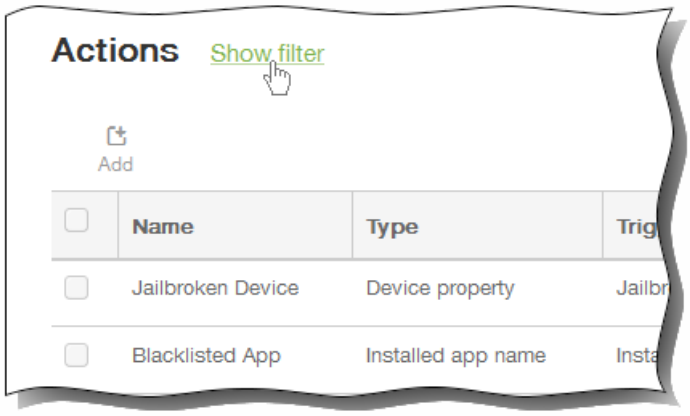
En la siguiente ilustración se muestra cómo aparecen las opciones en el área Device Policies de la consola. Solo se muestran 10 artículos por página. Haga clic en los triángulos situados en la esquina inferior derecha de la página para moverse hacia delante y hacia atrás por las páginas.



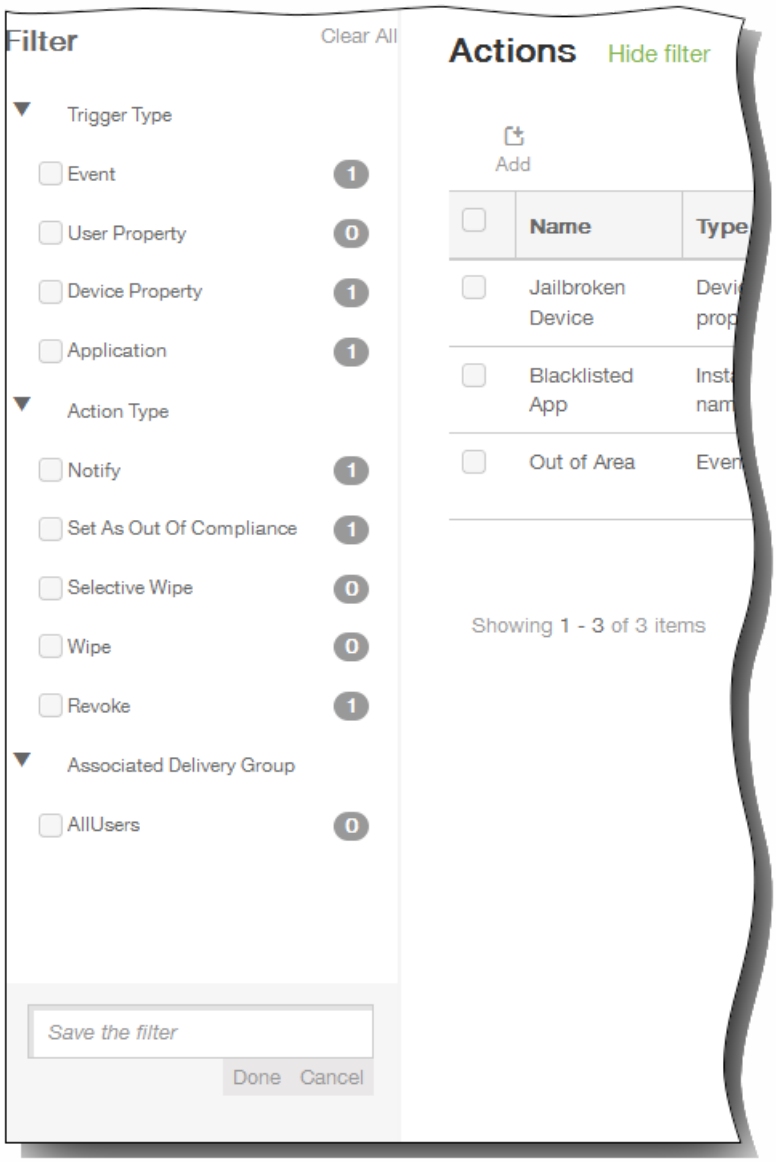
Si quiere ver un subconjunto específico de la información en un área de la consola (como los dispositivos, la inscripción, las

directivas de dispositivos, las aplicaciones, las acciones y los grupos de entrega), puede filtrar la lista en función de los criterios que seleccione. En este procedimiento, se utiliza la página Actions como ejemplo, pero los pasos para filtrar información son los mismos en toda la consola.

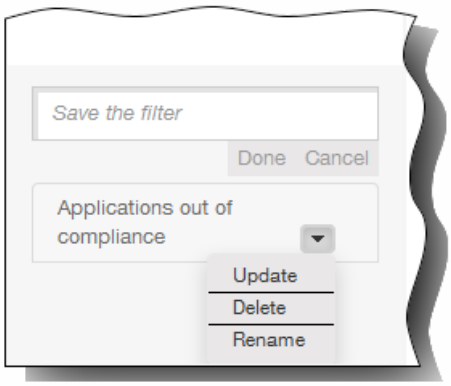
1. En la página Actions, haga clic en Show Filter.



Aparece el panel de filtrado con los criterios según los que se puede filtrar la lista Actions. Los números situados a la derecha de los criterios representan la cantidad de acciones que incluye ese criterio.



2. Haga clic en el triángulo situado a la izquierda de un filtro para mostrar las opciones disponibles de ese filtro.
3. Seleccione los criterios de filtrado que se van a utilizar. La lista Actions está limitada a las acciones que coinciden con los criterios seleccionados.
4. Lleve a cabo una de las siguientes acciones:
   - Haga clic en Hide Filter para continuar trabajando con la lista filtrada.
   - Haga clic en Clear All para volver a la lista completa.
5. Si quiere guardar los criterios seleccionados en un filtro personalizado, en el campo Save the filter, situado en la parte inferior del panel Filter, indique un nombre descriptivo y, a continuación, haga clic en Done. Si decide no guardar el filtro, haga clic en Cancel.



6. Después de guardar el filtro, podrá seleccionarlo en la parte inferior del panel Filter.
   Nota: Si hace clic en el triángulo situado a la derecha del nombre del filtro, puede eliminar el filtro o cambiarle el nombre, así como actualizarlo con criterios nuevos o modificados.

Notificaciones

May 05, 2016

Puede utilizar notificaciones en XenMobile para los siguientes propósitos:

- Comunicarse con grupos específicos de usuarios para ciertas funciones relacionadas con el sistema. También puede destinar estas notificaciones a ciertos usuarios; por ejemplo, usuarios con dispositivos iOS, usuarios cuyos dispositivos no cumplen los requisitos de cumplimiento o usuarios con dispositivos que son propiedad de los empleados, entre otros.
- Inscribir usuarios y sus dispositivos.
- Notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se den ciertas condiciones. Por ejemplo, cuando el acceso de un dispositivo de usuario al dominio de la empresa está a punto de bloquearse debido a problemas de incumplimiento, o cuando un dispositivo se ha liberado por jailbreak o por rooting. Para obtener información detallada acerca de las acciones automatizadas, consulte Creación de acciones automatizadas en XenMobile.

Para poder enviar notificaciones con XenMobile, debe configurar una puerta de enlace y un servidor de notificaciones. En XenMobile, puede establecer un servidor de notificaciones para configurar el Protocolo simple de transferencia de correo (SMTP) y los servidores de puerta de enlace del Servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y de texto (SMS) a los usuarios. Puede utilizar las notificaciones para enviar mensajes a través de dos canales: SMTP o SMS.

- SMTP es un protocolo de texto y orientado a conexiones, mediante el que el remitente de un correo se comunica con el receptor de un correo al emitir cadenas de comandos y suministrar los datos necesarios. Por regla general, este protocolo se utiliza a través de una conexión de Protocolo de control de transmisión (TCP). Las sesiones SMTP constan de comandos originados por un cliente SMTP (la persona que envía el mensaje) y las respuestas correspondientes del servidor SMTP.
- SMS es un componente del servicio de mensajería de texto propio de los sistemas de comunicación móvil, telefónica o por Web. Usa protocolos de comunicación estandarizados para permitir que dispositivos de teléfono móvil o de línea fija intercambien mensajes cortos de texto.

En XenMobile, también puede establecer una puerta de enlace SMS de operador y, así, configurar las notificaciones que se envían a través de la puerta de enlace SMS de un operador. Los operadores utilizan las puertas de enlace SMS para enviar transmisiones SMS a una red de telecomunicaciones o recibir dichas transmisiones de una red de telecomunicaciones. Estos mensajes de texto usan protocolos de comunicación estandarizados para permitir que dispositivos de teléfono móvil o de línea fija intercambien mensajes cortos de texto.

En los procedimientos de este tema se describe la forma de agregar un servidor SMTP, una puerta de enlace SMS y una puerta de enlace SMS de operador.

Para configurar un servidor SMTP y una puerta de enlace SMS

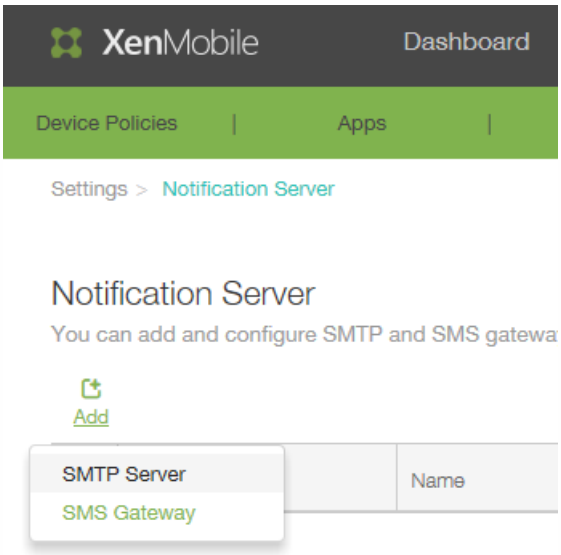
Requisitos previos:

- Antes de configurar la puerta de enlace SMS, acuda al administrador del sistema para obtener la información del servidor. Es importante saber si el servidor SMS está alojado en un servidor interno de la empresa o si el servidor forma parte de un servicio de correo electrónico alojado, en cuyo caso se necesita información procedente del sitio Web del proveedor del servicio.
- Debe configurar el servidor de notificaciones SMTP para enviar mensajes a los usuarios. Si el servidor está alojado en un servidor interno, póngase en contacto con el administrador del sistema para obtener información acerca de la configuración. Si el servidor es un servidor de servicio de correo electrónico, busque la información de configuración en el

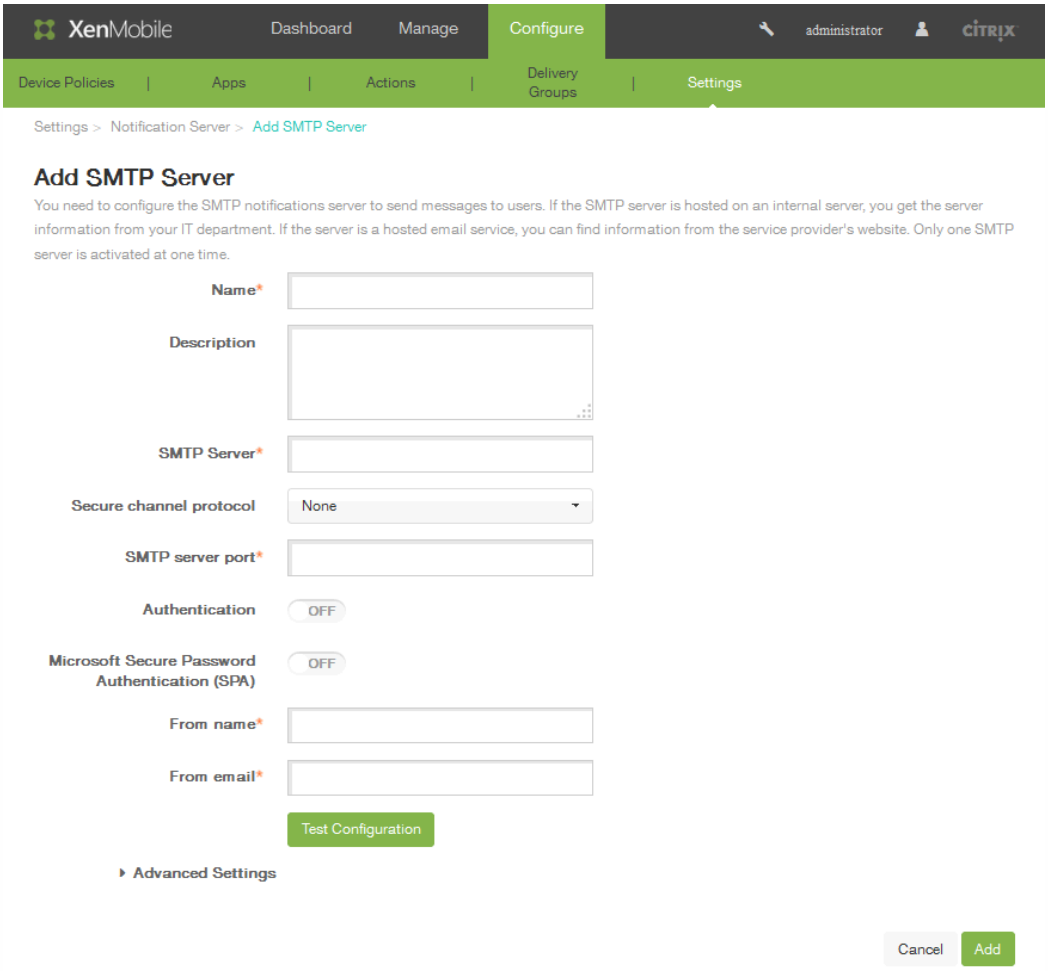
sitio Web del proveedor del servicio.

- Solo hay activo un solo servidor SMTP y un solo servidor SMS a la vez.
- Debe abrir el puerto 25 desde XenMobile (ubicado en la zona DMZ de la red) para apuntarlo al servidor SMTP de la red interna para que las notificaciones se envíen correctamente.

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Notification Server.
   Aparecerá la página de configuración Notification Server.



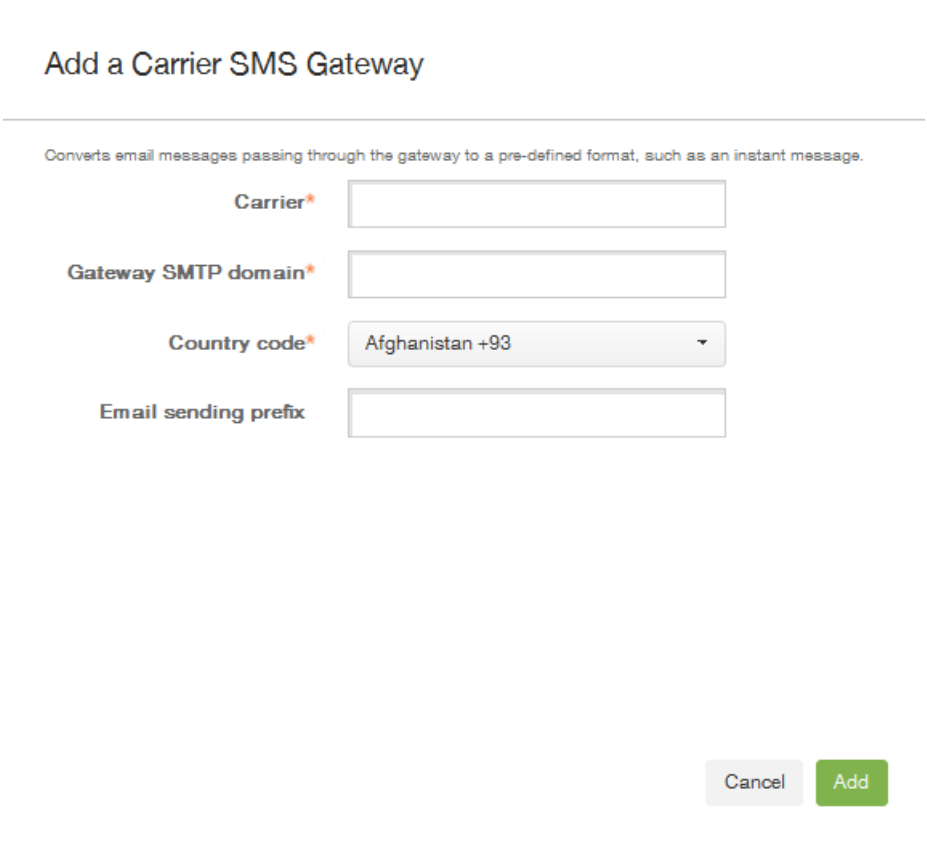
2. Haga clic en Add, en SMTP Server o SMS Gateway y, a continuación, siga las instrucciones de la opción correspondiente.
   - Para agregar un servidor SMTP, siga los pasos del 3 al 6.
   - Para agregar una puerta de enlace SMS, siga los pasos del 7 al 9.
3. Si hace clic para agregar un servidor SMTP, aparecerá la página Add SMTP Server.



4. Configure los siguientes parámetros:
   - Name. Escriba el nombre asociado a esta cuenta del servidor SMTP.
   - Description. Si quiere, introduzca una descripción del servidor.
   - SMTP Server. Escriba el nombre de host del servidor. El nombre de host puede ser una dirección IP o un nombre de dominio completo (FQDN).
   - Secure channel protocol. En la lista, haga clic en el protocolo correspondiente de canal seguro que utiliza el servidor (si el servidor está configurado para usar la autenticación segura): SSL, TLS o None. De forma predeterminada, este campo se establece como None.
   - SMTP server port. Escriba el puerto que usa el servidor SMTP. De forma predeterminada, el puerto definido es el 25. En cambio, si las conexiones SMTP usan el protocolo SSL de canal seguro, el puerto definido es 465.
   - Authentication. Seleccione ON u OFF. De forma predeterminada, esta función está inhabilitada.
   - Microsoft Secure Password Authentication (SPA). Si el servidor SMTP usa la autenticación SPA, haga clic en ON. De forma predeterminada, esta función está inhabilitada.
   - From Name. Escriba el nombre que aparece en el cuadro From cuando un cliente recibe un correo electrónico de notificación procedente de este servidor. Por ejemplo, Departamento de TI de la empresa.
   - From email. Escriba la dirección de correo electrónico utilizada si un destinatario de correo electrónico responde a la notificación enviada por el servidor SMTP.
   - Test Configuration. Haga clic para enviar una notificación de correo electrónico de prueba.
5. Expanda Advanced Settings y, a continuación, configure los siguientes parámetros:
   - Number of SMTP retries. Escriba el número de reintentos de envío de un mensaje fallido enviado por el servidor SMTP. De forma predeterminada, este campo está establecido en 5.

- SMTP Timeout. Escriba la duración del tiempo de espera (en segundos) al enviar una solicitud SMTP. Aumente este valor si el envío de mensajes falla continuamente debido a los tiempos de espera. Tenga cuidado al reducir este número, porque podría aumentar la cantidad de mensajes sin entregar y de mensajes cuyo tiempo de espera se ha agotado. De forma predeterminada, este campo está establecido en 30 segundos.
- Maximum number of SMTP recipients. Escriba la cantidad máxima de destinatarios por mensaje de correo electrónico enviado por el servidor SMTP. De forma predeterminada, este valor está establecido en 100.

6. Después de configurar el servidor SMTP, haga clic en **Add**.
7. Si quiere establecer una puerta de enlace SMS, en la página de configuración Notification Server, haga clic en Add y, luego, haga clic en SMS Gateway.
   Aparecerá la página Add SMS Gateway.



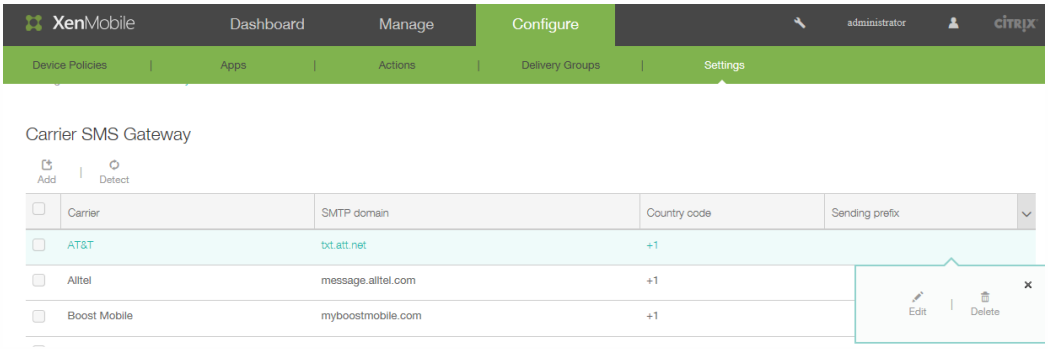
   Nota: XenMobile solo admite el envío de mensajes SMS de Nexmo. Si aún no tiene una cuenta para usar la mensajería de Nexmo, visite su sitio Web para crear una.
8. Configure los siguientes parámetros:
   - Name. Identifique la configuración de la puerta de enlace SMS.
   - Description. Si quiere, introduzca una descripción de la configuración.
   - Key. Escriba el identificador numérico proporcionado por el administrador del sistema para la activación de la cuenta.
   - Secret. Escriba un secreto proporcionado por el administrador del sistema; este secreto se usa para acceder a su cuenta en caso de robo o pérdida de la contraseña.
   - Virtual Phone Number. Este campo se usa para enviar mensajes a números de teléfono de Estados Unidos (con el prefijo +1). Debe escribir un número de teléfono virtual de Nexmo; de lo contrario, especifique una etiqueta o un nombre significativos. Puede adquirir números de teléfono virtuales en el sitio Web de Nexmo.
   - HTTPS. Seleccione esta opción si quiere utilizar HTTPS para la transmisión de solicitudes de SMS a Nexmo.
   - Country Code. En la lista, haga clic en el prefijo predeterminado del código del país para mensajes SMS de los destinatarios de la empresa. Este campo siempre comienza con un símbolo +.
   - Test Configuration. Haga clic para enviar un mensaje de prueba con la configuración actual. Los errores de conexión,

como los fallos de autenticación o de números de teléfonos virtuales, se detectan y aparecen inmediatamente. Los mensajes se reciben en el mismo período de tiempo que los que se envían entre teléfonos móviles.

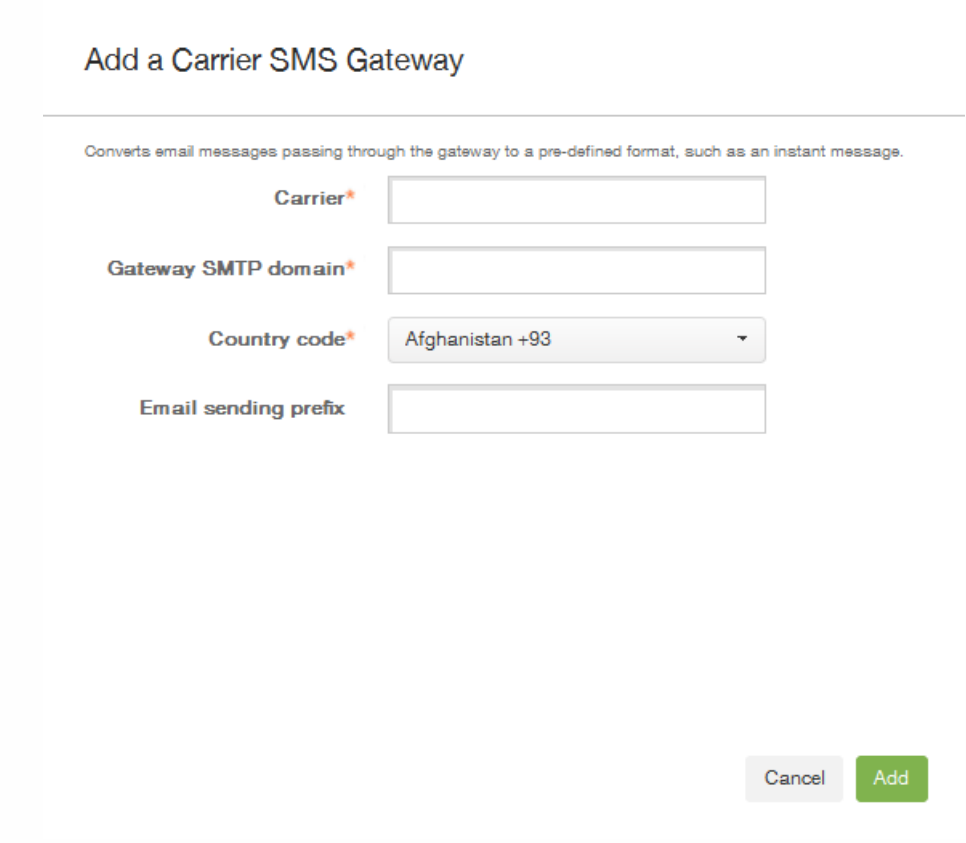
9. Haga clic en Agregar.

En XenMobile, puede establecer una puerta de enlace SMS de operador y, así, configurar las notificaciones que se envían a través de la puerta de enlace SMS de un operador. Los operadores utilizan las puertas de enlace Short Message Service (SMS) para enviar transmisiones SMS a una red de telecomunicaciones o recibir dichas transmisiones de una red de telecomunicaciones. Estos mensajes de texto usan protocolos de comunicación estandarizados para permitir que dispositivos de teléfono móvil o de línea fija intercambien mensajes cortos de texto.

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Carrier SMS Gateway. Se abrirá la página de configuración Carrier SMS Gateway.



2. Haga clic en Add para agregar un nuevo operador. Haga clic en Detect para detectar automáticamente una puerta de enlace. Aparecerá el cuadro de diálogo Add a Carrier SMS Gateway.



3. Nota: XenMobile solo admite el envío de mensajes SMS de Nexmo. Si aún no tiene una cuenta para usar la mensajería de Nexmo, visite su sitio Web para crear una.
    1. Carrier. Escriba el nombre del operador.
    2. Gateway SMTP domain. Escriba el dominio asociado a la puerta de enlace SMTP.
    3. Country code. En la lista, haga clic en el código del país del operador.
    4. Email sending prefix. Si lo prefiere, puede especificar un prefijo de envío de correo electrónico.

Certificados

Oct 31, 2016

En XenMobile, puede usar certificados para crear conexiones seguras y para autenticar usuarios.

De forma predeterminada, XenMobile incluye un certificado autofirmado de capa de sockets seguros (SSL), generado durante la instalación para proteger los flujos de comunicación con el servidor. Citrix recomienda reemplazar ese certificado SSL por un certificado SSL de confianza procedente de una entidad de certificación conocida.

XenMobile también usa su propio servicio de infraestructura de clave pública (PKI) u obtiene certificados de la entidad de certificación para los certificados de cliente. Todos los productos Citrix admiten certificados comodín y de nombre alternativo de sujeto (SAN). Para la mayoría de las implementaciones, solo se necesitan dos certificados SAN o comodín.

Para inscribir y administrar dispositivos iOS con XenMobile, debe configurar y crear un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Para obtener más información, consulte Solicitud de un certificado APNs.

En la siguiente tabla se muestran los formatos y los tipos de certificado para cada componente de XenMobile:

Componente XenMobile	Formato del certificado	Tipo de certificado requerido
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL, raíz NetScaler Gateway convierte automáticamente el formato PFX en PEM.
Servidor XenMobile	PEM o PFX (PKCS#12)	SSL, SAML, APNs XenMobile también genera una infraestructura de clave pública completa durante el proceso de instalación. XenMobile Server no respalda certificados con la extensión PEM. Use el comando openssl para generar un archivo PFX a partir del archivo PEM: openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX (PKCS#12)	SSL, raíz

XenMobile respalda los certificados SSL de escucha y certificados de cliente con longitudes de bits de 4096, 2048 y 1024. Tenga en cuenta que el riesgo es alto con certificados de 1024 bits.

Para NetScaler Gateway y el servidor XenMobile, Citrix recomienda obtener certificados de servidor procedentes de una entidad de certificación pública, como VeriSign, DigiCert o Thawte. Puede crear una solicitud de firma de certificado (CSR) desde la herramienta de configuración de NetScaler Gateway o de XenMobile. Después de crear la solicitud de firma de

certificado, envíela a la entidad de certificación para que la firme. Cuando la entidad de certificación devuelva el certificado firmado, podrá instalarlo en NetScaler Gateway o XenMobile.

NetScaler Gateway admite certificados de cliente para la autenticación. Los usuarios que inician sesiones en NetScaler Gateway también se pueden autenticar con los atributos del certificado del cliente que se presenta ante el servidor virtual. La autenticación de certificados de cliente también puede utilizarse con otro tipo de autenticación, como LDAP o RADIUS, para la autenticación de dos factores.

Para autenticar usuarios basándose en los atributos del certificado del cliente, la autenticación de clientes debe estar habilitada en el servidor virtual y se debe solicitar el certificado del cliente. Es necesario vincular un certificado raíz al servidor virtual de NetScaler Gateway.

La autenticación de dispositivos con Netscaler Gateway no recibe respaldo para certificados obtenidos a través de una entidad de certificación (CA) discrecional.

Cuando los usuarios inician sesiones en NetScaler Gateway, después de la autenticación, la información de nombre de usuario se extrae del campo especificado del certificado. Normalmente, este campo es Sujeto:CN. Si el nombre de usuario se extrae correctamente, se puede autenticar al usuario con éxito. Si el usuario no presenta un certificado válido durante la conexión de Secure Sockets Layer (SSL), o si falla la extracción del nombre de usuario, la autenticación también fallará.

Se puede autenticar usuarios basándose en el certificado del cliente, definiendo el tipo de autenticación predeterminado para que use el certificado del cliente. También se puede crear una acción de certificado que defina lo que hay que hacer durante la autenticación basada en un certificado SSL del cliente.

La función de integración de infraestructuras de clave pública (PKI) de XenMobile permite administrar la distribución y el ciclo de vida de los certificados de seguridad en los dispositivos.

XenMobile crea una infraestructura de clave pública interna para la autenticación de dispositivos durante el proceso de instalación.

Las infraestructuras de clave pública externas también se pueden usar para emitir certificados para los dispositivos que se van a utilizar en las directivas de configuración o para la autenticación de cliente ante NetScaler Gateway.

La función principal del sistema de PKI es la entidad de infraestructura de clave pública. Una entidad de infraestructura PKI modela un componente back-end para las operaciones de PKI. Este componente forma parte de la infraestructura empresarial, como una infraestructura de clave pública de Microsoft, RSA, Entrust, Symantex u OpenTrust. La entidad de infraestructura PKI gestiona la emisión y la revocación de certificados back-end. La entidad de infraestructura PKI es el origen de autoridad para el estado del certificado. Por regla general, la configuración de XenMobile contiene exactamente una entidad de infraestructura PKI por componente back-end de PKI.

La segunda función del sistema de PKI es el proveedor de credenciales. Un proveedor de credenciales es una configuración específica de emisión y ciclo de vida de certificados. El proveedor de credenciales se encargará de aspectos como el formato del certificado (sujeto, clave, algoritmos) y las condiciones para su renovación o revocación, si las hubiera. Los proveedores de credenciales delegan operaciones a las entidades de infraestructura PKI. En otras palabras, aunque los proveedores de credenciales gestionan cuándo y con qué datos se llevan a cabo las operaciones de PKI, las entidades de infraestructura PKI controlan cómo se realizan esas operaciones. Por regla general, la configuración de XenMobile contiene varios proveedores de credenciales por entidad de infraestructura PKI.

Administración de certificados en XenMobile

Se recomienda hacer un seguimiento de los certificados que utilice en la implementación de XenMobile, sobre todo de sus fechas de caducidad y sus contraseñas respectivas. El objetivo de esta sección es facilitarle la tarea de administración de certificados en XenMobile.

Su entorno puede contener alguno o todos los certificados siguientes:

XenMobile Server
Certificado SSL para FQDN de MDM
Certificado SAML (para ShareFile)
Certificados de CA raíz e intermedios para los certificados anteriores y otros recursos internos (StoreFront, Proxy, etc.)
Certificado APNs para la administración de dispositivos iOS
Certificado APNs interno para notificaciones XMS de WorxHome
Certificado de usuario PKI para la conectividad con PKI

MDX Toolkit
Certificado de desarrollador de Apple
Perfil de aprovisionamiento de Apple (por aplicación)
Certificado APNs de Apple (para usar con WorxMail)
Archivo JKS de Android
Certificado Windows Phone – Symantec

NetScaler
Certificado SSL para FQDN de MDM
Certificado SSL para FQDN de Gateway
Certificado SSL para FQDN de StorageZones Controller de ShareFile
Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)
Certificado SSL para el equilibrio de carga con StoreFront
Certificados de CA raíz e intermedios para los certificados anteriores

Si un certificado caduca, dejará de ser válido, por lo que no podrá seguir ejecutando operaciones seguras en su entorno ni acceder a los recursos de XenMobile.

> ## Nota
>
> La entidad de certificación (CA) le pedirá que renueve su certificado SSL antes de la fecha de caducidad.

Como los certificados de Apple Push Notification service (APNs) caducan al año, cree un nuevo certificado SSL de Apple Push Notification service y actualícelo en el portal de Citrix antes de que caduque. Si el certificado caduca, los usuarios sufrirán interrupciones del servicio de notificaciones push de WorxMail. Tampoco podrá seguir enviando notificaciones push a sus aplicaciones.

Para inscribir y administrar dispositivos iOS en XenMobile, debe configurar y crear un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Si el certificado caduca, los usuarios no podrán inscribirse en XenMobile y usted no podrá administrar sus dispositivos iOS. Para obtener más información, consulte Solicitud de un certificado APNs.

Para ver el estado y la fecha de caducidad del certificado APNs, inicie sesión en el portal Apple Push Certificate Portal. Debe iniciar sesión con el mismo usuario con que creó el certificado.

Asimismo, Apple le enviará una notificación por correo electrónico 30 y 10 días antes de la fecha de caducidad. Esa notificación contendrá un mensaje del tipo:

"El siguiente certificado Apple Push Notification Service, creado para el ID de cliente o ID de Apple caducará el DD/MM/AAAA. Revocar este certificado o dejar que caduque tendrá como consecuencia que los dispositivos existentes deban volver a inscribirse con un nuevo certificado push.

Póngase en contacto con su proveedor para generar una nueva solicitud (una solicitud de firma de certificado firmada) y vaya a https://identity.apple.com/pushcert para renovar su certificado Apple Push Notification Service.

Atentamente,

Servicio de notificaciones push de Apple"

Cualquier aplicación que se ejecute en un dispositivo iOS físico (aparte de las aplicaciones del App Store de Apple) debe estar firmada con un perfil de aprovisionamiento y un certificado de distribución correspondiente.

Tenga en cuenta que el certificado existente de iOS Developer for Enterprise y el perfil de aprovisionamiento pueden no ser compatibles con iOS 9. Para obtener información más detallada, consulte "Empaquetado de aplicaciones Worx para iOS 9".

Para comprobar que dispone de un certificado de distribución iOS válido, lleve a cabo lo siguiente:

1. Desde el portal Apple Enterprise Developer, cree un ID de aplicación explícito para cada aplicación que quiera empaquetar con MDX Toolkit. Un ejemplo de un ID de aplicación válido es: com.NombreEmpresa.NombreProducto.
2. Desde el portal Apple Enterprise Developer, vaya a **Provisioning Profiles** > **Distribution** y cree un perfil de aprovisionamiento interno. Repita este paso para cada ID de aplicación que haya creado en el paso anterior.
3. Descargue todos los perfiles de aprovisionamiento. Para obtener más información, consulte Empaquetado de aplicaciones móviles iOS.

Para confirmar que todos los certificados de servidor XenMobile son válidos, lleve a cabo lo siguiente:

1. En la consola de XenMobile, haga clic en **Settings** y, a continuación, en **Certificates**.
2. Compruebe que todos los certificados (APNS, escucha de SSL, raíz e intermedio) son válidos.

KeyStore es un archivo que contiene los certificados utilizados para firmar su aplicación de Android. Cuando caduca el período de validez de su clave, los usuarios ya no pueden actualizarse a nuevas versiones de su aplicación.

Symantec es el proveedor exclusivo de certificados de firma de código para el servicio App Hub de Microsoft. Los desarrolladores y los editores de software se registran en App Hub para distribuir aplicaciones Windows Phone y Xbox 360 que a continuación se pueden descargar desde el catálogo de soluciones de Windows. Para obtener información más detallada, consulte Symantec Code Signing Certificates for Windows Phone en la documentación de Symantec.

Si el certificado caduca, los usuarios de Windows Phone no podrán inscribirse, instalar aplicaciones publicadas y firmadas por la empresa ni iniciar aplicaciones de empresa que estén instaladas en el teléfono.

Para obtener información más detallada sobre cómo gestionar los certificados de NetScaler que caducan, consulte How to handle certificate expiry on NetScaler en Knowledge Center de la asistencia de Citrix.

Si un certificado de NetScaler caduca, los usuarios no podrán inscribirse, acceder a Worx Store, conectarse al servidor Exchange cuando utilicen WorxMail ni enumerar o abrir aplicaciones HDX (según el certificado caducado).

Command Center (Centro de comandos) y Expiry Monitor (Centro de supervisión de caducidad) son dos herramientas que pueden ayudarle a hacer un seguimiento de los certificados de NetScaler y notificarle cuando estos caduquen. Esas dos herramientas ayudan a supervisar los siguientes certificados de Netscaler:

Certificado SSL para FQDN de MDM
Certificado SSL para FQDN de Gateway
Certificado SSL para FQDN de StorageZones Controller de ShareFile
Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)
Certificado SSL para el equilibrio de carga con StoreFront
Certificados de CA raíz e intermedios para los certificados anteriores

Carga de certificados en XenMobile

May 05, 2016

El servidor XenMobile utiliza certificados de manera funcional. Puede cargar certificados en XenMobile desde el área Certificates de la consola de XenMobile. En el grupo de certificados se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar el área Certificates como almacén para los certificados que quiera implementar en los dispositivos. Este uso se aplica especialmente a certificados de CA utilizados para establecer una relación de confianza en el dispositivo.

Cada certificado cargado se representa mediante una entrada en la tabla Certificates, con un resumen de su contenido. Cuando configure los componentes de integración de PKI que requieran un certificado, se le solicitará elegir un certificado de una lista de aquellos certificados de servidor que cumplan los criterios de contexto. Por ejemplo, es posible que quiera configurar XenMobile para integrarlo con la entidad de certificación (CA) de Microsoft. La conexión a la entidad de certificación de Microsoft debe autenticarse mediante un certificado de cliente.

Requisitos de clave privada

XenMobile puede contener o no la clave privada de un certificado determinado. Del mismo modo, XenMobile puede requerir o no una clave privada para los certificados que usted cargue.

Carga de certificados en la consola

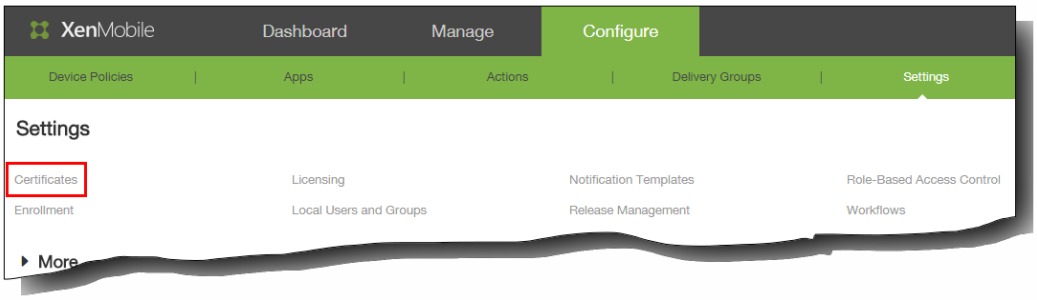
Puede cargar el certificado de CA (sin la clave privada) que usará la entidad de certificación para firmar las solicitudes. También puede cargar un certificado SSL de cliente (con la clave privada) para la autenticación de cliente. Cuando configure la entidad de certificación de Microsoft, es necesario especificar el certificado de CA. Podrá elegirlo de una lista que contiene todos los certificados de servidor que son certificados de CA. Del mismo modo, cuando configure la autenticación de cliente, podrá seleccionar un certificado de servidor de una lista que contiene todos los certificados de servidor para los que XenMobile tiene la clave privada.

XenMobile admite los siguientes formatos de entrada para los certificados:

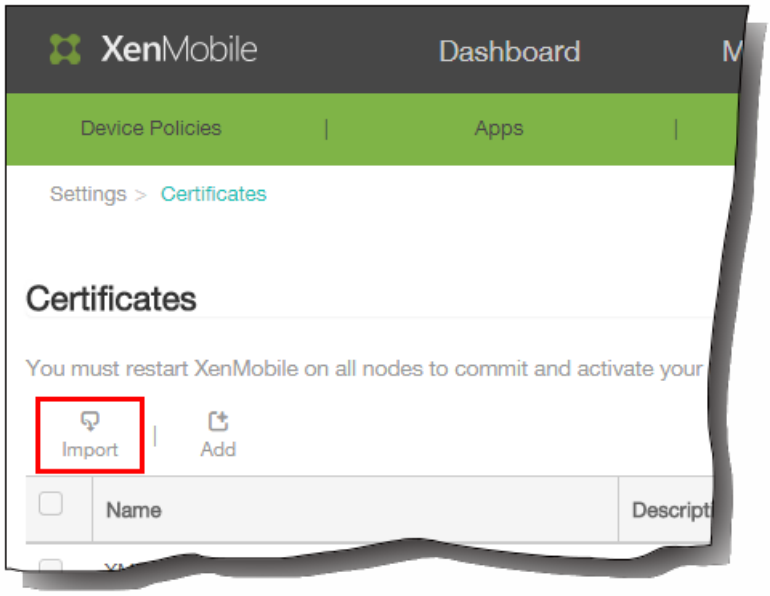
- Archivos de certificado cifrados en DER o PEM
- Archivos de certificado cifrados en DER o PEM con un archivo asociado de clave privada cifrado en DER o PEM
- Almacenes de claves PKCS #12 (P12, también conocido como archivo PFX en Windows)

Los almacenes de claves, por diseño, pueden contener varias entradas. Al cargar entradas de un almacén de claves, por lo tanto, se le solicitará que especifique el alias de entrada que identifica la entrada que quiera cargar. Si no se especifica ningún alias, se cargará la primera entrada del almacén. Como los archivos PKCS #12 suelen contener solo una entrada, el campo de alias no aparece cuando se selecciona PKCS #12 como tipo de almacén de claves.

1. En la consola de XenMobile, haga clic en Configure > Settings > Certificates.

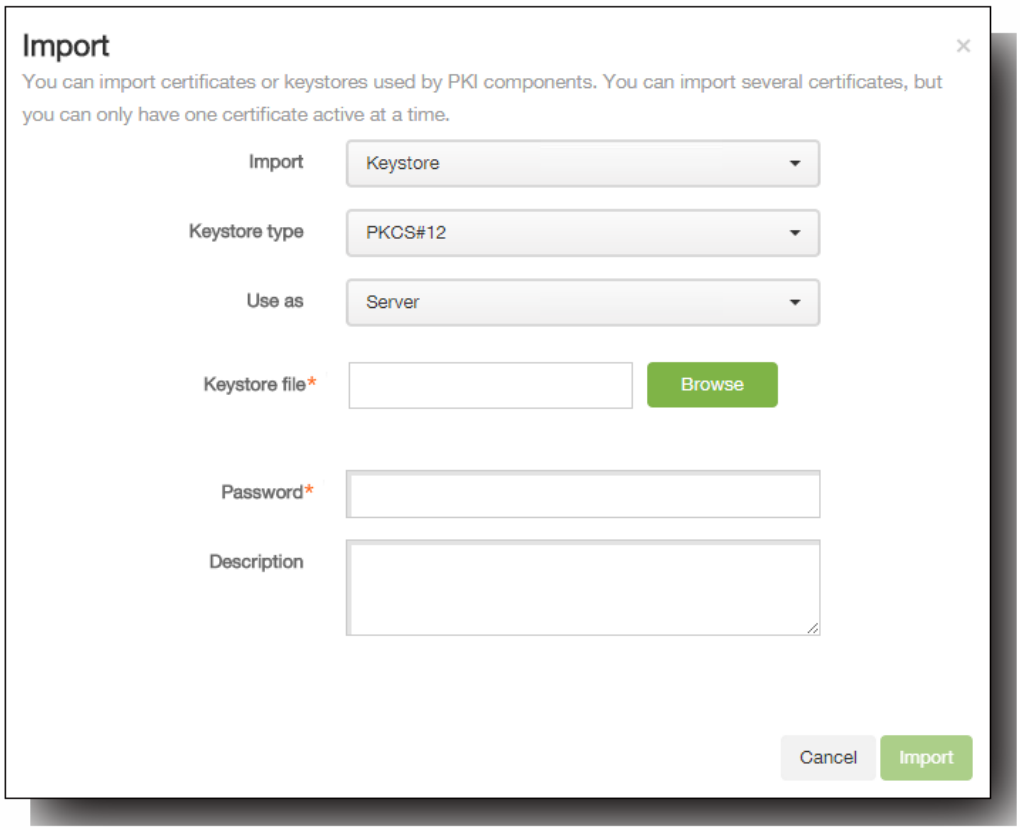


2. En la página Certificates, haga clic en Import.



Aparecerá el cuadro de diálogo Import.

3. En el cuadro de diálogo Import, en Import, haga clic en Keystore.



El cuadro de diálogo Import cambiará para reflejar las opciones disponibles del almacén de claves, como se muestra en la ilustración anterior.

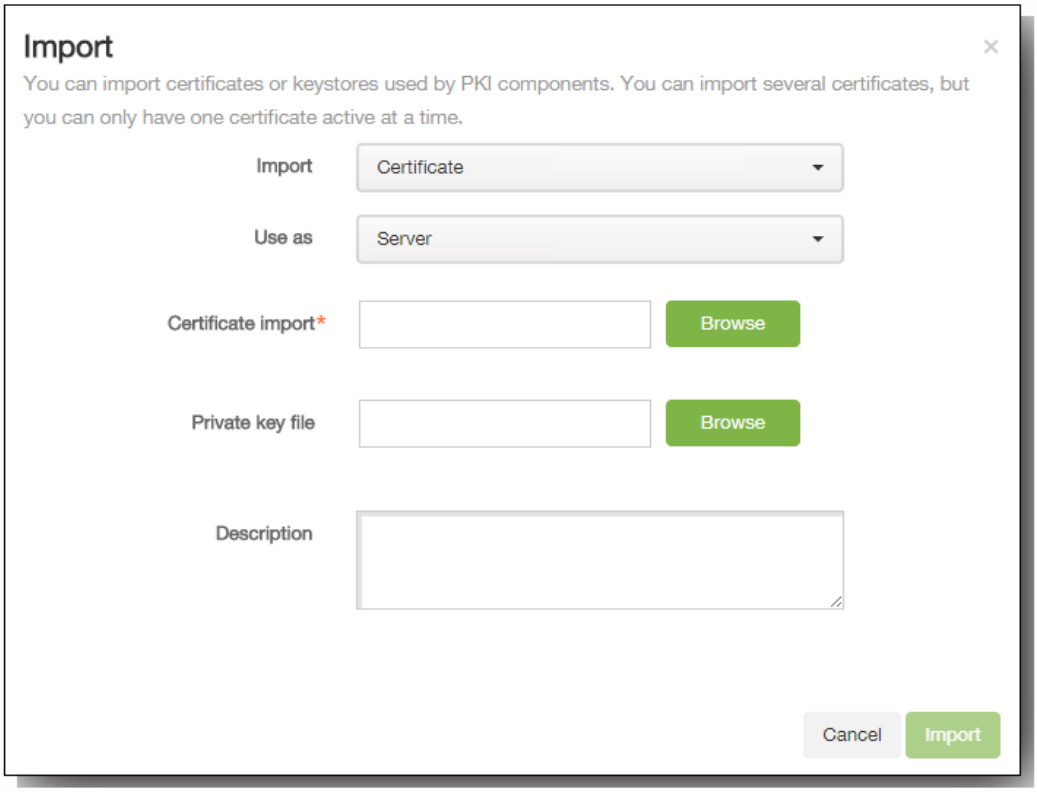
4. En el tipo Keystore, haga clic en PKCS#12.
5. En Use as, haga clic en la forma en que se usará el almacén de claves. Las opciones disponibles son:
   - **Server**. Los certificados de servidor son aquellos que usa el servidor XenMobile de manera funcional, que se cargan en la consola Web de XenMobile. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Este uso se aplica especialmente a certificados de entidades de certificación utilizados para establecer una relación de confianza en el dispositivo.
   - **SAML**. La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On (SSO) a los servidores, los sitios Web y las aplicaciones.
   - **APNs**. Los certificados del servicio de notificaciones push de Apple (APN) permiten la administración de dispositivos móviles a través de Apple Push Network.
   - **SSL Listener**. La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.
6. Busque el almacén de claves a importar.
7. En Password, escriba la contraseña asignada al certificado.
8. Si quiere, escriba una descripción del almacén de claves que le ayude a distinguirlo de otros almacenes.
9. Haga clic en Import. El almacén de claves se agrega a la tabla Certificates.

Al importar un certificado (ya sea mediante un archivo o mediante una entrada del almacén de claves), XenMobile intenta crear una cadena de certificados desde la entrada, e importa todos los certificados de esa cadena (con lo que creará una

entrada de certificado de servidor para cada certificado). Esta operación solo funciona si los certificados del archivo o de la entrada del almacén de claves forman una cadena; por ejemplo, si cada certificado de la cadena es el emisor del anterior.

Si lo prefiere, puede agregar una descripción para el certificado importado. La descripción solo se vincula al primer certificado de la cadena. Más tarde, podrá actualizar la descripción de los certificados restantes.

1. En la consola de XenMobile, haga clic en Configure > Settings > Certificates.
2. En la página Certificates, haga clic en Import. Aparecerá el cuadro de diálogo Import.
3. En el cuadro de diálogo Import, en Import, si no se ha seleccionado ya, haga clic en Certificate.



El cuadro de diálogo Import cambiará para reflejar las opciones de certificado disponibles.

4. En Use as, haga clic en la forma en que se usará el almacén de claves. Las opciones disponibles son:
   - **Server**. Los certificados de servidor son aquellos que usa el servidor XenMobile de manera funcional, que se cargan en la consola Web de XenMobile. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Esta opción se aplica especialmente a entidades de certificación utilizadas para establecer una relación de confianza en el dispositivo.
   - **SAML**. La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On (SSO) a los servidores, los sitios Web y las aplicaciones.
   - **SSL Listener**. La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.
5. Busque el certificado a importar.
6. Busque el archivo de clave privada optativa del certificado. Junto con el certificado, la clave privada se usa para el cifrado y el descifrado.
7. Si quiere, escriba una descripción del certificado que le ayude a distinguirlo de otros certificados.

8. Haga clic en Import. El certificado se agrega a la tabla Certificates.

XenMobile solo permite que exista un certificado por clave pública en el sistema y en un momento dado. Si intenta importar un certificado del mismo par de claves que un certificado ya importado, tendrá la opción de reemplazar la entrada existente o de eliminarla.

Para actualizar certificados de forma más eficaz, en la consola de XenMobile, en Configure > Settings > Certificates, en el cuadro de diálogo Import, importe el certificado nuevo. Cuando se actualice un certificado del servidor, los componentes que utilizaban el certificado anterior empiezan automáticamente a utilizar el nuevo. Del mismo modo, si ha implementado el certificado de servidor en dispositivos, el certificado se actualizará automáticamente en la siguiente implementación.

Entidades de infraestructura PKI

May 05, 2016

La configuración de una entidad de infraestructura de clave pública (PKI) de XenMobile representa un componente que lleva a cabo operaciones de PKI (emisión, revocación e información de estado). Estos componentes pueden ser internos de XenMobile, (en cuyo caso se llaman discrecionales) o externos a XenMobile (si forman parte de la infraestructura corporativa).

XenMobile admite los siguientes tipos de entidades de infraestructura PKI:

- Entidades de certificación discrecionales (CA)
- Infraestructuras de clave pública genéricas (GPKI)
- Microsoft Certificate Services

XenMobile respalda el uso de los siguientes servidores de CA:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Independientemente de su tipo, cada entidad de infraestructura de clave pública (PKI) tiene un subconjunto de las siguientes funciones:

- sign: Emitir un nuevo certificado a partir de una solicitud de firma de certificado (CSR).
- fetch: Recuperar un par de claves y un certificado existentes.
- revoke: Revocar un certificado de cliente.

Acerca de los certificados de CA

Cuando configure una entidad de infraestructura PKI, deberá indicar a XenMobile el certificado de CA que va a actuar como firmante de los certificados que esta entidad emita (o de aquellos certificados que se recuperen de ella). La misma y única entidad de infraestructura PKI puede devolver certificados (ya sean recuperados o recién firmados) que haya firmado una cantidad indefinida de entidades de certificación (CA). Debe proporcionar el certificado de cada una de estas entidades de certificación como parte de la configuración de la entidad de infraestructura PKI. Para ello, cargue los certificados a XenMobile y, a continuación, vincúlelos en la entidad de infraestructura PKI. En caso de entidades de certificación discrecionales, el certificado es, de forma implícita, el certificado de la entidad de certificación que firma. En cambio, en caso de entidades externas, deberá especificarlo manualmente.

El protocolo de infraestructura de clave pública genérica (GPKI) es un protocolo de XenMobile propietario que se ejecuta sobre una capa de servicios Web SOAP con la finalidad de uniformar la interacción con las interfaces de varias soluciones de infraestructura de clave pública. El protocolo GPKI define las siguientes tres operaciones fundamentales de infraestructura de clave pública:

- sign. El adaptador puede hacerse cargo de las solicitudes de firma de certificado (CSR), transmitirlas a la infraestructura de clave pública y devolver los certificados recién firmados.
- fecth. El adaptador puede recuperar certificados y pares de claves existentes (según los parámetros de entrada) de la

infraestructura de clave pública.
- revoke. El adaptador puede hacer que la infraestructura de clave pública revoque un certificado existente.

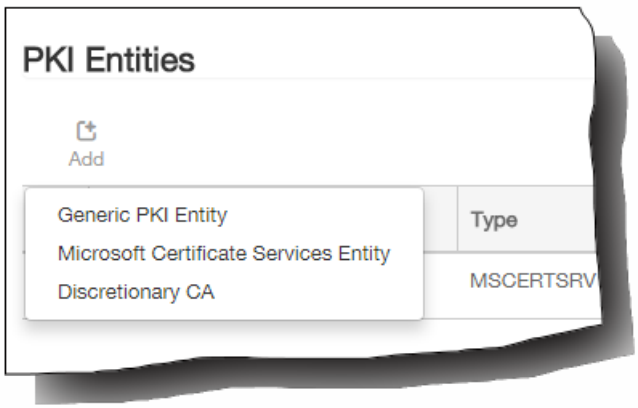
El receptor final del protocolo GPKI es el adaptador de GPKI. El adaptador traduce las operaciones fundamentales para el tipo específico de infraestructura de clave pública para el que se creó. En otras palabras, hay un adaptador de GPKI para RSA, otro para EnTrust, y así sucesivamente.

El adaptador de GPKI, como punto final de servicios Web SOAP, publica un archivo (o definición) en formato WSDL (Web Services Description Language) que se puede analizar de forma autónoma. Crear una entidad de infraestructura de clave pública genérica significa facilitar a XenMobile esa definición en formato WSDL, ya sea a través de una dirección URL o cargando el archivo en cuestión.

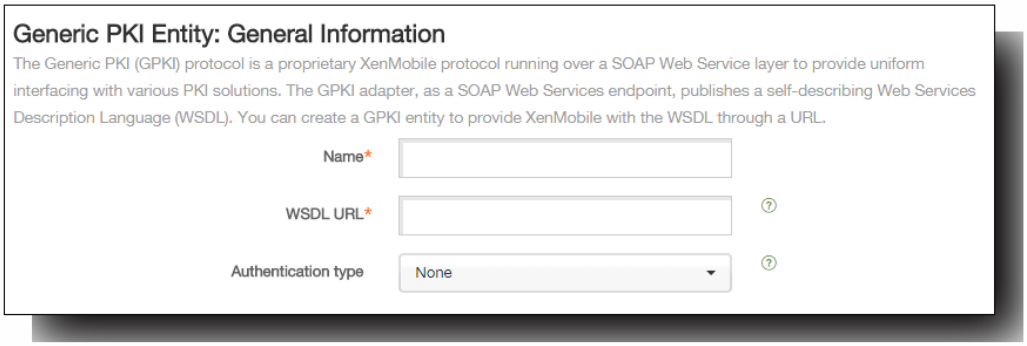
Admitir cada una de las operaciones de PKI en un adaptador es opcional. Si un adaptador admite esa operación, es que tiene la funcionalidad correspondiente (firmar, obtener o revocar). Cada una de estas capacidades se puede asociar a un conjunto de parámetros de usuario.

Los parámetros de usuario son aquellos parámetros que define el adaptador de GPKI para una operación específica, y cuyos valores debe proporcionar a XenMobile. Tras analizar el archivo WSDL, XenMobile determina las operaciones que admite el adaptador (las capacidades que tiene) y los parámetros que necesita para cada una de ellas. Si lo prefiere, utilice la autenticación SSL de cliente para proteger la conexión entre XenMobile y el adaptador de GPKI.

1. En la consola de XenMobile, haga clic en Configure > Settings > More > PKI Entities.
2. En la página PKI Entities, haga clic en Add.
   Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.



3. Haga clic en Generic PKI Entity.
   Aparecerá la página Generic PKI Entity: General Information.



4. En la página Generic PKI Entity: General Information, lleve a cabo lo siguiente:
   1. Name. Escriba un nombre descriptivo para la entidad de infraestructura PKI.
   2. WSDL URL. Escriba la ubicación del archivo WSDL que describe el adaptador.
   3. Authentication type. Haga clic en el método de autenticación que se va a utilizar.
      - Ninguno.
      - HTTP Basic. Proporcione el nombre de usuario y la contraseña necesarios para conectarse al adaptador.
      - Client certificate. Seleccione el certificado SSL de cliente correspondiente.
   4. Haga clic en Siguiente.
      Aparecerá la página Generic PKI Entity: Adapter Capabilities.

5. En la página Generic PKI Entity: Adapter Capabilities, revise las funciones y los parámetros asociados al adaptador y, a continuación, haga clic en Next.
   Aparecerá la página Generic PKI Entity: Issuing CA Certificates.

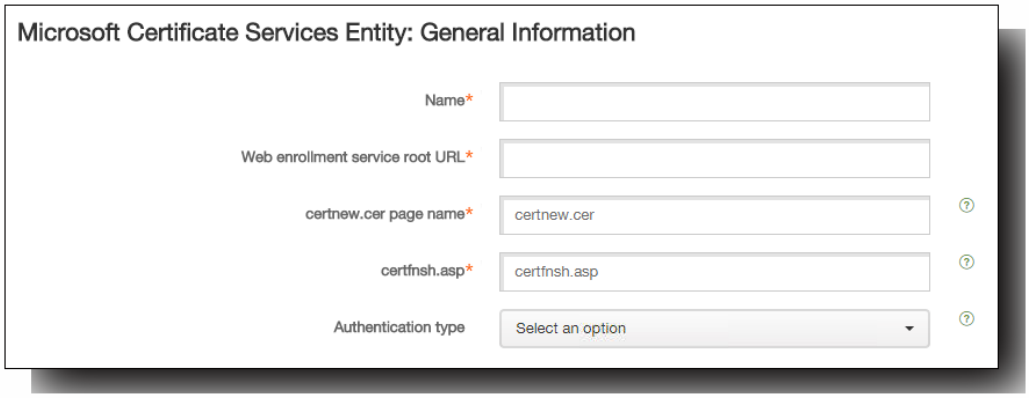
6. En la página Generic PKI Entity: Issuing CA Certificates, seleccione los certificados que se van a utilizar para la entidad.
   Nota: Aunque las entidades puedan devolver certificados firmados por entidades de certificación diferentes, todos los certificados obtenidos de un proveedor de certificados determinado deben estar firmados por la misma entidad de certificación. Por lo tanto, al configurar el parámetro Credential Provider, en la página Distribution, seleccione uno de los certificados configurados aquí.
7. Haga clic en Save.
   La entidad se muestra en la tabla PKI Entities.

XenMobile interactúa con Microsoft Certificate Services a través de su interfaz de inscripción Web. XenMobile admite solo la emisión de certificados nuevos a través de esa interfaz (el equivalente de la funcionalidad de firma de GPKI).

Para crear una entidad de certificación de infraestructura PKI de Microsoft en XenMobile, debe especificar la URL base de la interfaz Web de los Servicios de servidor de certificados. Si lo prefiere, utilice la autenticación SSL de cliente para proteger la conexión entre XenMobile y la interfaz Web de los Servicios de servidor de certificados.

1. En la consola de XenMobile, haga clic en Configure > Settings > More > PKI Entities.
2. En la página PKI Entities, haga clic en Add.
   Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.

3. Haga clic en Microsoft Certificate Services Entity.
   Aparecerá la página Microsoft Certificate Services Entity: General Information.



4. En la página Microsoft Certificate Services Entity: General Information, lleve a cabo lo siguiente:
   1. Name. Escriba un nombre para la nueva entidad. Lo utilizará más tarde para hacer referencia a esa entidad. Los nombres de entidad deben ser únicos.
   2. Web enrollment service root URL. Especifique la dirección URL base del servicio de inscripción Web de la entidad de certificación de Microsoft, como, por ejemplo, https://192.0.2.13/certsrv/. La URL puede usar HTTP sin formato o HTTP sobre SSL.
   3. certnew.cer page name. El nombre de la página certnew.cer. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.
   4. certfnsh.asp. El nombre de la página certfnsh.asp. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.
   5. Authentication type. Haga clic en el método de autenticación que se va a utilizar.
      - Ninguno.
      - HTTP Basic. Proporcione el nombre de usuario y la contraseña necesarios para la conexión.
      - Client certificate. Seleccione el certificado SSL de cliente correspondiente.
      - Haga clic en Siguiente.
        Aparece la página Microsoft Certificate Services Entity: Templates. En esta página, especifique los nombres internos de las plantillas que admite la entidad de certificación de Microsoft. Cuando cree proveedores de credenciales, seleccione una plantilla de la lista definida aquí. Todos los proveedores de credenciales que utilicen esta entidad se valen de una plantilla exactamente igual.

5. En la página Microsoft Certificate Services Entity: Templates, haga clic en Add, escriba el nombre de la plantilla y, a continuación, haga clic en Save. Repita este paso para cada plantilla a agregar.
6. Haga clic en Next.
   Aparecerá la página Microsoft Certificate Services Entity: HTTP parameters. En esta página, puede especificar parámetros personalizados que XenMobile debe insertar en la solicitud HTTP para la interfaz de inscripción Web de Microsoft. Esta opción solo es útil si tiene scripts personalizados que se ejecutan en la entidad de certificación.

7. En la página Microsoft Certificate Services Entity: HTTP parameters, haga clic en Add, escriba el nombre y el valor de los parámetros HTTP a agregar y, a continuación, haga clic en Next.
   Aparecerá la página Microsoft Certificate Services Entity: CA Certificates. En esta página, debe indicar a XenMobile los firmantes de los certificados que el sistema va a obtener a través de esta entidad. Cuando se renueve el certificado de CA, actualícelo en XenMobile, y el cambio se aplicará a la entidad de forma transparente.

8. En la página Microsoft Certificate Services Entity: CA Certificates, seleccione los certificados que se van a utilizar para la entidad.

9. Haga clic en Save.
   La entidad se muestra en la tabla PKI Entities.

Se crea una entidad de certificación discrecional al proporcionar a XenMobile un certificado de CA y la clave privada asociada. XenMobile gestiona la emisión, la revocación y la información de estado de certificados internamente en función de los parámetros especificados.

Cuando configure una entidad de certificación discrecional, dispone de la opción para activar el respaldo del protocolo Online Certificate Status Protocol (OCSP) para dicha entidad de certificación. Si (y solo si) se habilita el respaldo de OCSP, la entidad de certificación agrega una extensión id-pe-authorityInfoAccess a los certificados que emita la entidad de certificación, y apuntará al respondedor OCSP interno de XenMobile en la siguiente ubicación.

https://server/instance/ocsp
Al configurar el servicio OCSP, debe especificar un certificado de firma de OCSP para la entidad discrecional en cuestión. Puede usar el certificado de CA en sí como firmante. Para evitar una exposición innecesaria de la clave privada de la entidad de certificación (recomendado), cree un certificado de firma de OCSP delegado, firmado por la entidad de certificación, e incluya una extensión id-kp-OCSPSigning extendedKeyUsage.

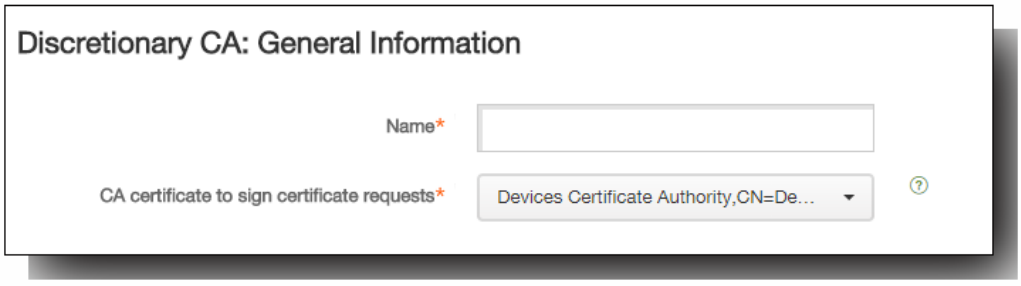
El servicio de respondedor OCSP de XenMobile respalda el uso de respuestas de OCSP básicas y los siguientes algoritmos de hash en las solicitudes:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Las respuestas se firman con SHA-256 y el algoritmo de clave del certificado de firma (DSA, RSA o ECDSA).

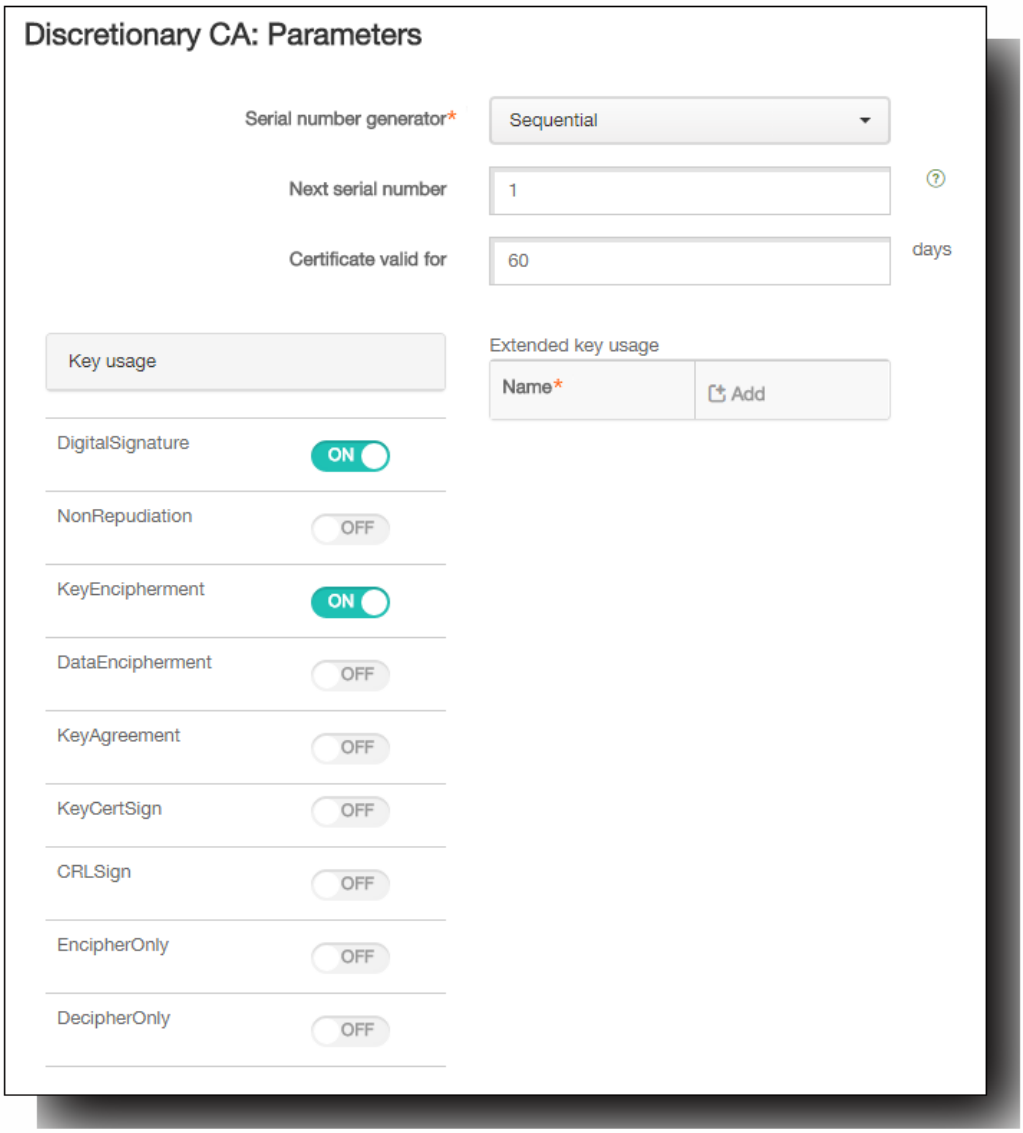
1. En la consola de XenMobile, haga clic en Configure > Settings > More > PKI Entities.
2. En la página PKI Entities, haga clic en Add.
   Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.

3. Haga clic en Discretionary CA.
   Aparece la página Discretionary CA: General Information.



4. En la página Discretionary CA: General Information, lleve a cabo lo siguiente:

1. Name. Escriba un nombre descriptivo para la entidad de certificación discrecional.
2. CA certificate to sign certificate requests. Haga clic en un certificado de la entidad de certificación discrecional que se utilizará para firmar solicitudes de certificados. Esta lista de certificados se genera a partir de los certificados de CA con las claves privadas que se cargaron en XenMobile, en Configure > Settings > Certificates.
3. Haga clic en Siguiente.
   Aparece la página Discretionary CA: Parameters.



5. En la página Discretionary CA: Parameters, lleve a cabo lo siguiente:
   1. Serial number generator. La entidad de certificación discrecional genera números de serie para los certificados que emite. En esta lista, haga clic en Sequential o en Non-sequential para determinar el modo en que se generan los números.
   2. Next serial number. Escriba un valor para determinar el siguiente número a emitir.
   3. Certificate valid for. Escriba la cantidad de días durante los que el certificado será válido.
   4. Key usage. Identifique el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, deberá establecer las claves apropiadas en On. Una vez establecidas, la entidad de certificación está limitada a la emisión de certificados para esos fines.

5. Extended key usage. Para agregar parámetros adicionales, haga clic en Add, escriba el nombre de la clave y, a continuación, haga clic en Save.
6. Haga clic en Siguiente.
   Aparecerá la página Discretionary CA: Distribution.

6. En la página Discretionary CA: Distribution, seleccione un modo de distribución:
   - Centralized: server-side key generation. Citrix recomienda la opción centralizada. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
   - Distributed: device-side key generation. Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
7. Haga clic en Next.
   Aparece la página Discretionary CA: Online Certificate Status Protocol (OCSP).

8. En la página Discretionary CA: Online Certificate Status Protocol (OCSP), lleve a cabo lo siguiente:
   1. Para agregar una extensión AuthorityInfoAccess (RFC2459) a los certificados firmados por esta entidad de certificación, establezca Enable OCSP support for this CA en On. Esta extensión apunta al respondedor OCSP de la entidad de certificación en https://server/instance/ocsp.
   2. Si ha habilitado el respaldo de OCSP, seleccione un certificado de firma de CA OSCP. Esta lista de certificados se genera a partir de los certificados de CA que se cargaron en XenMobile, en Configure > Settings > Certificates.
9. Haga clic en Save.
   La entidad de certificación discrecional se muestra en la tabla PKI Entitites.

Proveedores de credenciales

May 05, 2016

Los proveedores de credenciales son las configuraciones de certificado en cuestión que se usarán en las distintas partes del sistema de XenMobile. Definen las fuentes, los parámetros y los ciclos de vida de los certificados. También determinan si los certificados forman parte de configuraciones de dispositivo o son independientes; es decir, si se insertan tal cual en el dispositivo.

La inscripción de dispositivos limita el ciclo de vida de los certificados. Es decir, XenMobile no emite certificados antes de la inscripción, aunque XenMobile puede emitir algunos certificados como parte de la inscripción. Además, los certificados que emita la infraestructura de clave pública interna en el contexto de una inscripción se revocan cuando la inscripción en cuestión se revoca. Una vez que la relación de administración haya finalizado, no queda ningún certificado válido.

Puede usar una configuración de proveedores de credenciales en varios sitios, con lo que una sola configuración puede gestionar una cantidad infinita de certificados al mismo tiempo. Entonces, la unidad radica en el recurso de la implementación y en la implementación. Por ejemplo: si el proveedor de credenciales P se implementa en el dispositivo D como parte de la configuración C, los parámetros de emisión de P determinan el certificado que se implementará en D. Del mismo modo, los parámetros de renovación previstos para D se aplicarán cuando se actualice C, y los parámetros de revocación previstos para D también se aplicarán cuando C se elimine o cuando D se revoque.

Teniendo esto en cuenta, la configuración del proveedor de credenciales en XenMobile lleva a cabo lo siguiente:

- Determina la fuente de los certificados.
- Determina el método con que se obtienen los certificados: mediante la firma de un certificado nuevo o la obtención (recuperación) de un par de claves y un certificado existentes.
- Determina los parámetros para la emisión o la recuperación. Por ejemplo: los parámetros de la solicitud de firma de certificado (CSR), como el tamaño de la clave, el algoritmo de clave, el nombre distintivo y las extensiones del certificado, entre otros.
- Determina el modo en que los certificados se entregarán al dispositivo.
- Determina las condiciones de revocación. Mientras que todos los certificados se revocan en XenMobile cuando finaliza la relación de administración, la configuración puede especificar que la revocación ocurra antes; por ejemplo, cuando se elimina la configuración asociada al dispositivo. Además, en algunas ocasiones, la revocación del certificado asociado en XenMobile se puede enviar a la infraestructura de clave pública (PKI) back-end; es decir, la revocación en XenMobile puede causar la revocación en la infraestructura de clave pública.
- Determina los parámetros de renovación. Los certificados que se obtienen mediante un proveedor de credenciales determinado se pueden renovar automáticamente cuando se acerque su fecha de caducidad. Además, independientemente de esas circunstancias, se pueden emitir notificaciones cuando se acerque esa fecha de caducidad.

La disponibilidad de las opciones de configuración depende principalmente del tipo de entidad de infraestructura PKI y del método de emisión seleccionado para un proveedor de credenciales.

Puede obtener un certificado mediante procesos conocidos como métodos de emisión de dos maneras:

- sign. Con este método, la emisión implica crear una nueva clave privada, crear una solicitud de firma de certificado y enviar esa solicitud a una entidad de certificación (CA) para su firma. XenMobile respalda el método de firma de las tres entidades PKI (MS Certificate Services Entity, Generic PKI y Discretionary CA).
- fetch. Con este método, la emisión (en lo relativo a XenMobile) consiste en la recuperación de un par de claves que ya existe. XenMobile respalda el método "fetch" solo para Generic PKI.

Un proveedor de credenciales usa los métodos de emisión "sign" o "fetch". El método seleccionado determina las opciones de configuración disponibles. Por ejemplo, la configuración de las solicitudes de firma de certificado y la entrega distribuida solo están disponibles si el método de emisión es "sign". El certificado obtenido siempre se envía al dispositivo en formato PKCS #12, el equivalente del modo de entrega centralizado del método "sign".

En XenMobile, hay disponibles dos modos de entrega de certificados: centralizada y distribuida. El modo distribuido usa SCEP (Protocolo de inscripción de certificados simple) y solo está disponible en los casos en que el cliente admite el protocolo (solo para iOS). El modo distribuido llega a ser obligatorio en algunas situaciones.

Para que un proveedor de credenciales admita la entrega distribuida (mediante SCEP), se necesita un paso especial de configuración: se deben configurar certificados de una entidad de registro (RA). Los certificados de RA son necesarios porque, cuando se usa el protocolo SCEP, XenMobile actúa como un delegado (un registrador) para la entidad de certificación y debe demostrar al cliente que tiene autoridad para actuar como tal. Para establecer esta entidad, debe facilitar a XenMobile los certificados mencionados anteriormente.

Se necesitan dos roles de certificados (aunque un solo certificado pueda satisfacer ambos requisitos): la firma de RA y el cifrado de RA. A continuación se presentan las restricciones de esos roles:

- El certificado de firma de RA debe tener una firma digital de uso de clave X.509.
- El certificado de cifrado de RA debe tener un cifrado de clave de uso de clave X.509.

Para configurar los certificados de RA del proveedor de credenciales, usted debe cargarlos a XenMobile y, a continuación, vincularlos a ellos en el proveedor de credenciales.

Se considera que un proveedor de credenciales admite la entrega distribuida solamente si tiene un certificado configurado para los roles de certificado. Cada proveedor de credenciales se puede configurar para preferir el modo centralizado o el modo distribuido, o bien para requerir el modo distribuido. El resultado real depende del contexto: si el contexto no admite el modo distribuido mientras que el proveedor de credenciales lo requiere, la implementación falla. Del mismo modo, si el contexto requiere el modo distribuido pero el proveedor de credenciales no lo admite, la implementación falla. En todos los demás casos, se respeta la preferencia asignada.

En la siguiente tabla se muestra la distribución de SCEP mediante XenMobile:

Contexto	Se admite SCEP	Se requiere SCEP
Servicio de perfil de iOS	Sí	Sí
Inscripción y administración de dispositivos móviles iOS	Sí	No
Perfiles de configuración de iOS	Sí	No
Inscripción de SHTP	No	No
Configuración de SHTP	No	No
Inscripción de Windows Phone	No	No

Contexto	Se admite SCEP	Se requiere SCEP
Configuración de Windows Phone	No	No

Existen tres tipos de revocación.

- **Internal revocation** (Revocación interna). La revocación interna afecta al estado del certificado que mantiene XenMobile. Este estado se tiene en cuenta cuando XenMobile evalúa un certificado que se le presenta o cuando debe proporcionar información del estado OCSP de un certificado. La configuración del proveedor de credenciales determina el impacto sobre el estado cuando se dan varias condiciones. Por ejemplo, el proveedor de credenciales puede especificar que los certificados obtenidos mediante él deban marcarse como revocados cuando se hayan eliminado del dispositivo.
- **Externally propagated revocation** (Revocación propagada de forma externa). También conocida como revocación de XenMobile, este tipo de revocación se aplica a certificados obtenidos de una infraestructura de clave pública externa. Este certificado se revoca en la infraestructura de clave pública cuando XenMobile lo revoca internamente si se cumplen las condiciones definidas en la configuración del proveedor de credenciales. La llamada para realizar la revocación requiere una entidad de infraestructura de clave pública genérica (GPKI) que tenga la capacidad de revocar.
- **Externally induced revocation** (Revocación inducida externamente). También conocida como infraestructura de clave pública de revocación, este tipo de revocación también se aplica solo a certificados obtenidos de una infraestructura de clave pública externa. Siempre que XenMobile evalúa el estado de un certificado concreto, XenMobile consulta ese estado a la infraestructura de clave pública. Si el certificado se revoca, XenMobile lo revoca internamente. Este mecanismo utiliza el protocolo OCSP.

Estos tres tipos de revocación no se excluyen mutuamente, sino que se pueden aplicar de forma conjunta: la revocación interna se produce por una revocación externa o por otros motivos; a su vez, la revocación interna tiene como resultado potencial una revocación externa.

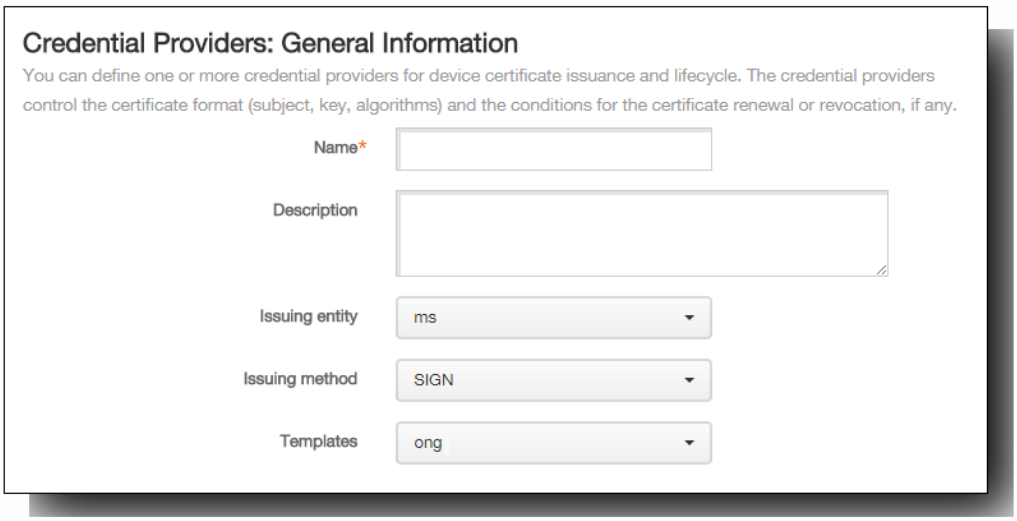
La renovación de un certificado es la combinación de una revocación del certificado existente y una emisión de otro certificado.

Tenga en cuenta que XenMobile primero intenta obtener el nuevo certificado antes de revocar el anterior a fin de evitar la interrupción del servicio si la emisión falla. Si se usa la entrega distribuida (respaldada por SCEP), la revocación a su vez se dará solo cuando el certificado se haya instalado correctamente en el dispositivo; de lo contrario, la revocación se produce antes de que el nuevo certificado se envíe al dispositivo, independientemente del resultado de la instalación.

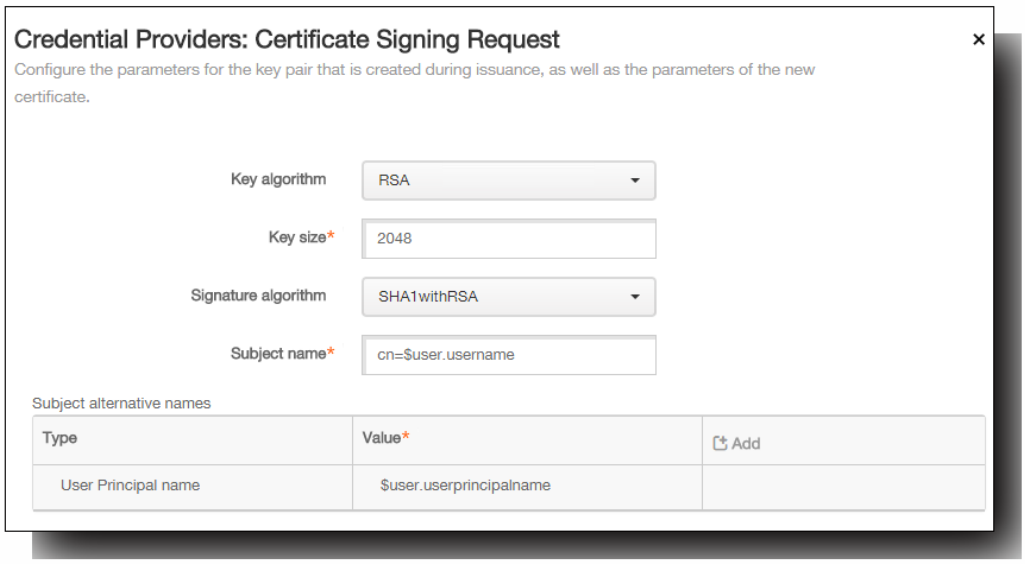
La configuración de la revocación requiere que especifique una duración (en días). Cuando el dispositivo se conecta, el servidor comprueba si la fecha NotAfter del certificado es posterior a la fecha actual, menos el tiempo especificado. Si lo es, se empieza una renovación.

La configuración de un proveedor de credenciales varía principalmente en la entidad de emisión y el método de emisión elegidos para el proveedor de credenciales. Puede distinguir entre un proveedor de credenciales que usa una entidad interna (por ejemplo, discrecional) y un proveedor de credenciales que usa una entidad externa, como una infraestructura GPKI o una entidad de certificación de Microsoft. El método de emisión de una entidad discrecional es siempre "sign", de manera que, con cada operación de emisión, XenMobile firma un nuevo par de claves con el certificado de CA seleccionado para la entidad. El método de distribución seleccionado determina si el par de claves se genera en el dispositivo o en el servidor.

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Credential Providers.
2. En la página Credential Providers, haga clic en Add.
   Aparecerá la página Credential Providers: General Information.



3. En la página Credential Providers: General Information, lleve a cabo lo siguiente:
   1. Name. Escriba un nombre exclusivo para la configuración del nuevo proveedor. Este nombre se usará posteriormente para hacer referencia a la configuración en otras partes de la consola de XenMobile.
   2. Description. Describa el proveedor de credenciales. Aunque este campo sea optativo, una descripción puede resultar útil más adelante para ayudarle a recordar datos concretos acerca de este proveedor de credenciales.
   3. Issuing entity. Haga clic en la entidad emisora de certificados.
   4. Issuing method. Haga clic en Sign o en Fetch para designar el método que usará el sistema para obtener certificados de la entidad configurada.
   5. Si la lista de plantillas está disponible, seleccione una plantilla para el proveedor de credenciales.
      Nota: Estas plantillas pasan a estar disponibles cuando las entidades de Microsoft Certificate Services se agregan en Configure > Settings > More > PKI Entities.
   6. Haga clic en Siguiente.
      Aparecerá la página Credential Providers: Certificate Signing Request.

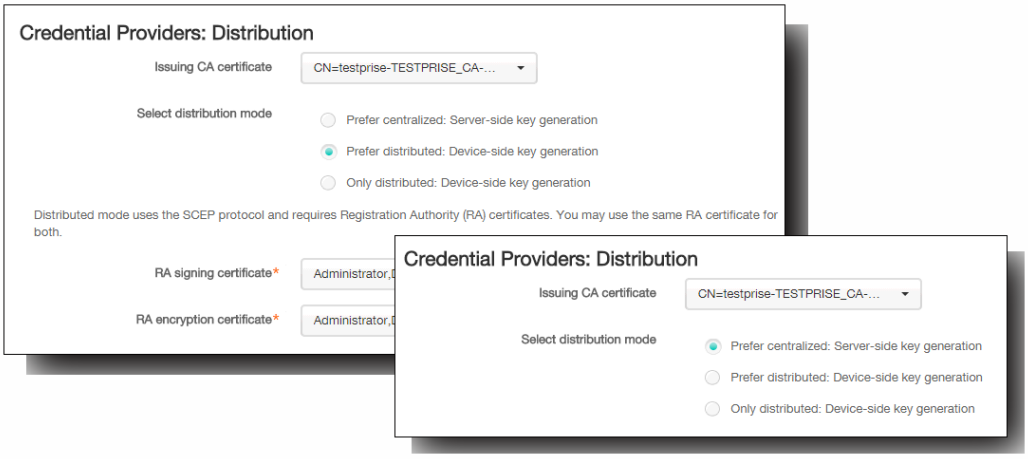


4. En la página Credential Providers: Certificate Signing Request, lleve a cabo lo siguiente:
   1. Key algorithm. Haga clic en el algoritmo de clave para el nuevo par de claves. Los valores disponibles son: RSA, DSA y ECDSA.
   2. Key size. Escriba el tamaño, en bits, del par de claves. Este campo es obligatorio.
      Nota: Los valores permitidos dependen del tipo de clave. Por ejemplo, el tamaño máximo de las claves DSA es de 1024 bits. Para evitar falsos negativos, los cuales dependerán del hardware y software subyacentes, XenMobile no aplicará tamaños de clave. Debe probar siempre las configuraciones del proveedor de credenciales en un entorno de prueba antes de activarlas en producción.
   3. Signature algorithm. Haga clic en un valor para el nuevo certificado. Los valores dependen del algoritmo de clave.
   4. Subject name. Escriba el nombre distintivo (DN) del sujeto del nuevo certificado. Por ejemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`. Este campo es obligatorio.
   5. Para agregar una nueva entrada a la tabla Subject alternative names, haga clic en Add. Seleccione el tipo de nombre alternativo y, a continuación, escriba un valor en la segunda columna.
      Nota: En cuanto al nombre del sujeto, puede hacer uso de las macros de XenMobile en el campo del valor.
   6. Haga clic en Siguiente.
      Aparecerá la página Credential Providers: Distribution.

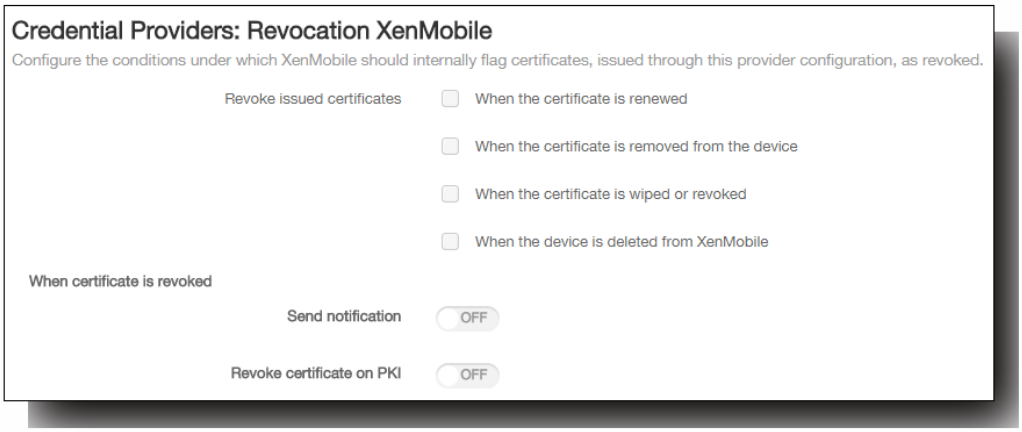
5. En la página Credential Providers: Distribution, lleve a cabo lo siguiente:
   1. En la lista Issuing CA certificate, haga clic en el certificado de CA ofrecido. Dado que el proveedor de credenciales usa una entidad de certificación discrecional, el certificado de CA de ese proveedor siempre será el certificado de CA configurado en la propia entidad; se mostrará aquí por coherencia con las configuraciones que usan entidades externas.
   2. En Select distribution mode, haga clic en una de las siguientes maneras de generar y distribuir claves:
      - Prefer centralized: Server-side key generation. Citrix recomienda esta opción centralizada. Admite todas las plataformas respaldadas por XenMobile y es necesaria cuando se usa la autenticación de NetScaler Gateway. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
      - Prefer distributed: Device-side key generation. Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.

- Only distributed: Device-side key generation. Esta opción funciona de la misma forma que Prefer distributed: Device-side key generation, salvo que no se permite ninguna otra opción si se produce un error en la generación de claves por parte del dispositivo o esta no está disponible.

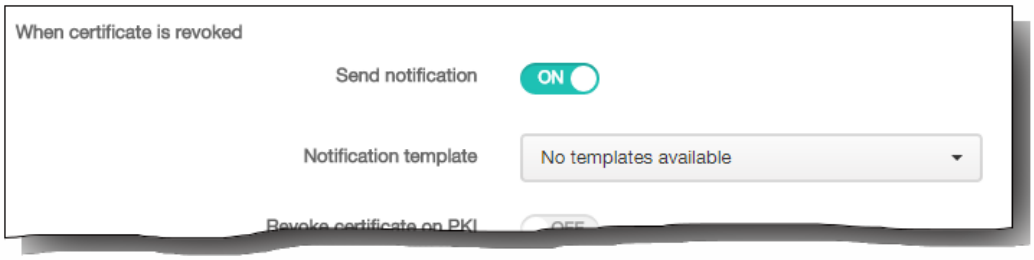
Si selecciona Prefer distributed: Device-side key generation u Only distributed: Device-side key generation, también debe seleccionar un certificado de firma de RA y un certificado de cifrado de RA. Aparecerán campos nuevos para esos certificados.



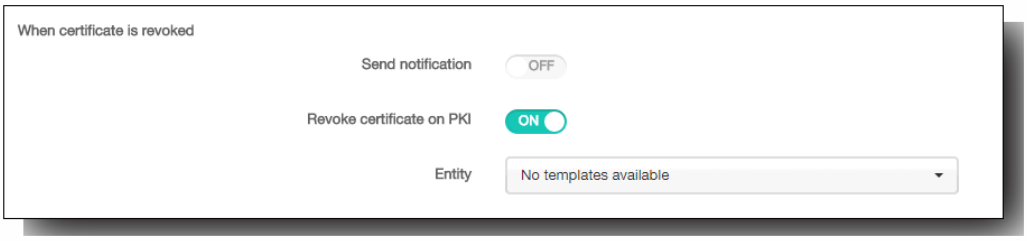
3. Si selecciona Prefer distributed: Device-side key generation u Only distributed: Device-side key generation, haga clic en el certificado de firma de RA y en el certificado de cifrado de RA. Se puede usar el mismo certificado tanto para el cifrado como para la firma.
4. Haga clic en Siguiente.
   Aparecerá la página Credential Providers: Revocation XenMobile. En esta página, puede configurar las condiciones bajo las que XenMobile deberá marcar internamente como revocados los certificados que se emitan con esta configuración de proveedor.



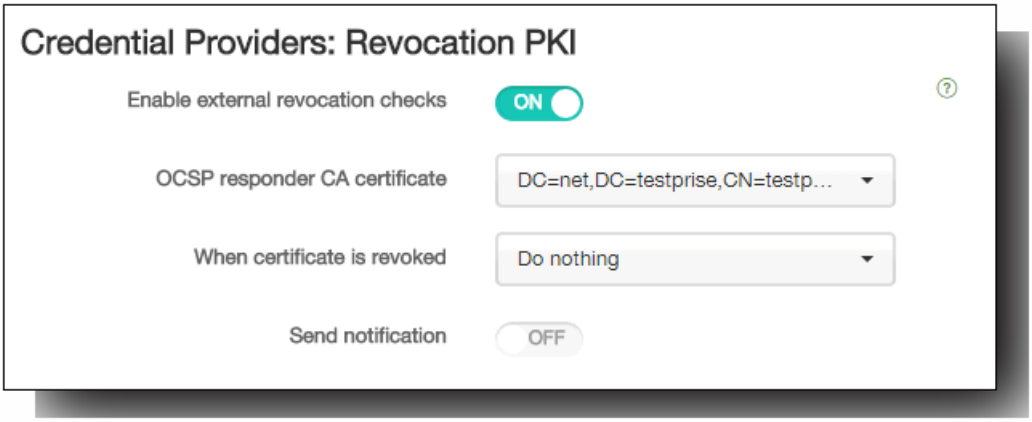
6. En la página Credential Providers: Revocation XenMobile, lleve a cabo lo siguiente:
   1. En Revoke issued certificates, seleccione una de las opciones que indican el momento en que se deben revocar los certificados.
   2. Si quiere que XenMobile envíe una notificación cuando el certificado se revoque, establezca el valor de Send notification en On y seleccione una plantilla de notificaciones.



3. Si quiere revocar el certificado presente en la infraestructura de clave pública cuando este se haya revocado en XenMobile, establezca Revoke certificate on PKI en On y, en la lista Entity, haga clic en una plantilla. La lista Entity muestra todas las entidades de infraestructura GPKI disponibles con capacidades de revocación. Cuando el certificado se revoque en XenMobile, se enviará una llamada de revocación a la infraestructura de clave pública seleccionada de la lista Entity.



4. Haga clic en Siguiente.
   Aparecerá la página Credential Providers: Revocation PKI. En esta página, puede identificar las acciones que se deben realizar en la infraestructura de clave pública si se revoca el certificado. También tiene la opción de crear un mensaje de notificación.

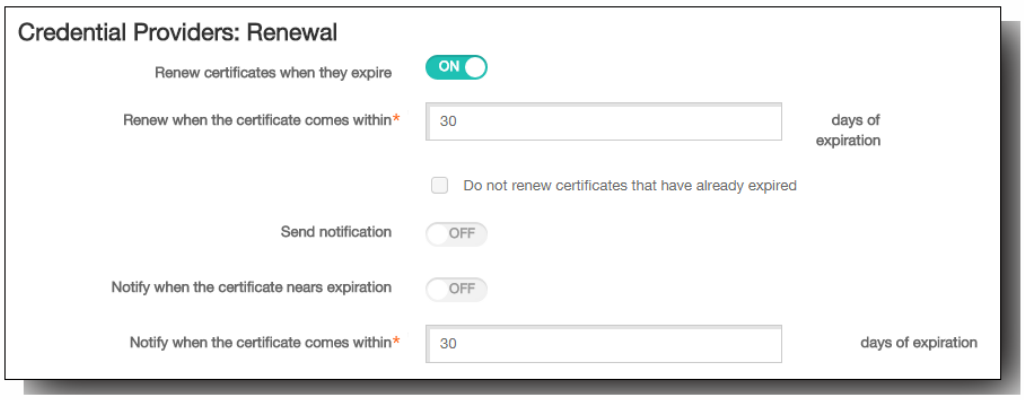


7. En la página Credential Providers: Revocation PKI, lleve a cabo lo siguiente si quiere revocar certificados procedentes de la infraestructura de clave pública:
   1. Cambie la opción Enable external revocation checks a On.
      Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
   2. En la lista OCSP responder CA certificate, haga clic en el nombre distintivo (DN) del sujeto del certificado.

Nota: Puede usar macros de XenMobile para los valores de los campos del DN. Por ejemplo: CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation

3. En la lista When certificate is revoked, haga clic en una de las siguientes acciones a realizar en la entidad de infraestructura PKI cuando se revoque el certificado:
   - No hacer nada.
   - Renovar el certificado.
   - Revocar y borrar el dispositivo.
4. Si quiere que XenMobile envíe una notificación cuando el certificado se revoque, establezca el valor de Send notification en On.
   Puede elegir entre dos opciones de notificación:
   - Si selecciona Select notification template, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista Notification template.
   - Si elige Enter notification details, puede escribir su propio mensaje de notificación. Además de facilitar la dirección de correo electrónico del destinatario y el mensaje, puede configurar la frecuencia con que se envía la notificación.
5. Haga clic en Siguiente.
   Aparecerá la página Credential Providers: Renewal. En esta página, puede determinar que XenMobile opere de la siguiente manera:
   - Renovar el certificado y, si quiere, enviar una notificación cuando finalice el proceso (notificación de renovación) y, también si lo prefiere, excluir de la operación los certificados ya caducados.
   - Emitir una notificación para aquellos certificados cuya fecha de caducidad se acerca (notificación antes de renovación).

8. En la página Credential Providers: Renewal, lleve a cabo lo siguiente si quiere renovar certificados cuando estos caduquen:
   1. Establezca Renew certificates when they expire en On.
      Aparecerán campos adicionales.



   2. En el campo Renew when the certificate comes within, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe realizarse la renovación.
   3. Si quiere, seleccione Do not renew certificates that have already expired.
      Nota: En este caso, "already expired" significa que la fecha NotAfter del certificado ha pasado, no que ha sido revocado. XenMobile no renovará certificados una vez que se hayan revocado internamente.
   4. Si quiere que XenMobile envíe una notificación cuando el certificado se haya renovado, establezca el valor de Send notification en On.
      Puede elegir entre dos opciones de notificación:

- Si selecciona Select notification template, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista Notification template.
- Si elige Enter notification details, puede escribir su propio mensaje de notificación. Además de facilitar la dirección de correo electrónico del destinatario y el mensaje, puede configurar la frecuencia con que se envía la notificación.

5. Si quiere que XenMobile envíe una notificación cuando la fecha de caducidad de la certificación se acerque, establezca Notify when certificate nears expiration en On.
   Puede elegir entre dos opciones de notificación:

   - Si selecciona Select notification template, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista Notification template.
   - Si elige Enter notification details, puede escribir su propio mensaje de notificación. Además de facilitar la dirección de correo electrónico del destinatario y el mensaje, puede configurar la frecuencia con que se envía la notificación.

6. En el campo Notify when the certificate comes within, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe enviarse la notificación.

9. Haga clic en Save.
   El proveedor de credenciales se agregará a la tabla Credential Providers.

Solicitud de un certificado APNs

May 05, 2016

Para inscribir y administrar dispositivos iOS con XenMobile, debe configurar y crear un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. En esta sección se describen los pasos básicos para solicitar el certificado APNs:

- Utilice un servidor Windows Server 2012 R2 o Windows 2008 R2 y Microsoft Internet Information Server (IIS) o un equipo Mac para generar una solicitud de firma de certificado (CSR).
- Contacte con Citrix para que firmen la solicitud CSR.
- Solicite un certificado APNs de Apple.
- Importe el certificado en XenMobile.

Nota:

- El certificado APNs de Apple permite la administración de dispositivos móviles a través de Apple Push Network. Si revoca el certificado, ya sea accidental o intencionadamente, ya no podrá administrar los dispositivos.
- Si se ha utilizado el programa iOS Developer Enterprise Program para crear un certificado push para MDM, es posible que necesite actuar debido a la migración de los certificados existentes al portal Apple Push Certificate Portal.

Los temas que ofrecen los procedimientos paso a paso se muestran por orden en esta sección, como se indica a continuación:

Paso 1	Creación de una solicitud CSR en IIS Creación de una solicitud CSR en un equipo Mac	Genere una solicitud de firma de certificado en un equipo Mac o con un servidor Windows 2008 R2 o Windows Server 2012 R2 y Microsoft IIS. Citrix recomienda este método.
Paso 2	Para firmar una solicitud de firma de certificado	Envíe la solicitud de firma de certificado a Citrix por medio del sitio Web XenMobile APNs CSR Signing website (se requiere el ID de MyCitrix). Citrix firma la solicitud de firma de certificado con el certificado de firma de administración de dispositivos móviles y devuelve el archivo firmado en un formato .plist.
Paso 3	Envío de una solicitud CSR firmada a Apple	Envíe la solicitud de firma de certificado firmada a Apple por medio del portal Apple Push Certificate Portal (se requiere ID de Apple) y, a continuación, descargue el certificado APNs de Apple.
Paso 4	Para crear un certificado APNs con extensión PFX mediante Microsoft IIS Para crear un certificado APNs con extensión .pfx en un equipo Mac	Exporte el certificado APNs como un certificado PCKS #12 (.pfx) (en IIS, Mac o SSL).

	Creación de un certificado APNs con extensión PFX mediante OpenSSL	
Paso 5	Importar un certificado APNs en XenMobile	Importe el certificado en XenMobile.

Los certificados push para la administración de dispositivos móviles (MDM), creados en el programa iOS Developer Enterprise Program, se han migrado al portal Apple Push Certificates Portal. Esta migración afecta a la creación de nuevos certificados push para MDM, así como a la renovación, la revocación y la descarga de certificados push para MDM existentes. La migración no afecta a otros certificados APNs (es decir, certificados que no sean MDM).

Si su certificado push para MDM se creó en el seno del programa iOS Developer Enterprise Program, se aplican las siguientes situaciones:

- El certificado se ha migrado de forma automática para usted.
- Puede renovar el certificado en el portal Apple Push Certificates Portal sin que esto afecte a los usuarios.
- Debe usar el programa iOS Developer Enterprise Program para revocar o descargar un certificado que ya existía.

Si no se acerca la fecha de caducidad de ninguno de los certificados push para MDM, no es necesario hacer nada. En cambio, si dispone de un certificado push para MDM que caducará pronto, póngase en contacto con el proveedor de soluciones de MDM. A continuación, haga que el Agente del programa iOS Developer Enterprise Program inicie sesión en el portal Apple Push Certificates Portal con su ID de Apple.

Todos los certificados push para MDM nuevos deben crearse en el portal Apple Push Certificates Portal. El programa iOS Developer Enterprise Program ya no permitirá la creación de un ID de aplicación con un identificador de paquete (apartado APNs) que contenga com.apple.mgmt.

Nota: Debe realizar un seguimiento del ID de Apple usado para crear el certificado. Además, el ID de Apple debe ser un ID de la empresa, no un ID personal.

El primer paso para generar una solicitud de certificado APNs para los dispositivos iOS consiste en crear una solicitud de firma de certificado (CSR). En un servidor Windows 2008 R2 o Windows 2012 R2, puede generar una solicitud CSR mediante Microsoft IIS.

1. Abra Microsoft IIS.
2. Haga doble clic en el icono de Certificados de servidor para IIS.
3. En la ventana Certificados de servidor, haga clic en **Crear una solicitud de certificado**.
4. Escriba la información de nombre distintivo (DN) correspondiente y, a continuación, haga clic en **Siguiente**.
5. Seleccione el **Proveedor de cifrado Microsoft RSA SChannel** como proveedor de servicios de cifrado. Asimismo, seleccione **2048** para la longitud en bits y, a continuación, haga clic en **Siguiente**.
6. Escriba un nombre de archivo y especifique una ubicación para guardar la solicitud de firma de certificado y, a continuación, haga clic en **Finalizar**.

1. En un equipo Mac con Mac OS X, en **Aplicaciones** > **Utilidades**, inicie la aplicación Acceso a Llaveros.
2. Abra el menú **Acceso a Llaveros** y, a continuación, haga clic en **Preferencias**.
3. Haga clic en la ficha **Certificados**, cambie las opciones de **OCSP** y **CRL** a **No** y, a continuación, cierre la ventana Preferencias.
4. En el menú **Acceso a Llaveros**, haga clic en **Asistente para Certificados** > **Solicitar un certificado de una autoridad de certificación**.
5. El Asistente para Certificados solicitará que introduzca la información siguiente:
   1. **Dirección de correo**. Dirección de correo electrónico de la cuenta de la persona o del rol responsable de administrar el certificado.
   2. **Nombre común**. Nombre común de la cuenta de la persona o del rol responsable de administrar el certificado.
   3. **Dirección de correo de la CA**. Dirección de correo electrónico de la entidad de certificación.
6. Seleccione las opciones **Se guarda en el disco** y **Permitirme especificar la información del par de llaves** y, a continuación, haga clic en **Continuar**.
7. Asigne y escriba un nombre para el archivo de solicitud de firma de certificado, guárdelo en el equipo y, a continuación, haga clic en **Guardar**.
8. Para especificar la información del par de claves, seleccione un **Tamaño de la clave** de 2048 bits y el **algoritmo RSA** y, a continuación, haga clic en **Continuar**. El archivo de solicitud de firma de certificado está listo para su carga como parte del proceso de certificado APNs.
9. Haga clic en **OK** cuando el Asistente para Certificados haya terminado el proceso de solicitud de la firma de certificado.

Si no puede utilizar un servidor Windows 2012 R2 o Windows 2008 R2 y Microsoft Internet Information Server (IIS) o un equipo Mac para generar una solicitud de firma de certificado (CSR) que enviar a Apple para el certificado del servicio de notificaciones push de Apple (APNs), puede usar OpenSSL.

Nota: Para usar OpenSSL con el fin de crear una solicitud CSR, primero debe descargar e instalar OpenSSL desde el sitio Web de OpenSSL.

1. En el equipo donde se instaló OpenSSL, ejecute el siguiente comando desde el shell o del símbolo del sistema.
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. Aparece el siguiente mensaje con información pertinente para asignar nombres de certificado. Escriba la información tal y como se indica.
   Se le va a pedir información que será incorporada
   en la solicitud de certificado.
   Lo que está a punto de suministrar es lo que se conoce como nombre distintivo o nombre DN.
   Existen varios campos aunque puede dejar algunos en blanco
   Para algunos campos habrá un valor predeterminado,
   Si introduce '.', el campo quedará en blanco.

   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:CA
   Locality Name (eg, city) []:RWC
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer
   Organizational Unit Name (eg, section) []:Marketing
   Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com

3. En el siguiente mensaje, escriba una contraseña para la clave privada de la solicitud CSR.
   Introduzca los siguientes atributos adicionales
   para enviarlos con su solicitud de certificado
   A challenge password []:
   An optional company name []:

4. Envíe la solicitud CSR resultante a Citrix.

Citrix preparará la solicitud CSR firmada y le devolverá el archivo a través de correo electrónico.

Antes de enviar el certificado a Apple, Citrix debe firmarlo para que se pueda usar con XenMobile.

1. En el explorador Web, vaya al sitio Web XenMobile APNs CSR Signing.
2. Haga clic en **Upload the CSR**.
3. Busque y seleccione el certificado.
   Nota: El certificado debe estar en el formato PEM o TXT.

4. En la página de firma de solicitudes de certificados APNs para XenMobile, haga clic en **Sign**. La solicitud se firma y se guarda automáticamente en la carpeta de descargas definida.

Después de recibir la solicitud de firma de certificado (CSR) de Citrix, debe enviarla a Apple para obtener el certificado APNs.

Nota: Algunos usuarios han informado de problemas para iniciar sesión en el portal de certificados push de Apple. Como alternativa, puede iniciar sesión en el Portal para desarrolladores de Apple (http://developer.apple.com/devcenter/ios/index.action) antes de ir al enlace de identity.apple.com del Paso 1.

1. En un explorador Web, vaya a https://identity.apple.com/pushcert.
2. Haga clic en **Create a Certificate**.
3. Si es la primera vez que crea un certificado con Apple, marque la casilla de verificación **I have read and agree to these terms and conditions** y, a continuación, haga clic en **Accept**.
4. Haga clic en **Choose File**, vaya al certificado firmado ubicado en el equipo y, a continuación, haga clic en **Upload**. Debe aparecer un mensaje de confirmación donde se indica que la carga se ha realizado correctamente.
5. Haga clic en **Download** para obtener el certificado .pem.
   Nota: Si está utilizando Internet Explorer y falta la extensión de archivo, haga clic en **Cancel** dos veces y, a continuación, descárguelo desde la ventana siguiente.

Para usar el certificado APNs de Apple con XenMobile, debe completar la solicitud de certificado en Microsoft IIS, exportar el certificado como PCKS #12 (.pfx) y, a continuación, importar el certificado APNs en XenMobile.

Importante: Debe usar el mismo servidor IIS para esta tarea que el servidor usado para generar la solicitud de firma de certificado.

1. Abra Microsoft IIS.

2. Haga clic en el icono de certificados del servidor.
3. En la ventana **Certificados de servidor**, haga clic en **Completar solicitud de certificado**.
4. Busque el archivo Certificate.pem de Apple. Escriba un nombre descriptivo o el nombre del certificado y haga clic en **OK**.
5. Seleccione el certificado que identificó en el paso 4 y, a continuación, haga clic en **Exportar**.
6. Especifique una ubicación y un nombre de archivo para el certificado .pfx, así como una contraseña, y, a continuación, haga clic en **Aceptar**.
   Nota: Necesitará la contraseña del certificado durante la instalación de XenMobile.
7. Copie el certificado .pfx al servidor en el que se instalará XenMobile.
8. Inicie sesión en la consola de XenMobile como administrador o como un usuario con acceso a la ficha **About**.
9. Haga clic en la ficha **About** y, a continuación, haga clic en **Update APNs Certificate**.
10. En el cuadro de diálogo **Update APNs Certificate**, vaya al archivo .pfx de certificado APN en el equipo y, a continuación, escriba una contraseña nueva.
11. Haga clic en **Load APNs Certificate**.
12. Haga clic en **Update**.

1. En el mismo equipo Mac con Mac OS X que se ha utilizado para generar la solicitud de firma de certificado, busque el certificado de identidad de producción PEM recibido de Apple.
2. Haga doble clic en el archivo del certificado para importarlo en el llavero.
3. Si se le solicita agregar el certificado a un llavero concreto, mantenga seleccionado el llavero predeterminado de inicio de sesión y, a continuación, haga clic en **OK**. El certificado recién agregado aparecerá en la lista de certificados.
4. Haga clic en el certificado y, a continuación, en el menú **Archivo**, haga clic en **Exportar** para comenzar a exportar el certificado en un formato PCKS #12 (.pfx).
5. Asigne un nombre único al archivo del certificado para su uso con el servidor XenMobile, elija una ubicación de carpeta para guardar el certificado, seleccione el formato de archivo .pfx y, a continuación, haga clic en **Guardar**.
6. Escriba una contraseña para exportar el certificado. Citrix recomienda usar una contraseña única y segura. Además, compruebe que el certificado y la contraseña se encuentren en un lugar seguro para su uso y referencia posteriores.
7. La aplicación Acceso a Llaveros le solicitará la contraseña de inicio de sesión o el llavero seleccionado. Escriba la contraseña y, a continuación, haga clic en **OK**. Ahora, el certificado guardado está listo para su uso con el servidor XenMobile.
   Nota: En caso de que no se conserven ni mantengan ni el equipo ni la cuenta de usuario que se usaron en su momento para generar la solicitud de firma de certificado y para completar el proceso de exportación de certificado, Citrix recomienda guardar o exportar las claves públicas y personales desde el sistema local. De lo contrario, no se podrá acceder a los certificados APNs para volver a usarlos y se deberá repetir el proceso de la solicitud CSR y APNs desde el principio.

Después de usar OpenSSL para crear una solicitud de firma de certificado (CSR), también puede usar OpenSSL para crear un certificado APNs de extensión .pfx.

1. En el shell o en el símbolo del sistema, ejecute el siguiente comando.
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. Escriba una contraseña para el archivo de certificado de extensión .pfx. Recuerde esta contraseña porque necesitará volver a utilizarla al cargar el certificado en XenMobile.
3. Tome nota de la ubicación del archivo de certificado .pfx y cópielo al servidor XenMobile, para poder usar la consola de

XenMobile para cargar el archivo.

Después de solicitar y recibir un nuevo certificado APNs, importe ese certificado en XenMobile, ya sea para agregar el certificado por primera vez o para reemplazar un certificado existente.

1. Inicie sesión como administrador en la consola de XenMobile.
2. Haga clic en **Configure** > **Settings** > **Certificates**.
3. En la página **Certificates**, haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
4. Busque el archivo .p12 en su equipo.
5. Escriba la contraseña y, a continuación, haga clic en **Import**.

Para obtener más información acerca de los certificados en XenMobile, consulte la sección Certificados:

Para renovar un certificado APNs, debe realizar los mismos pasos que seguiría si creara un nuevo certificado. Luego, puede visitar el portal Apple Push Certificates Portal y cargar el certificado nuevo. Después de iniciar sesión, podrá ver el certificado existente, o es posible que vea un certificado que se ha importado desde su cuenta anterior de desarrollador de Apple. En el portal de certificados, la única diferencia cuando se renueva el certificado es que tiene que hacer clic en **Renew**. Debe tener una cuenta de desarrollador en el portal de certificados para acceder al sitio.

Nota: Para determinar cuándo caduca su certificado APNs, en la consola de XenMobile, haga clic en **Configure** > **Settings** > **Certificates**. Sin embargo, si el certificado está caducado, no lo revoque.

1. Genere una solicitud de firma de certificado mediante Microsoft Internet Information Services (IIS).
2. En el sitio Web XenMobile APNs CSR Signing, cargue la nueva solicitud de firma de certificado y, a continuación, haga clic en **Sign**.
3. Envíe la solicitud de firma de certificado firmado a Apple Push Certificate Portal.
4. Haga clic en **Renew**.
5. Genere un certificado APNs PCKS #12 (.pfx) mediante Microsoft IIS.
6. Actualice el nuevo certificado APNs en XenMobile en **Configure** > **Settings** > **Certificates**.
7. En el cuadro de diálogo **Import** , importe el nuevo certificado.

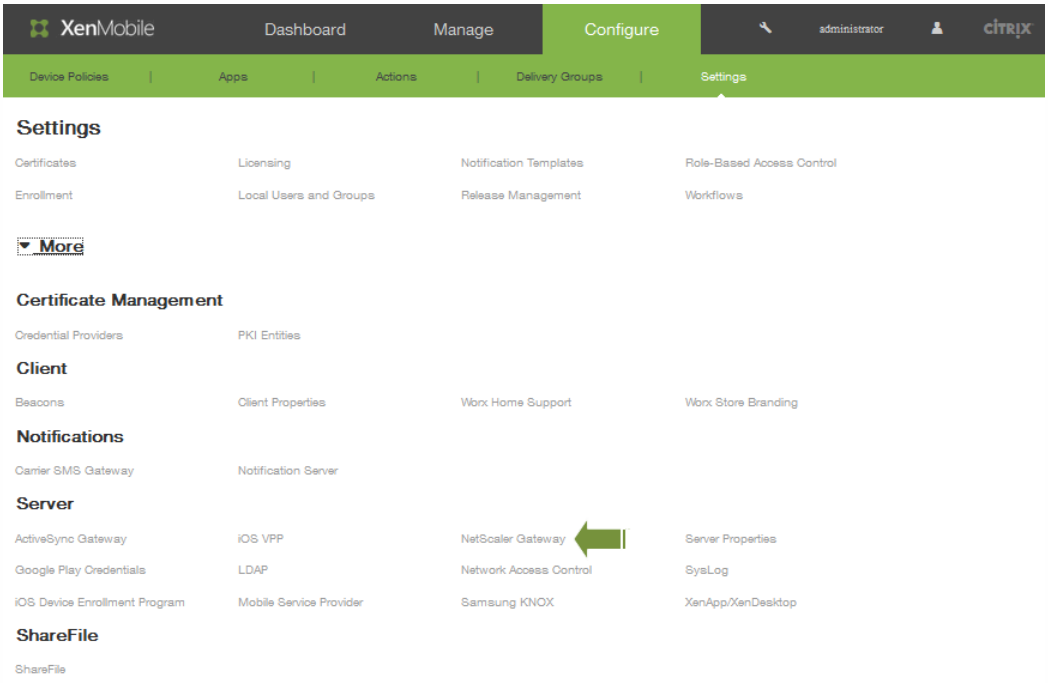
XenMobile y NetScaler Gateway

May 05, 2016

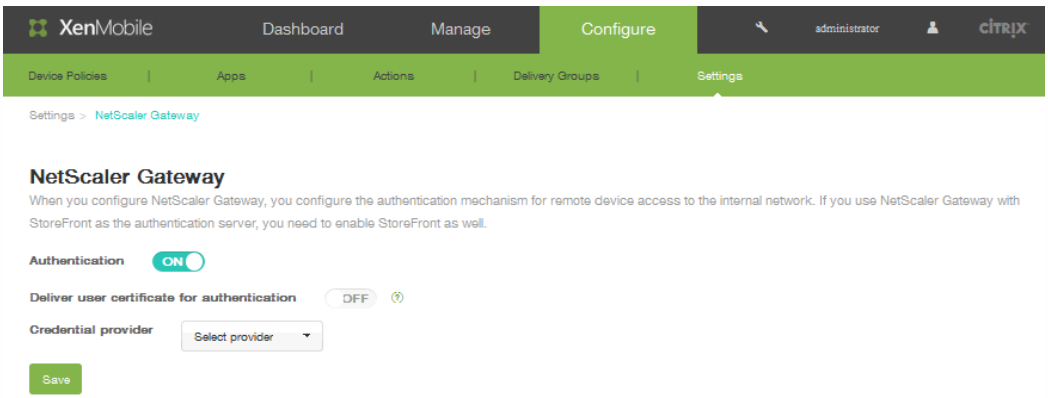
Al configurar NetScaler Gateway mediante XenMobile, debe establecer el mecanismo de autenticación para el acceso de dispositivos remotos a la red interna. Esta función permite a las aplicaciones de un dispositivo móvil acceder a los servidores de empresa ubicados en la intranet mediante la creación de una microrred VPN que va de las aplicaciones del dispositivo a NetScaler Gateway. Para ello, debe configurar NetScaler Gateway mediante la consola de XenMobile.

Nota: Consulte Configuración de parámetros para el entorno de XenMobile para obtener información acerca de la configuración de NetScaler Gateway para XenMobile en NetScaler.

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > NetScaler Gateway.



2. En Authentication, seleccione ON.

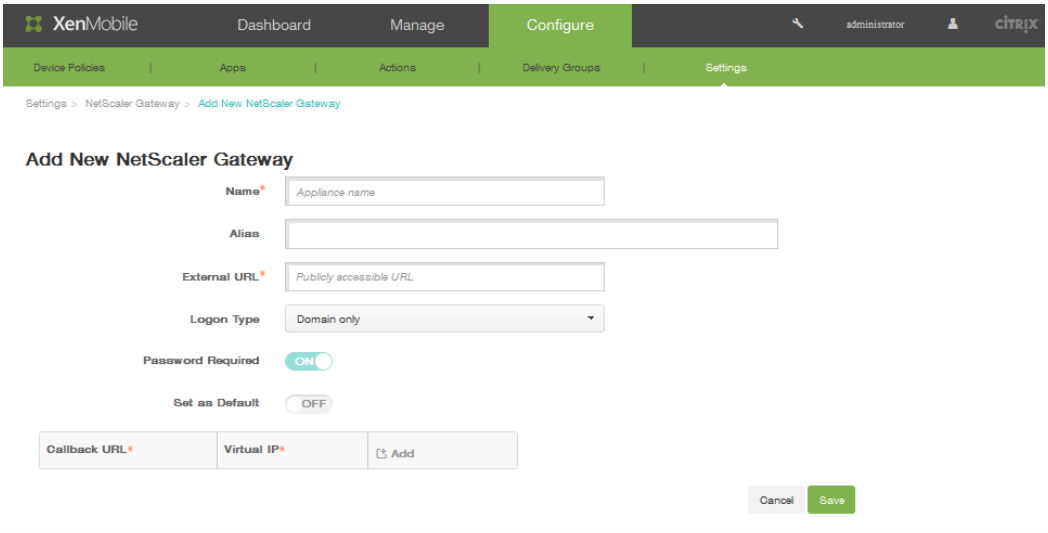


3. Si quiere que XenMobile comparta el certificado de autenticación con Worx Home para que NetScaler Gateway

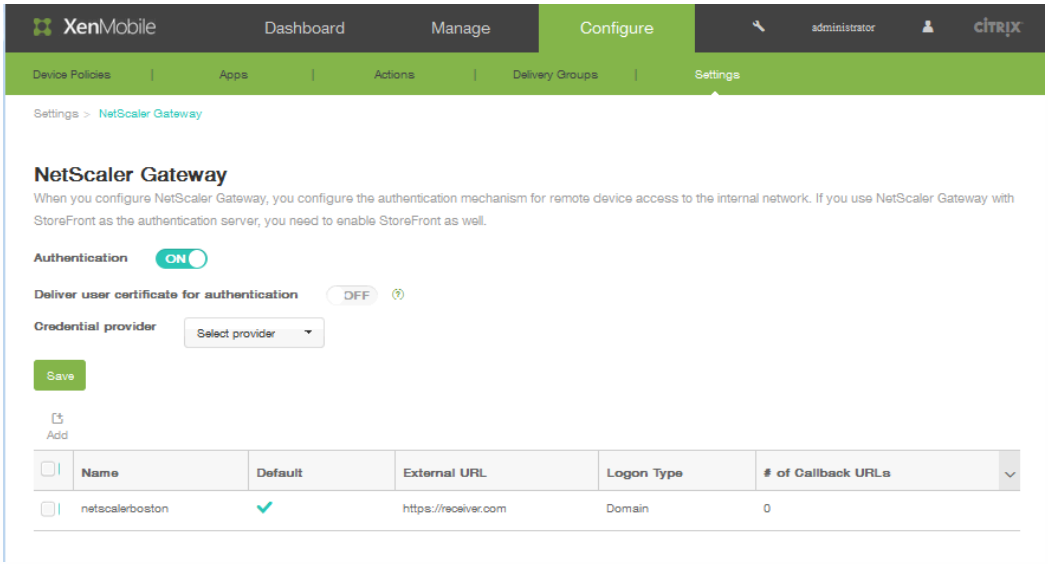
gestione la autenticación de certificados de cliente, seleccione ON en Deliver user certificate for authentication.

4. En la lista Credential Provider, haga clic en el proveedor de credenciales. Para obtener más información, consulte Proveedores de credenciales.
5. Haga clic en Guardar.

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > NetScaler Gateway.
2. Sobre la tabla, haga clic en Add. Aparecerá la página Add New NetScaler Gateway.

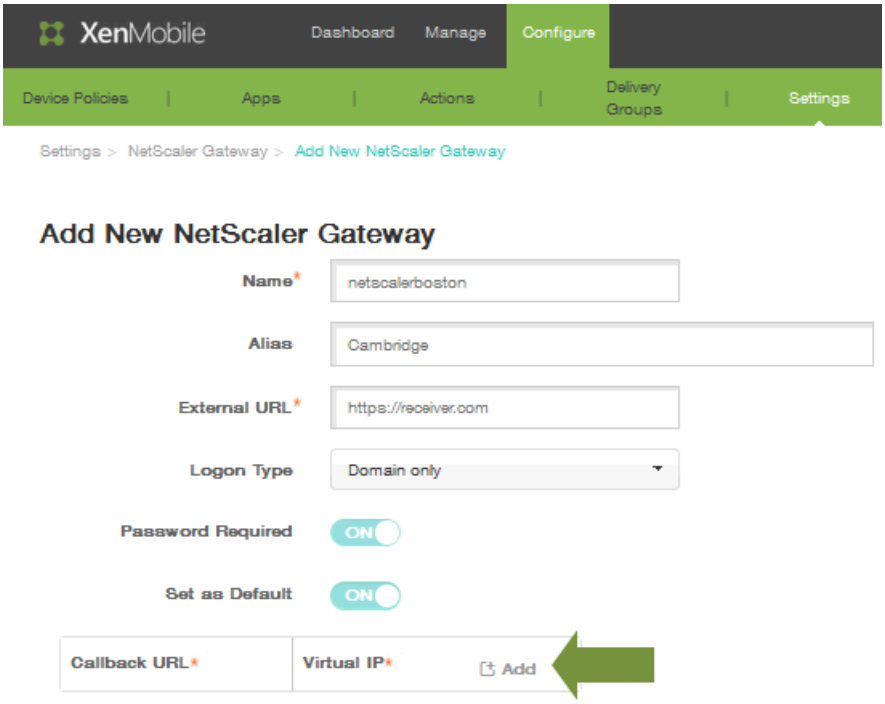


3. En Name, escriba un nombre para la instancia de NetScaler Gateway.
4. Si quiere, en Alias, puede incluir un alias.
5. En External URL, introduzca la URL de acceso público de NetScaler Gateway. Por ejemplo, https://receiver.com.
6. En la lista Logon Type, haga clic en un tipo de inicio de sesión. Los tipos incluyen: Domain only, Security token only, Domain and security token, Certificate, Certificate and domain y Certificate and security token. De forma predeterminada, el tipo de inicio de sesión está establecido en **Domain only**. Si tiene varios dominios, **Domain only** no funcionará. Debe usar **Certificate and domain**. En el caso de algunas opciones, por ejemplo para Domain only, no puede cambiar el campo Password. Para este tipo de inicio de sesión, el campo siempre está activado (ON). Además, los valores predeterminados del campo Password Required cambian en función del tipo de inicio de sesión (Logon Type) seleccionado.
7. En **Password Required**, seleccione ON si quiere que se solicite la contraseña para la autenticación.
8. En **Set as Default**, seleccione ON para usar esta instancia de NetScaler Gateway como predeterminada.
9. Haga clic en **Guardar**. La nueva instancia de NetScaler Gateway se agregará y aparecerá en la tabla. Puede modificar o eliminar una instancia si hace clic en su nombre en la lista.

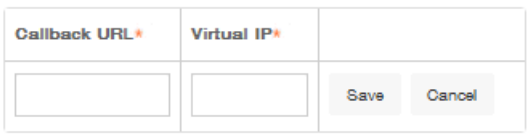


Después de agregar la instancia de NetScaler Gateway, puede agregar una dirección URL de respuesta y especificar una dirección IP virtual de VPN de NetScaler Gateway. **Nota**: Este campo es optativo, pero se puede configurar para obtener seguridad adicional, especialmente cuando el servidor XenMobile está en la zona desmilitarizada (DMZ).

1. En la pantalla NetScaler Gateway, seleccione NetScaler Gateway en la tabla y haga clic en **Add**.
2. En la página Add New NetScaler Gateway, en la tabla de direcciones URL de respuesta, haga clic en Add.



3. Especifique la URL de respuesta en **Callback URL**. Este campo representa el nombre de dominio completo (FQDN) y comprueba que la solicitud se ha originado en NetScaler Gateway.



4. Introduzca la dirección IP virtual de NetScaler Gateway en **Virtual IP** y haga clic en **Save**.

Configuración de LDAP

May 05, 2016

En XenMobile, puede configurar una conexión a varios directorios (como Active Directory) compatibles con el protocolo ligero de acceso a directorios (LDAP). Luego, puede utilizar la configuración del protocolo LDAP para importar grupos, cuentas de usuario y propiedades relacionadas. El protocolo LDAP es un protocolo de aplicación de código abierto y no vinculado a ningún proveedor específico. Se utiliza para acceder a servicios de información sobre directorios distribuidos a través de una red de protocolo de Internet (IP) y a su mantenimiento. Los servicios de información de directorios se usan para compartir información acerca de usuarios, sistemas, redes, servicios y aplicaciones disponibles a través de la red. Es habitual que el protocolo LDAP se utilice para ofrecer acceso Single Sign-On (SSO) a los usuarios. En este tipo de acceso, se comparte una sola contraseña (por usuario) entre varios servicios, lo que permite a un usuario iniciar sesión una vez en el sitio Web de una empresa y, a su vez, iniciar sesión automáticamente en la intranet de la empresa.

Cómo funciona el protocolo LDAP

Un cliente inicia una sesión LDAP al conectarse a un servidor LDAP, que se denomina Directory System Agent (DSA). El cliente envía una solicitud de operación al servidor, y el servidor responde con la autenticación pertinente.

Para configurar conexiones LDAP en XenMobile

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > LDAP.
   Aparecerá la página de configuración LDAP.

2. Haga clic en Add.
   Aparecerá la página Add LDAP.

3. Configure los siguientes parámetros:
   - Directory type. Haga clic en el tipo de directorio correspondiente. De forma predeterminada, está seleccionado Microsoft Active Directory.
   - Primary server. Introduzca el servidor principal usado para el protocolo LDAP; puede escribir la dirección IP o el nombre de dominio completo (FQDN).
   - Secondary server. Si quiere, puede introducir la dirección IP o el nombre de dominio completo (FQDN) del servidor secundario (si se ha configurado).
   - Port. Introduzca el número de puerto que utiliza el servidor LDAP. De forma predeterminada, el número de puerto es 389 para conexiones LDAP no protegidas. Use el número de puerto 636 para conexiones LDAP protegidas, el 3268 para conexiones LDAP no protegidas de Microsoft o el 3269 para conexiones LDAP protegidas de Microsoft.
   - Domain name. Introduzca el nombre de dominio.
   - User base DN. Mediante un identificador único, introduzca la ubicación de los usuarios en Active Directory. Algunos ejemplos de sintaxis: ou=usuarios, dc=ejemplo, dc=com.
   - Group base DN. Introduzca el nombre del grupo de DN base especificado como cn=nombre_de_grupo. Por ejemplo, puede introducir cn=users, dc=nombre_de_servidor, dc=net, donde cn=users es el nombre del grupo; el DN y el nombre de servidor representan el servidor con Active Directory.
   - User ID. Introduzca el ID de usuario asociado a la cuenta de Active Directory.
   - Password. Introduzca la contraseña asociada al usuario.
   - Domain alias. Introduzca un alias del nombre de dominio.
   - XenMobile Lockout Limit. Introduzca un número comprendido entre 0 y 999 para la cantidad de intentos fallidos de inicio de sesión. Si introduce 0 en este campo, indicará a XenMobile que nunca bloquee al usuario en función de los intentos fallidos de inicio de sesión.

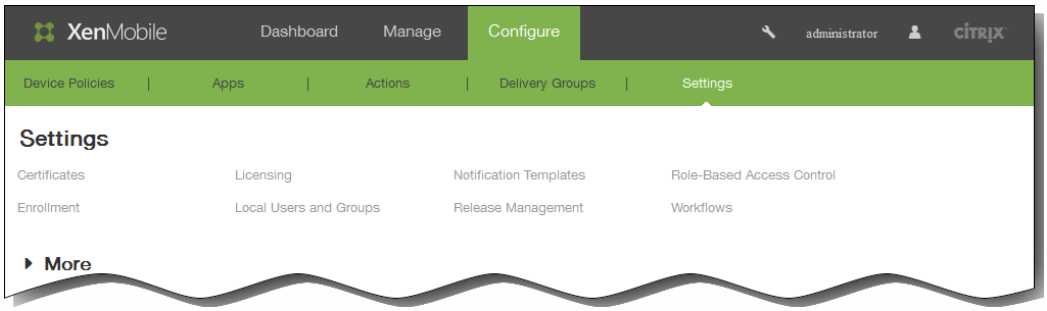
- XenMobile Lockout Time. Introduzca un número comprendido entre 0 y 99999 que representará la cantidad de minutos que el usuario debe esperar una vez superado el límite de bloqueo. Si introduce 0 en este campo, indicará que el usuario no deberá esperar después de un bloqueo.
- Global Catalog TCP Port. Introduzca el número del puerto TCP destinado al servidor de catálogo global. De forma predeterminada, el número de puerto TCP está establecido en 3268; para las conexiones SSL, utilice el número de puerto 3269.
- Global Catalog Root Context. Si quiere, puede introducir el valor del parámetro Global Root Context utilizado para habilitar una búsqueda en el catálogo global de Active Directory. Esta búsqueda se añade a la búsqueda estándar LDAP en cualquier dominio y sin necesidad de especificar el nombre de dominio real.
- User search by. En la lista, haga clic en userPrincipalName o en sAMAccountName.
- Use secure connection. Haga clic en YES para permitir conexiones protegidas.

4. Haga clic en Save.

Parámetros de inscripción, cuentas de usuario y roles

May 05, 2016

En XenMobile, puede configurar usuarios y grupos, roles para usuarios y grupos, así como el modo de inscripción y las invitaciones mediante la página Settings de la consola de XenMobile.



En la página Settings, puede realizar lo siguiente:

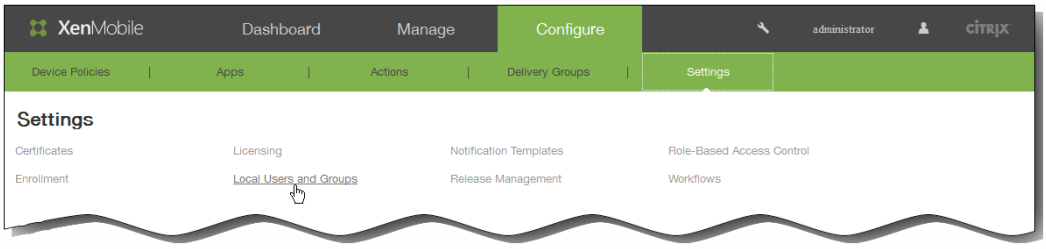
- Haga clic en Local Users and Groups para agregar cuentas de usuario de forma manual. También puede usar un archivo CSV de aprovisionamiento para importar las cuentas y administrar grupos locales. Consulte los siguientes apartados para obtener más información:
  - Para agregar, modificar o eliminar usuarios locales en XenMobile
  - Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV y Formatos de archivo de aprovisionamiento
  - Para agregar o quitar grupos en XenMobile
- Haga clic en Enrollment para configurar un máximo de siete modos, cada uno con su propio nivel de seguridad y cantidad de pasos que deberán seguir los usuarios para inscribir sus dispositivos y para enviar invitaciones de inscripción. Consulte los siguientes apartados para obtener más información:
  - Para configurar modos de inscripción y habilitar el portal Self Help Portal
  - Para activar la detección automática en XenMobile para la inscripción de usuarios
- Haga clic en Role-Based Access Control para asignar roles predefinidos o conjuntos de permisos a usuarios y grupos. Con estos permisos, se puede controlar el nivel de acceso de los usuarios a las funciones del sistema. Consulte los siguientes apartados para obtener más información:
  - Para crear o actualizar roles personalizados en XenMobile con RBAC
- Haga clic en Notification Templates para utilizar plantillas de notificaciones en acciones automatizadas, inscripciones y el envío de mensajes de notificación estándar a los usuarios. Puede configurar plantillas de notificaciones para enviar mensajes a través de tres canales diferentes: Worx Home, SMTP o SMS. Consulte los siguientes apartados para obtener más información:
  - Para crear o actualizar plantillas de notificaciones en XenMobile

Para agregar, modificar o eliminar usuarios locales en XenMobile

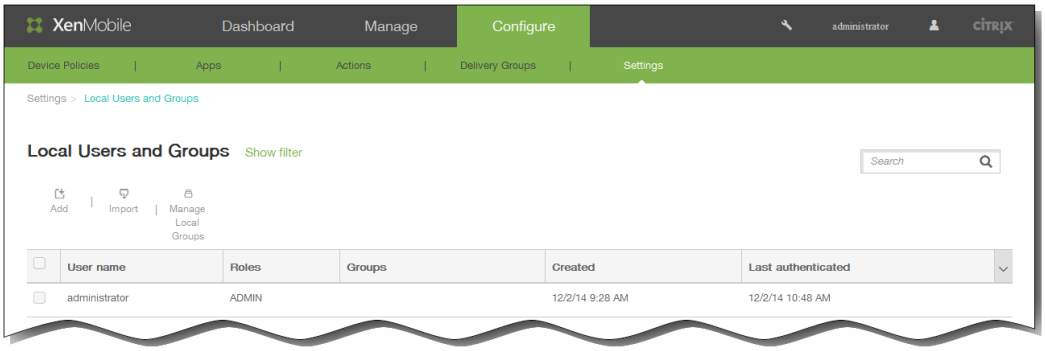
May 05, 2016

Puede agregar cuentas de usuario local a XenMobile de forma manual, o bien puede usar un archivo de aprovisionamiento para importar las cuentas. Consulte Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV para obtener información acerca de los pasos necesarios para importar usuarios a partir de un archivo de aprovisionamiento.

1. En la consola de XenMobile, haga clic en Configure > Settings > Local Users and Groups.

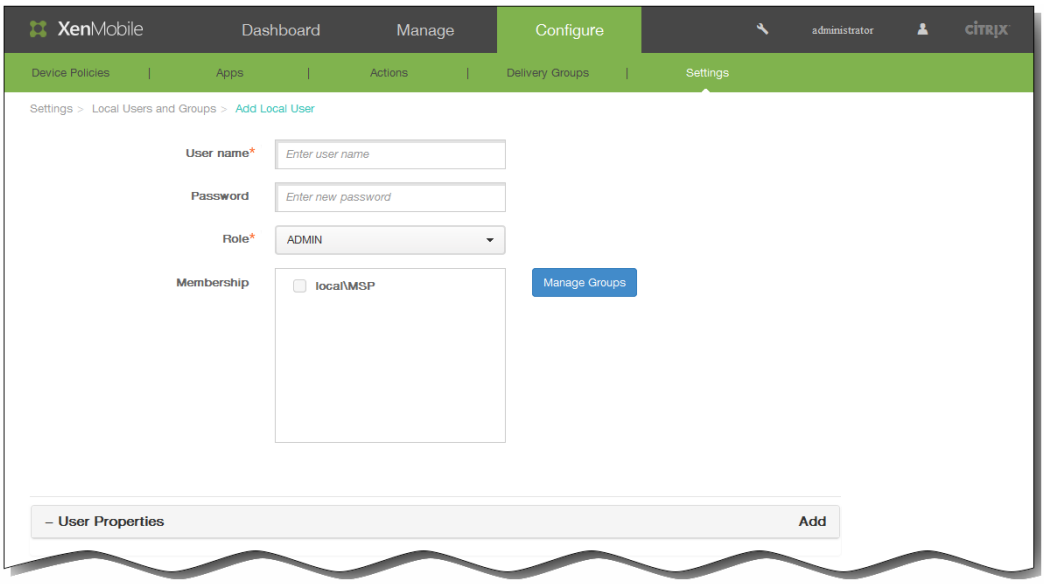


Aparecerá la página Local Users and Groups.

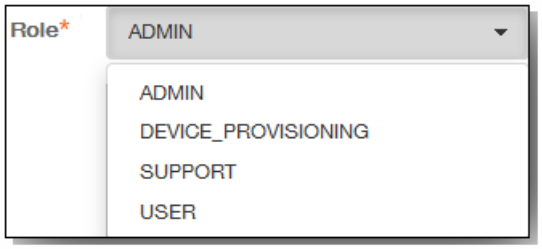


Con este procedimiento, se agrega un usuario a XenMobile. Para agregar varios usuarios, consulte Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV.

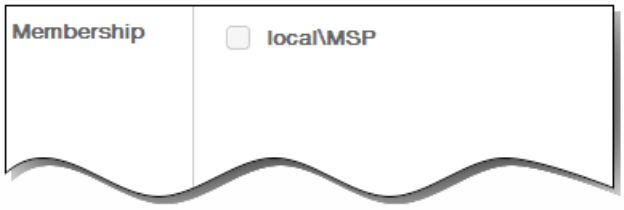
1. En la página Local Users and Groups, haga clic en Add. Aparecerá la página Add Local User.



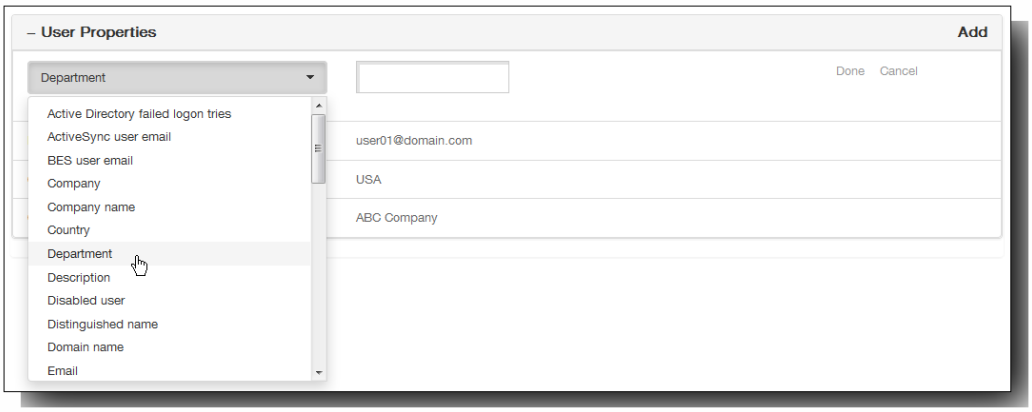
2. Escriba la siguiente información para agregar un nuevo usuario local:
   1. User name. Escriba el nombre del usuario. Este campo es obligatorio.
   2. Password. Escriba una contraseña opcional de usuario.
   3. Role. En la lista Role, haga clic en el rol del usuario. Para obtener más información acerca de los roles, consulte Para crear o actualizar roles personalizados en XenMobile con RBAC.



   4. Membership. En la lista Membership, haga clic en el grupo o en los grupos a los que agregar el usuario.

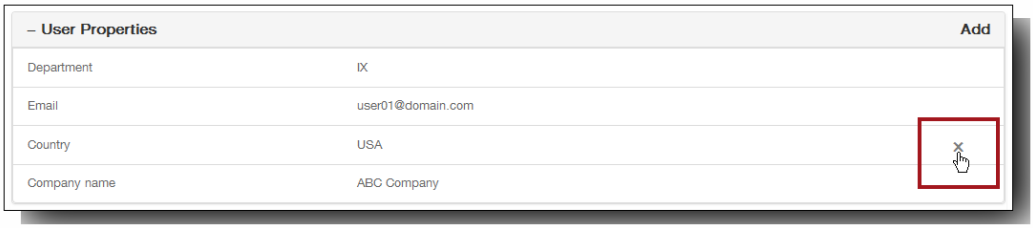


3. Si quiere, para agregar las propiedades de usuario, siga estos pasos:
   1. Junto a User Properties, haga clic en Add.
   2. En la lista User Properties, haga clic en una propiedad.
   3. Escriba el atributo de la propiedad de usuario en el campo situado junto a la lista.



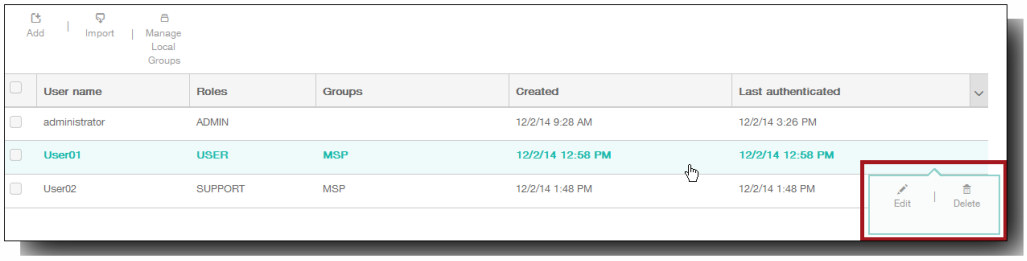
4. Haga clic en Done para guardar la propiedad de usuario o haga clic en Cancel para cancelar la operación.
5. Repita los pasos b, c y d para las demás propiedades a agregar.

4. También puede modificar propiedades de usuario. Para ello, deberá hacer lo siguiente:
   1. Haga clic en la propiedad de usuario a modificar.
   2. Cambie el atributo de la propiedad de usuario.
   3. Haga clic en Done para guardar los cambios o haga clic en Cancel para cancelar la operación.
5. Si quiere, también puede eliminar propiedades de usuario. Para ello, deberá hacer lo siguiente:
   1. Coloque el cursor sobre la línea que contiene la propiedad de usuario a eliminar.
   2. Haga clic en el signo X que aparece en el lado derecho de la línea.



   La propiedad se elimina inmediatamente.
6. Haga clic en Save para guardar el nuevo usuario.

1. En la página Local Users and Groups, en la lista de usuarios, haga clic para seleccionar un usuario.

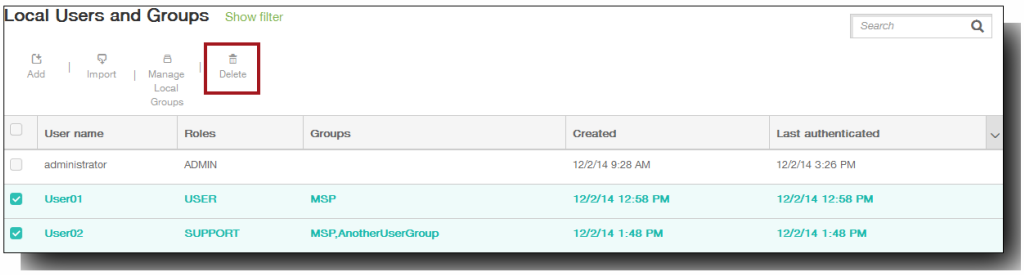


   Aparecerá la página Edit Local User.
2. Cambie la siguiente información como corresponda:
   1. User name. Escriba el nombre del usuario. Este campo es obligatorio.

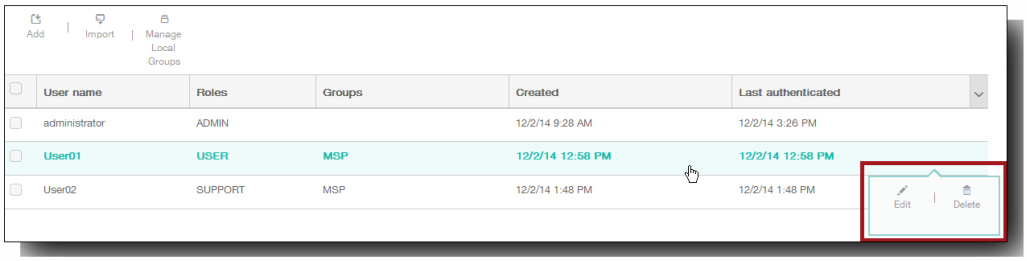
2. Password. Escriba una contraseña opcional de usuario.
3. Role. En la lista Role, haga clic en el rol del usuario.
4. Membership. En la lista Membership, haga clic en el grupo o en los grupos a los que agregar el usuario.
5. User properties. Agregue nuevas propiedades de usuario o modifique las ya existentes.

3. Haga clic en Save para guardar los cambios.

1. En la página Local Users and Groups, en la lista de usuarios, realice una de las siguientes acciones:
   - Marque la casilla situada junto a los usuarios a eliminar y, a continuación, haga clic en Delete.



   - Haga clic en la línea de un usuario que quiera eliminar y, en el menú que aparecerá a la derecha, haga clic en Delete.



Se muestra un cuadro de diálogo de confirmación. Haga clic en Delete para confirmar la operación y eliminar el usuario o usuarios.
Importante: Esta operación no se puede deshacer.

Importación de cuentas de usuario

May 05, 2016

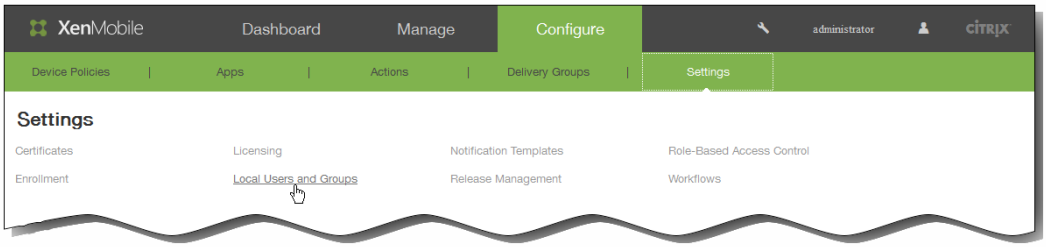
Puede importar propiedades y cuentas de usuario desde un archivo de formato CSV llamado "archivo de aprovisionamiento", el cual puede crear manualmente. Para obtener información acerca de formatos de los archivos de aprovisionamiento, consulte Formatos de archivo de aprovisionamiento.

Nota:

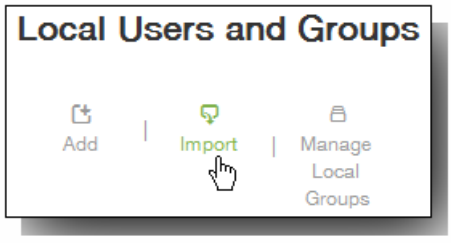
- Si importa los usuarios desde un directorio LDAP, utilice el nombre de dominio, junto con el nombre de usuario en el archivo de importación. Por ejemplo, nombredeusuario@dominio.com. Esta sintaxis evitará búsquedas adicionales que pueden reducir la velocidad de importación.
- Si importa usuarios al directorio interno de usuarios de XenMobile, inhabilite el dominio predeterminado para acelerar el proceso de importación. Puede volver a habilitar el dominio predeterminado después de la importación de usuarios internos.
- Los usuarios locales pueden tener el formato del nombre principal de usuario (UPN), aunque Citrix recomienda no usar el dominio administrado. Así, por ejemplo, si ejemplo.com está administrado, no cree un usuario local con el formato UPN "usuario@ejemplo.com".

Después de preparar un archivo de aprovisionamiento, siga estos pasos para importar el archivo en XenMobile.

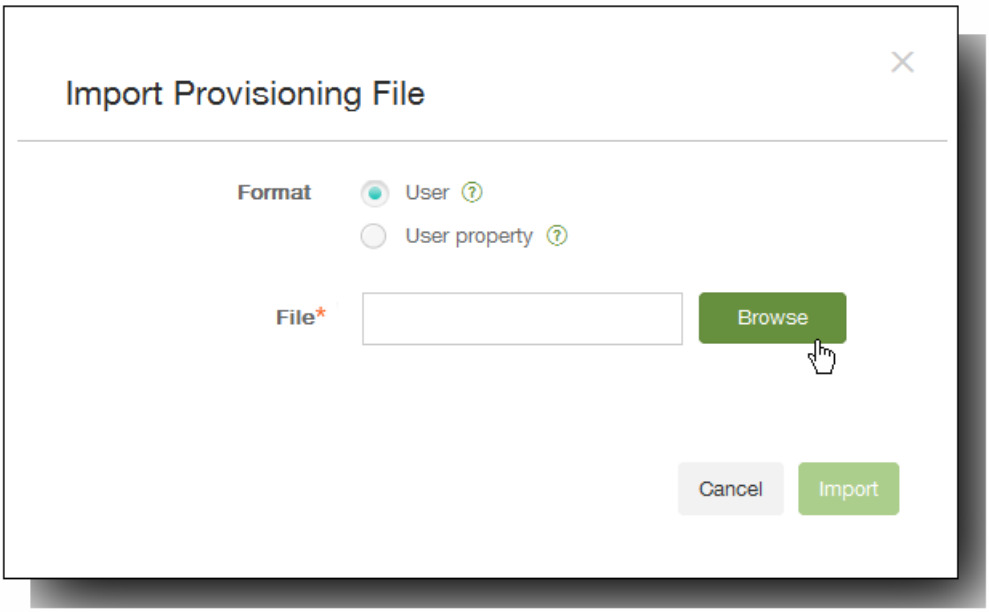
1. En la consola de XenMobile, haga clic en Configure > Settings > Local Users and Groups.



2. En la página Local Users and Groups, haga clic en Import.



   Aparecerá el cuadro de diálogo Import Provisioning File.
3. En el cuadro de diálogo Import Provisioning File, seleccione el formato del archivo de aprovisionamiento a importar.



4. Junto a File, haga clic en Browse para desplazarse a la ubicación del archivo de aprovisionamiento y, a continuación, haga clic en Import.

Formatos de archivo de aprovisionamiento

May 05, 2016

Un archivo de aprovisionamiento que se crea manualmente y se usa para importar en XenMobile propiedades y cuentas de usuario debe tener los siguientes formatos:

- Campos de archivo de aprovisionamiento de usuarios: `usuario;contraseña;rol;grupo1;grupo2`
- Campos de archivo de aprovisionamiento de atributos de usuario: `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

Nota:

- Los campos del archivo de aprovisionamiento están separados por un punto y coma (;). Si parte de un campo contiene un punto y coma, debe contener también un carácter de barra diagonal inversa (\). Por ejemplo, la propiedad `propertyV;test;1;2` debe escribirse como `propertyV\;test\;1\;2` en el archivo de aprovisionamiento.
- Los valores válidos para el campo "rol" son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE_PROVISIONING, además de los roles adicionales que haya definido.
- El punto (.) se usa como separador para crear una jerarquía de grupo; por lo tanto, no puede usar un punto en nombres de grupo.
- En los archivos de aprovisionamiento de atributos, los atributos de las propiedades deben estar en minúsculas. La base de datos distingue entre mayúsculas y minúsculas.

La entrada `user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01`significa:

- Usuario: user01
- Contraseña: pwd;01
- Rol: USER
- Grupos:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users01

La entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value`significa:

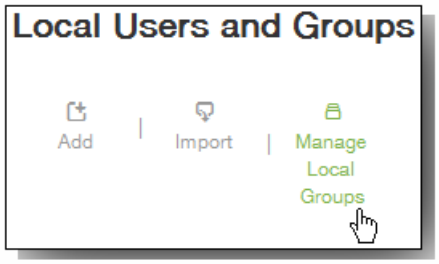
- Usuario: user01
- Propiedad 1:
  - nombre: propertyN
  - valor: propertyV;test;1;2
- Propiedad 2:
  - nombre: prop 2
  - valor: prop2 value

Incorporación y eliminación de grupos

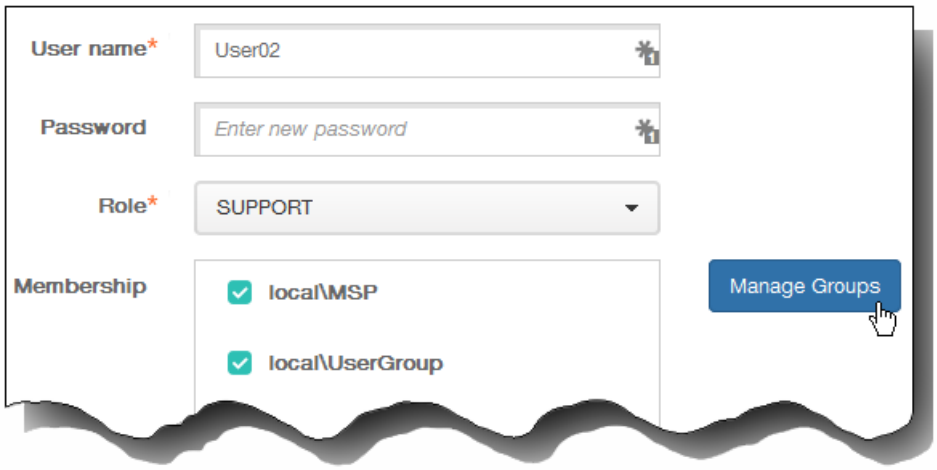
May 05, 2016

Puede administrar grupos en el cuadro de diálogo Manage Groups de la consola de XenMobile, que encontrará en las páginas Local Users and Groups, Add Local User o Edit Local User. No hay ningún comando de modificación de grupos. Si quita un grupo, tenga en cuenta que quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios a ese grupo. Asimismo, los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados a ese grupo. Sin embargo, las demás asociaciones de grupos permanecen intactas. Si los usuarios no están asociados a ningún otro grupo local, se asocian al nivel superior.

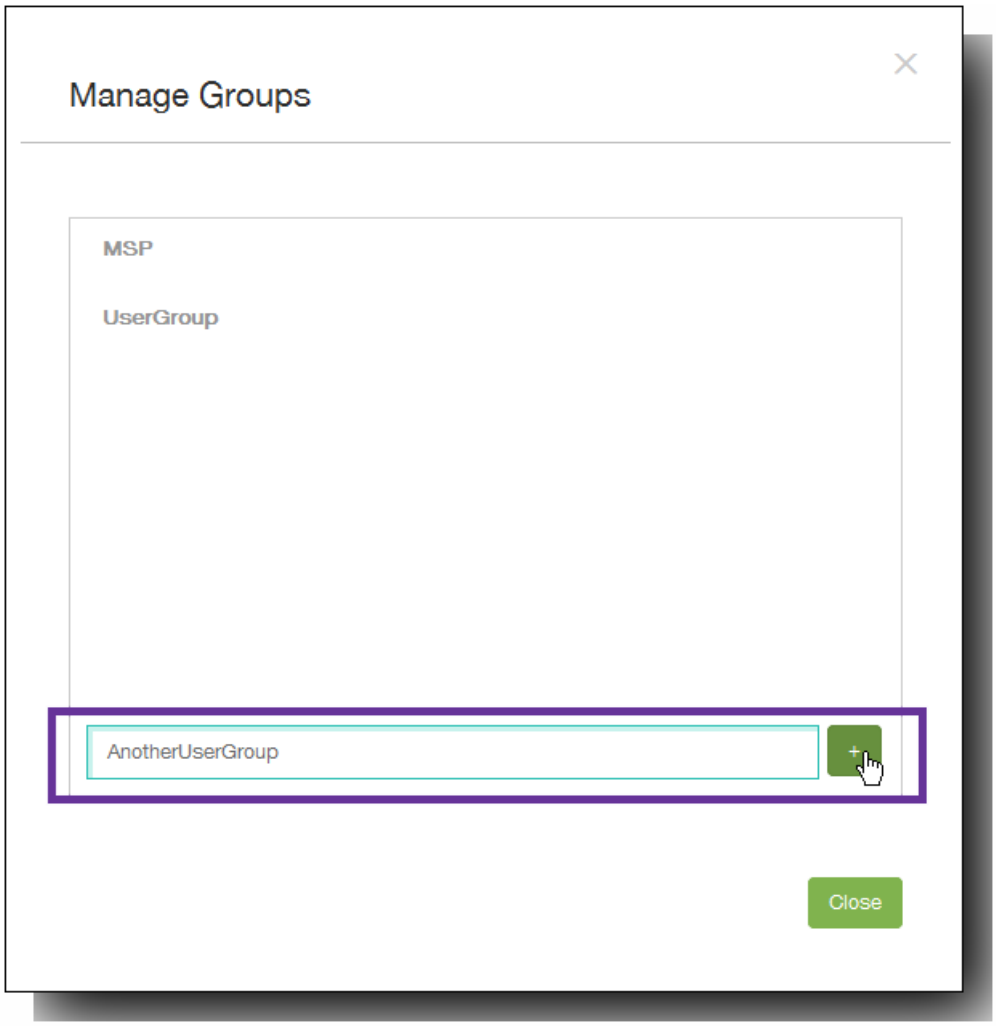
1. Lleve a cabo una de las siguientes acciones:
   - En la página Local Users and Groups, haga clic en Manage Local Groups.



   - Ya sea en la página Add Local User o Edit Local User, haga clic en Manage Groups.



   Aparecerá el cuadro de diálogo Manage Groups.
2. Bajo la lista de grupos, escriba un nuevo nombre de grupo y, a continuación, haga clic en el signo más (+).



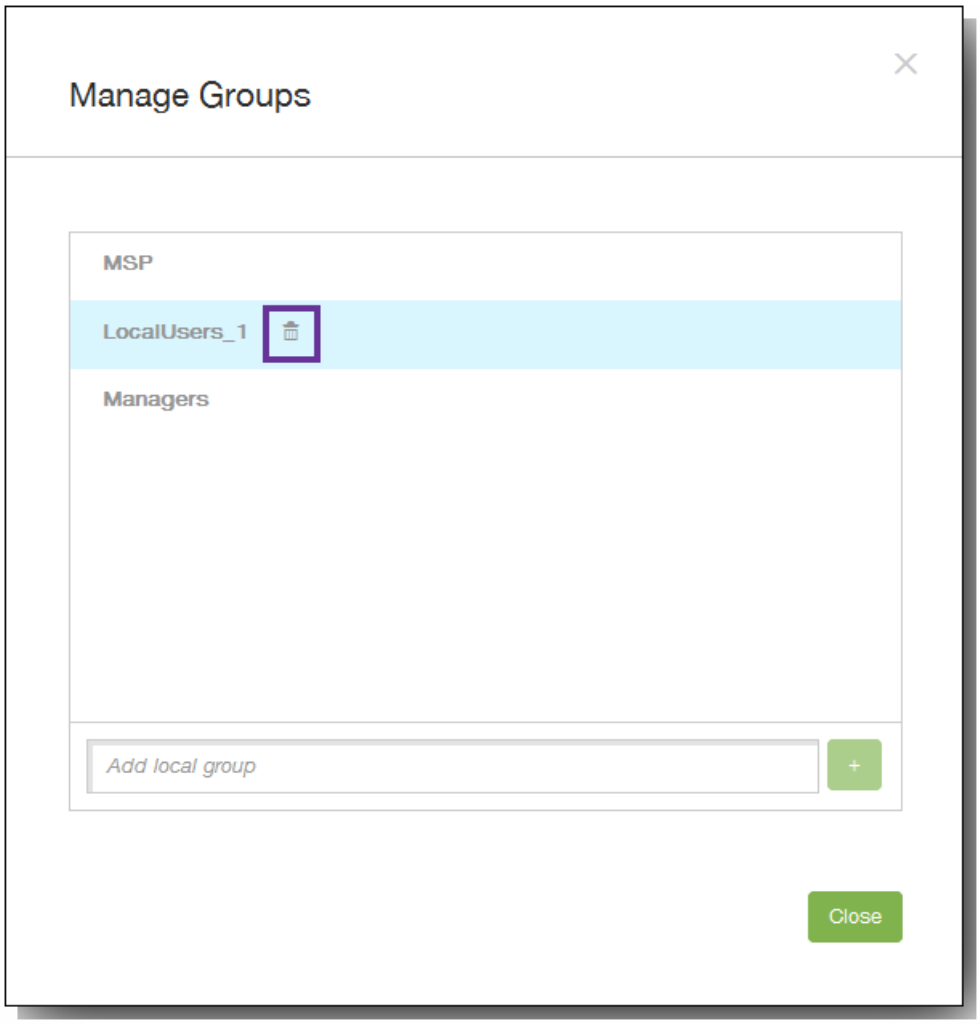
El grupo de usuarios se agrega a la lista.

3. Haga clic en Close.

Nota: Quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios a ese grupo. Asimismo, los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados a ese grupo. Sin embargo, las demás asociaciones de grupos permanecen intactas. Si los usuarios no están asociados a ningún otro grupo local, se asocian al nivel superior.

1. Lleve a cabo una de las siguientes acciones:
   - En la página Local Users and Groups, haga clic en Manage Local Groups.
   - Ya sea en la página Add Local User o Edit Local User, haga clic en Manage Groups.

   Aparecerá el cuadro de diálogo Manage Groups.
2. En el cuadro de diálogo Manage Groups, haga clic en el grupo a eliminar.



3. Haga clic en el icono con forma de papelera situado a la derecha del nombre de grupo. Aparecerá un cuadro de diálogo de confirmación.
4. Haga clic en Delete para confirmar la operación y eliminar el grupo.
   Importante: Esta operación no se puede deshacer.
5. En el cuadro de diálogo Manage Groups, haga clic en Close.

Para configurar modos de inscripción y habilitar el portal Self Help Portal

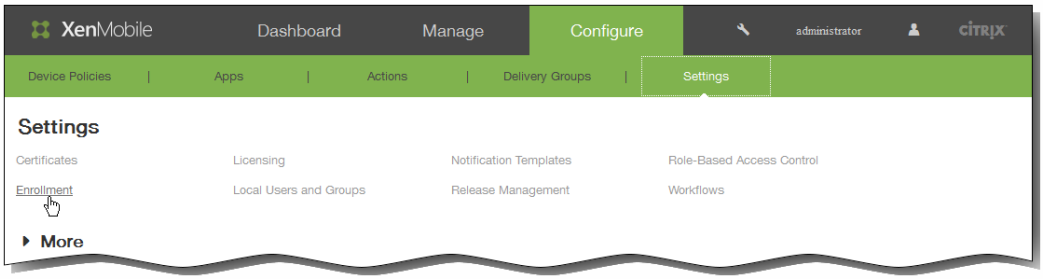
May 05, 2016

Puede configurar modos de inscripción de dispositivos para que los usuarios puedan inscribir sus dispositivos en XenMobile. XenMobile ofrece siete modos, cada uno con su propio nivel de seguridad y unos pasos propios que los usuarios deberán seguir para inscribir sus dispositivos. Puede poner algunos modos a disposición de los usuarios en el portal Self Help Portal. Los usuarios pueden iniciar sesión en ese portal y generar enlaces de inscripción que les permitan inscribir sus propios dispositivos o enviarse la invitación a una inscripción.

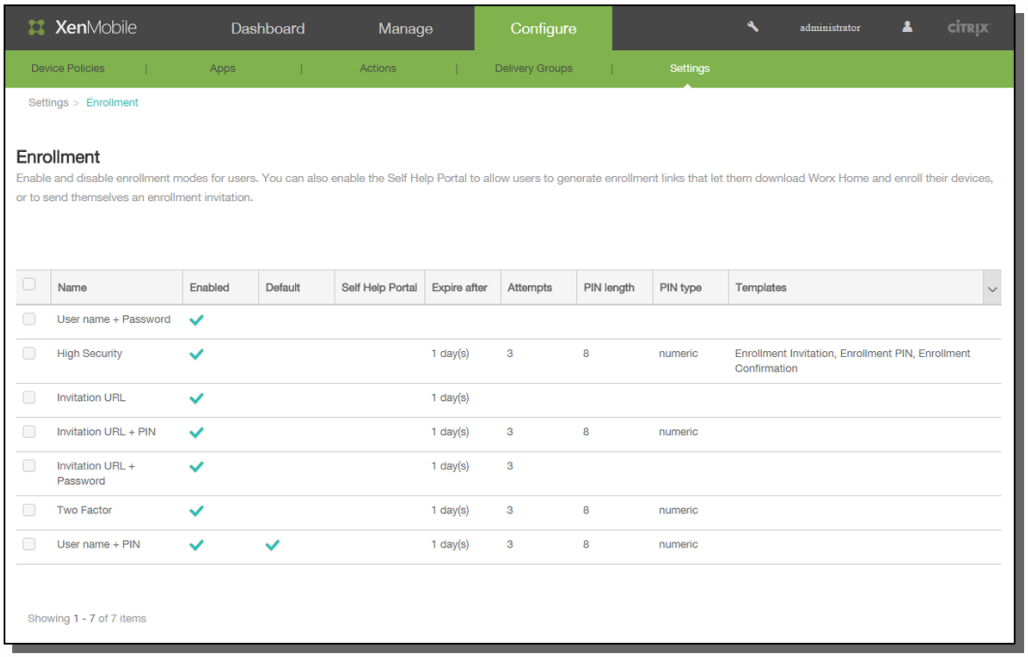
Los modos de inscripción se configuran en la consola de XenMobile, desde la página Settings > Enrollment. En la consola de XenMobile, puede enviar invitaciones a inscripciones desde la página Manage > Enrollment (consulte Inscripción de usuarios y dispositivos en XenMobile).

Nota: Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.

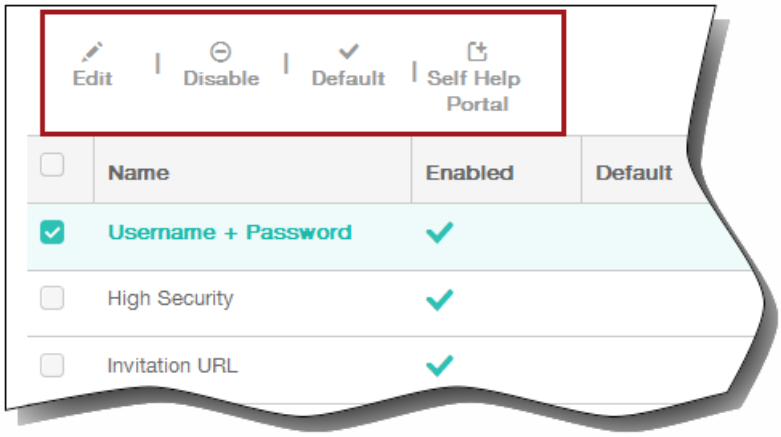
1. En la consola de XenMobile, haga clic en Configure > Settings > Enrollment.

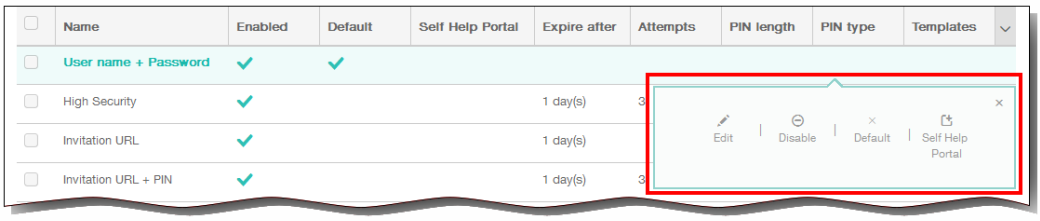


Aparecerá la página Enrollment, que contiene una tabla de todos los modos de inscripción disponibles.



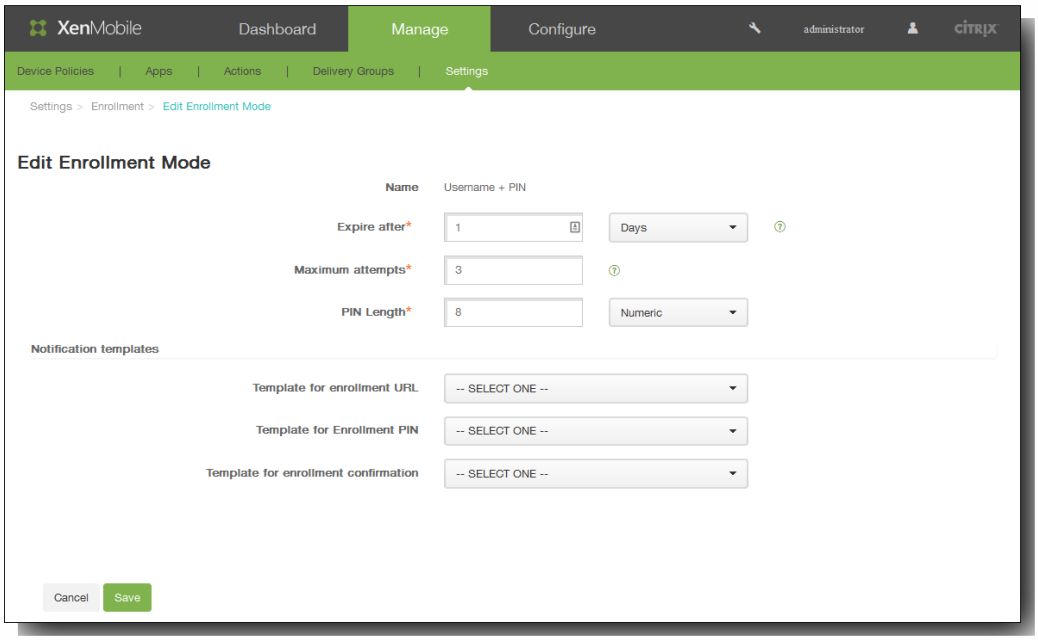
2. Seleccione un modo de inscripción de la lista para modificarlo y, a continuación, establezca ese modo como predeterminado, elimínelo, o bien permita a los usuarios acceder a él a través del portal Self Help Portal.
   Nota: Si marca la casilla situada junto a un modo de inscripción, el menú de opciones aparecerá encima de la lista del modo de inscripción. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.



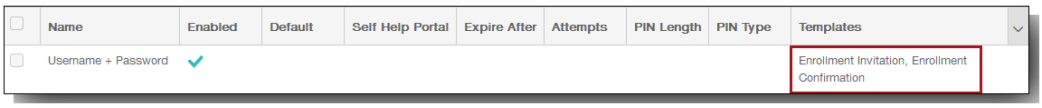


1. En la lista Enrollment, seleccione un modo de inscripción y, a continuación, haga clic en Edit. Según el modo que

seleccione, es posible que vea opciones distintas de las que se muestran en la siguiente ilustración.



2. Cambie la siguiente información como corresponda:
    1. Expire after. Introduzca una fecha límite de caducidad, después de la que los usuarios no podrán inscribir sus dispositivos.
       Nota: Introduzca 0 para evitar que la invitación caduque.
    2. Days. Seleccione Days o Hours, de acuerdo con la fecha límite de caducidad que ha introducido en Expire after.
    3. Maximum Attempts. Introduzca la cantidad de intentos de inscripción que un usuario puede llevar a cabo antes de que se bloquee el proceso de inscripción.
       Nota: Introduzca 0 para permitir una cantidad ilimitada de intentos.
    4. PIN length. Introduzca un número para la cantidad de dígitos o caracteres que contendrá el PIN generado.
    5. Numeric. Seleccione Numeric o Alphanumeric para el tipo de PIN.
3. En Notification templates, modifique las siguientes opciones según corresponda:
    1. Template For Enrollment URL. Seleccione una plantilla para la URL de inscripción. Por ejemplo, mediante la plantilla de invitaciones a inscripciones, se envía a los usuarios una invitación por correo electrónico o por SMS, según como haya configurado la plantilla que les permite inscribir sus dispositivos en XenMobile. Para obtener más información acerca de las plantillas de notificaciones, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.
    2. Template for enrollment confirmation. Seleccione la plantilla a utilizar para informar al usuario de que la inscripción se ha realizado correctamente.
4. Haga clic en Save para guardar los cambios.

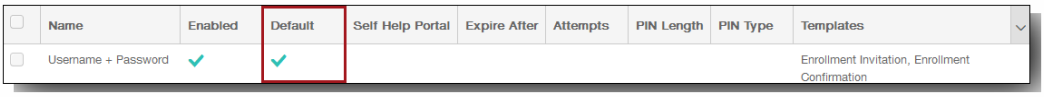


Al establecer un modo de inscripción como predeterminado, ese modo se usará para todas las solicitudes de inscripción de

dispositivos a menos que se seleccione otro modo de inscripción. Si no hay ningún modo de inscripción establecido como predeterminado, debe crear una solicitud de inscripción para cada inscripción de dispositivo.

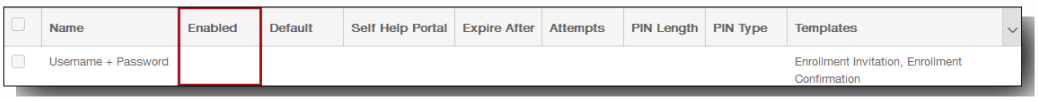
Nota: Solo se pueden establecer los modos Username + Passwords, Two Factor o Username + PIN como modos de inscripción predeterminados.

1. Seleccione uno de los modos, ya sea Username + Passwords, Two Factor o Username + PIN, para establecerlo como modo de inscripción predeterminado.
   Nota: El modo seleccionado debe estar habilitado para poder establecerlo como predeterminado.
2. Haga clic en Default. A partir de ahora, el modo seleccionado es el predeterminado. Si se había establecido otro modo de inscripción como predeterminado, ese modo deja de serlo.



Al inhabilitar un modo de inscripción, ese modo no se podrá usar ni para las invitaciones de grupo a las inscripciones ni en el portal Self Help Portal. Puede cambiar la manera de permitir a los usuarios que inscriban sus dispositivos. Para ello, deberá inhabilitar un modo de inscripción y habilitar otro.

1. Seleccione un modo de inscripción.
   Nota: No se puede inhabilitar el modo de inscripción predeterminado. Si quiere inhabilitar el modo de inscripción predeterminado, primero debe quitar su estado predeterminado.
2. Haga clic en Disable. El modo de inscripción deja de estar habilitado.



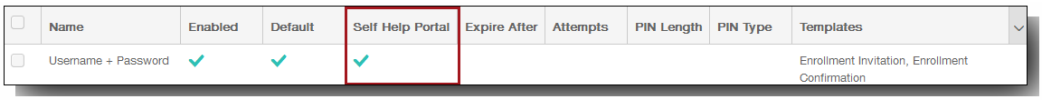
Para habilitar un modo de inscripción en el portal Self Help Portal

Habilitar un modo de inscripción en el portal Self Help Portal permite a los usuarios inscribir sus dispositivos en XenMobile uno a uno.

Nota:

- Para que un modo de inscripción esté disponible en el portal Self Help Portal, debe estar habilitado y enlazado a plantillas de notificaciones.
- Solo puede habilitar un modo de inscripción en el portal Self Help Portal en un momento dado.

1. Seleccione un modo de inscripción.
2. Haga clic en Self Help Portal. El modo de inscripción seleccionado ya está disponible para los usuarios en el portal Self Help Portal. Cualquier otro modo que ya estuviera habilitado en el portal Self Help Portal deja de estar disponible para los usuarios.



	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
☐	Username + Password	✓	✓	✓					Enrollment Invitation, Enrollment Confirmation

Configuración de roles con RBAC

May 05, 2016

En XenMobile, la función del control de acceso basado en roles (RBAC) permite asignar roles predefinidos o conjuntos de permisos a usuarios y grupos. Con estos permisos, se puede controlar el nivel de acceso de los usuarios a las funciones del sistema.

XenMobile implementa cuatro roles de usuario predeterminados para separar de manera lógica el acceso a las funciones del sistema:

- **Administrator**. Concede acceso completo al sistema.
- **Provisioning**. Mediante la herramienta de aprovisionamiento de dispositivos, los administradores utilizan este rol para aprovisionar todos los dispositivos Windows Mobile o Windows CE como si se tratara de un grupo.
- **Support**. Concede acceso para la asistencia remota.
- **User**. Rol utilizado por los usuarios que pueden inscribir dispositivos y acceder al portal Self Help Portal.

Puede crear nuevos roles de usuario con permisos para acceder a funciones específicas del sistema aparte de las funciones definidas por estos roles predeterminados; para ello, puede utilizar las funciones predeterminadas como plantillas personalizables.

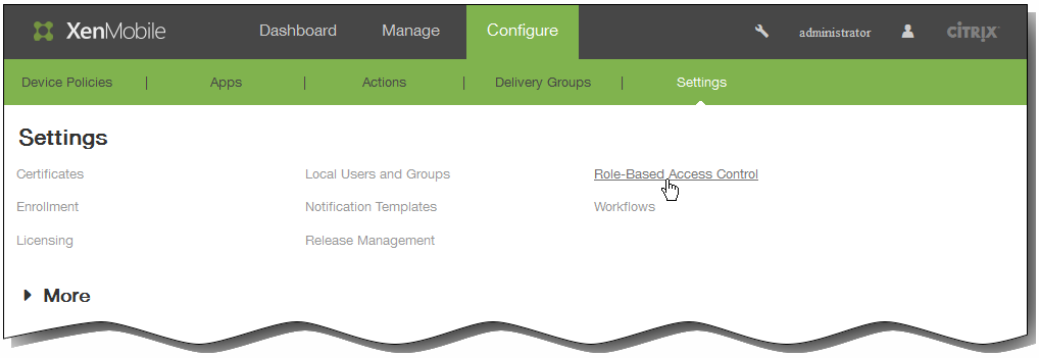
Los roles se pueden asignar a usuarios locales (a nivel de usuario) o a grupos de Active Directory (todos los usuarios de ese grupo tendrán los mismos permisos). Si un usuario pertenece a varios grupos de Active Directory, todos los permisos se combinan entre sí para definir los permisos de ese usuario concreto. Por ejemplo: si los usuarios del grupo ADGroupA pueden ubicar los dispositivos de los administradores, y los usuarios del grupo ADGroupB pueden borrar los dispositivos de los empleados, entonces un usuario que pertenezca a ambos grupos podrá ubicar y borrar dispositivos de administradores *y* de empleados.

Nota: Los usuarios locales solo pueden tener un rol asignado.

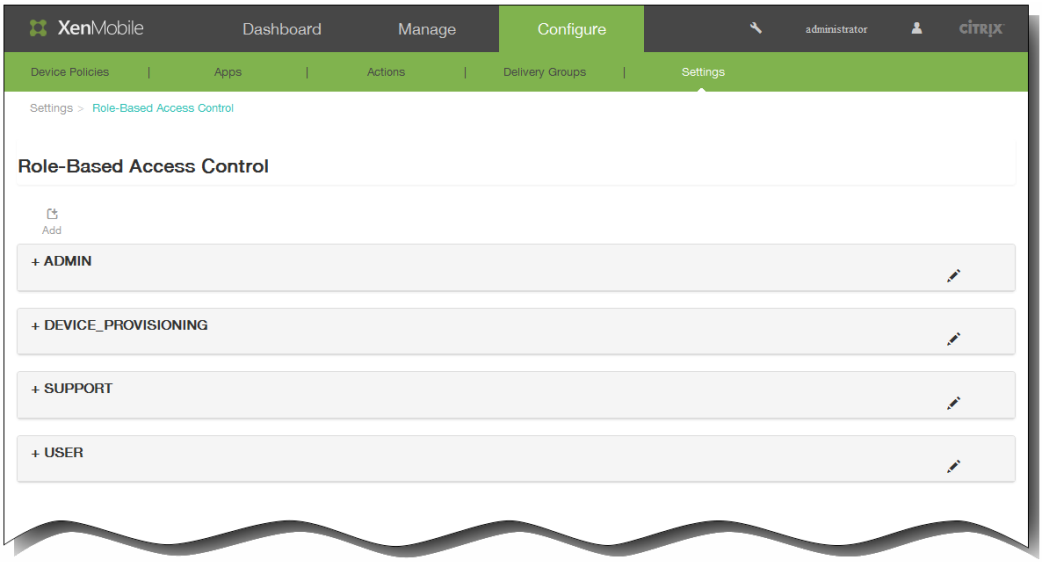
En XenMobile, puede usar la función de control de acceso basado en roles (RBAC) para realizar las siguientes acciones:

- Crear un nuevo rol.
- Agregar grupos a un rol.
- Asociar usuarios locales a roles.

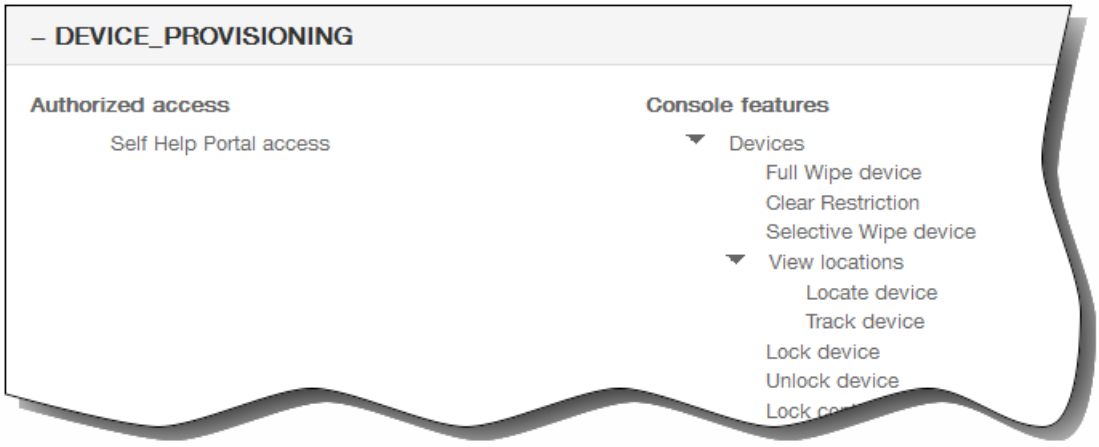
1. En la consola de XenMobile, haga clic en Configure > Settings > Role-Based Access Control.



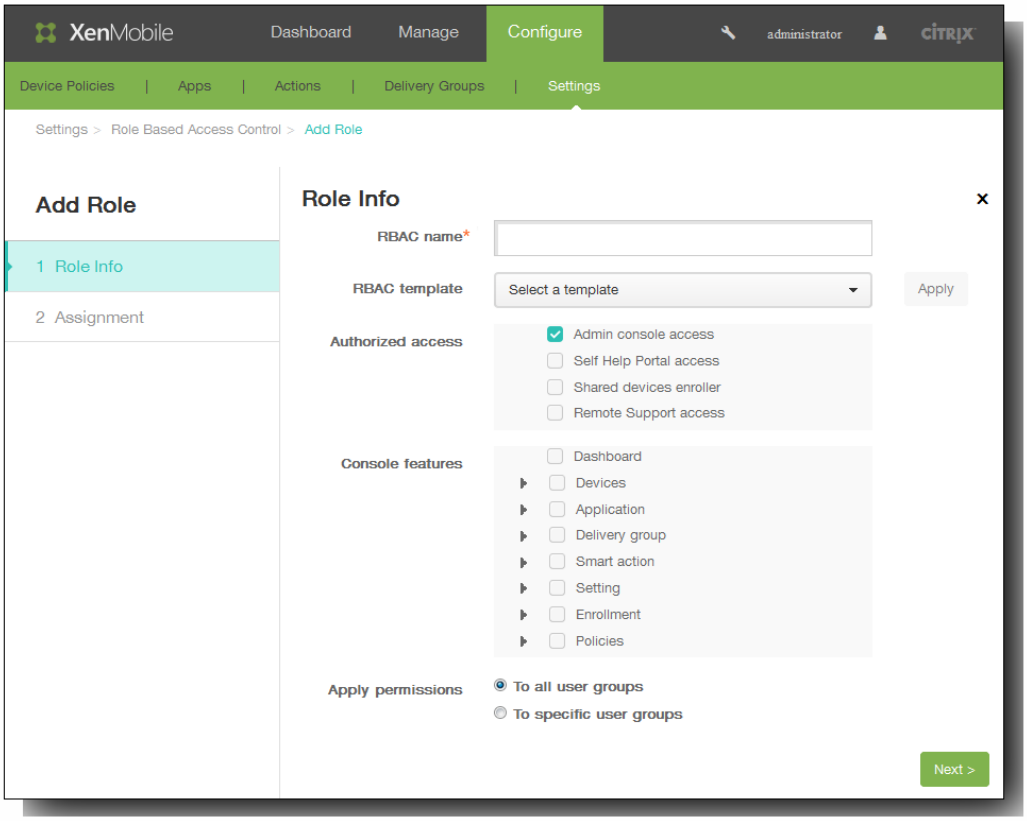
Aparecerá la página Role con los cuatro roles de usuario predeterminados, además de los roles que haya agregado antes.



Nota: Si hace clic en el signo más (+) situado junto a un rol, ese rol se expande para mostrar todos los permisos que se le han concedido, tal y como se muestra en la siguiente imagen.

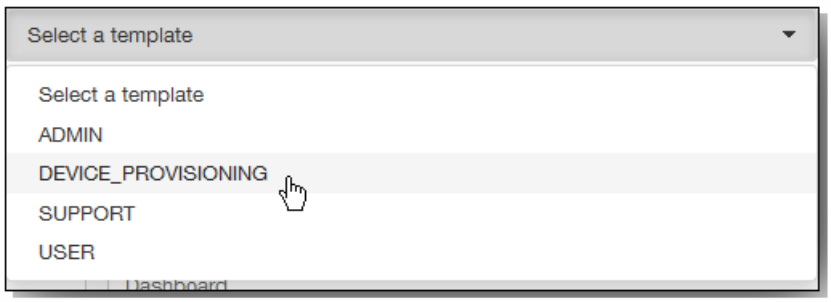


2. Haga clic en Add para agregar un nuevo rol de usuario. También puede hacer clic en el icono de lápiz situado a la derecha de un rol existente para modificarlo, y puede hacer clic en el icono de papelera situado a la derecha de un rol previamente definido para eliminarlo. No se pueden eliminar los roles de usuario predeterminados.
   - Si hace clic en Add o en el icono de lápiz, aparecerán la página Add Role o la página Edit Role.



- Si hace clic en el icono de papelera, aparecerá un diálogo de confirmación. Haga clic en Delete para quitar el rol seleccionado.

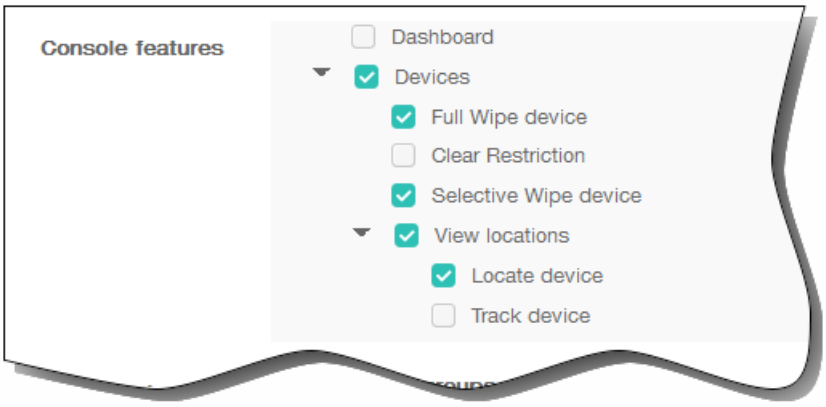
3. Escriba la siguiente información para crear un nuevo rol de usuario o para modificar un rol de usuario existente:
   1. RBAC name. Indique un nombre descriptivo para el nuevo rol de usuario. No se puede cambiar el nombre de un rol existente.
   2. RBAC template. Haga clic en una plantilla como punto de partida para el nuevo rol, o bien haga clic en la nueva plantilla de un rol existente.
      Nota: Las plantillas RBAC son los roles de usuario predeterminados y los roles que se hayan definido previamente. Determinan el acceso a las funciones del sistema que tienen los usuarios asociados a ese rol. Tras seleccionar una plantilla RBAC, puede ver todos los permisos asociados a ese rol en los campos Authorized Access y Console Features. Usar plantillas es opcional; puede seleccionar directamente las opciones que quiera asignar a un rol en los campos Authorized Access y Console Features.



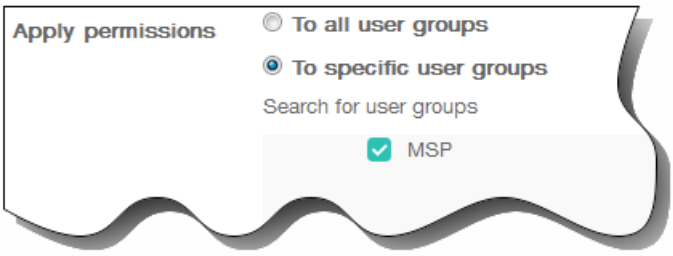
- Haga clic en Apply para rellenar las casillas de Authorized access y Console features con los permisos concedidos de

funciones y acceso predefinidos para la plantilla seleccionada.

- Marque y desmarque las casillas de verificación de Authorized access y Console features para personalizar el rol. Nota: Si hace clic en el triángulo situado junto a función de consola, aparecerán los permisos específicos de esa función y podrá marcarlos o desmarcarlos. Si marca la casilla del nivel superior de la lista, habilitará el acceso de solo lectura a esa parte de la consola. Debe marcar de forma individual las opciones situadas debajo de la casilla del nivel superior para habilitar el acceso de escritura o de actualización a esa opción. Por ejemplo, en la siguiente ilustración, el usuario tiene acceso de solo lectura a la opción Clear Restrictions.

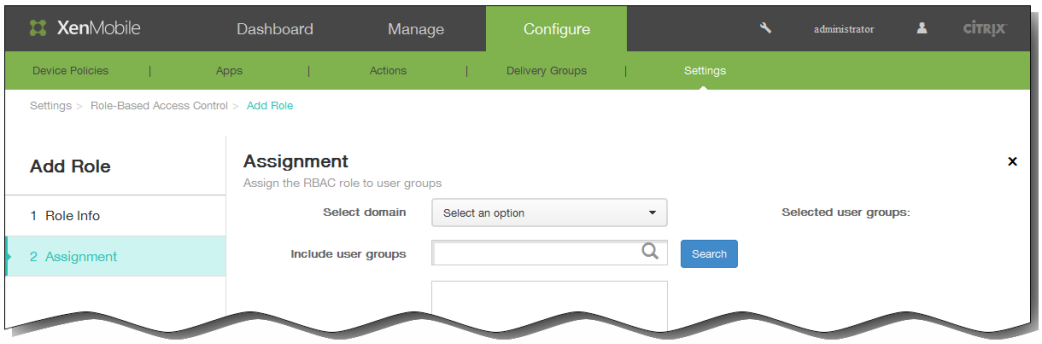


3. Apply permissions. Marque los grupos a los que aplicar los permisos seleccionados.



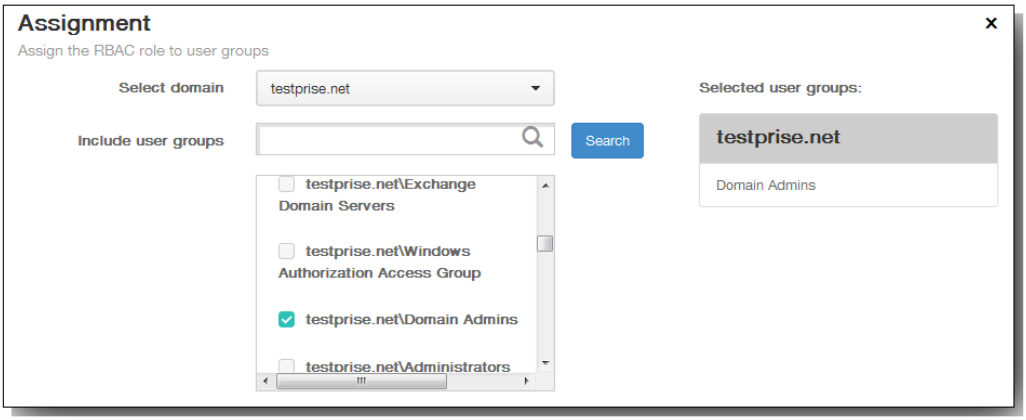
Si hace clic en To specific user groups, aparecerá una lista de grupos. De esa lista, puede seleccionar un grupo o varios.

4. Haga clic en Next. Aparecerá la página Assignment.



5. Escriba la siguiente información para asignar el rol a los grupos de usuarios y, a continuación, haga clic en Save.

1. Select domain. En la lista, haga clic en un dominio.
2. Include user groups. Haga clic en Search para ver una lista de todos los grupos disponibles o escriba un nombre de grupo completo o parcial para limitar la lista a solo aquellos grupos que tengan ese nombre.
3. En la lista que aparezca, seleccione los grupos de usuarios a los que asignar el rol. Cuando seleccione un grupo de usuarios, ese grupo aparecerá en una lista de los grupos seleccionados situada a la derecha del cuadro de búsqueda.



Para quitar un grupo de usuarios de la lista Selected user groups, realice una de las siguientes acciones:

- Haga clic en Search para ver una lista de todos los grupos de usuarios del dominio seleccionado.
- Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en Search para limitar la lista de grupos de usuarios.

Los grupos de usuarios que están incluidos en la lista tienen una casilla de verificación junto a sus nombres en la lista de resultados. Desplácese por la lista y desmarque la casilla de cada grupo que quiera quitar.

Para activar la detección automática en XenMobile para la inscripción de usuarios

Oct 31, 2016

La detección automática simplifica el proceso de inscripción para los usuarios. Con ella, pueden utilizar sus nombres de usuario y contraseñas de Active Directory para inscribir sus dispositivos, en lugar de tener que especificar también datos del servidor XenMobile. Los usuarios deben especificar su nombre de usuario en el formato del nombre principal de usuario (UPN); por ejemplo, usuario@miempresa.com.

Para habilitar la detección automática, puede acceder al portal Autodiscovery Service en https://xenmobiletools.citrix.com. Para obtener más información sobre el portal Autodiscovery Service de detección automática, consulte el tema XenMobile Autodiscovery Service.

En algunos casos, puede que tenga que ponerse en contacto con el servicio de asistencia técnica Citrix Support para habilitar la detección automática. Para hacerlo, siga los procedimientos indicados a continuación para facilitar la información relativa a la implementación. En el caso de dispositivos Windows, también deberá facilitar un certificado SSL al equipo de Asistencia técnica de Citrix. Después de que Citrix reciba esta información, cuando los usuarios inscriban sus dispositivos, se extraerá la información de dominio y esta se asignará a una dirección de servidor. Esta información se conserva en la base de datos de XenMobile para que siempre esté accesible y disponible cuando los usuarios se inscriban.

1. Si no puede habilitar la detección automática desde el portal Autodiscovery Service en https://xenmobiletools.citrix.com, abra un caso de asistencia técnica en el portal de Citrix Support y facilite esta información:
   - El dominio que contiene las cuentas con las que se van a inscribir los usuarios.
   - El nombre de dominio completo (FQDN) de XenMobile.
   - El nombre de la instancia de XenMobile. De forma predeterminada, el nombre de la instancia es zdm y en el campo se distinguen mayúsculas y minúsculas.
   - El tipo de ID de usuario, que puede ser UPN o correo electrónico. De forma predeterminada, el tipo es UPN.
   - El puerto utilizado para la inscripción de iOS si se ha cambiado el número del puerto predeterminado (8443) a otro número de puerto.
   - El puerto a través del cual el servidor XenMobile acepta las conexiones, si se ha cambiado el número del puerto predeterminado (443) a otro número de puerto.
   - Si quiere, puede agregar una dirección de correo electrónico para el administrador de XenMobile.
2. Para inscribir dispositivos Windows, lleve a cabo lo siguiente:
   1. Obtenga un certificado SSL firmado públicamente y sin comodines, para enterpriseenrollment.mycompany.com, donde mycompany.com es el dominio que contiene las cuentas con las que se inscribirán los usuarios. Adjunte el certificado SSL en formato .pfx y su contraseña para la solicitud.
   2. Cree un registro de nombre canónico (CNAME) en el servidor DNS y asigne la dirección del certificado SSL (enterpriseenrollment.mycompany.com) a autodisc.zc.zenprise.com. Cuando el usuario de un dispositivo Windows se inscribe con un nombre UPN, además de proporcionar la información del servidor XenMobile, el servidor de inscripciones de Citrix ordena al dispositivo que solicite un certificado válido al servidor XenMobile.

Su caso de asistencia técnica se actualizará cuando sus datos y su certificado, si procede, se hayan agregado a los servidores Citrix. A partir de este momento, los usuarios pueden empezar a inscribirse con la detección automática.

Nota: También puede usar un certificado de dominios múltiples, en caso de que quiera inscribirse con más de un dominio. El certificado de dominios múltiples debe tener la siguiente estructura:

- Un nombre SubjectDN con un nombre CN que especifica el dominio principal al que está relacionado (por ejemplo, enterpriseenrollment.mycompany1.com).
- Las redes de área de almacenamiento apropiadas para el resto de los dominios (por ejemplo, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com, entre otros).

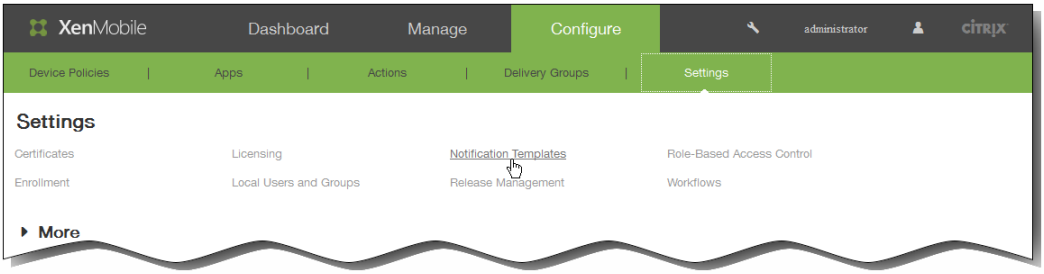
Creación y actualización de plantillas de notificación

May 05, 2016

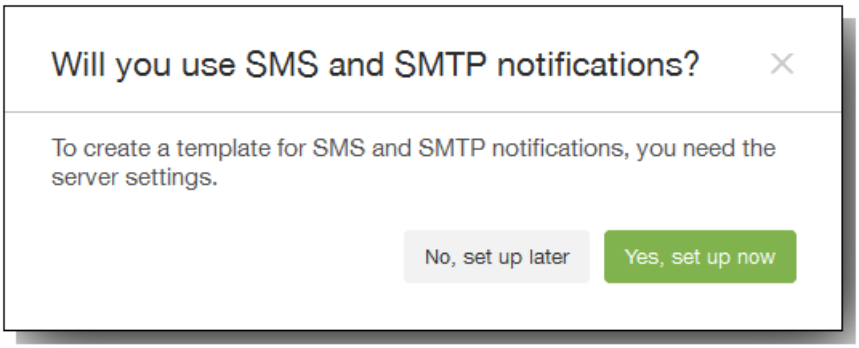
En XenMobile, puede crear o actualizar plantillas de notificaciones que se van a usar en acciones automatizadas, inscripciones y el envío de mensajes de notificación estándar a los usuarios. Puede configurar plantillas de notificaciones para enviar mensajes a través de tres canales diferentes: Worx Home, SMTP o SMS.

Nota: Si quiere utilizar los canales de SMTP o SMS para enviar notificaciones a los usuarios, debe configurar los canales antes de activarlos. XenMobile solicitará configurar los canales cuando usted agregue las plantillas de notificaciones si no están ya configuradas. Para obtener información más detallada, consulte Notificaciones en XenMobile.

1. En la consola de XenMobile, haga clic en Configure > Settings > Notification Templates.



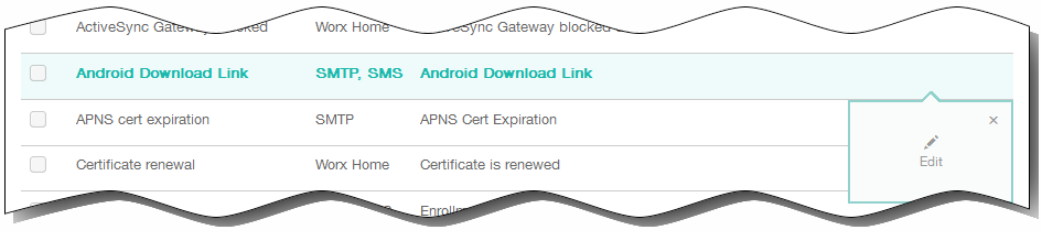
2. Lleve a cabo una de las siguientes acciones:
   - Haga clic en Add para agregar una nueva plantilla de notificaciones. Si no se ha definido ningún servidor SMTP o ninguna puerta de enlace SMS, aparece un mensaje sobre el uso de las notificaciones de SMS y SMTP. Puede optar por configurar el servidor SMTP o la puerta de enlace SMS ahora o más tarde. Para obtener información más detallada, consulte Notificaciones en XenMobile.
     Nota: Si elige configurar el servidor SMTP o SMS ahora, se le redirigirá a la página Configure > Settings > Notification Server. Después de configurar los canales que se van a utilizar, puede volver a la página Configure > Settings > Notification Template para continuar agregando o modificando plantillas de notificaciones.
     Importante: Si elige configurar el servidor SMTP o SMS más tarde, no podrá activar esos canales cuando agregue o modifique una plantilla de notificaciones, lo que significa que esos canales no estarán disponibles para el envío de notificaciones de usuario.



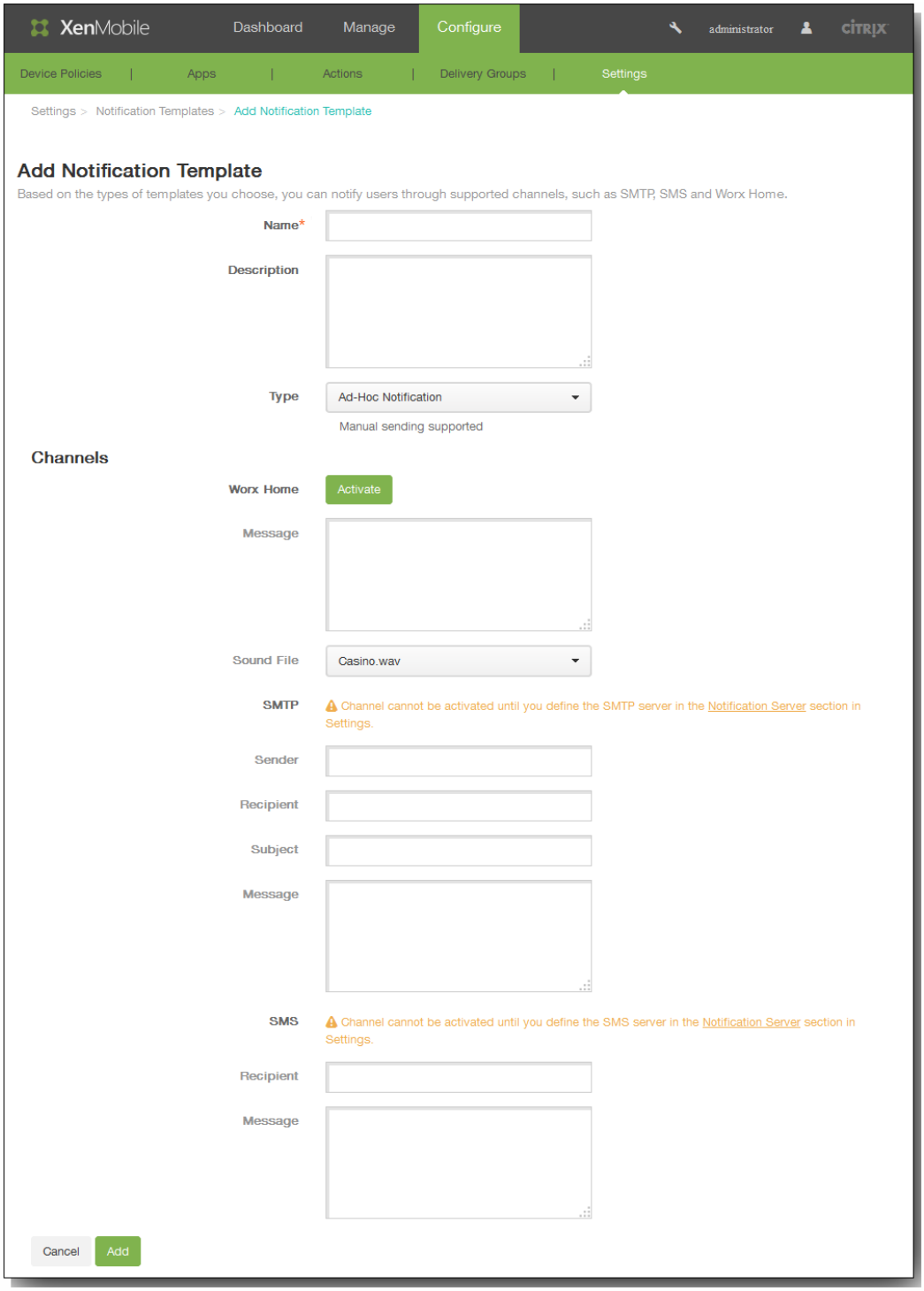
   - Seleccione una plantilla existente para modificarla o eliminarla. Haga clic en la opción pertinente.
     Nota:
     - Solo puede eliminar las plantillas de notificaciones que haya agregado; no podrá eliminar las plantillas de

notificaciones predeterminadas.

- Si marca la casilla situada junto a una plantilla de notificaciones, el menú de opciones aparecerá encima de la lista de plantillas de notificaciones. En cambio, si hace clic en cualquier lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.
- XenMobile incluye varias plantillas de notificaciones predefinidas, las cuales reflejan los distintos tipos de eventos a los que XenMobile responde automáticamente en relación a cada dispositivo del sistema.



Al hacer clic para agregar una plantilla, aparecerá la página Add Notification Template.



3. En la página Add Notification Template (o en la página Edit Notification Template si va a modificar una notificación existente), escriba o modifique la información siguiente:
   1. Name. Escriba un nombre descriptivo para la plantilla.
   2. Description. Escriba una descripción para la plantilla.
   3. Type. Seleccione el tipo de notificación. Solo se muestran los canales admitidos para el tipo de notificación seleccionado.

      Nota: En algunos tipos de plantilla aparece la frase Manual sending supported debajo del tipo. Esto significa que la plantilla está disponible en la lista Notifications del Dashboard y en la página Devices para que usted pueda enviar notificaciones manualmente a los usuarios. Independientemente del canal utilizado, el envío manual no está disponible

para las plantillas que utilizan las siguientes macros en los campos Subject o Message:

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

Atención: Solo se permite la plantilla predefinida de caducidad APNS Cert Expiration. Esto significa que no se puede agregar una nueva plantilla de este tipo.

4. Channels. Escriba o modifique la información de cada canal que se va a utilizar con esta notificación. Puede elegir un canal cualquiera o todos. Los canales que seleccione dependen de la forma en que quiera enviar notificaciones:
   - Si elige Worx Home, solo los dispositivos iOS y Android recibirán las notificaciones, que aparecerán en la bandeja de notificaciones de los dispositivos en cuestión.
   - Si elige SMS, solo los usuarios con dispositivos dotados de una tarjeta SIM recibirán las notificaciones.
   - Si elige SMTP, la mayoría de los usuarios debe recibir el mensaje porque se habrán inscrito con sus direcciones de correo electrónico.

   Worx Home
   1. Activate. Haga clic para habilitar el canal de notificación.
   2. Message. Escriba el mensaje que se enviará al usuario. Este campo es obligatorio si está usando Worx Home.
   3. Sound File. Seleccione el sonido de notificación que oirá el usuario cuando reciba la notificación.

   SMTP
   1. Haga clic en Activate para habilitar el canal de notificación.
      Importante: Solo se puede activar la notificación de SMTP si ya se ha configurado el servidor SMTP. Para obtener información más detallada, consulte Notificaciones en XenMobile.
   2. Sender. Escriba un remitente optativo para la notificación, que puede consistir en un nombre, una dirección de correo electrónico o ambos.
   3. Recipient. Este campo contiene una macro previamente generada para todas las notificaciones salvo las ad-hoc. De este modo, se garantiza que las notificaciones se envían a la dirección correcta de destino de SMTP. Citrix recomienda no modificar macros de plantillas. También puede agregar destinatarios (por ejemplo, el administrador de empresa), además del usuario. Para ello, agregue sus direcciones separadas por un punto y coma (;). Para enviar notificaciones ad hoc, puede especificar destinatarios específicos en esta página, o bien puede seleccionar los dispositivos desde la página Manage > Devices y enviar notificaciones desde allí. Para obtener información más detallada, consulte Cómo agregar dispositivos y ver información de los mismos en XenMobile.
   4. Subject. Escriba un asunto descriptivo para la notificación. Este campo es necesario si usa SMTP.
   5. Message. Escriba el mensaje que se enviará al usuario.

   SMS
   1. Haga clic en Activate para habilitar el canal de notificación.
      Importante: Solo se puede activar la notificación de SMTP si ya se ha configurado el servidor SMTP. Para obtener información más detallada, consulte Notificaciones en XenMobile.
   2. Recipient. Este campo contiene una macro previamente generada para todas las notificaciones salvo las ad-hoc. De este modo, se garantiza que las notificaciones se envían a la dirección correcta de destino de SMTP. Citrix recomienda no modificar macros de plantillas. Para enviar notificaciones ad hoc, puede escribir destinatarios específicos o bien puede seleccionar los dispositivos desde la página Manage > Devices. Para obtener información más detallada, consulte Cómo agregar dispositivos y ver información de los mismos en XenMobile.
   3. Message. Escriba el mensaje que se enviará al usuario. Este campo es necesario si usa SMS.
      Importante: Solo se puede activar la notificación de SMS si ya se ha configurado una puerta de enlace SMS. Para obtener información más detallada, consulte Notificaciones en XenMobile.
5. Haga clic en Add para agregar la nueva plantilla, o bien haga clic en Save para guardar los cambios. Cuando todos los canales se hayan configurado correctamente, aparecen en este orden en la página Notification Templates: SMTP, SMS y Worx Home. Los canales configurados incorrectamente aparecen después de los canales configurados correctamente.

Administración de grupos de entrega

May 05, 2016

Los grupos de entrega indican la categoría de usuarios en cuyos dispositivos se implementan las combinaciones de directivas, aplicaciones y acciones. Por regla general, la inclusión en un grupo de entrega se basa en las características de los usuarios (por ejemplo, la empresa, el país, el departamento, el título y la dirección de la oficina). Los grupos de entrega permiten ejercer más control sobre quién obtiene qué recursos y cuándo lo hacen. Puede implementar un grupo de entrega para todos los usuarios, o bien para un grupo más definido de ellos.

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS y Windows Phone 8.1 y tabletas Windows 8.1 que pertenezcan a ese grupo de entrega para que se vuelvan a conectar a XenMobile con el fin de que se puedan volver a evaluar los dispositivos e implementar en ellos aplicaciones, directivas y acciones. Aquellos usuarios que tengan dispositivos con otras plataformas reciben los recursos de inmediato si ya están conectados o la próxima vez que se conecten, según la directiva de programación definida.

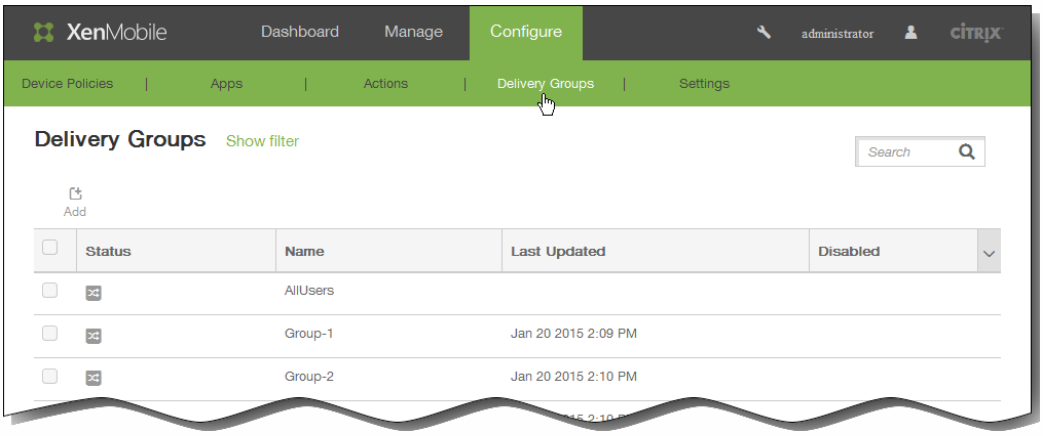
Al instalarse y configurarse XenMobile, se crea el grupo de entrega predeterminado AllUsers. Este grupo contiene todos los usuarios locales y los usuarios de Active Directory. No se puede eliminar el grupo AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios.

En XenMobile, puede agregar, modificar, inhabilitar, habilitar, implementar y eliminar grupos de entrega para administrar el modo en que se implementan las directivas, las aplicaciones y las acciones para los usuarios. Cada una de estas acciones se describe con más detalle en los apartados siguientes de este tema:

- Para agregar un grupo de entrega
- Para modificar un grupo de entrega
- Para habilitar e inhabilitar el grupo de entrega AllUsers
- Para implementar grupos de entrega
- Para eliminar grupos de entrega

Para empezar a administrar los grupos de entrega, abra la página Delivery Groups de la siguiente manera:

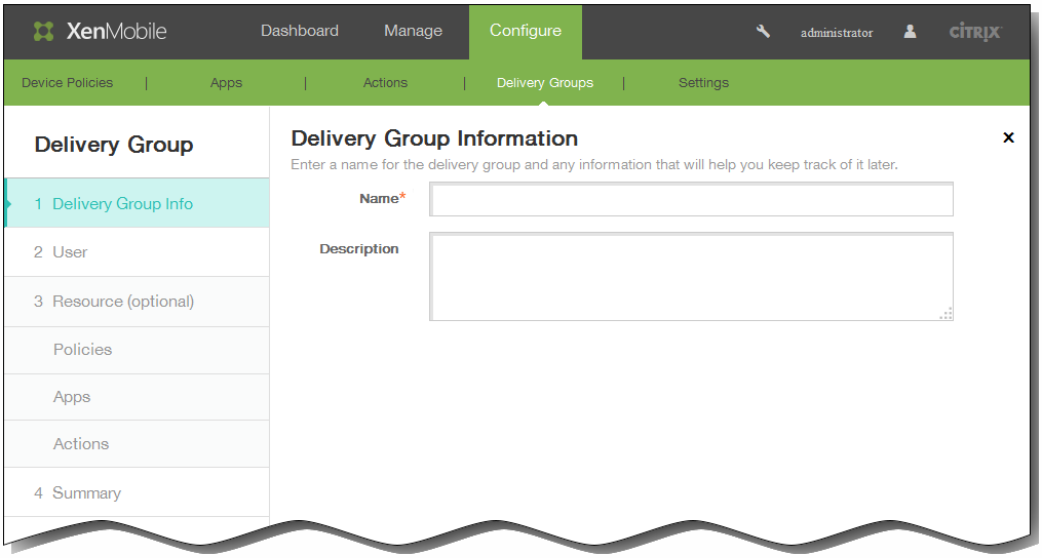
1. En la consola de XenMobile, haga clic en Configure > Delivery Groups.



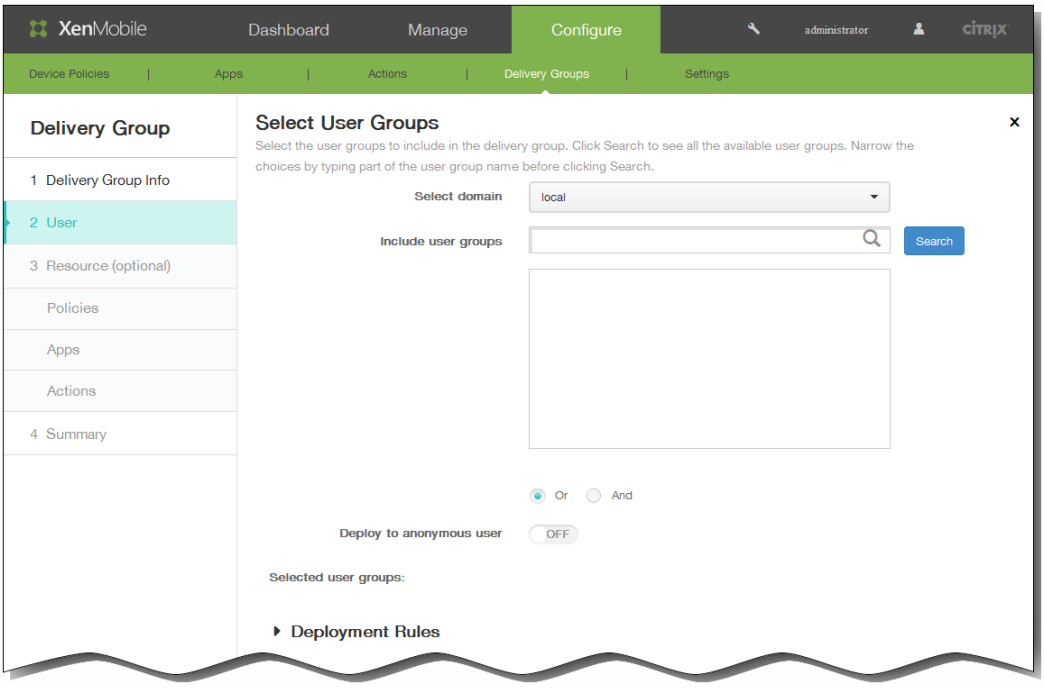
Aparecerá la página Delivery Groups. A continuación, consulte el tema concreto de eDocs dedicado a la acción que

quiera realizar.

1. En la página Delivery Groups, haga clic en Add. Aparecerá la página Delivery Group Information.

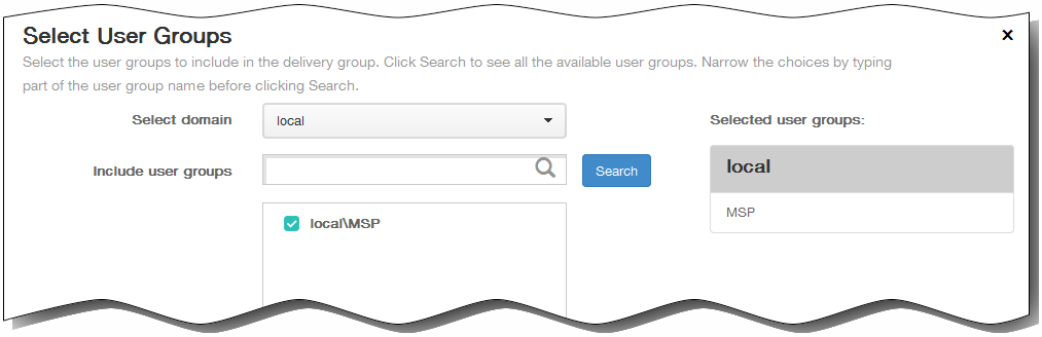


2. En el panel Delivery Group Information, escriba la información siguiente:
   1. Name. Indique un nombre descriptivo para el grupo de entrega.
   2. Description. Escriba, si quiere, una descripción del grupo de entrega.
3. Haga clic en Siguiente. Aparecerá la página Delivery Group User.



4. En el panel Select User Groups, escriba la información siguiente:

1. Select domain. En la lista, seleccione el dominio del que se elegirá a los usuarios.
2. Include user groups. Realice una de las siguientes acciones:
   - Haga clic en Search para ver una lista de todos los grupos de usuarios del dominio seleccionado.
   - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en Search para limitar la lista de grupos de usuarios.
3. En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista Selected user groups.



   Para quitar un grupo de usuarios de la lista Selected user groups, realice una de las siguientes acciones:
   - Haga clic en Search para ver una lista de todos los grupos de usuarios del dominio seleccionado.
   - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en Search para limitar la lista de grupos de usuarios.

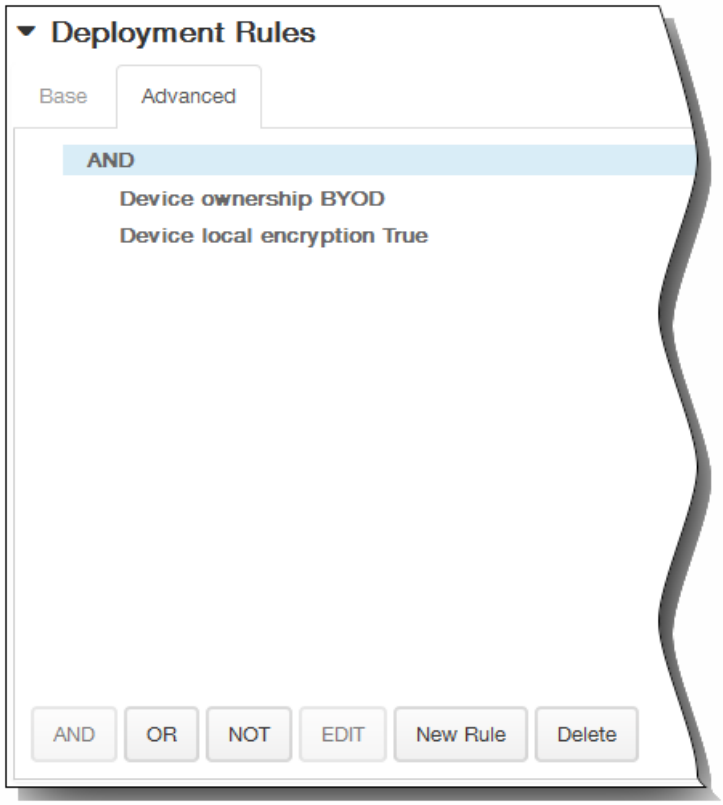
   Los grupos de usuarios que están incluidos en la lista Selected user groups tienen una casilla de verificación junto a sus nombres en la lista de resultados. Desplácese por la lista y desmarque la casilla de cada grupo que quiera quitar.

4. Or/And. Seleccione si los usuarios pueden estar en cualquier grupo (Or) o si deben estar en todos los grupos (And) para que se implemente el recurso para ellos.
5. Deploy to anonymous user. Seleccione si implementar recursos para usuarios sin autenticar del grupo de entrega. Nota: Los usuarios sin autenticar son aquellos que no han podido autenticarse pero a cuyos dispositivos se les ha permitido conectarse a XenMobile de todas formas.
5. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.

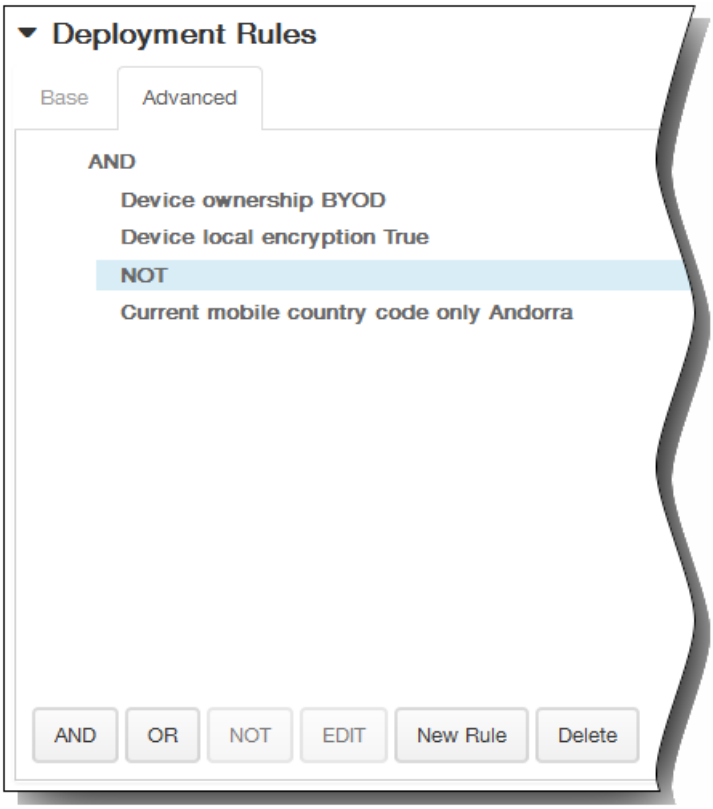
2. Haga clic en New Rule para definir las condiciones.
3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.

2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

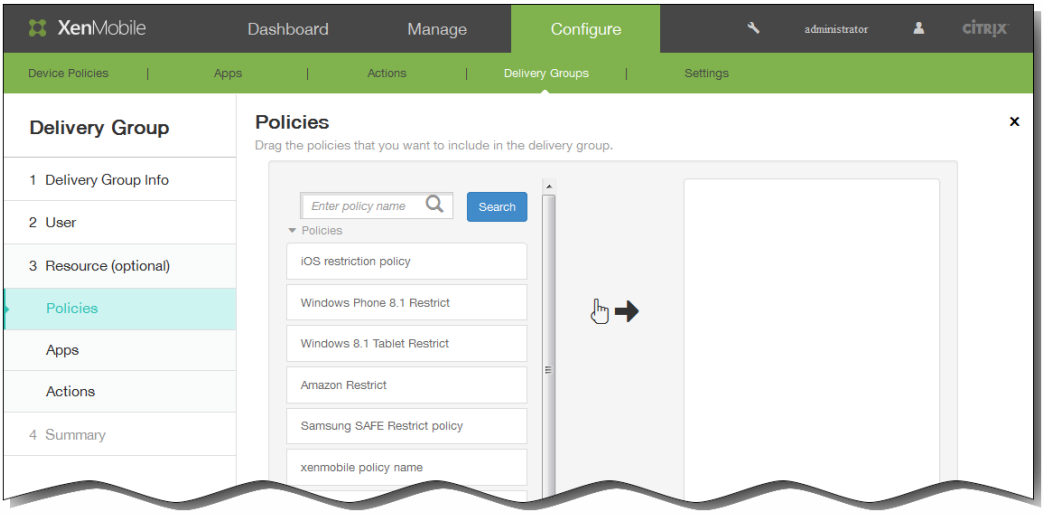


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.

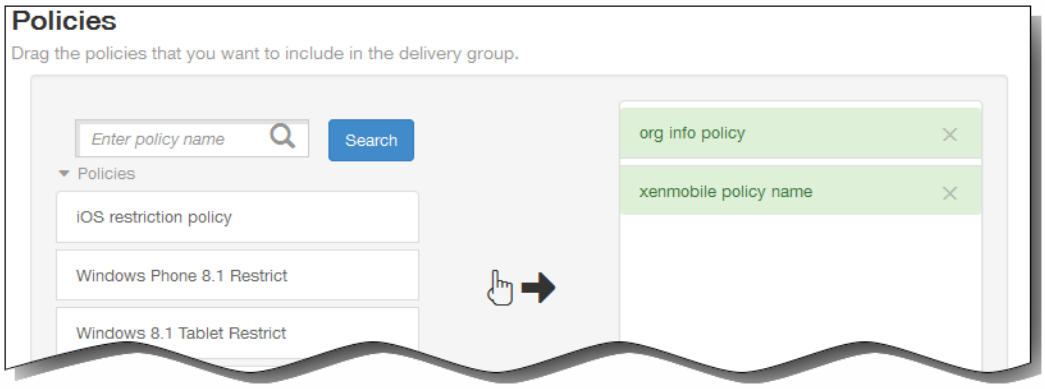


6. Haga clic en Siguiente. Aparecerá la página Delivery Group Resources. Si quiere, aquí puede agregar directivas, aplicaciones o acciones al grupo de entrega. Para omitir este paso, en Delivery Group, haga clic en Summary para ver un resumen de la configuración del grupo de entrega; de lo contrario, puede hacer lo siguiente:
   Nota: Para omitir un recurso, en Resources (optional), haga clic en el recurso que quiere agregar y siga los pasos de ese recurso.
   Para agregar directivas



1. Desplácese por la lista de las directivas disponibles hasta encontrar la directiva que quiera agregar. Para limitar la lista de directivas, escriba el nombre completo o parcial de esta en el cuadro de búsqueda y, a continuación, haga clic en Search.

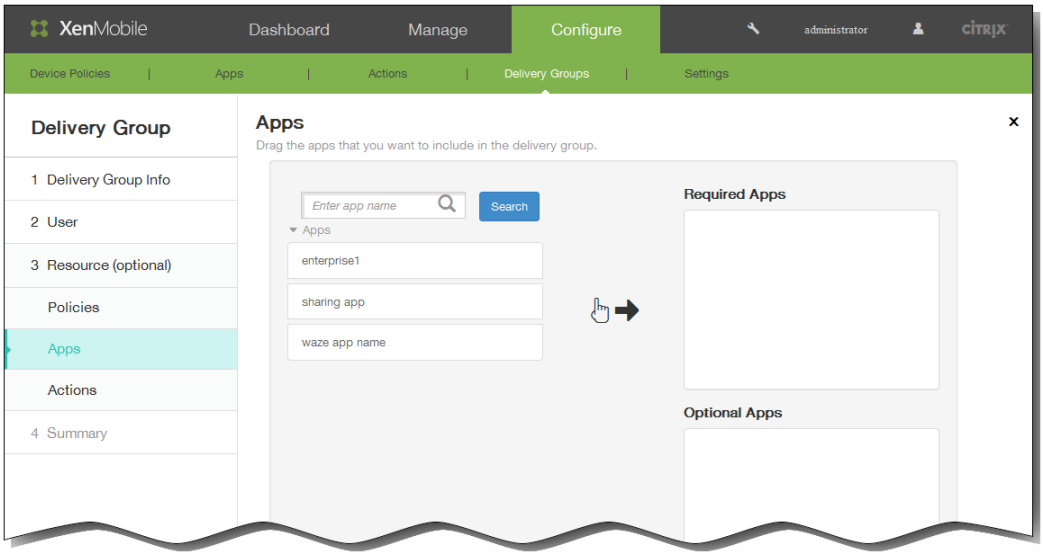
2. Haga clic en una directiva y arrástrela al cuadro de la derecha.
3. Repita los pasos a. y b. para agregar más directivas.



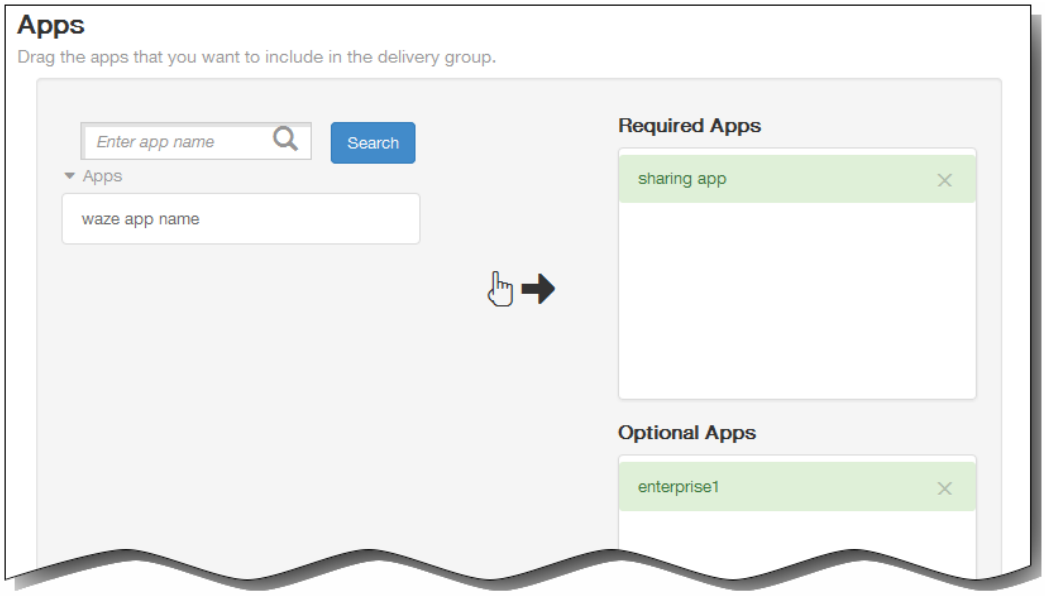
Para eliminar una directiva, haga clic en la X situada junto al nombre de esa directiva.

4. Haga clic en Next para ir a la página del recurso Apps. Si no va a agregar más recursos, en Delivery Group, haga clic en Summary. Aparecerán la página Apps o la página Summary.

Para agregar aplicaciones



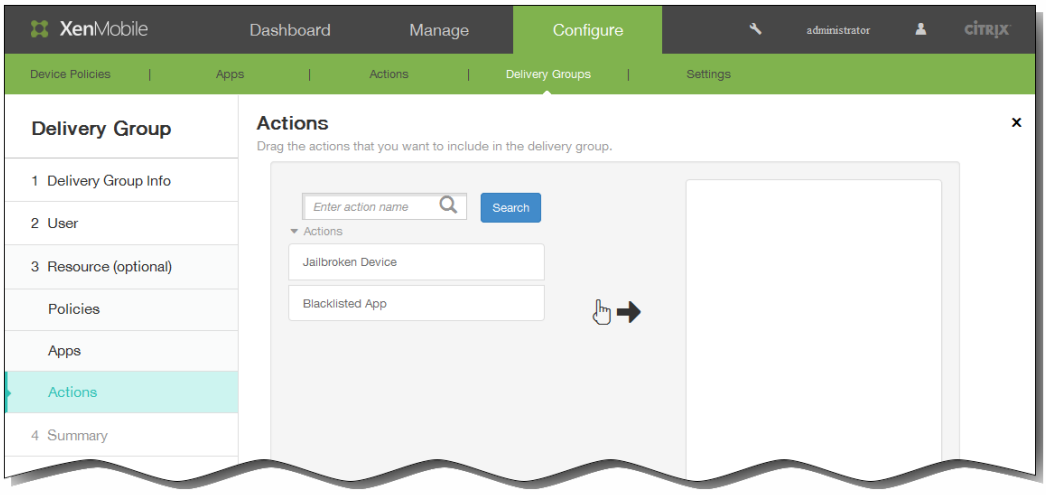
1. Desplácese por la lista de las aplicaciones disponibles hasta encontrar la aplicación que quiera agregar. Para limitar la lista de aplicaciones, escriba el nombre completo o parcial de ésta en el cuadro de búsqueda y, a continuación, haga clic en Search.
2. Haga clic en una aplicación y arrástrela al cuadro Required Apps o al cuadro Optional Apps.
3. Repita los pasos a. y b. para agregar más aplicaciones.



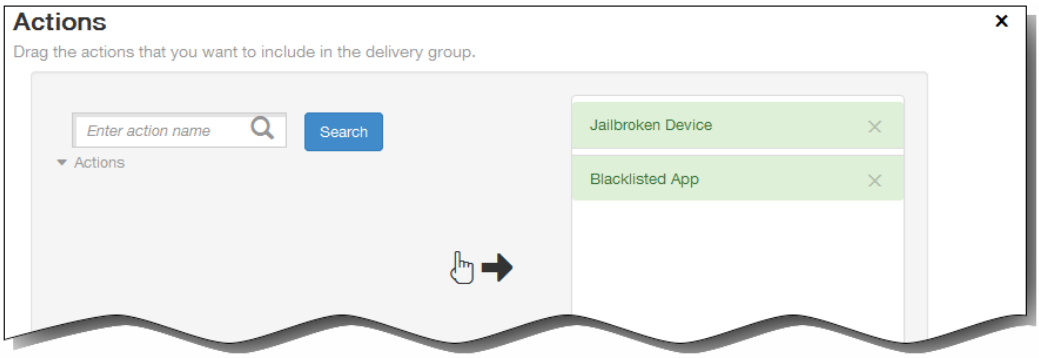
Para eliminar una aplicación, haga clic en la X situada junto al nombre de esa aplicación.

4. Haga clic en Next para ir a la página del recurso Actions. Si no va a agregar más recursos, en Delivery Group, haga clic en Summary. Aparecerán la página Actions o la página Summary.

Para agregar acciones

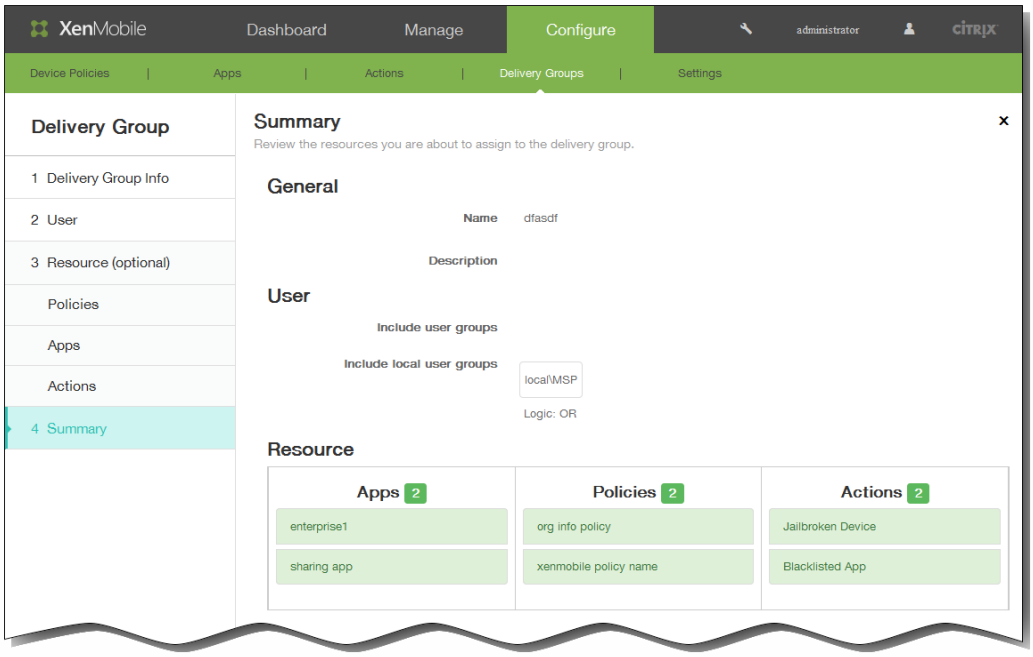


1. Desplácese por la lista de las acciones disponibles hasta encontrar la acción que quiera agregar. Para limitar la lista de acciones, escriba el nombre completo o parcial de ésta en el cuadro de búsqueda y, a continuación, haga clic en Search.
2. Haga clic en una acción y arrástrela al cuadro de la derecha.
3. Repita los pasos a. y b. para agregar más acciones.



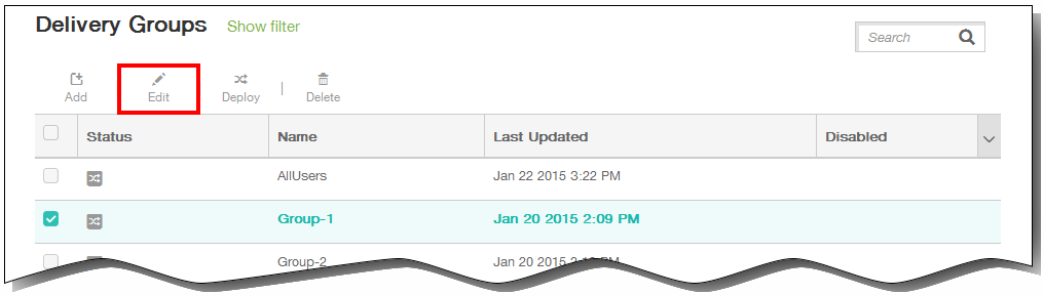
Para eliminar una acción, haga clic en la X situada junto al nombre de esa acción.

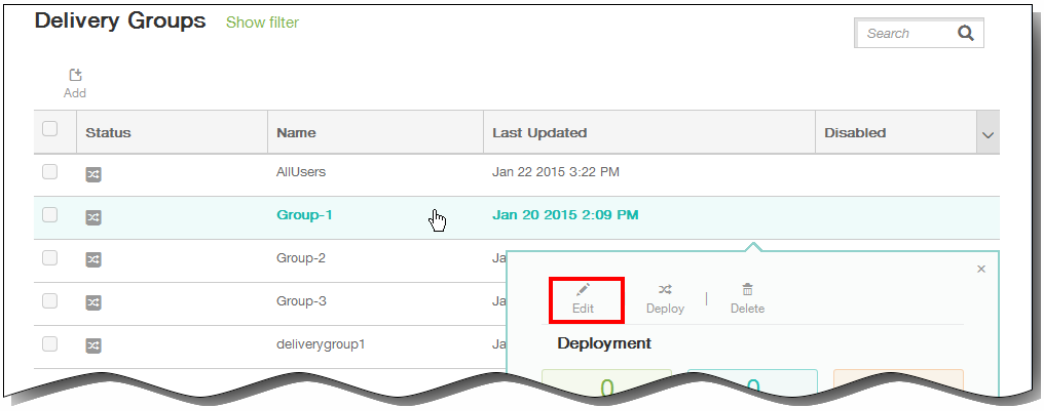
4. Haga clic en Next. Aparecerá la página Summary.



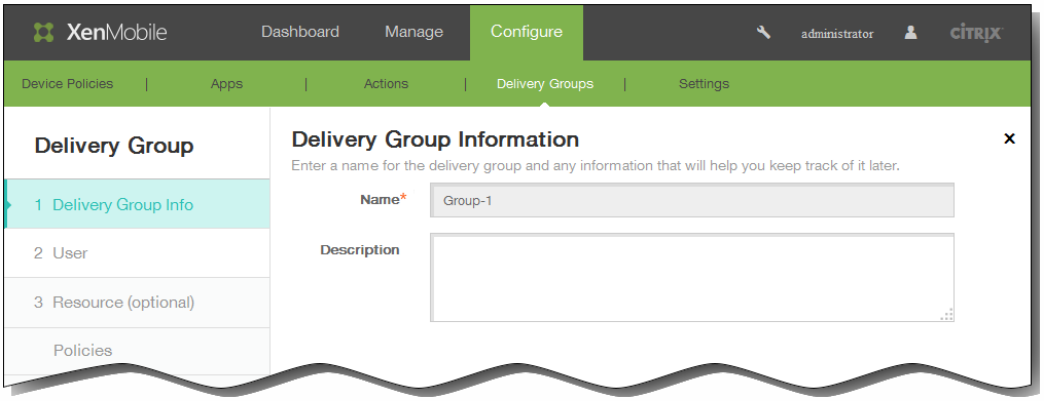
7. En la página Summary, revise las opciones que haya configurado para el grupo de entrega. Haga clic en Back para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.
8. Haga clic en Save para guardar el grupo de entrega.

1. En la página Delivery Groups, seleccione el grupo de entrega que quiera modificar. Puede seleccionarlo de dos maneras: marcando la casilla de verificación que aparece junto a su nombre o haciendo clic en la línea que contiene su nombre.
2. Haga clic en Edit.
   Nota: Según cómo haya seleccionado el grupo de entrega, el comando Edit aparecerá encima o a la derecha del grupo de entrega.

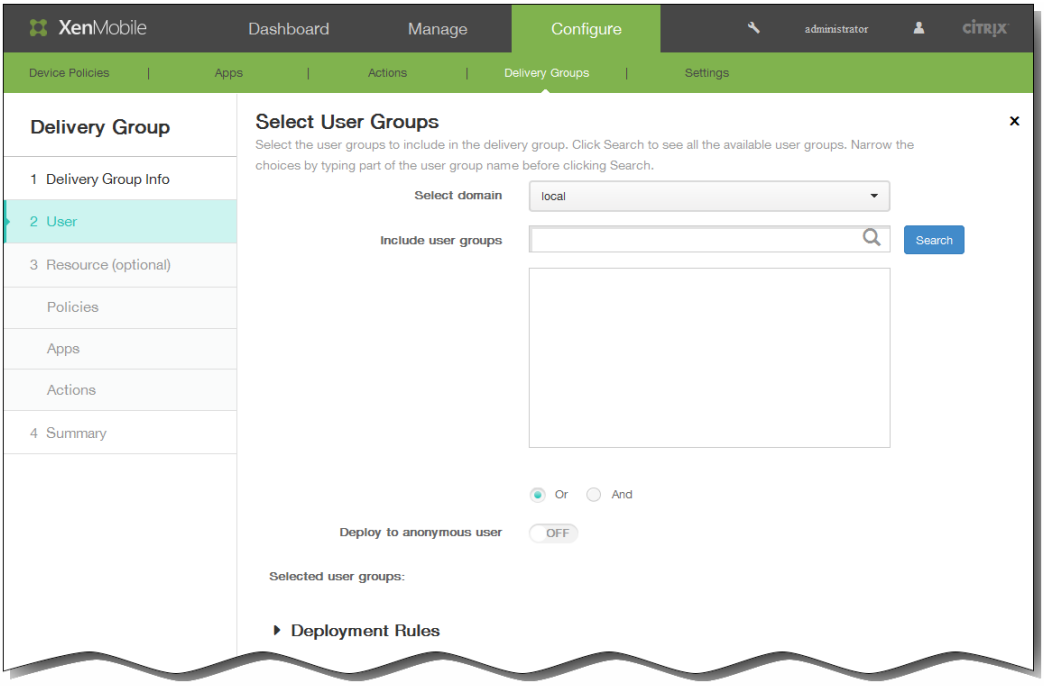




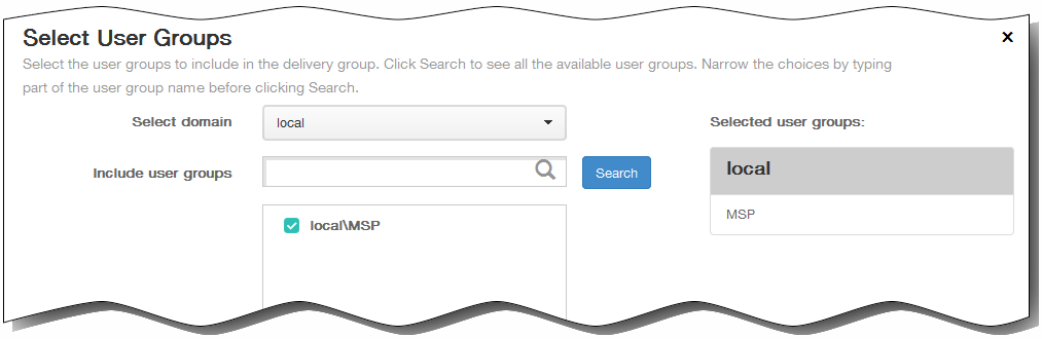
Aparecerá la página para modificar la información de grupos de entrega Delivery Group Information.



3. Agregue o cambie el campo Description.
   Nota: No se puede cambiar el nombre de un grupo existente.
4. Haga clic en Siguiente. Aparecerá la página Select User Groups.



5. En el panel Select User Groups, escriba o cambie la información siguiente:
   1. Select domain. En la lista, seleccione el dominio del que se elegirán los usuarios.
   2. Include user groups. Realice una de las siguientes acciones:
      - Haga clic en Search para ver una lista de todos los grupos de usuarios del dominio seleccionado.
      - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en Search para limitar la lista de grupos de usuarios.
   3. En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista Selected user groups.

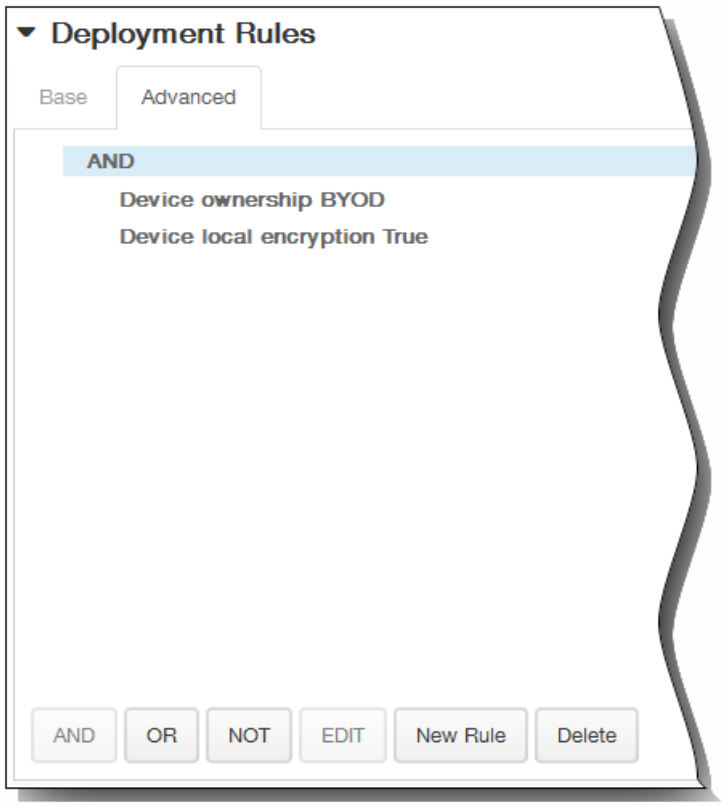


   Nota: Para quitar grupos de usuarios, haga clic en Search y, en la lista de los grupos de usuarios, desmarque la casilla situada junto al grupo o grupos que quiera quitar. Puede escribir un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, hacer clic en Search para limitar la cantidad de grupos de usuarios que se mostrarán en la lista.
   4. Or/And. Seleccione si los usuarios pueden estar en cualquier grupo (Or) o si deben estar en todos los grupos (And) para que se implemente el recurso para ellos.
   5. Deploy to anonymous user. Seleccione si implementar recursos para usuarios sin autenticar del grupo de entrega. Nota: Los usuarios sin autenticar son aquellos que no han podido autenticarse pero a cuyos dispositivos se les ha

permitido conectarse a XenMobile.

6. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

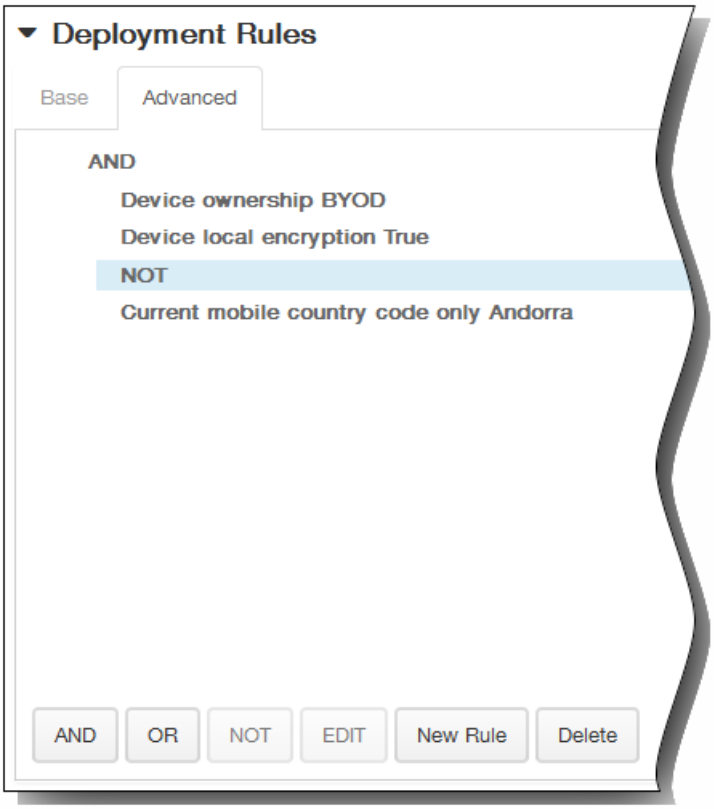
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



Las condiciones que haya elegido aparecerán en la ficha Base.

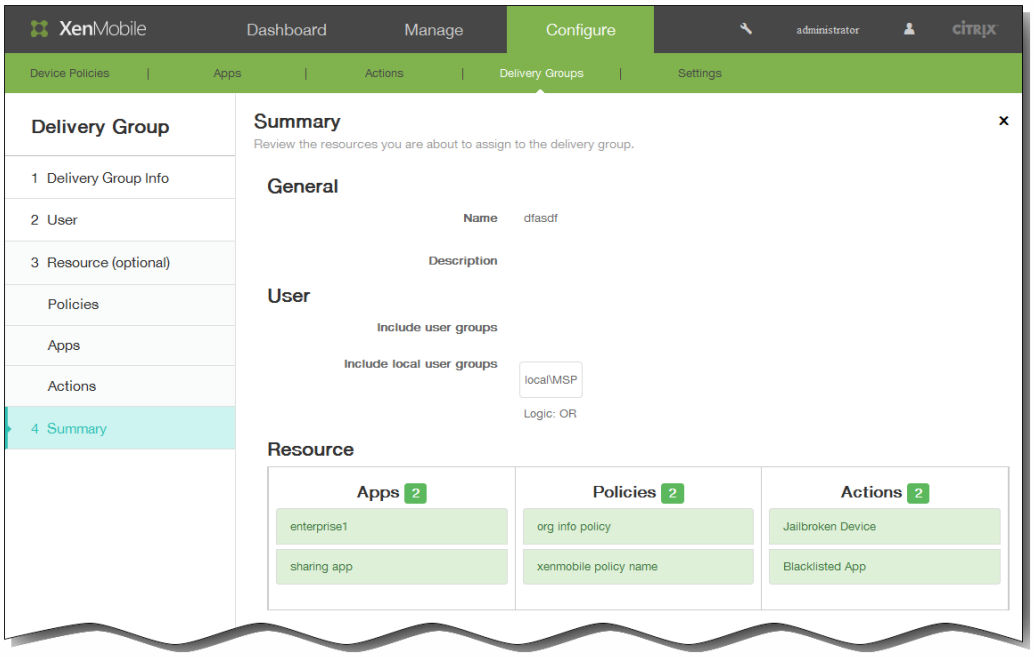
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
    En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.

    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
    En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



7. Haga clic en Siguiente. Aparecerá la página Delivery Group Resources. Desde aquí, puede agregar o eliminar directivas, aplicaciones o acciones. Para omitir este paso, en Delivery Group, haga clic en Summary para ver un resumen de la configuración del grupo de entrega.
Cuando termine de modificar un recurso, haga clic en Next, o bien, en Delivery Group, haga clic en Summary.

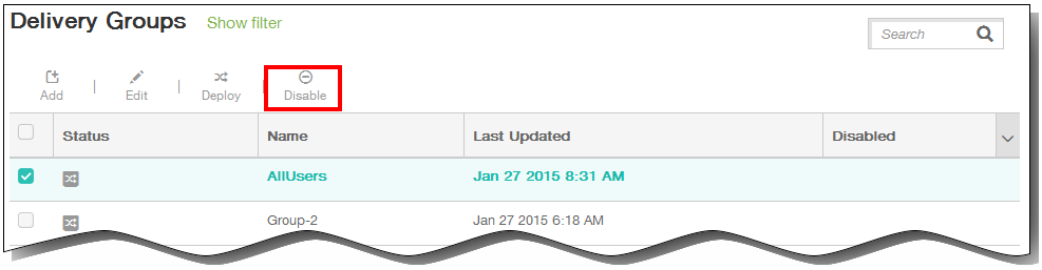
    Aparecerán la página del siguiente recurso o la página Summary.

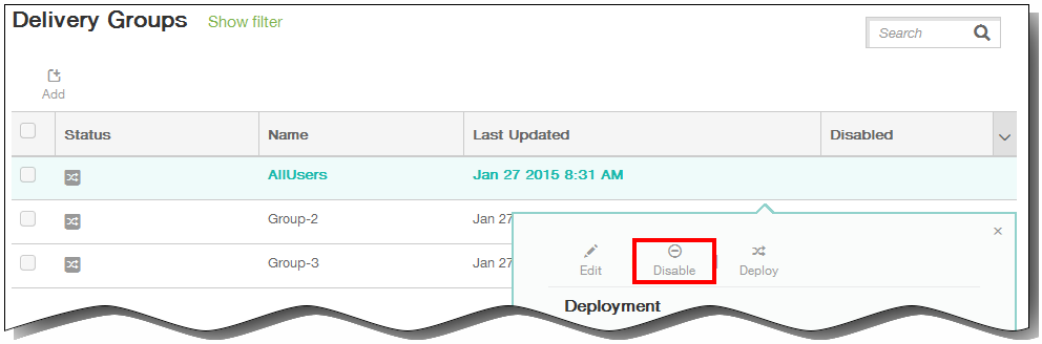


8. En la página Summary, revise los cambios que haya realizado. Haga clic en Back para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.
9. Haga clic en Save para guardar los cambios.

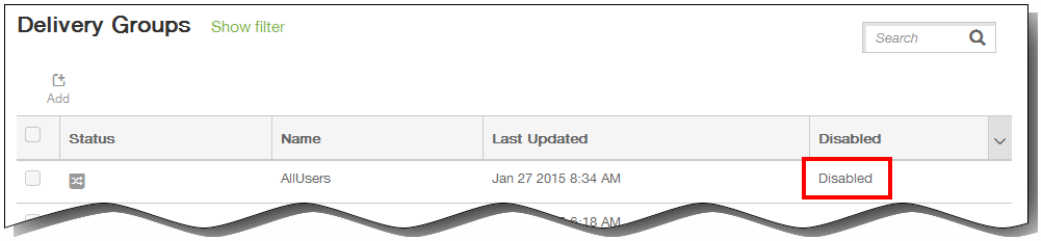
Nota: AllUsers es el único grupo de entrega que puede habilitar o inhabilitar.

1. Desde la página Delivery Groups, seleccione el grupo de entrega AllUsers marcando la casilla junto al nombre AllUsers o haciendo clic en la línea que contiene AllUsers. A continuación, lleve a cabo una de las siguientes acciones:
   Nota: Según cómo haya seleccionado el grupo de entrega AllUsers, los comandos Enable o Disable aparecerán encima o a la derecha del grupo de entrega AllUsers.





- Haga clic en Disable para inhabilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está habilitado (valor predeterminado).
  Una vez inhabilitado, aparecerá bajo el encabezado Disabled en la tabla del grupo de entrega.

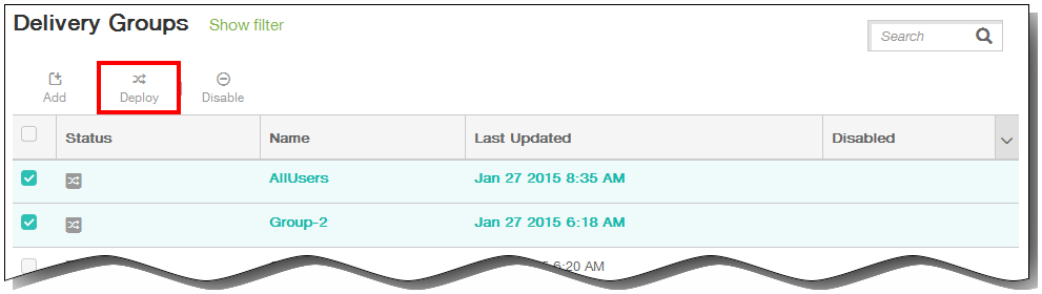


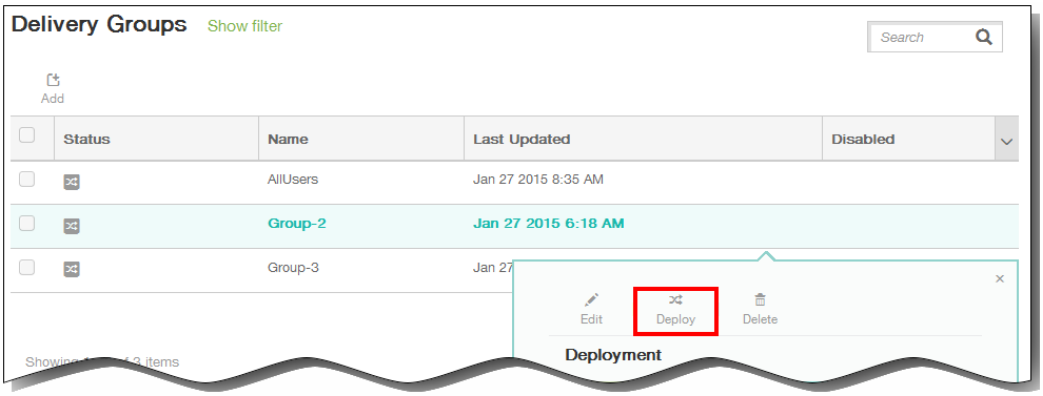
- Haga clic en Enable para habilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está inhabilitado.
  Una vez habilitado, desaparecerá del encabezado Disabled de la tabla del grupo de entrega.

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS y Windows Phone 8.1 y tabletas Windows 8.1 que pertenezcan a ese grupo de entrega para que se vuelvan a conectar a XenMobile con el fin de que se puedan volver a evaluar los dispositivos e implementar en ellos aplicaciones, directivas y acciones. Aquellos usuarios que tengan dispositivos con otras plataformas reciben los recursos de inmediato si ya están conectados o la próxima vez que se conecten, según la directiva de programación definida.

Nota: Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de la instancia de Worx Store presente en los dispositivos Android de los usuarios, primero debe implementar una directiva de inventario de aplicaciones en los dispositivos de los usuarios.

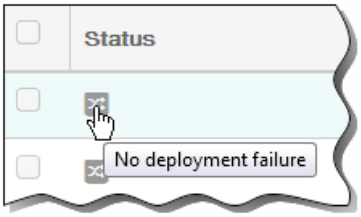
1. En la página Delivery Groups, realice una de las siguientes acciones:
   - Para implementar recursos en más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos en los que quiere realizar la implementación.
   - Para implementar recursos en un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en Deploy.
   Nota: Según cómo seleccione el grupo de entrega, el comando Deploy aparecerá encima o a la derecha del grupo de entrega.



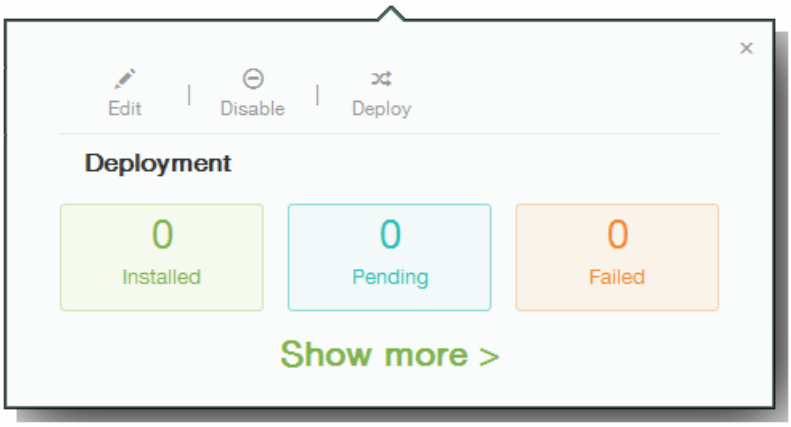


Aparecerá el cuadro de diálogo Deploy Devices.

3. Compruebe que los grupos a los que se van a implementar aplicaciones, directivas y acciones se encuentran en la lista y, a continuación, haga clic en Deploy. Las aplicaciones, las directivas y las acciones se implementan en los grupos seleccionados en función de la plataforma de los dispositivos y de la directiva de programación.
   Puede comprobar el estado de implementación en la página Delivery Groups de una de las siguientes maneras:
   - Mire el icono de implementación, en el encabezado Status del grupo de entrega, el cual indica si hay algún error en la implementación.

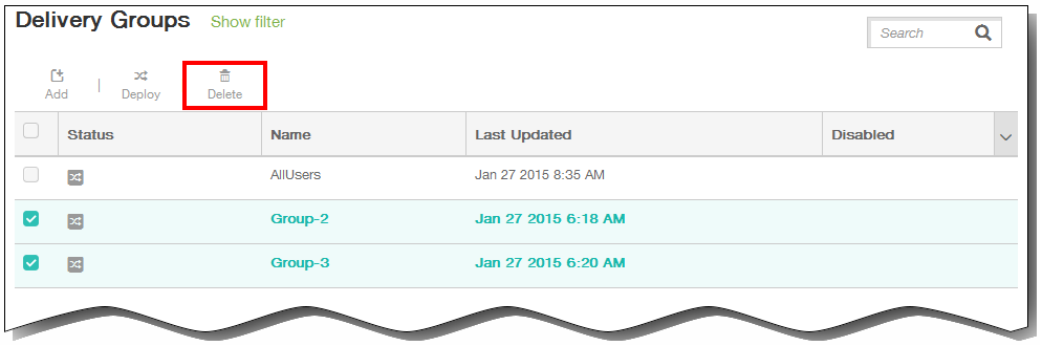


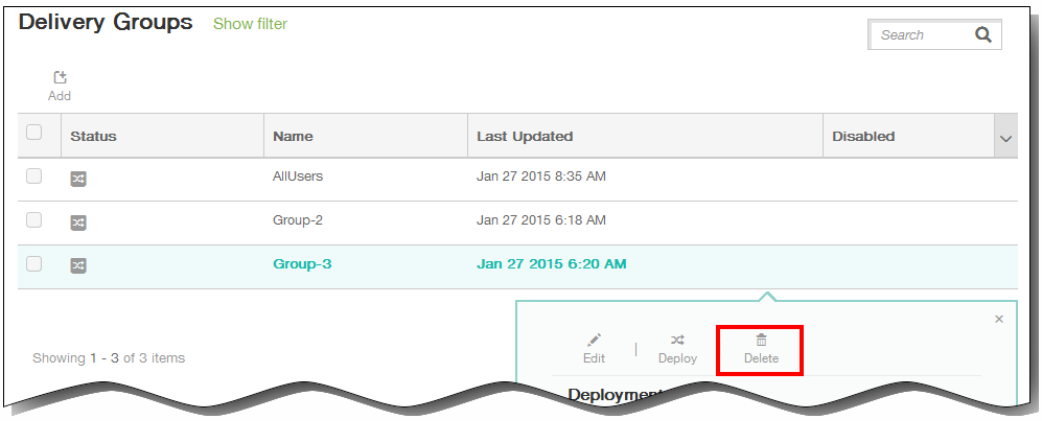
   - Haga clic en la línea que contiene el grupo de entrega para mostrar una superposición que indica las implementaciones instaladas, las pendientes y las erróneas.



Nota: No se puede eliminar el grupo de entrega AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios.

1. En la página Delivery Groups, realice una de las siguientes acciones:
   - Para eliminar más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos que quiere eliminar.
   - Para eliminar un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en Delete.
   Nota: Según cómo seleccione el grupo de entrega, el comando Delete aparecerá encima o a la derecha del grupo de entrega.





   Aparecerá el cuadro de diálogo Delete.
3. Haga clic en Delete en el cuadro de diálogo Delete.
   Importante: Esta acción no se puede deshacer.

Inscripción de usuarios y dispositivos

May 05, 2016

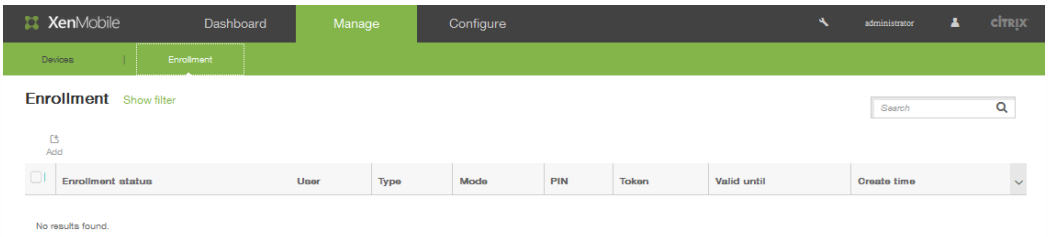
Para poder administrar dispositivos de usuario de forma remota y segura, dichos dispositivos deben estar inscritos en XenMobile. El software cliente de XenMobile debe estar instalado en el dispositivo del usuario, el usuario debe haberse autenticado, y XenMobile y el perfil de usuario deben estar instalados. Después de inscribir los dispositivos, en la consola de XenMobile, puede realizar tareas de administración de dispositivos, como aplicar directivas, implementar aplicaciones, insertar datos en los dispositivos, así como bloquear, borrar y localizar dispositivos perdidos o robados.

Para inscribir usuarios, primero debe agregarlos a XenMobile si aún no ha establecido una conexión de Active Directory. En los temas de esta sección se describen los siguientes pasos necesarios para la inscripción de usuarios:

- Configuración de los modos de inscripción (Predeterminado, SHP).
- Configuración de los servidores de notificaciones (SMTP y SMS).
- Configuración de la plantilla de notificaciones de inscripción.
- Envío de la notificación de inscripción.

Nota: Antes de poder inscribir usuarios de dispositivos iOS, debe solicitar un certificado APN. Para obtener más información, consulte Certificados en XenMobile.

Desde la consola de XenMobile, puede acceder a las opciones de configuración para usuarios y dispositivos. Para ello, haga clic en **Manage > Enrollment**:



Dispositivos Android

May 05, 2016

1. Vaya a Google Play o a la Tienda Apps de Amazon en el dispositivo Android, descargue la aplicación Citrix Worx Home y, a continuación, toque la aplicación.
2. Cuando se le solicite la instalación de la aplicación, haga clic en Siguiente y, a continuación, haga clic en Instalar.
3. Después de que Worx Home se instale, toque Abrir.
4. Introduzca las credenciales de empresa, como el nombre del servidor XenMobile de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico y, a continuación, haga clic en Siguiente.
5. En la pantalla Activate device administrator, toque Activate.
6. Escriba la contraseña de empresa y, a continuación, toque Iniciar sesión.
7. Según la configuración de XenMobile que tenga, es posible que se le solicite la creación de un PIN de Worx. Podrá utilizar este PIN para iniciar sesión en Worx Home o en otras aplicaciones habilitadas para Worx, como WorxMail, WorxWeb, ShareFile. En la pantalla Crear PIN de Worx, escriba un número PIN que consista en cualquier combinación de seis números.
8. Vuelva a escribir el PIN.

Ya se ha inscrito con su dispositivo Android. Toque Worx Store para acceder al almacén de aplicaciones empresariales, así como a las aplicaciones habilitadas para Worx (como WorxMail, WorxWeb y ShareFile, entre otros).

Actualizado: 12-02-2015

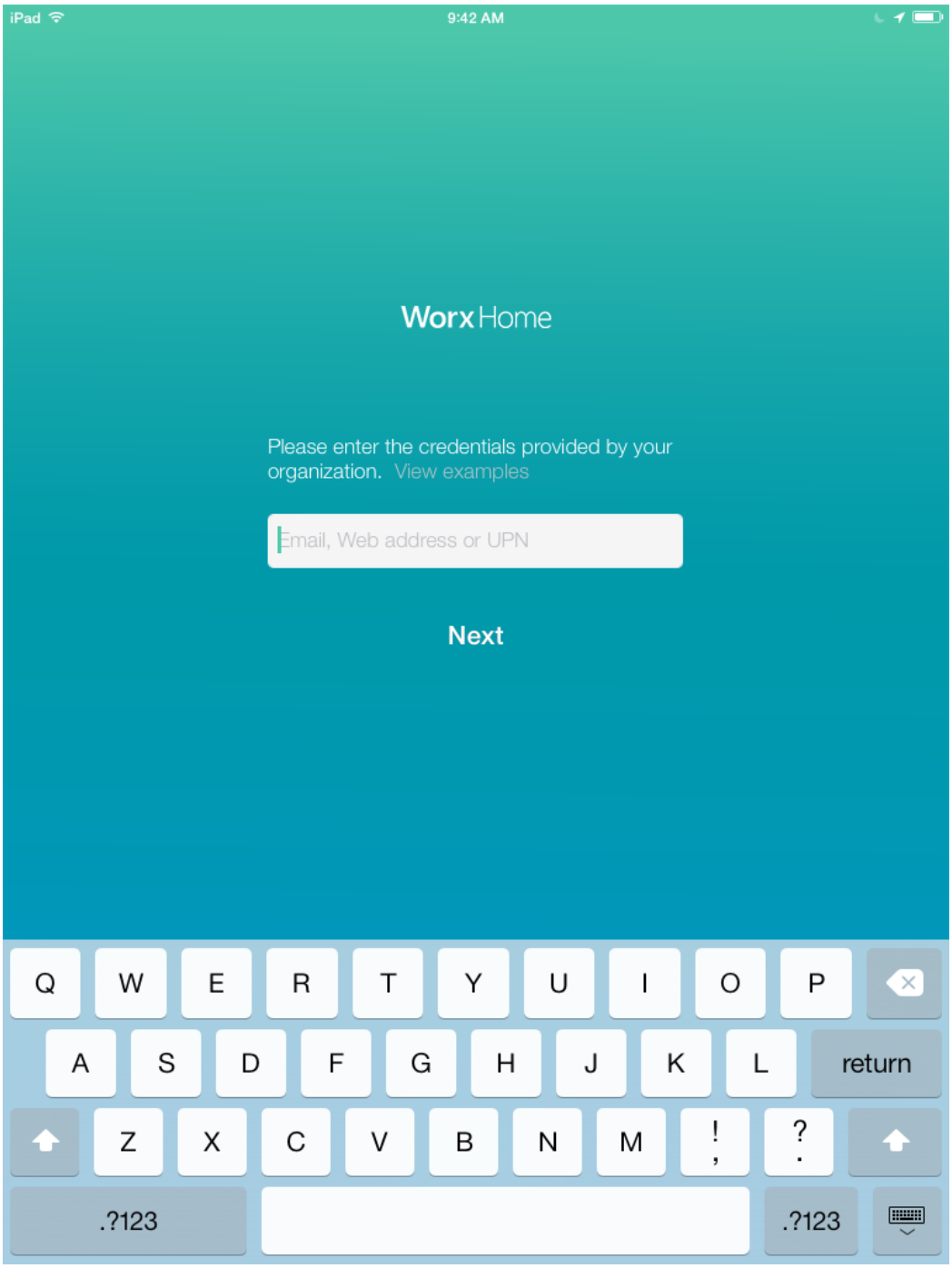
Antes de volver a inscribir un dispositivo, ese dispositivo debe primero debe dejar de estar inscrito. Mientras el dispositivo no esté inscrito y hasta que se vuelva a inscribir, XenMobile no lo administrará aunque dicho dispositivo siga apareciendo en la lista de inventario de dispositivos en la consola de XenMobile. No se puede realizar el seguimiento de un dispositivo ni supervisar su estado de cumplimiento si XenMobile no lo administra.

1. Toque la aplicación Worx Home para abrirla.
2. Toque el icono Parámetros en la parte superior izquierda de la ventana de la aplicación.
3. Toque Reinscribir. Aparecerá un mensaje para confirmar que quiere volver a inscribir el dispositivo.
4. Toque Aceptar. Esta acción tiene como consecuencia la desinscripción de su dispositivo.
5. Siga las instrucciones que aparecen en pantalla para volver a inscribir su dispositivo.

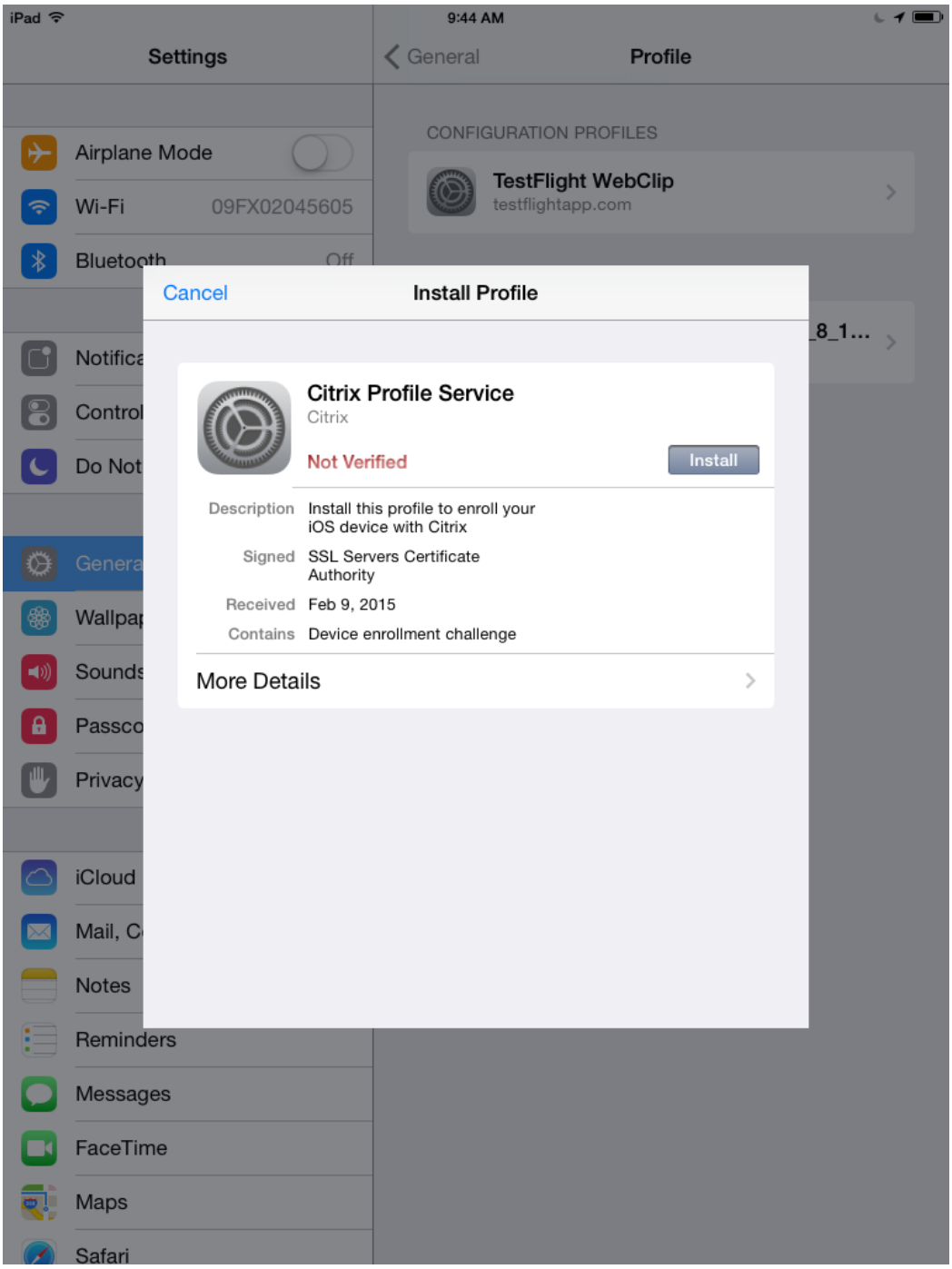
Dispositivos iOS

May 05, 2016

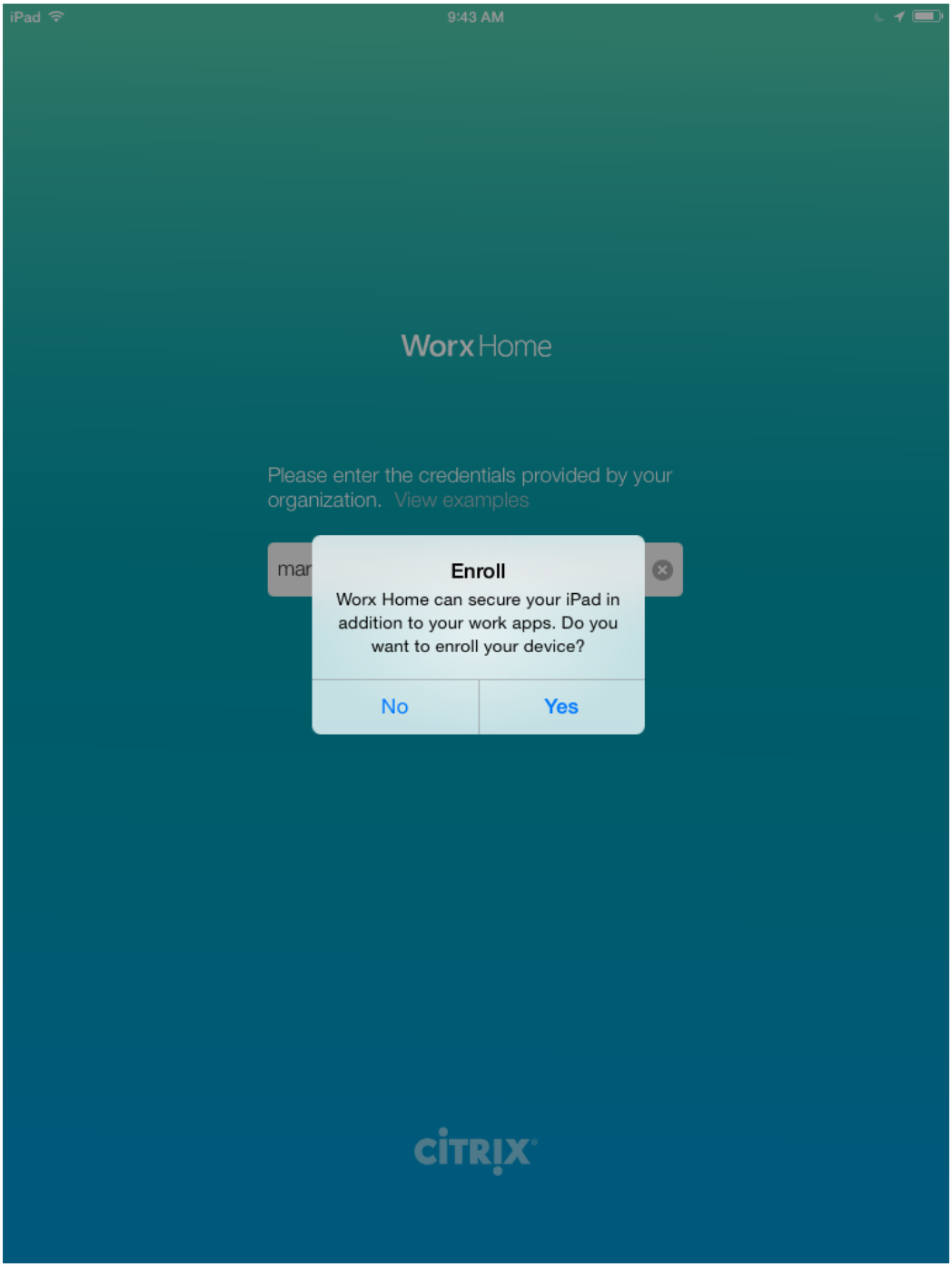
1. Descargue la aplicación Worx Home desde el App Store de Apple, iTunes, al dispositivo y, a continuación, instale la aplicación en el dispositivo.
2. En la pantalla de inicio del dispositivo iOS, toque la aplicación Worx Home.
3. Cuando se inicie la aplicación Worx Home, introduzca las credenciales de empresa, como el nombre del servidor XenMobile de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico; a continuación, haga clic en Siguiente.



4. Introduzca su nombre de usuario y contraseña. Se abre un explorador para comenzar el proceso de inscripción.
5. Toque Instalar para instalar el servicio de perfiles de Citrix.



6. Si se muestra un mensaje de advertencia, toque Instalar ahora.
7. Si el dispositivo está configurado con un código de acceso, se le pedirá que escriba el código de acceso para instalar el perfil.
8. Toque Instalar.
9. Cuando finalice la instalación del perfil, toque Listo para completar el proceso de instalación del perfil de la empresa.
10. Cuando aparezca Worx Home, toque Sí para permitir que Worx Home use la ubicación actual.

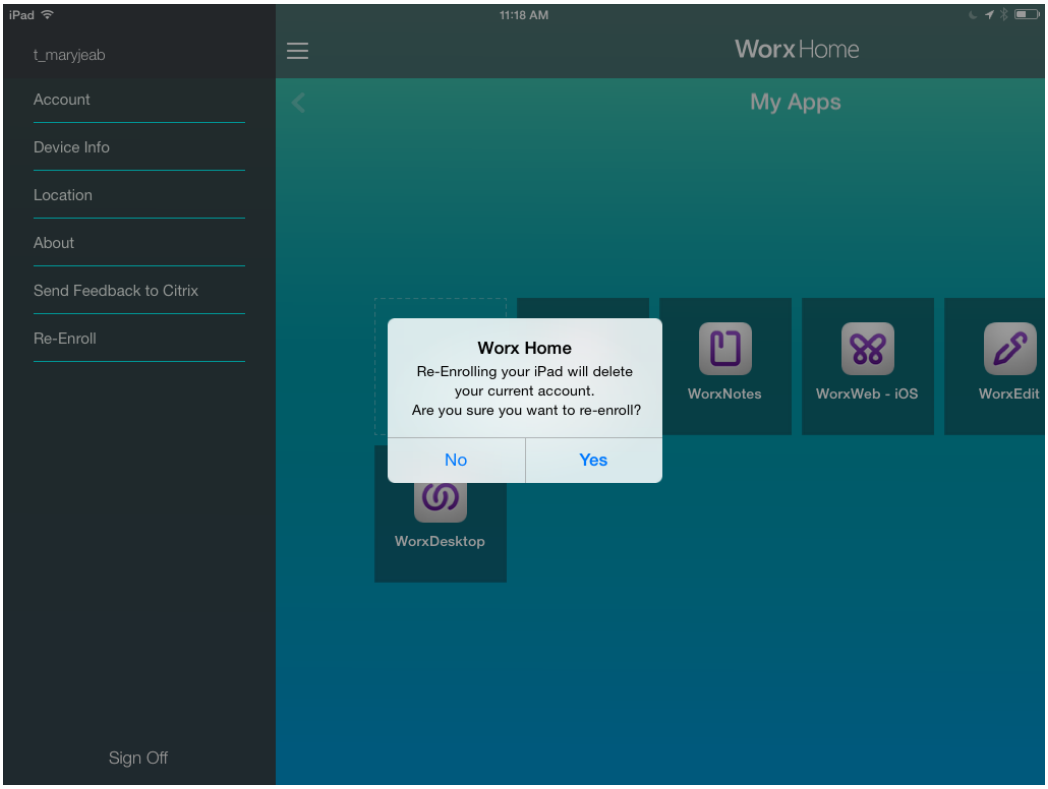


11. Según la configuración de XenMobile que tenga, es posible que se le solicite la creación de un PIN de Worx. Podrá utilizar este PIN para iniciar sesión en Worx Home o en otras aplicaciones habilitadas para Worx, como WorxMail, WorxWeb, ShareFile. Deberá introducir su PIN de Worx dos veces. Worx Home se abre. Ahora, puede acceder a Worx Store para ver las aplicaciones que puede instalar en el dispositivo iOS.
12. Toque Worx Store para abrir el almacén de aplicaciones de empresa.
13. Si ha configurado XenMobile de manera que las aplicaciones aparezcan automáticamente en los dispositivos de los usuarios después de la inscripción, aparecen mensajes con solicitudes de instalación de las aplicaciones. Toque Instalar para instalar las aplicaciones.

Actualizado: 13-02-2015

Antes de volver a inscribir un dispositivo, ese dispositivo debe primero debe dejar de estar inscrito. Mientras el dispositivo no esté inscrito y hasta que se vuelva a inscribir, XenMobile no lo administrará aunque dicho dispositivo siga apareciendo en la lista de inventario de dispositivos en la consola de XenMobile. No se puede realizar el seguimiento de un dispositivo ni supervisar su estado de cumplimiento si XenMobile no lo administra.

1. Toque la aplicación Worx Home para abrirla.
2. Toque el icono Settings en la parte superior izquierda de la ventana de la aplicación.
3. Toque Re-enroll. Aparecerá un mensaje para confirmar que quiere volver a inscribir el dispositivo.



4. Toque Yes. Esta acción tiene como consecuencia la desinscripción del dispositivo.
5. Siga las instrucciones que aparecen en pantalla para volver a inscribir el dispositivo.

Inscripción de dispositivos Windows en XenMobile

May 05, 2016

XenMobile respalda la inscripción de dispositivos que funcionen con los siguientes sistemas operativos Windows:

- Windows
- Windows Phone

Los usuarios de Windows y Windows Phone se inscriben directamente a través de sus dispositivos.

Debe configurar la detección automática para la inscripción de usuarios con el fin de permitir la administración de dispositivos Windows y Windows Phone.

> ## Nota
>
> Para que los dispositivos Windows se puedan inscribir, el certificado SSL de escucha debe ser un certificado público. La inscripción falla si se ha cargado un certificado SSL autofirmado

Los usuarios pueden inscribir dispositivos que ejecutan Windows RT 8.1, así como versiones de 32 y 64 bits de Windows 8.1 Pro y Windows 8.1 Enterprise. Para habilitar la administración de dispositivos Windows 8.1, Citrix recomienda configurar la detección automática. Para obtener más información, consulte Para activar la detección automática en XenMobile para la inscripción de usuarios.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows. Este paso es particularmente importante cuando se actualiza desde Windows 8 a Windows 8.1, porque es posible que no se notifique automáticamente a los usuarios de todas las actualizaciones disponibles.
2. En el menú de accesos, toque Configuración y, a continuación, toque Configuración de PC > Red > Área de trabajo.
3. Escriba la dirección de correo electrónico de empresa y luego toque Activar. Para inscribirse como un usuario local, introduzca una dirección de correo electrónico que no exista y un nombre de dominio correcto (por ejemplo, foo@midominio.com). Esto permite omitir una restricción conocida de Microsoft; en el cuadro de diálogo Conectando con un servicio, escriba el nombre de usuario y la contraseña asociados al usuario local. El dispositivo detecta automáticamente el servidor XenMobile y se inicia el proceso de inscripción.
4. Introduzca la contraseña. Utilice la contraseña asociada a una cuenta que forme parte de un grupo de usuarios en XenMobile.
5. En el cuadro de diálogo Permitir aplicaciones y servicios del administrador de TI, indique que acepta que el dispositivo sea administrado y, a continuación, toque Activar.

Puede inscribir dispositivos Windows 8.1 sin detección automática. Sin embargo, Citrix recomienda configurar la detección automática. Debido a que la inscripción sin la detección automática consiste en una llamada al puerto 80 antes de conectarse a la URL pertinente, no se aconseja para una implementación de producción. Citrix recomienda utilizar este proceso solo en entornos de prueba y en el contexto de una implementación de prueba de concepto.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows. Este paso es particularmente

importante cuando se actualiza desde Windows 8 a Windows 8.1, porque es posible que no se notifique automáticamente a los usuarios de todas las actualizaciones disponibles.
2. En el menú de accesos, toque Configuración y, a continuación, toque Configuración de PC > Red > Área de trabajo.
3. Introduzca la dirección de correo electrónico de empresa.
4. Si la opción Detectar la dirección del servidor automáticamente está activada, tóquela para desactivarla.
5. En el campo Enter server address, escriba la dirección del servidor en el siguiente formato: https://*serverfqdn:8443/serverInstance*/Discovery.svc. Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice en esta dirección ese número de puerto en lugar de 8443.
6. Introduzca la contraseña.
7. En el cuadro de diálogo Permitir aplicaciones y servicios del administrador de TI, indique que acepta que el dispositivo sea administrado y, a continuación, toque Activar.

Actualizado: 11-02-2015

Para inscribir dispositivos Windows Phone 8.1 en XenMobile, los usuarios necesitan su dirección de correo electrónico y su contraseña de Active Directory o de la red interna. Si la detección automática no está configurada, los usuarios también necesitan la dirección Web del servidor XenMobile. A continuación, deben seguir este procedimiento en sus dispositivos para inscribirse.

Nota: Para implementar aplicaciones mediante la tienda Windows Phone de la empresa, antes de que se inscriban los usuarios, compruebe que ha configurado la directiva Enterprise Hub (con una aplicación firmada de Citrix Worx Home para Windows Phone 8.x).

1. En la pantalla principal del teléfono Windows Phone 8.1, toque el icono Configuración.
2. Toque Mi empresa.
3. En la pantalla Mi empresa, toque Agregar cuenta.
4. En la pantalla siguiente, introduzca una dirección de correo electrónico y una contraseña y, a continuación, toque iniciar sesión. Si se ha configurado la detección automática para el dominio, la información solicitada en los siguientes pasos se completa automáticamente. Vaya al paso 8. En cambio, si no se ha configurado la detección automática para el dominio, continúe al paso siguiente. Para inscribirse como un usuario local, introduzca una dirección de correo electrónico que no exista y un nombre de dominio correcto (por ejemplo, foo@midominio.com). Esto permite omitir una restricción conocida de Microsoft; en el cuadro de diálogo Conectando con un servicio, escriba el nombre de usuario y la contraseña asociados al usuario local.
5. En la pantalla siguiente, introduzca la dirección Web del servidor XenMobile, como: https://://wpe. Por ejemplo: https://miempresa.mdm.com:8443/zdm/wpe. **Nota:** Debe adaptar el número de puerto a la implementación, pero debe ser el mismo puerto que se ha usado para la inscripción de iOS.
6. Introduzca el nombre de usuario y el dominio si la autenticación se valida mediante un nombre de usuario y un dominio. A continuación, toque Iniciar sesión.
7. Si aparece una pantalla informando sobre un problema con el certificado, el error se debe al uso de un certificado autofirmado. Si el servidor es de confianza, toque Continuar. De lo contrario, toque Cancelar.
8. Una vez agregada la cuenta, tiene la opción de seleccionar Instalar aplicación de empresa. Si el administrador ha configurado un almacén de aplicaciones de la empresa, seleccione esta opción y, a continuación, toque Listo. Si desactiva esta opción, para poder recibir el almacén de aplicaciones de la empresa, deberá volver a inscribirse.
9. En la pantalla Cuenta agregada, toque Listo.
10. Para forzar la conexión con el servidor, toque el icono de actualización. Si el dispositivo no se conecta manualmente al servidor, XenMobile intenta reconectarse. XenMobile se conecta al dispositivo cada 3 minutos 5 veces sucesivas; después, se conecta cada 2 horas. Puede modificar este intervalo de conexión en Intervalo de latidos del servicio WNS, ubicado en

Propiedades del servidor. Una vez finalizada la inscripción, Worx Home se inscribe en segundo plano. No aparece ningún indicador tras completarse la instalación. Abra Worx Home desde la pantalla Todas las aplicaciones.

Dispositivos Symbian

May 05, 2016

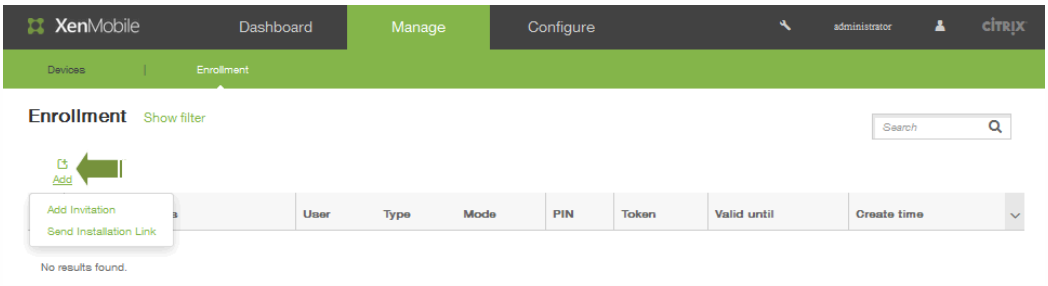
1. Vaya a la dirección Web de XenMobile correspondiente a su empresa. La dirección Web tiene el siguiente formato: https://.dominio.com//setup
   Nota: Puede usar el prefijo HTTPS solo si dispone de un certificado emitido por una entidad de confianza, como VeriSign o Thawte.
2. En la pantalla Install, toque OK.
3. Toque la opción Phone Memory para que sea la ubicación donde se instalará el agente de XenMobile.
4. Cuando se complete la instalación, toque Yes para abrir XenMobile.
5. En la pantalla Security Details, toque OK para permitir que XenMobile acceda al teléfono.
6. Escriba los primeros cuatro números del código de servidor, como 2831, y luego toque OK.
7. En la pantalla Control Request Accepted, toque OK.
8. Escriba el nombre de usuario y la contraseña, el nombre de servidor, el puerto y el nombre de instancia para el servidor XenMobile y luego toque OK. Aparece la información de conexión.
9. Toque Options para revisar los datos de conexión de servidor y, a continuación, toque Close para finalizar la instalación.

Envío de una invitación de inscripción en XenMobile

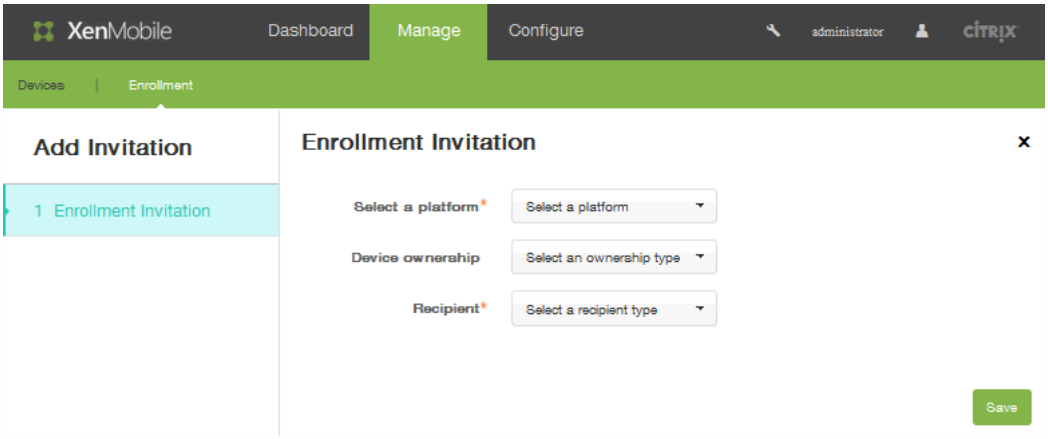
May 05, 2016

Desde la consola de XenMobile, puede enviar a los usuarios una invitación para la inscripción de dispositivos iOS y Android.

1. En la consola de XenMobile, haga clic en Manage > Enrollment.
2. En la pantalla Enrollment, haga clic en Add. Aparecerá un menú con las opciones para agregar una invitación o enviar un enlace de instalación.

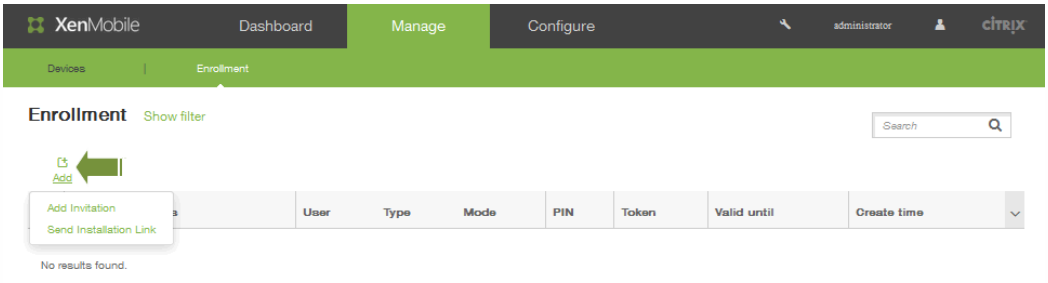


3. Haga clic en Add Invitation. Aparecerá la pantalla Enrollment Invitation.

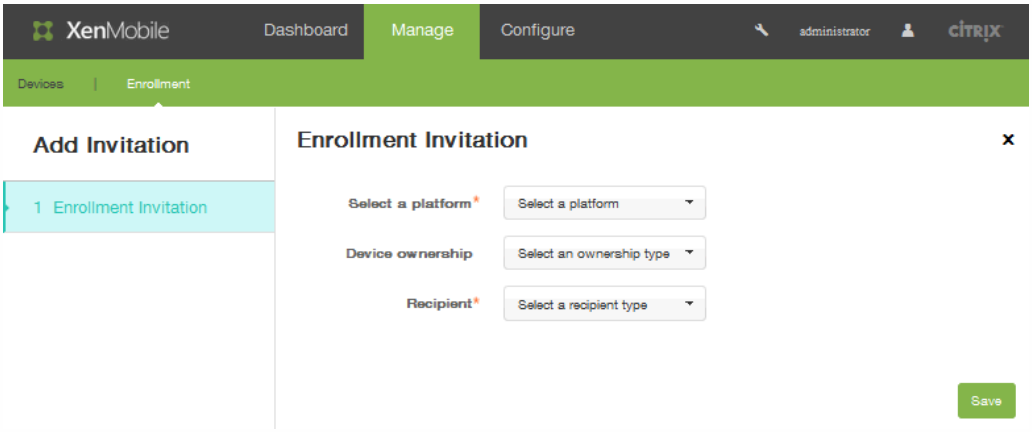


4. En la lista Select a platform, haga clic en iOS o Android.
5. En la lista Device ownership, haga clic en Corporate o Employee.
6. En la lista Recipient, haga clic en User o Group. Cuando se selecciona un usuario como destinatario, la interfaz cambia para mostrar opciones de configuración adicionales. Siga los pasos que se describen en estos apartados para completar la configuración de las invitaciones en función del tipo de destinatario que seleccione:

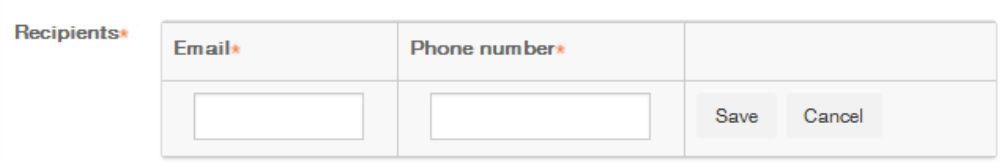
1. En la consola de XenMobile, haga clic en Manage > Enrollment.
2. En la pantalla Enrollment, haga clic en Add. Aparecerá un menú en el que puede elegir si agregar una invitación o enviar un enlace de instalación.



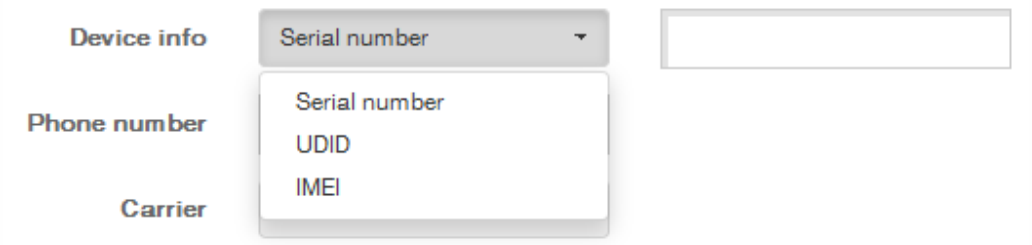
3. Haga clic en Add Invitation. Aparecerá la pantalla Enrollment Invitation.



4. En la lista Select a platform, haga clic en iOS o Android.
5. En la lista Device ownership, haga clic en Corporate o Employee.
6. En la lista Recipient, haga clic en User. La interfaz cambia para mostrar las opciones de configuración relacionadas con la inscripción de usuarios.



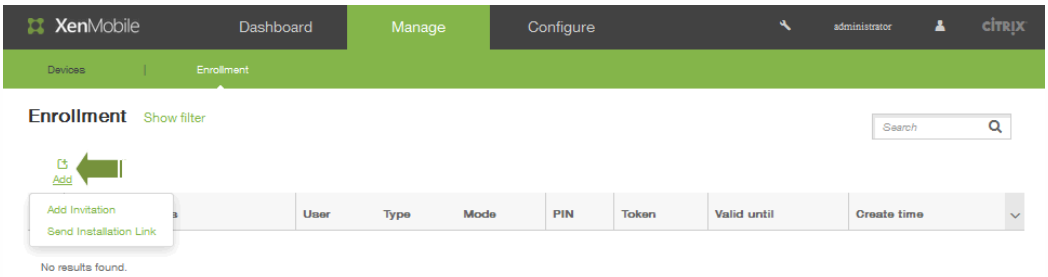
7. En User name, escriba un nombre de usuario. Este usuario debe existir en el servidor XenMobile como usuario local, o bien como usuario en Active Directory. Si el usuario es local, compruebe que la propiedad de correo electrónico del usuario está configurada para enviar notificaciones. Si se trata de un usuario de Active Directory, compruebe que el protocolo LDAP está configurado.
8. En la lista Device info, seleccione Serial number, UDID o IMEI. Después de elegir una opción, la interfaz cambia para mostrar un campo en el que puede introducir el valor correspondiente del dispositivo:



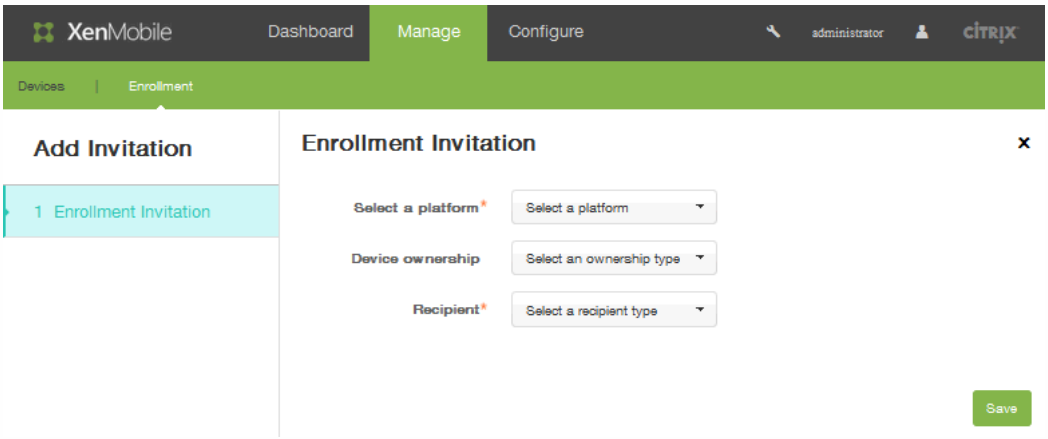
9. En Phone number, de forma optativa, puede introducir el número de teléfono del usuario.

10. En la lista Carrier, seleccione un operador al que asociar el número de teléfono del usuario.
11. En la lista Enrollment mode, seleccione User name + Password (esta es la selección predeterminada), High Security, Invitation URL, Invitation URL + PIN, Invitation URL + Password Two Factor o User name + PIN.
12. En la lista Template for agent download, las posibilidades para esta opción varían en función del tipo de plataforma. Por ejemplo, aparece iOS Download Link como opción si ha seleccionado iOS como plataforma en el paso 1.
13. En la lista Template for enrollment URL, haga clic en Enrollment Invitation.
14. En la lista Template for enrollment confirmation, haga clic en Enrollment Confirmation. La invitación a la inscripción caduca tras un período de tiempo determinado. El campo Expire after indica cuándo caduca la inscripción. El campo Maximum Attempts muestra la cantidad máxima de veces que tiene lugar el proceso de inscripción.
15. En Send invitation, haga clic en ON.
16. Haga clic en Guardar.

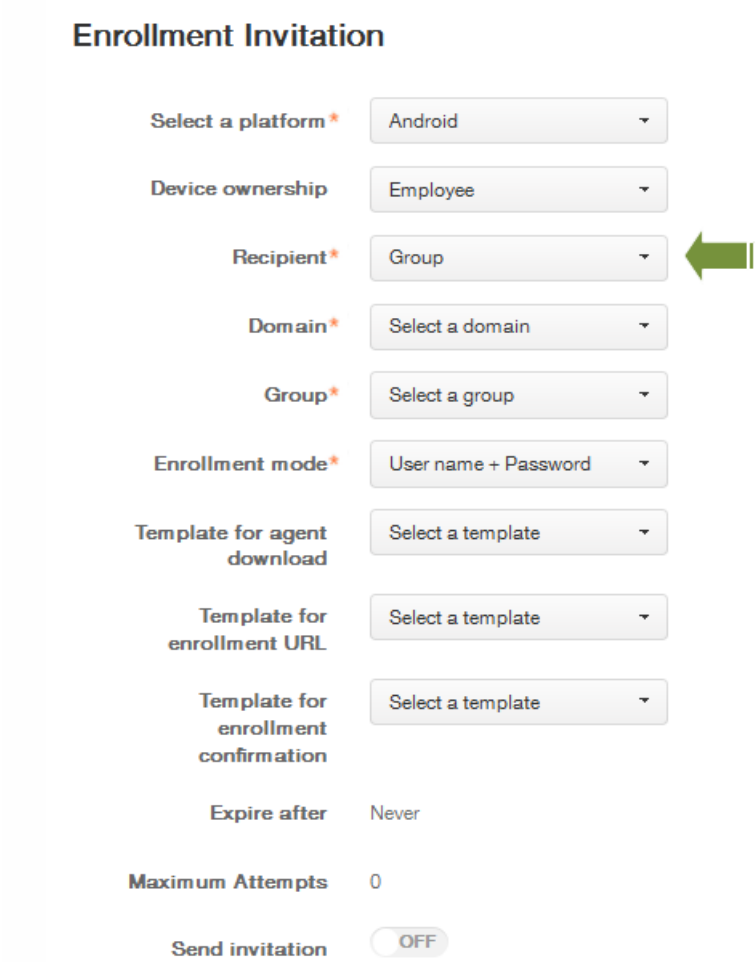
1. En la consola de XenMobile, haga clic en Manage > Enrollment.
2. En la pantalla Enrollment, haga clic en Add. Aparecerá un menú en el que puede elegir si agregar una invitación o enviar un enlace de instalación.



3. Haga clic en Add Invitation. Aparecerá la pantalla Enrollment Invitation.



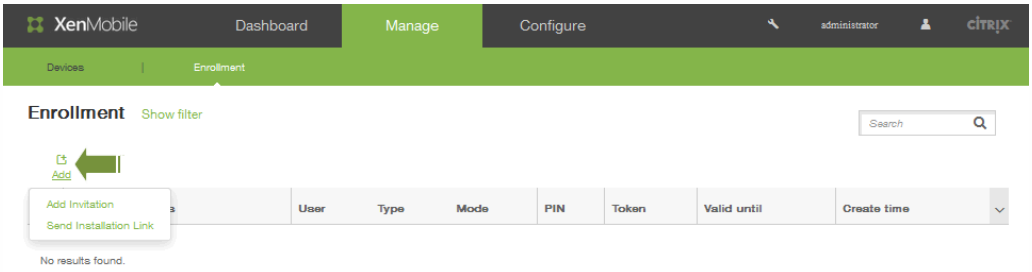
4. En la lista Select a platform, seleccione iOS o Android.
5. En la lista Device ownership, seleccione Corporate o Employee.
6. En la lista Recipient, seleccione Group. La interfaz cambia para mostrar las opciones de configuración de la inscripción de grupos:



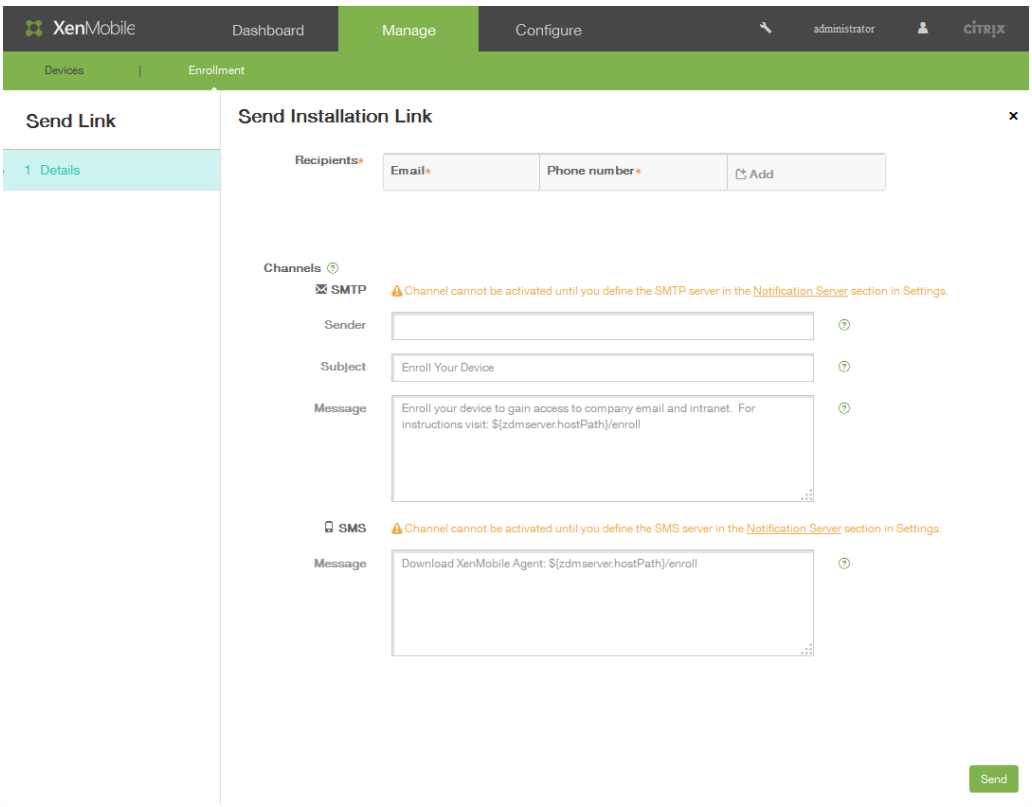
7. En Domain, seleccione el dominio en el que reside el grupo de destinatarios.
8. En Group, seleccione el grupo al que enviar una notificación de inscripción.
9. En Enrollment mode, seleccione User name + Password (esta es la selección predeterminada), High Security, Invitation URL + PIN, Invitation URL + Password, Two Factor o User name + PIN.
10. En la lista Template for agent download, las posibilidades para esta opción varían en función del tipo de plataforma. Por ejemplo, iOS Download Link aparece como opción si ha seleccionado iOS en el paso 1.
11. En la lista Template for enrollment URL, seleccione Enrollment Invitation.
12. En la lista Template for enrollment confirmation, seleccione Enrollment Invitation. La invitación a la inscripción caduca tras un período de tiempo determinado. El campo Expire after indica cuándo caduca la inscripción. El campo Maximum Attempts muestra la cantidad máxima de veces que tiene lugar el proceso de inscripción.
13. En Send invitation, haga clic en ON para enviar la invitación de inscripción al grupo seleccionado.
14. Haga clic en Guardar.

Antes de enviar un enlace de instalación para la inscripción, deberá configurar canales (SMTP o SMS) en el servidor de notificaciones: Configure > Settings > Notification Server. Para obtener más información, consulte Notificaciones en XenMobile.

1. En la consola de XenMobile, haga clic en Manage > Enrollment.
2. En la pantalla Enrollment, haga clic en Add. Aparecerá un menú en el que puede elegir si agregar una invitación o enviar enlaces de instalación.



3. Haga clic en Send Installation Link. La interfaz cambia para mostrar las opciones de Send Installation Link.



4. En Recipient, haga clic en Add para identificar un destinatario al que enviar un enlace de instalación para la inscripción. El campo Recipient se expande para permitirle agregar una dirección de correo electrónico y un número de teléfono.

5. Introduzca una dirección de correo electrónico en Email address y un número de teléfono en Phone number para el usuario que recibirá el enlace de invitación a la inscripción. Estos campos son obligatorios.
6. En Channels, seleccione el canal que se va a usar para enviar el enlace de instalación para la inscripción. Las notificaciones se envían a través de SMTP o SMS. **Nota:** Estos canales (SMTP o SMS) no se pueden activar hasta que configure los parámetros de servidor en Configure > Settings > Notification Server. Para obtener más información, consulte Notificaciones en XenMobile.
7. Si configura el campo SMTP, especifique el remitente en Sender. Este campo es opcional, y se usa en el campo de

formulario de un mensaje SMTP. Si no se especifica un remitente aquí, se utiliza el valor especificado en el campo Settings > Notification Server.

8. Para las notificaciones SMTP, si quiere, puede incluir el asunto en Subject. Por ejemplo, "inscriba su dispositivo".
9. Proporcione un mensaje en Message, que será el contenido del mensaje que se enviará al destinatario. Por ejemplo, "Inscriba su dispositivo para acceder a la intranet y al correo electrónico de la empresa".
10. Para enviar notificaciones por SMS, escriba un mensaje que se enviará al destinatario. Este campo es obligatorio para las notificaciones por SMS. **Nota:** En Norteamérica, los mensajes SMS que superen los 160 caracteres se entregan en varios mensajes.
11. Haga clic en Send.

> ## Nota
>
> Si su entorno hace uso de los nombres SAMAccountName, después de que los usuarios reciben la invitación y hacen clic en el enlace, deben modificar el nombre de usuario para completar la autenticación. Por ejemplo, tienen que quitar la parte del *nombre de dominio* de SAMAccountName@*nombre de dominio*.com.

Configuración de reglas de implementación

Oct 31, 2016

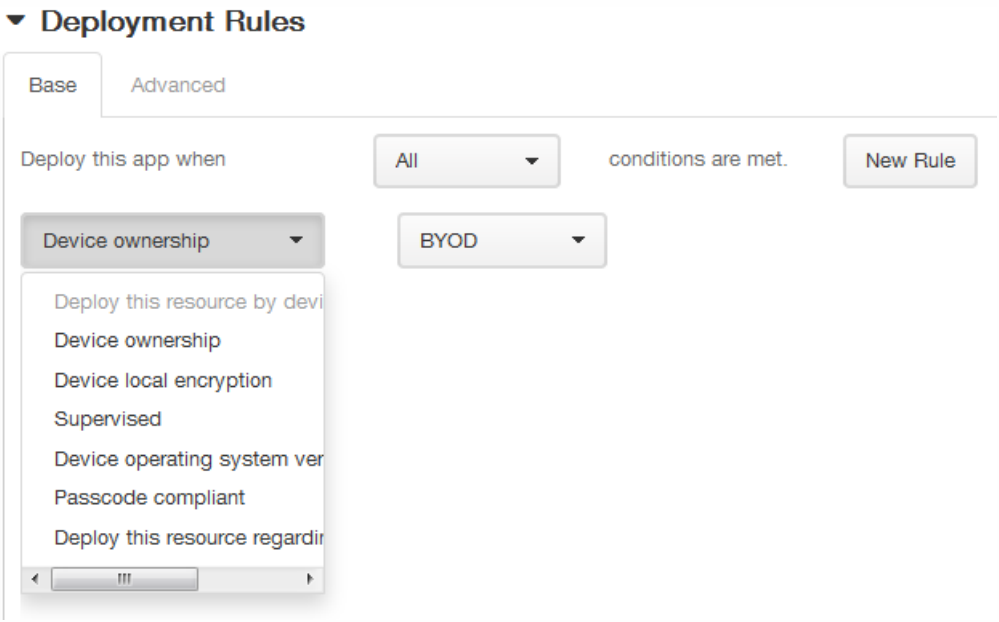
Esta sección describe:

- Reglas de implementación: parámetros que afectan al resultado de la implementación de un paquete.
- Programaciones de implementación: opciones que especifican cuando envía XenMobile los paquetes a un dispositivo.

Configuración de reglas de implementación

Puede establecer cuantos parámetros quiera de los que influirán sobre los resultados de implementación de un paquete.

Por ejemplo, el paquete de implementación puede basarse en una versión específica de sistema operativo o en una plataforma de hardware concreta, entre otros. Este asistente contiene tanto un editor de reglas básicas (Base Rule Editor) como uno de reglas avanzadas (Advanced Rule Editor). La vista Advanced es un editor de forma libre. En la siguiente imagen se muestra la pantalla Deployment Rules, accesible al agregar o modificar una aplicación:



Reglas básicas de implementación

Las reglas básicas de implementación se componen de pruebas predefinidas y acciones resultantes. Cuando es posible, los resultados se generan previamente en pruebas de ejemplo. Por ejemplo, cuando un paquete de implementación se basa en una plataforma de hardware, todas las plataformas conocidas existentes se incluyen en la prueba resultante, con lo que se reduce considerablemente el tiempo de creación de la regla y se limitan posibles errores.

Haga clic en **New rule** para agregar una regla al paquete.

Nota: El generador de reglas incluye información adicional, específica para cada prueba.

Para crear una nueva regla, seleccione una plantilla de reglas, seleccione el tipo de condición, y personalice la regla. Personalizar la regla implica modificar la descripción. Cuando haya terminado de configurar los parámetros, podrá agregar la

regla al paquete.

Puede agregar cuantas reglas quiera. El paquete se implementa cuando todas las reglas coinciden.

Reglas avanzadas de implementación

Si hace clic en la ficha **Advanced**, aparecerá el editor **Advanced Rule Editor**.

En este modo, puede especificar la relación entre las reglas. Los operadores **AND**, **OR** y **NOT** están disponibles.

Configuración de programaciones de implementación

XenMobile utiliza la programación de implementación que usted especifique para acciones, aplicaciones y directivas de dispositivo con el fin de controlar la implementación de esos elementos. Puede especificar que una implementación se aplique inmediatamente, o en una determinada fecha y hora, o de acuerdo con las condiciones de implementación. La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always-on connections**, que no se aplicará para iOS.

Si no cambia las opciones de programación de la implementación, la implementación tiene lugar inmediatamente en cada conexión. Las opciones de programación de implementaciones son:

Deploy. La opción predeterminada es **ON**. Para impedir la implementación, establezca esta opción en **OFF**.

Deployment Schedule. La opción predeterminada es **Now**. Para especificar el momento de la implementación, seleccione **Later** y, a continuación, elija una fecha y una hora.

Deployment condition. La opción predeterminada es **On every connection**. Para limitar las implementaciones, cambie esta opción a **Only when previous deployment has failed**.

Deploy for always-on connections. La opción predeterminada es **OFF**. Para dispositivos iOS y Windows Mobile: Si establece la opción **Connection Scheduling Policy** en **Always**, debe cambiar **Deploy for always-on connections** a **ON**. Para dispositivos Android: La propiedad del servidor XenMobile **Background Deployment** requiere que establezca **Deploy for always-on connections** en **ON** para cada directiva implementada en dispositivos Android.

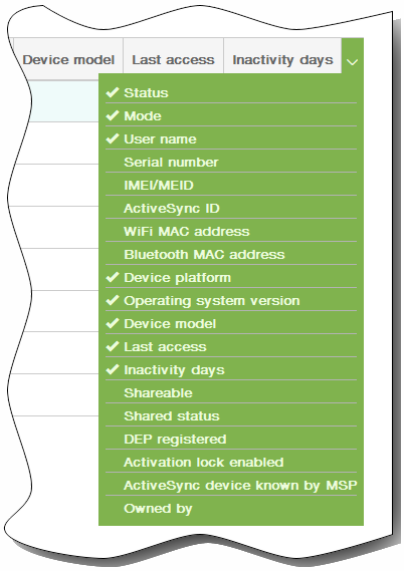
Cómo agregar dispositivos y ver información de los mismos

May 05, 2016

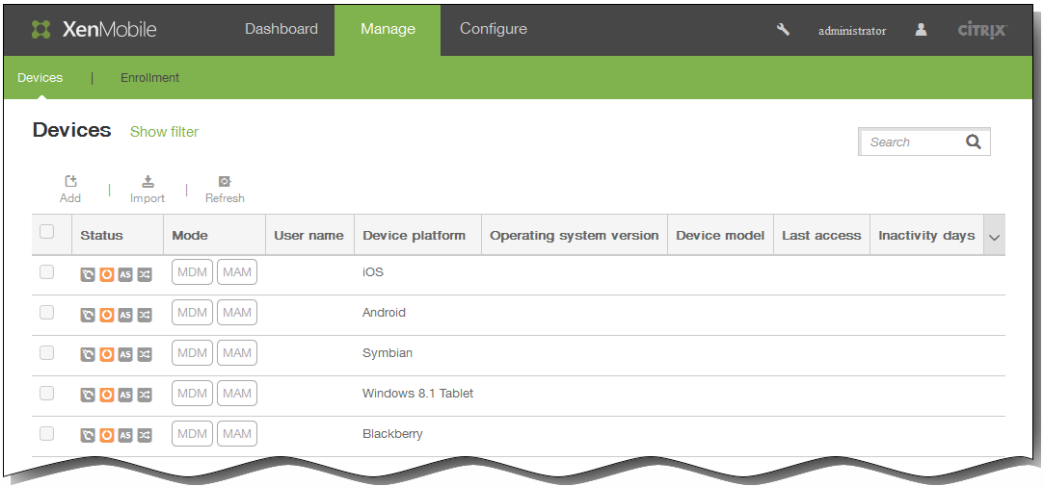
La base de datos del repositorio relacionado con el servidor de la consola de XenMobile almacena una lista de dispositivos móviles. Cada dispositivo móvil está definido por un número de serie exclusivo y/o una identificación International Mobile Station Equipment Identity (IMEI) o Mobile Equipment Identifier (MEID). Para rellenar la consola de XenMobile con los datos de los dispositivos, puede agregar los dispositivos de forma manual o importar una lista de dispositivos desde un archivo. Consulte Formatos del archivo de aprovisionamiento de dispositivos

En la página Devices de la consola, encontrará una tabla con cada uno de los dispositivos junto con la información siguiente: el estado (dispositivo no liberado por jailbreak, dispositivo no administrado, Active Sync Gateway no disponible, sin errores de implementación), el modo (MDM, MAM), el nombre de usuario, la plataforma del dispositivo, la versión del sistema operativo, el modelo del dispositivo, la fecha del último acceso y los días de inactividad.

Nota: Los encabezados mencionados son los predeterminados. Puede personalizar lo que aparece en la tabla. Para ello, haga clic en la flecha hacia abajo del último encabezado y, a continuación, haga clic en los encabezados que quiera mostrar o elimine los que no.

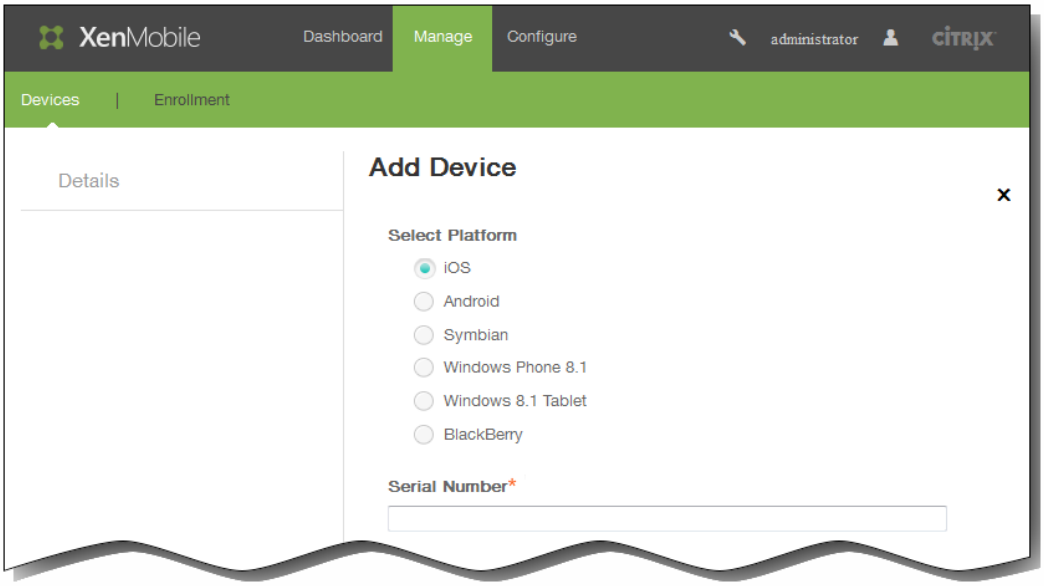


Puede agregar un nuevo dispositivo manualmente si hace clic en Add. También puede importar un archivo de aprovisionamiento si hace clic en Import. Para actualizar la tabla, haga clic en Refresh.

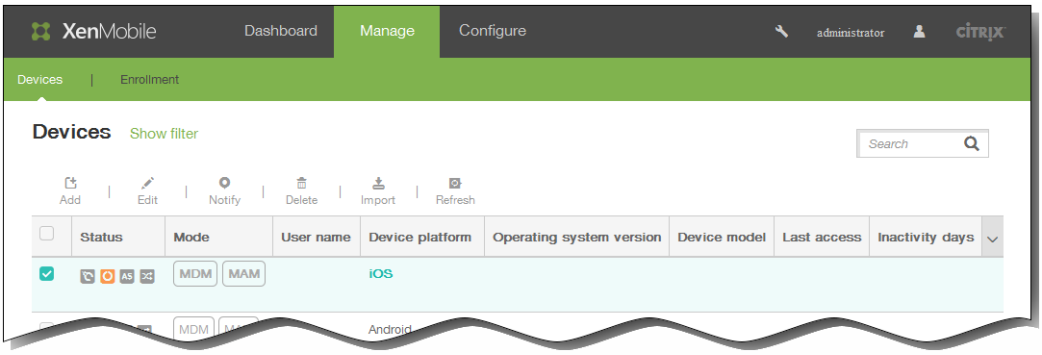


Cómo agregar dispositivos manualmente

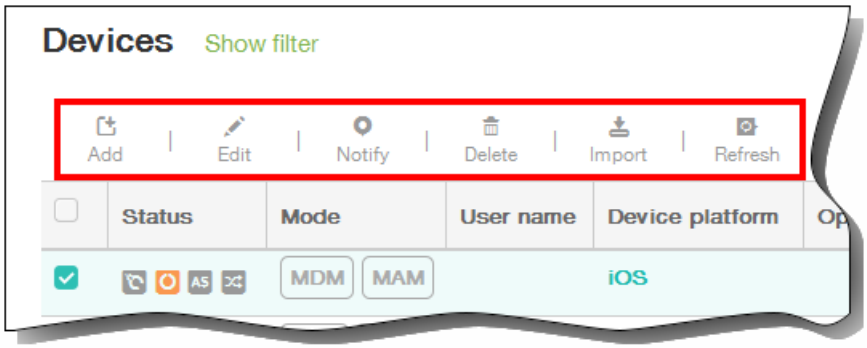
1. En la consola de XenMobile, haga clic en Manage > Devices y luego haga clic en Add. Aparecerá la página Add Device.

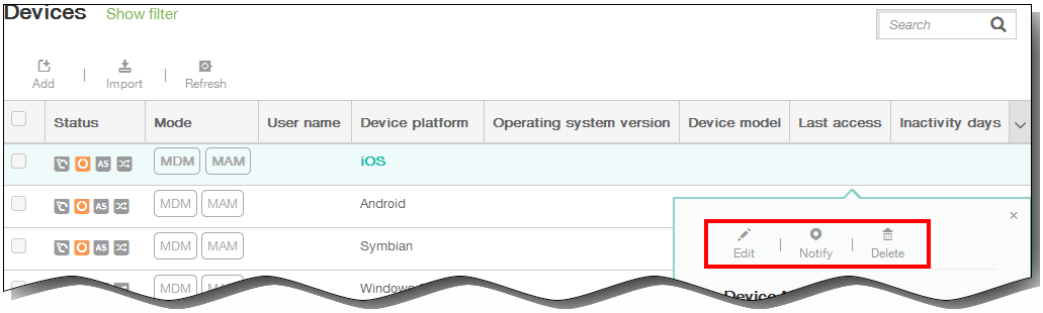


2. En Select platform, haga clic en iOS, Android, Symbian, Windows Phone 8.1, Windows 8.1 Tablet o BlackBerry.
3. Introduzca la siguiente información:
    1. iOS. Introduzca el número de serie en Serial Number.
    2. Android. Introduzca el número de serie en Serial Number y el identificador en IMEI/MEID.
    3. Symbian: Introduzca el identificador en IMEI/MEID.
    4. Windows Phone 8.1. Introduzca el número de serie en Serial Number y el identificador en IMEI/MEID.
    5. Windows 8.1 Tablet. Introduzca el número de serie en Serial Number y el identificador en IMEI/MEID.
    6. BlackBerry. Introduzca el número de serie en Serial Number y el identificador en IMEI/MEID.
4. Haga clic en Add. La tabla Devices aparecerá con el dispositivo agregado al final de la lista.
5. En la lista, seleccione el dispositivo agregado y, a continuación, en el menú que aparecerá, haga clic en Edit para ver y confirmar los detalles del dispositivo.

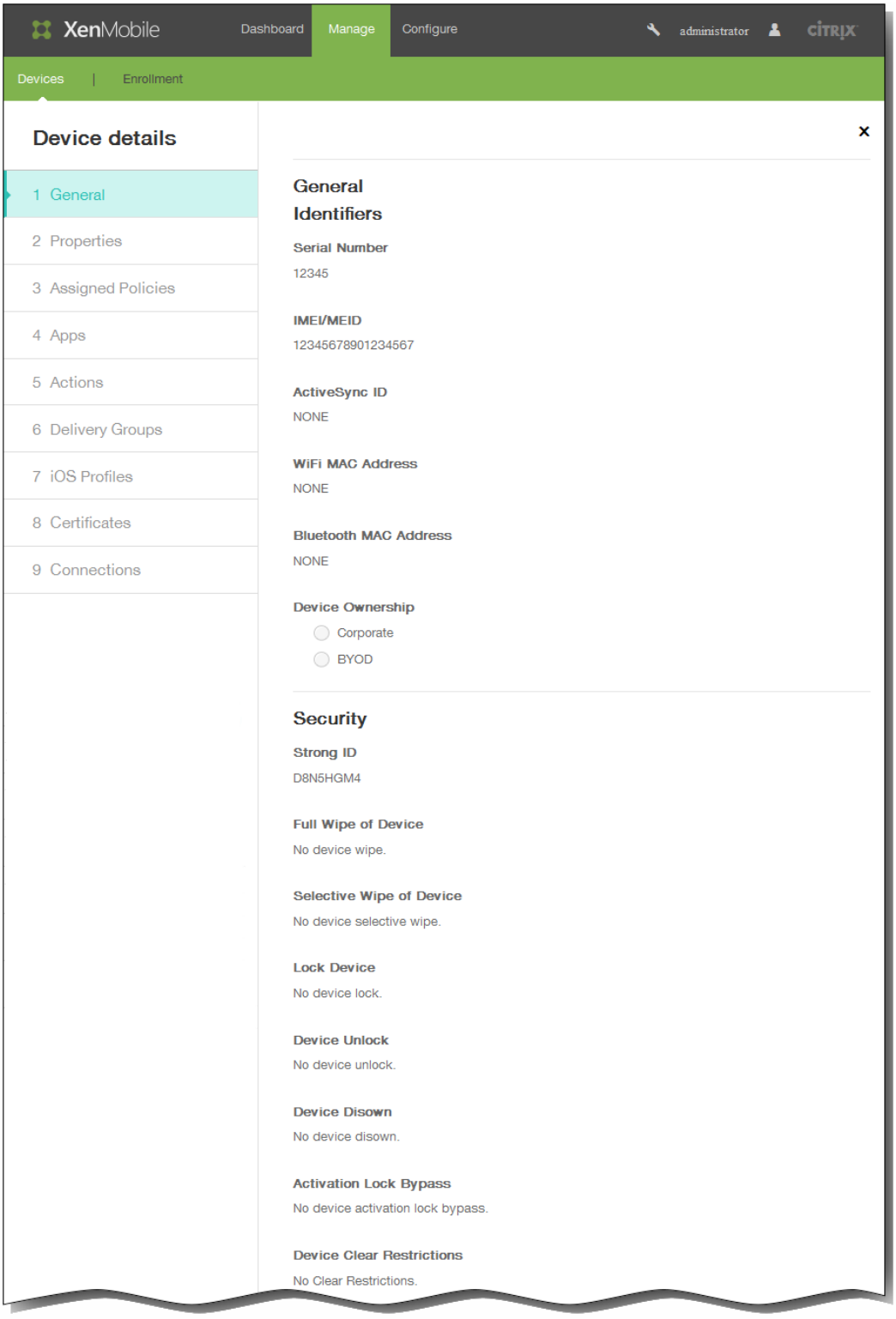


Nota: Si marca la casilla situada junto a un dispositivo, el menú de opciones aparecerá encima de la lista de dispositivos. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.



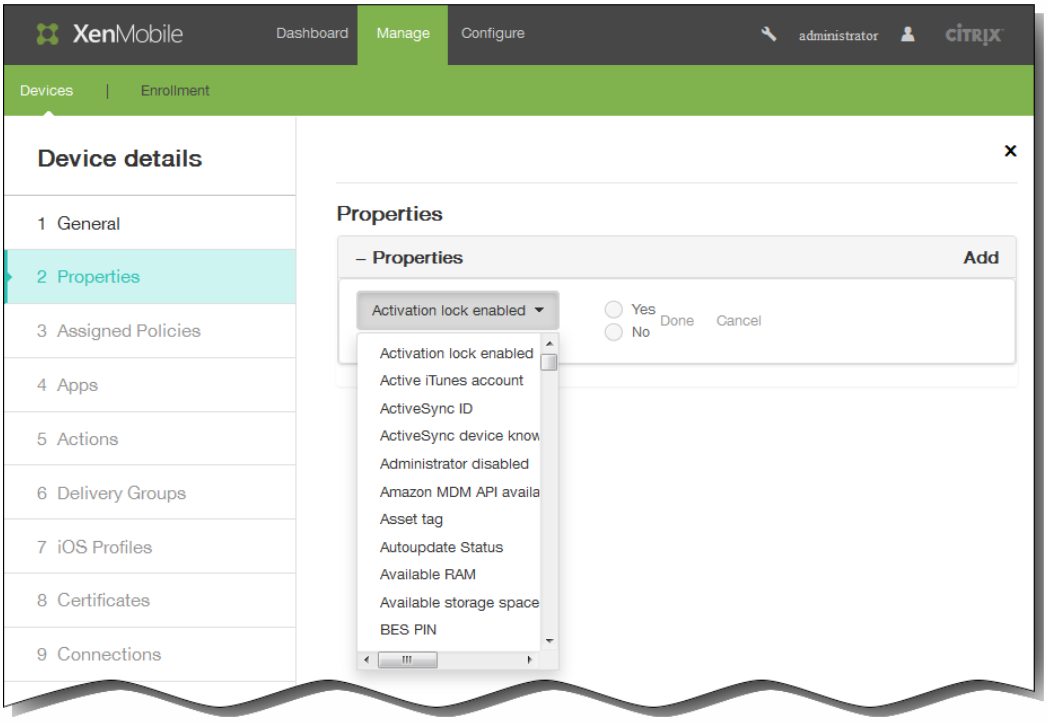


6. En General Identifiers, confirme la información mostrada (la lista de parámetros exacta varía según el tipo de plataforma): el número de serie, el identificador IMEI/MEID, el identificador de ActiveSync, la dirección MAC de la red Wi-Fi, la dirección MAC de Bluetooth y la propiedad del dispositivo: si pertenece a la empresa o al empleado, con la iniciativa Bring Your Own Device, que fomenta el uso de dispositivos personales en el trabajo.

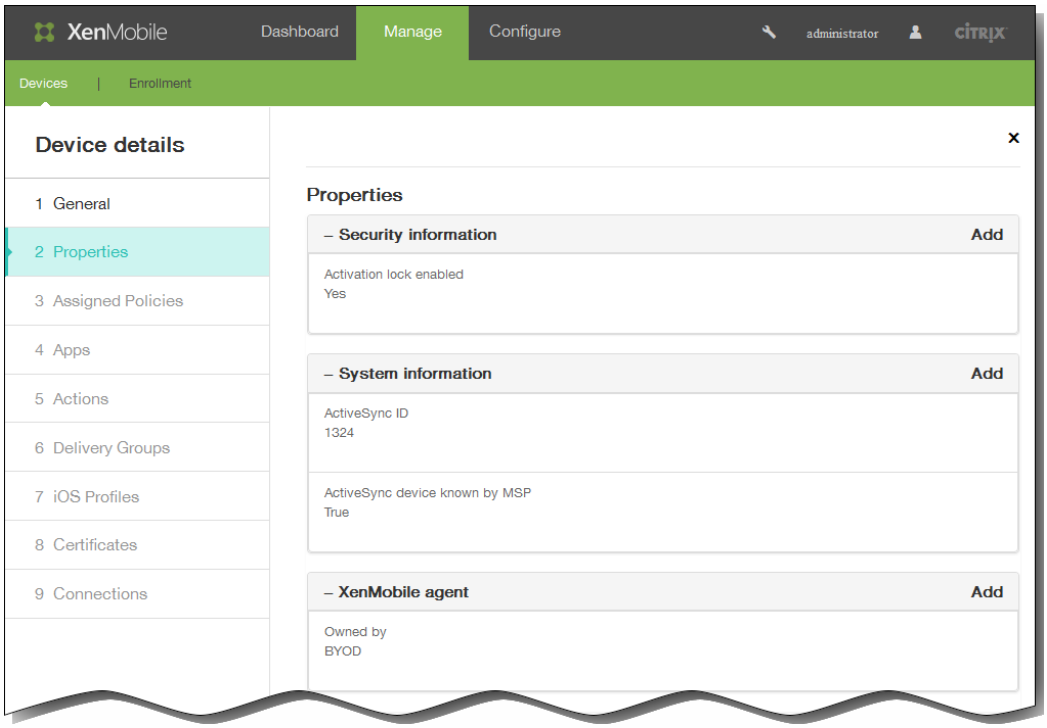


7. En Security, confirme la información mostrada (la lista exacta de parámetros varía según el tipo de plataforma): el ID seguro, el borrado total del dispositivo, el borrado selectivo del dispositivo, el bloqueo del dispositivo, el desbloqueo del dispositivo, la anulación de la posesión del dispositivo, la omisión dl bloqueo de activación y las restricciones de borrado del dispositivo.
8. Haga clic en Next para agregar propiedades.
9. En la página Properties, haga clic en Add para ver una lista de las propiedades que puede aprovisionar al dispositivo.

Aparecerá la lista de las propiedades disponibles.



10. En la lista, haga clic en la propiedad que se va a aprovisionar y, a continuación, establezca su valor. Por ejemplo, en la imagen anterior, la propiedad Activation lock enabled está seleccionada con un valor que se puede establecer en Yes o No.
11. Después de configurar una propiedad, haga clic en Done.
12. Repita los pasos del 9 al 11 para cada una de las propiedades que quiera aprovisionar y, a continuación, haga clic en Next. Nota: Al agregar propiedades, todas ellas aparecerán en Properties. Más adelante, cuando vuelva a la página Properties, las propiedades estarán divididas en categorías diferentes.



La sección **Assigned Policies** y las secciones siguientes contienen información resumida referente al dispositivo.

- Assigned Policies. Muestra la cantidad de directivas asignadas, incluidas las directivas implementadas, pendientes y erróneas. También aparecerán el nombre, el tipo y la última información implementada de cada directiva.
- Apps. Muestra la cantidad de aplicaciones según el último inventario, incluidas las aplicaciones instaladas, pendientes y erróneas.
  - En el caso de aplicaciones instaladas, aparece la siguiente información: el nombre, el propietario, la versión, el autor, el tamaño, el estado de su instalación, el identificador y el tipo.
  - En el caso de aplicaciones pendientes y fallidas, aparece la siguiente información: el nombre, la fecha de la última implementación, el identificador y el tipo.
- Actions. Muestra la cantidad de acciones, incluidas las acciones implementadas, pendientes y erróneas. Cada acción muestra el nombre y la última información implementada.
- Delivery Groups. Muestra la cantidad de grupos de entrega correctos, pendientes y erróneos. Cada acción va acompañada de información acerca de los grupos de entrega y de la hora. Además, aparece información más detallada del grupo de entrega, incluido el estado, la acción, el propietario y la fecha.
- iOS Profiles (solo para dispositivos iOS). Muestra el último inventario de perfiles iOS, incluidos el nombre, el tipo, la organización y la descripción.
- Certificates. Muestra la cantidad de certificados válidos, caducados o revocados, incluida la información sobre el tipo, el proveedor, el emisor, el número de serie, y las fechas de comienzo y finalización de la validez.
- Connections. Muestra los estados de la primera y la última conexión. Para cada conexión, aparecen el nombre de usuario, la penúltima y la última autenticación.
- TouchDown (solo para dispositivos Android). Muestra la última autenticación del dispositivo, así como la información acerca del último usuario autenticado. Aparecen todos los nombres y valores de directiva correspondientes.

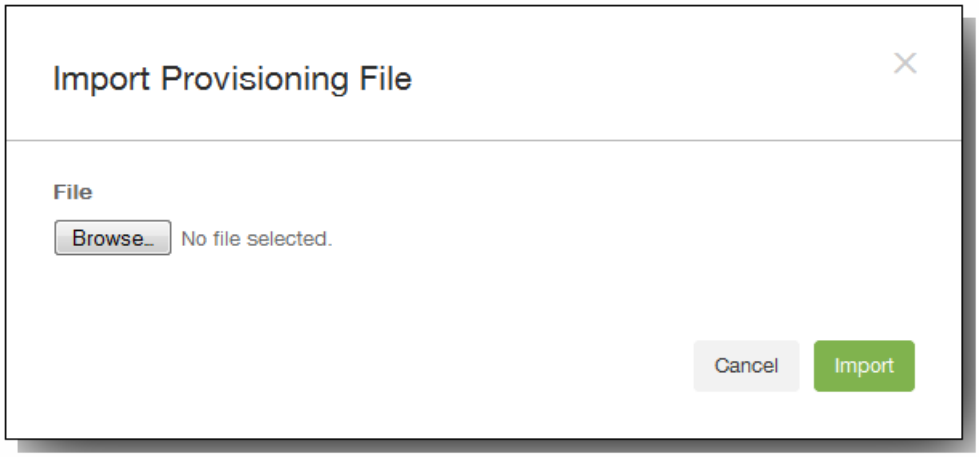
13. Haga clic en Save.

Cómo importar dispositivos desde un archivo de aprovisionamiento

Puede importar un archivo proporcionado por operadores de telefonía móvil o fabricantes de dispositivos móviles. También puede crear su propio archivo de aprovisionamiento de dispositivos. Consulte Formatos del archivo de aprovisionamiento de

dispositivos

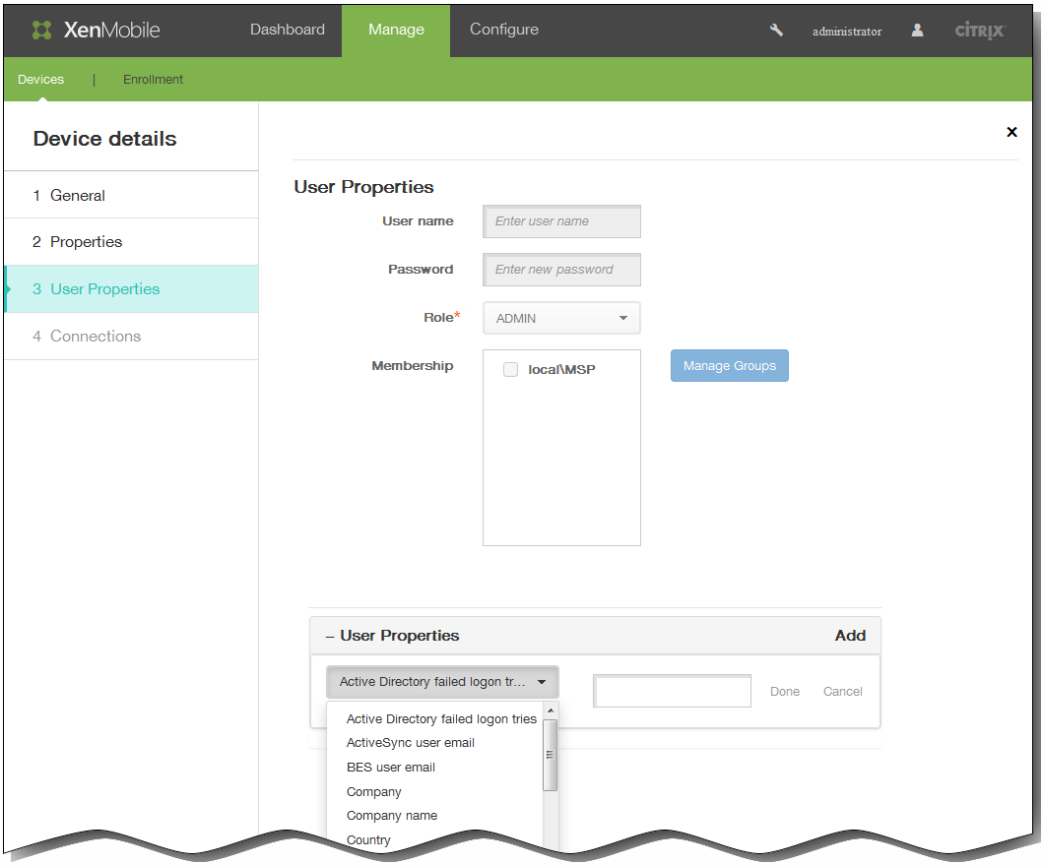
1. En el menú situado encima de la tabla Devices, haga clic en Import. Aparece el cuadro de diálogo Import Provisioning File.



2. Para seleccionar el archivo a importar, haga clic en Browse y vaya a la ubicación de ese archivo.
3. Haga clic en Import. Los archivos importados se agregarán a la tabla Devices.

Cómo modificar dispositivos

1. Seleccione el dispositivo a modificar y, a continuación, haga clic en Edit. Aparecerá la página Device Details.
2. En General Identifiers, el único campo que puede modificar es Device Ownership, y lo puede establecer en Corporate o en BYOD.
3. Haga clic en Next. Aparecerá la página Properties.
4. En la página Properties, agregue, modifique o elimine las propiedades como corresponda.
   - Para modificar una propiedad, haga clic en ella, modifique su configuración y, a continuación, haga clic en Done o en Cancel.
   - Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa situada en el lado derecho. El elemento se eliminará inmediatamente.
5. Haga clic en Next. La página que aparecerá a continuación depende del dispositivo seleccionado. Para algunos dispositivos, aparecerá User Properties mientras que, para otros, aparecerá Assigned Properties.
6. Si aparece User Properties, agregue, modifique o elimine las propiedades del usuario como se indica a continuación. De lo contrario, las páginas restantes contienen información resumida referente al dispositivo. Para obtener una descripción de estas páginas, consulte Para agregar dispositivos manualmente.



Note: La parte superior de la página User Properties no se puede modificar.

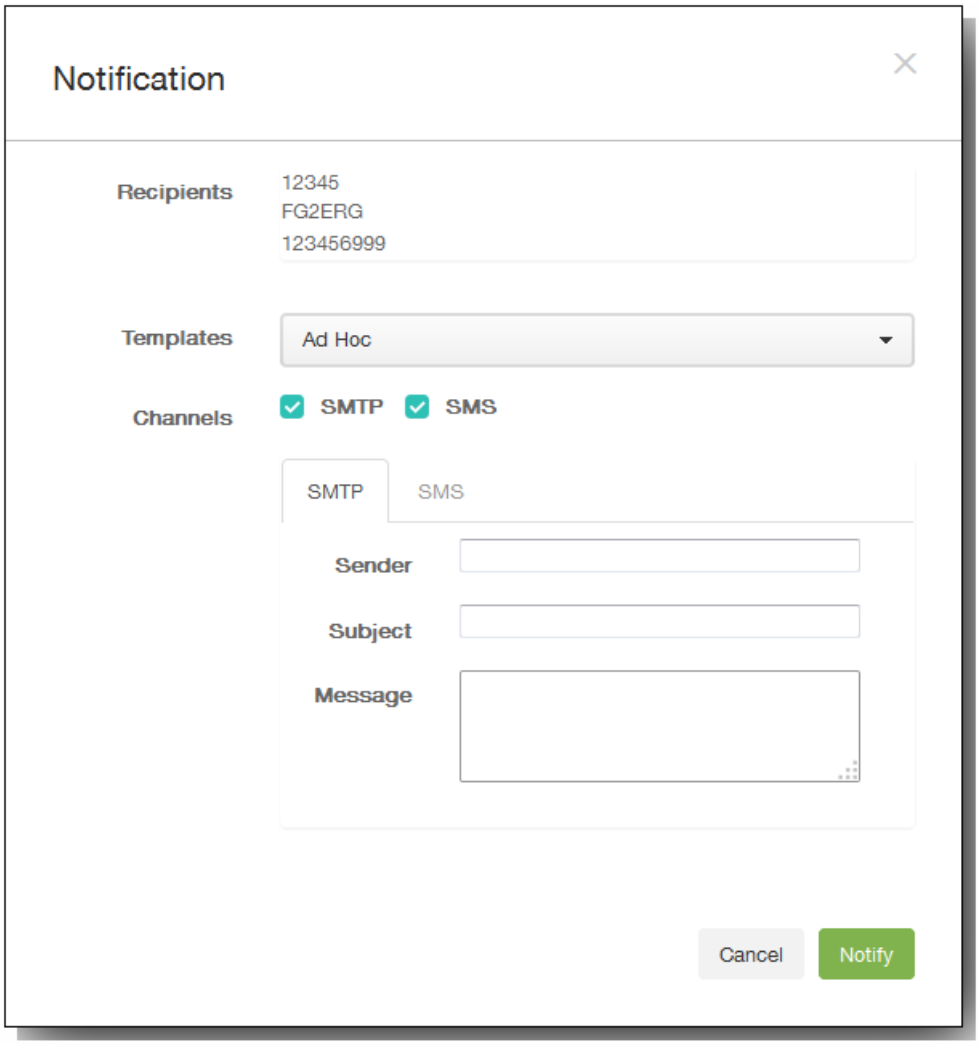
- Para agregar una propiedad de usuario, haga clic en Add.
  - En la lista, haga clic en la propiedad que quiera agregar, especifique el valor de la propiedad y, a continuación, haga clic en Done o en Cancel. Repita este paso para cada propiedad que quiera agregar.
- Para modificar una propiedad, haga clic en ella, modifique su configuración y, a continuación, haga clic en Done o en Cancel.
- Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa situada en el lado derecho. El elemento se eliminará inmediatamente.

7. Haga clic en Next en cada una de las páginas siguientes para ver información resumida.
8. En la página final, haga clic en Save para guardar los cambios realizados en el dispositivo.

Cómo enviar una notificación a los dispositivos

Puede enviar notificaciones a los dispositivos desde la página Devices. Para obtener más información acerca de notificaciones, consulte Para crear o actualizar plantillas de notificación en XenMobile

1. Seleccione los dispositivos a los que quiera enviar una notificación.
2. Haga clic en Notify. Aparecerá el cuadro de diálogo Notification. En Recipients, se ofrece una lista de todos los dispositivos que van a recibir la notificación.



3. Defina la siguiente información:
   1. Templates. En la lista, haga clic en el tipo de notificación que quiera enviar.
      Los campos Subject y Message se rellenarán con el texto configurado de la plantilla que eligió, excepto en el caso de haber elegido Ad Hoc.

   2. Channels. Seleccione cómo enviar el mensaje. El valor predeterminado es SMTP
      —y
      SMS.
      Puede hacer clic en las fichas SMTP y SMS para ver el formato del mensaje de cada canal.

   3. Sender. Escriba un remitente opcional.
   4. Subject. Escriba un asunto para un mensaje "Ad Hoc".
   5. Message. Escriba el mensaje para un mensaje "Ad Hoc".
4. Haga clic en Notify.

Cómo eliminar dispositivos

1. En la tabla Devices, seleccione los dispositivos que quiere eliminar.
2. Haga clic en Delete. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en Delete.
   Importante: Esta operación no se puede deshacer.

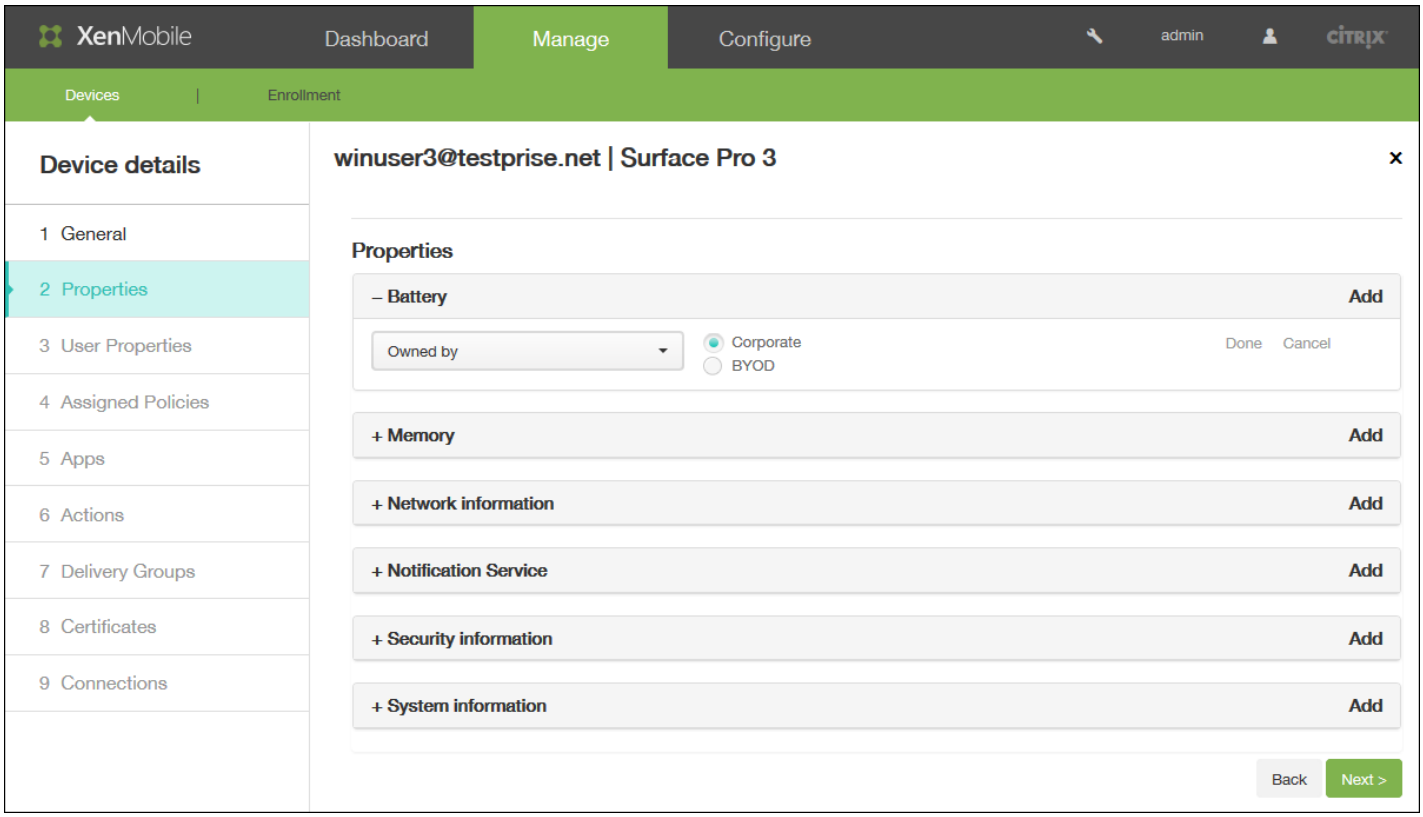
Etiquetado manual de dispositivos de usuario

May 05, 2016

Puede etiquetar manualmente un dispositivo en XenMobile de una de las siguientes maneras:

- Etiquetar el dispositivo durante el proceso de inscripción por invitación.
- Etiquetar el dispositivo durante el proceso de inscripción al portal Self Help Portal.
- Etiquetar el dispositivo añadiendo el propietario del mismo como una de sus propiedades.

Tiene la opción de etiquetar el dispositivo definiendo como propietario del mismo a la empresa o al empleado. Cuando usa el portal Self Help Portal para inscribir un dispositivo, también puede etiquetarlo con su propietario, ya sea la empresa o el empleado. Como se ve en esta imagen, también puede etiquetar un dispositivo manualmente agregando una propiedad al mismo desde la ficha **Devices** en la consola de XenMobile, agregando la propiedad **Owned by** y eligiendo **Corporate** (si la empresa es la propietaria del dispositivo) o **BYOD** (si el empleado es el propietario del dispositivo).



Formatos del archivo de aprovisionamiento de dispositivos

May 05, 2016

Muchos operadores móviles o fabricantes de dispositivos proporcionan listas de dispositivos móviles autorizados. Puede usar estas listas para no tener que introducir una larga lista de dispositivos móviles de forma manual. XenMobile es compatible con un formato de archivo de importación común para los tres tipos de dispositivos respaldados: Android, iOS y Windows.

Un archivo de aprovisionamiento que se crea manualmente y se usa para importar dispositivos en XenMobile debe tener el siguiente formato:

- SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

Nota:

- El conjunto de caracteres del archivo debe ser UTF-8.
- Los campos del archivo de aprovisionamiento están separados por un punto y coma (;). Si parte de un campo contiene un punto y coma, debe contener también un carácter de barra diagonal inversa (\). Por ejemplo, la propiedad propertyV;test;1;2 debe escribirse como propertyV\;test\;1\;2 en el archivo de aprovisionamiento.
- SerialNumber es necesario si IMEI no está especificado.
- SerialNumber es obligatorio para dispositivos iOS porque el número de serie es el identificador del dispositivo iOS.
- IMEI es necesario si SerialNumber no está especificado.
- Los valores válidos para OperatingSystemFamily son: WINDOWS, ANDROID o iOS.

Ejemplo de un archivo de aprovisionamiento de dispositivos

Las siguientes líneas describen un dispositivo dentro de un archivo de aprovisionamiento de dispositivos.

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

La primera entrada significa lo siguiente:

- SerialNumber: 1050BF3F51730108161006551059039 1
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Macros en XenMobile

May 05, 2016

XenMobile pone a su disposición potentes macros para rellenar datos de propiedad de usuario o de dispositivo en los campos de texto de un perfil, una directiva, una notificación o una plantilla de inscripción (para algunas acciones), entre otros usos. Con las macros, puede configurar una sola directiva, para implementarla a un usuario básico, además de definir que aparezcan valores específicos por usuario para cada usuario de destino. Por ejemplo, puede rellenar de antemano el valor del buzón de correo relativo a un solo usuario en un perfil de Exchange entre miles de usuarios.

Por el momento, esta función solo está disponible en el contexto de configuraciones y plantillas para dispositivos iOS y Android.

Definición de macros de usuario

Las siguientes macros de usuario siempre están disponibles:

- loginname (nombre de usario más nombre de dominio)
- username (nombre de inicio de sesión menos el dominio, si existe)
- domainname (nombre de dominio o el dominio predeterminado)

Las siguientes propiedades definidas por el administrador pueden estar disponibles:

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename

- postalcode
- postofficebox
- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (anula la propiedad descrita anteriormente)

Además, si el usuario está autenticado mediante un servidor de autenticación (como LDAP), están disponibles todas las propiedades asociadas al usuario que se encuentren en ese almacén.

Sintaxis de macros

Una macro puede presentar el siguiente formato:

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

Como regla general, todos los elementos de sintaxis posteriores al signo de dólar ($), deben estar entre llaves ({ }).

- Los nombres de propiedad calificados hacen referencia ya sea a una propiedad de usuario, una propiedad de dispositivo , o una propiedad personalizada.
- Los nombres de propiedad calificados se componen de un prefijo, seguido del nombre en sí de la propiedad.
- Las propiedades de usuario presentan el formato ${user.[PROPERTYNAME] (prefix="user.")}.
- Las propiedades de dispositivo presentan el formato ${device.[PROPERTYNAME] (prefix="device.")}.

Por ejemplo, ${user.username} rellena el valor de nombre de usuario en el campo de texto de una directiva. Esto es útil para configurar perfiles de Exchange ActiveSync y otros perfiles utilizados por varios usuarios.

Para macros personalizadas (propiedades que usted define), el prefijo es ${custom}. Puede omitir el prefijo.

Nota: Los nombres de propiedad distinguen mayúsculas de minúsculas.

Directivas de dispositivo

May 05, 2016

Puede configurar el funcionamiento de XenMobile en los dispositivos gracias a la creación de directivas. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre dispositivos iOS, Android y Windows, e incluso entre los diferentes fabricantes de aquellos dispositivos con Android.

Antes de crear una directiva nueva, lleve a cabo estos pasos:

- Crear los grupos de entrega que se van a utilizar.
- Instalar los certificados de CA necesarios.

A continuación, se presentan los pasos básicos necesarios para crear una directiva de dispositivos:

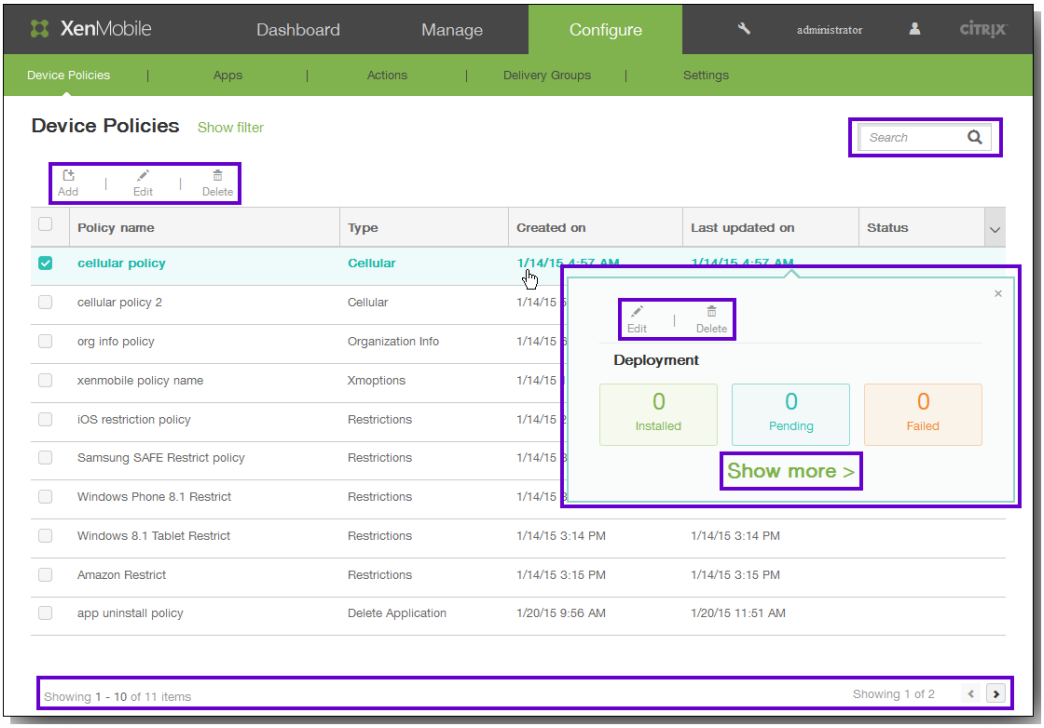
1. Especificar el nombre y la descripción de la directiva.
2. Configurar una o varias plataformas.
3. Crear las reglas de implementación (opcional).
4. Asignar la directiva a grupos de entrega.
5. Configurar la programación de las implementaciones (opcional).

La página de directivas de dispositivos en la consola

En la consola de XenMobile, puede trabajar con directivas de dispositivos desde la página Device Policies. Para llegar a la página Device Policies, haga clic en Configure > Device Policies. Desde aquí, puede agregar, modificar o eliminar directivas y ver el estado de las existentes.

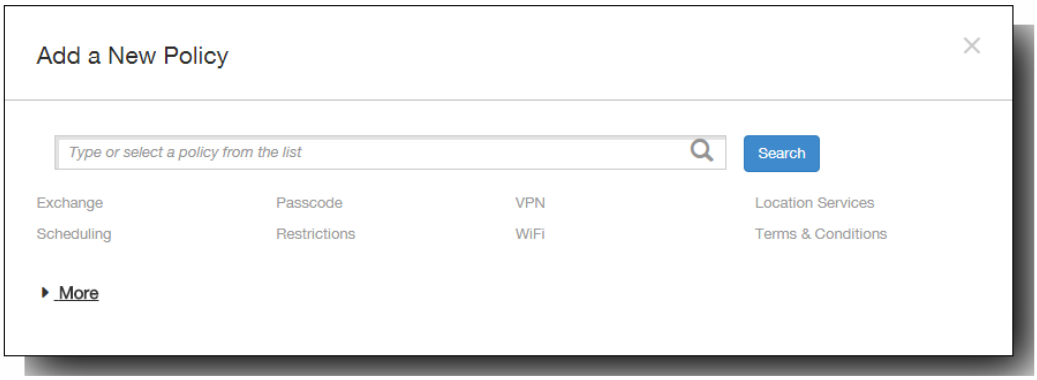
La página Device Policies contiene una tabla que muestra todas las directivas en vigor.

Para modificar o eliminar una directiva de la página Device Policies, marque la casilla situada junto a esa directiva para que aparezca el menú de opciones encima de la lista de directivas. También puede hacer clic en una directiva de la lista para que aparezca el menú de opciones en el lado derecho de la lista. Si hace clic en Show More, aparecerán datos detallados de la directiva.

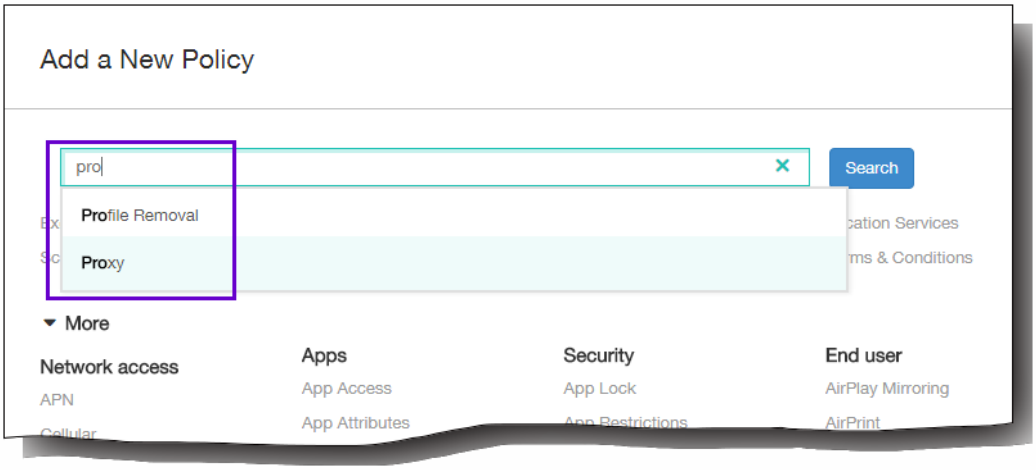


Para agregar una directiva de dispositivo

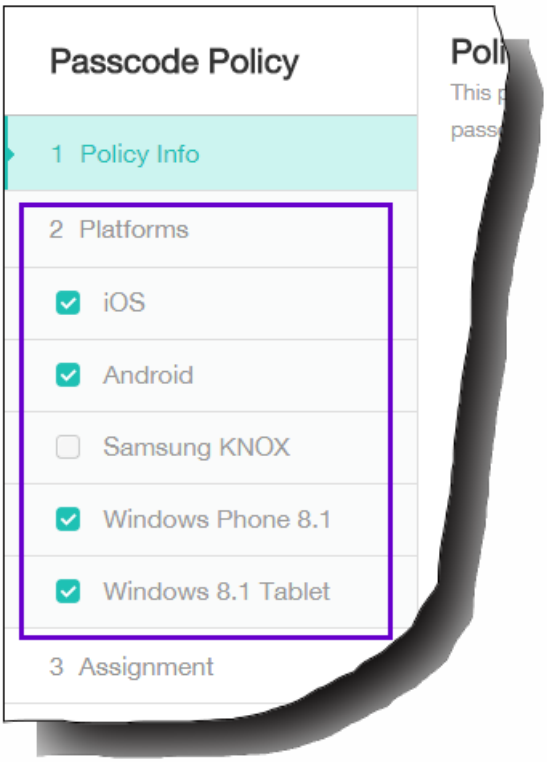
1. En la página Device Policies, haga clic en Add.
   Aparecerá el cuadro de diálogo Add a New Policy. Puede hacer clic en More para ver más directivas.



2. Para encontrar la directiva que quiere agregar, lleve a cabo una de las siguientes acciones:
   - Haga clic en la directiva.
     Aparecerá la página Policy Information referente a la directiva seleccionada.
   - Escriba el nombre de la directiva en el campo de búsqueda. Cuando escriba, aparecerán posibles coincidencias. Si la directiva está en la lista, haga clic en ella. Solo permanecerá en el cuadro de diálogo la directiva que seleccione. Haga clic en la directiva para abrir la página Policy Information referente a ella.
     Importante: Si la directiva seleccionada está en el área More, solo será visible si expande More.

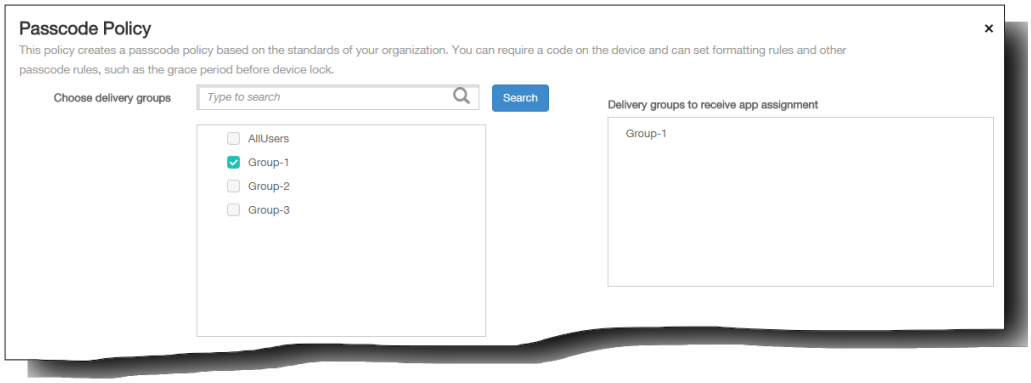


3. Seleccione las plataformas a incluir en la directiva. Las páginas de configuración referentes a las plataformas seleccionadas aparecerán en el paso 5.
   Nota: Solo se mostrarán en la lista aquellas plataformas que sean compatibles con la directiva.



4. Complete los datos de la página Policy Information y haga clic en Next. La página Policy Information recopila información (como el nombre de la directiva) para ayudarle a identificar sus directivas y realizar un seguimiento de ellas. Esta página es similar para todas las directivas.
5. Complete las páginas de plataformas. Aparecerán páginas de plataformas para cada plataforma que haya seleccionado en el paso 3. Estas páginas son distintas para cada directiva. Todas las directivas pueden ser diferentes en función de las plataformas. No todas las plataformas admiten todas las directivas. Haga clic en Next para ir a la siguiente página de plataforma o, cuando haya completado todas las páginas de plataforma, para ir a la página Assignment.
6. En la página Assignment, seleccione los grupos de entrega a los que se aplicará la directiva. Al hacer clic en un grupo de entrega, el grupo aparecerá en el cuadro Delivery groups to receive app assignment.

Nota: El cuadro Delivery groups to receive app assignment no aparecerá hasta que seleccione un grupo de entrega.



7. Haga clic en Save.
   La directiva se agrega a la tabla Device Policies.

Para modificar o eliminar una directiva de dispositivos

1. En la tabla **Device Policies**, marque la casilla situada junto a la directiva que se va a modificar o eliminar.
2. Haga clic en Edit o Delete.
   - Si hace clic en Edit, puede modificar todos o algunos de los valores de configuración.
   - Si hace clic en Delete, haga clic en Delete de nuevo en el cuadro de diálogo de confirmación.

Directivas de dispositivos de XenMobile desglosadas por plataforma

May 05, 2016

En la siguiente tabla se muestran las directivas de dispositivos que se pueden agregar y configurar en XenMobile 10.0 para dispositivos Amazon, iOS, Android, Samsung SAFE, Samsung KNOX, Symbian, Windows Phone 8.1 y tabletas Windows 8.1. Puede agregar y configurar las directivas de dispositivos en la consola de XenMobile, desde Configure > Device Policies. Nota: Android Sony solo admite la directiva de cifrado de almacenamiento. Android HTC solo respalda la directiva de Exchange.

Directiva de dispositivos	**Amazon**	**iOS**	**Android**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Tableta Windows 8.1**
Common								
Exchange		X	X	X	X		X	
Programación			X			X		
Passcode		X	X		X		X	X
Restrictions	X	X		X			X	X
VPN	X	X	X	X	X			X
WiFi		X	X				X	X
Location Services		X	X					
Terms & Conditions	X	X	X	X	X	X	X	X
Network access								
APN		X	X		X			
Cellular			X					
Personal Hotspot		X						

Directiva de dispositivos	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Tableta Windows 8.1
Proxy		X						
Remote Support					X			
Roaming		X						
Samsung Firewall				X				
Tunnel			X					
	Amazon	**iOS**	**Android**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Tableta Windows 8.1**
Custom								
Custom XML						X	X	X
Import iOS Profile		X						
Removal								
Profile Removal		X						
Apps								
App Access		X	X			X		
App Attributes		X						
App Configuration		X						
App Inventory		X	X		X	X	X	X
App Uninstall		X	X		X			X
App Uninstall Restrictions	X			X				
Files			X					

Directiva de dispositivos	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Tableta Windows 8.1
Samsung Browser				X	X			
Sideloading Key								X
Signing Certificate								X
Webclip		X	X					X
Worx Store		X	X					X

	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Tableta Windows 8.1
Security								
App Lock		X	X					
Restricciones de aplicaciones					X			
Contacts (CardDAV)		X						
Credentials		X	X					X
Kiosk				X				
Managed Domains		X						
SCEP		X						
Samsung MDM License Key				X	X			
Storage Encryption			X	X			X	
Web Content Filter		X						
Agente de XenMobile								
Enterprise Hub							X	

Directiva de dispositivos	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Tableta Windows 8.1
XenMobile Options			X			X		
XenMobile Uninstall			X					
End user								
AirPlay Mirroring		X						
AirPrint		X						
Calendar (CalDav)		X						
Font		X						
LDAP		X						
MDM Options		X						
Mail		X						
Organization Info		X						
SSO Account		X						
Subscribed Calendars		X						

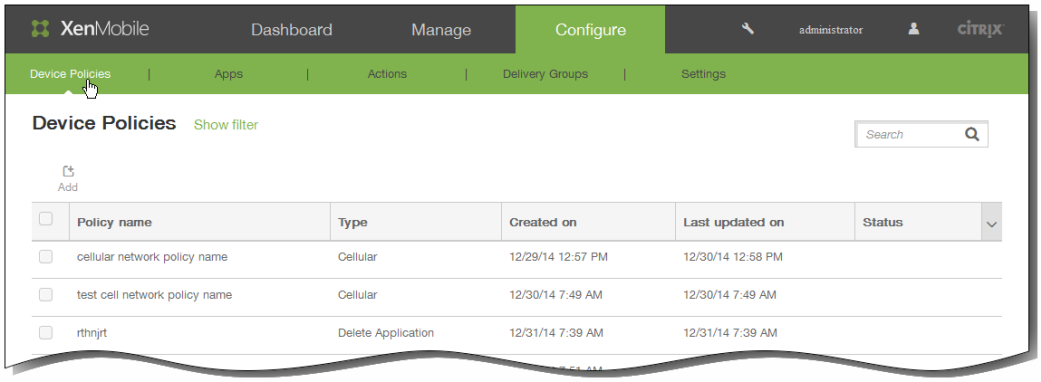
Para agregar una directiva de acceso de aplicaciones para dispositivos

May 05, 2016

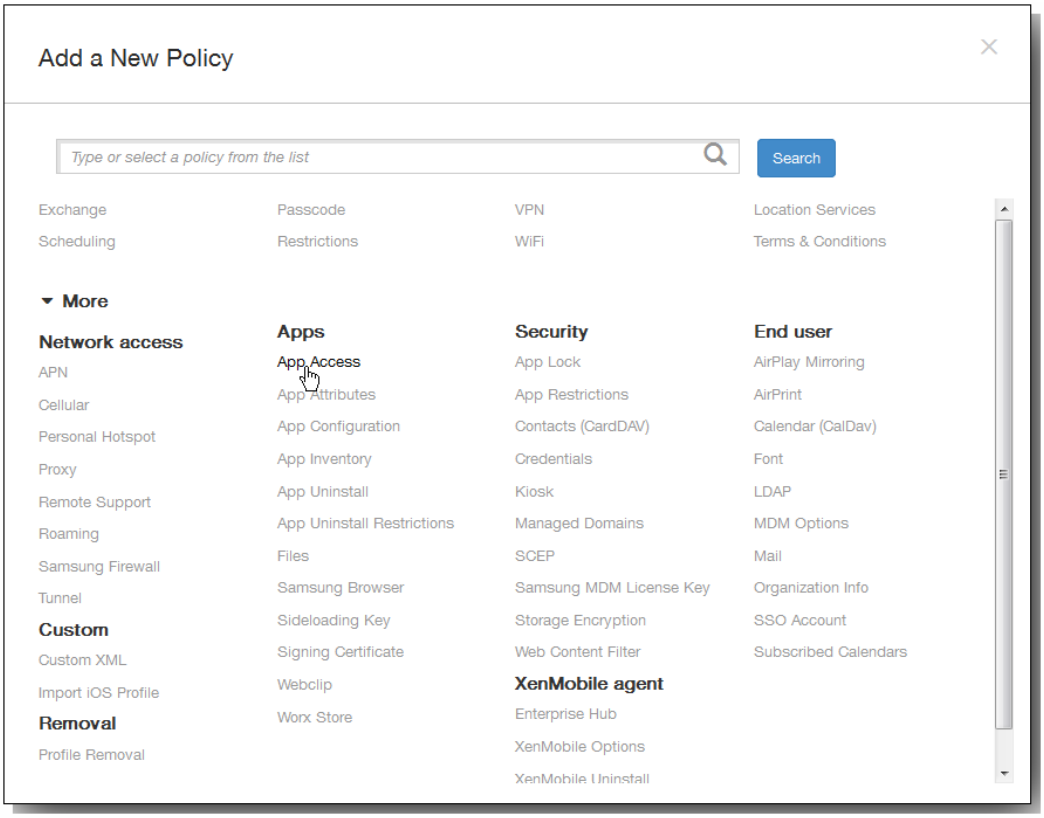
En XenMobile, la directiva de acceso de aplicaciones permite definir una lista de las aplicaciones que deben estar instaladas en el dispositivo, pueden estar instaladas en el dispositivo o no deben estar instaladas en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento del dispositivo con los requisitos de dicha lista de aplicaciones. Puede crear directivas de acceso de aplicaciones para dispositivos iOS, Android o Symbian.

Solo puede configurar un tipo de directiva de acceso en un momento dado. Puede agregar una directiva referente a una lista de aplicaciones necesarias, de aplicaciones recomendadas o de aplicaciones prohibidas, pero una mezcla en la misma directiva de acceso no. Si crea una directiva para cada tipo de lista, se recomienda prestar atención al nombrar cada directiva para saber qué directiva se aplica exactamente a qué lista de aplicaciones concreta en XenMobile.

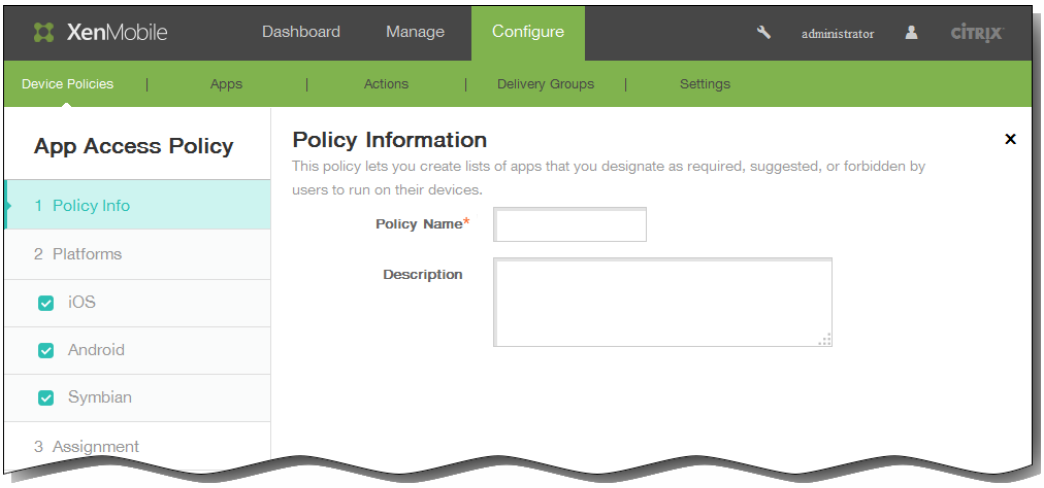
1. En la consola de XenMobile, haga clic en Configure > Device Policies.



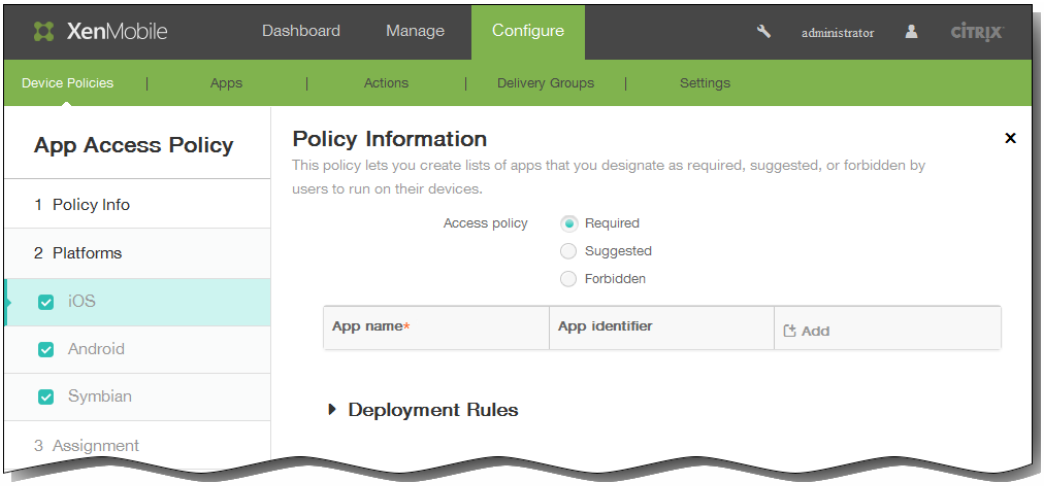
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More > App Access. Aparecerá la página de información App Access Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y la primera página de configuración que se muestra pertenece a la plataforma de iOS.



6. En Platforms, seleccione las plataformas que quiera agregar y, a continuación, lleve a cabo lo siguiente para cada plataforma:
   1. Access policy. Haga clic en Required, Suggested o Forbidden. El valor predeterminado es Required.
   2. Para agregar una o varias aplicaciones a la lista, haga clic en Add y, a continuación, lleve a cabo lo siguiente:
      1. App name. Escriba un nombre de aplicación.
      2. App Identifier. Escriba un identificador opcional de la aplicación.
      3. Haga clic en Save o Cancel.
      4. Repita los pasos de i. a iii. para cada aplicación que quiera agregar.

      Nota: Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

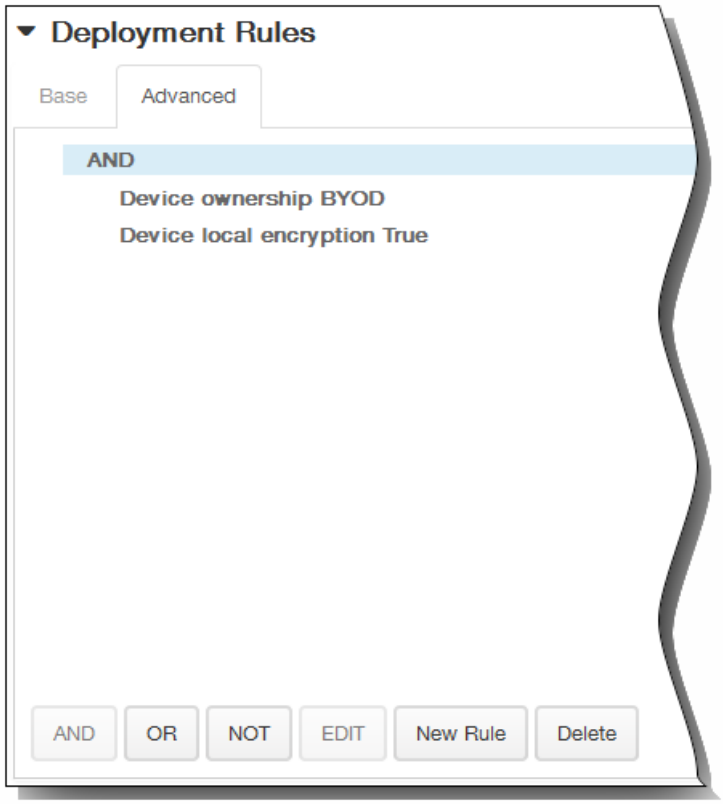
      Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
      2. Haga clic en New Rule para definir las condiciones.
      3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.

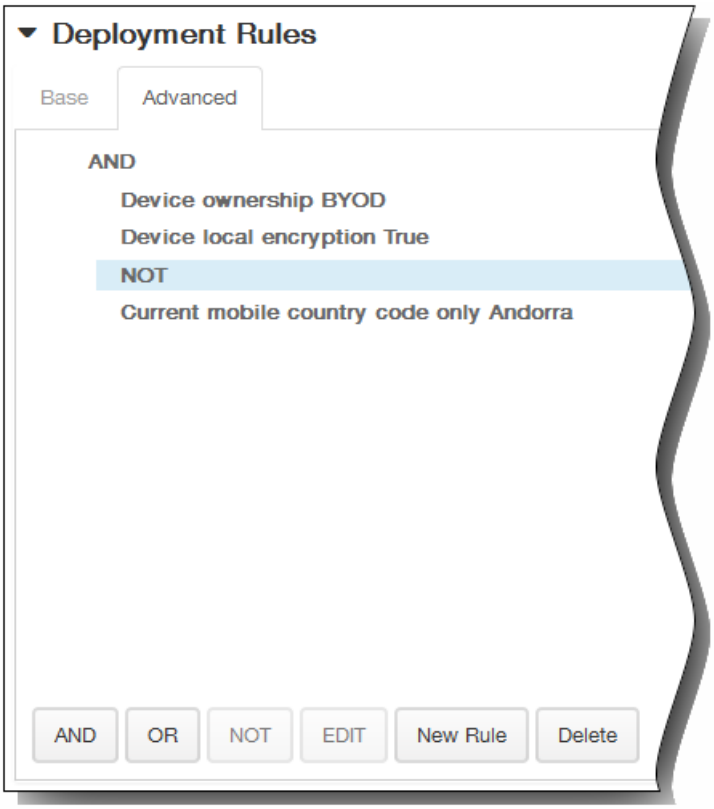
4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.

2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

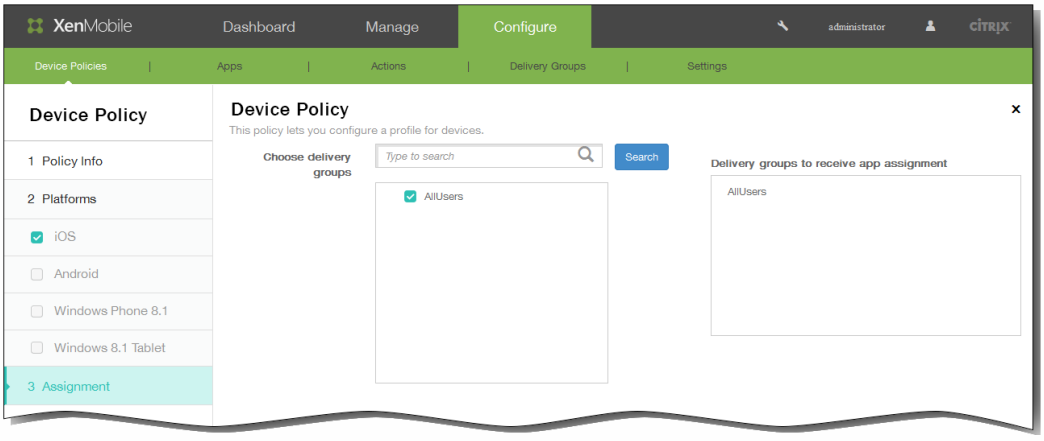


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
       En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
       En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



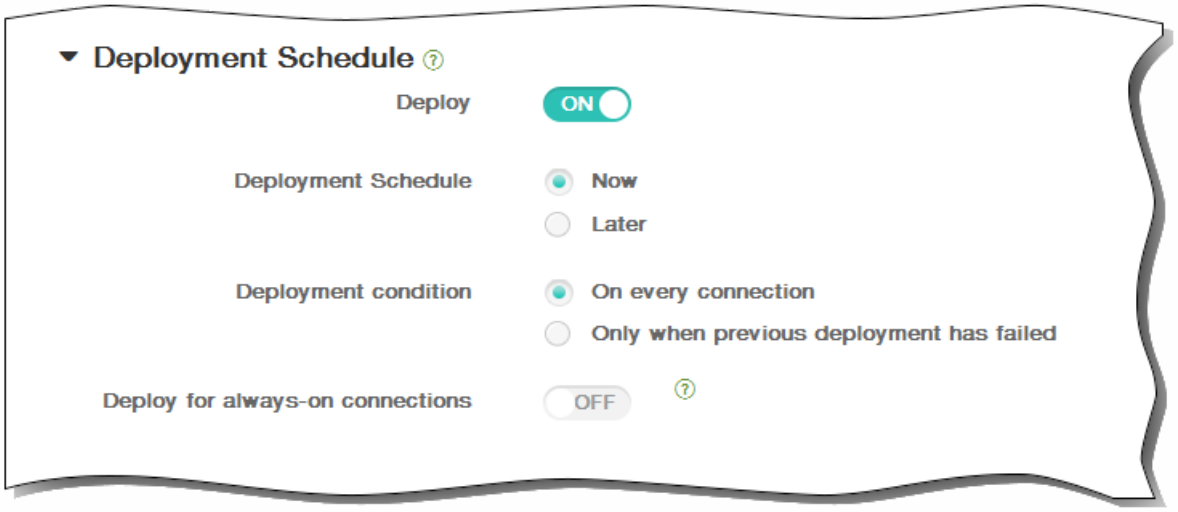
8. Haga clic en Next. Aparecerá la página de la siguiente plataforma o la página de la directiva Assignment.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

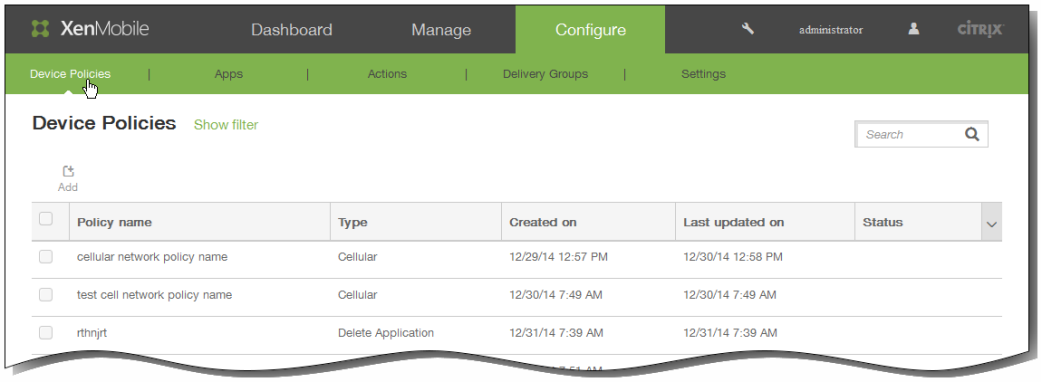
Para agregar una directiva de inventario de aplicaciones para dispositivos

May 05, 2016

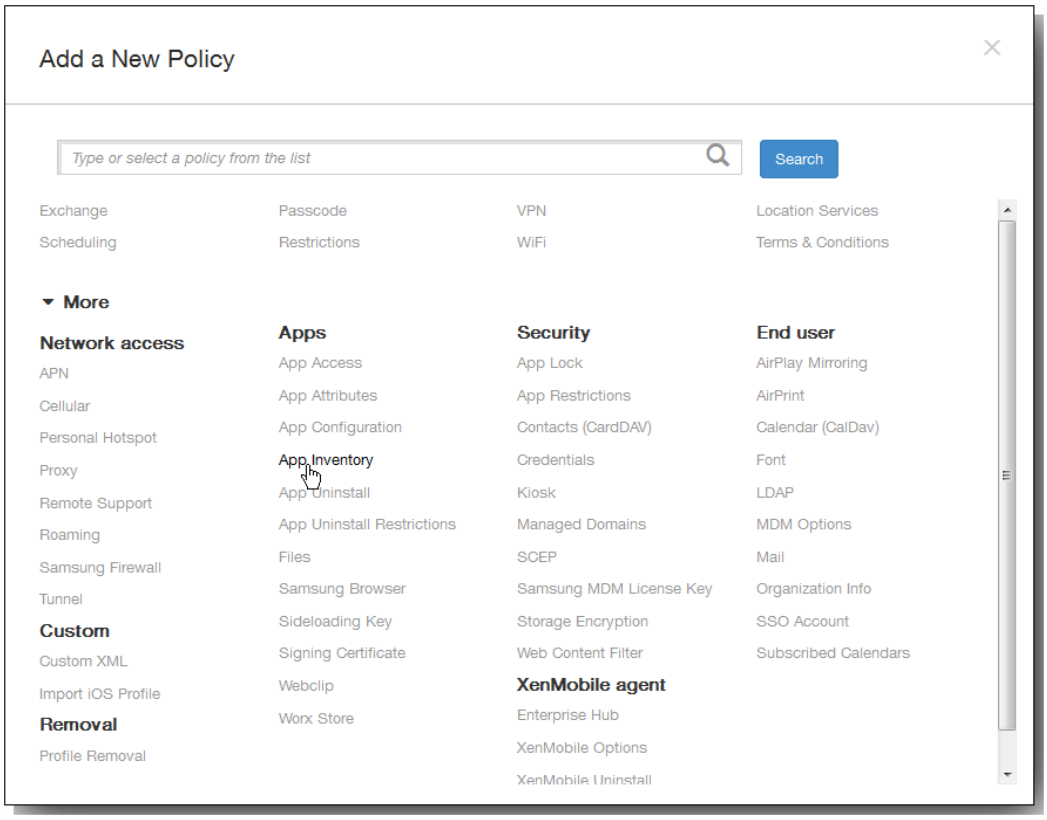
En XenMobile, una directiva de inventario de aplicaciones permite obtener un inventario de las aplicaciones presentes en los dispositivos administrados. A continuación, el inventario se compara con las directivas de acceso de aplicaciones implementadas en esos dispositivos. De esta forma, podrá detectar aplicaciones que aparezcan en la lista de aplicaciones prohibidas (prohibidas en una directiva de acceso de aplicaciones) o en la lista de aplicaciones permitidas (requeridas en una directiva de acceso de aplicaciones) para actuar consecuentemente.

Importante: Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de la instancia de Worx Store presente en los dispositivos Android de los usuarios, primero debe implementar esta directiva en los dispositivos de los usuarios.

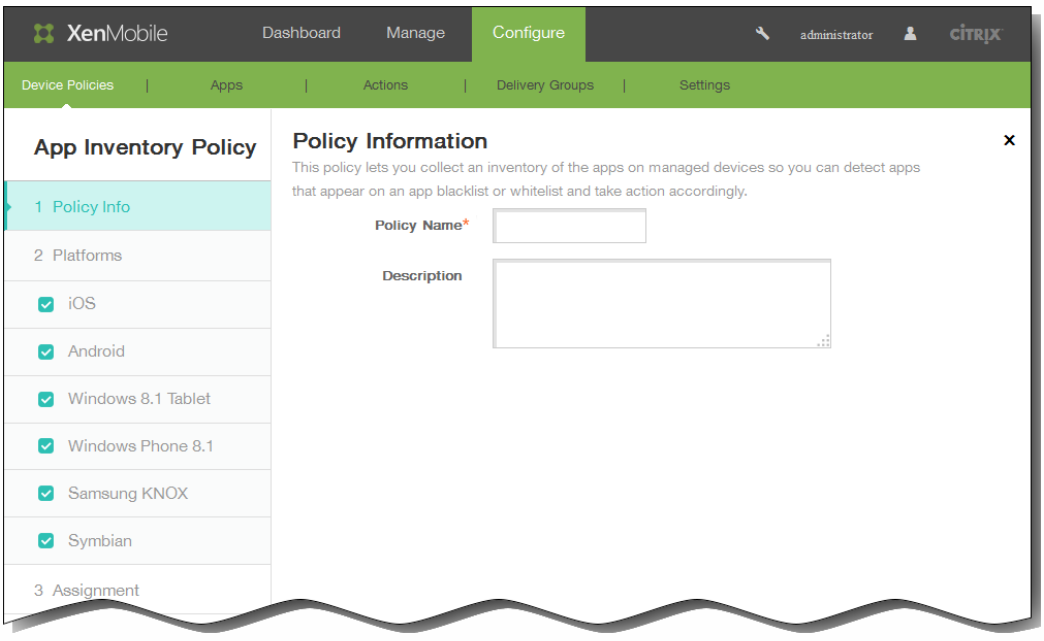
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



2. Haga clic en Agregar. Aparecerá la página Add a New Policy.

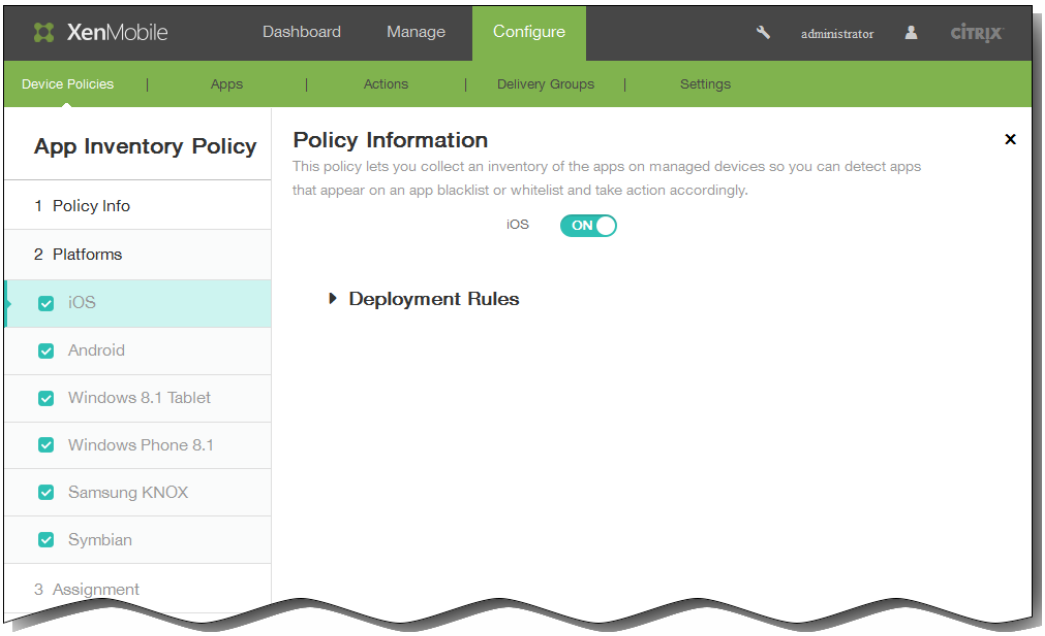


3. Haga clic en More > App Inventory. Aparecerá la página App Inventory Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.

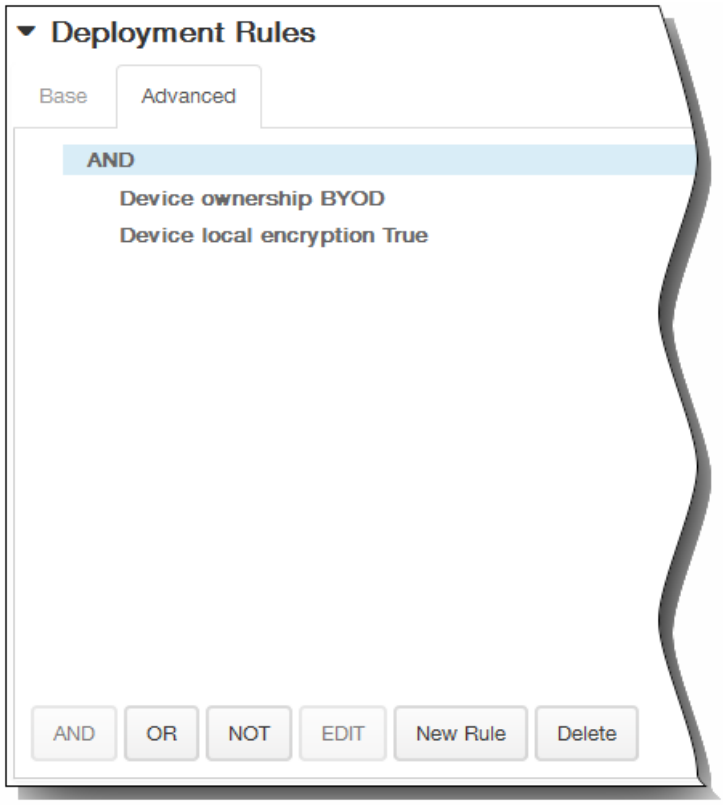
Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS.



Seleccione las plataformas que quiera agregar y, a continuación, lleve a cabo lo siguiente para cada plataforma:

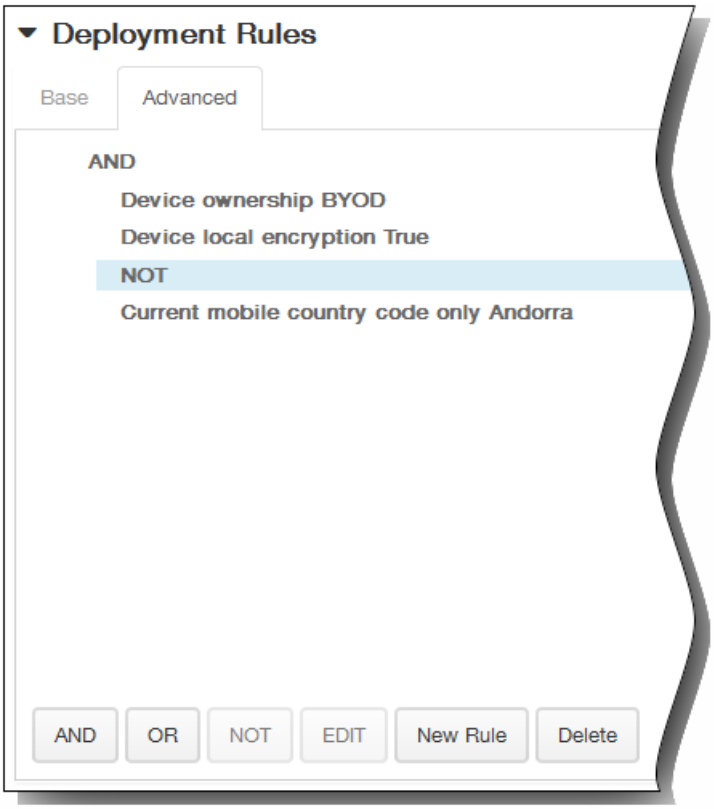
6. Deje el parámetro predeterminado o cámbielo a OFF. El valor predeterminado es ON.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

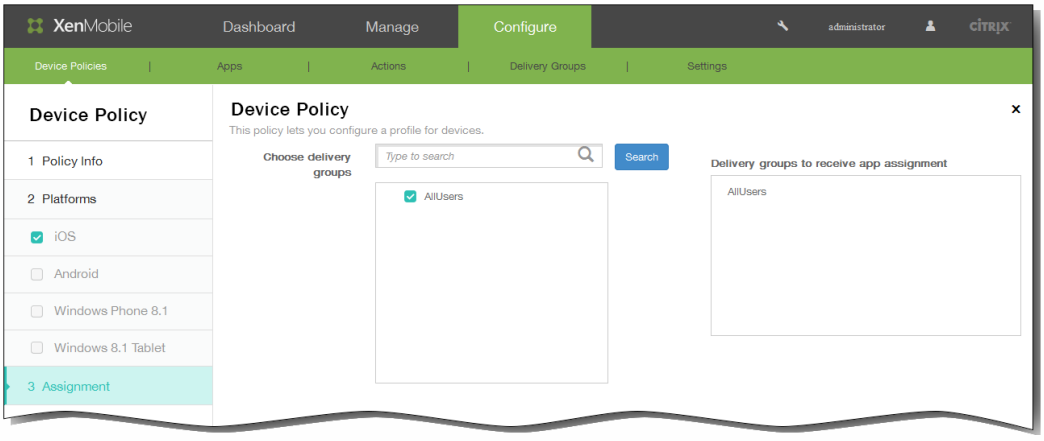


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



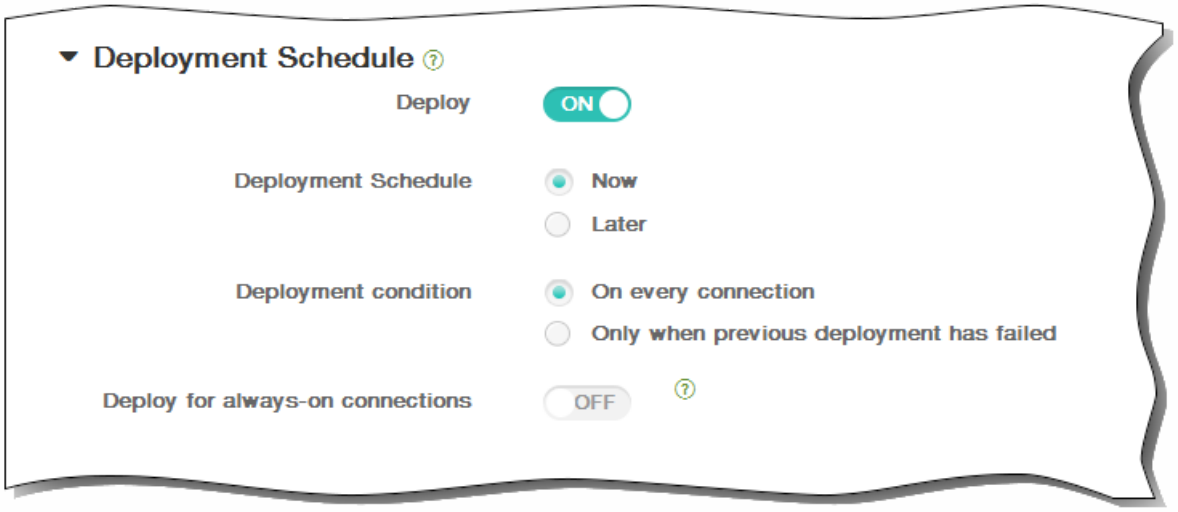
8. Haga clic en Next. Aparecerá la página de la siguiente plataforma o la página de la directiva Assignment.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

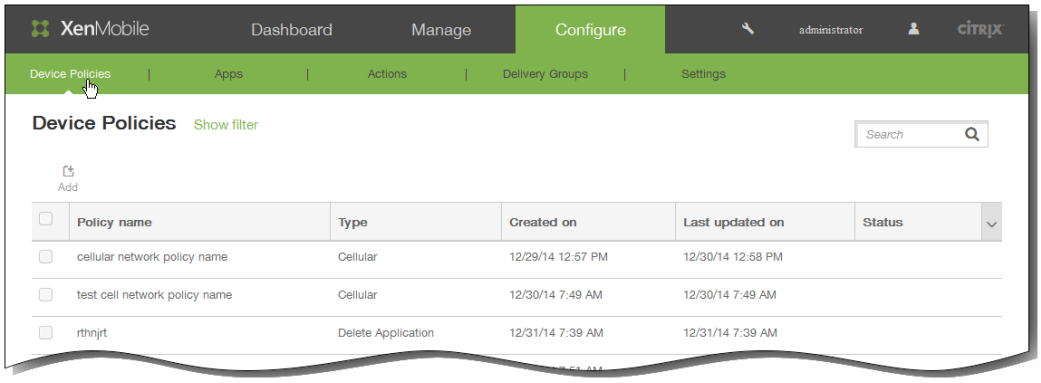
Para agregar una directiva de túneles de aplicaciones para Android

May 05, 2016

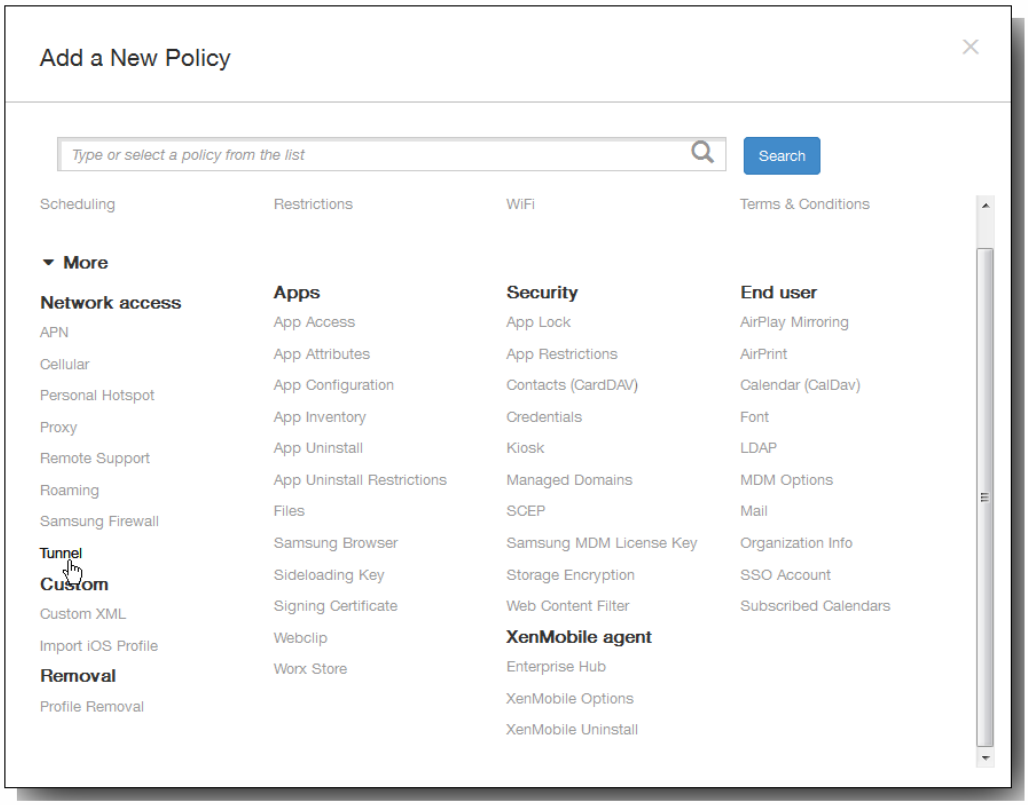
Los túneles de aplicaciones tienen por objetivo aumentar la continuidad del servicio y la fiabilidad de la transferencia de datos de las aplicaciones para móvil. Los túneles de aplicaciones se usan para definir parámetros de proxy entre el componente del cliente de cualquier aplicación del dispositivo móvil y el componente del servidor de aplicaciones. También puede usar túneles de aplicaciones con el objetivo de crear túneles de asistencia remota dirigidos a un dispositivo para ofrecer asistencia en administración.

Nota: Todo tráfico de aplicaciones enviado a través de un túnel definido en esta directiva se dirigirá a través de XenMobile antes de redirigirse al servidor que ejecuta la aplicación.

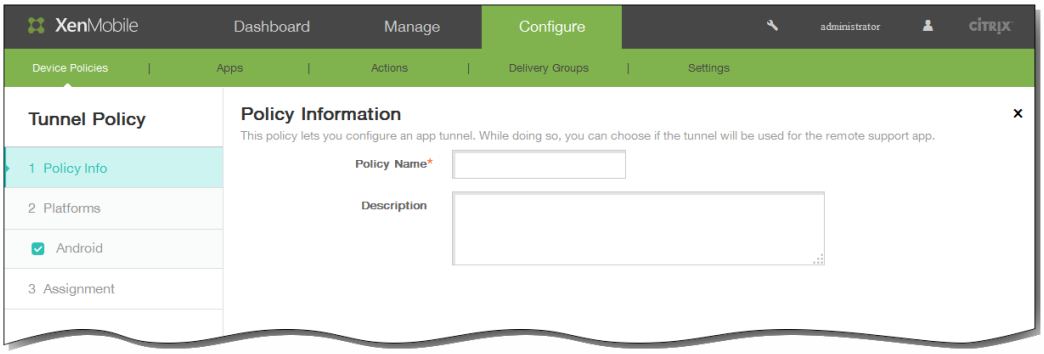
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



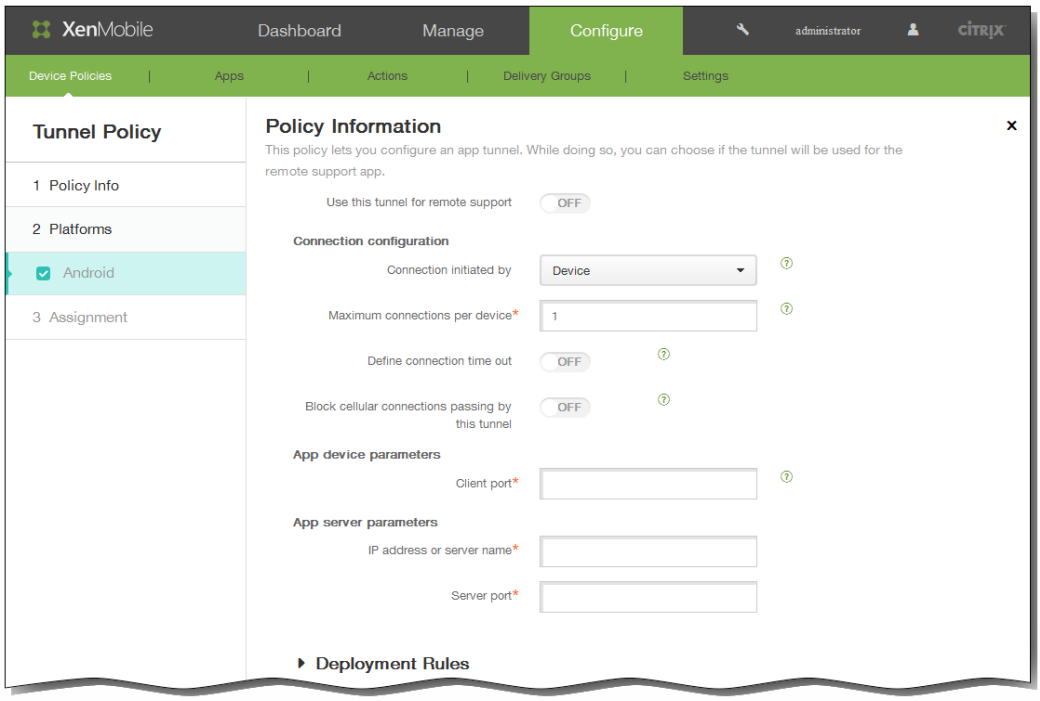
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en Network access, haga clic en Tunnel. Aparecerá la página Tunnel Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de la plataforma Android Policy.



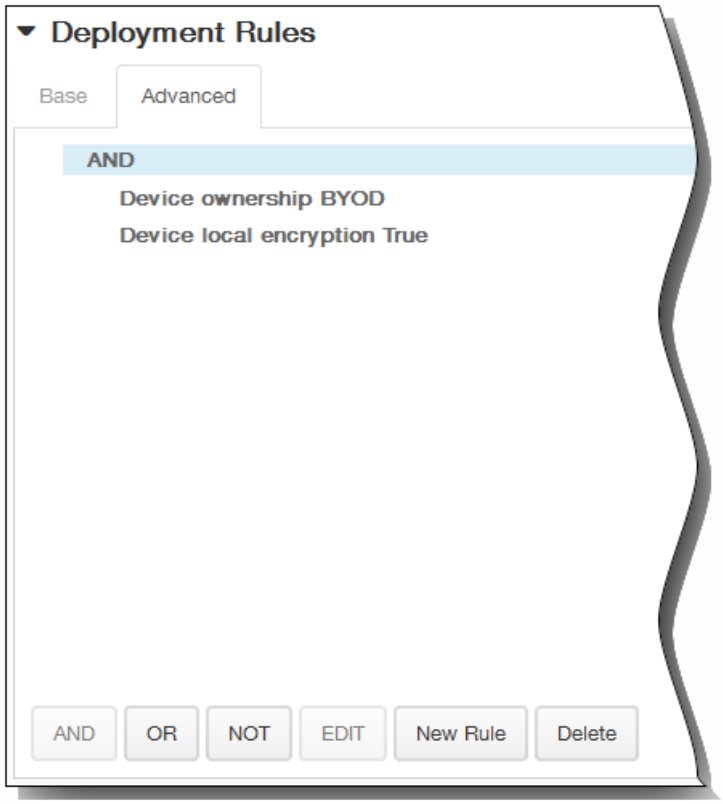
6. En Use this tunnel for remote support, seleccione si el túnel se usará para la asistencia remota.
   Nota: Los pasos de configuración son distintos según si se selecciona la asistencia remota o no.
   Si **no** selecciona la asistencia remota, lleve a cabo lo siguiente:
   1. Connection initiated by. Haga clic en Device o Server para indicar la fuente que inicia la conexión.
   2. Maximum connections per device. Escriba la cantidad de conexiones TCP simultáneas que puede establecer la aplicación. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
   3. Define connection time out. Seleccione si establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
   4. Connection time out. Si establece Define connection time out en On, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
   5. Block cellular connections passing by this tunnel. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en itinerancia.
      Nota: Las conexiones Wi-Fi y USB no se bloquearán.
   6. Client port. Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del puerto del servidor.
   7. IP address or server name. Escriba el nombre o la dirección IP del servidor de aplicaciones. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
   8. Server port. Escriba el número de puerto del servidor.

   Si **selecciona** la asistencia remota, lleve a cabo lo siguiente:
   1. Use this tunnel for remote support. Establecido en On.
   2. Define connection time out. Seleccione si establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
   3. Connection time out. Si establece Define connection time out en On, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
   4. Use SSL connection. Seleccione si usar una conexión SSL segura para este túnel.
   5. Block cellular connections passing by this tunnel. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en itinerancia.

Nota: Las conexiones Wi-Fi y USB no se bloquearán.

7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

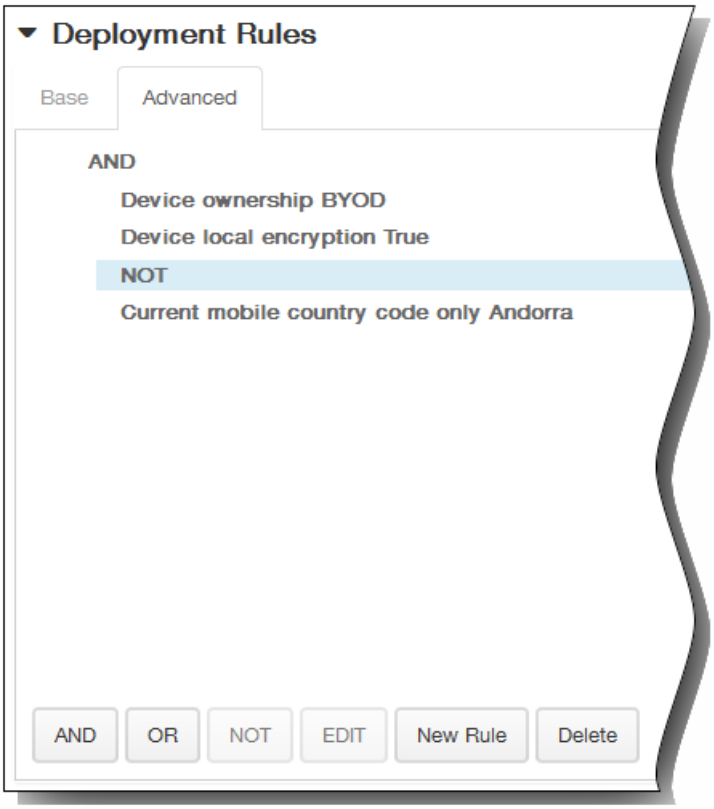
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



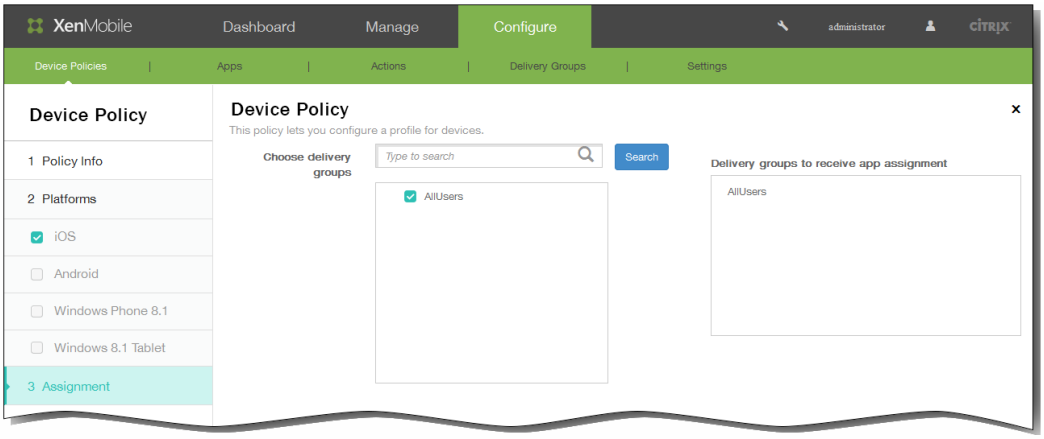
Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
       En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.

    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
       En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.

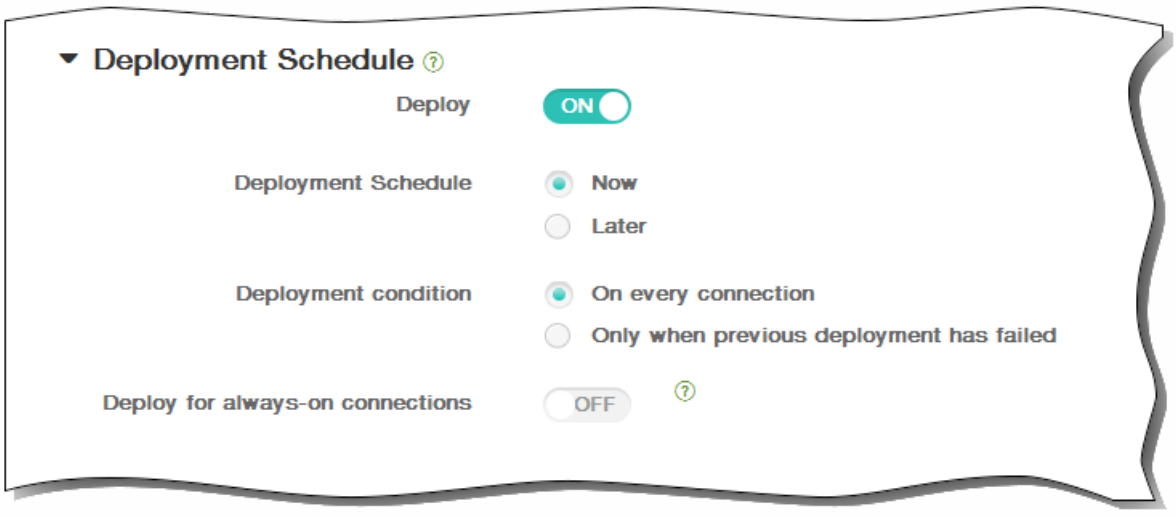


8. Haga clic en Next. Aparecerá la página de asignación Tunnel Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
    5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
       Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

    Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

Directivas de contenido XML personalizado

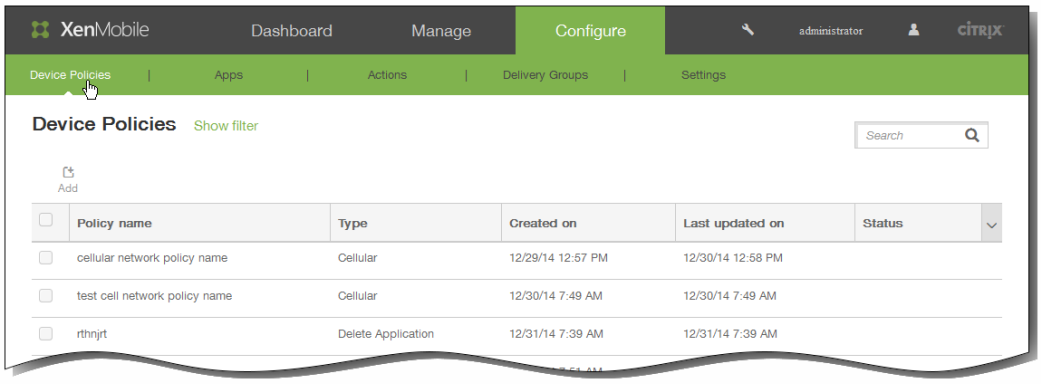
May 05, 2016

En XenMobile, puede crear sus propias directivas de contenido XML para personalizar las siguientes funciones en dispositivos Symbian y Windows Phone 8.1 y tabletas Windows 8.1:

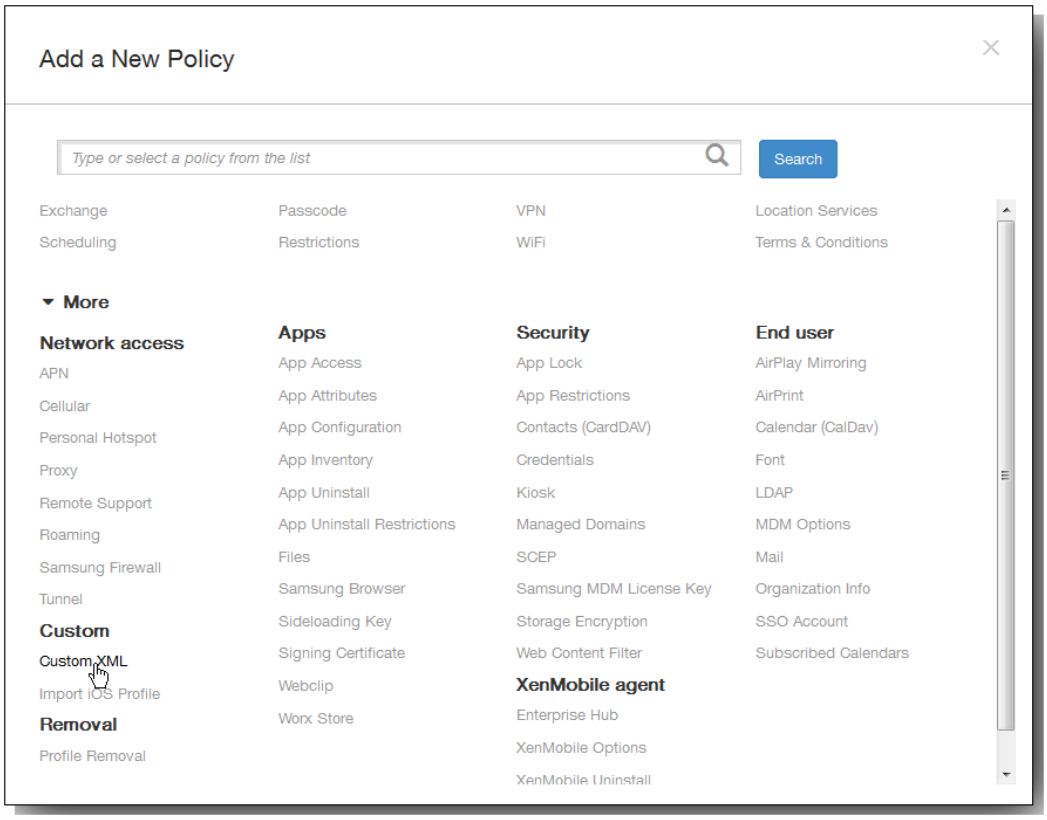
- El aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o inhabilitación de las funciones.
- La configuración de dispositivos, que incluye la capacidad para permitir a los usuarios cambiar la configuración y los parámetros de sus dispositivos.
- Las actualizaciones de software, que incluye la capacidad para proporcionar software nuevo o correcciones de errores que se vayan a cargar en el dispositivo, incluidas las aplicaciones y el software del sistema.
- Los errores de administración, que incluye la recepción de informes de error y de estado del dispositivo.

Puede crear su propia configuración de contenido XML mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows 8.1. Este apartado no abarca la creación de contenido XML personalizado con la API de OMA DM. Para obtener más información sobre el uso de la API de OMA DM, consulte OMA Device Management en el sitio de Microsoft Developer Network.

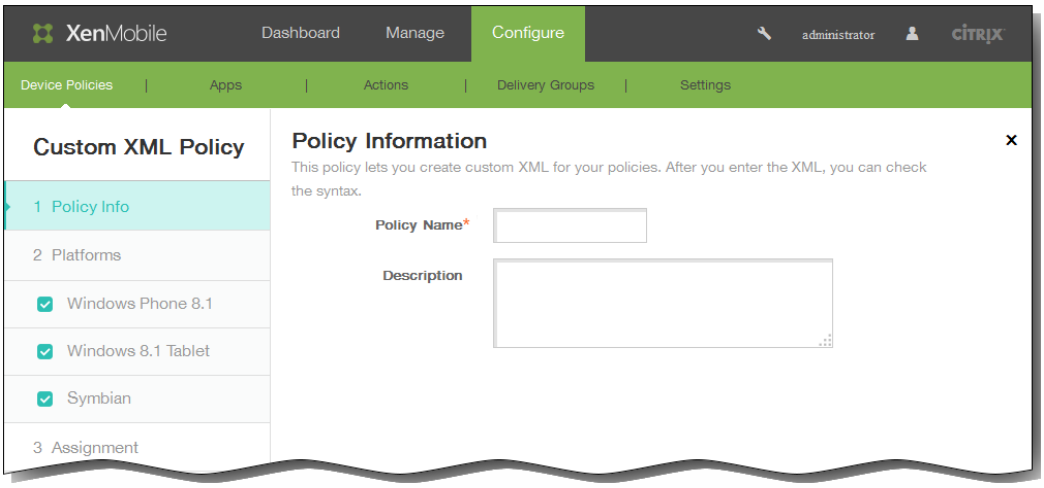
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



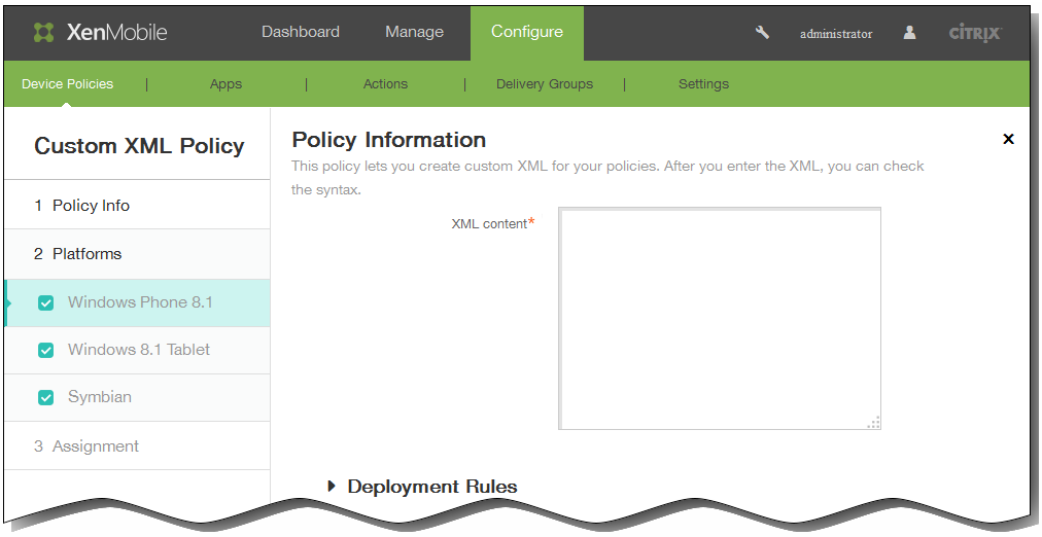
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.



3. Haga clic en More y, a continuación, en Custom, haga clic en Custom XML. Aparecerá la página de información Custom XML Policy.

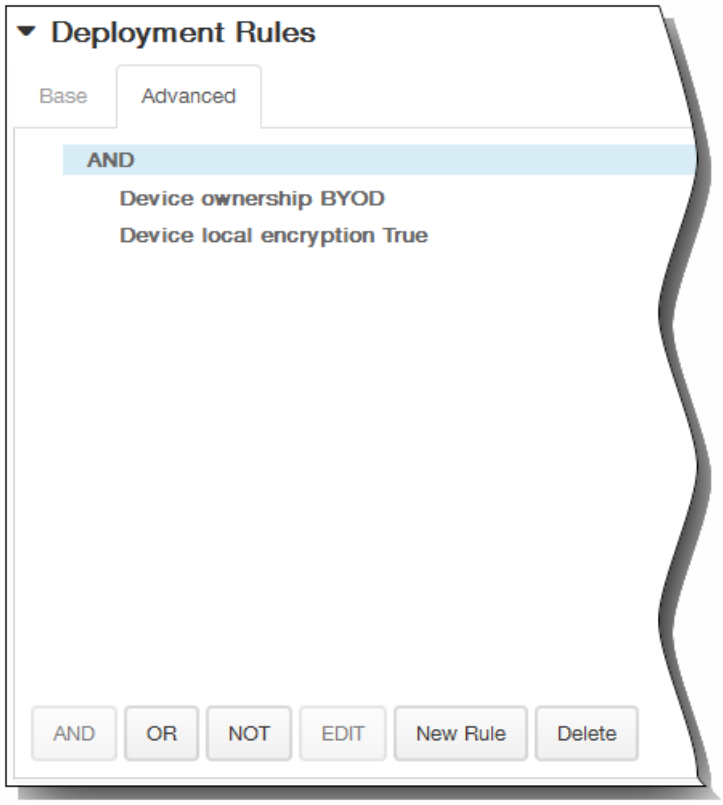


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Cuando aparezca la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma Windows Phone 8.1.



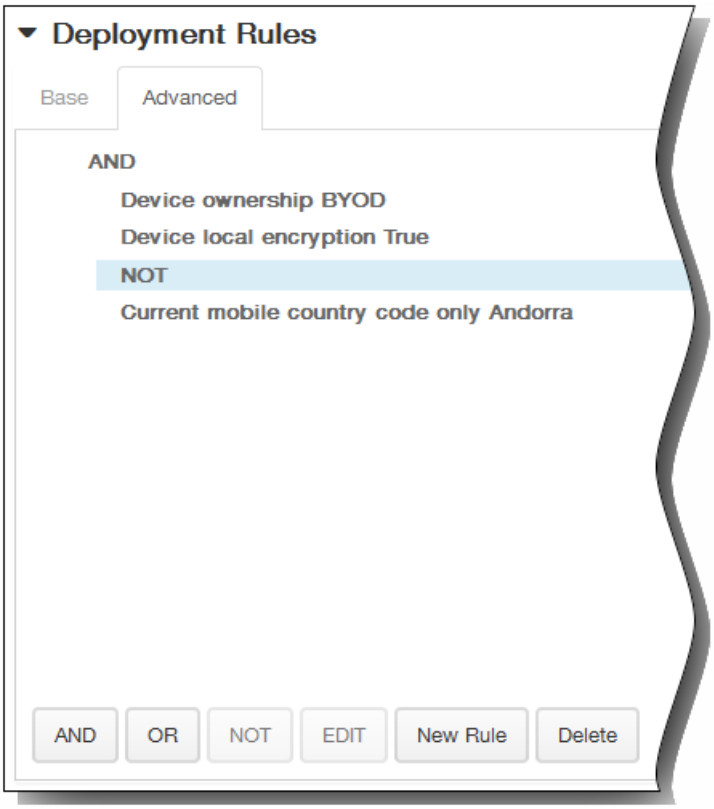
6. En Platforms, compruebe que solo están seleccionadas aquellas plataformas que quiere agregar.
7. En XML content, introduzca el código XML personalizado que se va a agregar a la directiva. Si el contenido es largo, puede cortar y pegar el código del archivo de origen.
8. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



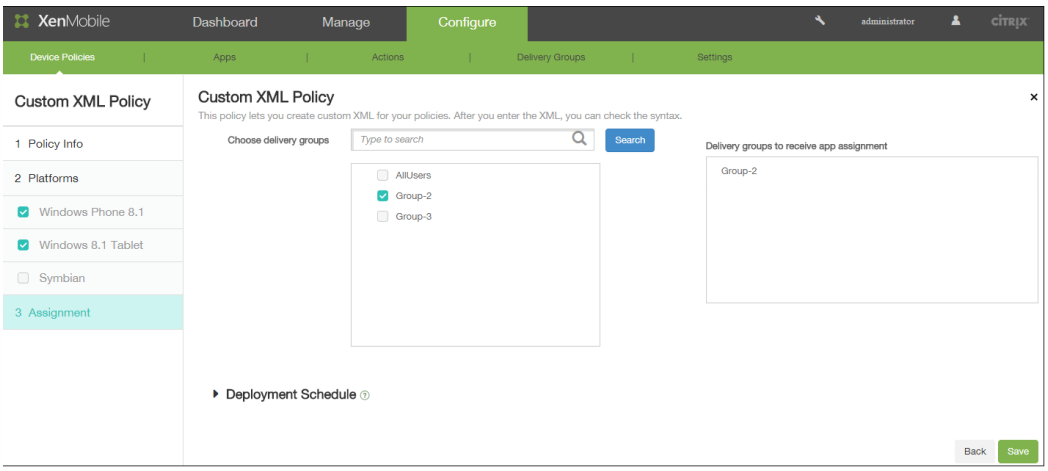
Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



9. Haga clic en Next. XenMobile comprueba la sintaxis del contenido XML. Los errores de sintaxis aparecerán bajo el cuadro del contenido. Antes de continuar, debe corregir los errores que haya.
   Si no hay errores de sintaxis, aparecerá la página de asignación Custom XML Policy.

10. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.

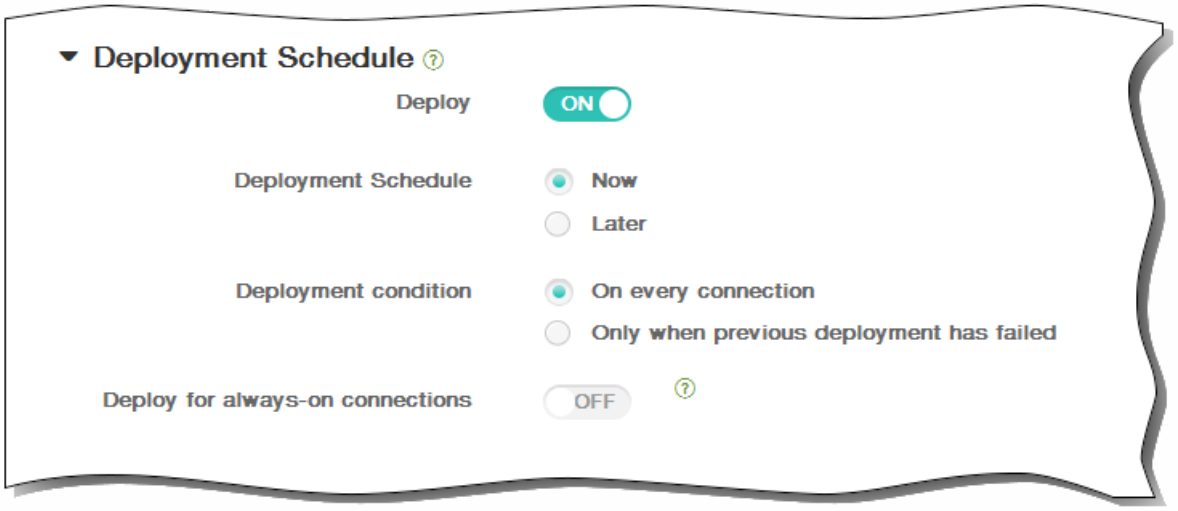


11. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la

implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas.



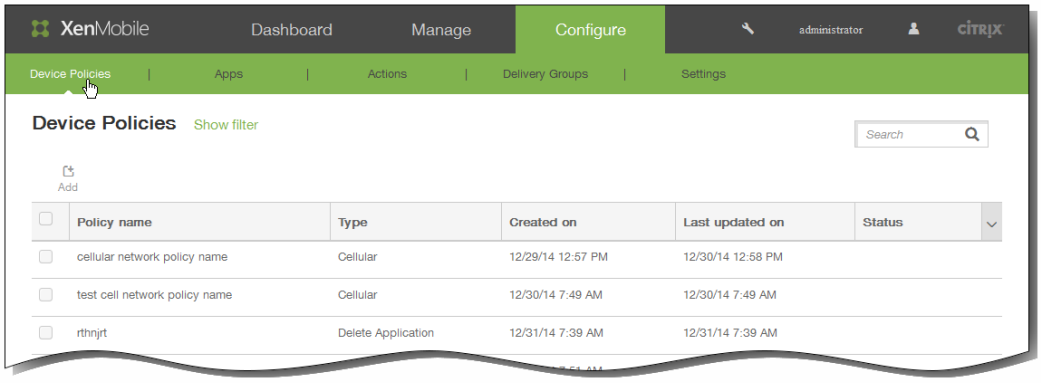
12. Haga clic en Save para guardar la directiva.

Directivas de dispositivo para desinstalación de aplicaciones

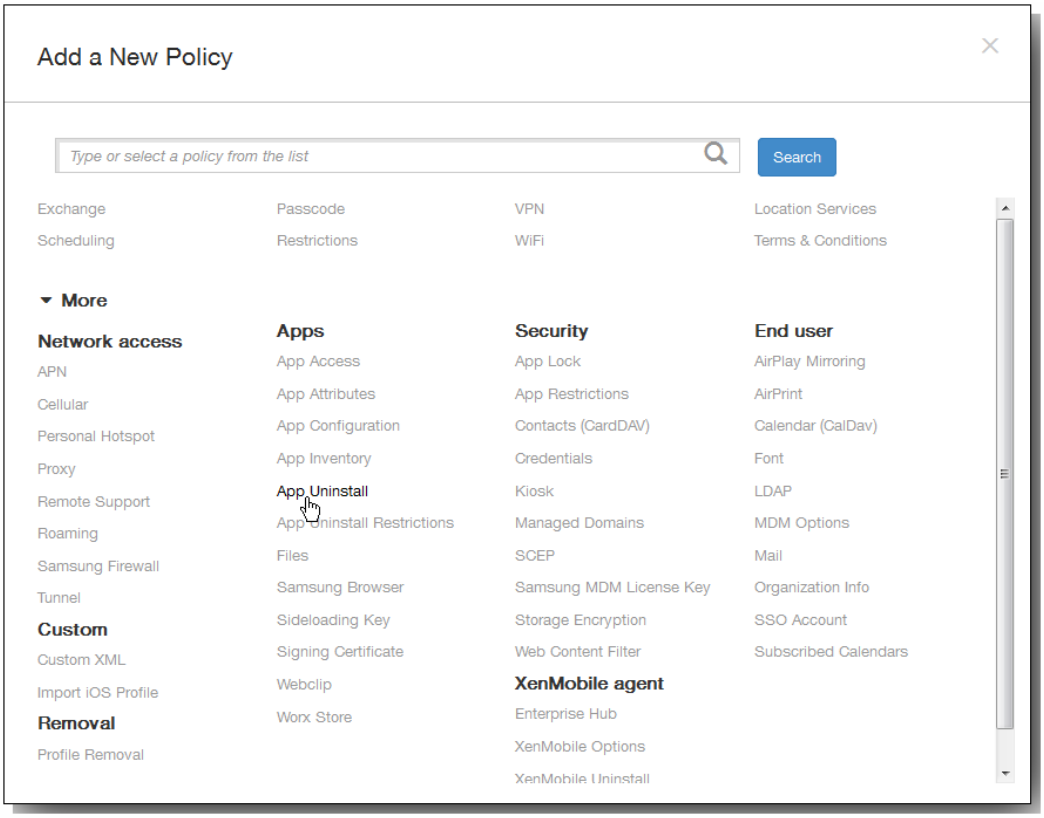
May 05, 2016

Puede crear una directiva de desinstalación de aplicaciones para las plataformas iOS, Android, Samsung KNOX y Windows 8.1 Tablet. Una directiva de desinstalación de aplicaciones permite quitar aplicaciones de los dispositivos de usuarios por las razones pertinentes. Es posible que ya no quiera respaldar ciertas aplicaciones o que la empresa quiera sustituir las aplicaciones existentes por aplicaciones similares provenientes de otros proveedores, entre varios motivos. Las aplicaciones se quitan cuando esta directiva se implementa en los dispositivos de los usuarios. A excepción de los dispositivos Samsung KNOX, los usuarios reciben una solicitud para desinstalar la aplicación; los usuarios de dispositivos Samsung KNOX no recibirán ninguna solicitud para desinstalar la aplicación.

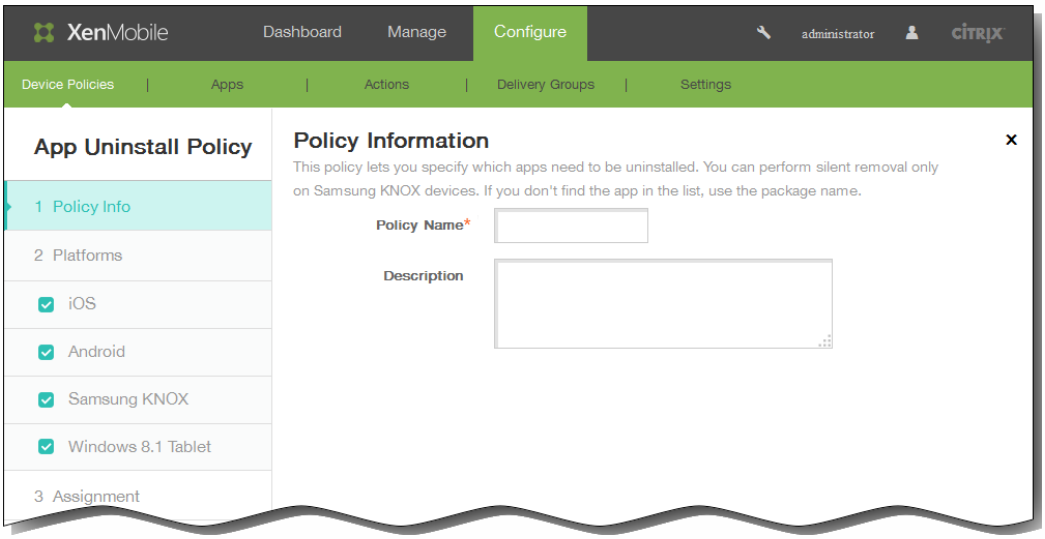
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies. En la página Device Policies, haga clic en Add.



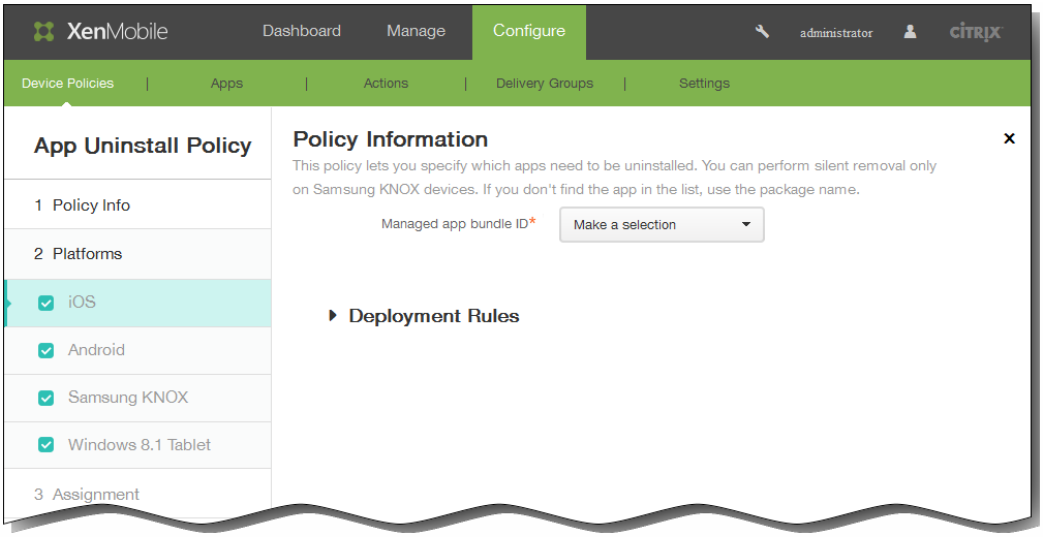
2. En el cuadro de diálogo Add a New Policy, haga clic en More y, a continuación, en Apps, haga clic en App Uninstall.



3. En el panel de información App Uninstall Policy, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
   3. Haga clic en Siguiente.

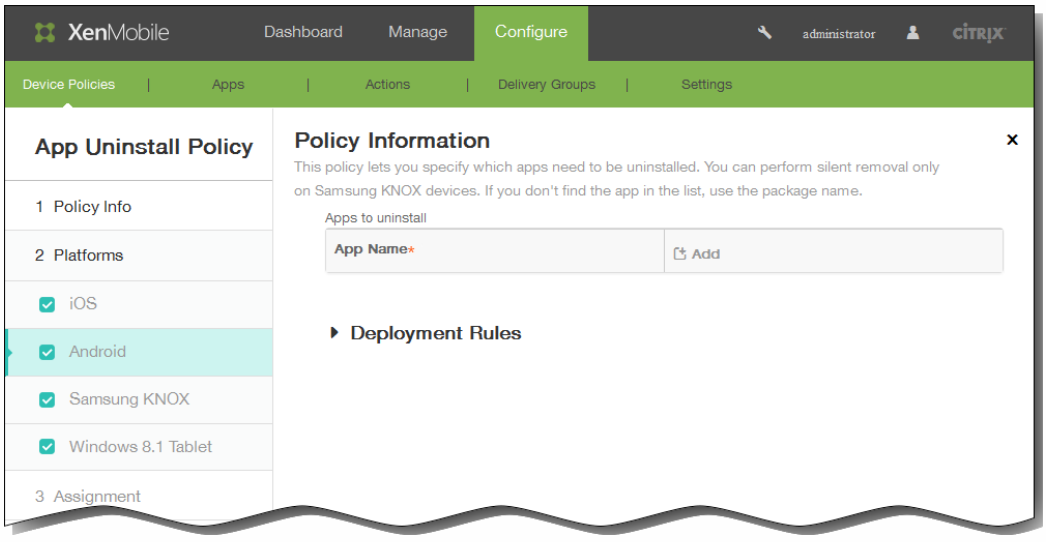


4. Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS. En Platforms, seleccione la plataforma o las plataformas que quiere agregar y anule la selección de las que no.



5. Configure los siguientes parámetros según cada una de las plataformas seleccionadas.
   1. Si ha seleccionado iOS, en la lista Managed app bundle ID, haga clic en una aplicación existente, o bien haga clic en Add new.

      Nota: Si no hay ninguna aplicación configurada para esta plataforma, la lista estará vacía y deberá agregar una nueva aplicación.
      Cuando haga clic en Add, aparecerá un campo donde podrá escribir un nombre de aplicación.
   2. Si ha elegido Android, Samsung KNOX o Windows 8.1 Tablet:



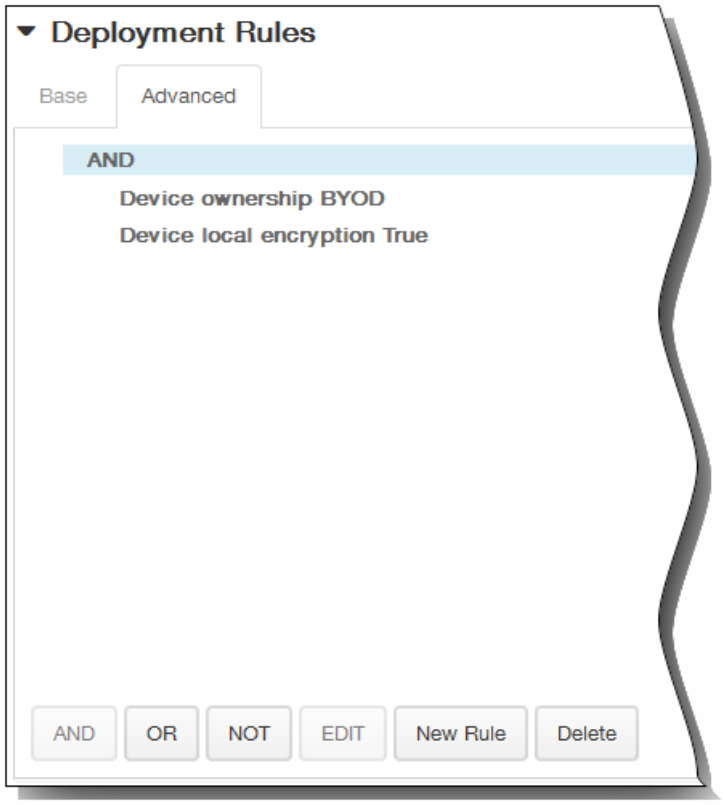
   En Apps to uninstall, haga clic en Add y lleve a cabo lo siguiente:

   1. App name. En la lista, haga clic en una aplicación existente, o bien haga clic en Add new para introducir un nuevo nombre de aplicación.
      Nota: Si no hay ninguna aplicación configurada para esta plataforma, la lista estará vacía y deberá agregar aplicaciones nuevas.
   2. Haga clic en Add para agregar la aplicación, o bien haga clic en Cancel para no agregarla.

3. Repita los pasos de i. y ii. para cada aplicación que quiera agregar a la directiva de desinstalación.
   Nota: Para eliminar una aplicación existente de la directiva de desinstalación, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo. Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

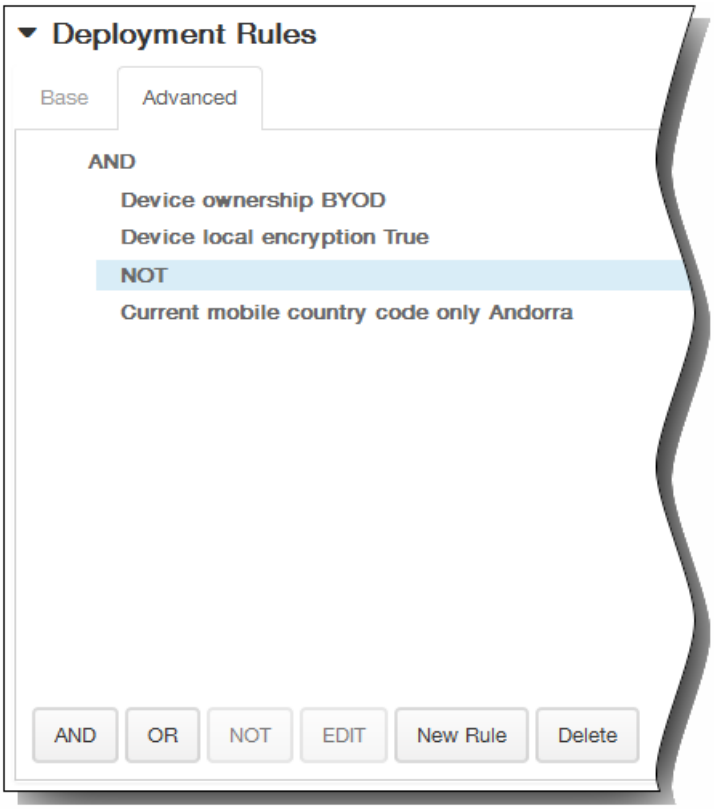
6. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

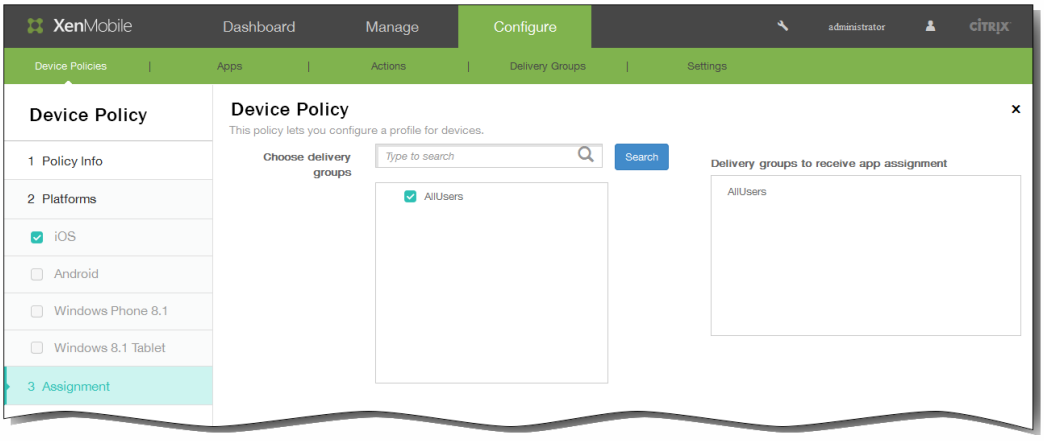


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



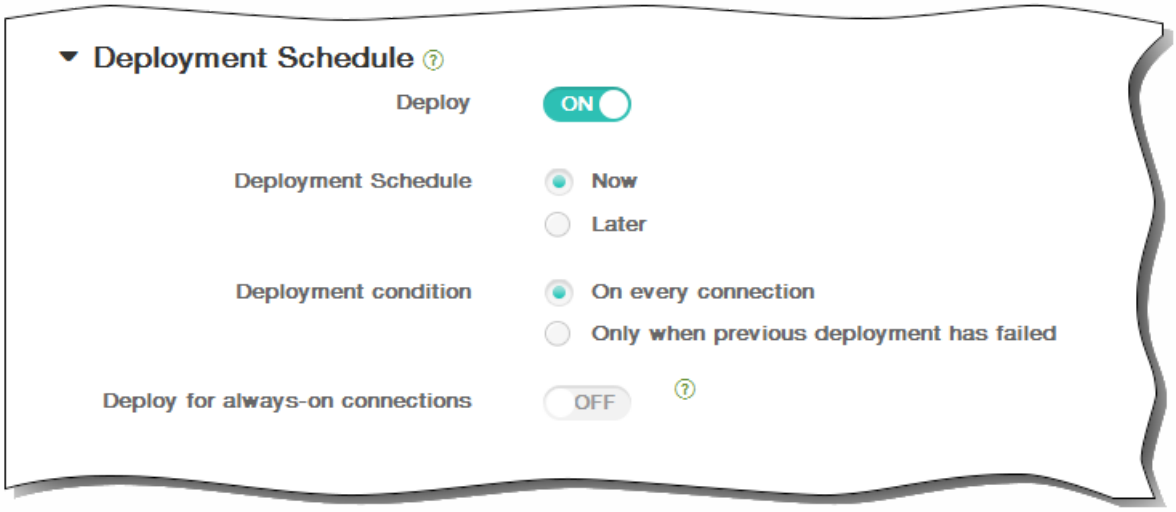
7. Haga clic en Next. Aparecerá la página de asignación App Uninstall Policy.
8. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



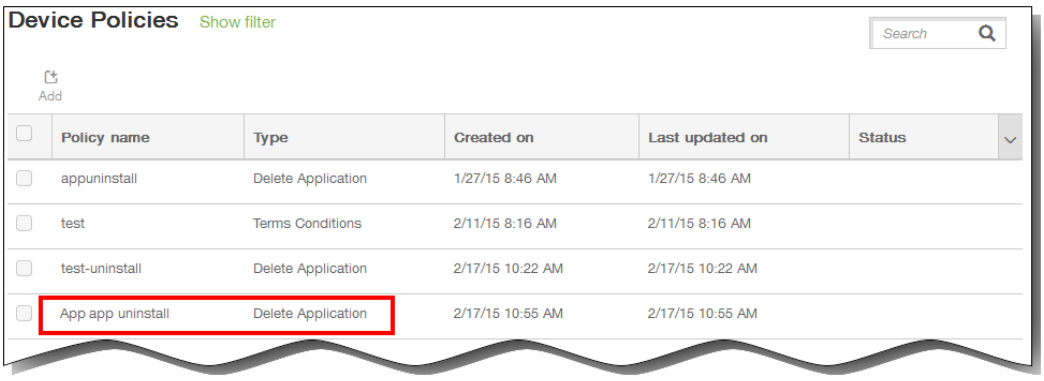
9. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



10. Haga clic en Save para guardar la directiva. En la página Device Policies, en la columna Type, la directiva que ha agregado aparecerá clasificada como "Delete Application".

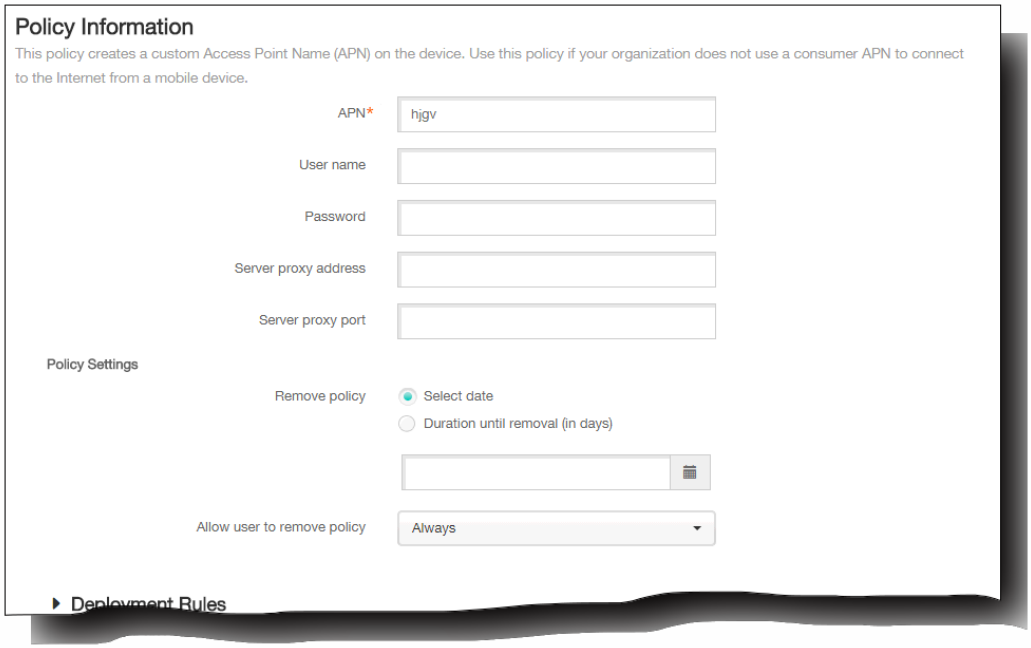


Para agregar una directiva de nombres APN

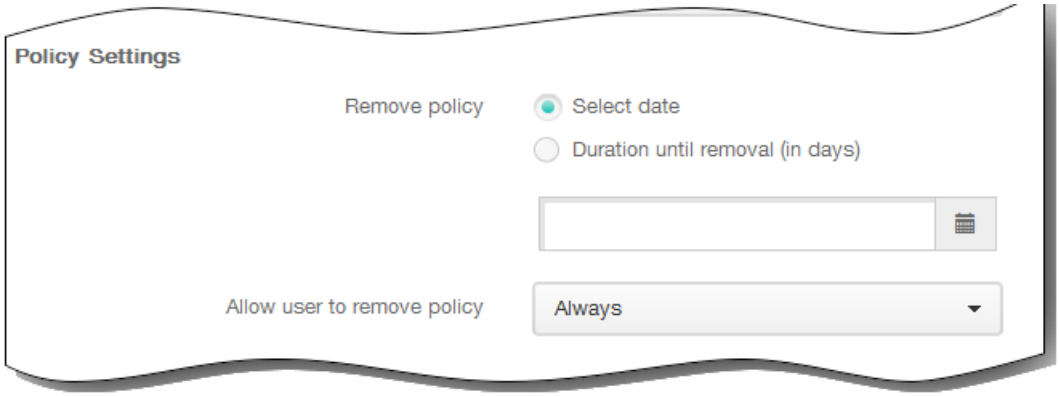
May 05, 2016

Esta directiva permite configurar un nombre de punto de acceso (APN) personalizado en dispositivos iOS, Android o Samsung KNOX. Una directiva de nombres APN determina la configuración utilizada para conectar sus dispositivos al servicio GPRS de un operador concreto. Esta configuración ya está definida en la mayoría de los teléfonos más recientes.

1. En la consola de XenMobile, haga clic en Configure > Device Policies > Add.
2. En la página Add a New Policy, haga clic en More y en Network Access, haga clic en APN.
3. Seleccione las plataformas a incluir en la directiva. Las páginas de configuración referentes a la plataforma seleccionada aparecerán en el paso 5.
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información referente a la primera plataforma.
6. Si ha seleccionado la plataforma de iOS, en la página de información de la plataforma de iOS, haga lo siguiente:

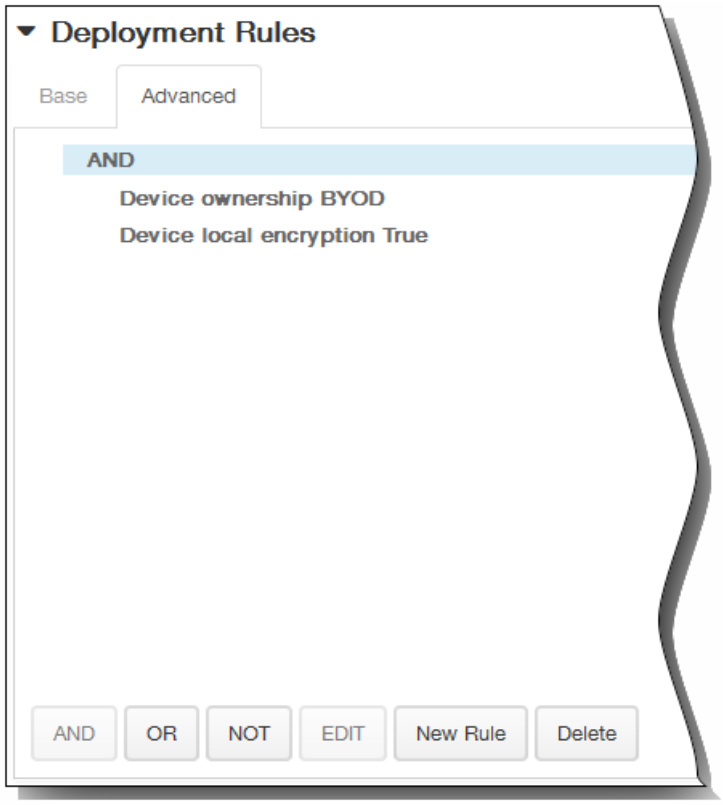


   1. APN. Escriba el nombre del punto de acceso.
   2. User name. Esta cadena especifica el nombre de usuario para este nombre APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.
   3. Password. La contraseña de usuario para este nombre APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.
   4. Server proxy address. La dirección IP o la URL del proxy de APN.
   5. Server proxy port. El número de puerto para el proxy de APN.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



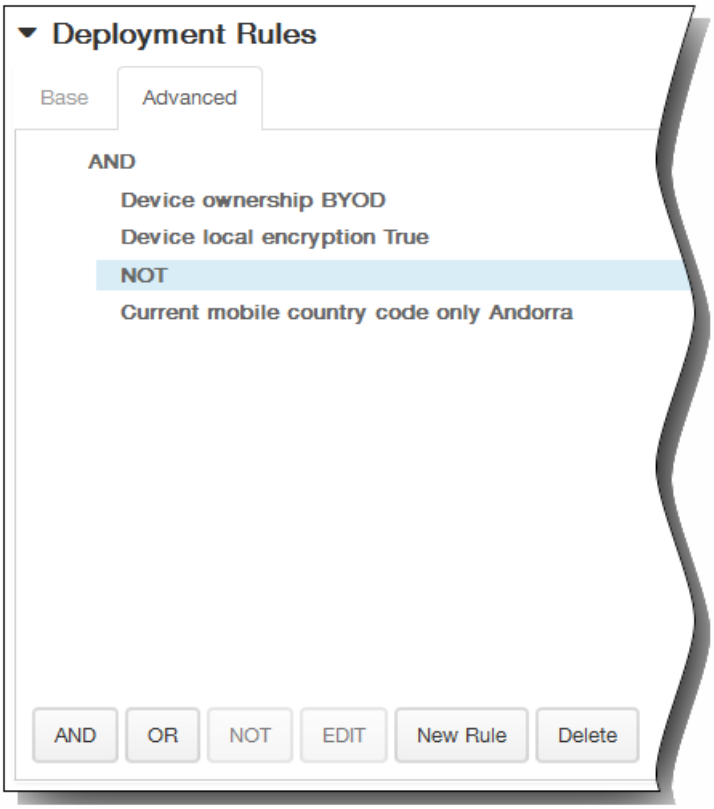
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

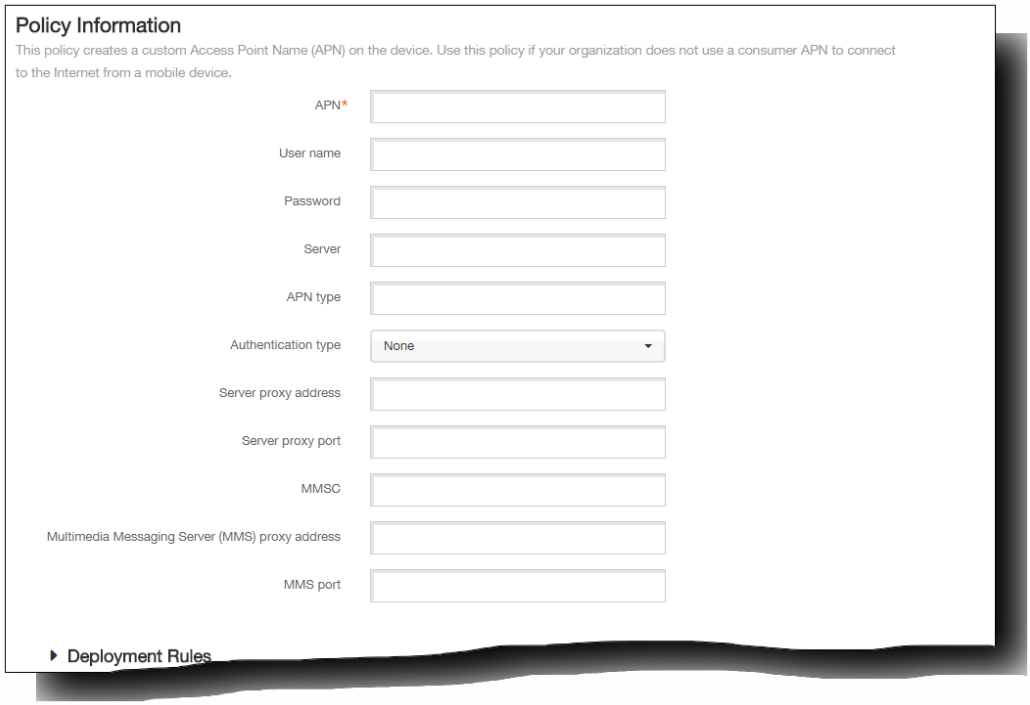


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



12. Si ha seleccionado las plataformas Android o Samsung KNOX, en la página de información de la plataforma, lleve a cabo lo siguiente:

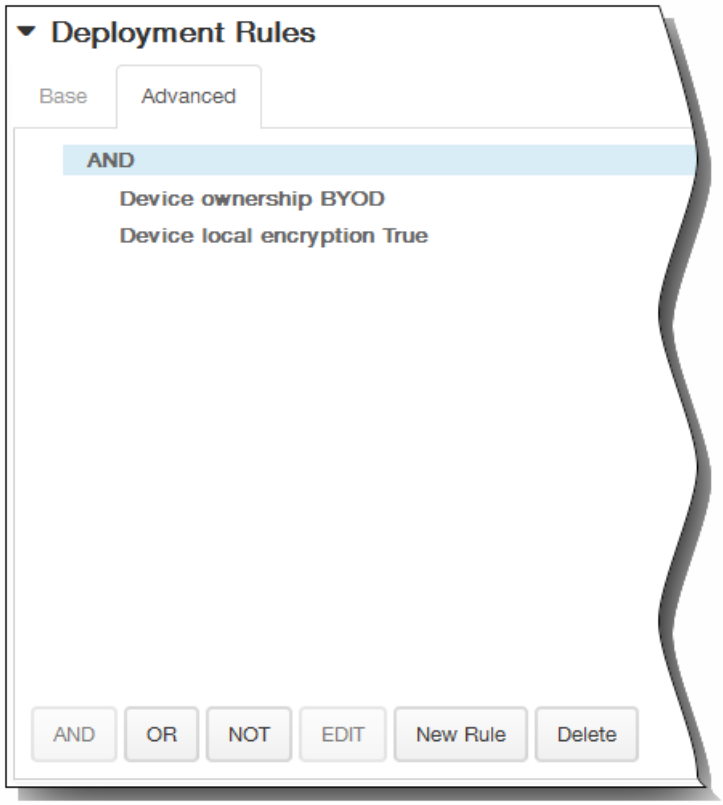


1. APN. Escriba el nombre del punto de acceso.

2. User name. Esta cadena especifica el nombre de usuario para este nombre APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.
3. Password. La contraseña de usuario para este nombre APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.
4. Server. Este parámetro es anterior a los smartphones y normalmente está vacío. Hace referencia a un servidor de puerta de enlace para protocolos de aplicación inalámbrica (WAP), destinado a teléfonos que no pueden acceder a sitios Web estándar o mostrarlos.
5. APN type. Este parámetro debe coincidir con el uso previsto del operador para el punto de acceso. Es una cadena separada por comas que contiene especificadores del servicio APN, y debe coincidir con las definiciones publicadas del operador inalámbrico. Por ejemplo:
   - *. Todo el tráfico de red pasa por este punto de acceso.
   - mms. El tráfico multimedia pasa por este punto de acceso.
   - default. Todo el tráfico de red, incluido el multimedia, pasa por este punto de acceso.
   - supl. El protocolo Secure User Plane Location está asociado al GPS asistido.
   - dun. El acceso telefónico a redes está obsoleto y no debe usarse con frecuencia.
   - hipri. Redes de alta prioridad.
   - fota. El firmware over-the-air se usa para recibir actualizaciones de firmware.
6. Authentication type. Debe contener PAP, CHAP, o bien PAP or CHAP. El valor predeterminado es None.
7. Server proxy address. La dirección IP o la URL del proxy de APN.
8. Server proxy port. El número de puerto para el proxy de APN.
9. MMSC. Se trata del servidor del servicio de mensajería multimedia para el tráfico MMS. Los mensajes MMS sustituyeron a los mensajes SMS para enviar mensajes más largos con contenido multimedia, como imágenes o vídeos. Estos servidores requieren protocolos específicos (como MM1 y similares hasta MM11).
10. Multimedia Messaging Server (MMS) proxy address. Se trata del servidor proxy HTTP para el tráfico MMS.
11. MMS port. El puerto utilizado por el proxy de MMS.

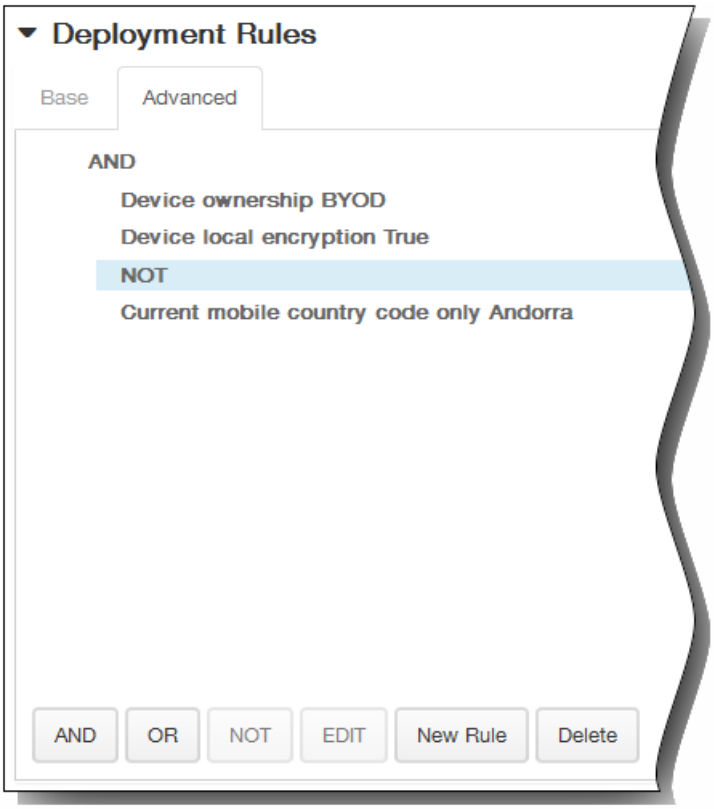
13. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

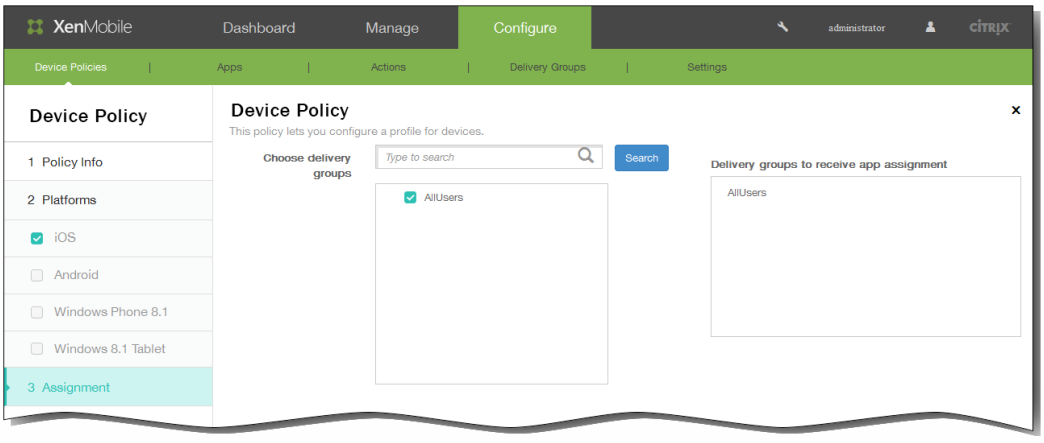


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



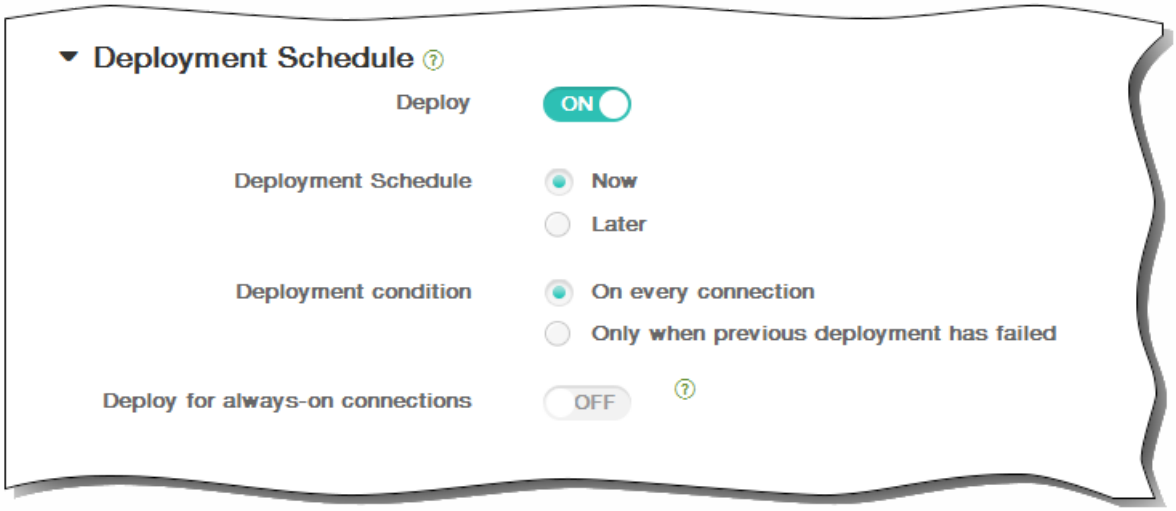
14. Si ha seleccionado ambas plataformas, Android y Samsung KNOX, repita el paso 8 para completar la página de información de la plataforma Samsung KNOX y, a continuación, haga clic en Next. Aparecerá la página APN Policy Assignment.
15. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



16. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.

3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



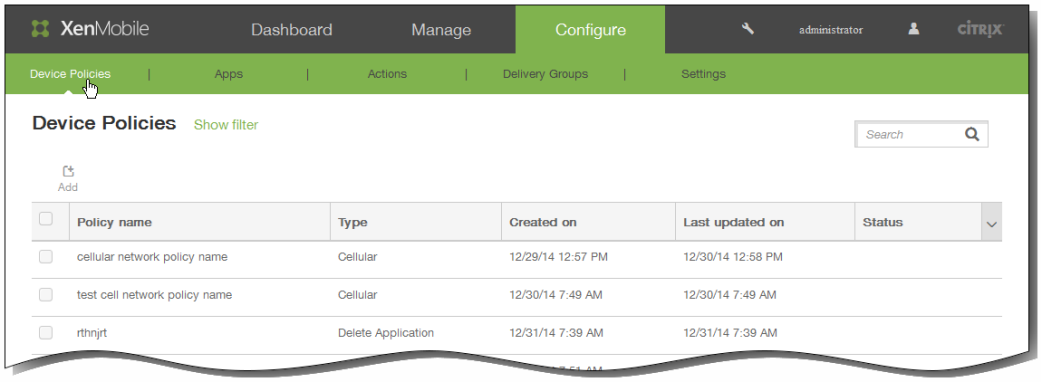
17. Haga clic en Save para guardar la directiva.

Para agregar una directiva de redes de telefonía móvil para iOS

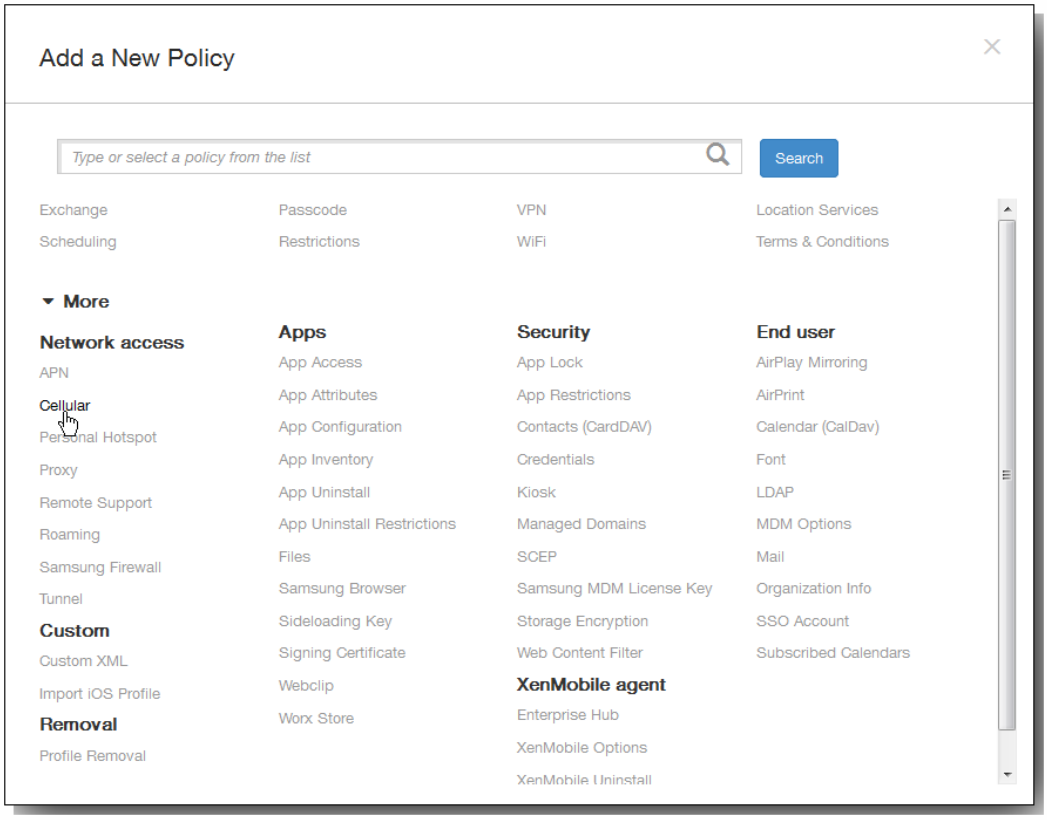
May 05, 2016

Esta directiva permite configurar parámetros de redes de telefonía móvil en un dispositivo iOS.

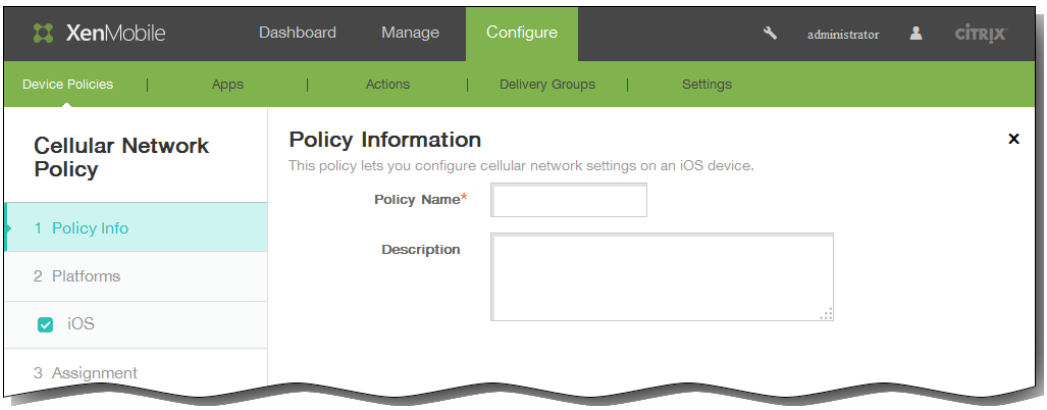
1. En la consola de XenMobile, haga clic en Configure > Device Policies.



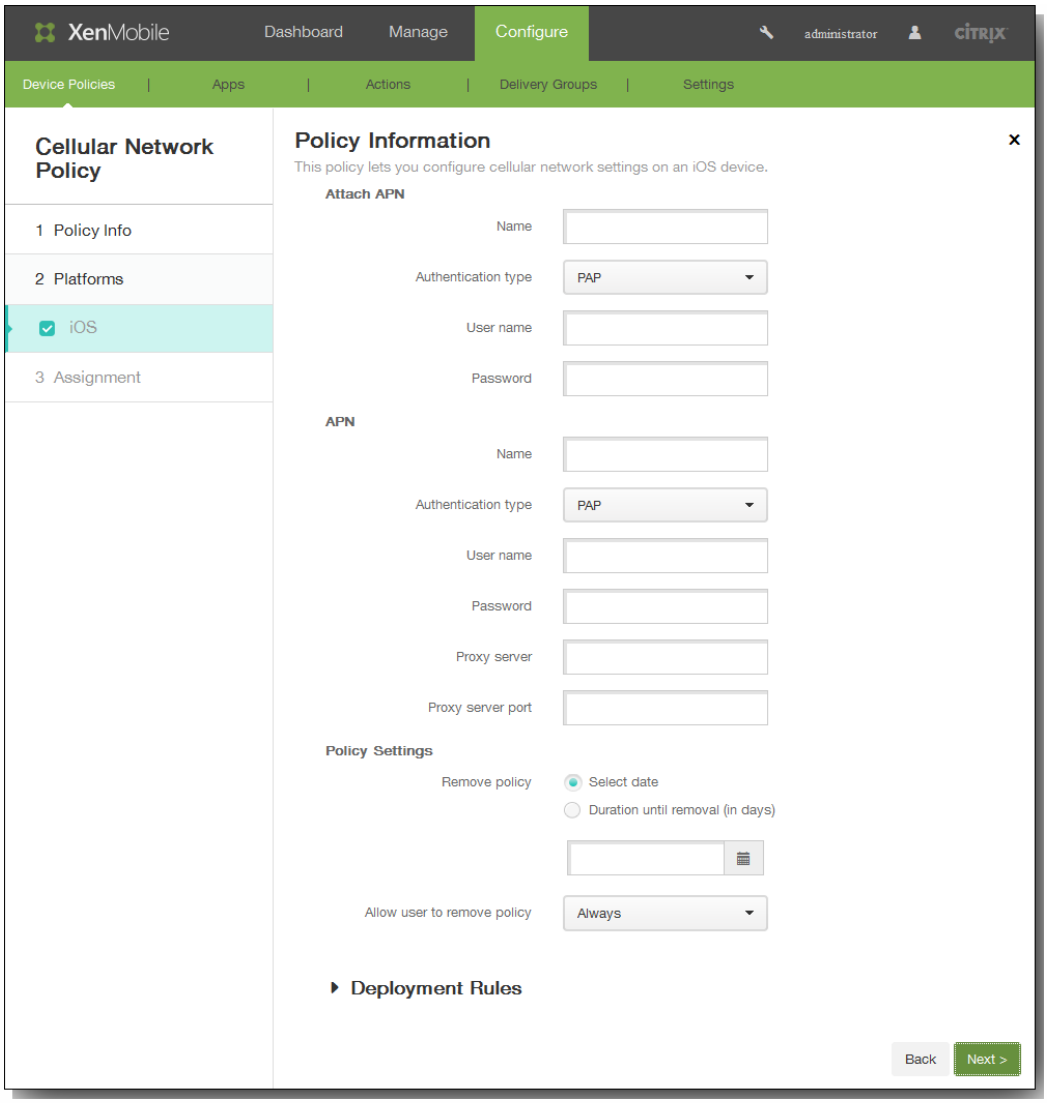
2. Haga clic en Agregar.
   Aparecerá la página Add a New Policy.



3. En la página Add a New Policy, haga clic en More y, en Network Access, haga clic en Cellular. Aparecerá la página de información Cellular Network Policy.

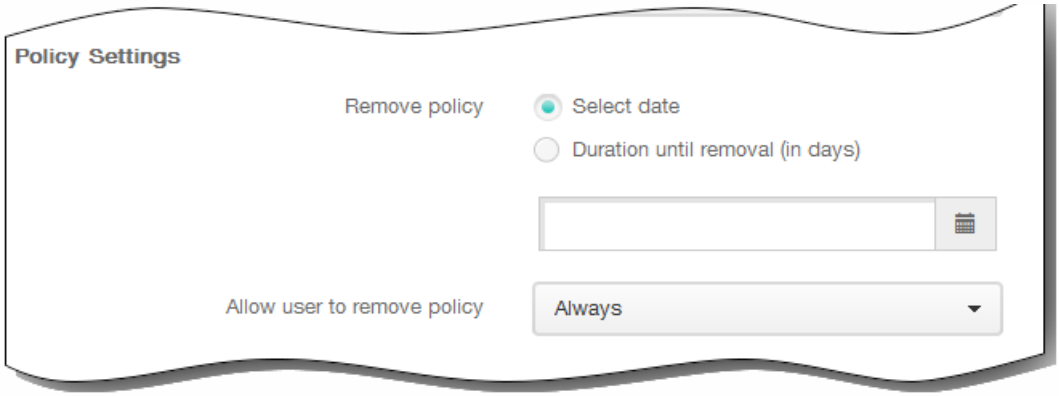


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.

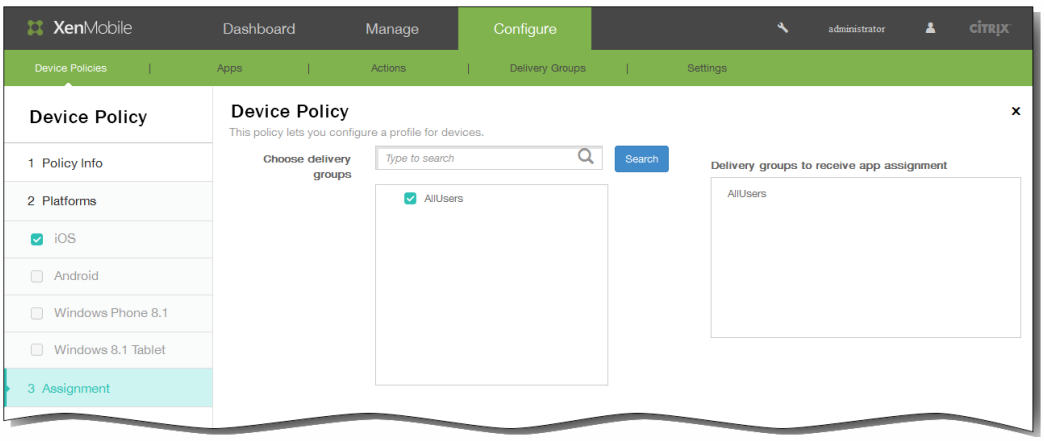


6. En la página iOS Platform Information, escriba la información siguiente: En **Attach APN**:
   1. Name. Escriba un nombre para esta configuración.
   2. Authentication type. En la lista, haga clic en el Protocolo de autenticación por desafío mutuo (CHAP) o el Protocolo de autenticación por contraseña (PAP). El valor predeterminado es PAP.
   3. User name. Escriba el nombre de usuario que se usará para la autenticación.
   4. Password. Escriba una contraseña para la autenticación.

   En **APN**:
   1. Name. Escriba un nombre para la configuración del nombre de punto de acceso (APN).
   2. Authentication type. En la lista, haga clic en CHAP o PAP. El valor predeterminado es PAP.
   3. User name. Escriba el nombre de usuario que se usará para la autenticación.
   4. Password. Escriba una contraseña para la autenticación.
   5. Proxy server. Escriba la dirección de red del servidor proxy.
   6. Proxy server port. Escriba el puerto del servidor proxy.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

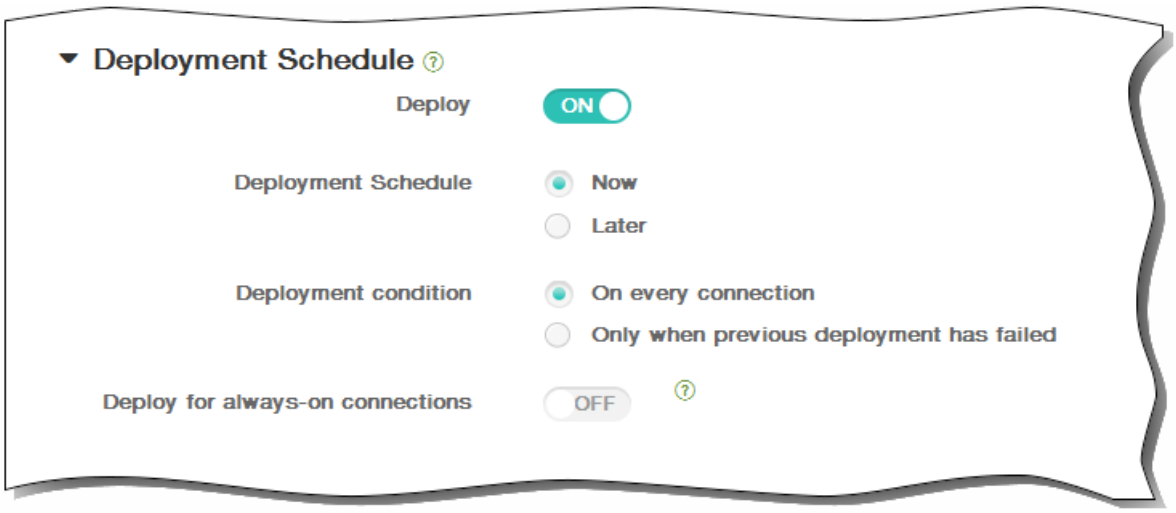


11. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



12. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
    5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
       Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

    Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



13. Haga clic en Save para guardar la directiva.

Para agregar una directiva Enterprise Hub para dispositivos Windows Phone 8.1

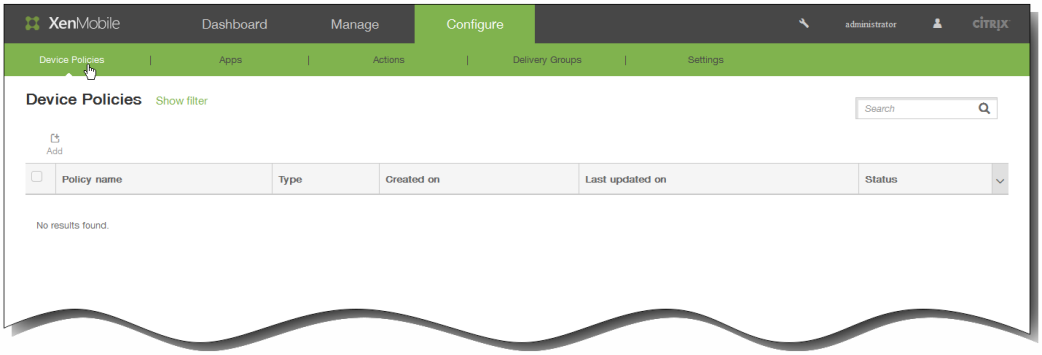
May 05, 2016

Una directiva Enterprise Hub para dispositivos Windows Phone 8.1 permite distribuir aplicaciones a través del almacén Enterprise Hub de la empresa.

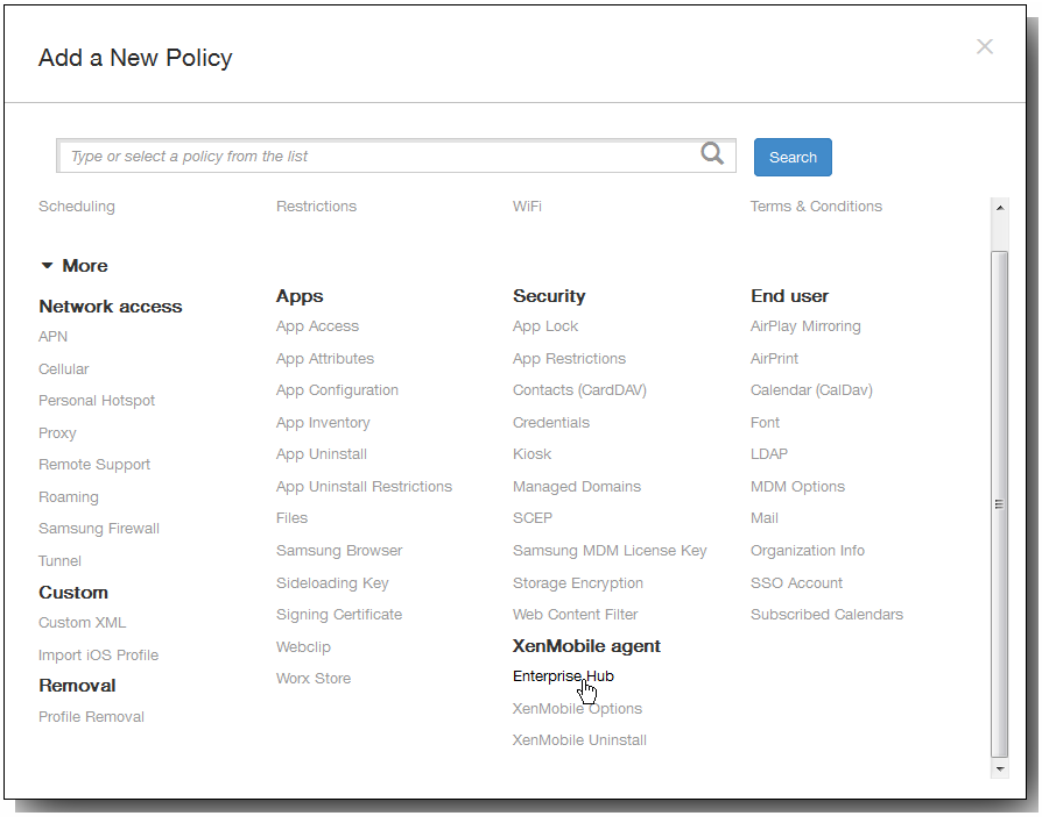
Antes de crear la directiva, necesita lo siguiente:

- Un certificado de firma AET (.aetx) de Symantec
- La aplicación Citrix Company Hub firmada mediante la herramienta de firma de aplicaciones de Microsoft (XapSignTool.exe)

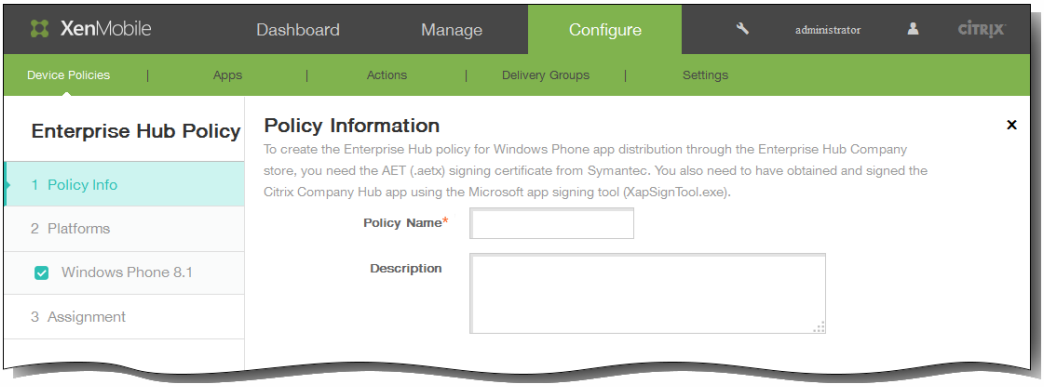
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



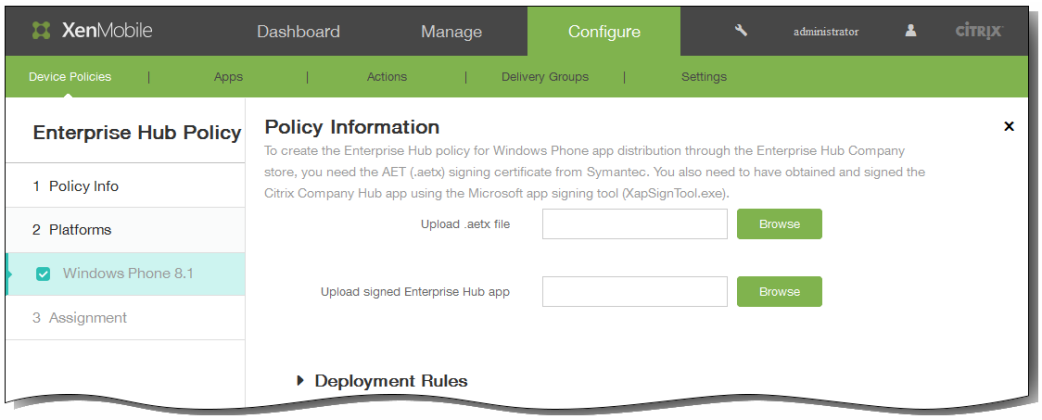
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en XenMobile agent, haga clic en Enterprise Hub. Aparecerá la página Enterprise Hub Policy.

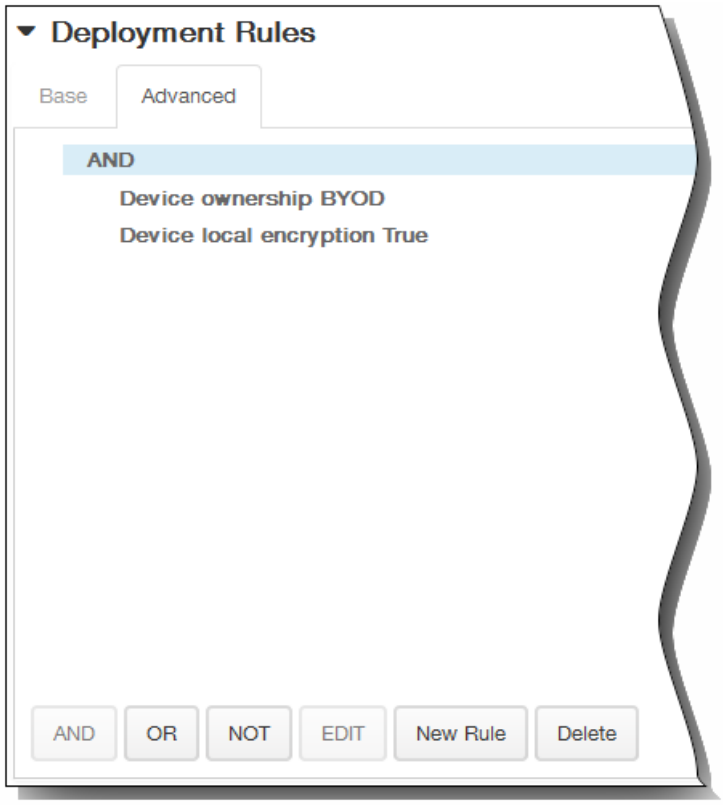


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, proporcione una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de la plataforma Windows Phone 8.1.



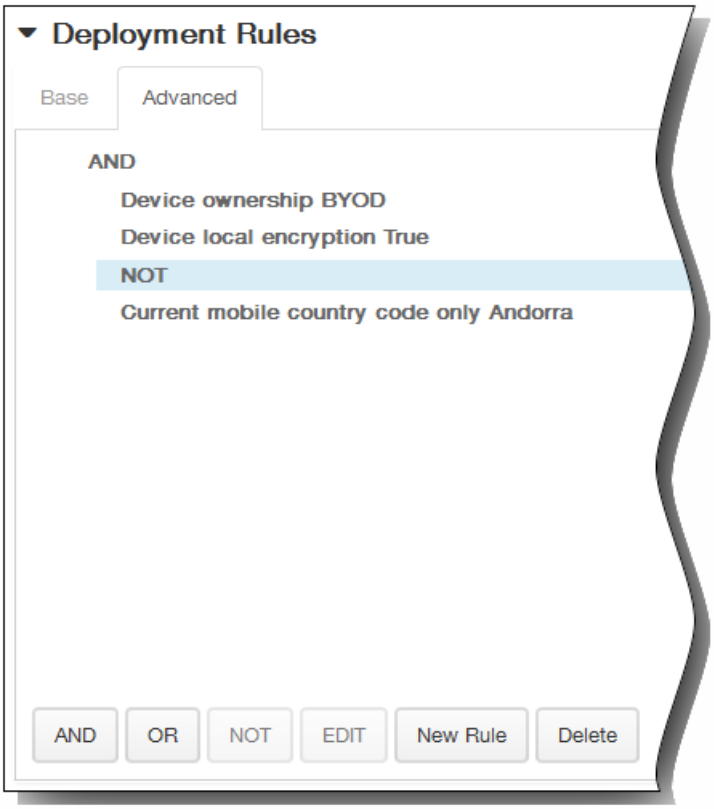
6. Configure los siguientes parámetros:
   1. Upload .aetx file. Vaya a la ubicación del archivo AETX y selecciónelo.
   2. Upload signed Enterprise Hub app. Vaya la ubicación de la aplicación Enterprise Hub y selecciónela.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
      2. Haga clic en New Rule para definir las condiciones.
      3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
      4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
   2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

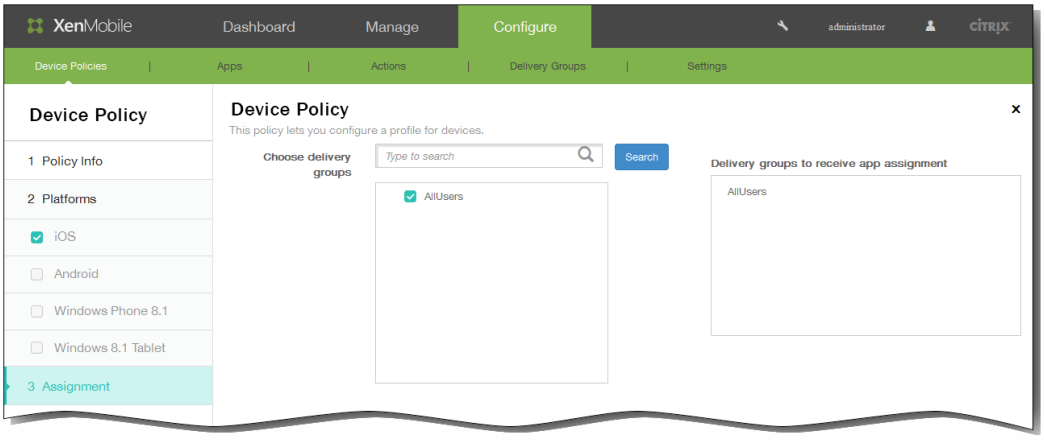


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



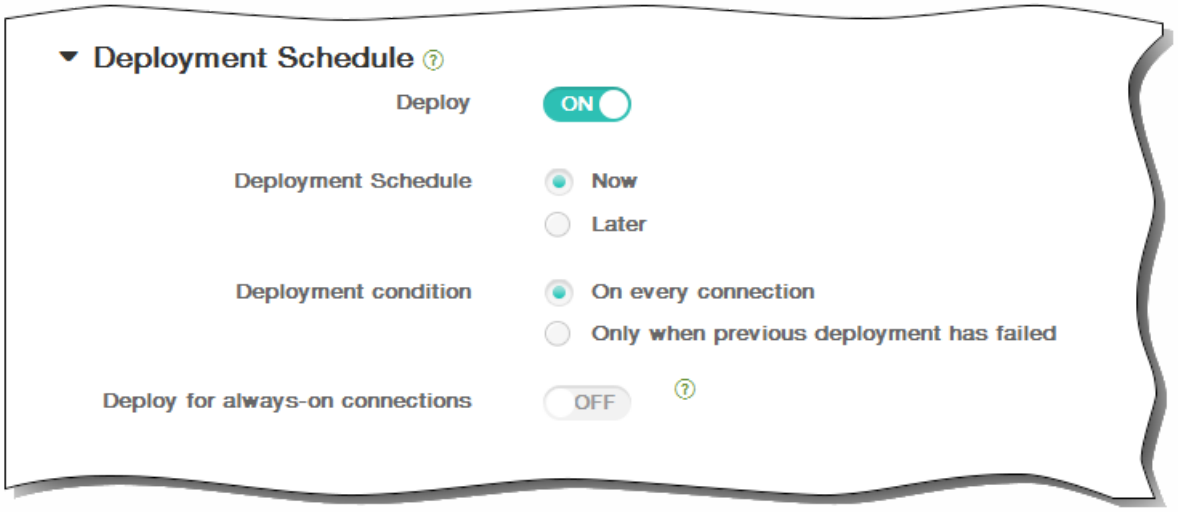
8. Haga clic en Next. Aparecerá la página de asignación Enterprise Hub Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

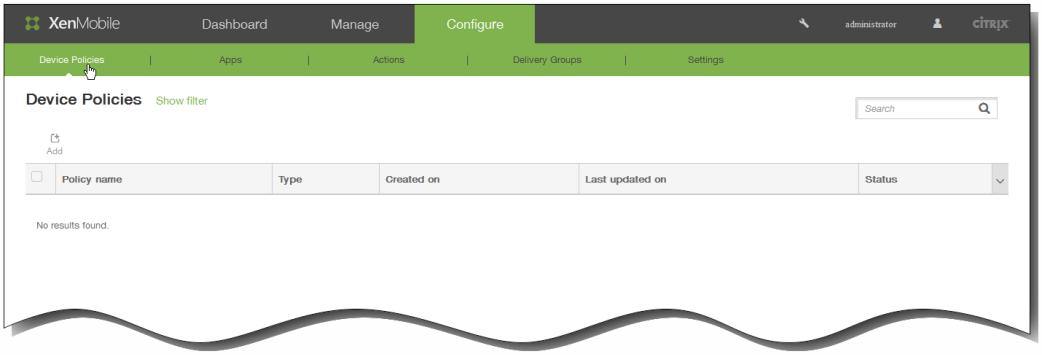
Directivas de Microsoft Exchange ActiveSync

May 05, 2016

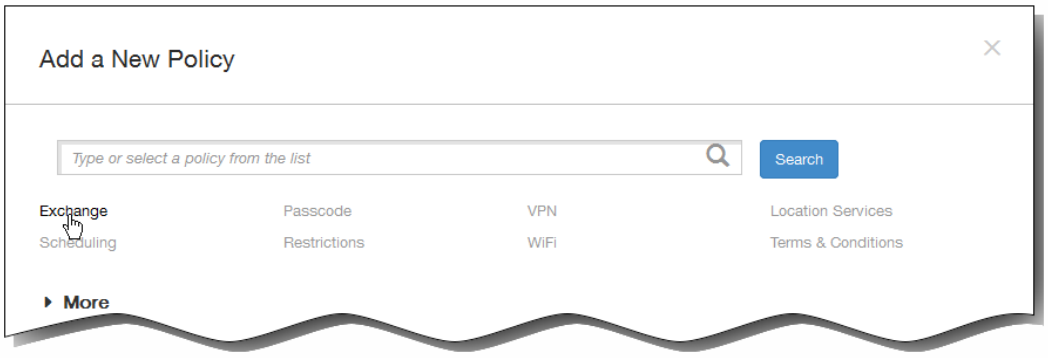
Puede usar la directiva de Exchange ActiveSync para configurar un cliente de correo electrónico en los dispositivos de los usuarios con el fin de que estos, a su vez, puedan acceder al correo electrónico de su empresa alojado en Exchange. Puede crear directivas para iOS, Android HTC, Android TouchDown, Samsung SAFE, Samsung KNOX y Windows Phone 8.1. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en los siguientes apartados:

Antes de crear esta directiva, debe conocer el nombre de host o la dirección IP del servidor Exchange.

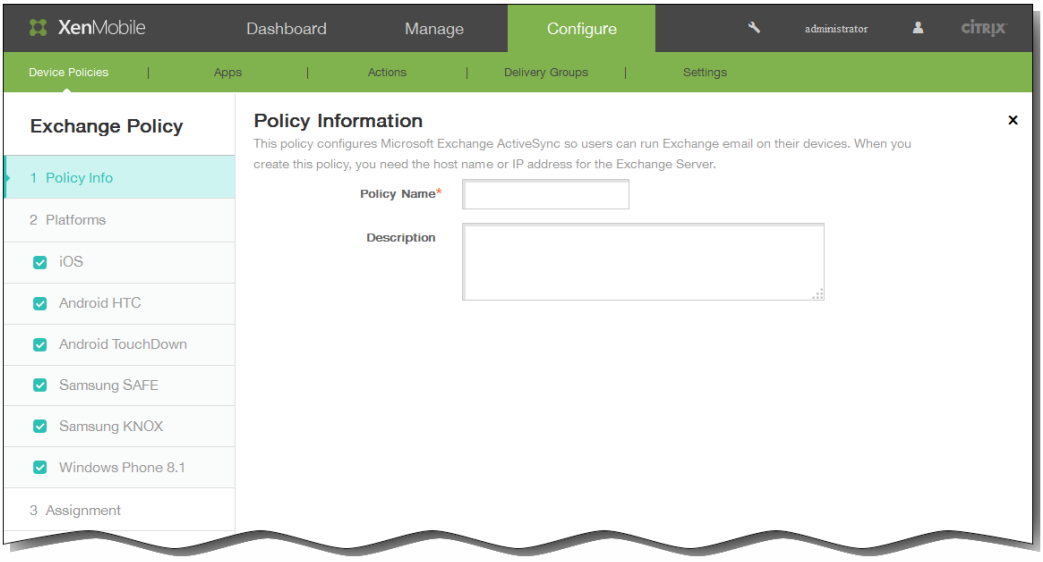
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



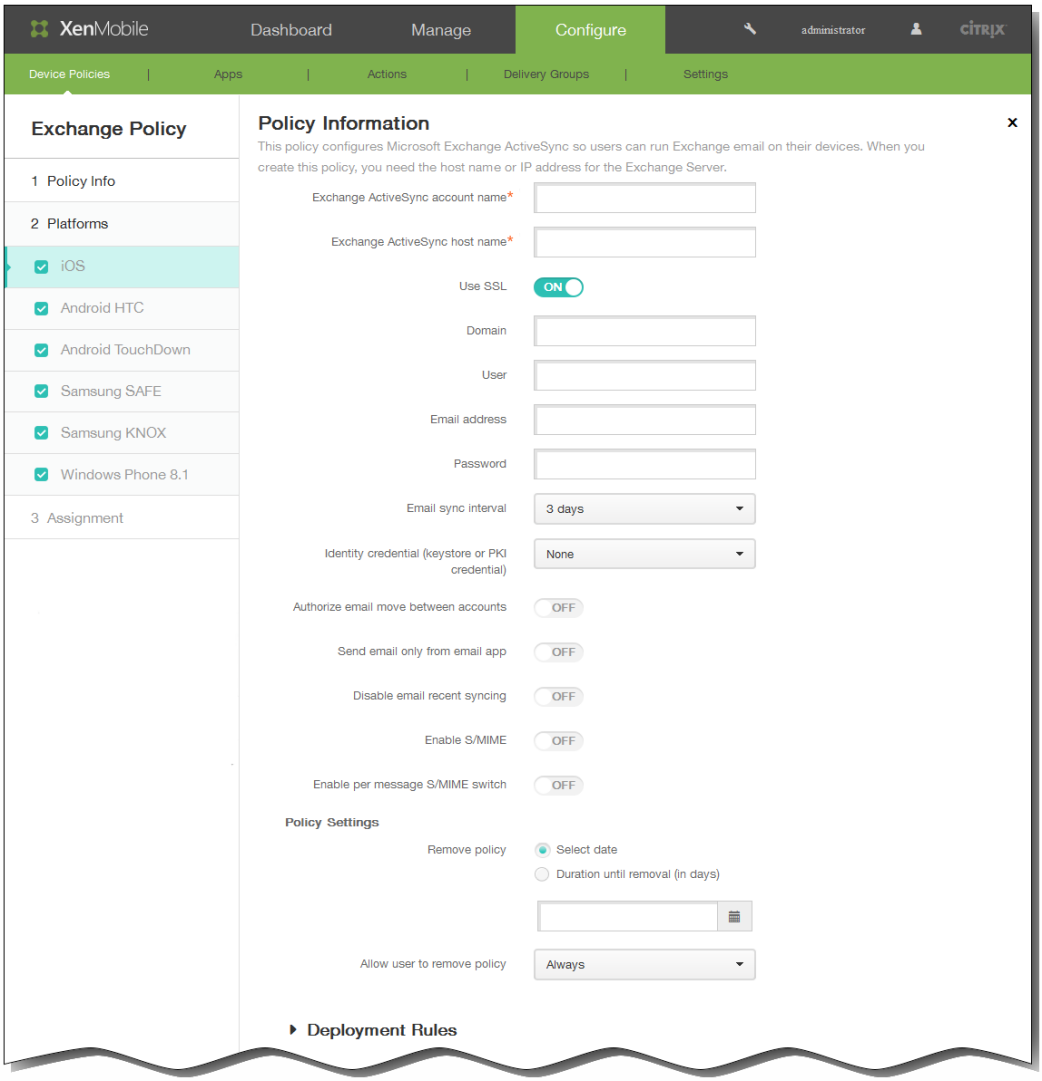
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.



3. Haga clic en Exchange. Aparecerá la página de información Exchange Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS.



6. En Platforms, seleccione la plataforma o las plataformas que quiere agregar.
   - Si ha seleccionado iOS, configure los siguientes parámetros:

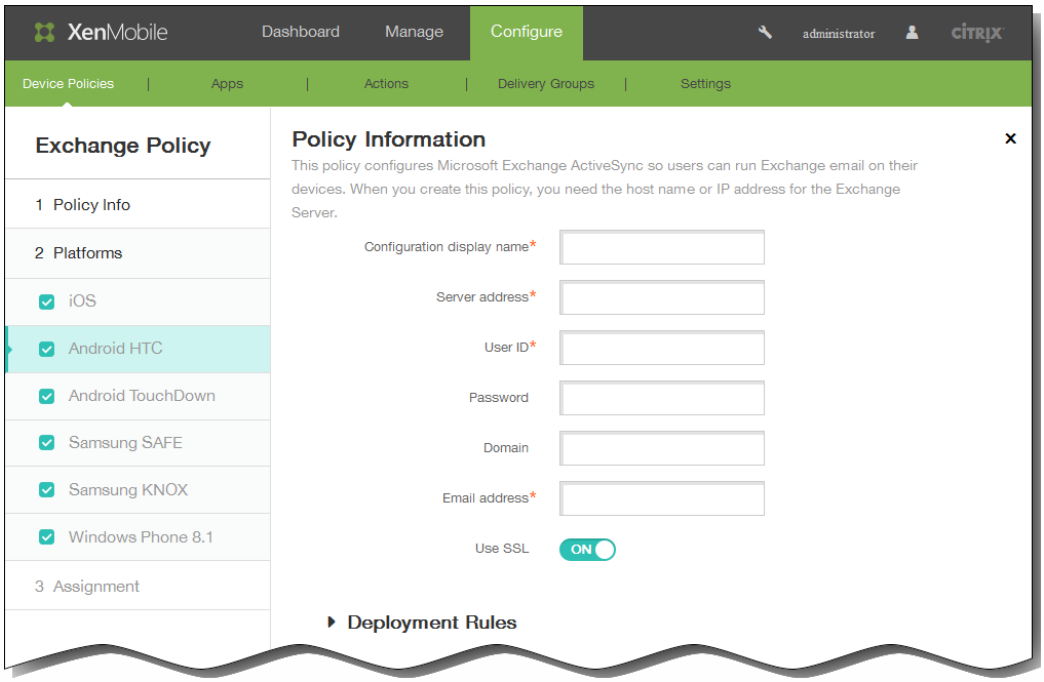
     Configuration display name. Escriba el nombre de esta directiva que aparecerá en los dispositivos de los usuarios.

     Server address. Escriba el nombre de host o la dirección IP del servidor Exchange.

     User ID. Especifique el nombre de usuario de la cuenta de usuario de Exchange.
     Nota: Puede utilizar la macro de sistema ${user.username} en este campo para buscar automáticamente los nombres de los usuarios.
     Password. Escriba una contraseña opcional para la cuenta de usuario de Exchange.

     Domain. Escriba el dominio en el que reside el servidor Exchange.
     Nota: Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
     Email address. Especifique la dirección de correo electrónico completa del usuario.
     Nota: Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
     Use SSL. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es On.

- Si ha seleccionado Android HTC, configure los siguientes parámetros:



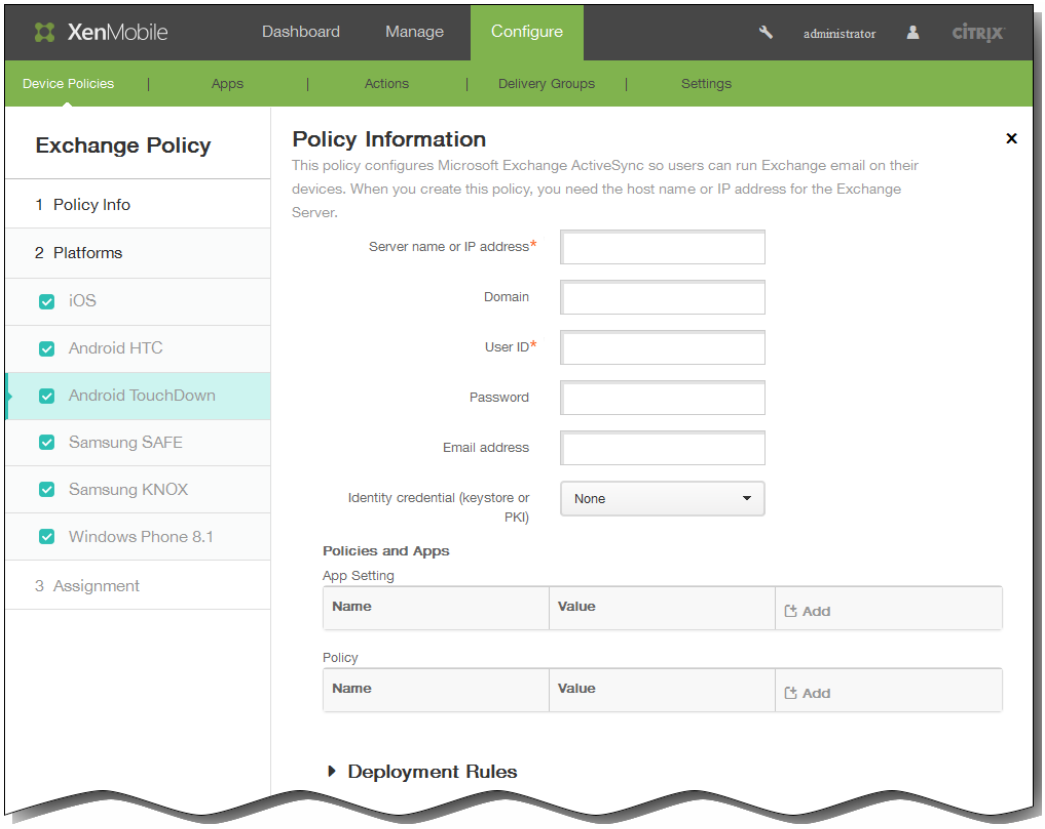
Configuration display name. Escriba el nombre de esta directiva que aparecerá en los dispositivos de los usuarios.

Server address. Escriba el nombre de host o la dirección IP del servidor Exchange.

User ID. Especifique el nombre de usuario de la cuenta de usuario de Exchange.
Nota: Puede utilizar la macro de sistema ${user.username} en este campo para buscar automáticamente los nombres de los usuarios.
Password. Escriba una contraseña opcional para la cuenta de usuario de Exchange.

Domain. Escriba el dominio en el que reside el servidor Exchange.
Nota: Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
Email address. Especifique la dirección de correo electrónico completa del usuario.
Nota: Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
Use SSL. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es On.

- Si ha seleccionado Android TouchDown, configure los siguientes parámetros:



Server name or IP address. Escriba el nombre de host o la dirección IP del servidor Exchange.

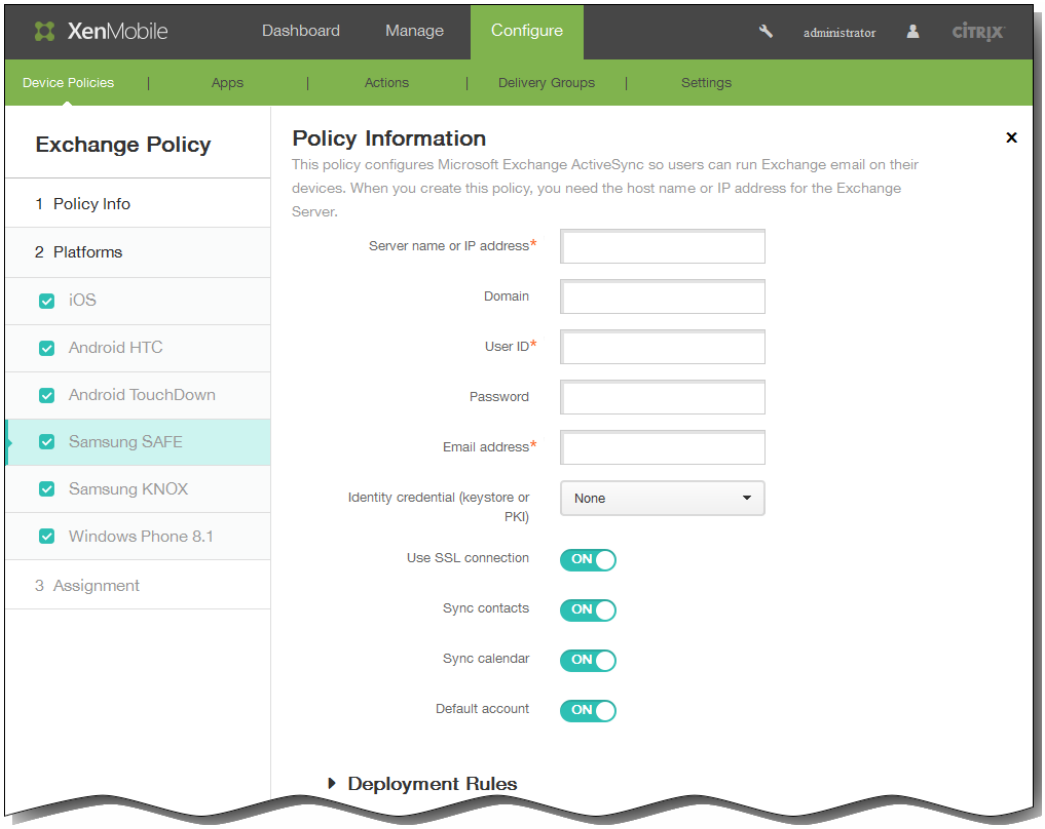
Domain. Escriba el dominio en el que reside el servidor Exchange.
Nota: Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
User ID. Especifique el nombre de usuario de la cuenta de usuario de Exchange.
Nota: Puede utilizar la macro de sistema ${user.username} en este campo para buscar automáticamente los nombres de los usuarios.
Password. Escriba una contraseña opcional para la cuenta de usuario de Exchange.

Email address. Especifique la dirección de correo electrónico completa del usuario.
Nota: Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
Identity credential (keystore or PKI). En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidad para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente.

App Setting. Si quiere, puede agregar opciones de configuración de aplicaciones TouchDown a esta directiva.

Policy. Si quiere, puede agregar directivas de TouchDown a esta directiva.

- Si ha seleccionado Samsung SAFE o Samsung KNOX, configure los siguientes parámetros:



Server name or IP address. Escriba el nombre de host o la dirección IP del servidor Exchange.

Domain. Escriba el dominio en el que reside el servidor Exchange.
Nota: Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
User ID. Especifique el nombre de usuario de la cuenta de usuario de Exchange.
Nota: Puede utilizar la macro de sistema ${user.username} en este campo para buscar automáticamente los nombres de los usuarios.
Password. Escriba una contraseña opcional para la cuenta de usuario de Exchange.

Email address. Especifique la dirección de correo electrónico completa del usuario.
Nota: Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
Identity credential (keystore or PKI). En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidad para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente.

Use SSL connection. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es On.

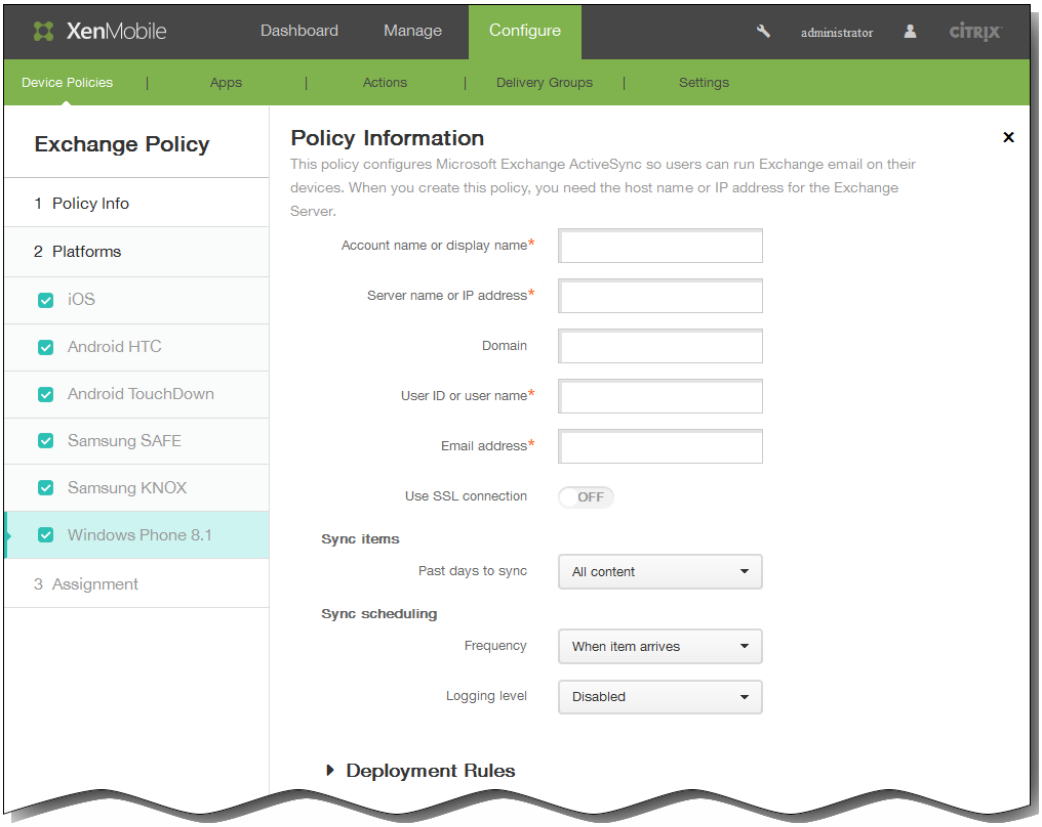
Sync contacts. Marque la casilla para habilitar la sincronización de los contactos de los usuarios entre sus dispositivos y el servidor Exchange. El valor predeterminado es On.

Sync calendar. Marque la casilla para habilitar la sincronización de los calendarios de los usuarios entre sus dispositivos y el servidor Exchange. El valor predeterminado es On.

Default account. Marque la casilla para que la cuenta de usuarios Exchange sea la predeterminada para enviar correos electrónicos desde sus dispositivos. El valor predeterminado es On.

- Si ha seleccionado Windows Phone 8.1, configure los siguientes parámetros.

  Nota: Esta directiva no permite establecer la contraseña de usuario. Los usuarios deben establecer ese parámetro desde sus dispositivos después de la inserción de la directiva.



Account name or display name. Escriba el nombre de la cuenta de Exchange ActiveSync.

Server name or IP address. Escriba el nombre de host o la dirección IP del servidor Exchange.

Domain. Escriba el dominio en el que reside el servidor Exchange.
Nota: Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
User ID or user name. Especifique el nombre de usuario para la cuenta de usuario de Exchange.
Nota: Puede utilizar la macro de sistema ${user.username} en este campo para buscar automáticamente los nombres de los usuarios.
Email address. Especifique la dirección de correo electrónico completa del usuario.
Nota: Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
Use SSL connection. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es Off.

Past days to sync. En la lista, haga clic en la cantidad de días pasados necesarios para sincronizar todo el contenido del

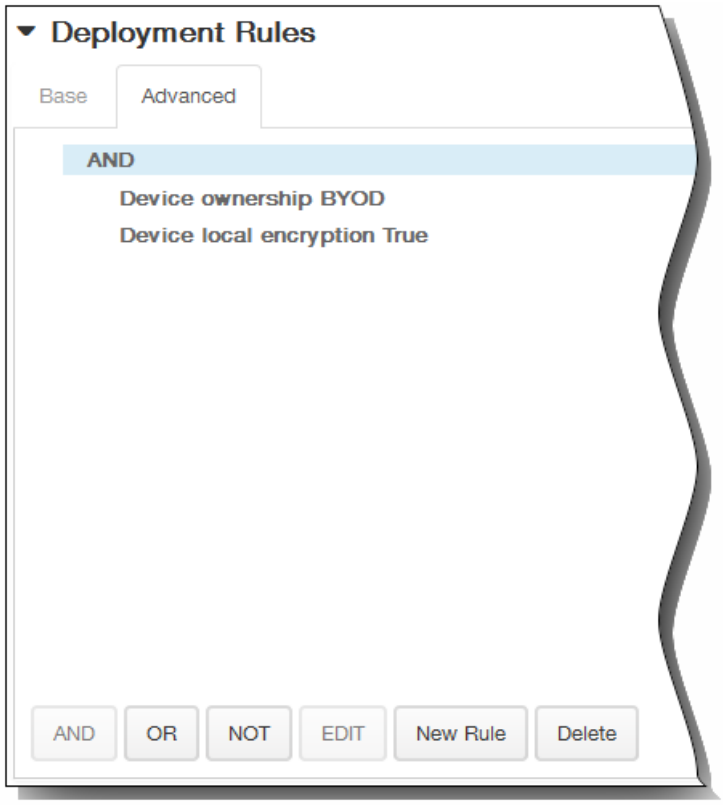
dispositivo con el servidor Exchange.

Frequency. En la lista, haga clic en la programación que se usará para sincronizar los datos que se envíen al dispositivo desde el servidor Exchange.

Logging level. En la lista, haga clic en Disabled, Basic o Advanced para especificar el nivel de detalle que se seguirá a la hora de registrar la actividad de Exchange.

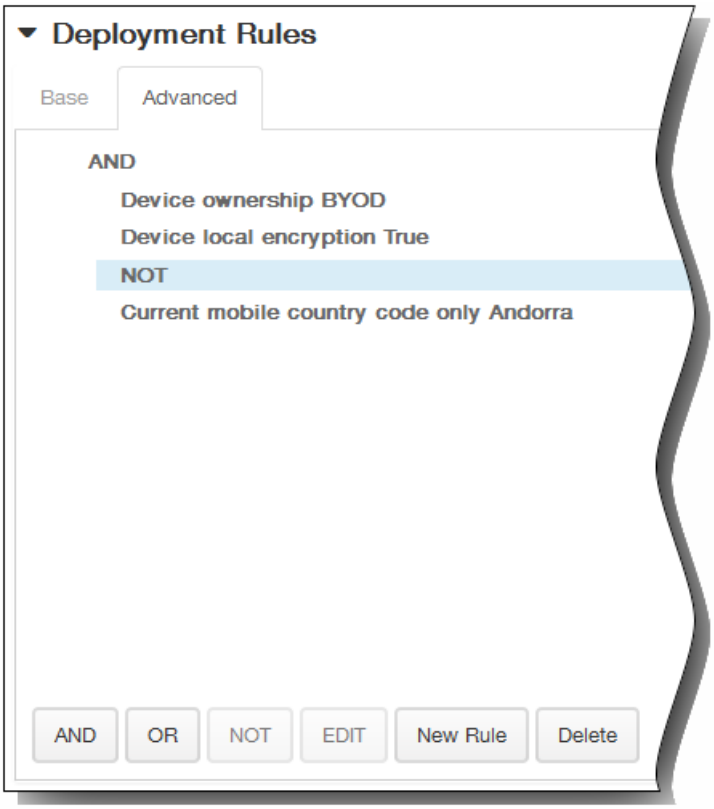
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

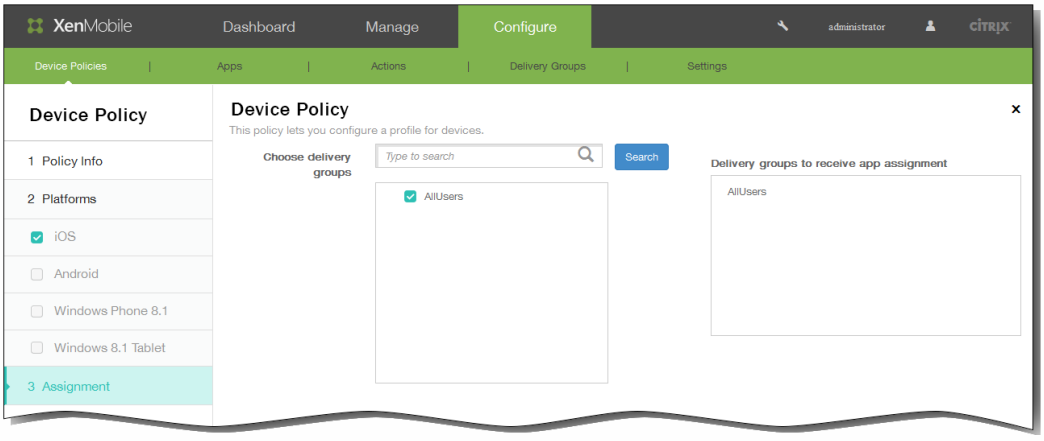


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



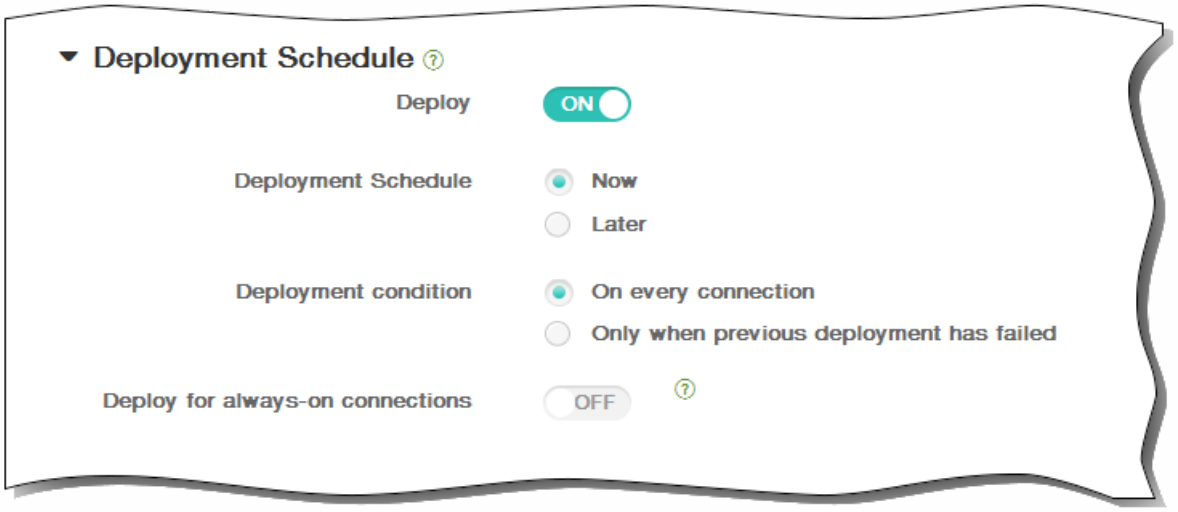
8. Haga clic en Next. Aparecerá la página Exchange Policy Assignment.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save.

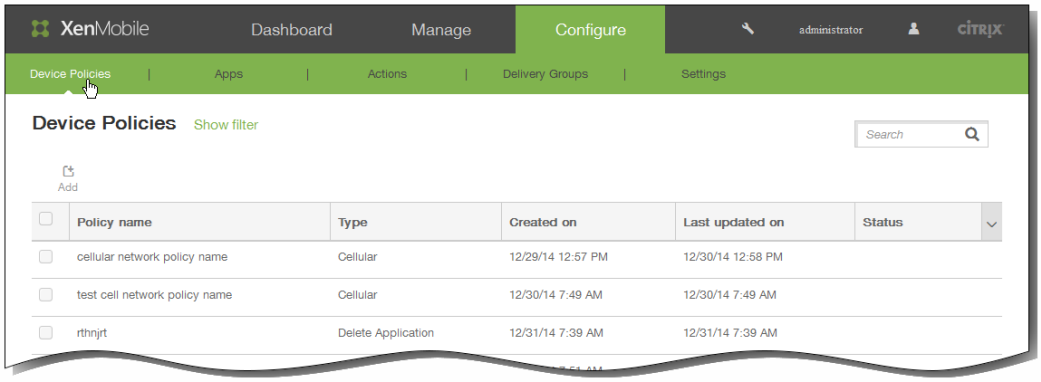
Directivas de ubicación

May 05, 2016

En XenMobile, puede crear directivas de ubicación para aplicar límites geográficos y realizar un seguimiento de la ubicación y del movimiento de los dispositivos de los usuarios. Cuando los usuarios abandonen el perímetro definido (también conocido como geovalla), XenMobile puede realizar un borrado completo o selectivo de los datos del dispositivo, ya sea inmediatamente o tras un período de tiempo específico establecido para permitir a los usuarios volver a la ubicación permitida.

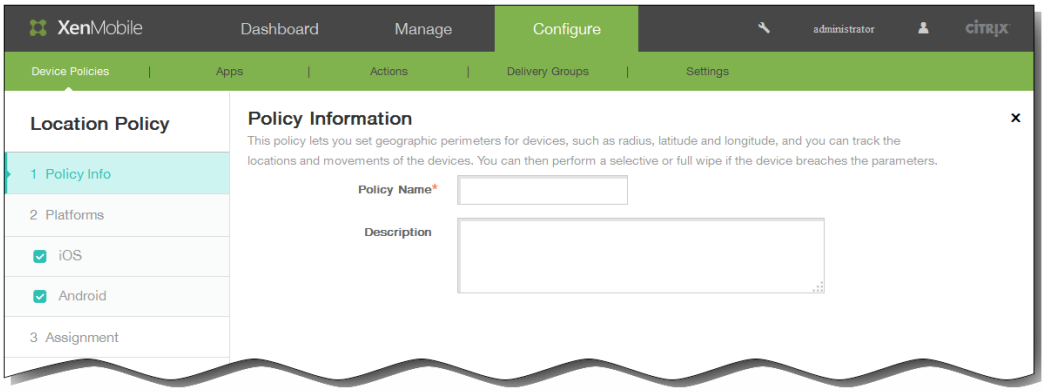
Puede crear directivas de ubicación para dispositivos iOS y para Android. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.

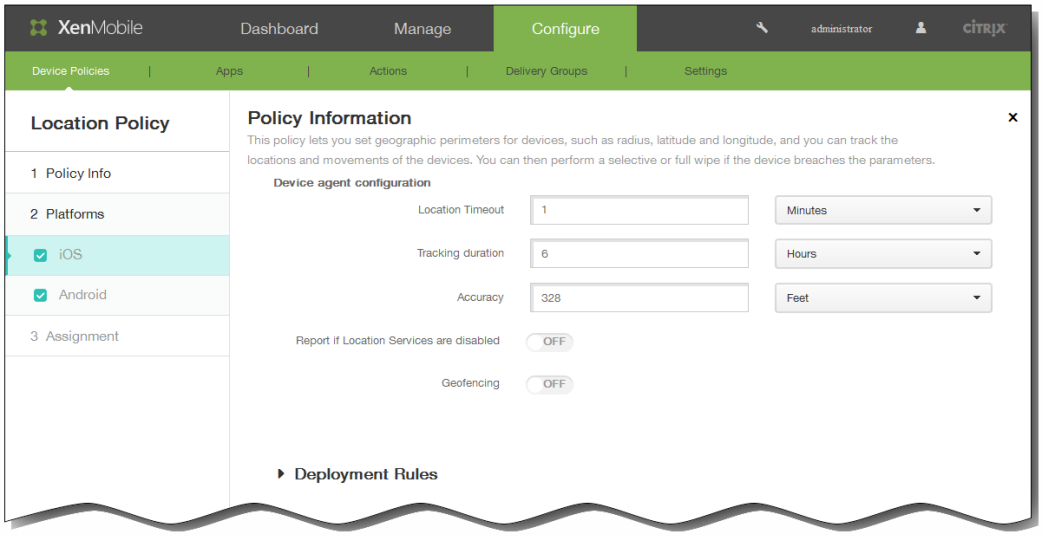


2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.

3. Haga clic en Location Services. Aparecerá la página de información Location Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, ambas plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS.



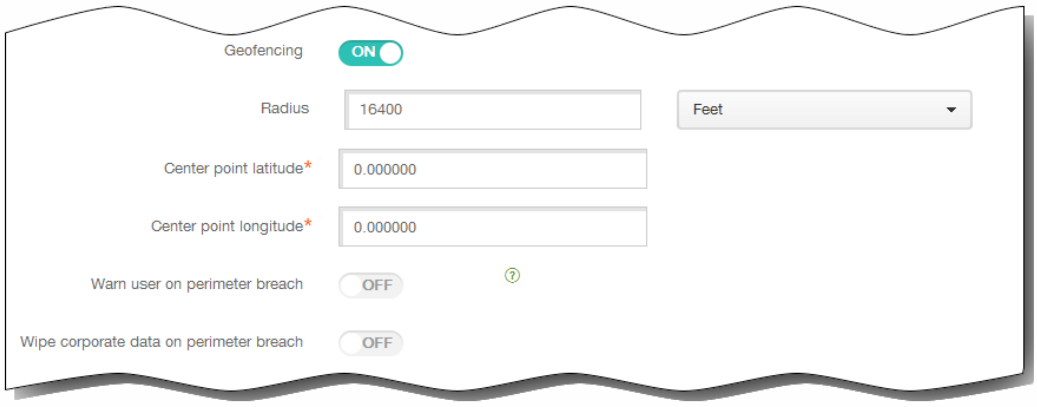
6. En Platforms, seleccione las plataformas que quiera agregar.
   - Si ha seleccionado iOS, configure los siguientes parámetros:
     Location timeout. Escriba un número y, en la lista, haga clic en Seconds o Minutes para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es de 1 minuto.

     Tracking duration. Escriba un número y, en la lista, haga clic en Hours o Minutes para definir la duración con que XenMobile realiza el seguimiento del dispositivo. Los valores válidos son de 1 a 6 horas o de 10 a 360 minutos. El valor predeterminado es de 6 horas.

     Accuracy. Escriba un número y, en la lista, haga clic en Meters, Feet o Yards la precisión con que XenMobile realiza el seguimiento del dispositivo. Los valores válidos varían entre 10 y 5000 yardas o metros, o bien entre 30 y 15000 pies. El valor predeterminado es de 328 pies.

Report if Location Services are disabled. Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. El valor predeterminado es OFF.

Geofencing. Seleccione esta opción para configurar los siguientes parámetros:



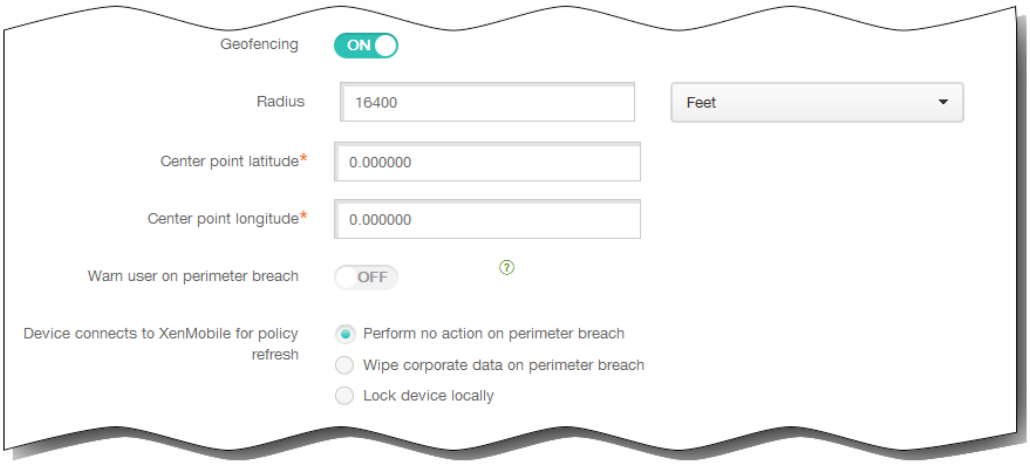
- Radius. Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies.
  Los valores válidos para el radio del perímetro son:
  - De 164 a 164 000 pies
  - De 1 a 50 kilómetros
  - De 50 a 50 000 metros
  - De 54 a 54 680 yardas
  - De 1 a 31 millas
- Center point latitude. Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geovalla.
- Center point longitude. Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geovalla.
- Warn user on perimeter breach. Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es OFF. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- Wipe corporate data on perimeter breach. Seleccione si borrar los datos de los dispositivos de los usuarios cuando estos abandonen el perímetro. El valor predeterminado es OFF.
  Si habilita esta opción, aparece el campo Delay on local wipe.

  Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.

- Si ha seleccionado Android, configure los siguientes parámetros:
  Poll interval. Escriba un número y, en la lista, haga clic en Minutes, Hours o Days para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 1 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier número de días. El valor predeterminado es 10 minutos.
  Nota: Establecer un valor menor de 10 minutos puede afectar de forma negativa a la duración de la batería del

dispositivo.
Report if Location Services are disabled. Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. El valor predeterminado es OFF.

Geofencing. Seleccione esta opción para configurar los siguientes parámetros:



- Radius. Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies.
  Los valores válidos para el radio del perímetro son:
  - De 164 a 164 000 pies
  - De 1 a 50 kilómetros
  - De 50 a 50 000 metros
  - De 54 a 54 680 yardas
  - De 1 a 31 millas
- Center point latitude. Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geovalla.
- Center point longitude. Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geovalla.
- Warn user on perimeter breach. Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es OFF. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- Device connects to XenMobile for policy refresh. Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
  - Perform no action on perimeter breach. No hacer nada. Ésta es la opción predeterminada.
  - Wipe corporate data on perimeter breach. Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado.
    Si habilita esta opción, aparece el campo Delay on local wipe.

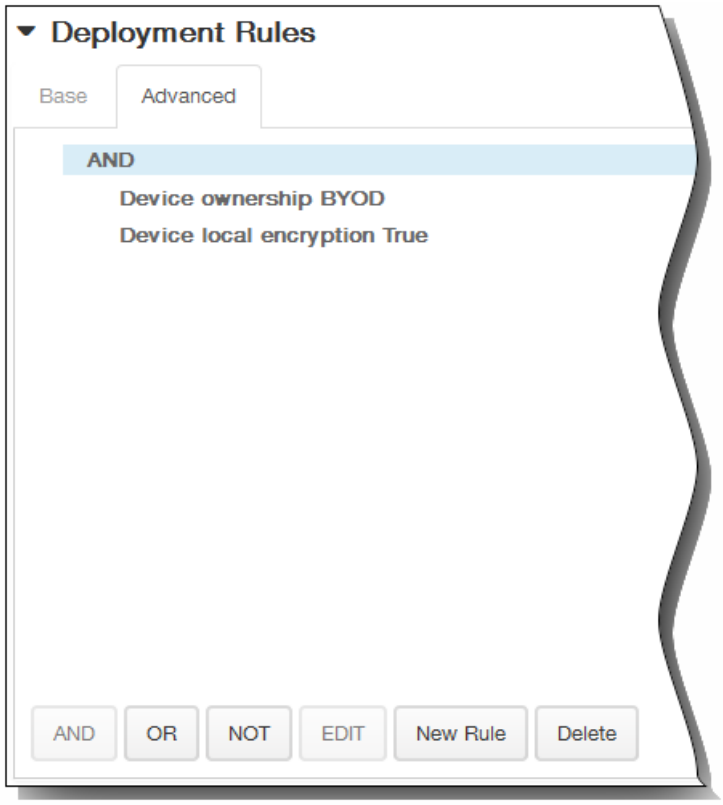
    Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.

- Delay on lock. Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparece el campo Delay on lock.

  Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile bloquee sus dispositivos. El valor predeterminado es de 0 segundos.

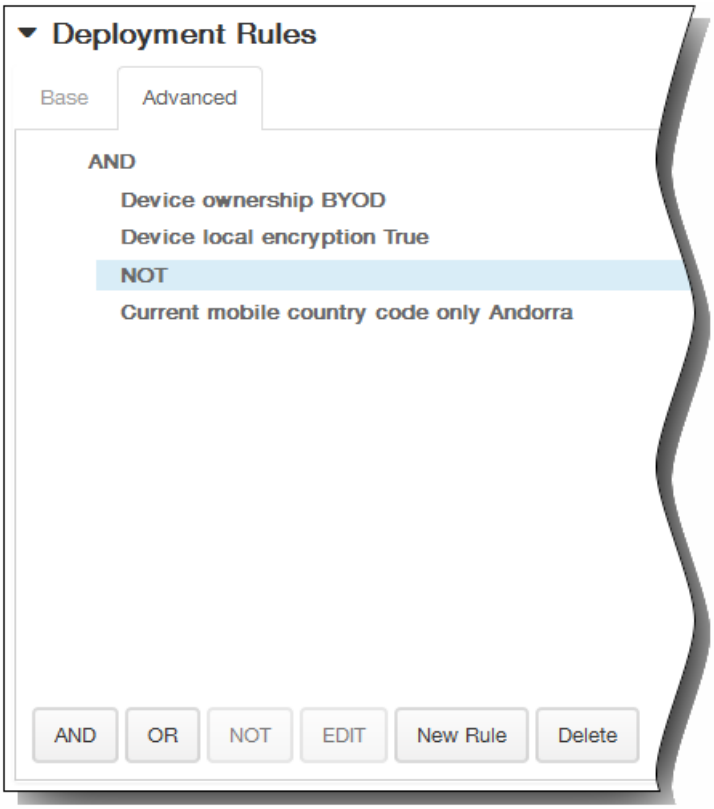
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

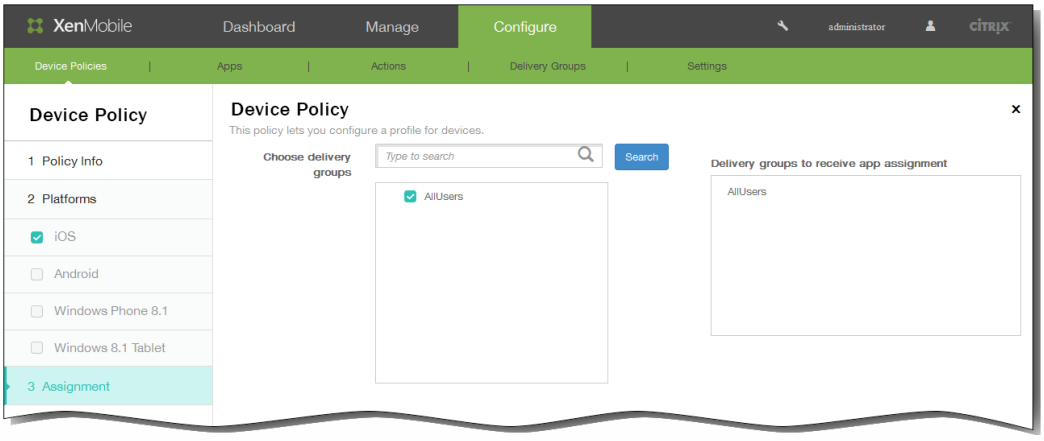


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
       En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
       En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



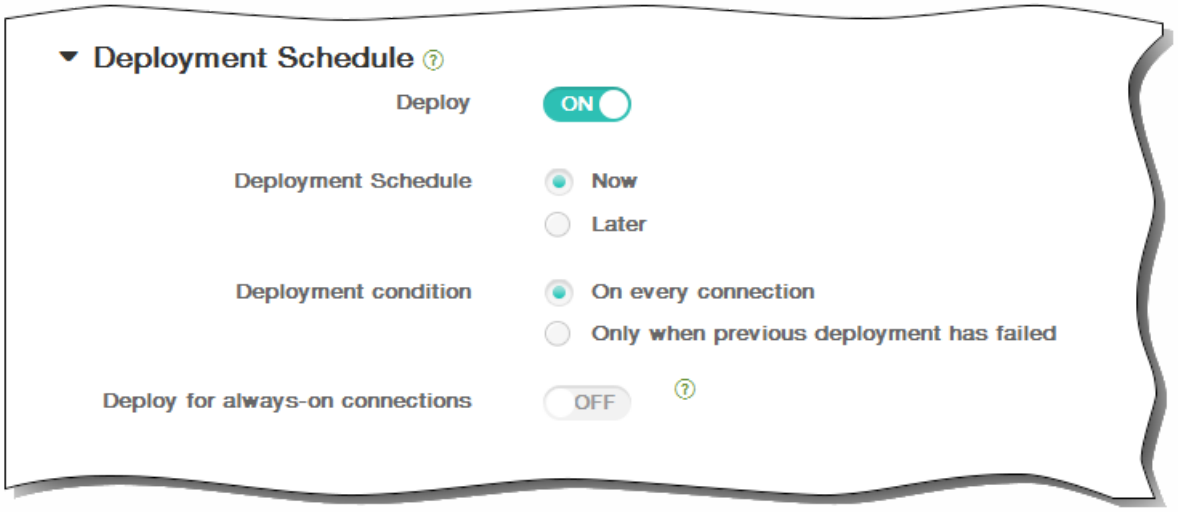
8. Haga clic en Next. Aparecerá la página de asignación Location Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



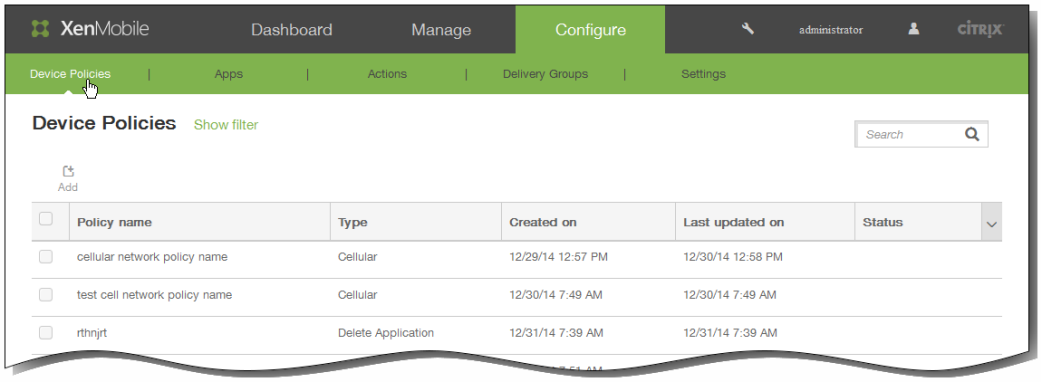
11. Haga clic en Save para guardar la directiva.

Directivas de programación de conexiones

May 05, 2016

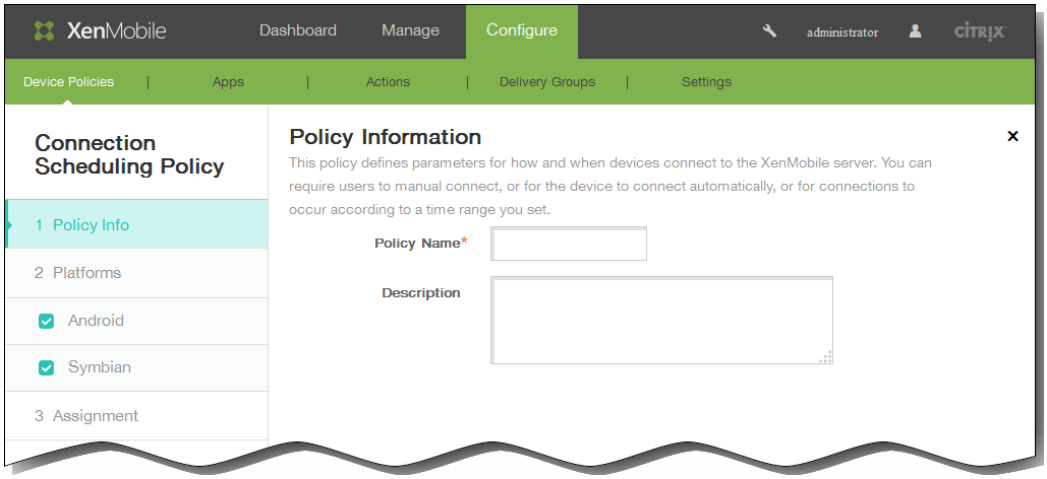
Puede crear directivas de programación de conexiones para controlar cómo y cuándo los usuarios de dispositivos Android y Symbian se conectan a XenMobile. Puede especificar que los usuarios conecten sus dispositivos manualmente, que los dispositivos permanezcan conectados de forma permanente o que los dispositivos se conecten dentro de un período de tiempo definido.

1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.

3. Haga clic en Scheduling. Aparecerá la página de información Connection Scheduling Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, ambas plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de Android.
6. En Platforms, seleccione las plataformas que quiera agregar.
7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas: Require devices to connect. Haga clic en la opción que quiera establecer para esta programación.
   - Always. Mantiene la conexión activa de forma permanente. La instancia de XenMobile en el dispositivo del usuario intenta volver a conectarse al servidor XenMobile después de perder la conexión de red; la conexión se supervisa mediante la transmisión de paquetes de control en intervalos regulares.
     Esta opción no se recomienda porque consume mucha batería y genera una gran cantidad de tráfico de red.
   - Never. Se conecta manualmente. Los usuarios deben iniciar la conexión desde la instancia de XenMobile presente en sus dispositivos.
   - Every. Se conecta en el intervalo predeterminado. Los dispositivos se conectan automáticamente después de una cantidad definida de minutos.
     Si se selecciona esta opción, aparece el campo Connect every N minutes. En él, debe introducir la cantidad de minutos tras los que el dispositivo debe volver a conectarse. El valor predeterminado es 20.
   - Define schedule. La instancia de XenMobile en el dispositivo del usuario intenta volver a conectarse al servidor XenMobile después de perder la conexión de red; la conexión se supervisa mediante la transmisión de paquetes de control en intervalos regulares en el período de tiempo que usted defina. En la siguiente sección, se describe cómo definir un período de tiempo de conexión.
     Para definir un período de tiempo de conexión

     Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. Cada cuadrado de la escala de tiempo es de 30 minutos, de modo que, si quiere una conexión entre las 8:00 a. m. y las 9:00 a. m. todos los días de la semana, haga clic en los dos cuadrados ubicados entre 8 a. m. y 9 a. m. todos los días de la semana.

     Por ejemplo: las dos escalas de tiempo de la siguiente ilustración requieren una conexión permanente entre las 8:00

a. m. y las 9:00 a. m. todos los días laborables de la semana, una conexión permanente entre las 12:00 a. m. del sábado y la 1:00 a. m. del domingo, además de al menos una conexión cada día laborable entre las 5:00 a. m. y las 8:00 a. m. o entre las 10:00 y a. m. las 11:00 p. m.

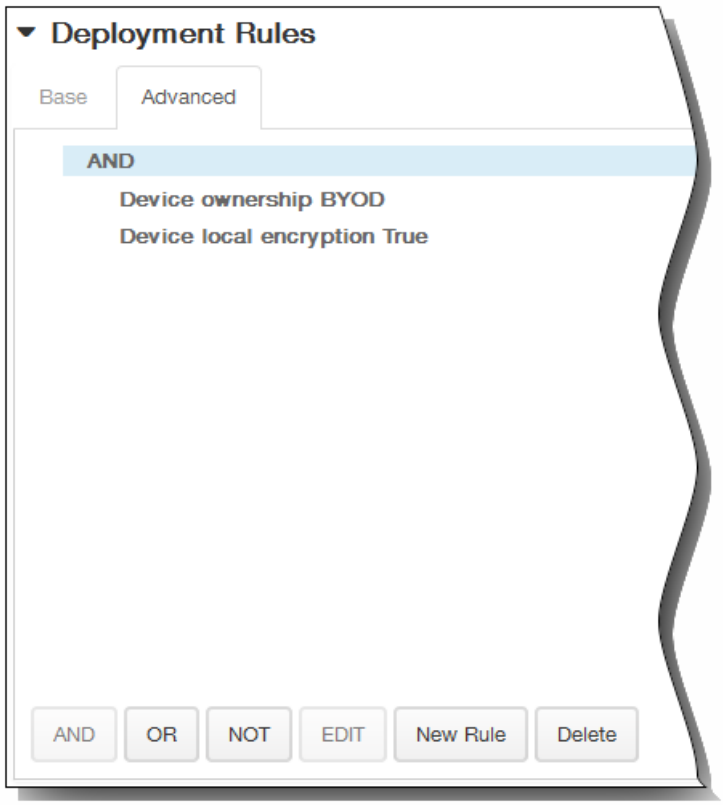
Maintain permanent connection during these hours. Los dispositivos de los usuarios deben estar conectados durante el período de tiempo definido.

Require a connection within each of these ranges. Los dispositivos de usuario deben conectarse al menos una vez en cualquier período de tiempo definido.

Use local device time rather than UTC. Sincroniza los períodos de tiempo definidos con la hora local del dispositivo en lugar de la hora universal coordinada (UTC).

8. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

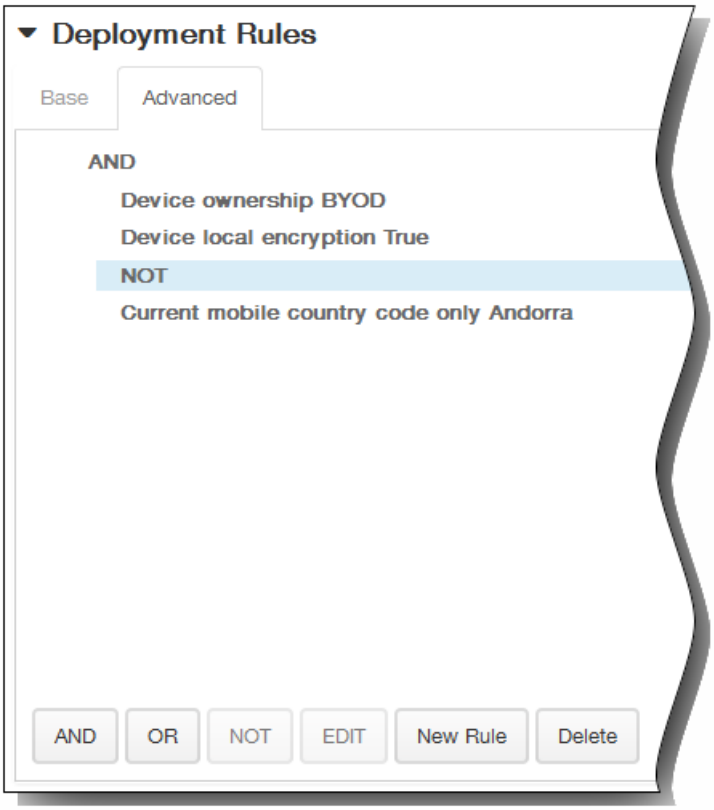
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



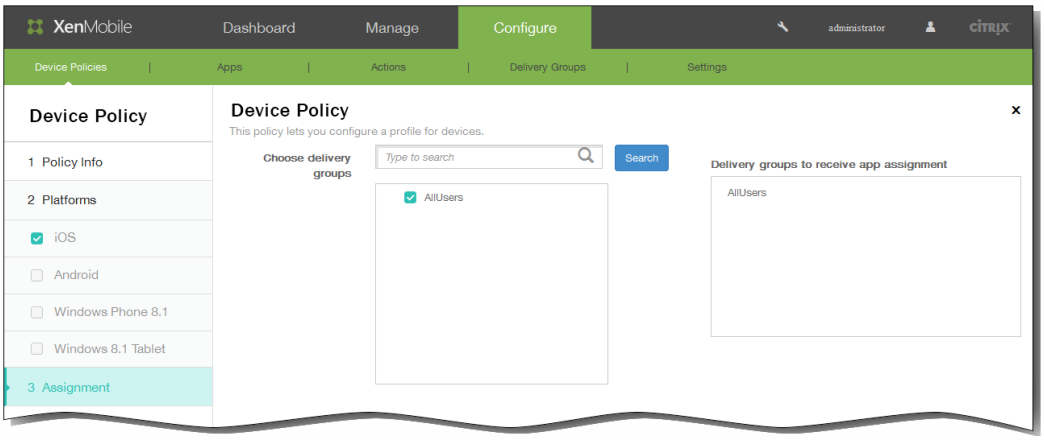
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



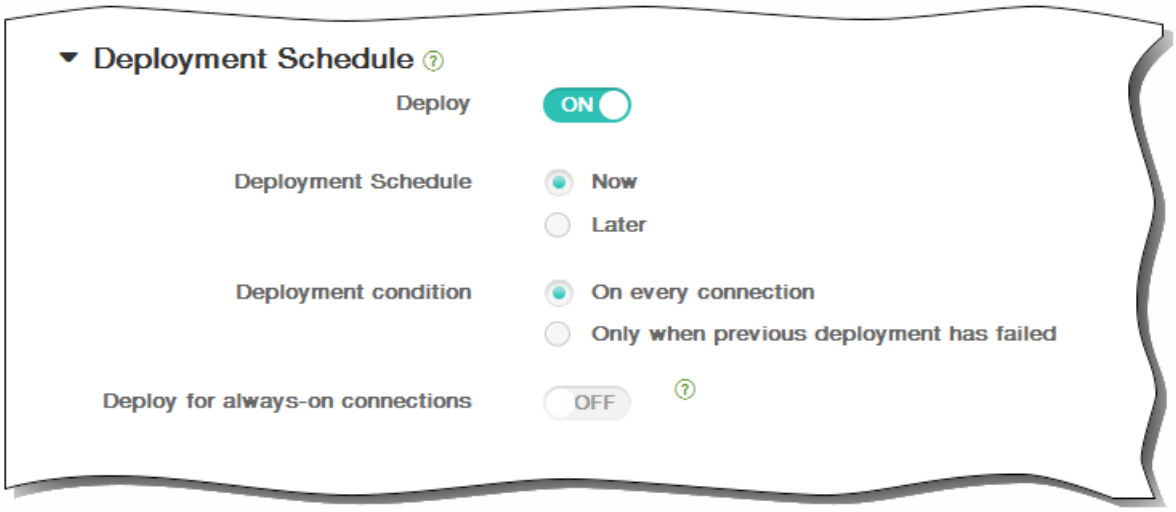
9. Haga clic en Next. Aparecerá la página de asignación Connection Scheduling Policy.
10. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



11. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



12. Haga clic en Save para guardar la directiva.

Para agregar una directiva de duplicación de AirPlay para dispositivos iOS

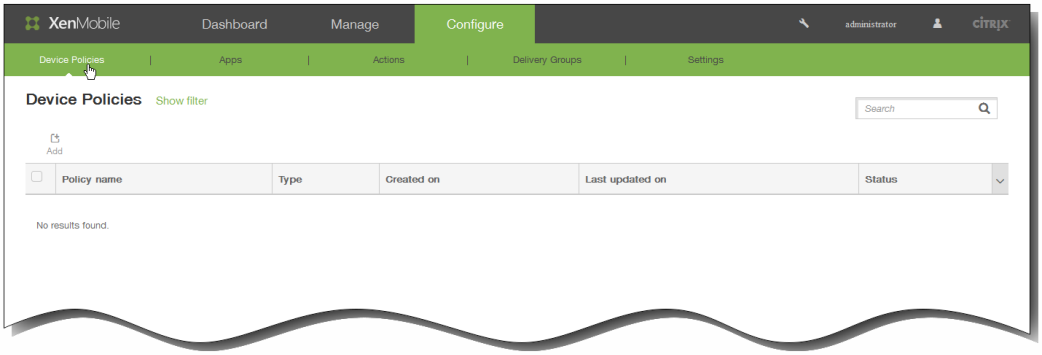
May 05, 2016

La función AirPlay de Apple permite a los usuarios reproducir contenido desde un dispositivo iOS a una pantalla de TV de forma inalámbrica y a través de Apple TV. También permite replicar de forma exacta lo que aparece en la pantalla de un dispositivo en la pantalla de una TV o de otro equipo Mac.

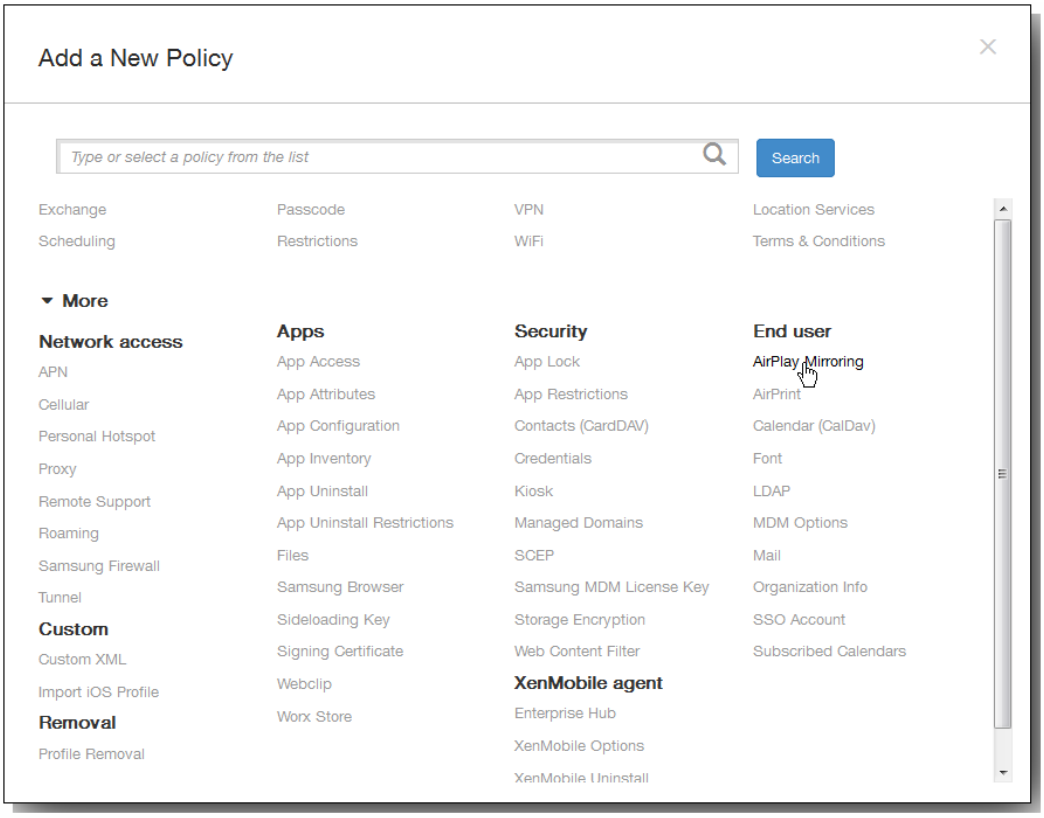
En XenMobile, puede agregar una directiva de dispositivos para agregar dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) en los dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos permitidos supervisados, lo que limitará a los usuarios a utilizar únicamente los dispositivos AirPlay que se encuentren en ella. Para obtener información sobre cómo colocar un dispositivo en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

Nota: Antes de continuar, compruebe que dispone de los ID de los dispositivos pertinentes, así como de las contraseñas de todos los dispositivos que quiera agregar.

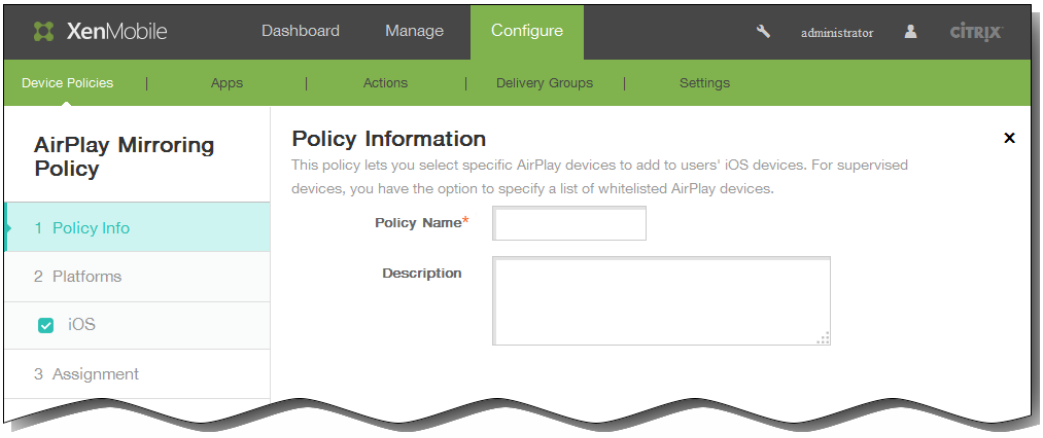
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



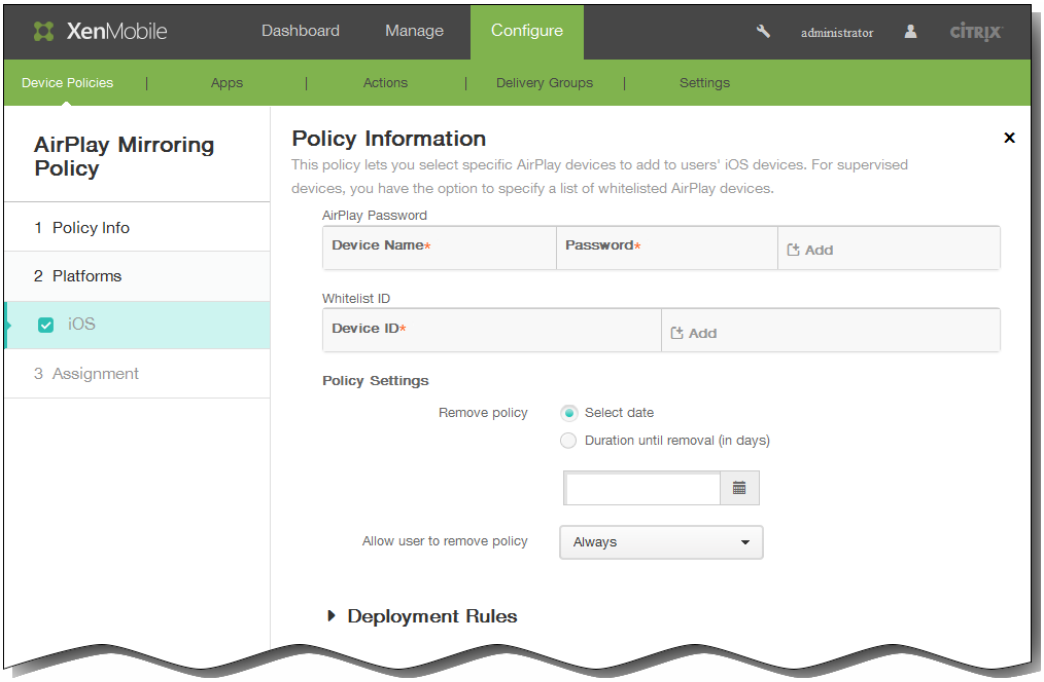
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en AirPlay Mirroring. Aparecerá la página AirPlay Mirroring Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.

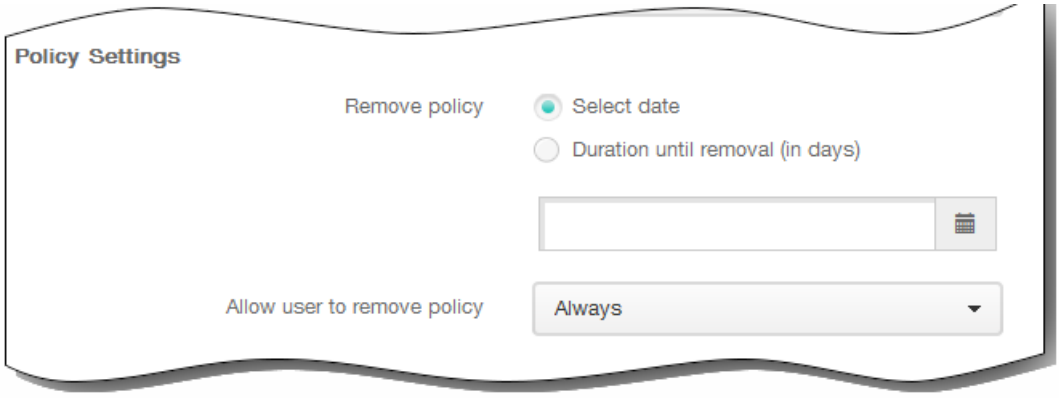


6. En la página de información iOS Platform, escriba la información siguiente:
   1. AirPlay Password. Haga clic en Add y lleve a cabo lo siguiente:
      1. Device ID. Introduzca el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
      2. Password. Escriba una contraseña opcional para el dispositivo.
      3. Haga clic en Add para agregar el dispositivo, o bien haga clic en Cancel para no agregar el dispositivo.
      4. Repita los pasos de i. a iii. para cada dispositivo que quiera agregar.
   2. Whitelist ID. Haga clic en Add y realice lo siguiente para restringir los dispositivos supervisados a solamente aquellos ID de dispositivo que se encuentren en la lista:

      Nota: Esta lista se omite para los dispositivos no supervisados.
      1. Device ID. Introduzca el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx . Este campo no distingue entre mayúsculas y minúsculas.
      2. Haga clic en Add para agregar el dispositivo, o bien haga clic en Cancel para no agregar el dispositivo.
      3. Repita los pasos de i. y ii. para cada dispositivo que quiera agregar a la lista de dispositivos permitidos.

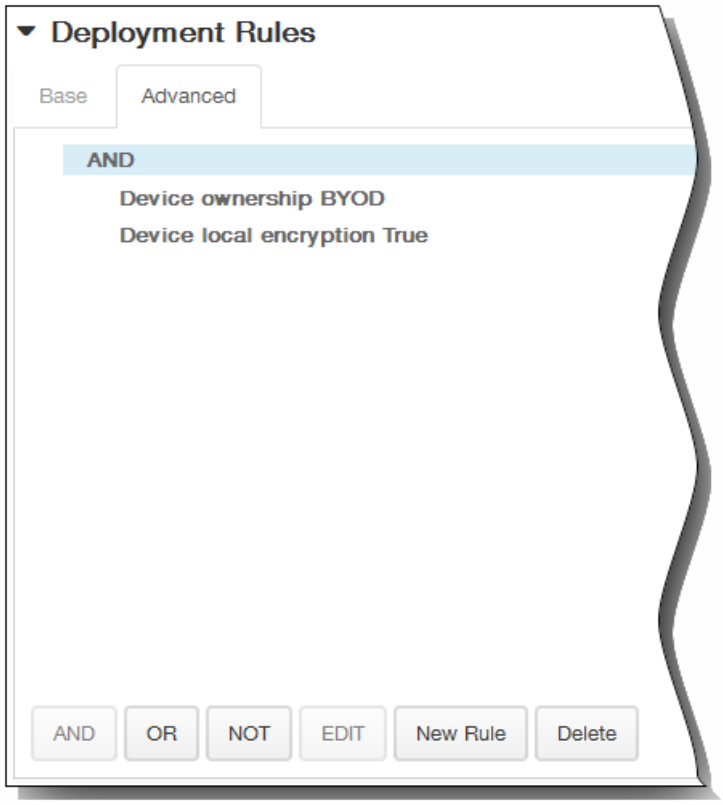
      Nota: Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

      Para modificar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



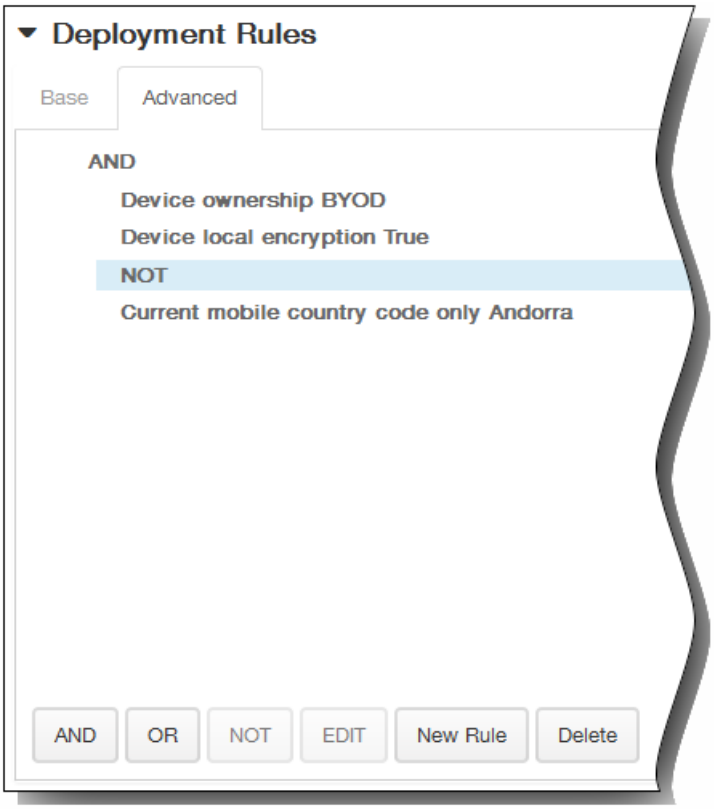
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

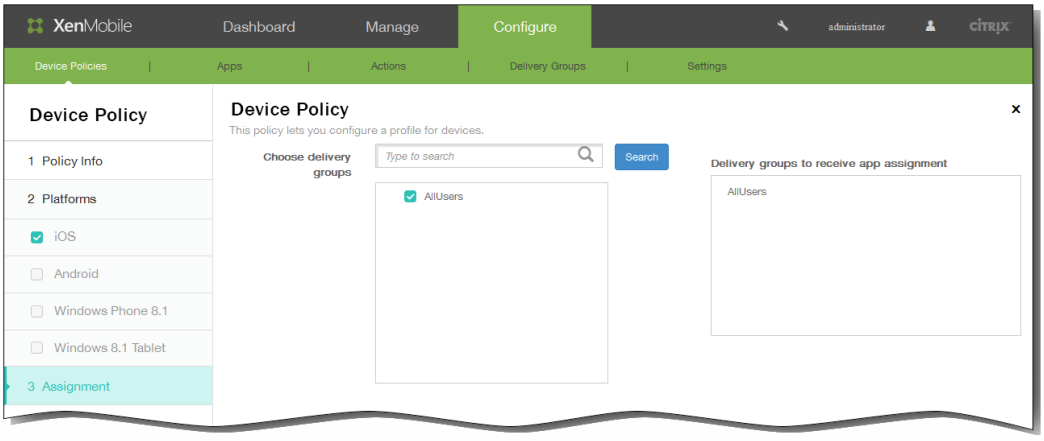


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



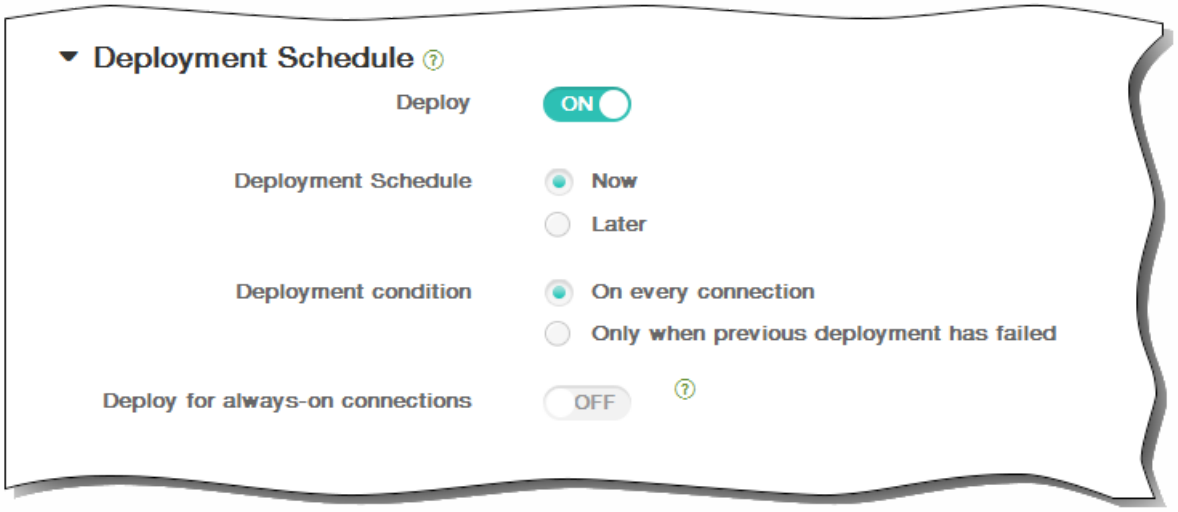
12. Haga clic en Next. Aparecerá la página de asignación AirPlay Mirroring Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



15. Haga clic en Save para guardar la directiva.

Para agregar una directiva de AirPrint para iOS

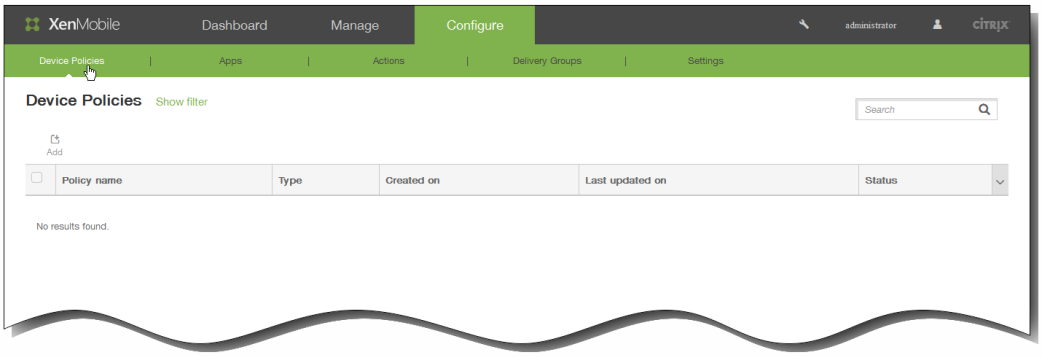
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para añadir impresoras AirPrint a la lista de impresoras AirPrint de los dispositivos iOS de los usuarios. Esta directiva facilita el respaldo de entornos en los que las impresoras y los dispositivos están en subredes diferentes.

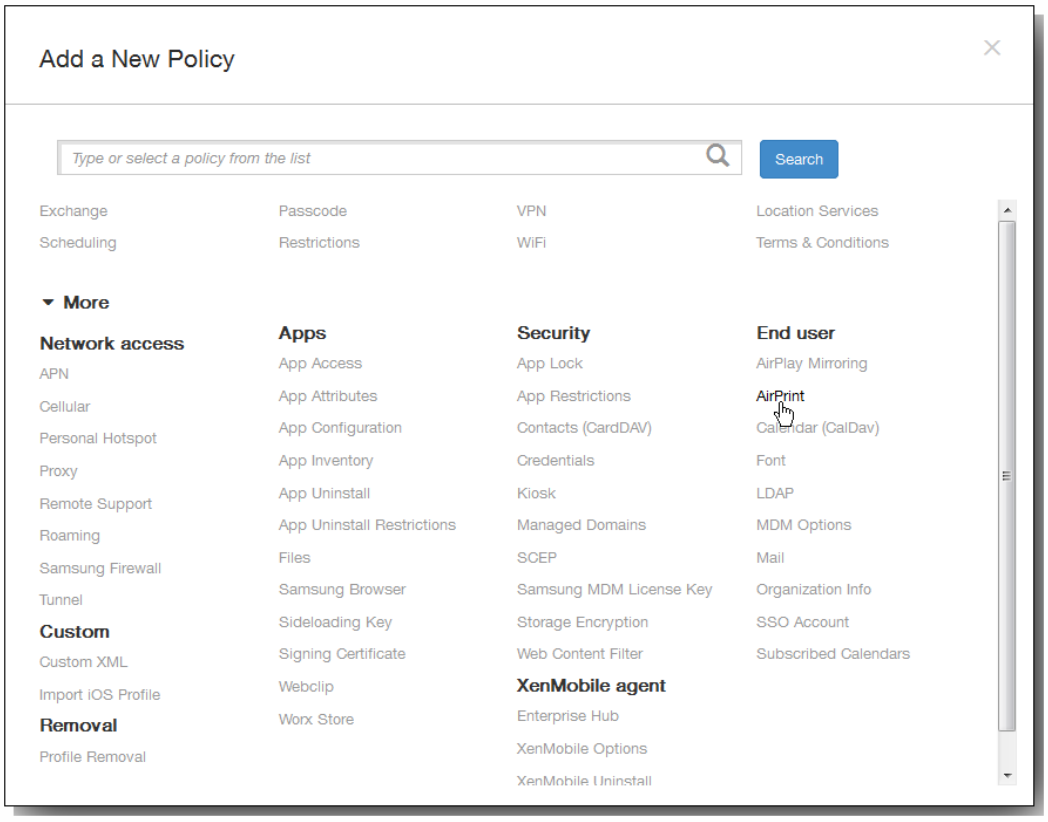
Nota:

- Esta directiva se aplica a iOS 7.0 y versiones posteriores.
- Compruebe que dispone de la dirección IP y de la ruta de recursos para cada impresora.

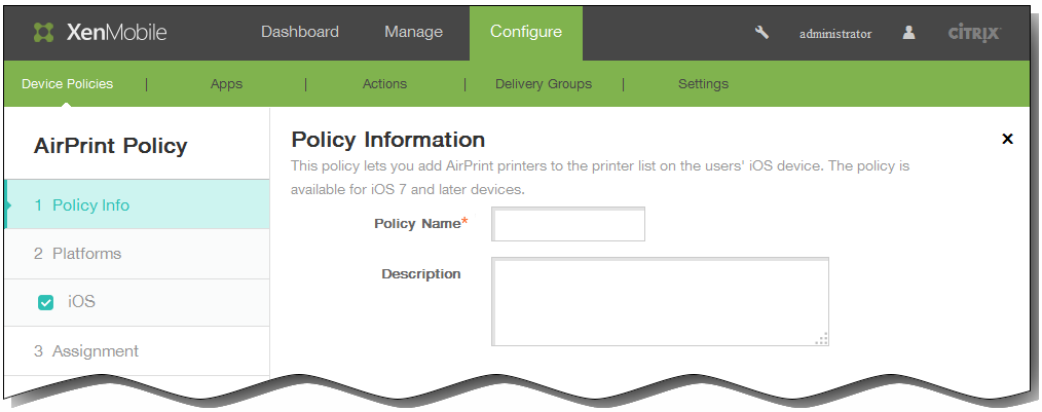
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



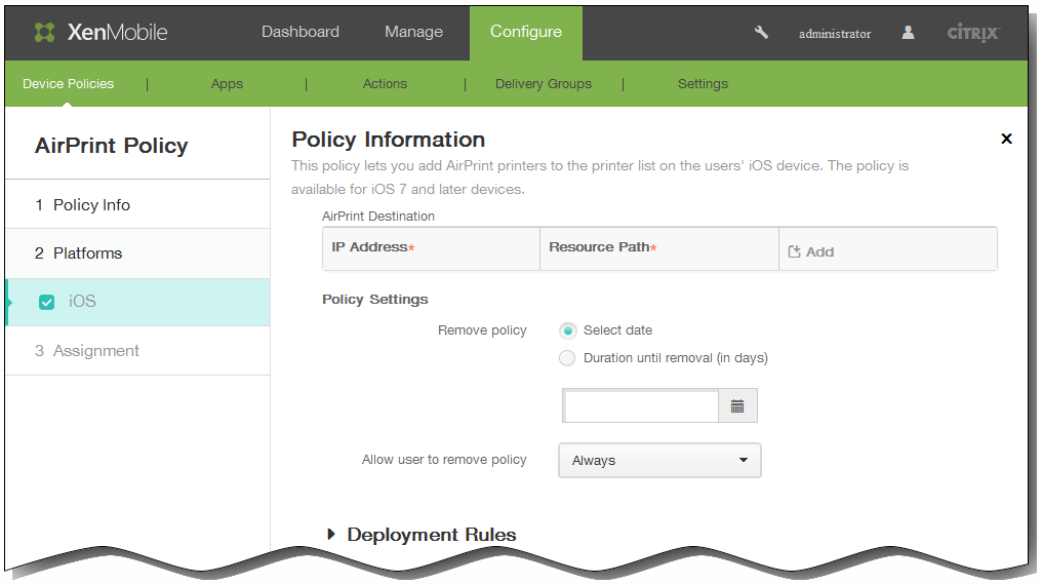
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en AirPrint. Aparecerá la página AirPrint Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.

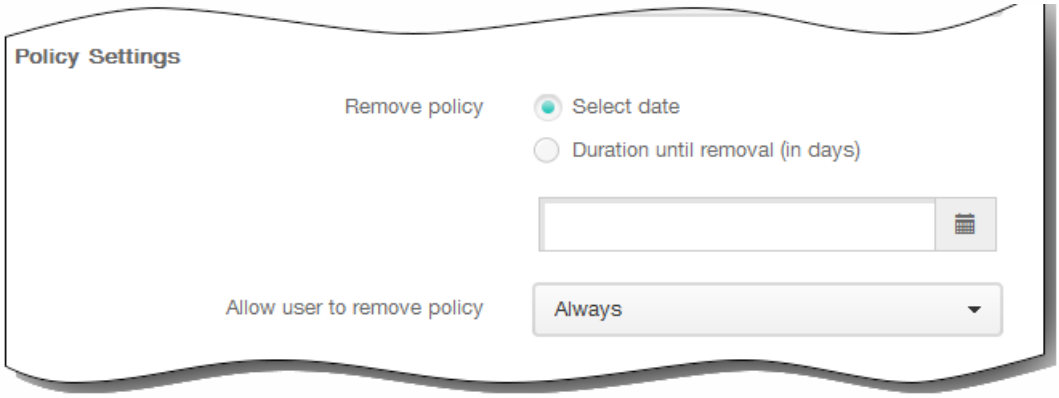


6. En la página de información iOS Platform, escriba la información siguiente:
   1. AirPrint Destination. Haga clic en Add y lleve a cabo lo siguiente:
      1. IP Address. Escriba la dirección IP de la impresora AirPrint.
      2. Resource Path. Escriba la ruta de recursos asociada a la impresora. Este valor corresponde al parámetro del registro Bonjour de _ipps.tcp. Por ejemplo, printers/Canon_MG5300_series o printers/Xerox_Phaser_7600.
      3. Haga clic en Add para agregar la impresora, o bien haga clic en Cancel para no agregarla.
      4. Repita los pasos de i. a iii. para cada dispositivo que quiera agregar.

      Nota: Para eliminar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga

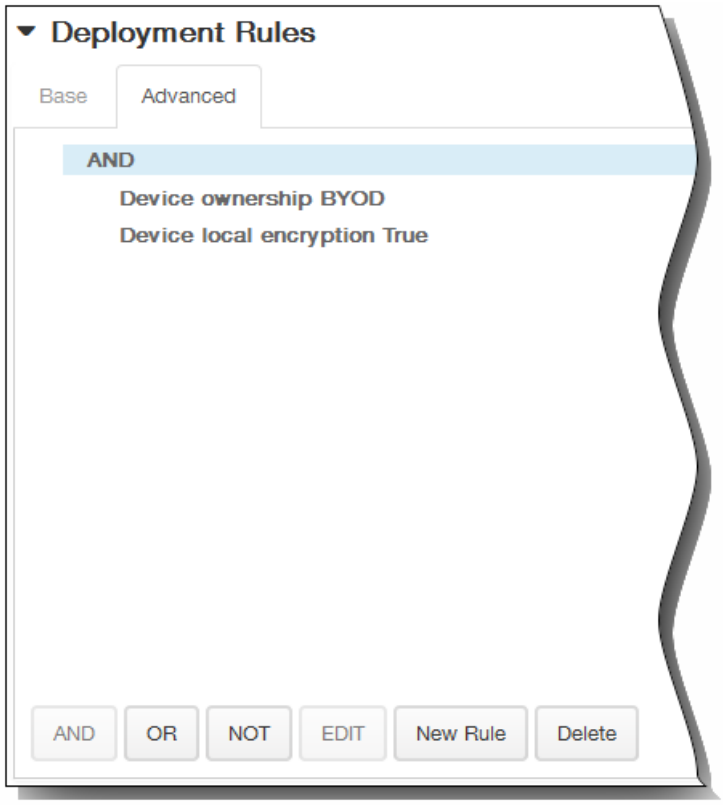
clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.
Para modificar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



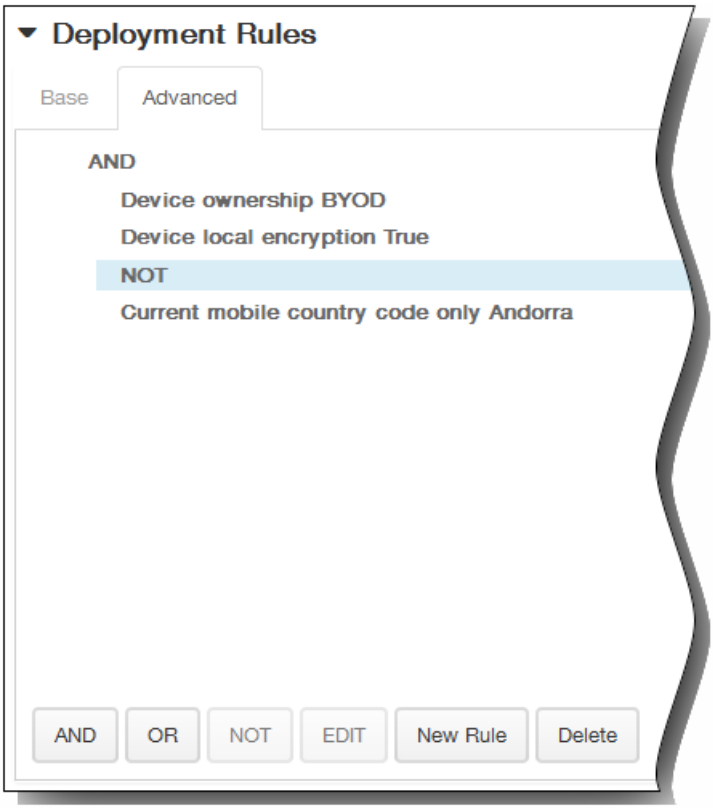
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

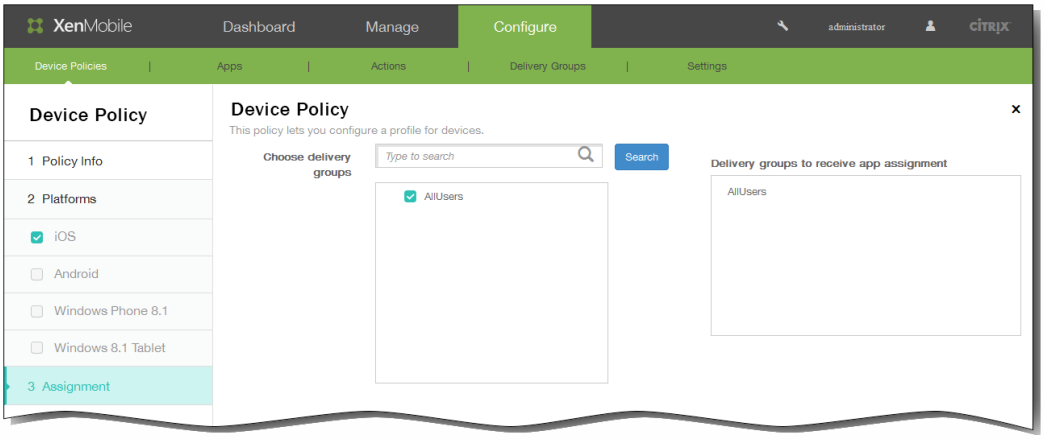


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



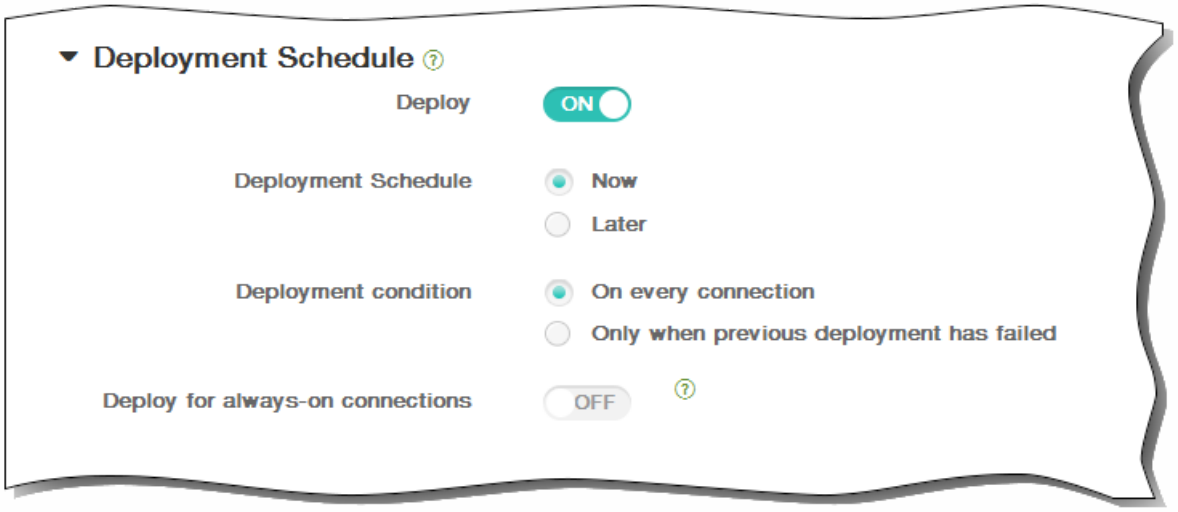
12. Haga clic en Next. Aparecerá la página de asignación AirPrint Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



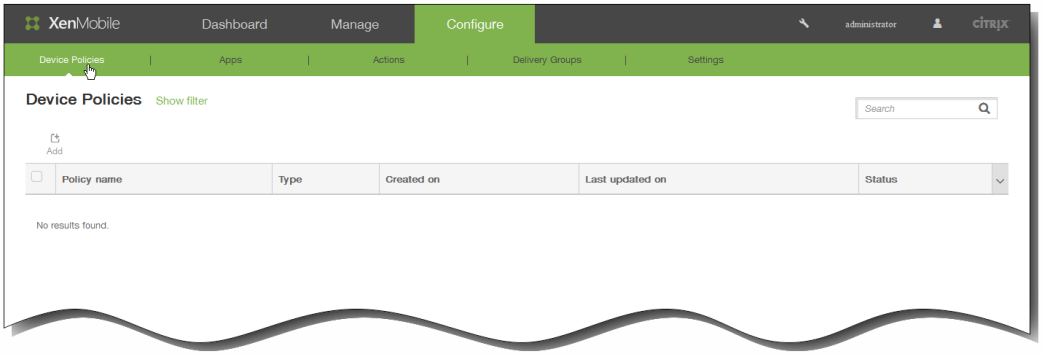
15. Haga clic en Save para guardar la directiva.

Para agregar una directiva de calendarios (CalDAV) para dispositivos iOS

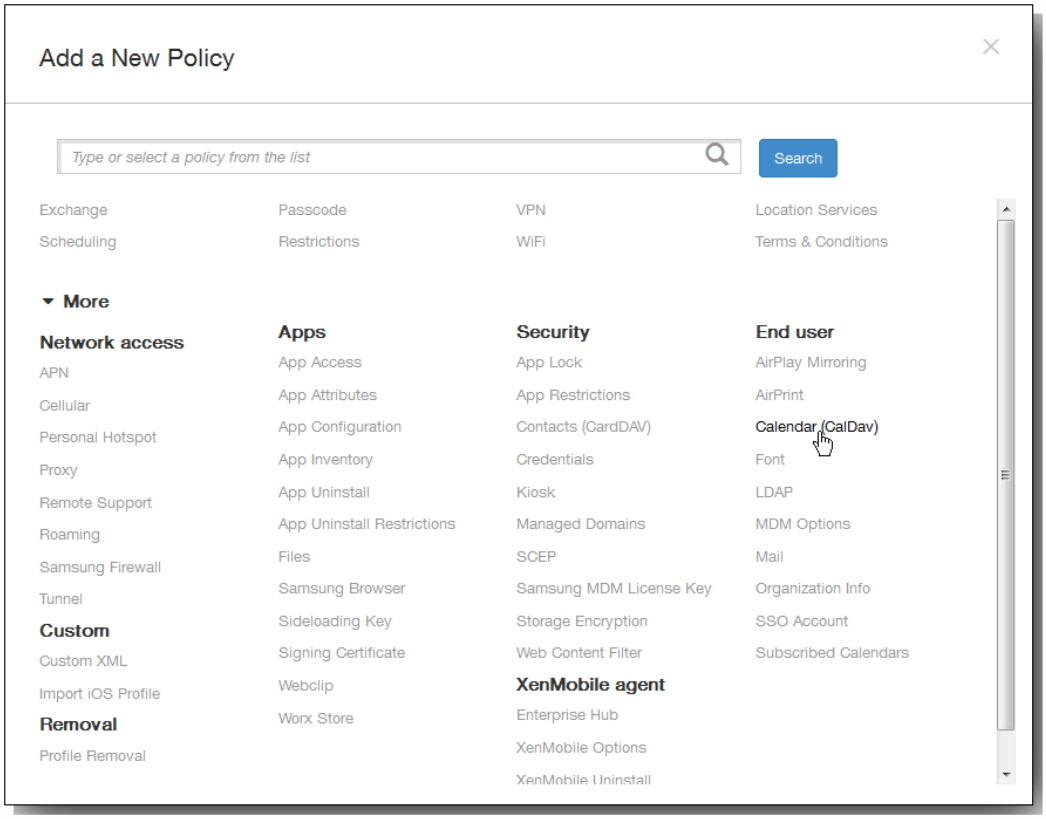
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos si quiere agregar una cuenta de calendarios iOS (CalDAV) a los dispositivos iOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de planificación con cualquier servidor que admita CalDAV.

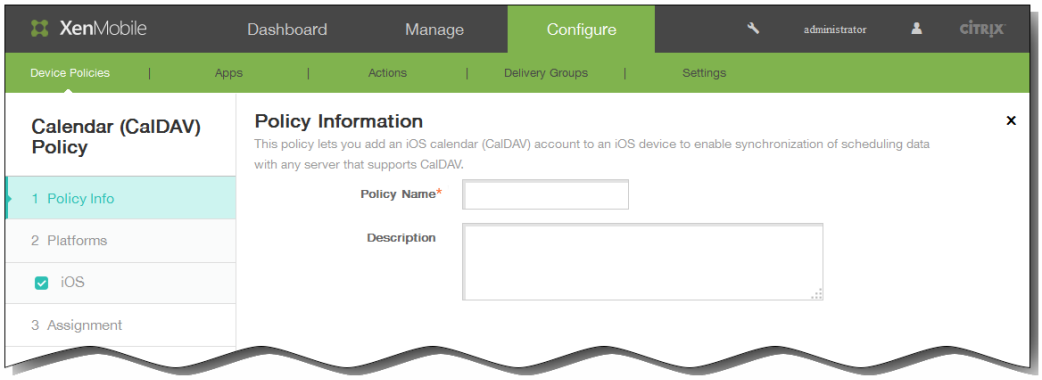
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



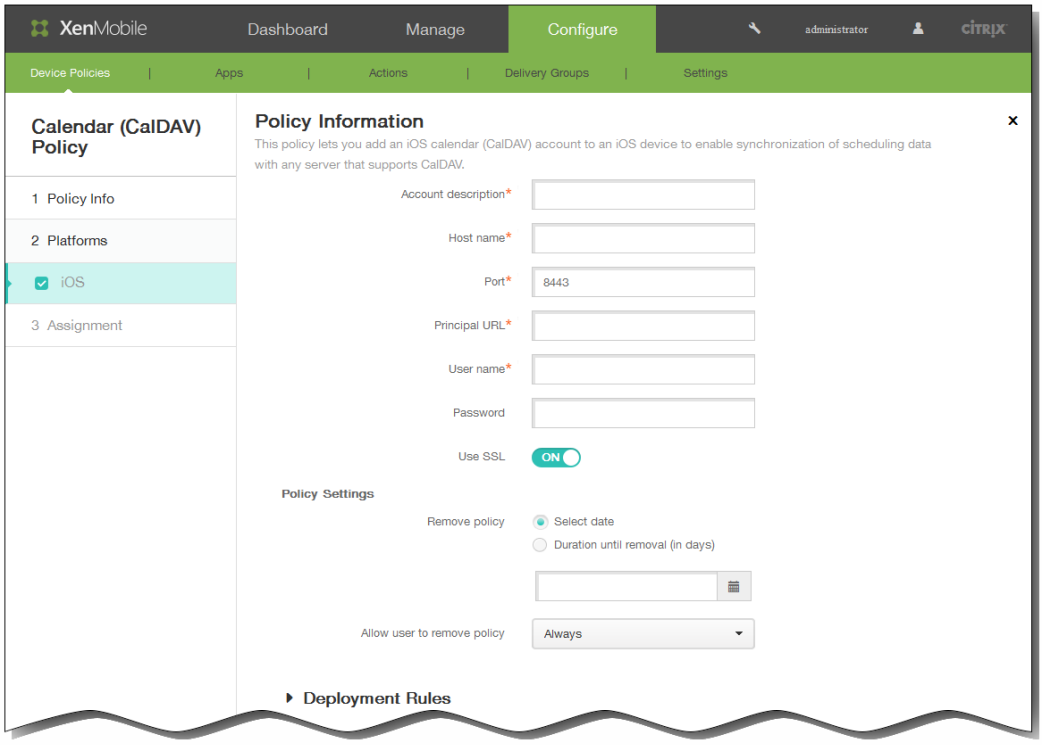
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en Calendar (CalDAV). Aparecerá la página Calendar (CalDAV) Policy.



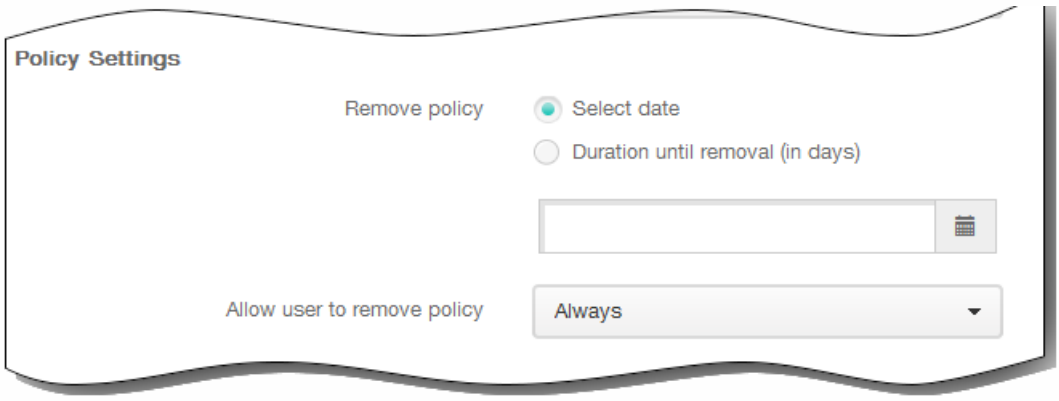
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



6. En la página de información iOS Platform, escriba la información siguiente:
   1. Account description. Escriba la descripción de la cuenta. Este campo es obligatorio.
   2. Host name. Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
   3. Port. Especifique el puerto con el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es 8443.
   4. Principal URL. Indique la URL base del calendario del usuario.
   5. User name. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.

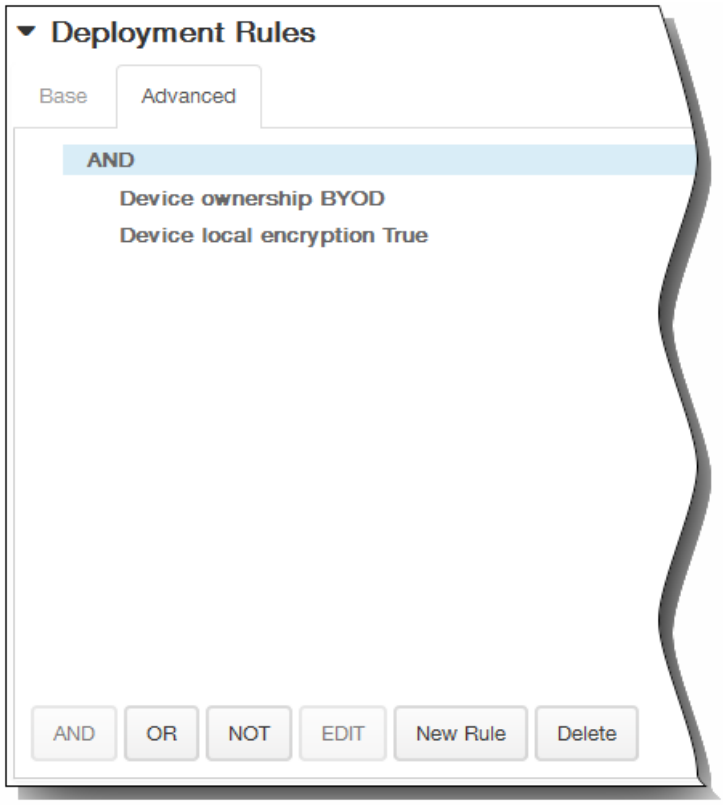
6. Password. Escriba una contraseña opcional de usuario.
7. Use SSL. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. El valor predeterminado es On.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



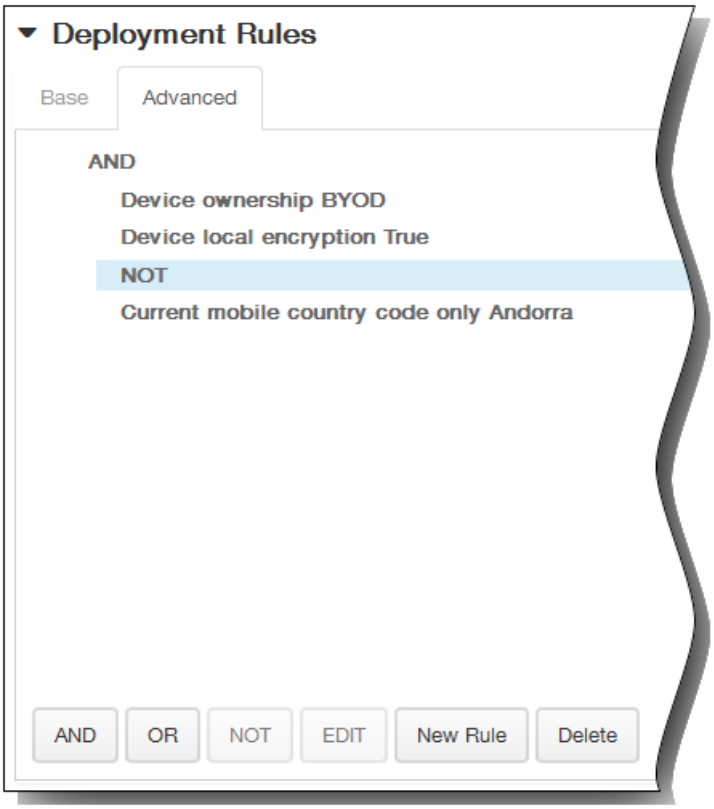
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

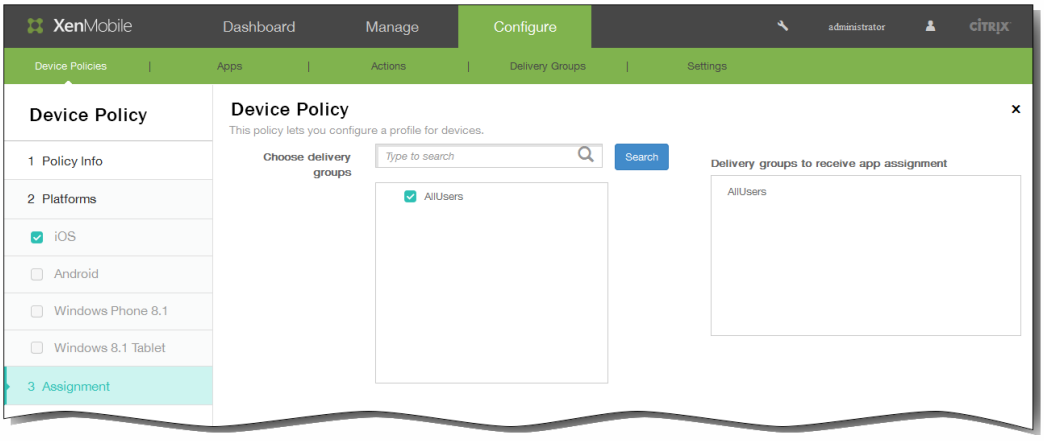


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



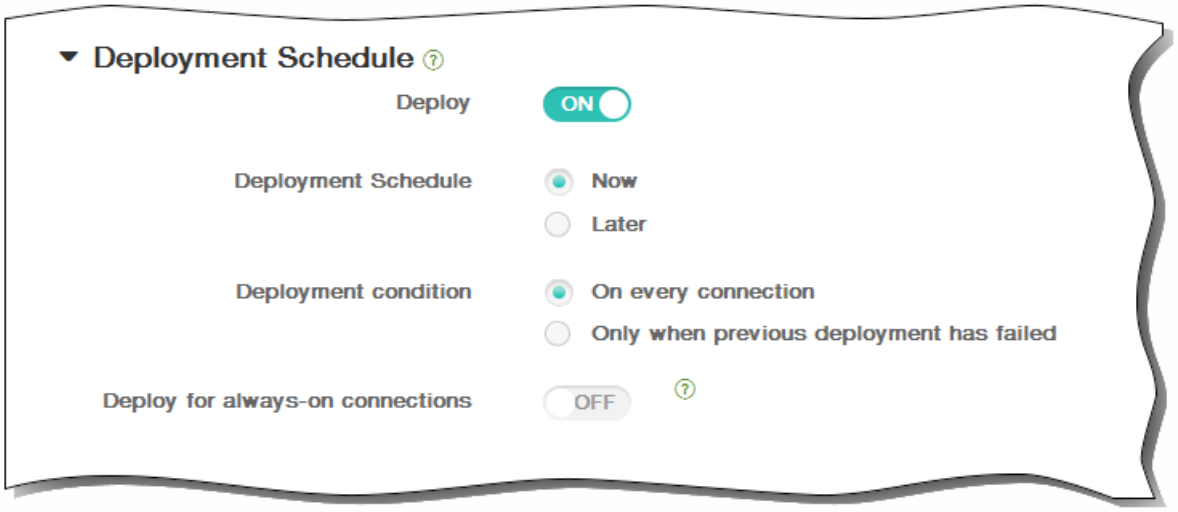
12. Haga clic en Next. Aparecerá la página de asignación Calendar (CalDAV) Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



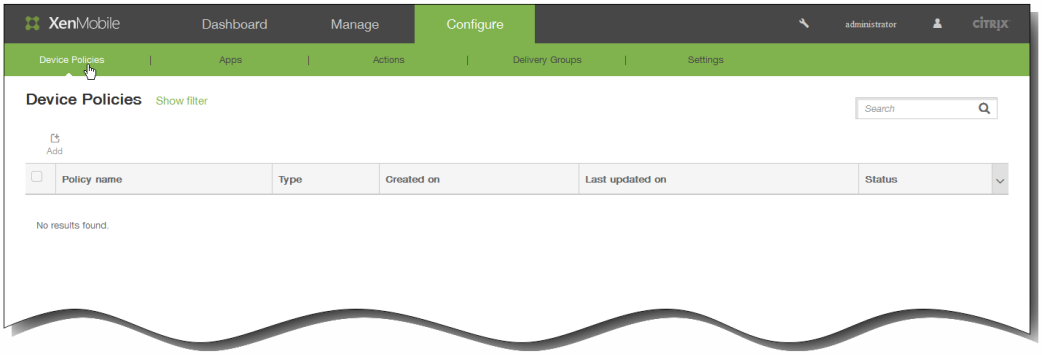
15. Haga clic en Save para guardar la directiva.

Para agregar una directiva de contactos (CardDAV) para dispositivos iOS

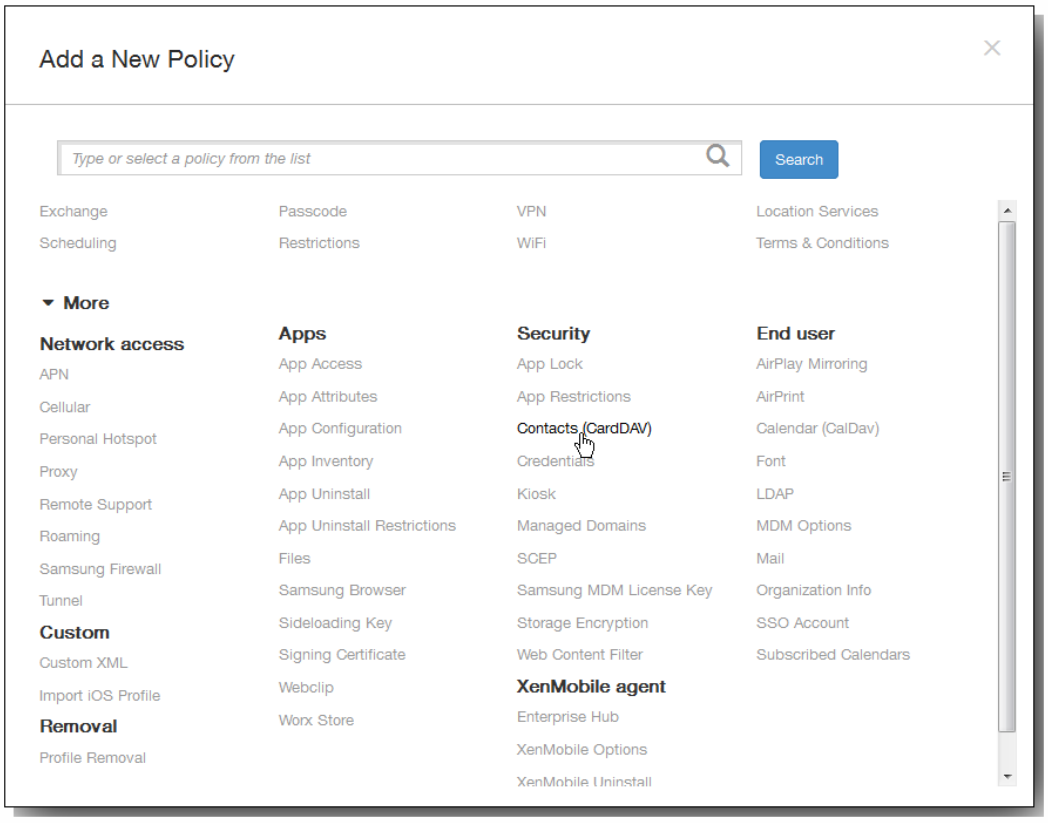
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos si quiere agregar una cuenta de contactos iOS (CardDAV) en los dispositivos iOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de contacto con cualquier servidor que admita CardDAV.

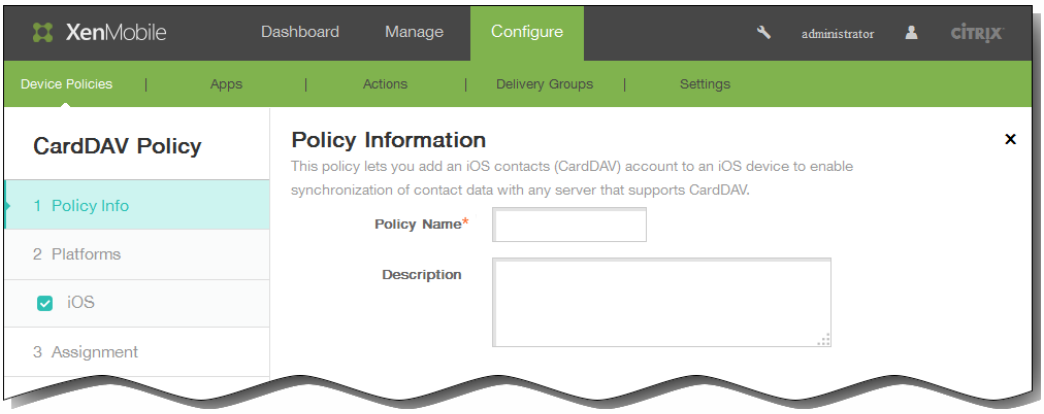
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



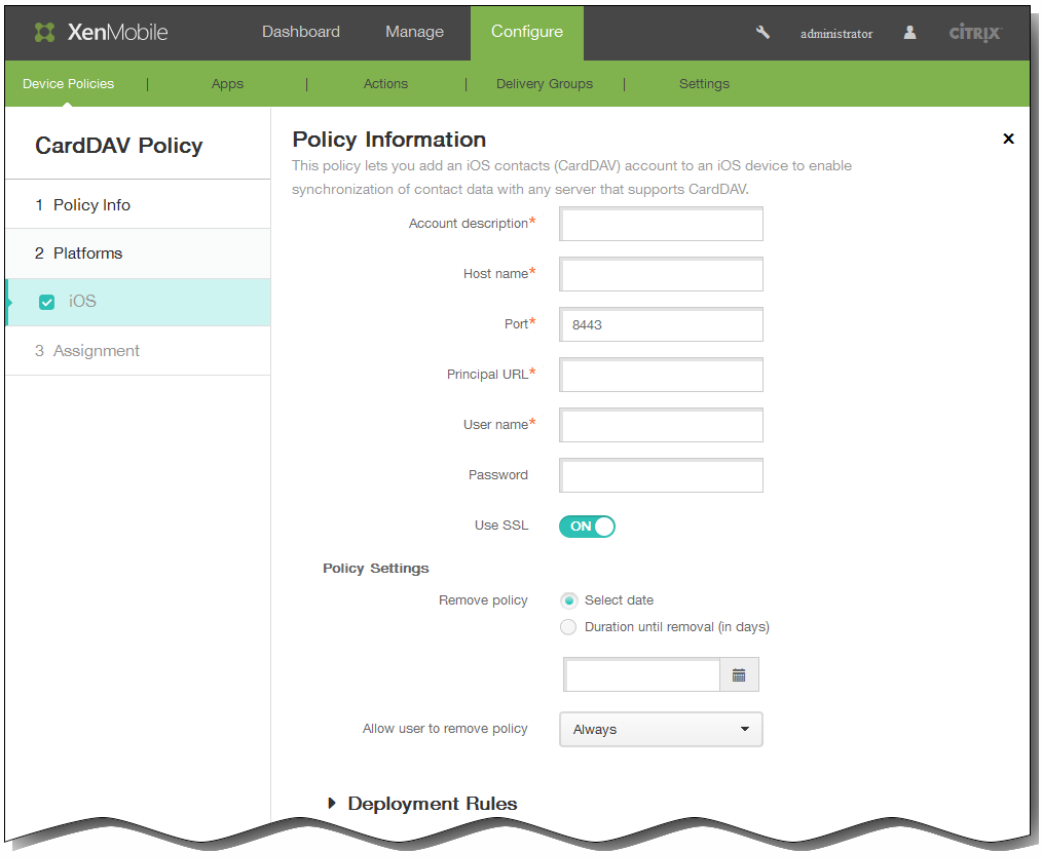
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, a continuación, en Security, haga clic en Contacts CardDAV. Aparecerá la página CardDAV Policy.



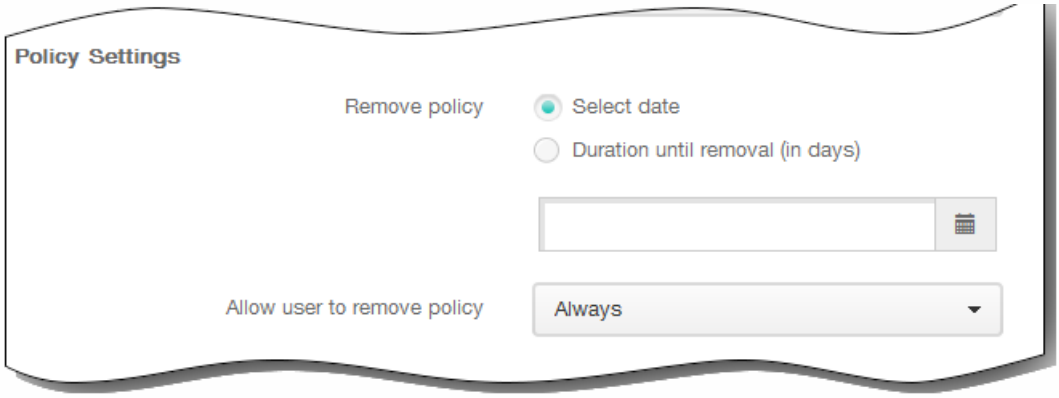
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



6. En la página de información iOS Platform, escriba la información siguiente:
   1. Account description. Indique una descripción de la cuenta. Este campo es obligatorio.
   2. Host name. Escriba la dirección del servidor CardDAV. Este campo es obligatorio.

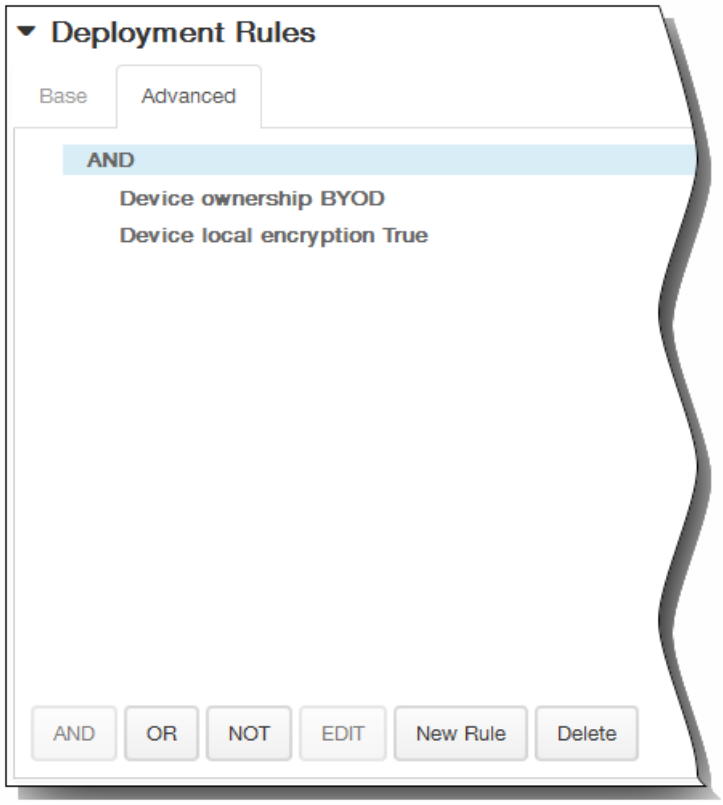
3. Port. Especifique el puerto con el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es 8443.
4. Principal URL. Indique la URL base para el calendario del usuario.
5. User name. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
6. Password. Escriba una contraseña opcional de usuario.
7. Use SSL. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. El valor predeterminado es ON.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



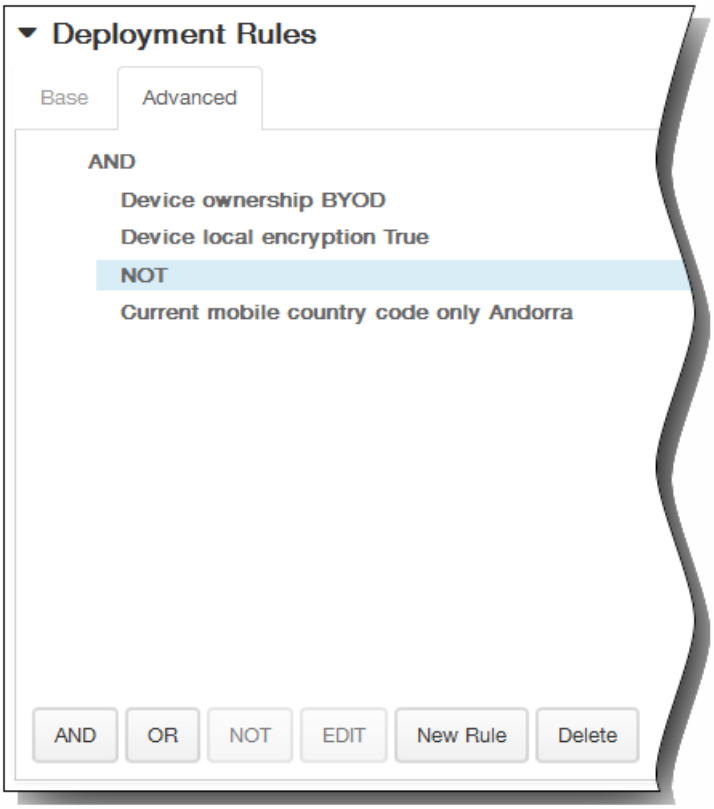
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

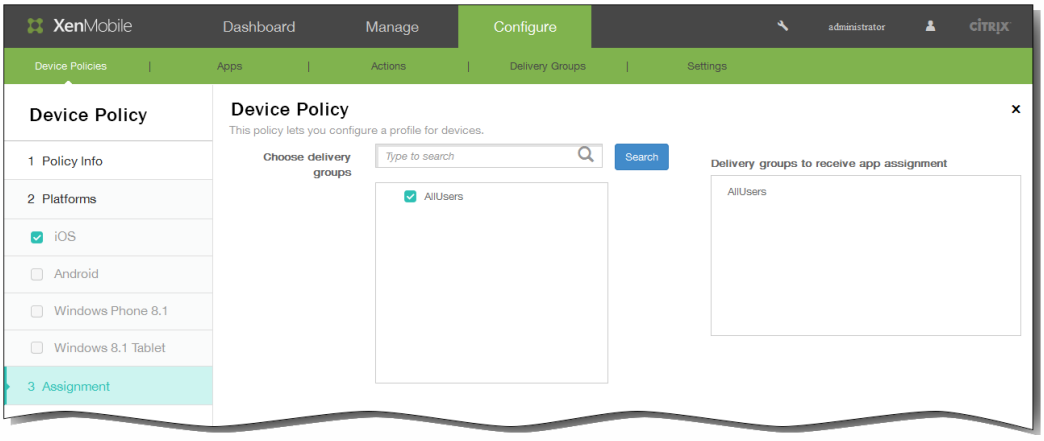


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



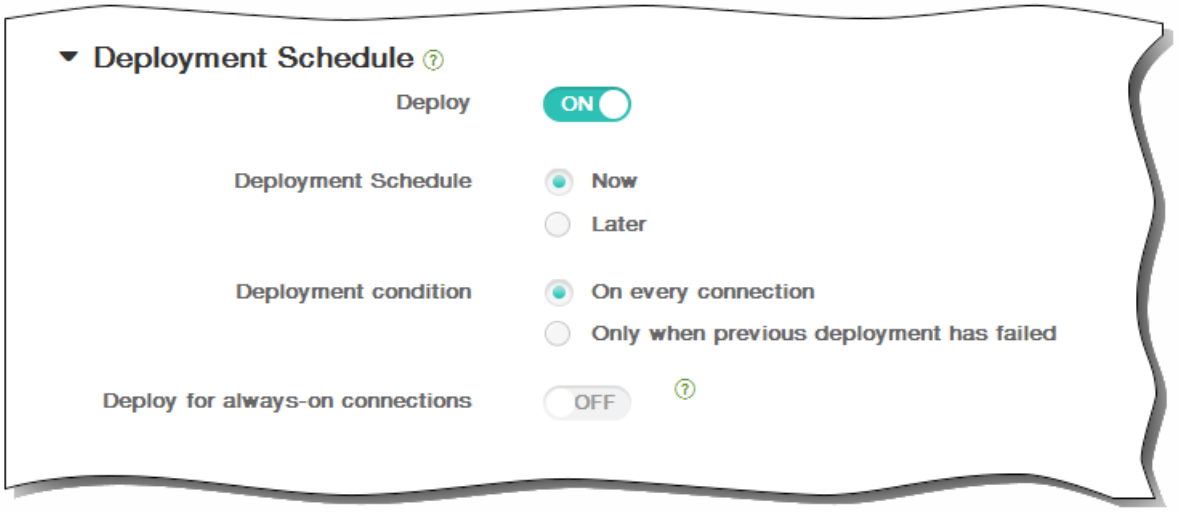
12. Haga clic en Next. Aparecerá la página de asignación CardDAV Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



15. Haga clic en Save para guardar la directiva.

Directivas de credenciales

May 05, 2016

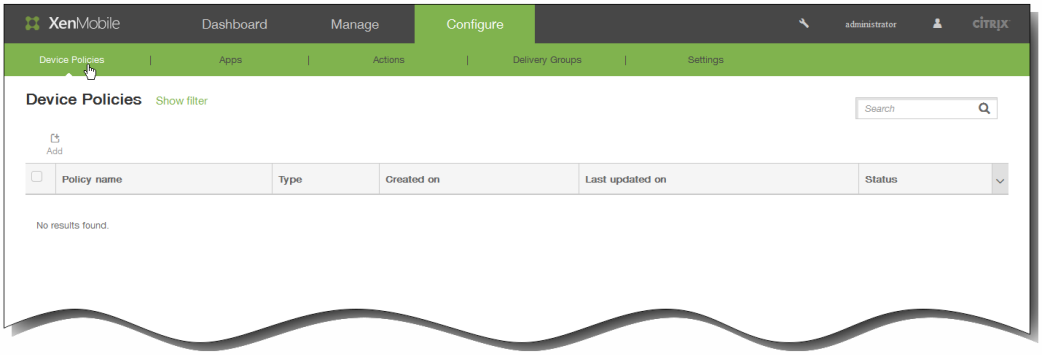
En XenMobile, puede crear directivas de credenciales para habilitar la autenticación integrada con la configuración de PKI (como una entidad de infraestructura PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor). Para obtener más información acerca de las credenciales, consulte Certificados en XenMobile.

Puede crear directivas de credenciales para dispositivos iOS, Android y tabletas Windows 8.1. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

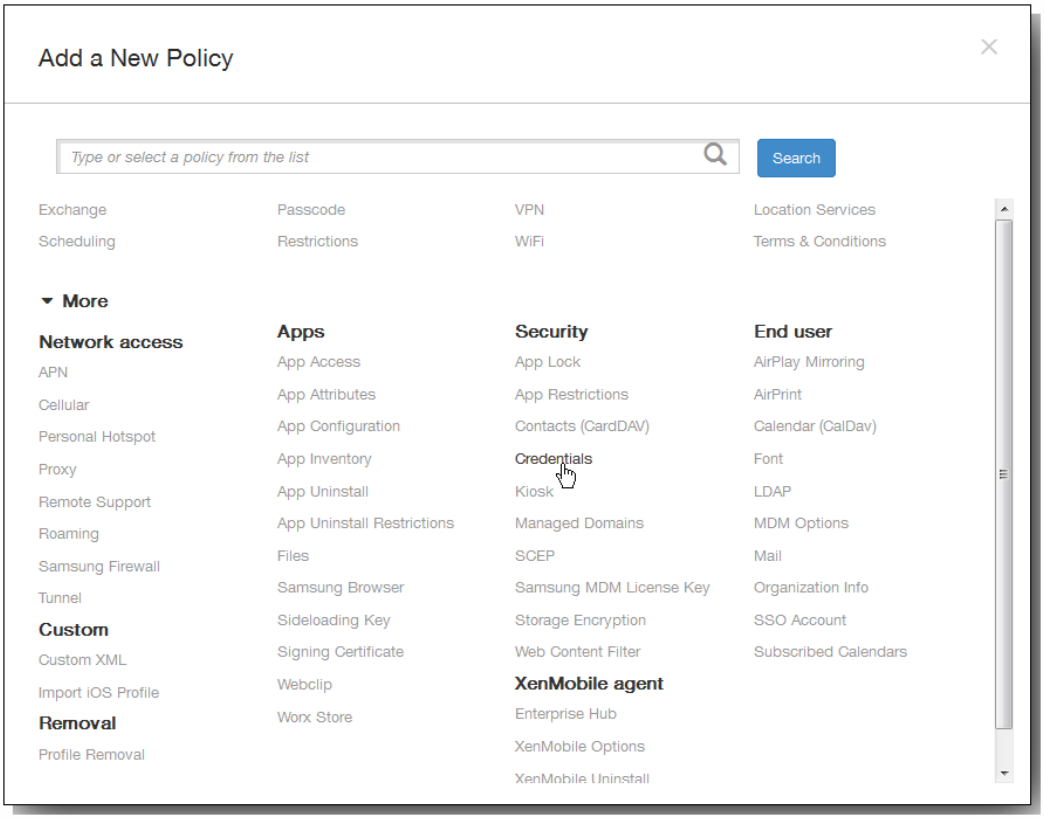
Para crear esta directiva, necesita la siguiente información:

- Información acerca de las credenciales que se utilizarán para cada plataforma, además de los certificados y las contraseñas que vaya a usar.

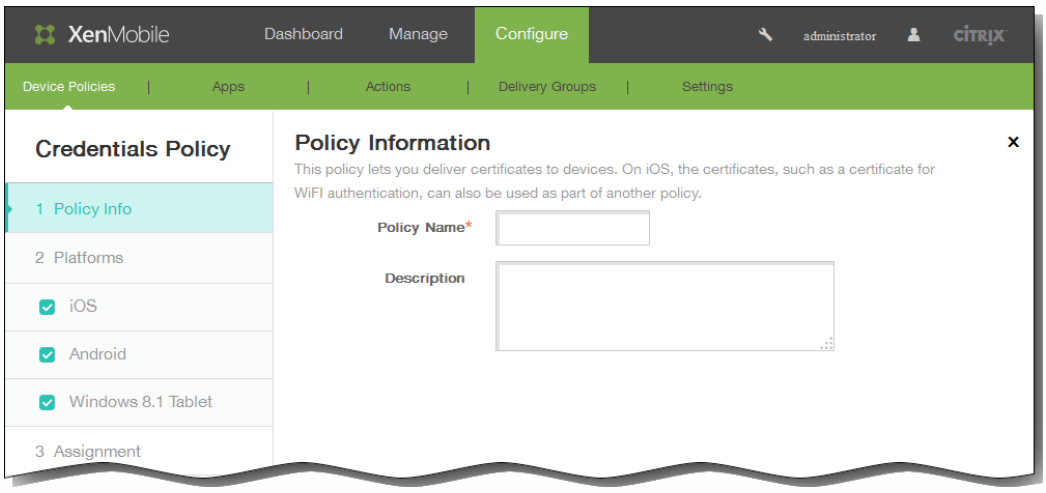
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



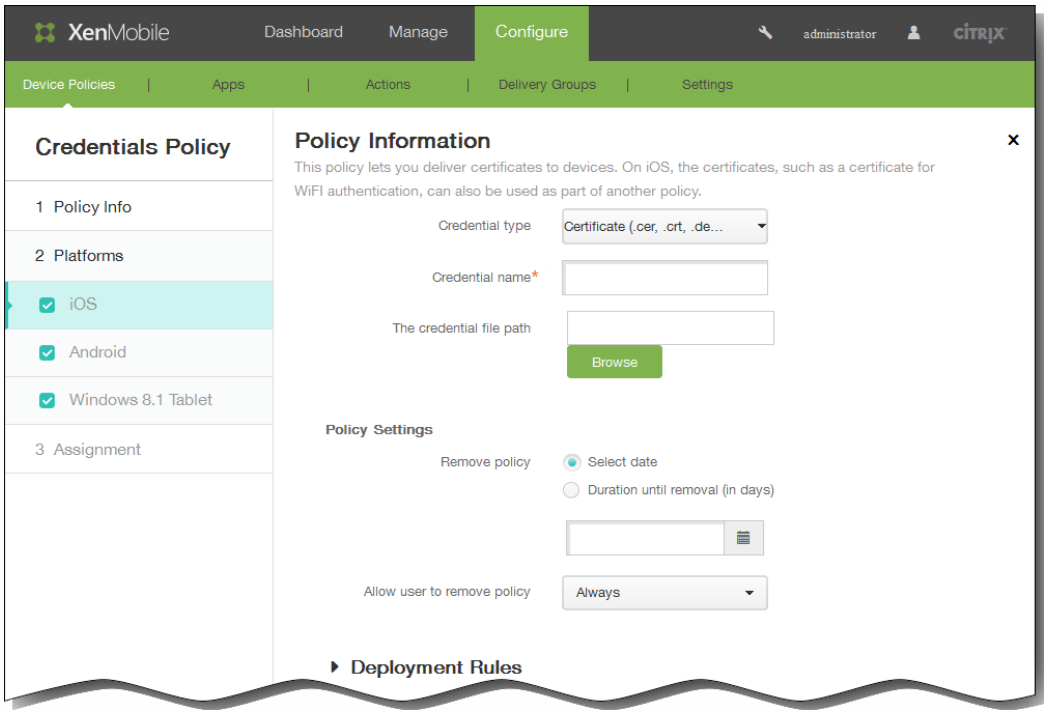
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.



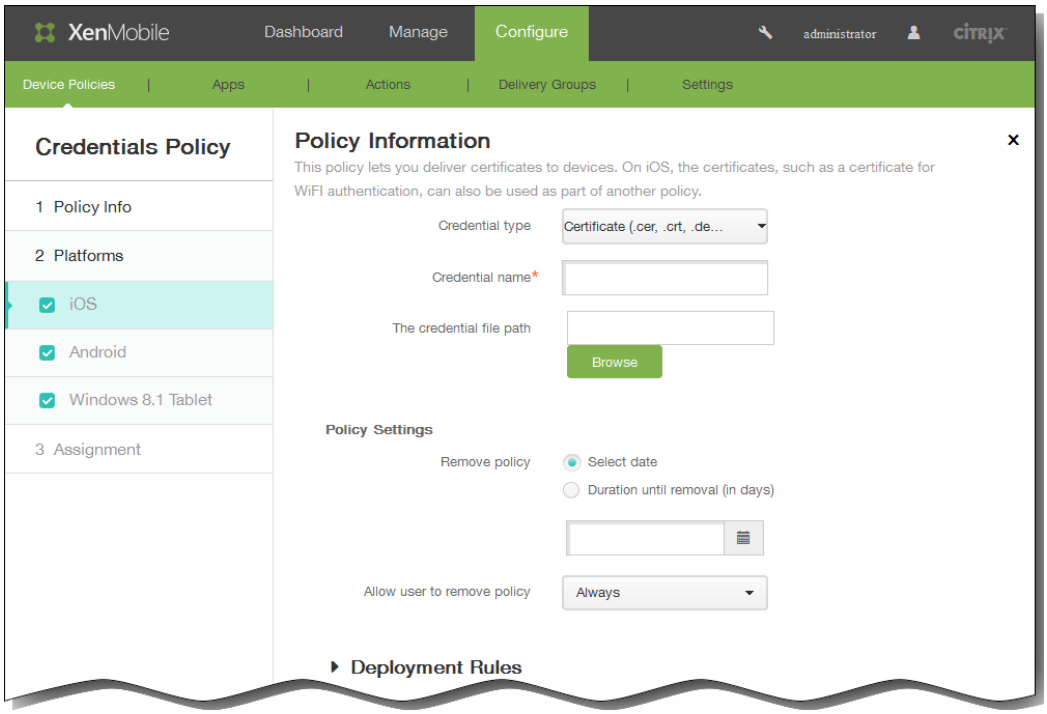
3. Haga clic en More y, a continuación, en Security, haga clic en Credentials. Aparecerá la página de información Credentials Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS.



6. En Platforms, seleccione las plataformas que quiera agregar.
   - Si ha seleccionado iOS, configure los siguientes parámetros:



Credential type. En la lista, haga clic en el tipo de credencial que se va a utilizar con esta directiva.

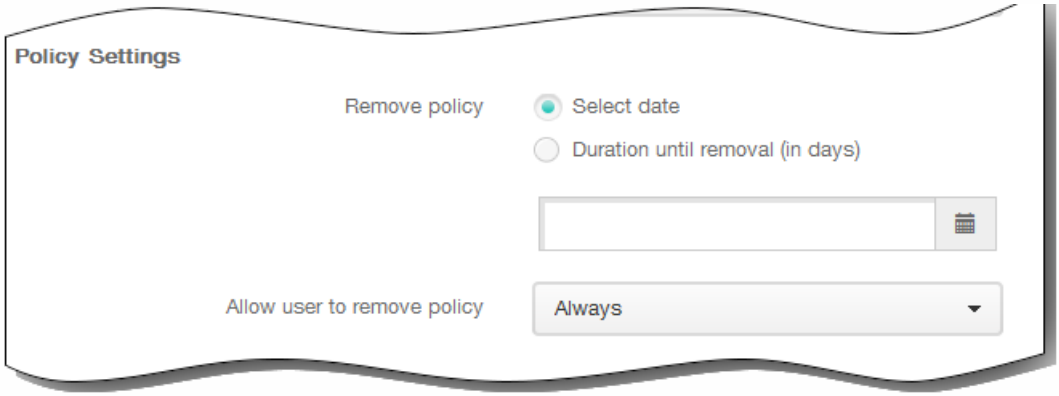
Proporcione la siguiente información para la credencial seleccionada:

- **Certificado**
  - Credential name. Escriba un nombre único para la credencial.

- The credential file path. Seleccione el archivo de credenciales. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.

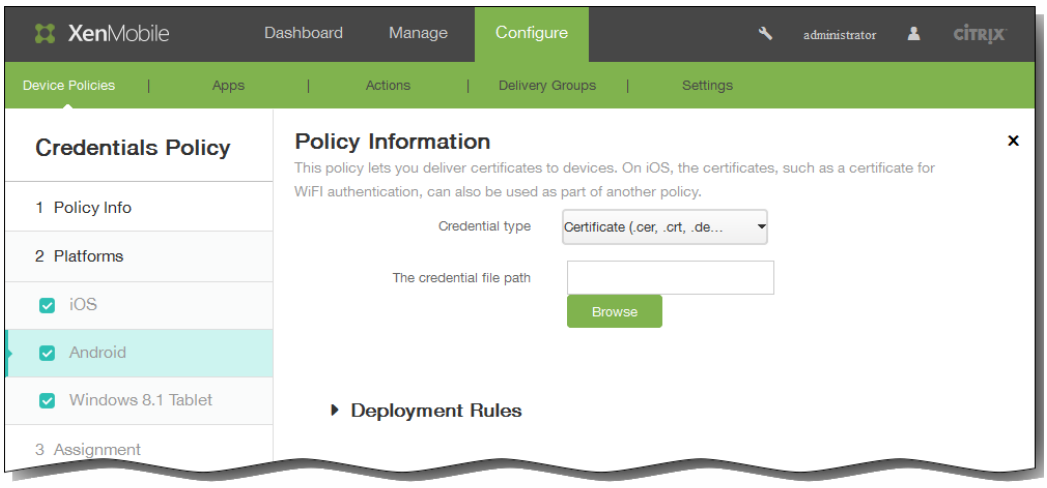
- Almacén de claves
  - Credential name. Escriba un nombre único para la credencial.
  - The credential file path. Seleccione el archivo de credenciales. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.
  - Password. Escriba una contraseña de almacén de claves para la credencial.
- Server certificate
  - Server certificate. En la lista, haga clic en el certificado que se va a utilizar.
- Credential provider
  - Credential provider. En la lista, haga clic en el nombre del proveedor de credenciales.

Configuraciones de directivas



1. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
2. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
3. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
4. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

- Si ha seleccionado Android, configure los siguientes parámetros:

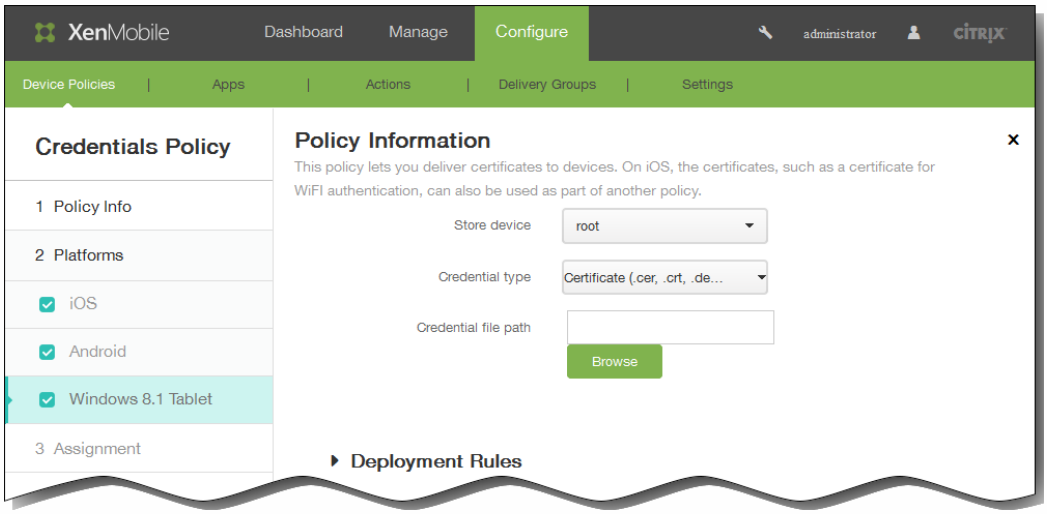


Credential type. En la lista, haga clic en el tipo de credencial que se va a utilizar con esta directiva.

Proporcione la siguiente información para la credencial seleccionada:

- Certificado
  - Credential name. Escriba un nombre único para la credencial.
  - The credential file path. Seleccione el archivo de credenciales. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.
- Almacén de claves
  - Credential name. Escriba un nombre único para la credencial.
  - The credential file path. Seleccione el archivo de credenciales. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.
  - Password. Escriba una contraseña de almacén de claves para la credencial.
- Server certificate
  - Server certificate. En la lista, haga clic en el certificado que se va a utilizar.
- Credential provider
  - Credential provider. En la lista, haga clic en el nombre del proveedor de credenciales.

- Si ha seleccionado Windows 8.1 Tablet, configure los siguientes parámetros:



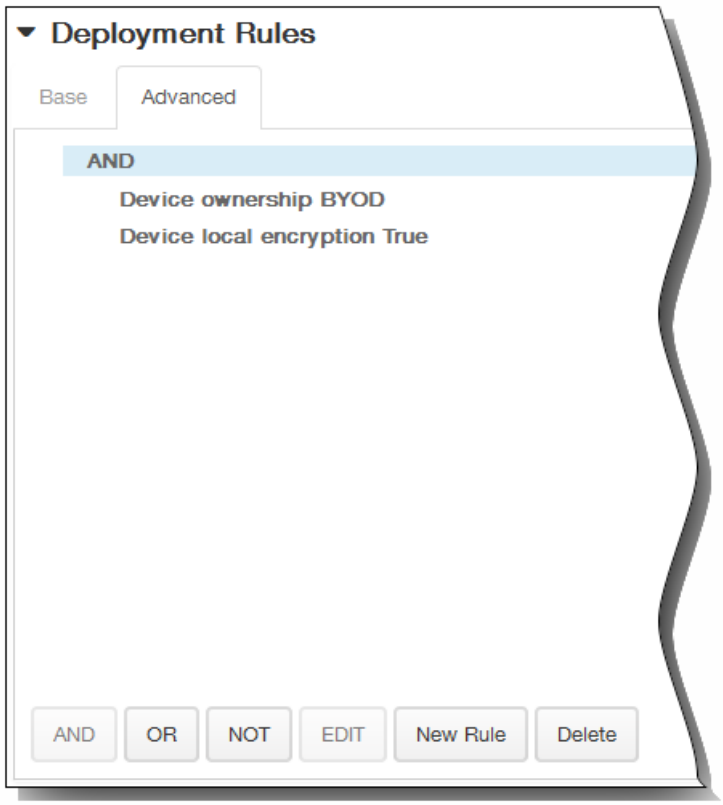
Store device. En la lista, haga clic en root, My o CA para designar la ubicación del almacén de certificados para la credencial. Con la opción My, la credencial se guarda en los almacenes de certificados de los usuarios.

Con la opción Credential type, el certificado es el único tipo de credencial para tabletas Windows 8.1.

The credential file path. Seleccione el archivo de credenciales. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.

7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

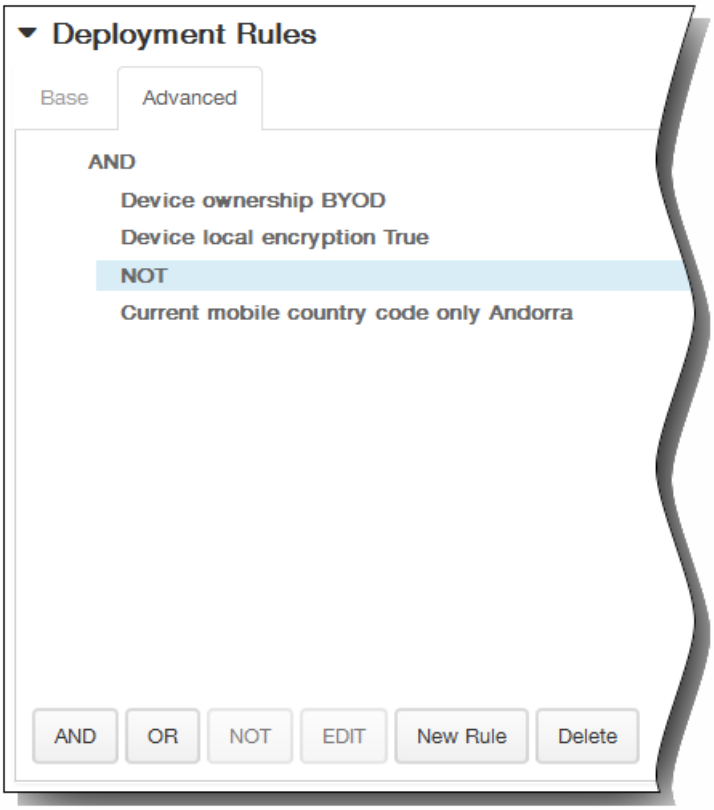
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



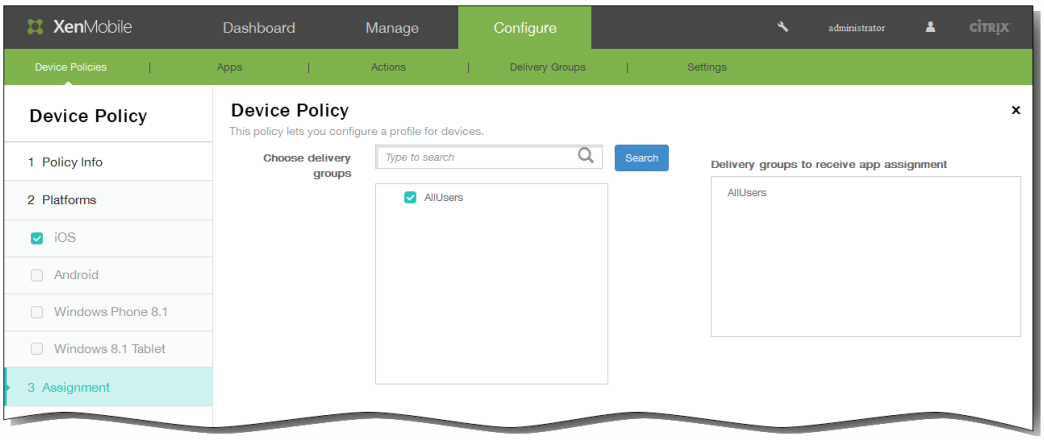
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



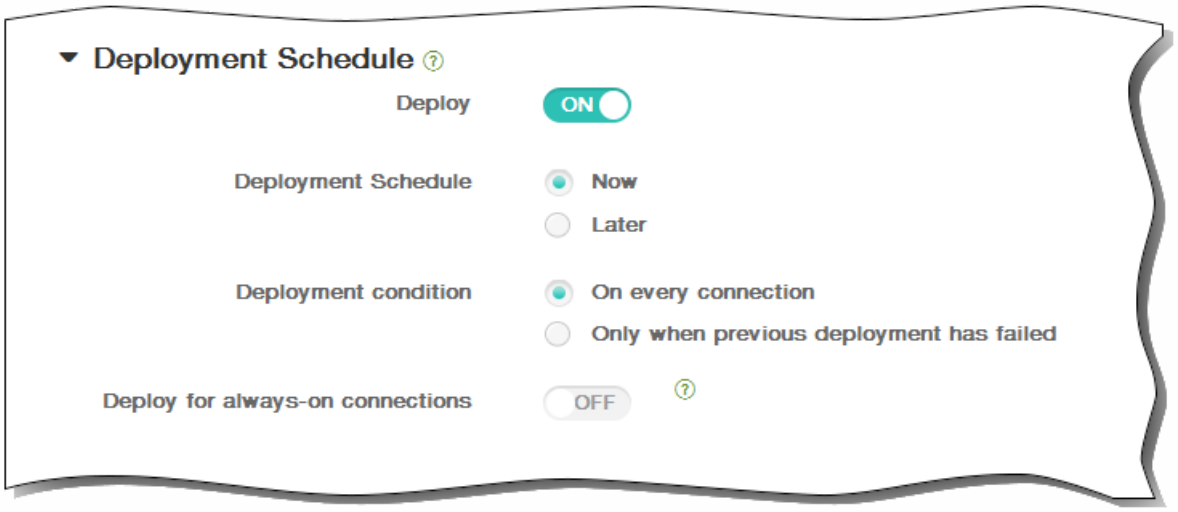
8. Haga clic en Next. Aparecerá la página de asignación Credentials Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

Para agregar una directiva de pantalla completa para dispositivos Samsung SAFE

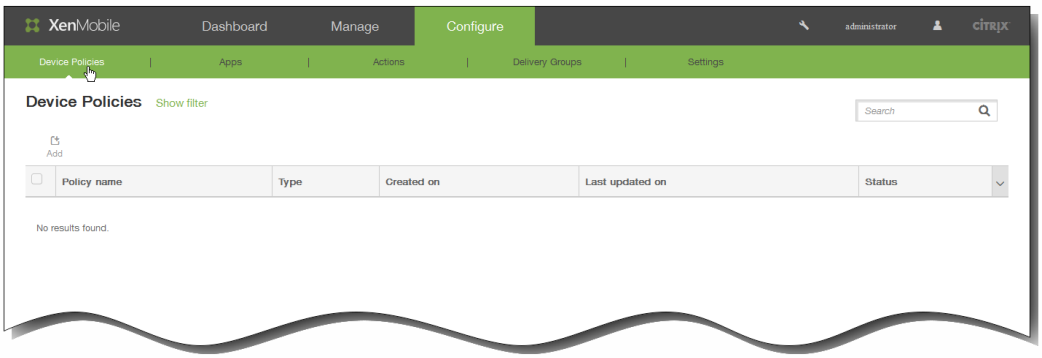
May 05, 2016

En XenMobile, puede crear una directiva de pantalla completa para especificar que, en los dispositivos Samsung SAFE, solo se puede utilizar una aplicación o unas aplicaciones concretas. Esta directiva es útil para los dispositivos de empresa diseñados para ejecutar solo un tipo o clase específicos de aplicaciones. Asimismo, esta directiva permite elegir imágenes personalizadas para la pantalla de inicio y fondos para la pantalla de bloqueo del dispositivo cuando el dispositivo está en modo de pantalla completa.

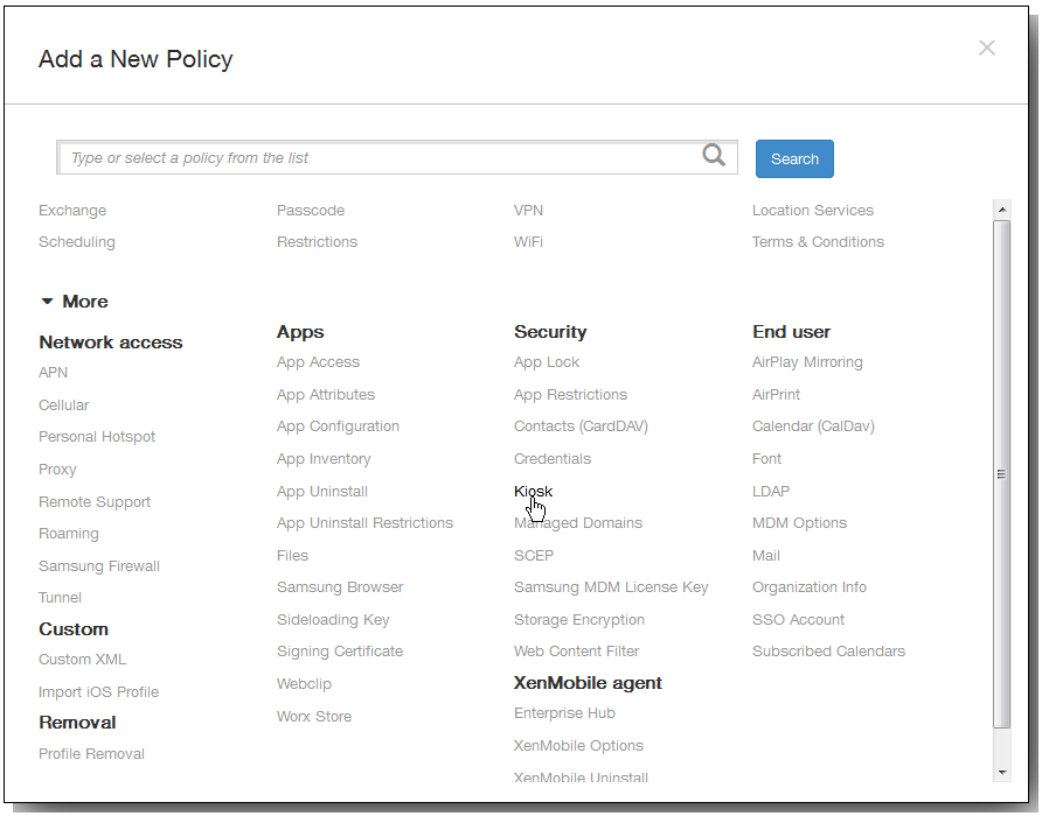
Nota:

- Todas las aplicaciones que especifique para el modo de pantalla completa deben estar ya instaladas en los dispositivos de los usuarios.
- Algunas opciones solo se aplican a Samsung Mobile Device Management API 4.0 y versiones posteriores.

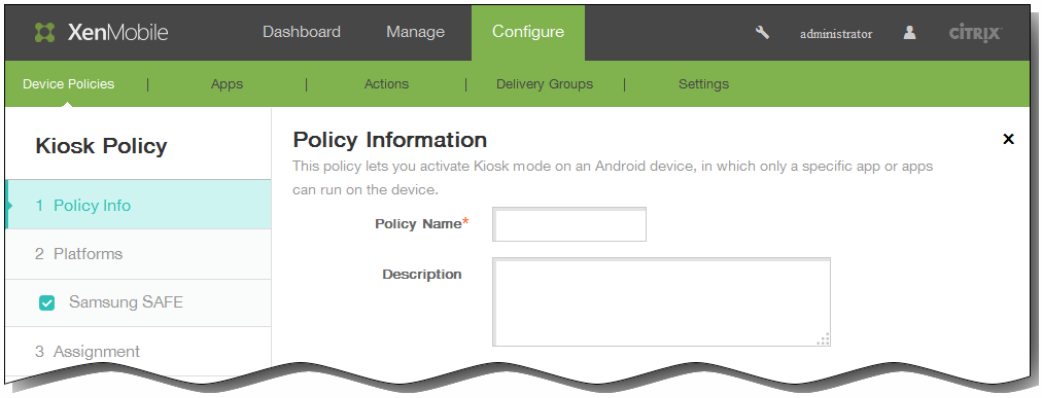
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



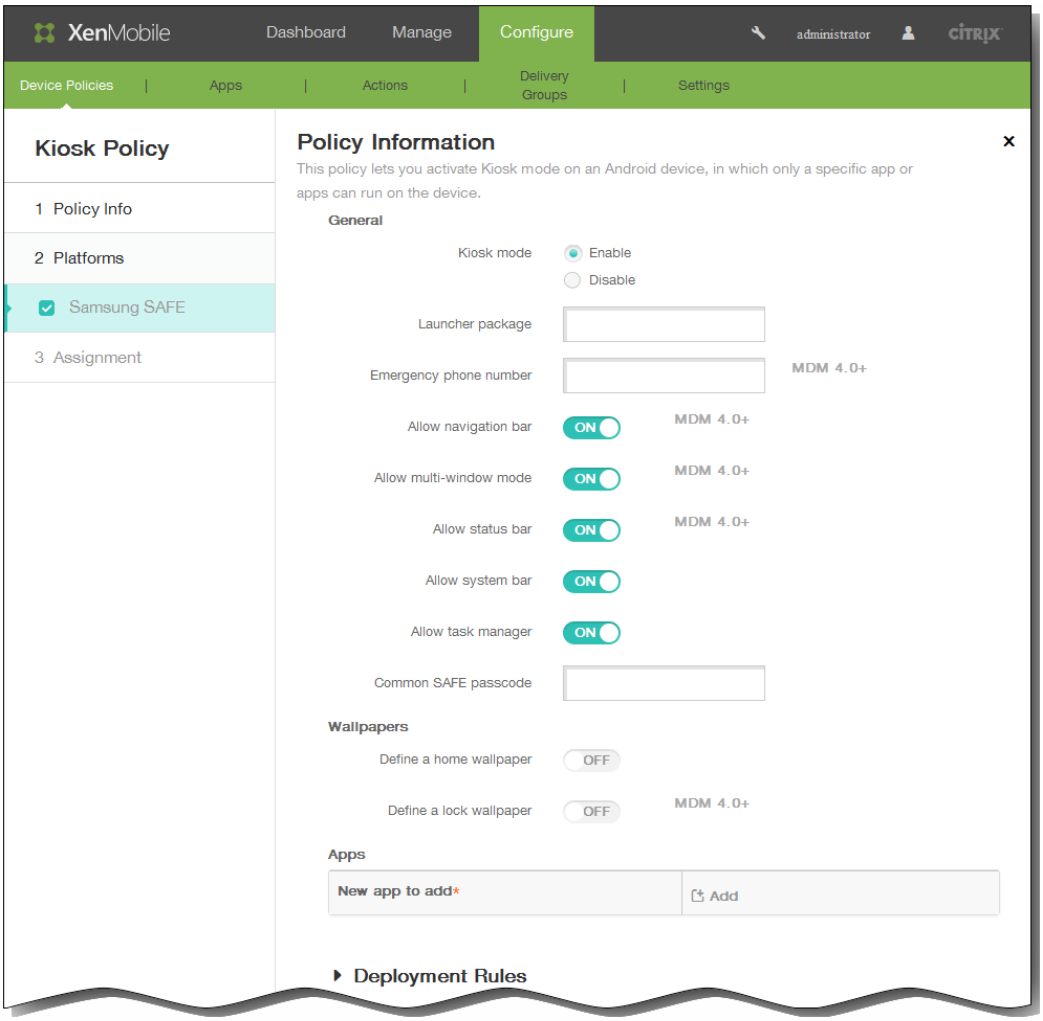
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, a continuación, en Security, haga clic en Kiosk. Aparecerá la página Kiosk Policy.



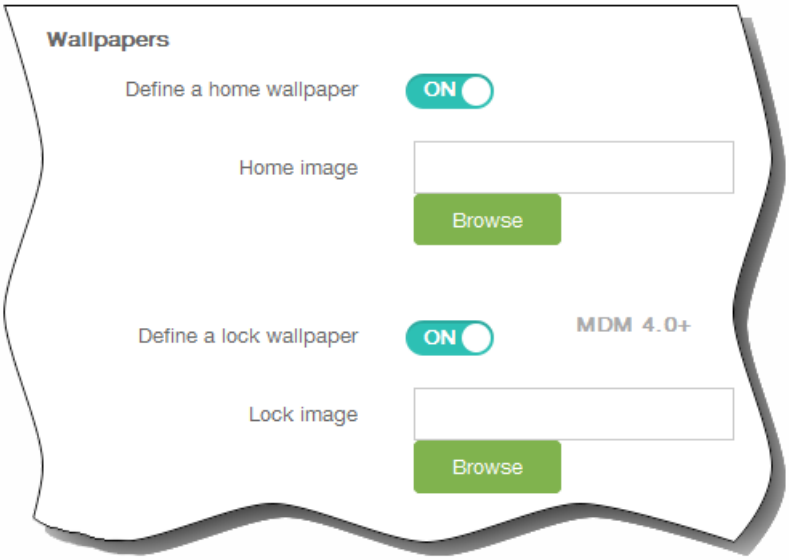
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información acerca de la plataforma Samsung SAFE.



6. En la página de información acerca de la plataforma Samsung SAFE, escriba la información siguiente:
    1. Kiosk mode. Haga clic en Enable o Disable. El valor predeterminado es Enable. Si hace clic en Disable, desaparecerán todas las opciones siguientes.
    2. Launcher package. Citrix recomienda dejar este campo en blanco si no se ha desarrollado internamente un programa de inicio para permitir que los usuarios abran la aplicación o las aplicaciones de pantalla completa. Si está usando un programa interno de inicio, escriba el nombre completo del paquete de aplicaciones de ese programa.
    3. Emergency phone number. Escriba un número de teléfono opcional. Una persona que encuentre un dispositivo perdido podrá usar este número para ponerse en contacto con su empresa. Solo se aplica a Samsung Mobile Device Management API 4.0 y versiones posteriores.
    4. Allow navigation bar. Seleccione si permitir que los usuarios vean y usen la barra de navegación en el modo de pantalla completa. Se aplica solo a MDM 4.0 y versiones posteriores.
    5. Allow multi-window mode. Seleccione si permitir que los usuarios usen varias ventanas en el modo de pantalla completa. Se aplica solo a MDM 4.0 y versiones posteriores.
    6. Allow status bar. Seleccione si permitir que los usuarios vean la barra de estado en el modo de pantalla completa. Se aplica solo a MDM 4.0 y versiones posteriores.
    7. Allow system bar. Seleccione si permitir que los usuarios vean la barra del sistema en el modo de pantalla completa.
    8. Allow task manager. Seleccione si permitir que los usuarios vean y usen el Administrador de tareas en el modo de pantalla completa.
    9. Common SAFE passcode. Si ha configurado una directiva general de códigos de acceso para todos los dispositivos

Samsung SAFE, escriba el mismo código opcional de la directiva en este campo.

10. Define a home wallpaper. Seleccione si utilizar una imagen personalizada para la pantalla de inicio en el modo de pantalla completa. El valor predeterminado es OFF.
11. Define a lock wallpaper. Seleccione si utilizar una imagen personalizada para la pantalla de bloqueo en el modo de pantalla completa. El valor predeterminado es OFF. Se aplica solo a MDM 4.0 y versiones posteriores. Si se habilita alguna de las opciones anteriores, aparece un campo para seleccionar la imagen personalizada. Para ello, haga clic en Browse y vaya a la ubicación de la imagen.



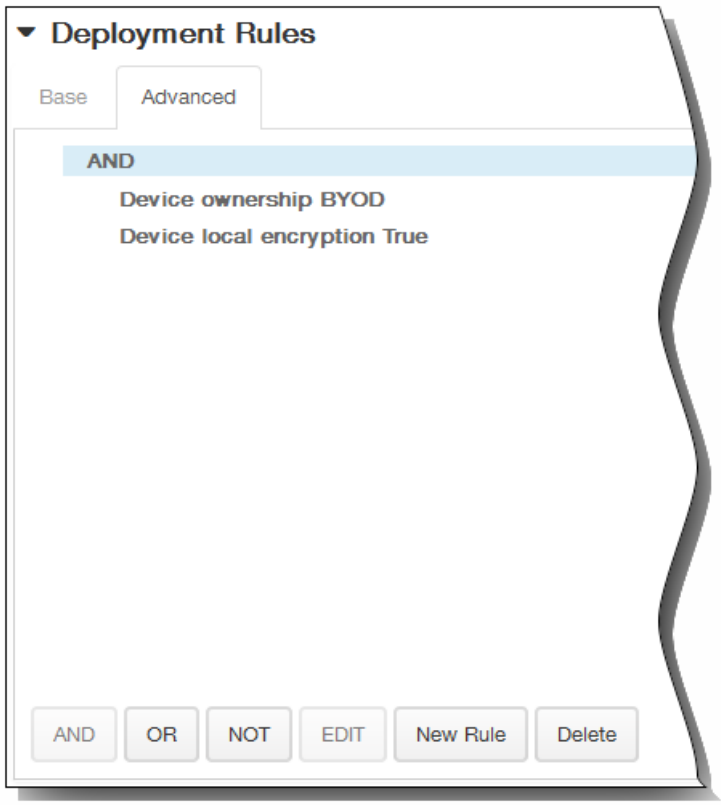
12. Apps. Haga clic en Add y lleve a cabo lo siguiente:
    1. New app to add. Escriba el nombre completo de la aplicación que se va a agregar. Por ejemplo, com.android.calendar permite a los usuarios utilizar la aplicación Calendario de Android.
    2. Haga clic en Add para agregar la aplicación, o bien haga clic en Cancel para no agregarla.
    3. Repita los pasos de i. y ii. para cada aplicación que quiera agregar.

    Nota: Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

    Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

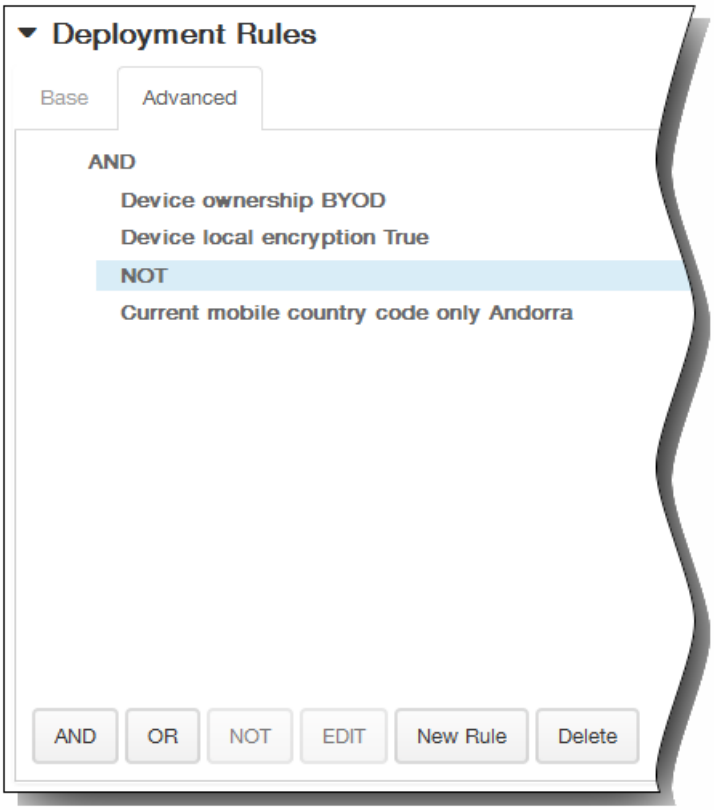
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



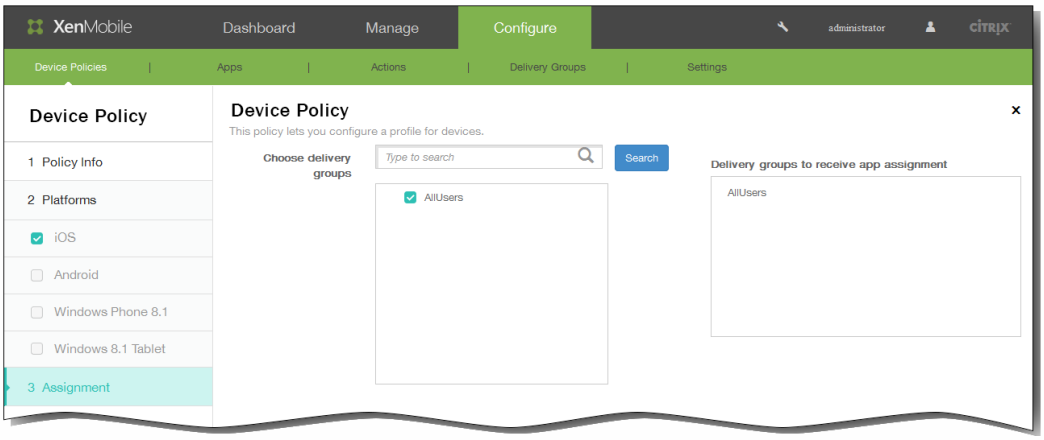
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



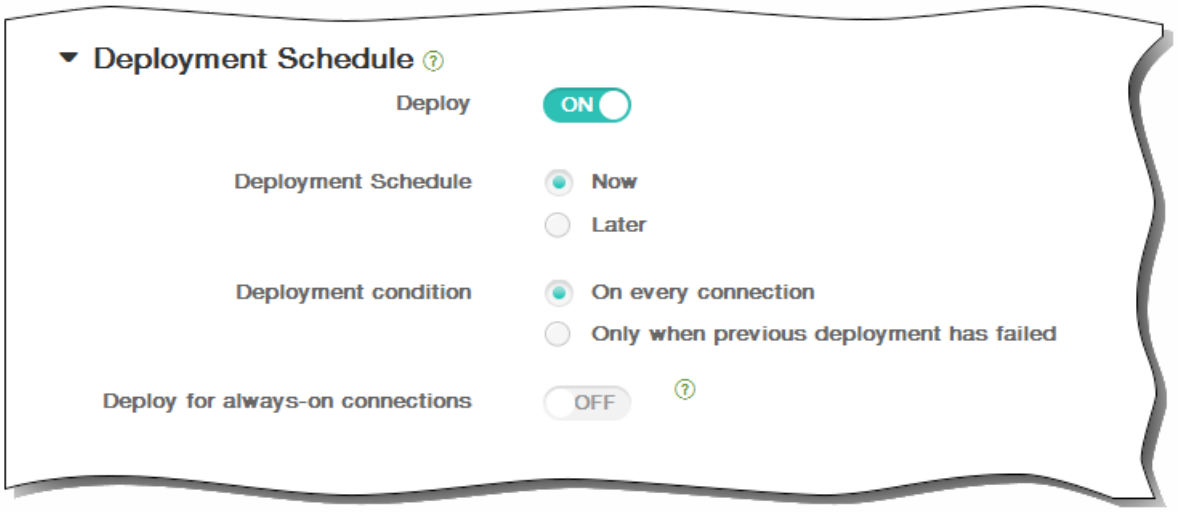
8. Haga clic en Next. Aparecerá la página de asignación Kiosk Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

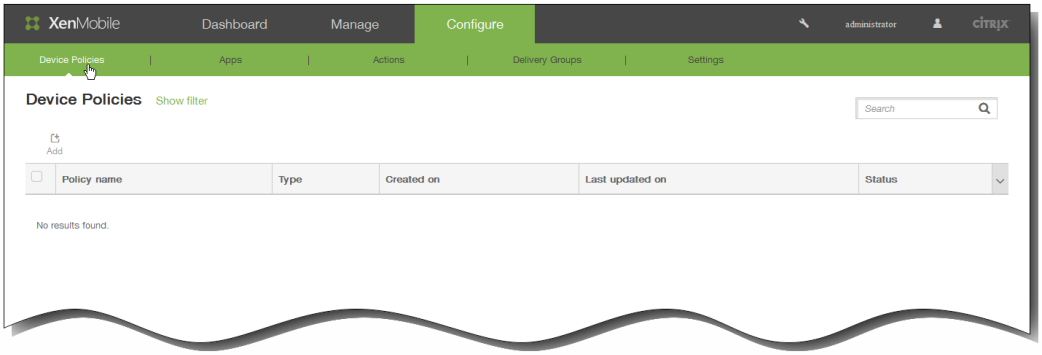
Para agregar una directiva de fuentes para dispositivos iOS

May 05, 2016

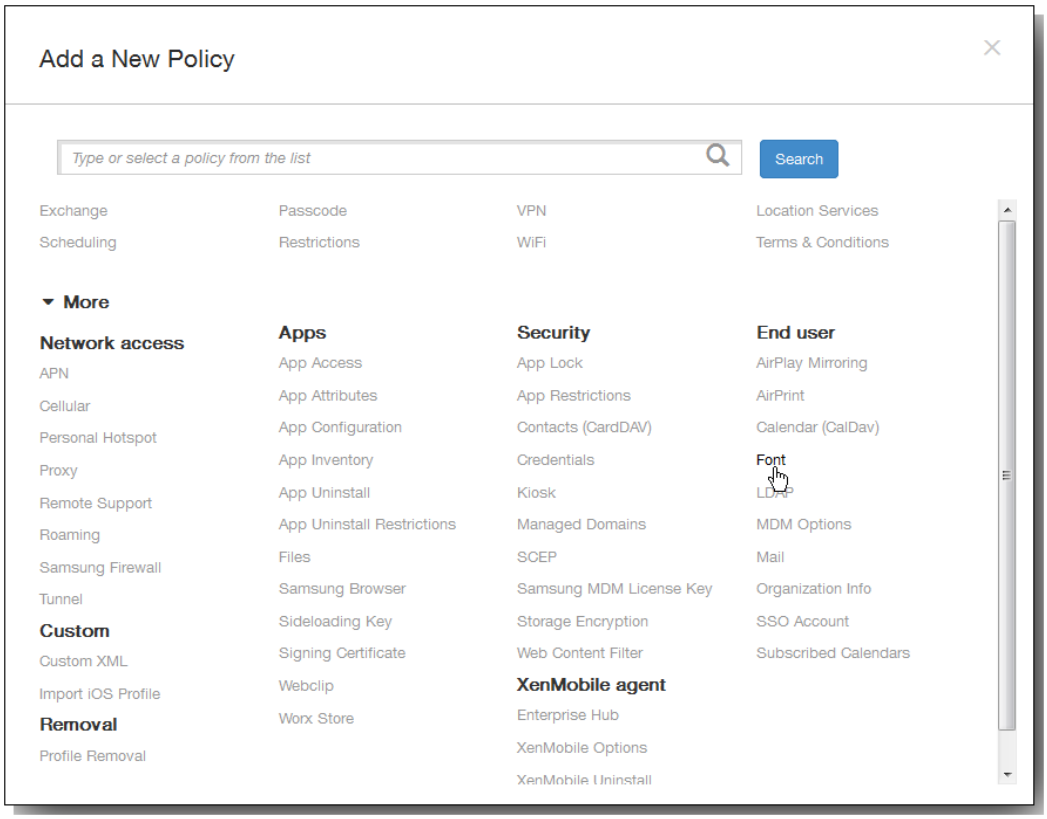
En XenMobile, puede agregar una directiva de dispositivos para agregar fuentes de texto adicionales a los dispositivos de los usuarios. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.oft). No se admiten las colecciones de fuentes (.ttc o .otc).

Nota: Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.

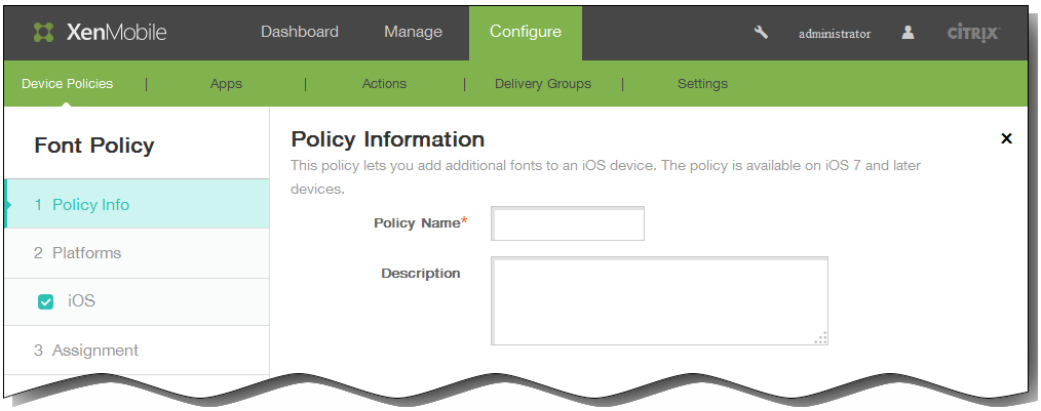
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



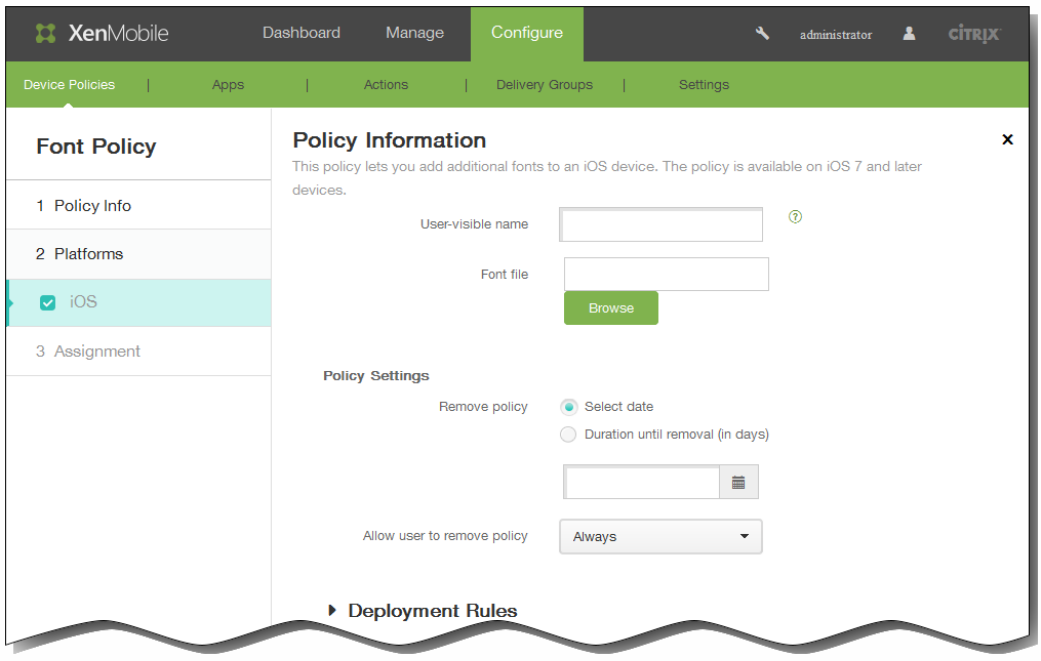
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en Font. Aparecerá la página Font Policy.

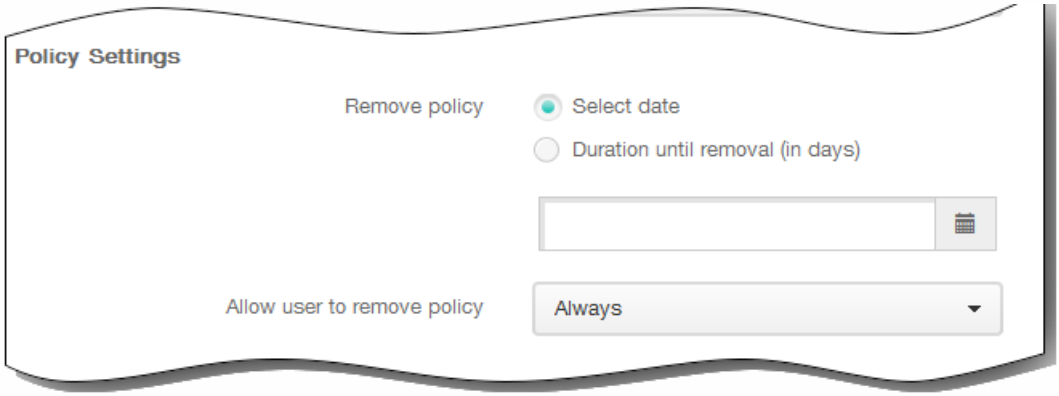


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



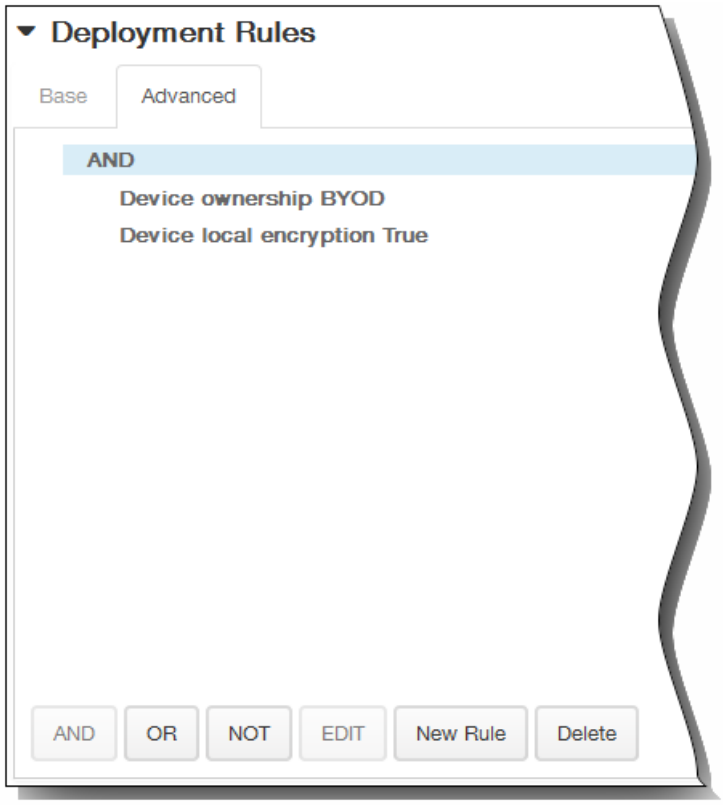
6. En la página de información iOS Platform, escriba la información siguiente:
   1. User-visible name. Escriba el nombre que verán los usuarios en sus listas de fuentes.
   2. Font file. Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en Browse y vaya a la ubicación del archivo.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.

10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



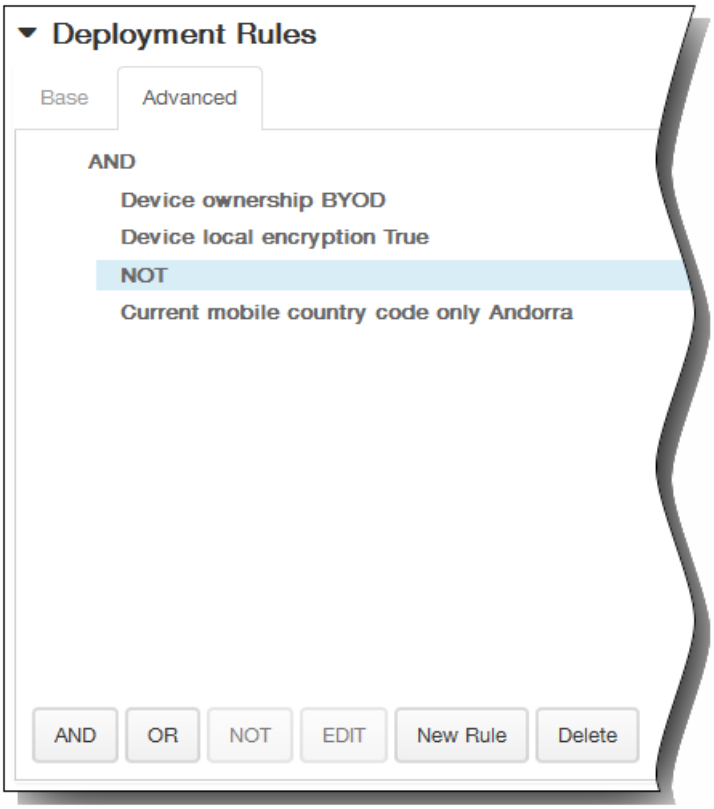
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

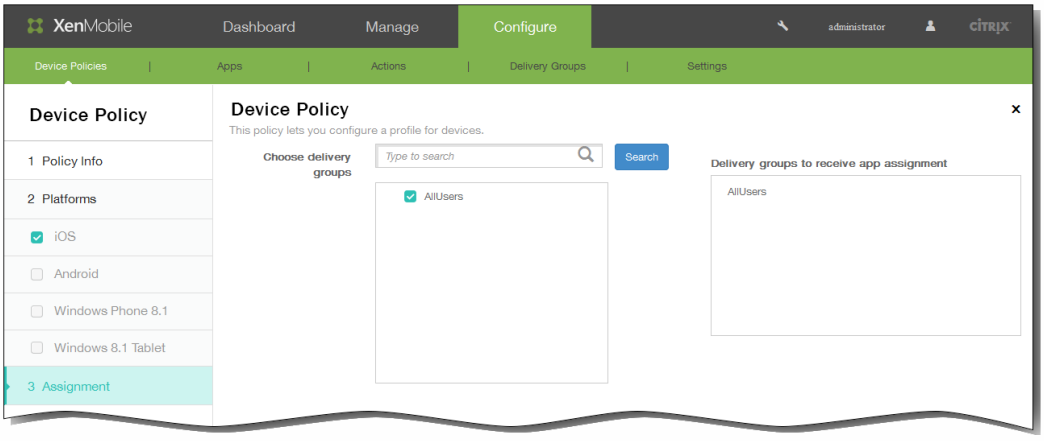


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



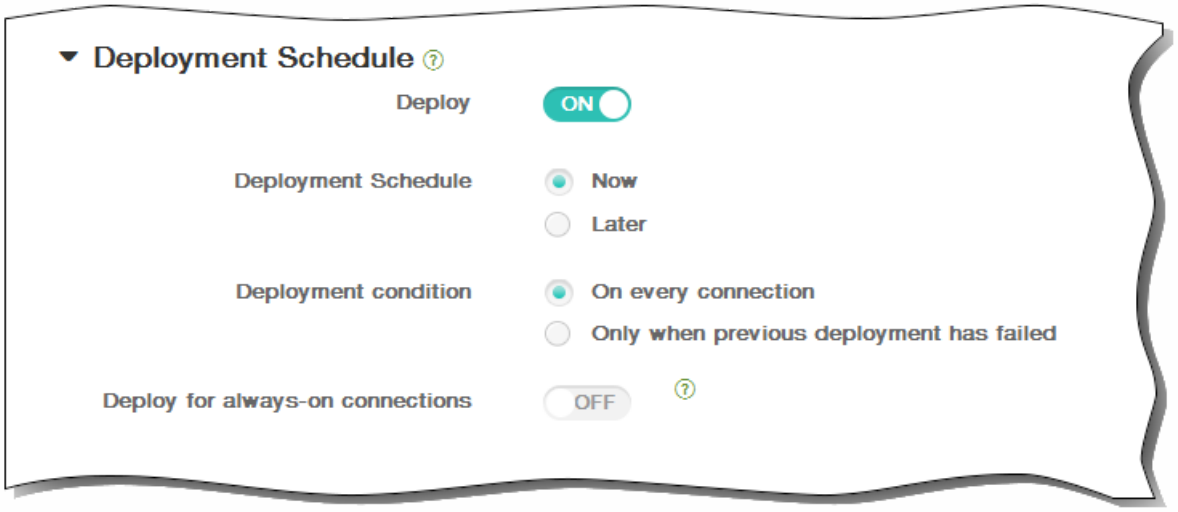
12. Haga clic en Next. Aparecerá la página de asignación Font Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



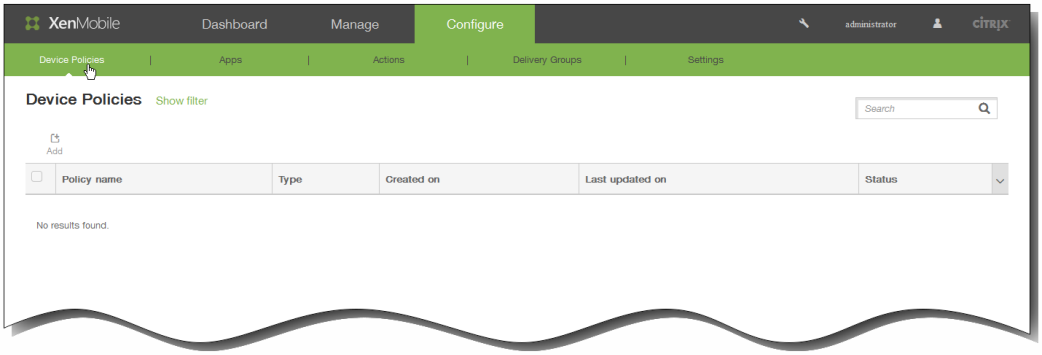
15. Haga clic en Save para guardar la directiva.

Para agregar una directiva de información de organización para dispositivos iOS

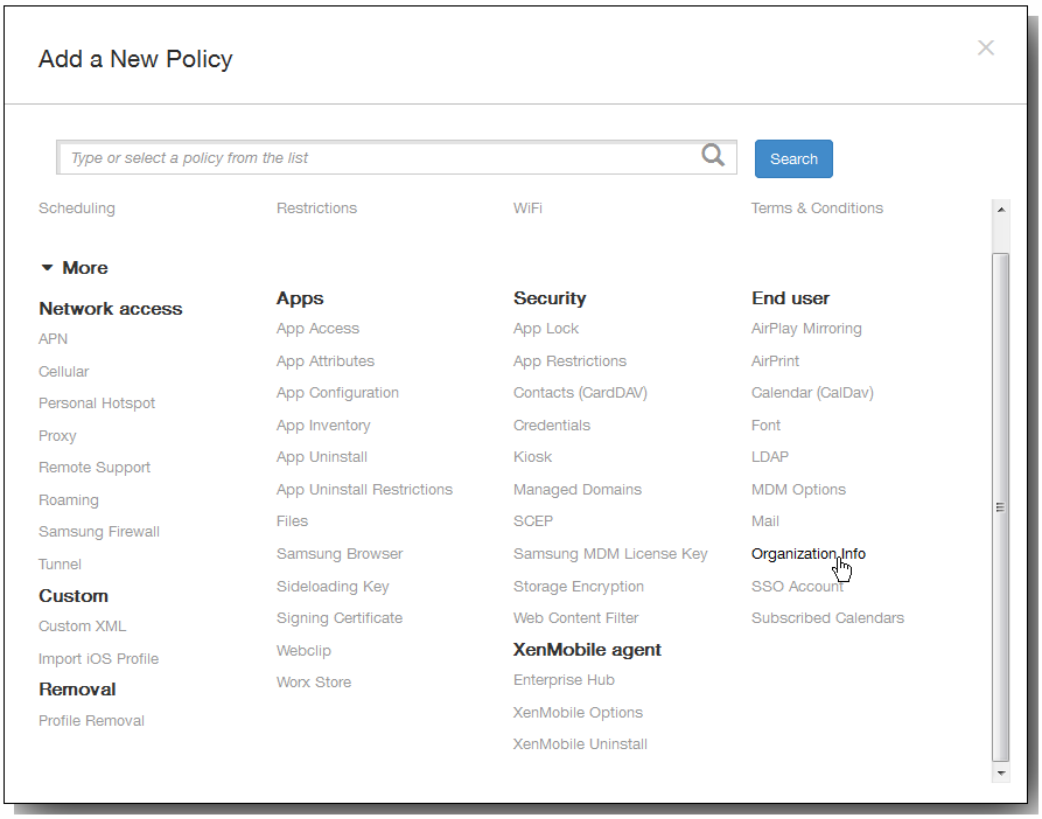
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para especificar la información de su organización que se utilizará en los mensajes de alerta que envía XenMobile a dispositivos iOS. La directiva está disponible para los dispositivos iOS 7 y versiones posteriores.

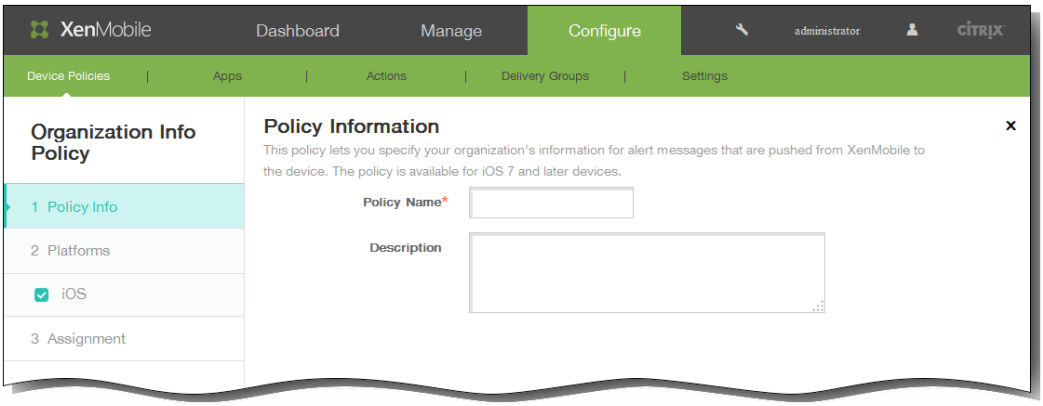
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



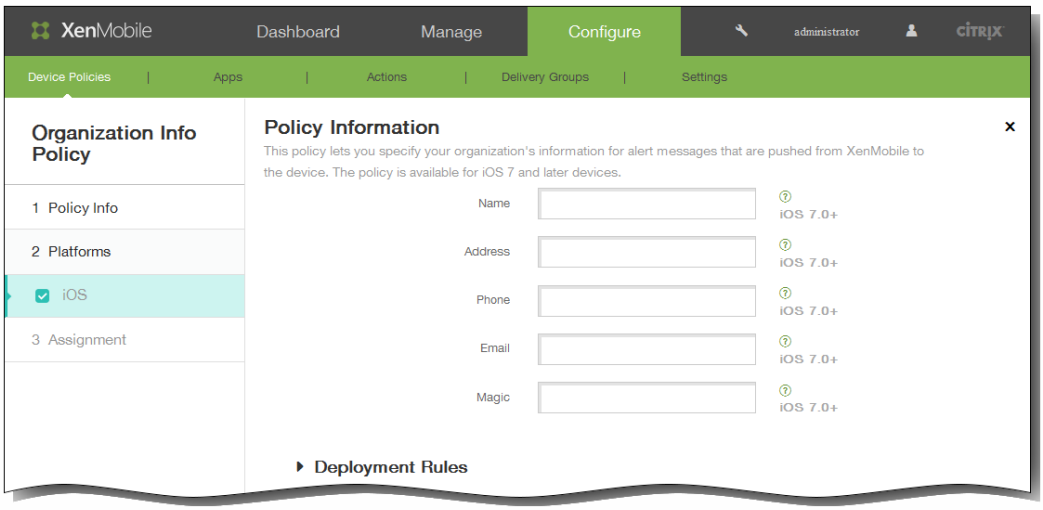
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en Organization info. Aparecerá la página Organization Info Policy.

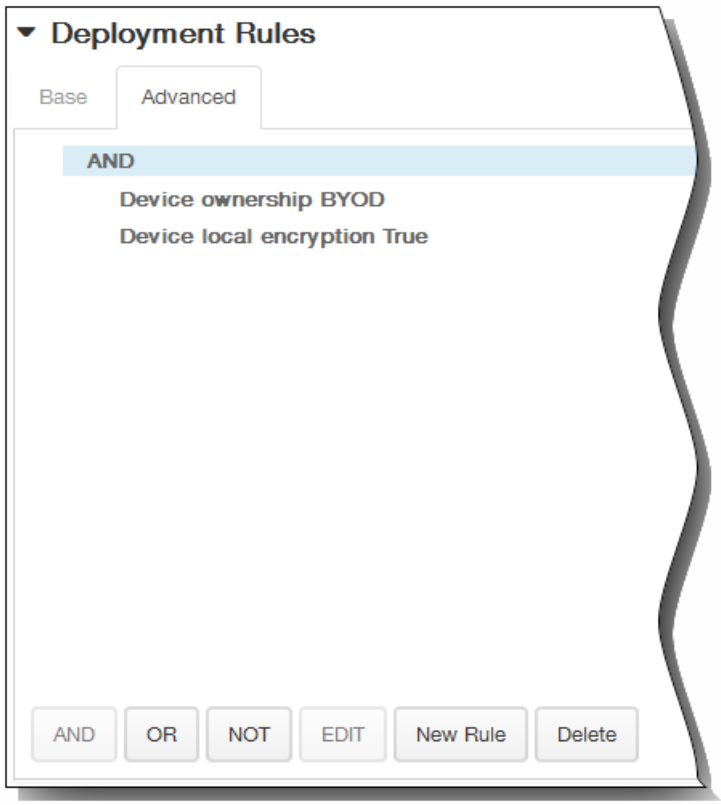


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



6. En la página de información iOS Platform, escriba la información siguiente:
   1. Name. Escriba el nombre de la organización con XenMobile.
   2. Address. Escriba la dirección de la organización.
   3. Phone. Escriba el número de teléfono de asistencia de la organización.
   4. Email. Escriba la dirección de correo electrónico de asistencia.
   5. Magic. Escriba una palabra o frase que describa los servicios que administra esa organización.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

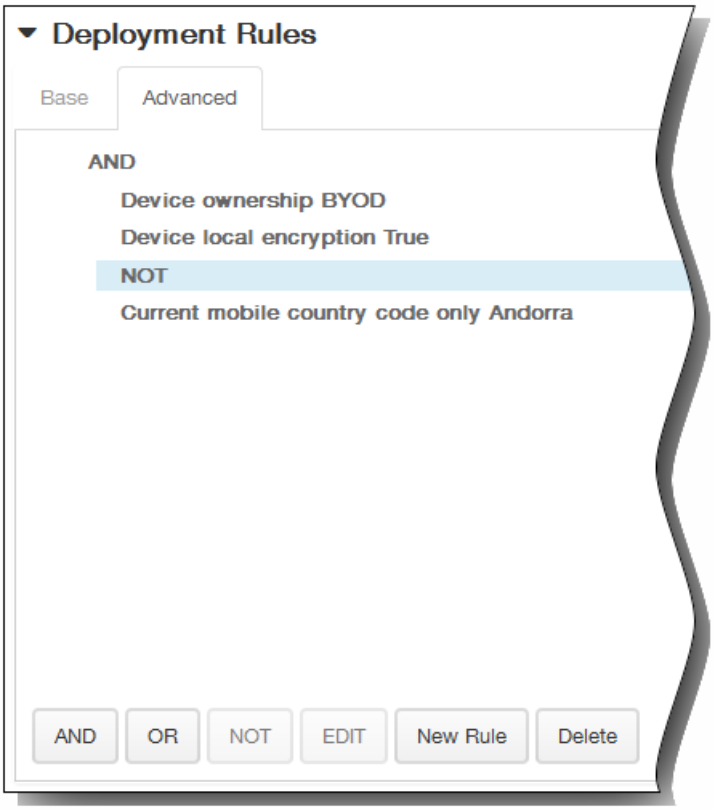
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



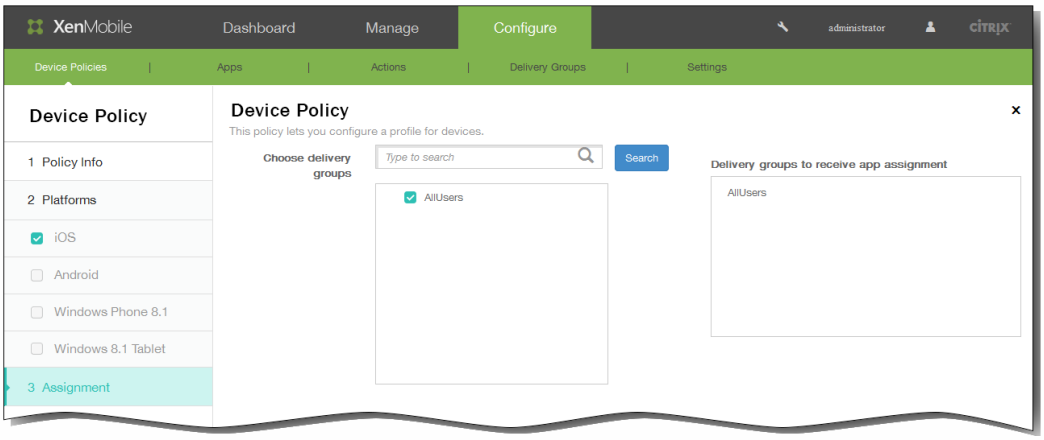
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



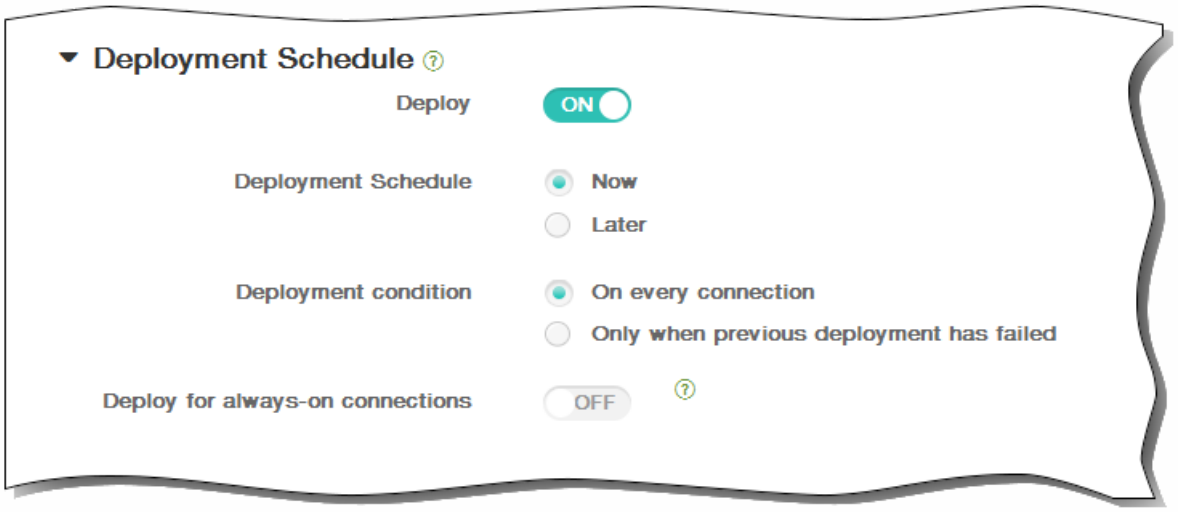
8. Haga clic en Next. Aparecerá la página de asignación Organization Info Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

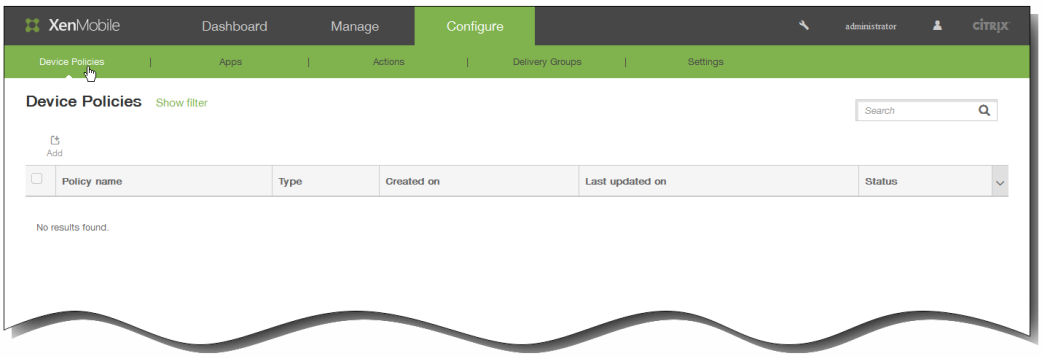
Para agregar una directiva de protocolo LDAP para dispositivos iOS

May 05, 2016

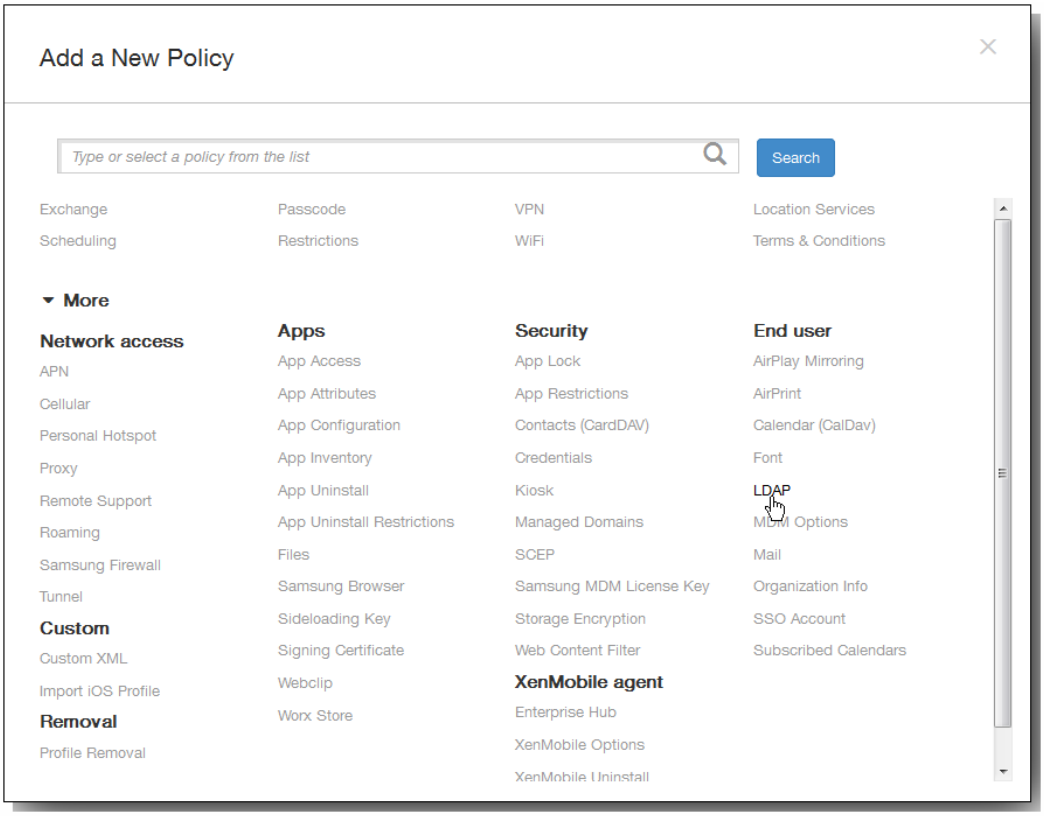
En XenMobile, puede crear una directiva de protocolo LDAP para dispositivos iOS con el fin de proporcionar información sobre el servidor LDAP a utilizar, incluida la información de cuenta necesaria. La directiva también ofrece un conjunto de directivas de búsquedas LDAP a usar cuando se consulta el servidor LDAP.

Es necesario el nombre de host del servidor LDAP antes de configurar esta directiva.

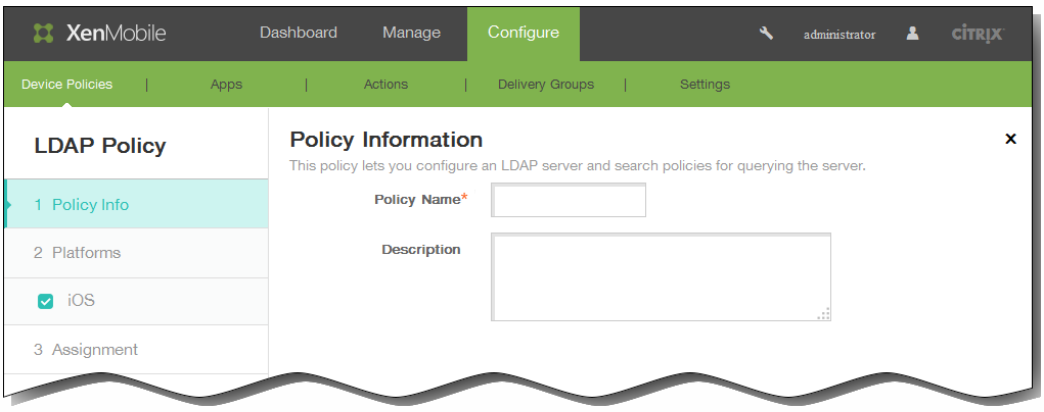
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



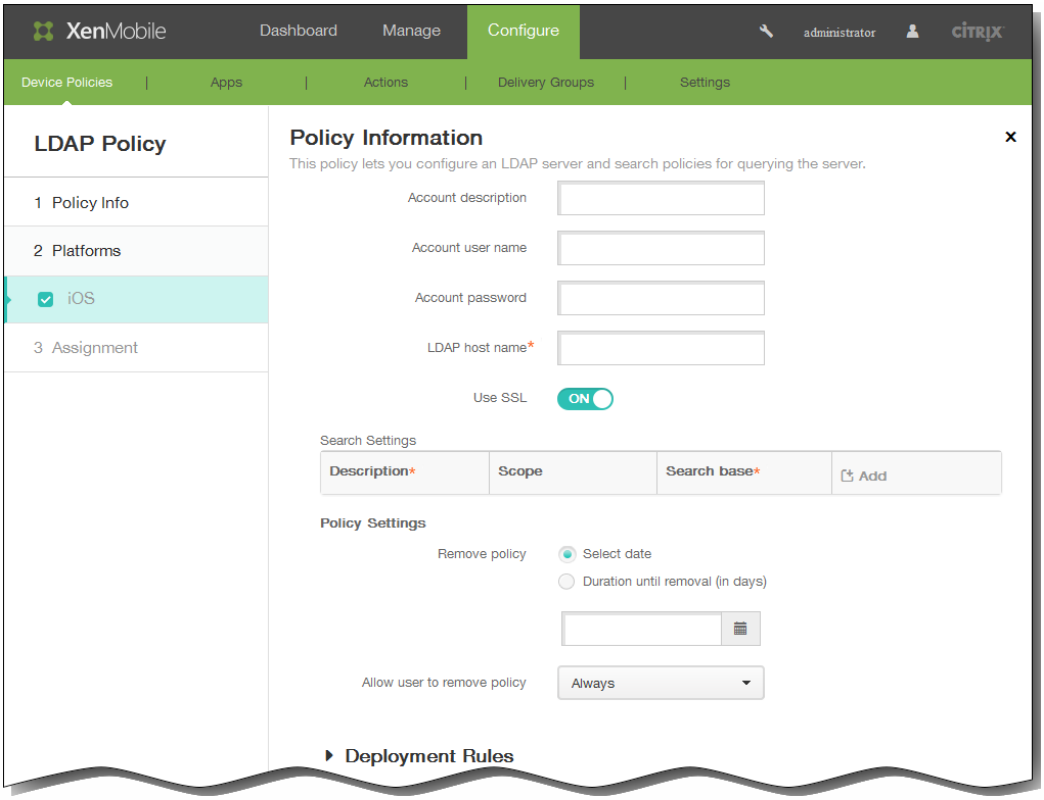
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en LDAP. Aparecerá la página LDAP Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información iOS Platform.

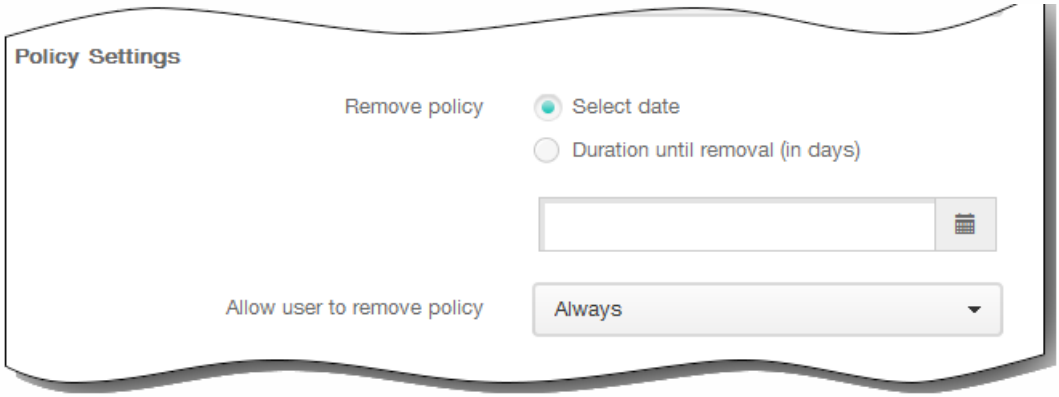


6. En la página de información iOS Platform, escriba la información siguiente:
   1. Account description. Indique una descripción opcional de la cuenta.
   2. Account user name. Escriba un nombre de usuario opcional.
   3. Account password. Escriba una contraseña opcional. Use esta opción solo con perfiles cifrados.
   4. LDAP host name. Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
   5. Use SSL. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor LDAP. El valor predeterminado es ON.
   6. Search Settings. Haga clic en Add y lleve a cabo lo siguiente:
      Nota: Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar.
      1. Description. Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
      2. Scope. En la lista, haga clic en Base, One level o Subtree para definir los niveles de búsqueda en el árbol LDAP. El valor predeterminado es Base.
         - El nivel Base busca en el nodo al que apunta Search base.
         - El nivel One level busca en el nodo Base y en un nivel por debajo de él.
         - El nivel Subtree busca en el nodo Base, además de todos sus elementos secundarios, independientemente de la profundidad.
      3. Search base. Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo: `ou=people` o `0=example corp`. Este campo es obligatorio.
      4. Haga clic en Add para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
      5. Repita los pasos de i. a iv. para cada opción de búsqueda que quiera agregar.

      Nota: Para eliminar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.
      Para modificar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación,

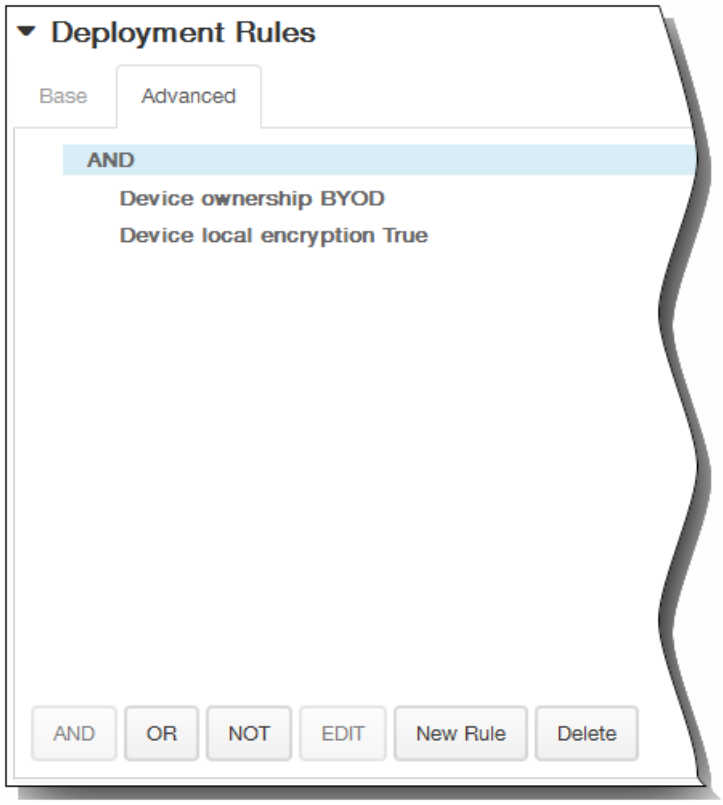
haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



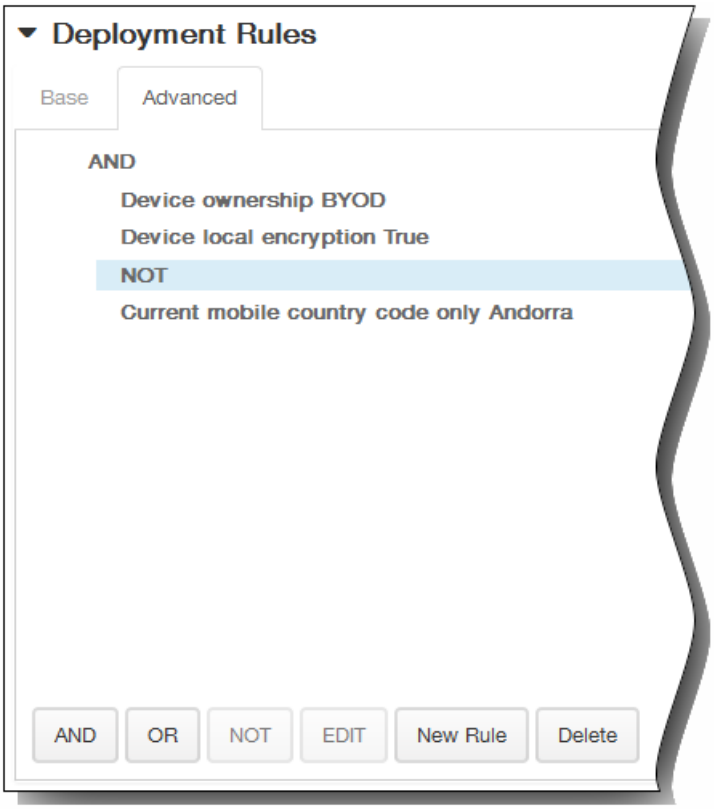
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

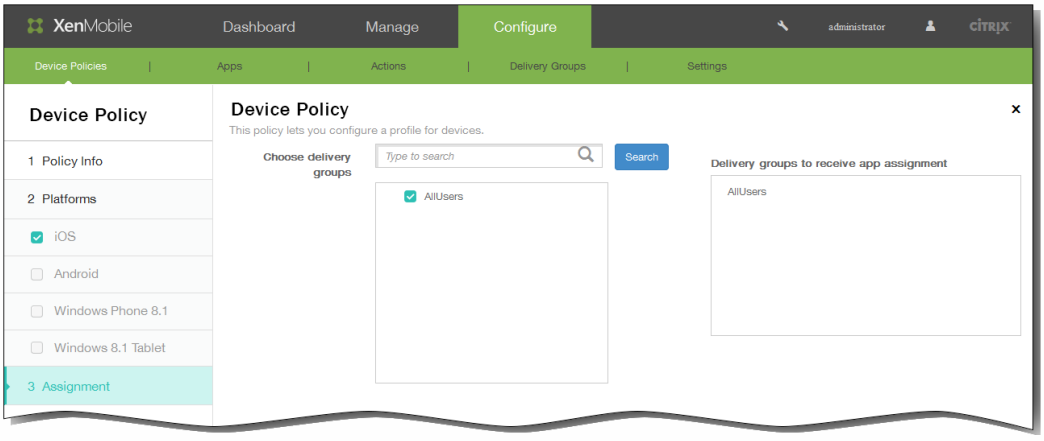


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



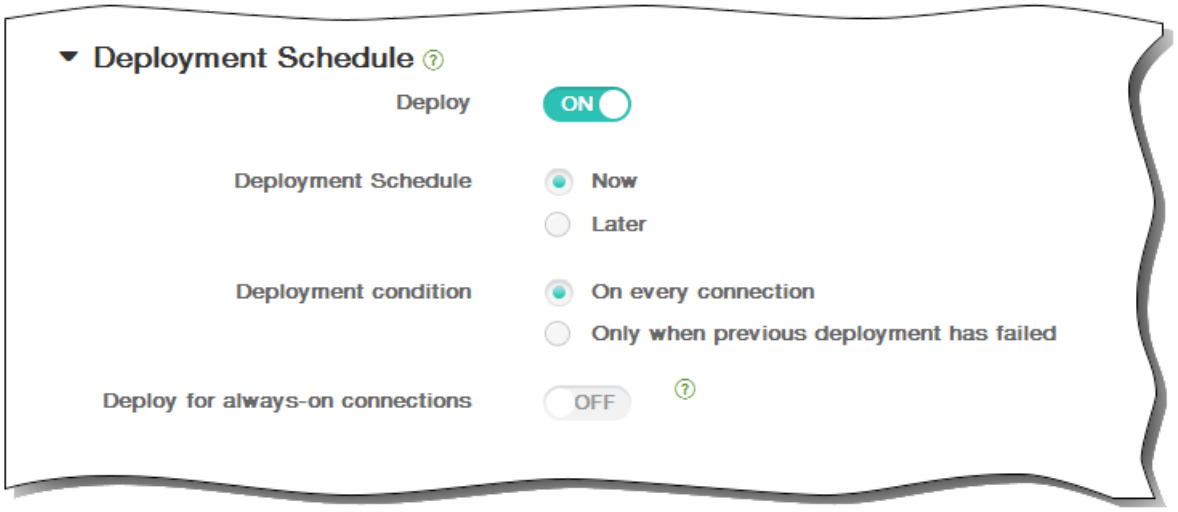
12. Haga clic en Next. Aparecerá la página de asignación LDAP Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



15. Haga clic en Save para guardar la directiva.

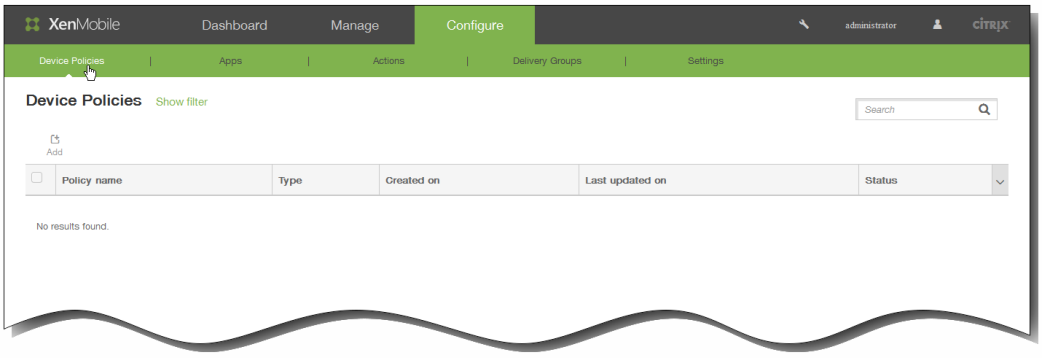
Para agregar una directiva de cuentas Single Sign-On para dispositivos iOS

May 05, 2016

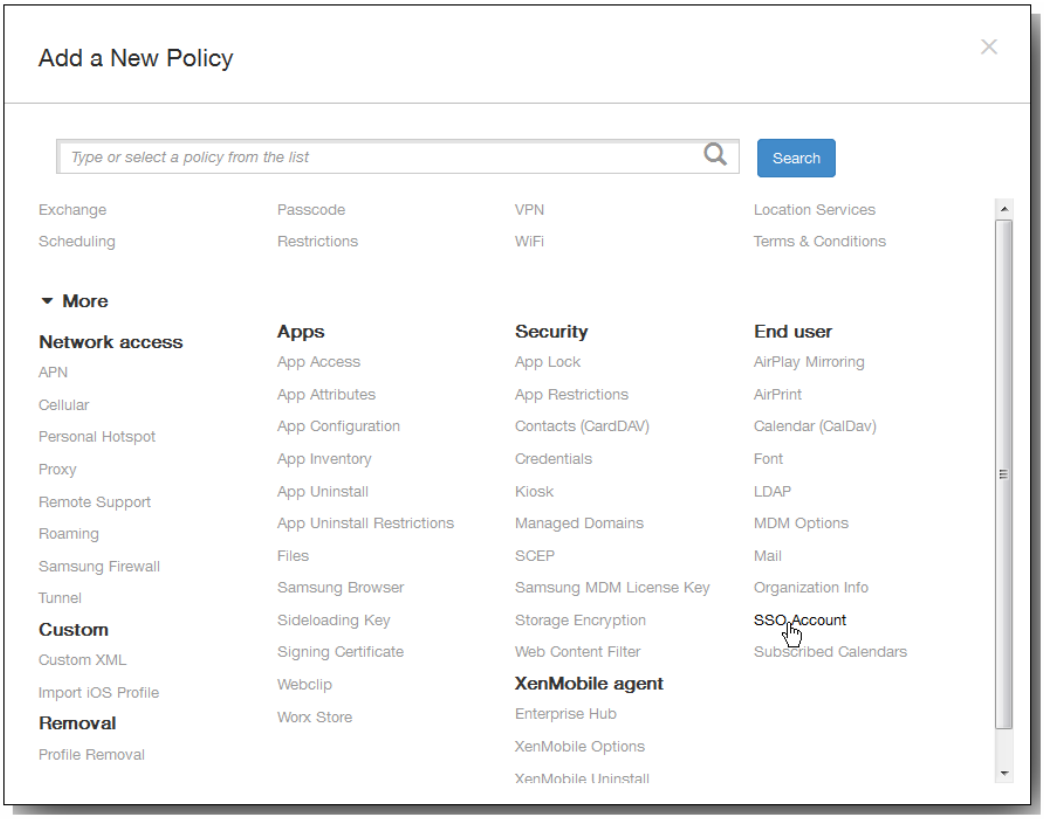
En XenMobile, puede crear cuentas de inicio de sesión único (SSO) para que los usuarios solo deban iniciar sesión una vez para acceder a XenMobile y a los recursos internos de la empresa desde varias aplicaciones. Así, no es necesario que los usuarios almacenen credenciales en el dispositivo. Las credenciales de usuario de empresa de la cuenta SSO se pueden usar en varias aplicaciones, incluidas las aplicaciones del App Store de Apple. Esta directiva está pensada para funcionar con un servidor back-end de autenticación Kerberos.

Nota: Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.

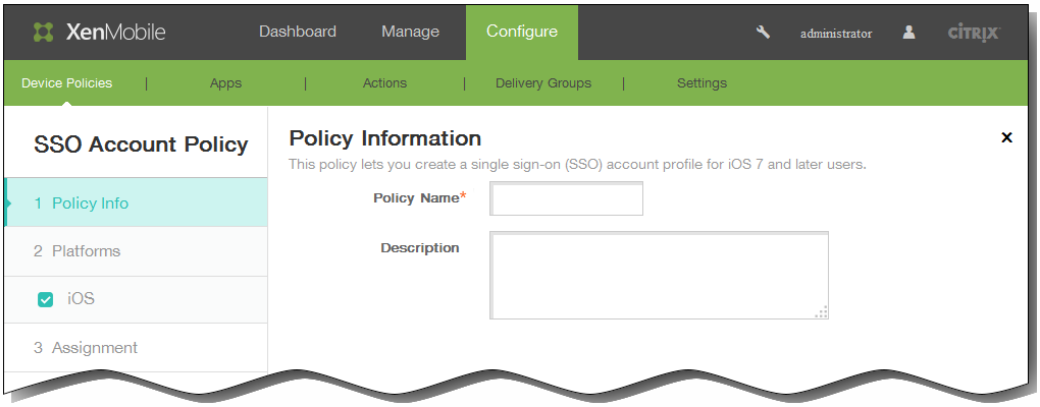
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



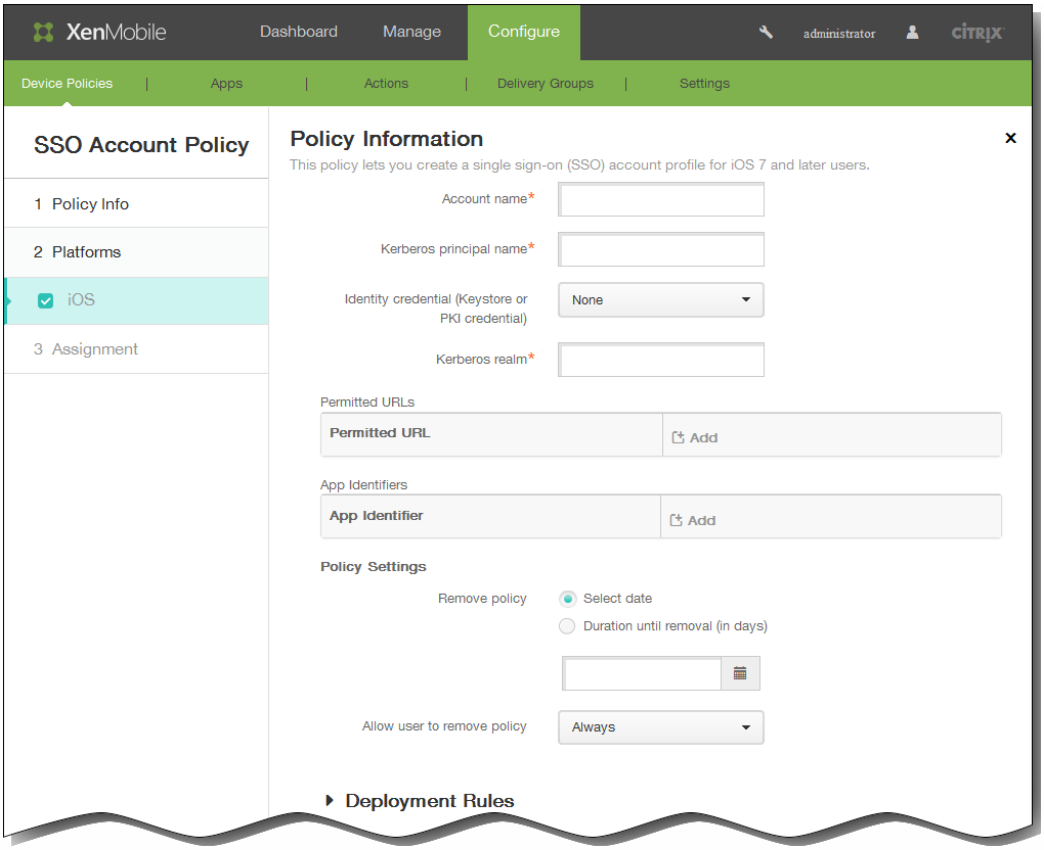
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en End user, haga clic en SSO Account. Aparecerá la página SSO Account Policy.



4. En el panel de información SSO Account Policy, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información iOS Platform.

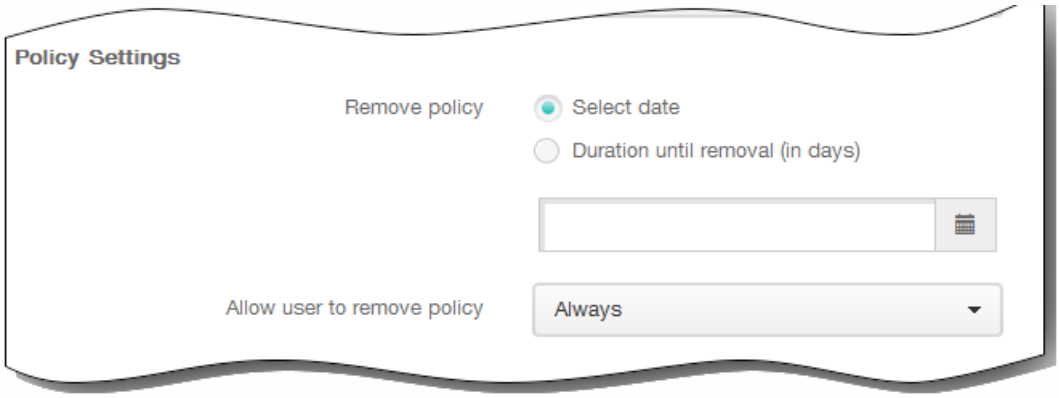


6. En la página de información iOS Platform, escriba la información siguiente:
    1. Account name. Escriba el nombre de la cuenta SSO de Kerberos que aparece en los dispositivos de los usuarios. Este campo es obligatorio.
    2. Kerberos principal name. Escriba el nombre de la entidad de seguridad asignada a Kerberos. Este campo es obligatorio.
    3. Identity credential (Keystore or PKI credential). En la lista, haga clic en una de las credenciales de identidad opcionales que se pueden usar para renovar la credencial de Kerberos sin la interacción del usuario.
    4. Kerberos realm. Escriba el dominio de Kerberos designado a esta directiva. Por regla general, se trata de su nombre de dominio en letras mayúsculas (por ejemplo, EJEMPLO.COM). Este campo es obligatorio.
    5. Permitted URLs. Haga clic en Add y lleve a cabo lo siguiente:
        1. Permitted URL. Escriba la URL que requerirá el inicio de sesión único cuando un usuario la visite desde el dispositivo iOS.
           Por ejemplo: cuando un usuario intenta abrir un sitio Web y este sitio pide una comprobación de Kerberos, si ese sitio no está en la lista de direcciones URL, el dispositivo iOS no intenta el inicio de sesión único con el token de Kerberos que se haya almacenado en caché en el dispositivo como consecuencia de un inicio de sesión Kerberos previo. La coincidencia debe ser exacta en el host de la URL; por ejemplo: http://shopping.apple.com es correcta, pero http://*.apple.com no lo es. Además, si Kerberos no se activa en función de la coincidencia de host, la URL sigue recurriendo a una llamada de HTTP estándar. Esto puede tener varias consecuencias, incluida una comprobación de contraseña estándar o un error de HTTP si la URL se ha configurado solo para el inicio de sesión único mediante Kerberos.
        2. Haga clic en Add para agregar la URL, o bien haga clic en Cancel para cancelar la operación.
        3. Repita el paso de i. y ii. para cada URL que quiera agregar.
    6. App Identifiers. Haga clic en Add y lleve a cabo lo siguiente:
        1. App Identifier. Escriba el identificador de aplicación perteneciente a una aplicación que pueda utilizar esta

credencial.
Nota: Si no se agrega ningún identificador de aplicación, esta credencial coincidirá con **todos** los identificadores de aplicación.
2. Haga clic en Add para agregar el identificador de aplicación, o bien haga clic en Cancel para cancelar la operación.
3. Repita el paso de i. y ii. para cada identificador de aplicación que quiera agregar.

Nota: Para eliminar una URL o un identificador de aplicación existente, coloque el cursor sobre la línea que los contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.
Para modificar una URL o un identificador de aplicación existentes, coloque el cursor sobre la línea que los contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



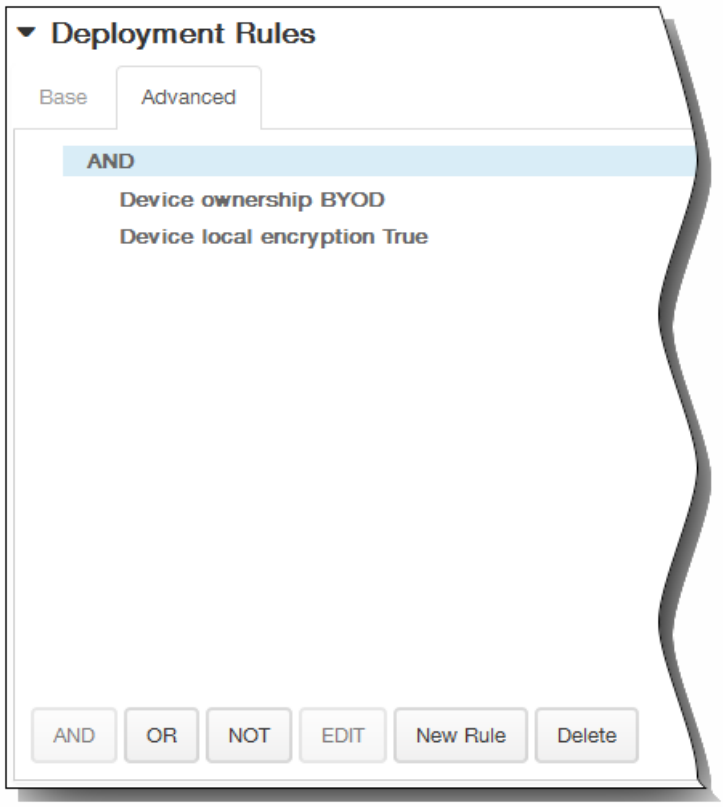
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la

ilustración anterior.

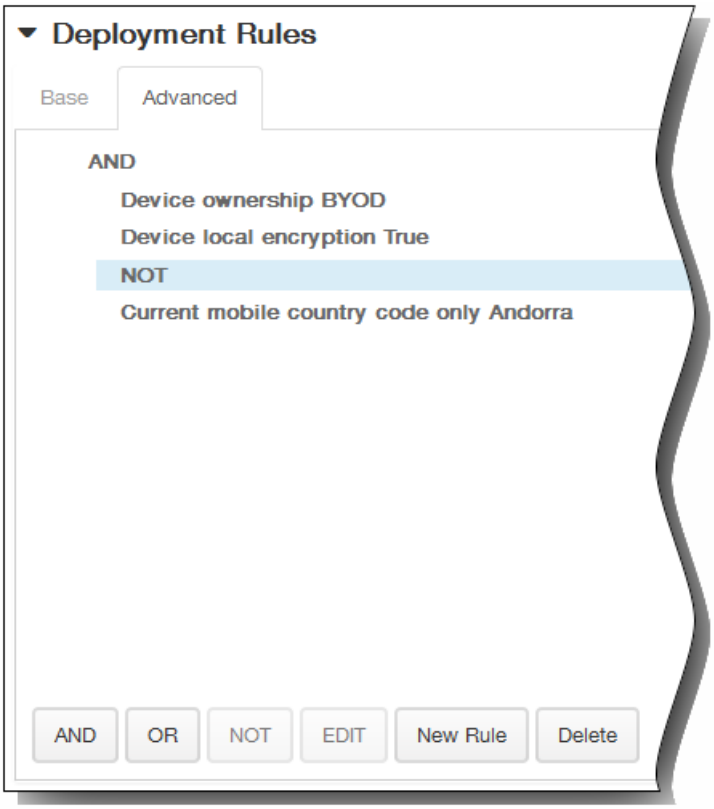
4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.

2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

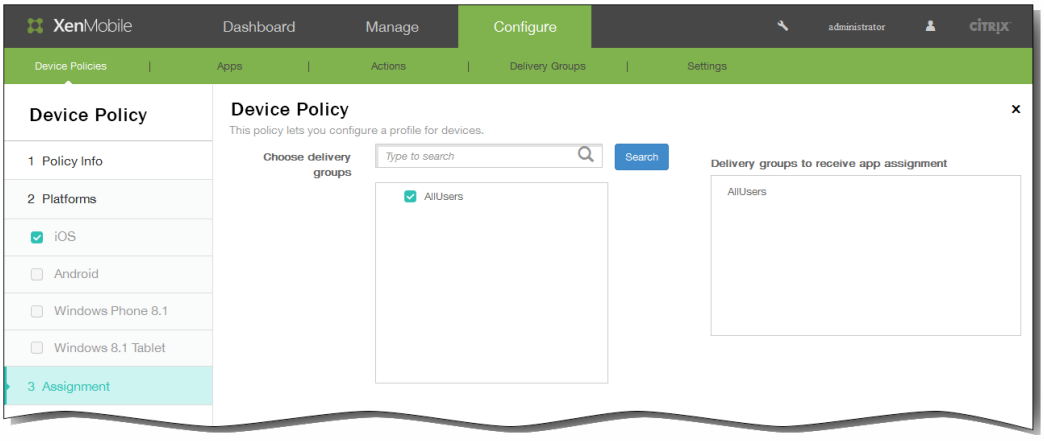


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



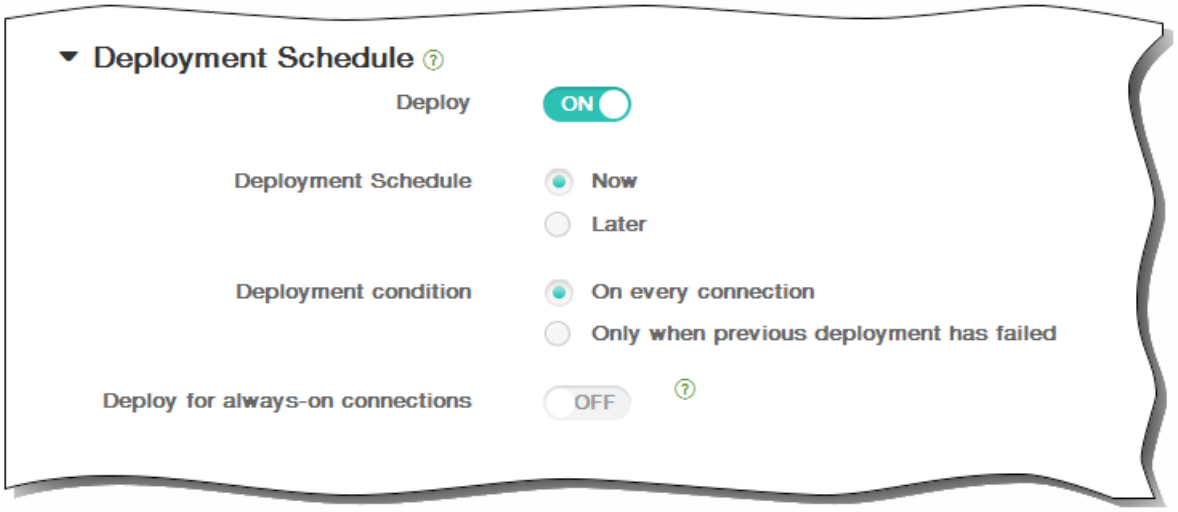
12. Haga clic en Next. Aparecerá la página de asignación SSO Account Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



15. Haga clic en Save para guardar la directiva.

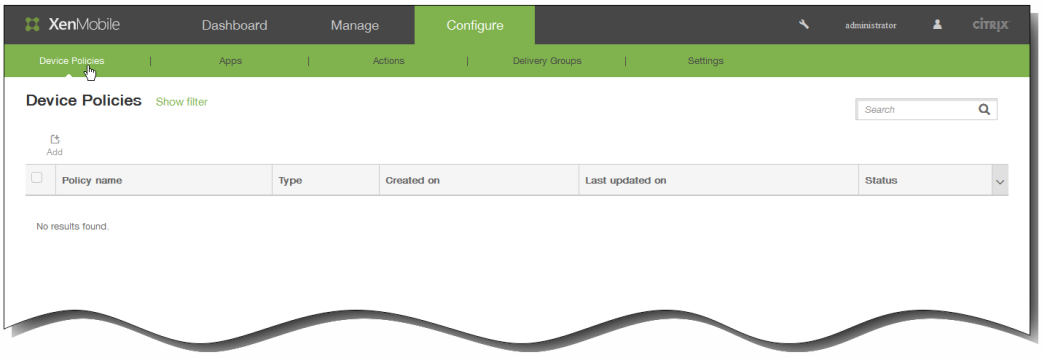
Para agregar una directiva de calendarios suscritos para dispositivos iOS

May 05, 2016

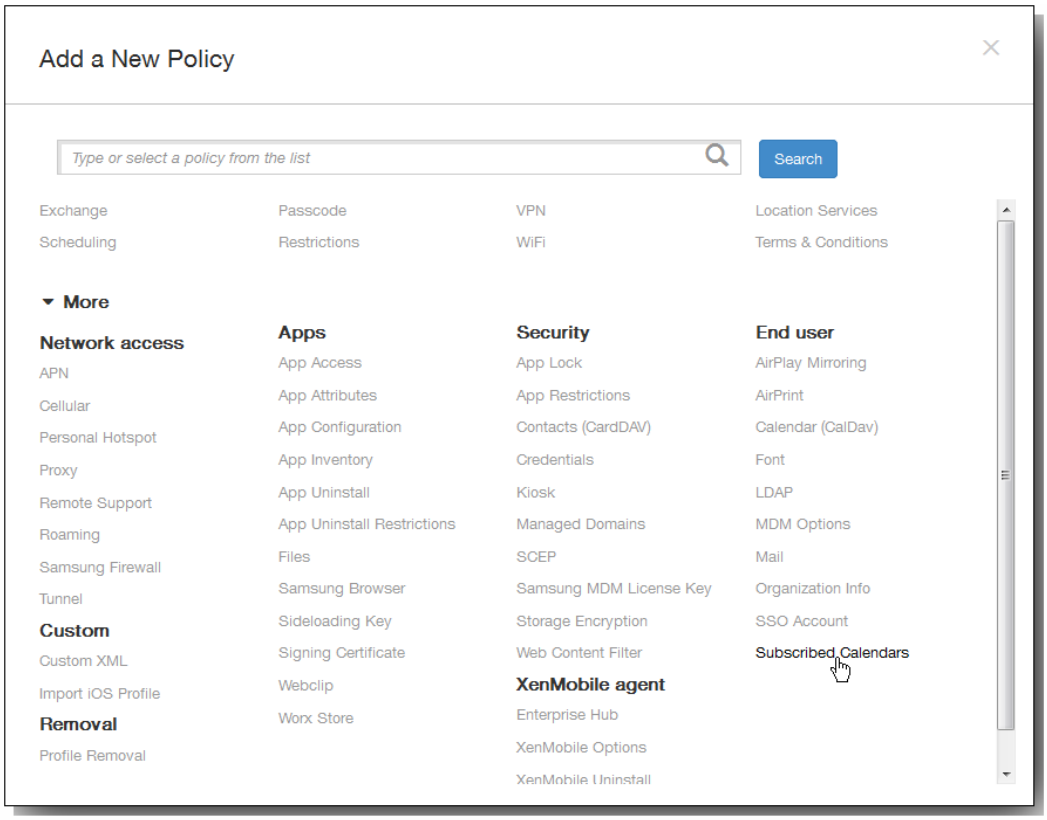
En XenMobile, puede agregar una directiva de dispositivos para agregar un calendario suscrito a la lista de calendarios en los dispositivos iOS de los usuarios. La lista de los calendarios públicos a los que se puede suscribir está disponible en www.apple.com/downloads/macosx/calendars.

Nota: Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.

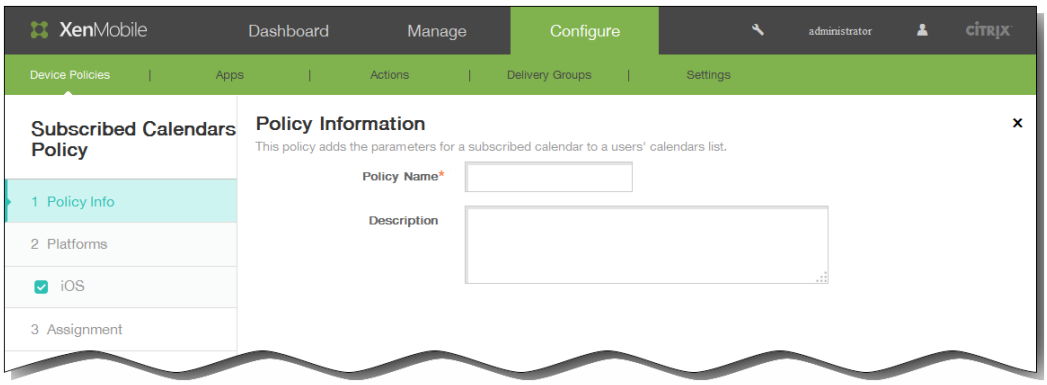
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



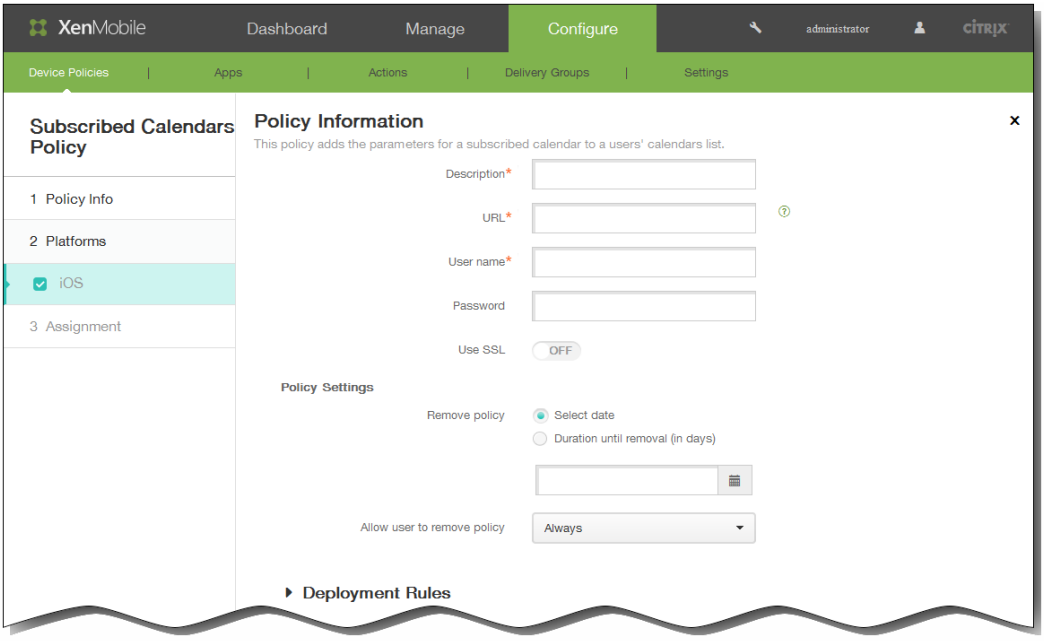
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



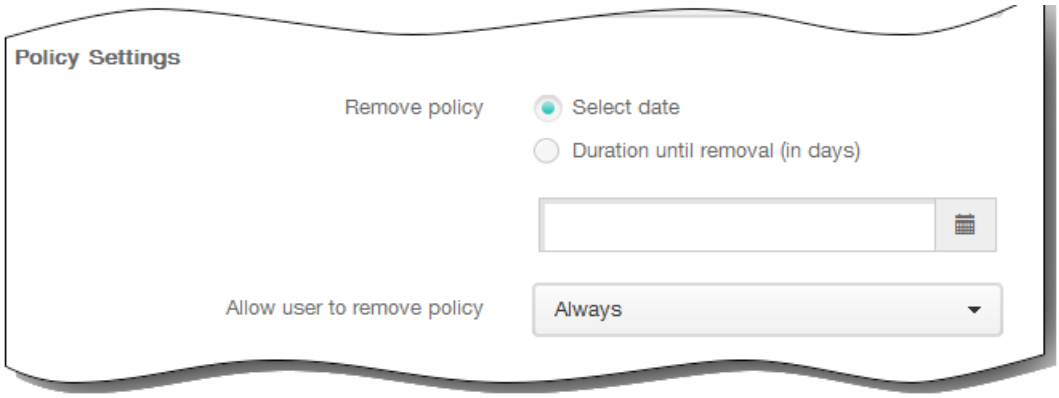
3. Haga clic en More y, en End user, haga clic en Subscribed Calendars. Aparecerá la página Subscribed Calendars Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.

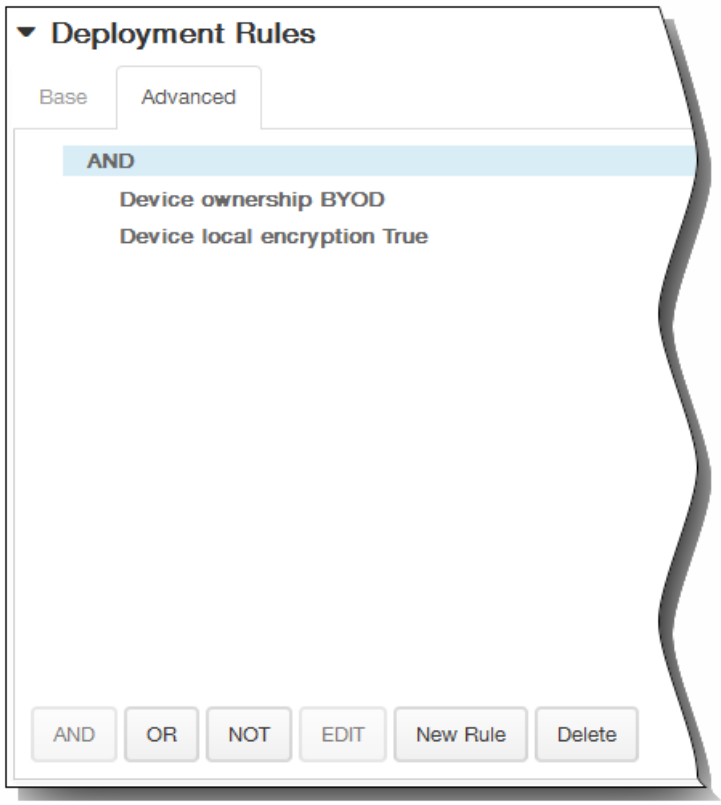


6. En la página de información iOS Platform, escriba la información siguiente:
   1. Description. Introduzca una descripción del calendario. Este campo es obligatorio.
   2. URL. Introduzca la dirección URL del calendario. Puede introducir una dirección URL webcal:// o un enlace http:// a un archivo de iCalendar (.ics). Este campo es obligatorio.
   3. User name. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
   4. Password. Escriba una contraseña opcional de usuario.
   5. Use SSL. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el calendario. El valor predeterminado es Off.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

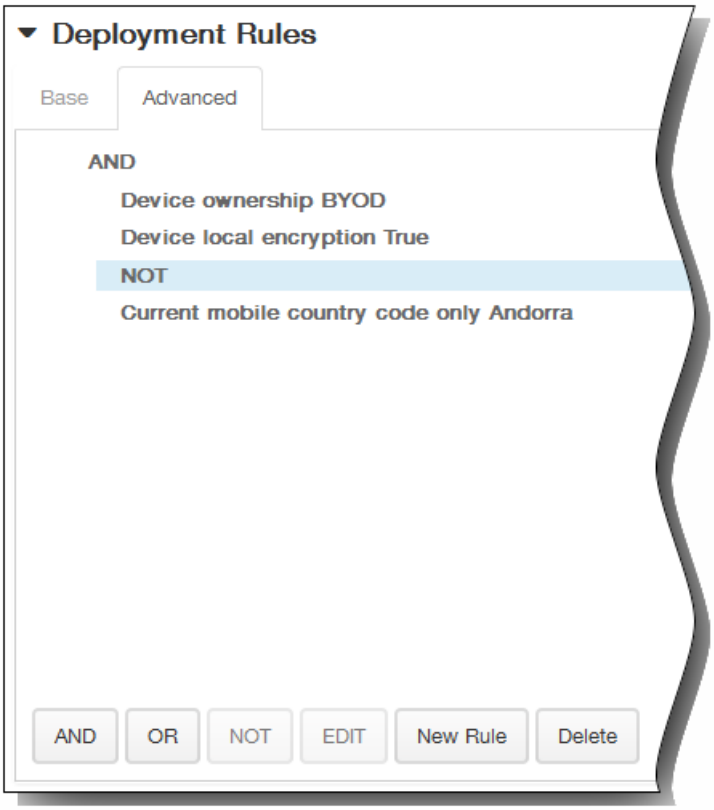
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



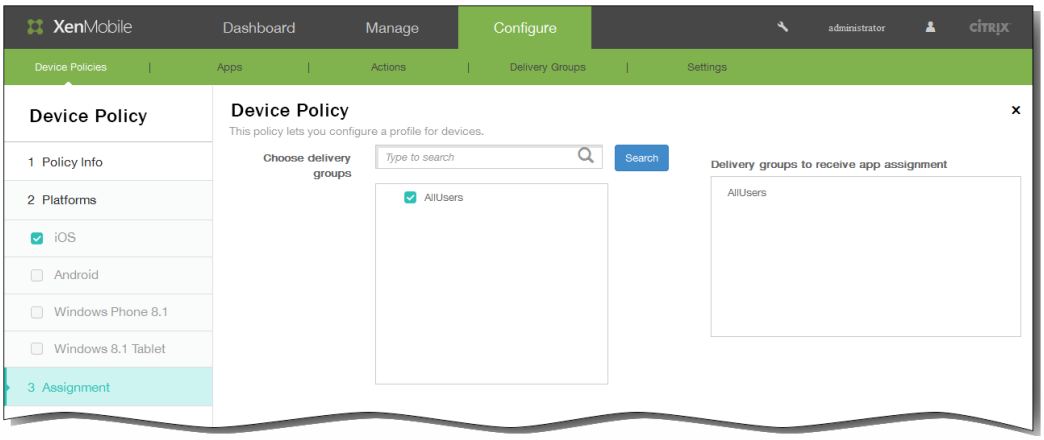
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



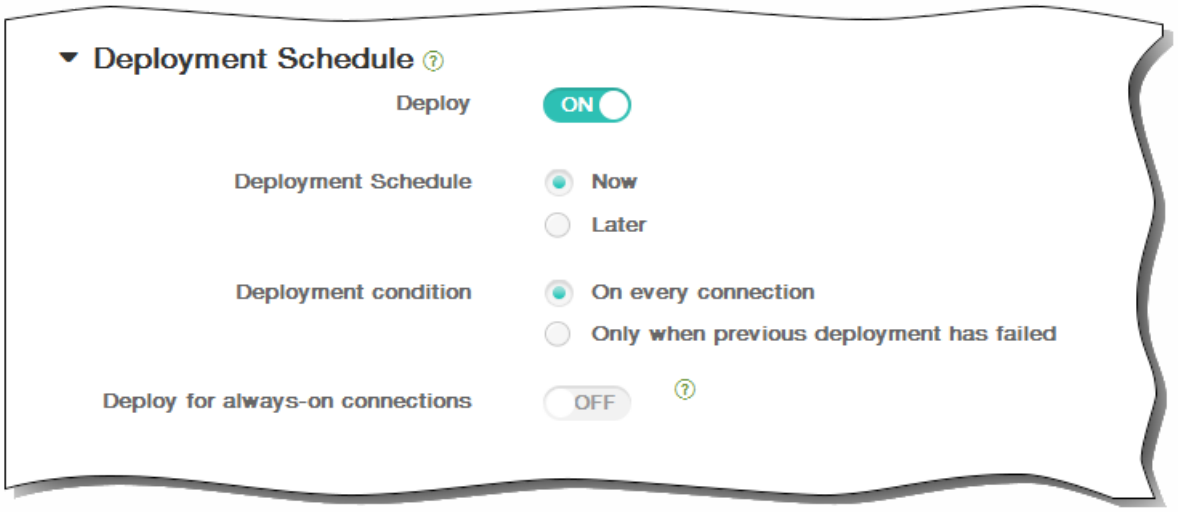
12. Haga clic en Next. Aparecerá la página de asignación Subscribed Calendars Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



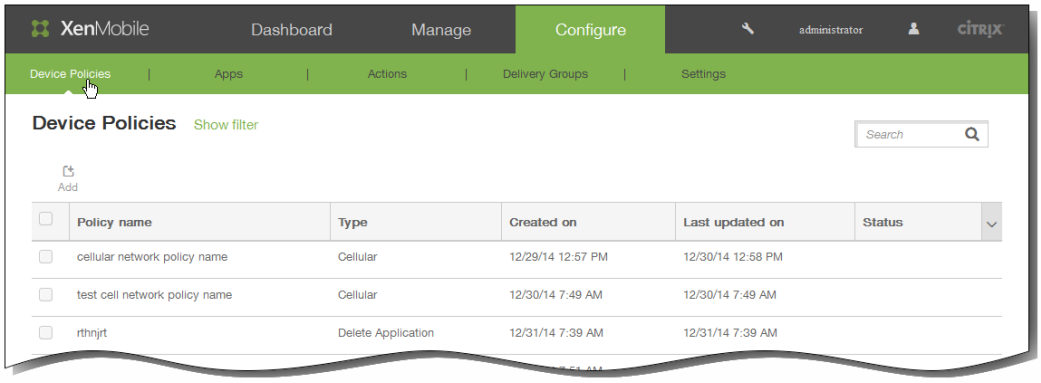
15. Haga clic en Save para guardar la directiva.

Directivas de códigos de acceso

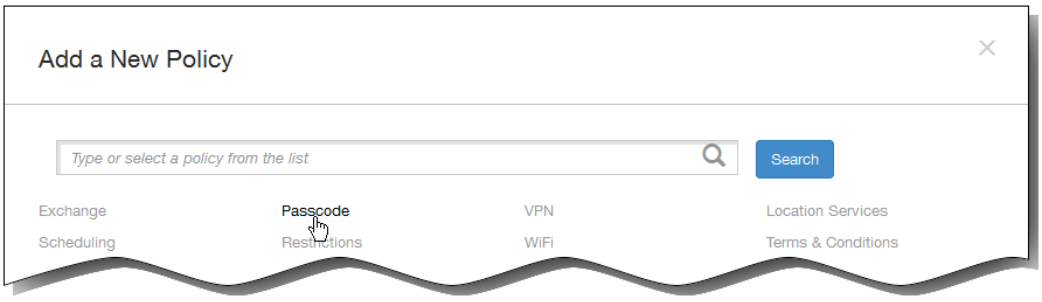
May 05, 2016

En XenMobile, puede crear una directiva de códigos de acceso en función de los requisitos de su empresa. Puede solicitar códigos de acceso en los dispositivos de los usuarios y configurar varias reglas de formatos y de códigos de acceso. Puede crear directivas para iOS, Android, Samsung KNOX, Windows Phone 8.1 y tabletas Windows 8.1. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

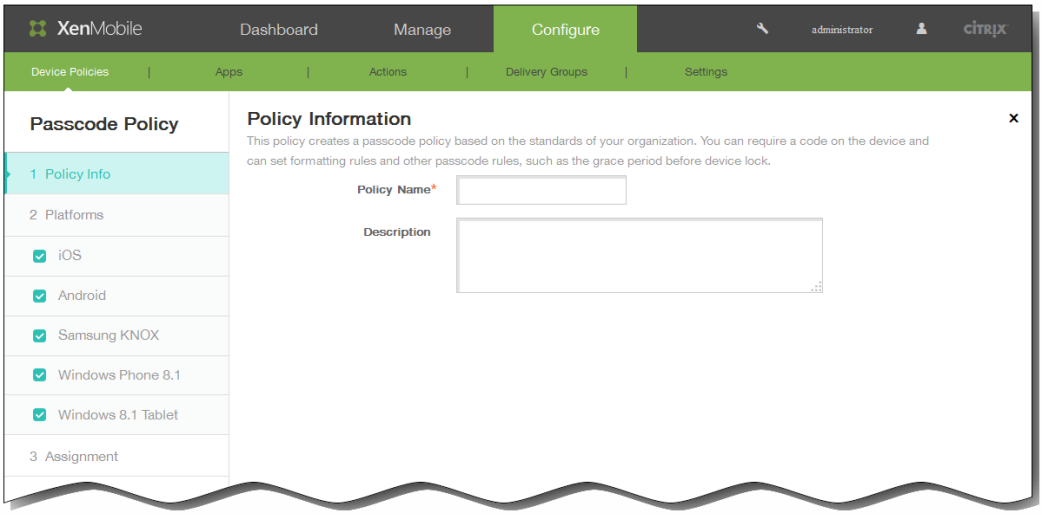
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies. Haga clic en Add para agregar una nueva directiva.



2. En la página Add New Policy, haga clic en Passcode.

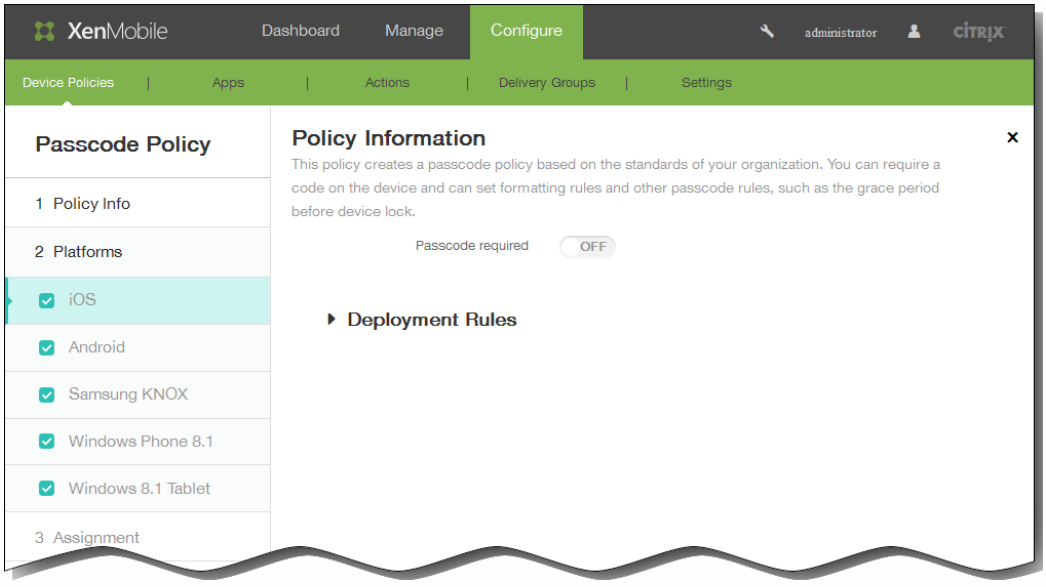


3. En el panel Policy Information, escriba la información siguiente:

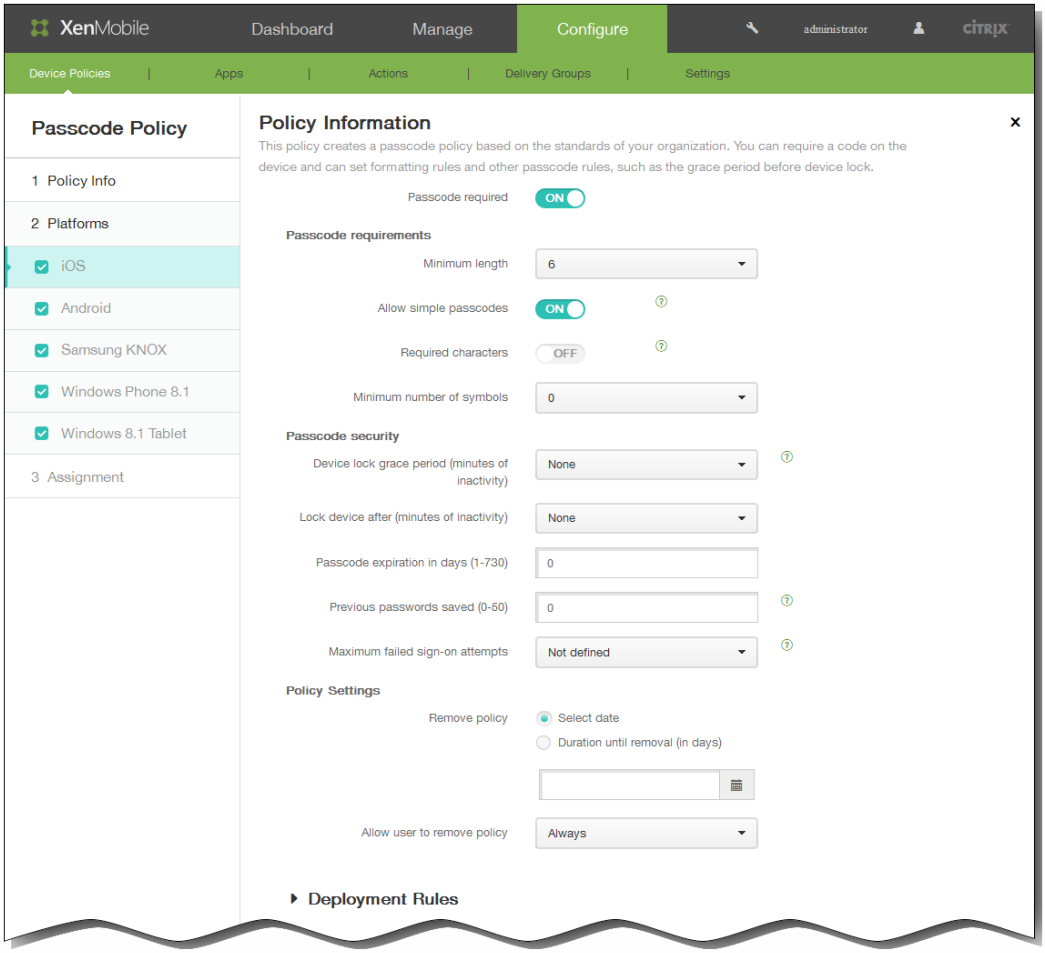


1. Policy Name. Escriba un nombre descriptivo para la directiva.
2. Description. Escriba, si quiere, una descripción para la directiva.
3. Haga clic en Next.

4. En Platforms, seleccione las plataformas para las que quiera configurar esta directiva.
   Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de iOS.



- Si ha seleccionado iOS, configure los siguientes parámetros:



Passcode required. Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de códigos de acceso para dispositivos iOS. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y configuraciones de directiva.

Requisitos de códigos de acceso

Minimum length. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.

Allow simple passcodes. Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es ON.

Required characters. Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. El valor predeterminado es OFF.

Minimum number of symbols. En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso.

Seguridad de códigos de acceso

Device lock grace period (minutes of inactivity). En la lista, haga clic en el período de tiempo que debe transcurrir antes de que los usuarios introduzcan un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es None.

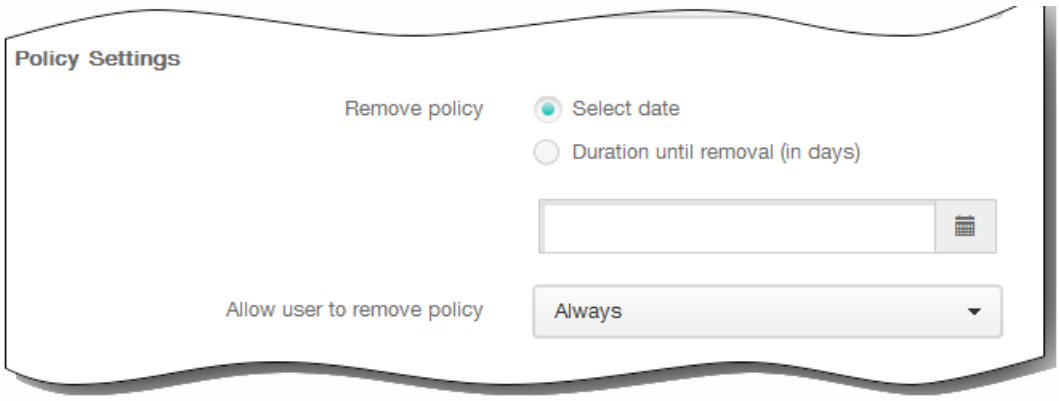
Lock device after (minutes of inactivity). En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es None.

Passcode expiration in days (1-730). Especifique la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es 0, lo que significa que el código de acceso no caduca nunca.

Previous passwords saved (0-50). Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es 0, lo que significa que los usuarios pueden volver a usar las contraseñas.

Maximum failed sign-on attempts. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se borre completamente el contenido del dispositivo. El valor predeterminado es Not defined.

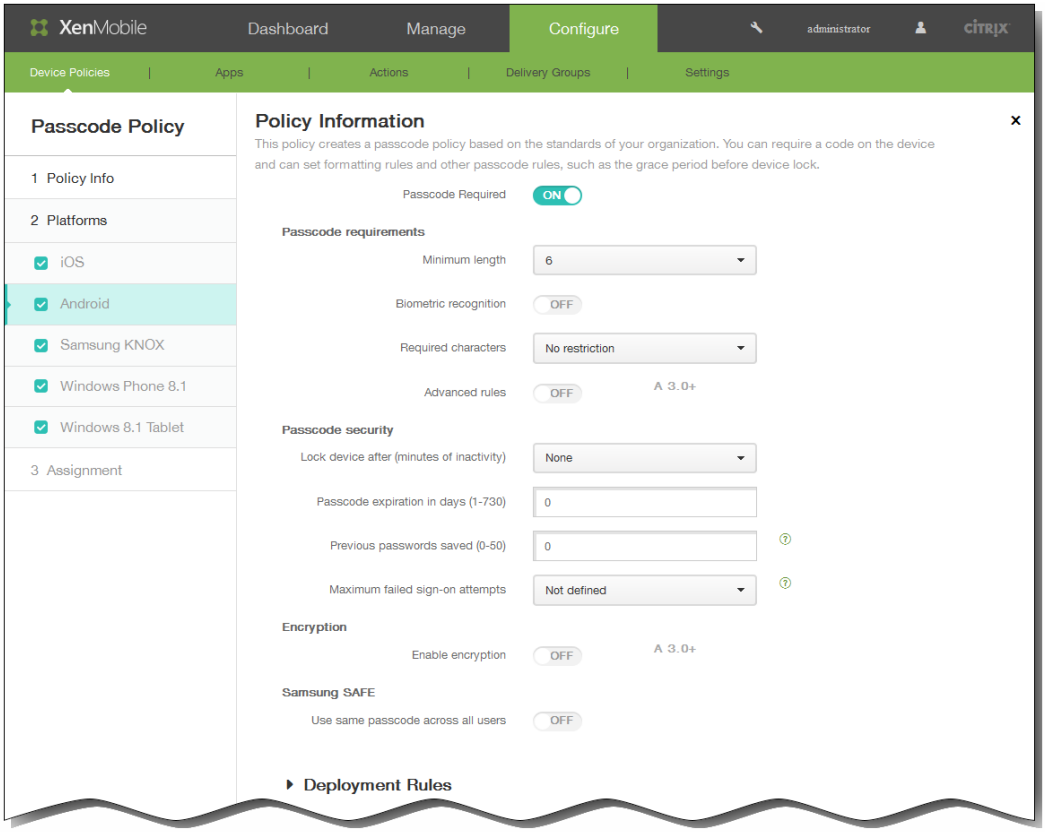
Configuraciones de directivas



1. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
2. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
3. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
4. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

- Si ha seleccionado Android, configure los siguientes parámetros:

  Nota: El valor predeterminado de las opciones de configuración para Android es OFF. La página se expande para que pueda definir las opciones de configuración de Samsung SAFE, los requisitos de los códigos de acceso, la seguridad de dichos códigos y el cifrado.



Requisitos de códigos de acceso

Minimum length. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.

Biometric recognition. Seleccione si habilitar el reconocimiento biométrico. Si se habilita esta opción, se oculta el campo Required characters. El valor predeterminado es OFF.

Required characters. En la lista, haga clic en No Restriction, Both numbers and letters, Numbers only o Letters only para configurar la composición de los códigos de acceso. El valor predeterminado es No restriction.

Advanced rules. Seleccione si aplicar reglas avanzadas de códigos de acceso. Esta opción está disponible para Android 3.0 y versiones posteriores. El valor predeterminado es OFF.

Si Advanced rules está establecido en ON, en cada una de las siguientes listas, haga clic en la cantidad mínima de cada tipo de carácter que un código de acceso debe contener:

- Symbols. La cantidad mínima de símbolos.
- Letters. La cantidad mínima de letras.
- Lowercase letters. La cantidad mínima de minúsculas.
- Uppercase letters. La cantidad mínima de mayúsculas.
- Numbers or symbols. La cantidad mínima de números o símbolos.
- Numbers. La cantidad mínima de números.

Seguridad de códigos de acceso

Lock device after (minutes of inactivity). En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es None.

Passcode expiration in days (1-730). Especifique la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es 0, lo que significa que el código de acceso no caduca nunca.

Previous passwords saved (0-50). Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es 0, lo que significa que los usuarios pueden volver a usar las contraseñas.

Maximum failed sign-on attempts. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se borre completamente el contenido del dispositivo. El valor predeterminado es Not defined.

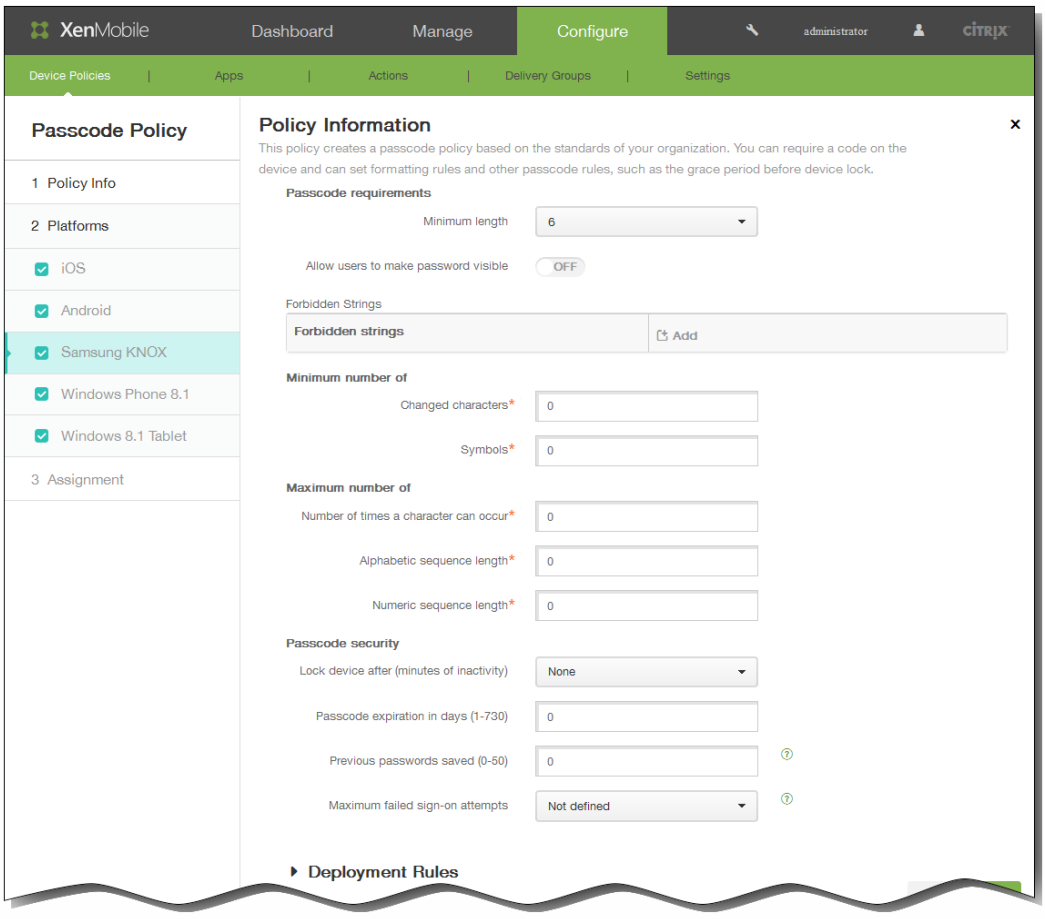
Cifrado

Enable encryption. Seleccione si habilitar el cifrado. Esta opción está disponible para Android 3.0 y versiones posteriores. La opción está disponible independientemente de la opción de configuración Passcode required.

Use same passcode across all users. Seleccione si utilizar el mismo código de acceso para todos los usuarios. Esta opción solo se aplica a dispositivos Samsung SAFE y está disponible independientemente de la opción de configuración Passcode required. El valor predeterminado es OFF.

Escriba el código de acceso pertinente en el campo que aparece cuando se habilita esta opción.

- Si ha seleccionado Samsung KNOX, configure los siguientes parámetros:



Requisitos de códigos de acceso

Minimum length. En la lista, haga clic en la longitud mínima del código de acceso.

Allow users to make password visible. Seleccione si permitir que los usuarios hagan visible su contraseña.

- Forbidden strings. Cree cadenas prohibidas para evitar que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como "contraseña", "contra", "bienvenida", "123456" o "111111", entre otras. Lleve a cabo una de las siguientes acciones:
  - Para agregar una cadena prohibida
    1. Haga clic en Agregar.
    2. Escriba la cadena no permitida.
    3. Haga clic en Save para guardar la cadena, o bien en Cancel para no agregarla.
    4. Repita los pasos de i. a iii. para cada cadena prohibida que quiera agregar.
  - Para modificar una cadena prohibida
    1. Previous passwords saved (0-50). Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es 0, lo que significa que los usuarios pueden reutilizar contraseñas.
    1. Coloque el cursor sobre la cadena a modificar.
    2. Haga clic en el icono de lápiz situado a la derecha de la lista.
    3. Realice los cambios pertinentes en la cadena.
    4. Haga clic en Save para guardar la cadena, o bien en Cancel para no modificarla.

Cantidad mínima de

Changed characters. Escriba la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es 0.

Symbols. Especifique la cantidad mínima de símbolos necesarios en un código de acceso. El valor predeterminado es 0.

Cantidad máxima de

Number of times a character can occur. Especifique la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es 0.

Alphabetic sequence length. Escriba la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es 0.

Numeric sequence length. Escriba la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es 0.

Seguridad de códigos de acceso

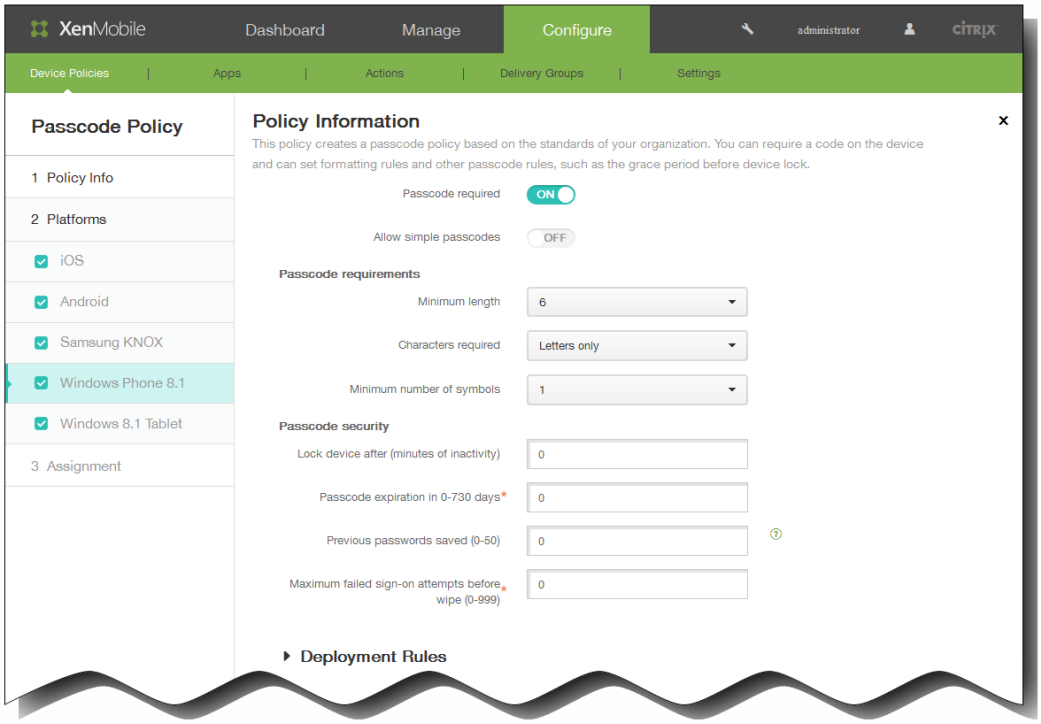
Lock device after (minutes of inactivity). En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es None.
Nota: Aunque este campo tenga la etiqueta "minutes of inactivity", XenMobile aplica el bloqueo una vez transcurrida la cantidad especificada de *segundos*.
Passcode expiration in days (1-730). Especifique la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es 0, lo que significa que el código de acceso no caduca nunca.

Previous passwords saved (0-50). Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado

es 0, lo que significa que los usuarios pueden reutilizar contraseñas.

Maximum failed sign-on attempts. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se bloquee el dispositivo. El valor predeterminado es Not defined.

- Si ha seleccionado Windows Phone 8.1, configure los siguientes parámetros:



Passcode required. Seleccione esta opción para no requerir un código de acceso en los dispositivos Windows Phone 8.1. El parámetro predeterminado es ON, lo que requiere un código de acceso. La página se contrae y las siguientes opciones desaparecen. Si no desactiva el requisito del código de acceso, siga definiendo las siguientes opciones de configuración.

Allow simple passcodes. Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es OFF.

Requisitos de códigos de acceso

Minimum length. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.

Characters required. En la lista, haga clic en Numeric or alphanumeric, Letters only o Numbers only para definir la composición de los códigos de acceso. El valor predeterminado es Letters only.

Minimum number of symbols. En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es 1.

Seguridad de códigos de acceso

Lock device after (minutes of inactivity). En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar

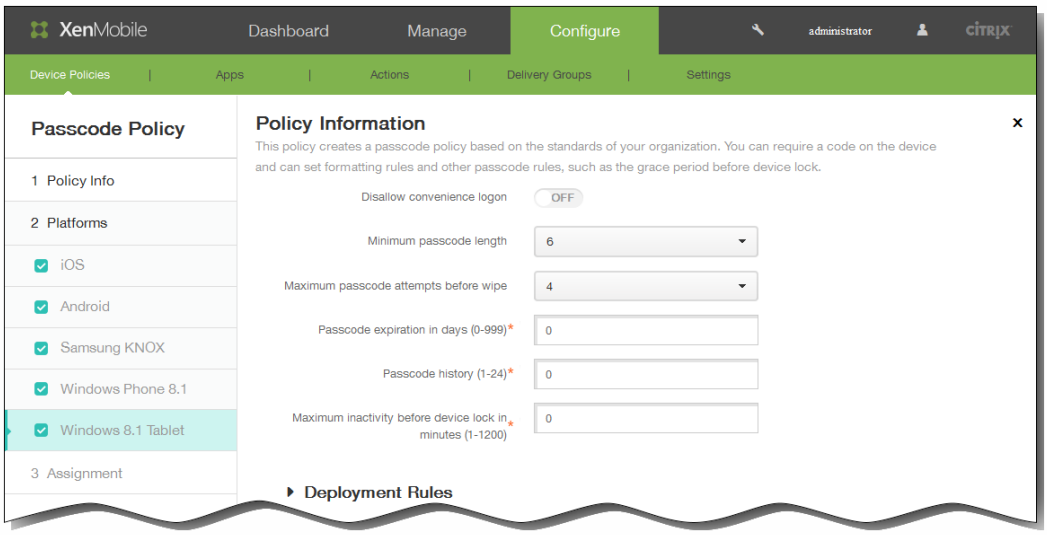
inactivo antes de bloquearse. El valor predeterminado es 0.

Passcode expiration in 0-730 days. Especifique la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es 0, lo que significa que el código de acceso no caduca nunca.

Previous passwords saved (0-50). Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es 0, lo que significa que los usuarios pueden volver a usar las contraseñas.

Maximum failed sign-on attempts before wipe (0-999). En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión hasta que los datos de empresa de borren del dispositivo. El valor predeterminado es 0.

- Si ha seleccionado Windows 8.1 Tablet, configure los siguientes parámetros:



Disallow convenience logon. Seleccione si permitir que los usuarios accedan a sus dispositivos con contraseñas de imagen o inicios de sesión biométricos. El valor predeterminado es OFF.

Minimum passcode length. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.

Maximum passcode attempts before wipe. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se borre toda la información del dispositivo. El valor predeterminado es 4.

Passcode expiration in days (0-999). Especifique la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 999 es válido. El valor predeterminado es 0, lo que significa que el código de acceso no caduca nunca.

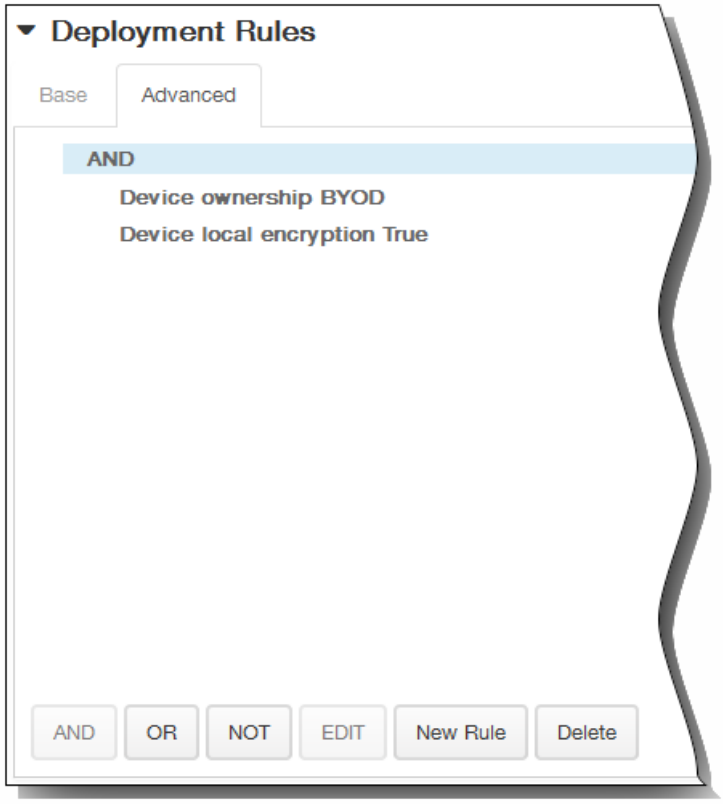
Passcode history: (1-24). Introduzca la cantidad de códigos de acceso utilizados a guardar. Los usuarios no pueden usar ningún código de acceso que esté incluido en esta lista. Cualquier valor entre 1 y 24 es válido. En este campo debe escribir un número entre 1 y 24.

Maximum inactivity before device lock in minutes (1-1200). Introduzca la cantidad de tiempo (en minutos) que un dispositivo puede estar inactivo antes de bloquearse. Cualquier valor entre 1 y 1200 es válido. En este campo debe

escribir un número entre 1 y 1200.

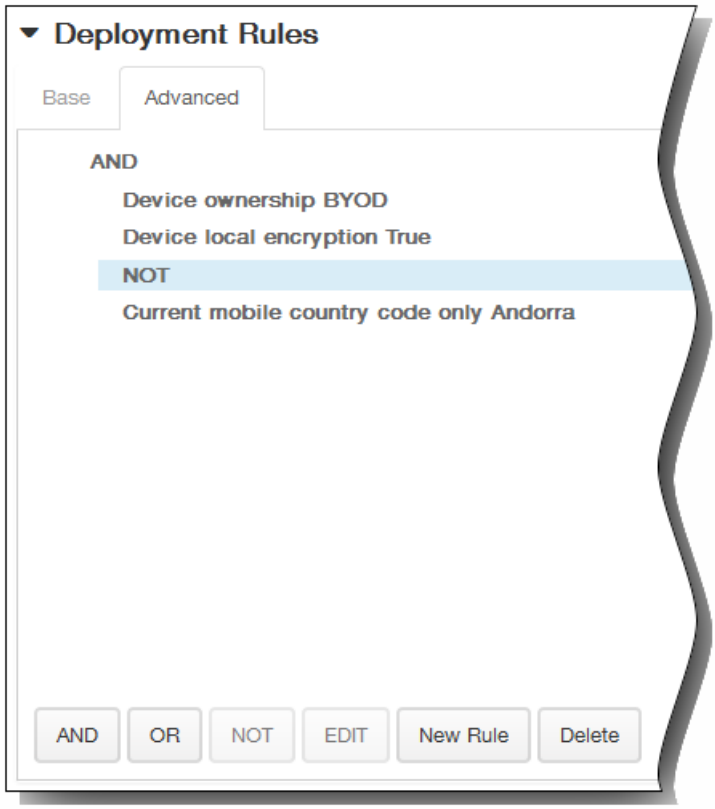
5. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

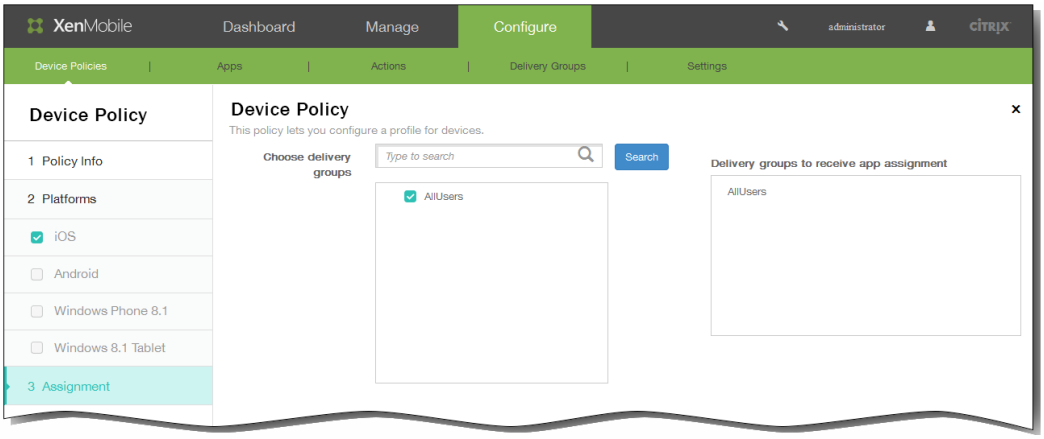


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.

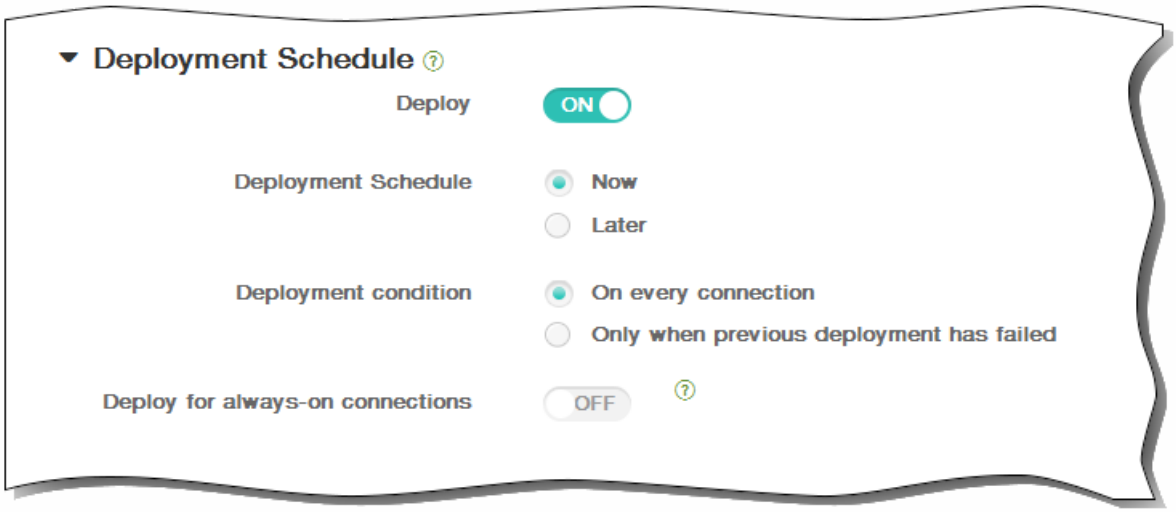


6. Haga clic en Next. Aparecerá la página de asignación Passcode Policy.
7. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



8. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
   1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
   2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
   3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
   4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
   5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
      Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

   Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



9. Haga clic en Guardar.

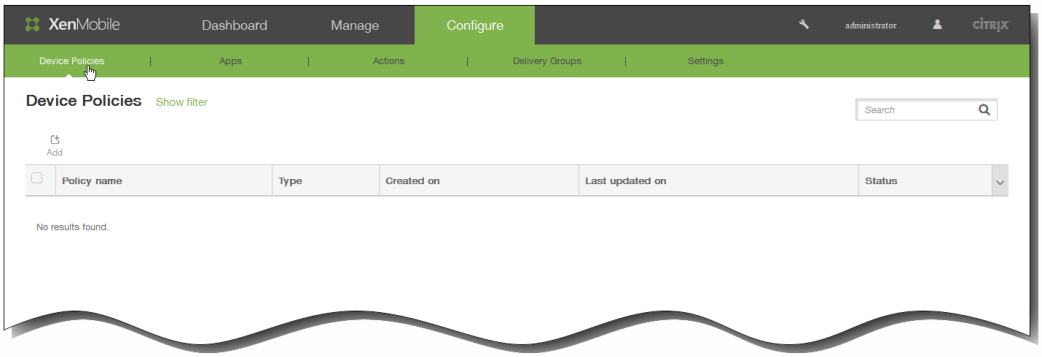
Para agregar una directiva de proxy para dispositivos iOS

May 05, 2016

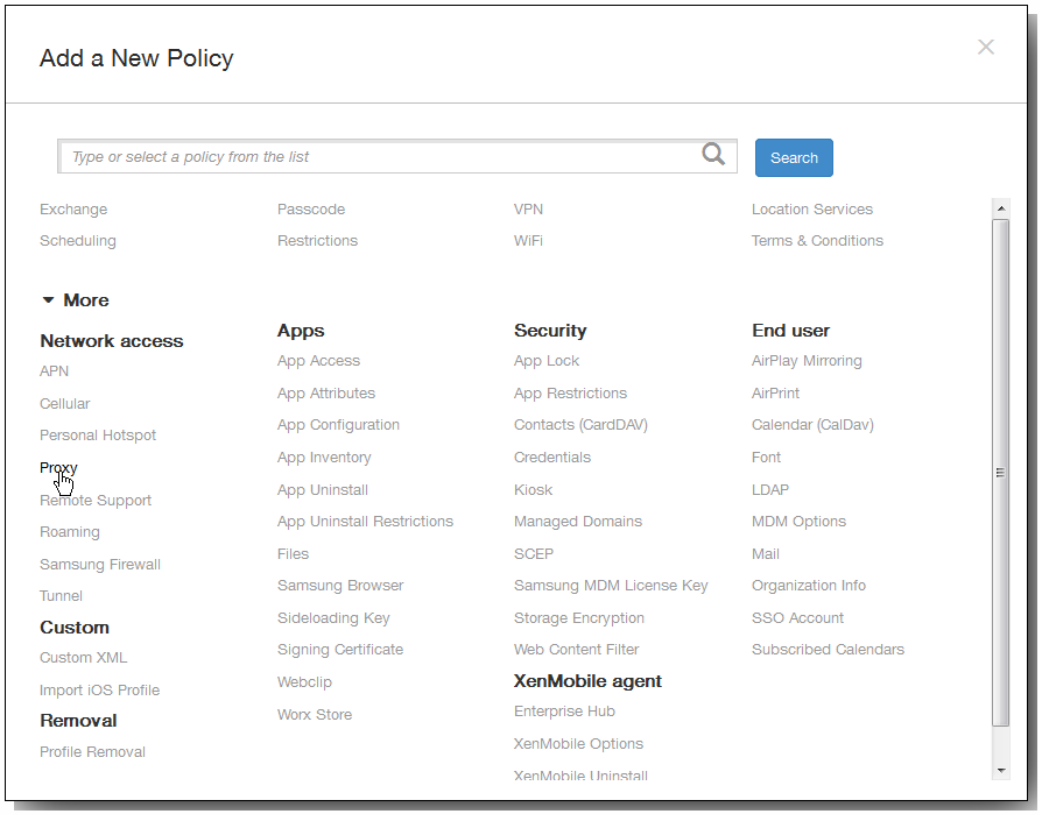
En XenMobile, puede agregar una directiva de dispositivos para especificar la configuración global de proxy HTTP en dispositivos con iOS 6.0 o versiones posteriores. Puede implementar solamente una directiva global de proxy HTTP por dispositivo.

Nota: Antes de implementar esta directiva, coloque en modo supervisado todos los dispositivos iOS para los que quiere establecer un proxy global de HTTP. Para obtener información más detallada, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

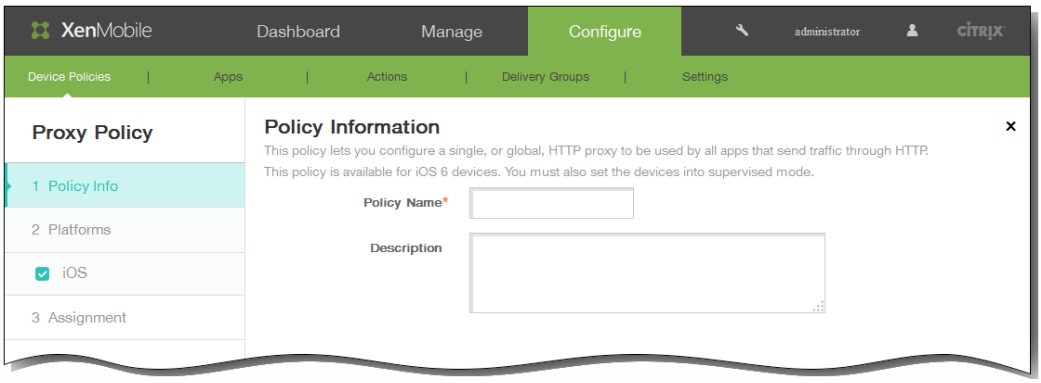
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



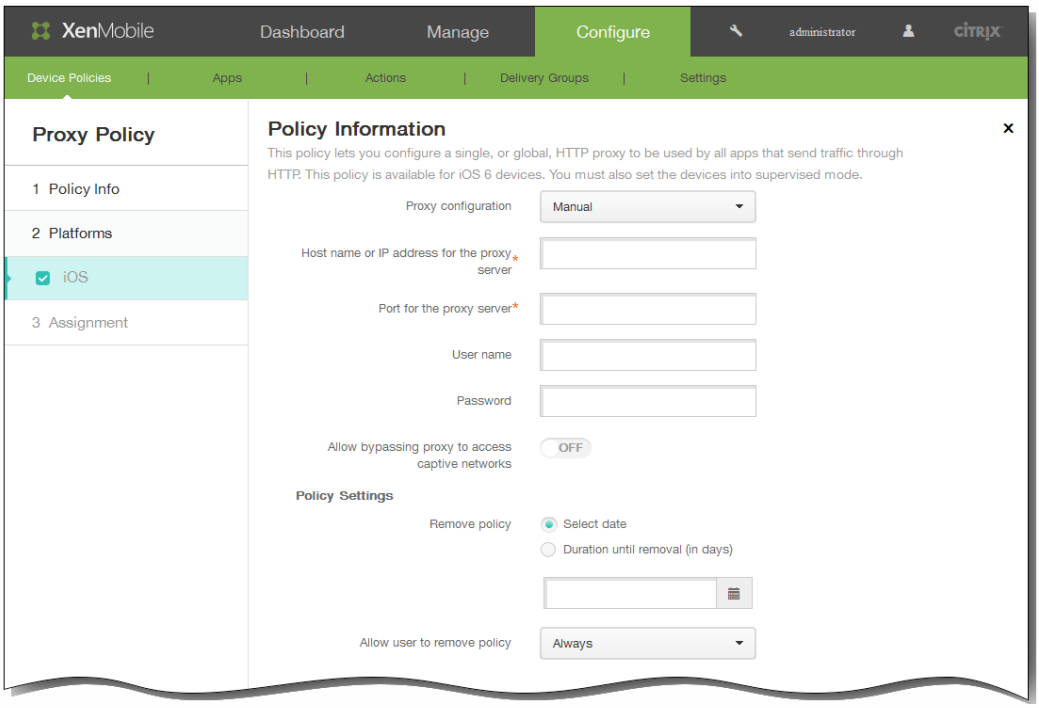
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en Network access, haga clic en Proxy. Aparecerá la página Proxy Policy.



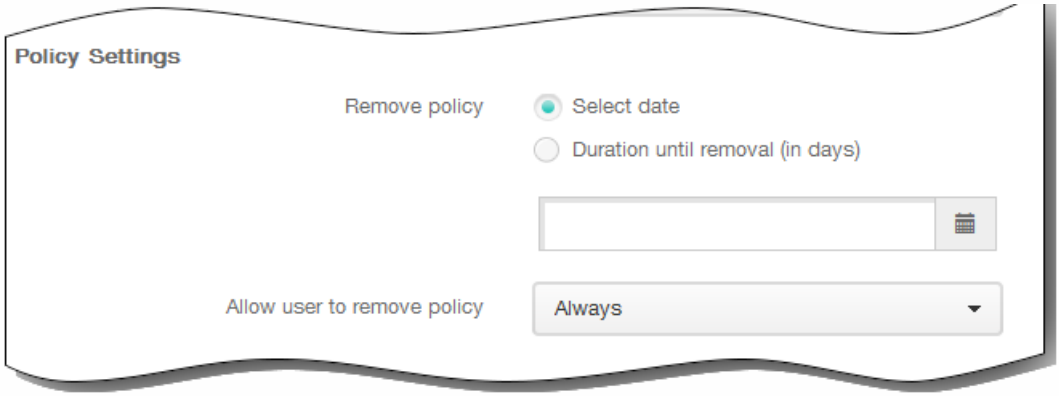
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



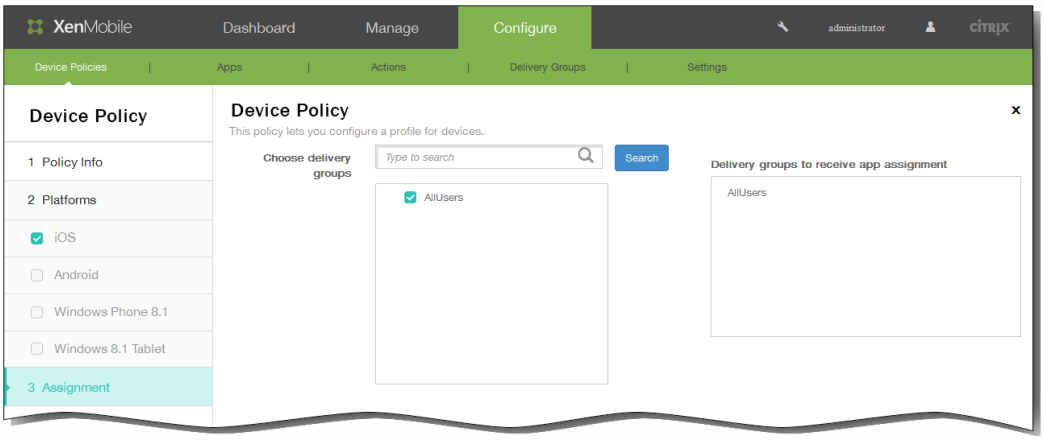
6. En la página de información iOS Platform, escriba la información siguiente:
   1. Proxy configuration. Haga clic en Manual o Automatic para determinar cómo se configurará el proxy en los dispositivos de los usuarios. En la siguiente tabla se ofrece una lista de las opciones disponibles para cada configuración de proxy. Cada celda indica si la opción no es aplicable (–), si es necesaria o si es opcional.

	Manual	Automatic
Host name or IP address for the proxy server	Requerido	–
Port for the proxy server	Requerido	–
User name	Opcional	–
Contraseña	Opcional	–
Proxy PAC URL	–	Opcional
Allow direct connection if PAC is unreachable	–	OFF

   2. Allow bypassing proxy to access captive networks. Seleccione si permitir que el dispositivo omita el servidor proxy y pueda acceder a redes cautivas.
7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

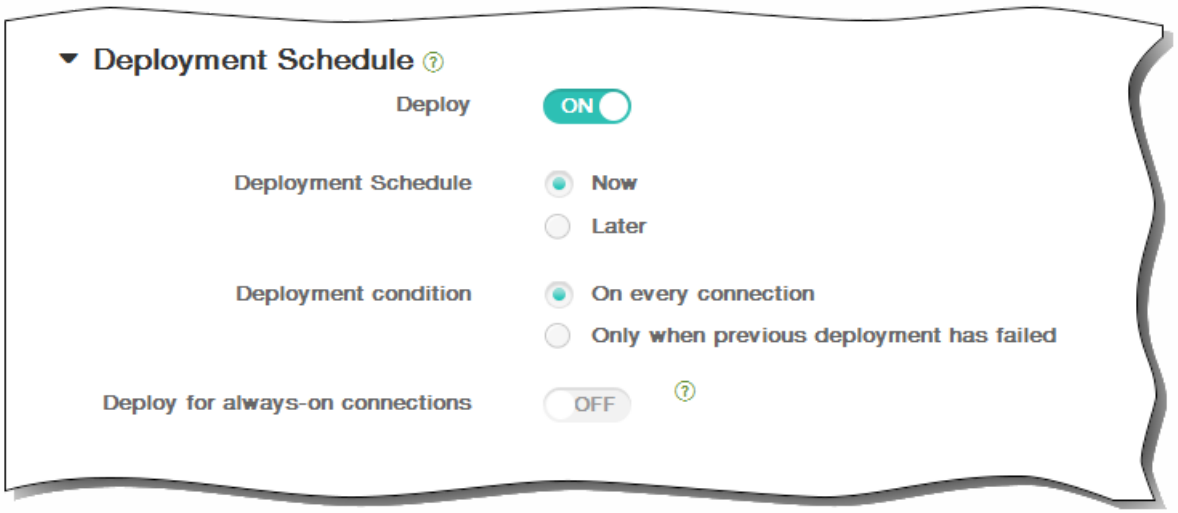


11. Haga clic en Next. Aparecerá la página de asignación Proxy Policy.
12. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



13. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
    5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
       Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

    Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



14. Haga clic en Save para guardar la directiva.

Para agregar una directiva de asistencia remota para dispositivos Samsung KNOX

May 05, 2016

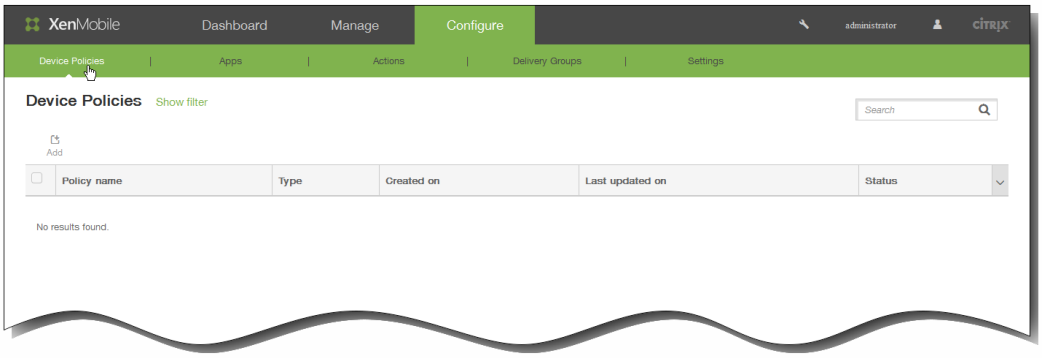
En XenMobile, puede crear una directiva de asistencia remota mediante la que puede acceder de forma remota a los dispositivos Samsung KNOX de los usuarios. Puede configurar dos tipos de asistencia:

- **Basic**. Esta opción permite ver la información de diagnóstico referente al dispositivo, como la información del sistema, los procesos que se están ejecutando, el administrador de tareas (el uso de memoria y de CPU) o el contenido de las carpetas del software instalado, entre otros.
- **Premium**. Esta opción permite controlar de forma remota la pantalla del dispositivo, incluido el control sobre los colores (ya sea en la ventana principal o en una ventana separada flotante). Asimismo, permite establecer una sesión mediante voz sobre IP (VoIP) entre el servicio de asistencia técnica y el usuario, configurar parámetros y establecer una sesión de chat entre el usuario y el departamento de asistencia técnica.

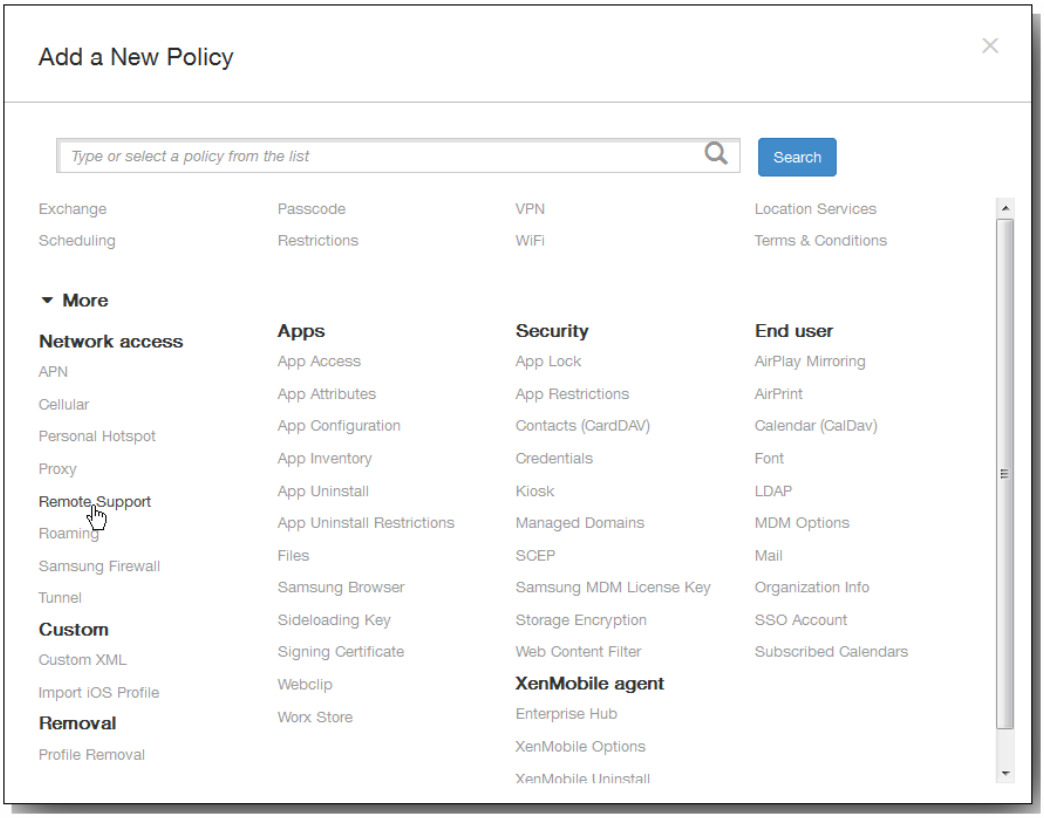
Nota: Para implementar esta directiva, debe realizar lo siguiente:

- Instalar la aplicación XenMobile Remote Support en su entorno.
- Configurar un túnel de aplicaciones para asistencia remota. Para obtener información más detallada, consulte Para agregar una directiva de túneles de aplicaciones para dispositivos Android.
- Configurar una directiva de asistencia remota para dispositivos Samsung KNOX como se describe en este apartado.
- Implementar la directiva de asistencia remota por túnel de aplicaciones y la directiva de asistencia remota de Samsung KNOX en los dispositivos de los usuarios.

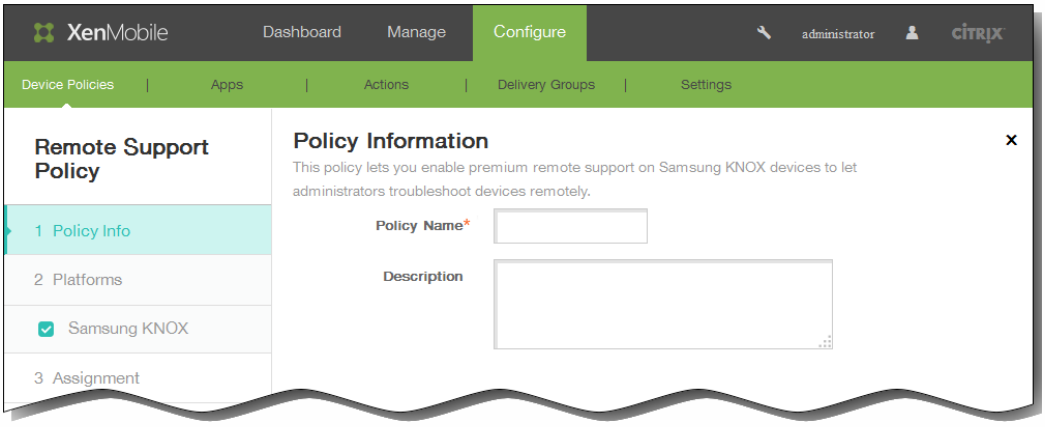
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



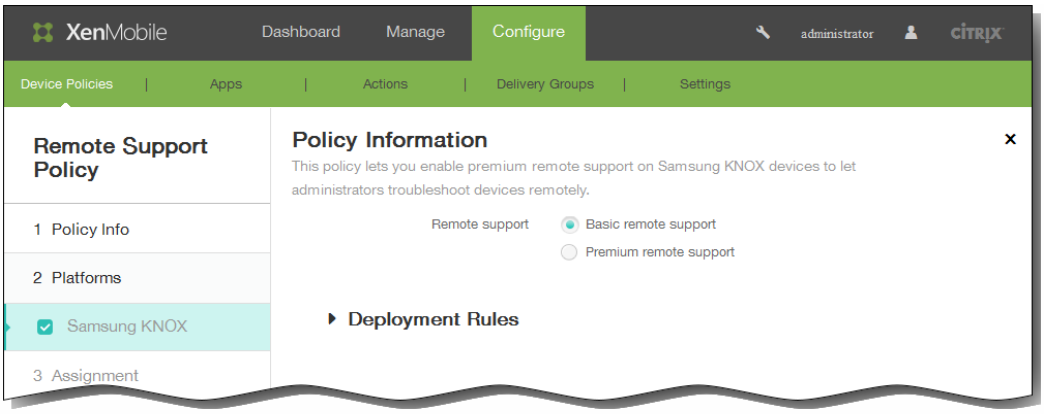
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en Network access, haga clic en Remote Support. Aparecerá la página Remote Support Policy.

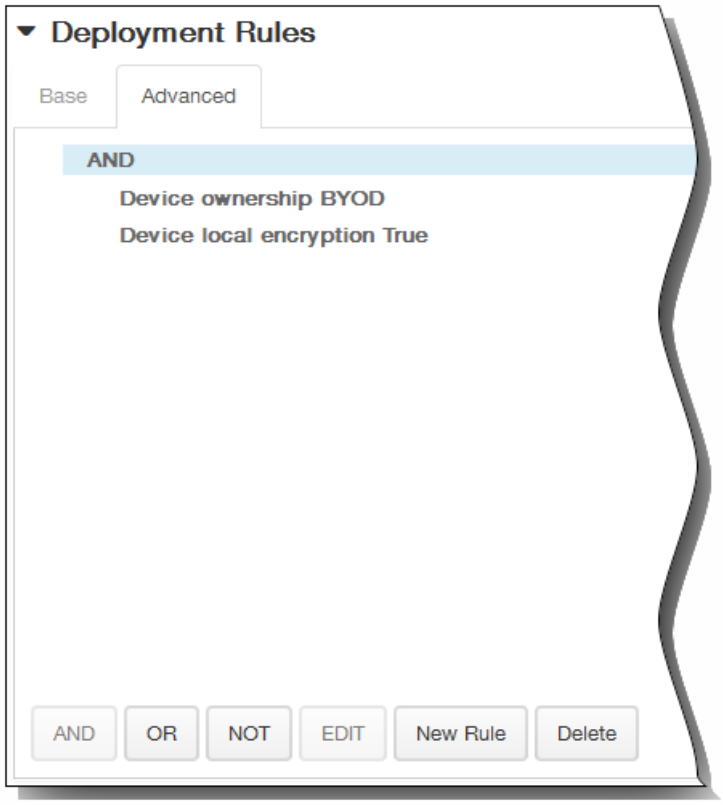


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información acerca de la plataforma Samsung KNOX.



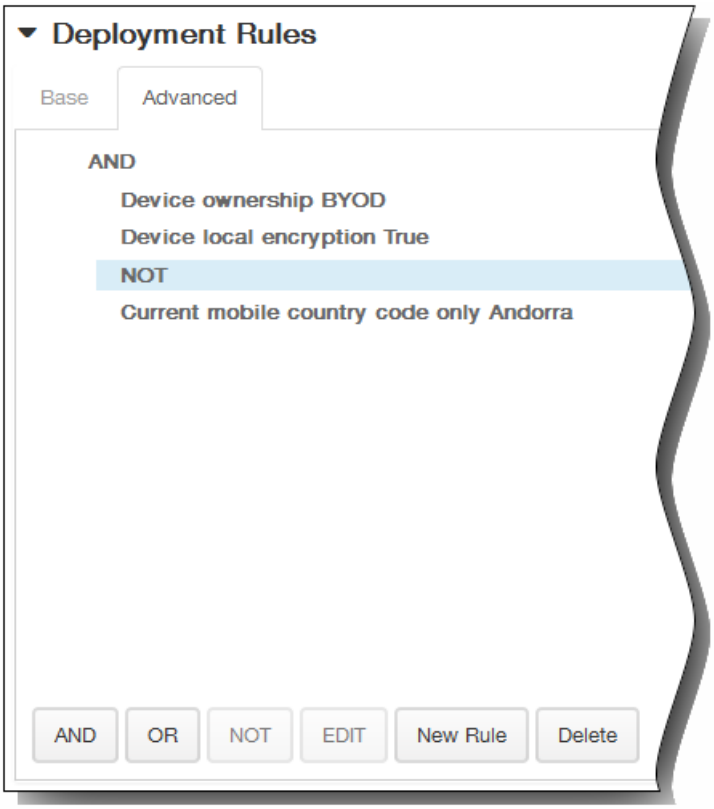
6. En la página de información acerca de la plataforma Samsung KNOX, escriba la información siguiente:
   1. Remote support. Seleccione Basic remote support o Premium remote support. El valor predeterminado es Basic remote support.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
      2. Haga clic en New Rule para definir las condiciones.
      3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
      4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
   2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

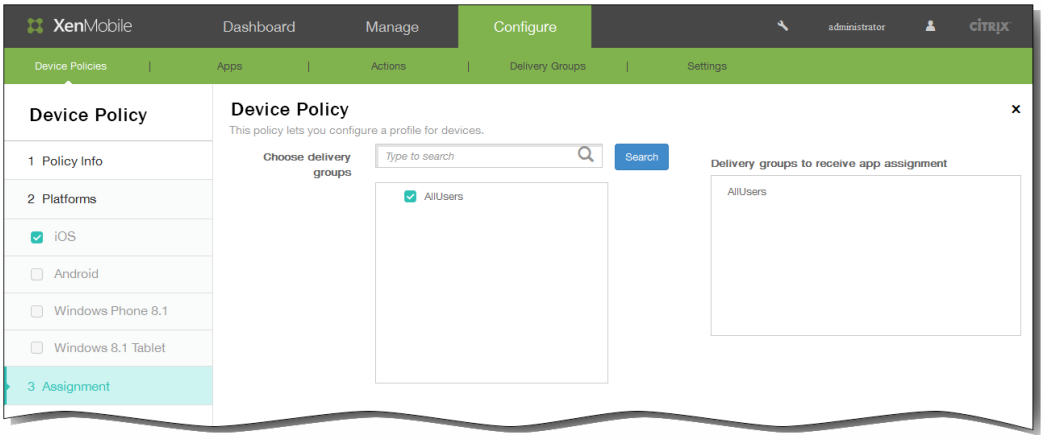


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



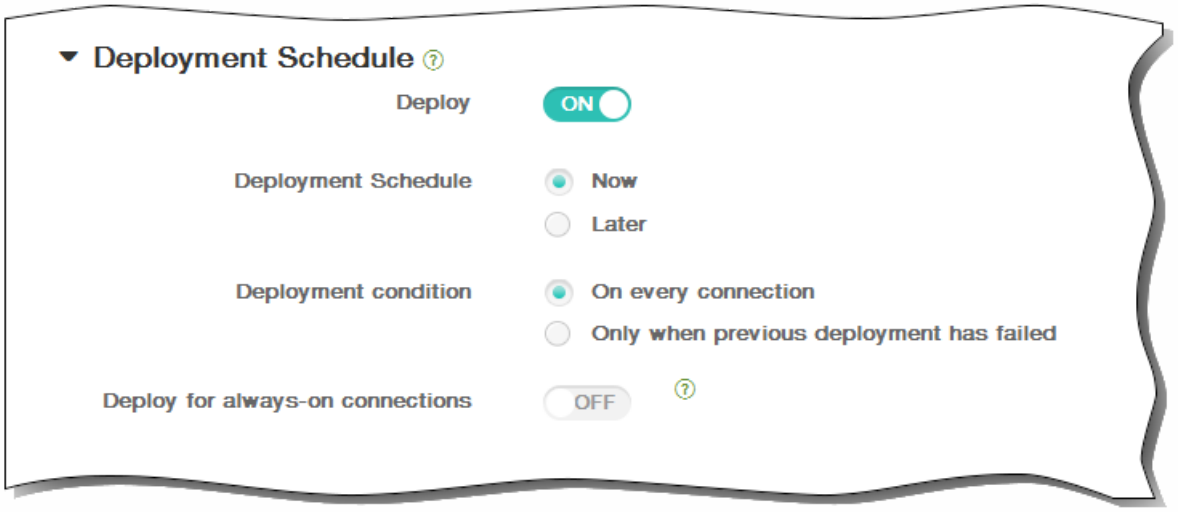
8. Haga clic en Next. Aparecerá la página de asignación Remote Support Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

Directivas de restricciones

May 05, 2016

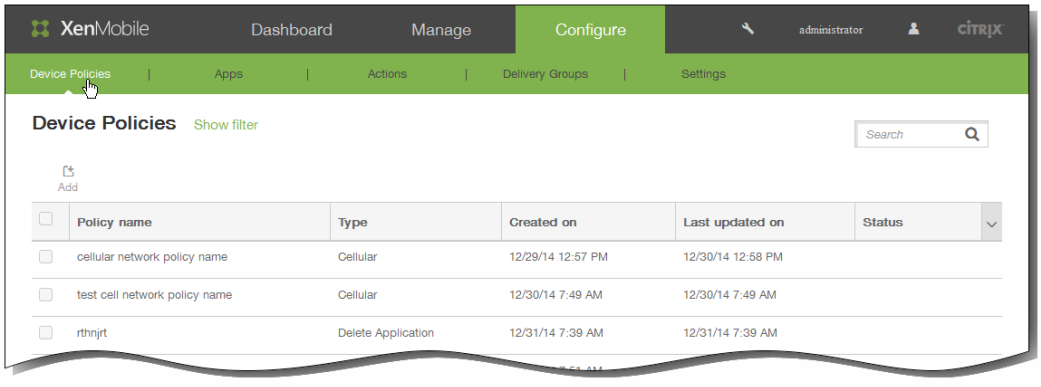
En XenMobile, puede agregar una directiva de dispositivos para restringir algunas funciones en los teléfonos, las tabletas y los dispositivos de los usuarios, entre otros. Puede configurar la directiva de restricciones para las plataformas siguientes: iOS, Samsung SAFE, tabletas Windows 8.1, Windows Phone 8.1 y Amazon. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

Esta directiva permite o prohíbe a los usuarios utilizar funciones determinadas, como la cámara, en sus dispositivos. También puede estipular restricciones de seguridad, de contenido multimedia y de tipos de aplicaciones que los usuarios puedan o no puedan instalar. El valor predeterminado de la mayoría de las opciones de restricción es ON o
— allows
. La excepción principal es la función "Security - Force", cuyo valor predeterminado es OFF o
— restricts
.
Sugerencia: Si selecciona
— ON
para alguna opción, el usuario podrá realizar la operación o usar la función. Por ejemplo:

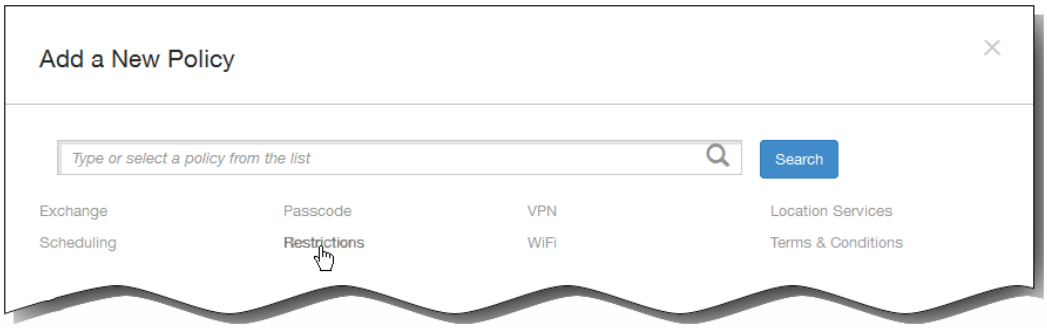
- Camera. Si la opción está establecida en ON, el usuario puede usar la cámara en su dispositivo. Si está establecida en OFF, el usuario no puede usar la cámara en su dispositivo.
- **Screen shots**. Si la opción está establecida en ON, el usuario puede realizar capturas de pantalla en su dispositivo. Si está establecida en OFF, el usuario no puede realizar capturas de pantalla en su dispositivo.

Nota: Algunas opciones de restricción de iOS solo se aplican a versiones específicas de iOS (si es el caso, estas versiones se mencionan en la página de la consola de XenMobile). Además, algunas opciones solo se aplican si el dispositivo se coloca en el modo supervisado. Por ejemplo, la capacidad para permitir o bloquear AirDrop solo se respalda en dispositivos con iOS 7 y versiones posteriores, mientras que la capacidad para permitir o bloquear Photo Stream se respalda en dispositivos con iOS 5 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

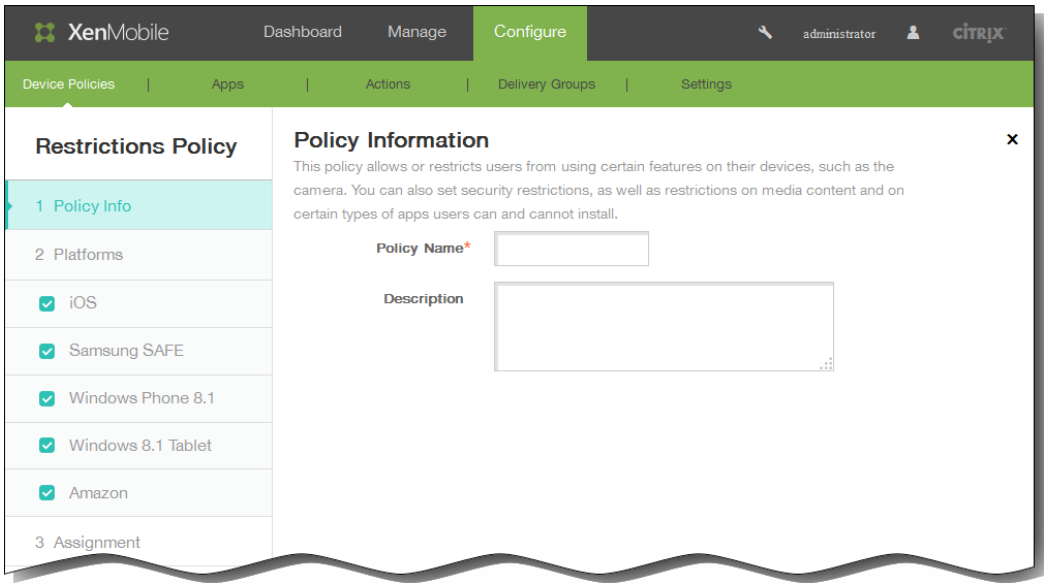
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



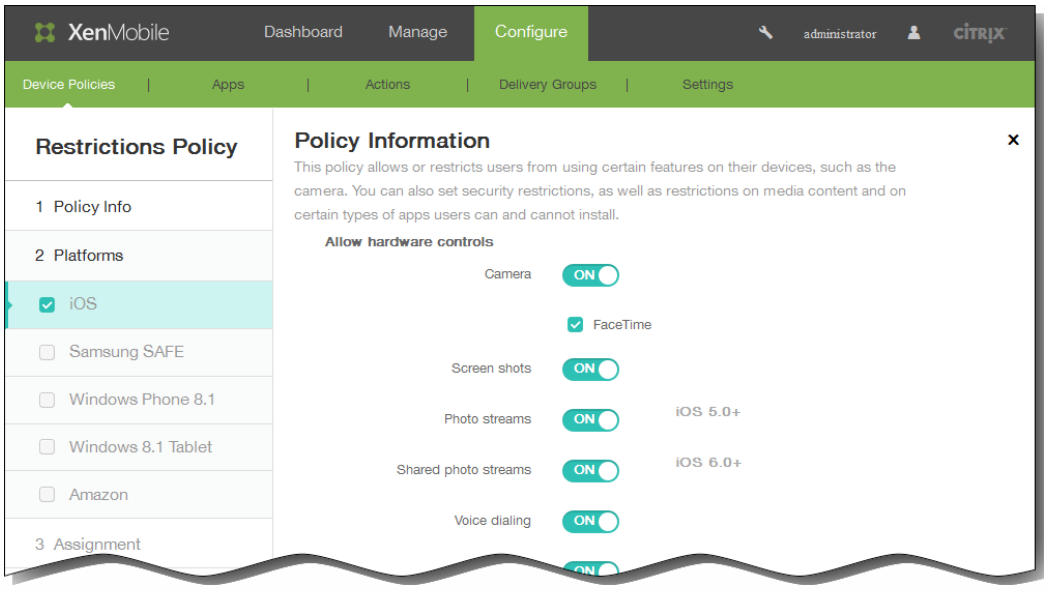
2. Haga clic en Agregar. Aparecerá la página Add a New Policy.



3. Haga clic en Restrictions.
   Aparecerá la página de información Restrictions Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. En Platforms, seleccione la plataforma o las plataformas que quiere agregar. Puede cambiar la información de la directiva para cada plataforma seleccionada. Haga clic para restringir las funciones de los siguientes apartados, con lo que cambiará la opción de configuración a OFF. A menos que se indique lo contrario, el valor predeterminado es habilitar la función.
   - Si ha seleccionado iOS, configure los siguientes parámetros:



- Allow hardware controls:

  Camera; FaceTime

  Screen shots

  Photo streams (disponible en iOS 5.0 y versiones posteriores)

  Shared photo streams (disponible en iOS 6.0 y versiones posteriores)

  Voice dialing

  Siri:
  - Allow while device is locked. Deje la opción marcada de forma predeterminada, o bien desmarque la casilla de verificación.
  - Siri profanity filter. Deje la opción desmarcada de forma predeterminada, o bien marque la casilla de verificación. (El valor predeterminado de la opción de configuración es el de función restringida.)

  Installing apps

- Allow apps:

  YouTube

  iTunes Store

  In-app purchases: Require iTunes password for purchases. Deje la opción desmarcada de forma predeterminada, o bien marque la casilla de verificación (disponible en iOS 5.0 y versiones posteriores). (El valor predeterminado de la opción de configuración es el de función restringida.)

  Safari:
  - Autofill. Deje la opción marcada de forma predeterminada, o bien desmarque la casilla de verificación.
  - Force fraud warning. Deje la opción desmarcada de forma predeterminada, o bien marque la casilla de verificación. (El valor predeterminado de la opción de configuración es el de función restringida.)
  - Enable JavaScript. Deje la opción marcada de forma predeterminada, o bien desmarque la casilla de verificación.

- Block pop-ups. Deje la opción desmarcada de forma predeterminada, o bien marque la casilla de verificación. (El valor predeterminado de la opción de configuración es el de función restringida.)

En Accept cookies, haga clic en una de las siguientes opciones:

- Always
- Never
- From visited sites only

La opción predeterminada es Always.

- Network - Allow iCloud actions:

  Documents and data sync (disponible en iOS 5.0 y versiones posteriores)

  Device backup (disponible en iOS 5.0 y versiones posteriores)

  Automatic sync while roaming

  iCloud keychain (disponible en iOS 7.0 y versiones posteriores)

- Security - Force:

  Encrypted backups. El valor predeterminado es OFF.

  Limited ad tracking (disponible en iOS 7.0 y versiones posteriores). El valor predeterminado es OFF.

  Passcode on first Airplay pairing (disponible en iOS 7.0 y versiones posteriores). El valor predeterminado es OFF.

- Security - Allow:

  Accepting untrusted SSL certificates (disponible en iOS 5.0 y versiones posteriores)

  Automatic update to certificate trust settings (disponible en iOS 7.0 y versiones posteriores)

  Documents from managed apps in unmanaged apps

  Documents from unmanaged apps in managed apps

  Diagnostic submission to Apple

  Touch ID to unlock device (disponible en iOS 7.0 y versiones posteriores)

  Passbook notifications when locked (disponible en iOS 6.0 y versiones posteriores)

  Handoff (disponible en iOS 8.0 y versiones posteriores)

  iCloud sync for managed apps (disponible en iOS 8.0 y versiones posteriores)

  Backup for enterprise books (disponible en iOS 8.0 y versiones posteriores)

  Notes and highlights sync for enterprise books (disponible en iOS 8.0 y versiones posteriores)

- Supervised only settings - Allow:

  Internet results in Spotlight (disponible en iOS 8.0 y versiones posteriores)

  Erase all content and settings (disponible en iOS 8.0 y versiones posteriores)

Configuring restriction (disponible en iOS 8.0 y versiones posteriores)

Installing configuration profiles (disponible en iOS 6.0 y versiones posteriores)

AirDrop (disponible en iOS 7.0 y versiones posteriores)

iMessage (disponible en iOS 6.0 y versiones posteriores)

Siri user-generated content (disponible en iOS 7.0 y versiones posteriores)

iBooks (disponible en iOS 6.0 y versiones posteriores)

Removing apps (disponible en iOS 7.0 y versiones posteriores)

Game Center (disponible en iOS 6.0 y versiones posteriores)
- Add friends. Deje la opción marcada de forma predeterminada, o bien desmarque la casilla de verificación.
- Multiplayer gaming. Deje la opción marcada de forma predeterminada, o bien desmarque la casilla de verificación.

Modifying account settings (disponible en iOS 7.0 y versiones posteriores)

Modifying app cellular data settings (disponible en iOS 7.0 y versiones posteriores)

Modifying Find My Friends settings (disponible en iOS 7.0 y versiones posteriores)

Pairing with non-Configurator hosts (disponible en iOS 7.0 y versiones posteriores)

Single App bundle ID. En App name, introduzca una o varias aplicaciones.

- Security - Show in lock screen:

  Control Center (disponible en iOS 7.0 y versiones posteriores)

  Notification (disponible en iOS 7.0 y versiones posteriores)

  Today view

- Media content - Allow:

  Explicit music, podcasts, and iTunes U material

  Explicit sexual content in iBooks (disponible en iOS 6.0 y versiones posteriores)

  Ratings region. Haga clic en un país de la lista. El valor predeterminado es United States.

  Movies. Haga clic en una de estas opciones: Allow all movies, Block movies, G, PG, PG-13, R o NC-17. El valor predeterminado es Allow all movies.

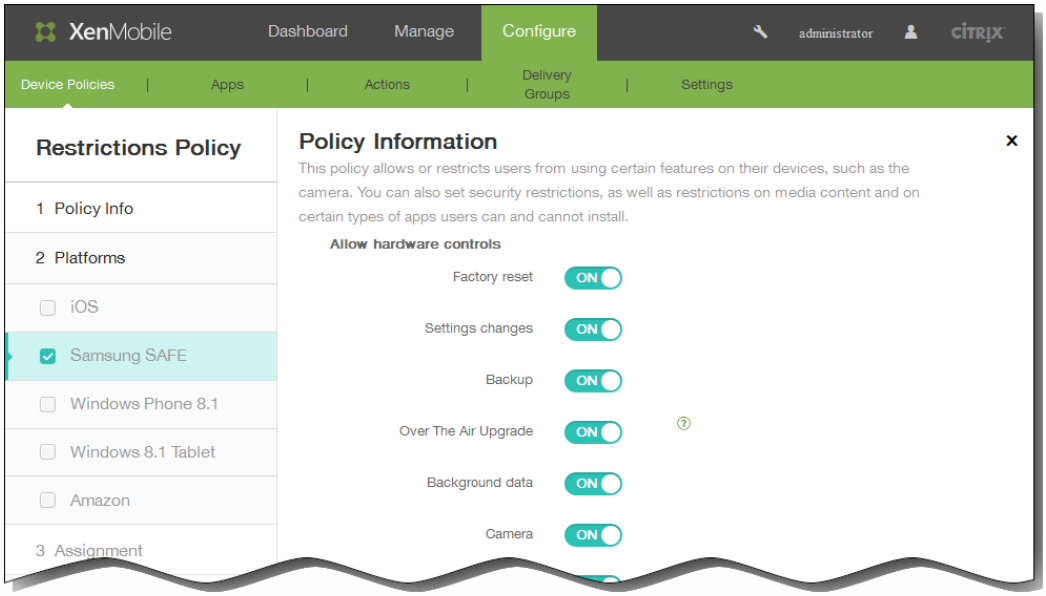
  TV Shows. Haga clic en una de estas opciones: Allow all TV shows, Block TV shows, TV-Y, TV-Y7, TV-G, TV-PG, TV-PG14 o TV-MA. El valor predeterminado es Allow all TV Shows.

  Apps. Haga clic en una de estas opciones: Allow all apps, Block apps, 4+, 9+, 12+ o 17+. El valor predeterminado es Allow all apps.

- Si ha seleccionado Samsung SAFE, configure los siguientes parámetros:

  Nota: Algunas opciones solo están disponibles en Samsung Mobile Device Management API 4.0 y versiones

posteriores; están marcadas con (MDM 4.0 y versiones posteriores).



- En Allow hardware controls:

  Factory Reset

  Settings changes

  Backup

  Over The Air Upgrade (MDM 4.0 y versiones posteriores)

  Background data

  Camera

  Clipboard

  Clipboard share (MDM 4.0 y versiones posteriores)

  Home key

  Microphone

  Mock location

  NFC (Near Field Communication) (MDM 4.0 y versiones posteriores)

  Power off (MDM 4.0 y versiones posteriores)

  Screenshot

  SD card

  Voice Dialer (MDM 4.0 y versiones posteriores)

SBeam (MDM 4.0 y versiones posteriores)

SVoice (MDM 4.0 y versiones posteriores)

- En Allow apps:

  Browser

  YouTube

  GooglePlay/Marketplace

  Allow No-Google Play apps

  Stop system app (MDM 4.0 y versiones posteriores)

- En Network:

  Bluetooth; Tethering

  WiFi; Tethering, Direct (MDM 4.0 y versiones posteriores)

  Tethering

  Cellular data

  Allow roaming. El valor predeterminado es OFF.

  Only secure connections

  Android beam (MDM 4.0 y versiones posteriores)

  Audio record (MDM 4.0 y versiones posteriores)

  Video record (MDM 4.0 y versiones posteriores)

  Servicios de localización

  Limit by day (MB). Escriba la cantidad de MB al día que se permite a los usuarios. El valor predeterminado es 0, lo que inhabilita esta función. (MDM 4.0 y versiones posteriores.)

  Limit by week (MB). Escriba la cantidad de MB por semana que se permite a los usuarios. El valor predeterminado es 0, lo que inhabilita esta función. (MDM 4.0 y versiones posteriores.)

  Limit by month (MB). Escriba la cantidad de MB al mes que se permite a los usuarios. El valor predeterminado es 0, lo que inhabilita esta función. (MDM 4.0 y versiones posteriores.)

- En Allow USB actions:

  Debugging

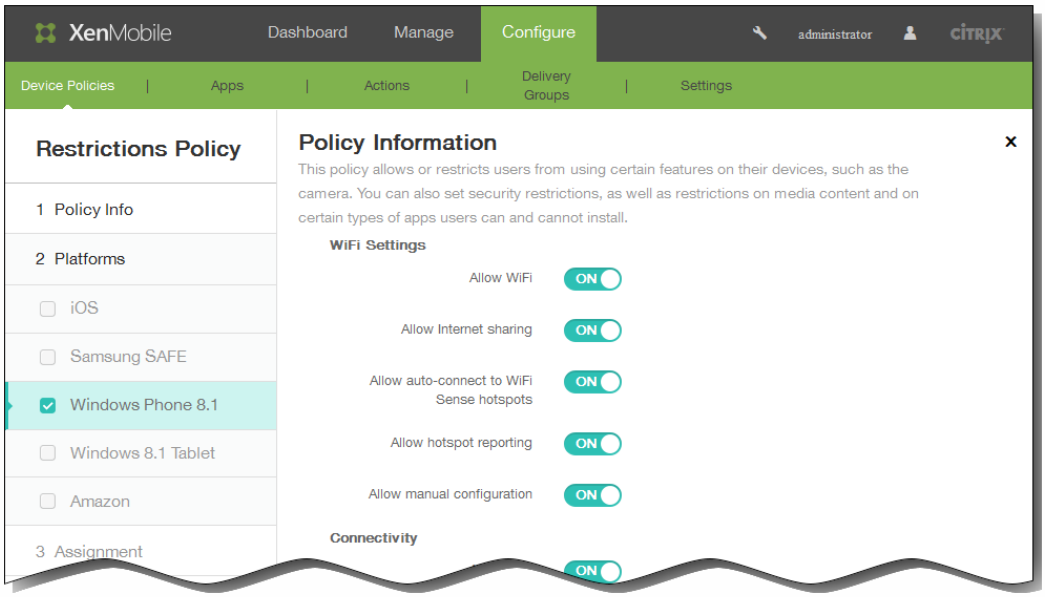
  Host storage

  Mass storage

  Kies media player

Tethering

- Si ha seleccionado Windows Phone 8.1, configure los siguientes parámetros:



- WiFi Settings:

  Allow WiFi

  Allow Internet sharing

  Allow auto-connect to WiFiSense hotspots

  Allow hotspot reporting

  Allow manual configuration

- Connectivity:

  Allow NFC (Near Field Communication)

  Allow Bluetooth

  Allow VPN over cellular

  Allow VPN over cellular while roaming

  Allow USB connection

  Allow cellular data roaming

- Accounts:

  Allow Microsoft account connection

Allow non-Microsoft email

- Search:

  Allow search to use location

  Filter adult content (El valor predeterminado es OFF.)

  Allow Bing Vision to store images

- System:

  Allow storage card

  Allow location services

  Allow use of camera

  Telemetry. Haga clic en uno de estos parámetros: Allowed, Not Allowed o Allowed except for secondary data request. El valor predeterminado es Allowed.

- Security:

  Allow manual root certificate installation

  Require device encryption. El valor predeterminado es OFF.

  Allow copy and paste

  Allow screen capture

  Allow voice recording

  Allow Save As of Office files

  Allow action center notifications

  Allow Cortana

  Allow sync of device settings

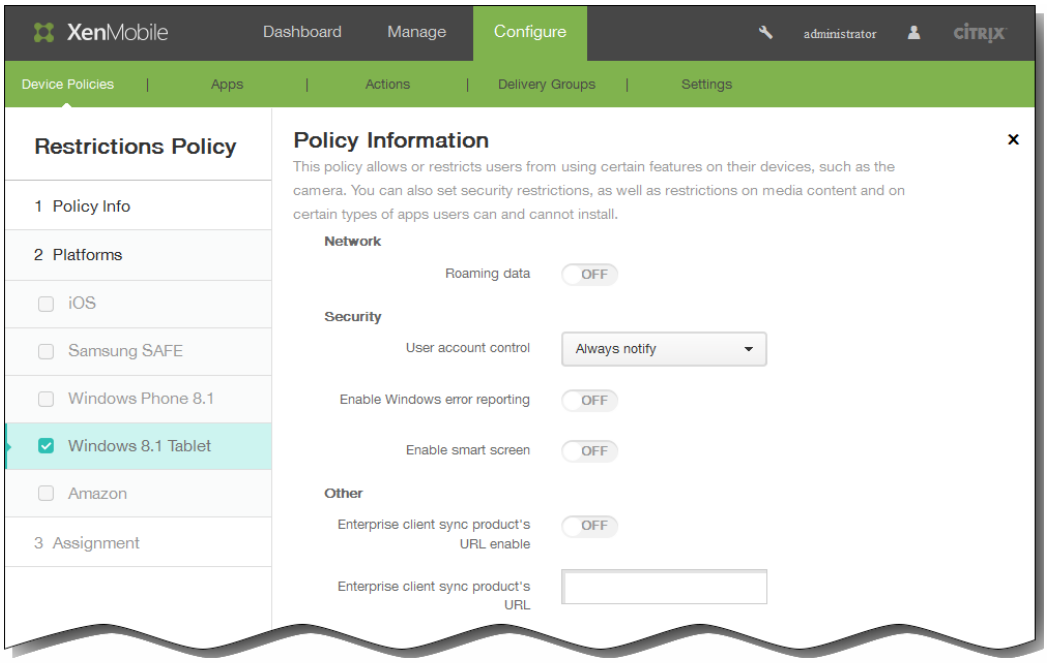
- Apps:

  Allow store access

  Allow developer unlock

  Allow web browser access

- Si ha seleccionado Windows 8.1 tablet, configure los siguientes parámetros:



- Network:

  Roaming data

- Security:

  User account control. En la lista, haga clic en una de las siguientes opciones: Always notify, Notify app changes, Notify app changes (no dim) o Never notify. El valor predeterminado es Always notify.

  Enable Windows error reporting

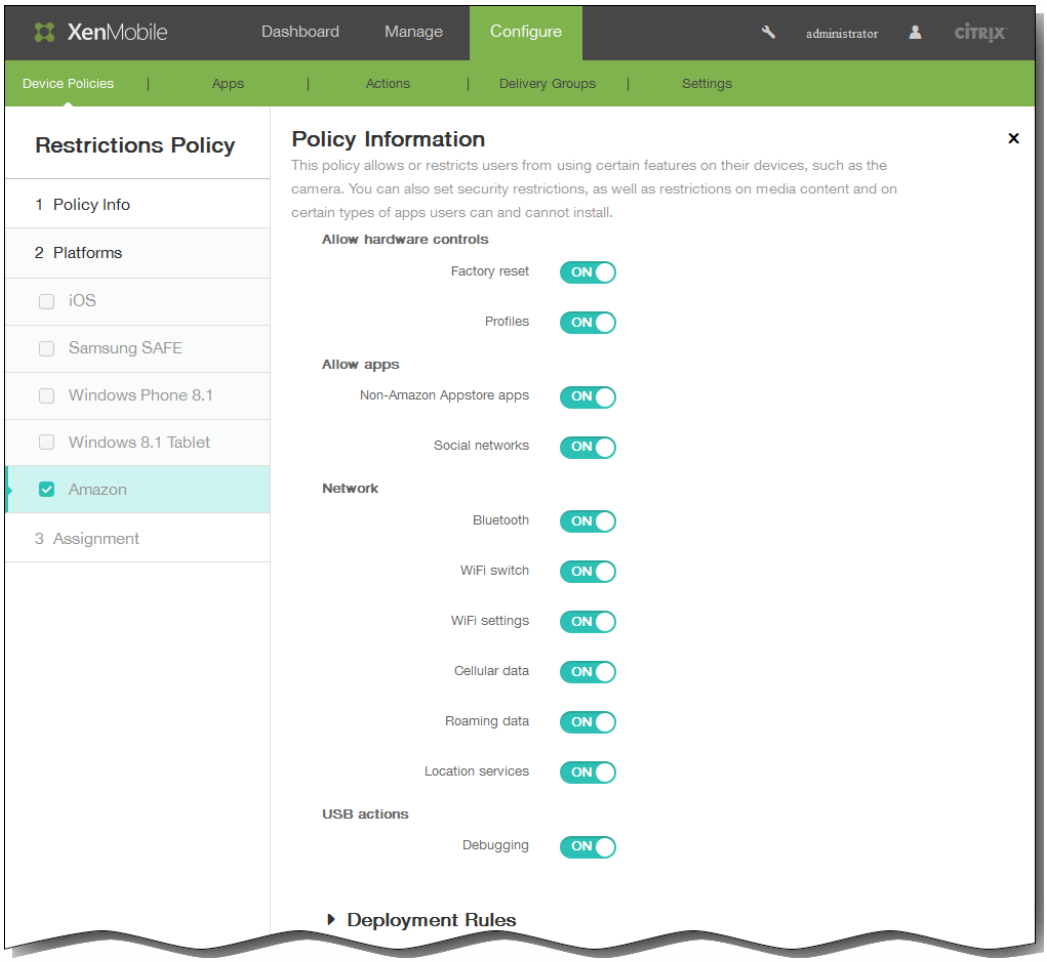
  Enable smart screen

- Other:

  Enterprise client sync product's URL enable

  Enterprise client sync product's URL. Escriba una dirección URL válida.

- Si ha seleccionado Amazon, configure los siguientes parámetros:



- Allow hardware controls:

  Factory reset

  Profiles

- Allow apps:

  Non-Amazon Appstore apps

  Social networks

- Network:

  Bluetooth

  WiFi switch

  WiFi settings

  Cellular data

  Roaming data

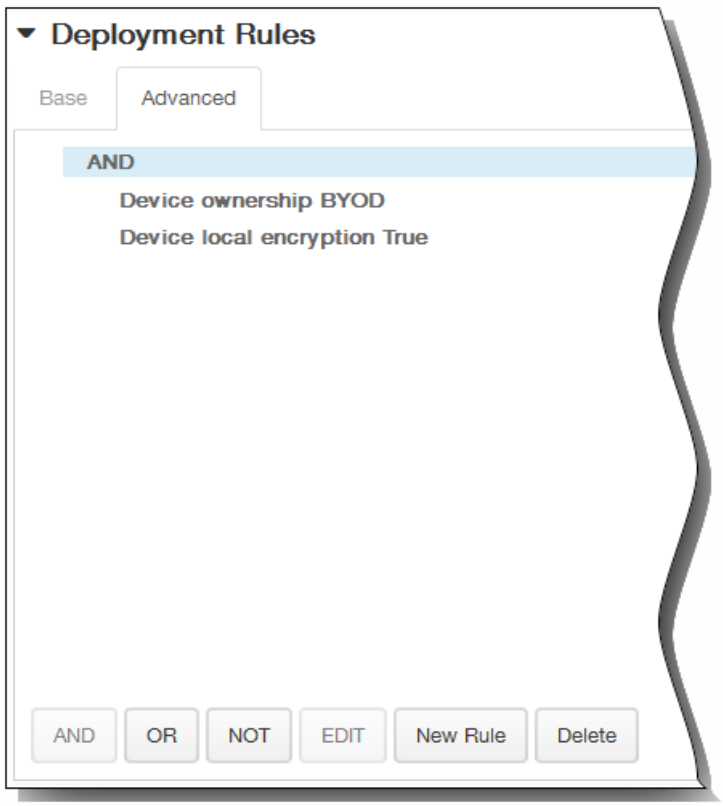
  Servicios de localización

- USB actions:

  Debugging

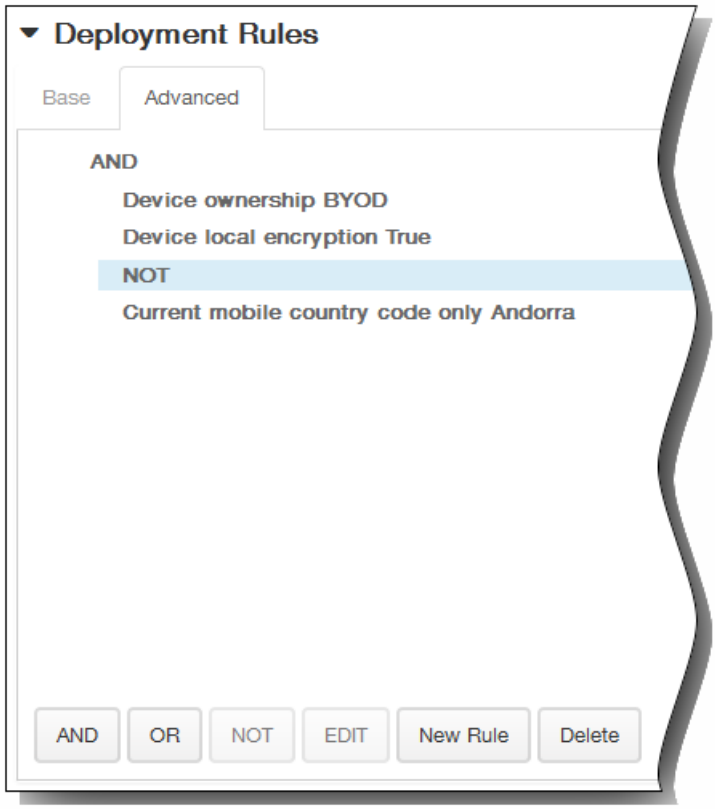
6. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

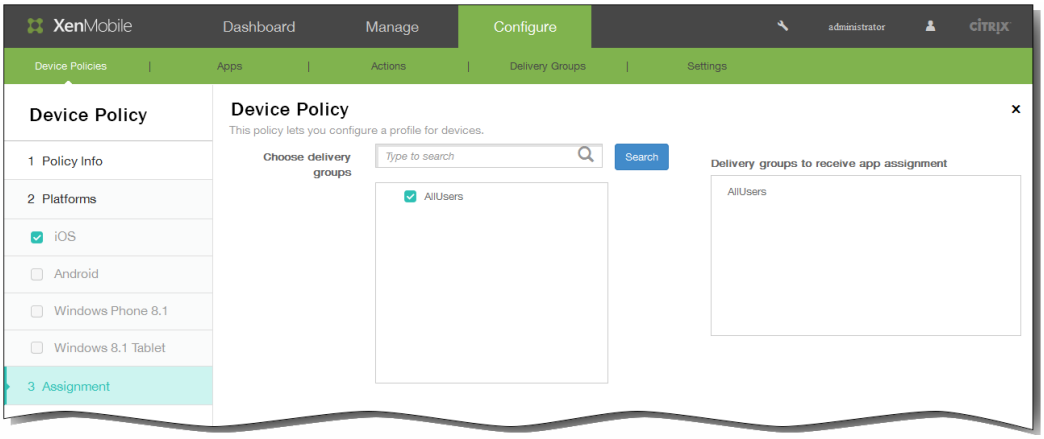


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.

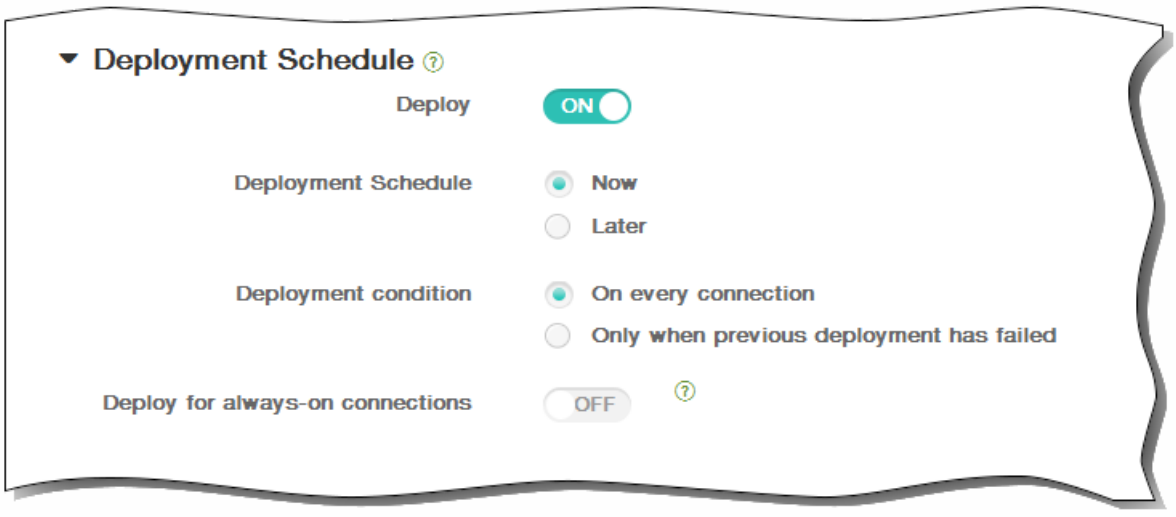


7. Cuando termine de definir la configuración de una o varias plataformas y haga clic en Next, aparecerá la página Assignment.
8. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



9. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
   1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
   2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
   3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
   4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
   5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
      Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

   Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



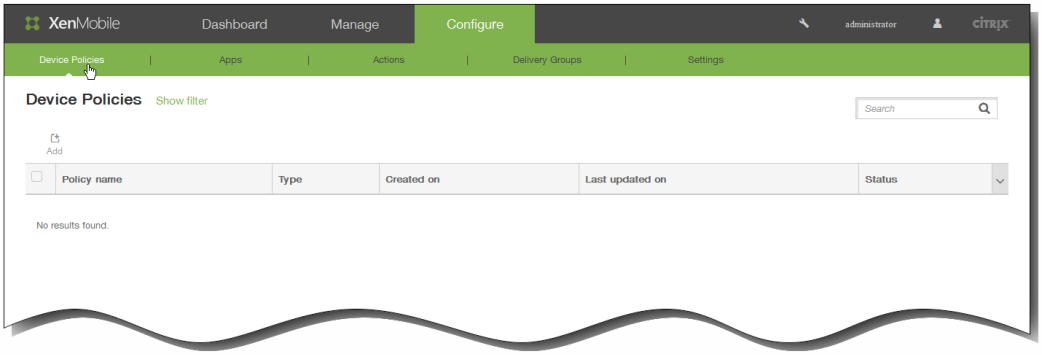
10. Haga clic en Save para guardar la directiva.

Para agregar una directiva de dispositivos con movilidad para iOS

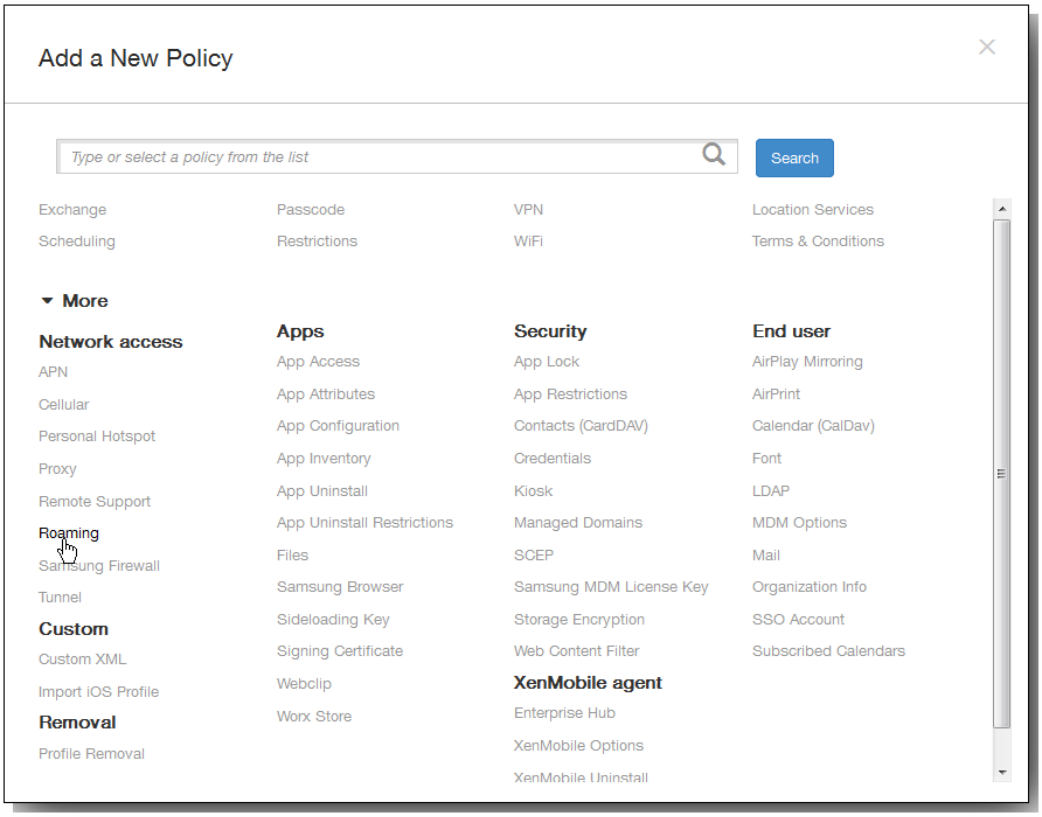
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para configurar si se permite la movilidad de voz y de datos en los dispositivos iOS de los usuarios. Si se inhabilita la movilidad de voz, la movilidad de datos se inhabilita automáticamente. Esta directiva solo está disponible para dispositivos iOS 5.0 y versiones posteriores.

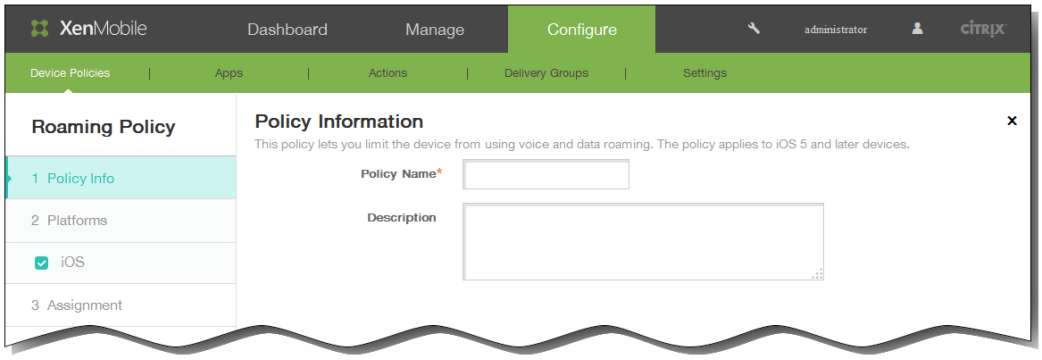
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



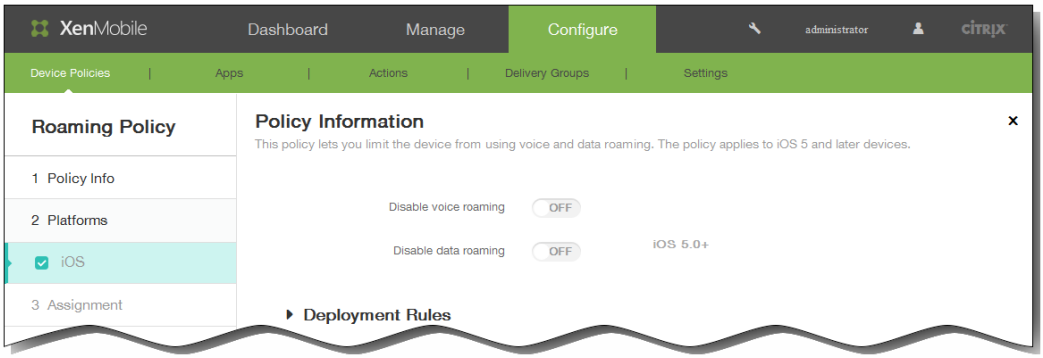
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en Network access, haga clic en Roaming. Aparecerá la página Roaming Info Policy.

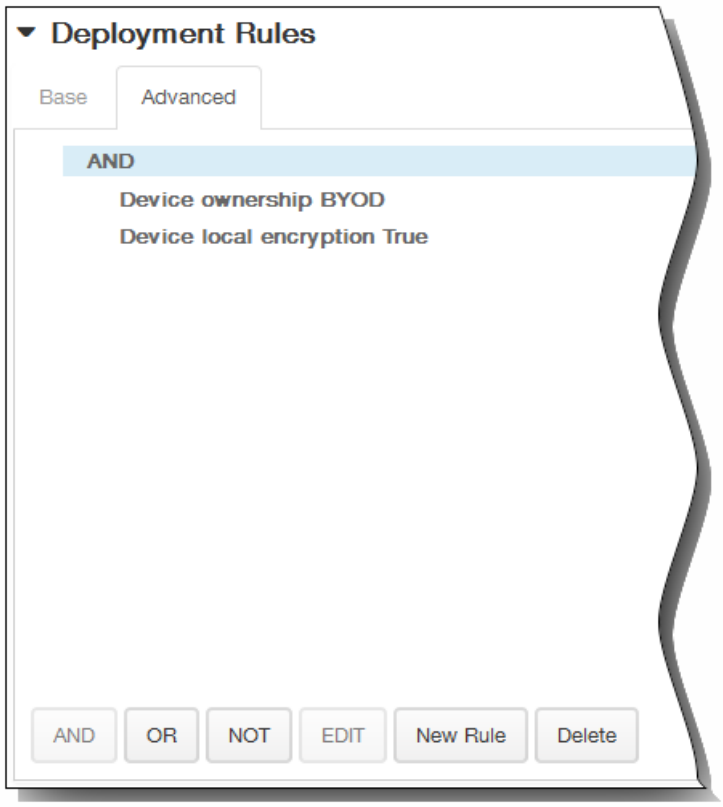


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página iOS Platform Information.



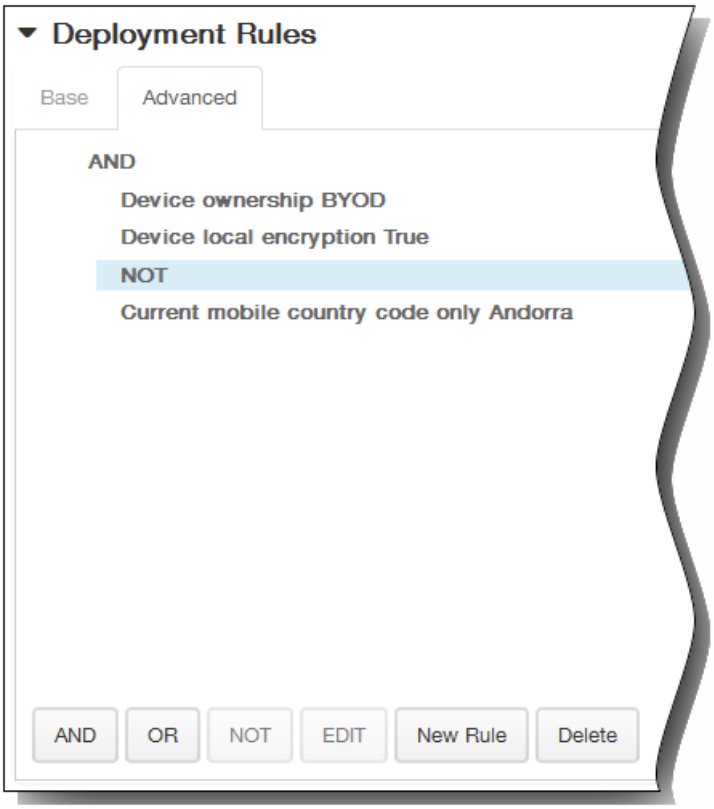
6. En la página de información iOS Platform, escriba la información siguiente:
   1. Disable voice roaming. Seleccione si inhabilitar la movilidad de voz. Si se inhabilita esta opción, la movilidad de datos se inhabilita automáticamente. El valor predeterminado es OFF, lo que permite la movilidad de voz.
   2. Disable data roaming. Seleccione si inhabilitar la movilidad de datos. Esta opción solo está disponible cuando la movilidad de voz está habilitada. El valor predeterminado es OFF, lo que permite la movilidad de datos.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

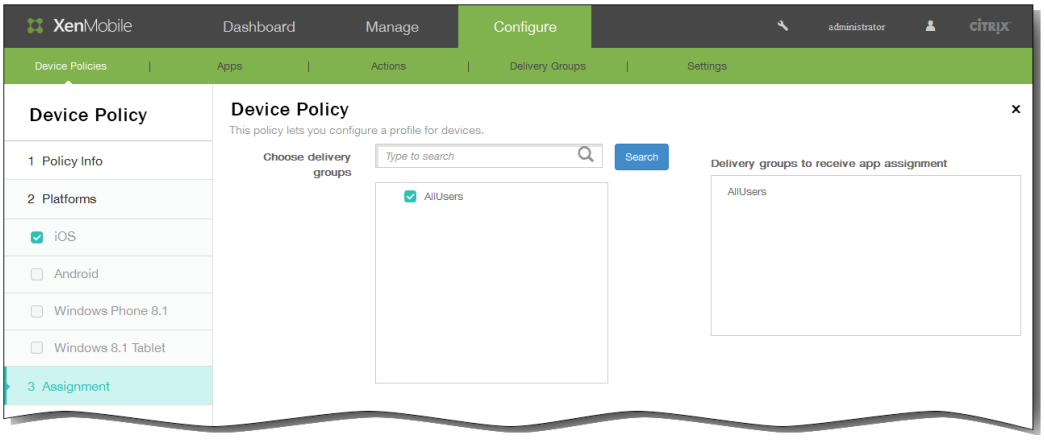


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
       En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
       En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



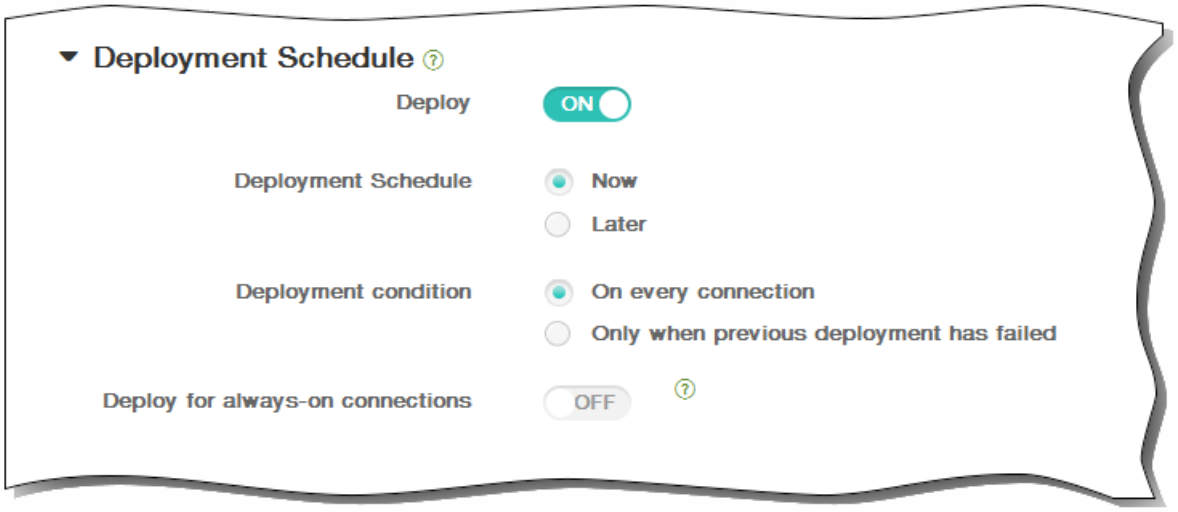
8. Haga clic en Next. Aparecerá la página de asignación Roaming Info Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



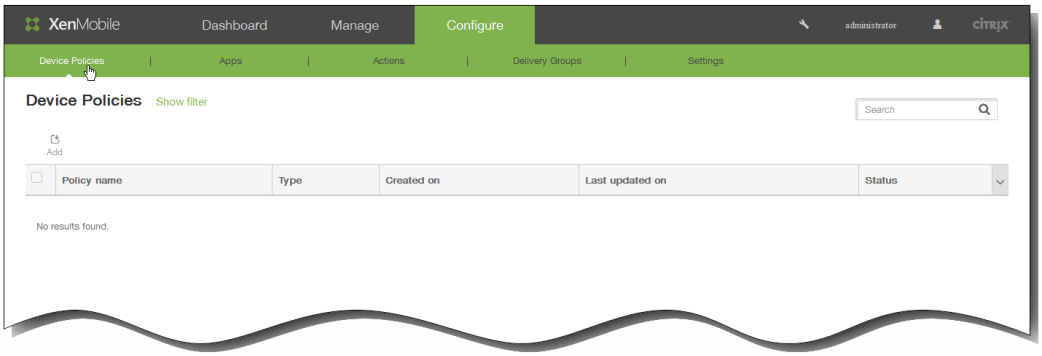
11. Haga clic en Save para guardar la directiva.

Para agregar una directiva de protocolo SCEP para dispositivos iOS

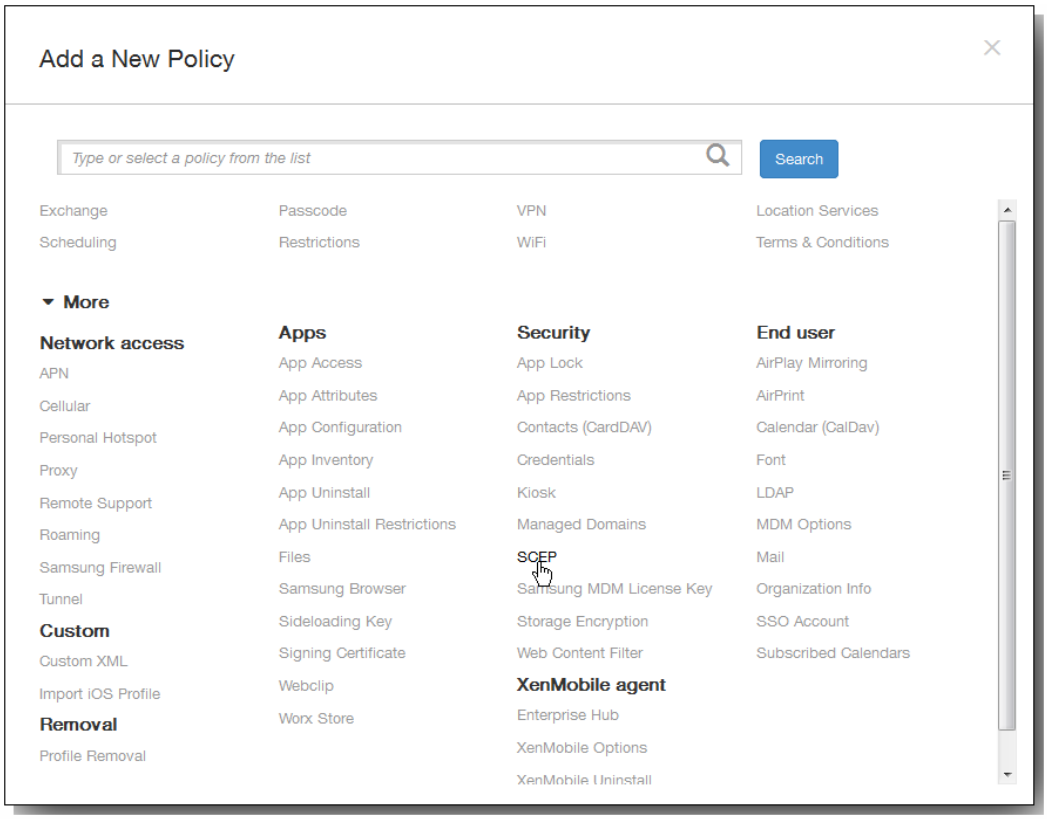
May 05, 2016

Esta directiva permite configurar dispositivos iOS para obtener un certificado mediante el Protocolo de inscripción de certificados simple (SCEP) desde un servidor SCEP externo. Si quiere entregar un certificado al dispositivo mediante el protocolo SCEP desde una infraestructura de clave pública que está conectada a XenMobile, debe crear una entidad de infraestructura de clave pública y un proveedor de PKI en modo distribuido. Para obtener más información, consulte Entidades de infraestructura PKI.

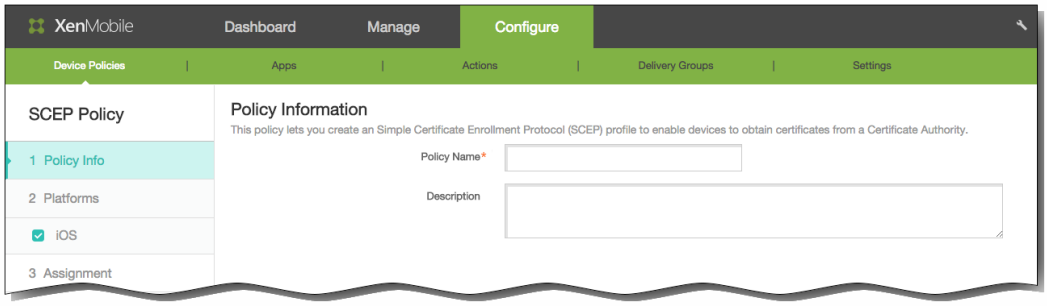
1. En la consola de XenMobile, haga clic en Configure > Device Policies.
   Aparecerá la página Device Policies.



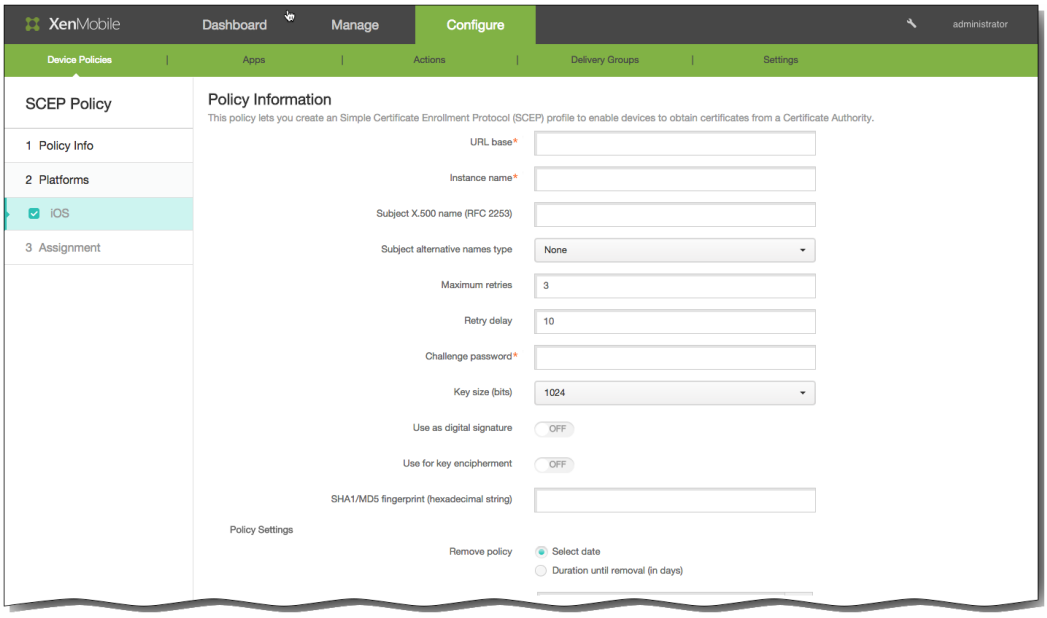
2. Haga clic en Agregar.
   Aparecerá la página Add a New Policy.



3. En la página Add a New Policy, haga clic en More y, en Security, haga clic en SCEP.
   Aparecerá la página de información SCEP Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next.
   Aparecerá la página iOS Platform Information.

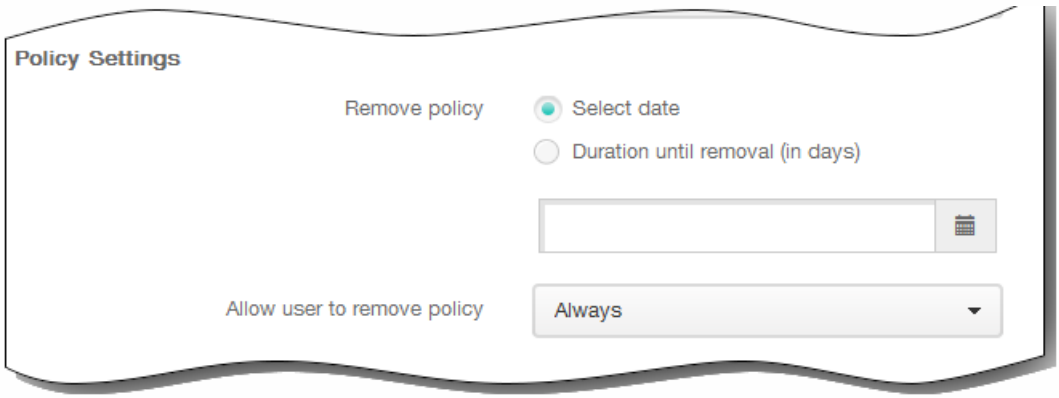


6. En la página de información iOS Platform, escriba la información siguiente:
    1. URL base. Escriba la dirección del servidor SCEP para definir dónde se enviarán las solicitudes SCEP, ya sea por HTTP o por HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que enviar la solicitud sin cifrar puede ser una opción segura. Sin embargo, si se permite volver a utilizar la contraseña de un solo uso, debe utilizar HTTPS para proteger la contraseña. Este paso es obligatorio.
    2. Instance name. Escriba cualquier cadena que reconozca el servidor SCEP. Por ejemplo, puede ser un nombre de dominio, como ejemplo.org. Si una entidad de certificación dispone de varios certificados de CA, puede usar este campo para diferenciar el dominio pertinente. Este paso es obligatorio.
    3. Subject X.500 name (RFC 2253). Escriba la representación de un nombre de X.500 representado como una matriz de identificadores OID y valores. Por ejemplo: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se podría traducir como: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. Los identificadores OID se pueden representar como números con puntos y que disponen de accesos directos para el país (C), la localidad (L), el estado (ST), la organización (O), la unidad organizativa (OU) y el nombre común (CN).
    4. Subject alternative names type. En la lista, seleccione un tipo de nombre alternativo. Si lo prefiere, la directiva de SCEP puede especificar un tipo de nombre alternativo que proporciona los valores que requiere la entidad de certificación para emitir un certificado. Puede especificar None, RFC 822 name, DNS name o URI.
    5. Maximum retries. Escriba la cantidad de reintentos permitidos cuando un usuario introduce una contraseña incorrecta. El valor predeterminado es 3.
    6. Retry delay. Escriba un intervalo de tiempo después del cual los usuarios superan la cantidad máxima de reintentos y se bloquea su acceso. El valor predeterminado es 10.
    7. Challenge password. Escriba un secreto previamente compartido. Este paso es obligatorio.
    8. Key size (bits). En la lista, haga clic en el tamaño de la clave en bits, ya sea 1024 o 2048. El valor predeterminado es 1024.
    9. Use as digital signature. Indique esta opción si quiere que el certificado se use como una firma digital. Si alguien usa el certificado para comprobar una firma digital (por ejemplo, para averiguar si el certificado ha sido emitido por una entidad de certificación), el servidor SCEP podría comprobar si ese certificado se puede usar de esa forma antes de usar la clave pública para descifrar el hash.
    10. Use for key encipherment. Indique esta opción si quiere que el certificado se use para el cifrado de clave. Si un servidor utiliza la clave pública en un certificado proporcionado por un cliente para comprobar que una parte de los datos se ha

cifrado mediante la clave privada, el servidor puede comprobar primero si el certificado se puede usar para el cifrado de clave. Si no es así, la operación no se puede realizar.

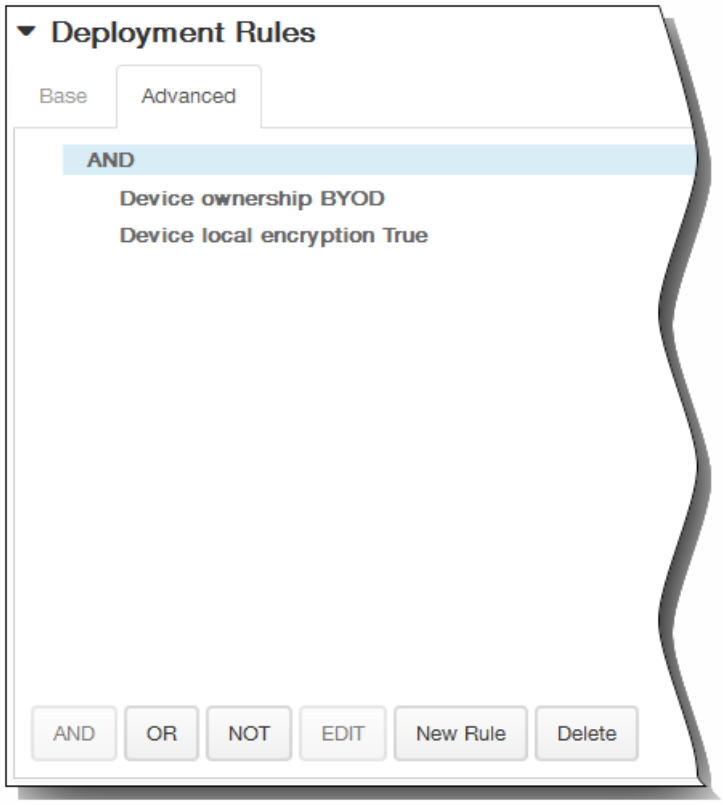
11. SHA1/MD5 fingerprint (hexadecimal string). Si la entidad de certificación utiliza HTTP, utilice este campo para la huella digital del certificado de CA; el dispositivo se vale de él para confirmar la autenticidad de la respuesta de la entidad durante la inscripción. Puede escribir una huella digital MD5 o SHA-1. También puede seleccionar un certificado para importar su firma.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



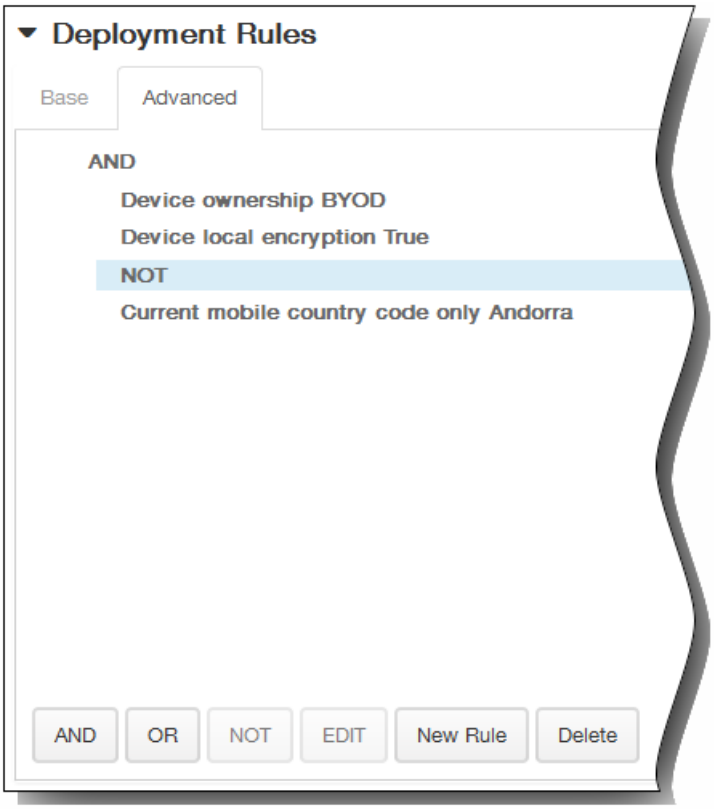
11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

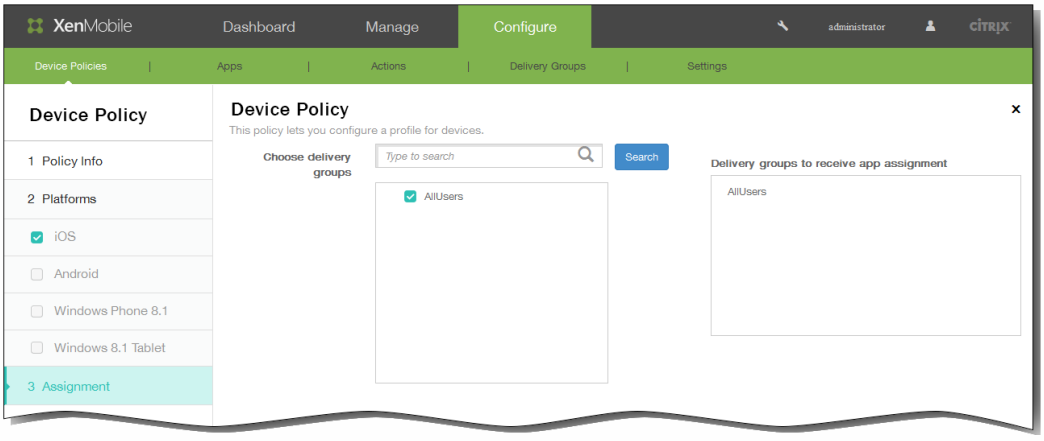


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



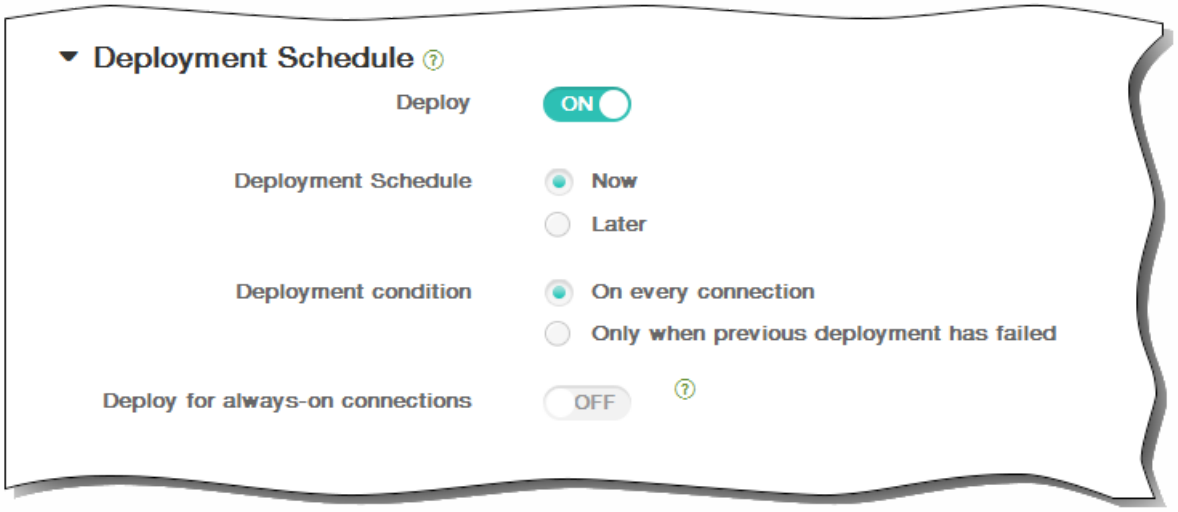
12. Haga clic en Next. Aparecerá la página de asignación SCEP Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



15. Haga clic en Save para guardar la directiva.

Directivas de claves de licencia para la administración de dispositivos móviles Samsung

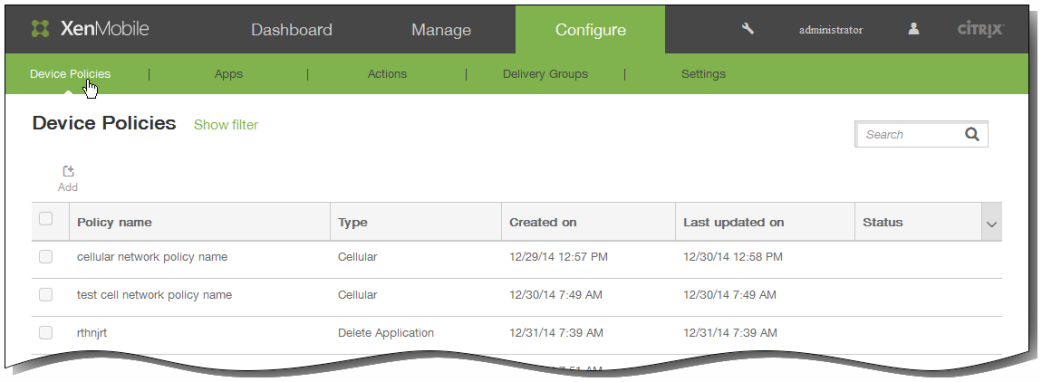
May 05, 2016

XenMobile respalda y extiende directivas de Samsung for Enterprise (SAFE) y Samsung KNOX. SAFE es una gama de soluciones que ofrece mejoras de seguridad y funciones para negocios mediante la integración con las soluciones de administración de dispositivos móviles. SAMSUNG KNOX es una solución incluida en el programa SAFE, que ofrece una plataforma Android más segura para la empresa.

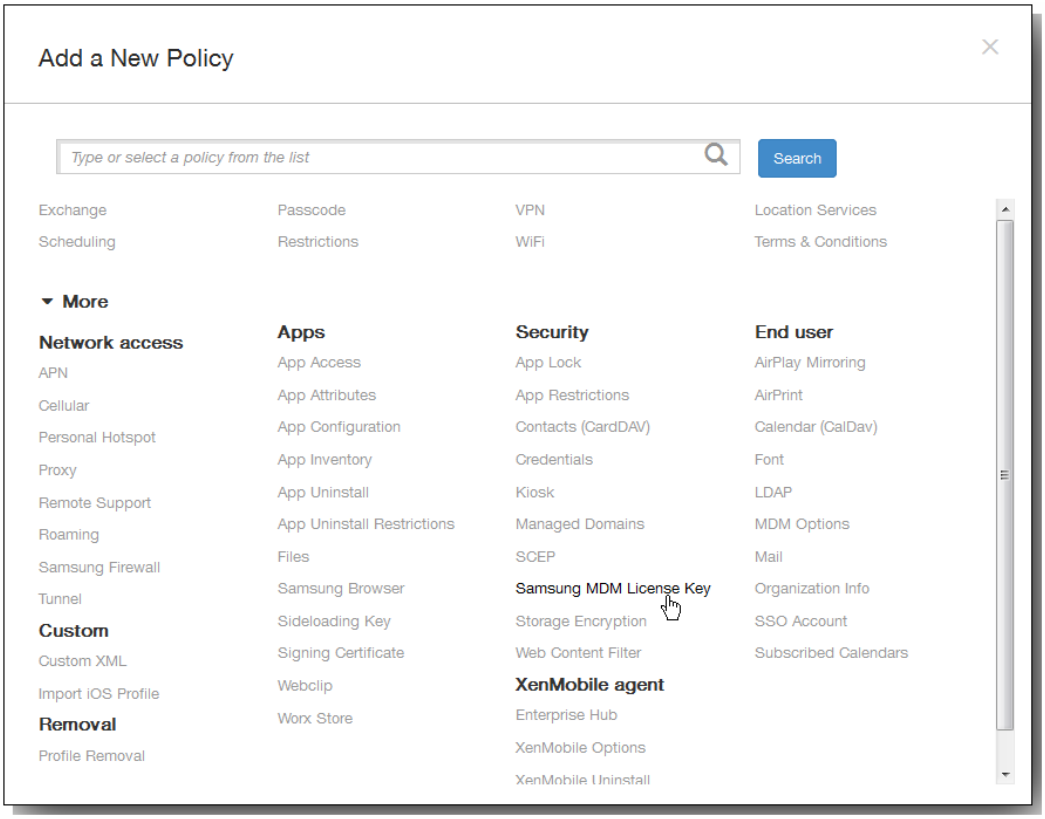
Debe habilitar las API de la solución SAFE por medio de la implementación de la clave integrada de Samsung Enterprise License Management (ELM) a un dispositivo antes de implementar directivas y restricciones de la solución SAFE. Para habilitar la API de Samsung KNOX, además de implementar la clave ELM de Samsung, también deberá adquirir una licencia de Samsung KNOX mediante el sistema Samsung KNOX License Management System (KLMS). Samsung KLMS aprovisiona licencias válidas a las soluciones de administración de dispositivos móviles para permitirles activar las API de Samsung KNOX en los dispositivos móviles. Estas licencias se deben obtener de Samsung; no las proporciona Citrix.

Debe implementar Worx Home junto con la clave de Samsung ELM para habilitar las API de Samsung KNOX y SAFE. Puede comprobar que las API de SAFE están habilitadas si comprueba las propiedades del dispositivo. Cuando la clave de Samsung ELM está implementada, el parámetro "Samsung MDM API available" tiene el valor True.

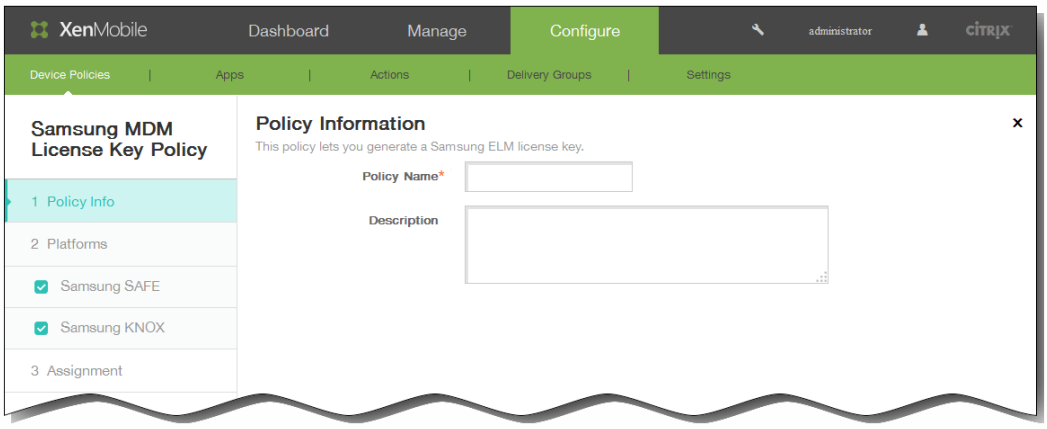
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



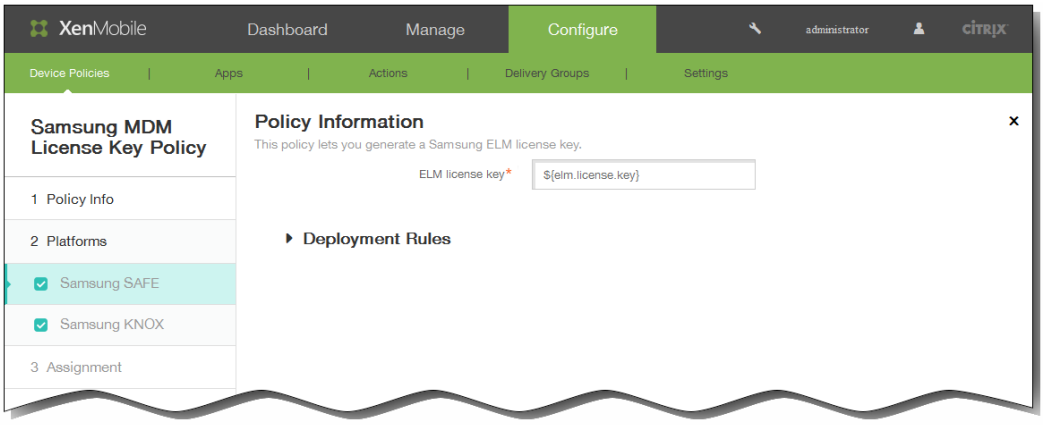
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.



3. Haga clic en More y, a continuación, en Security, haga clic en Samsung MDM Licence Key. Aparecerá la página de información Samsung MDM Licence Key Policy.

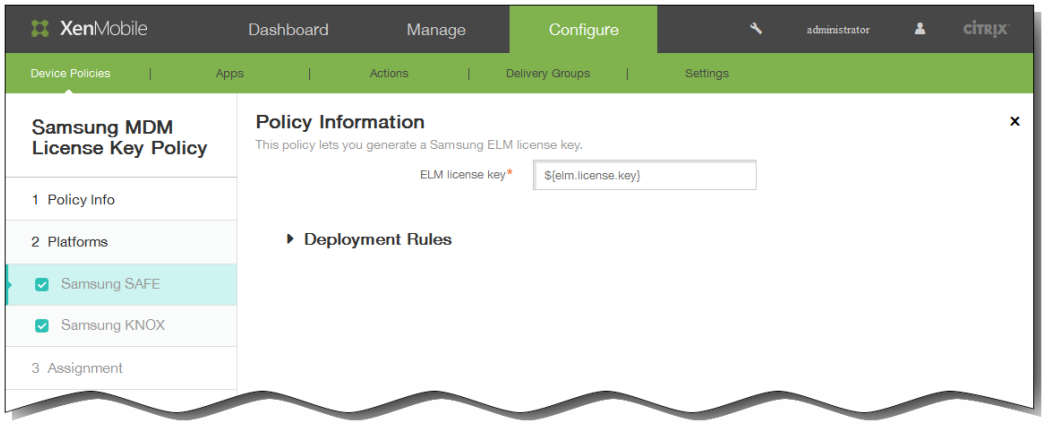


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, ambas plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de Samsung SAFE.

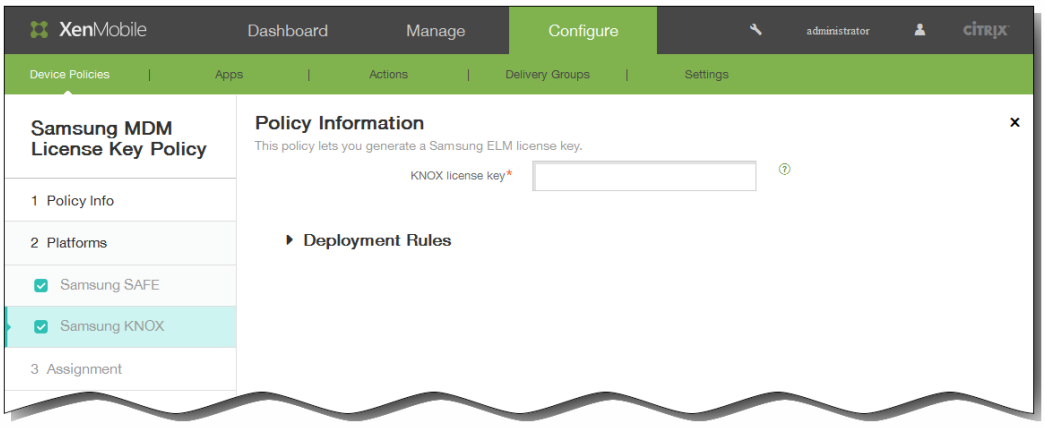


6. En Platforms, seleccione las plataformas de Samsung para las que quiera configurar esta directiva. Borre cualquier otra plataforma seleccionada que no quiera incluir en esta directiva.

   - Si ha elegido Samsung SAFE, en ELM license key, escriba la macro ${elm.license.key} para generar la clave de licencia ELM. El campo ya debería contener la macro:

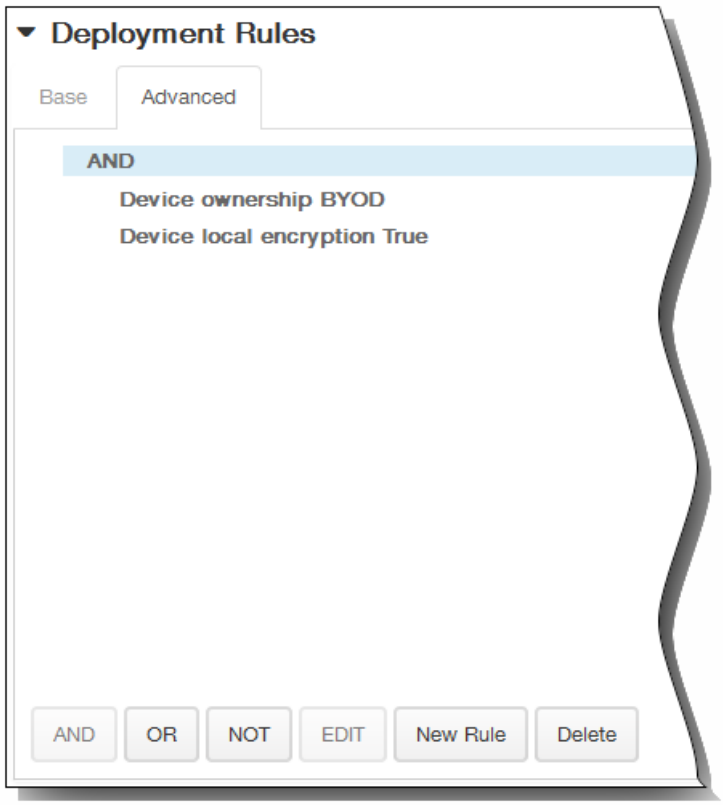


   - Si ha elegido Samsung KNOX, en KNOX license key, escriba la clave de licencia de KNOX de 25 dígitos:



7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

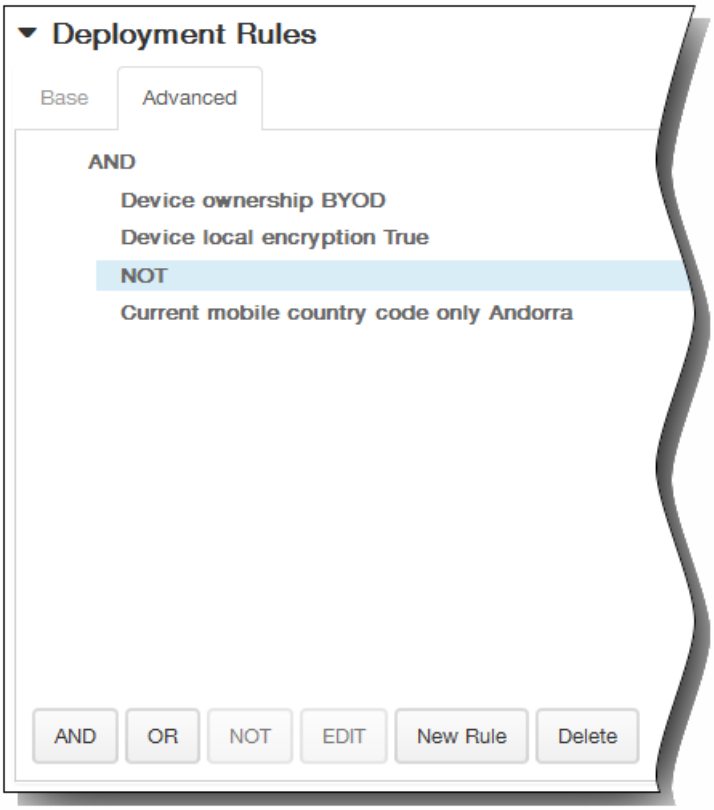
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



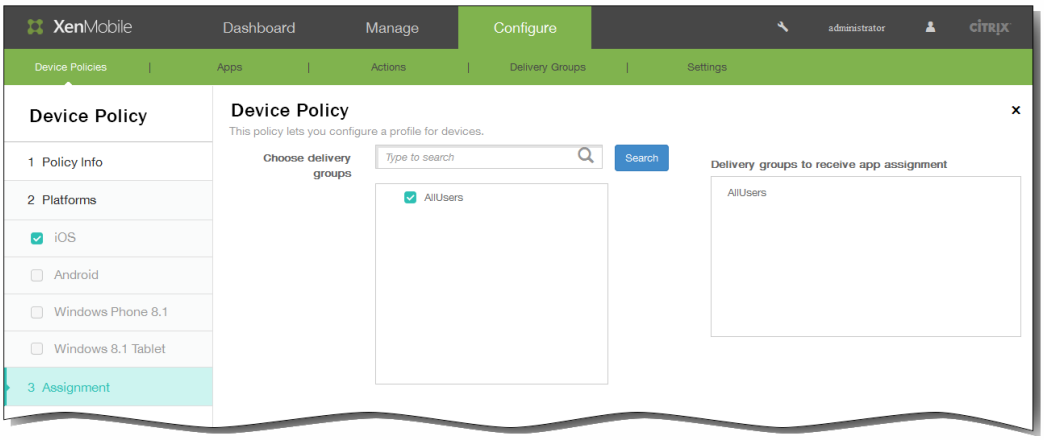
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



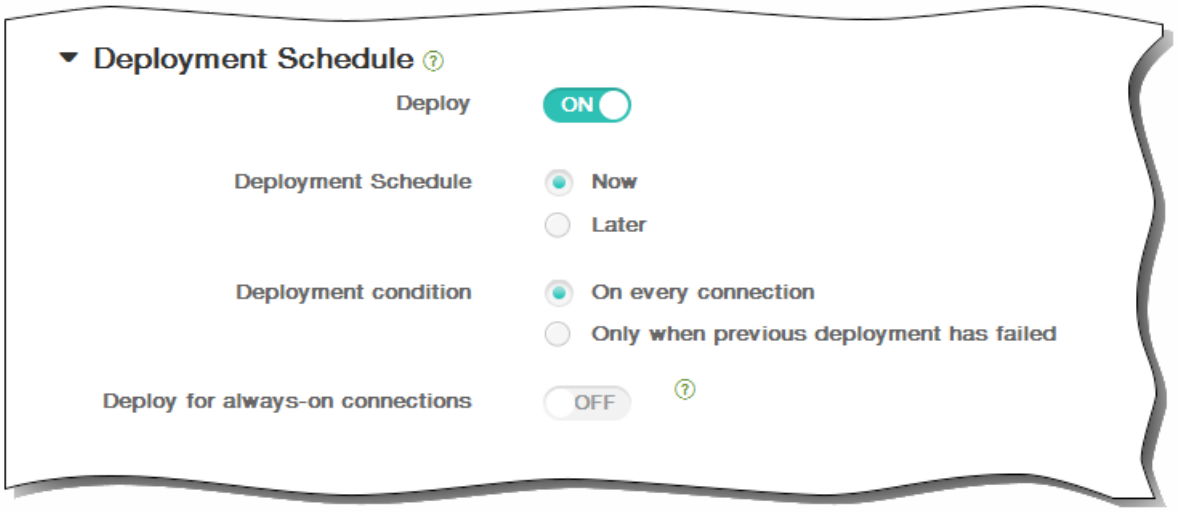
8. Haga clic en Next. Aparecerá la página Samsung MDM License Key Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

Directivas de cifrado de almacenamiento

May 05, 2016

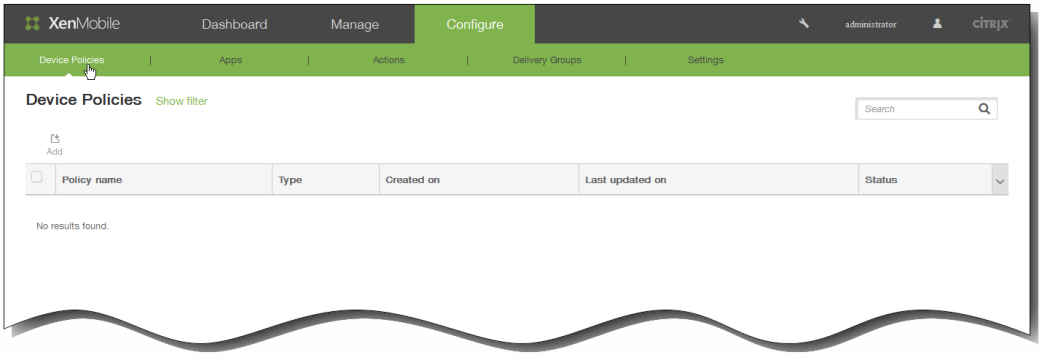
En XenMobile, puede crear directivas de cifrado de almacenamiento para cifrar almacenamientos internos y externos. Asimismo, según el dispositivo, esta directiva puede servir para evitar que los usuarios utilicen tarjetas de almacenamiento en sus dispositivos.

Puede crear directivas para dispositivos Android Sony y Samsung SAFE, además de tabletas Windows 8.1. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en los siguientes pasos.

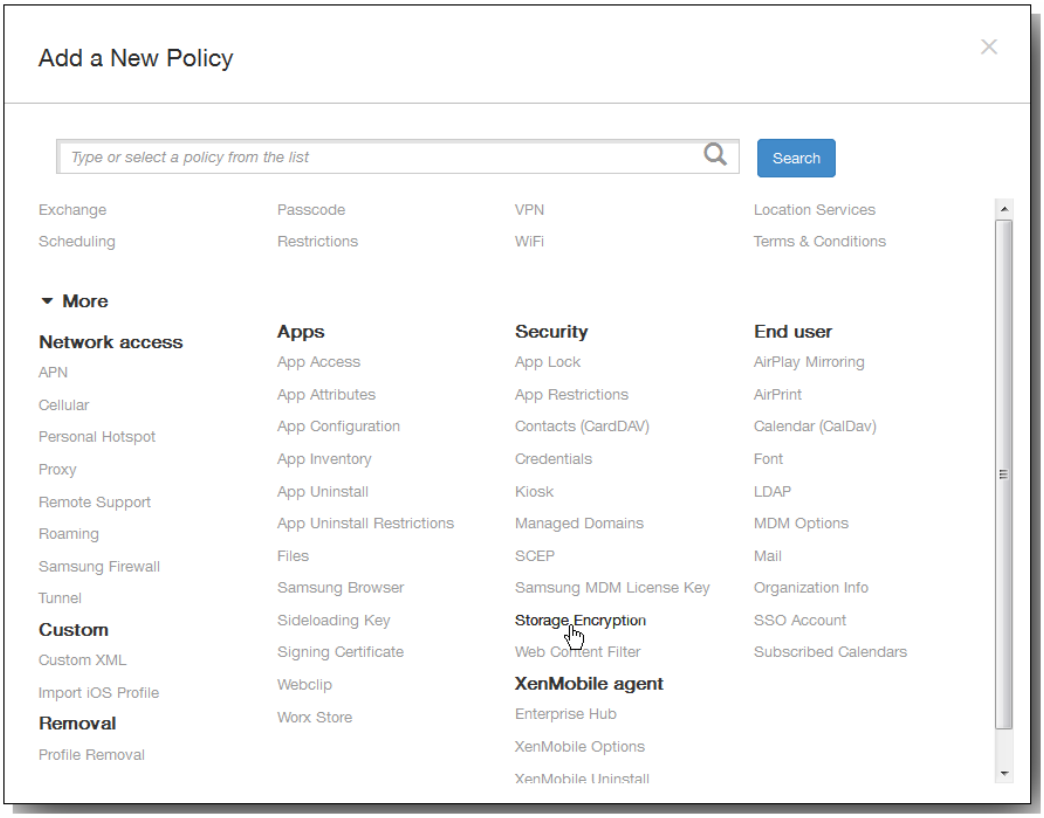
Nota: Para dispositivos Samsung SAFE, antes de configurar esta directiva, compruebe que se cumplen los siguientes requisitos:

- Debe establecer la opción de bloqueo de pantalla en los dispositivos de los usuarios.
- Los dispositivos de los usuarios deben estar conectados y cargados al 80 %.
- El dispositivo debe requerir una contraseña que contenga números y letras o símbolos.

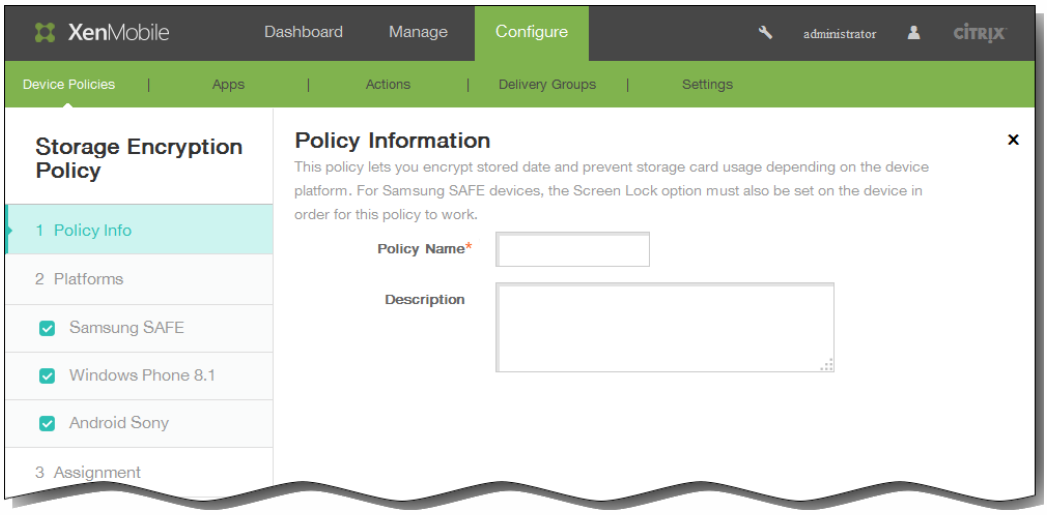
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.

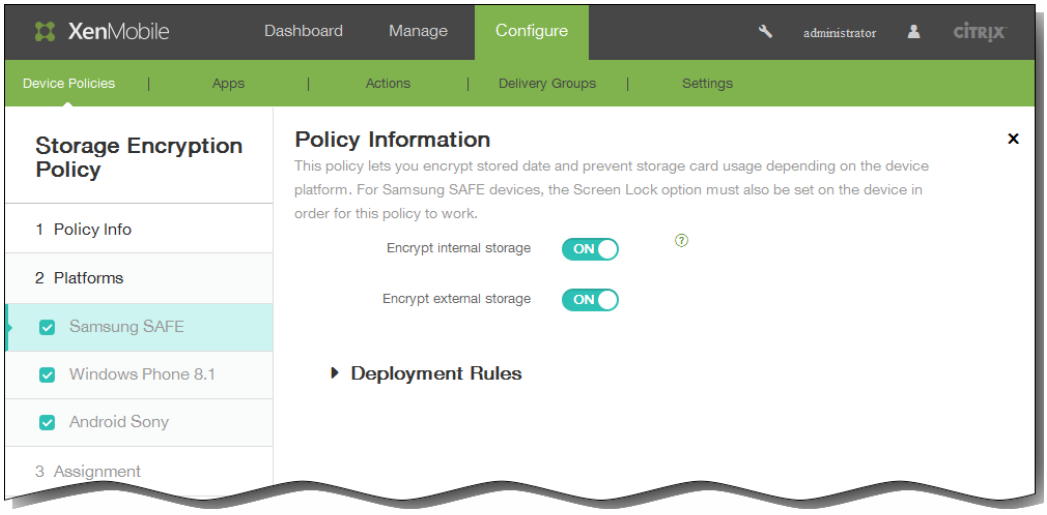


3. Haga clic en More y, a continuación, en Security, haga clic en Storage Encryption. Aparecerá la página de información Storage Encryption Policy.

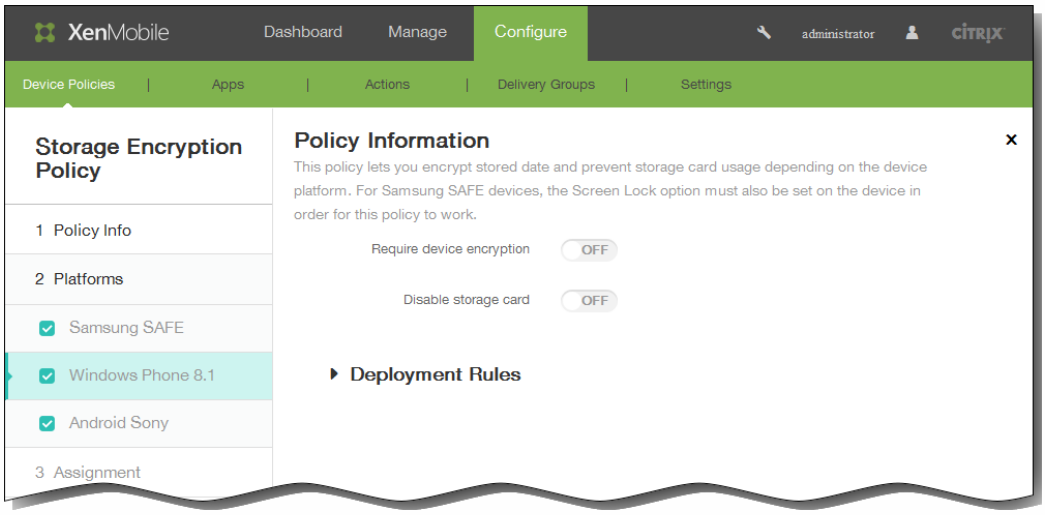


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, todas las plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de Samsung SAFE.

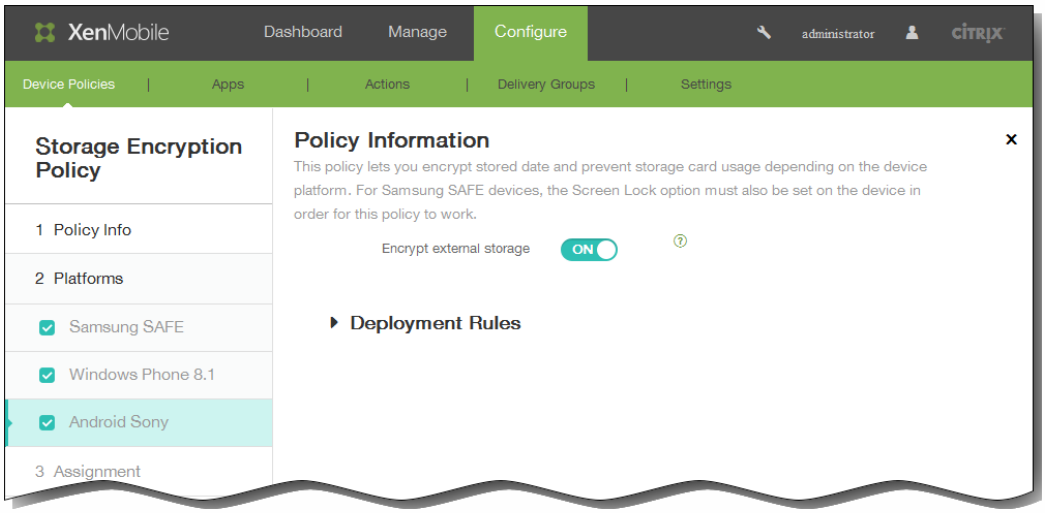
6. En Platforms, seleccione las plataformas para las que quiera configurar esta directiva. Si esta es la única plataforma que está configurando, desmarque todas las demás plataformas seleccionadas.
   - Si selecciona Samsung SAFE:
     - Encrypt internal storage. Seleccione si cifrar el almacenamiento interno en los dispositivos de los usuarios. El almacenamiento interno incluye el almacenamiento interno y la memoria del dispositivo. El valor predeterminado es ON.
     - Encrypt external storage. Seleccione si cifrar el almacenamiento externo en los dispositivos de los usuarios. El valor predeterminado es ON.



   - Si selecciona Windows Phone 8.1:
     - Require device encryption. Seleccione esta opción para cifrar los dispositivos de los usuarios. El valor predeterminado es OFF.
     - Disable storage card. Seleccione esta opción para evitar que los usuarios utilicen tarjetas de almacenamiento en sus dispositivos. El valor predeterminado es OFF.

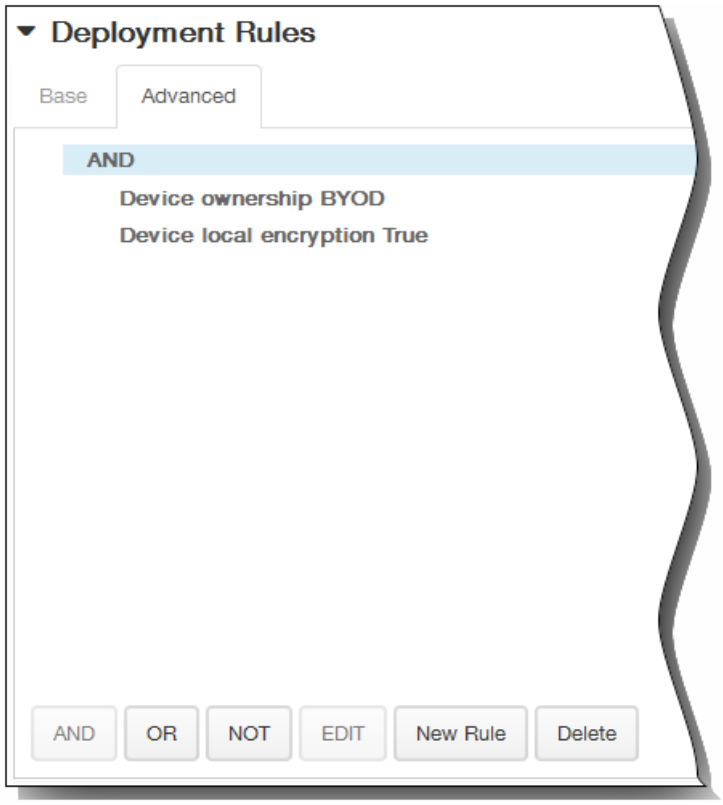


   - Si selecciona Android Sony, en Encrypt external storage, seleccione si cifrar el almacenamiento externo en los dispositivos de los usuarios. El dispositivo debe requerir una contraseña que contenga números y letras o símbolos. El valor predeterminado es ON.



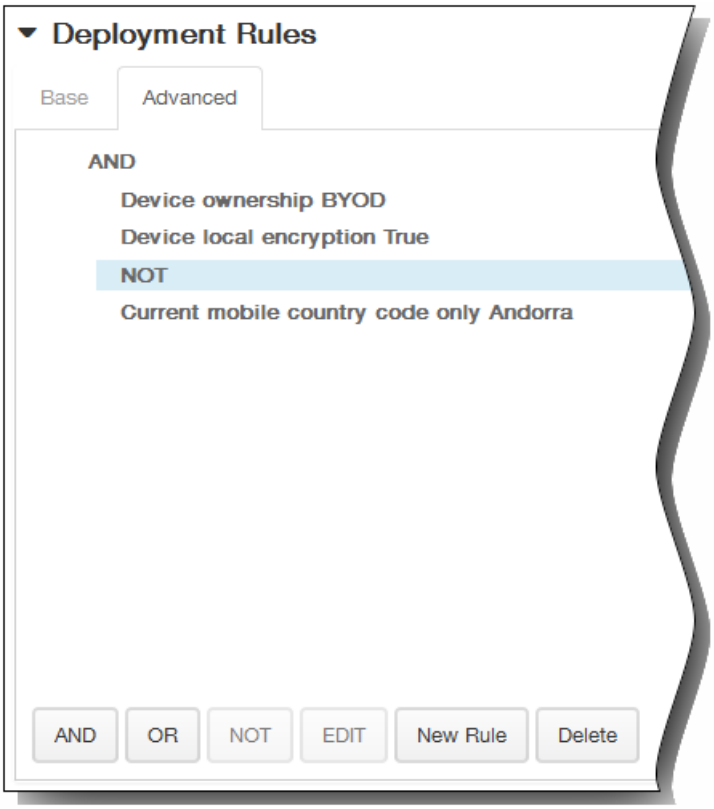
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

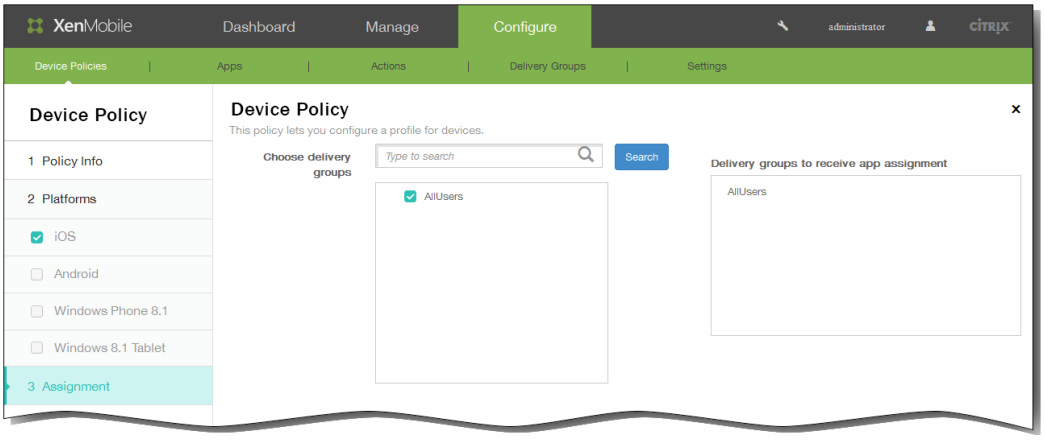


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



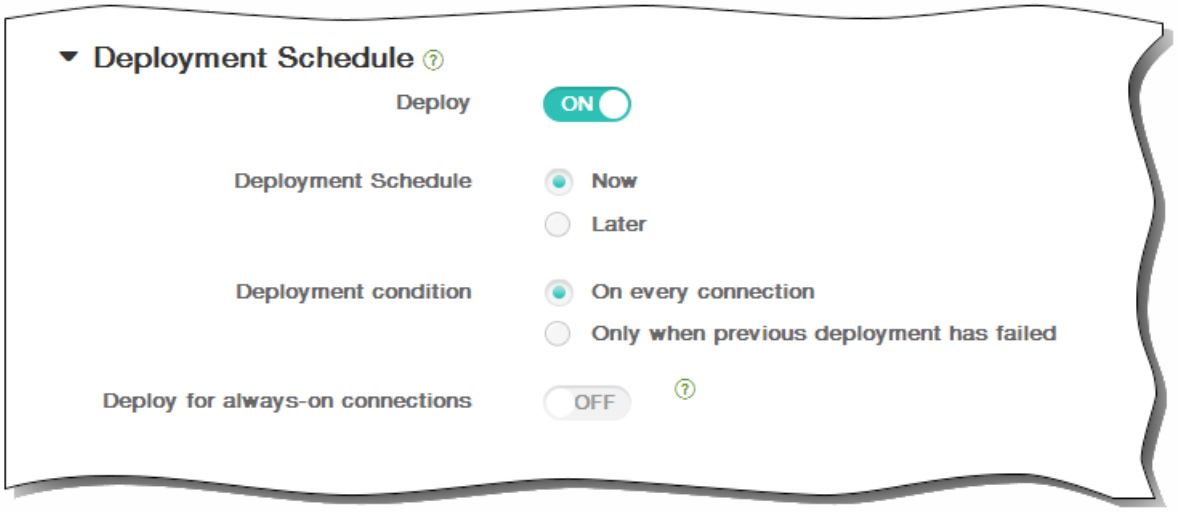
8. Haga clic en Next. Aparecerá la página de asignación Storage Encryption Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



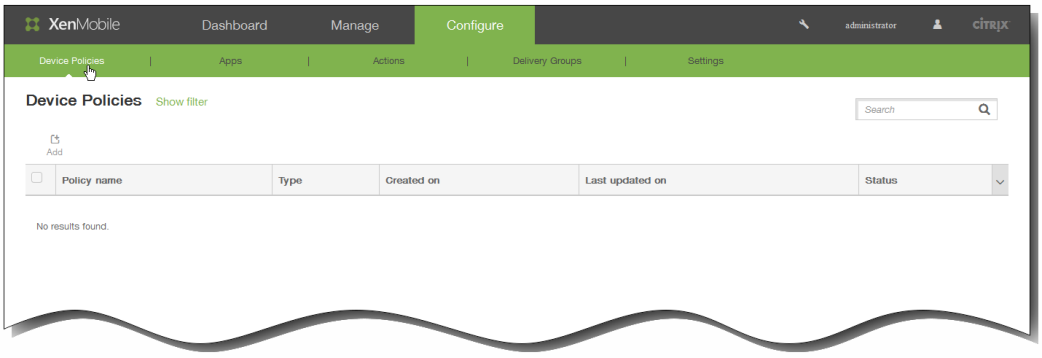
11. Haga clic en Save para guardar la directiva.

Para agregar una directiva de dispositivo sobre contenidos Web para iOS

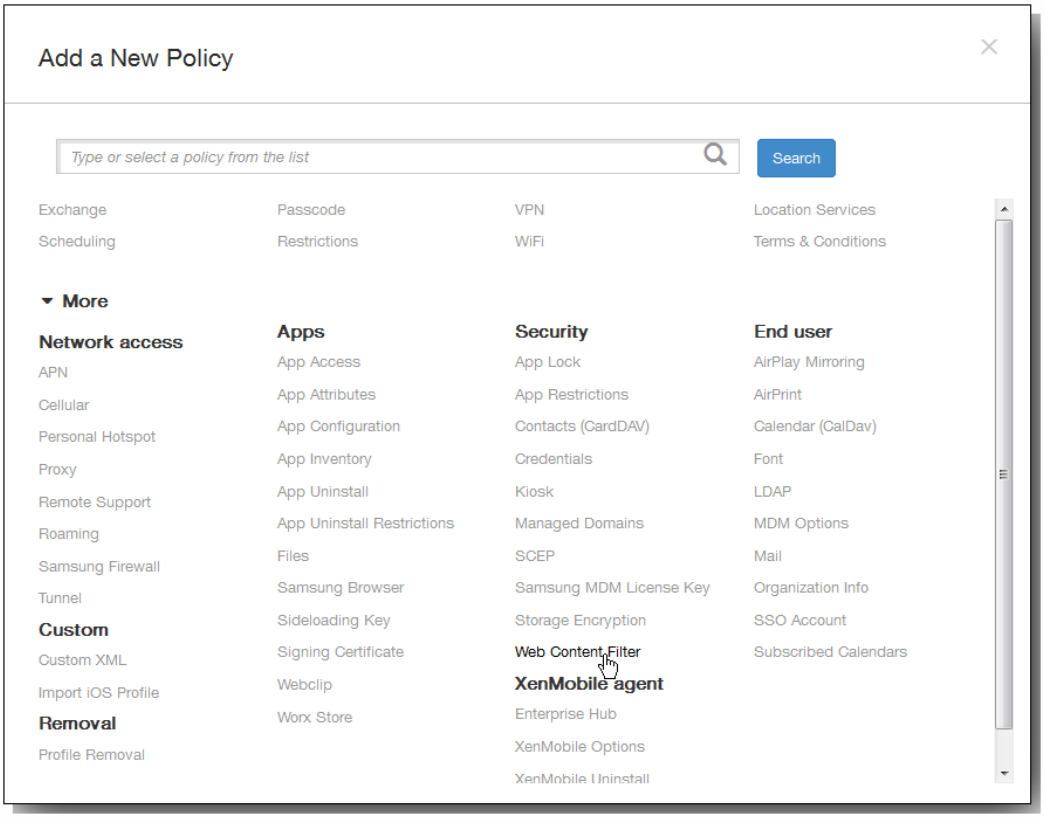
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para filtrar el contenido Web en dispositivos iOS. Para ello, deberá utilizar la función de filtrado automático de Apple en combinación con sitios específicos que usted agregue a listas de sitios permitidos y prohibidos. Esta directiva solo está disponible para dispositivos iOS 7.0 y versiones posteriores en modo supervisado. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

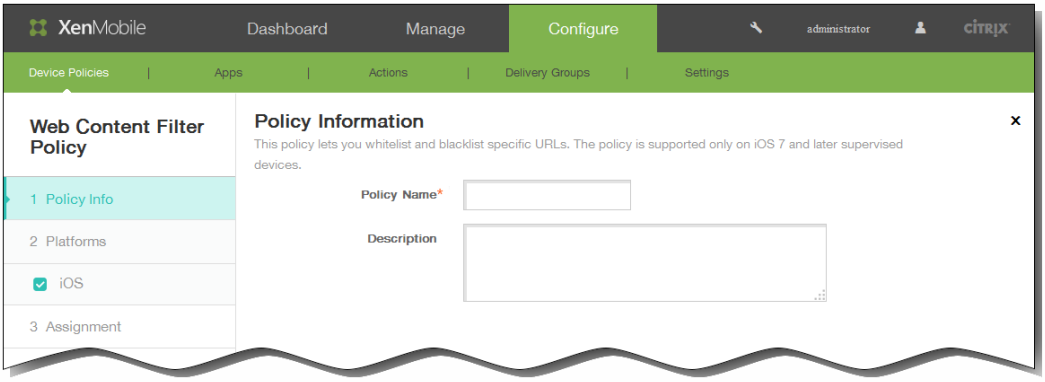
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



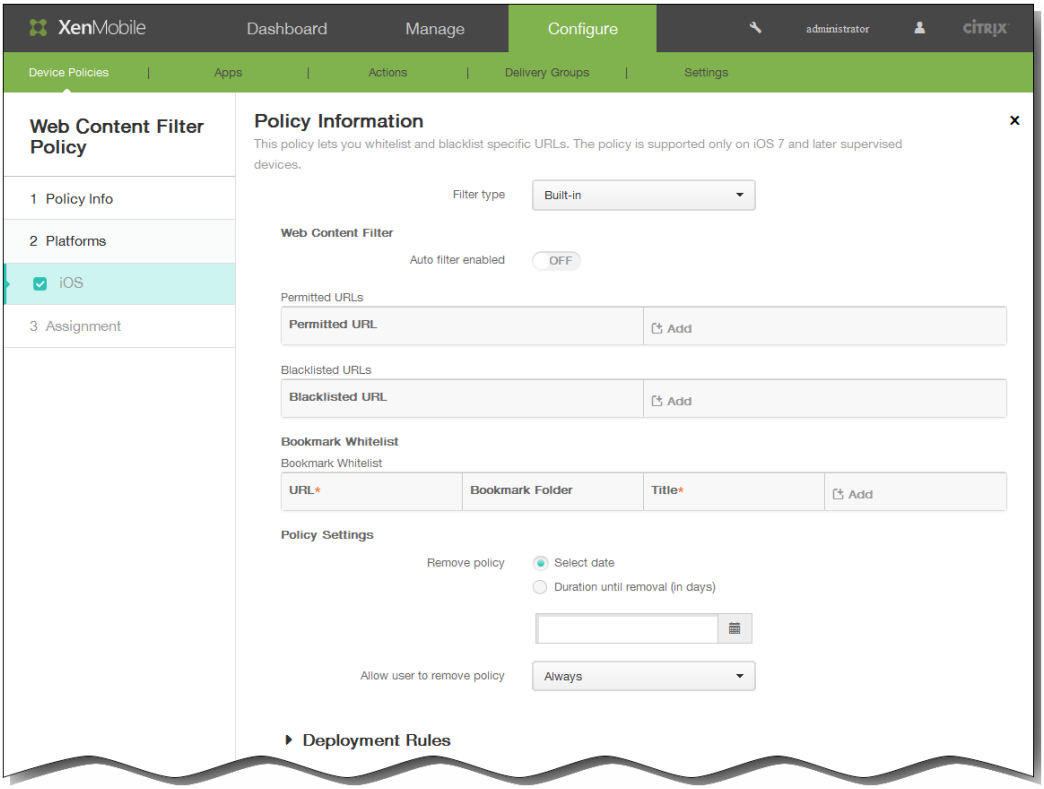
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, a continuación, en el apartado Security, haga clic en Web Content Filter. Aparecerá la página Web Content Filter Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información iOS Platform.



6. En la página iOS Platform Information, en la lista Filter type, realice una de las siguientes acciones y siga los procedimientos posteriores que se indican en este apartado según la opción que elija:
   - Deje el tipo de filtro predeterminado Built-in.
   - Haga clic en Plug-in para configurar el tipo de filtro Plug-in.

   Para configurar el tipo de filtro Built-in

   1. Auto filter enabled. Seleccione si utilizar la función de filtro automático de Apple para analizar sitios Web en busca de contenido inapropiado. El valor predeterminado es OFF.
   2. Permitted URLs. Esta lista se omite si la opción Auto filter enabled está establecida en OFF. Si la opción Auto filter enabled está establecida en ON, los elementos de esta lista son siempre accesibles, independientemente de si el filtro automático permite el acceso.
      Haga clic en Add y, a continuación, realice lo siguiente para agregar sitios Web a la lista de sitios permitidos:

      1. Escriba la URL del sitio Web permitido. Debe agregar http:// o https:// antes de la dirección Web.
      2. Haga clic en Save para guardar el sitio Web en la lista de sitios permitidos, o bien haga clic en Cancel para cancelar la operación.
      3. Repita los pasos de i. y ii. para cada sitio Web que quiera agregar a la lista de sitios permitidos.
   3. Blacklisted URLs. Los elementos de esta lista están siempre bloqueados.
      Haga clic en Add y, a continuación, realice lo siguiente para agregar sitios Web a la lista de sitios prohibidos:

      1. Escriba la URL del sitio Web que quiere bloquear. Debe agregar http:// o https:// antes de la dirección Web.
      2. Haga clic en Save para guardar el sitio Web en la lista de sitios prohibidos, o bien haga clic en Cancel para cancelar la operación.
      3. Repita los pasos de i. y ii. para cada sitio Web que quiera agregar a la lista de sitios prohibidos.
   4. Bookmark whitelist. Los elementos de esta lista son los únicos sitios a los que pueden acceder los usuarios.
      Haga clic en Add y, a continuación, realice lo siguiente para agregar sitios Web a los marcadores:

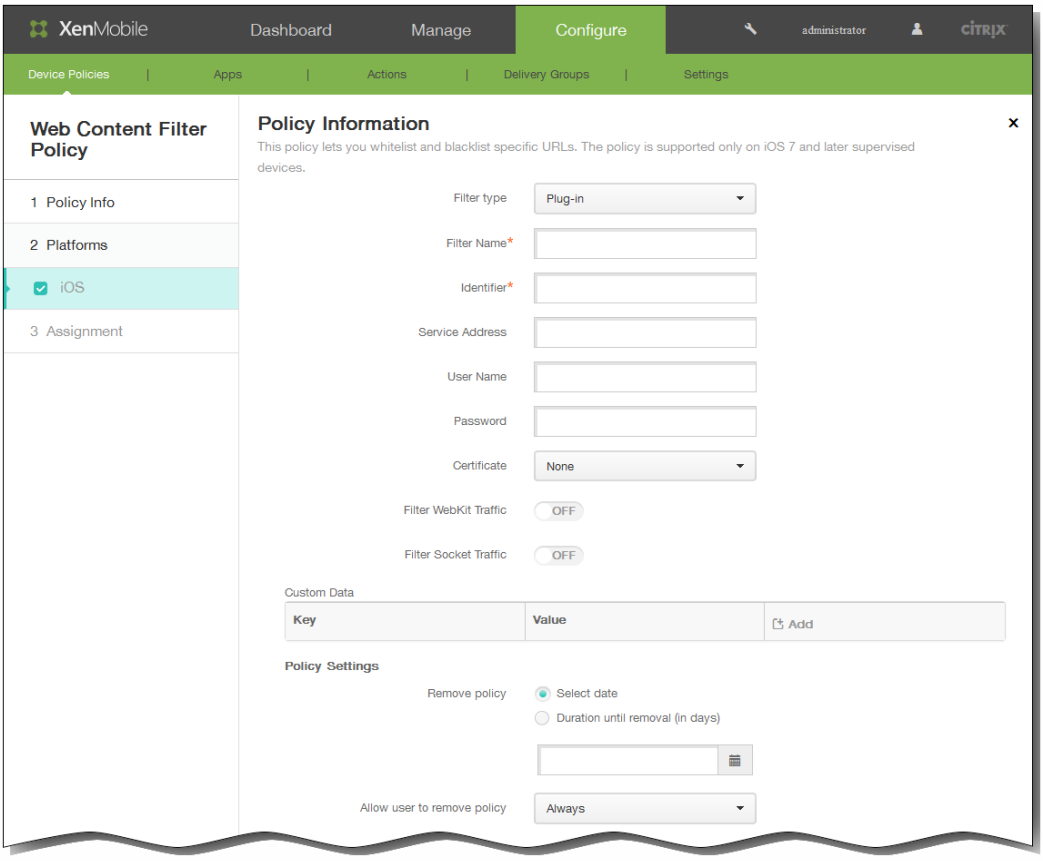
1. URL. Escriba la URL del sitio Web que se va a incluir como marcador. Debe agregar http:// o https:// antes de la dirección Web. Este campo es obligatorio.
2. Bookmark folder. Escriba un nombre opcional para la carpeta de marcadores. Si este campo se deja en blanco, el marcador se agrega al directorio predeterminado de marcadores.
3. Title. Escriba un título descriptivo para el sitio Web. Por ejemplo, introduzca "Google" para la dirección URL http://google.com.
4. Haga clic en Save para guardar el sitio Web en la lista de sitios prohibidos, o bien haga clic en Cancel para cancelar la operación.
5. Repita los pasos de i. a iv. para cada sitio Web que quiera agregar a marcadores.

Nota: Para eliminar un sitio Web existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

Para modificar un sitio Web existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

5. Consulte el paso 7 para finalizar la configuración del filtro Built-in.

Para configurar el tipo de filtro Plug-in



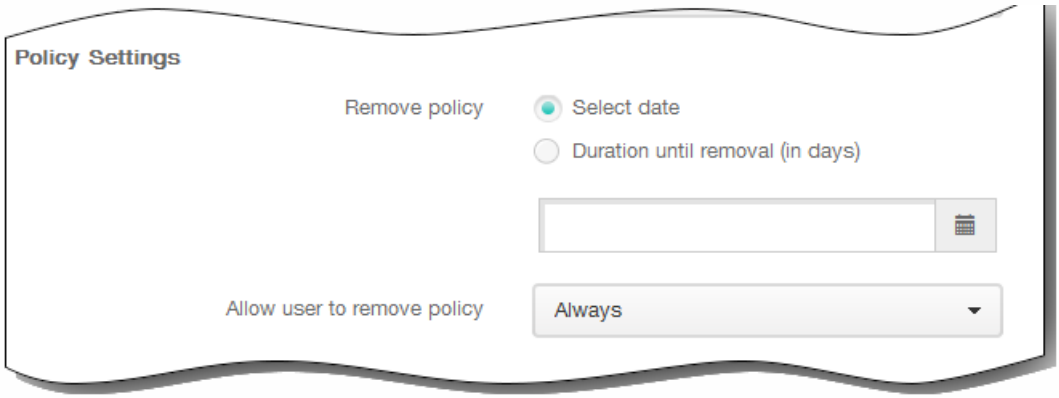
1. Filter name. Escriba un nombre único para el filtro.
2. Identifier. Escriba el ID de paquete del plugin que proporciona el servicio de filtrado.
3. Service address. Escriba una dirección de servidor opcional. Los formatos válidos son la dirección IP, el nombre de host o la dirección URL.

4. User name. Escriba un nombre de usuario opcional para el servicio.
5. Password. Escriba una contraseña opcional para el servicio.
6. Certificate. En la lista, haga clic en el certificado de identidad opcional que se va a usar para autenticar al usuario en el servicio. El valor predeterminado es None.
7. Filter WebKit traffic. Seleccione si se debe filtrar el tráfico WebKit.
8. Filter Socket traffic. Seleccione si filtrar el tráfico de sockets.
9. Custom Data. Haga clic en Add y, a continuación, realice lo siguiente para agregar datos personalizados al filtro de contenidos Web:
    1. Key. Especifique la clave personalizada.
    2. Value. Escriba un valor para la clave personalizada.
    3. Haga clic en Save para guardar la clave personalizada, o bien haga clic en Cancel para cancelar la operación.
    4. Repita los pasos de i. a iii. para cada clave personalizada que quiera agregar.

    Nota: Para eliminar una clave existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

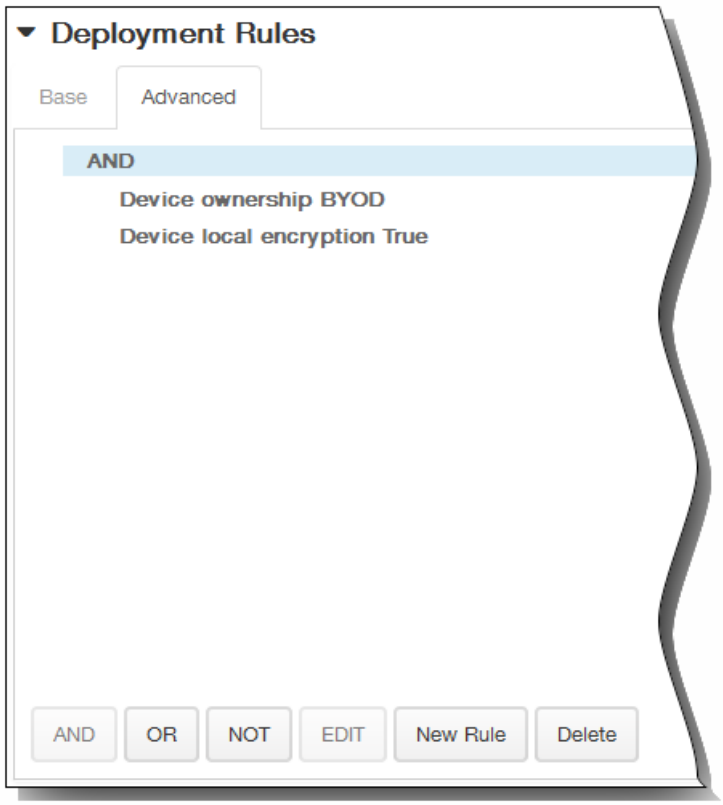
    Para modificar una clave existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

7. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
8. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
9. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
10. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.



11. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

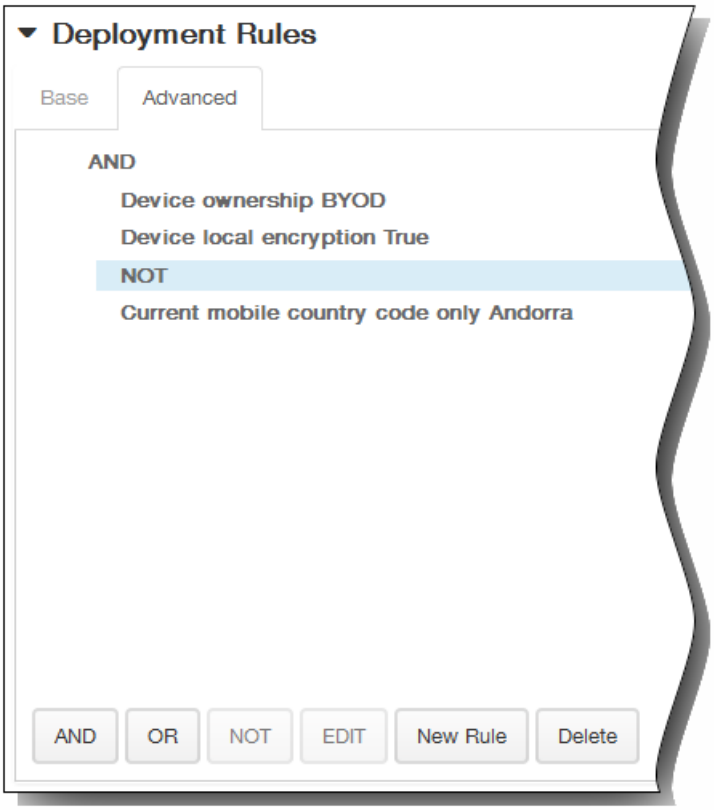
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



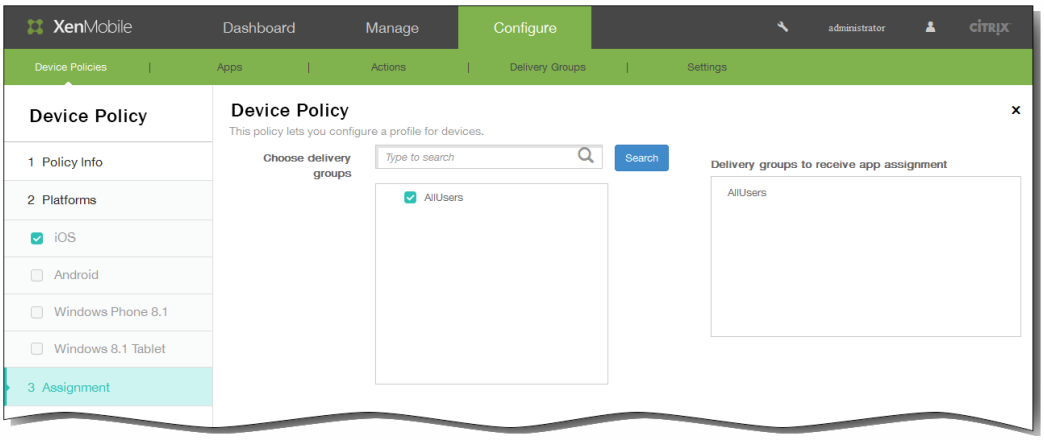
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



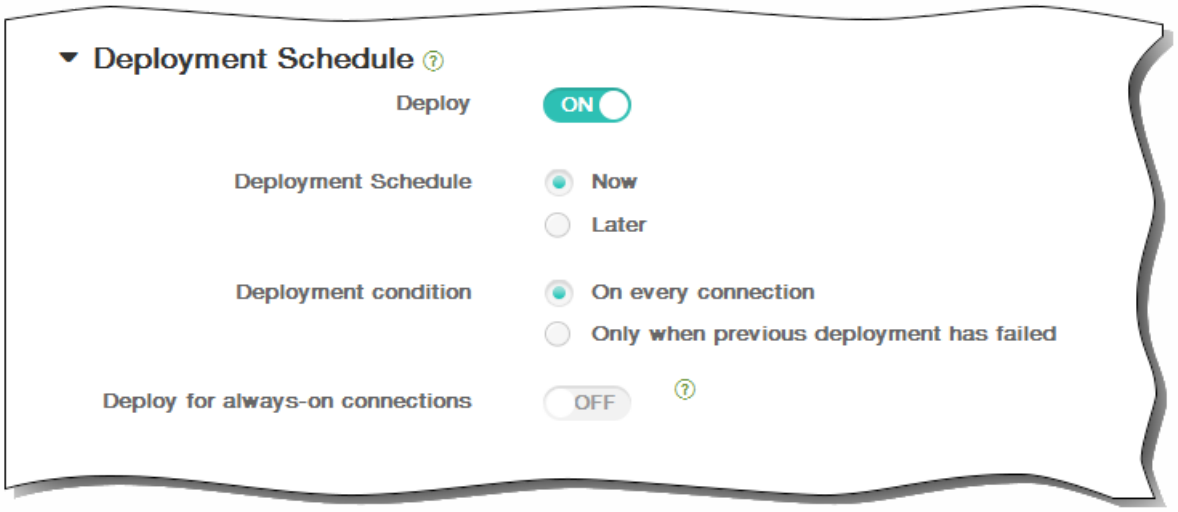
12. Haga clic en Next. Aparecerá la página de asignación Web Content Filter Policy.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



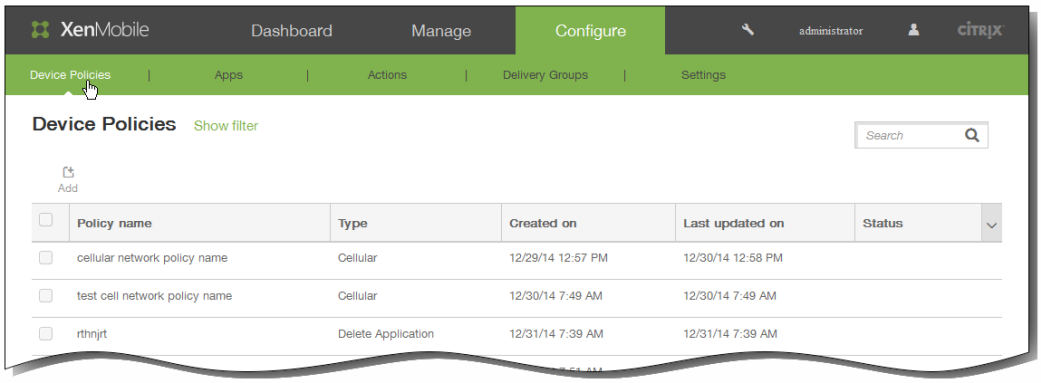
15. Haga clic en Save para guardar la directiva.

Directivas de exploradores Web para dispositivos Samsung

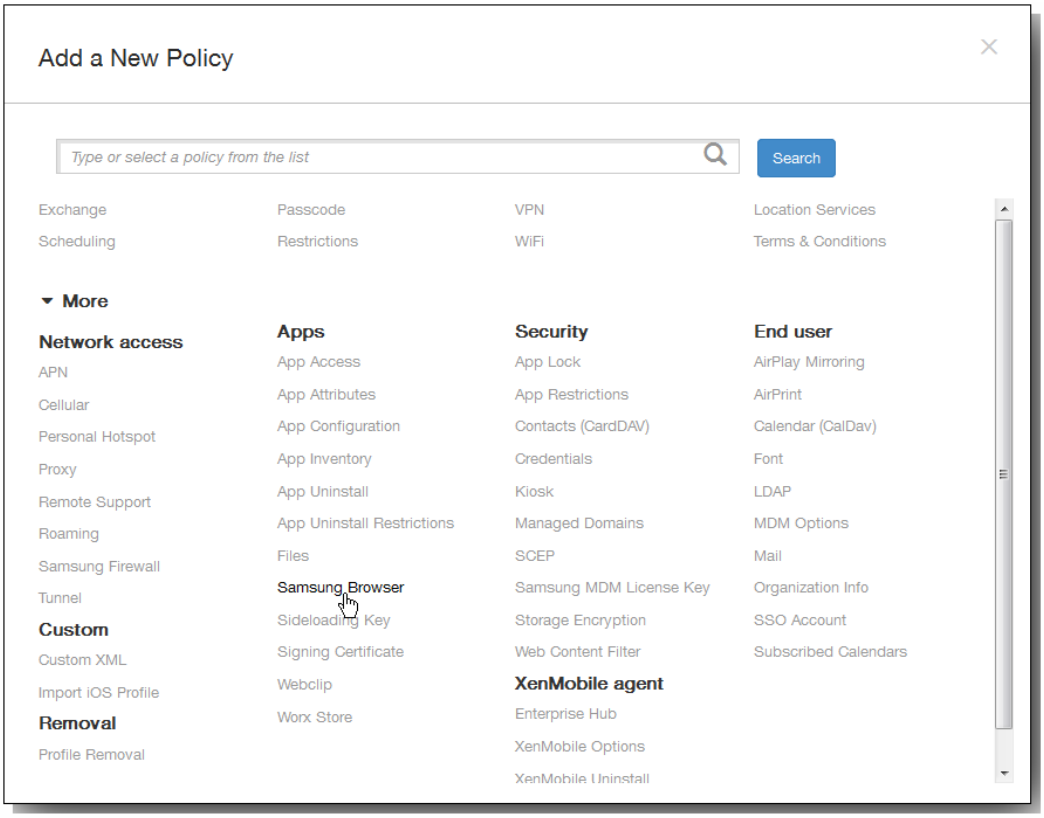
May 05, 2016

Puede crear directivas de exploradores Web para dispositivos Samsung SAFE y Samsung KNOX con el objetivo de definir si los dispositivos de los usuarios pueden usar el explorador Web o de limitar las funciones del explorador que puedan usar los dispositivos de los usuarios. Puede inhabilitar completamente el explorador, puede habilitar o inhabilitar los elementos emergentes, JavaScript, las cookies y la función de completado automático, y también puede decidir si forzar advertencias de fraude.

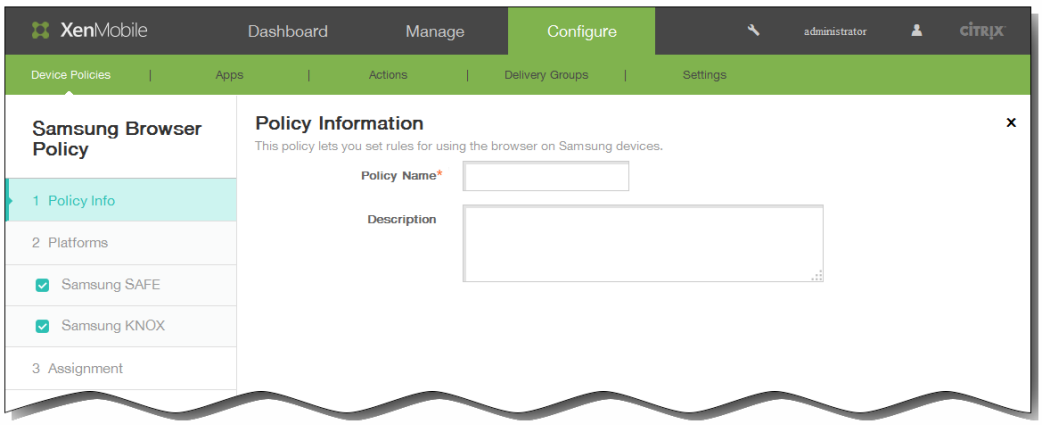
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



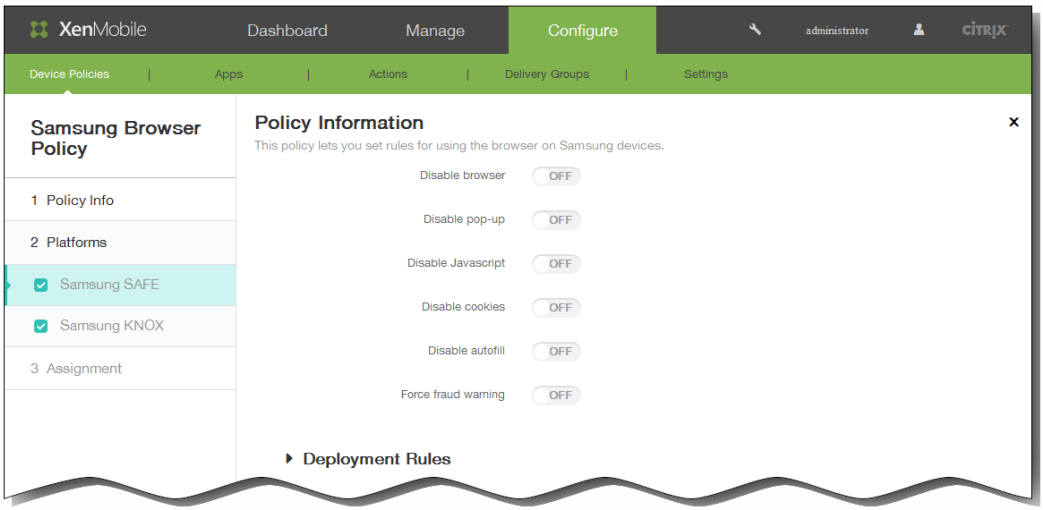
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add New Policy.



3. Haga clic en More y, a continuación, en Apps, haga clic en Samsung Browser. Aparecerá la página de información Samsung Browser Policy.

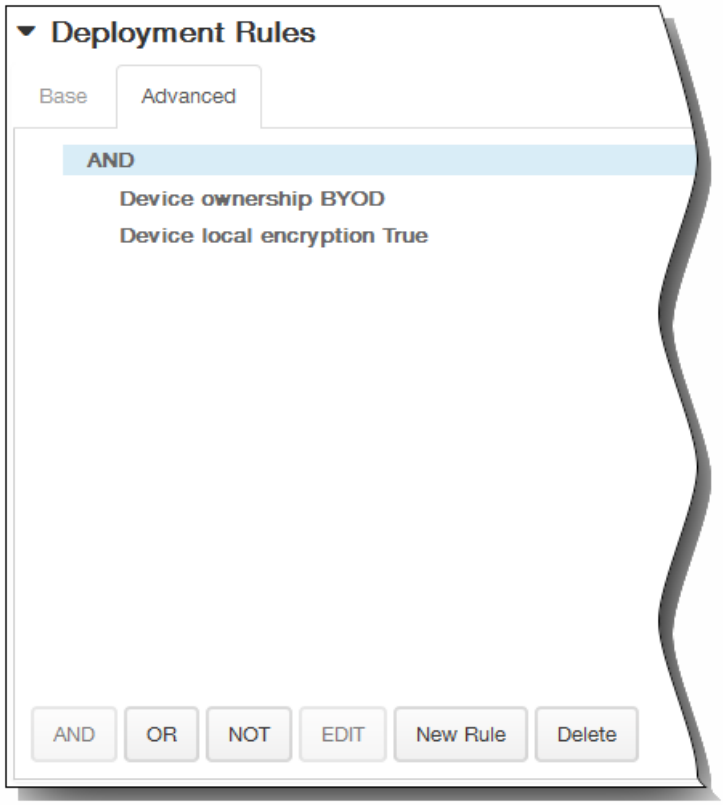


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
5. Haga clic en Next. Aparecerá la página Policy Platforms.
   Nota: Al aparecer la página Policy Platforms, ambas plataformas están seleccionadas, y el primer panel de configuración que se muestra pertenece a la plataforma de Samsung SAFE.



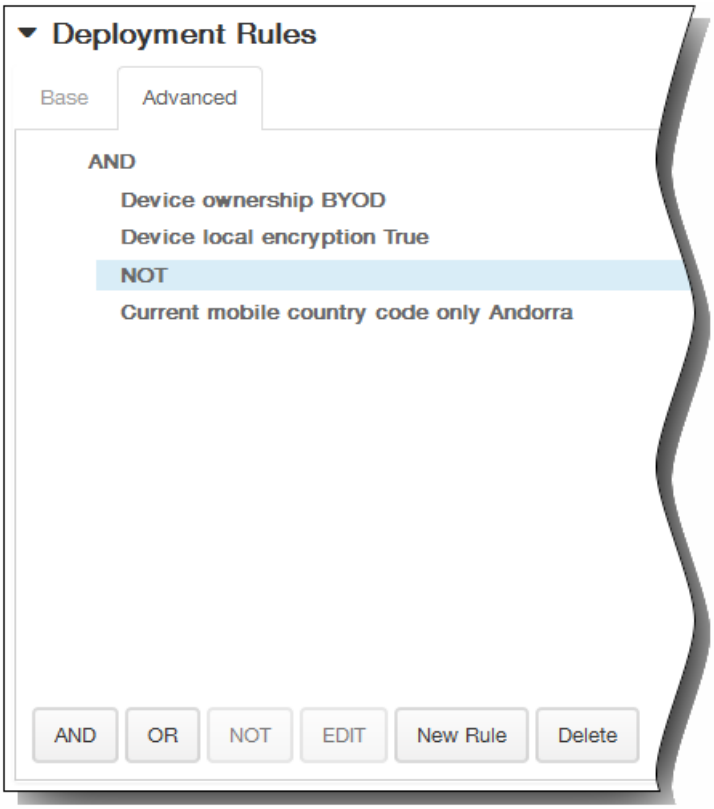
6.
7. En Platforms, seleccione las plataformas Samsung que quiera agregar. Si solo configura una plataforma, desmarque las demás y, a continuación, configure los siguientes parámetros:
   1. Disable browser. Seleccione esta opción para inhabilitar completamente el explorador Web de Samsung en los dispositivos de los usuarios. El valor predeterminado es OFF, con lo que los usuarios pueden utilizar el explorador. Si inhabilita el explorador Web, las siguientes opciones desaparecerán.
   2. Disable pop-up. Seleccione si permitir o no los mensajes emergentes en el explorador.
   3. Disable Javascript. Seleccione si permitir o no que se ejecute JavaScript en el explorador.
   4. Disable cookies. Seleccione si permitir o no las cookies.
   5. Disable autofill. Seleccionar si permitir a los usuarios activar la función de completado automático del explorador.
   6. Force fraud warning. Seleccione si mostrar una advertencia cuando los usuarios visiten un sitio Web fraudulento o no seguro.
8. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
      2. Haga clic en New Rule para definir las condiciones.
      3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
      4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
   2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

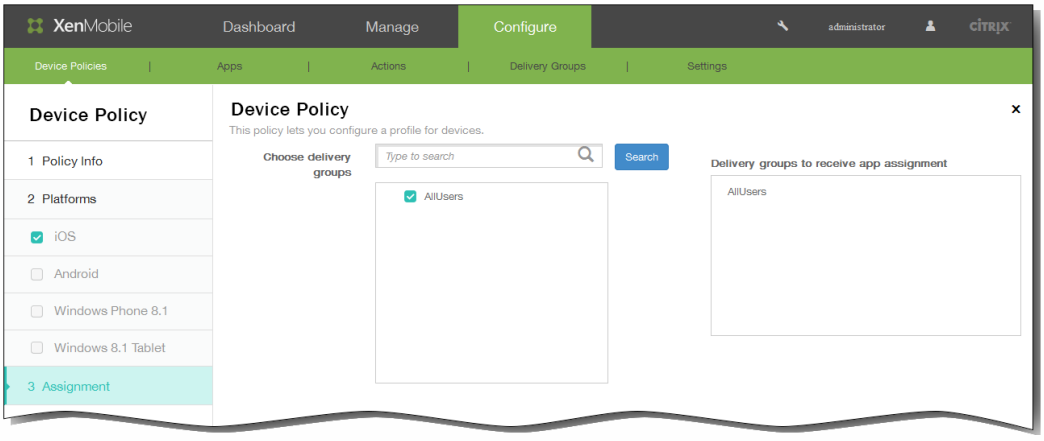


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



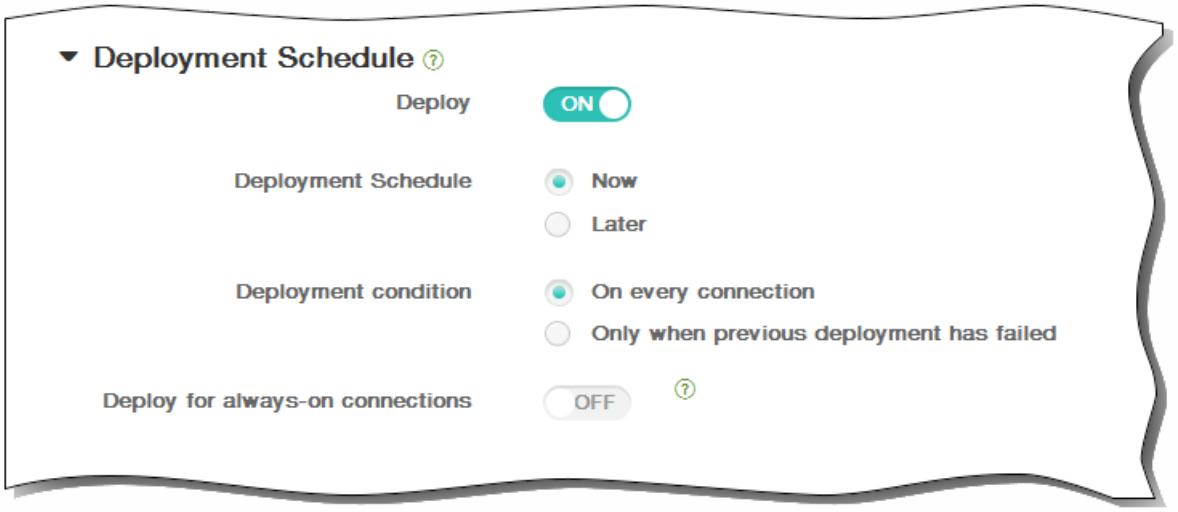
9. Haga clic en Next. Aparecerá la página de información Samsung Browser Device Policy.
10. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



11. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



12. Haga clic en Save para guardar la directiva.

Para agregar una directiva de claves de instalación de prueba para tabletas Windows 8.1

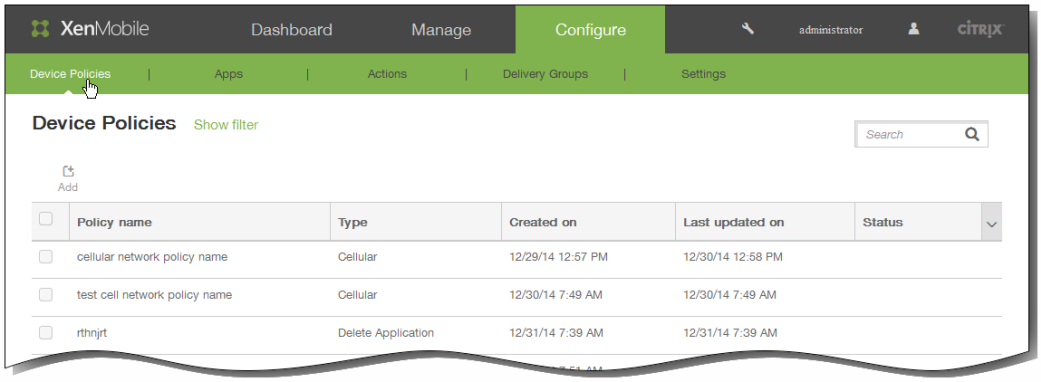
May 05, 2016

En XenMobile, la instalación de prueba permite implementar en dispositivos Windows 8.1 aplicaciones no adquiridas de la Tienda Windows. Por regla general, se realiza una instalación de prueba de aquellas aplicaciones que se desarrollan para uso corporativo y que no están pensadas para hacerse públicas en la Tienda Windows. Para realizar una instalación de prueba de las aplicaciones, configure la clave de instalación de prueba y las activaciones de la clave. A continuación, puede implementar esas aplicaciones en los dispositivos de los usuarios.

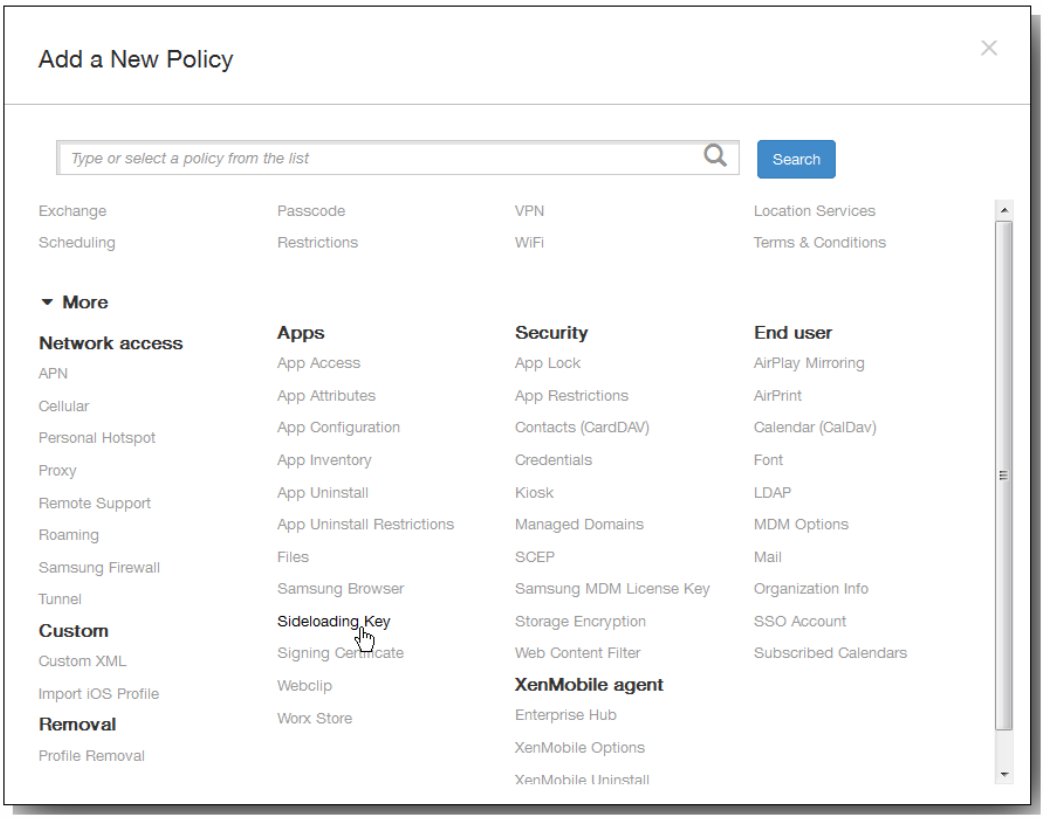
Para crear esta directiva, necesita la siguiente información:

- La clave del producto de instalación de prueba, que obtiene al iniciar sesión en el Centro de servicios de licencias por volumen de Microsoft
- La activación de la clave, que se crea mediante la línea de comandos después de obtener la clave del producto de instalación de prueba

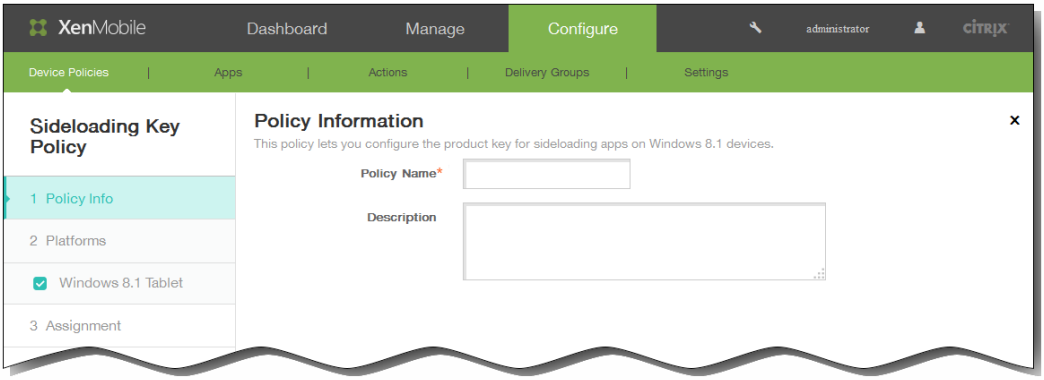
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



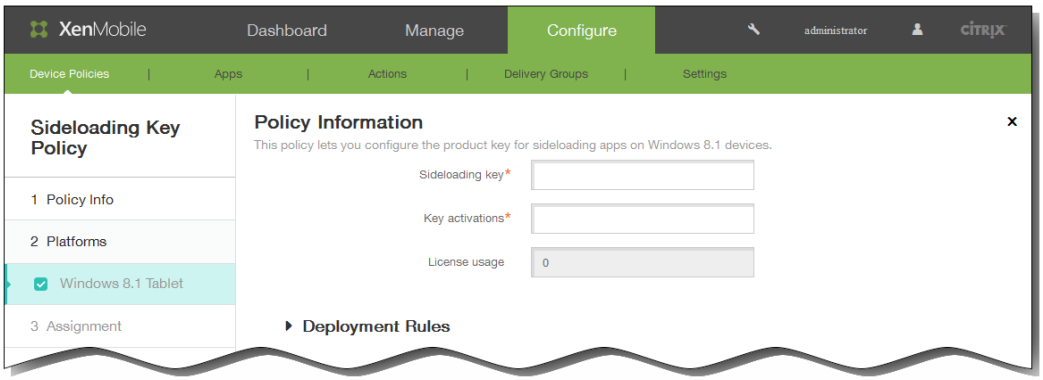
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add New Policy.



3. Haga clic en More y, a continuación, en Apps, haga clic en Sideloading Key. Aparecerá la página Sideloading Key Policy.

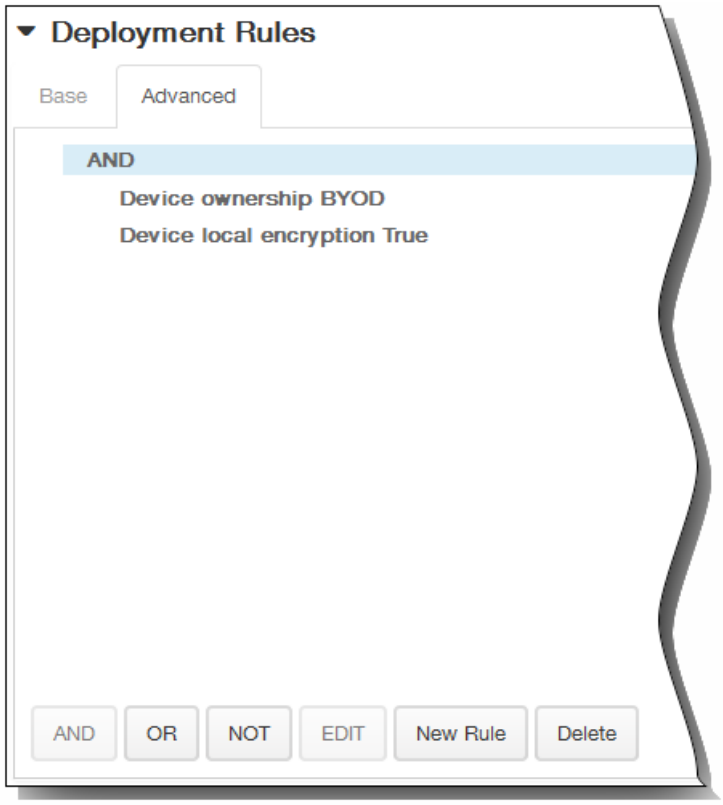


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next.
   Aparecerá la página de información Windows 8.1 Tablet Platform.



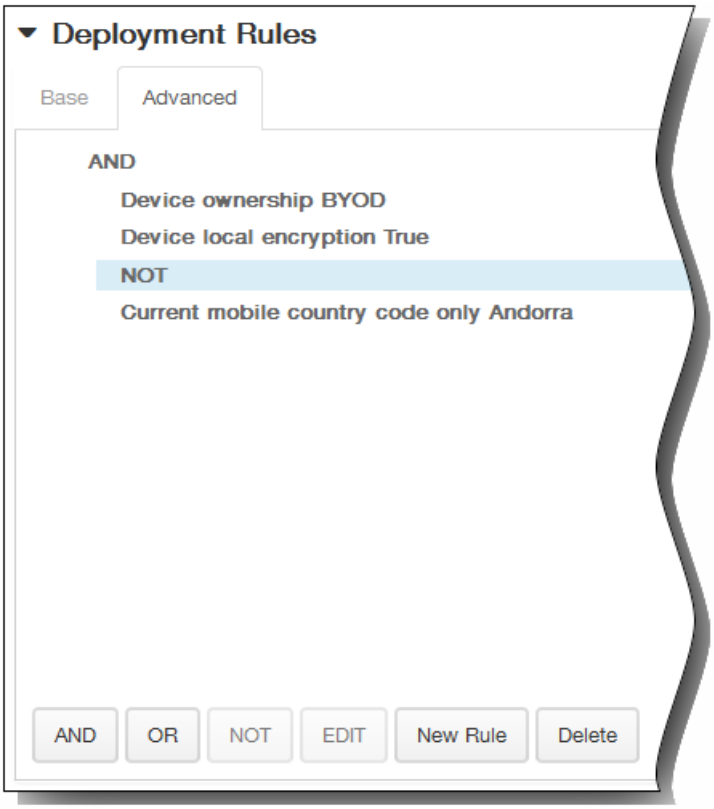
6. Configure los siguientes parámetros:
   1. Sideloading key. Escriba la clave de instalación de prueba obtenida del Centro de servicios de licencias por volumen de Microsoft.
   2. Key activations. Escriba la activación de la clave creada para la clave de instalación de prueba.
   3. License usage. XenMobile calcula este valor según el número de tabletas inscritas. Este campo no puede cambiarse.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
      2. Haga clic en New Rule para definir las condiciones.
      3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
      4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
   2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

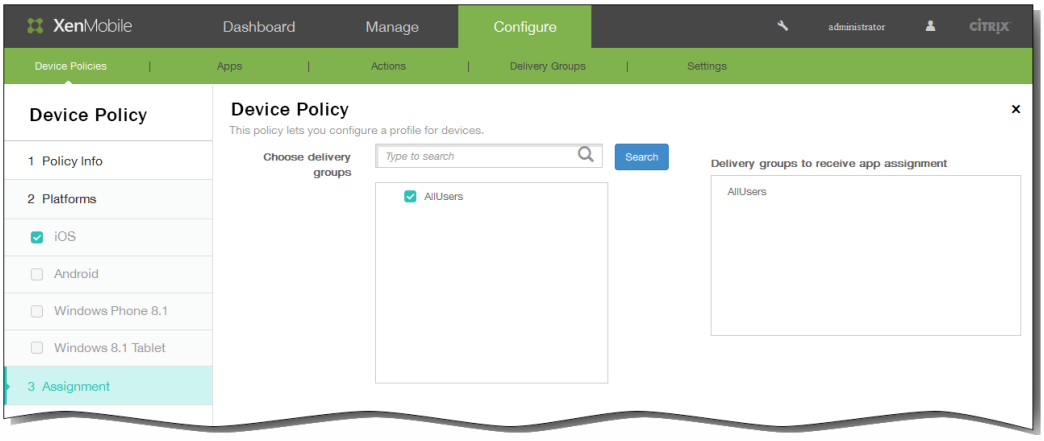


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



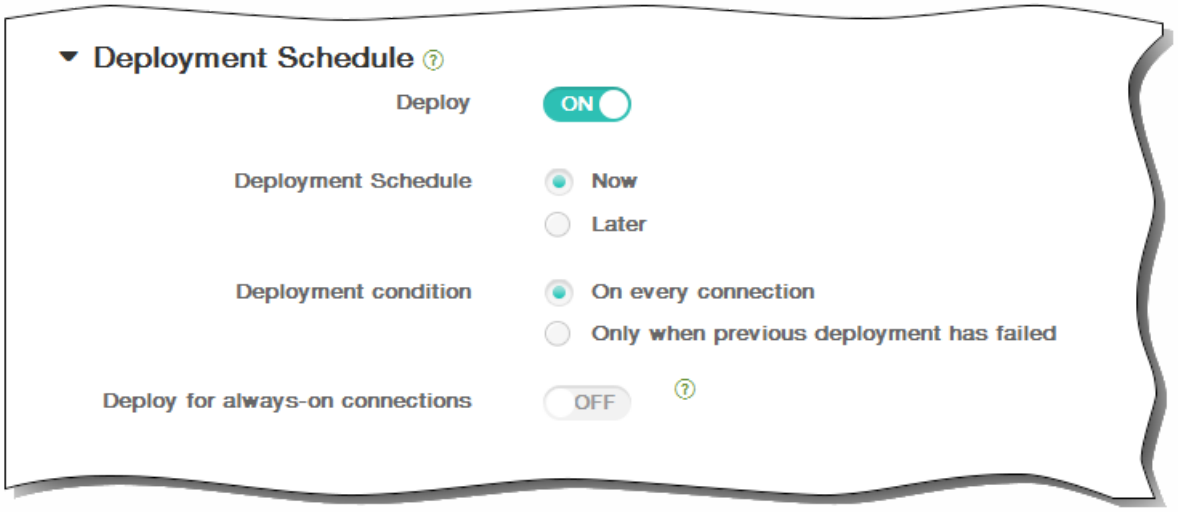
8. Haga clic en Next. Aparecerá la página de asignación Sideloading Key Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.

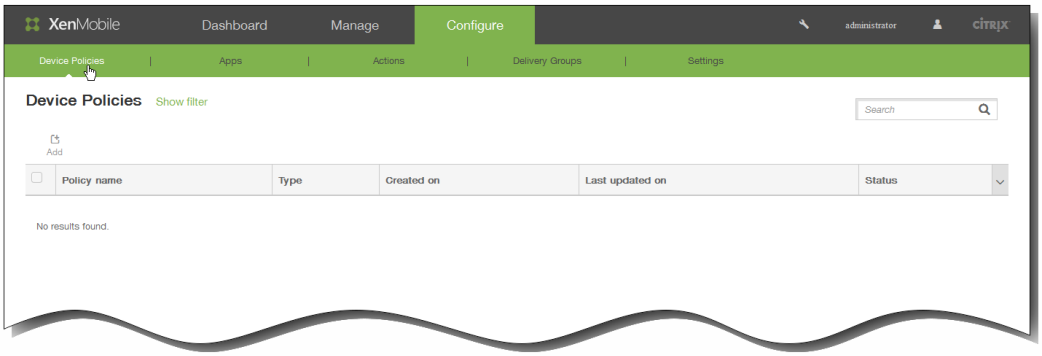


Para agregar una directiva de certificados de firma para tabletas Windows 8.1

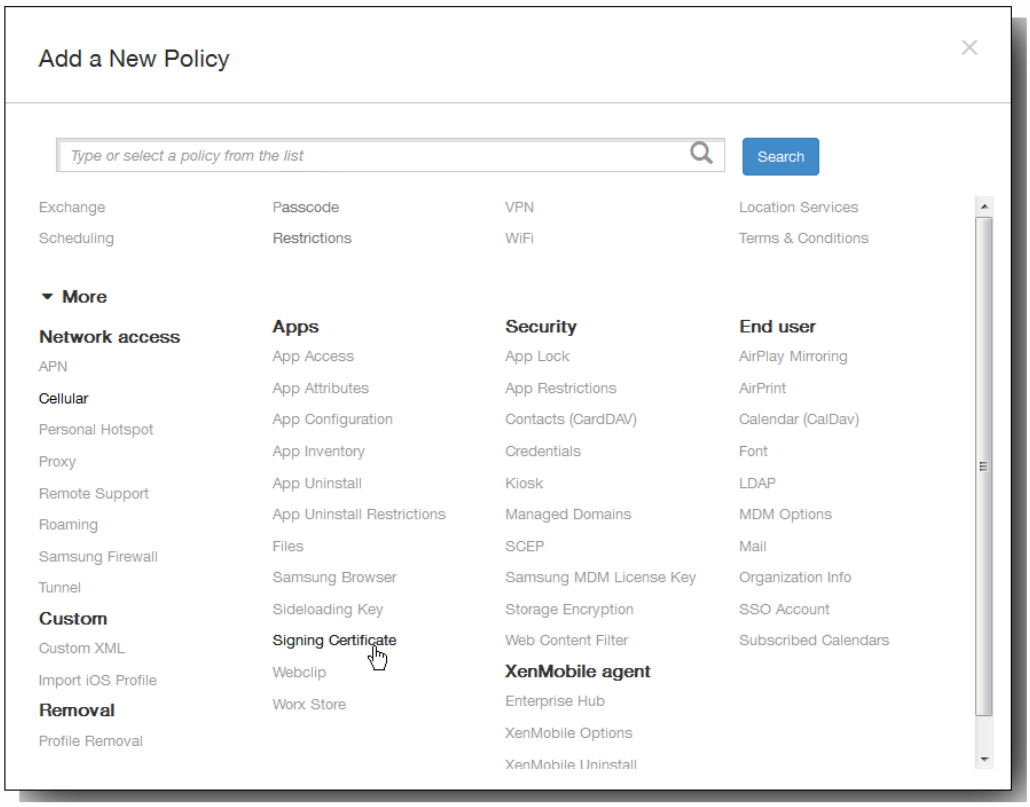
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para configurar los certificados de firma utilizados para firmar archivos APPX. Necesita certificados de firma si quiere distribuir archivos APPX a los usuarios para que puedan instalarse aplicaciones en sus tabletas Windows 8.1.

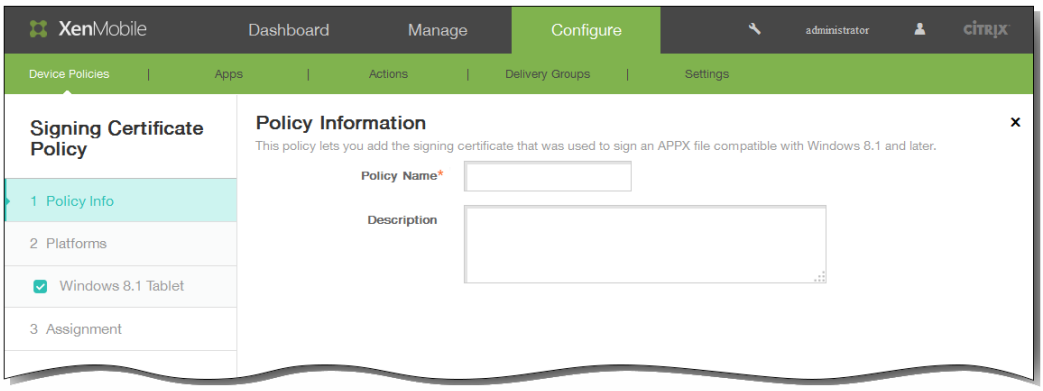
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



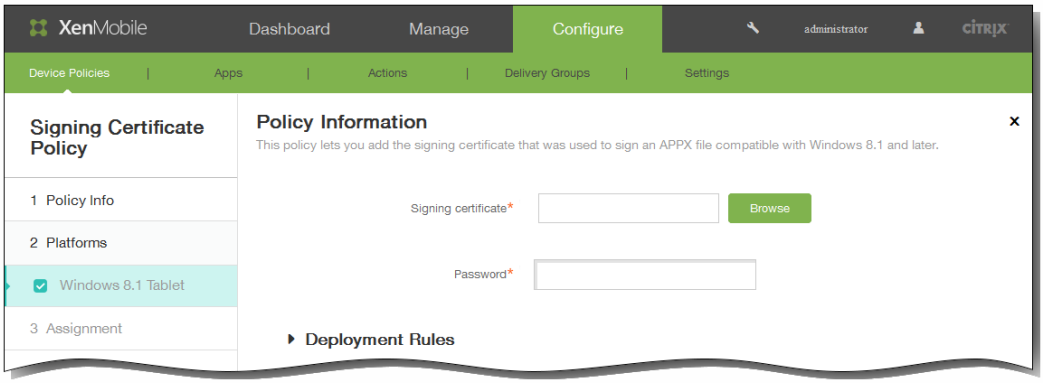
2. Haga clic en Add para agregar una nueva directiva. Cuando haga clic en Add, aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, a continuación, en Apps, haga clic en Signing Certificate. Aparecerá la página Signing Certificate Policy.

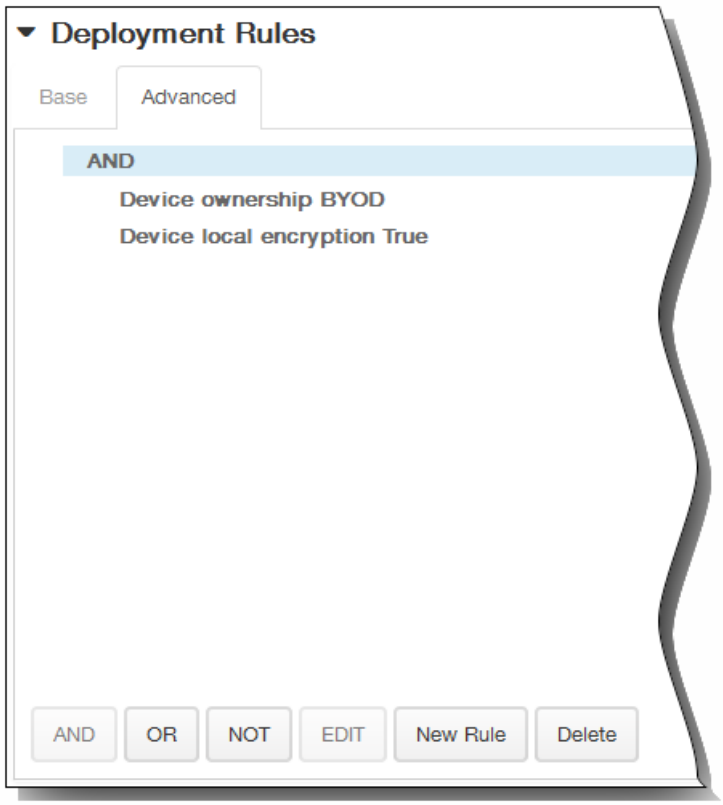


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página Platform Information.



6. Configure los siguientes parámetros:
   1. Signing certificate. Vaya a la ubicación del certificado utilizado para firmar el archivo APPX y selecciónelo.
   2. Password. Escriba la contraseña requerida para acceder al certificado de firma.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

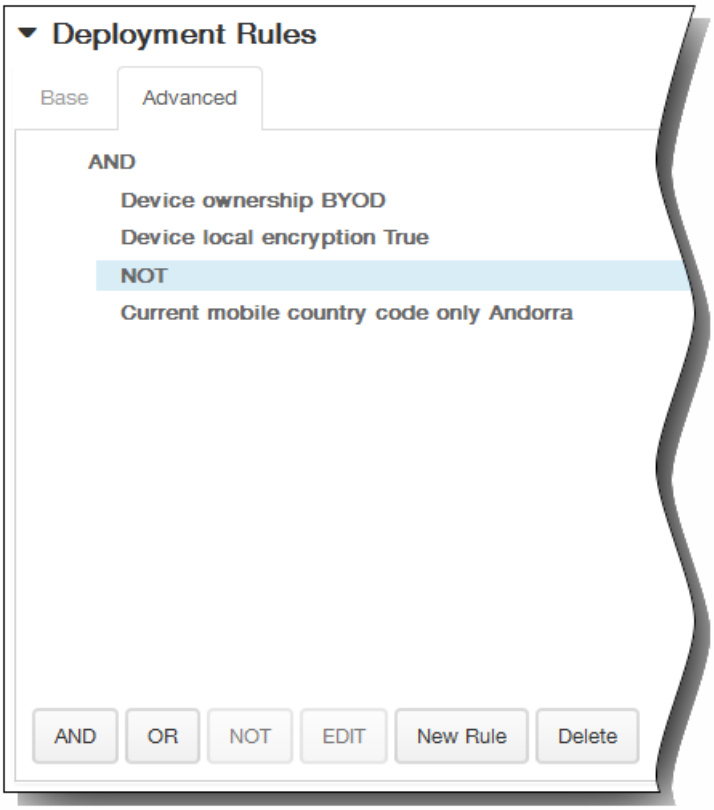
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



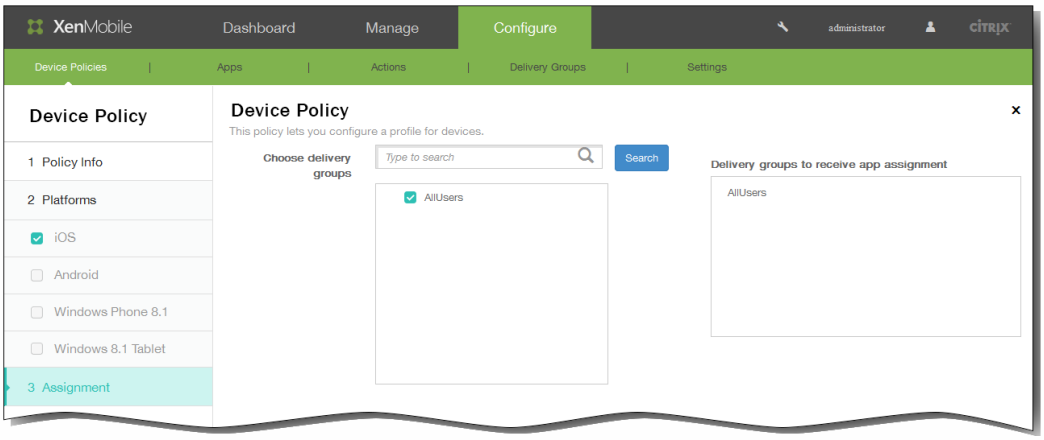
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



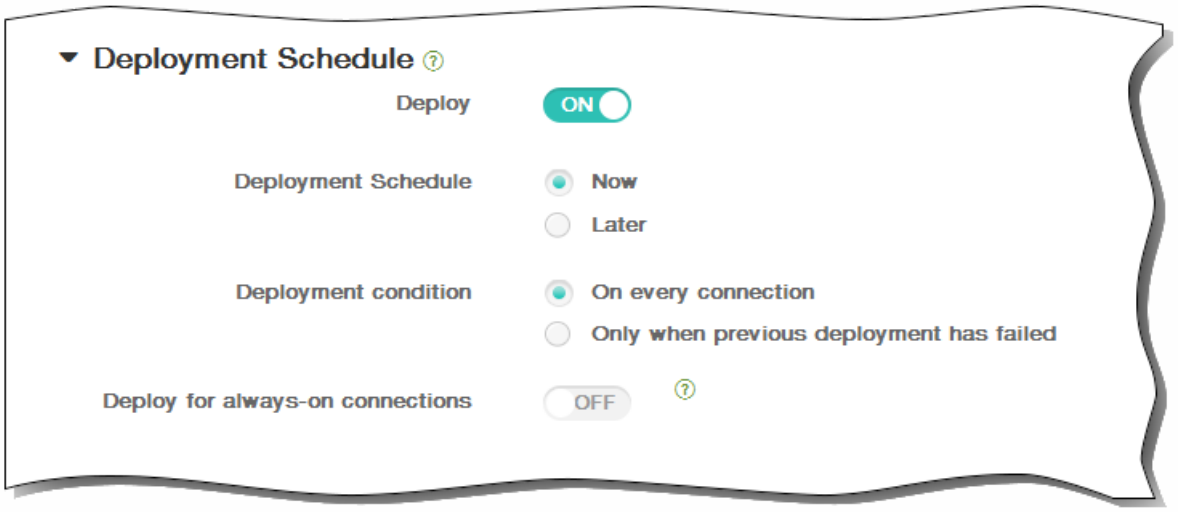
8. Haga clic en Next. Aparecerá la página Assignment.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

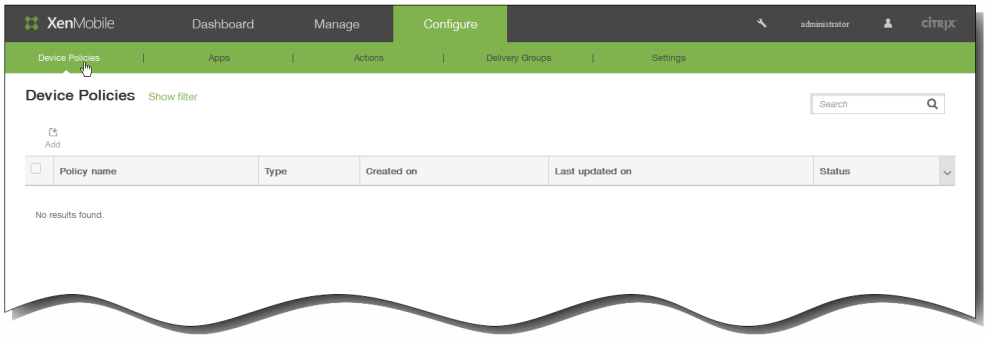
Directivas VPN de dispositivos

May 05, 2016

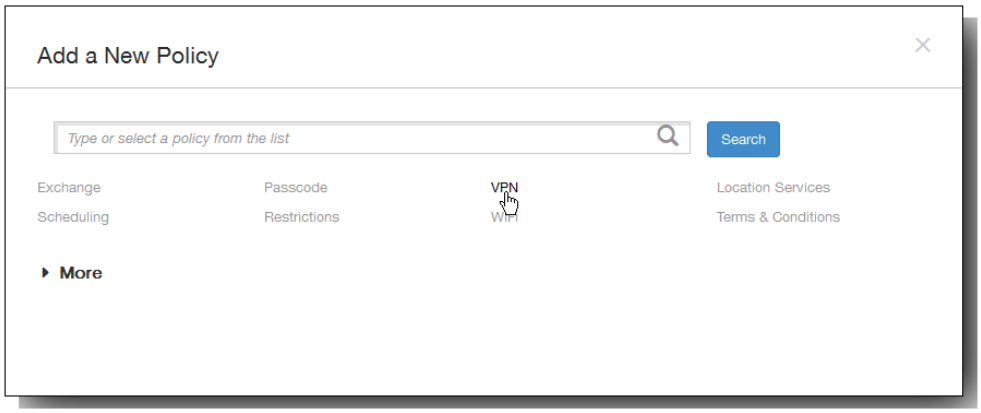
En XenMobile, puede agregar una directiva de dispositivos para configurar los parámetros de una red privada virtual (VPN) que permita a los dispositivos de los usuarios conectarse de forma segura a los recursos de la empresa. Puede configurar la directiva de redes VPN para las plataformas siguientes: iOS, Android, Samsung SAFE, Samsung KNOX, tabletas Windows 8.1 y Amazon. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Para agregar una directiva de redes VPN

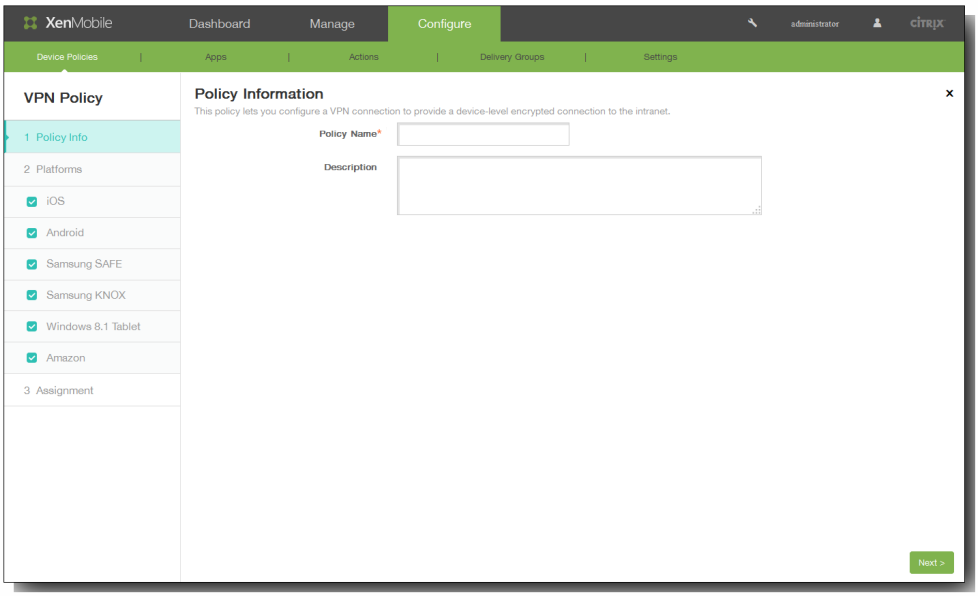
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



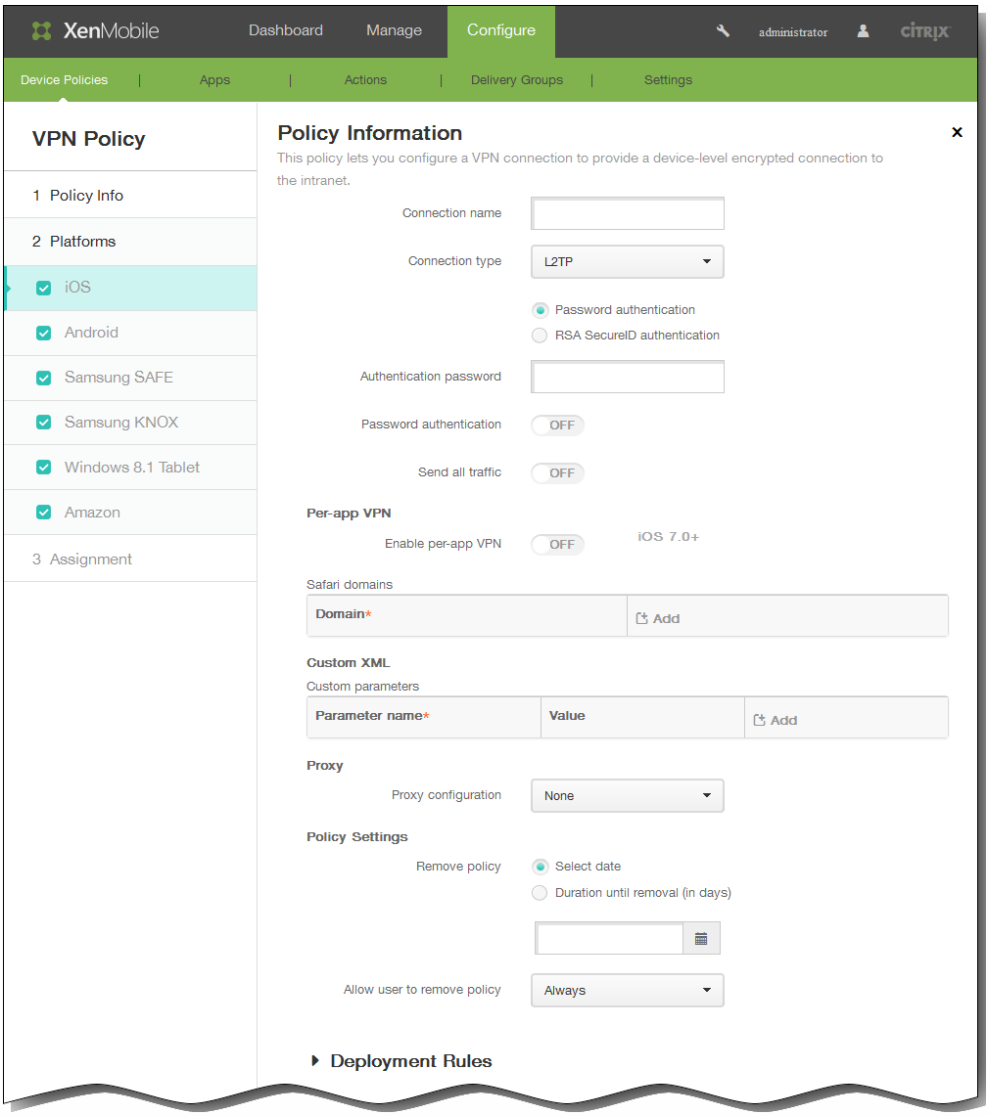
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en VPN. Aparecerá la página VPN Policy.



4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
   3. Haga clic en Siguiente.
5. En Platforms, seleccione la plataforma o las plataformas que quiere agregar.
   Si ha seleccionado iOS, configure los siguientes parámetros:



1. Connection name. Escriba un nombre para la conexión.
2. Connection type. En la lista, haga clic en el protocolo que se va a usar para esta conexión.
   - L2TP. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida. Esta es la opción predeterminada.
   - PPTP. Túnel punto a punto.
   - IPsec. La conexión VPN de su empresa.
   - Cisco AnyConnect. Cliente VPN de Cisco AnyConnect.
   - Juniper SSL. Cliente SSL VPN de Juniper Networks.
   - F5 SSL. Cliente SSL VPN de F5 Networks.
   - SonicWALL Mobile Connect. Cliente VPN unificado de Dell para iOS.
   - Ariba VIA. Cliente de acceso virtual a Internet de Ariba Networks.
   - IKEv2 (iOS only). Intercambio de claves por red versión 2 solo para iOS.
   - Custom SSL. Capa de sockets seguros (SSL) personalizada.

   En las siguientes secciones se enumeran las opciones de configuración para cada uno de los tipos de conexión mencionados.

Cómo configurar las siguientes opciones para el protocolo L2TP

1. Seleccione Password authentication o RSA SecureID authentication.
2. Authentication password. Escriba una contraseña de autenticación opcional.

3. Password authentication. Seleccione si la autenticación mediante contraseña está activada o desactivada.
4. Send all traffic. Seleccione si enviar todo el tráfico a través de la red privada virtual (VPN).

Cómo configurar las siguientes opciones para el protocolo PPTP

1. Seleccione Password authentication o RSA SecureID authentication.
2. Authentication password. Escriba una contraseña de autenticación opcional.
3. Password authentication. Seleccione si la autenticación mediante contraseña está activada o desactivada.
4. Encryption level. Seleccione el nivel de cifrado.
5. Send all traffic. Seleccione si enviar todo el tráfico a través de la red privada virtual (VPN).

Cómo configurar las siguientes opciones para el protocolo IPsec

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo de Cisco AnyConnect

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Group. Escriba un nombre de grupo opcional.
3. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido

Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo SSL de Juniper

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Realm. Escriba un nombre de dominio kerberos opcional.
3. Role. Escriba un nombre de rol opcional.
4. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF

Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo SSL de F5

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo Mobile Connect de SonicWALL

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Logon group or domain. Escriba un dominio o grupo de inicio de sesión opcional.
3. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF

	Contraseña	Certificado	Secreto compartido
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo VIA Ariba

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Password authentication	OFF	OFF	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	–

Cómo configurar las siguientes opciones para el protocolo IKEv2 (solo para iOS)

1. Authentication password. Escriba una contraseña de autenticación opcional.
2. Password authentication. Seleccione si la autenticación mediante contraseña está activada o desactivada.
3. Always-on VPN. Seleccione si la conexión VPN siempre está activada.
   Las siguientes opciones solo se aplican si Always-on VPN está establecido en ON.
4. Server name or IP address. Escriba el nombre o la dirección IP del servidor VPN.
5. User Account. Escriba una cuenta de usuario opcional.
6. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Contraseña	**Certificado**	**Secreto compartido**
Group name	–	–	Opcional
Shared secret	–	–	Opcional
Use hybrid authentication	–	–	OFF
Pedir contraseña	–	–	OFF
Allow user to disable automatic connection	OFF	OFF	OFF
Local identifier	Requerido	Requerido	Requerido
Remote identifier	Requerido	Requerido	Requerido
Extended Authentication Enabled	OFF	OFF	OFF
Dead Peer Detection Interval	Ninguno.	Ninguno.	Ninguno.
Encryption Algorithm	2DES	2DES	2DES
Integrity Algorithm	SHA1-96	SHA1-96	SHA1-96
Diffie-Hellman Group	2	2	2
LifeTime (en minutos)	1440	1440	1440
Voice Mail	Permitir el tráfico a través de un túnel	Permitir el tráfico a través de un túnel	Permitir el tráfico a través de un túnel

Allow traffic from captive web sheet outside the VPN	OFF	OFF	OFF
Allow traffic from all captive networking apps outside the VPN tunnel	OFF	OFF	OFF
AirPrint	Permitir el tráfico a través de un túnel	Permitir el tráfico a través de un túnel	Permitir el tráfico a través de un túnel
Captive networking app bundle identifiers	Opcional	Opcional	Opcional

Cómo configurar las siguientes opciones para el protocolo SSL personalizado

1. Custom SSL identifier (reverse DNS format). Escriba el identificador de SSL en formato DNS inverso.
2. Authentication password. Escriba una contraseña de autenticación opcional.
3. Password authentication. Seleccione si la autenticación mediante contraseña está activada o desactivada.
4. Authentication type for the connection. Seleccione el tipo de autenticación para esta conexión.

En la siguiente tabla aparecen las opciones disponibles para cada tipo de conexión. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

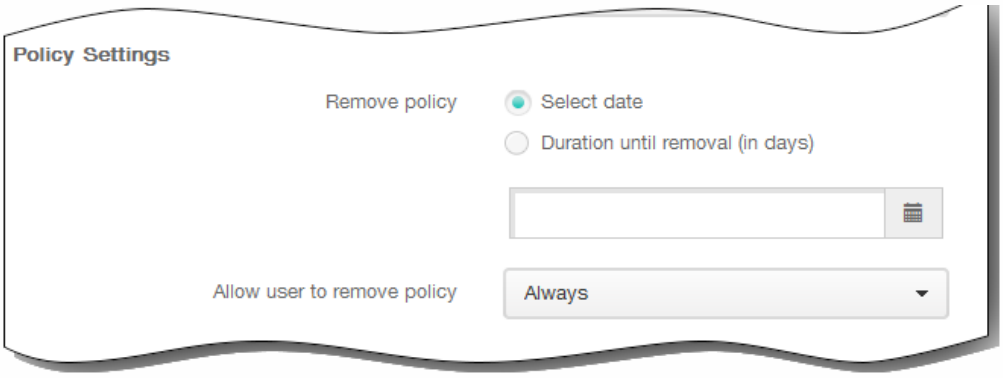
	Contraseña	Certificado	Secreto compartido
Group name	–	–	Opcional
Pedir contraseña	–	–	OFF
Auth password	Opcional	–	OFF
Identity credential	–	Ninguno.	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Necesario si Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF

3. Enable per-app VPN. Habilitar o inhabilitar la red privada virtual Per-App (disponibles para cada aplicación, iOS 7 y versiones posteriores). Si está habilitada, habilite o inhabilite On-demand match enabled.
4. Safari domains. Haga clic en Add para agregar un dominio de Safari que permita a la aplicación crear una conexión VPN Per-App segura a través de Safari.
5. Custom XML. Haga clic en Add para introducir los pares de nombre del parámetro en Parameter name y su valor en Value respectivamente para personalizar la configuración.
6. Proxy configuration. En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy y configure las opciones adicionales.

En la siguiente tabla se ofrece una lista de las opciones disponibles para Manual y Automatic; si no aparece nada, no requiere configuración adicional. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

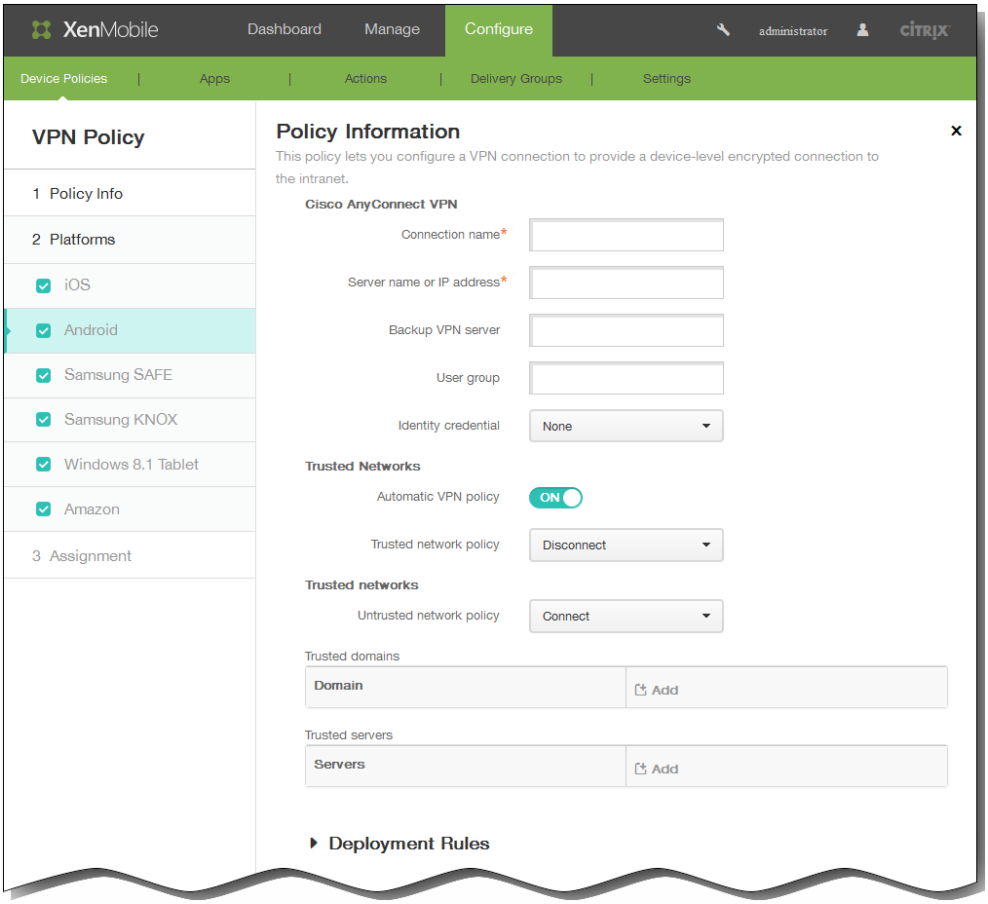
	Manual	Automatic
Host name or IP address for the proxy server	Requerido	–
Port for the proxy server	Requerido	–
User name	Opcional	–
Contraseña	Opcional	–
Proxy server URL	–	Requerido

Configuraciones de directivas



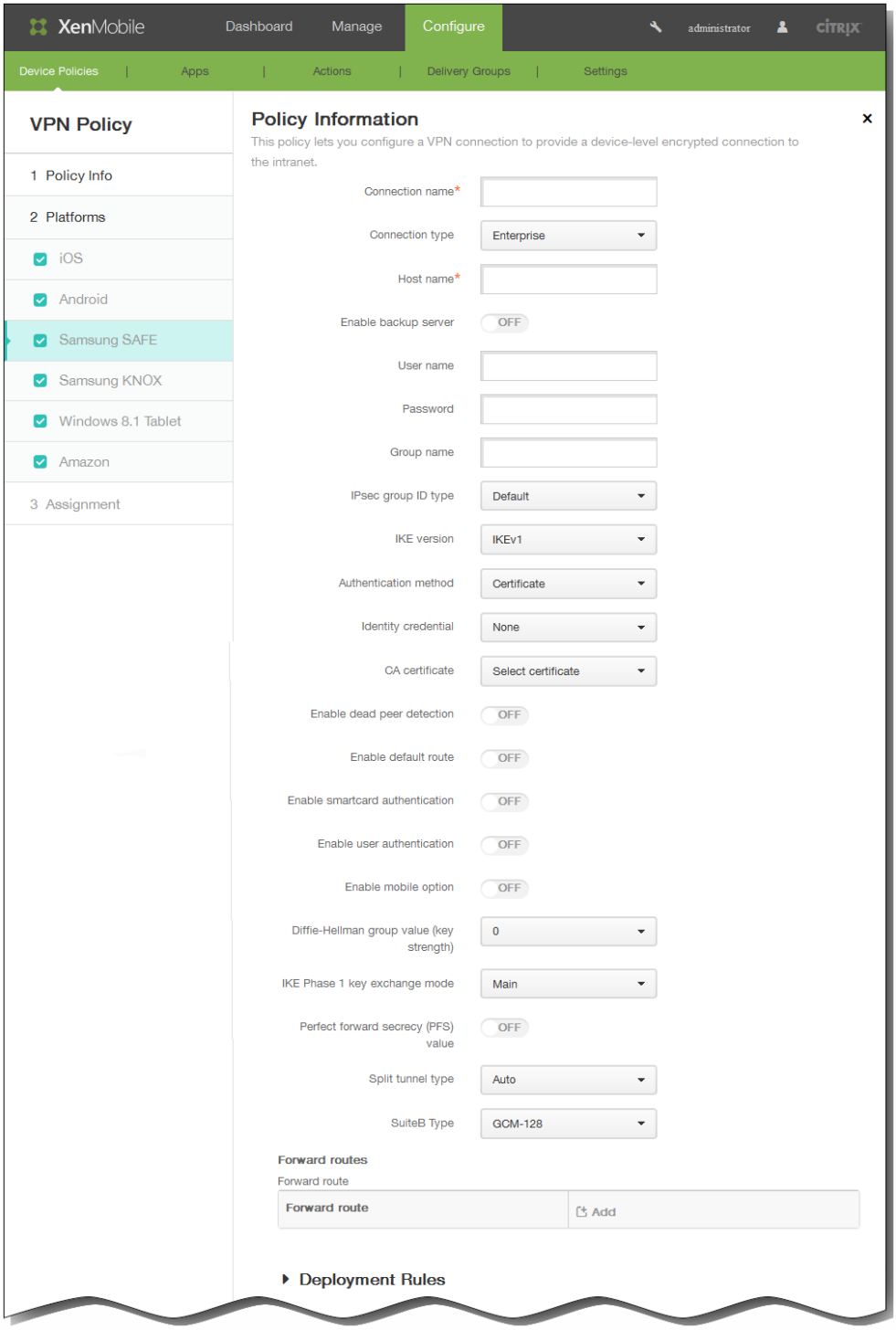
1. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
2. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
3. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
4. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

Si ha seleccionado Android, configure los siguientes parámetros:



1. Connection name. Escriba un nombre para la conexión VPN de Cisco AnyConnect.
2. Server name or IP address. Escriba el nombre o la dirección IP del servidor VPN.
3. Backup VPN server. Escriba la información del servidor VPN de respaldo.
4. User group. Escriba la información del grupo de usuarios.
5. Identity credential. En la lista, seleccione una credencial de identidad.
6. Automatic VPN policy. Habilite o inhabilite esta opción para establecer cómo reaccionará la red privada virtual ante redes con las que se haya establecido una relación de confianza o de no confianza. Si esta opción está habilitada, escriba la información siguiente:
   - Trusted network policy. En la lista, haga clic en la directiva pertinente.
   - Untrusted network policy. En la lista, haga clic en la directiva pertinente.

Si ha seleccionado Samsung SAFE, configure los siguientes parámetros:



1. Connection name. Escriba un nombre para la conexión.
2. Connection type. En la lista, haga clic en el protocolo que se va a usar para esta conexión:
   - L2TP with pre-shared key. Protocolo Layer 2 Tunneling Protocol con autenticación de clave previamente compartida. Esta es la opción predeterminada.
   - L2TP with certificate. Protocolo Layer 2 Tunneling Protocol con certificado.
   - PPTP. Túnel punto a punto.
   - Enterprise. La conexión VPN de su empresa.

   En la siguiente tabla se muestran las opciones de configuración para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la

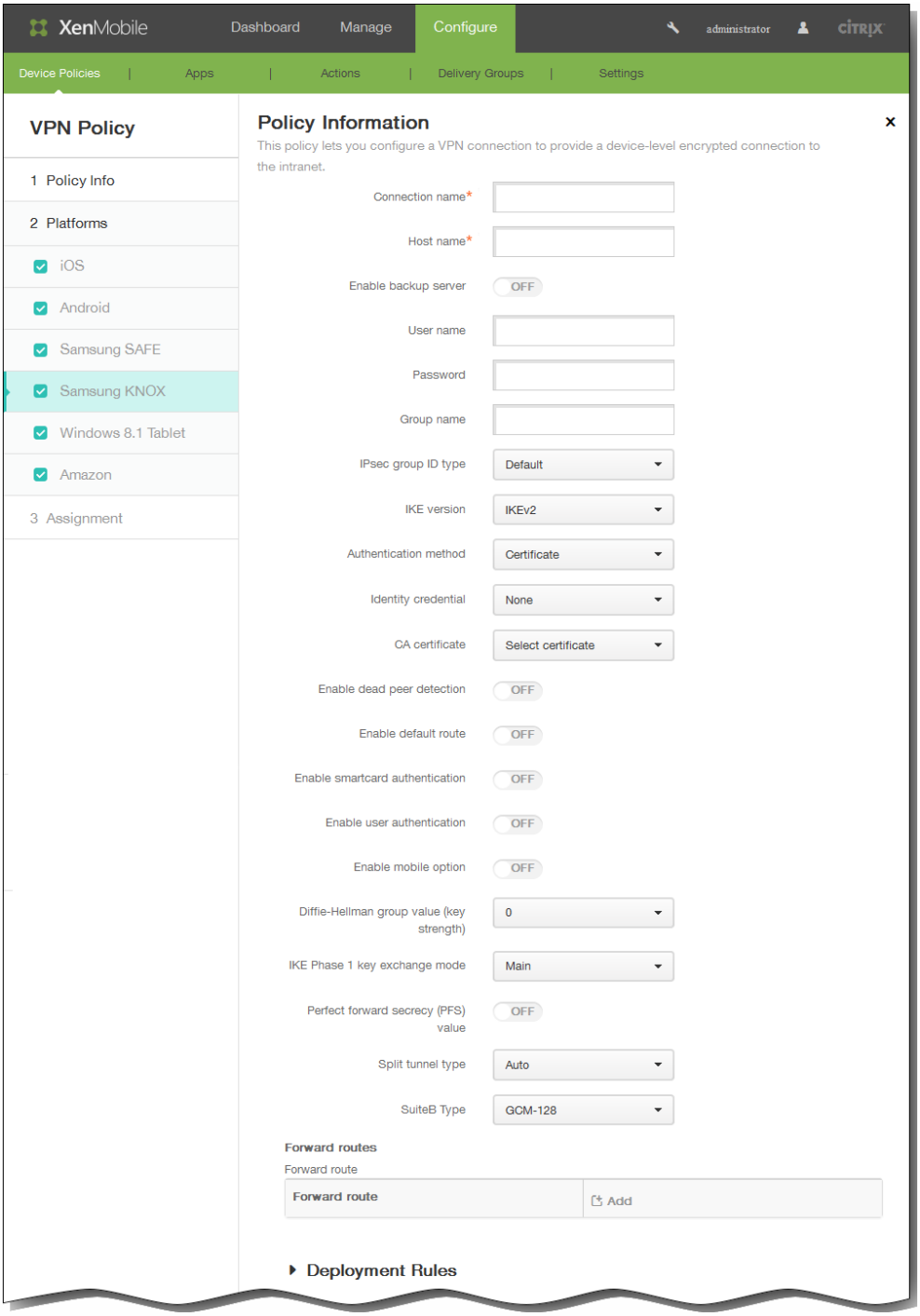
opción no se puede aplicar (–), si es necesaria o si es opcional.

	L2TP with pre-shared key	**L2TP with certificate**	**PPTP**	**Enterprise**				
Host name	Requerido	Requerido	Requerido	Requerido				
Enable backup server	–	–	–	Off				
Backup VPN server	–	–	–	Es necesario si Enable backup server = On				
User name	Opcional	Opcional	Opcional	Opcional				
Contraseña	Opcional	Opcional	Opcional	Opcional				
Group name	–	–	–	Opcional				
IPsec group ID type	–	–	–	Predeterminado				
IKE version	–	–	–	IKEv1				
Authentication method	–	–	–	Certificate (predeterminado)	Pre-shared key	Hybrid RSA	EAP MD5	EAP MSCHAPv2
Identity credential	–	Requerido	–	Ninguno.	Ninguno.	–	–	–
CA certificate	–	–	–	Seleccione el certificado.				
Enable dead peer detection	–	–	–	Off				
Enable default route	–	–	–	Off				
Enable smartcard authentication	–	–		Off				
Enable user authentification	–	–	–	Off				
Enable mobile								

option Diffie-Hellman group value (nivel de clave)	**L2TP with pre-shared key** –	**L2TP with certificate** –	**PPTP** –	**Enterprise** Off 0				
IKE Phase 1 key exchange mode	–	–	–	Principal				
Perfect forwarded secrecy (PFS) value	–	–	–	Off				
Split tunnel type	–			Auto				
SuiteB Type	–	–	–	GCM-128				
Pre-shared key	Requerido	–	–	–	Opcional	–	–	–
Enable encryption	–	–	Off	–	–	–	–	–

3. Forward routes. Agregue rutas de reenvío opcionales si el servidor VPN de la empresa es compatible con varias tablas de enrutamiento.

Si ha seleccionado Samsung KNOX, configure los siguientes parámetros:



1. Connection name. Escriba el nombre de la conexión.
2. Host name. Escriba el nombre de host.
3. Enable backup server. Seleccione si habilitar un servidor VPN de respaldo. Si selecciona esta opción, aparecerá un campo adicional. Introduzca los datos del servidor de respaldo.
4. User name. Escriba un nombre de usuario opcional.
5. Password. Escriba una contraseña opcional.
6. Group name. Escriba un nombre de grupo opcional.
7. IPsec group ID type. En la lista, haga clic en el tipo de ID de grupo IPsec.
8. IKE version. En la lista, haga clic en la versión IKE.
9. Authentication method. En la lista, haga clic en el método de autenticación.

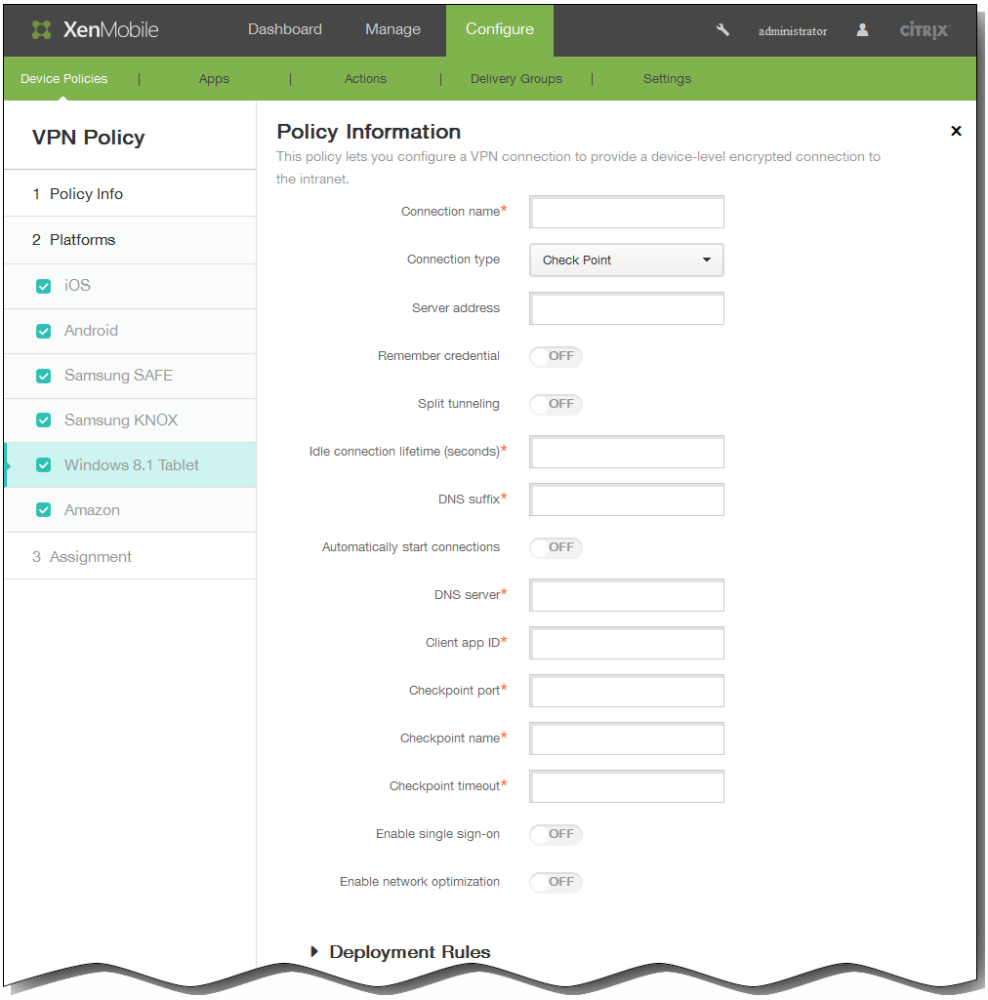
- Certificate. Autenticación basada en certificados.
- Pre-shared key. Autenticación mediante una clave previamente compartida.
- Hybrid RSA. Autenticación híbrida con certificados RSA.
- EAP MD5. Protocolo de autenticación extensible con la función hash de MD5.
- EAP MSCHAPv2. Protocolo de autenticación extensible con la versión 2 del Protocolo de autenticación por desafío mutuo de Microsoft.

En la siguiente tabla se muestran las opciones de configuración para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Certificado	**Pre-shared key**	**Hybrid RSA**	**EAP MD5**	**EAP MSCHAPv2**
Pre-shared key	–	Requerido	–	–	–
Identity credential	Ninguno.	Ninguno.	–	–	–
CA certificate	Requerido	Requerido	Requerido	Requerido	Requerido
Enable dead peer detection	OFF	OFF	OFF	OFF	OFF
Enable default route	OFF	OFF	OFF	OFF	OFF
Enable smartcard authentication	OFF	OFF	OFF	OFF	OFF
Enable user authentication	OFF	OFF	OFF	OFF	OFF
Enable mobile option	OFF	OFF	OFF	OFF	OFF
DIfffie-Hellman group value (nivel de clave)	0	0	0	0	0
IKE Phase 1 key exchange mode	Principal	Principal	Principal	Principal	Principal
Perfect forward secrecy (PFS) value	OFF	OFF	OFF	OFF	OFF
Split tunnel type	Auto	Auto	Auto	Auto	Auto
SuiteB Type	GCM-128	GCM-128	GCM-128	GCM-128	GCM-128

10. Forward route. Agregue rutas de reenvío opcionales si el servidor VPN de la empresa es compatible con varias tablas de enrutamiento.

Si ha seleccionado Windows 8.1 tablet, configure los siguientes parámetros:



1. Connection name. Escriba el nombre de la conexión.
2. Connection type. En la lista, haga clic en el tipo de conexión.
   - SonicWALL. Cliente VPN unificado de Dell para Windows.
   - Check Point. Cliente SSL VPN de Check Point Software Technologies.
   - Juniper. Cliente SSL VPN de Juniper Networks.
   - Microsoft. Cliente VPN de Microsoft.
   - F5. Cliente SSL VPN de F5 Networks.

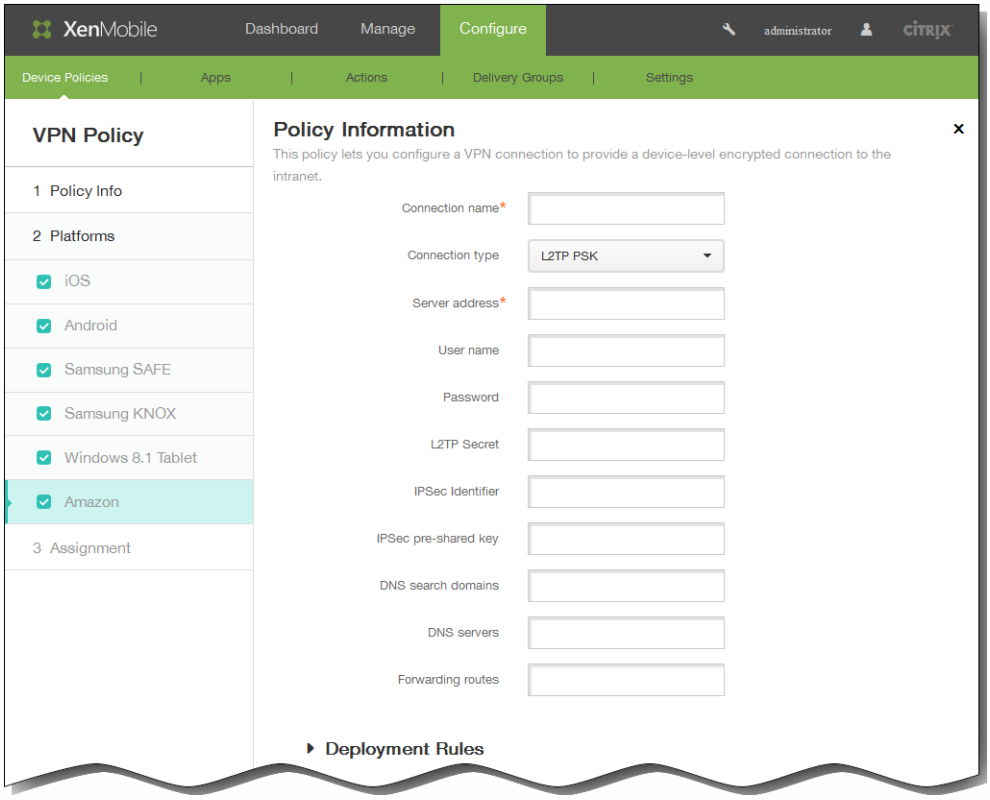
   En la siguiente tabla se muestran las opciones de configuración para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	SonicWALL	Check Point	Juniper	Microsoft	F5
Server address	Opcional	Opcional	Opcional	Opcional	Opcional
Remember credential	OFF	OFF	OFF	OFF	OFF
Split tunneling	OFF	OFF	OFF	OFF	OFF
Idle connection lifetime (segundos)	Requerido	Requerido	Requerido	Requerido	Requerido

DNS suffix	SonicWALL	Check Point	Juniper	Microsoft	F5
	Requerido	Requerido	Requerido	Requerido	Requerido
Automatically start connections	OFF	OFF	OFF	–	OFF
Servidor DNS	Requerido	Requerido	Requerido	–	Requerido
Client app ID	Requerido	Requerido	Requerido	–	Requerido
Checkpoint port	–	Requerido	–	–	–
Checkpoint name	–	Requerido	–	–	–
Checkpoint timeout	–	Requerido	–	–	–
Enable Single Sign-On	–	OFF	–	–	–
Enable network optimization	–	OFF	–	–	–
Enable compression	OFF	–	–	–	–
Require smart card certificate	OFF	–	–	–	–
Automatically select client certificate	OFF	–	–	–	–
Enable client logging	OFF	–	–	–	–
Enable packet capture	OFF	–	–	–	–
Use single sign-on credentials	–	–	OFF	–	–
Make connection available to all users	–	–	–	OFF	–
Tunneling protocol	–	–	–	Requerido	–
Authentication method	–	–	–	Requerido	–
VPN server name	–	–	–	Requerido	–
VPN friendly name	–	–	–	Requerido	–

Automatically detect settings	SonicWALL –	Check Point –	Juniper –	Microsoft OFF	F5 –
Bypass proxy server for local addresses	–	–	–	OFF	–
Automatically use Windows credentials	–	–	–	OFF	–
Client certificate issuer	–	–	–	–	Requerido

Si ha seleccionado Amazon, configure los siguientes parámetros:



1. Connection name. Escriba el nombre de la conexión.
2. Connection type. Haga clic en el tipo de conexión.
   - L2TP PSK. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
   - L2TP RSA. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación RSA.
   - IPSEC XAUTH PSK. Protocolo de seguridad de Internet con clave previamente compartida y autenticación ampliada.
   - IPSEC XAUTH RSA. Protocolo de seguridad de Internet con RSA y autenticación ampliada.
   - IPSEC HYBRID RSA. Protocolo de seguridad de Internet con autenticación RSA híbrida.
   - PPTP. Túnel punto a punto.

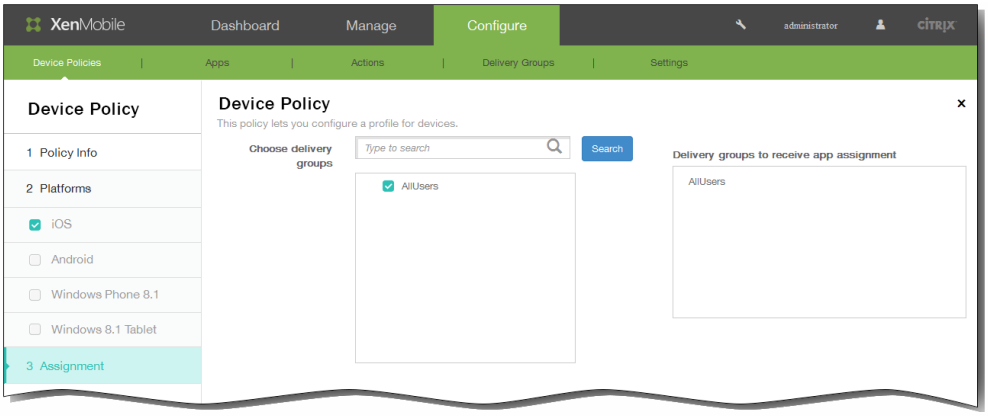
   En la siguiente tabla se muestran las opciones de configuración para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	L2TP PSK	L2TP RSA	IPSEC XAUTH PSK	IPSEC XAUTH RSA	IPSEC HYBRID RSA	PPTP

Server address	Requerido **L2TP PSK**	Requerido **L2TP RSA**	Requerido **IPSEC XAUTH PSK**	Requerido **IPSEC XAUTH RSA**	Requerido **IPSEC HYBRID RSA**	Requerido **PPTP**
User name	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional
Contraseña	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional
L2TP Secret	Opcional	Opcional	–	–	–	–
IPsec identifier	Opcional	–	Opcional	–	–	–
IPsec pre-shared key	Opcional	–	Opcional	–	–	–
DNS search domains	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional
DNS servers	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional
Forwarding routes	Opcional	Opcional	Opcional	Opcional	Opcional	Opcional
Server certificate	–	Selección	–	Selección	Selección	–
CA certificate	–	Selección	–	Selección	Selección	–
Identity credential	–	Requerido	–	Requerido	–	–
PPP encryption (MMPE)	–	–	–	–	–	OFF

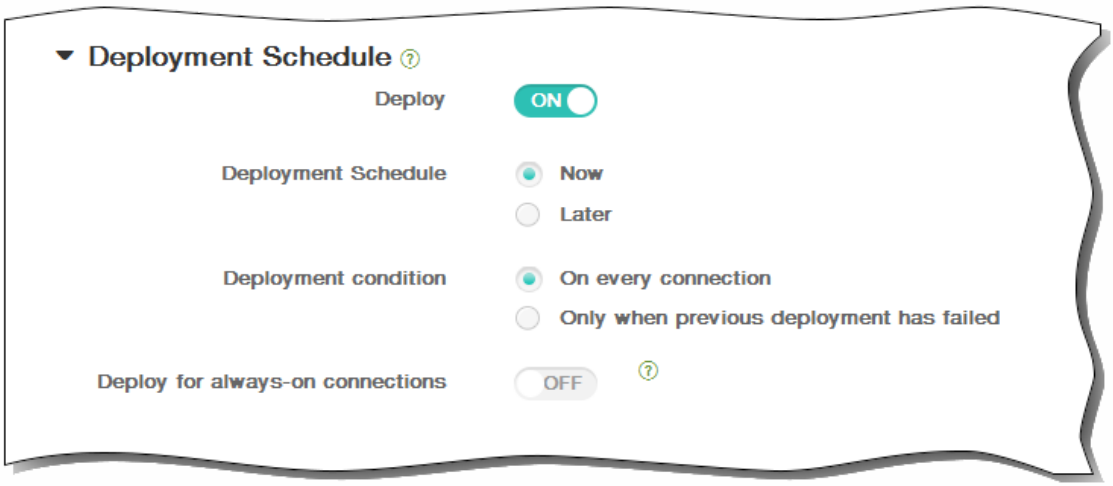
3. Forwarding route. Agregue rutas de reenvío opcionales si el servidor VPN de la empresa es compatible con varias tablas de enrutamiento.

6. Cuando termine de definir la configuración de una o varias plataformas y haga clic en Next, aparecerá la página de asignación VPN Policy.
7. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



8. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
   1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
   2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
   3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
   4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
   5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
      Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

   Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



9. Haga clic en Save para guardar la directiva.

Directivas WiFi de dispositivos

May 05, 2016

En XenMobile, puede crear o modificar las directivas de Wi-Fi desde la página Device Policies de la consola de XenMobile. Mediante las directivas de redes Wi-Fi, puede administrar el modo en que los usuarios conectan sus dispositivos a redes inalámbricas Wi-Fi. Para ello, deberá definir los nombres y los tipos de red, las directivas de seguridad y de autenticación, si se van a usar servidores proxy, y otros datos relacionados con redes Wi-Fi de manera uniforme para todos los usuarios de las plataformas de dispositivo que seleccione.

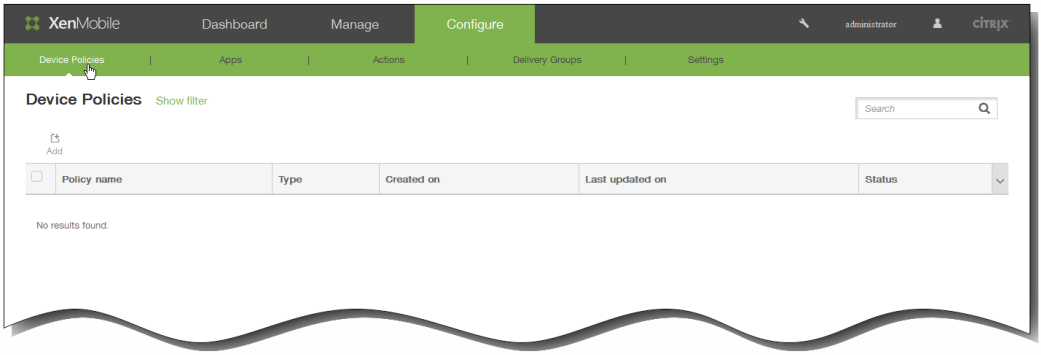
Puede configurar parámetros de red inalámbrica Wi-Fi para los usuarios de las plataformas siguientes: iOS, Android, Windows Phone 8.1 y las tabletas Windows 8.1. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Importante: Antes de crear una directiva nueva, lleve a cabo estos pasos:

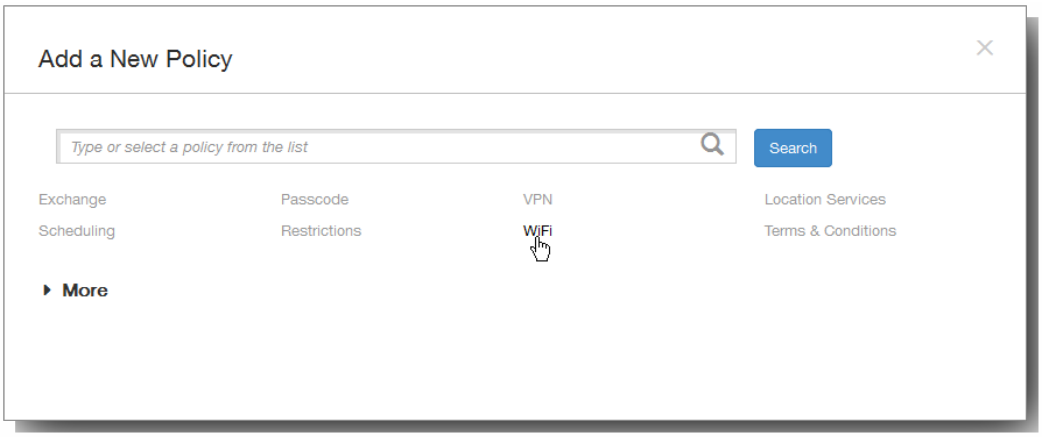
- Crear los grupos de implementación que se van a utilizar.
- Saber el nombre y el tipo de red.
- Conocer los tipos de seguridad o de autenticación que se van a utilizar.
- Conocer cualquier información del servidor proxy que pueda necesitar.
- Instalar los certificados de CA necesarios.
- Disponer de todas las claves compartidas necesarias.

Para crear una nueva directiva de redes Wi-Fi

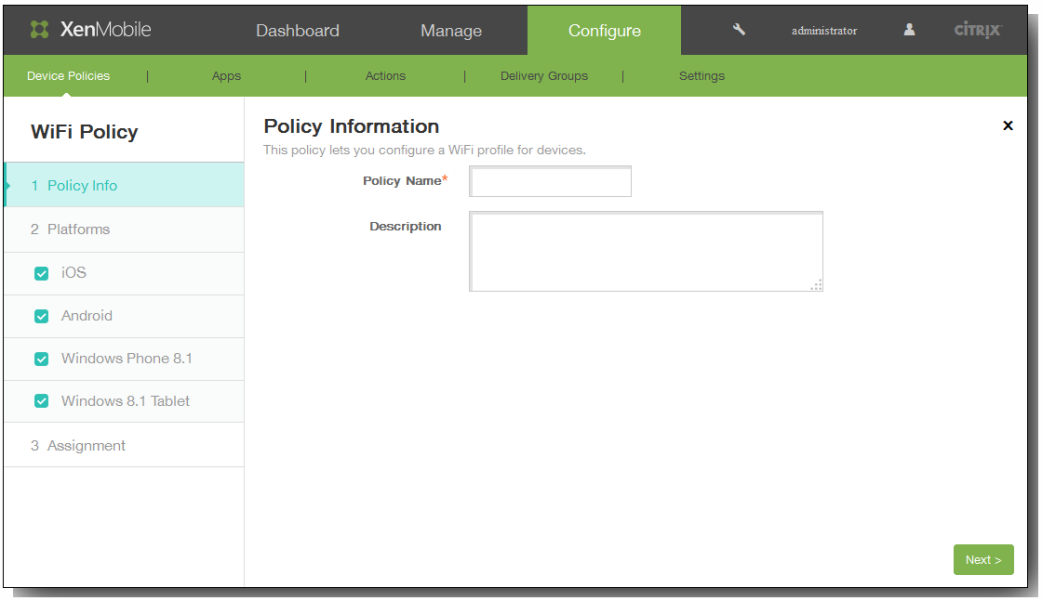
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



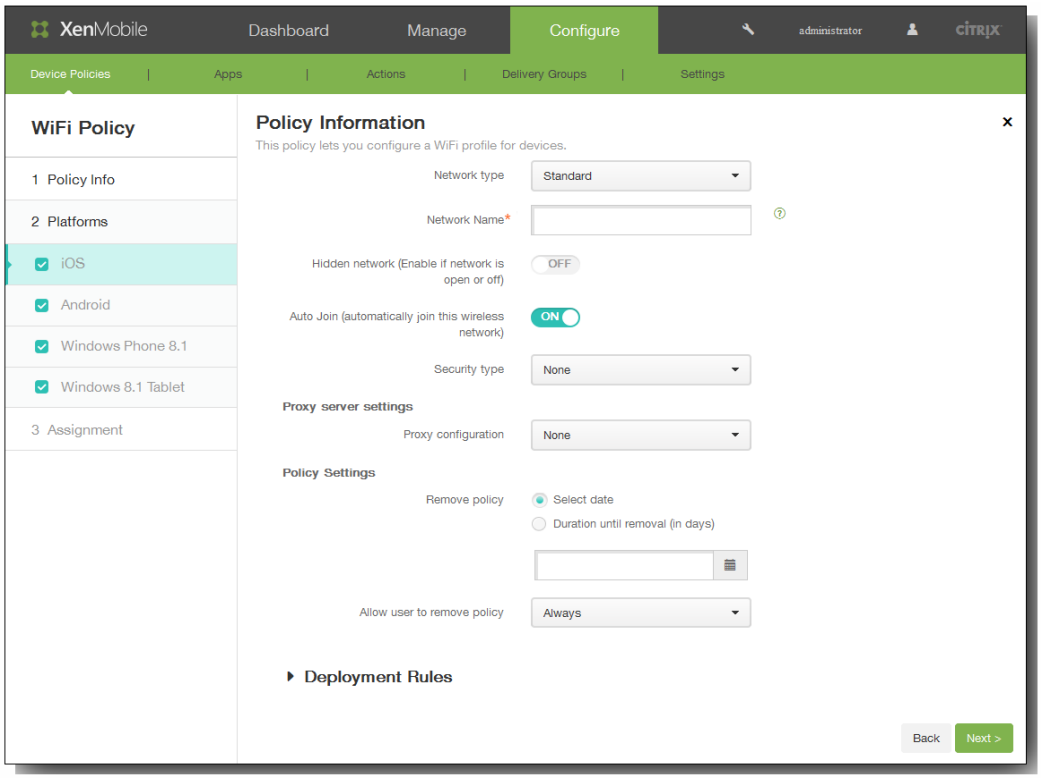
2. Haga clic en Add para agregar una nueva directiva. Aparecerá el cuadro de diálogo Add a New Policy. Haga clic en WiFi.



Aparecerá la página WiFi Policy.



3. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
   3. Haga clic en Next.
4. En Platforms, seleccione la plataforma o las plataformas que quiere agregar o modificar. Borre aquellas plataformas para las que no quiere configurar la directiva.
   Si ha seleccionado iOS, configure los siguientes parámetros:



1. En la lista Network type, haga clic en el tipo de red que va a usar.
2. Si hace clic en Standard o Legacy Hotspot, escriba la información siguiente:
   1. Network Name. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo.
   2. Hidden network (enable if network is open or off). Seleccione si la red está oculta o no.
   3. Auto Join. Seleccione si la conexión con la red es automática.
3. Si hace clic en Hotspot 2.0, escriba la información siguiente, que aparece después de la información Security type:
   Nota: Estas opciones solo se aplican a iOS 7.0 y versiones posteriores.
   1. Displayed operator name. Escriba el nombre de operador que se va a mostrar.
   2. Domain name. Introduzca el nombre de dominio.
   3. Allow connecting to roaming partner networks. Seleccione si permitir a los dispositivos conectarse a redes asociadas móviles.
   4. Roaming Consortium Organization Identifiers (OI). Si quiere, agregue identificadores Roaming Consortium Organization Identifiers.
   5. Network Access Identifier (NAI) realm names: Si quiere, agregue nombres de dominio kerberos NAI.
   6. Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs): Si quiere, agregue códigos MCC y configuraciones MNC.
4. Security type. En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
   - Ninguno.
   - WEP
   - WPA o WPA2 Personal
   - Cualquiera (Personal)
   - WEP Enterprise
   - WPA/WPA2 Enterprise
   - Cualquiera (Enterprise)

   En la siguiente tabla aparecen las opciones a configurar para cada uno de los tipos de conexión mencionados. Cada

celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

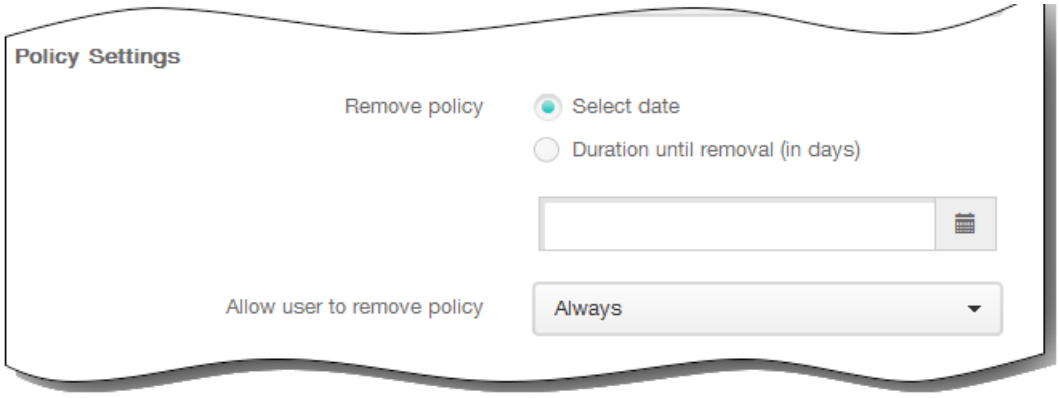
	Ninguno.	**WEP**	**WPA o WPA2 Personal**	**Cualquiera (Personal)**	**WEP Enterprise**	**WPA/WPA2 Enterprise**	**Cualquiera (Enterprise)**
Contraseña	–	Opcional	Opcional	Opcional	–	–	–
TLS	–	–	–	–	OFF	OFF	OFF
TTLS	–	–	–	–	OFF	OFF	OFF
LEAP	–	–	–	–	OFF	OFF	OFF
PEAP	–	–	–	–	OFF	OFF	OFF
EAP-FAST	–	–	–	–	OFF	OFF	OFF
EAP-SIM	–	–	–	–	OFF	OFF	OFF
Inner authentication (TTLS)	–	–	–	–	MSCHAPv2 (si TTLS = ON)	**MSCHAPv2 (si TTLS = ON)**	MSCHAPv2 (si TTLS = ON)
Outer identity	–	–	–	–	Opcional (si PEAP, TTLS o EAP-FAST = ON)	Opcional (si PEAP, TTLS o EAP-FAST = ON)	Opcional (si PEAP, TTLS o EAP-FAST = ON)
Mediante PAC	–	–	–	–	OFF	OFF	OFF
Provisioning PAC	–	–	–	–	OFF (si Use PAC = ON)	OFF (si Use PAC = ON)	OFF (si Use PAC = ON)
Provisioning PAC anonymously	–	–	–	–	OFF (si Provisioning PAC = ON)	OFF (si Provisioning PAC = ON)	OFF (si Provisioning PAC = ON)
User name	–	–	–	–	Opcional	Opcional	Opcional
Per-connection password	–	–	–	–	OFF	OFF	OFF
Contraseña	–	–	–	–	Opcional	Opcional	Opcional

Identity credential (Keystore or PKI credential)	**Ninguno.** –	**WEP** –	**WPA o WPA2 Personal** –	**Cualquiera (Personal)** –	**WEP Enterprise** Ninguno.	**WPA/WPA2 Enterprise** Ninguno.	**Cualquiera (Enterprise)** Ninguno.
Requires a TLS certificate	–	–	–	–	OFF	OFF	OFF
Trusted certificates	–	–	–	–	Opcional	Opcional	Opcional
Trusted server certificate names	–	–	–	–	Opcional	Opcional	Opcional
Allow trust exceptions	–	–	–	–	ON	ON	ON

5. Proxy configuration. En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales.
   En la siguiente tabla se ofrece una lista de las opciones disponibles para Manual y Automatic; si no aparece nada, no requiere configuración adicional. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

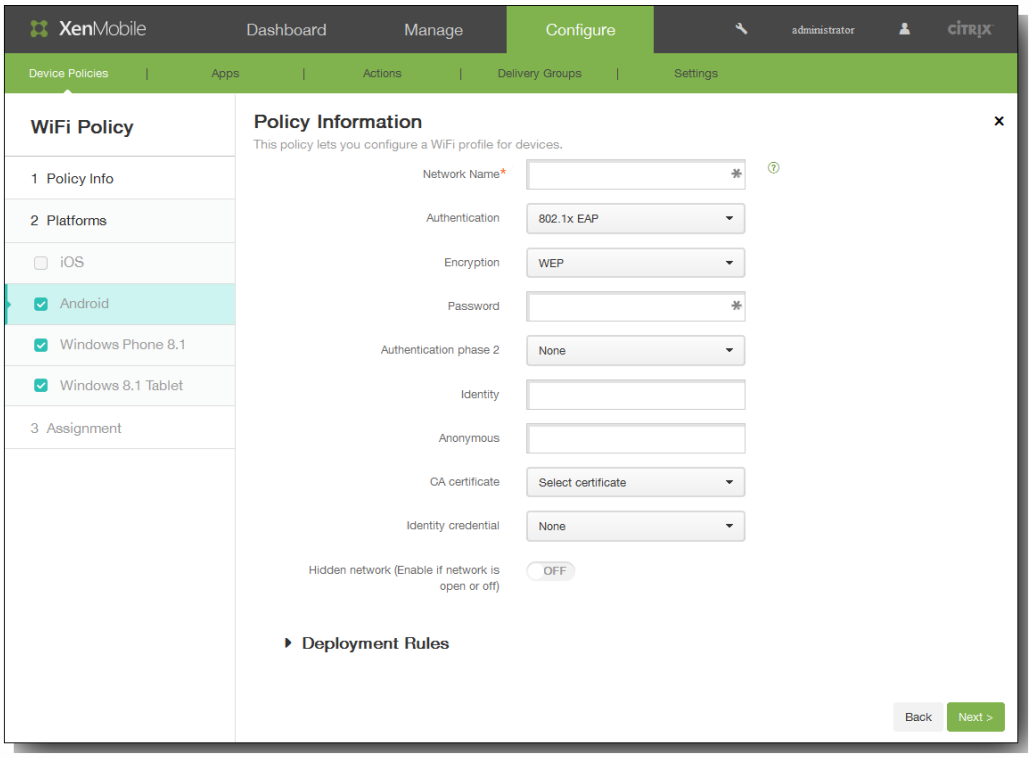
	Manual	**Automatic**
Host name or IP address for the proxy server	Requerido	–
Port for the proxy server	Requerido	–
User name	Opcional	–
Contraseña	Opcional	–
Proxy server URL	–	Requerido
Allow direct connection if PAC is unreachable	–	ON (para iOS 7.0 y versiones posteriores)

Configuraciones de directivas



1. En Policy Settings, junto a Remove policy, haga clic en Select date o Duration until removal (in days).
2. Si hace clic en Select date, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
3. En la lista Allow user to remove policy, haga clic en Always, Password required o Never.
4. Si hace clic en Password required, junto a Removal password, escriba la contraseña en cuestión.

Si ha seleccionado Android, configure los siguientes parámetros:



1. Network name. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
2. Authentication. En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
   - Abierta
   - Compartida
   - WPA
   - WPA-PSK

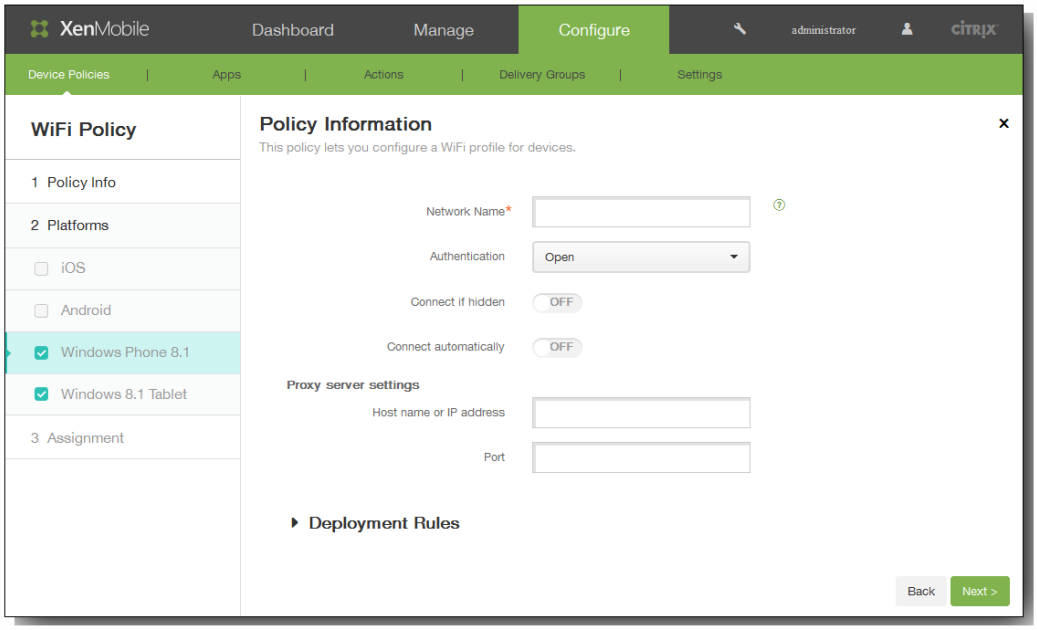
- WPA2
- WPA2-PSK
- 802.1x EAP

En la siguiente tabla aparecen las opciones a configurar para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Abierta	**Compartida**	**WPA**	**WPA-PSK**	**WPA2**	**WPA2-PSK**	**802.1 EAP**
Cifrado	WEP	WEP	TKIP	TKIP	TKIP	TKIP	–
Contraseña	Opcional	Opcional	–	–	–	–	Opcional
EAP type	–	–	–	–	–	–	PEAP
Authentication phase 2	–	–	–	–	–	–	Ninguno.
Identity	–	–	–	–	–	–	Opcional
Anónimo	–	–	–	–	–	–	Opcional
CA certificate	–	–	–	–	–	–	Selección
Identity credential	–	–	–	–	–	–	Ninguno.

3. Hidden network (Enable if network is open or off). Seleccione si la red está oculta o no.

Si ha seleccionado Windows Phone 8.1, configure los siguientes parámetros:



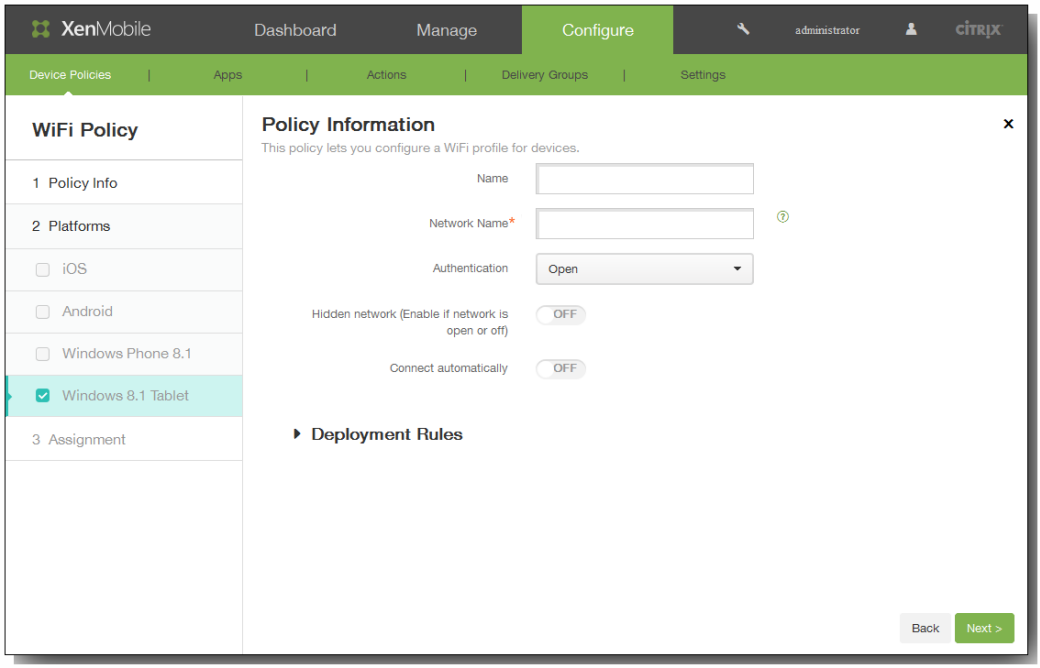
1. Network name. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
2. Authentication. En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
   - Abierta
   - WPA Personal
   - WPA-2 Personal
   - WPA-2 Enterprise

   En la siguiente tabla aparecen las opciones a configurar para cada uno de los tipos de conexión mencionados. Cada celda contiene el valor predeterminado de una opción, si existe ese valor predeterminado. Si no existe, la celda indica si la opción no se puede aplicar (–), si es necesaria o si es opcional.

	Abierta	WPA Personal	WPA-2 Personal	WPA-2 Enterprise
Cifrado	–	AES	AES	AES
Shared key	–	Opcional	Opcional	–

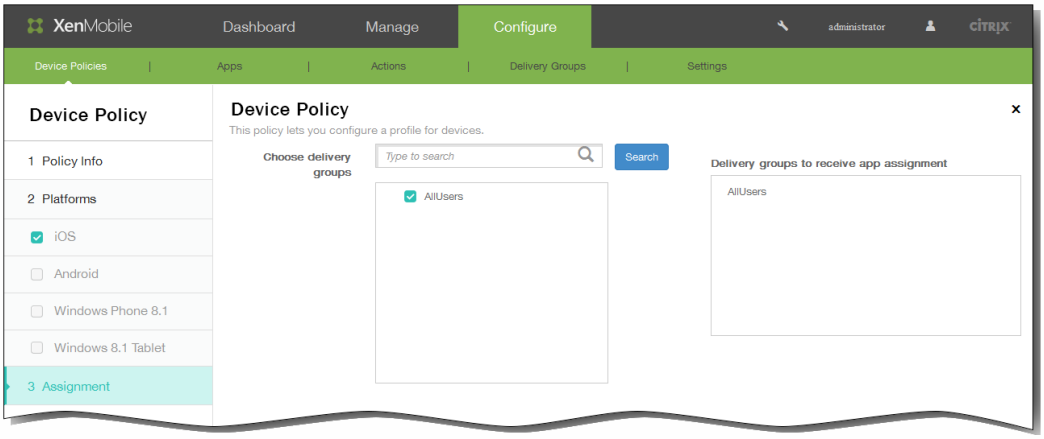
3. Connect if hidden. Seleccione si establecer conexión cuando la red esté oculta.
4. Connect automatically. Seleccione si establecer conexión con la red de forma automática.
5. Host name or IP address. Escriba el nombre o la dirección IP de un servidor proxy.
6. Port. Escriba el número de puerto del servidor proxy.

Si ha seleccionado Windows 8.1 tablet, configure los siguientes parámetros:



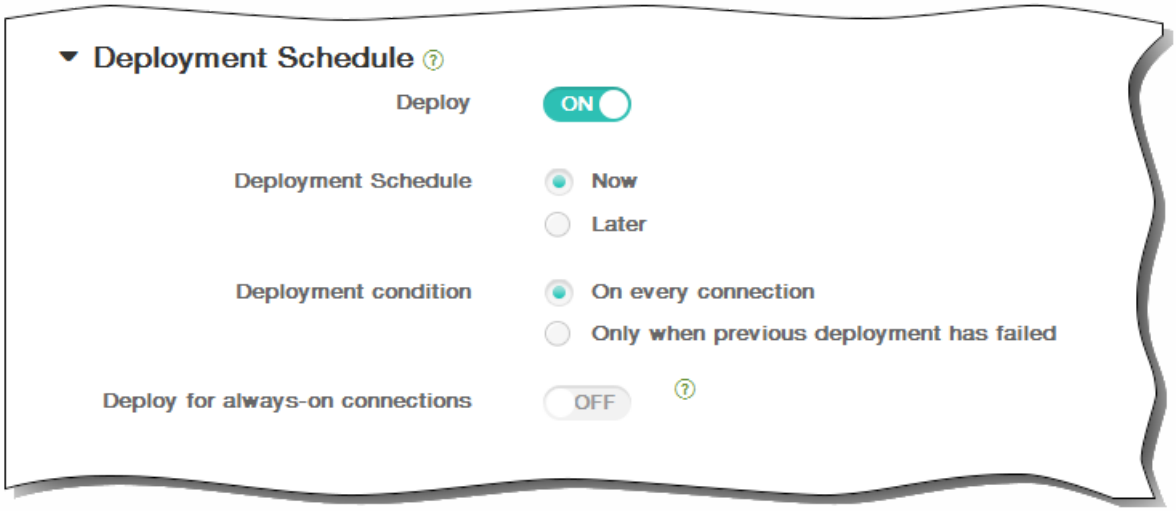
1. Name. Escriba un nombre para la red.
2. Network name. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
3. Authentication. En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
   - Abierta
   - WPA Personal
   - WPA-2 Personal
   - WPA Enterprise
   - WPA-2 Enterprise
4. Hidden network (Enable if network is open or off). Seleccione si la red está oculta o no.
5. Connect automatically. Seleccione si establecer conexión con la red de forma automática.

5. Cuando termine de definir la configuración de una o varias plataformas y haga clic en Next, aparecerá la página Assignment.
6. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



7. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
   1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
   2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
   3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
   4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
   5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
      Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

   Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



8. Haga clic en Save para guardar la directiva.

Para agregar una directiva de términos y condiciones para todas las plataformas

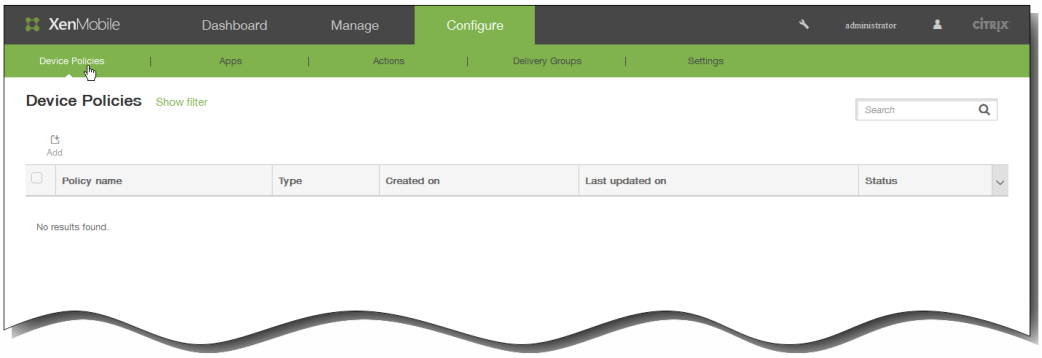
May 05, 2016

En XenMobile, puede crear directivas de términos y condiciones cuando quiera que los usuarios acepten aquellas directivas específicas de la empresa que rijan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos con XenMobile, se les presentarán los términos y las condiciones, y deberán aceptarlos para llevar a cabo la inscripción. Si rechazan dichos términos y condiciones, se cancelará el proceso de inscripción.

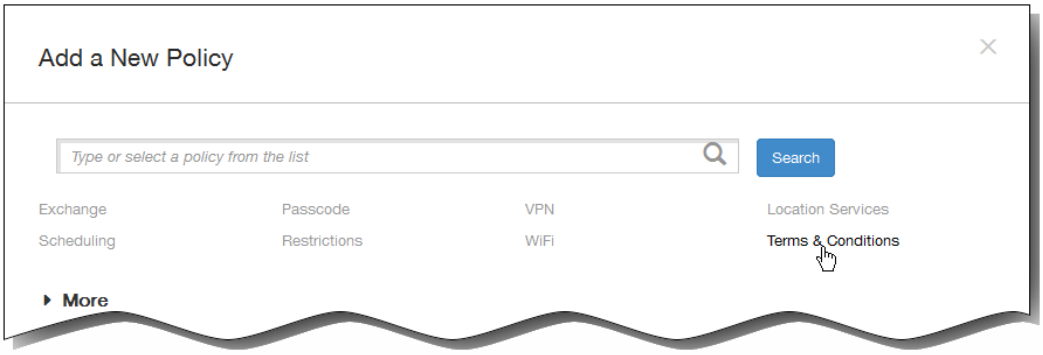
Si la empresa tiene usuarios internacionales y quiere que acepten los términos y las condiciones en su idioma nativo, puede crear directivas distintas para los términos y las condiciones en diferentes idiomas.

Nota: Los archivos de términos y condiciones deben estar en formato PDF.

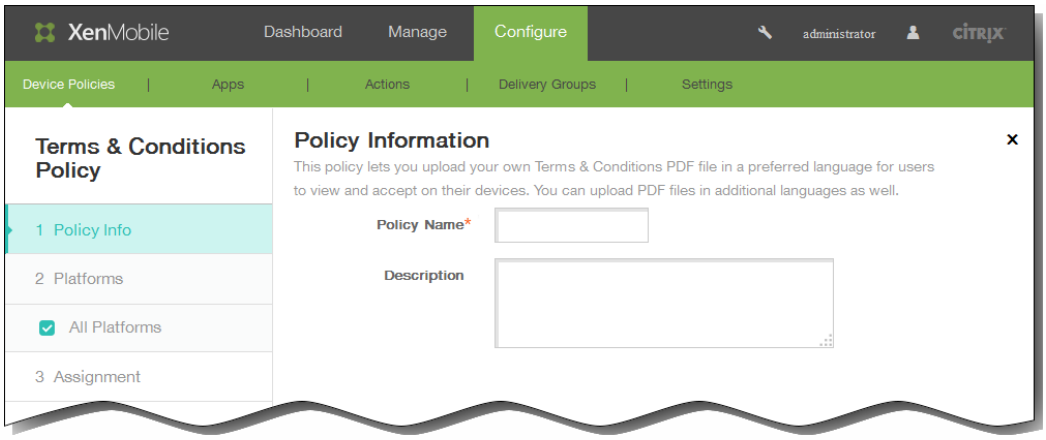
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



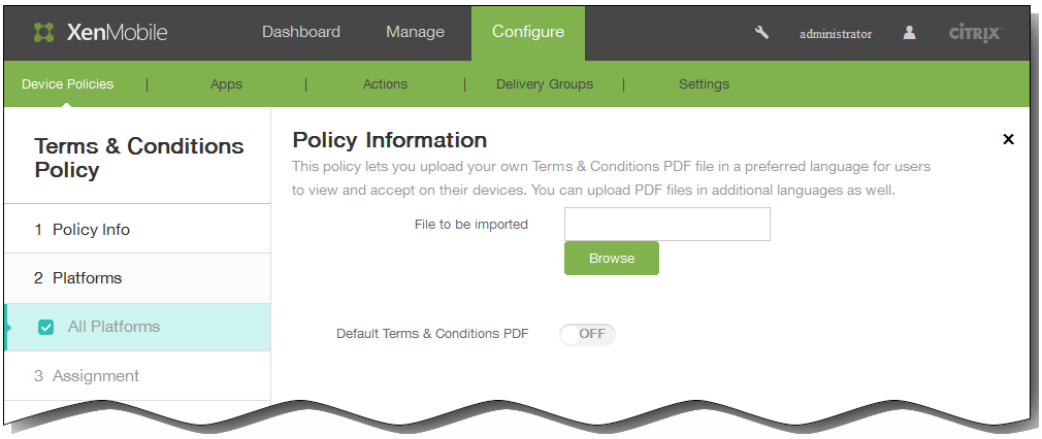
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en Terms & Conditions. Aparecerá la página Terms & Conditions Policy.

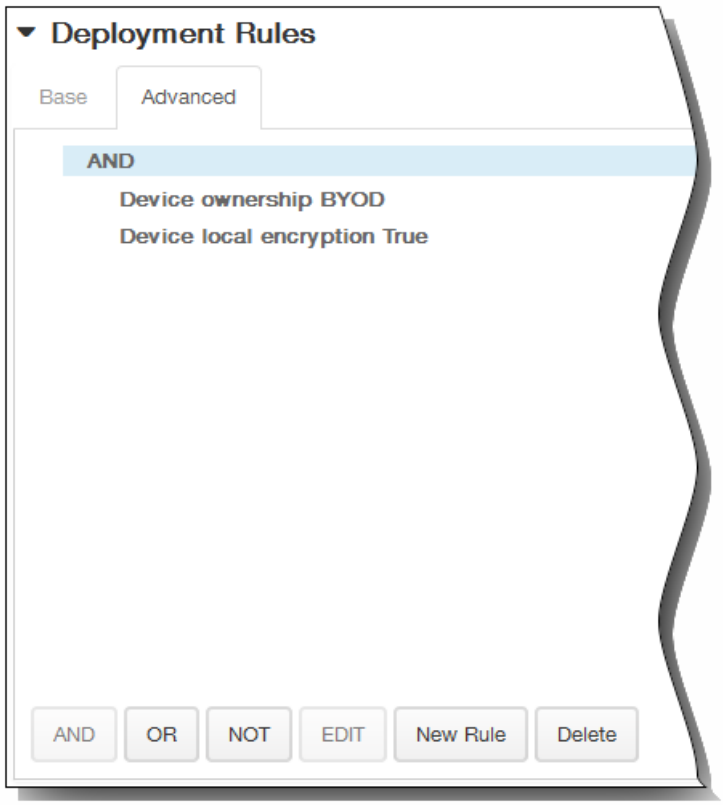


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información Android Platforms.



6. En la página de información All Platforms, escriba la información siguiente:
   1. File to be imported. Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en Browse y, a continuación, vaya a la ubicación del archivo.
   2. Default Terms & Conditions PDF. Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. El valor predeterminado es OFF.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

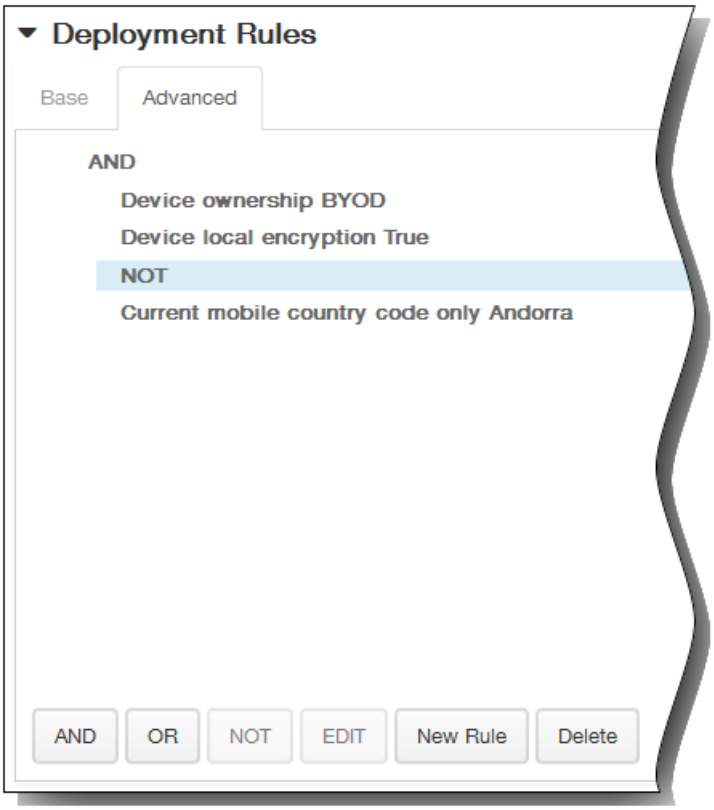
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
   1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



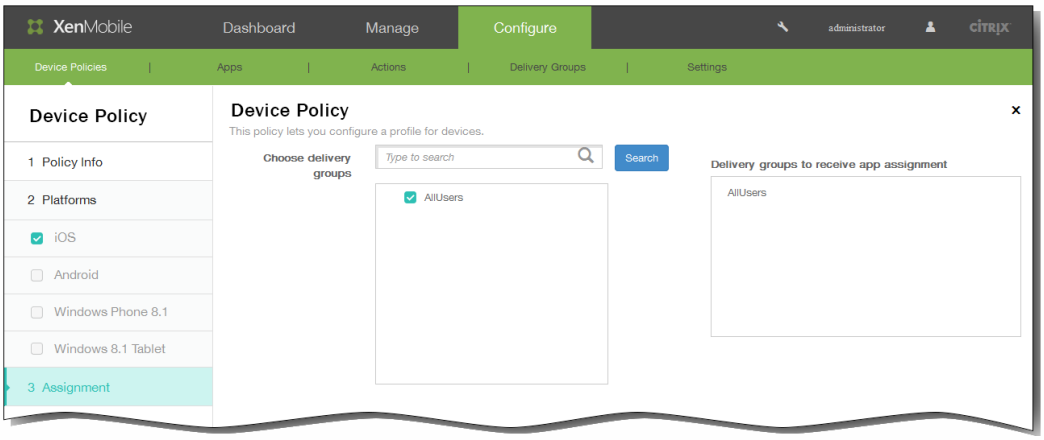
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT

o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



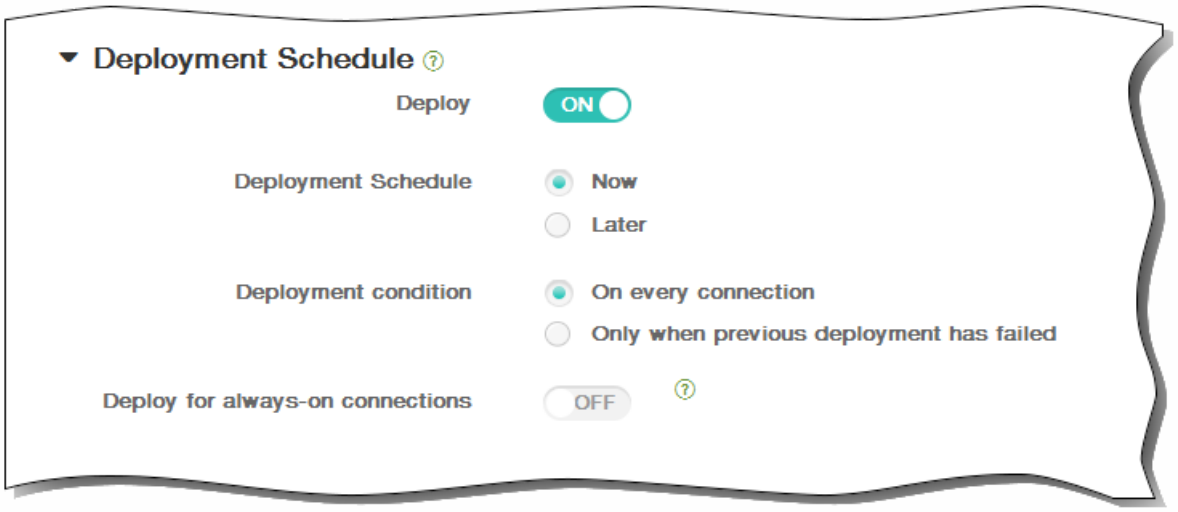
8. Haga clic en Next. Aparecerá la página de asignación Terms & Conditions Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



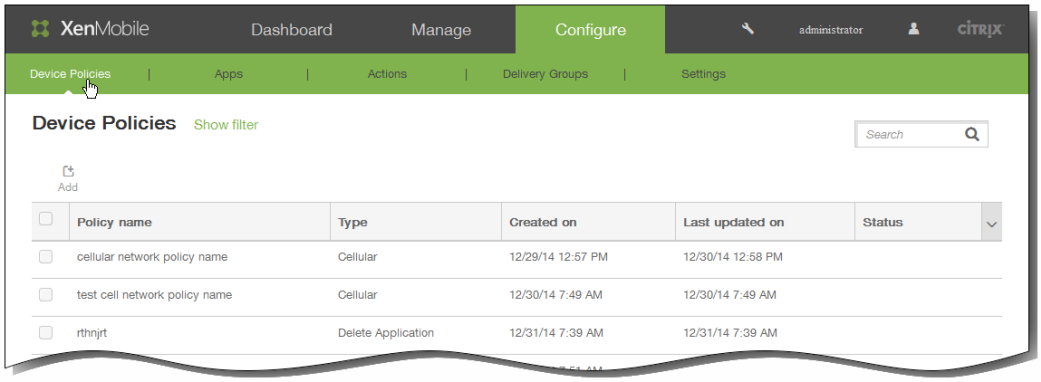
11. Haga clic en Save para guardar la directiva.

Para agregar una directiva de dispositivos de Worx Store

May 05, 2016

Esta directiva permite especificar el momento en que los dispositivos mostrarán un Web Clip vinculado a Worx Store en los dispositivos. La directiva se puede aplicar a las plataformas siguientes: iOS, Android o tabletas Windows 8.1.

1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.

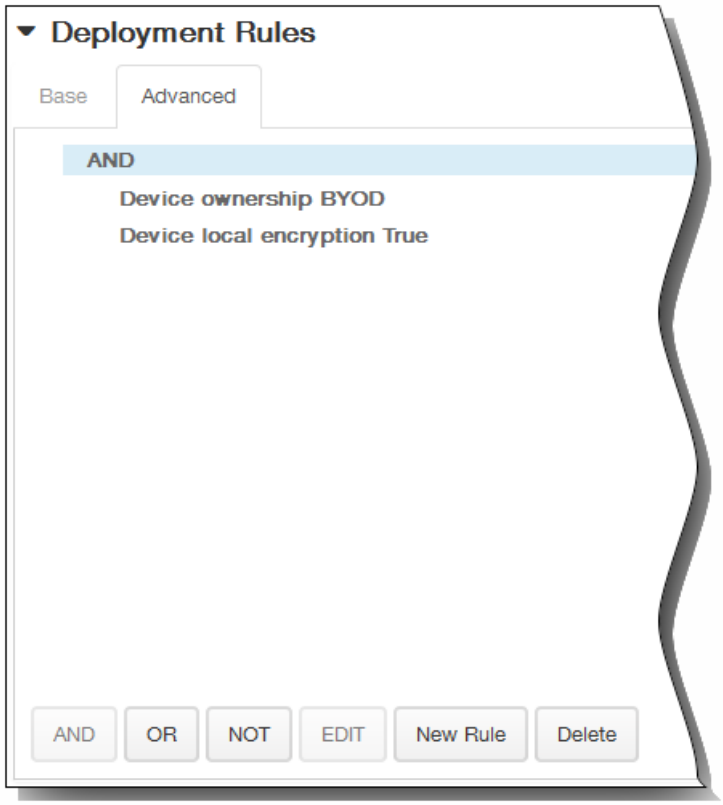


2. En la página Add a New Policy, haga clic en More > Worx Store.
3. En la página Worx Store Policy, en el panel Policy Information, escriba la información siguiente y, a continuación, haga clic en Next.
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
4. En Platforms, seleccione la plataforma o las plataformas que quiere agregar.
5. En cada plataforma que seleccione, deje el valor predeterminado ON, o bien haga clic en OFF, si no quiere que aparezca un Web Clip vinculado a Worx Store en los dispositivos.
6. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

   1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
      1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.

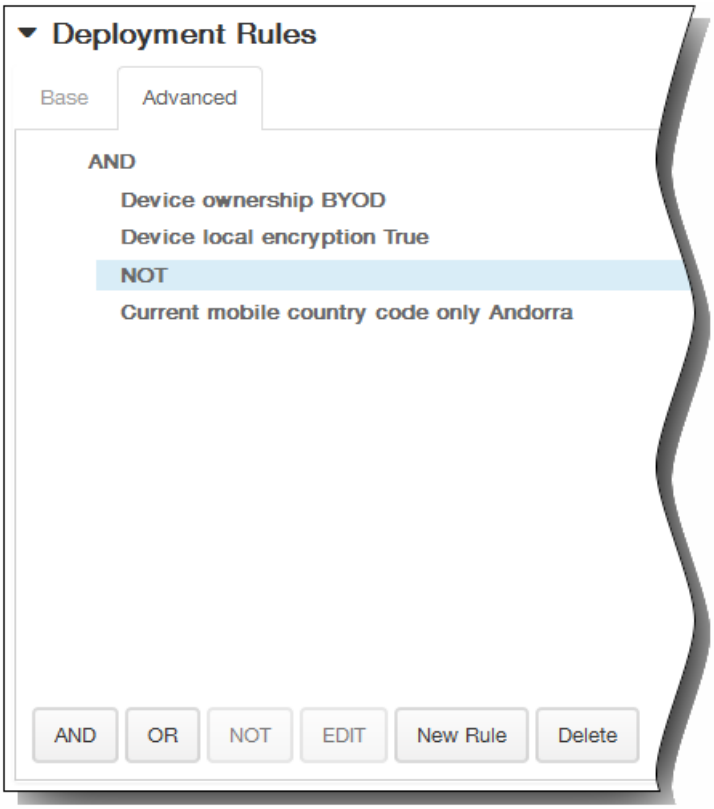
2. Haga clic en New Rule para definir las condiciones.
3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.

2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

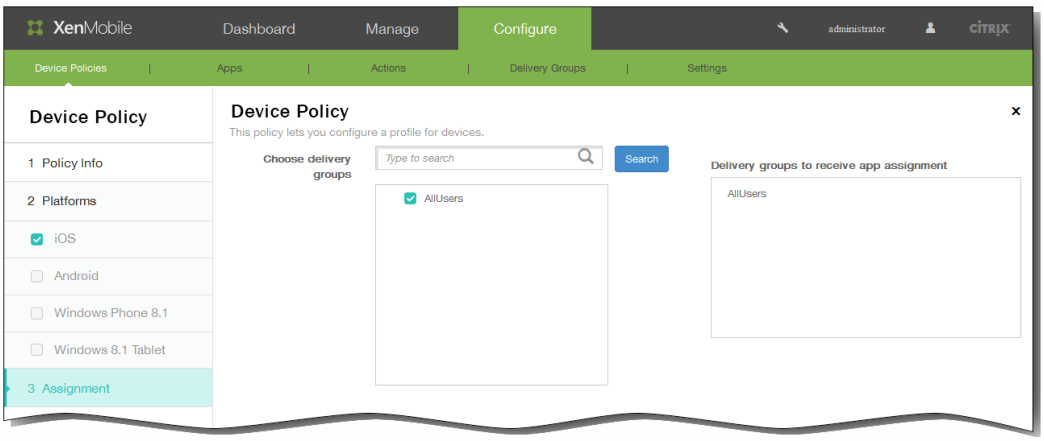


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



7. Cuando termine de definir la configuración de una o varias plataformas y haga clic en Next; aparecerá la página Assignment.
8. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.

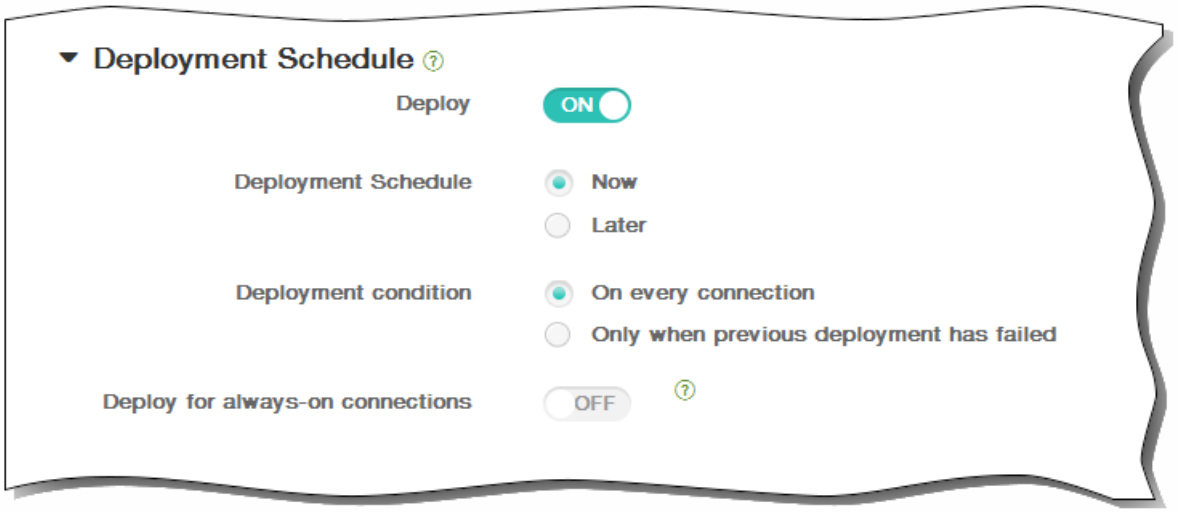


9. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la

implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



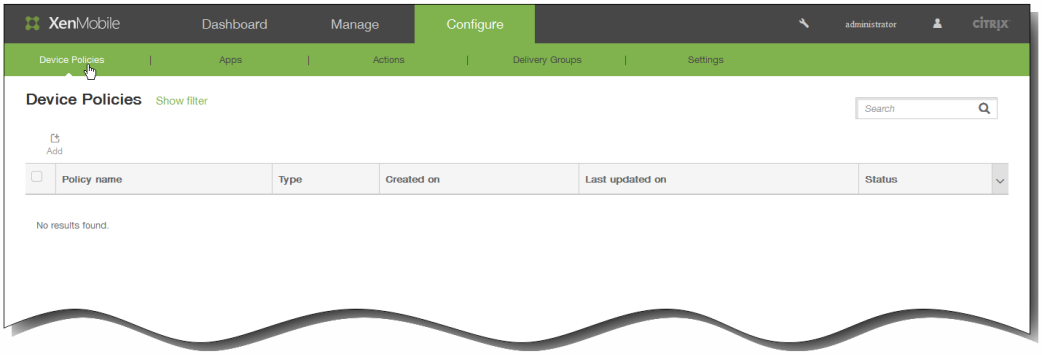
10. Haga clic en Save para guardar la directiva.

Directivas de opciones de XenMobile

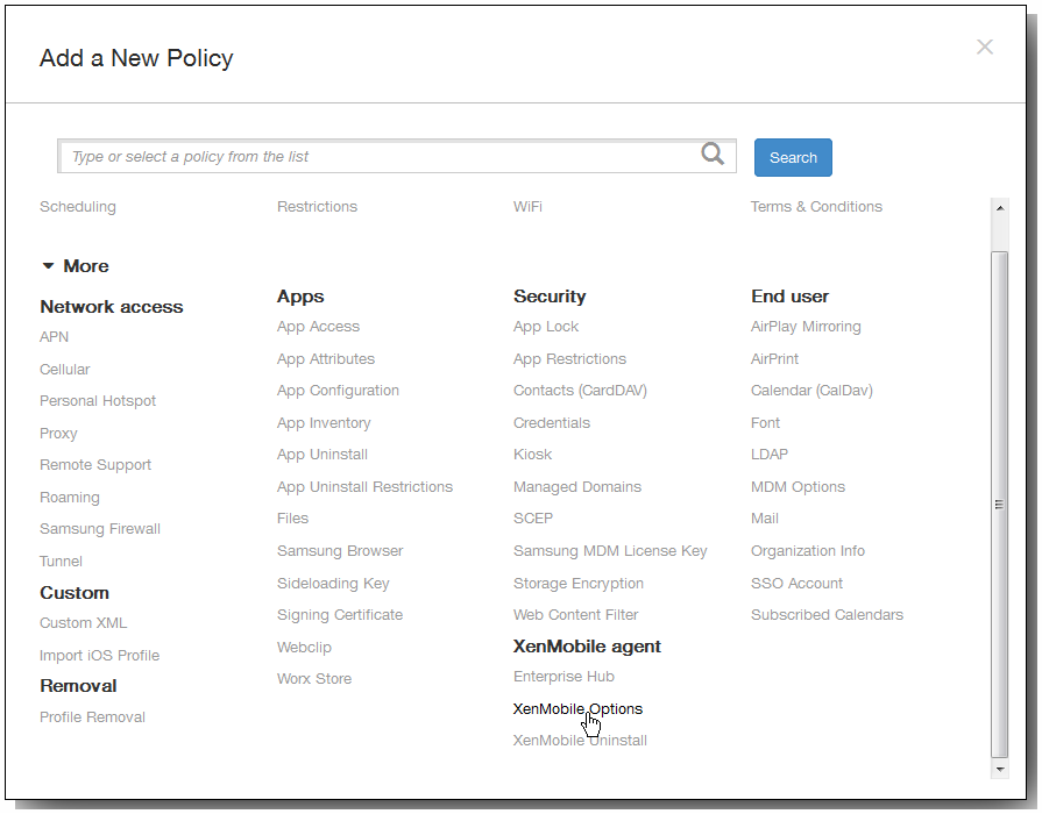
May 05, 2016

Puede agregar una directiva de opciones de XenMobile para configurar el comportamiento de Worx Home al conectarse a XenMobile desde dispositivos Android y Symbian.

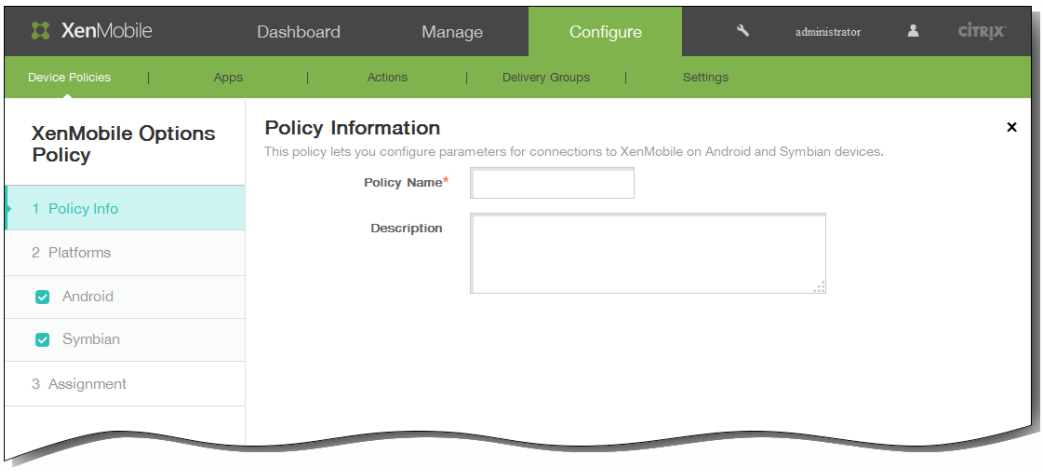
1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.



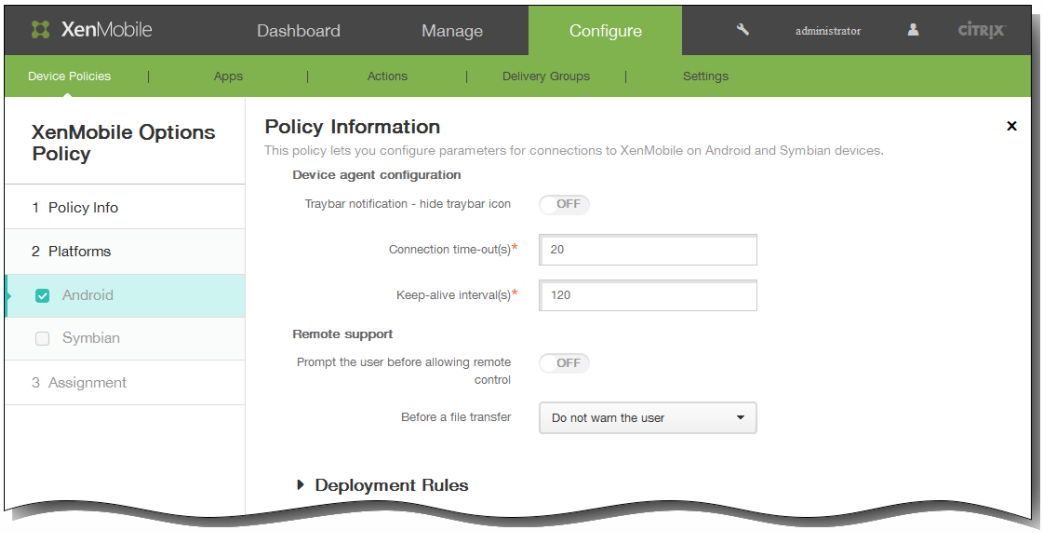
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add a New Policy.



3. Haga clic en More y, en XenMobile agent, haga clic en XenMobile Options. Aparecerá la página XenMobile Options Policy.



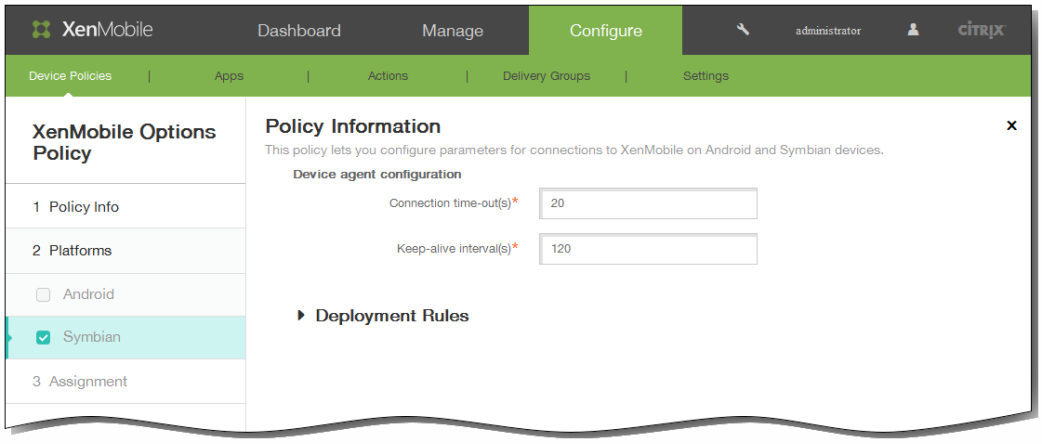
4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Escriba, si quiere, una descripción para la directiva.
   3. Haga clic en Siguiente.
5. En Platforms, seleccione la plataforma o las plataformas que quiere agregar.
   Si ha seleccionado Android, configure los siguientes parámetros:



1. Traybar notification - hide traybar icon. Seleccione si el icono de la barra de la bandeja será visible o no.
2. Connection: time-out(s). Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor predeterminado es de 20 segundos.
3. Keep-alive interval(s). Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
4. Prompt the user before allowing remote control. Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota.
5. Before a file transfer. En la lista, haga clic en si se debe avisar al usuario sobre una transferencia de archivo o si se pide

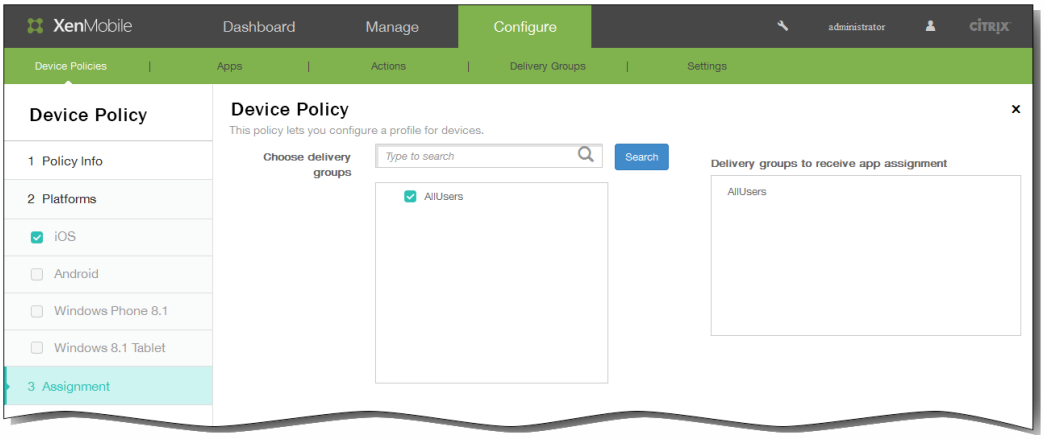
permiso al usuario.

Si ha seleccionado Symbian, configure los siguientes parámetros:



1. Connection time-outs. Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor predeterminado es de 20 segundos.
2. Keep-alive interval(s). Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.

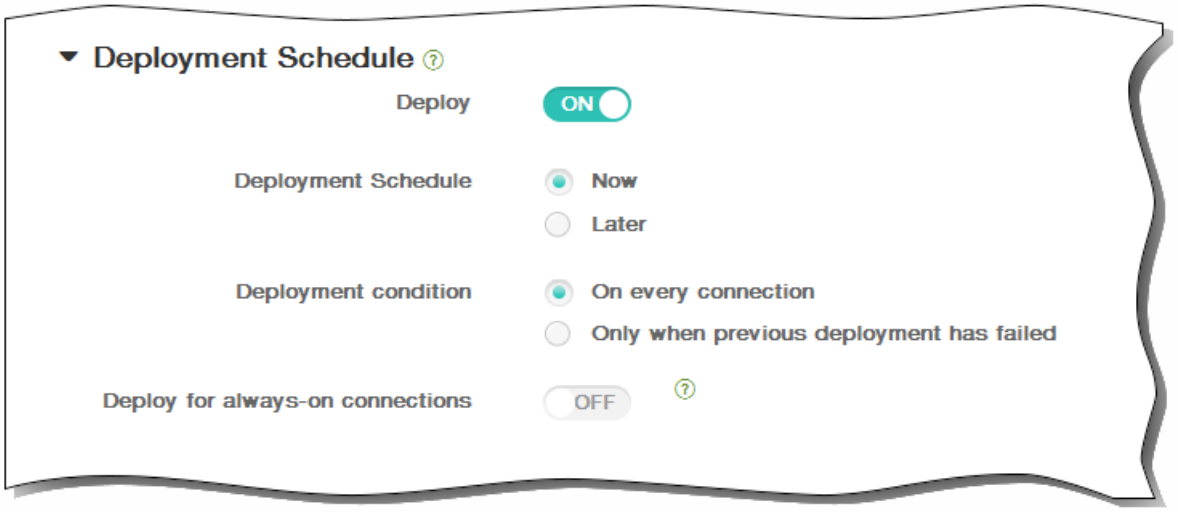
6. Cuando termine de definir la configuración de una o varias plataformas y haga clic en Next, aparecerá la página Assignment.
7. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



8. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
   1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
   2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
   3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



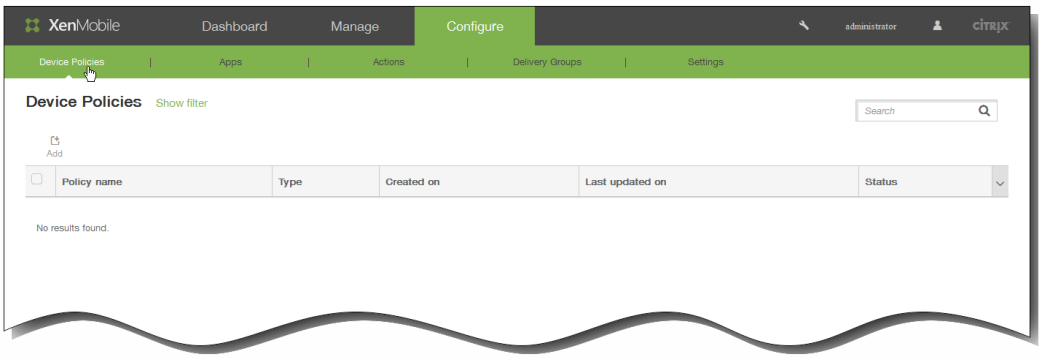
9. Haga clic en Save para guardar la directiva.

Para agregar una directiva de desinstalación de XenMobile para dispositivos Android

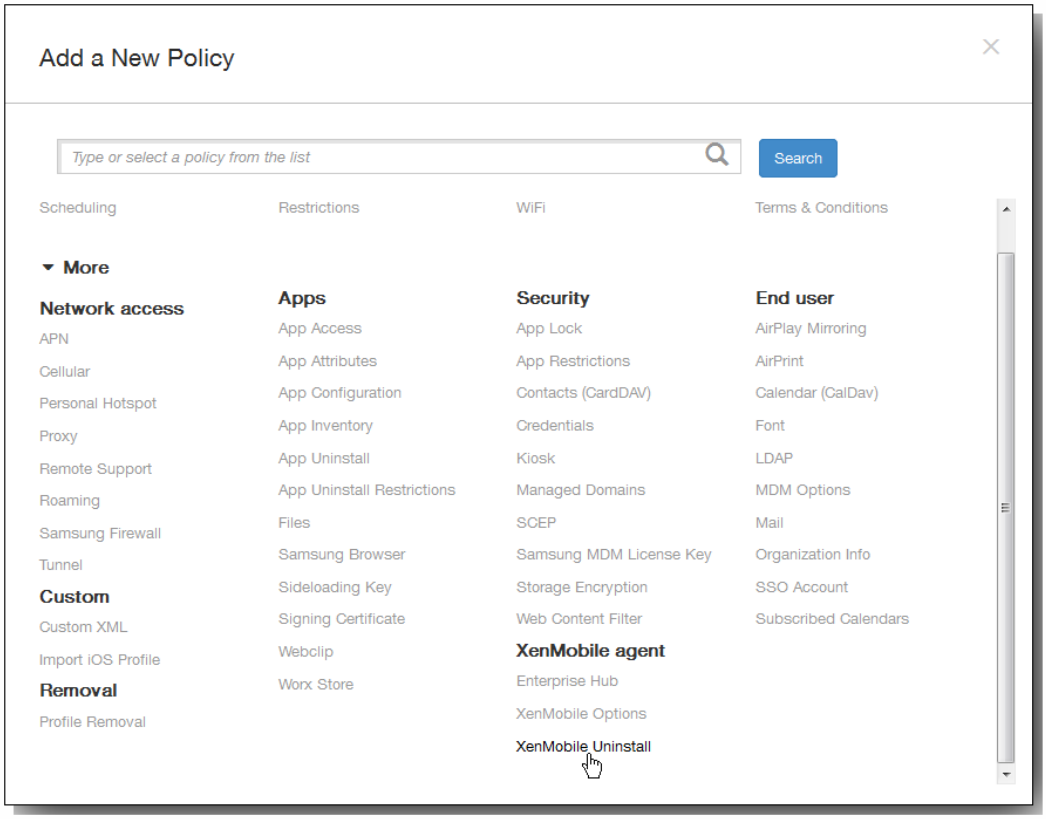
May 05, 2016

En XenMobile, puede agregar una directiva de dispositivos para desinstalar XenMobile de dispositivos Android. Cuando se implementa, esta directiva elimina XenMobile de todos los dispositivos Android que contenga el grupo de implementación.

1. En la consola de XenMobile, haga clic en Configure > Device Policies. Aparecerá la página Device Policies.

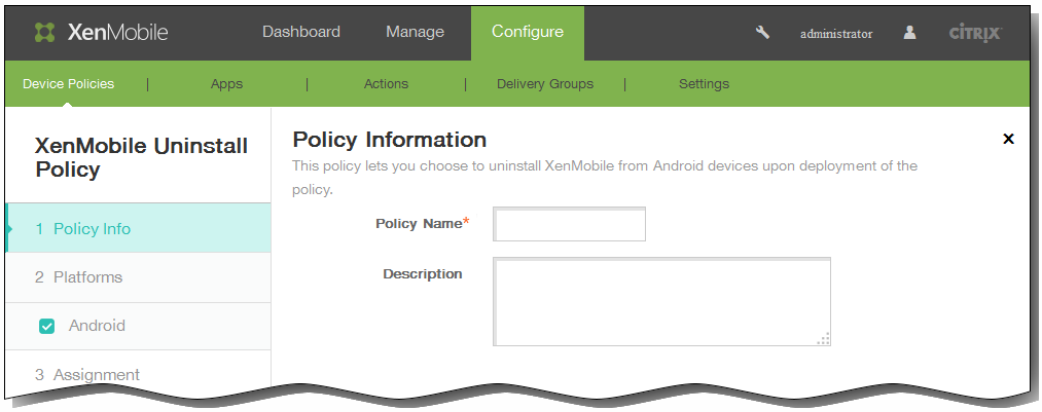


2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add a New Policy.

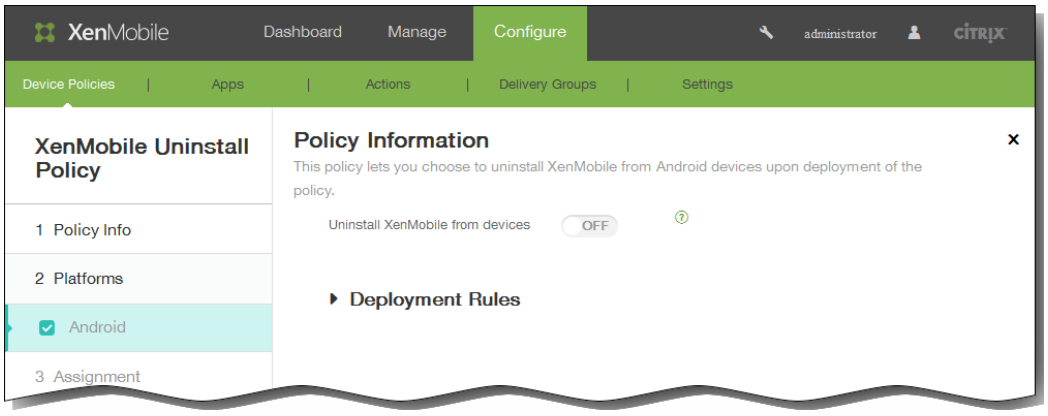


3. Haga clic en More y, en XenMobile agent, haga clic en XenMobile Uninstall. Aparecerá la página XenMobile Uninstall

Policy.

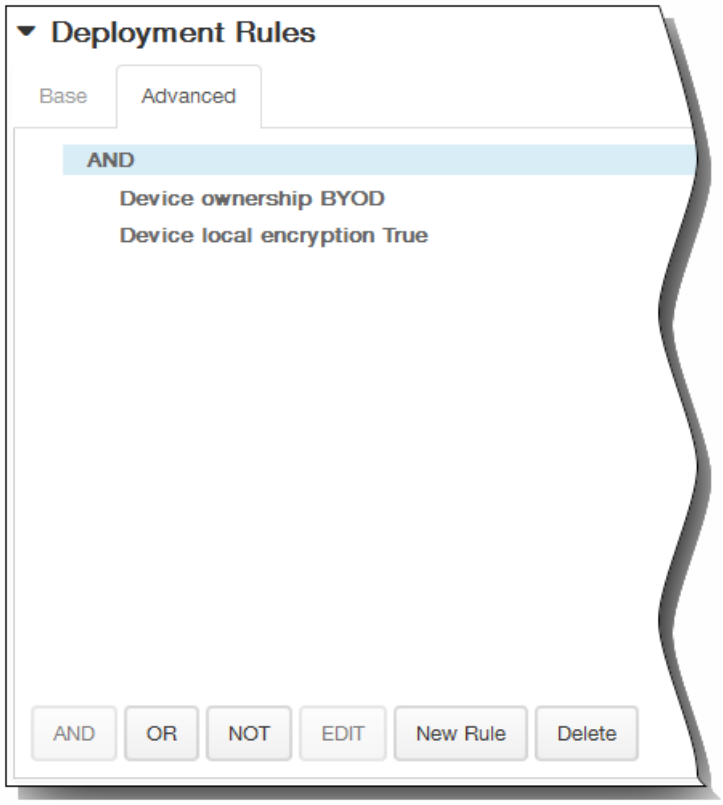


4. En el panel Policy Information, escriba la información siguiente:
   1. Policy Name. Escriba un nombre descriptivo para la directiva.
   2. Description. Si quiere, escriba una descripción de la directiva.
5. Haga clic en Next. Aparecerá la página de información Android Platform.



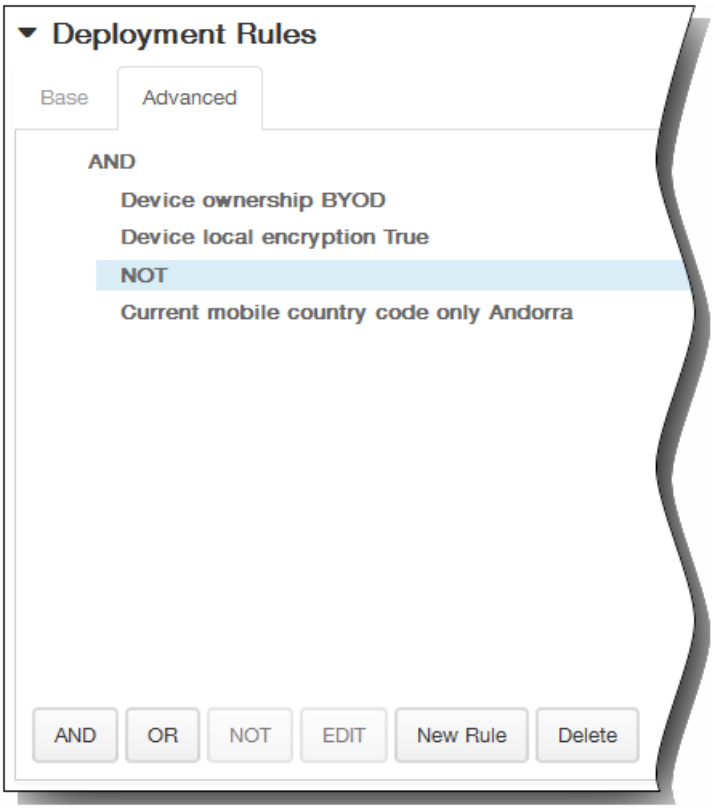
6. En la página de información Android Platform, escriba la información siguiente:
   1. Uninstall XenMobile from devices. Seleccione si desinstalar XenMobile de los dispositivos Android. El valor predeterminado es OFF.
7. Expanda Deployment Rules y, a continuación, configure los siguientes parámetros: La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva.
    1. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

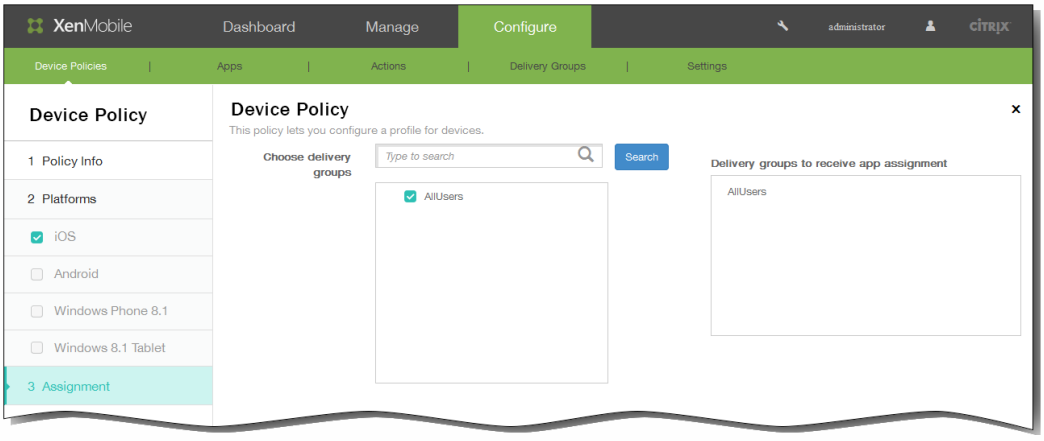


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
    1. Haga clic en AND, OR o NOT.
    2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
       En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
    3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
       En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True y el código móvil del país del dispositivo no puede ser solo Andorra.



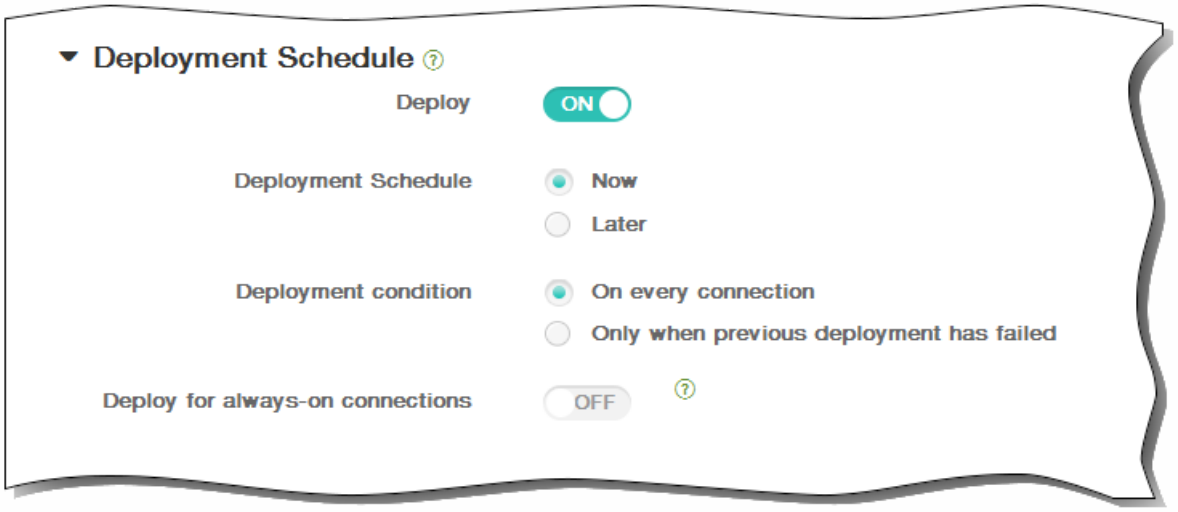
8. Haga clic en Next. Aparecerá la página de asignación XenMobile Uninstall Policy.
9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



11. Haga clic en Save para guardar la directiva.

Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

May 05, 2016

Para usar Apple Configurator, necesita un equipo de Apple con OS X 10.7.2 o una versión más reciente.

> ## Important
>
> Colocar un dispositivo en el modo supervisado instalará la versión seleccionada de iOS en el dispositivo. Con este proceso, se borran del dispositivo todos los datos de usuario o aplicaciones almacenados previamente.

1. Instale Apple Configurator desde iTunes.
2. Conecte el dispositivo iOS a su equipo de Apple.
3. Inicie Apple Configurator. Apple Configurator muestra que hay un dispositivo a preparar para la supervisión.
4. Para preparar el dispositivo para la supervisión:
    1. Cambie el control Supervision a On. Citrix recomienda elegir esta opción si quiere mantener el control del dispositivo de forma continua mediante la aplicación de una configuración con regularidad.
    2. Si lo prefiere, puede proporcionar un nombre para el dispositivo.
    3. En iOS, haga clic en Latest para ver la versión más reciente de iOS que quiera instalar.
5. Cuando esté listo para preparar el dispositivo para la supervisión, haga clic en Prepare.

Incorporación de aplicaciones

May 05, 2016

Puede agregar aplicaciones a XenMobile para administrarlas. Puede agregar aplicaciones a la consola de XenMobile, donde puede organizarlas por categorías e implementarlas para los usuarios. Siga el procedimiento descrito en este apartado para agregar categorías de aplicaciones.

Puede agregar los siguientes tipos de aplicaciones a XenMobile:

- **MDX**. Aplicaciones empaquetadas con la herramienta MDX Toolkit (y las directivas asociadas). Puede implementar las aplicaciones MDX obtenidas de almacenes internos y públicos. Por ejemplo, WorxMail.
- **Public App Store**. Estas aplicaciones incluyen aplicaciones, gratuitas o de pago, disponibles en una tienda o almacén público, como iTunes o Google Play. Por ejemplo, GoToMeeting.
- **Web and SaaS**. Estas aplicaciones incluyen aquellas a las que se puede acceder a través de una red interna (aplicaciones Web) o a través de una red pública (aplicaciones SaaS). Puede crear sus propias aplicaciones o puede elegirlas de un conjunto de conectores de aplicaciones para el acceso Single Sign-On en aplicaciones Web existentes. Por ejemplo, GoogleApps_SAML.
- **Enterprise**. Estas aplicaciones representan las aplicaciones nativas que no están empaquetadas con la herramienta MDX Toolkit y no contienen las directivas asociadas a aplicaciones MDX.
- **Web Link**. Una dirección Web (URL) a un sitio público o privado, o bien a una aplicación Web que no requiere Single Sign-On.

Funcionamiento de las aplicaciones MDX y móviles

XenMobile respalda aplicaciones iOS, Android y Windows Phone 8.x, incluidas las aplicaciones Worx (como Worx Home, WorxMail y WorxWeb) y el uso de directivas de MDX. Con la consola Web de XenMobile, puede cargar aplicaciones móviles y entregarlas a los dispositivos de usuario. Además de las aplicaciones Worx, puede agregar los siguientes tipos de aplicaciones para móvil:

- Aplicaciones que desarrolle para sus usuarios.
- Aplicaciones en las que desea permitir o restringir funciones del dispositivo mediante el uso de directivas de MDX.

Citrix ofrece la herramienta MDX Toolkit, la cual empaqueta aplicaciones para móvil para dispositivos iOS, Android y Windows Phone 8.x con las directivas y la lógica de Citrix. Esta herramienta puede empaquetar de forma segura tanto una aplicación creada dentro de la organización como una aplicación para móvil creada fuera.

Funcionamiento de las aplicaciones Web y SaaS

XenMobile viene con un conjunto de conectores de aplicaciones, que son plantillas que se pueden configurar para Single Sign-on (SSO) en aplicaciones Web y SaaS y, en algunos casos, para la creación y administración de cuentas de usuario. XenMobile incluye conectores SAML (Security Assertion Markup Language). Los conectores SAML se utilizan para aplicaciones Web que admiten el protocolo SAML para la autenticación SSO y la administración de cuentas de usuario. XenMobile es compatible con SAML 1.1 y SAML 2.0.

También puede crear sus propios conectores SAML de empresa.

Funcionamiento de las aplicaciones de empresa

En XenMobile, puede crear su propio conector de aplicaciones. Este tipo de aplicaciones residen normalmente en la red interna. Los usuarios se pueden conectar a las aplicaciones mediante Worx Home. Al agregar una aplicación de empresa, se

crea simultáneamente el conector de aplicaciones.

Funcionamiento del almacén público de aplicaciones

Puede configurar ciertos parámetros para obtener los nombres y las descripciones de las aplicaciones para móvil del App Store de Apple, de Google Play y de la Tienda Windows. Cuando recupera la información de la aplicación del almacén, XenMobile sobrescribe el nombre y la descripción existentes.

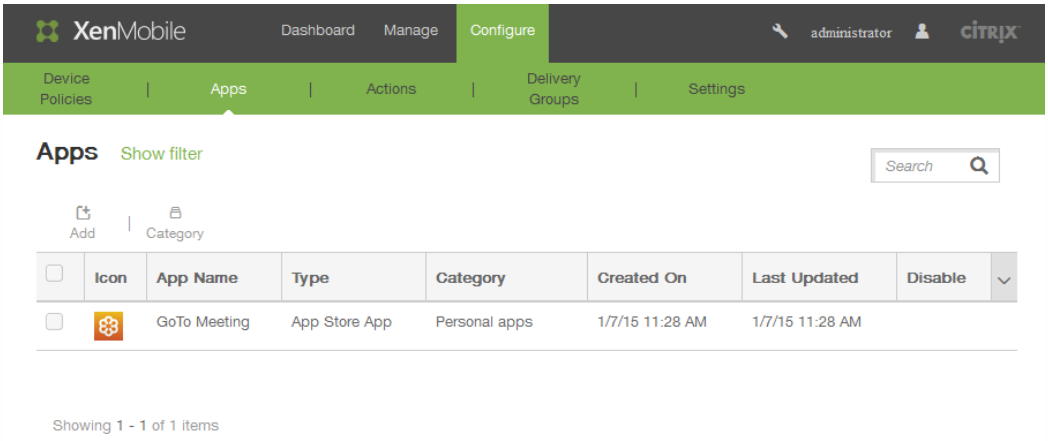
Funcionamiento de los vínculos Web

Un enlace Web es una dirección Web a un sitio de Internet o de intranet. Un enlace Web también puede apuntar a una aplicación Web que no requiere autenticación SSO. Una vez configurado el enlace Web, este aparece como un icono en Worx Store. Cuando los usuarios inician sesión en Worx Home, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Para agregar una aplicación mediante la consola, debe llevar a cabo los siguientes cuatro pasos:

- Agregar información acerca de la aplicación.
- Seleccionar y configurar la aplicación para cada plataforma respaldada, como iOS o Android.
- Definir un método de aprobación optativo.
- Configurar asignaciones optativas de grupos de entrega.

1. En la consola de XenMobile, haga clic en **Configure > Apps**.
   Aparecerá la página Apps.



   Nota: La primera vez que se conecte a la consola de XenMobile, la tabla Apps está vacía; las únicas opciones disponibles son **Add** y **Category**.
2. Haga clic en Add y siga los pasos que se describen en estos apartados de eDocs según el tipo aplicación a agregar:

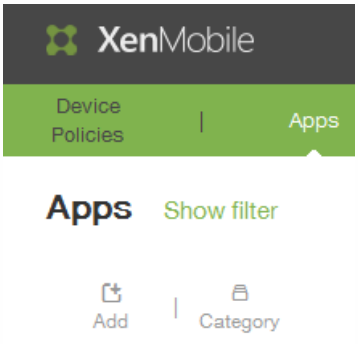
- Para agregar aplicaciones MDX a XenMobile
- Para agregar una aplicación de un almacén público de aplicaciones a XenMobile
- Para agregar aplicaciones Web y SaaS a XenMobile
- Para agregar aplicaciones de empresa a XenMobile
- Para agregar aplicaciones de enlaces Web a XenMobile

Nota: Después de agregar una aplicación, esta aparecerá en la tabla de la página Apps, donde podrá modificarla o asignarle categorías en cualquier momento.

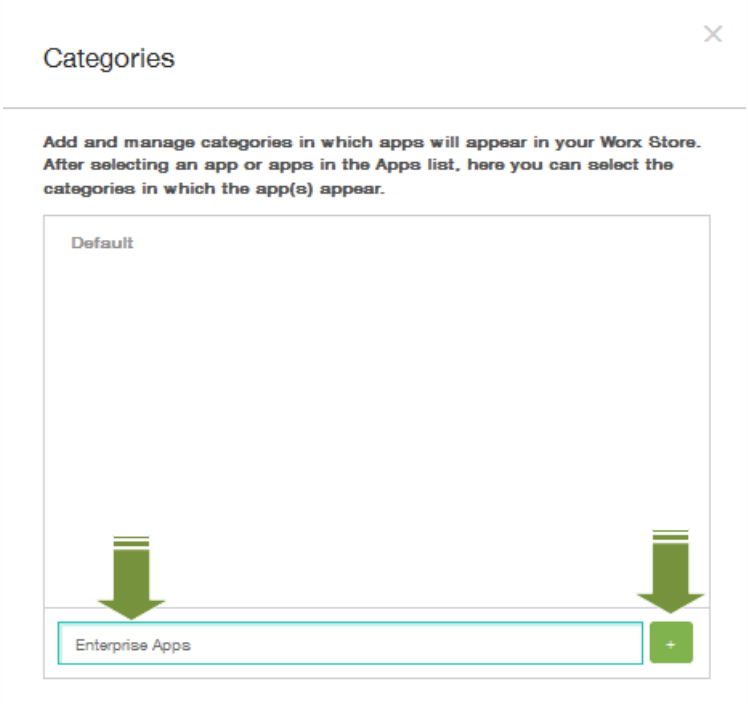
Para agregar categorías de aplicaciones

Cuando los usuarios inician sesión en Worx Home, reciben una lista de las aplicaciones, los enlaces Web y los almacenes que se hayan agregado a XenMobile y configurado en él. Puede usar las categorías de aplicaciones para permitir que los usuarios accedan únicamente a aquellas aplicaciones, almacenes o enlaces Web que quiera. Por ejemplo, puede crear una categoría llamada Finanzas y agregar a esa categoría aplicaciones que solo pertenezcan al ámbito financiero. O bien puede configurar una categoría llamada Ventas y asignarle aplicaciones de ventas. También puede configurar una categoría Apple para su App Store.
Las categorías se configuran en la página Apps de la consola de XenMobile. A continuación, al configurar o modificar una aplicación, un enlace Web o un almacén, puede agregar dicha aplicación a una de las categorías que ha configurado.

1. En la consola de XenMobile, haga clic en Configure > Apps. Aparecerá la página Apps.
2. En la página Apps, haga clic en Category.



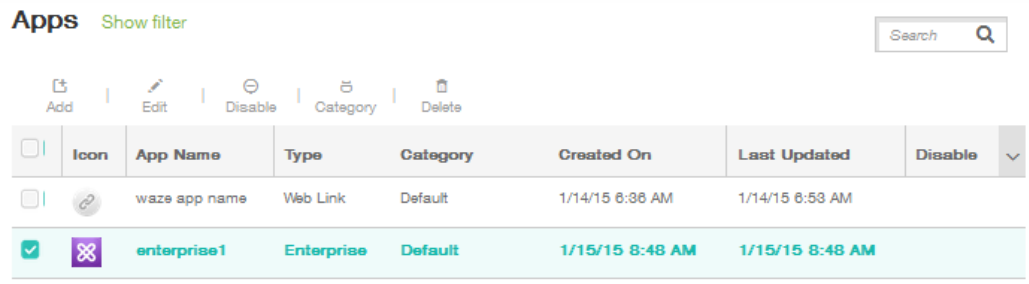
3. En el cuadro de diálogo Categories, introduzca el nombre de la categoría que quiere agregar y, a continuación, haga clic en el signo más (+). Por ejemplo, introduzca *Enterprise Apps* y haga clic en el signo más (+).



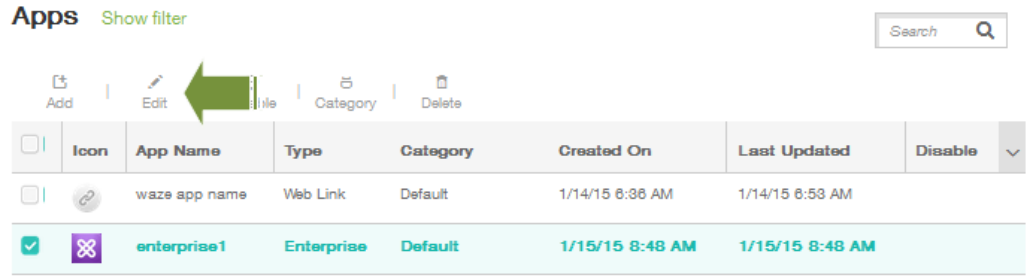
La categoría recién creada se agregará y aparecerá en el mismo cuadro de diálogo Categories. Si no hay categorías configuradas, solo aparecerá la categoría **Default**.

4. Repita el paso 3 para agregar cuantas categorías nuevas quiera y, a continuación, cierre el cuadro de diálogo Categories.
5. En la página Apps, puede vincular una aplicación existente a una categoría nueva. Seleccione la aplicación que quiera

categorizar.

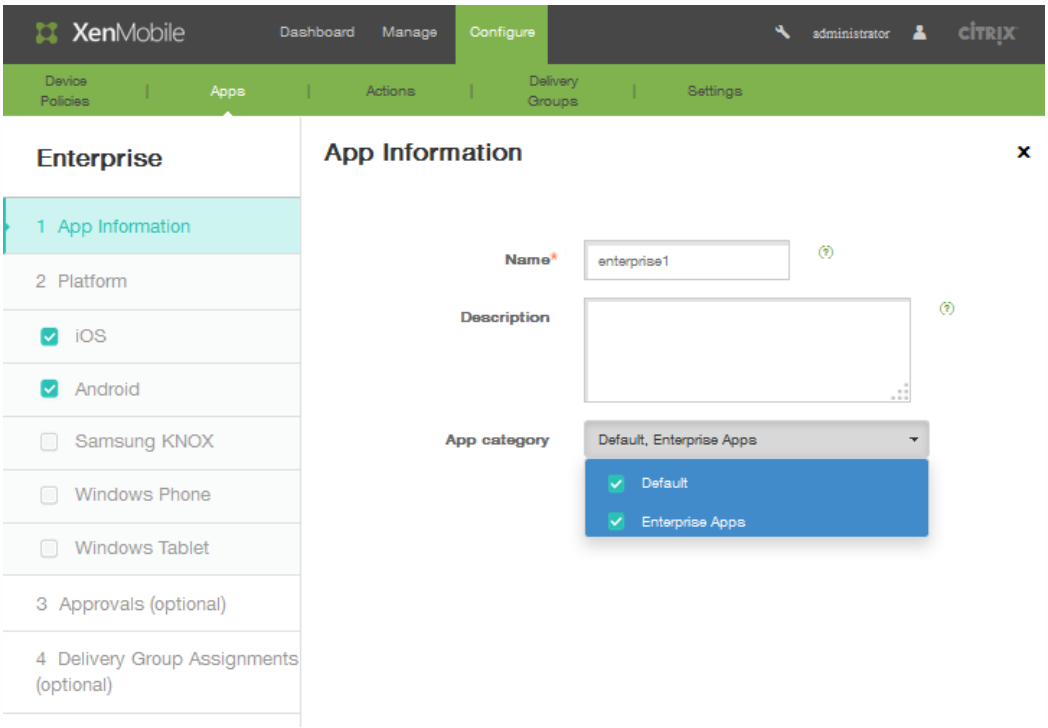


6. Haga clic en Edit para categorizar la aplicación.

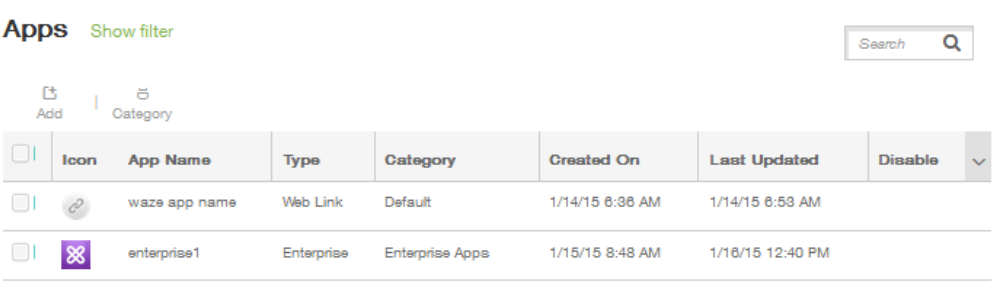


Aparecerá la página App Information.

7. En la lista App category, aplique una categoría marcando la casilla de verificación de la categoría en cuestión.



8. Haga clic en Next para desplazarse por las páginas restantes de la configuración de la aplicación.
9. En la última página, haga clic en Save para aplicar la categoría. La recién creada categoría se aplicará a la aplicación y aparecerá en la tabla Apps.

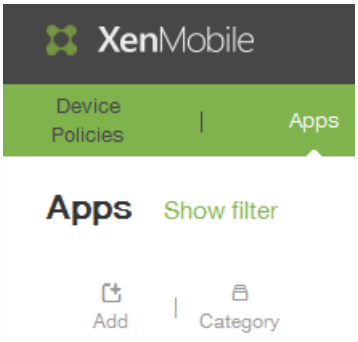


Para agregar aplicaciones MDX a XenMobile

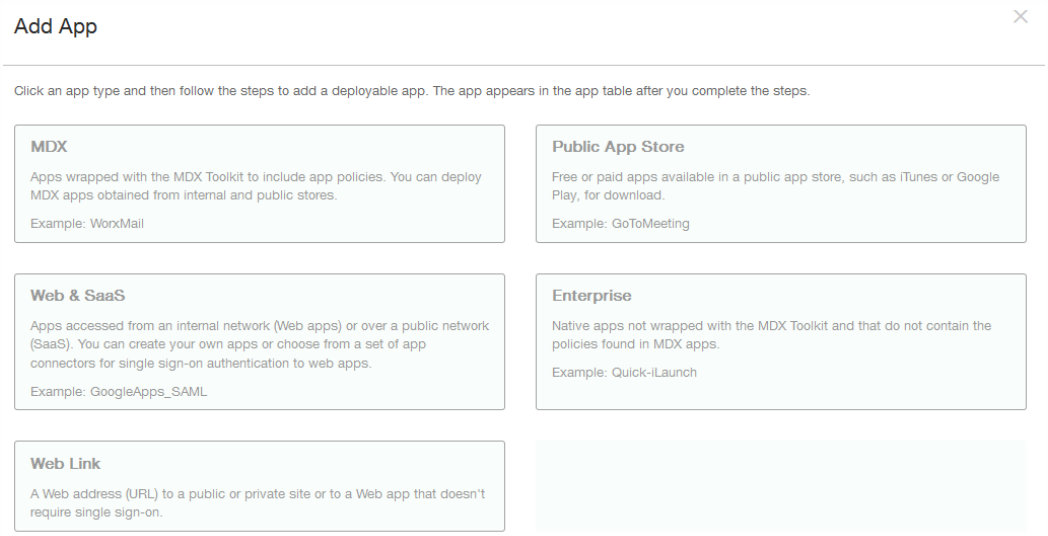
May 05, 2016

Al recibir una aplicación MDX para móvil empaquetada para un dispositivo iOS, Android o Windows Phone, puede cargarla en XenMobile. Después de cargar la aplicación, puede definir sus datos y configuraciones de directiva. Para obtener más información acerca de las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivo, consulte Directivas MDX para iOS, Android y Windows Phone. También encontrará descripciones detalladas de las directivas en esa sección.

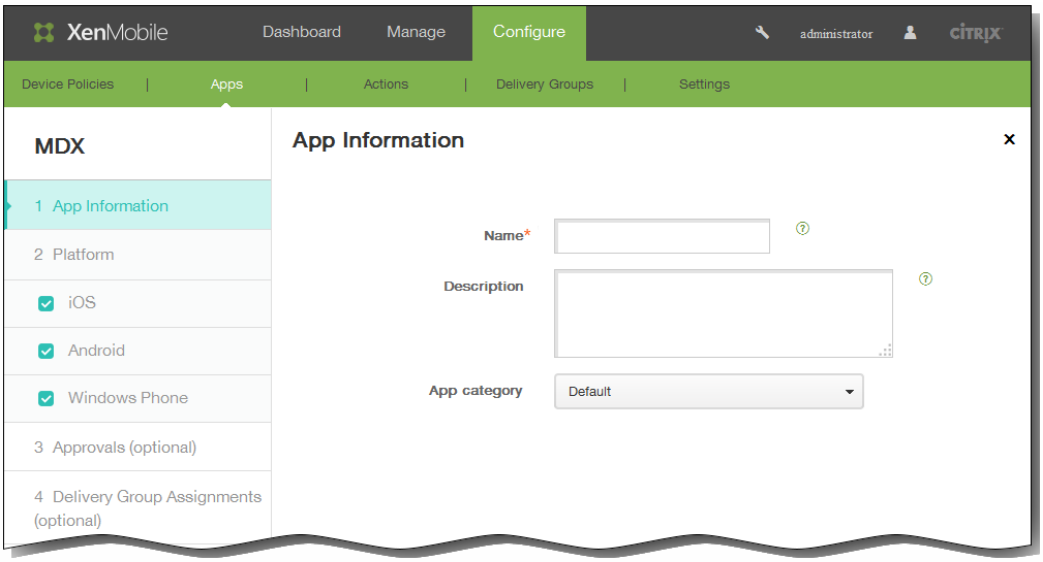
1. En la consola de XenMobile, haga clic en Configure > Apps. Aparecerá la página Apps.
2. Haga clic en Agregar.



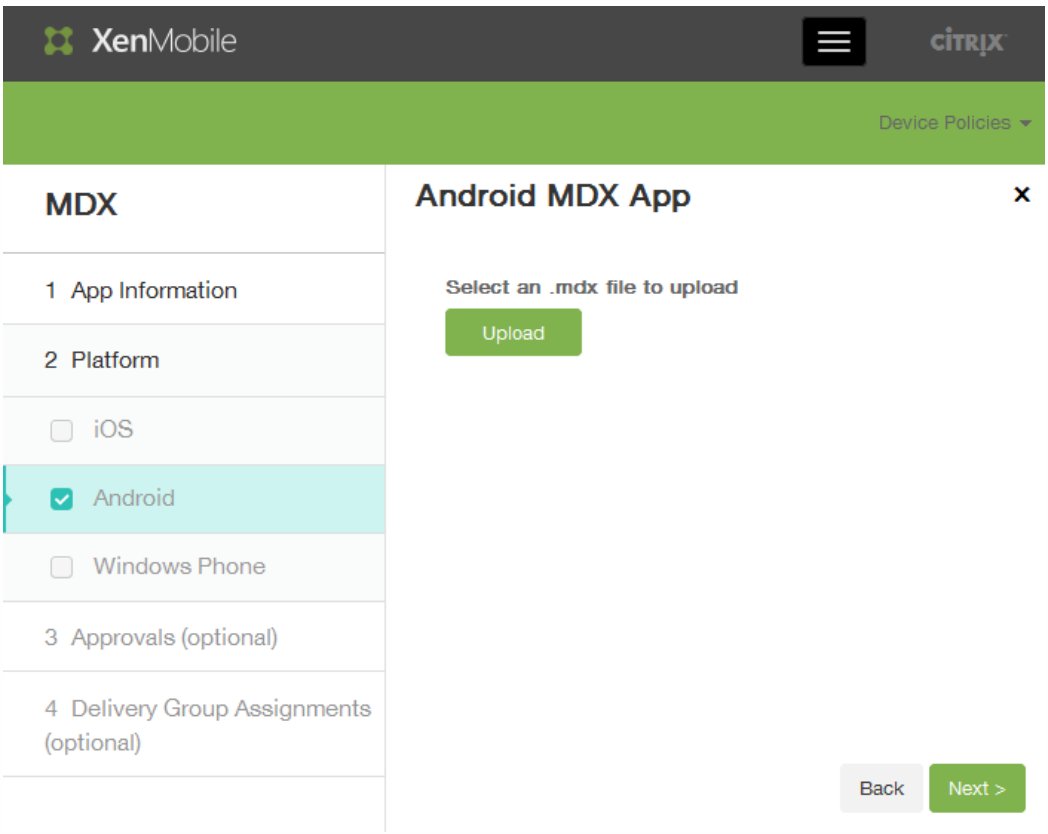
3. En la pantalla Add App, haga clic en MDX.



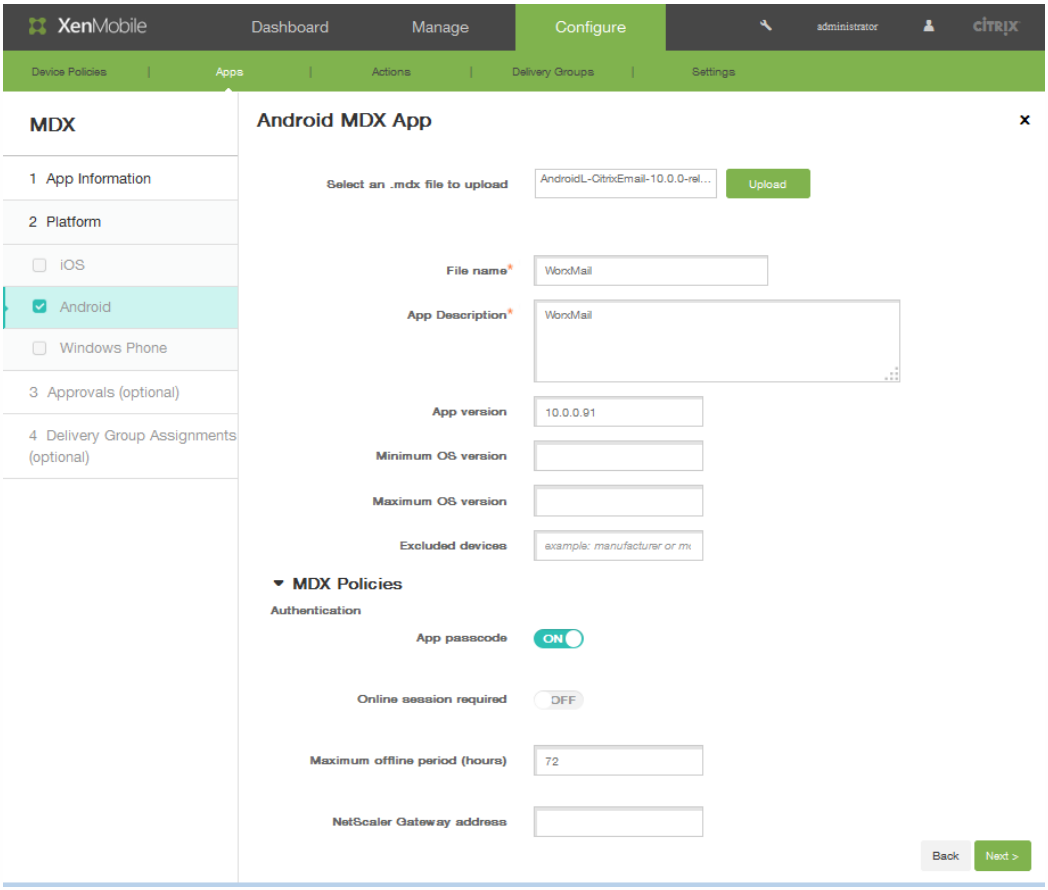
4. En la página App Information, escriba un nombre y, si quiere, una descripción de la aplicación en los campos Name y Description respectivamente. Estos campos son de uso interno. Si agrega aplicaciones para varios dispositivos, utilice las casillas situadas en la parte izquierda de la pantalla para seleccionarlos.



5. En la lista App category, haga clic en la categoría de aplicación. Consulte Para agregar una categoría para obtener información adicional.
6. Haga clic en Next.
7. Haga clic en Upload para seleccionar el archivo MDX a cargar y, a continuación, haga clic en Next.

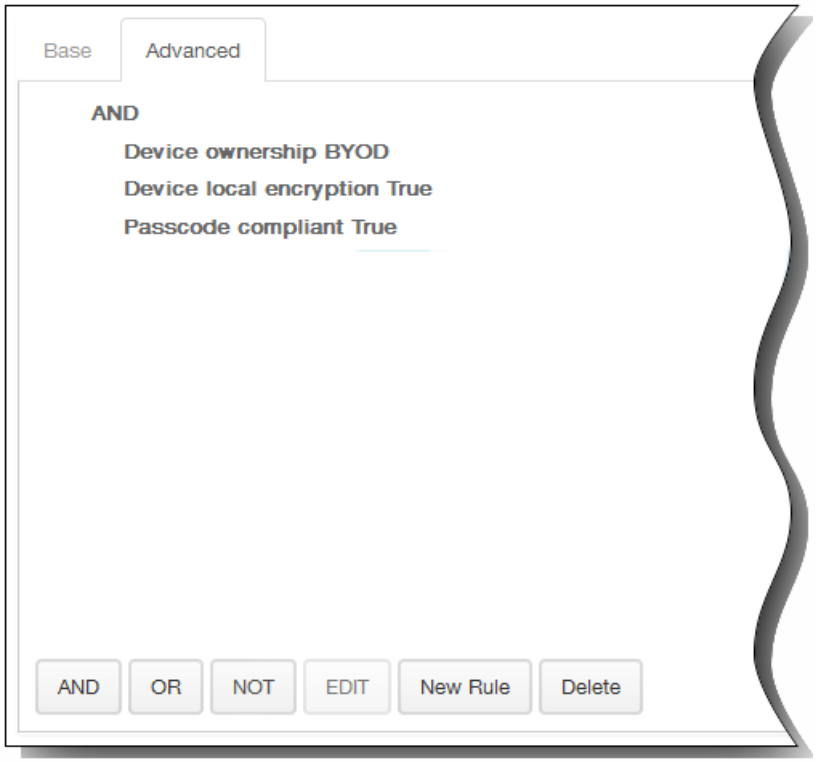


Aparecerán los campos de las directivas de MDX y los datos de la aplicación.



8. Configure los siguientes parámetros:
   1. File name. Introduzca el nombre del archivo asociado a la aplicación.
   2. App Description. Introduzca una descripción de la aplicación.
   3. Minimum OS version. Escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   4. Maximum OS version. Escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   5. Excluded devices. Escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
9. En la sección MDX Policies, defina las configuraciones de directiva que Worx Store aplicará en el área de la autenticación, la seguridad de dispositivos, los requisitos de red y acceso, el cifrado, la interacción de las aplicaciones y las restricciones de aplicaciones, entre otros.
   Nota: En la consola, puede mantener el cursor sobre el nombre de la directiva para ver su descripción. Para obtener más información sobre las directivas de aplicaciones para las aplicaciones MDX (por ejemplo, una tabla en la que se muestran las directivas que se aplican a los tipos de plataforma), consulte Directivas MDX para iOS, Android y Windows Phone.
10. Expanda Deployment Rules. La ficha Base aparece de forma predeterminada.

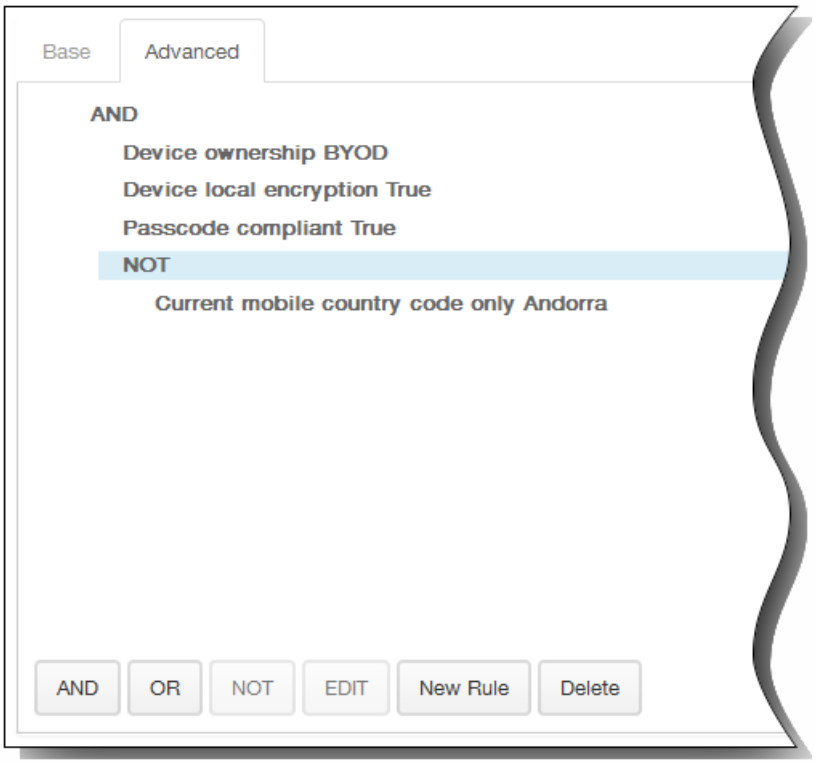
1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la aplicación.
   1. Puede optar por implementar la aplicación cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.



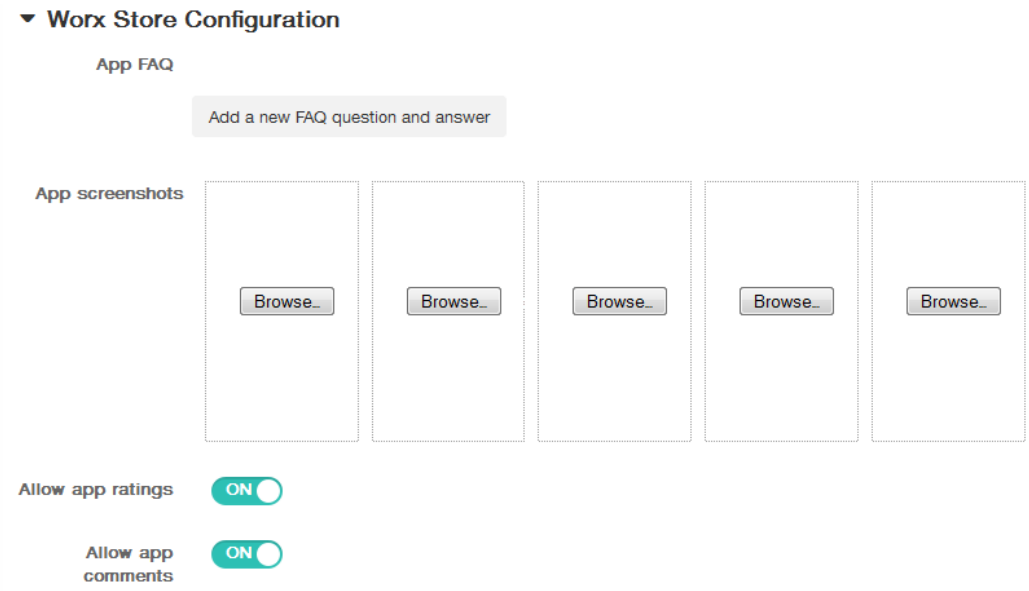
   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.

En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True, el dispositivo debe cumplir el código de acceso y el código móvil del país del dispositivo no puede ser solo Andorra.

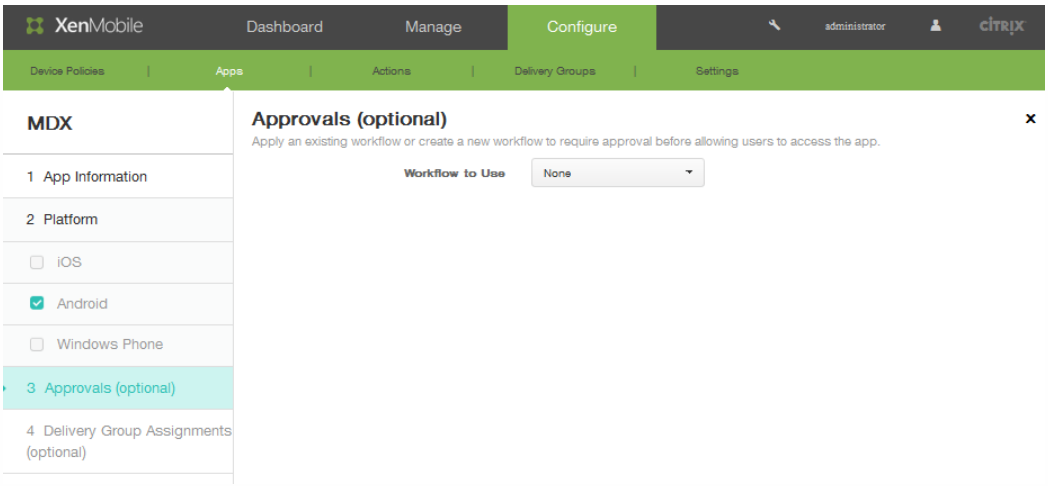


11. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.

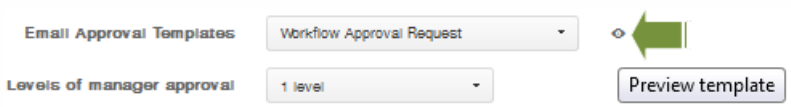


En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.

12. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.
13. Haga clic en Next. Aparecerá la pantalla Approvals.



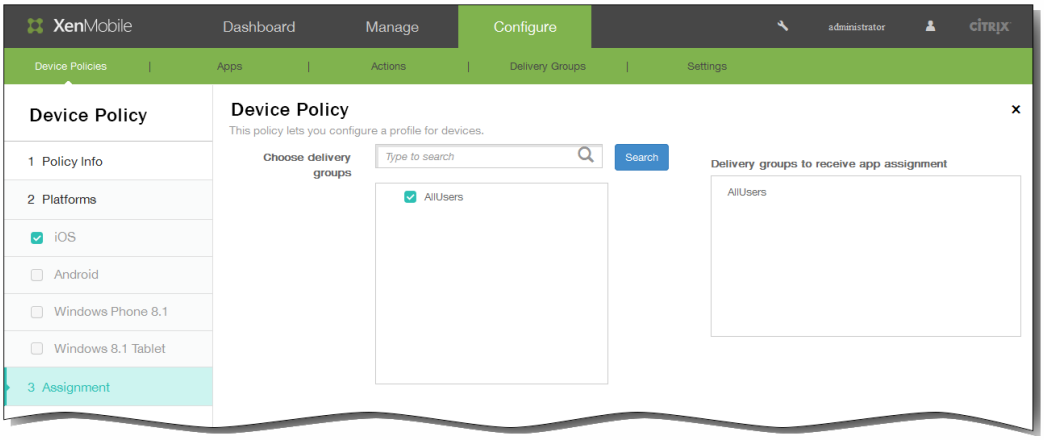
14. Al crear un nuevo flujo de trabajo, la consola de XenMobile cambia para mostrar las opciones de configuración para el proceso de aprobación. Cada uno de estos campos se describe en los pasos siguientes. Configure esos campos si necesita aprobación para crear una cuenta de usuario.
    1. Especifique un nombre en el campo **Name** para el flujo de trabajo.
    2. Si quiere, indique una descripción en **Description**.
    3. En el campo **Email Approval Templates**, haga clic en una opción de notificación. Haga clic en el **icono de vista** para una vista previa de la plantilla elegida.



    4. En **Levels of manager approval**, haga clic en el nivel pertinente; puede elegir desde None hasta 3. .
    5. En **Select Active Directory domain**, haga clic en el dominio.

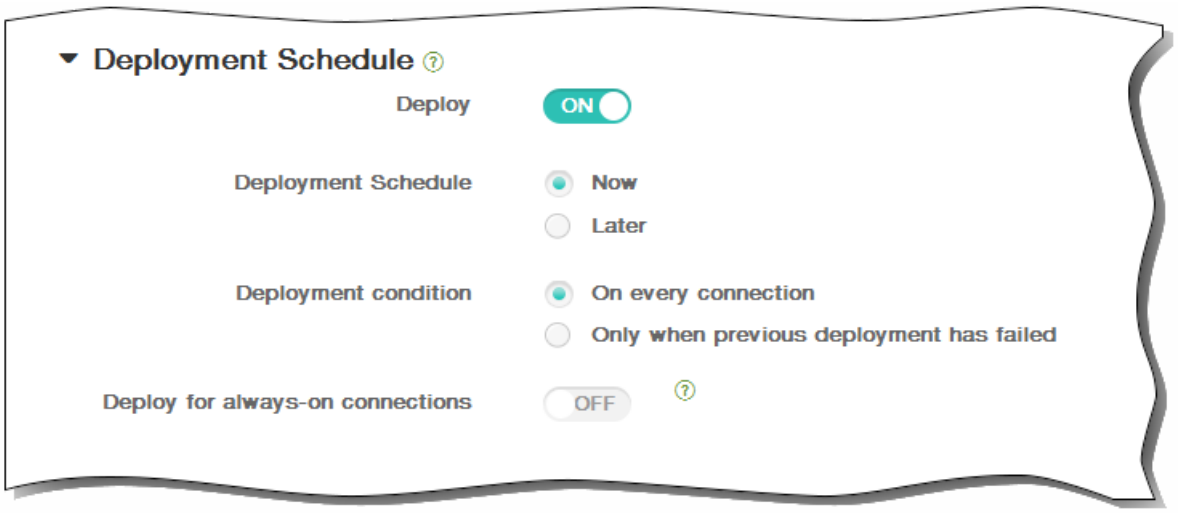
6. Si quiere, en Find additional required approvers, indique otros usuarios aptos para la aprobación que sean necesarios y, a continuación, haga clic en Search.

15. Haga clic en Next.
16. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



17. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
    5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
       Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

    Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



18. Haga clic en Guardar. La consola de XenMobile aplicará la información de la aplicación.

Creación de categorías de aplicaciones en XenMobile

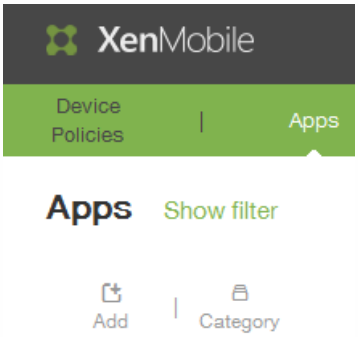
May 05, 2016

Cuando los usuarios inician sesión en Worx Home, reciben una lista de las aplicaciones, los enlaces Web y los almacenes que se hayan agregado a XenMobile y configurado en él. Puede usar las categorías de aplicaciones para permitir que los usuarios accedan únicamente a aquellas aplicaciones, almacenes o enlaces Web que quiera. Por ejemplo, puede crear una categoría llamada Finanzas y agregar a esa categoría aplicaciones que solo pertenezcan al ámbito financiero. O bien puede configurar una categoría llamada Ventas y asignarle aplicaciones de ventas. También puede configurar una categoría Apple para su App Store.

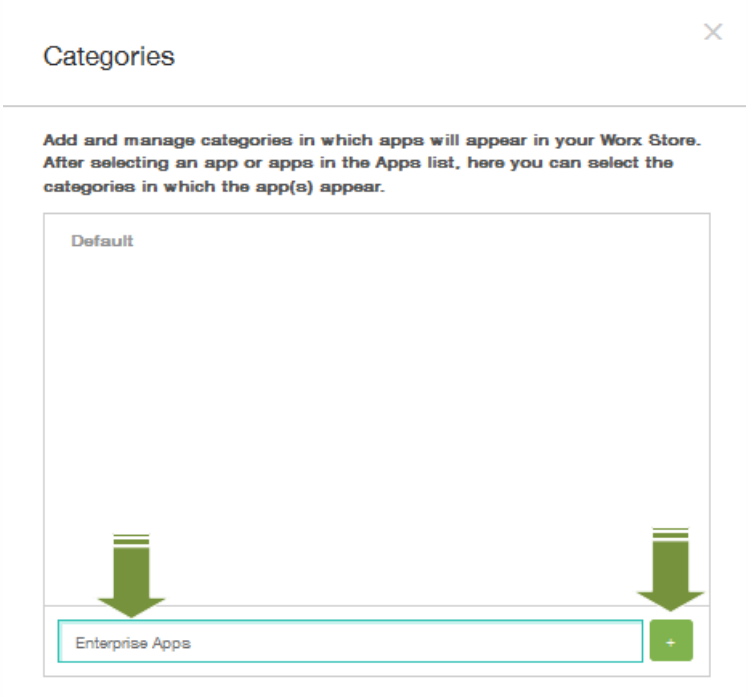
Las categorías se configuran en la página Apps de la consola de XenMobile. A continuación, al configurar o modificar una aplicación, un enlace Web o un almacén, puede agregar dicha aplicación a una de las categorías que ha configurado.

Para agregar una categoría

1. En la consola de XenMobile, haga clic en Configure > Apps. Aparecerá la página Apps.
2. En la página Apps, haga clic en Category.

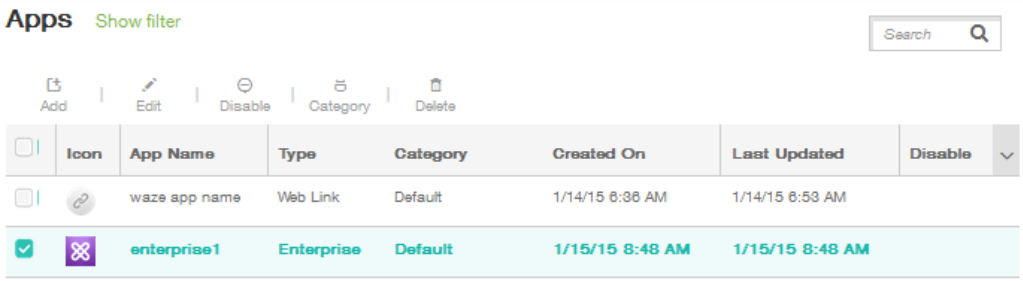


3. En el cuadro de diálogo Categories, introduzca el nombre de la categoría que quiere agregar y, a continuación, haga clic en el signo más (+). Por ejemplo, introduzca *Enterprise Apps* y haga clic en el signo más (+).

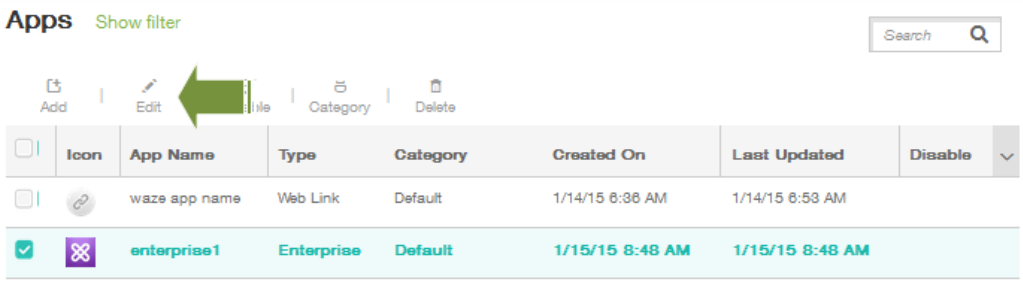


La categoría recién creada se agregará y aparecerá en el mismo cuadro de diálogo Categories. Si no hay categorías configuradas, solo aparecerá la categoría **Default**.

4. Repita el paso 3 para agregar cuantas categorías nuevas quiera y, a continuación, cierre el cuadro de diálogo Categories.
5. En la página Apps, puede vincular una aplicación existente a una categoría nueva. Seleccione la aplicación que quiera categorizar.

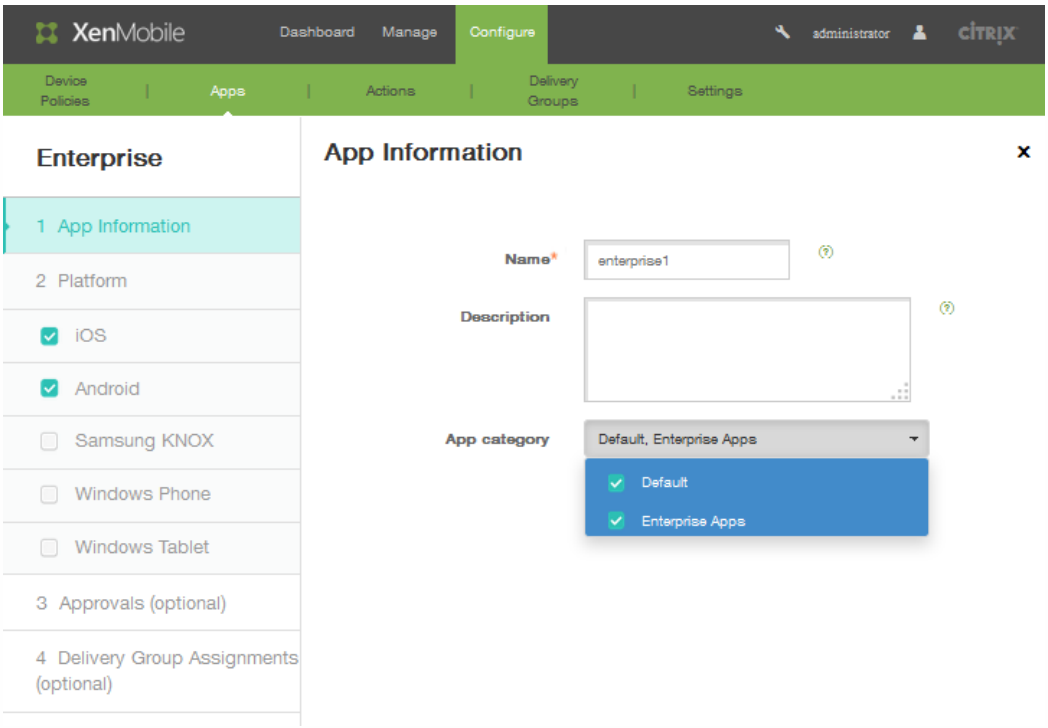


6. Haga clic en Edit para categorizar la aplicación.

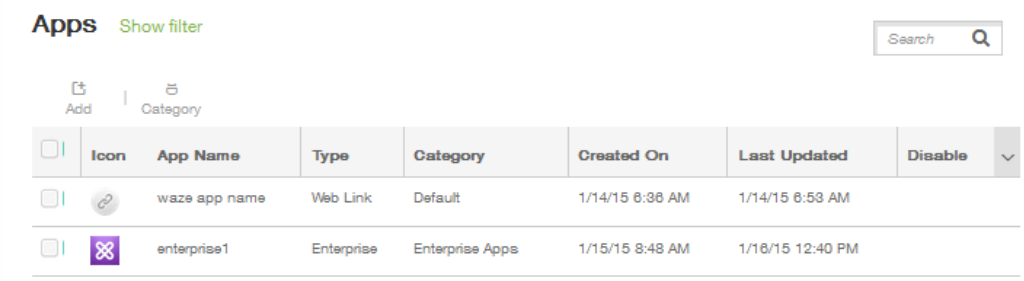


Aparecerá la página App Information.

7. En la lista App category, aplique una categoría marcando la casilla de verificación de la categoría en cuestión.



8. Haga clic en Next para desplazarse por las páginas restantes de la configuración de la aplicación.
9. En la última página, haga clic en Save para aplicar la categoría. La recién creada categoría se aplicará a la aplicación y aparecerá en la tabla Apps.

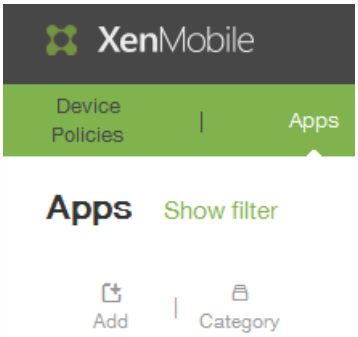


Para agregar la aplicación de un almacén público de aplicaciones a XenMobile

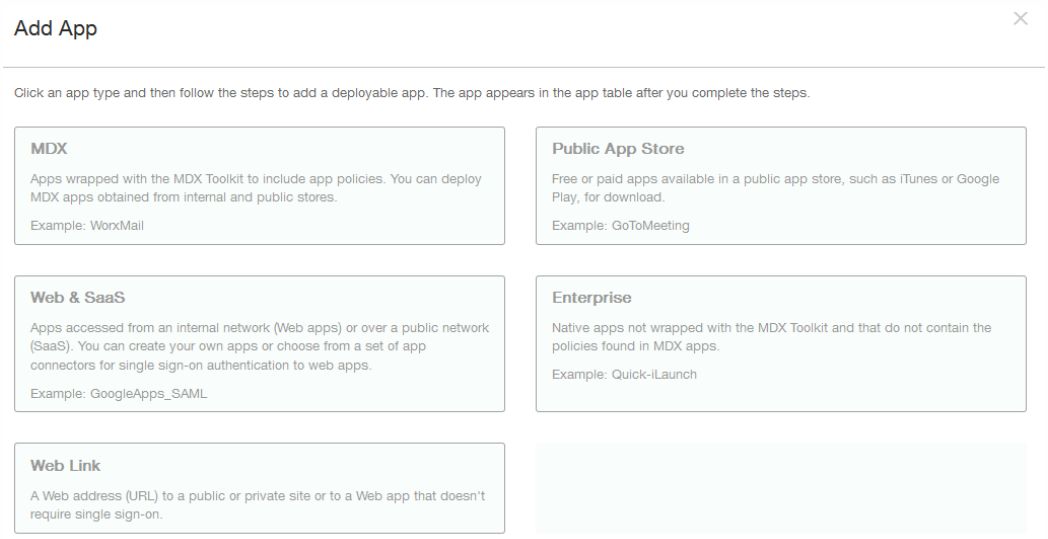
May 05, 2016

Se pueden agregar a XenMobile aplicaciones gratuitas o de pago disponibles en una tienda o un almacén público de aplicaciones, como iTunes o Google Play. Por ejemplo, GoToMeeting.

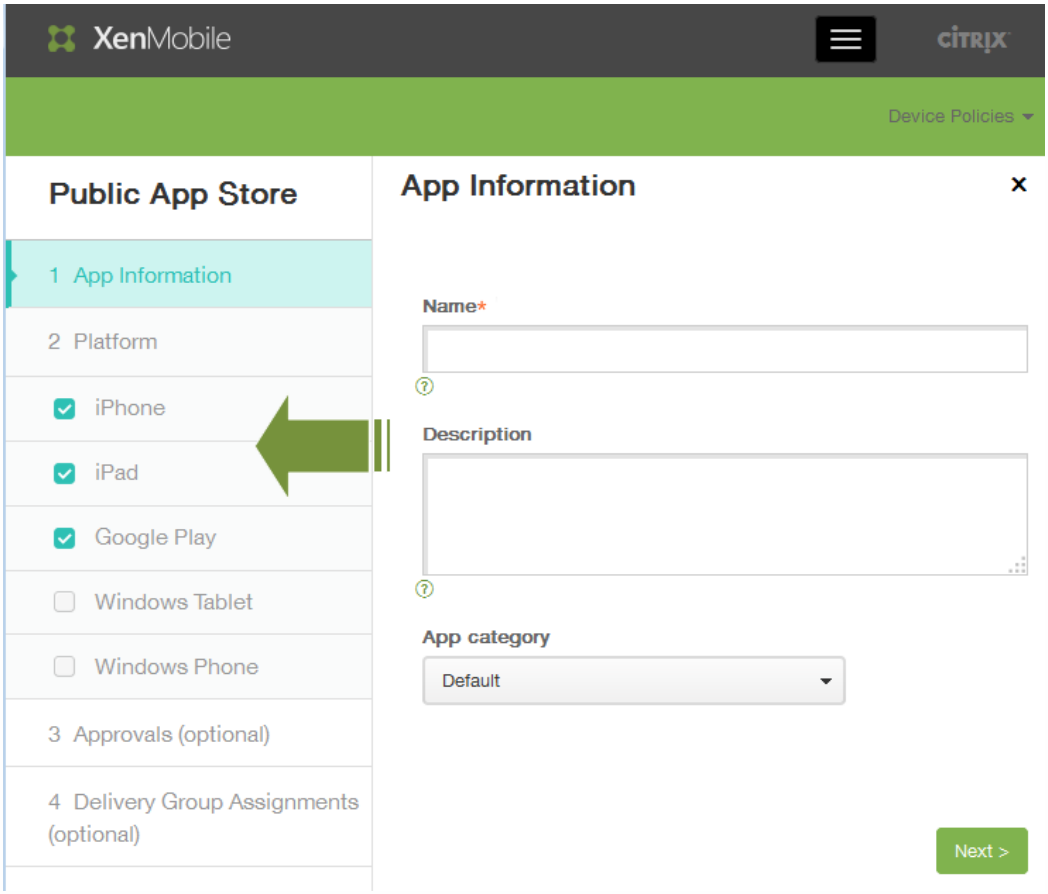
1. En la consola de XenMobile, haga clic en Configure > Apps. Aparecerá la pantalla Apps.



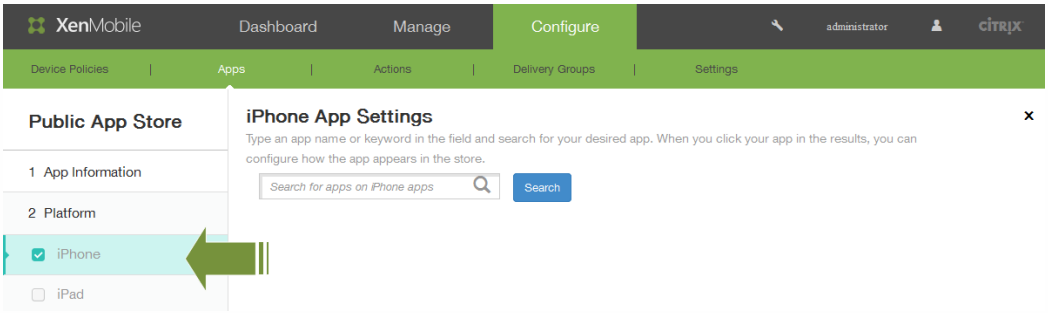
2. Haga clic en Add.
3. En la pantalla Add App, haga clic en Public App Store.



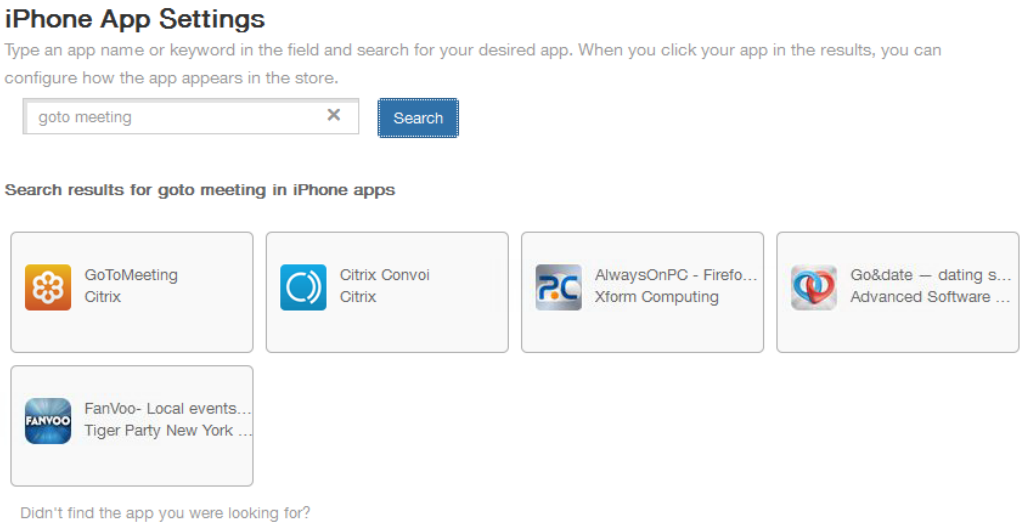
4. En la página App Information, escriba un nombre y una descripción de la aplicación en los campos Name y Description respectivamente. Estos campos son de uso interno. Si agrega aplicaciones para varios dispositivos (por ejemplo, iPhone, iPad y Google Play), utilice las casillas situadas en la parte izquierda de la pantalla para seleccionarlos.



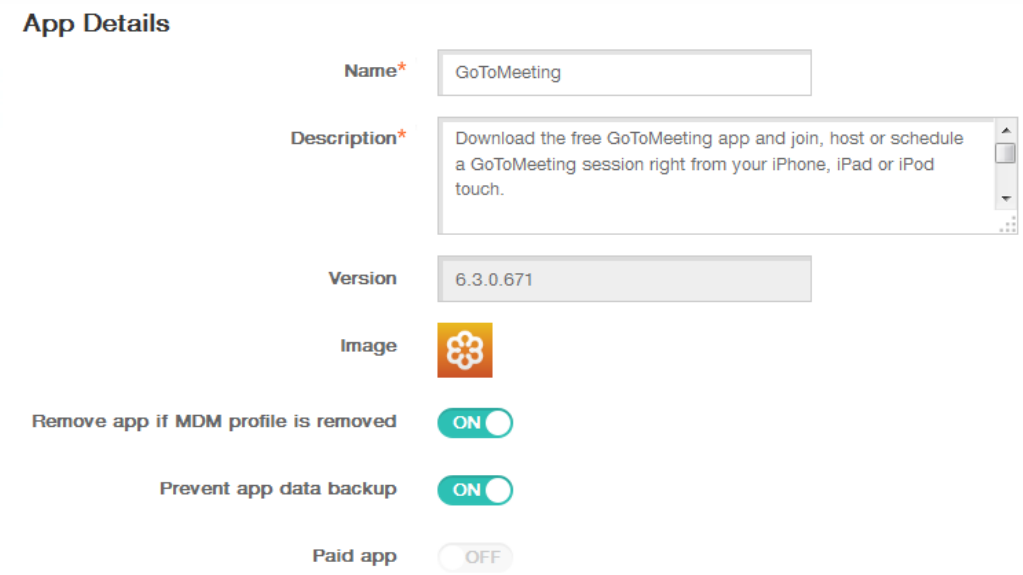
5. En la lista App category, haga clic en la categoría de aplicación.
6. Haga clic en Next.
7. En la pantalla Platform del tipo de plataforma, en el campo de búsqueda, escriba el nombre o la palabra clave de una aplicación para buscar la aplicación a agregar. Por ejemplo, si quiere agregar una aplicación para iPhone, la consola de XenMobile buscará aquellas aplicaciones que estén relacionadas con dispositivos iPhone. Si quiere agregar aplicaciones para varias plataformas, los resultados aparecerán para cada una de ellas.



En la siguiente ilustración, se muestran las aplicaciones que coinciden con los criterios de búsqueda (por ejemplo, GoToMeeting).

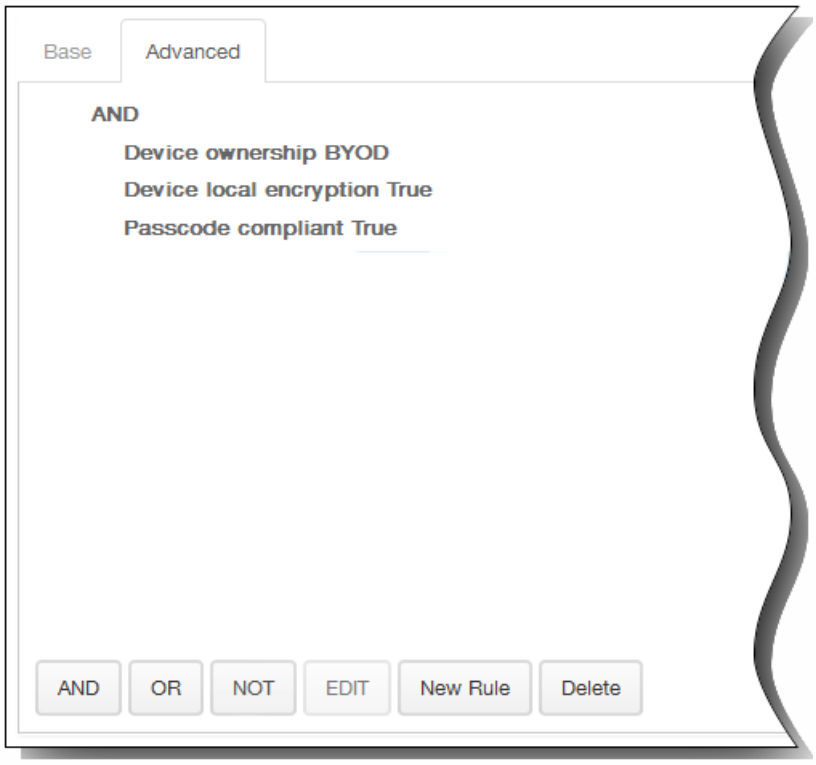


8. Haga clic en una aplicación de los resultados para configurar la forma en que la aplicación aparecerá en el almacén. En la pantalla App Details, los campos aparecerán ya rellenados con información relativa a la aplicación seleccionada (incluidos el nombre, la descripción, el número de versión y la imagen asociada). Si fuera necesario, cambie el nombre y la descripción de la aplicación.



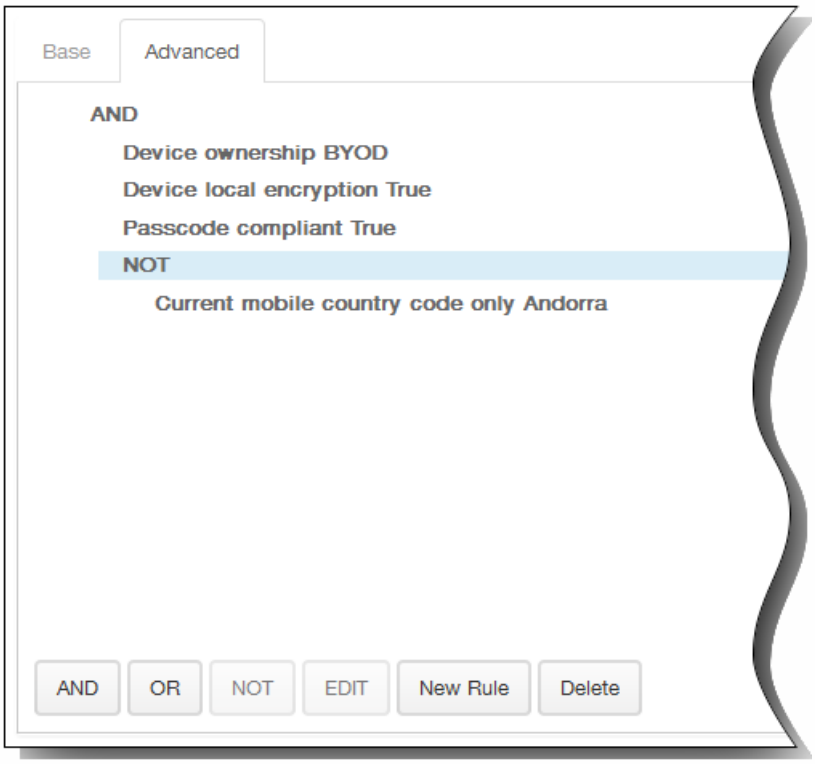
   1. En Remove app if MDM profile is removed, haga clic en ON si quiere quitar la aplicación en caso de que el perfil de MDM se quite. De forma predeterminada, esta opción está establecida en ON.
   2. En Prevent app data backup, haga clic en ON si quiere evitar que se realicen copias de seguridad de los datos de la aplicación. De forma predeterminada, esta opción está establecida en ON.
   3. El campo **Paid app** está preconfigurado y no se puede cambiar.
9. Expanda Deployment Rules. La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la aplicación.
   1. Puede optar por implementar la aplicación cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
   2. Haga clic en New Rule para definir las condiciones.
   3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
   4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

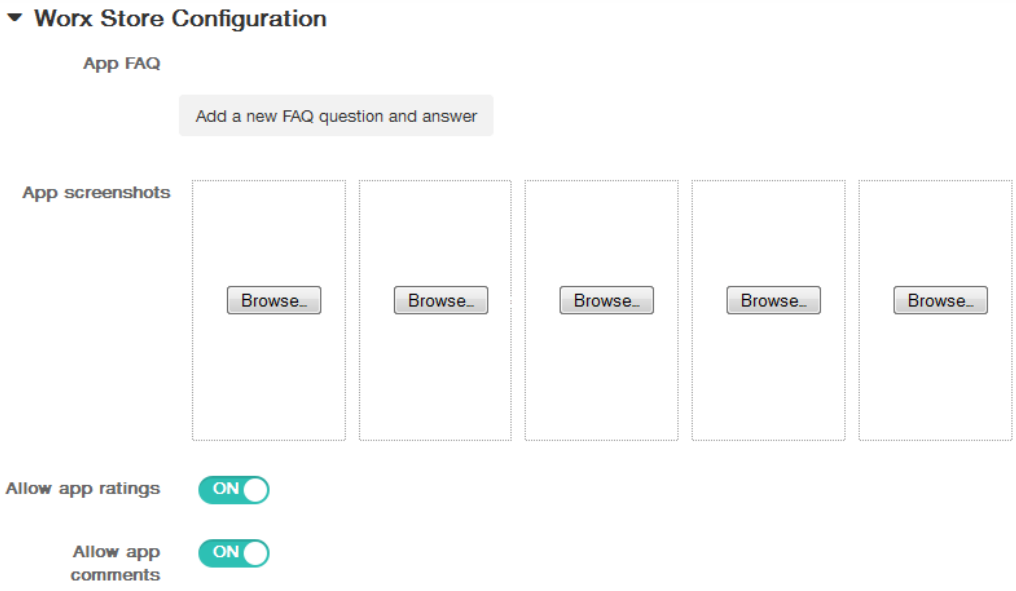


   Las condiciones que haya elegido aparecerán en la ficha Base.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.

3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
   En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True, el dispositivo debe cumplir el código de acceso y el código móvil del país del dispositivo no puede ser solo Andorra.

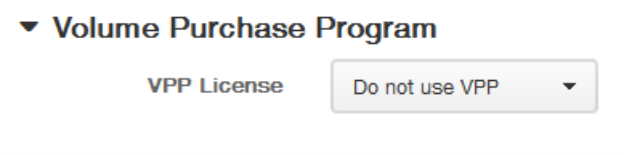


10. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.

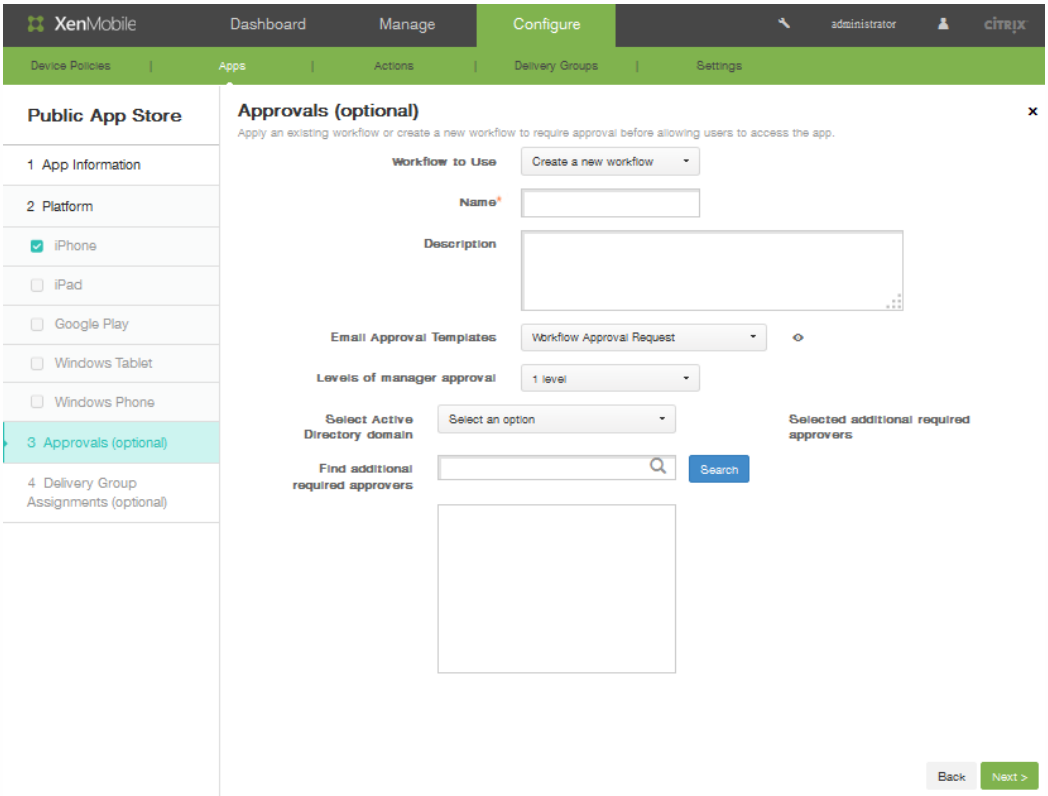


   En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.
11. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.

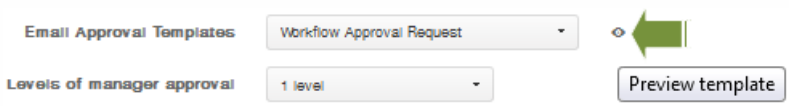
12. Expanda Volume Purchase Program y, a continuación, en la lista VPP license, haga clic en Upload a VPP license file si quiere permitir que XenMobile aplique una licencia VPP para la aplicación.



13. Haga clic en Next y, a continuación, repita los pasos del 7 al 16 para cada tipo de plataforma a la que quiera agregar aplicaciones públicas.
14. Si quiere, en la página Approvals, en la lista Workflow to use, haga clic en un flujo de trabajo o en Create a new workflow.



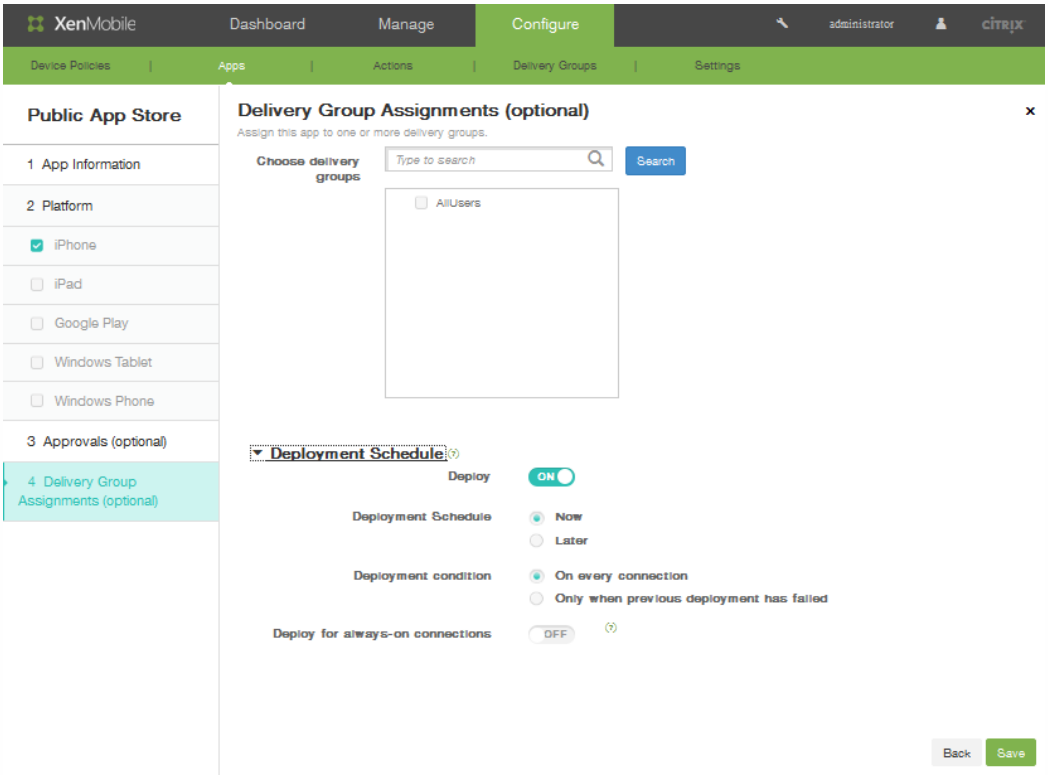
15. Al crear un nuevo flujo de trabajo, la consola de XenMobile cambia para mostrar las opciones de configuración para el proceso de aprobación. Cada uno de estos campos se describe en los pasos siguientes. Configure esos campos si necesita aprobación para crear una cuenta de usuario. El archivo VPP cargado solo se aplica a la versión antigua del programa VPP. En cuanto al nuevo programa, la gestión de licencias es automática en función de las licencias que haya adquirido la empresa. Esta información se define en **Settings > iOS VPP**.
    1. Especifique un nombre en el campo **Name** para el flujo de trabajo.
    2. Si quiere, indique una descripción en **Description**.
    3. En el campo **Email Approval Templates**, haga clic en una opción de notificación. Haga clic en el **icono de vista** para una vista previa de la plantilla elegida.



    4. En **Levels of manager approval**, haga clic en el nivel pertinente; puede elegir desde None hasta 3. .

5. En **Select Active Directory domain**, haga clic en el dominio.
6. Si quiere, en Find additional required approvers, indique otros usuarios aptos para la aprobación que sean necesarios y, a continuación, haga clic en Search.

16. Haga clic en Next.
17. Si quiere, en la página **Delivery Groups Assignment**, puede asignar la aplicación a un grupo de entrega o a varios.



18. En Choose delivery groups, busque un grupo de entrega (o varios). Marque la casilla de verificación **All Users** para asignar la aplicación a cada usuario de XenMobile.
19. Expanda Deployment Schedule para precisar más el grupo de entrega.
    1. Deploy. Haga clic en ON para habilitar la programación de una implementación.
    2. Deployment Schedule. Haga clic en Now o Later para establecer la programación de la implementación.
    3. Deployment condition. Haga clic para implementar la aplicación en cada conexión o solo si la implementación anterior falla.
    4. En Deploy for always-on connections, haga clic en ON para que la implementación se efectúe cuando esté establecida la directiva de conexión "Always-on".
       Nota: Esta opción se aplica cuando también se han configurado las claves de implementación global en segundo plano en la sección Server Properties del área Settings de la consola de XenMobile. La directiva Deploy for always-on connection no está disponible para dispositivos iOS.
20. Haga clic en Save. La consola de XenMobile aplicará la información de la aplicación.

Para agregar aplicaciones Web y SaaS a XenMobile

May 05, 2016

Con la consola de XenMobile, es posible ofrecer a los usuarios el inicio de sesión único, conocido como Single Sign-on (SSO), para sus aplicaciones móviles, de empresa, Web y SaaS. Puede habilitar aplicaciones para SSO. Para ello, debe utilizar plantillas de conectores de aplicaciones. Para obtener una lista de los tipos de conectores disponibles en XenMobile, consulte Lista de tipos de conectores de aplicaciones.

También puede crear su propio conector en XenMobile.

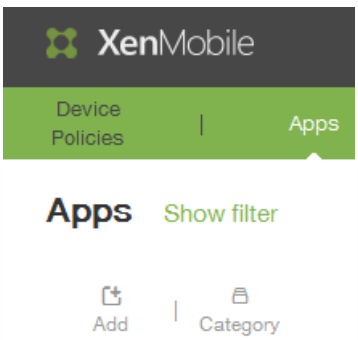
Para configurar un conector, proporcione los siguientes parámetros:

- Nombres diferentes (opcional). Haga uso de cualquier conector de aplicaciones que se muestre en la consola. Box connector ya no se admite.
- Descripción de la aplicación.
- Dirección Web, con el nombre completo de dominio (FQDN). Por ejemplo, si quiere agregar LinkedIn a la lista de aplicaciones, visite http://www.linkedin.com y haga clic en Iniciar sesión. Cuando aparezca la página de inicio de sesión, use la dirección Web https://www.linkedin.com cuando configure la aplicación.
- Ubicación de la aplicación, ya sea en Internet o en la red interna.
- Credenciales para SSO. Los usuarios pueden utilizar las credenciales de aplicación.
- Categoría de la aplicación. Las categorías permiten organizar las aplicaciones en Worx Home.
- Directivas de aplicaciones para cada aplicación que configure en XenMobile.
- Parámetros de aprobación de flujos de trabajo para todas las aplicaciones que incluyen especificar las personas que pueden aprobar la cuenta de usuario.
- Un grupo de entrega de usuarios al que asignar la aplicación.

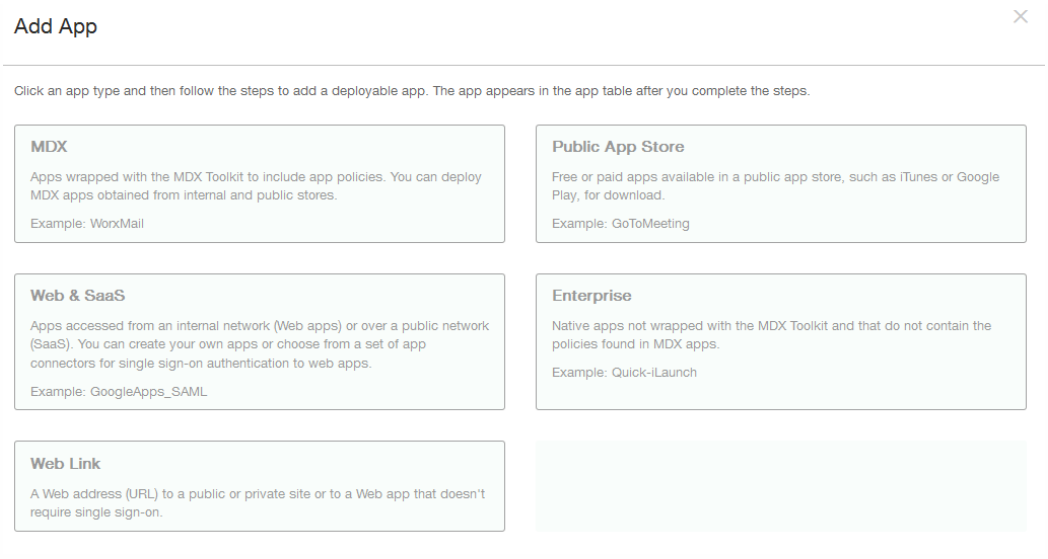
Si una aplicación solo está disponible para SSO, al finalizar la configuración de los parámetros anteriores, guárdelos para que la aplicación aparezca en la ficha Apps de la consola de XenMobile.

Para agregar un conector de aplicaciones en XenMobile

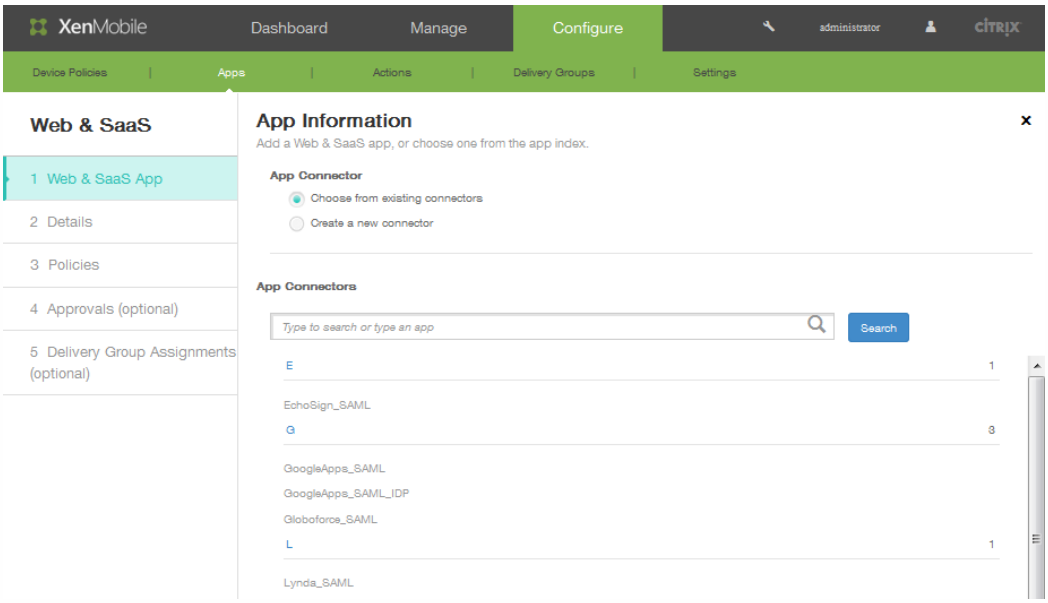
1. En la consola Web de XenMobile, haga clic en Configure > Apps. Se abrirá la página Apps.
2. En la página Apps, haga clic en **Add**.



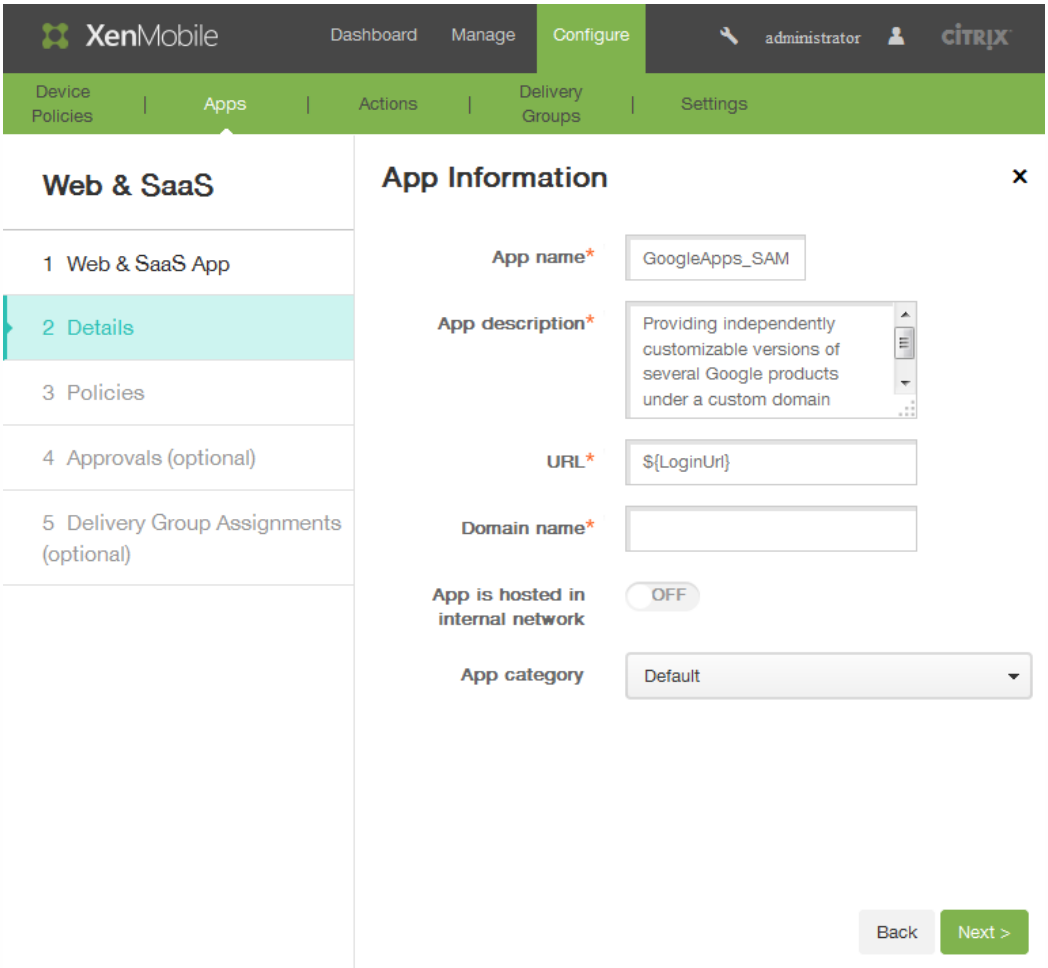
3. En la página **Add App**, haga clic en **Web & SaaS**.



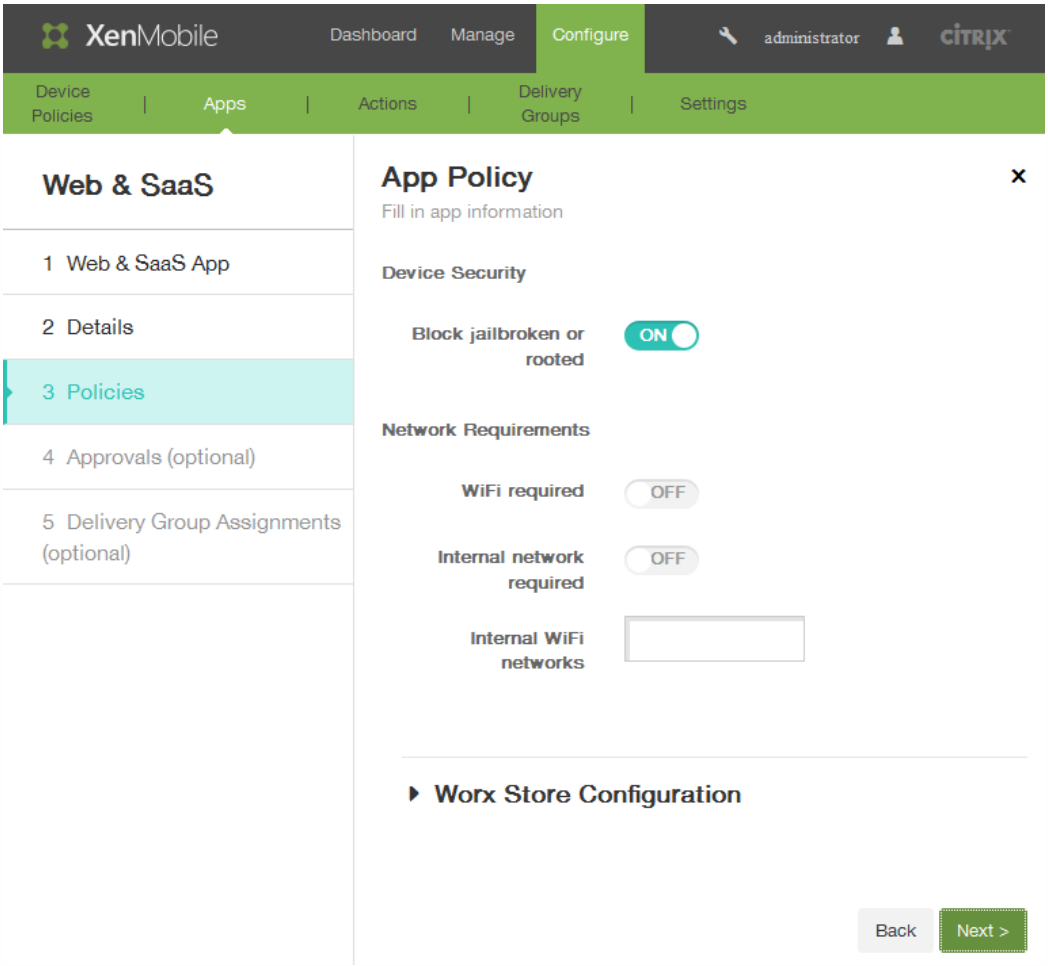
4. En la página App Information, haga clic en Choose from existing connector o en Create a new connector.



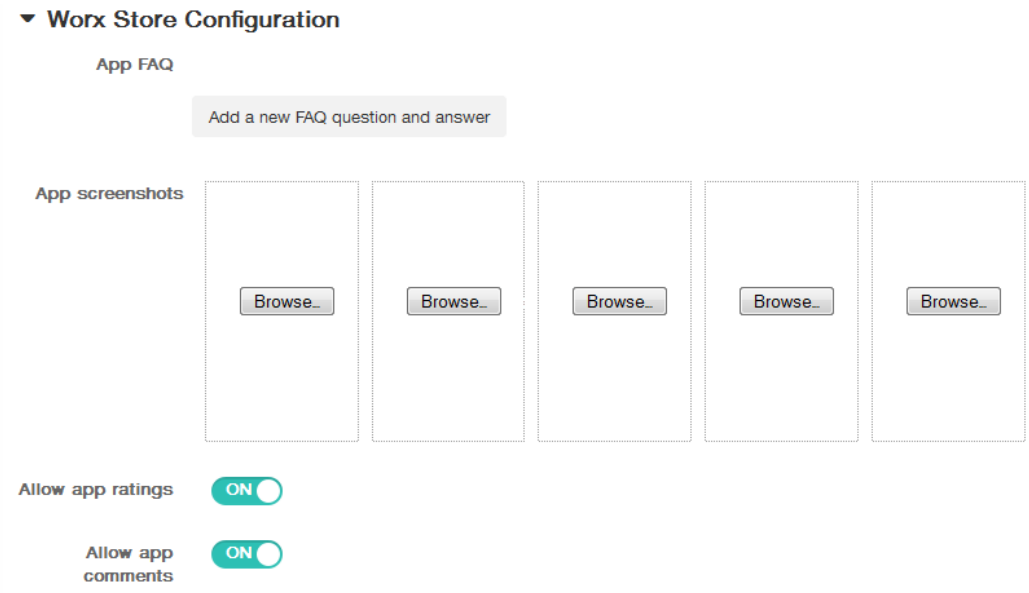
5. Si hace clic en una aplicación de la lista, se abrirá la página Details. Los campos App name, Description y URL aparecerán previamente rellenados.



1. Si corresponde, en URL, introduzca la dirección Web de la aplicación o mantenga la dirección predeterminada.
2. En App is hosted in internal network, haga clic en ON si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si establece esta opción en ON, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway.
3. En la lista App category, haga clic en una categoría.
4. En Enable user management for provisioning, haga clic en On. Si utiliza el conector Globalforce_SAML, debe activar Enable user management for provisioning para garantizar una integración perfecta del inicio de sesión único (SSO).
6. Haga clic en Siguiente. Aparecerá la página Policies.

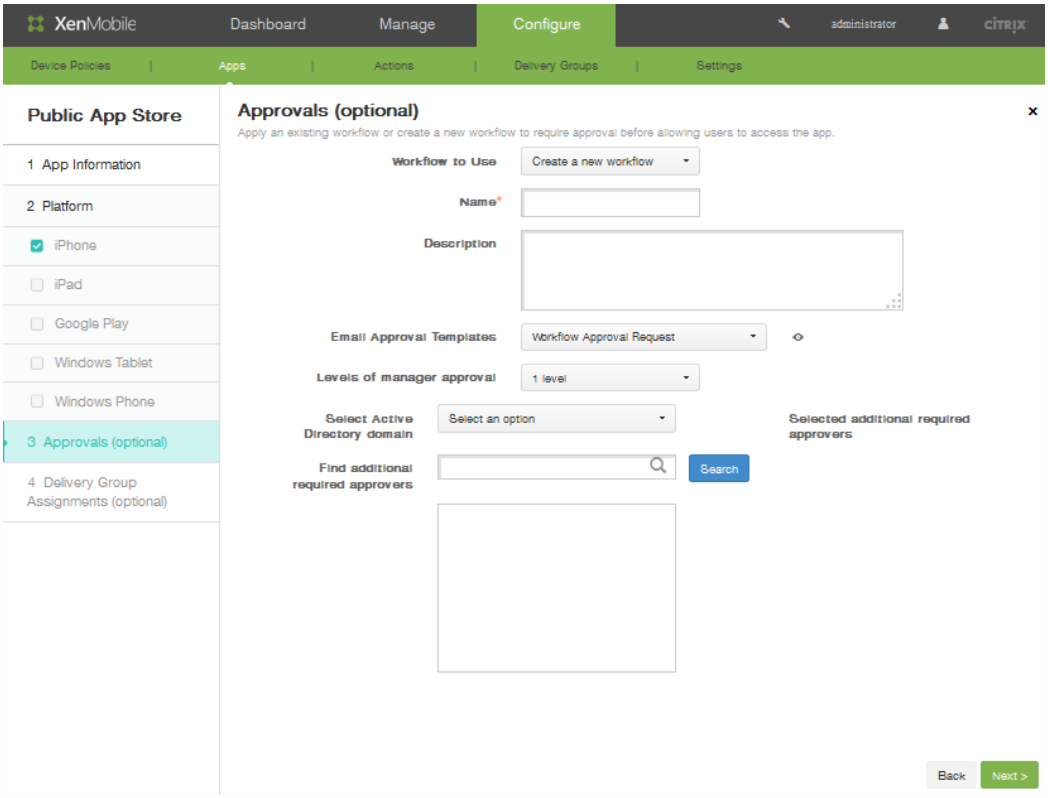


7. En Device Security, en Block jailbroken or rooted, haga clic en ON.
8. En Network Requirements, configure los siguientes parámetros:
   1. En WiFi required, haga clic en ON y, a continuación, especifique las redes Wi-Fi internas.
   2. En Internal network required, haga clic en ON si es necesaria una red interna para ejecutar la aplicación.
9. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.



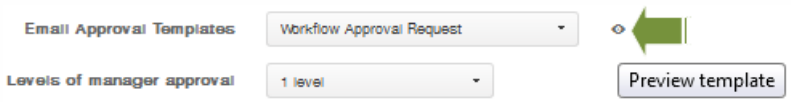
En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.

10. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.
11. Haga clic en Siguiente.
12. Si quiere, en la página Approvals, en la lista Workflow to use, haga clic en un flujo de trabajo o en Create a new workflow.



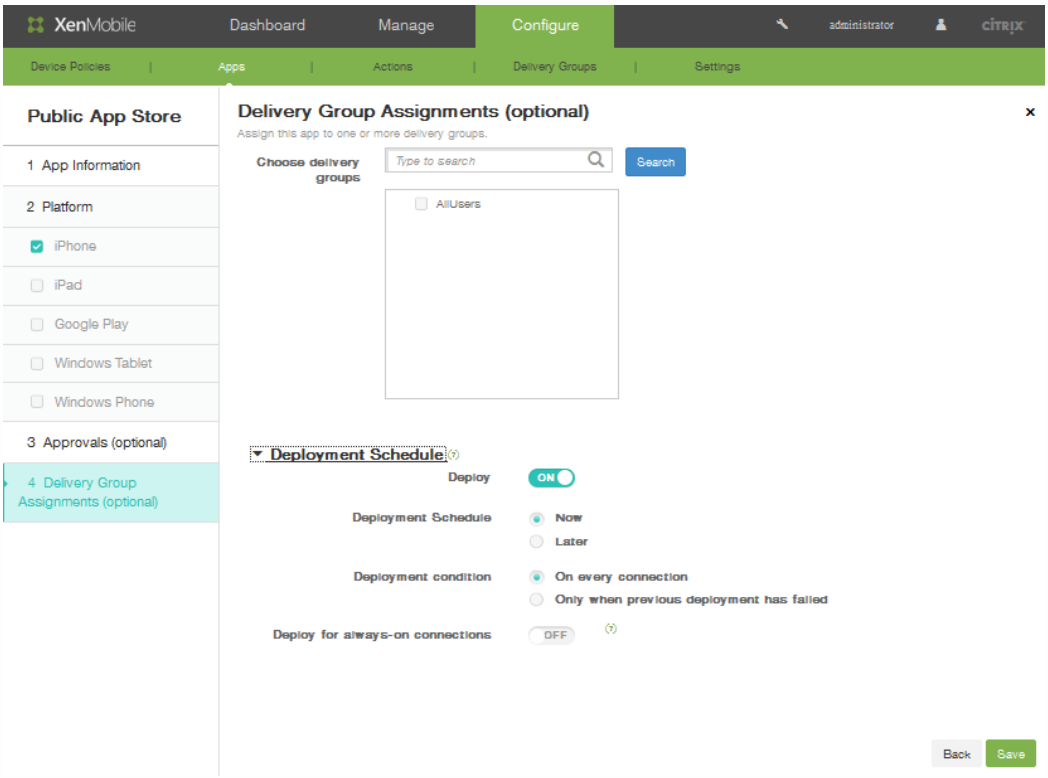
13. Al crear un nuevo flujo de trabajo, la consola de XenMobile cambia para mostrar las opciones de configuración para el proceso de aprobación. Cada uno de estos campos se describe en los pasos siguientes. Configure esos campos si necesita aprobación para crear una cuenta de usuario.
    1. Especifique un nombre en el campo **Name** para el flujo de trabajo.

2. Si quiere, indique una descripción en **Description**.
3. En el campo **Email Approval Templates**, haga clic en una opción de notificación. Haga clic en el **icono de vista** para una vista previa de la plantilla elegida.

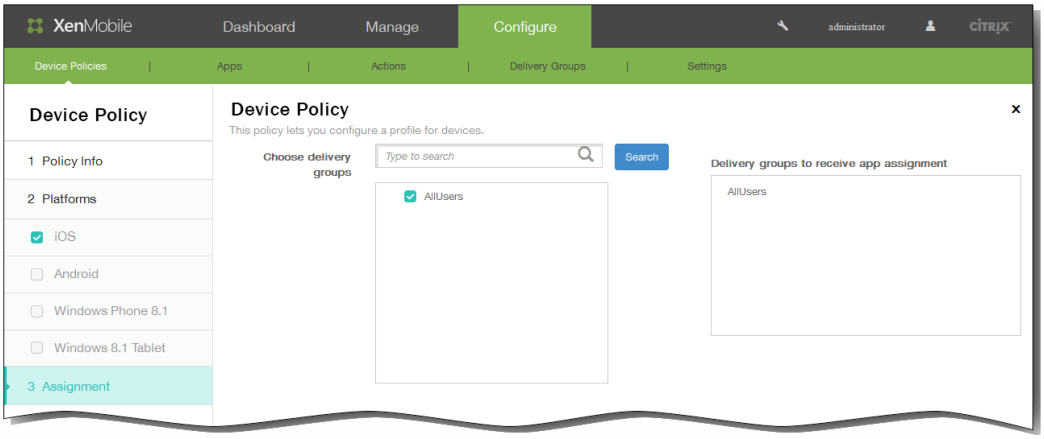


4. En **Levels of manager approval**, haga clic en el nivel pertinente; puede elegir desde None hasta 3.
5. En **Select Active Directory domain**, haga clic en el dominio.
6. Si quiere, en Find additional required approvers, indique otros usuarios aptos para la aprobación que sean necesarios y, a continuación, haga clic en Search.

14. Haga clic en Siguiente.
15. Si quiere, en la página **Delivery Groups Assignment**, puede asignar la aplicación a un grupo de entrega o a varios.

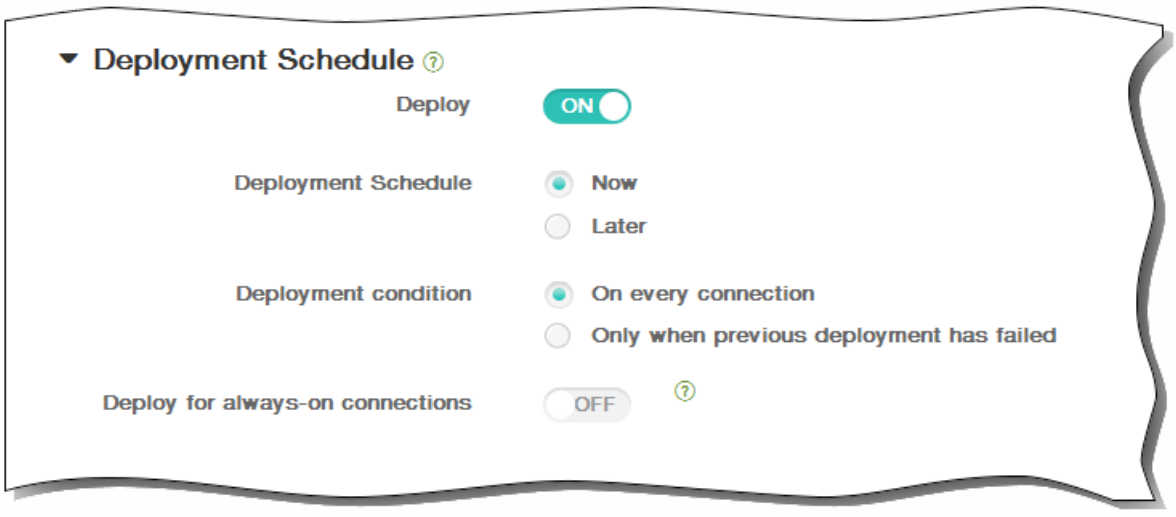


16. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



17. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
    5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
       Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

    Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



18. Haga clic en **Guardar**.

Lista de tipos de conectores de aplicaciones

May 05, 2016

En la siguiente tabla, se muestran los conectores y los tipos de conectores que están disponibles en XenMobile. En la tabla también se indica si el conector respalda el uso de administración de cuentas de usuario, que permite crear cuentas nuevas automáticamente o con un flujo de trabajo.

Nombre del conector	SSO SAML	Respalda administración de cuentas de usuario
EchoSign_SAML	S	S
Globoforce_SAML		**Nota:** Al utilizar este conector, debe habilitar la opción User Management for Provisioning para una correcta integración del inicio de sesión seguro.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

Para agregar aplicaciones de empresa a XenMobile

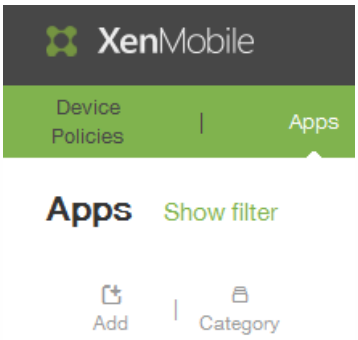
May 05, 2016

En XenMobile, las aplicaciones de empresa representan las aplicaciones nativas que no están empaquetadas con la herramienta MDX Toolkit y no contienen las directivas asociadas a aplicaciones MDX. Puede cargar una aplicación de empresa en la ficha Apps de la consola de XenMobile. Las aplicaciones de empresa admiten las siguientes plataformas (y sus tipos de archivo correspondientes):

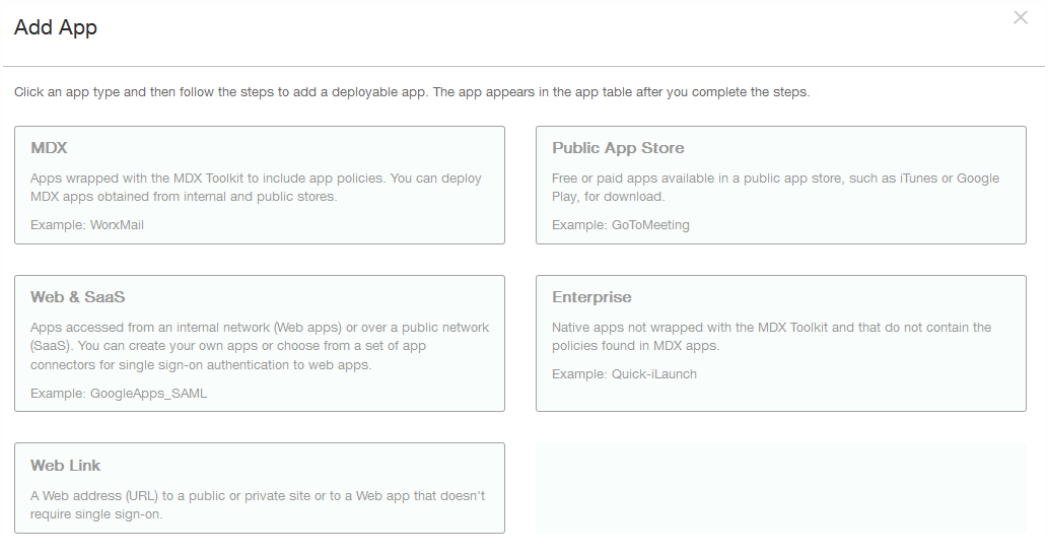
- iOS (archivo .ipa)
- Android (archivo .apk)
- Samsung KNOX (archivo .apk)
- Windows Phone (archivo .xap o .appx)
- Tableta Windows (archivo .appx)

Para crear una aplicación de empresa

1. En la consola de XenMobile, haga clic en Configure > Apps.
2. En la página Apps, haga clic en **Add**.

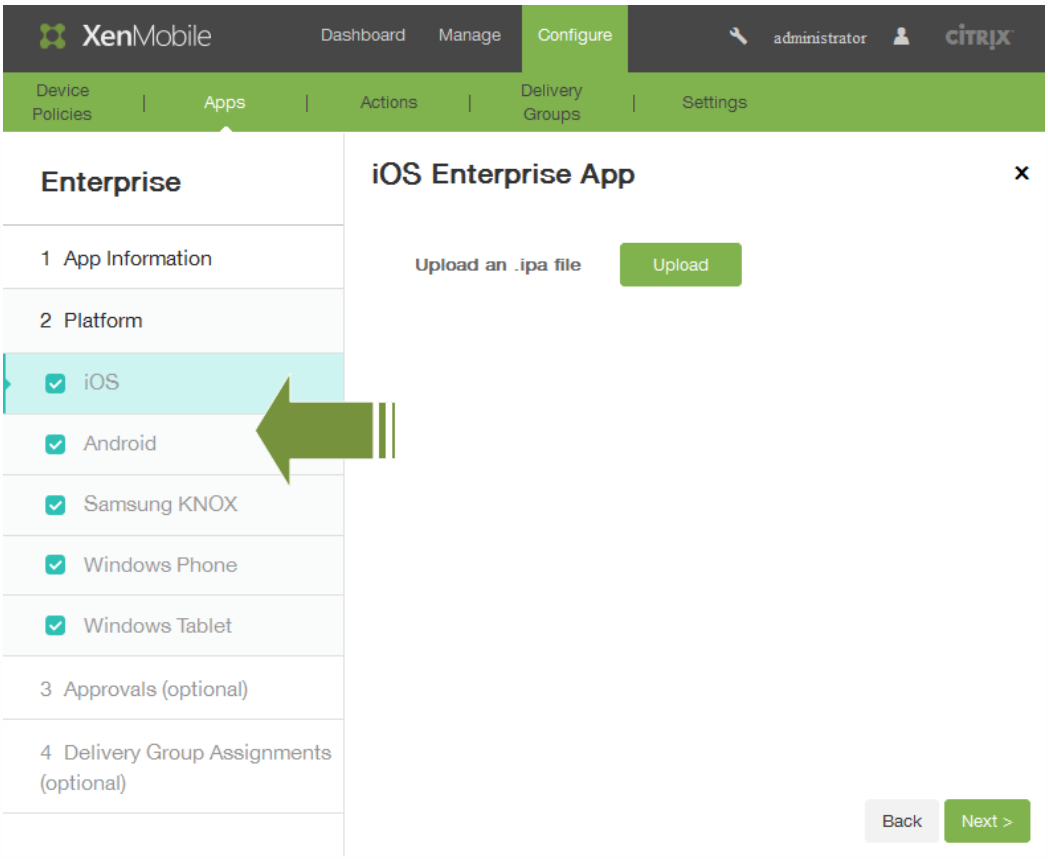


3. En la página Add App, haga clic en **Enterprise**.

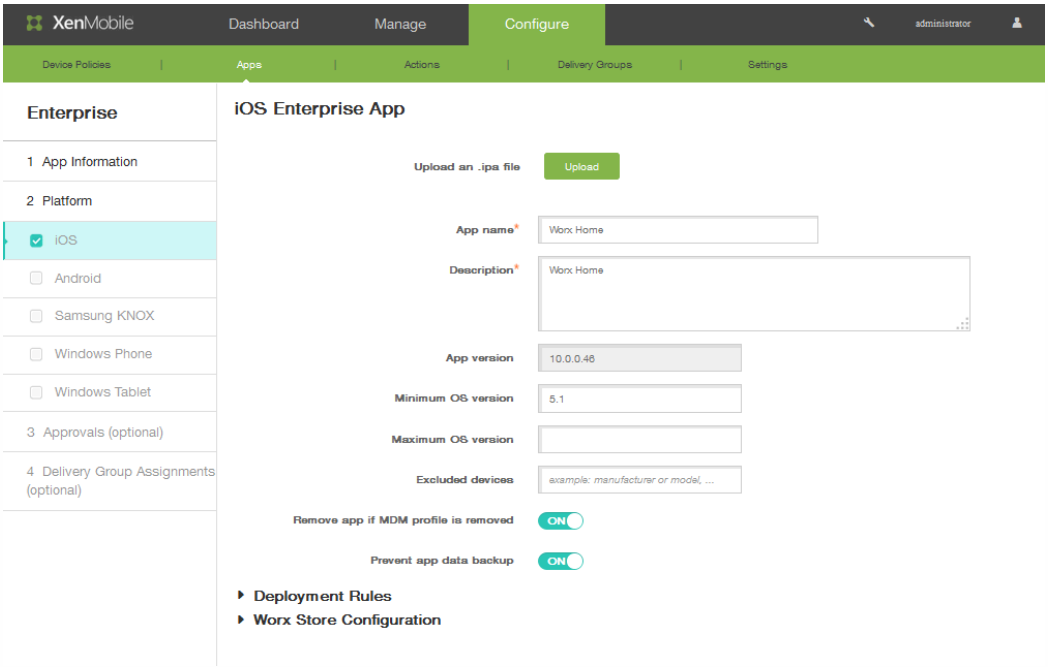


4. En el catálogo, haga clic en New enterprise app.

5. En la página App Information, complete los pasos siguientes:
   1. Name. Escriba un nombre para la aplicación.
   2. Description. Escriba una descripción para la aplicación.
      Nota: Si quiere configurar una segunda aplicación con la misma dirección Web, debe darle a la aplicación un nombre diferente.
   3. En **App category**, haga clic en una categoría y, a continuación, haga clic en Next.
6. En el área Platform de la parte izquierda de la página, seleccione las plataformas de dispositivo para las que quiere agregar la aplicación (por ejemplo, iOS o Android).

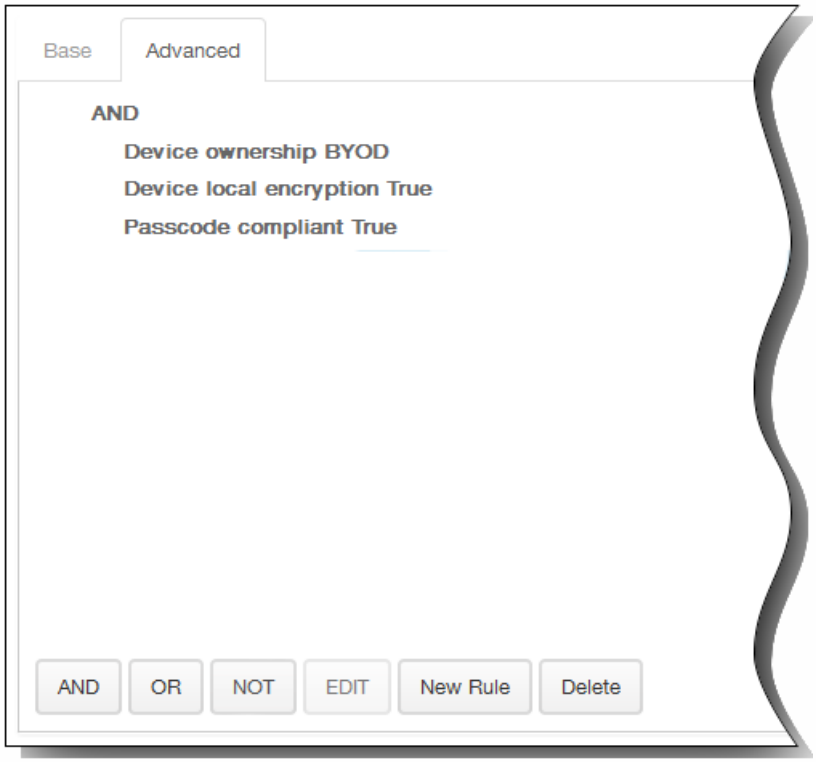


7. Haga clic en Upload para ir a la ubicación del archivo y, a continuación, haga clic en Next. Aparecerá la página de información referente a la aplicación para el tipo de plataforma pertinente. Los campos aparecerán ya rellenados con información relativa a la aplicación seleccionada (incluido el nombre, la descripción, el número de versión y la imagen asociada). Si fuera necesario, cambie el nombre y la descripción de la aplicación.



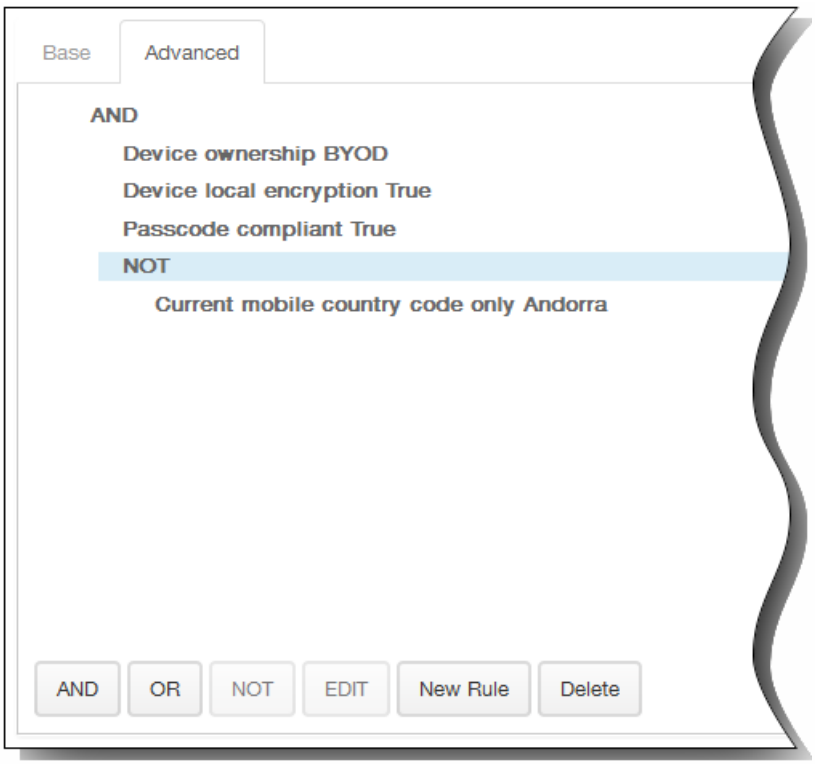
8. En Remove app if MDM profile is removed, haga clic en ON si quiere quitar la aplicación en caso de que el perfil de MDM se quite. De forma predeterminada, esta opción está establecida en ON.
9. En Prevent app data backup, haga clic en ON si quiere evitar que se realicen copias de seguridad de los datos de la aplicación. De forma predeterminada, esta opción está establecida en ON.
10. Expanda Deployment Rules. La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la aplicación.
    1. Puede optar por implementar la aplicación cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

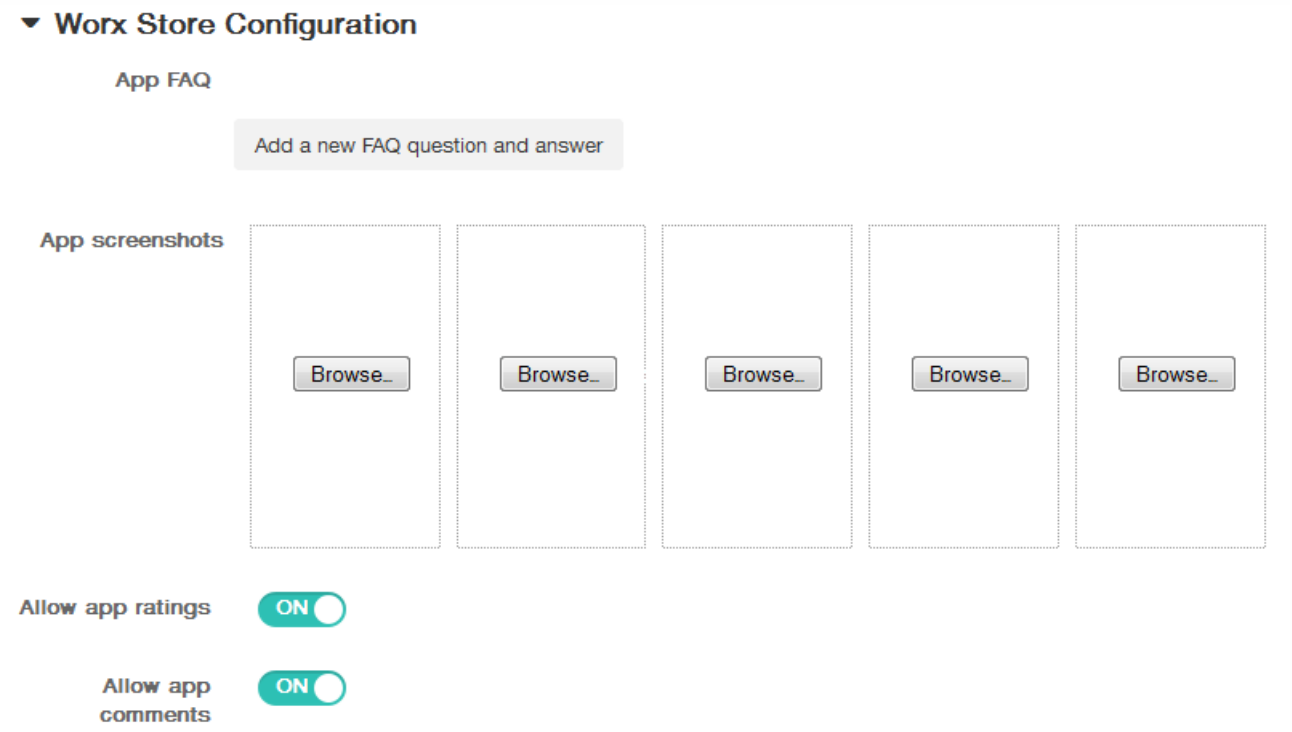


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True, el dispositivo debe cumplir el código de acceso y el código móvil del país del dispositivo no puede ser solo Andorra.



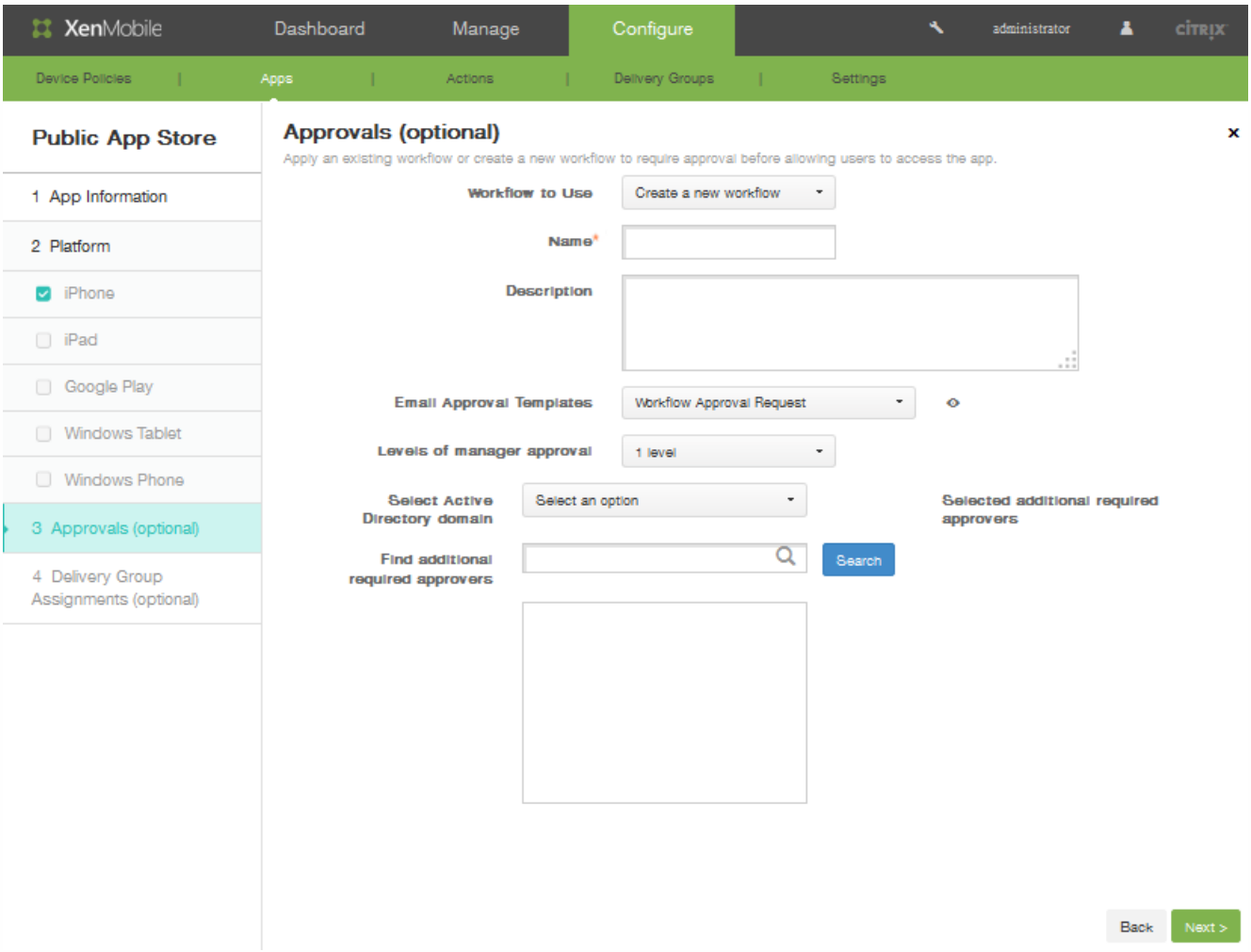
11. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.



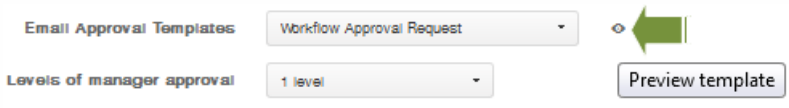
En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.

12. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.

13. Haga clic en Siguiente.
14. Si quiere, en la página Approvals, en la lista Workflow to use, haga clic en un flujo de trabajo o en Create a new workflow.



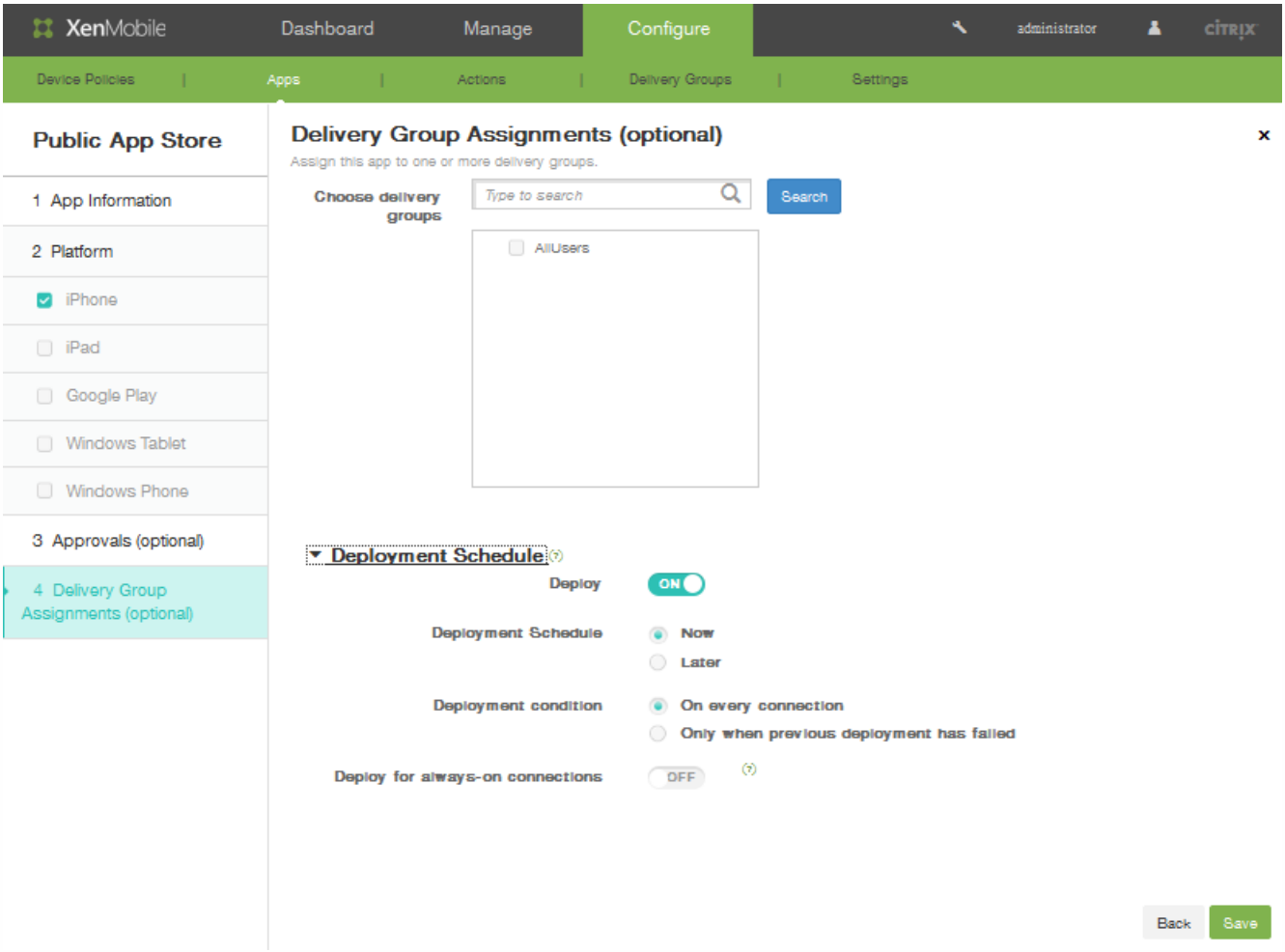
15. Al crear un nuevo flujo de trabajo, la consola de XenMobile cambia para mostrar las opciones de configuración para el proceso de aprobación. Cada uno de estos campos se describe en los pasos siguientes. Configure esos campos si necesita aprobación para crear una cuenta de usuario.
    1. Especifique un nombre en el campo **Name** para el flujo de trabajo.
    2. Si quiere, indique una descripción en **Description**.
    3. En el campo **Email Approval Templates**, haga clic en una opción de notificación. Haga clic en el **icono de vista** para una vista previa de la plantilla elegida.



    4. En **Levels of manager approval**, haga clic en el nivel pertinente; puede elegir desde None hasta 3.
    5. En **Select Active Directory domain**, seleccione un dominio del menú desplegable; solo los dominios unidos de Active Directory aparecerán en esta lista (por ejemplo, testprise.net):

6. Si quiere, en Find additional required approvers, indique otros usuarios aptos para la aprobación que sean necesarios y, a continuación, haga clic en Search.

16. Si quiere, en la página **Delivery Groups Assignment**, puede asignar la aplicación a un grupo de entrega o a varios.



17. En Choose delivery groups, busque un grupo de entrega (o varios). Marque la casilla de verificación **All Users** para asignar la aplicación a cada usuario de XenMobile.
18. Expanda Deployment Schedule para precisar más el grupo de entrega.
    1. Deploy. Haga clic en ON para habilitar la programación de una implementación.
    2. Deployment Schedule. Haga clic en Now o en Later para establecer la programación de la implementación.
    3. Deployment condition. Haga clic para implementar la aplicación en cada conexión o solo si la implementación anterior falla.
    4. En Deploy for always-on connections, haga clic en ON para que la implementación se efectúe cuando esté establecida la directiva de conexión "Always-on".
       Nota: Esta opción se aplica cuando también se han configurado las claves de implementación global en segundo plano en la sección Server Properties del área Settings de la consola de XenMobile. La directiva Deploy for always-on connection no está disponible para dispositivos iOS.

19. Haga clic en Guardar.

Para agregar aplicaciones de enlaces Web a XenMobile

May 05, 2016

En XenMobile, se puede establecer una dirección Web (URL) que lleve a un sitio público o privado, o bien que lleve a una aplicación Web que no requiera Single Sign-On.

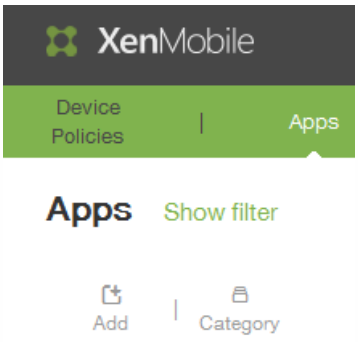
Puede configurar enlaces Web desde la ficha Apps de la consola de XenMobile. Una vez configurado el enlace Web, este aparece como un icono de enlace en la lista de la tabla Apps. Cuando los usuarios inician sesión en Worx Home, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Para agregar el enlace, debe proporcionar la siguiente información:

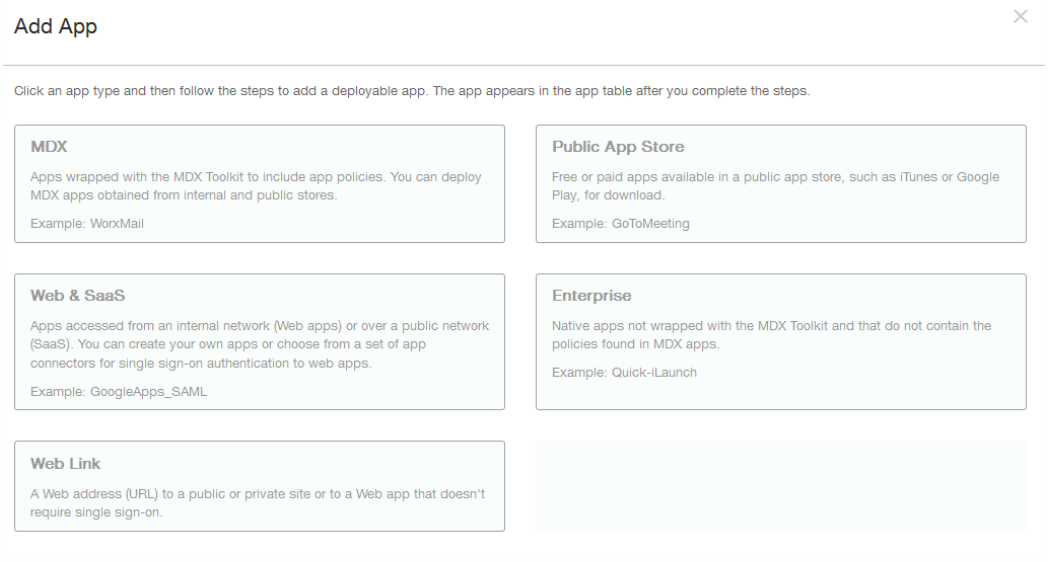
- Nombre para el enlace
- Descripción del enlace
- Dirección Web (URL)
- Categoría
- Rol
- Imagen en formato PNG (optativo)

Para agregar enlaces Web a XenMobile

1. Configure > Apps. Se abrirá la página Apps.
2. En la página Apps, haga clic en Add.

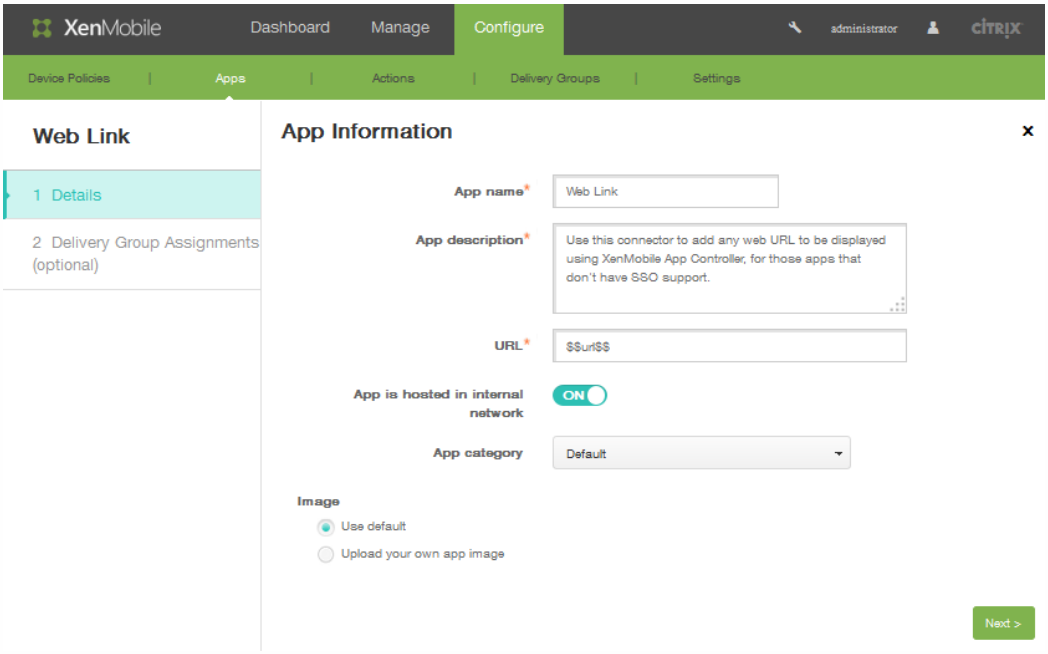


3. En la página Add App, haga clic en Web Link.

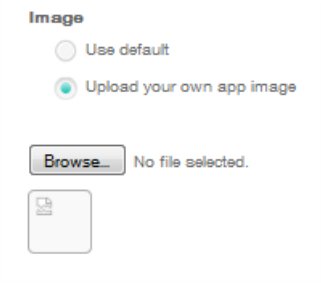


Aparecerá la página App Information.

4. Los campos App name, Description y URL aparecerán previamente rellenados.

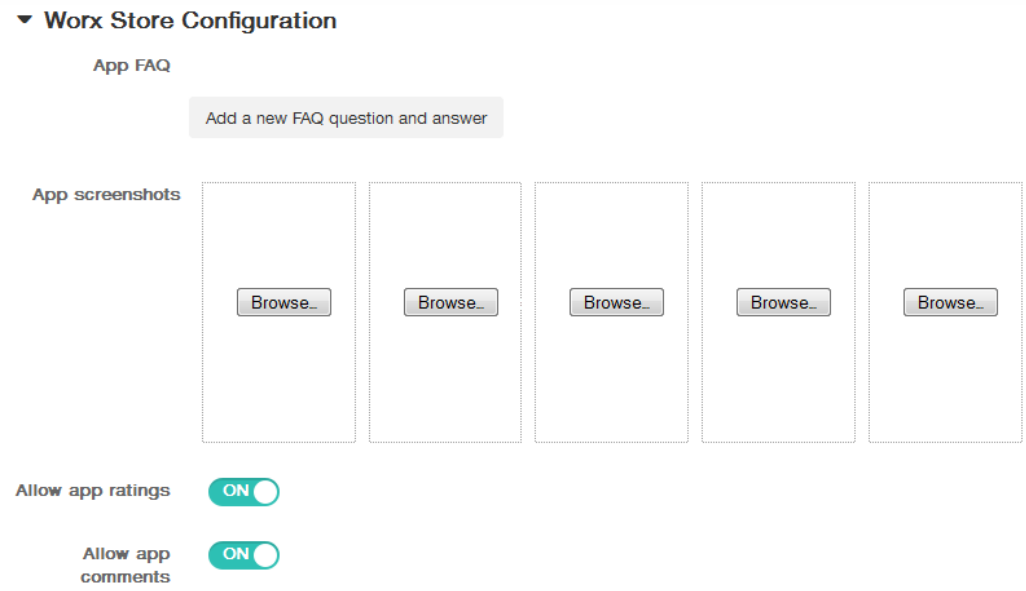


1. Si corresponde, en URL, introduzca la dirección Web de la aplicación o mantenga la dirección predeterminada.
2. En App is hosted in internal network, haga clic en ON si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si establece esta opción en ON, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway.
3. En la lista App category, haga clic en una categoría.
4. Si quiere asociar su propia imagen en miniatura al conector, marque Upload your own app image. Haga clic en Browse para buscar la imagen pertinente:



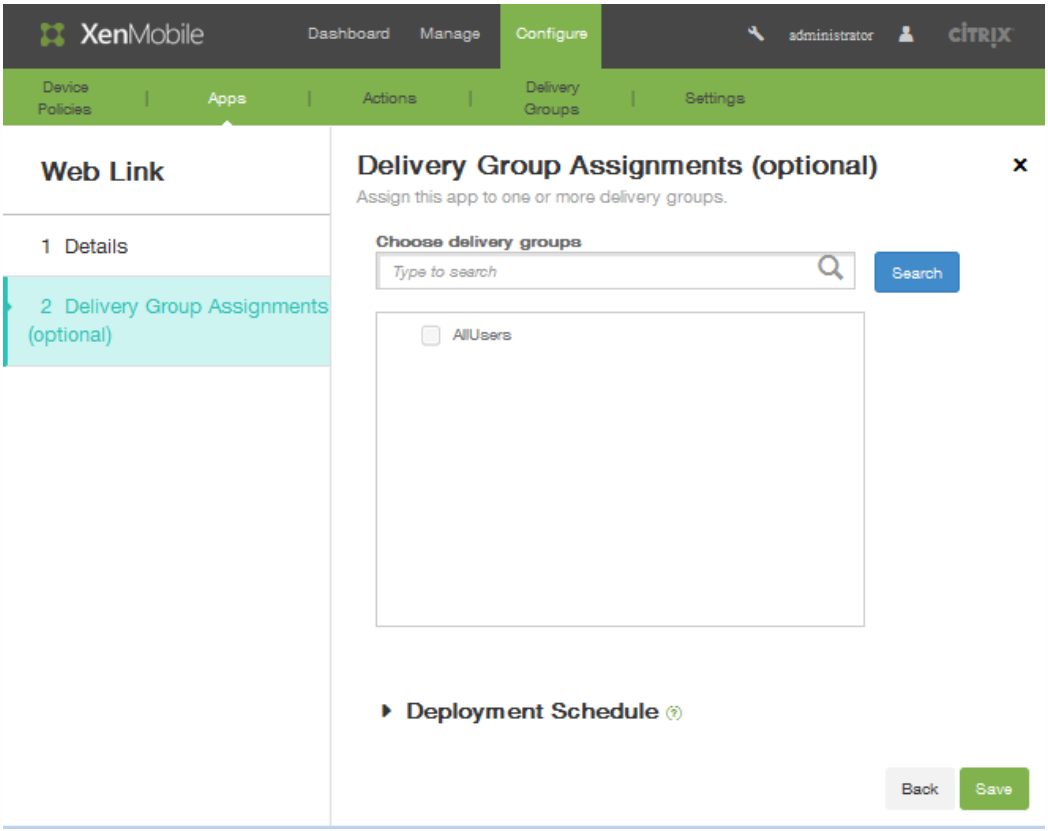
Las imágenes deben ser del tipo PNG.

5. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.

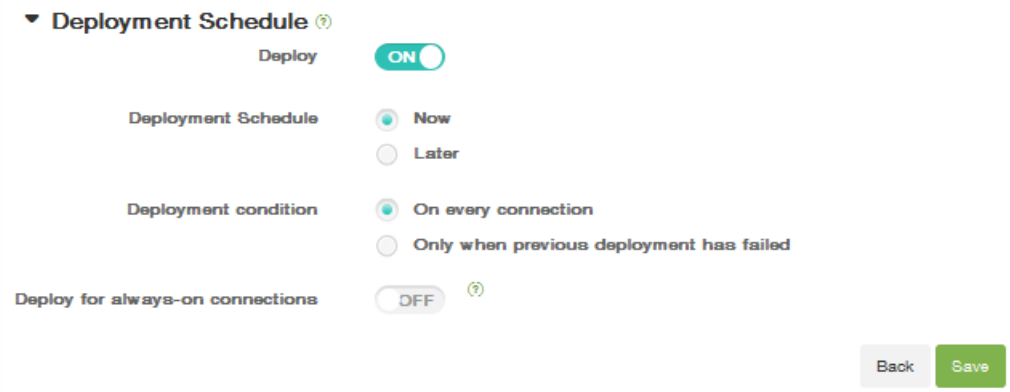


En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.

6. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.
7. Haga clic en Next.
8. Si quiere, en la página **Delivery Groups Assignment**, puede asignar la aplicación a un grupo de entrega o a varios.



9. En Choose delivery groups, busque un grupo de entrega (o varios). Marque la casilla de verificación **All Users** para asignar la aplicación a cada usuario de XenMobile.
10. Expanda Deployment Schedule para precisar más el grupo de entrega.



1. Deploy. Haga clic en ON para habilitar la programación de una implementación.
2. Deployment Schedule. Haga clic en Now o en Later para establecer la programación de la implementación.
3. Deployment condition. Haga clic para implementar la aplicación en cada conexión o solo si la implementación anterior falla.
4. En Deploy for always-on connections, haga clic en ON para que la implementación se efectúe cuando esté establecida la directiva de conexión "Always-on".
   Nota: Esta opción se aplica cuando también se han configurado las claves de implementación global en segundo plano en la sección Server Properties del área Settings de la consola de XenMobile. La directiva Deploy for always-on connection no está disponible para dispositivos iOS.
11. Haga clic en Save.

Para crear y administrar flujos de trabajo

May 05, 2016

Puede utilizar flujos de trabajo para administrar la creación y la eliminación de cuentas de usuario. Antes de poder usar un flujo de trabajo, es necesario identificar las personas dentro de su organización que tienen la autoridad de aprobar solicitudes de cuentas de usuario. Después, podrá utilizar la plantilla de flujo de trabajo para crear y aprobar solicitudes de cuentas de usuario.

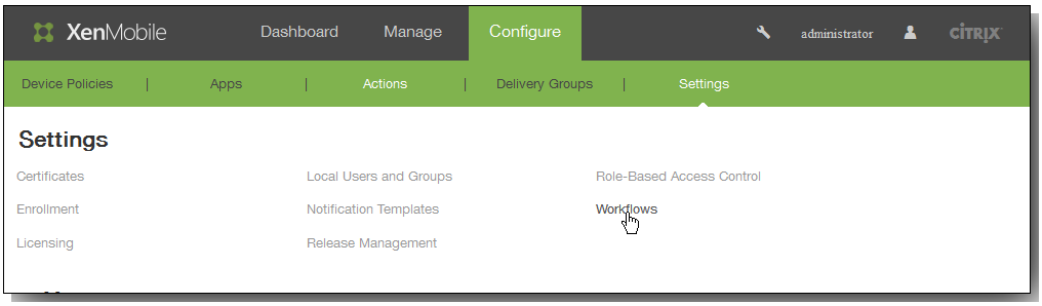
Cuando se configura XenMobile por primera vez, se definen los parámetros de correo electrónico del flujo de trabajo. Debe configurar estos parámetros para poder utilizar flujos de trabajo. Puede cambiar los parámetros de correo electrónico del flujo de trabajo en cualquier momento. Estos parámetros incluyen servidor de correo electrónico, puerto, dirección de correo electrónico, y si la solicitud para crear la cuenta de usuario requiere aprobación o no.

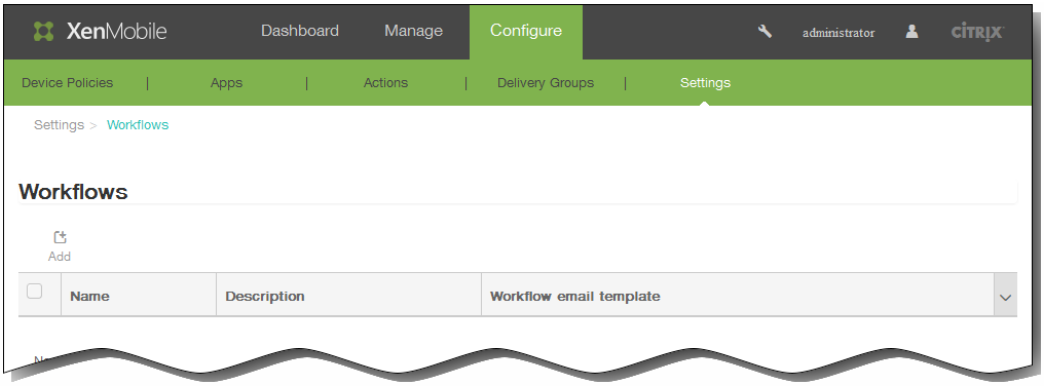
Puede configurar flujos de trabajo en dos lugares de XenMobile:

- En la página Workflows, en la consola de XenMobile. En la página Workflows, se pueden configurar varios flujos de trabajo para su uso con configuraciones de aplicaciones. Al configurar flujos de trabajo en la página Workflows, puede seleccionar el flujo de trabajo cuando configure la aplicación.
- Cuando configure un conector de aplicaciones, en la aplicación, deberá proporcionar un nombre de flujo de trabajo y definir a las personas que pueden aprobar la solicitud de cuenta de usuario. Consulte Incorporación de aplicaciones a XenMobile.

Se puede asignar hasta tres niveles de la aprobación del tipo administrador para cuentas de usuario. Si necesita que otros individuos aprueben la cuenta de usuario, puede buscar y seleccionar a más personas por su nombre o dirección de correo electrónico. Cuando XenMobile las encuentre, podrá agregarlas al flujo de trabajo. Todas las personas en el flujo de trabajo reciben correos electrónicos para aprobar o denegar la nueva cuenta de usuario.

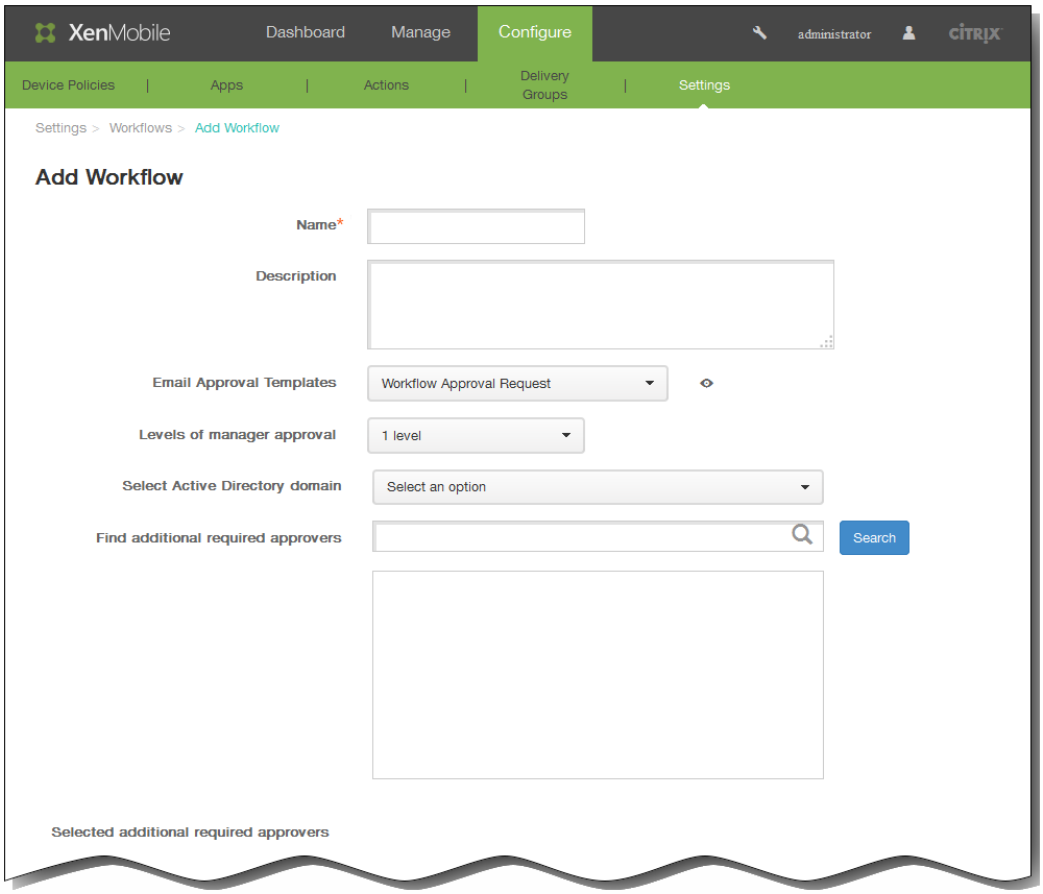
1. En la consola de XenMobile, haga clic en Configure > Settings > Workflows.





Aparecerá la página Workflows.

2. En la página Workflows, haga clic en Add. Aparecerá la página Add Workflow.



3. En la página Add Workflow, en el campo Name, escriba un nombre único para el flujo de trabajo.
4. En Description, escriba una descripción del flujo de trabajo.
5. En la lista Email Approval Templates, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. En la consola de XenMobile, puede crear plantillas de correo electrónico en la sección Notification Templates, en Settings. Cuando haga clic en el icono de la vista de datos a la derecha del campo, aparece la siguiente información.

6. En la lista Levels of manager approval, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo.
7. En la lista Select Active Directory domain, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
8. Junto a Find additional required approvers, escriba los nombres de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en Search. Los nombres se originan en Active Directory.
9. Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista Selected additional required approvers.
   Para quitar a una persona de la lista Selected additional required approvers, realice una de las siguientes acciones:
   - Haga clic en Search para ver una lista de todos los usuarios del dominio seleccionado.
   - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en Search para limitar los resultados de la búsqueda.

   Las personas de la lista Selected additional required approvers tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.
10. Haga clic en Save.
    El flujo de trabajo creado se muestra en la página Workflows.

    Después de crear el flujo de trabajo, puede ver sus detalles, las aplicaciones que tiene asociadas, o bien puede eliminarlo. El flujo de trabajo no se puede modificar una vez creado. Si necesita un flujo de trabajo con otros niveles de aprobación o con aprobadores diferentes, debe crear un nuevo flujo de trabajo.

Para ver los detalles de un flujo de trabajo y cómo eliminar uno

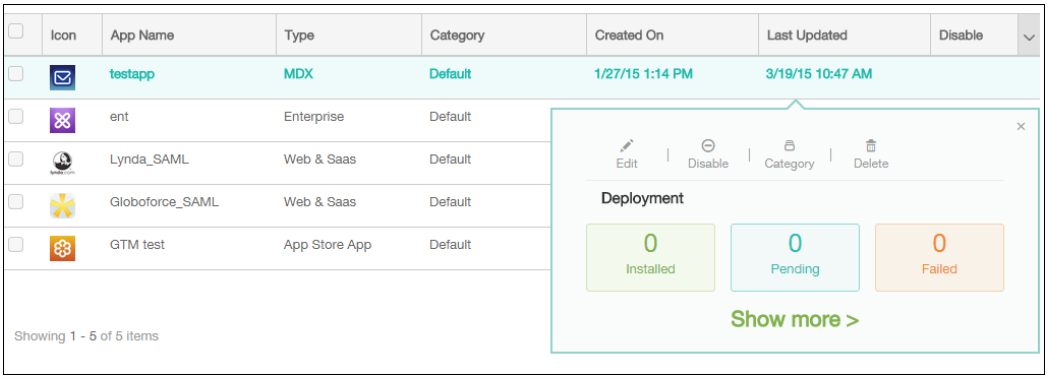
1. En la página Workflows, en la lista de los flujos de trabajo existentes, seleccione un flujo de trabajo concreto haciendo clic en la fila de la tabla o marcando la casilla de verificación situada junto al flujo de trabajo.
2. Para eliminar un flujo de trabajo determinado, haga clic en Delete. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en Delete.
   Importante: Esta operación no se puede deshacer.

Actualización de aplicaciones en XenMobile

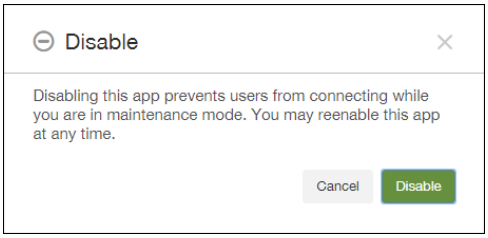
May 05, 2016

Para actualizar una aplicación en XenMobile, puede inhabilitar dicha aplicación en la consola de XenMobile y cargar luego la nueva versión de esta.

1. En la consola de XenMobile, haga clic en Configure > Apps.
2. En el caso de dispositivos administrados (dispositivos inscritos en XenMobile para la administración de dispositivos móviles), vaya directamente al paso 3. En el caso de dispositivos no administrados (dispositivos inscritos en XenMobile solo para la administración de aplicaciones de empresa), lleve a cabo lo siguiente:
   1. En la ficha de aplicaciones, haga clic para seleccionar la aplicación a actualizar y, en el menú que aparece, haga clic en Disable.

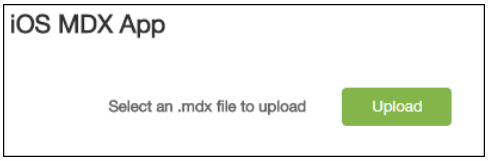


   2. En el cuadro de diálogo de confirmación, haga clic en Disable.



   La aplicación mostrará el estado Disabled en la tabla Apps.

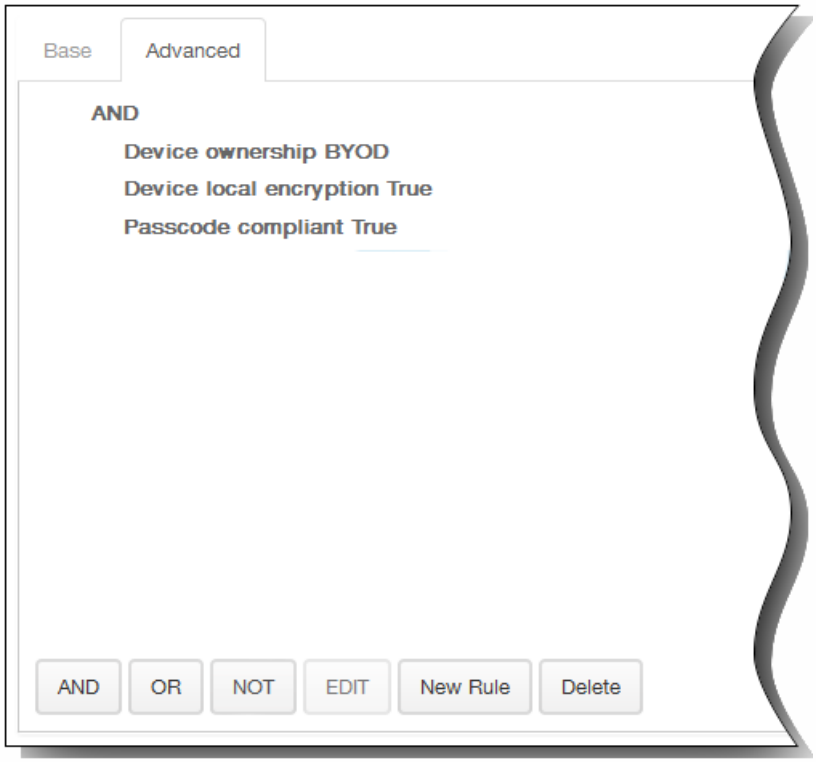
   Nota: Inhabilitar una aplicación significa colocarla en modo de mantenimiento. Mientras la aplicación esté inhabilitada, los usuarios no se podrán volver a conectar a ella después de cerrar sesión. Inhabilitar una aplicación es algo optativo, aunque Citrix recomienda inhabilitarla para evitar problemas de funcionalidad en ella. Pueden ocurrir problemas debido a actualizaciones de directivas, por ejemplo, o si los usuarios solicitan una descarga al mismo tiempo que se carga la aplicación en XenMobile.
3. Haga clic para seleccionar la aplicación y, en el menú que aparece, haga clic en Edit. La plataforma elegida en su momento para la aplicación aparecerá seleccionada.
4. Si quiere, en la página App Information, puede cambiar los valores de Name, Description o App category. A continuación, haga clic en Next.
5. Haga clic en Upload para seleccionar el archivo que se cargará para reemplazar la aplicación actual y, a continuación, haga clic en Next.



La aplicación se cargará en XenMobile. Si quiere, puede cambiar los datos de la aplicación y la configuración de la directiva.

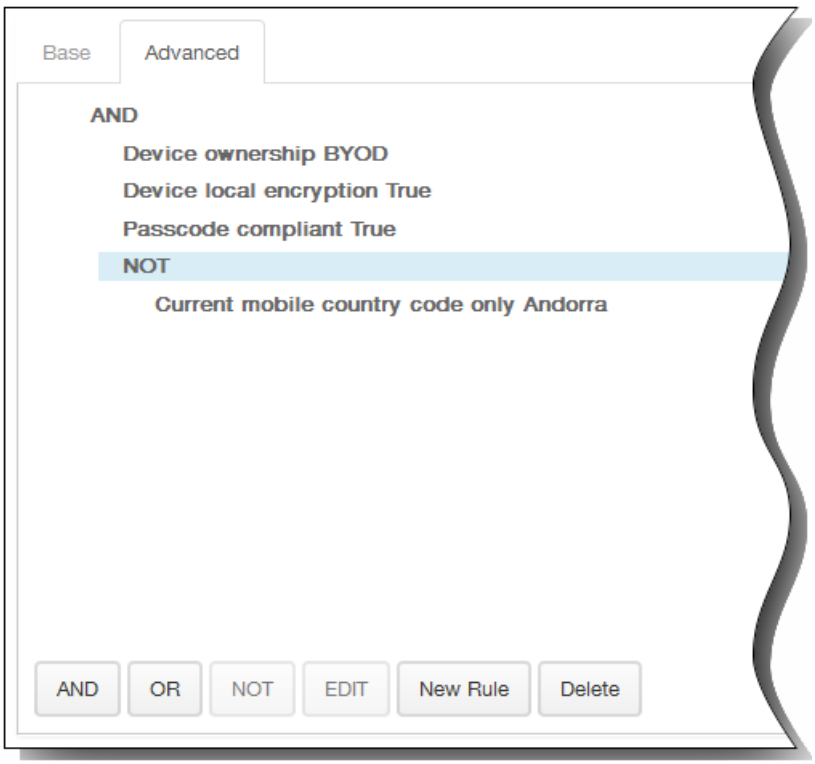
6. Haga clic en Next y, en los pasos del 8 al 14, deje los parámetros tal cual o realice los cambios relacionados con la actualización.
7. Expanda Deployment Rules. La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la aplicación.
    1. Puede optar por implementar la aplicación cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

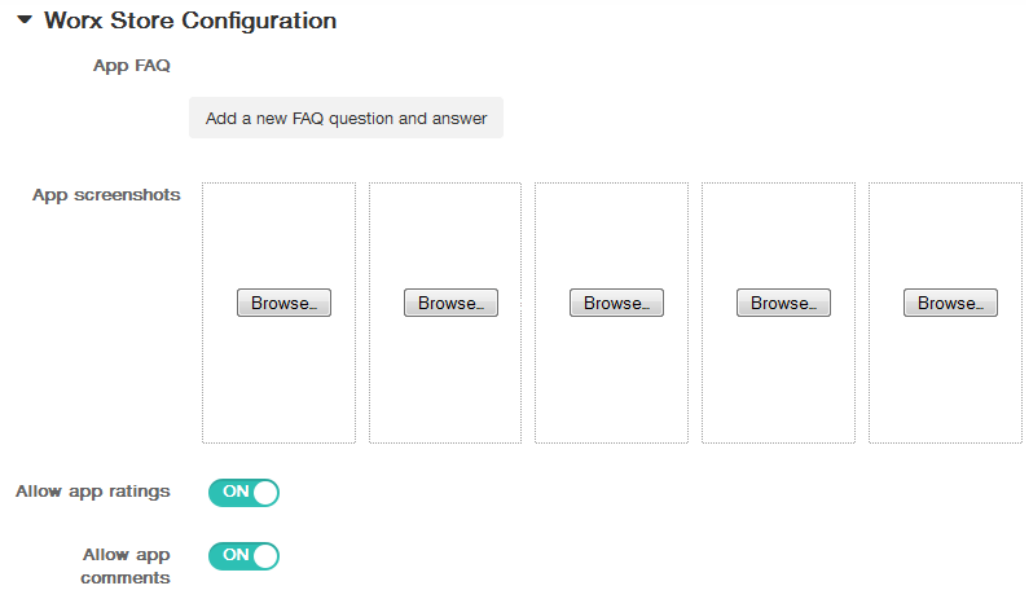


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True, el dispositivo debe cumplir el código de acceso y el código móvil del país del dispositivo no puede ser solo Andorra.

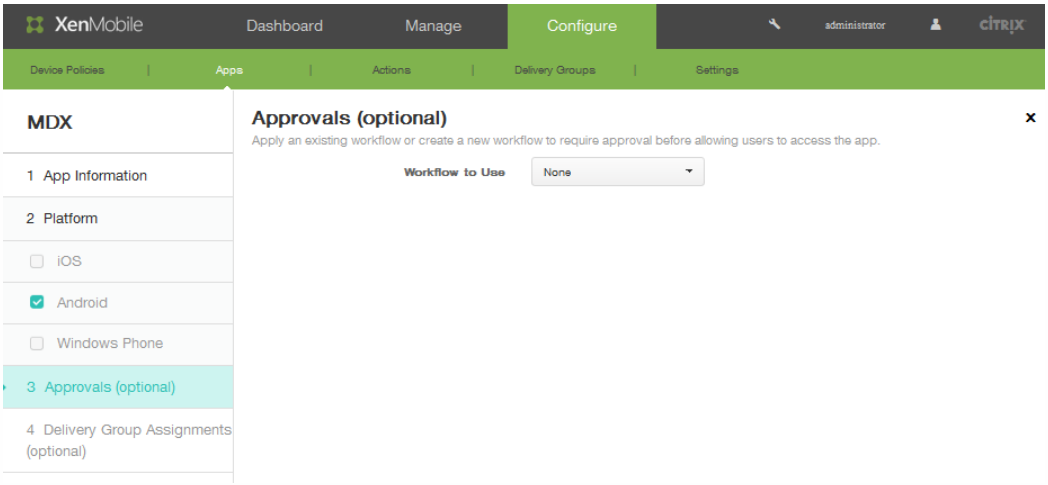


8. Expanda Worx Store Configuration para agregar preguntas frecuentes acerca de la aplicación o adjuntar capturas de pantalla para clasificar la aplicación en Worx Store. El gráfico que cargue debe estar en formato PNG. No puede cargar imágenes en formato GIF o JPEG.

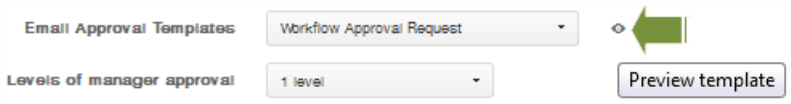


En Allow app ratings, haga clic en ON para permitir al usuario puntuar la aplicación.

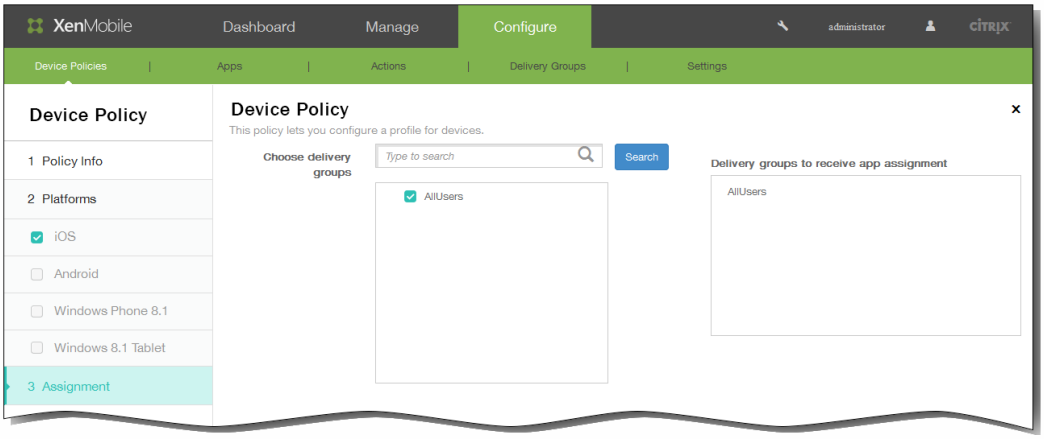
9. En Allow app comments, haga clic en ON para permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.
10. Haga clic en Next. Aparecerá la pantalla Approvals.



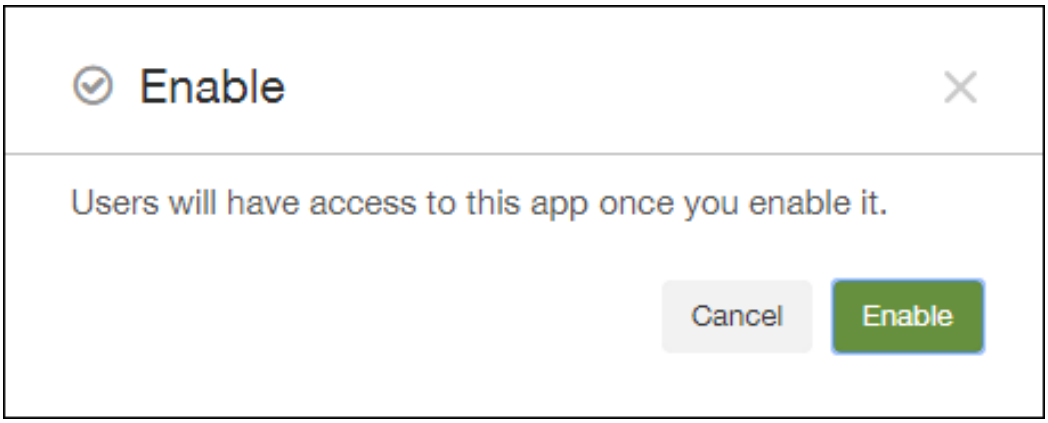
11. Al crear un nuevo flujo de trabajo, la consola de XenMobile cambia para mostrar las opciones de configuración para el proceso de aprobación. Cada uno de estos campos se describe en los pasos siguientes. Configure esos campos si necesita aprobación para crear cuentas de usuario.
    1. Especifique un nombre en el campo **Name** para el flujo de trabajo.
    2. Si quiere, indique una descripción en **Description**.
    3. En el campo **Email Approval Templates**, haga clic en una opción de notificación. Haga clic en el **icono de vista** para una vista previa de la plantilla elegida.



    4. En **Levels of manager approval**, haga clic en el nivel pertinente; puede elegir desde None hasta 3. .
    5. En **Select Active Directory domain**, haga clic en el dominio.
    6. Si quiere, en Find additional required approvers, indique otros usuarios aptos para la aprobación que sean necesarios y, a continuación, haga clic en Search.
12. Haga clic en Next.
13. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.



14. Haga clic en Save. Aparecerá la página Apps.
15. Si ha inhabilitado la aplicación en el paso 2, haga lo siguiente:
    1. En la ficha Apps, haga clic para seleccionar la aplicación actualizada y, en el menú que aparece, haga clic en Enable.
    2. En el mensaje de confirmación que aparece, haga clic en Enable.



Ahora, los usuarios podrán acceder a la aplicación y recibir una notificación que les pedirá actualizarla.

Vista general de las directivas de aplicaciones MDX

May 05, 2016

Para ver una lista de las directivas de aplicación MDX para iOS, Android y Windows Phone con notas sobre las restricciones aplicables y recomendaciones de Citrix, consulte Vista general de las directivas de aplicaciones MDX en la documentación de MDX Toolkit.

Nota: Worx Home actualiza las directivas durante determinadas acciones. Para obtener más información, consulte Administración de Worx Home.

Acciones automatizadas

May 05, 2016

En XenMobile, puede crear acciones automatizadas para programar una respuesta ante determinados eventos, ante propiedades de dispositivo o de usuario, o bien ante la existencia de ciertas aplicaciones en los dispositivos de usuario. Cuando se crea una acción automatizada, se establece el efecto en el dispositivo del usuario cuando este se conecta a XenMobile. Este efecto se establece según los desencadenadores de la acción. Cuando un evento tiene lugar, usted puede enviar una notificación al usuario para corregir el problema antes de tomar medidas más terminantes.

Por ejemplo: si quiere detectar una aplicación que ya haya bloqueado (por ejemplo, Words with Friends), puede especificar un desencadenador que establezca un dispositivo de usuario como dispositivo que no cumple los requisitos cuando se detecte Words with Friends en él. La acción notifica a dicho usuario de que debe quitar la aplicación para que su dispositivo vuelva a cumplirlos. Puede establecer un límite de tiempo de espera antes del cual el usuario debe cumplir los requisitos antes de tomar medidas más terminantes, como borrar el dispositivo de forma selectiva.

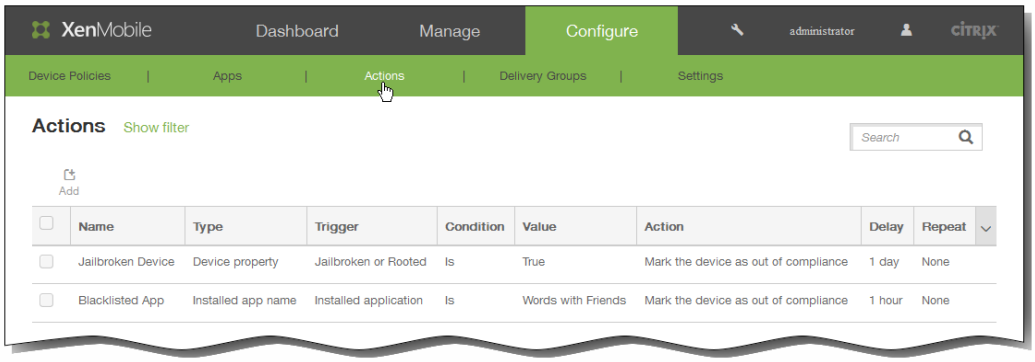
Los efectos automáticos que establezca varían entre:

- Borrar totalmente o de forma selectiva el dispositivo.
- Establecer el dispositivo como dispositivo que no cumple los requisitos.
- Revocar el dispositivo.
- Enviar una notificación al usuario para corregir el problema antes de tomar medidas más terminantes.

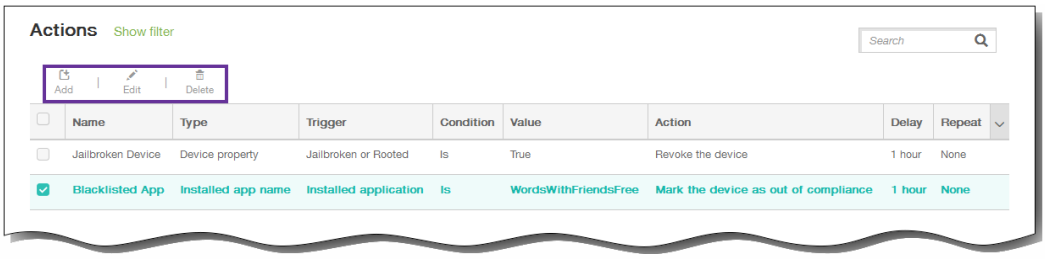
Nota: Antes de notificar a los usuarios, primero debe configurar los servidores de notificaciones en Settings para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes (consulte Notificaciones en XenMobile). Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificaciones, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.

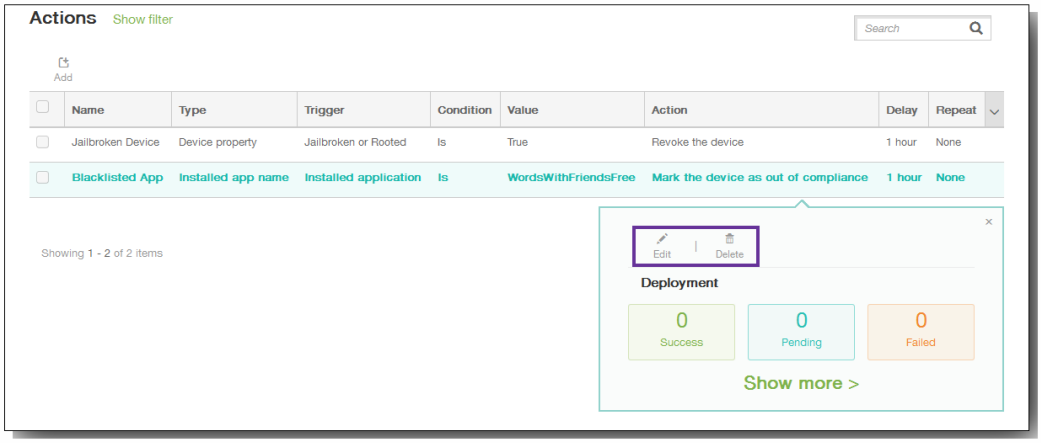
En este apartado, se explica cómo agregar, modificar y filtrar acciones automatizadas en XenMobile.

1. En la consola de XenMobile, haga clic en Configure > Actions. Aparecerá la página Actions.

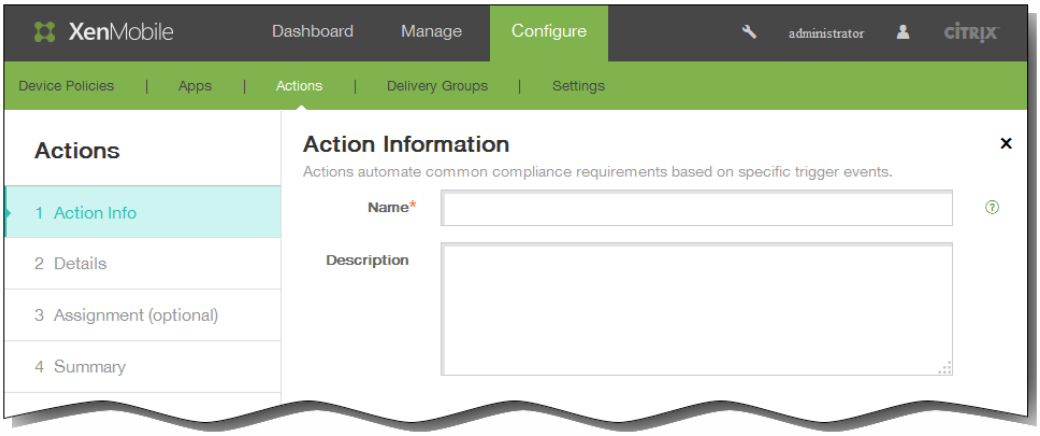


2. En la página Actions, lleve a cabo alguna de estas acciones:
   - Haga clic en Add para agregar una nueva acción.
   - Seleccione una acción existente para modificarla o eliminarla. Haga clic en la opción pertinente.
     Nota: Si marca la casilla situada junto a una acción, el menú de opciones aparecerá encima de la lista de acciones. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.

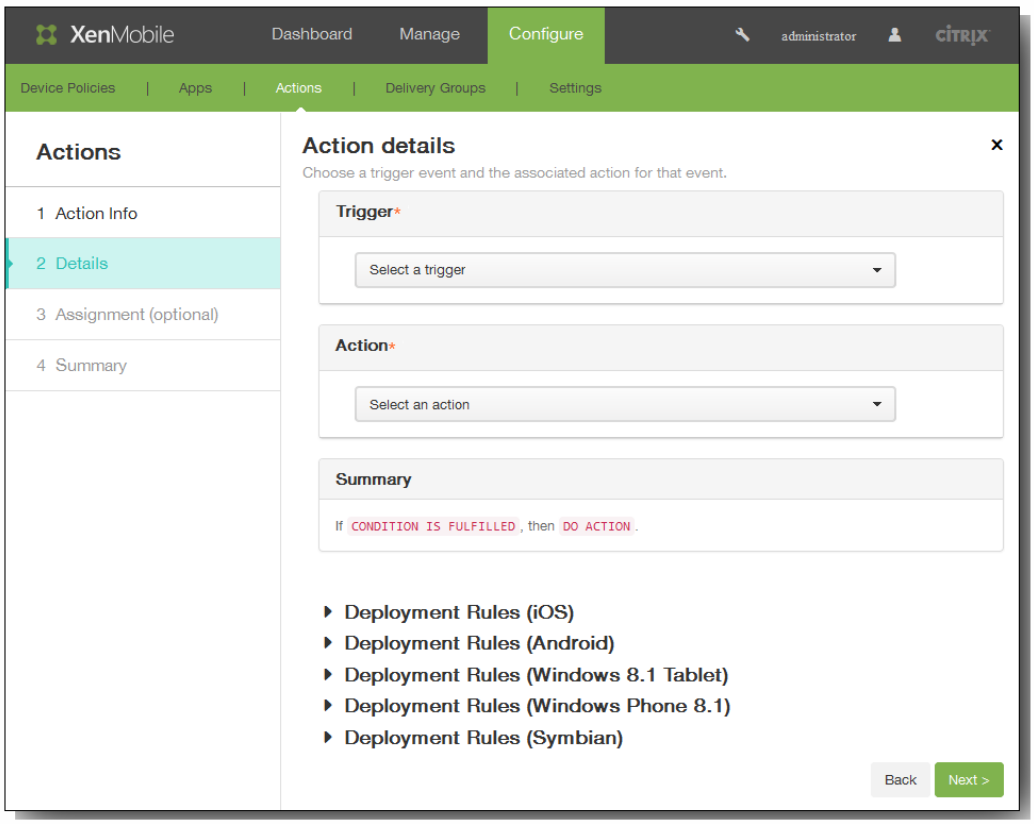




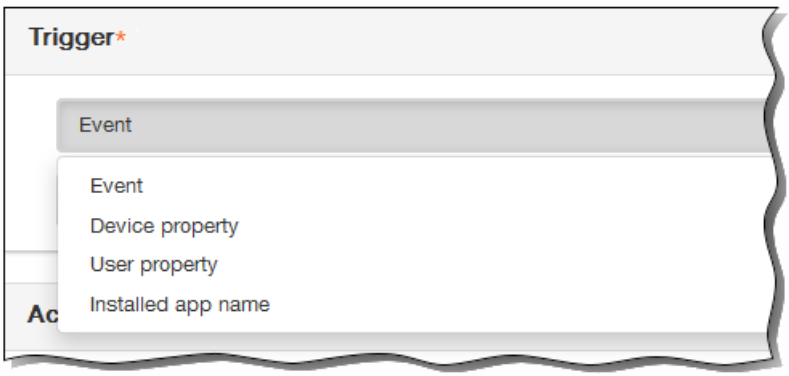
Aparecerá la página Action Information.



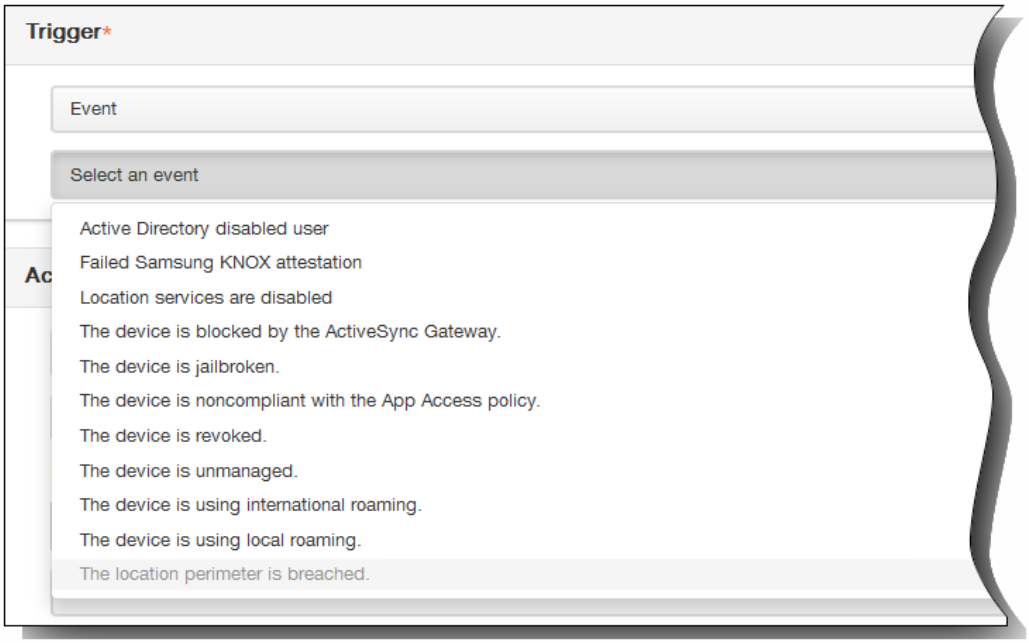
3. En la página Action Information, escriba o modifique la información siguiente:
   1. Name. Escriba un nombre para identificar de forma exclusiva la acción. Este campo es obligatorio.
   2. Description. Describa en qué consiste la acción.
4. Haga clic en Next. Aparecerá la página Action details.
   Nota: En el siguiente ejemplo se muestra cómo configurar un desencadenador de eventos. Si selecciona otro activador, las opciones resultantes serán distintas a las mostradas aquí.



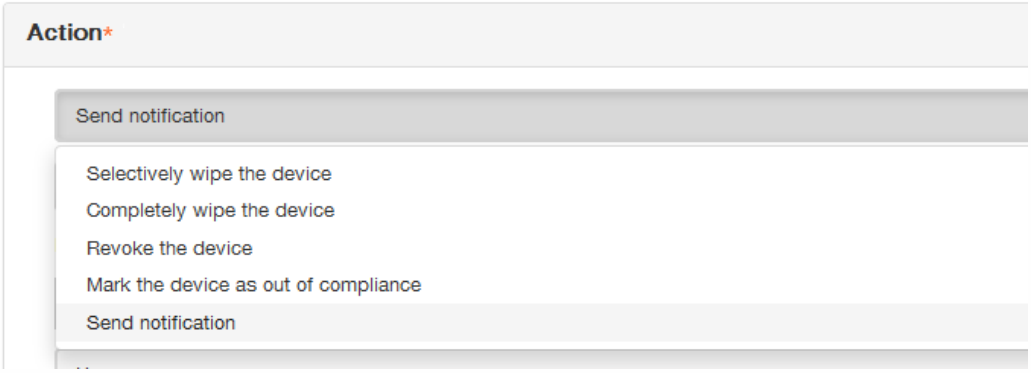
5. En la página Action details, escriba o modifique la información siguiente:
   1. En la lista Trigger, haga clic en el tipo de desencadenador de eventos para esta acción. El significado de cada desencadenador es el siguiente:
      - Event. Reacciona ante un evento determinado.
      - Device property. Comprueba un atributo de dispositivo en el dispositivo recopilado en el modo de administración de dispositivos móviles y reacciona ante él.
      - User property. Reacciona ante un atributo de usuario, generalmente de Active Directory.
      - Installed app name. Reacciona ante una aplicación instalada. Requiere que la directiva de inventario de aplicaciones esté habilitada en el dispositivo. De forma predeterminada, la directiva de inventario de aplicaciones está habilitada en todas las plataformas. Para obtener más información, consulte Para agregar una directiva de inventario de aplicaciones para dispositivos.



2. En la siguiente lista, haga clic en la respuesta del desencadenador.

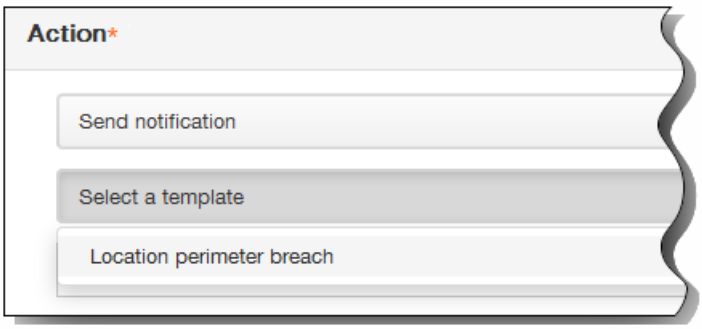


3. En la lista Action, haga clic en la acción que se debe realizar cuando se cumplan los criterios del desencadenador. A excepción de Send notification, puede elegir un intervalo de tiempo en que los usuarios puedan resolver el problema que haya activado el desencadenador. Si el problema no se resuelve en ese período de tiempo, se llevará a cabo la acción seleccionada.



En la parte restante de este procedimiento, se explica la acción de enviar una notificación.

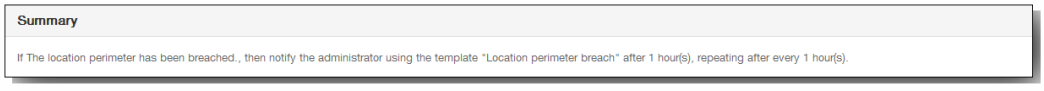
4. En la siguiente lista, seleccione la plantilla a utilizar para la notificación. Aparecerán las plantillas de las notificaciones pertinentes para el evento seleccionado.
Nota: Antes de notificar a los usuarios, primero debe configurar los servidores de notificaciones en Settings para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes (consulte Notificaciones en XenMobile). Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificación, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.



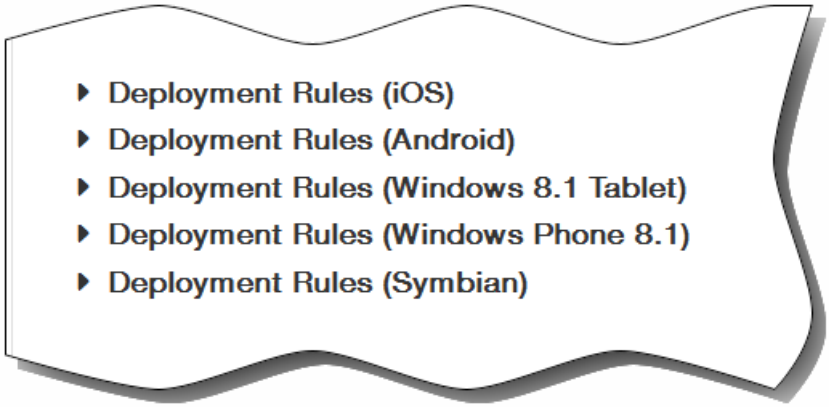
Nota: Después de seleccionar la plantilla, puede obtener una vista previa de la notificación al hacer clic en Preview notification message.

5. En los siguientes campos, establezca el tiempo que debe transcurrir en días, horas y minutos antes de tomar medidas, así como el intervalo en el que la acción se repite hasta que el usuario resuelva la situación.

6. En Summary, verifique que la acción automatizada que ha creado es la acción esperada.

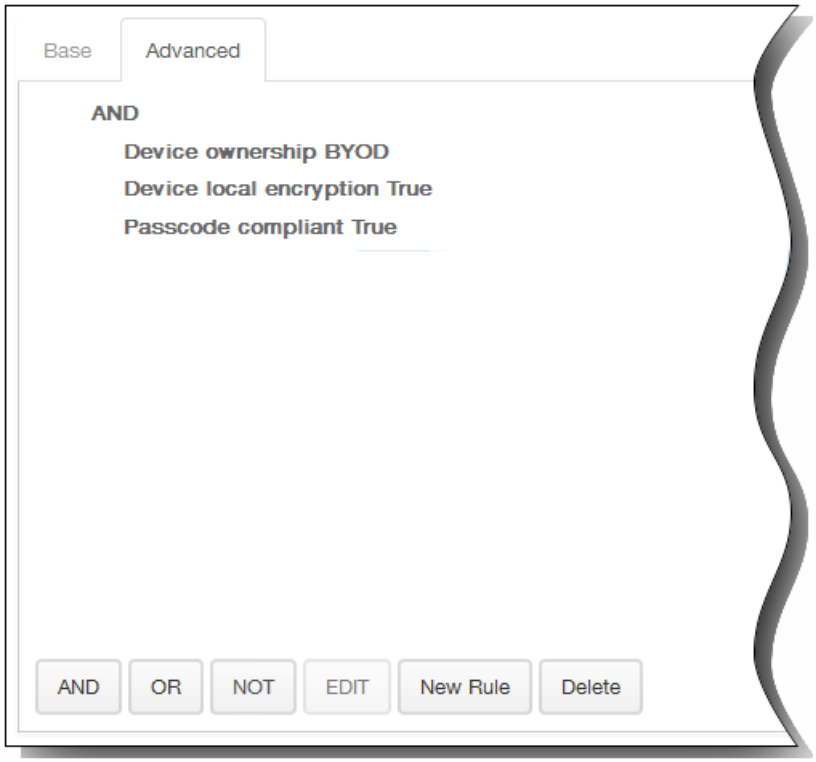


Después de configurar los datos detallados de la acción, puede configurar las reglas de implementación correspondientes a cada plataforma de forma individual: iOS, Android, tabletas Windows 8.1, Windows Phone 8.1 y Symbian. Para ello, siga los pasos del 6 al 9 para cada plataforma seleccionada.



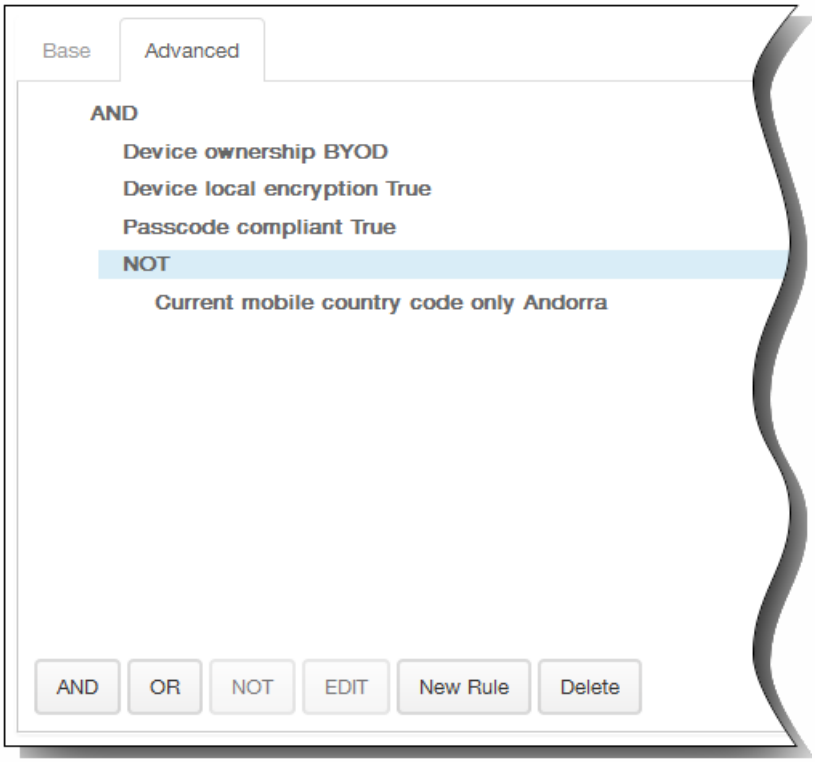
6. Expanda Deployment Rules. La ficha Base aparece de forma predeterminada.

1. En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la acción.
    1. Puede optar por implementar la acción cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es All.
    2. Haga clic en New Rule para definir las condiciones.
    3. En las listas, haga clic en las condiciones (por ejemplo, Device ownership y BYOD) tal y como se muestra en la ilustración anterior.
    4. Si quiere agregar más condiciones, haga clic en New Rule de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha Advanced para combinar las reglas con opciones booleanas.

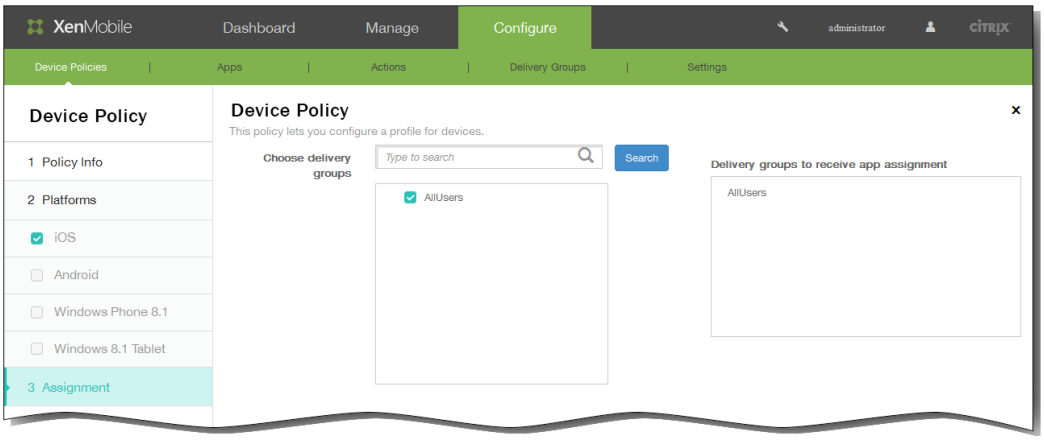


Las condiciones que haya elegido aparecerán en la ficha Base.

3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   1. Haga clic en AND, OR o NOT.
   2. En la lista que aparece, seleccione las condiciones que quiere agregar a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho para agregarlas.
      En cualquier momento, puede hacer clic y seleccionar una condición para modificarla o eliminarla si hace clic en EDIT o en Delete respectivamente.
   3. Si quiere agregar más condiciones, haga clic en New Rule de nuevo.
      En este ejemplo, el dispositivo debe ser personal del empleado, el cifrado local del dispositivo debe ser True, el dispositivo debe cumplir el código de acceso y el código móvil del país del dispositivo no puede ser solo Andorra.



7. Tras configurar las reglas de implementación de las plataformas para la acción, haga clic en Next. Aparecerá la página de asignación Actions, en la que puede asignar la acción a un grupo o grupos de entrega. Este paso es opcional.
8. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.

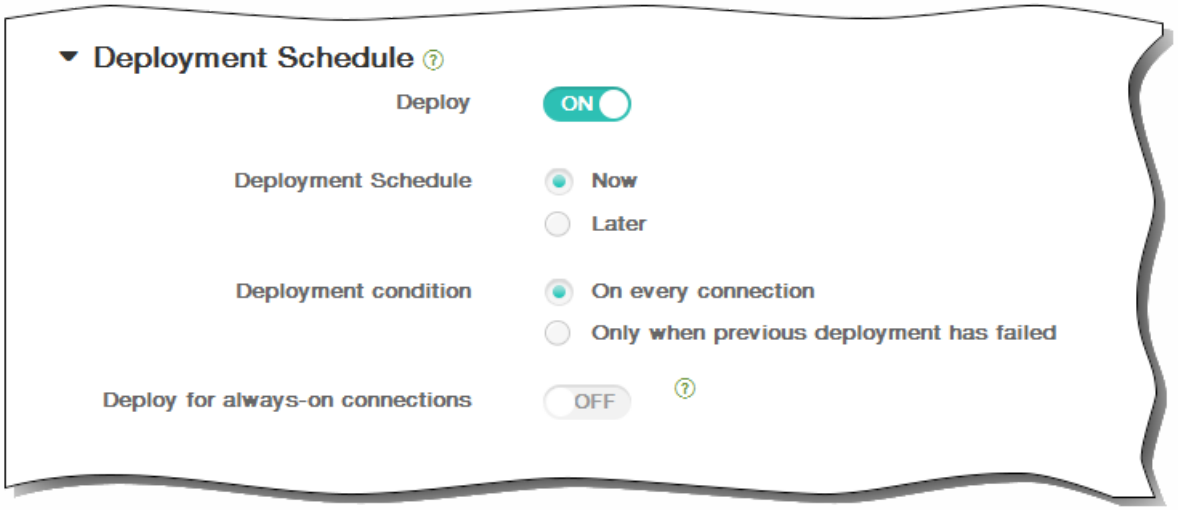


9. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:
    1. Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
    2. Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
    3. Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    4. Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has

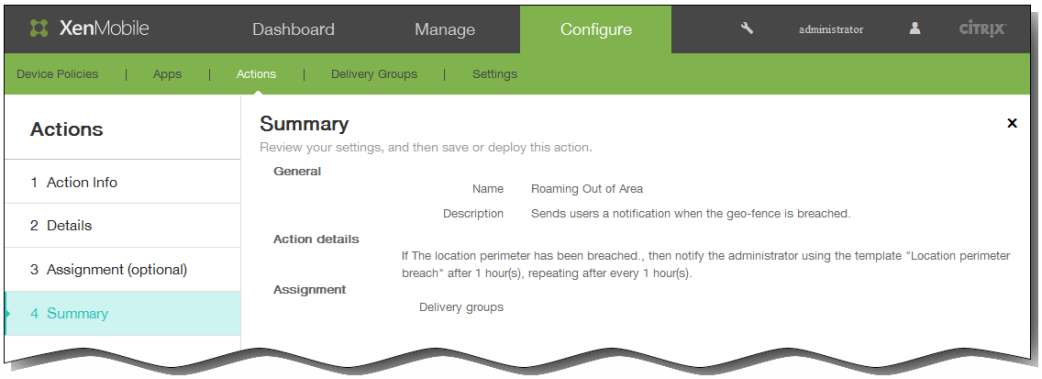
failed. La opción predeterminada es On every connection.

5. Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.
   Nota: Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.



10. Haga clic en Next. Aparecerá la página Summary, donde puede comprobar la configuración de la acción.



11. Haga clic en Save para guardar la acción.

Parámetros de cliente en XenMobile

May 05, 2016

En XenMobile, puede configurar los parámetros de cliente mediante la consola Web de XenMobile.

1. En la consola de XenMobile, haga clic en Configure y, a continuación, haga clic en Settings. Aparecerá la página Settings.
2. Haga clic en More.
3. En **Client**, haga clic en la opción que quiere configurar.

Para crear marcas personalizadas de Worx Store en dispositivos iOS

Oct 31, 2016

Puede configurar el modo en que aparecen las aplicaciones en la tienda o almacén de aplicaciones y agregar un logotipo de su propia marca en Worx Home y WorxStore en dispositivos móviles iOS y Android.

Nota: Antes de comenzar, compruebe que la imagen de personalización de marca está preparada y se puede acceder a ella.

- El nombre del archivo debe estar en formato PNG.
- Use un texto o logotipo blancos puros con un fondo transparente de 72 ppp.
- El logotipo de empresa no debe superar el alto o el ancho de 170 píxeles x 25 píxeles (1x) + 340 píxeles x 50 píxeles (2x).
- Establezca el nombre de los archivos como Header.png y Header@2x.png.
- Cree un archivo ZIP con los archivos, no una carpeta con los archivos en ella.

1. En la consola de XenMobile, haga clic en Configure > Settings > More > Worx Store Branding.
2. Junto a Default store view, seleccione Category o A-Z.
3. Junto a Device option, seleccione Phone o Tablet.
4. Junto a Branding file, haga clic en Browse para seleccionar una imagen o archivo ZIP de imágenes a utilizar para la personalización de marca. A continuación, haga clic en Save.

Para implementar este paquete en los dispositivos de los usuarios, debe crear un paquete de implementación e implementarlo en los dispositivos.

Para crear opciones de asistencia de Worx Home y GoToAssist

May 05, 2016

1. En la consola de XenMobile, haga clic en Configure > Settings > More > Worx Home Support.
2. En la página Worx Home Support, escriba un valor para los siguientes campos:
    1. Support email (IT help desk)
    2. Support phone (IT help desk)
    3. Token for GoToAssist chat
    4. GoToAssist support ticket email

La información de asistencia de Worx Home que cree aparecerá en la lista Client Properties, en la consola de XenMobile, asociada a las siguientes claves: SUPPORT_EMAIL, SUPPORT_PHONE, GTA_CHAT y GTA_TICKET.

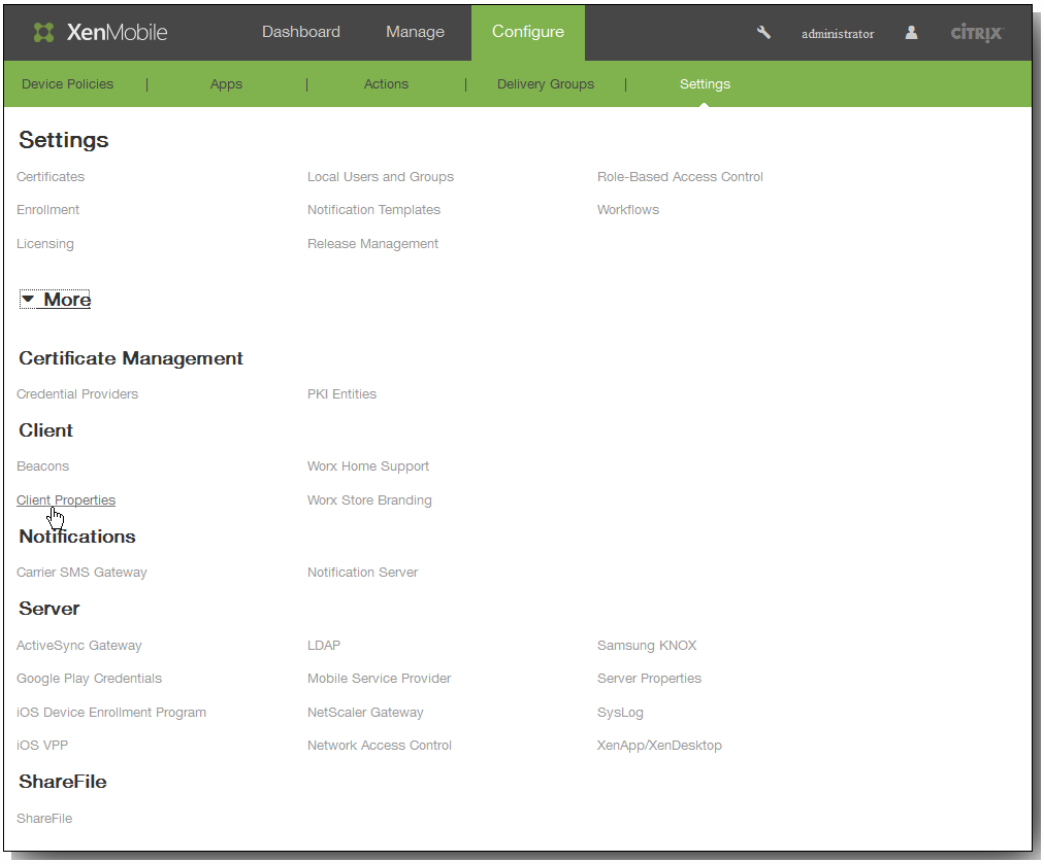
Para agregar, modificar o eliminar propiedades de cliente

May 05, 2016

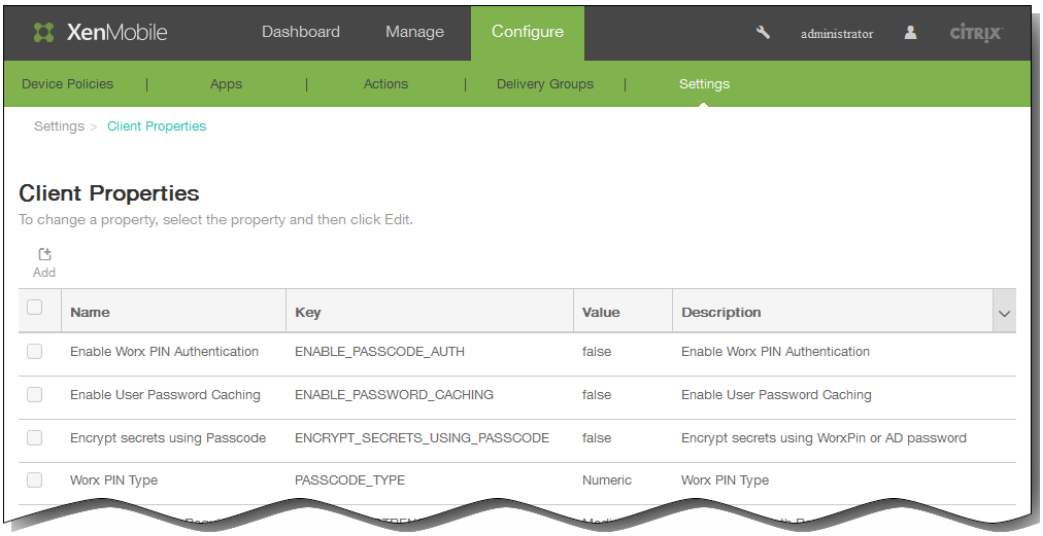
Las propiedades de cliente contienen información que se proporciona directamente a Worx Home en los dispositivos de los usuarios. Estas propiedades se usan para definir parámetros de configuración avanzada, como el PIN de Worx. Las propiedades de cliente se obtienen del servicio de asistencia de Citrix.

Nota: Las propiedades de cliente están sujetas a cambios en cada versión de las aplicaciones cliente, especialmente Worx Home.

1. En la consola de XenMobile, haga clic en Configure > Settings > More > Client Properties.

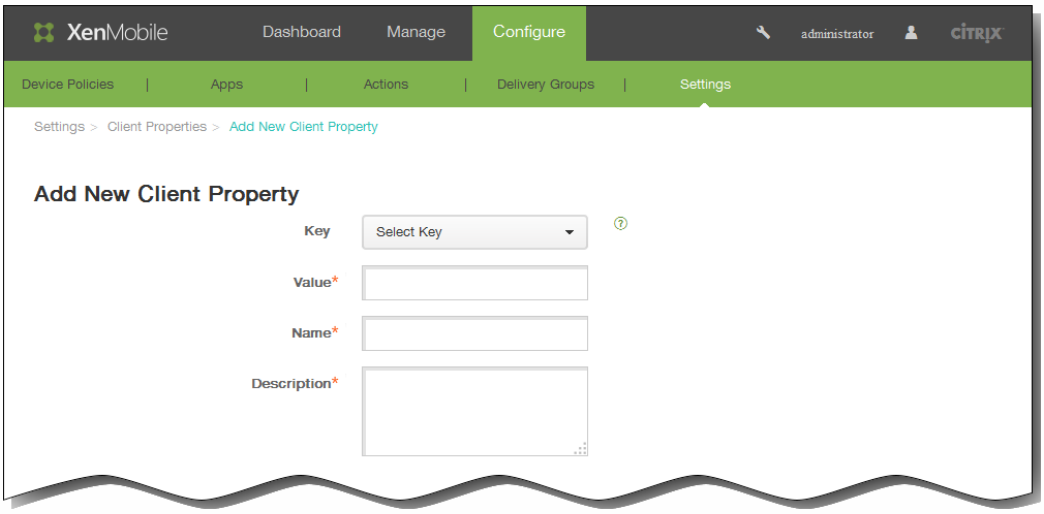


Aparecerá la página Client Properties. Puede agregar, modificar y eliminar las propiedades de cliente desde esta página.



Para agregar una propiedad de cliente

1. En la página Client Properties, haga clic en Add. Aparecerá la página Add New Client Property.

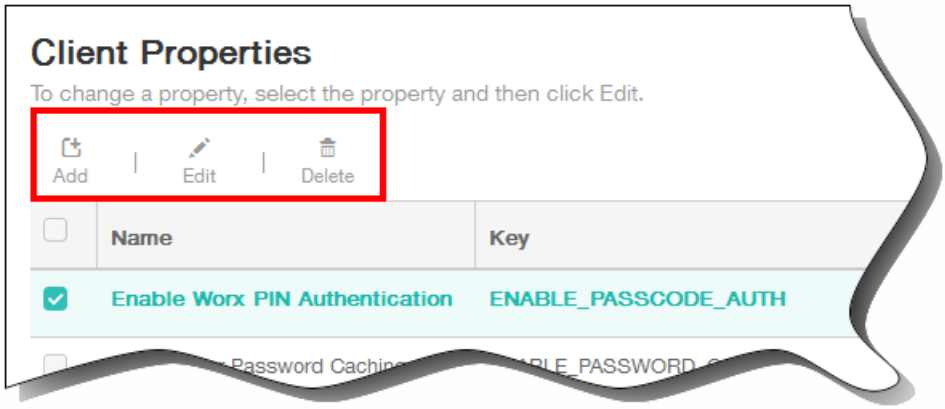


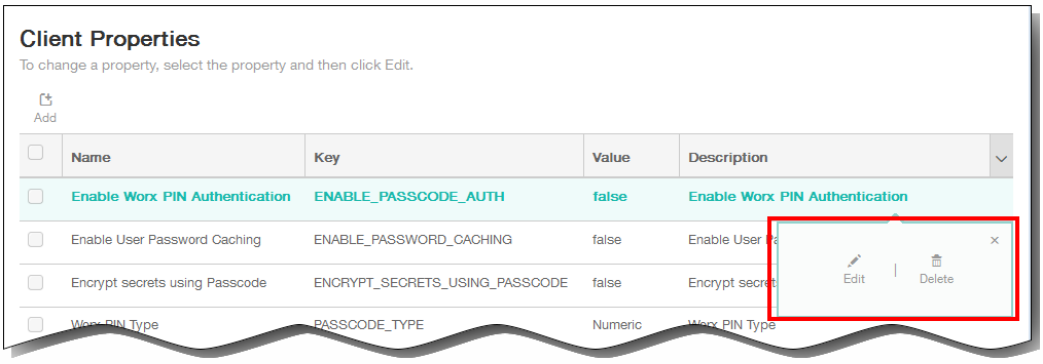
2. En la página Add New Client Property, escriba la información siguiente:
   Nota: Todos los campos son obligatorios.
   1. Key. En la lista, haga clic en la clave de propiedad que quiera agregar.
      Importante: Póngase en contacto con el servicio de asistencia de Citrix antes de realizar cambios o solicite una clave especial para realizar algún cambio.
   2. Value. Introduzca el valor de la propiedad seleccionada.
   3. Name. Introduzca un nombre para la propiedad.
   4. Description. Introduzca una descripción de la propiedad.

Para modificar una propiedad de cliente

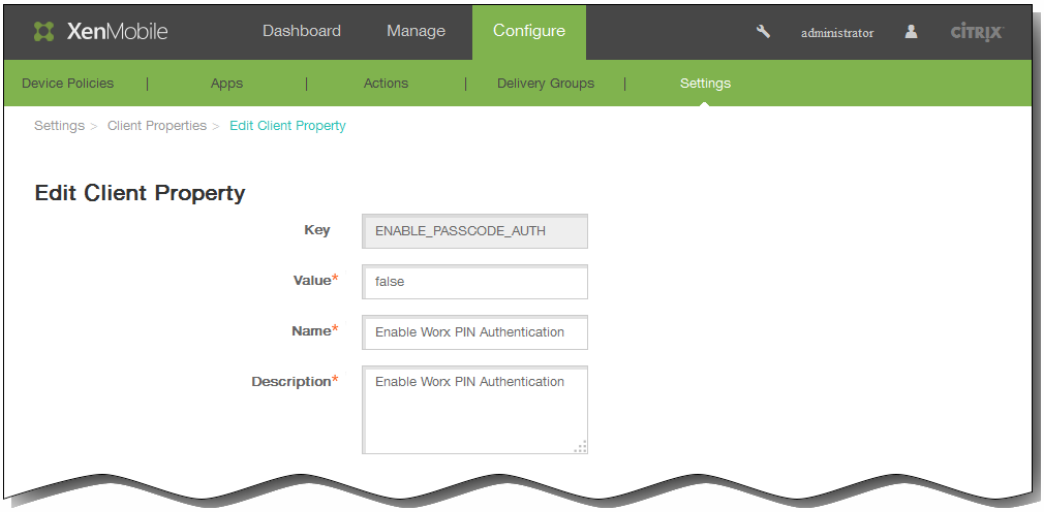
1. En la tabla Client Properties, seleccione la propiedad de cliente que quiere modificar.
   Nota: Si marca la casilla situada junto a una propiedad de cliente, el menú de opciones aparecerá encima de la lista de propiedades de cliente. En cambio, si hace clic en cualquier lugar de la lista, el menú de opciones aparecerá en el lado

derecho de la lista.





2. Haga clic en Edit. Aparecerá la página Edit Client Property.



3. Cambie la siguiente información como corresponda:
   1. Value. El valor de la propiedad seleccionada.
   2. Name. El nombre de la propiedad.

3. Description. La descripción de la propiedad.
4. Haga clic en Save para guardar los cambios o en Cancel para no realizar cambios en la propiedad.

Para eliminar una propiedad de cliente

1. En la tabla Client Properties, seleccione la propiedad de cliente que quiere eliminar.
   Nota: Puede eliminar más de una propiedad. Para ello, deberá marcar la casilla de verificación situada junto a cada propiedad.
2. Haga clic en Delete. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en Delete.

Referencia de propiedades del cliente

Oct 31, 2016

A continuación, se indican las propiedades de cliente predefinidas en XenMobile, así como sus valores predeterminados.

ENABLE_PASSCODE_AUTH

Nombre simplificado: Habilitar la autenticación de PIN de Worx

Esta clave permite activar la función de PIN de Worx. Si se activa la función de PIN o código de acceso de Worx, se solicita a los usuarios que definan un número PIN que se usará en lugar de su contraseña de Active Directory. Este parámetro se habilita automáticamente si la propiedad ENABLE_PASSWORD_CACHING está habilitada o si XenMobile usa la autenticación de certificados.

Si los usuarios realizan una autenticación sin conexión, el PIN de Worx se valida localmente y se permite a los usuarios acceder a la aplicación o al contenido solicitado. Si los usuarios realizan una autenticación con conexión, se utiliza el PIN o el código de acceso de Worx para desbloquear la contraseña de Active Directory o el certificado, que luego se envía para realizar la autenticación en XenMobile.

Valores posibles: true o false

Valor predeterminado: false

ENABLE_PASSWORD_CACHING

Nombre simplificado: Habilitar el almacenamiento en caché de la contraseña de usuario

Esta clave permite que la contraseña de Active Directory de los usuarios se almacene en la memoria caché local del dispositivo móvil. Al establecer esta clave en true, se solicita a los usuarios que establezcan un PIN o un código de acceso de Worx. El valor de la clave ENABLE_PASSCODE_AUTH debe establecerse en true si esta clave se establece en true.

Valores posibles: true o false

Valor predeterminado: false

ENCRYPT_SECRETS_USING_PASSCODE

Nombre simplificado: Cifrar secretos mediante un código de acceso

Esta clave permite que los datos confidenciales se almacenen en el dispositivo móvil, en un almacén secreto, en lugar de guardarse en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta clave de configuración permite un cifrado seguro de los artefactos de la clave, pero también agrega entropía de usuario (un código PIN aleatorio generado por el usuario y que solo el usuario conoce).

Citrix recomienda habilitar esta clave para facilitar una mayor seguridad en los dispositivos de usuario.

Nota: La habilitación de esta clave afecta a la experiencia de los usuarios en cuanto a una mayor cantidad de solicitudes de autenticación para el PIN de Worx.

Valores posibles: true o false

Valor predeterminado: false

PASSCODE_TYPE

Nombre simplificado: Tipo de PIN de Worx

Esta clave define si el usuario puede definir un PIN numérico de Worx o un código de acceso alfanumérico de Worx. Si selecciona el valor Numeric, el usuario solo podrá definir un valor numérico para el PIN de Worx. Si selecciona el valor Alphanumeric, el usuario podrá utilizar una combinación de letras y números para el código de acceso a Worx.

Nota: Si cambia este parámetro, se solicitará a los usuarios que establezcan un nuevo PIN o código de acceso a Worx la próxima vez que deban autenticarse.

Valores posibles: Numeric o Alphanumeric

Valor predeterminado: Numeric

PASSCODE_EXPIRY

Nombre simplificado: Requerimiento de caducidad del PIN de Worx

Esta clave define el tiempo en días durante los que el PIN o código de acceso de Worx es válido. Una vez transcurrido ese período, se obliga al usuario a cambiar su PIN o código de acceso de Worx. Si cambia este parámetro, el nuevo valor se establece solamente cuando el PIN o el código de acceso de Worx actuales caducan.

Valores posibles: de 1 a 99

Valor predeterminado: 90

PASSCODE_HISTORY

Nombre simplificado: Números PIN anteriores de Worx

Esta clave define la cantidad de números PIN o códigos de acceso de Worx usados anteriormente que los usuarios no pueden volver a utilizar cuando cambien sus números PIN o códigos de acceso de Worx. Si cambia esta opción de configuración, el nuevo valor se establece la próxima vez que el usuario restablezca su PIN o código de acceso a Worx.

Valores posibles: de 1 a 99

Valor predeterminado: 5

PASSCODE_MAX_ATTEMPTS

Nombre simplificado: Cantidad máxima de intentos del PIN de Worx

Esta clave define cuántos números PIN o códigos de acceso de Worx incorrectos pueden introducir los usuarios antes de que se les solicite una autenticación completa. Después de que los usuarios realicen correctamente una autenticación completa, se les solicita que creen un nuevo PIN o código de acceso de Worx.

Valores posibles: Cualquier número entero positivo

Valor predeterminado: 15

INACTIVITY_TIMER

Nombre simplificado: Temporizador de inactividad

Esta clave define el tiempo en minutos que los usuarios pueden dejar su dispositivo inactivo y luego acceder a una aplicación sin que se solicite un PIN o un código de acceso de Worx. Si quiere habilitar este parámetro para una aplicación MDX, debe establecer el parámetro App Passcode en On. Si el parámetro App Passcode está establecido en Off, se redirige a los usuarios a Worx Home para una autenticación completa. Al cambiar este parámetro, el valor se aplicará la próxima vez que los usuarios deban autenticarse. **Nota**: En iOS, el temporizador de inactividad también controla el acceso a Worx Home, no solo a las aplicaciones MDX.

Valores posibles: Cualquier número entero positivo

Valor predeterminado: 15

PASSCODE_STRENGTH

Nombre simplificado: Requerimiento de seguridad del PIN de Worx

Esta clave define la seguridad del PIN o código de acceso de Worx. Si cambia este parámetro, se solicitará a los usuarios que establezcan un nuevo PIN o código de acceso de Worx la próxima vez que deban autenticarse.

Valores posibles: Low, Medium, o Strong

Valor predeterminado: Medium

En la siguiente tabla se describen las reglas de contraseña para cada parámetro de nivel de seguridad, basado en el parámetro que seleccione para PASSCODE_TYPE:

Seguridad del código de acceso	Reglas para un código de acceso de tipo numérico	Reglas para un código de acceso de tipo alfanumérico
Baja	Se permiten todos los números y todas las secuencias	Debe contener al menos una letra y un número. **No permitido**: AAAaaa, aaaaaa, abcdef **Permitido**: aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Media (parámetro predeterminado)	1. Los números no pueden ser iguales. Por ejemplo, no se permite 444444. 2. Los números no pueden ser consecutivos. Por ejemplo, no se permite 123456 o 654321. **Permitido**: 444333, 124567, 136790, 555556, 788888	Además de las reglas para el nivel bajo de seguridad del código de acceso: 1. Las letras y los números no pueden ser iguales. Por ejemplo, no se permiten aaaa11, aa11aa o aaa111. 2. Ni letras ni números pueden ser consecutivos. Por ejemplo, no se permiten abcd12, bcd123, 123abc, xy1234, xyz345, o cba123. **Permitido**: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~

Nivel de seguridad alto	Lo mismo que para el nivel medio del PIN o código de acceso de Worx.	El código de acceso debe incluir al menos un número, un símbolo especial, una letra mayúscula y una letra minúscula. **No permitido**: abcd12, Abcd12, dfgh12, jkrtA2 **Permitido**: Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

ENABLE_CRASH_REPORTING

Nombre simplificado: Habilitar la generación de informes de errores

Esta clave habilita o inhabilita los informes de errores que utilizan Crashlytics para aplicaciones Worx.

Valores posibles: true o false

Valor predeterminado: true

DISABLE_LOGGING

Nombre simplificado: Inhabilitar los registros

Esta clave permite inhabilitar la capacidad de los usuarios para recopilar y cargar registros desde sus dispositivos. Se inhabilita el registro para Worx Home y para todas las aplicaciones MDX instaladas. Los usuarios no pueden enviar registros de ninguna aplicación desde la página de asistencia; aunque aparezca el cuadro de diálogo para redactar correos, los registros no se adjuntan y se muestra un mensaje que indica que el registro está inhabilitado. Además del efecto en los dispositivos de los usuarios, en la consola de XenMobile no puede modificar los parámetros de registro para Worx Home y las aplicaciones MDX.

Cuando esta clave se establece en true, Worx Home establece en true la opción Block application logs, con lo que las aplicaciones MDX dejan de registrar eventos cuando se aplica la nueva directiva.

Valores posibles: true o false

Valor predeterminado: false (el registro está habilitado)

Parámetros de servidor en XenMobile

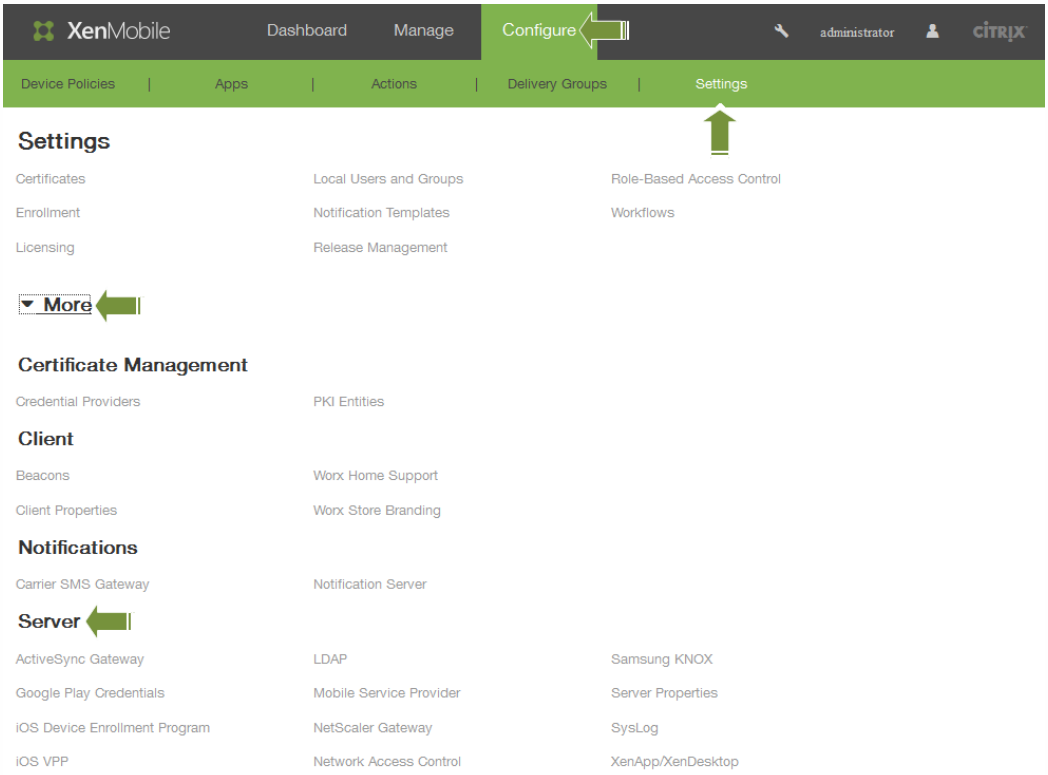
May 05, 2016

En XenMobile, puede configurar los parámetros de servidor mediante la consola Web de XenMobile.

Opciones de configuración del servidor:

ActiveSync Gateway	Programa VPP de iOS	NetScaler Gateway	Propiedades de servidor
Credenciales de Google Play	LDAP	Control de acceso de red	SysLog
iOS Device Enrollment Program	Proveedor de servicios móviles	Samsung KNOX	XenApp/XenDesktop

1. En la consola de XenMobile, haga clic en Configure y, a continuación, haga clic en Settings. Aparecerá la página Settings.



2. Haga clic en More.
3. En **Server**, haga clic en la opción que quiere configurar.

ActiveSync Gateway en XenMobile

May 05, 2016

ActiveSync es un protocolo de sincronización de datos móviles desarrollado por Microsoft. ActiveSync sincroniza datos entre dispositivos móviles y equipos de escritorio (o portátiles). Puede configurar reglas de ActiveSync Gateway en XenMobile. En función de estas reglas, se puede permitir o denegar el acceso de los dispositivos a datos ActiveSync. Por ejemplo, si activa la regla Missing Required Apps, XenMobile comprueba la directiva App Access para ver cuáles son las aplicaciones requeridas y deniega acceso a los datos de ActiveSync si faltan esas aplicaciones.

XenMobile admite las siguientes reglas:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Failed Samsung KNOX attestation: Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung KNOX.

Forbidden Apps: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva App Access.

Implicit Allow and Deny: Esta acción es la predeterminada de ActiveSync Gateway, lo que crea una lista de dispositivos que incluye todos los dispositivos que no cumplen ninguno de los demás criterios del filtro y permite o deniega conexiones basándose en esa lista. Si no coincide ninguna regla, el valor predeterminado es permitir implícitamente (Implicit Allow).

Inactive Devices: Comprueba si un dispositivo está inactivo según se define en el parámetro Device Inactivity Days Threshold en Server Properties.

Missing Required Apps: Comprueba si en un dispositivo faltan aplicaciones requeridas, según se definen en la directiva App Access.

Non-suggested Apps: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva App Access.

Noncompliant Password: Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, XenMobile puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva de códigos de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva de códigos de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Out of Compliance Devices: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo Out of Compliance. Esa propiedad es modificada normalmente por las acciones automatizadas o por las API de XenMobile de terceros.

Revoked Status: Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no puede reinscribirse hasta que vuelva a ser autorizado.

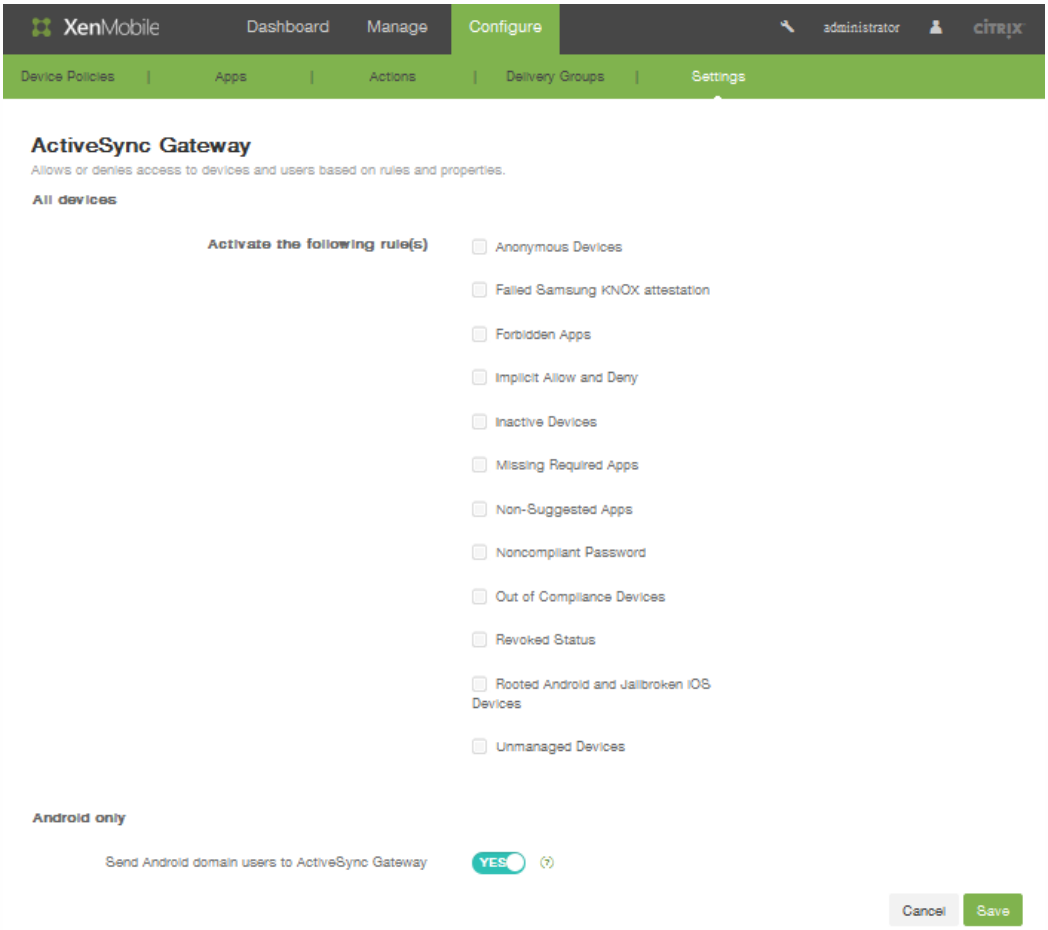
Rooted Android and Jailbroken iOS Devices: Comprueba si un dispositivo iOS o Android está liberado por jailbreak.

Unmanaged Devices: Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por ejemplo, un dispositivo que se ejecute en modo MAM o que se haya desinscrito no es un dispositivo administrado.

Send Android domain users to ActiveSync Gateway: Haga clic en **YES** para asegurarse de que XenMobile envía información de los dispositivos Android a ActiveSync Gateway. Si esta opción está habilitada, se garantiza que XenMobile envíe información de dispositivos Android a ActiveSync Gateway en el caso de que XenMobile no disponga del identificador de ActiveSync correspondiente al usuario del dispositivo Android.

Para configurar ActiveSync Gateway en XenMobile

1. En la consola de XenMobile, haga clic en **Configure > Settings > More > ActiveSync Gateway**. Aparecerá la página de configuración **ActiveSync Gateway**.



2. En **Activate the following rules**, seleccione las reglas que quiera activar.
3. En **Android-only**, en **Send Android domain users to ActiveSync Gateway**, haga clic en **YES** para que XenMobile envíe información de dispositivos Android a Secure Mobile Gateway.
4. Haga clic en **Save**.

Credenciales de Google Play

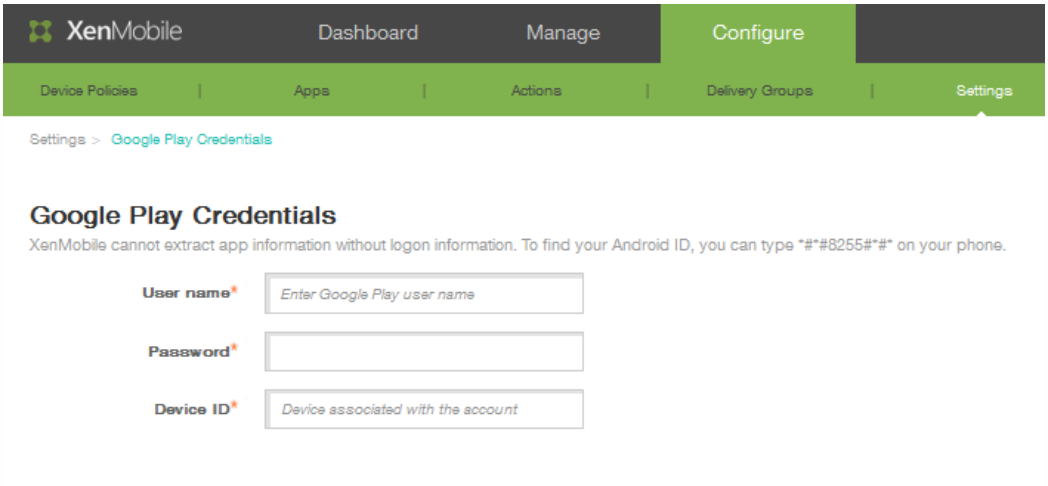
May 05, 2016

XenMobile utiliza las credenciales de Google Play para extraer información de las aplicaciones de un dispositivo.

Nota: Para buscar el ID de Android, escriba *#*#8255#*#* en el teléfono.
Importante: Si quiere que XenMobile pueda extraer información de las aplicaciones, deberá configurar su cuenta de Gmail para permitir conexiones no seguras. Para saber los pasos a seguir, consulte el sitio Web de asistencia técnica de Google.

Para configurar XenMobile para que use credenciales de Google Play

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Google Play Credentials.
   Aparecerá la pantalla de configuración Google Play Credentials.



2. En User name, escriba el nombre asociado a la cuenta de Google Play.
3. En Password, escriba la contraseña de usuario.
4. En Device ID, escriba su ID de Android.
   Escriba *#*#8255#*#* en el teléfono para determinar el ID de Android.
5. Haga clic en Save.

Programa de inscripción de dispositivos iOS

May 05, 2016

En XenMobile, es posible configurar un Programa de inscripción de dispositivos iOS para los dispositivos móviles con iOS. Esta función permite que los dispositivos iOS envíen una notificación a los servidores de Apple acerca de un perfil que personaliza la experiencia del asistente de instalación de dispositivos; este perfil se puede asignar a dispositivos específicos.

Cómo configurar el Programa de inscripción de dispositivos iOS en XenMobile

Antes de continuar, debe haber creado una cuenta DEP de Apple en deploy.apple.com. Después de haber creado una cuenta DEP, debe configurar un servidor MDM virtual para permitir la comunicación entre XenMobile y Apple. Para ello, debe cargar una clave pública de XenMobile en Apple. Después de recibir la clave pública, Apple devuelve un token de servidor que usted debe importar en XenMobile. Siga estos pasos para establecer la conexión entre XenMobile y Apple.

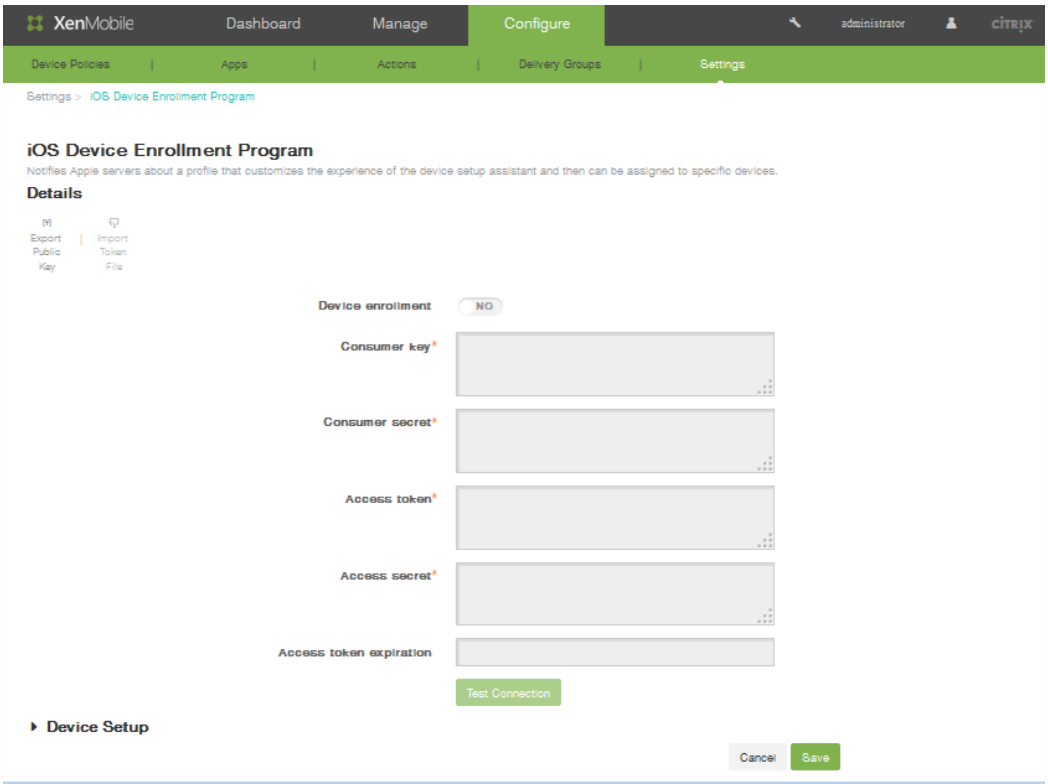
1. Para obtener la clave pública y cargarla en Apple, en la página, **iOS Device Enrollment Program** en la sección **Settings > More**, haga clic en **Export Public Key** y guarde el archivo en su equipo.

2. Vaya a deploy.apple.com, inicie sesión en la cuenta DEP y siga las instrucciones para configurar un servidor MDM. Durante este proceso, Apple entrega un token de servidor.

3. En la página **iOS Device Enrollment Program**, defina **Device enrollment** con el valor **Yes** y después haga clic en **Import Token File** para agregar el token de servidor de Apple a XenMobile.

4. Los campos **Server tokens** se rellenan automáticamente una vez cargado el archivo de token en XenMobile.

5. Haga clic en **Test Connectivity** para confirmar que XenMobile y Apple pueden comunicarse. Si la prueba de conexión falla, confirme que tiene abiertos los puertos necesarios, porque ésta suele ser la causa de estos fallos. Para obtener más información sobre los puertos que deben abrirse en XenMobile, consulte Requisitos de puertos.



En **Details**, configure los parámetros siguientes para completar la configuración de DEP:

- Device enrollment. Haga clic en YES.
- Consumer key: Introduzca la clave de consumidor.
- Consumer secret. Especifique un secreto de consumidor.
- Access token. Especifique un token de acceso.
- Access secret. Especifique el secreto del token de acceso.
- Access token expiration. Si quiere, también puede especificar la fecha de caducidad del token de acceso.
- Haga clic en Test Connection para comprobar la conexión.

- Expanda Device Setup y, a continuación, configure los siguientes parámetros:
  - Business unit. Escriba el nombre asociado a la unidad de negocio.
  - Support phone number. Escriba el número de teléfono de asistencia.
  - Support email address. Si quiere, también puede introducir la dirección de correo electrónico de asistencia.
  - Unique service ID: Puede incluir un ID de servicio único.

- En Device Settings, configure los siguientes parámetros de dispositivo asociados al Programa de inscripción de dispositivos iOS:
  - Allow or deny pairing. Haga clic en Allow para que el dispositivo se pueda administrar mediante herramientas de Apple como iTunes y Apple Configurator.

> ## Nota
>
> Si permite el emparejamiento y usa Apple Configurator, en **Supervised mode**, seleccione **YES**.

- - Device profile removal. Si prefiere que el dispositivo use un perfil que se pueda quitar de forma remota, haga clic en Allow.
  - Require device enrollment. Marque esta casilla de verificación para evitar que los usuarios omitan el proceso de inscripción.

- En Device Setup Steps, configure los siguientes parámetros:
  - Location services: Haga clic en Set up para que el dispositivo pueda compartir la ubicación, o bien haga clic en Skip para evitar que el dispositivo la comparta.
  - Restore from backup: Haga clic en Set up para que el dispositivo pueda restaurar datos a partir de un archivo de copia de seguridad.
  - Apple and iCloud: Haga clic en Set up para que el dispositivo use iCloud y el ID de Apple.
  - Terms and Conditions. Haga clic en Set up.
  - Passcode. Haga clic en Set up si quiere utilizar un código de acceso para la inscripción de dispositivos.
  - Siri: Haga clic en Set up para que el dispositivo pueda usar Siri
  - Touch ID. Haga clic en Set up para usar la tecnología Touch ID en el dispositivo.
  - Apple Pay: Haga clic en Set up para habilitar Apple Pay para el dispositivo.
  - Zoom: Haga clic en Set up para habilitar el zoom.
  - Diagnostics. Haga clic en Set up para permitir que el dispositivo comparta datos de diagnósticos.

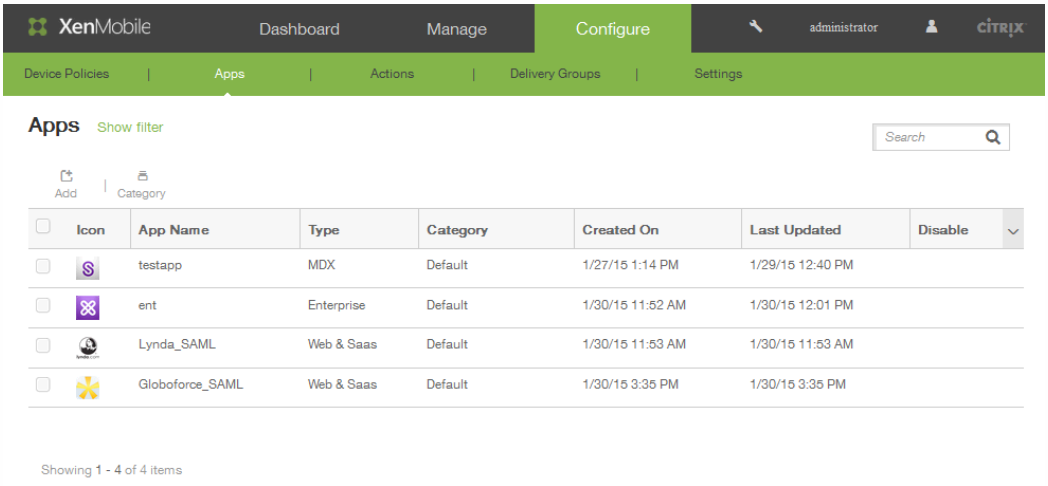
- Haga clic en Save.

Programa VPP de iOS

May 05, 2016

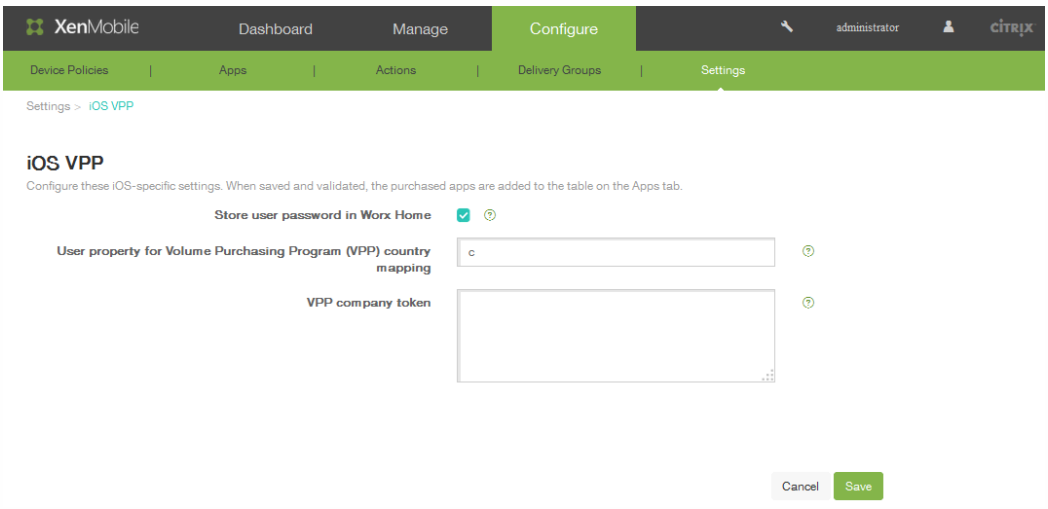
En XenMobile, puede configurar parámetros específicos del Programa de compras por volumen (VPP) de iOS. El programa VPP de iOS simplifica el proceso de búsqueda, compra y distribución de aplicaciones (y otros datos) de forma masiva en una organización. El programa VPP ofrece una solución sencilla y flexible para gestionar las necesidades de contenido de una organización.

Después de guardar y validar la configuración del programa VPP de iOS en XenMobile, las aplicaciones adquiridas se agregan a la tabla situada en la ficha Apps de la consola de XenMobile.



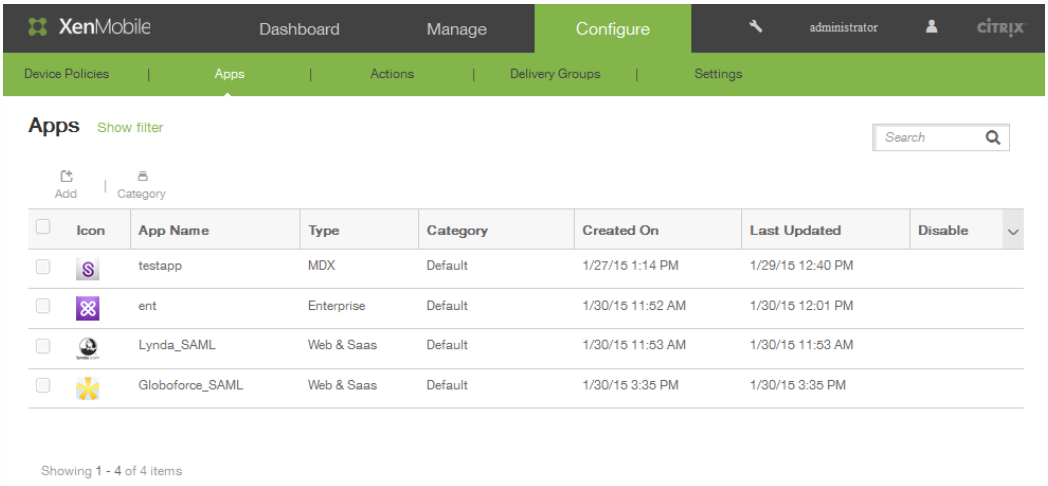
Para configurar el programa VPP de iOS en XenMobile

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > iOS VPP. Aparecerá la pantalla de configuración iOS VPP.



2. En Store user password in Worx Home, marque la casilla de verificación para almacenar de forma segura un nombre de usuario y la contraseña correspondiente en Worx Home de cara a la autenticación de XenMobile.
3. En User property for Volume Purchasing Program (VPP) country mapping, escriba un código para que los usuarios puedan descargar aplicaciones de los almacenes de aplicaciones específicos de cada país.
   Esta asignación se usa para elegir la agrupación de propiedades del programa VPP. Por ejemplo, si la propiedad del usuario es Estados Unidos, dicho usuario no puede descargar aplicaciones si el código del programa VPP de la aplicación se distribuye en el Reino Unido. Póngase en contacto con el administrador de planes del programa VPP para obtener más información acerca del código de asignación de país.

4. En VPP company token, escriba un token que represente el token de servicio del programa VPP que se genera cuando un usuario compra algo del App Store de Apple a través de una cuenta de empresa. El token se utiliza para validar la licencia del programa VPP. Por ejemplo, si dispone de una cuenta del programa VPP de Apple para la empresa, vaya a https://vpp.itunes.com, haga clic en **Business** e inicie sesión con las credenciales de su cuenta del programa VPP de Apple para obtener la información correspondiente.
5. Haga clic en Save. A continuación, la información aparece en la tabla de aplicaciones:



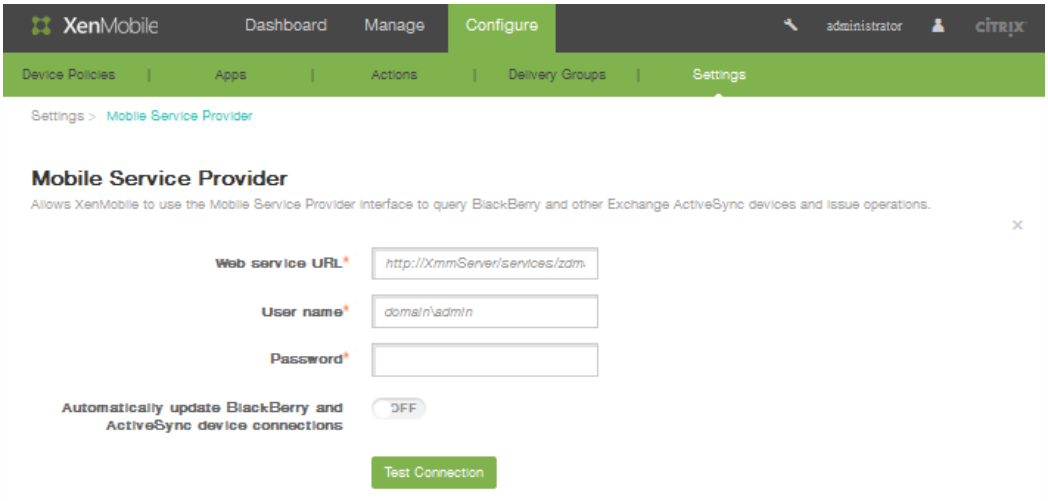
Proveedor de servicios móviles

May 05, 2016

Puede habilitar XenMobile para que utilice la interfaz del proveedor de servicios móviles, emita operaciones y consulte dispositivos de BlackBerry y Exchange ActiveSync.

Para configurar el proveedor de servicios móviles

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Mobile Service Provider. Aparece la página de configuración Mobile Service Provider.



2. En Web service URL, escriba la dirección URL del servicio Web, como http://XmmServer/services/xdmservice.
3. En User name, escriba el nombre de usuario en el formato domain\admin
4. En Password, escriba la contraseña.
5. Para habilitar la opción Automatically update BlackBerry and ActiveSync device connections, haga clic en ON. El valor predeterminado de este parámetro es OFF.
6. Haga clic en Test connection para comprobar la conexión.
7. Haga clic en Save.

Control de acceso de red

May 05, 2016

Si tiene un dispositivo de control de acceso a la red (Network Access Control, NAC) configurado en la red, como Cisco ISE, en XenMobile puede habilitar filtros para configurar dispositivos como conformes o no conformes a NAC, en función de reglas o propiedades. En XenMobile, si un dispositivo administrado no cumple los criterios especificados y, como resultado, se marca como No conforme, el dispositivo de NAC bloquea ese dispositivo en la red.

En la consola de XenMobile, seleccione los criterios de la lista correspondientes para establecer un dispositivo como no conforme.

XenMobile da respaldo a los siguientes filtros de conformidad para NAC:

Anonymous Devices: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Failed Samsung KNOX attestation: Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung KNOX.

Forbidden Apps: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva App Access.

Implicit Allow and Deny: Esta acción es la predeterminada de ActiveSync Gateway, lo que crea una lista de dispositivos que incluye todos los dispositivos que no cumplen ninguno de los demás criterios del filtro y permite o deniega conexiones basándose en esa lista. Si no coincide ninguna regla, el valor predeterminado es permitir implícitamente (Implicit Allow).

Inactive Devices: Comprueba si un dispositivo está inactivo según se define en el parámetro Device Inactivity Days Threshold en Server Properties.

Missing Required Apps: Comprueba si en un dispositivo faltan aplicaciones requeridas, según se definen en la directiva App Access.

Non-suggested Apps: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva App Access.

Noncompliant Password: Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, XenMobile puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva de códigos de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva de códigos de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Out of Compliance Devices: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo Out of Compliance. Esa propiedad es modificada normalmente por las acciones automatizadas o por las API de XenMobile de terceros.

Revoked Status: Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no puede reinscribirse hasta que vuelva a ser autorizado.

Rooted Android and Jailbroken iOS Devices: Comprueba si un dispositivo iOS o Android está liberado por jailbreak.

Unmanaged Devices: Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por

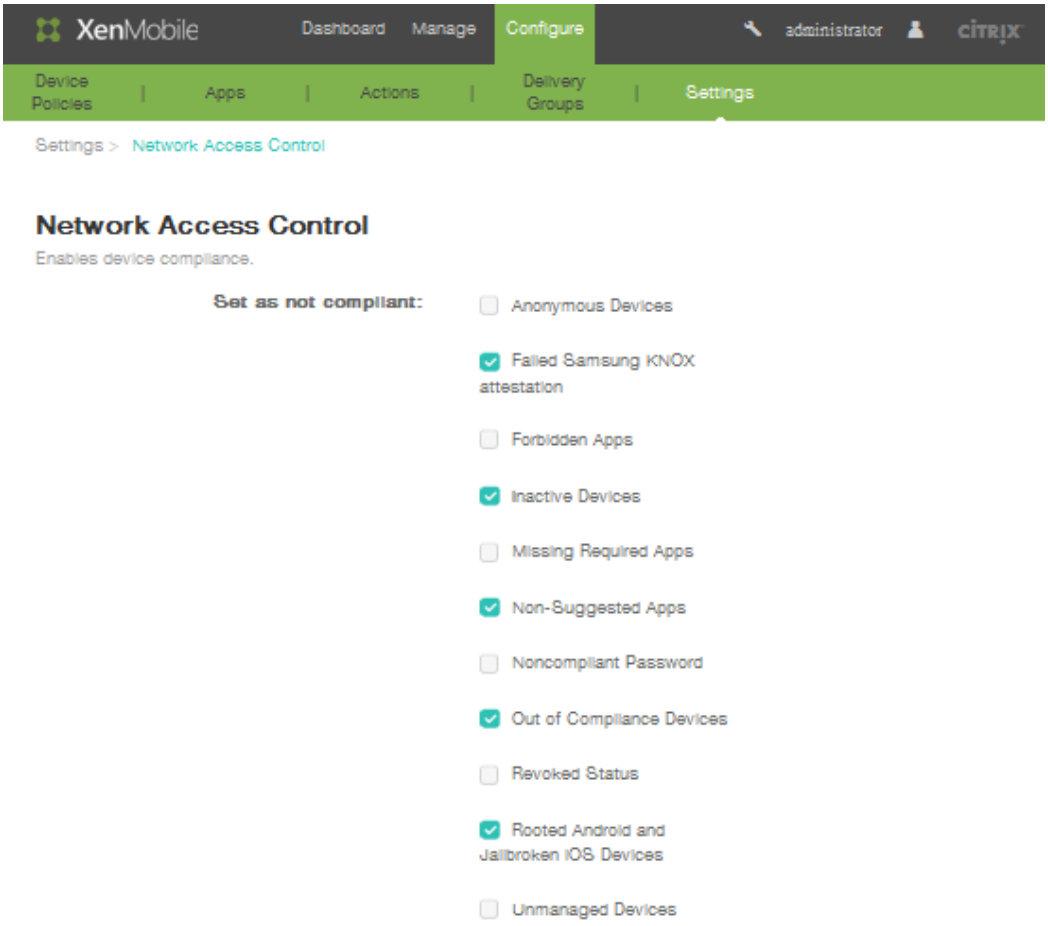
ejemplo, un dispositivo que se ejecute en modo MAM o que se haya desinscrito no es un dispositivo administrado.

Send Android domain users to ActiveSync Gateway: Haga clic en **YES** para asegurarse de que XenMobile envía información de los dispositivos Android a ActiveSync Gateway. Si esta opción está habilitada, se garantiza que XenMobile envíe información de dispositivos Android a ActiveSync Gateway en el caso de que XenMobile no disponga del identificador de ActiveSync correspondiente al usuario del dispositivo Android.

> ## Nota
>
> El filtro de dispositivos que cumplen los requisitos de forma implícita o que no los cumplen establece el valor predeterminado solo en los dispositivos que administra XenMobile. Por ejemplo, los dispositivos que tienen instalada una aplicación prohibida y/o que no están inscritos se marcan como no conformes y el dispositivo de NAC bloqueará su acceso a la red.

Para configurar el control de acceso a la red en XenMobile

1. En la consola Web de XenMobile, haga clic en **Configure > Settings > More > Network Access Control**. Aparece la página de configuración **Network Access Control**.



2. Marque las casillas de verificación de los filtros de **Set as not compliant** que quiera habilitar.
3. Haga clic en **Save**.

Samsung KNOX

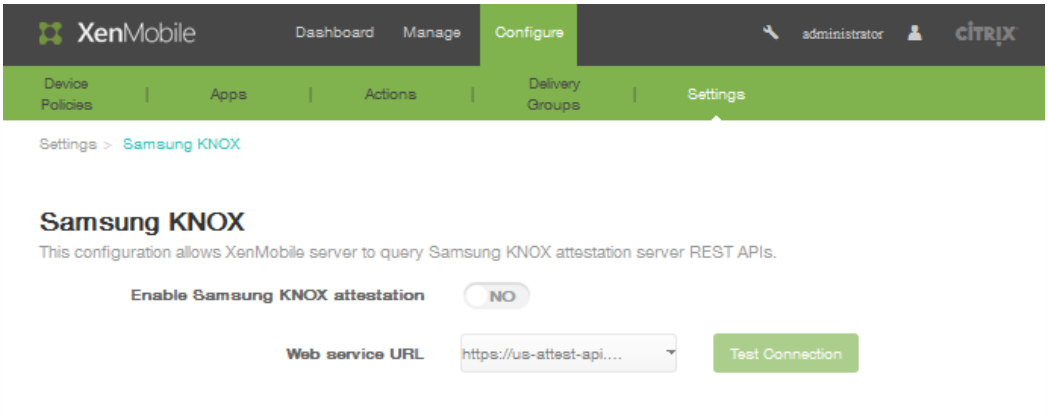
May 05, 2016

Puede configurar XenMobile para consultar las API de REST del servidor de atestación de Samsung KNOX.

Samsung KNOX aprovecha las funcionalidades de seguridad de hardware y ofrece varios niveles de protección para el sistema operativo y las aplicaciones. Un nivel de esta seguridad se encuentra en la plataforma mediante la atestación. Un servidor de atestación ofrece la comprobación del software del sistema principal del dispositivo móvil (por ejemplo, los cargadores de arranque y el kernel) en tiempo de ejecución en función de los datos recopilados durante un arranque seguro.

Para habilitar la atestación de Samsung KNOX

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Samsung KNOX.
   Aparecerá la página de configuración Samsung KNOX.



2. En Enable Samsung KNOX attestation, haga clic en **YES**.
3. Cuando haga clic en YES en el paso 2, se habilitará la opción **Web service URL**. En la lista, haga clic en el servidor de atestación correspondiente.
4. Haga clic en **Test Connection** para comprobar la conexión.
5. Haga clic en **Save**.

Propiedades de servidor

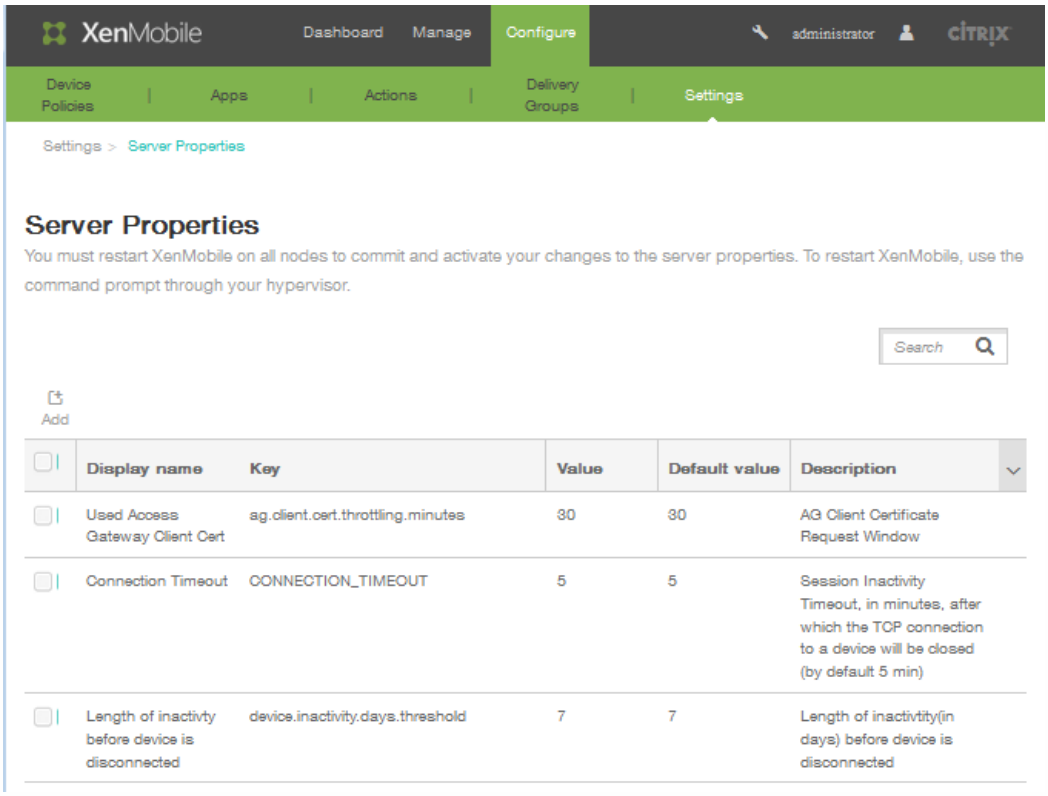
May 05, 2016

En XenMobile, se pueden aplicar propiedades al servidor. Después de realizar cambios, debe reiniciar XenMobile en todos los nodos para confirmar y activar los cambios.

Nota: Para reiniciar XenMobile, use la línea de comandos a través del hipervisor.

Para configurar las propiedades de servidor en XenMobile

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Server Properties.
   Aparecerá la página de configuración Server Properties.



2. Lleve a cabo una de las siguientes acciones:
   - Haga clic en Add para agregar una nueva propiedad de servidor.
   - En la tabla, haga clic para seleccionar una propiedad existente y, a continuación, en el menú que aparece, haga clic en Edit.
3. Si ha hecho clic en Add en el paso 2, configure los campos siguientes:

- Key. En la lista, seleccione la clave apropiada.
  Nota: Las claves distinguen mayúsculas y minúsculas. Debe ponerse en contacto con el servicio de asistencia técnica de Citrix antes de realizar cambios o de solicitar una clave especial.

- **Value**. Escriba un valor en función de la clave seleccionada.
- **Display name**. Especifique el nombre del nuevo valor de propiedad que aparece en la tabla Server Properties.

- **Description**. Si lo prefiere, puede incluir una descripción de la nueva propiedad de servidor. A continuación, haga clic en Save.

SysLog

May 05, 2016

Puede configurar XenMobile para enviar archivos de registros a un servidor de registros de sistemas (syslog). Se necesita el nombre de host del servidor o la dirección IP.

Syslog es un protocolo estándar de captura de registros con dos componentes: un módulo de auditoría (que se ejecuta en el dispositivo) y un servidor (que se puede ejecutar en un sistema remoto). El protocolo Syslog usa el protocolo de datos de usuario (UDP) para la transferencia de datos.

Puede configurar el servidor para recopilar los siguientes tipos de información:

- Los registros del sistema representan las acciones llevadas a cabo por XenMobile.
- Los registros de auditoría representan un registro cronológico de las actividades del sistema referentes a XenMobile.

La información de registro que obtiene un servidor syslog de un dispositivo se almacena en un archivo de registros en forma de mensajes. Por regla general, estos mensajes contienen la siguiente información:

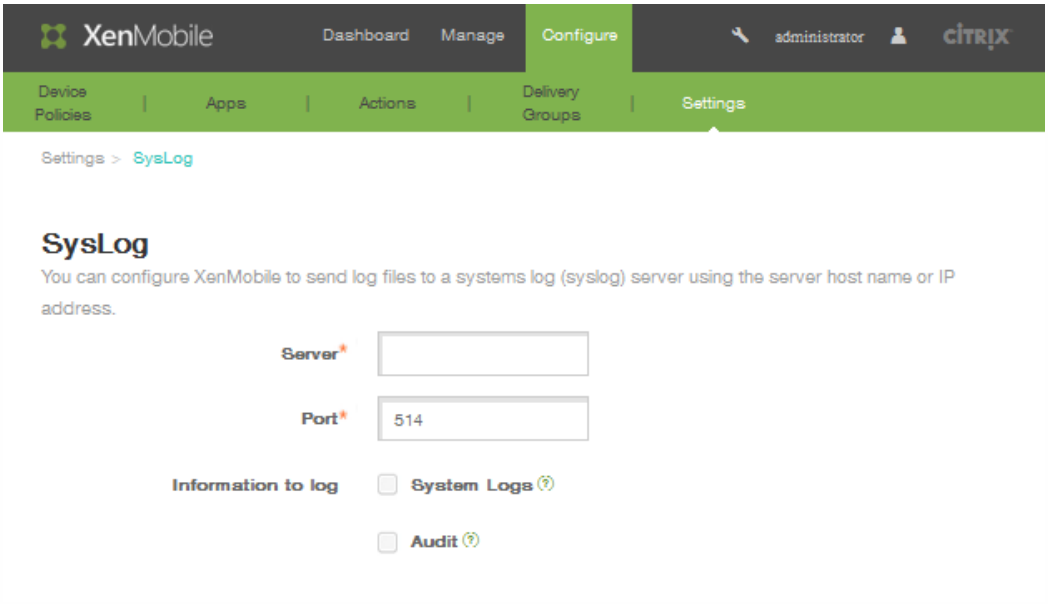
- La dirección IP del dispositivo que generó el mensaje de registro
- Una marca de tiempo
- El tipo de mensaje
- El nivel de registro asociado a un evento (crítico, error, aviso, advertencia, informativo, depuración, alerta o emergencia)
- La información del mensaje

Puede usar esta información para analizar el origen de la alerta y, si fuera necesario, realizar las correcciones oportunas.

> ## Nota
>
> En implementaciones de nube con XenMobile, Citrix no respalda la integración de syslog con un servidor syslog ubicado en las instalaciones locales. En su lugar, puede descargar los registros de la página Support de la consola de XenMobile. Al hacerlo, debe hacer clic en Descargar todo para poder obtener los registros del sistema. Para obtener información detallada, consulte Cómo ver y analizar archivos de registros en XenMobile.

Para configurar un servidor syslog en XenMobile

1. En la consola Web de XenMobile, haga clic en Configure > Settings > More > Syslog.
   Aparecerá la página de configuración Syslog.



2. En Name, escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor syslog.
3. En Port, introduzca el número de puerto. De forma predeterminada, el puerto está configurado en 514.
4. En Information to log, seleccione System Logs y Audit o anule su selección.
   - Los registros del sistema representan las acciones llevadas a cabo por XenMobile.
   - Los registros de auditoría representan un registro cronológico de las actividades del sistema referentes a XenMobile.
5. Haga clic en **Save**.

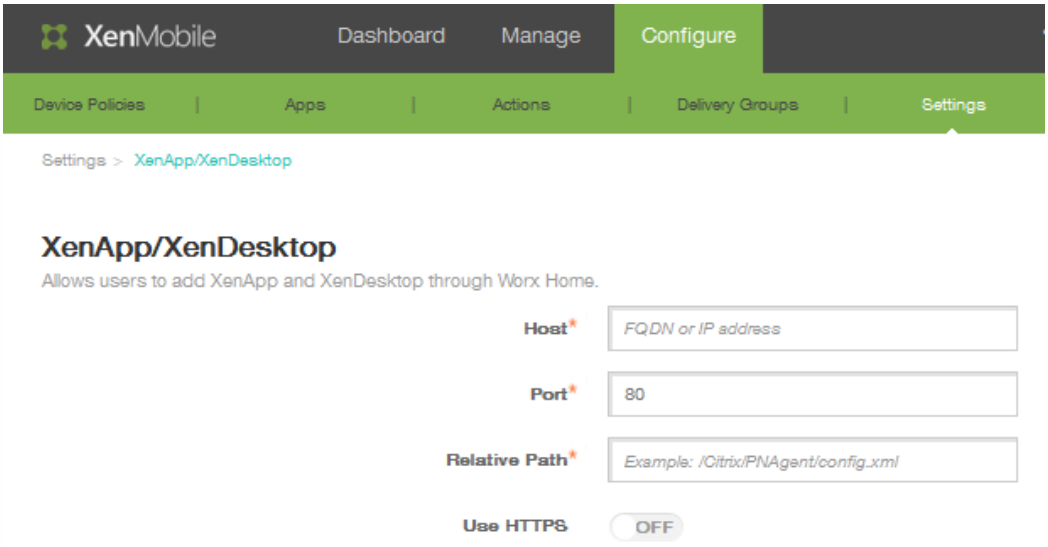
Cómo configurar XenApp y XenDesktop

May 05, 2016

XenMobile puede recopilar aplicaciones desde XenApp y XenDesktop y ponerlas a disposición de los usuarios de dispositivos móviles a través de Worx Store. Los usuarios se suscriben a las aplicaciones directamente en Worx Store y las inician desde Worx Home. La aplicación Receiver debe estar instalada en los dispositivos de los usuarios para iniciar las aplicaciones, pero no es necesario configurarlas.

Para configurar este parámetro, se necesita el nombre de dominio completo (FQDN) o la dirección IP y el número de puerto del sitio de StoreFront o Interfaz Web.

1. En la consola Web de XenMobile, haga clic en **Configure > Settings > More > XenApp/XenDesktop**. Aparecerá la página de configuración XenApp/XenDesktop.



2. En Host, introduzca el nombre de dominio completo (FQDN) o la dirección IP del sitio de StoreFront o Interfaz Web.
3. En Port, introduzca el número de puerto del sitio de StoreFront o Interfaz Web. El valor predeterminado es 80.
4. En Relative Path, introduzca la ruta de acceso. Por ejemplo, /Citrix/Store/PNAgent/config.xml.
5. En Use HTTPS, seleccione ON para habilitar la autenticación segura entre el sitio de StoreFront o Interfaz Web y el dispositivo cliente. El valor predeterminado es OFF.
6. Haga clic en **Save**.

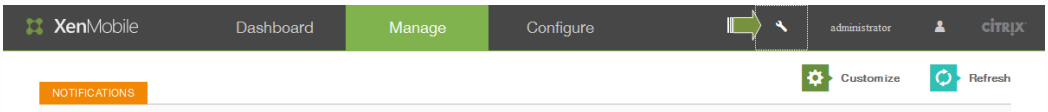
Mantenimiento y asistencia de XenMobile

Oct 31, 2016

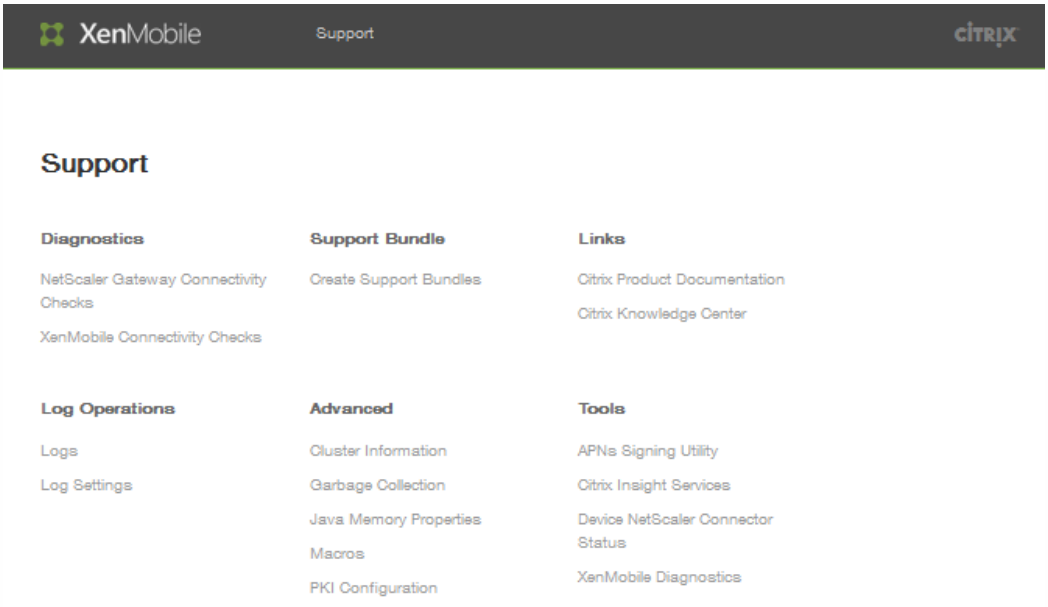
Use la página Support de XenMobile para acceder a un repertorio de datos informativos y herramientas relacionadas con la asistencia. También puede realizar acciones desde la interfaz de línea de comandos. Para obtener información más detallada, consulte Opciones de la interfaz de línea de comandos en XenMobile.

Para acceder a la página Support

En la consola de XenMobile, haga clic en el icono con forma de llave inglesa , situado en la esquina superior derecha de la consola:



La página Support aparece en una nueva pestaña del explorador:



Use la página Support de XenMobile para:

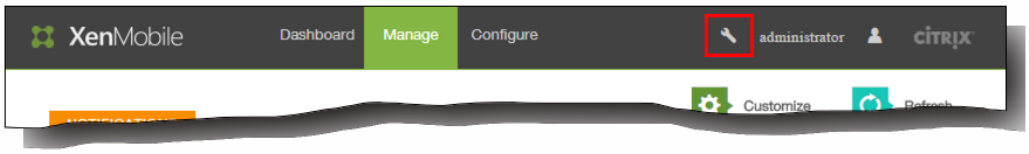
- Acceder a datos de diagnóstico
- Crear paquetes de asistencia
- Acceder a enlaces que llevan a la documentación de productos y al Knowledge Center de Citrix
- Acceder a operaciones de registro
- Disponer de un conjunto de opciones avanzadas de configuración e información
- Acceder a un conjunto de herramientas y utilidades

Comprobaciones de conectividad

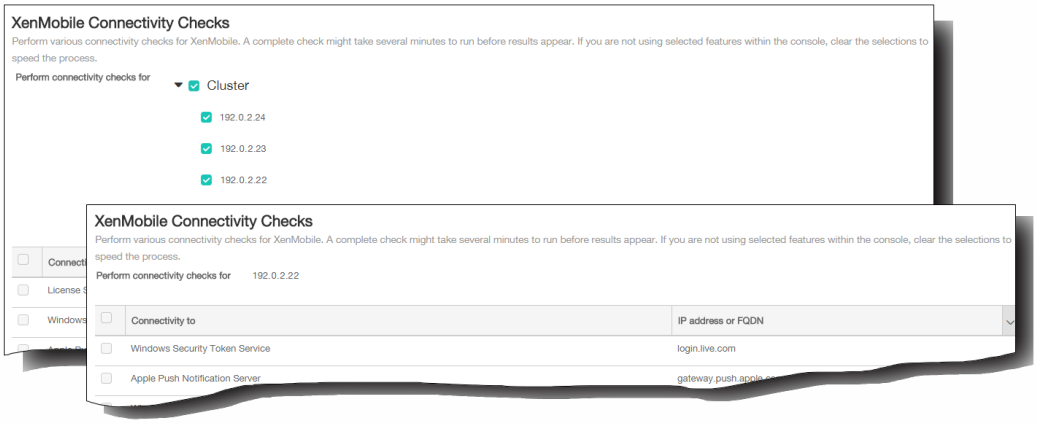
May 05, 2016

En la página Support de XenMobile, puede comprobar la conexión de XenMobile con NetScaler Gateway y con otros servidores y ubicaciones. Para acceder a la página Support, lleve a cabo lo siguiente:

1. Desde la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. El icono con forma de llave inglesa está disponible en cualquier página de la consola de XenMobile. Es posible que tenga que introducir su nombre de usuario y su contraseña.



   Se abre una nueva pestaña del explorador llamada XenMobile Support. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.



Comprobaciones de conectividad de XenMobile

1. En la página Support, haga clic en XenMobile Connectivity Checks. Aparecerá la página XenMobile Connectivity Checks.
2. Seleccione los servidores a incluir en la prueba de conectividad y, a continuación, haga clic en Test Connectivity. Aparecerán los resultados.
3. Seleccione un servidor de la tabla Test Results para ver los resultados detallados de dicho servidor.

Comprobaciones de conectividad de NetScaler Gateway

1. En la página Support, haga clic en NetScaler Gateway Connectivity Checks. Aparecerá la página NetScaler Gateway Connectivity Checks.
2. Haga clic en Agregar. Aparecerá el cuadro de diálogo Add NetScaler Gateway Server.
3. En NetScaler Gateway Management IP, escriba la dirección IP del servidor con NetScaler Gateway que usted quiere probar.
   Nota: Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado,

se proporciona la dirección IP.

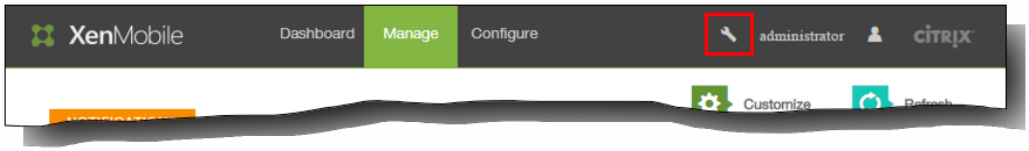
4. Escriba las credenciales de administrador de este servidor NetScaler Gateway.
   Nota: Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado, se proporciona el nombre de usuario.
5. Haga clic en Agregar. El servidor NetScaler Gateway se agrega a la tabla en la página NetScaler Gateway Connectivity Checks.
6. Haga clic en Test Connectivity. Los resultados aparecerán en la tabla Test Results.
7. Seleccione un servidor de la tabla Test Results para ver los resultados detallados de dicho servidor.

Creación de paquetes de asistencia en XenMobile

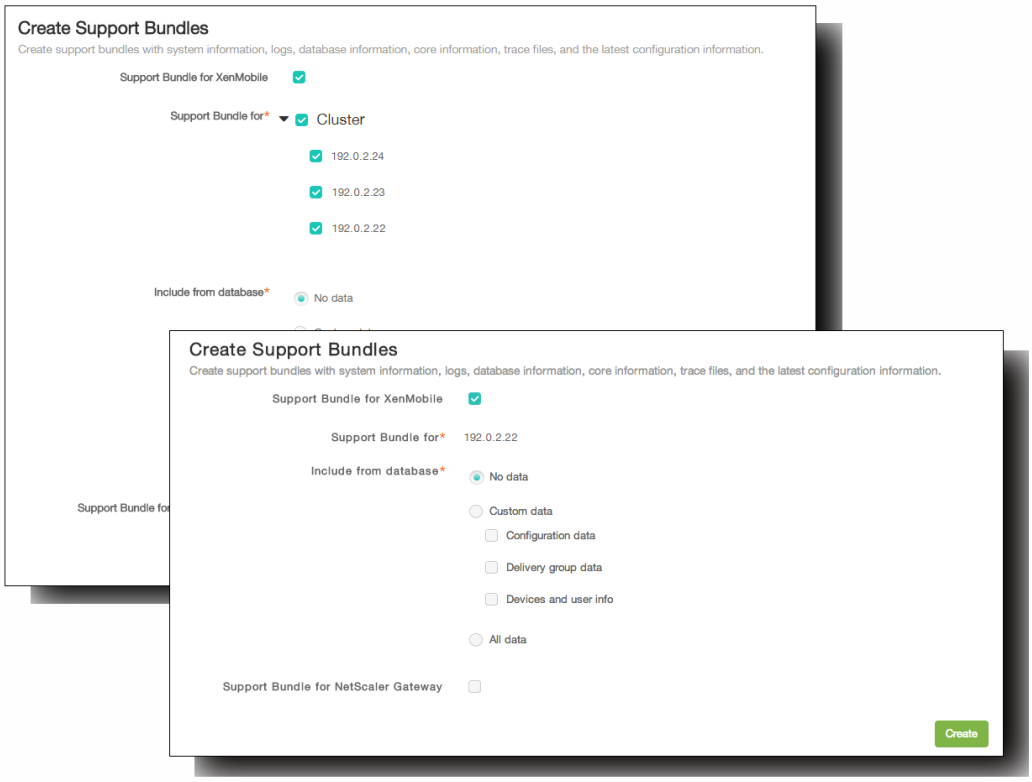
May 05, 2016

Para informar a Citrix de un problema o para solucionar un problema, puede crear un paquete de asistencia y cargarlo en Citrix Insight Services (CIS).

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. El icono con forma de llave inglesa está disponible en cualquier página de la consola de XenMobile.
   Nota: Es posible que tenga que introducir su nombre de usuario y su contraseña.



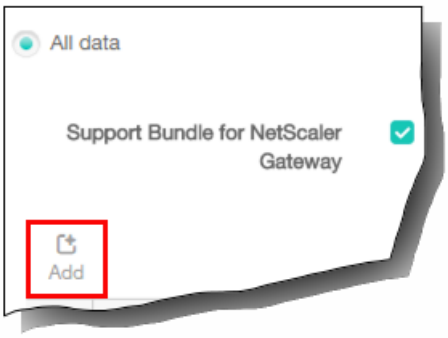
   La página XenMobile Support se abre en una nueva ventana del explorador.
2. En la página Support, haga clic en Create Support Bundles. Aparecerá la página Create Support Bundles. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.



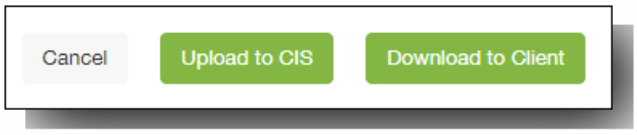
3. Compruebe que está marcada la casilla de verificación Support Bundle for XenMobile.
4. Si su entorno de XenMobile contiene nodos en clúster, en Support Bundle for, seleccione todos los nodos o cualquier combinación de nodos de los que obtener datos.
5. En Include from Database, realice una de las siguientes acciones:

- Haga clic en No data.
- Haga clic en Custom data y, a continuación, seleccione una de las siguientes opciones:
  - Configuration data. Incluye las configuraciones de certificados y las directivas del administrador de dispositivos.
  - Delivery group data. Incluye información acerca de las aplicaciones de los grupos de entrega; esta información contiene detalles acerca de los tipos de aplicación y sobre las directivas referentes a la entrega de aplicaciones.
  - Devices and user info. Incluye aplicaciones, acciones, grupos de entrega y directivas de dispositivos.
- Haga clic en All data.

6. Marque Support Bundle for NetScaler Gateway para incluir paquetes de asistencia de NetScaler Gateway y, a continuación, realice lo siguiente:
   1. Haga clic en Agregar.



   Aparecerá el cuadro de diálogo Add NetScaler Gateway Server.
   2. En NetScaler Gateway Management IP, escriba la dirección IP de administración de NetScaler referente al dispositivo de NetScaler Gateway del que se va a extraer el paquete de asistencia.
   Nota: Si va a crear un paquete de un servidor NetScaler Gateway que ya se ha agregado, se proporciona la dirección IP.
   3. En User name y Password, escriba las credenciales de usuario necesarias para acceder al servidor que ejecuta NetScaler Gateway.
   Nota: Si va a crear un paquete de un servidor NetScaler Gateway que ya se ha agregado, se proporciona el nombre de usuario.
   4. Haga clic en Agregar. El nuevo paquete de asistencia de NetScaler Gateway se agrega a la tabla.
   5. Si es necesario, repita el paso 6 para agregar más paquetes de asistencia de NetScaler Gateway.
7. Haga clic en Create. Se crea el paquete de asistencia y aparecen dos nuevos botones: Upload to CIS y Download to Client.

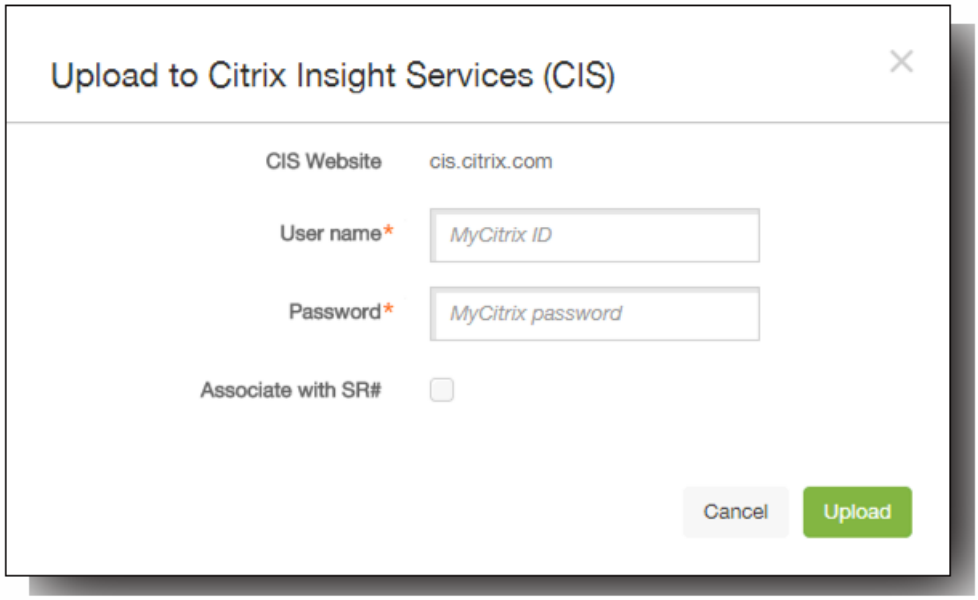


Continúe los procedimientos para cargar paquetes de asistencia en Citrix Insight Services o descargarlos en un cliente mediante las opciones **Uploading Support Bundles to Citrix Insight Services** o **Downloading Support Bundles to a Client** respectivamente.

Carga de paquetes de asistencia en Citrix Insight Services

Después de crear un paquete de asistencia, puede cargarlo en Citrix Insight Services (CIS) o descargarlo en su equipo. A continuación, se presentan los pasos necesarios para cargar el paquete en CIS.

1. En la página Create Support Bundles, haga clic en Upload to CIS. Aparecerá el cuadro de diálogo Upload to Citrix Insight Services (CIS).



2. En User Name, escriba su ID de MyCitrix.
3. En Password, escriba su contraseña de MyCitrix.
4. Para vincular este paquete con el número de una solicitud de servicio existente, marque la casilla de verificación Associate with SR# y, en los dos campos que aparecen, lleve a cabo lo siguiente:
   1. En SR#, escriba los 8 dígitos del número de solicitud de servicio a la que se va a asociar este paquete.
   2. En SR Description, escriba una descripción de la solicitud de servicio.
5. Haga clic en Upload. El paquete de asistencia se carga en CIS.

Descarga de paquetes de asistencia en el equipo

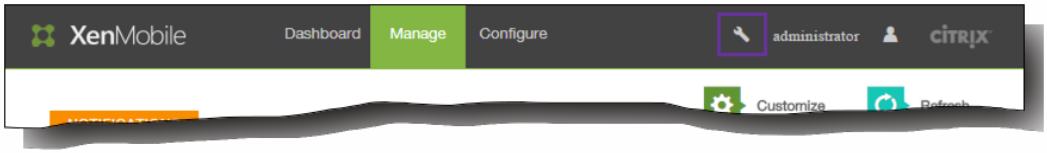
Después de crear un paquete de asistencia, puede cargarlo en CIS o descargarlo en su equipo. Para resolver cualquier problema por su cuenta, descargue el paquete de asistencia en su equipo.
En la página Create Support Bundles, haga clic en Download to Client. El paquete se descargará en su equipo.

Para ver el archivo del registro de depuración

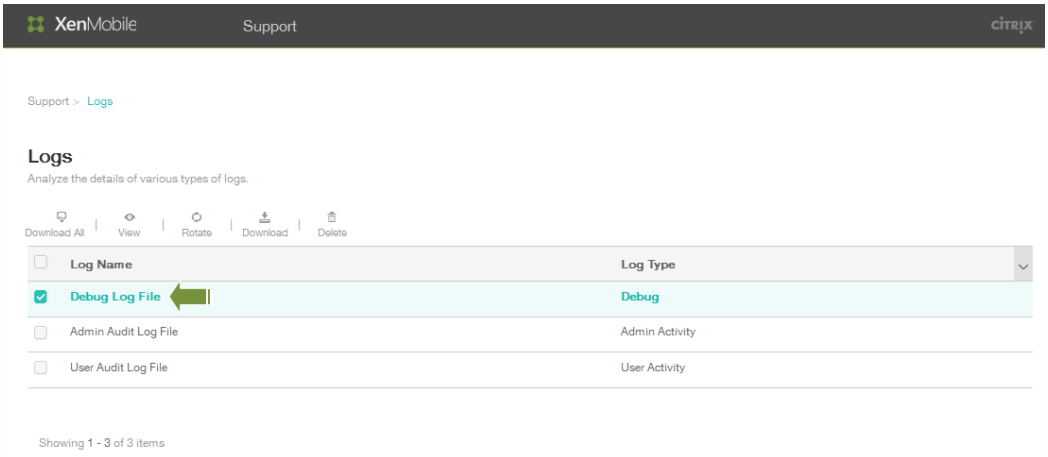
May 05, 2016

Para informar a Citrix de un problema o para solucionar un problema, puede crear un paquete de asistencia y cargarlo en Citrix Insight Services (CIS).

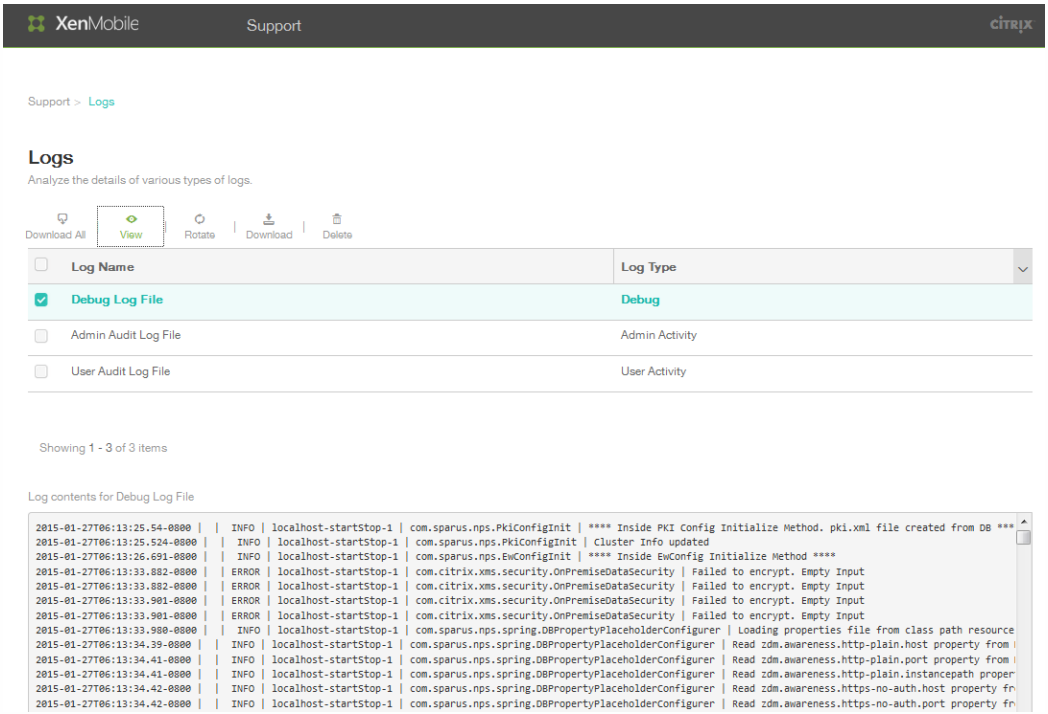
1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. El icono con forma de llave inglesa está disponible en cualquier página de la consola de XenMobile.



2. En la página Support, haga clic en Logs. Aparece la pantalla Logs.



3. Seleccione Debug Log File y, a continuación, haga clic en View para mostrar el contenido de los registros.



Después de analizar el archivo de registros, utilice la opción Download File para guardar los datos, o bien haga clic en Delete para quitar el contenido de registros de la base de datos.

Para configurar parámetros de registro

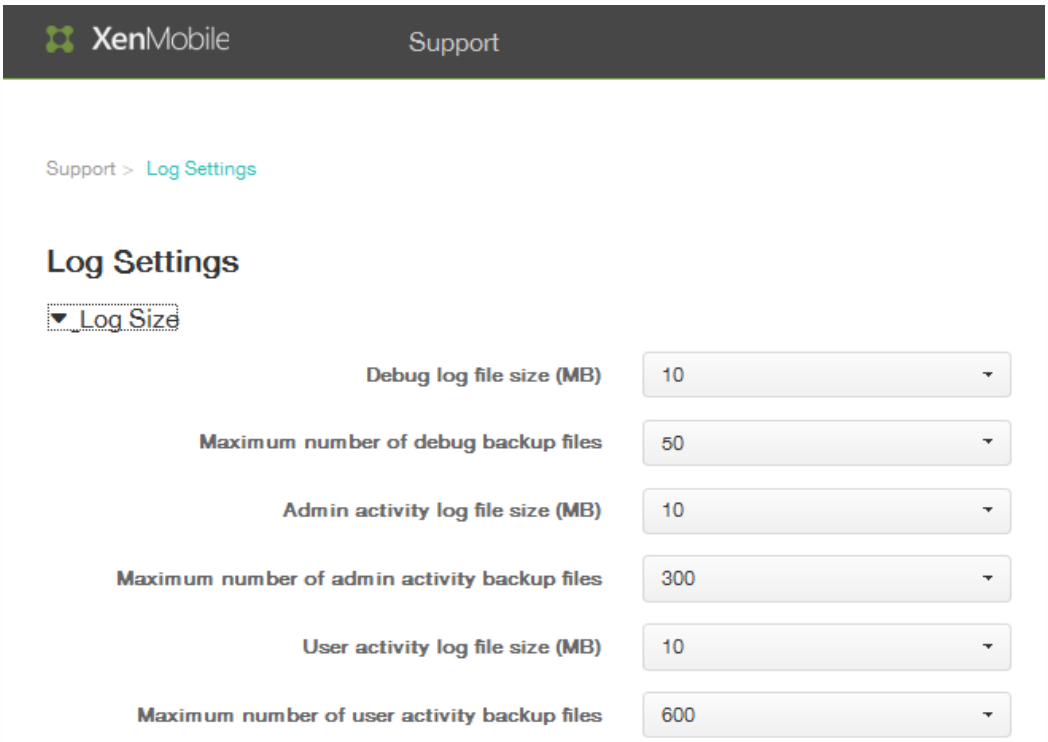
May 05, 2016

Puede configurar los parámetros de registro para personalizar los registros que genera XenMobile. En la consola de XenMobile, haga clic en Support > Log Settings para acceder a las siguientes opciones:

- Log Size. Use esta opción para el tamaño del archivo de registro y la cantidad máxima de copias de seguridad del archivo de registro que se conservarán en la base de datos. El tamaño del archivo de registro se aplica a cada uno de los registros que admite XenMobile (el registro de depuración, el registro de la actividad del administrador y el registro de la actividad del usuario).
- Log Level. Use esta opción para cambiar el nombre de la clase, el nombre de la subclase o el nivel del registro, o bien para conservar la configuración.
- Custom Logger. Use esta opción para crear un registrador personalizado; los registros personalizados requieren un nombre de clase y un nivel de registro.

Para configurar las opciones de tamaño del registro

1. Haga clic en Support > Log Settings y, a continuación, expanda Log Size.



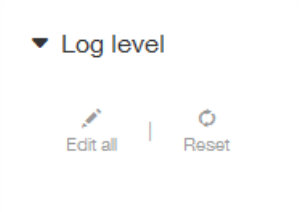
2. En la lista Debug log file size (MB), seleccione un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de depuración. De forma predeterminada, el tamaño del archivo es de 10 MB.
3. En la lista Maximum number of debug backup files, seleccione de 5 a 300 archivos de depuración para ajustar la cantidad máxima de archivos de depuración que se conservarán en el servidor. De forma predeterminada, XenMobile conserva 50 archivos de copias de seguridad en el servidor.
4. En la lista Admin activity log, seleccione un tamaño comprendido entre 5 y 20 MB. De forma predeterminada, el tamaño del archivo es de 10 MB.
5. En la lista Maximum number of admin backup files, seleccione de 5 a 300 archivos de depuración para ajustar la cantidad

máxima de archivos de copias de seguridad acerca de la actividad del administrador que se conservarán en el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.

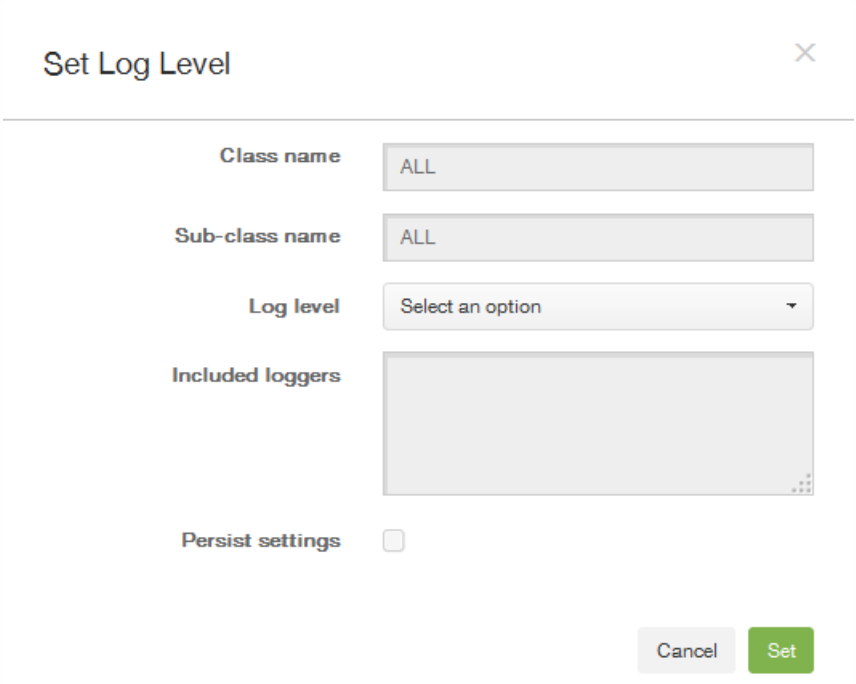
6. En la lista User activity log size, seleccione un tamaño comprendido entre 5 y 20 MB. De forma predeterminada, el tamaño del archivo es de 10 MB.
7. En la lista Maximum number of admin backup files, seleccione de 5 a 300 archivos de depuración para ajustar la cantidad máxima de archivos de copias de seguridad acerca de la actividad del administrador que se conservarán en el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.

Para configurar las opciones de nivel de registro

1. Haga clic en Support > Log Settings y, a continuación, expanda Log level para ver las opciones de configuración. Haga clic en Edit all para configurar elementos del nivel de registro.



Aparecerá la pantalla Set Log Level.

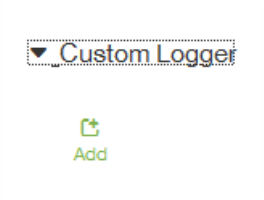


2. Escriba el nombre de clase en Class Name. De forma predeterminada, este campo está establecido en All.
3. Escriba el nombre de subclase en Sub-class name. De forma predeterminada, este campo está establecido en All.
4. En la lista Log level, seleccione un nivel de registro. Los niveles de registro admitidos son: Fatal, Error, Warning, Info, Debug, Trace u Off. El campo Included Loggers muestra los niveles de registro actualmente configurados para cada clase definida.
5. Si quiere mantener la configuración del nivel de registro, marque la casilla Persist settings.

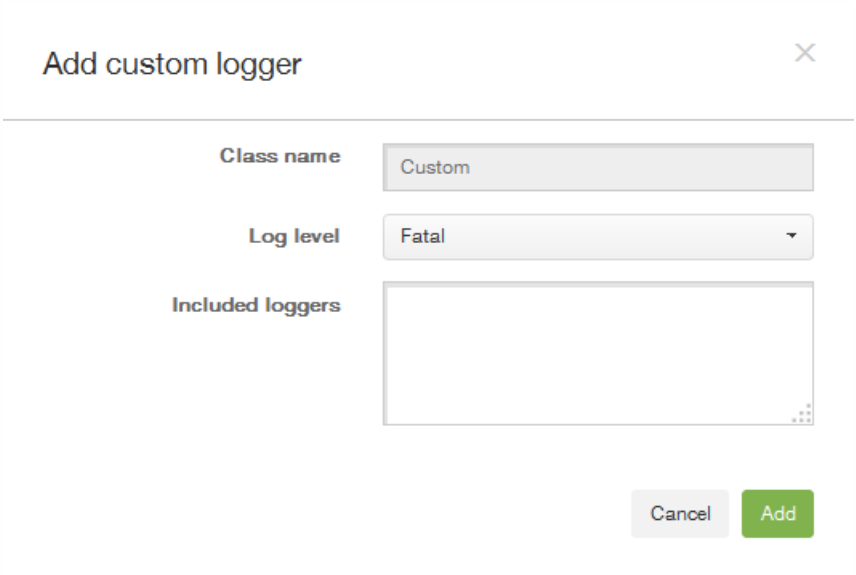
6. Haga clic en Set para confirmar los cambios.

Para agregar un registrador personalizado

1. Para agregar un registrador personalizado, haga clic en Add.



Aparecerá la pantalla Add custom logger.

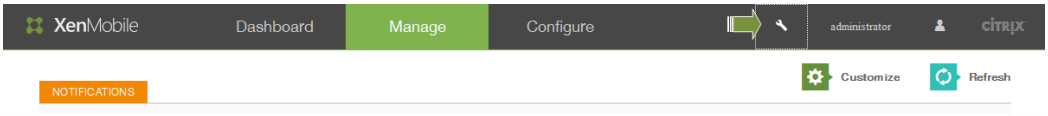


2. Especifique un nombre de clase en Class name.
3. En la lista Log level, seleccione un nivel de registro. Los niveles de registro admitidos son: Fatal, Error, Warning, Info, Debug, Trace u Off. El campo Included Loggers muestra los niveles de registro actualmente configurados para cada clase definida.
4. Haga clic en Agregar.

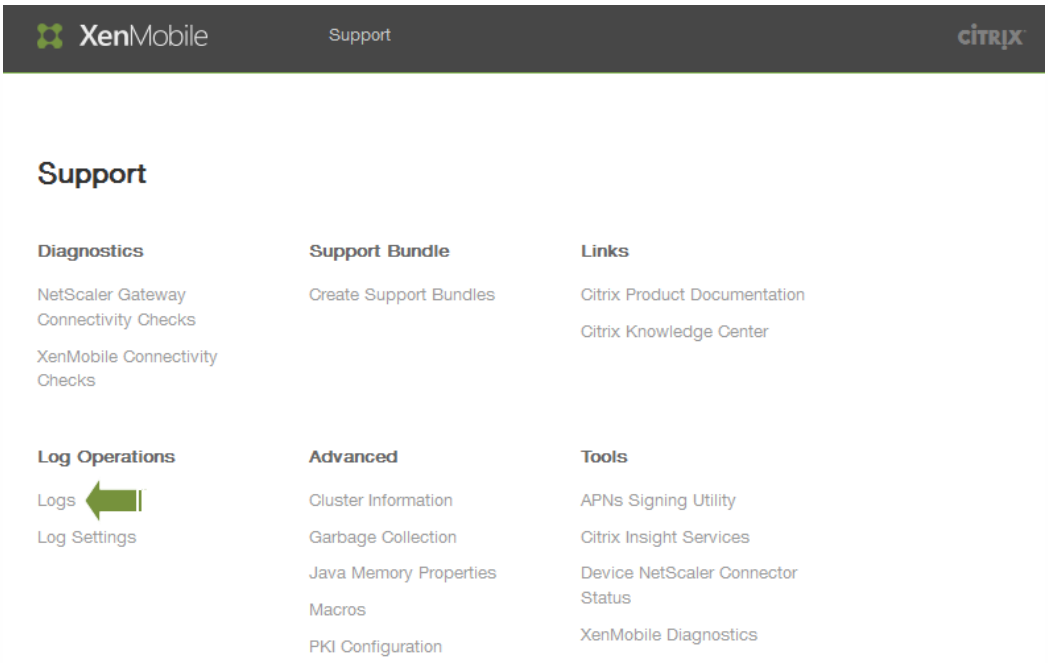
Cómo ver y analizar archivos de registros en XenMobile

May 05, 2016

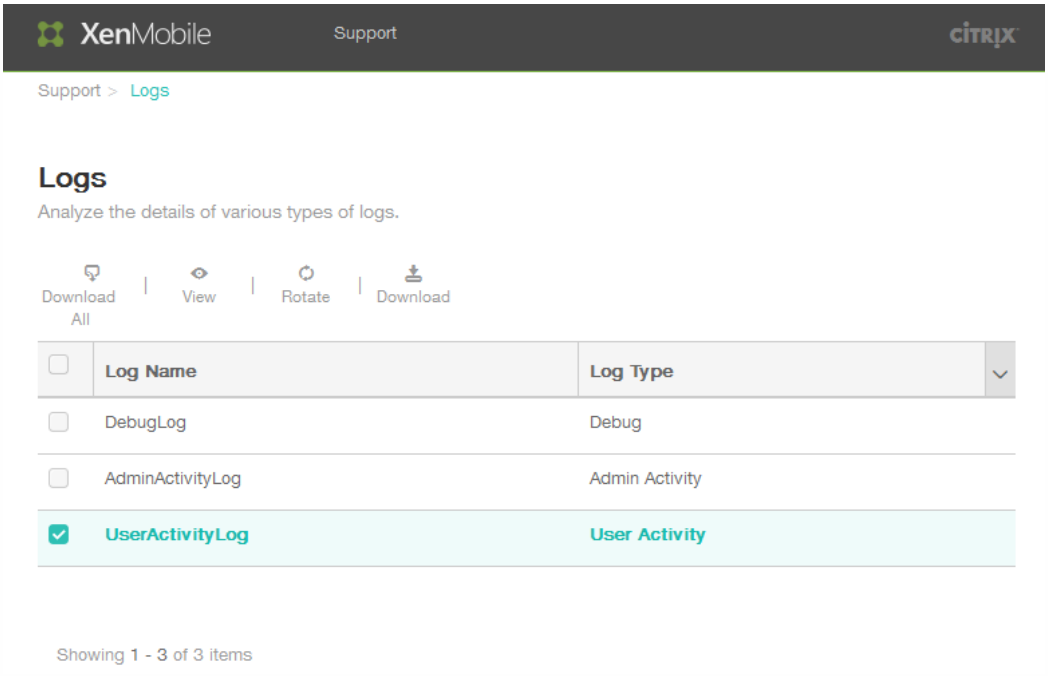
1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa , situado en la esquina superior derecha de la consola. Se abrirá la página Support en una nueva ventana del explorador.



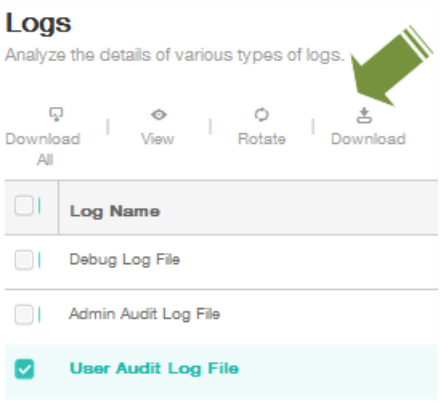
2. En Log Operations, haga clic en **Logs**. Aparecerá la pantalla **Logs**. Los registros individuales se muestran en una tabla.



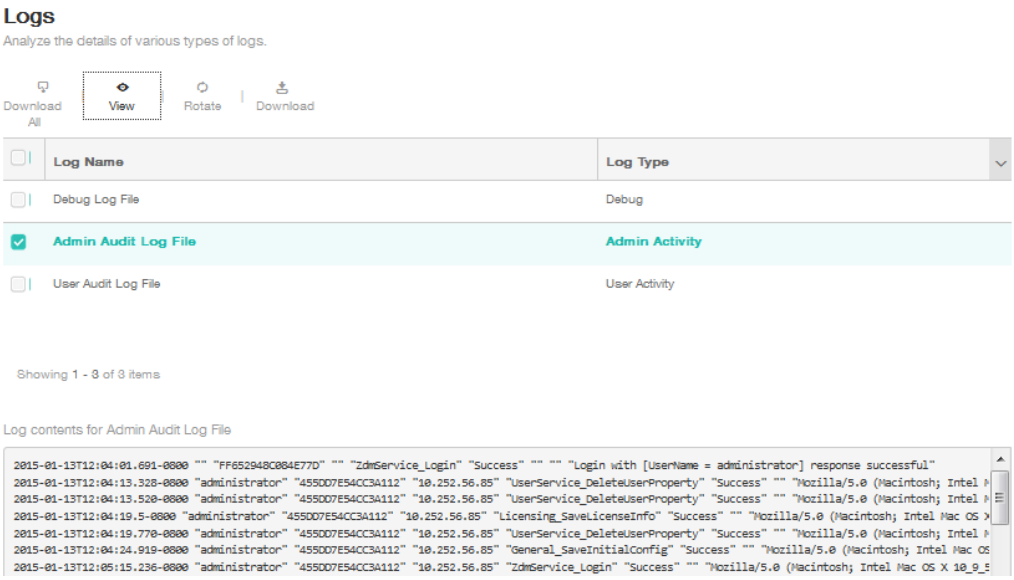
3. Seleccione el registro que quiera ver. Un registro de depuración contiene información útil para el personal de asistencia técnica de Citrix, como mensajes de error y acciones relacionadas con el servidor. En cambio, los registros de actividad de usuario contienen información relacionada con cada usuario configurado. Aparecerá la pantalla **Logs**. Los registros individuales se muestran en una tabla.



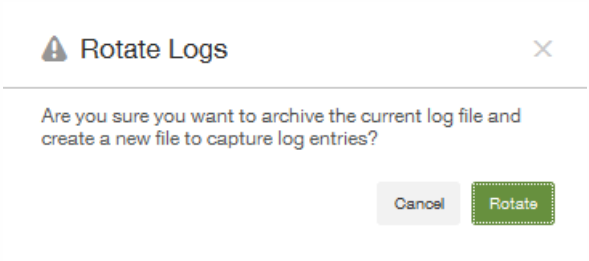
4. Mediante las indicaciones situadas en la parte superior de la tabla, realice las siguientes acciones:
   - Download All. La consola descarga todos los registros del sistema (como los registros de depuración, los registros del servidor y los registros referentes a la actividad de usuarios o administradores). Haga clic en Download para guardar solo los registros seleccionados (también se descargan registros almacenados).



   - View. Muestra, a continuación de la tabla, el contenido del registro.



- Delete. Quita permanentemente un archivo de registros seleccionado.
- Rotate: Almacena el archivo de registros actual y se crea un nuevo archivo para capturar entradas de registro. Al almacenar un archivo de registros, aparece un cuadro de diálogo; ahí, haga clic en Rotate para continuar.



Opciones de la interfaz de línea de comandos en XenMobile

May 05, 2016

Puede acceder en cualquier momento a las opciones de la interfaz de línea de comandos (CLI), presente en el hipervisor en el que se ha instalado XenMobile: Citrix XenServer, Microsoft Hyper-V o VMware ESXi.

A continuación, se presentan las opciones de que dispone a partir del menú principal y de los menús que aparecen para cada una de las cuatro primeras opciones: Configuration, Clustering, System y Troubleshooting.

Menú principal

---

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

Choice: [0 - 5]

Opciones del menú Configuration

En el menú principal, cuando seleccione la opción Configuration, aparecerán los siguientes menús:

[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

Choice: [0 - 4]

Si elige la opción Network, se le pedirá que reinicie para guardar los cambios.

Si elige la opción Firewall, aparecerá el siguiente mensaje:

Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:

- comma separated list of hosts or networks

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

- enter c as value to clear list

HTTP service

Port: 80

Enable access (y/n) [y]:

Management HTTPS service

Port: 4443

Enable access (y/n) [y]:

SSH service

Port [22]:

Enable access (y/n) [y]:

Access white list []:

Management API (for initial staging) HTTPS service

Port [30001]:

Enable access (y/n) [y]:

Access white list []:

Remote support tunnel

Port [8081]:

Enable access (y/n) [n]:

Si elige la opción Database, aparecerá el siguiente mensaje:

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

Opciones del menú Clustering

En el menú principal, cuando seleccione la opción Clustering, aparecerán los siguientes menús:

[0] Back to Main Menu

[1] Show Cluster Status

[2] Enable/Disable cluster

[3] Cluster member white list

[4] Enable or Disable SSL offload

[5] Display Hazelcast Cluster

Choice: [0 - 5]

Si opta por habilitar el uso de clústeres, aparecerá el siguiente mensaje:

To enable realtime communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.

Si opta por inhabilitar el uso de clústeres, aparecerá el siguiente mensaje:

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

Si elige la lista permitida de miembros del clúster y ha inhabilitado la agrupación en clústeres, aparecerá el siguiente mensaje:

Cluster is disabled. Please enable it.

Si ha habilitado la agrupación en clústeres, aparecerán las siguientes opciones:

Current White List:

- comma separated list of hosts or network

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

Please enter hosts or networks to be white listed:

Si opta por habilitar o inhabilitar la descarga de SSL, aparecerá el siguiente mensaje:

Enabling SSL offload will open port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.

Si opta por mostrar Hazelcast Cluster, aparecerán las siguientes opciones:

Hazlecast Cluster Members:

[IP address listed]

NOTE: If an configured node is not part of the cluseter, please reboot that node.

Opciones del menú System

En el menú principal, cuando seleccione la opción System, aparecerán los siguientes menús:

---

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

Choice: [0 - 9]

Opciones del menú Troubleshooting

En el menú principal, cuando seleccione la opción Troubleshooting, aparecerán los siguientes menús:

---

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

Choice: [0 - 3]

Si elige la opción Network Utilities, aparecerá el siguiente menú:

---

[0] Back to Troubleshooting Menu

[1] Network Information

[2] Show Routing Table

[3] Show Address Resolution Protocol (ARP) Table

[4] PING

[5] Traceroute

[6] DNS Lookup

[7] Network Trace

Choice: [0 - 7]

Si elige la opción Logs, aparecerá el siguiente menú:

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

Las API de XenMobile 10

May 05, 2016

En XenMobile 10, se pueden usar las siguientes API de servicios Web para la administración de dispositivos móviles. Puede descargar las API y los SDK para XenMobile del sitio XenMobile Developer Community.

Nombre WSDL	Llama
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

Nombre WSDL	Llama
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice

Nombre WSDL	Llama
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	createOTP
	getAvailableEnrollmentModes
	getOtpInfo
	triggerNotification

XenMobile Mail Manager 10

May 05, 2016

XenMobile Mail Manager ofrece la funcionalidad que amplía las capacidades de XenMobile de este modo:

- Control de acceso dinámico para dispositivos Exchange Active Sync (EAS). Se puede bloquear o permitir inmediatamente el acceso de dispositivos EAS a servicios de Exchange.
- Proporciona a XenMobile la capacidad de acceder a la información de asociación del dispositivo EAS, facilitada por Exchange.
- Proporciona a XenMobile la capacidd de realizar un borrado EAS en un dispositivo móvil.
- Proporciona a XenMobile la capacidad de acceder a la información acerca de dispositivos BlackBerry y realizar operaciones de control tales como un borrado (Wipe) y un restablecimiento de contraseña (ResetPassword).

A continuación, se presentan los problemas conocidos y resueltos de la versión actual de XenMobile Mail Manager 10.0. Para descargar XenMobile Mail Manager, vaya al apartado Server Components de XenMobile 10 Server en Citrix.com.

Problemas conocidos

- La versión instalada de XenMobile Mail Manager siempre muestra 8.5 durante la actualización a XenMobile Mail Manager 10; no obstante, la actualización tiene lugar. [539520]
- La notificación de "dispositivos encontrados" en la instantánea menor puede resultar confusa. Los mismos dispositivos pueden aparecer como "nuevos" en resúmenes de instantánea secundaria sucesivos si las instantáneas secundarias se ejecutan a continuación del inicio de una instantánea principal.

Problemas resueltos

Administración de PowerShell o Exchange

En algunos entornos de Microsoft Exchange (principalmente Office 365), se aplica una restricción sobre XenMobile Mail Manager que limita con eficacia el ancho de banda, lo que impide que una aplicación emita solicitudes de o comandos de PowerShell. Ahora, puede usar una ruta alternativa para el cmdlet de PowerShell en la ficha de configuración de Exchange, que coloca XenMobile Mail Manager en un modo alternativo de instantánea: este modo reemplaza la ruta de datos original.

Un nuevo indicador permite mostrar el marcador **AllowRedirection** para entornos que no son de Microsoft Office 365. Utilice la ficha de configuración de Microsoft Exchange para habilitar este marcador.

Administración de reglas

Ahora, las reglas locales de LDAP admiten un número infinito de grupos para entornos grandes de Active Directory.

XenMobile duplica la información de dispositivo para clientes de WorxMail. Para resolver este problema, deberá habilitar el respaldo a expresiones regulares en la parte del proveedor de servicios administrados (MSP) de XenMobile Mail Manager. Con ello, se filtran los conjuntos de registros devueltos a XenMobile. Aquellos dispositivos que encajen con el filtro no se devuelven a XenMobile.

Proveedor de servicios administrados (Managed Service Provider, MSP)

Ahora, los usuarios que se han quitado de la base de datos de Blackberry Enterprise Server (BES) también se quitarán de la base de datos local.

Interfaz de usuario

Ahora, puede usar una clase de diálogo de progreso para procesos persistentes. En un proceso de este tipo, XenMobile Mail Manager envía comentarios a los usuarios y les ofrece la oportunidad de cancelarlo, si fuera necesario.

El valor predeterminado para nuevas instancias de Microsoft Exchange está establecido en *Shallow*.

Programa de instalación

Aquellos componentes que hagan referencia a Zenprise se han modificado para reflejar XenMobile Mail Manager.

El programa de instalación no responde cuando no puede encontrar la ruta de instalación.

Ahora, el respaldo a binarios y scripts se encuentra en la carpeta Support después de la instalación.

En el menú Inicio de Windows, los accesos directos de XenMobile Mail Manager ahora se encuentran en la carpeta \Citrix\XenMobile Mail Manager.

Asistencia técnica

El modelo de asistencia ofrece la capacidad de habilitar la funcionalidad de la solución de problemas al incorporar un archivo config.xml. Puede usar este archivo para ayudar a solucionar problemas de Citrix. En esta versión de XenMobile Mail Manager, esta función solo se aplica a las pantallas Add y Edit de la configuración de Microsoft Exchange.
Nota: También puede habilitar esta funcionalidad de la solución de problemas si mantiene presionada la tecla Mayús al abrir la utilidad de configuración.

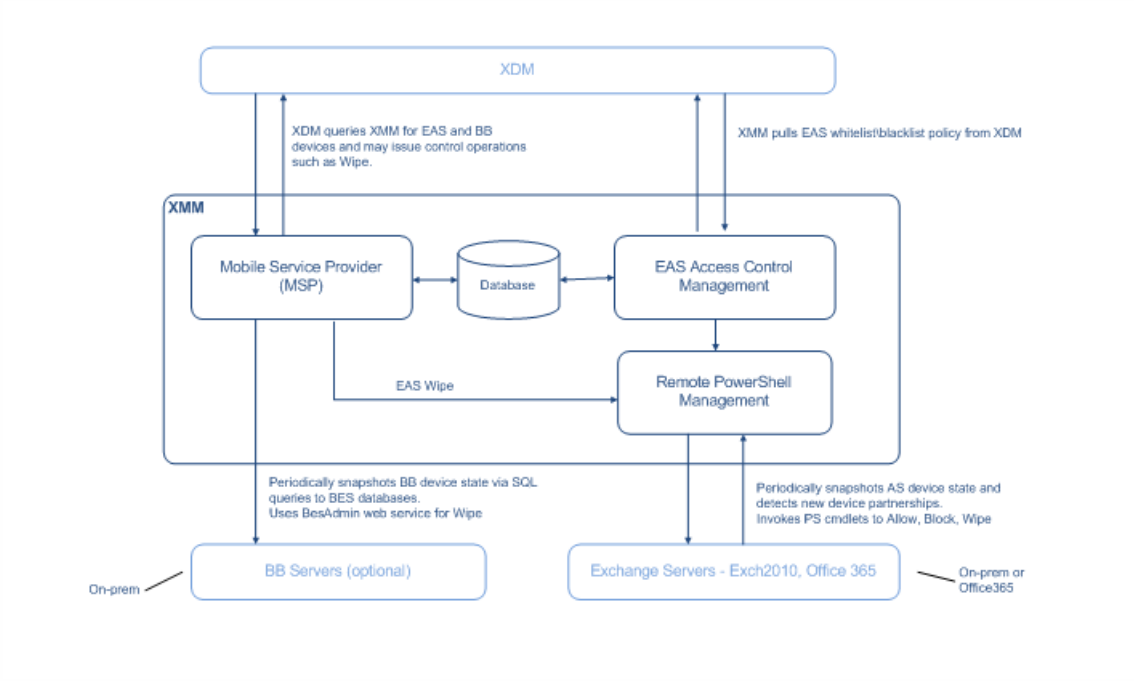
Logging

Ahora, los mensajes de error que devuelva PowerShell tienen asociado un identificador GUID. Use este valor para controlar lo que aparece en la ficha de información detallada Snapshot History.

Arquitectura

Oct 31, 2016

En el siguiente diagrama, se muestran los componentes principales de XenMobile Mail Manager. Para ver diagramas de referencia de arquitectura en detalle, consulte el artículo Reference Architecture for On-Premises Deployments en XenMobile Deployment Handbook.



Los tres componentes principales son:

- **Exchange ActiveSync Access Control Management**. Se comunica con XenMobile para recuperar una directiva de Exchange ActiveSync de XenMobile, y combina esta directiva con cualquier directiva definida localmente para determinar los dispositivos Exchange ActiveSync a los que se debe permitir o denegar el acceso a Exchange. Las directivas definidas localmente amplían las reglas de directivas para permitir el control de acceso en función del grupo de Active Directory, del usuario, del tipo de dispositivo o del agente del dispositivo de usuario (por lo general, la versión de la plataforma móvil).
- **Remote PowerShell Management**. Este componente se encarga de programar e invocar comandos de PowerShell remotos para aprobar la directiva compilada por la administración del control de acceso de Exchange ActiveSync. El componente crea, de forma periódica, una instantánea de la base de datos de Exchange ActiveSync para detectar dispositivos nuevos o modificados de Exchange ActiveSync.
- Mobile Service Provider. Proporciona una interfaz de servicio Web para que XenMobile envíe consultas a dispositivos Exchange ActiveSync o BlackBerry, y emita operaciones de control (como el borrado) destinados a ellos.

Requisitos del sistema y requisitos previos

May 05, 2016

Se deben cumplir los siguientes requisitos mínimos del sistema para XenMobile Mail Manager:

- Windows Server 2008 R2 (debe ser un servidor en idioma inglés)
- Microsoft SQL Server 2008, SQL Server 2012, SQL Server Express 2008, SQL Server 2012 o Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- BlackBerry Enterprise Service, versión 5 (optativo)

Versiones mínimas respaldadas de Microsoft Exchange Server

- Microsoft Office 365
- Exchange Server 2013
- Exchange Server 2010 SP2

Requisitos previos de XenMobile Mail Manager

- Windows Management Framework debe estar instalado.
  - PowerShell V4, V3 y V2
- La directiva de ejecución de PowerShell se debe establecer en RemoteSigned mediante Set-ExecutionPolicy RemoteSigned.
- El puerto TCP 80 debe estar abierto entre el equipo con XenMobile Mail Manager y el servidor Exchange remoto.

Requisitos para un equipo local con Exchange

- **Permisos**. El control de acceso basado en roles (RBAC) de Exchange no se va a tratar en esta documentación. Dicho esto, como mínimo, las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben permitir la conexión al servidor Exchange y deben tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- Si XenMobile Mail Manager está configurado para ver todo el bosque, se debe haber concedido permiso para ejecutar: Set-AdServerSettings -ViewEntireForest $true
- Las credenciales suministradas deben contar con derecho a conectarse al servidor Exchange mediante el shell remoto. De forma predeterminada, el usuario que haya instalado Exchange tiene ese derecho.
- Según http://technet.microsoft.com/en-us/library/dd315349.aspx, para establecer una conexión remota y ejecutar comandos remotos, las credenciales deben corresponder a un usuario que sea administrador en la máquina remota. De acuerdo con esta entrada de blog, http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx, Set-PSSessionConfiguration se puede usar para eliminar el requisito de administrador, pero el respaldo y el debate sobre los detalles de este comando no se tratarán en este documento.
- El servidor Exchange debe estar configurado para admitir solicitudes remotas de PowerShell a través de HTTP. Por regla

general, lo único que se necesita es que un administrador ejecute el siguiente comando de PowerShell en el servidor Exchange: `WinRM QuickConfig`.

- Exchange tiene muchas directivas de limitación de peticiones. Una de ellas controla la cantidad de conexiones simultáneas de PowerShell que se permiten por usuario. La cantidad predeterminada de conexiones simultáneas permitidas a un usuario es de 18 en Exchange 2010. Cuando se alcance el límite de conexiones, XenMobile Mail Manager no podrá conectarse al servidor Exchange. Hay maneras de cambiar la cantidad máxima de conexiones simultáneas permitidas a través de PowerShell, pero no se tratarán en esta documentación. Si le interesa, consulte las directivas de limitación de Exchange que estén relacionadas con la administración remota con PowerShell.

Requisitos para Office 365 Exchange

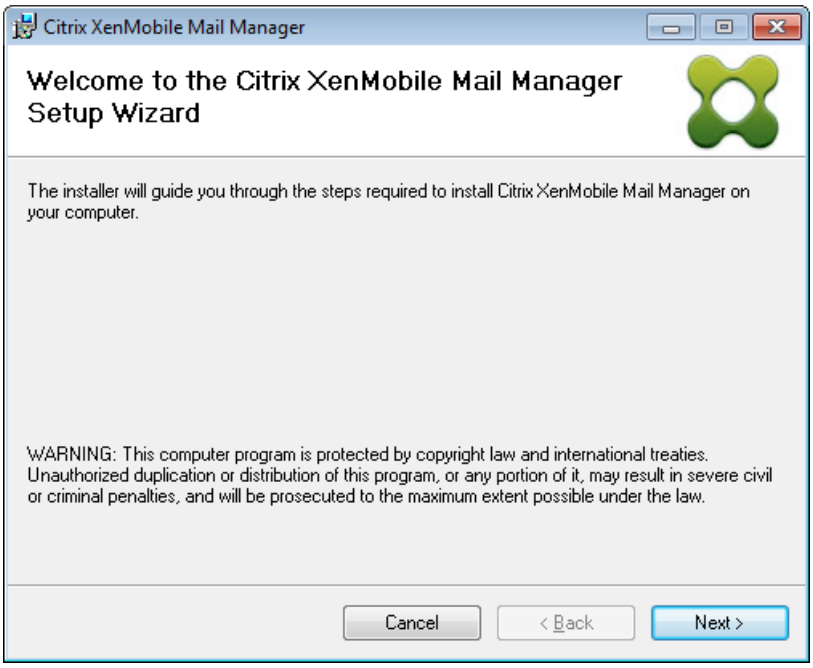
- **Permisos**. El control de acceso basado en roles (RBAC) de Exchange no se va a tratar en esta documentación. Dicho esto, como mínimo, las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben permitir la conexión a Office 365 y deben tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange:
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
- Las credenciales suministradas deben contar con el derecho a conectarse al servidor de Office 365 a través del shell remoto. De forma predeterminada, el administrador conectado de Office 365 tiene los privilegios requeridos.
- Exchange tiene muchas directivas de limitación de peticiones. Una de ellas controla la cantidad de conexiones simultáneas de PowerShell que se permiten por usuario. La cantidad predeterminada de conexiones simultáneas permitidas a un usuario es de tres en Office 365. Cuando se alcance el límite de conexiones, XenMobile Mail Manager no podrá conectarse al servidor Exchange. Hay maneras de cambiar la cantidad máxima de conexiones simultáneas permitidas a través de PowerShell, pero no se tratarán en esta documentación. Si le interesa, consulte las directivas de limitación de Exchange que estén relacionadas con la administración remota con PowerShell.

Instalación y configuración

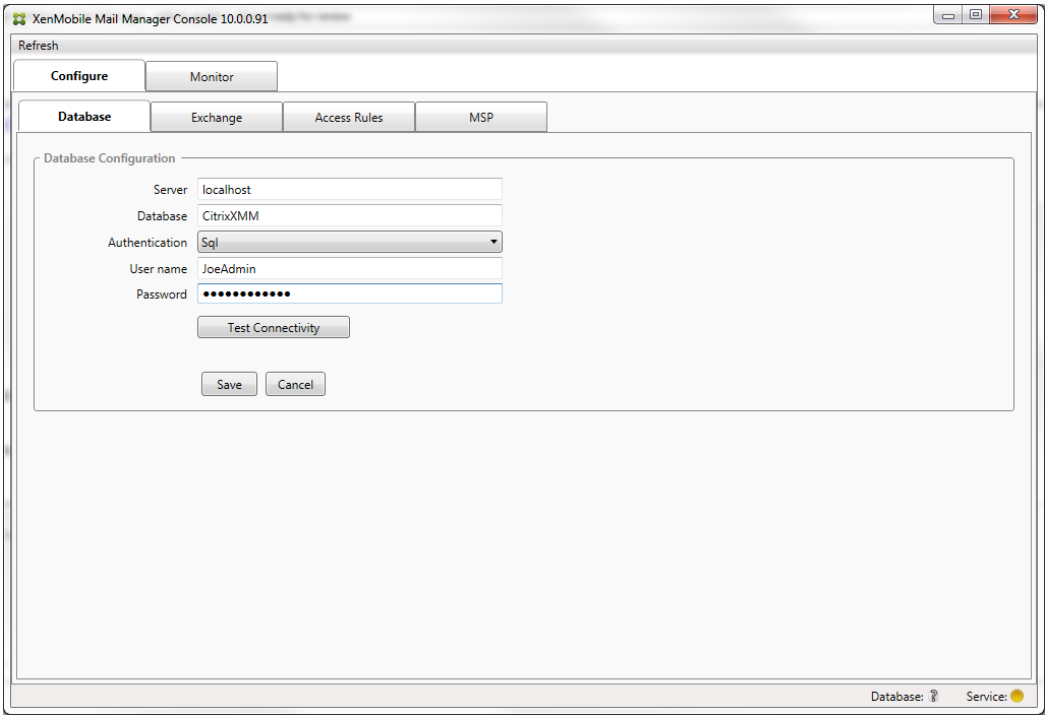
May 05, 2016

Siga estos pasos para instalar y configurar XenMobile Mail Manager. Antes de empezar, revise los requisitos previos y los requisitos del sistema. Para ver más información, consulte Requisitos previos y requisitos del sistema para XenMobile Mail Manager.

1. Haga clic en el archivo XmmSetup.msi y, a continuación, siga las instrucciones del programa de instalación para instalar XenMobile Mail Manager.

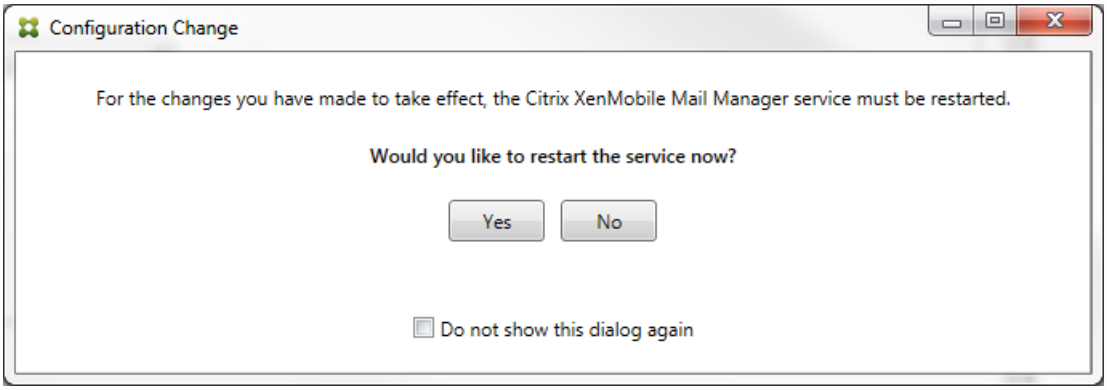


2. En el menú Inicio, abra XenMobile Mail Manager.
3. Configure las siguientes propiedades de base de datos:
   1. Seleccione la ficha Configure > Database.
   2. Escriba el nombre del servidor SQL Server (el valor predeterminado es localhost).
   3. Conserve la opción predeterminada de la base de datos, CitrixXmm.
   4. Seleccione uno de los siguientes modos de autenticación para SQL:
      - Sql. Escriba el nombre de usuario y la contraseña de un usuario de SQL válido.
      - Windows Integrated. Si elige esta opción, las credenciales de inicio de sesión del servicio de XenMobile Mail Manager se deben cambiar a una cuenta de Windows que tenga permisos para acceder al servidor SQL Server. Para ello, abra Panel de control > Herramientas administrativas > Servicios, haga clic con el botón secundario en la entrada del servicio de XenMobile Mail Manager y, a continuación, haga clic en la ficha Iniciar sesión.
        Nota: Si para la conexión de base de datos de BlackBerry también se selecciona la seguridad integrada de Windows, la cuenta de Windows que se especifique aquí también debe tener acceso a la base de datos de BlackBerry.

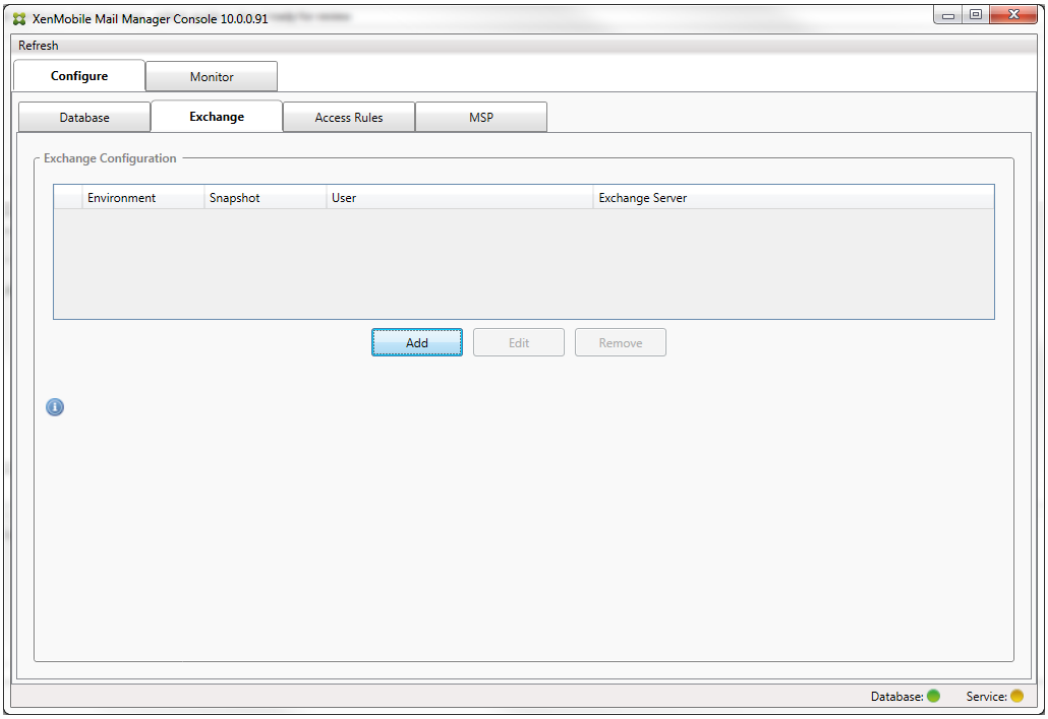


5. Haga clic en Test Connectivity para comprobar que se puede establecer conexión con el servidor SQL Server y, a continuación, haga clic en Save.

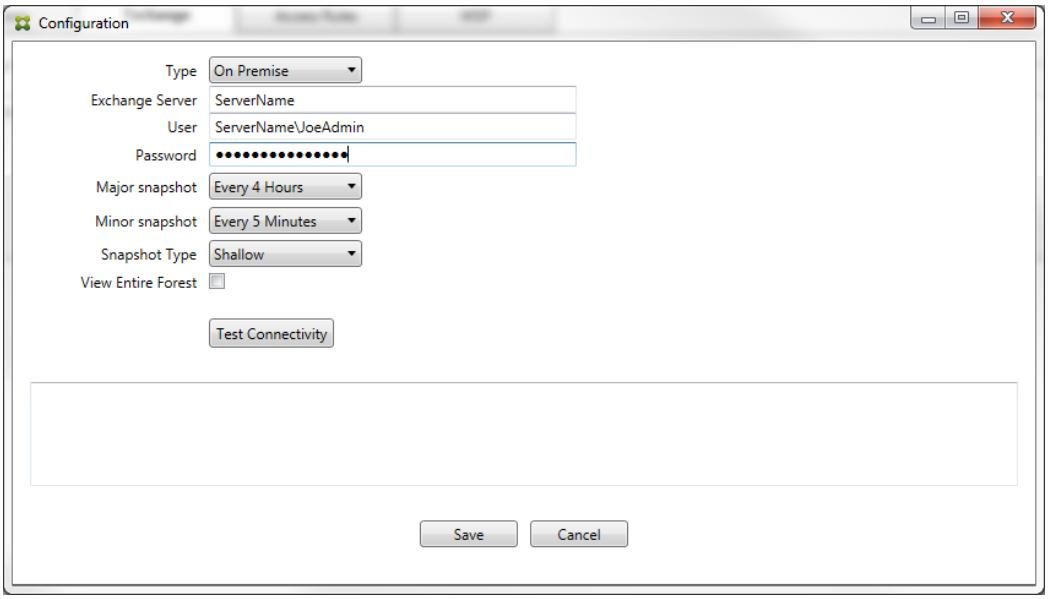
4. Un mensaje le solicitará que reinicie el servicio. Haga clic en Sí.



5. Configure uno o varios servidores Exchange:
   1. Si administra un solo entorno de Exchange, solo deberá especificar un servidor. Si administra varios entornos de Exchange, deberá especificar un servidor Exchange por cada entorno de Exchange.
   2. Haga clic en la ficha Configure > Exchange.



3. Haga clic en Add.
4. Seleccione el tipo de entorno de Exchange Server: On Premise o Office 365.

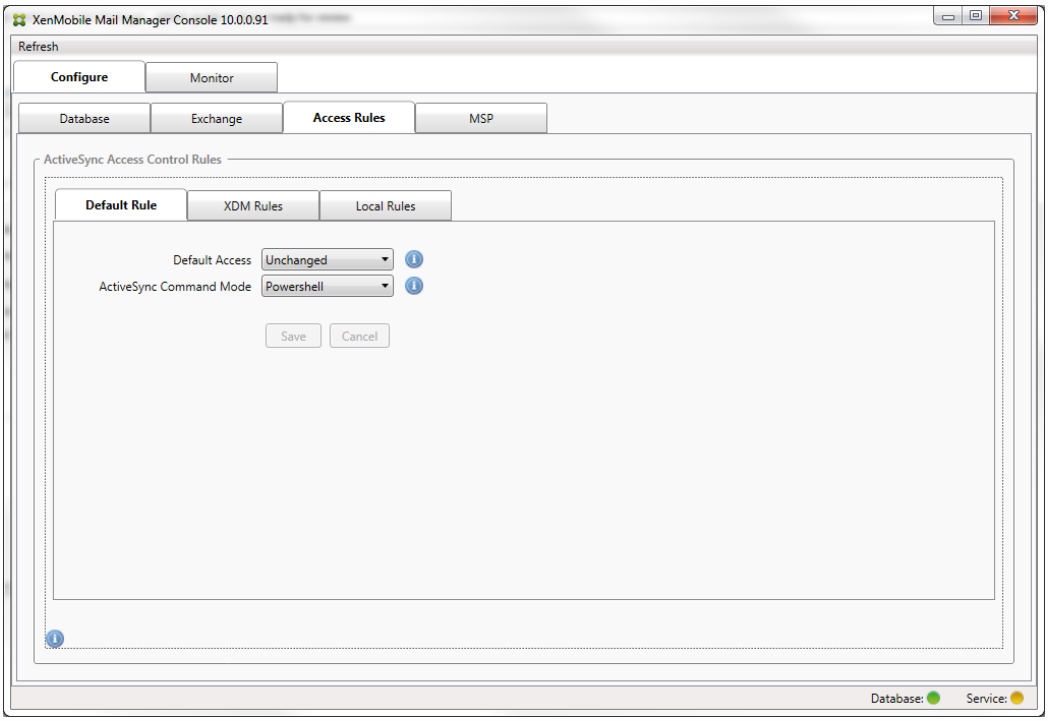


5. Si selecciona On Premise, escriba el nombre del servidor Exchange que se usará para los comandos remotos de PowerShell.
6. Escriba el nombre de usuario de una identidad de Windows que tenga los permisos apropiados en el servidor Exchange, como se especifica en el apartado de requisitos.
7. Escriba la contraseña del usuario en el campo Password.
8. Seleccione un horario para ejecutar las instantáneas principales. Una instantánea principal detecta cada asociación de Exchange ActiveSync.
9. Seleccione un horario para ejecutar las instantáneas secundarias. Una instantánea secundaria detecta asociaciones recién creadas de Exchange ActiveSync.
10. Seleccione el tipo de instantánea: Deep o Shallow. Las instantáneas superficiales (Shallow) son más rápidas y, con

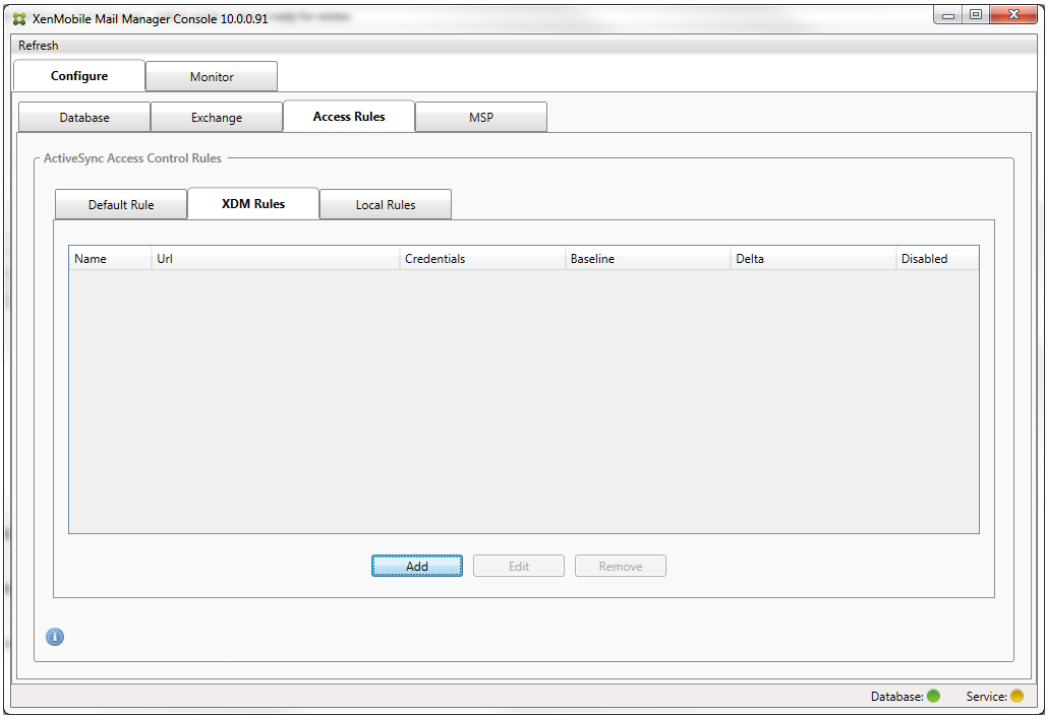
ellas, es suficiente para llevar a cabo todas las funciones de control de acceso de Exchange ActiveSync que se pueden realizar en XenMobile Mail Manager. Las instantáneas detalladas (Deep) pueden tardar mucho más y solo son necesarias si el proveedor de servicios móviles está habilitado para ActiveSync, lo que permite que XenMobile envíe consultas a dispositivos no administrados.

11. Haga clic en Test Connectivity para comprobar que se puede establecer conexión con el servidor Exchange y, a continuación, haga clic en Save.
12. Un mensaje le solicitará que reinicie el servicio. Haga clic en Sí.

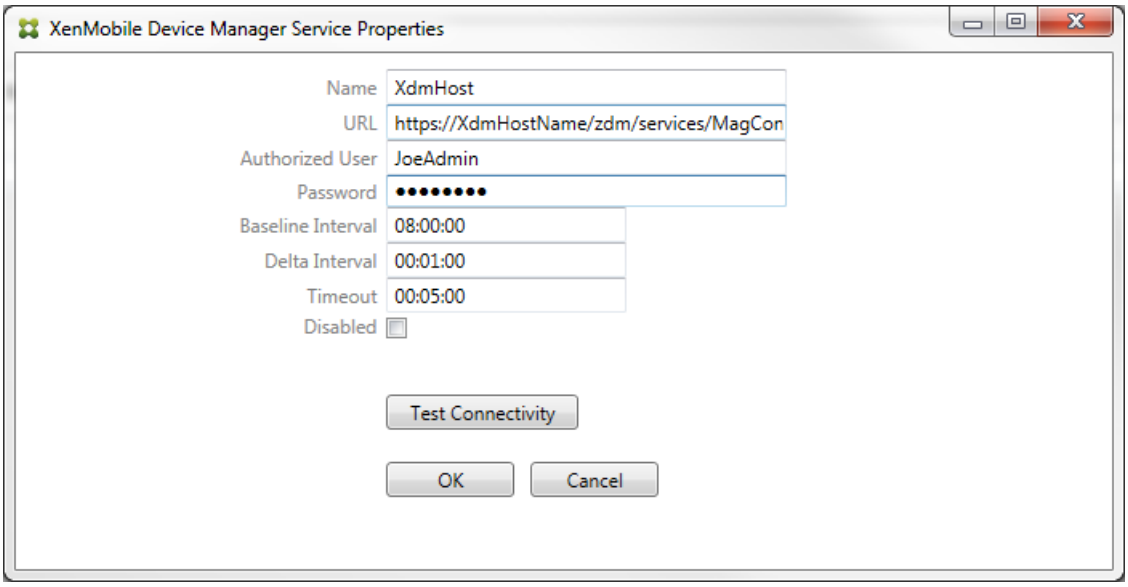
6. Configure las reglas de acceso:
    1. Seleccione la ficha Configure > Access Rules.



    2. Seleccione el acceso predeterminado: Allow, Block o Unchanged. Este parámetro controla cómo se tratarán todos los dispositivos, excepto aquellos que XenMobile o las reglas locales identifiquen de forma explícita. Si selecciona Allow, se permitirá el acceso de ActiveSync a todos los dispositivos; si selecciona Block, se denegará el acceso; si selecciona Unchanged, no se realizará ningún cambio.
    3. Seleccione el modo de comandos de ActiveSync: PowerShell o Simulation.
        - En el modo PowerShell, XenMobile Mail Manager emitirá comandos de PowerShell para habilitar el control de acceso pertinente.
        - En el modo Simulation, XenMobile Mail Manager no emitirá comandos de PowerShell, pero registrará en la base de datos el comando en cuestión, así como los resultados esperados. En el modo Simulation, el usuario puede usar la ficha Monitor para ver lo que podría haber ocurrido si se hubiera habilitado el modo PowerShell.
    4. Haga clic en Save.
7. Haga clic en la ficha XDM Rules.



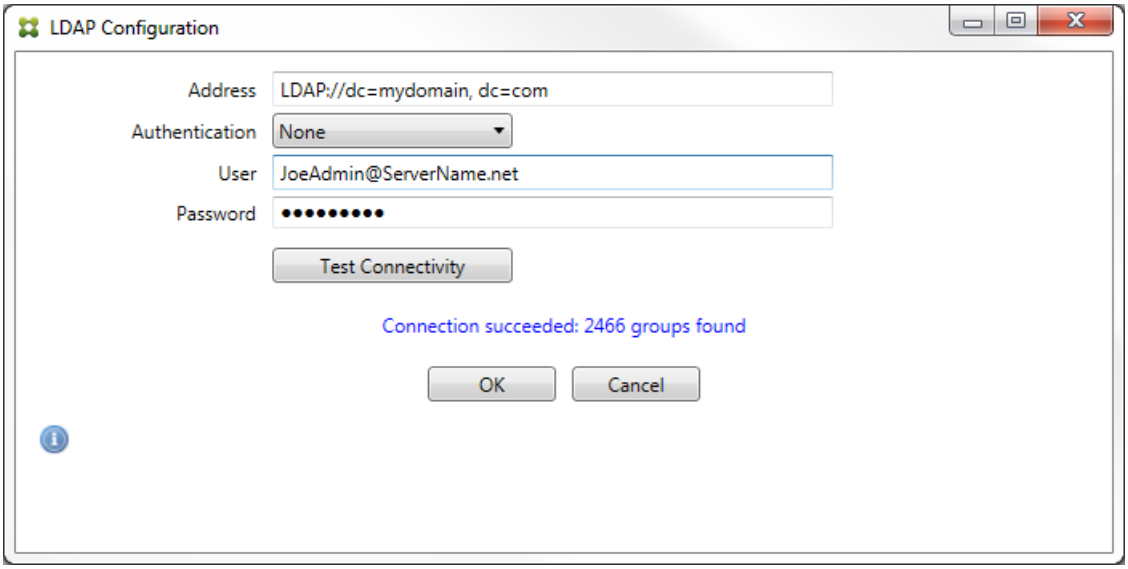
1. Haga clic en Agregar.
2. Escriba un nombre para las reglas XDM, como XdmHost.



3. Modifique la cadena de URL para que haga referencia al servidor XenMobile. Por ejemplo, si el nombre del servidor es XdmHost, especifique http://XdmHostName/zdm/services/MagConfigService.
4. Especifique un usuario autorizado en el servidor.
5. Escriba la contraseña del usuario.
6. Conserve los valores predeterminados de Baseline Interval, Delta Interval y Timeout values.
7. Haga clic en Test Connectivity para probar la conexión con el servidor.
   Nota: Si la casilla Disabled está marcada, el servicio de XenMobile Mail no recopilará directivas del servidor XenMobile.
8. Haga clic en Aceptar.

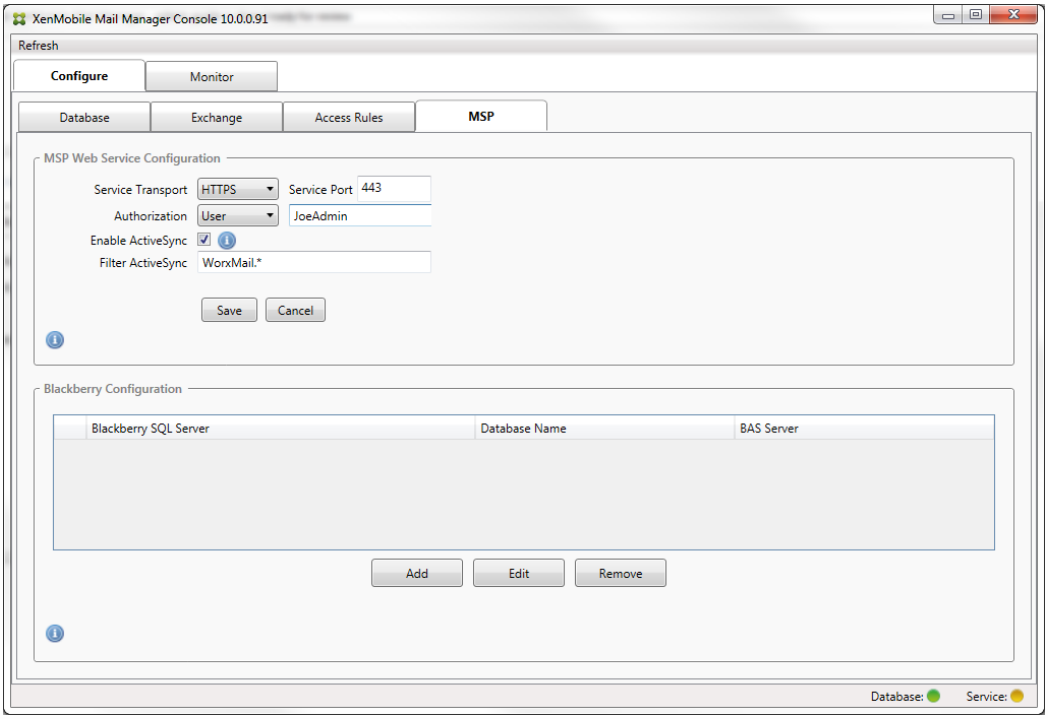
8. Haga clic en la ficha Local Rules.
   1. Si quiere crear reglas locales que operen en grupos de Active Directory, haga clic en Configure LDAP y, a continuación,

configure las propiedades de conexión de LDAP.



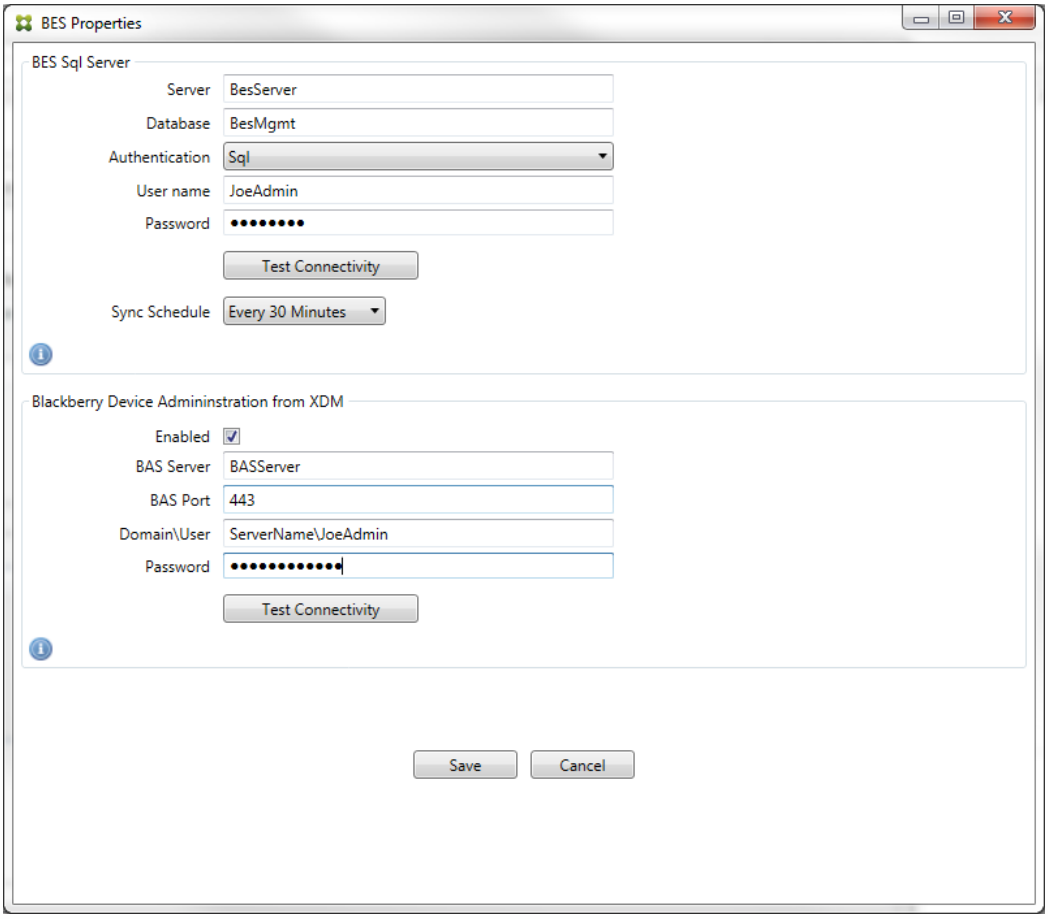
2. Puede agregar reglas locales en función de: ActiveSync Device ID (el ID de dispositivo de ActiveSync), Device Type (el tipo de dispositivo), AD Group (el grupo de Active Directory), User (el usuario) o UserAgent (el agente del usuario del dispositivo). En la lista, seleccione el tipo adecuado. Para ver información detallada, consulte Reglas de control de acceso de XenMobile Mail Manager.
3. Escriba texto o fragmentos de texto en el cuadro de texto. Si quiere, haga clic en el botón de consulta para ver las entidades que se corresponden con el fragmento.
   Nota: Para todos los criterios aparte de Group, el sistema se basa en los dispositivos que se han encontrado en una instantánea. Por lo tanto, si acaba de empezar y aún no ha completado ninguna instantánea, no habrá entidades disponibles.
4. Seleccione un valor de texto y, a continuación, haga clic en Allow o en Deny para agregarlo a Rule List en el lado derecho. Puede quitar reglas o cambiar su orden mediante los botones situados a la derecha del panel Rule List. El orden es importante porque las reglas se cotejan en el orden mostrado con un usuario y un dispositivo determinados. Por tanto, una correspondencia en una regla que se encuentre más arriba significa que las siguientes reglas no tendrán ningún efecto. Por ejemplo, si tiene una regla que permite todos los dispositivos iPad y otra regla posterior que bloquee al usuario “Sergio”, el iPad de Sergio aún tendrá permiso porque la regla “iPad” tiene una prioridad mayor (se coteja antes) que la regla “Sergio”.
5. Para llevar a cabo un análisis de las reglas de la lista con el fin de buscar posibles conflictos, invalidaciones o complementaciones, haga clic en Analyze.
6. Haga clic en Save.

9. Cómo configurar el proveedor de servicios móviles
   Nota: El proveedor de servicios móviles es optativo; solo es necesario si XenMobile también está configurado para usar la interfaz del proveedor de servicios móviles con el fin de consultar dispositivos no administrados.
   1. Seleccione la ficha Configure > MSP.



2. Establezca el tipo de servicio de transporte como HTTP o HTTPS para el servicio del proveedor de servicios móviles.
3. Establezca el puerto del servicio (por regla general, 80 y 443) para el servicio del proveedor de servicios móviles.
   Nota: Si usa el puerto 443, el puerto requiere un certificado SSL asociado a él en IIS.
4. Defina el usuario o el grupo de autorización. Esta opción establece el usuario o grupo de usuarios que podrán conectarse al proveedor de servicios móviles desde XenMobile.
5. Defina si se habilitan o no las consultas de ActiveSync.
   Nota: Si se habilitan las consultas de ActiveSync para el servidor XenMobile, el tipo de instantánea de uno o más servidores Exchange debe ser Deep, lo que puede generar costes importantes de rendimiento para realizar instantáneas.
6. De forma predeterminada, los dispositivos ActiveSync que se corresponden con la expresión regular WorxMail.* no se enviarán a XenMobile. Para cambiar este comportamiento, modifique el campo Filter ActiveSync como sea necesario.
   Nota: Dejarlo en blanco significa que todos los dispositivos se reenviarán a XenMobile.
7. Haga clic en Save.

10. Si quiere, puede configurar uno o más servidores BlackBerry Enterprise Server (BES):
    1. Haga clic en Agregar.
    2. Escriba el nombre del servidor SQL Server para BES.



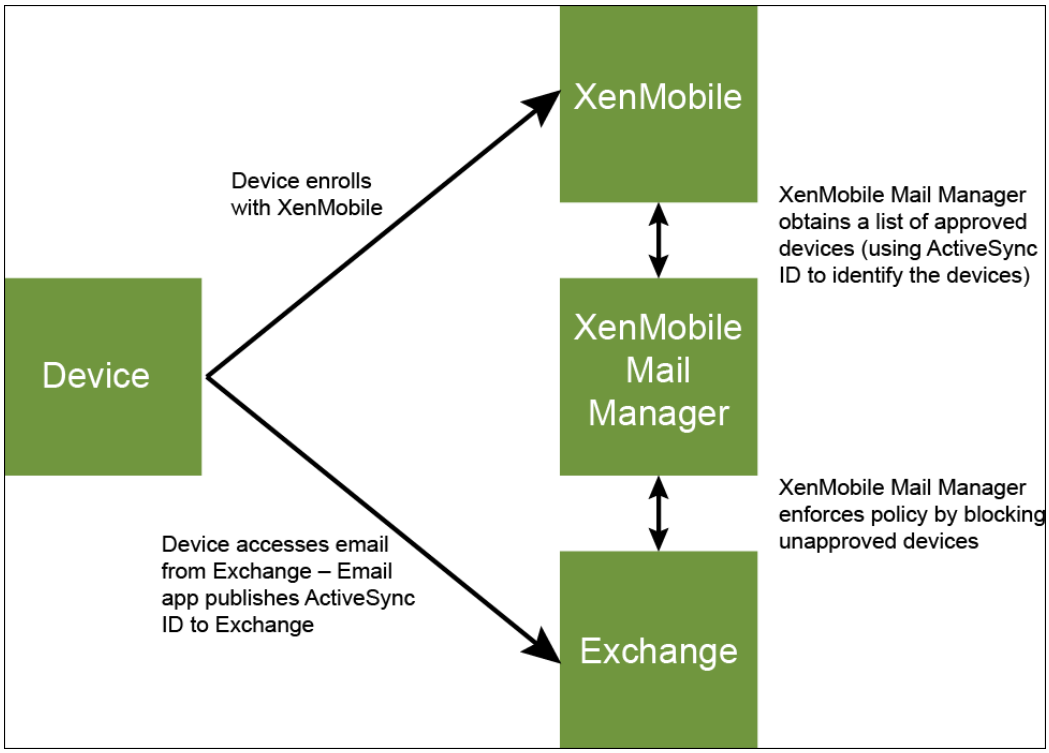
3. Escriba el nombre de la base de datos de administración de BES.
4. Seleccione el modo de autenticación. Si se selecciona la autenticación integrada de Windows, la cuenta de usuario del servicio de XenMobile Mail Manager será la cuenta utilizada para conectarse al servidor SQL Server para BES.
   Nota: Si también selecciona la seguridad integrada de Windows para la conexión de base de datos de XenMobile Mail Manager, la cuenta de Windows especificada aquí también debe tener acceso a la base de datos de XenMobile Mail Manager.
5. Si se selecciona SQL authentication, especifique el nombre de usuario y la contraseña.
6. Configure la programación de sincronización en Sync Schedule. Esta es la programación usada para conectarse al servidor SQL Server para BES y buscar actualizaciones de dispositivo.
7. Haga clic en Test Connectivity para comprobar la conectividad con el servidor SQL Server.
   Nota: Si se selecciona Windows Integrated (la seguridad integrada de Windows), esta prueba utiliza el usuario actual que ha iniciado sesión, no el usuario del servicio de XenMobile Mail Manager; por lo tanto, la prueba de autenticación de SQL no es precisa.
8. Si quiere admitir el borrado (Wipe) o el restablecimiento de contraseña (ResetPassword) remotos para los dispositivos BlackBerry desde XenMobile, marque la casilla Enabled.
   1. Introduzca el nombre de dominio completo (FQDN) del servidor BES.
   2. Escriba el puerto de BES usado para el servicio Web del administrador.
   3. Escriba el nombre del usuario y la contraseña completos requeridos por el servicio de BES.
   4. Haga clic en Test Connectivity para probar la conexión al servidor BES.
   5. Haga clic en Guardar.

Aplicación de directivas de correo electrónico con los ID de ActiveSync

May 05, 2016

Es posible que una directiva de correo electrónico de la empresa indique que ciertos dispositivos no tienen la aprobación para usar el correo electrónico de la empresa. Para cumplir con esta directiva, asegúrese de que los usuarios no pueden tener acceso al correo electrónico de la empresa desde dichos dispositivos. XenMobile Mail Manager y XenMobile funcionan conjuntamente para aplicar la directiva de correo electrónico. XenMobile define la directiva para el acceso de correo electrónico de la empresa y, cuando un dispositivo no aprobado se inscribe con XenMobile, XenMobile Mail Manager aplica la directiva.

El cliente de correo electrónico en un dispositivo se anuncia a Exchange Server (o Office 365) usando el ID del dispositivo, también conocido como el ID de ActiveSync, que se usa para identificar el dispositivo de manera exclusiva. Worx Home obtiene un identificador similar y envía el identificador a XenMobile cuando se inscribe el dispositivo. Comparando los dos ID de dispositivo, XenMobile Mail Manager puede determinar si un dispositivo en concreto debe tener acceso al correo electrónico de la empresa. En la siguiente ilustración se muestra este concepto.



Si XenMobile envía un ID de ActiveSync a XenMobile Mail Manager que es diferente del ID que el dispositivo publica en Exchange, XenMobile Mail Manager no puede indicar a Exchange qué hacer con el dispositivo.

Los ID de ActiveSync coincidentes funcionan con fiabilidad en la mayoría de las plataformas; sin embargo, Citrix ha detectado que en algunas implementaciones de Android, el ID de ActiveSync enviado desde el dispositivo es diferente del ID que el cliente de correo anuncia en Exchange. Para evitar este problema, puede hacer lo siguiente:

- En la plataforma Samsung SAFE, inserte la configuración de ActiveSync del dispositivo desde XenMobile.

- En todas las demás plataformas Android, inserte la configuración de la aplicación Touchdown y la configuration de Touchdown ActiveSync desde XenMobile.

No obstante, esto no impide que un empleado instale un cliente de correo electrónico distinto de Touchdown en un dispositivo Android. Para garantizar que la directiva de acceso al correo electrónico de la empresa se aplica correctamente, puede adoptar una postura de seguridad defensiva y configurar XenMobile Mail Manager para que bloquee los mensajes de correo electrónico definiendo la directiva estática con el valor Deny by default. Esto significa que si un empleado configura un cliente de correo electrónico distinto de Touchdown en un dispositivo Android, y si la detección de ID de ActiveSync no funciona correctamente, el acceso al correo electrónico de la empresa le será denegado a dicho empleado.

Reglas de control de acceso

May 05, 2016

XenMobile Mail Manager ofrece un enfoque basado en reglas para configurar de forma dinámica el control del acceso a los dispositivos Exchange ActiveSync. Una regla de control de acceso de XenMobile Mail Manager está compuesta de dos partes: una expresión correspondiente y un estado de acceso deseado (Permitir o Bloquear). Una regla se puede cotejar con un dispositivo Exchange ActiveSync concreto para determinar si se le puede aplicar (es decir, si se corresponde con el dispositivo). Hay varios tipos de expresiones correspondientes. Por ejemplo: una regla puede corresponderse con todos los dispositivos de un determinado tipo o un ID de Exchange ActiveSync o todos los dispositivos de un usuario concreto, entre otros.

En cualquier momento durante el proceso de agregar, quitar y cambiar el orden de las reglas en la lista de reglas, puede hacer clic en el botón Cancel para revertir la lista de reglas al estado en que estaba al abrirla. A menos que haga clic en Save, los cambios realizados en esta ventana se perderán si cierra la herramienta de configuración.

XenMobile Mail Manager dispone de tres tipos de reglas: reglas locales, reglas XDM y la regla del acceso predeterminado.

Local rules. Las reglas locales tienen la prioridad más alta: Si un dispositivo coincide con una regla local, el proceso de cotejo de reglas se detiene. No se consultarán ni las reglas XDM ni la regla del acceso predeterminado. Las reglas locales se configuran localmente en XenMobile Mail Manager, mediante la ficha Configure/Access Rules/Local Rules. La correspondencia de apoyo se basa en la pertenencia de un usuario de un grupo determinado de Active Directory. La correspondencia de apoyo se basa en expresiones regulares de los siguientes campos:

- ID del dispositivo ActiveSync
- Tipo de dispositivo ActiveSync
- Nombre principal de usuario (UPN)
- Agente del usuario de ActiveSync (normalmente, la plataforma del dispositivo o el cliente de correo electrónico)

Mientras una instantánea principal se complete y encuentre dispositivos, podrá agregar reglas, ya sean de expresión regular o normal. Si no se completa ninguna instantánea principal, solo podrá agregar reglas de expresión regular.

XDM rules. Las reglas XDM son referencias a un servidor externo de XenMobile que proporciona reglas de dispositivos administrados. El servidor XenMobile se puede configurar con sus propias reglas de alto nivel, que identifican aquellos dispositivos que se van a permitir o a bloquear en función de las propiedades que conozca XenMobile, como, por ejemplo, si el dispositivo se ha liberado por jailbreak o si contiene aplicaciones prohibidas. XenMobile coteja las reglas de alto nivel y genera un conjunto de identificadores de dispositivos ActiveSync permitidos o bloqueados. Después, estos ID se entregan a XenMobile Mail Manager.

Default access rule. La regla del acceso predeterminado es única en que es una correspondencia potencial con todos los dispositivos y siempre se coteja la última. Esta es una regla comodín, lo que significa que, si un dispositivo determinado no coincide con ninguna regla XDM o de acceso local, el estado de acceso deseado del dispositivo lo determina el estado de acceso deseado de la regla del acceso predeterminado.

- Default Access – Allow. Se permitirá el acceso de cualquier dispositivo que no coincida con una regla XDM o local.
- Default Access – Block. Se bloqueará el acceso de cualquier dispositivo que no coincida con una regla XDM o local.
- Default Access - Unchanged. XenMobile Mail Manager no modificará el estado de acceso de un dispositivo que no se corresponda con una regla XDM o local. Si Exchange ha puesto un dispositivo en el modo de cuarentena, no se realiza ninguna acción; por ejemplo, la única forma de quitar un dispositivo del modo de cuarentena es tener una regla local o XDM que ignore explícitamente la cuarentena.

Acerca de los cotejos de reglas

Las reglas se cotejan siguiendo un orden (de mayor a menor prioridad) con cada dispositivo sobre el que Exchange informa a XenMobile Mail Manager.

- Reglas locales
- Regla del acceso predeterminado
- Reglas XDM

Cuando se encuentra una correspondencia, el cotejo se detiene. Por ejemplo: si una regla local se corresponde con un dispositivo determinado, este no se cotejará con ninguna regla XDM ni con la regla del acceso predeterminado. Esto también se da en el caso de un tipo concreto de regla. Por ejemplo, si hay más de una correspondencia en la lista de reglas para un dispositivo concreto, tan pronto como se encuentre la primera correspondencia, el cotejo se detiene.

XenMobile Mail Manager vuelve a cotejar el conjunto de reglas definido cuando cambian las propiedades del dispositivo, cuando se agregan o quitan dispositivos o cuando cambian las reglas en sí. Las instantáneas principales pueden elegir cambios y eliminaciones de las propiedades de dispositivo a intervalos que se pueden configurar. Las instantáneas secundarias eligen dispositivos nuevos a intervalos que se pueden configurar.

Exchange ActiveSync también tiene reglas que controlan el acceso. Es importante entender la manera en que funcionan estas reglas en el contexto de XenMobile Mail Manager. Exchange se puede configurar con tres niveles de reglas: exenciones personales, reglas de dispositivos y parámetros de organización. XenMobile Mail Manager automatiza el control del acceso por la emisión, mediante programación, de solicitudes remotas de PowerShell que afectan a las listas de excepciones personales. Se trata de listas de identificadores de dispositivos Exchange ActiveSync permitidos o bloqueados asociados a un buzón de correo determinado. Cuando XenMobile Mail Manager se implementa, asume la capacidad de administración de las listas de exención en Exchange. Para obtener más información, consulte este artículo de Microsoft.

El análisis es especialmente útil en situaciones en que se han definido varias reglas para el mismo campo. Puede detectar problemas potenciales de las relaciones entre las reglas. El análisis se realiza con respecto a los campos de reglas; por ejemplo, las reglas se analizan en grupos basados en el campo correspondiente, como el ID del dispositivo ActiveSync, el tipo de dispositivo ActiveSync, el usuario y el agente de usuario, entre otros.

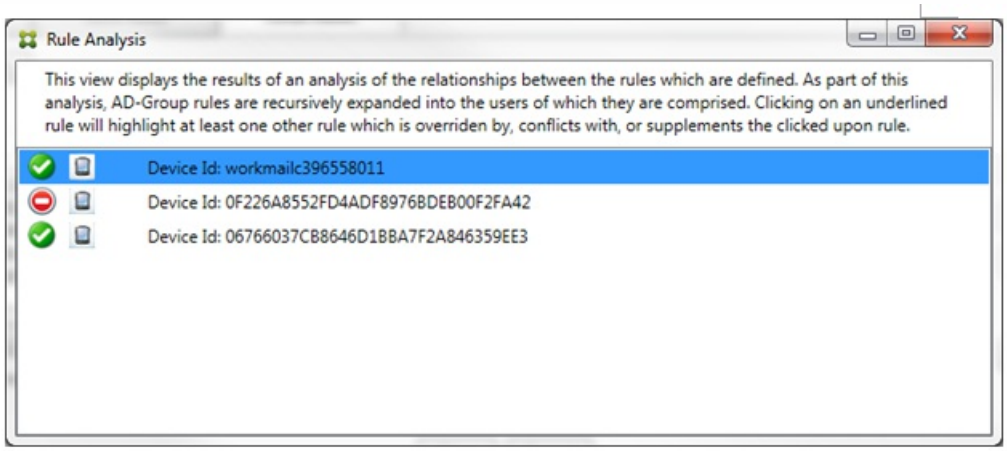
Terminología referente a las reglas:

- **Overriding rule** (Regla de invalidación). Se produce una invalidación cuando hay más de una regla que se podría aplicar al mismo dispositivo. Como las reglas se cotejan por prioridad en la lista, es posible que las últimas instancias de reglas que se podrían aplicar nunca se cotejen.
- **Conflicting rule** (Regla en conflicto). El conflicto se produce cuando hay más de una regla que se podría aplicar al mismo dispositivo, pero el acceso (permitir o bloquear) no se corresponde. Si las reglas conflictivas no son de expresión regular, un conflicto siempre tiene la connotación implícita de una invalidación.
- **Supplemental rule** (Regla adicional). Se produce una adición cuando hay varias reglas de expresión regular y, por lo tanto, es posible que necesite comprobar que las dos (o más) expresiones regulares se pueden combinar en una sola regla de expresión regular, o bien deberá comprobar que no dupliquen la funcionalidad. Una regla adicional también puede entrar en conflicto en el acceso (permitir o bloquear).
- **Primary rule** (Regla primaria). La regla primaria es aquella sobre la que se ha hecho clic en el cuadro de diálogo. La regla está indicada visualmente por una línea de borde sólido que la rodea. La regla también tiene una o dos flechas verdes que apuntan hacia arriba o hacia abajo. Si una flecha apunta arriba, indica que hay reglas auxiliares que preceden la regla primaria. Si una flecha apunta abajo, indica que hay reglas auxiliares que siguen a la regla primaria. Solo una regla primaria puede estar activa en un momento dado.

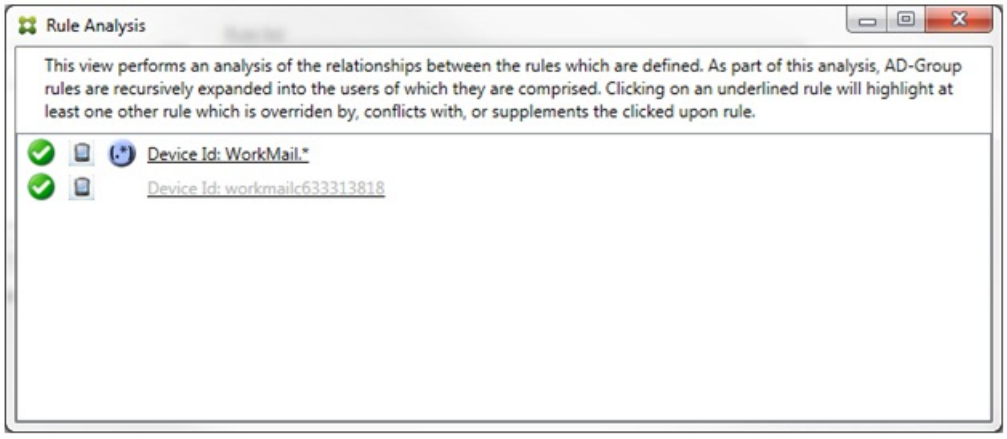
- **Ancillary rule** (Regla auxiliar). Una regla auxiliar está relacionada con la regla primaria, ya sea por invalidación, por conflicto o por reglas adicionales. Las reglas se indican visualmente con un borde discontinuo que las rodea. Puede haber entre una y varias reglas auxiliares por cada regla primaria. Al hacer clic en una entrada subrayada, las reglas auxiliares marcadas siempre se marcan con respecto a la regla primaria. Por ejemplo: la regla primaria invalidará la regla auxiliar, y/o la regla auxiliar entrará en conflicto en el acceso con la regla primaria, y/o la regla auxiliar complementará la regla primaria.

Aspecto de los tipos de reglas en el cuadro del análisis de reglas

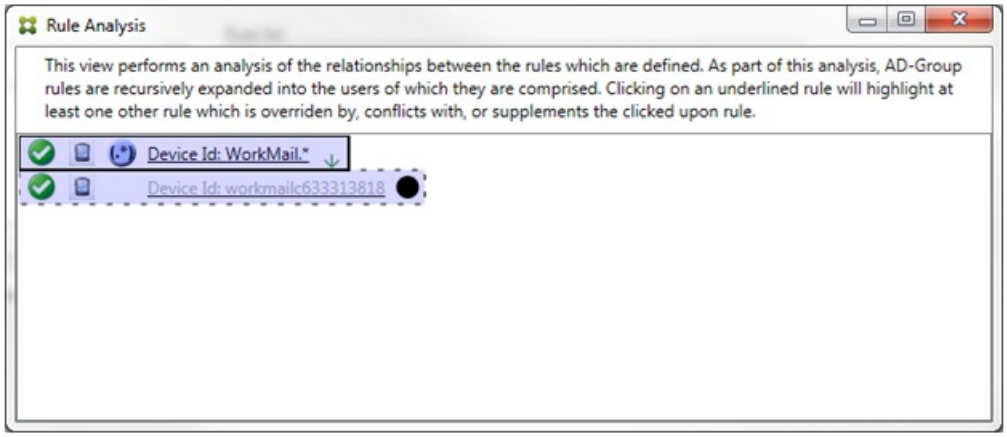
Cuando no haya conflictos, invalidaciones o complementaciones, el cuadro del análisis de reglas no contendrá entradas subrayadas. Hacer clic en alguno de los elementos no tiene ningún efecto: solo se habrá seleccionado el elemento de la manera habitual.



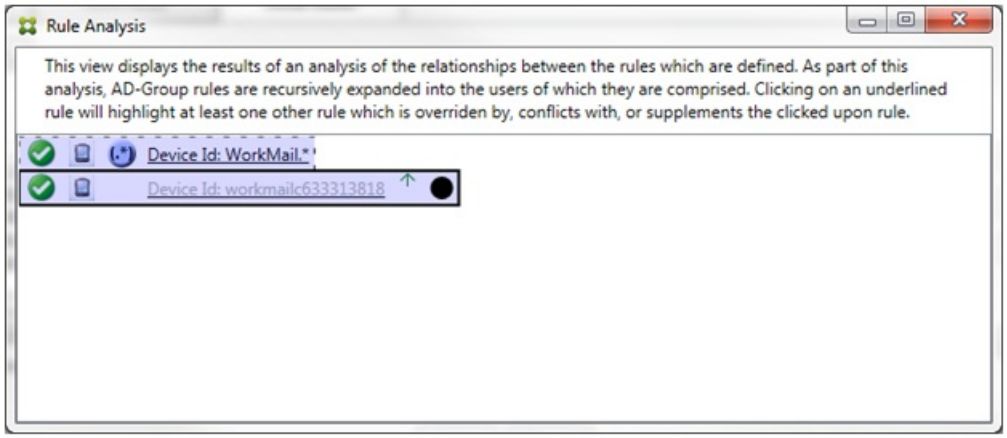
Cuando se produzca una invalidación, se subrayarán al menos dos reglas: la primaria y la(s) auxiliar(es). Al menos una regla auxiliar aparecerá con una fuente más atenuada para indicar que se ha reemplazado por otra regla de mayor prioridad. Puede hacer clic en la regla invalidada para averiguar qué regla o reglas la han invalidado. Cada vez que se marque una regla como invalidada, ya sea porque es la primaria o porque es la auxiliar, aparecerá un círculo negro junto a ella, a modo de indicación más visual de que la regla está inactiva. Por ejemplo, antes de hacer clic en la regla, el cuadro aparecerá de la siguiente manera:



Cuando haga clic en la regla de mayor prioridad, el cuadro aparecerá de la siguiente manera:

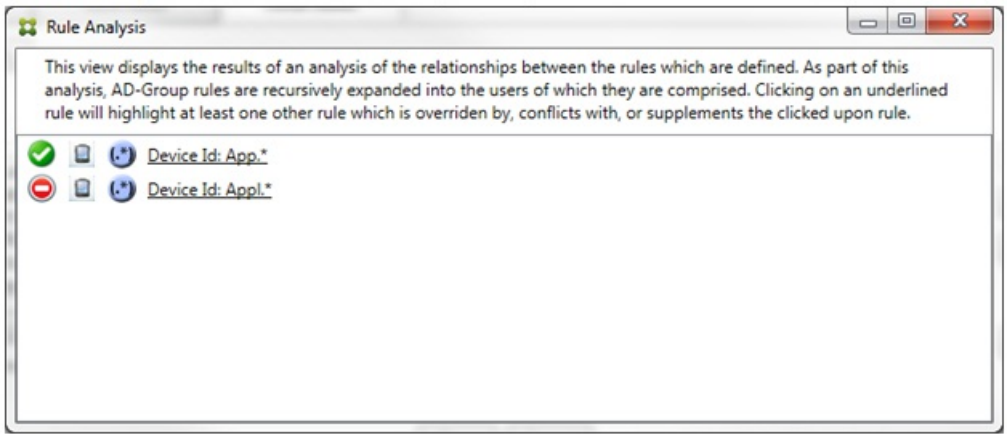


En este ejemplo, la regla de expresión regular WorkMail.* es la regla primaria (indicada con el borde sólido) y la regla normal workmailc633313818 es una regla auxiliar (indicada con el borde discontinuo). El punto negro junto a la regla auxiliar es una indicación visual de que la regla está inactiva (nunca se cotejará) debido a la regla de expresión regular de mayor prioridad que la precede. Después de hacer clic en la regla invalidada, el cuadro aparecerá de la siguiente manera:

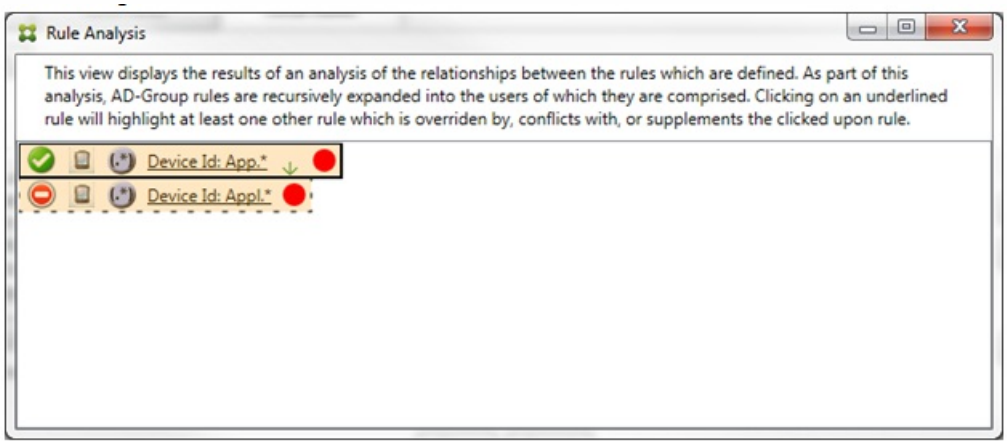


En el ejemplo anterior, la regla de expresión regular WorkMail.* es la regla auxiliar (indicada con el borde discontinuo) y la regla normal workmailc633313818 es la regla primaria (indicada con el borde sólido). En este sencillo ejemplo, no hay mucha diferencia. Para un ejemplo más complejo, consulte el ejemplo de expresión compleja más adelante en este apartado. En un entorno con varias reglas definidas, hacer clic en la regla invalidada identificaría rápidamente las reglas que la han invalidado.

Cuando se produzca un conflicto, se subrayarán al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas en conflicto se indican con un punto de color rojo. Aquellas reglas que solo entren en conflicto una con otra solo se dan cuando hay dos o más reglas de expresión regular definidas. En todos los demás casos de conflictos, no solo hay un conflicto, sino también una invalidación. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparecerá de la siguiente manera:

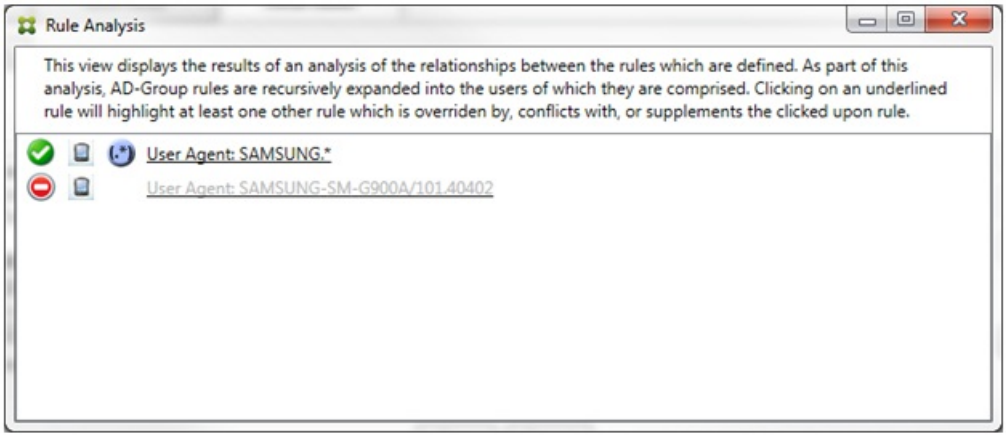


Tras examinar las dos reglas de expresiones regulares, es evidente que la primera regla permite el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "App" y la segunda regla niega el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "Appl". Además, aunque la segunda regla rechaza todos los dispositivos con un ID de dispositivo que contenga "Appl", no se negará el acceso a ningún dispositivo que se corresponda con ese criterio por la prioridad más alta de la regla que permite el acceso. Después de hacer clic en la primera regla, el cuadro aparecerá de la siguiente manera:



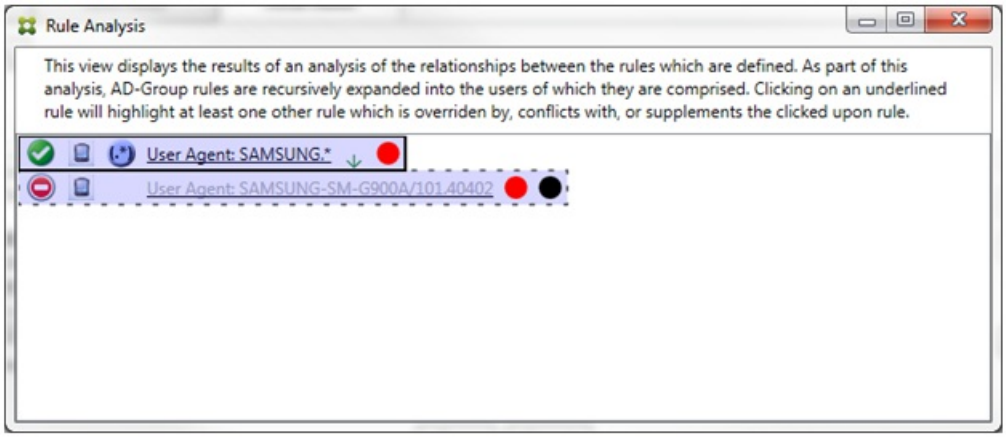
En este caso, tanto la regla primaria (la regla de expresión regular App.*) como la regla auxiliar (la regla de expresión regular Appl.*) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.

En un caso de conflicto e invalidación, la regla primaria (regla de expresión regular App.*) y la regla auxiliar (regla de expresión regular Appl.*) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.



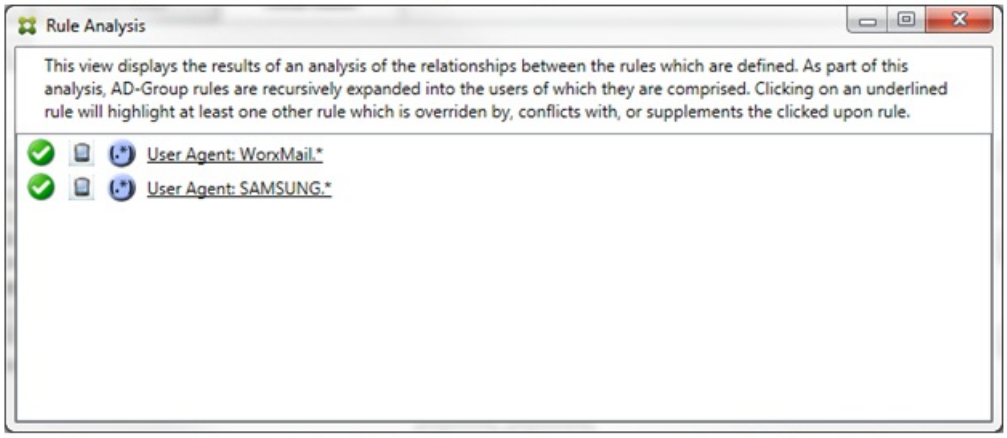
En el ejemplo anterior, es fácil observar que la primera regla (regla de expresión regular SAMSUNG.*) no solo invalida la siguiente regla (regla normal SAMSUNG-SM-G900A/101.40402), sino que las dos reglas se diferencian en su acceso (la primaria especifica Permitir, mientras que la auxiliar especifica Bloquear). La segunda regla (regla normal SAMSUNG-SM-G900A/101.40402) aparece con un texto más atenuada para indicar que se ha invalidado y está, por lo tanto, inactiva.

Después de hacer clic en la regla de expresión regular, el cuadro aparecerá de la siguiente manera:

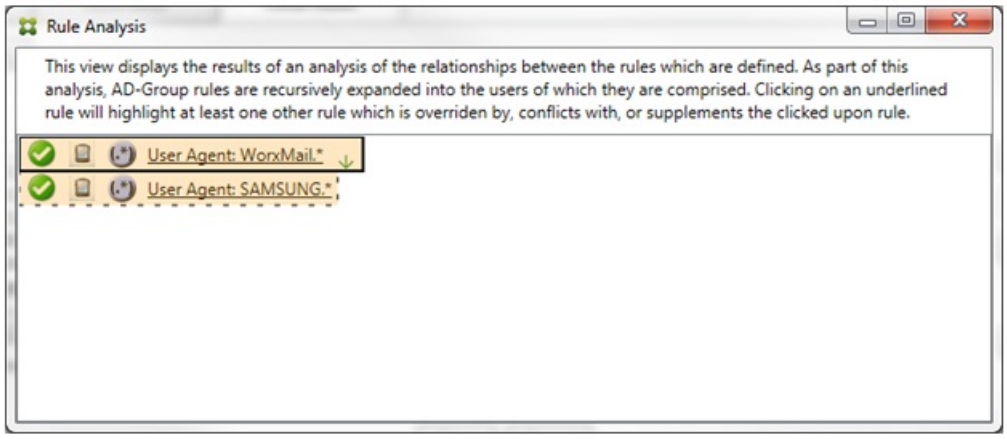


La regla primaria (regla de expresión regular SAMSUNG.*) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal SAMSUNG-SM-G900A/101.40402) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con la regla primaria. También va seguida de un punto negro para indicar que se ha invalidado y está inactiva.

Se subrayan al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas que solo se complementan entre ellas solo pueden ser reglas de expresión regular. Cuando las reglas se complementan entre ellas, se indican con una capa de color amarillo. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparecerá de la siguiente manera:



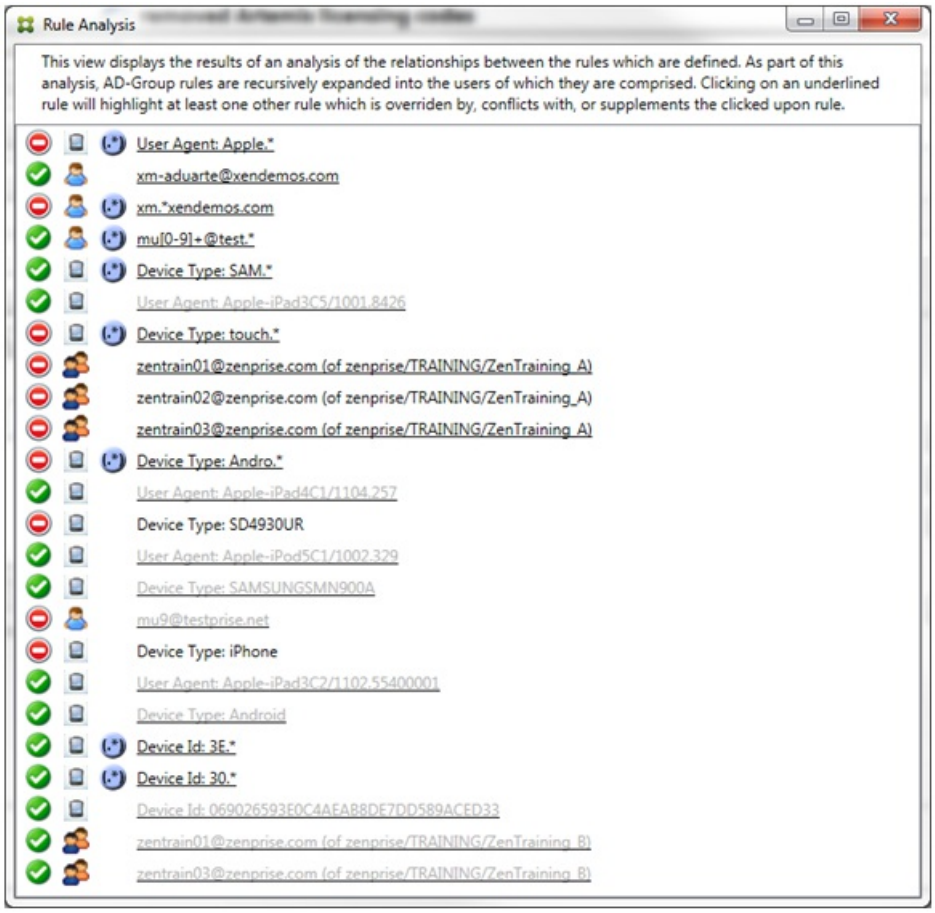
Tras echar un vistazo, es evidente que ambas reglas son de expresión regular y que se han aplicado al campo de ID de dispositivo ActiveSync en XenMobile Mail Manager. Después de hacer clic en la primera regla, el cuadro aparecerá de la siguiente manera:



La regla primaria (regla de expresión regular WorxMail.*) está resaltada con una capa amarilla para indicar que hay al menos una regla auxiliar adicional que es una expresión regular. La regla auxiliar (regla de expresión regular SAMSUNG.*) está resaltada en amarillo para indicar que ella y la regla primaria son reglas de expresión regular que se aplican al mismo campo en XenMobile Mail Manager; en este caso, el campo de ID de dispositivo ActiveSync. Las expresiones regulares pueden o no pueden superponerse. Le corresponde a usted decidir si sus expresiones regulares se han elaborado correctamente.

Ejemplo de una expresión compleja

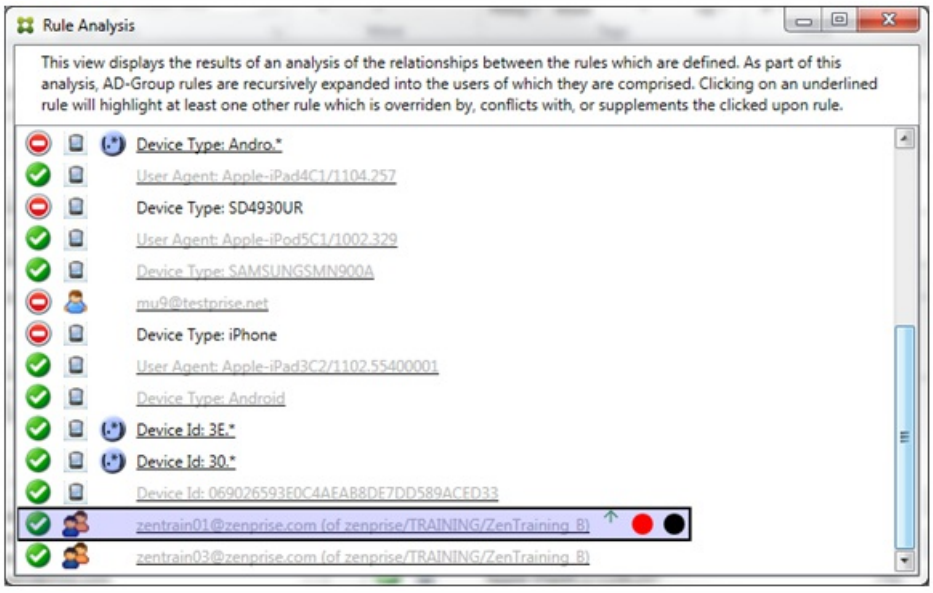
Se pueden producir tantos conflictos, invalidaciones o complementaciones que no se puede ofrecer un ejemplo para todos los casos posibles. En el siguiente ejemplo, se describe lo que no se recomienda hacer y también se ilustra el verdadero potencial de la construcción visual del análisis de reglas. En la siguiente imagen, la mayoría de los elementos están subrayados. Muchos de los elementos se representan con una fuente más atenuada que otras, lo que indica que la regla en cuestión se ha invalidado por una regla de mayor prioridad. También se han incluido en la lista reglas de expresión regular, indicadas con el icono (.*).



Cómo analizar una invalidación

Para ver qué regla o reglas han invalidado una regla determinada, haga clic en la regla.

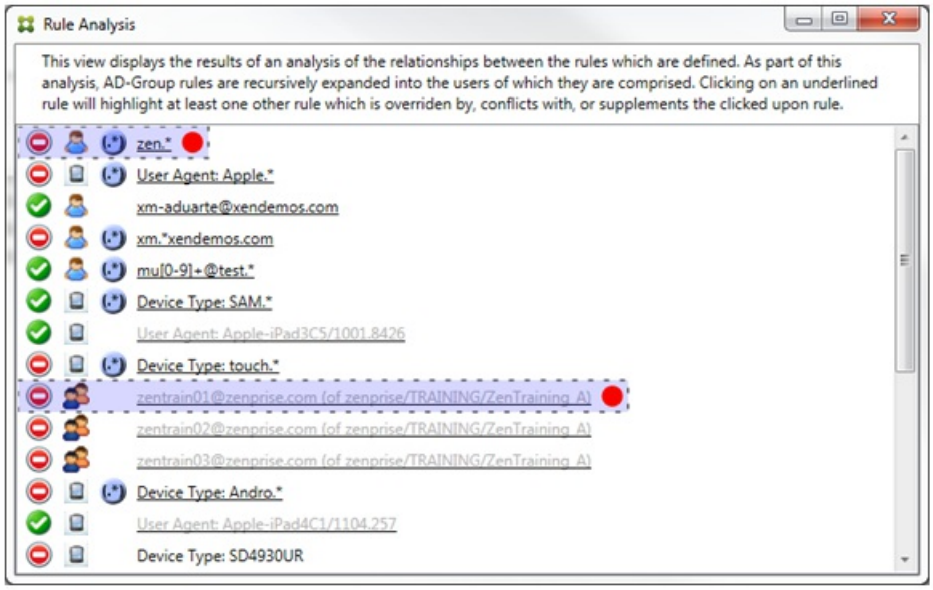
Ejemplo 1. En este ejemplo, se examina por qué zentrain01@zenprise.com se ha invalidado.



La regla primaria (regla del grupo de AD zenprise/TRAINING/ZenTraining B, de la que zentrain01@zenprise.com es miembro) tiene las siguientes características:

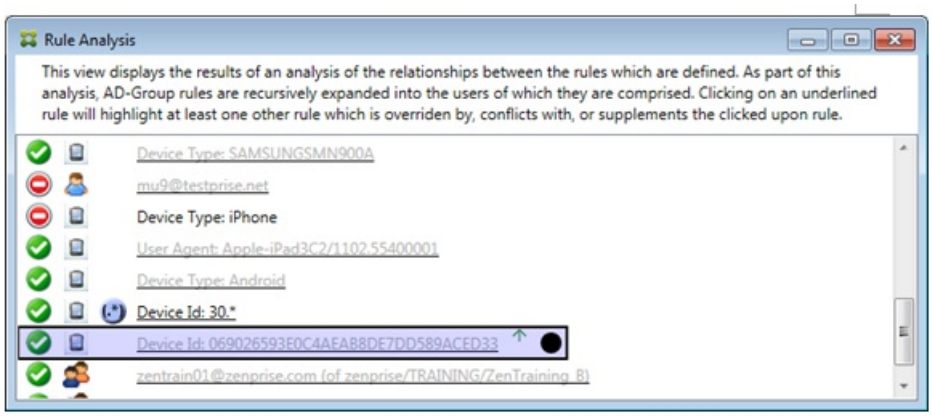
- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que las reglas auxiliares están todas encima de ella).
- Va seguida de un círculo rojo y uno negro para indicar, respectivamente, que una o más reglas están en conflicto con el acceso y que la regla primaria se ha invalidado y, por lo tanto, está inactiva.

Si se desplaza hacia arriba, verá lo siguiente:



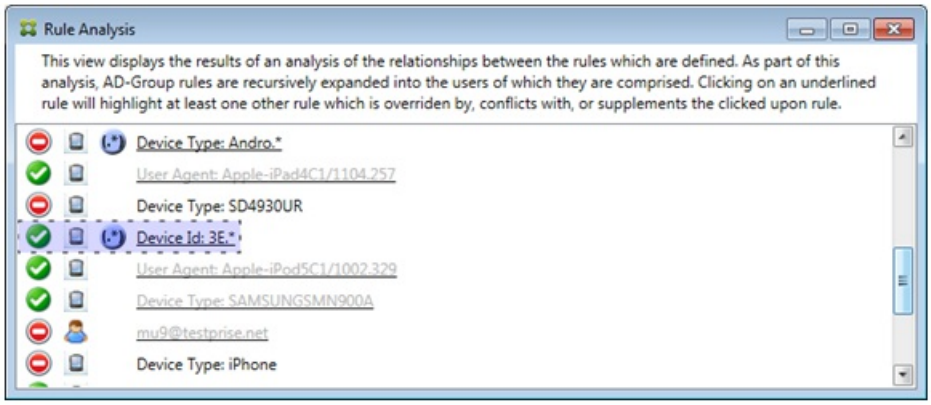
En este caso, hay dos reglas auxiliares que invalidan la regla primaria: la regla de expresión regular zen.* y la regla normal zentrain01@zenprise.com (de zenprise/TRAINING/ZenTraining A). En el caso de la última regla auxiliar, lo que ha ocurrido es que la regla del grupo de Active Directory ZenTraining A contiene el usuario zentrain01@zenprise.com y la regla del grupo de Active Directory de ZenTraining B también contiene el usuario zentrain01@zenprise.com. La regla auxiliar, por tener una prioridad mayor, ha invalidado la regla primaria. El acceso de la regla primaria es Permitir y, como el acceso de ambas reglas auxiliares es Bloquear, todas van seguidas de un círculo rojo para indicar un conflicto de acceso.

Ejemplo 2. En este ejemplo, se muestra por qué se ha invalidado el dispositivo con el ID de dispositivo ActiveSync 069026593E0C4AEAB8DE7DD589ACED33:



La regla primaria (regla normal de ID de dispositivo 069026593E0C4AEAB8DE7DD589ACED33) tiene las siguientes características:

- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que la regla auxiliar está encima de ella).
- Va seguida de un círculo negro para indicar que una regla auxiliar ha invalidado la primaria y, por lo tanto, está inactiva.



En este caso, una sola regla auxiliar invalida la regla primaria: la regla de ID de dispositivo ActiveSync de expresión regular 3E.*. Como la expresión regular 3E.* se correspondería con 069026593E0C4AEAB8DE7DD589ACED33, la regla primaria no se cotejará nunca.

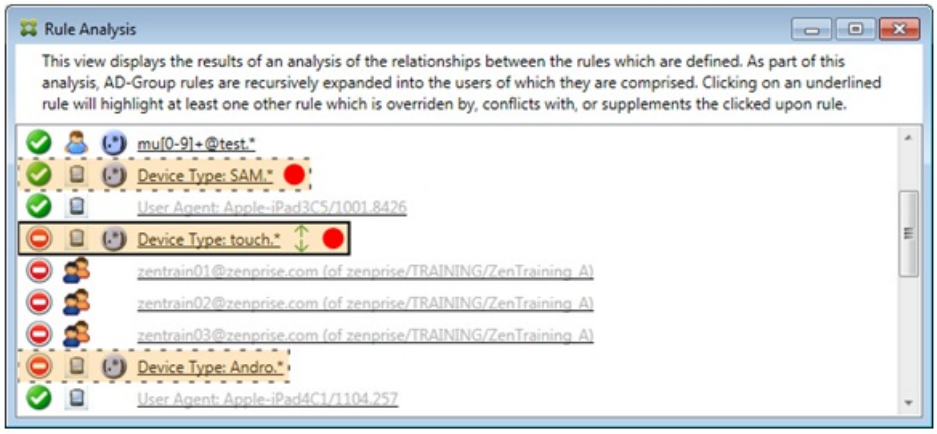
Cómo analizar una complementación y un conflicto

En este caso, la regla primaria es regla de tipo de dispositivo ActiveSync de expresión regular touch.*. Las características son las siguientes:

- Está indicada con un borde sólido y una capa amarilla a modo de advertencia de que hay más de una regla de expresión regular y solo un campo de regla concreto (en este caso: tipo de dispositivo ActiveSync).
- Una flecha que apunta hacia arriba y otra que apunta hacia abajo, lo que indica que hay al menos una regla auxiliar con mayor prioridad y al menos una regla auxiliar con menor prioridad.
- El círculo rojo situado junto a ella indica que hay al menos una regla auxiliar con el acceso establecido en Permitir, lo que está en conflicto con la regla primaria, cuyo acceso es Bloquear.
- Hay dos reglas auxiliares: la regla de tipo de dispositivo ActiveSync de expresión regular SAM.* y la regla de tipo de

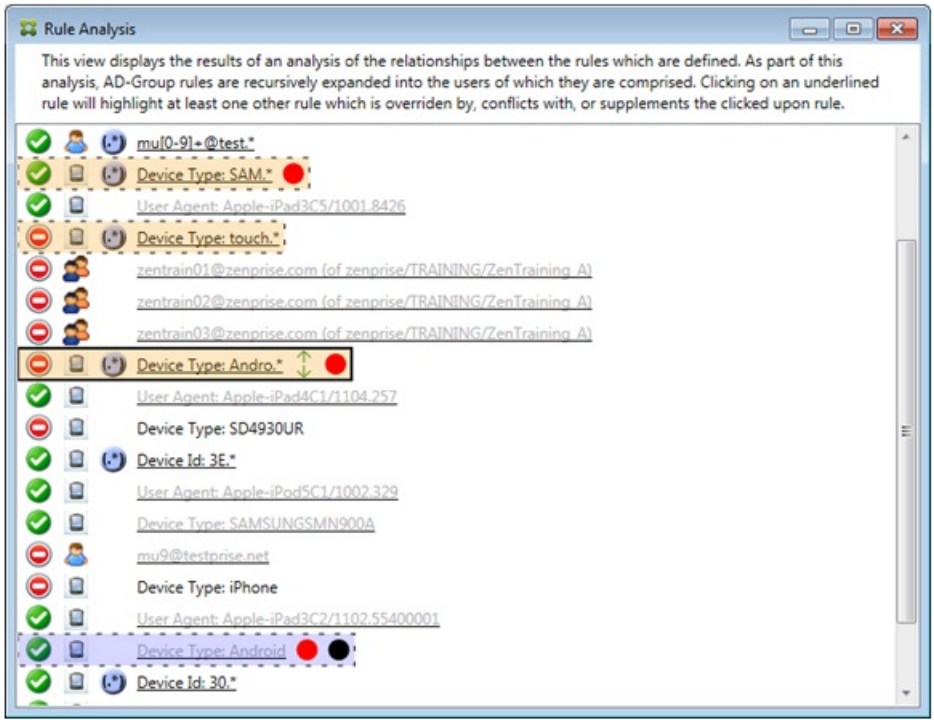
dispositivo ActiveSync de expresión regular Andro.*.

- Ambas reglas tienen bordes discontinuos para indicar que son auxiliares.
- Ambas reglas auxiliares tienen una capa amarilla para indicar que se aplican de forma complementaria al campo de regla de tipo de dispositivo ActiveSync.
- Debe comprobar, en estos casos, que las reglas de expresión regular no sean redundantes.



Cómo analizar las reglas al detalle

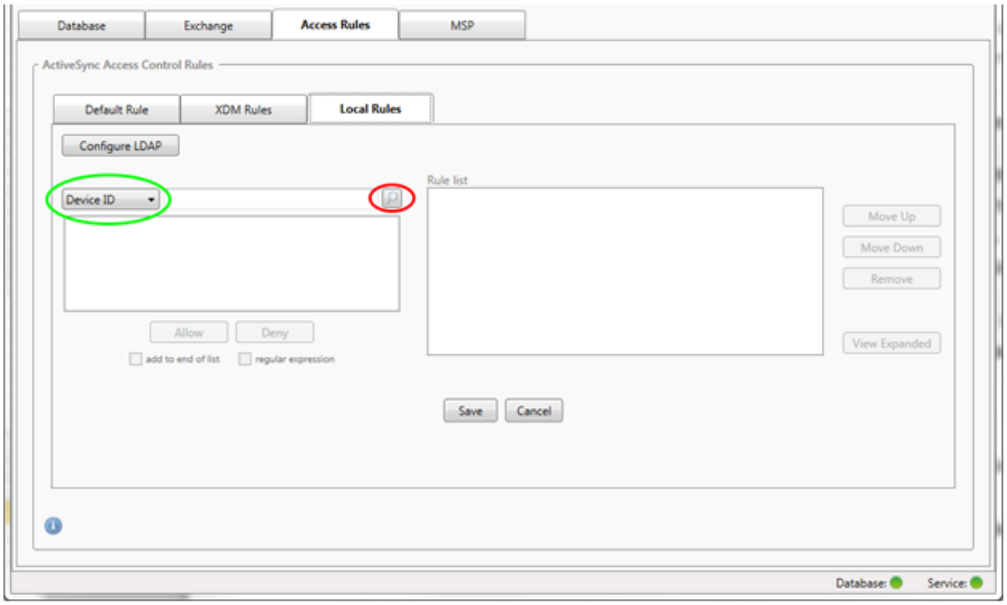
En este ejemplo, se describe cómo las relaciones entre reglas se dan siempre con respecto a la regla primaria. En el ejemplo anterior, se ha mostrado cómo un clic en la regla de expresión regular se aplicaba al campo de regla de tipo de dispositivo con el valor touch.*. Al hacer clic en la regla auxiliar Andro.*, se muestra un conjunto diferente de reglas auxiliares resaltadas.



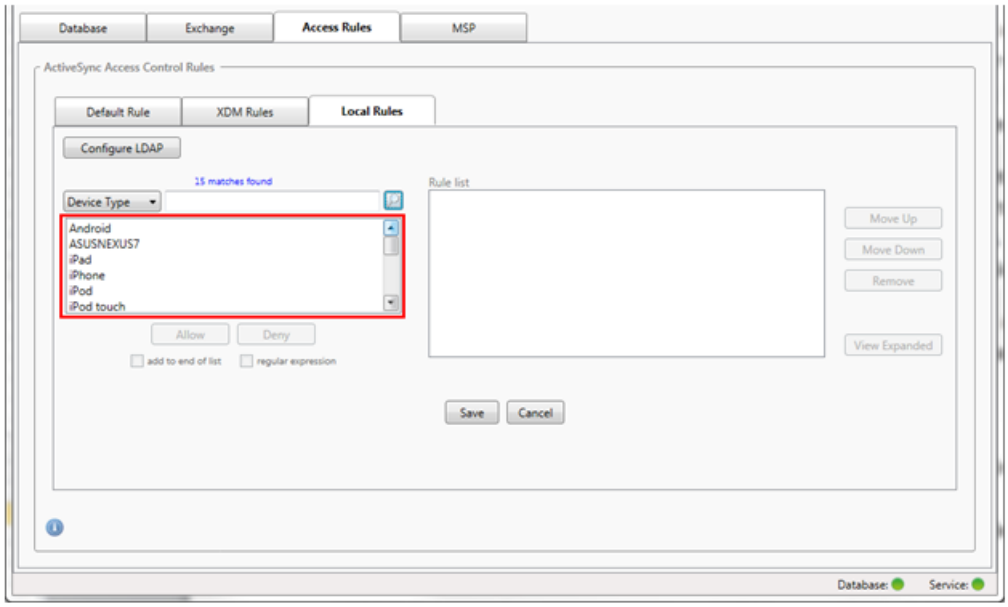
El ejemplo muestra una regla invalidada que se incluye en la relación de las reglas. Esta regla es la regla normal de tipo de dispositivo ActiveSync Android, que se ha invalidado (situación indicada con la fuente más atenuada y el círculo negro junto a ella) y también está en conflicto con el acceso de la regla primaria de tipo de dispositivo ActiveSync de expresión regular Andro.*; esa regla era anteriormente una regla auxiliar antes de que se hiciera clic en ella. En el ejemplo anterior, la regla normal de tipo de dispositivo ActiveSync Android no aparecía como una regla auxiliar porque, con respecto a la entonces regla primaria (la regla de tipo de dispositivo ActiveSync de expresión regular touch.*), no estaba relacionada con ella.

Para configurar una regla local de expresión normal

1. Haga clic en la ficha Access Rules.



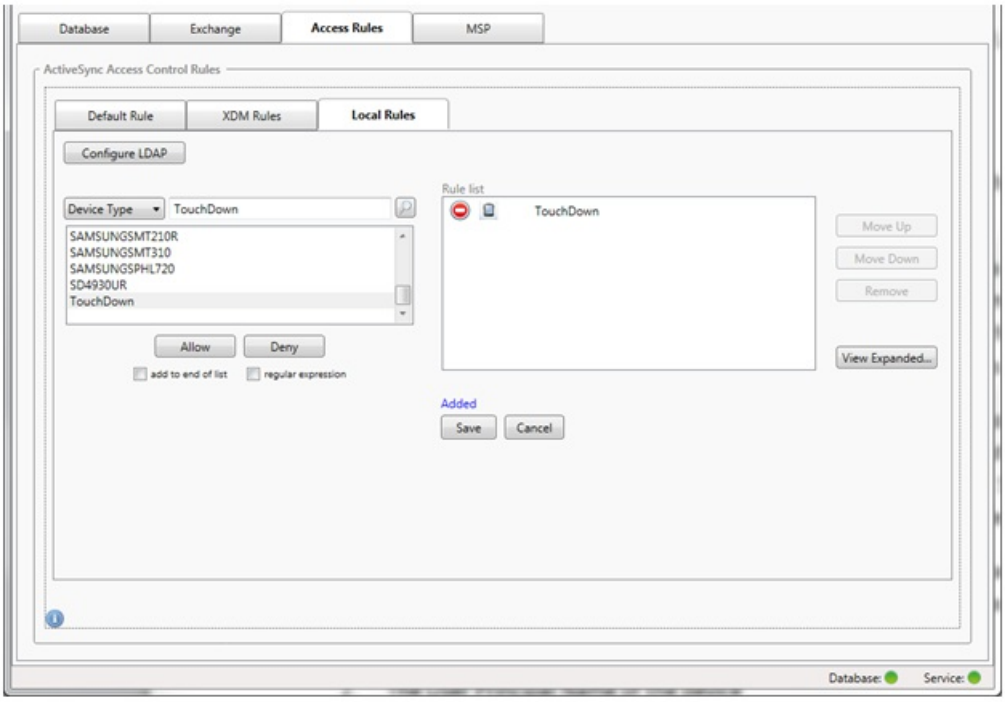
2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, en el cuadro de lista.



4. Haga clic en uno de los elementos de la lista de resultados y, a continuación, haga clic en una de las siguientes opciones:

- Allow significa que Exchange se configurará para permitir el tráfico de ActiveSync en todos los dispositivos que se correspondan.
- Deny significa que Exchange se configurará para denegar el tráfico de ActiveSync en todos los dispositivos que se correspondan.

En este ejemplo, se ha denegado el acceso a todos los dispositivos que tienen un tipo de dispositivo TouchDown.

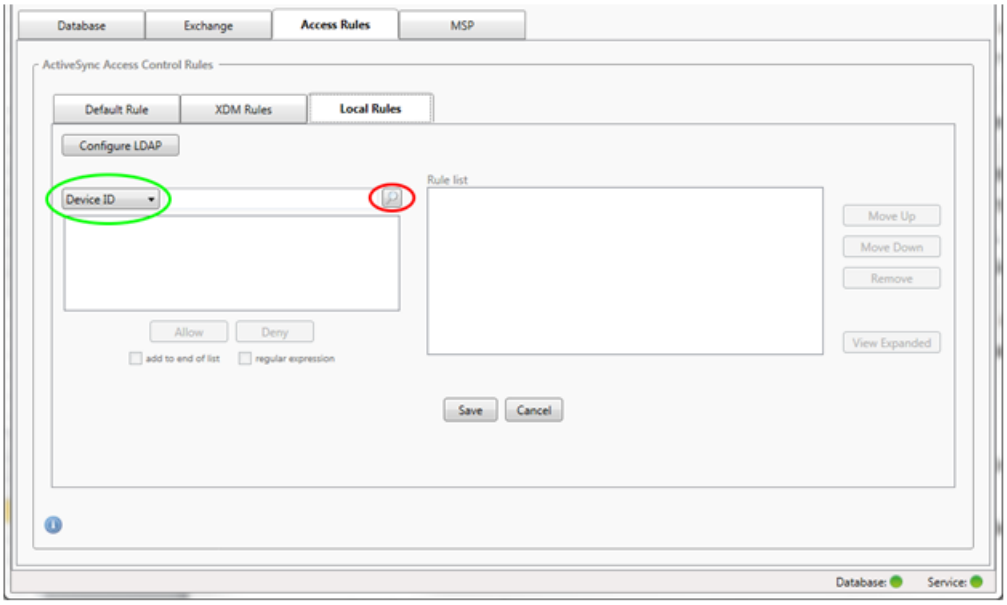


Para agregar una expresión regular

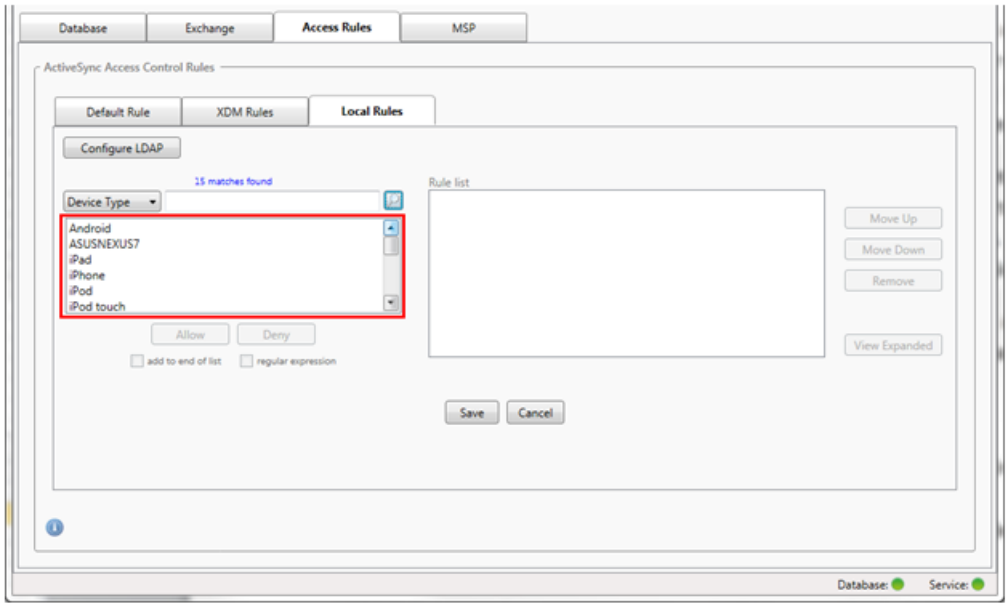
Las reglas locales de expresión regular se distinguen por el icono (.*) que aparece junto a ellas. Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados de un campo determinado (siempre que se haya completado una instantánea principal), o bien puede, simplemente, escribir la expresión regular que quiera.

Para crear una expresión regular a partir de un valor de campo existente

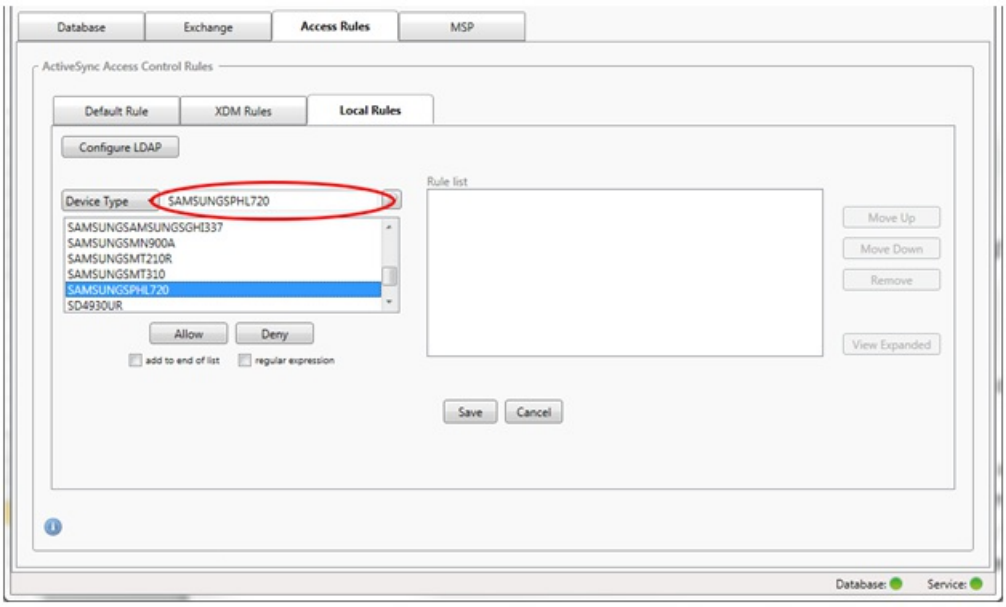
1. Haga clic en la ficha Access Rules.



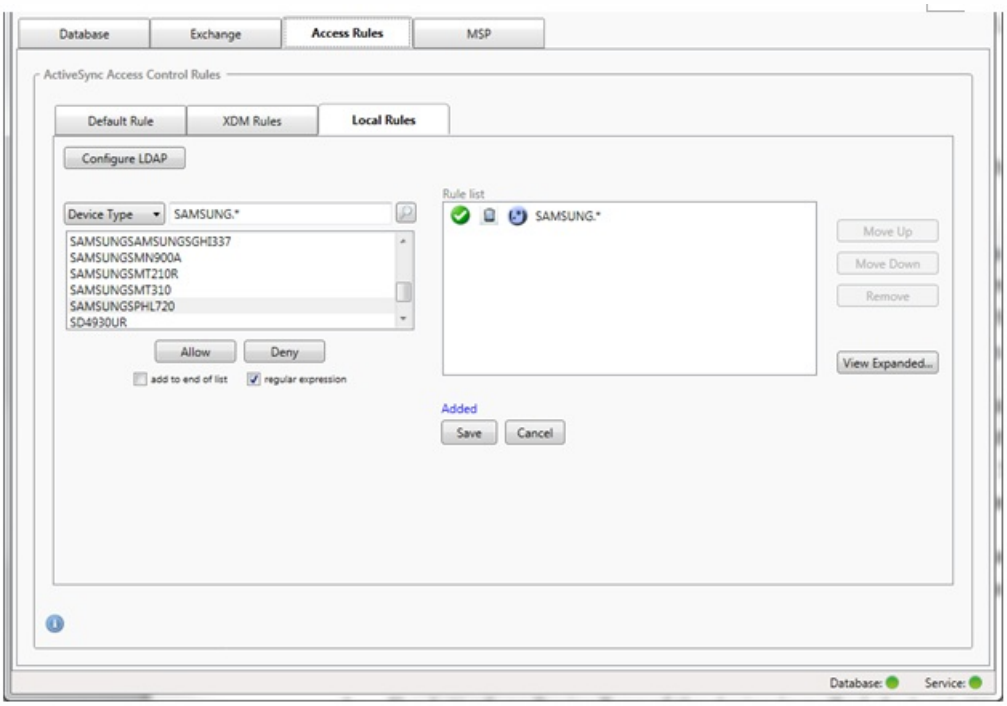
2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local de expresión regular.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, en el cuadro de lista.



4. Haga clic en uno de los elementos de la lista de resultados. En este ejemplo, se ha seleccionado SAMSUNGSPHL720 y aparece en el cuadro de texto adyacente a Device Type.

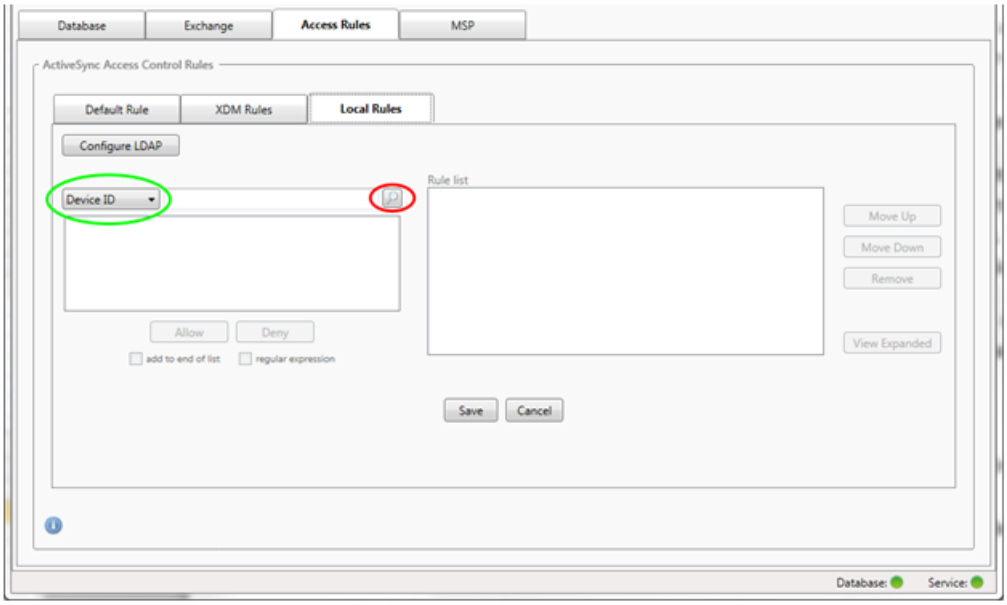


5. Para permitir el acceso a todos los tipos de dispositivos que contengan "Samsung" en su valor de tipo de dispositivo, siga estos pasos para agregar una regla de expresión regular:
   1. Haga clic en el cuadro de texto del elemento seleccionado.
   2. Cambie el texto de SAMSUNGSPHL720 a SAMSUNG.*
   3. Compruebe que la casilla de verificación regular expression está marcada.
   4. Haga clic en Allow.

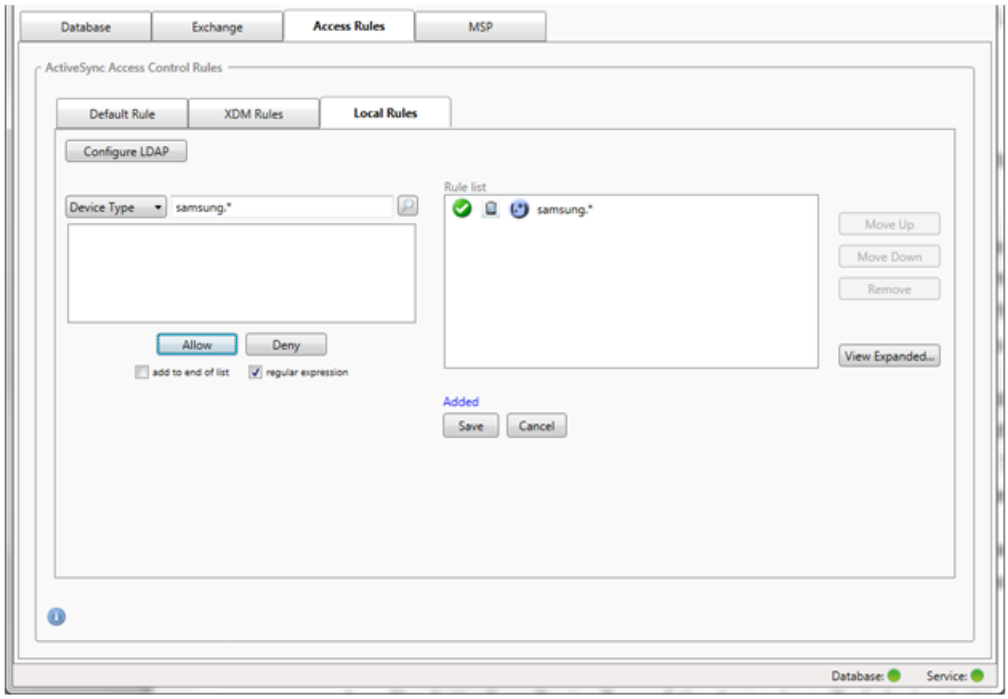


Para crear una regla de acceso

1. Haga clic en la ficha Local Rules.
2. Para escribir la expresión regular, deberá usar la lista Device ID y el cuadro de texto del elemento seleccionado.



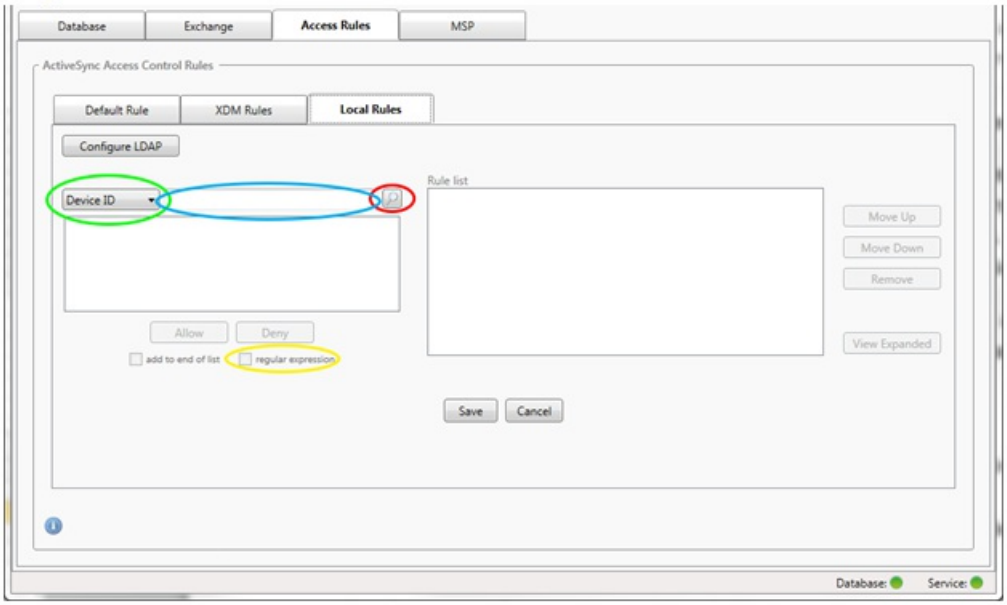
3. Seleccione el campo con el que corresponderse. En este ejemplo, se utiliza Device Type.
4. Escriba la expresión regular. En este ejemplo se usasamsung.*
5. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en Allow o Deny. En este ejemplo, la opción es Allow para que el resultado final sea el siguiente:



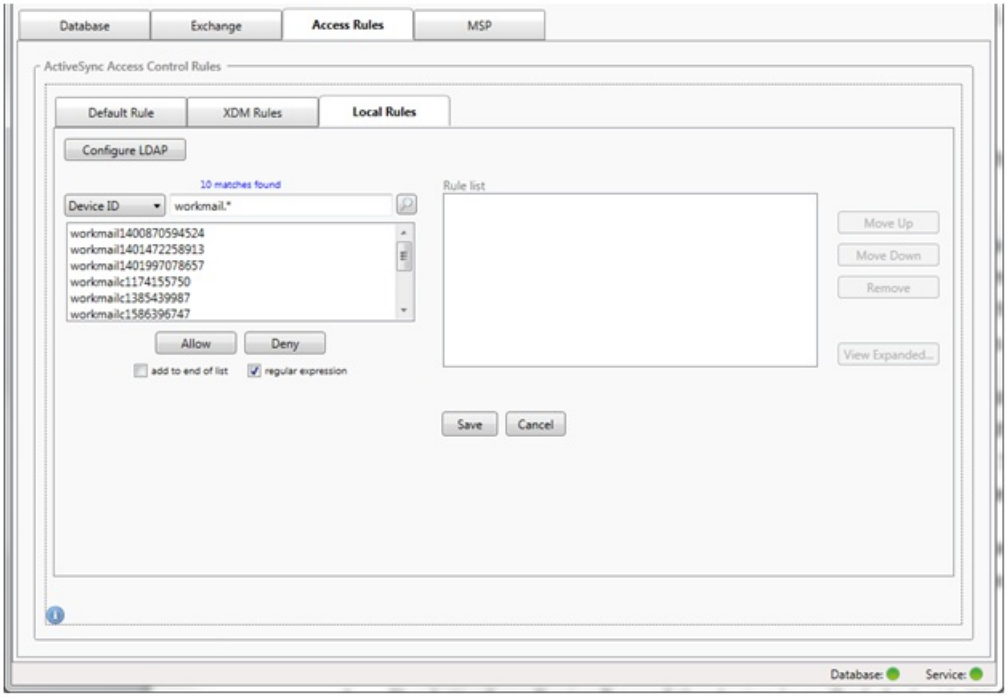
Para buscar dispositivos

Al marcar la casilla "regular expression", puede realizar búsquedas de dispositivos específicos que se corresponden con la expresión indicada. Esta función solo está disponible si una instantánea principal se ha completado correctamente. Puede usar esta función incluso si no planea utilizar reglas de expresión regular. Por ejemplo, supongamos que quiere buscar todos los dispositivos que contienen el texto "workmail" en el ID de sus dispositivos ActiveSync. Para ello, siga este procedimiento.

1. Haga clic en la ficha Access Rules.
2. Compruebe que el selector del campo de correspondencia del dispositivo es Device ID (opción predeterminada).



3. Haga clic en el cuadro de texto del elemento seleccionado (como se muestra en azul en la imagen anterior) y escribaworkmail.*.
4. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en el icono de lupa para ver los resultados, tal y como se muestra en la siguiente imagen.

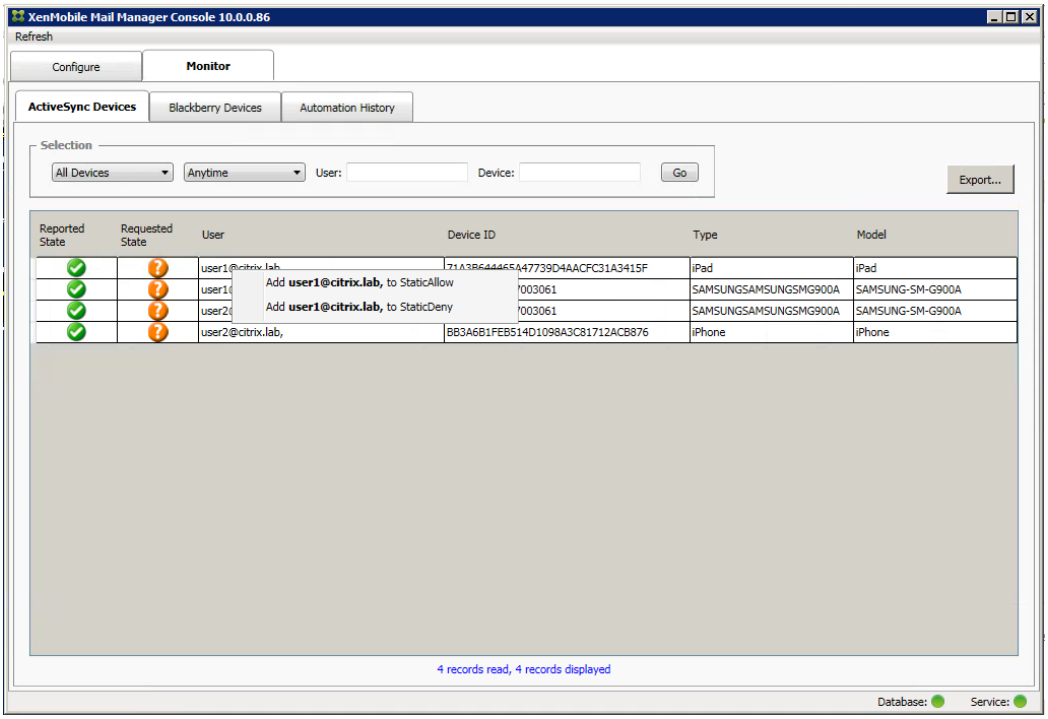


Para agregar un usuario individual, un dispositivo o un tipo de dispositivo a una regla

Puede agregar reglas estáticas basadas en el usuario, el ID de dispositivo o el tipo de dispositivo en la ficha ActiveSync Devices.

1. Haga clic en la ficha ActiveSync Devices.

2. En la lista, haga clic con el botón secundario en un usuario, un dispositivo o un tipo de dispositivo, y seleccione si permitir o denegar la selección.
   En la imagen siguiente, se muestra la opción de permitir o denegar cuando el usuario1 está seleccionado.



Supervisión de dispositivos

May 05, 2016

En XenMobile Mail Manager, la ficha Monitor permite explorar los dispositivos Exchange ActiveSync y BlackBerry que se hayan detectado y el historial de los comandos de PowerShell automatizados que se han emitido. La ficha Monitor contiene a su vez las siguientes tres fichas:

- ActiveSync Devices:
  - Para exportar las asociaciones de dispositivo ActiveSync mostradas, haga clic en el botón Export.
  - Para agregar reglas locales (estáticas), haga clic con el botón secundario en las columnas User, Device ID o Type y seleccione el tipo de regla apropiado, ya sea permitir o bloquear.
  - Para contraer una fila expandida, presione Ctrl y haga clic en la fila expandida.
- Dispositivos BlackBerry
- Historial de automatización

En la ficha Configure se muestra el historial de todas las instantáneas. La información que muestra el historial de instantáneas es: cuándo se realizó la instantánea, cuánto tiempo duró el proceso, cuántos dispositivos se detectaron y los errores que se produjeran.

- En la ficha Exchange, haga clic en el icono de información del servidor Exchange pertinente.
- En la ficha MSP, haga clic en el icono de información del servidor BlackBerry pertinente.

Solución de problemas y diagnósticos

May 05, 2016

XenMobile Mail Manager registra errores y demás información operativa en el archivo de registro: \log\XmmWindowsService.log. Asimismo, XenMobile Mail Manager registra sucesos significativos en el registro de eventos de Windows.

En la lista siguiente, se incluyen errores frecuentes:

El servicio de XenMobile Mail Manager no se inicia

Compruebe si se han registrado errores en el archivo de registro y el registro de eventos de Windows. Las causas habituales son las siguientes:

- El servicio de XenMobile Mail Manager no puede acceder al servidor SQL Server. Esto puede deberse a los siguientes problemas:
  - El servicio SQL Server no se está ejecutando.
  - Error de autenticación.

  Si la autenticación integrada de Windows está configurada, la cuenta de usuario del servicio de XenMobile Mail Manager debe tener permitido el inicio de sesión en SQL Server. La cuenta del servicio de XenMobile Mail Manager es, de forma predeterminada, el sistema local, pero se puede cambiar a una cuenta que tenga privilegios de administrador local. Si se configura la autenticación de SQL, el inicio de sesión de SQL debe estar correctamente configurado en SQL.

- El puerto configurado para el proveedor de servicios móviles (MSP) no está disponible. Se debe seleccionar un puerto de escucha que no utilice ningún otro proceso en el sistema.

XenMobile no puede conectarse a MSP

Compruebe que el puerto y el transporte del servicio de MSP están correctamente configurados en la ficha Configure > MSP de la consola de XenMobile Mail Manager. Compruebe que el usuario o el grupo de autorización están configurados correctamente.
Si se configura HTTPS, se debe instalar un certificado SSL de servidor válido. Si IIS está instalado, se puede utilizar IIS Manager para instalar el certificado. Si IIS no está instalado, consulte http://msdn.microsoft.com/en-us/library/ms733791.aspx para obtener más información acerca de la instalación de certificados.

XenMobile Mail Manager contiene un programa para probar la conectividad al servicio de MSP. Ejecute el programa MspTestServiceClient.exe, y establezca la URL y las credenciales en una URL y con unas credenciales que se configurarán en XenMobile. A continuación, haga clic en Test Connectivity. Así, se simulan las solicitudes del servicio Web que el servicio de XenMobile emite. Tenga en cuenta que si se ha configurado HTTPS, se debe especificar el nombre actual del host del servidor (el nombre especificado en el certificado SSL).

Nota: Cuando use **Test Connectivity**, asegúrese de tener al menos una entrada de registro de ActiveSyncDevice. De lo contrario, la prueba podría fallar.

XenMobile NetScaler Connector

Oct 31, 2016

XenMobile NetScaler Connector es una solución que controla el acceso, desde dispositivos móviles, al correo electrónico, al calendario y a los contactos de la empresa. XenMobile NetScaler Connector permite a los clientes enviar una lista de dispositivos que cumplen los requisitos desde XenMobile a NetScaler, que a su vez controla a qué dispositivos móviles se permite sincronizar con el servidor Exchange de la empresa.

XenMobile proporciona una protección completa para aplicaciones móviles, red y datos. Asimismo, garantiza la seguridad y el cumplimiento de extremo a extremo. NetScaler optimiza, protege y controla la entrega de todos los servicios empresariales y de nube. Juntos, estos dos productos Citrix ofrecen la posibilidad de ampliar implementaciones, garantizar una alta disponibilidad de aplicaciones y mantener la seguridad, al tiempo que reducen los costes de implementación y administración de entornos móviles.

XenMobile NetScaler Connector ofrece un servicio de autorización a NetScaler en el nivel de dispositivos de los clientes ActiveSync, por lo que actúa como proxy inverso para el protocolo de Exchange ActiveSync. La autorización se controla mediante una combinación de directivas que se definen en XenMobile y unas reglas definidas localmente por XenMobile NetScaler Connector.

Con XenMobile se pueden crear unas directivas de aplicaciones permitidas y prohibidas para los dispositivos, basándose en el cumplimiento de unas directivas de alto nivel, como por ejemplo, la detección de dispositivos liberados por jailbreak o la detección de aplicaciones específicas. Las reglas locales de XenMobile NetScaler Connector se usan normalmente para aumentar las reglas de XenMobile en aquellos casos en que se requieren reglas especiales que anulen las reglas generales; por ejemplo, si quiere bloquear todos los dispositivos que usen una determinada versión de un sistema operativo.

Las funciones clave de XenMobile NetScaler Connector son:

- **Control de acceso para solicitudes HTTP de ActiveSync**. XenMobile NetScaler Connector puede controlar las solicitudes HTTP de ActiveSync que los dispositivos móviles realizan de servidores de Exchange. Puede crear filtros en XenMobile NetScaler Connector que sirven para permitir o bloquear dispositivos de usuario, en función de las reglas y los criterios especificados. Al configurar reglas en XenMobile NetScaler Connector, puede activar y desactivarlas en XenMobile, y este luego administra la capacidad de los dispositivos para acceder al correo electrónico de la empresa.
- **Configuración remota**. XenMobile controla la línea base de referencia y las diferencias de intervalos que usa XenMobile NetScaler Connector.
- **Captura de registros**. En la ficha **Log** de la herramienta de configuración de XenMobile NetScaler Connector, puede consultar cuándo se habilitó el cifrado de un dispositivo determinado de usuario en el nivel de solicitud, además de consultar los dispositivos que están permitidos o bloqueados.

XenMobile NetScaler Connector ofrece las siguientes funciones:

- **Reglas basadas en filtros para permitir o bloquear el acceso**. XenMobile NetScaler Connector evalúa una solicitud determinada de cliente enrutada a través de NetScaler siguiendo las reglas de la organización. El resultado final es un estado binario *permitido* (al cliente se le permite establecer contacto con el servidor de acceso de cliente (CAS) de Microsoft Exchange 2010) o *bloqueado* (la solicitud de cliente se descarta y el acceso al servidor CAS de Exchange no se permite). En combinación con los parámetros de la consola de XenMobile, puede impedir que ciertos dispositivos de usuario accedan al correo electrónico de Exchange ActiveSync basándose en criterios de conformidad (por ejemplo, si una aplicación prohibida está instalada en el dispositivo o si el dispositivo está liberado por jailbreak).
- **Un modelo de filtro de dos niveles**. El primer nivel analiza las solicitudes HTTP entrantes basadas en información de

ruta específica. El segundo nivel filtra según información específica del dispositivo o del usuario. Puede configurar ambos niveles.

- **Reglas de filtrado almacenadas en archivos de configuración**. Las reglas de filtrado específicas que pertenecen a las cuentas de usuario y dispositivos de la organización se almacenan en los archivos de configuración XML de la puerta de enlace.

Para ver diagramas de referencia de arquitectura en detalle, consulte el artículo Reference Architecture for On-Premises Deployments de XenMobile Deployment Handbook.

Implementación de XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector permite utilizar NetScaler para redirigir mediante proxy y equilibrar la carga de la comunicación entre XenMobile y los dispositivos administrados. XenMobile NetScaler Connector se comunica de forma periódica con XenMobile para sincronizar las directivas. XenMobile NetScaler Connector y XenMobile se pueden agrupar en clústeres (ya sea en un mismo clúster o en clústeres diferentes), y NetScaler puede equilibrar su carga.

Componentes de XenMobile NetScaler Connector

XenMobile NetScaler Connector consta de los siguientes cuatro componentes:

- Servicio de XenMobile NetScaler Connector. Este servicio ofrece una interfaz de servicio Web REST que se puede invocar mediante NetScaler para determinar si se autoriza una solicitud de ActiveSync desde un dispositivo.
- Servicio de configuración de XenMobile. Este servicio se comunica con Device Manager para sincronizar los cambios de las directivas de Device Manager con XenMobile NetScaler Connector.
- Servicio de notificación de XenMobile. Este servicio envía notificaciones a Device Manager acerca de accesos de dispositivos no autorizados, con el objetivo de que Device Manager pueda tomar las medidas adecuadas, como notificar al usuario el motivo para el bloqueo del dispositivo.
- Herramienta de configuración de XenMobile NetScaler. Esta aplicación permite al administrador configurar y supervisar XenMobile NetScaler Connector.

Para configurar direcciones de escucha para XenMobile NetScaler Connector

Para que XenMobile NetScaler Connector pueda recibir solicitudes desde NetScaler y permitir el tráfico de ActiveSync, debe especificar el puerto en el que XenMobile NetScaler Connector escuchará las llamadas de servicio Web de NetScaler.

1. En el menú Inicio, seleccione XenMobile NetScaler configuration utility.
2. Haga clic en la ficha Web Service y, a continuación, escriba las direcciones de escucha para el servicio Web de XenMobile NetScaler Connector. Puede seleccionar HTTP y/o HTTPS. Si XenMobile NetScaler Connector y XenMobile están instalados en el mismo servidor, seleccione puertos que no entren en conflicto con XenMobile.
3. Después de configurar los valores, haga clic en Save y, a continuación, haga clic en Start Service para iniciar el servicio Web.

Para configurar directivas de control de acceso de dispositivo en XenMobile NetScaler Connector

Para configurar la directiva de control de acceso que quiere aplicar a los dispositivos administrados, haga lo siguiente:

1. En la herramienta de configuración de XenMobile NetScaler, haga clic en la ficha Path Filters.
2. Seleccione la primera fila Microsoft-Server-ActiveSync is for ActiveSync y, a continuación, haga clic en Edit.
3. En la lista Policy, seleccione la directiva pertinente. Para una directiva que incluya las directivas de XenMobile, seleccione Static + ZDM: Permit Mode o Static + ZDM: Block Mode. Estas directivas combinan reglas locales (o estáticas) con las reglas de XenMobile. El modo Permit Mode significa que se permite el acceso a ActiveSync por parte de todos los dispositivos no identificados específicamente mediante reglas. En cambio, el modo Block Mode significa que todos esos dispositivos serán bloqueados.
4. Después de establecer las directivas, haga clic en Save.

Para configurar la comunicación con XenMobile

La siguiente tarea le permitirá especificar el nombre y las propiedades del servidor de XenMobile (también llamado Config

Provider) que quiere utilizar con NetScaler y XenMobile NetScaler Connector.

Nota: En esta tarea se presupone que usted ya tiene XenMobile instalado y configurado.

1. En la herramienta de configuración de XenMobile NetScaler Connector, haga clic en la ficha Config Providers y, a continuación, haga clic en Add.
2. Indique el nombre y la dirección URL del servidor XenMobile utilizado en esta implementación. Si dispone de varios servidores XenMobile implementados como parte de una implementación multiarrendatario, este nombre debe ser único para cada instancia de servidor. Por ejemplo, en Name, podría escribirXMS.
3. En Url, introduzca la dirección Web de GlobalConfig Provider (GCP) de XenMobile. Por norma general, en el formato: https://DeviceManagerHost/zdm/services/MagConfigService. El nombre MagConfigService distingue mayúsculas de minúsculas.
4. En Password, introduzca la contraseña que se usará para la autorización básica de HTTP con el servidor Web de XenMobile.
5. En Managing Host, introduzca el nombre del servidor donde se instaló XenMobile NetScaler Connector.
6. En Baseline Interval, especifique un período de tiempo para la extracción, desde XenMobile, de un conjunto de reglas dinámicas actualizadas.
7. En Request Timeout, especifique el intervalo de tiempo de espera para solicitudes del servidor.
8. En Config Provider, seleccione si la instancia de servidor de Config Provider proporciona la configuración de directivas.
9. Habilite la opción Events Enabled si quiere que Secure Mobile Gateway notifique a XenMobile cuando se bloquee un dispositivo. Se requiere esta opción si se utilizan reglas de Secure Mobile Gateway en alguna de las acciones automatizadas de Device Manager.
10. Una vez configurado el servidor, haga clic en Test Connectivity para comprobar la conexión con el servidor XenMobile.
11. Cuando se haya establecido la conectividad, haga clic en Save.

Implementación de XenMobile NetScaler Connector para redundancia y escalabilidad

Si quiere ampliar la implementación de XenMobile NetScaler Connector y XenMobile, puede instalar instancias de XenMobile NetScaler Connector en varios servidores Windows que señalen a la misma instancia de XenMobile y, a continuación, puede utilizar NetScaler para equilibrar la carga de los servidores.

Hay dos modos de configurar XenMobile NetScaler Connector.

- En el modo no compartido (non-shared mode) cada instancia de XenMobile NetScaler Connector se comunica con un servidor XenMobile y mantiene su propia copia privada de la directiva resultante. Por ejemplo, si tiene un clúster de servidores XenMobile, puede ejecutar una instancia de XenMobile NetScaler Connector en cada servidor XenMobile, y XenMobile NetScaler Connector obtendría las directivas desde la instancia local de XenMobile.
- En modo compartido (shared mode), un nodo de XenMobile NetScaler Connector se designa como el nodo principal y se comunica con XenMobile. La configuración resultante se comparte entre los demás nodos, ya sea mediante una replicación de Windows o un recurso compartido de red Windows (o de terceros).

Toda la configuración de XenMobile NetScaler Connector se encuentra en una carpeta (de varios archivos XML). El proceso de XenMobile NetScaler Connector detecta los cambios en los archivos de esta carpeta y vuelve a cargar automáticamente la configuración. No hay ninguna conmutación por error para el nodo principal en el modo compartido. Sin embargo, el sistema puede tolerar que el servidor principal esté inactivo durante unos minutos (por ejemplo, para reiniciarse) porque la última configuración válida conocida se almacena en caché en el proceso de XenMobile NetScaler Connector.

Requisitos del sistema para XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector se comunica con NetScaler a través de un puente SSL configurado en el dispositivo NetScaler que permite al dispositivo enviar todo el tráfico seguro directamente a XenMobile. Puede instalar XenMobile NetScaler Connector en su propio servidor o en el mismo servidor que XenMobile. XenMobile NetScaler Connector requiere la siguiente configuración mínima de sistema:

Componente	Requisito
Equipo y procesador	Pentium III a 733 MHz o un procesador superior. Pentium III a 2,0 GHz o un procesador superior (recomendado)
NetScaler	Dispositivo NetScaler con la versión 10 de software
Memoria	1 gigabyte (GB)
Disco duro	Partición local con formato NTFS, con 150 MB de espacio disponible en disco duro
Sistema operativo	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2 (recomendado)
Otros dispositivos	Un adaptador de red compatible con el sistema operativo del host para la comunicación con la red interna
Mostrar	Monitor VGA o de mayor resolución

El equipo host de XenMobile NetScaler Connector requiere el siguiente espacio mínimo disponible en el disco duro:

- Application. De 10 a 15 MB (se recomienda 100 MB)
- Logging. 1 GB (se recomienda 20 GB)

Instalación de XenMobile NetScaler Connector

May 05, 2016

Puede instalar XenMobile NetScaler Connector en su propio servidor o en el mismo servidor donde se ha instalado XenMobile.

Puede plantearse instalar XenMobile NetScaler Connector en su propio servidor (separado de XenMobile) por los siguientes motivos:

- Si el servidor XenMobile está alojado de forma remota en la nube (ubicación física).
- Si no quiere que XenMobile NetScaler Connector se vea afectado por los reinicios del servidor XenMobile (disponibilidad).
- Si quiere que los recursos del sistema de un servidor se dediquen totalmente a XenMobile NetScaler Connector (rendimiento).

La carga de la CPU que pone XenMobile NetScaler Connector en un servidor depende de la cantidad de dispositivos administrados, aunque una regla general consiste en aprovisionar un núcleo de CPU adicional si XenMobile NetScaler Connector se implementa en el mismo servidor que XenMobile. En caso de una gran cantidad de dispositivos (más de 50000), es posible que necesite aprovisionar más núcleos si no dispone de un entorno de clústeres. La superficie de memoria de XenMobile NetScaler Connector no es lo suficientemente significativa para garantizar una memoria adicional.

Para instalar, actualizar o desinstalar XenMobile NetScaler Connector

May 05, 2016

1. Ejecute XncInstaller.exe con una cuenta de administrador para instalar XenMobile NetScaler Connector (XNC) o para permitir la actualización o la eliminación de un XenMobile NetScaler Connector existente.
2. Siga las instrucciones en pantalla para completar la instalación, la actualización o la desinstalación.

Después de instalar XenMobile NetScaler Connector, debe reiniciar manualmente el servicio de notificación y el servicio de configuración de XenMobile.

Para desinstalar XenMobile NetScaler Connector

May 05, 2016

1. Ejecute XncInstaller.exe con una cuenta de administrador.
2. Siga las instrucciones que aparecen en la pantalla para completar la desinstalación.

Administración de XenMobile NetScaler Connector

May 05, 2016

Puede usar XenMobile NetScaler Connector para generar reglas de control de acceso con el fin de permitir o bloquear el acceso a las solicitudes de conexión de ActiveSync provenientes de dispositivos administrados, basándose en el estado del dispositivo, las aplicaciones permitidas o prohibidas u otras condiciones de cumplimiento.

Con la herramienta de configuración de XenMobile NetScaler Connector, puede generar reglas dinámicas y estáticas que apliquen directivas de correo electrónico de empresa, por lo que podrá bloquear a los usuarios que infrinjan las normas. También puede configurar el cifrado de datos adjuntos de correo electrónico, de modo que todos esos datos que pasen a través del servidor Exchange hacia los dispositivos administrados se cifren y solo se puedan ver en dispositivos administrados por usuarios autorizados.

Elección de un modelo de seguridad para XenMobile NetScaler Connector

May 05, 2016

Modelo permisivo (Permit mode)

Establecer un modelo de seguridad es esencial para una buena implementación de dispositivos móviles en organizaciones de cualquier tamaño. A pesar de que la práctica de utilizar alguna forma de control de red protegida o en cuarentena para permitir el acceso a un usuario, un equipo o un dispositivo de forma predeterminada sea común, no se trata siempre de una buena práctica. Cada organización que administra de seguridad de IT puede tener un enfoque diferente o adaptado a la seguridad de los dispositivos móviles.

La misma lógica se aplica a la seguridad de los dispositivos móviles. La gran cantidad de tipos y de dispositivos móviles en sí, la cantidad de dispositivos móviles por usuario, así como la matriz de aplicaciones y plataformas de sistemas operativos disponibles convierten la sola idea de un modelo permisivo en una mala elección. En la mayoría de las organizaciones, el modelo restrictivo sería la elección más lógica.

Los tipos de configuración que permite Citrix para integrar XenMobile NetScaler Connector con XenMobile son:

El modelo de seguridad permisivo estipula que, de forma predeterminada, se permite o se concede acceso a todo. Solo se bloqueará el acceso a algo y se aplicará una restricción si existen reglas y filtros. El modelo de seguridad permisivo es una buena opción para organizaciones a las que la seguridad de dispositivos móviles preocupa relativamente poco, y la que solo aplica controles restrictivos para denegar el acceso cuando corresponda (cuando una regla de directiva haya fallado).

Modelo restrictivo (Block Mode)

El modelo de seguridad restrictivo estipula que, de forma predeterminada, no se permite o no se concede acceso a nada. Todo lo que pasa por el punto de control de seguridad se filtra y se comprueba; se le deniega el acceso a menos que las reglas de acceso lo permitan. El modelo de seguridad restrictivo es una buena opción para organizaciones con un criterio de seguridad de dispositivos móviles relativamente estricto. Este modo solo concede acceso para uso y funciones con los servicios de red cuando todas las reglas de acceso lo permitan.

Configuración de XenMobile NetScaler Connector

May 05, 2016

Puede configurar XenMobile NetScaler Connector para bloquear o permitir solicitudes de ActiveSync de forma selectiva, en función de las siguientes propiedades: Active Sync Service ID, Device type, User Agent (sistema operativo del dispositivo), Authorized user, y ActiveSync Command.

La configuración predeterminada admite una combinación de grupos estáticos y dinámicos. Debe mantener grupos estáticos mediante la herramienta de configuración del controlador SMG. Los grupos estáticos pueden constar solo de las categorías conocidas de los dispositivos, como, por ejemplo, todos los dispositivos con un agente determinado de usuario.

Los grupos dinámicos se mantienen mediante un recurso externo llamado Gateway Configuration Provider (proveedor de configuración de puerta de enlace). XenMobile NetScaler Connector recopila esos grupos de forma periódica. Con XenMobile puede exportar grupos de dispositivos y usuarios permitidos y bloqueados a XenMobile NetScaler Connector.

Una directiva es una lista ordenada de grupos, donde cada grupo tiene asociada una acción (permitir o bloquear), además de una lista de los miembros del grupo. Una directiva puede tener una cantidad infinita de grupos. El orden de los grupos en una directiva es importante porque, cuando se encuentra una coincidencia, se realiza la acción del grupo, y los demás grupos no se evalúan.

Un miembro define la manera de coincidir con las propiedades de una solicitud. Se puede coincidir con una sola propiedad, como ID de dispositivo, o con varias propiedades, como el tipo de dispositivo y el agente de usuario.

Configuración de los modos de directiva de XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector puede ejecutarse en los siguientes seis modos:

- Allow All. Este modo de directiva concede acceso a todo el tráfico que pasa por XenMobile NetScaler Connector. No se utiliza ninguna otra regla de filtrado.
- Deny All. Este modo de directiva bloquea el acceso a todo el tráfico que pasa por XenMobile NetScaler Connector. No se utiliza ninguna otra regla de filtrado.
- Static Rules: Block Mode. Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de denegar o bloquear al final. XenMobile NetScaler Connector bloquea aquellos dispositivos que otras reglas de filtrado no permitan.
- Static Rules: Permit Mode. Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de permitir al final. XenMobile NetScaler Connector permite aquellos dispositivos que otras reglas de filtrado no bloqueen o denieguen.
- Static + ZDM Rules: Block Mode. Este modo de directiva ejecuta primero las reglas estáticas, seguidas de las reglas dinámicas de XenMobile con una instrucción implícita de denegar o bloquear al final. Los dispositivos se permiten o deniegan según los filtros definidos y las reglas de Device Manager. Los dispositivos que no coincidan con las reglas y los filtros definidos se bloquean.
- Static + ZDM Rules: Permit Mode. Este modo de directiva ejecuta primero las reglas estáticas, seguidas de las reglas dinámicas de XenMobile con una instrucción implícita de permitir al final. Los dispositivos se permiten o deniegan en función de los filtros definidos y las reglas de XenMobile. Los dispositivos que no coincidan con las reglas y los filtros definidos se permiten.

El proceso de XenMobile NetScaler Connector permite o bloquea reglas dinámicas en función de identificadores únicos de ActiveSync para dispositivos iOS y dispositivos móviles de Windows recibidos desde XenMobile. El comportamiento de los dispositivos Android difiere según el fabricante y algunos no exponen con facilidad un ID único de ActiveSync. Para compensar, XenMobile envía información de ID del usuario de los dispositivos Android para la decisión de permitir o bloquear. Como resultado, si un usuario tiene un solo dispositivo Android, las acciones de permitir y bloquear funcionan de la manera habitual. En cambio, si el usuario dispone de varios dispositivos Android, se permiten todos los dispositivos porque los dispositivos Android no se pueden diferenciar de manera contundente. De todos modos, la puerta de enlace aún se puede configurar para bloquear estáticamente esos dispositivos por su ActiveSyncID (si se conoce). Esta puerta también se puede configurar para bloquear según el tipo de dispositivo o el agente de usuario.

Para especificar el modo de directiva, en la herramienta de configuración del controlador SMG, realice lo siguiente:

1. Haga clic en la ficha Path Filters y, a continuación, haga clic en Add.
2. En el cuadro de diálogo Path Properties, seleccione un modo de directiva de la lista desplegable Policy y, a continuación, haga clic en Save.

Puede revisar las reglas en la ficha Policies de la herramienta de configuración. En XenMobile NetScaler Connector, las reglas se procesan de arriba a abajo. Las directivas permitidas (Allow) se muestran con una marca de verificación verde. Las directivas denegadas (Deny) se muestran con un círculo rojo atravesado por una línea. Para actualizar la pantalla y ver las reglas actualizadas, haga clic en Refresh. También puede modificar el orden de las reglas en el archivo config.xml.

Para probar las reglas, haga clic en la ficha Simulator. Especifique los valores de los campos. Estos también se pueden obtener a partir de los registros. Aparecerá un mensaje de resultados con la especificación Allow o Block.

Para configurar reglas estáticas

Apr 01, 2016

Debe introducir reglas estáticas con valores que lean los filtros ISAPI de la solicitud HTTP de la conexión ActiveSync. Con las reglas estáticas, XenMobile NetScaler Connector puede permitir o bloquear el tráfico mediante los criterios siguientes:

- User. XenMobile NetScaler Connector usa la estructura del nombre y el valor del usuario autorizado capturado durante la inscripción del dispositivo. Generalmente, se encuentra como dominio\nombre_de_usuario, como consta en el servidor que ejecuta XenMobile conectado a Active Directory a través de LDAP. La ficha Log, en la herramienta de configuración de XenMobile NetScaler Connector, mostrará los valores que pasan a través de XenMobile NetScaler Connector si la estructura del valor debe determinarse o si es diferente.
- Deviceid (ActiveSyncID). También conocido como ActiveSyncID del dispositivo conectado. Este valor se suele encontrar en la página de propiedades del dispositivo específico, en la consola de XenMobile. Este valor también se puede consultar desde la ficha Log, en la utilidad de configuración XenMobile NetScaler Connector.
- DeviceType. XenMobile NetScaler Connector puede determinar si el dispositivo es un iPhone, un iPad, o cualquier otro tipo de dispositivo; puede permitirlos o bloquearlos basándose en esos criterios. En cuanto a otros valores, la herramienta de configuración de XenMobile NetScaler Connector puede revelar todos los tipos de dispositivos conectados que se están procesando para la conexión ActiveSync.
- UserAgent. Contiene información sobre el cliente de ActiveSync que se utiliza. En la mayoría de los casos, el valor especificado corresponde a una versión y build determinadas de sistema operativo para la plataforma del dispositivo móvil.

La herramienta de configuración de XenMobile NetScaler Connector que se ejecuta en el servidor siempre administra las reglas estáticas.

1. En la herramienta de configuración del controlador SMG, haga clic en la ficha Static Rules y, a continuación, haga clic en Add.
2. En el cuadro de diálogo Static Rule Properties, especifique los valores a usar como criterios. Por ejemplo, puede indicar un usuario al que permitir el acceso si escribe el nombre del usuario (por ejemplo,AllowedUser) y si, a continuación, desmarca la casilla Disabled.
3. Haga clic en Save. La regla estática está ahora activada. Además, puede usar expresiones regulares para definir los valores, pero debe habilitar el modo de procesamiento de reglas en el archivo config.xml.

Para configurar reglas dinámicas

Apr 01, 2016

En Device Manager, las reglas dinámicas se definen mediante directivas y propiedades de dispositivo. Esas reglas pueden activar un filtro dinámico de XenMobile NetScaler Connector basado en la presencia de una infracción de la directiva o en un parámetro de propiedad. Los filtros de XenMobile NetScaler Connector analizan un dispositivo para detectar la infracción de una directiva concreta o un parámetro de propiedad. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista de dispositivos Device List no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los dispositivos que cumplen los criterios definidos. Con las siguientes opciones de configuración, puede definir si quiere permitir o denegar los dispositivos de Device List mediante XenMobile NetScaler Connector.

Nota: Estas reglas dinámicas deben configurarse en la consola de XenMobile.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **ActiveSync Gateway**. Aparecerá la página ActiveSync Gateway.

3. En **Activate the following rules**, seleccione las reglas que quiera activar.

4. Solo en Android, en **Send Android domain users to ActiveSync Gateway**, haga clic en **YES** para que XenMobile envíe información de dispositivos Android a Secure Mobile Gateway. Si esta opción está habilitada, se garantiza que XenMobile envíe información de dispositivos Android a XenMobile NetScaler Connector en el caso de que XenMobile no disponga del identificador de ActiveSync correspondiente al usuario del dispositivo Android.

Para configurar directivas personalizadas mediante la modificación del archivo XML de XenMobile NetScaler Connector

Apr 01, 2016

En la herramienta de configuración de XenMobile NetScaler Connector, puede ver las directivas básicas en la configuración predeterminada de la ficha Policies. Si quiere crear directivas personalizadas, puede modificar el archivo de configuración XML de XenMobile NetScaler Connector (config\config.xml).

1. Busque la sección PolicyList en el archivo y, a continuación, agregue un nuevo elemento de Policy (directiva).
2. Si también se requiere un nuevo grupo, como un grupo estático adicional o un grupo para respaldar un proveedor GCP adicionales, agregue el nuevo elemento Group a la sección GroupList.
3. Si quiere, puede cambiar el orden de los grupos dentro de una directiva existente. Para ello, reorganice los elementos de GroupRef.

Configuración del archivo XML de XenMobile NetScaler Connector

Apr 01, 2016

XenMobile NetScaler Connector usa un archivo de configuración XML para indicar las acciones de XenMobile NetScaler Connector. Entre otras entradas, el archivo especifica el grupo de archivos y acciones asociadas que el filtro tendrá en cuenta al evaluar solicitudes HTTP. De forma predeterminada, el archivo se denomina config.xml y se encuentra en la siguiente ubicación: ..\Archivos de programa\Citrix\XenMobile NetScaler Connector\config\.

Los nodos GroupRef definen los nombres de grupo lógicos. De forma predeterminada, AllowGroup y DenyGroup.
Nota: Es importante el orden de aparición de los nodos GroupRef en el nodo GroupRefList.
El valor de ID de un nodo GroupRef identifica un contenedor lógico o una colección de miembros, que se utilizan para hacer coincidir dispositivos o cuentas de usuario específicos. Los atributos de la acción especifican cómo tratará el filtro a un miembro que coincida con una regla de la colección. Por ejemplo, un dispositivo o cuenta de usuario que coincida con una regla del conjunto AllowGroup podrá "pasar" (se le permitirá acceder a Exchange CAS), mientras que un dispositivo o cuenta de usuario que coincida con una regla del conjunto DenyGroup será "rechazada" (no se le permitirá acceder a Exchange CAS).

Cuando un dispositivo o una cuenta de usuario determinados, o bien una combinación, cumplen las reglas de ambos grupos, se usa una convención de precedencia para dirigir el resultado de la solicitud. La precedencia se expresa en el orden de los nodos GroupRef en el archivo config.xml de arriba a abajo. Los nodos GroupRef están clasificados por orden de prioridad. Las reglas de una condición determinada del grupo Allow (Permitir) siempre prevalecerán sobre las reglas de la misma condición en el grupo Deny (Denegar).

Además, el archivo config.xml define los nodos Group. Estos nodos enlazan los contenedores lógicos AllowGroup y DenyGroup a archivos XML. Las entradas almacenadas en los archivos externos forman la base de las reglas de filtrado.
Nota: En esta versión, solo se admiten los archivos XML externos.
La instalación predeterminada implementa dos archivos XML en la configuración: allow.xml y deny.xml.

Para importar una directiva desde XenMobile

May 05, 2016

1. En la herramienta de configuración de XenMobile NetScaler Connector, haga clic en la ficha Config Providers y, a continuación, haga clic en Add.
2. En el cuadro de diálogo Config Providers, en Name, escriba un nombre de usuario que se utilizará para la autorización HTTP básica con el servidor XenMobile y que tiene privilegios de administrador.
3. En Url, introduzca la dirección Web de XenMobile Gateway Configuration Service (GCS), normalmente en el formato https://xdmHost/xdm/services/MagConfigService. El nombre MagConfigService distingue mayúsculas de minúsculas.
4. En Password, introduzca la contraseña que se usará para la autorización básica de HTTP con el servidor XenMobile.
5. Haga clic en Test Connectivity para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si se produce un error de conexión, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.
6. Cuando la conexión se realice correctamente, desmarque la casilla Disabled y, a continuación, haga clic en Save.
7. En Managing Host, deje el nombre DNS predeterminado del equipo host local. Este parámetro se utiliza para coordinar la comunicación con XenMobile cuando hay varios servidores de Forefront Threat Management Gateway (TMG) configurados en una matriz.

Después de guardar la configuración, abra GCS.

Para configurar una conexión a XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector se comunica con XenMobile y otros proveedores remotos de configuración a través de servicios Web seguros.

1. En la herramienta de configuración de XenMobile NetScaler Connector, haga clic en la ficha Config Providers y, a continuación, haga clic en Add.
2. En el cuadro de diálogo Config Providers, en Name, escriba un nombre de usuario que tenga privilegios administrativos. Este usuario se utilizará para la autorización HTTP básica con el servidor XenMobile.
3. En Url, introduzca la dirección Web de GCS de XenMobile, normalmente en el formato https://ZdmHost/zdm/services/MagConfigService. El nombre MagConfigService distingue mayúsculas de minúsculas.
4. En Password, introduzca la contraseña que se usará para la autorización básica de HTTP con el servidor XenMobile.
5. En Managing Host, escriba el nombre del servidor de XenMobile NetScaler Connector.
6. En Baseline Interval, especifique un período de tiempo para la extracción, desde Device Manager, de un conjunto de reglas dinámicas actualizadas.
7. En Delta interval, especifique un período de tiempo para la extracción de una actualización de reglas dinámicas.
8. En Request Timeout, especifique el intervalo de tiempo de espera para solicitudes del servidor.
9. En Config Provider, seleccione si la instancia de servidor del proveedor de configuración proporciona la configuración de directivas.
10. En Events Enabled, habilite esta opción si quiere que XenMobile NetScaler Connector notifique a XenMobile cuando un dispositivo se bloquea. Se requiere esta opción si se utilizan reglas de XenMobile NetScaler Connector en alguna de las acciones automatizadas de XenMobile.
11. Haga clic en Save y, a continuación, haga clic en Test Connectivity para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si se produce un error de conexión, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.
12. Si la conexión se realiza correctamente, desmarque la casilla Disabled y, a continuación, haga clic en Save.

Al agregar un nuevo proveedor de configuración, XenMobile NetScaler Connector crea automáticamente una o más directivas asociadas a ese proveedor. Estas directivas se definen mediante una plantilla contenida en config\policyTemplates.xml, en la sección NewPolicyTemplate. Se crea una nueva directiva por cada elemento de Policy definido en esta sección. El operador puede agregar, quitar o modificar los elementos de directiva, siempre que el elemento de directiva corresponda con la definición de esquema y siempre que las cadenas de sustitución estándar (entre llaves) no se hayan modificado. Luego, agregue nuevos grupos para el proveedor y actualice la directiva para incluir los nuevos grupos.

Selección de filtros para XenMobile NetScaler Connector

May 05, 2016

Los filtros de XenMobile NetScaler Connector analizan un dispositivo para detectar la infracción de una directiva concreta o un parámetro de propiedad. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista de dispositivos, Device List, no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los dispositivos que cumplen los criterios definidos. Los siguientes filtros están disponibles para XenMobile NetScaler Connector en XenMobile.

- Blacklisted Apps. Permite o deniega dispositivos basándose en la lista de dispositivos definida por las directivas de aplicaciones prohibidas y la presencia de esas aplicaciones.
- Whitelisted Apps only. Permite o deniega dispositivos según la lista de dispositivos definida por las directivas de aplicaciones permitidas y la presencia de aplicaciones que no se han permitido.
- Unmanaged Devices. Crea una lista de todos los dispositivos de la base de datos de XenMobile. Mobile Application Gateway debe implementarse en un modo de bloqueo.
- Rooted Android /Jailbroken iOS Devices. Crea una lista de todos los dispositivos marcados como liberados por rooting y permite o deniega el acceso en función de ese estado.
- Out of Compliance Devices. Permite o deniega los dispositivos que cumplen los criterios internos propios de cumplimiento de TI. El cumplimiento es un valor arbitrario definido por la propiedad de dispositivo denominada Out of Compliance, un marcador booleano que puede ser True o False. (Puede crear esta propiedad de forma manual y establecer su valor, o puede usar las acciones automatizadas para crear esta propiedad en un dispositivo en función de si este cumple un criterio específico.)
  - Out of Compliance = True. Si el dispositivo no cumple los estándares de cumplimiento ni las definiciones de directivas establecidas por el departamento de TI, el dispositivo no cumple los requisitos.
  - Out of Compliance = False. Si el dispositivo cumple los estándares de cumplimiento y las definiciones de directivas establecidas por el departamento de TI, el dispositivo cumple los requisitos.
- Noncompliant password. Crea una lista de todos los dispositivos que no tienen un código de acceso en el dispositivo.
- Revoked Status. Crea una lista de todos los dispositivos y permite o prohíbe dispositivos según el estado de revocación.
- Inactive devices. Crea una lista de los dispositivos que no se han comunicado con XenMobile durante un período de tiempo específico (por lo tanto, se consideran inactivos) y permite o deniega esos dispositivos según corresponda.
- Anonymous Devices. Permite o deniega aquellos dispositivos inscritos en XenMobile cuya identidad de usuario es desconocida. Por ejemplo, puede tratarse de un usuario que se haya inscrito, pero cuyas contraseñas de Active Directory estén caducadas, o bien un usuario que se ha inscrito con credenciales desconocidas.
- Implicit Allow / Deny. Crea una lista de todos los dispositivos que no cumplen ninguno de los demás criterios de regla o filtro, y permite o deniega en función de esa lista. La opción Implicit Allow/Deny garantiza que se habilite el estado de XenMobile NetScaler Connector en la ficha Devices, y muestra el estado de XenMobile NetScaler Connector para los dispositivos. La opción Implicit Allow/Deny también controla todos los demás filtros de XenMobile NetScaler Connector que no se han seleccionado. Por ejemplo, XenMobile NetScaler Connector denegará (bloqueará) las aplicaciones Blacklists Apps, mientras que el resto de los filtros las permitirán porque la opción Implicit Allow/Deny está seleccionada en Allow.

Para simular tráfico de ActiveSync con XenMobile Netscaler Connector

May 05, 2016

Puede utilizar XenMobile NetScaler Connector para hacer una simulación del aspecto que presentaría el tráfico de ActiveSync en combinación con las directivas. En la herramienta de configuración de XenMobile Netscaler Connector, seleccione la ficha Simulations. Los resultados muestran la manera en que se aplicarán las directivas en función de las reglas que haya configurado.

Supervisión de XenMobile NetScaler Connector

May 05, 2016

La herramienta de configuración de XenMobile NetScaler Connector ofrece un registro detallado para, entre otros, consultar todo el tráfico que pasa por el servidor Exchange que Secure Mobile Gateway permite o bloquea.

Use la ficha Log para ver el historial de las solicitudes de ActiveSync que NetScaler ha reenviado a XenMobile NetScaler Connector para la autorización.

Además, para comprobar que el servicio Web de XenMobile NetScaler Connector se está ejecutando, puede cargar la siguiente URL en un explorador en el servidor de XenMobile NetScaler Connector: http:///services/ActiveSync/Version. Si la dirección URL devuelve la versión de producto como una cadena, el servicio Web funciona.