XenMobile Server 10.3.x

Oct 25, 2016

Acerca de XenMobile Server 10.3.6

Oct 31, 2016

Solo se puede actualizar directamente a XenMobile 10.3.6 Service Pack desde XenMobile 10.3.5.

> ## Nota
>
> Antes de actualizar a XenMobile 10.3.6, la fecha de Subscription Advantage (SA) en la licencia de Citrix debe ser posterior al 1 de junio de 2016. Puede ver la fecha de SA junto a la licencia en el servidor de licencias. Para renovar la fecha de SA en la licencia, descargue la versión más reciente del archivo de licencia desde el portal de Citrix y cargue el archivo al servidor de licencias. Para obtener más información, consulte http://support.citrix.com/article/CTX209580.

Para llevar a cabo la actualización, use el archivo xms_10.3.6.310.bin. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, haga clic en **Release Management**. Haga clic en **Upgrade** y cargue el archivo xms_10.3.6.310.bin. Para obtener más información acerca de actualizaciones en la consola, consulte Actualización de XenMobile.

Para completar una instalación nueva de XenMobile 10.3.6, consulte Instalación de XenMobile.

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 en XenMobile 10.3.6

La versión XenMobile 10.3.6 se centra en la calidad y la escalabilidad. Para obtener información sobre las correcciones de errores, consulte Problemas conocidos y resueltos en XenMobile 10.3.6. XenMobile 10.3.6 incluye las siguientes características nuevas:

Las mejoras significativas en la calidad de XenMobile Server 10.3.6 también ofrecen una mejor escalabilidad y rendimiento en áreas tales como las comunicaciones entre el servidor XenMobile y la base de datos, la integración de XenApp, las notificaciones de implementación en los dispositivos y las búsquedas LDAP.

- La enumeración HDX ha mejorado aproximadamente un 40% sobre XenMobile 10.3.5.
- Cuando se usa el comando **Server Tuning** en el menú de interfaz de línea de comandos de XenMobile (opción **5** bajo **Advanced Settings**), los valores predeterminados aplicados a estos parámetros ahora son distintos:

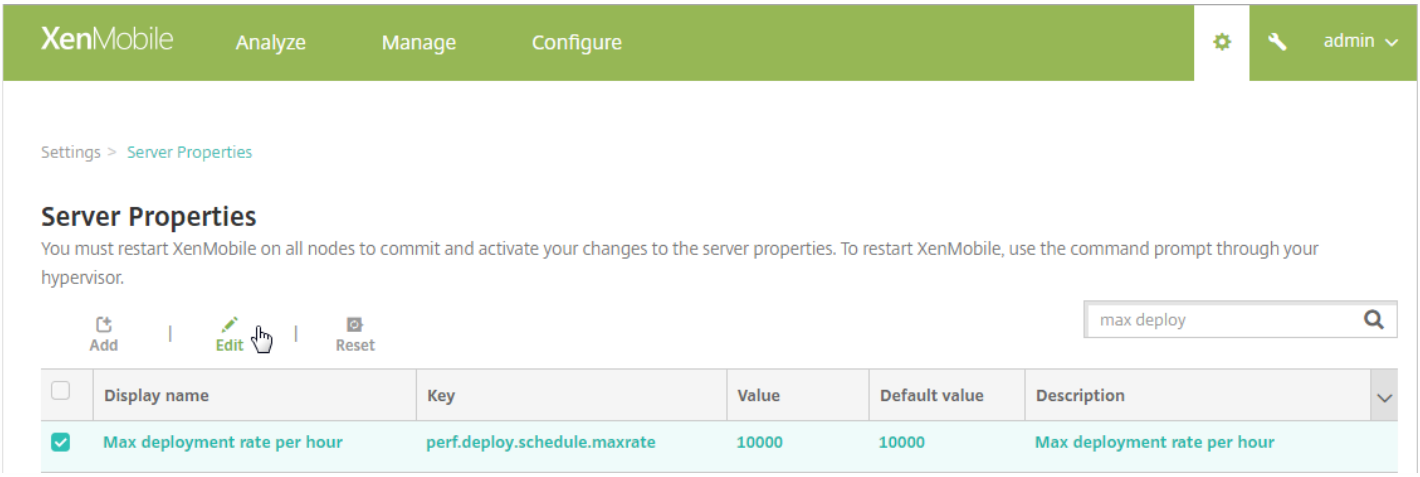
  Número máximo de conexiones en el puerto 443: El valor predeterminado se ha cambiado de **10000** a **12000**.

  Número máximo de conexiones en el puerto 8443: El valor predeterminado se ha cambiado de **10000** a **12000**.

  Número máximo de subprocesos en el puerto 443: El valor predeterminado se ha cambiado de **750** a **2000**.

  Número máximo de subprocesos en el puerto 8443: El valor predeterminado se ha cambiado de **750** a **2000**.

- XenMobile ahora envía notificaciones en una implementación por fases para evitar picos en las solicitudes de reconexión desde dispositivos iOS y Windows Phone, así como dispositivos Android configurados para Google Cloud Messaging. La velocidad de implementación predeterminada es de 10000 dispositivos por hora. Para cambiar la velocidad de implementación, modifique la propiedad del servidor **Max deployment rate** (perf.deploy.schedule.maxrate).



- Las implementaciones de XenMobile ahora tienen como destino solo los dispositivos que forman parte de los grupos de entrega de destino. Anteriormente, se implementaban todos los dispositivos independientemente del rol.

Worx Home

- **Enviar registros con WorxMail**. Cuando los usuarios envían registros para informar de un problema, ahora WorxMail se abre de forma predeterminada. Esto permite a los usuarios enviar archivos grandes sin problemas. En las versiones anteriores de Worx Home, a veces fallaba el envío de archivos si estos eran muy grandes.

WorxMail

- **Respaldo para Exchange Server 2016**. Puede integrar WorxMail con Exchange Server 2016. Active Sync 14 es compatible, pero WorxMail también debe ser compatible con Active Sync 16.
- **Adjuntar archivos desde ShareFile (Android)**. Los usuarios pueden tocar en **Adjuntar desde ShareFile** para adjuntar archivos a los mensajes de correo electrónico o los eventos de calendario.
- **Adjuntar archivos desde StorageZones restringidas y conectores (iOS) de ShareFile**. Cuando los usuarios tocan en **Adjuntar desde ShareFile** en un mensaje de correo electrónico o en un evento de calendario, pueden adjuntar archivos no solo desde ShareFile, sino también desde conectores y StorageZones restringidas tales como SharePoint y recursos compartidos de red.
- **Compartir datos de contactos con archivos .vcard**. Los usuarios pueden importar la información de contacto desde datos adjuntos enviados como archivos .vcard.
- **Nuevo valor predeterminado de acceso de red**. El valor predeterminado para la directiva **Network access** en el MDX Toolkit ahora es **Tunneled to the internal network.** Este cambio puede contribuir a evitar errores de configuración.

WorxWeb

- **Bloqueo de ventanas emergentes de forma predeterminada**. Si quiere que las ventanas emergentes de Safari se bloqueen de forma predeterminada, use la consola de XenMobile para establecer la opción **Block pop-ups** con el valor

On en la directiva de dispositivo **Restrictions**. Si tenía **Block pop-ups** configurado con el valor **Off** antes de actualizar a la versión 10.3.6, el parámetro permanece desactivado. De lo contrario, el valor es **On** y las ventanas emergentes se bloquean en Safari.

- **Abrir enlaces en ShareFile**. ShareFile 4.0 permite a los usuarios elegir si quieren abrir enlaces en un explorador Web o directamente en ShareFile.

WorxChat Technical Preview

- **Respaldo para Android.** WorxChat está ahora disponible en Android.
- **Respaldo para Lync 2013 y Skype Empresarial 2015**. Ahora puede integrar WorxChat con Lync 2013 y Skype Empresarial 2015 en el mismo grupo.

Secure Forms

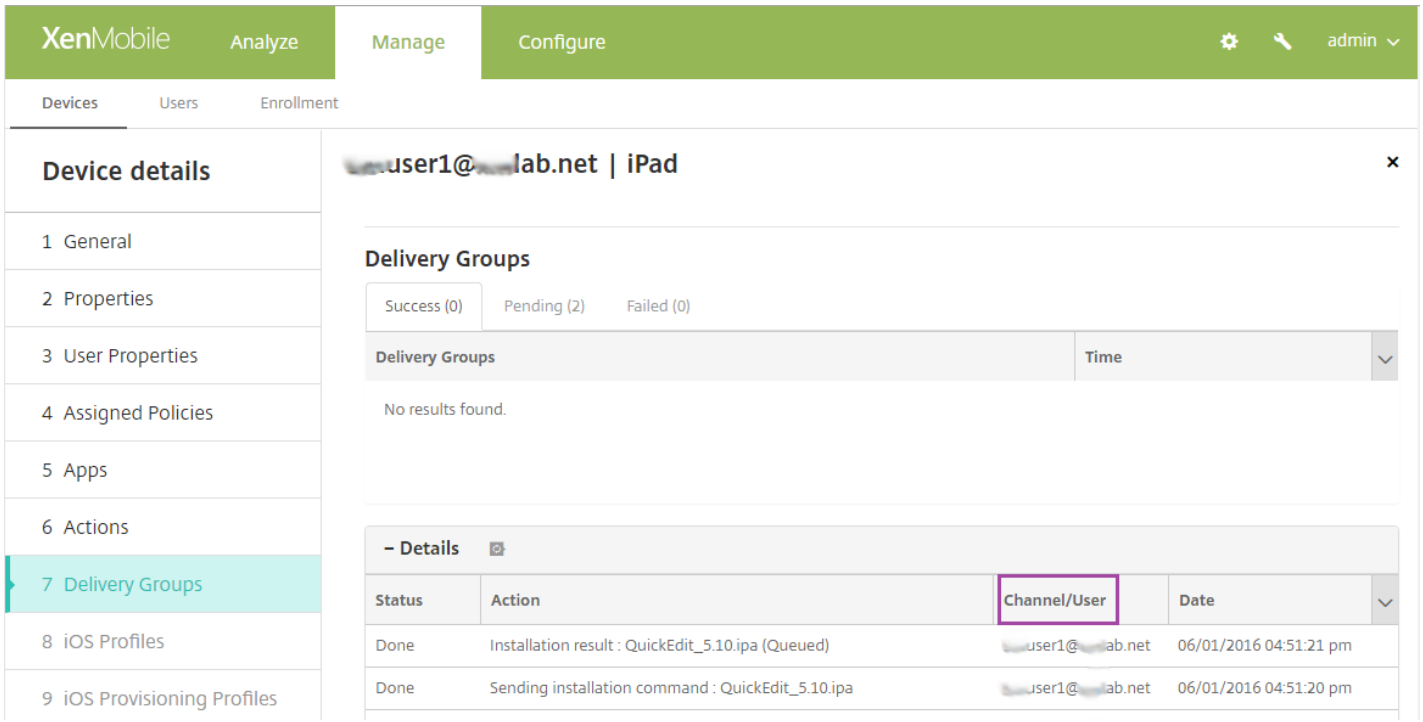
- **Respaldo para zonas restringidas de ShareFile**. Ahora puede configurar Secure Forms con zonas restringidas de ShareFile. Siga las instrucciones de instalación descritas en Integración de Secure formularios con ShareFile.
- **Capacidades iBeacon**. Con tecnología de iBeacon, puede configurar y realizar un seguimiento de balizas que permiten a los usuarios autorellenar formularios en la aplicación móvil. La información de balizas se incluye cuando los usuarios envían sus formularios. Para obtener información acerca de cómo configurar balizas, consulte Balizas.
- **Nombre del creador del formulario** Secure Forms Composer ahora muestra el nombre de la persona que creó el formulario. Esta característica facilita el seguimiento cuando hay varios usuarios que acceden a Composer.
- **Rango de números**. En el campo **Number** de Composer, puede especificar un rango de números que los usuarios pueden introducir al rellenar formularios.
- **Nuevo formato de nombre de archivo.** Los formularios y los datos adjuntos enviados en la aplicación móvil ahora se guardan junto con el nombre del remitente y una marca de tiempo, por lo que los nombres de archivo son más fáciles de leer y de organizar.

Para obtener más información, consulte Novedades de las aplicaciones móviles de Worx.

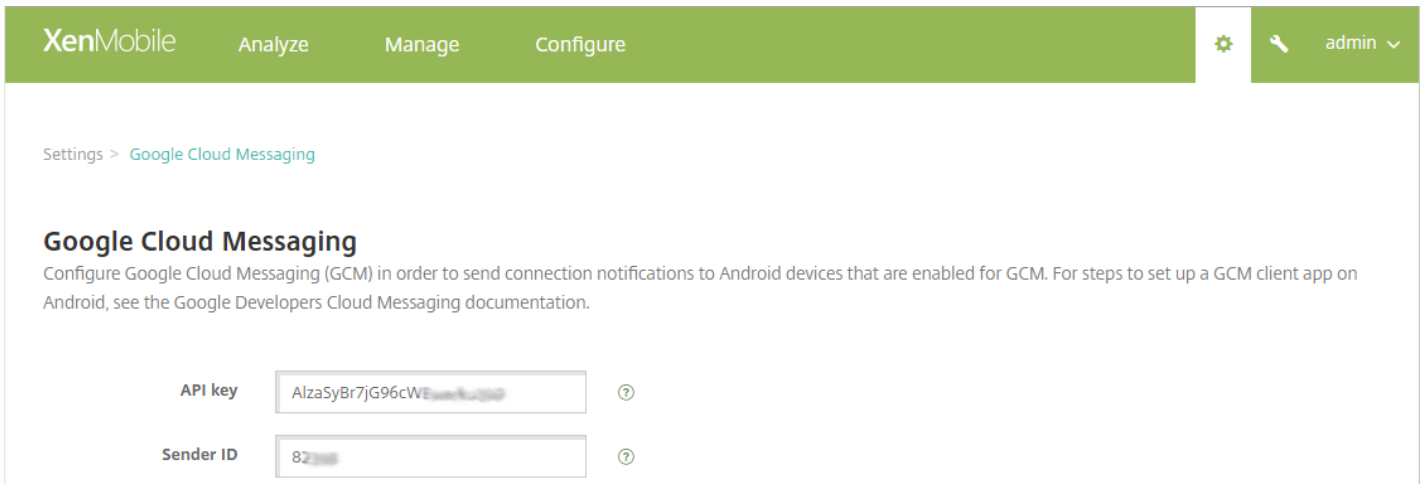
- **Respaldo para más versiones de componentes de Citrix.**
  - NetScaler Gateway 10.5.x, 11.0.x y 11.1.x (implementaciones locales de XenMobile)
  - NetScaler Gateway 10.5.57.7 (XenMobile Cloud)
  - XenApp and XenDesktop 7.9 y 7.8
  - StoreFront 3.6
  - License Server 11.13.1.2
- **Lista blanca de redes WiFi.** Con la directiva Whitelisted WiFi networks puede especificar redes permitidas. Las aplicaciones solo funcionarán cuando estén conectadas a una de las redes de la lista. Esta función está disponible en el modo MDM+MAM solamente.
- **Respaldo de ShareFile para dispositivos compartidos.** Ahora, la aplicación móvil ShareFile 4.4 respalda los dispositivos compartidos en modo MDM+MAM, lo que permite que varios usuarios compartan un dispositivo sin volver a inscribirse. Para obtener más información, consulte Dispositivos compartidos en XenMobile.
- **Gestión de iconos (iOS).** Ahora, los desarrolladores de aplicaciones pueden colocar archivos de iconos en la carpeta raíz del paquete de la aplicación, como alternativa a la práctica habitual de colocarlos en info.plist. Para que el Toolkit pueda encontrar los archivos de iconos, sus nombres deben tener los siguientes formatos:
  - icon.png
  - icon-60x2.pn
  - icon-72.png

- icon-76.png

- **Mejoras en la sincronización de correo (iOS).** Se han actualizado la sincronización de correo y la integración de ShareFile para hacer más fiable la sincronización.
- **Información adicional del dispositivo.** La página **Device details** en la consola de XenMobile ahora incluye una columna **Channel/User** que muestra el destino de una acción de implementación en el dispositivo. El destino puede mostrar un usuario que inscribió el dispositivo, un usuario conectado con un dispositivo compartido, o parámetros del sistema o acciones de implementación que no están asociadas a un usuario específico. Puede usar esta información para realizar un seguimiento del proceso de implementación, especialmente cuando hay muchos usuarios que usan un dispositivo o hay muchos contenedores en una plataforma específica como Mac OS X.

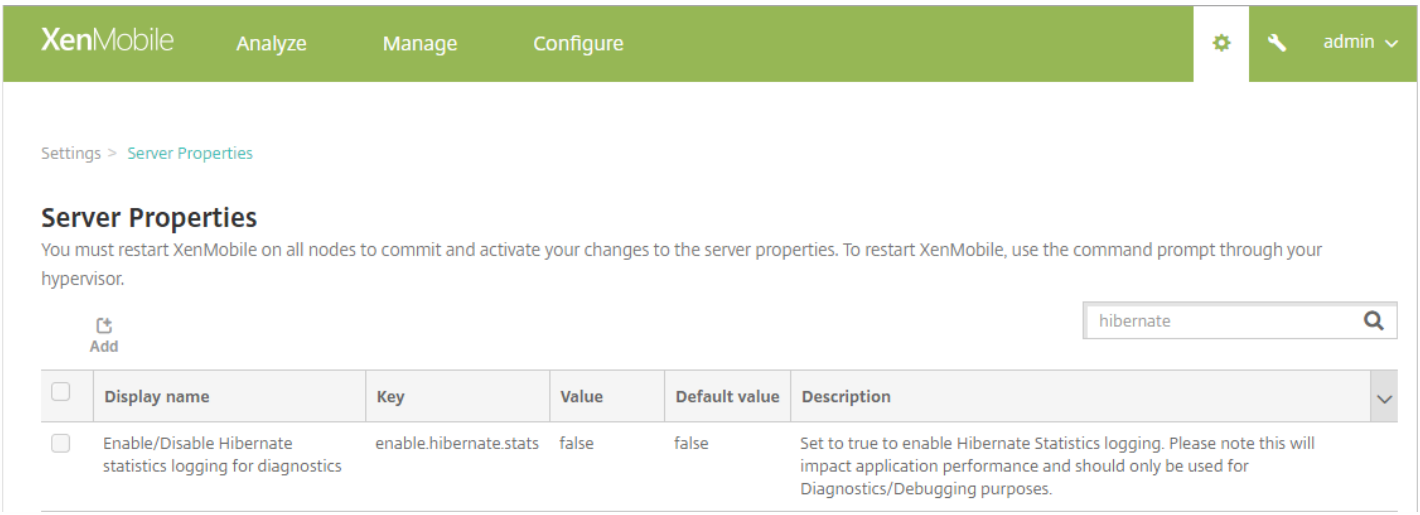


- **Nueva página en la consola de XenMobile.** La consola de XenMobile incluye una nueva página, **Settings > Google Cloud Messaging**, donde se puede especificar la clave API y el ID de remitente de GCM en los campos **API key** y **Sender ID** respectivamente. Anteriormente estos elementos solo aparecían en **Server Properties**.



- **Registros de estadísticas de Hibernate para diagnósticos.** Para ayudar a solucionar los problemas de rendimiento de las aplicaciones, XenMobile ahora puede proporcionar un informe de registros de estadísticas de registro para Hibernate, un componente que se utiliza para las conexiones de XenMobile con Microsoft SQL Server.

  Para habilitar el registro de estadísticas de Hibernate, cambie el valor de la propiedad de servidor **Enable/Disable Hibernate statistics logging for diagnostics** (enable.hibernate.stats) a **true**. De forma predeterminada, esta captura de registros está inhabilitada porque tiene un impacto en el rendimiento de las aplicaciones. Habilite esta captura de registros solo durante un espacio corto de tiempo para evitar crear un archivo de registros demasiado grande. XenMobile escribe los registros en /opt/sas/logs/hibernate_stats.log.



- **Actualizaciones en loa tienda de aplicaciones de Android.** La tienda de aplicaciones de Android mostrará una versión actualizada de la aplicación solo si la versión instalada en el dispositivo es anterior a la versión en la tienda de aplicaciones.
- **XenMobile Analyzer Tool.** Cuando tiene un problema con el entorno de XenMobile, contactar con Citrix Support puede costarle tiempo y dinero a su organización. Con XenMobile Analyzer puede analizar problemas comunes por si mismo antes de contactar con el servicio de asistencia técnica. XenMobile Analyzer Tool respalda varios casos de uso y opciones de implementación, incluidas MDM, MDM+MAM, y solo MAM; 5 escenarios de autenticación distintos y entornos móviles de iOS y Android.

  XenMobile Analyzer puede hacer lo siguiente:
  - Comprobar su entorno para detectar problemas y recomendar soluciones. Las comprobaciones del entorno de XenMobile Analyzer pueden detectar problemas de dispositivos, de inscripción de usuarios y de autenticación.
  - Guiarle por los pasos necesarios para recibir diagnósticos avanzados.
  - Dirigirle a herramientas para comprobar la disponibilidad de WorxMail y la conectividad de los servidores.
  - Si todo lo demás falla, la herramienta muestra un enlace directo al servicio de asistencia técnica Citrix Support.

  Para obtener más información, consulte XenMobile Analyzer Tool.

- **XenMobile AutoDiscovery Service**. Hasta ahora, para activar la detección automática había que crear un tiquet de asistencia técnica. Con el portal AutoDiscovery Service, usted puede configurar la detección automática por si mismo. El servicio le guiará a través de los pasos necesarios para reclamar su dominio y luego crear registros de detección automática. Para obtener más información, consulte XenMobile AutoDiscovery Service.

Problemas conocidos y resueltos en XenMobile 10.3.6

Jul 27, 2016

Estos son los problemas conocidos o resueltos de XenMobile 10.3.6:

Problemas conocidos

Cuando los usuarios intentan inscribir su dispositivo personal con una cuenta de trabajo de Microsoft, la inscripción falla. [#597037]

Cuando los usuarios se inscriben en XenMobile mediante una cuenta de Azure Active Directory, incluso después de haber borrado o revocado el dispositivo, pueden inscribirse de nuevo sin autorización. Este es un problema de terceros. [#628865]

Después de actualizar a XenMobile a la versión 10.3.6, en una configuración de clúster, la inscripción de dispositivos iOS puede fallar. Como solución temporal, consulte este artículo de conocimientos. [#650061]

Problemas resueltos

Los administradores de XenMobile que intentan obtener acceso a la consola de XenMobile, en vez de ello pueden ser redirigidos al portal Self-Help Portal de XenMobile. Esto puede ocurrir cuando se han creado grupos de administradores de XenMobile con acceso basado en roles y se mueve un grupo desde una unidad organizativa de Active Directory a otra. [#585032]

Con esta corrección, cuando un usuario establece el tamaño del archivo de registros y el número máximo de archivos de copia de seguridad de los registros, estos valores se configuran correctamente en XenMobile y los archivos se renuevan correctamente. Sin embargo, puede que la consola de XenMobile no refleje los valores actualizados, como se indica en la descripción del problema #551199. [#597772]

En las ediciones de XenMobile que tienen MDM y MAM unificado, a veces los dispositivos iOS no pueden inscribirse completamente. El dispositivo puede haberse inscrito en MDM pero no en MAM, o viceversa. [#610847]

Cuando se configura una directiva de Exchange ActiveSync para Windows y se define la opción **Only when previous deployment has failed** en las reglas de implementación, ocurre el siguiente problema: cuando los usuarios de Windows Phone cambian el periodo de sincronización de correo de Exchange Server, este cambio se anula la próxima vez que XenMobile envía una directiva de Exchange ActiveSync al dispositivo Windows. [#616725]

Cuando se busca un dispositivo o un usuario dentro de la consola de XenMobile y la base de datos contiene una gran cantidad de datos, el nivel de uso de CPU en SQL Server aumenta considerablemente y la búsqueda puede tardar más de 1 minuto. [#618371]

Cuando los usuarios de dispositivos iOS se inscriben en Worx Home, en ocasiones, Worx Home deja de responder durante dos minutos antes de solicitar a los usuarios que creen un PIN de Worx. Después de ocurrir esto, cuando los usuarios intentan abrir WorxStore, Worx Home deja de responder de nuevo. [#619945]

Puede fallar el envío de notificaciones SMS desde el servidor XenMobile a los dispositivos que ejecutan Windows 10. [#621229]

Cuando se agrega un grupo de nivel secundario de Active Directory a un grupo de nivel superior que contiene más de 1.500 miembros, las acciones que realice en la consola de XenMobile (como, por ejemplo, asignaciones de grupo de entrega) no se aplican a los usuarios del grupo secundario que ha agregado. [#622523]

Después de inscribir dispositivos iOS, no se pide a los usuarios que instalen las aplicaciones obligatorias hasta que abren WorxStore o intentan agregar una aplicación manualmente. [#622789]

Los usuarios no pueden autenticarse en Worx Home si se actualiza desde XenMobile 9.0 a XenMobile 10.1 y luego se configura la opción de LDAP "Buscar usuario por" con el valor sAMAccountName y después se actualiza a XenMobile 10.3.x. [#624340]

Las implementaciones de directivas y la asignación de roles de RBAC pueden fallar si el UPN explícito no coincide con el UPN implícito para un usuario. [#624612]

En implementaciones de servidores en clúster, puede haber problemas relacionados con el mapa distribuido de Hazelcast y la conectividad con el servidor SQL Server, que pueden hacer que el servidor XenMobile deje de responder de manera intermitente, lo que impide el inicio de sesiones y hace que fallen los intentos de inscripción. [#624931]

Cuando un dispositivo Android se conecta al servidor XenMobile por primera vez o se vuelve a conectar, las aplicaciones de Android se descargan muy lentamente o no se pueden descargar. [#625199]

La lista de aplicaciones puede no mostrarse para usuarios de WorxHome 10.3 si se agrega a la consola de XenMobile una aplicación pública que contiene el carácter ASCII 16 (el carácter de escape de línea) en su nombre o en su descripción. [#627059]

Los servidores en clúster pueden dejar de responder de manera intermitente si se ha implementado un mapa distribuido de Hazelcast. [#627114]

Cuando se actualizan dos instancias de servidor a XenMobile 10.3, después de ejecutarse un tiempo, el primer servidor deja de responder. [#628270]

Después de inscribirse correctamente, a veces los dispositivos iOS no pueden iniciar sesión en WorxStore y aparece un mensaje similar al siguiente: “No se puede obtener los recursos necesarios para continuar. Vuelva a intentarlo". Este problema ocurre porque el servidor XenMobile no encuentra el dispositivo por su ID de dispositivo de MAM. [#629900]

Los dispositivos eliminados de la consola de XenMobile siguen permitiendo el acceso a recursos de MAM. [#630137]

En ocasiones, tiene lugar un borrado selectivo para usuarios de iOS. [#630466]

En XenMobile 10.3.x, la vista de categorías de Worx Home puede no mostrar las aplicaciones HDX. La carpeta "Other", que contenía aplicaciones HDX de forma predeterminada en la vista de categorías para versiones anteriores de XenMobile, puede no aparecer. [#631439]

Cuando los usuarios inscriben un dispositivo, la inscripción MDM es correcta pero, en ocasiones, el registro en MAM falla y da un error, y las aplicaciones se bloquean. [#632073]

Las aplicaciones Android compiladas con el SDK de Android versión 22 o posterior, o con ofuscación de Dexguard, no se pueden cargar en XenMobile. [#632146]

De manera intermitente, después de que los usuarios se inscriben en Worx Home, se les solicita que desinstalen y vuelvan a instalar Worx Home. [#633095]

Al realizar un borrado selectivo o un borrado completo, o al eliminar una cuenta o un dispositivo en la consola de XenMobile, en ocasiones las licencias de VPP asociadas a aplicaciones que se han configurado en el dispositivo no se liberan. [#633366]

Algunas licencias de VPP tienen ID con valores negativos, como -123441212, en cuyo caso no se pueden distribuir las aplicaciones públicas. [#631443]

Cuando los usuarios se inscriben en un dispositivo, en ocasiones, Worx Home falla con un mensaje de error 403 donde se indica que el almacén de aplicaciones está bloqueado. De forma alternativa, los usuarios pueden inscribirse correctamente, pero cuando descargan una aplicación, se produce el mismo error o un error donde se indica que no se puede obtener información más detallada. [#633515]

Cuando los usuarios intentan configurar una directiva de Wi-Fi para dispositivos con una clave compartida en la consola de XenMobile para dispositivos basados en Windows, después de cambiar el tipo de autenticación a WPA Personal o WPA-2 Personal, la opción de clave compartida no aparece como se espera. [#633897]

Si tiene un dispositivo NetScaler configurado como un proxy de reenvío, las comprobaciones de conectividad de XenMobile 10.3 devuelven resultados incorrectos. [#633902]

Después de actualizar a XenMobile 10.3.5, los dispositivos ya no se inscriben en modo MAM. Además, las implementaciones de aplicaciones y directivas fallan para los dispositivos que están inscritos en modo MDM + MAM. [#634034]

En ediciones de XenMobile MDM que incluyen MDM y MAM unificados, la autenticación MAM puede fallar para dispositivos DEP autorizados cuando el campo de búsqueda de usuarios en los parámetros de LDAP está configurado para buscar por samAccountName. Como resultado de ello, es posible que no se complete el registro en Worx Home y que el dispositivo solo quede inscrito en MDM. [#637599]

Escalabilidad y rendimiento de XenMobile

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.

Los datos de este artículo están pensados para guiarle a la hora de determinar el rendimiento y la escalabilidad de la infraestructura de XenMobile 10.3.6. 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/ dispositivos).

- 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 se define como la integración de nuevos usuarios y 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.

Escalabilidad	Hasta 45000 dispositivos	
Índices de inicios de sesión	Integración (primer uso)	Un máximo de 833 dispositivos por hora
	Usuarios existentes	Un máximo de 2,812 dispositivos por hora
Configuración	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Clúster de 6 nodos del servidor XenMobile
	Base de datos	Base de datos externa de Microsoft SQL Server

> **Important**
>
> El requisito de automatización para este informe es de 1000 a 60,000 dispositivos. Los requisitos de más de 60,000 dispositivos quedan fuera del alcance de este informe.

En esta sección se describe la configuración de Active Directory, la cantidad de directivas de XenMobile, la cantidad y el tipo de las aplicaciones, las simulaciones de acciones de usuario y las simulaciones de acciones de administrador del perfil de prueba que se usó para cada configuración de hardware y la carga que se utilizó para obtener los resultados de las pruebas descritas en este artículo.

> **Nota**
>
> Este perfil de prueba está diseñado para usar más recursos que otros perfiles utilizados para probar escalabilidad en versiones anteriores de XenMobile. Por lo tanto, estos resultados de pruebas no son directamente comparables a los resultados de escalabilidad de las versiones anteriores.

Configuración de Active Directory (AD):

- 100 000 usuarios únicos de AD
- 200 000 grupos únicos de AD
- 5 niveles de anidamiento de los grupos de AD
- 200 usuarios por cada grupo de AD

Grupos de entrega:

- 20 grupos de entrega
- 50 aplicaciones asignadas a grupos de entrega
- 10 grupos de AD por cada grupo de entrega

Directivas de dispositivo de XenMobile:

- 300 directivas de dispositivo
- 20 directivas de dispositivos por usuario

Aplicaciones:

- 200 aplicaciones nativas de una tienda pública
- 50 aplicaciones nativas de distribución empresarial
- 100 aplicaciones Web y SaaS
- 50 aplicaciones por usuario

Acciones de usuario de XenMobile:

- 50 acciones configuradas en total

- Inicios de Worx Store:
  - Usuarios nuevos (FTU): 4
  - Usuarios existentes (RU): 1
- Inicios de aplicaciones:
  - MDX: 1
  - Web/SaaS: 1
- 150 validaciones de STA por usuario

Operaciones de administrador de XenMobile:
- Enumerar dispositivos, para simular escenarios de llamadas a la asistencia técnica: 32 operaciones cada 8 horas, una cada 15-20 minutos.
- Generar informes: 2 veces cada 8 horas.

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 60000 dispositivos. Estas directrices se basan en los resultados de las pruebas y las cargas de trabajo asociadas. Las recomendaciones tienen en cuenta 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 configurados 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.
- La cantidad de conexiones por sesión de usuario en NetScaler es una consideración importante.
- Para lograr la máxima escalabilidad, los recursos de CPU y RAM se aumentaron en XenMobile.
- La configuración del clúster de 6 nodos es la configuración validada más grande. Aumentar la escalabilidad de más de 6 nodos requiere una implementación adicional de XenMobile.

En la tabla siguiente se muestran los índices de inicios de sesión recomendados para usuarios existentes y nuevos, en función de 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 de inscripción y de inicios de sesión y, por el otro, las recomendaciones del hardware apropiado.

Cantidad estimada de dispositivos	1,000	10,000	30,000	45,000
Cantidad real de dispositivos	1,000	9,998	29,977	44,991
Índice de inicios de sesión				
Integración (primer uso)	250	625	833	833
Usuarios existentes (solo Worx)	1,000	1,666	3,750	883
Configuración				
Entorno de referencia	VPX-XenMobile en modo autónomo	MPX-XenMobile en modo autónomo	MPX-XenMobile con clústeres (3)	MPX-XenMobile con clústeres (6)
NetScaler Gateway	VPX con 2 GB de RAM 2 CPU virtuales	MPX-10500	MPX-11500	MPX-11500
Modo de XenMobile	Autónomo*	Autónomo*	Clúster	Clúster
Clústeres de XenMobile	N/D	N/D	3	6
Dispositivo virtual de XenMobile	8 GB de RAM y 4 CPU virtuales	8 GB de RAM y 4 CPU virtuales	16 GB de RAM y 6 CPU virtuales	16 GB de RAM y 8 CPU virtuales
Active Directory (AD)	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 RM y 4 CPU virtuales
Base de datos	Externa	Externa - Microsoft SQL Server Memoria = 16 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 32 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 48 GB Unidades vCPU = 16

MPX-XenMobile con clústeres (3)

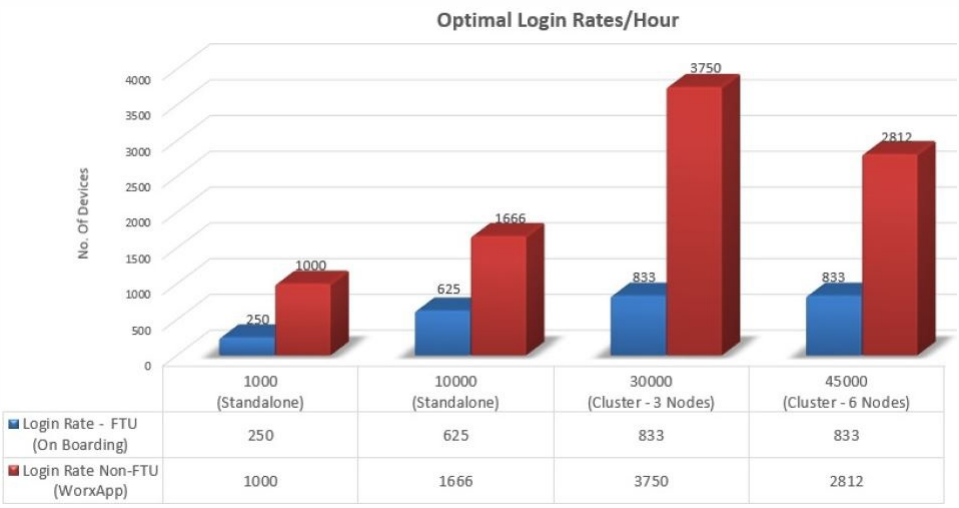
Clúster
Clúster
Clúster
Clúster
8 GB de RAM y 4 CPU virtuales
8 GB de RAM y 4 CPU virtuales

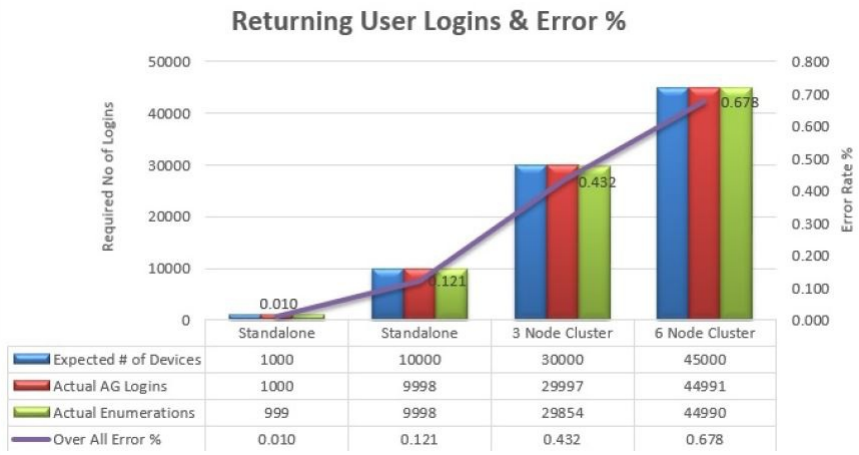
* Las implementaciones en modo autónomo no se recomiendan para aplicaciones que deben estar siempre disponibles para los usuarios. Citrix recomienda usar implementaciones en clúster, de alta disponibilidad, para la mayoría de los clientes.

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

La información siguiente ofrece puntos de datos adicionales que fueron registrados y que afectan a los resultados de la tabla anterior.

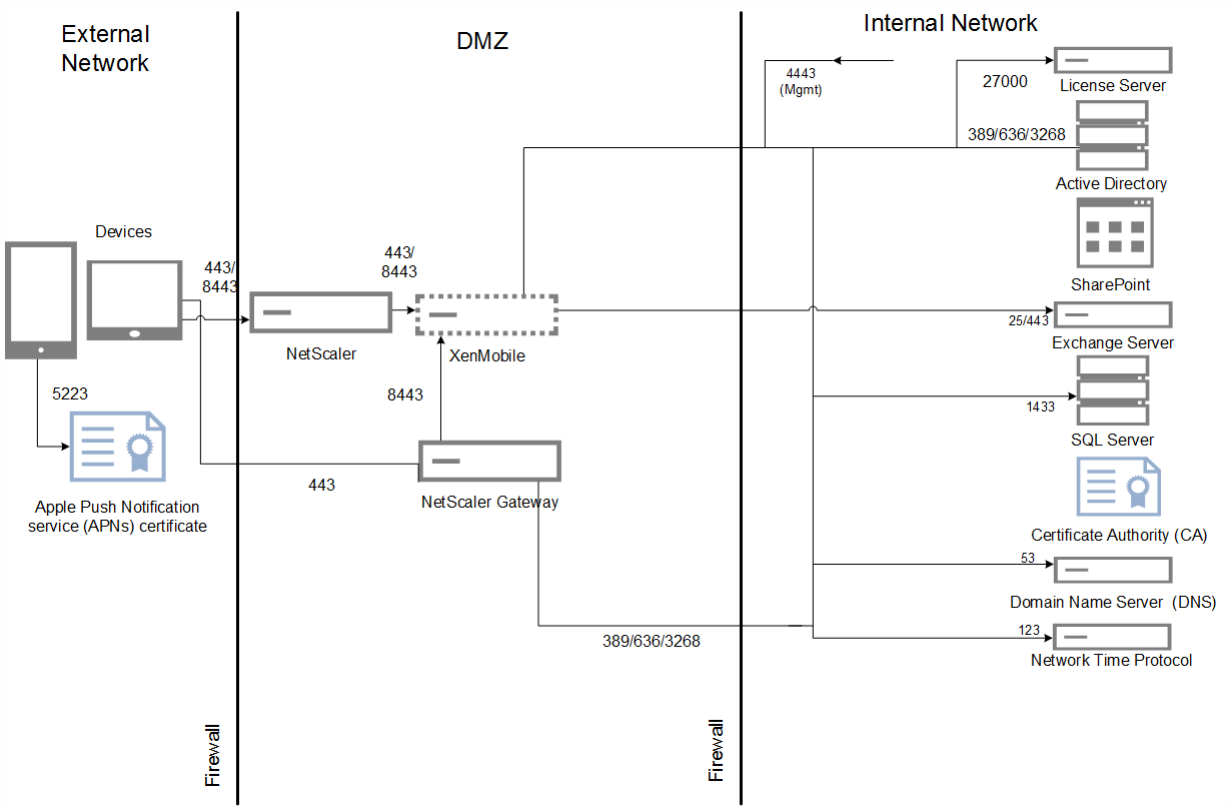
- Latencia de inscripción o de inicio de sesión (tiempo de ida y vuelta)
  - Latencia media total: de 0,5 a 1,5 segundos
  - Latencia media de un inicio de sesión de NetScaler Gateway: > 120 a 440 milisegundos
  - Latencia media de una solicitud de Worx Store: de 2 a 3 segundos
- Se ha observado una 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.
  - Respuesta lenta de la consola de XenMobile durante fases de carga alta.



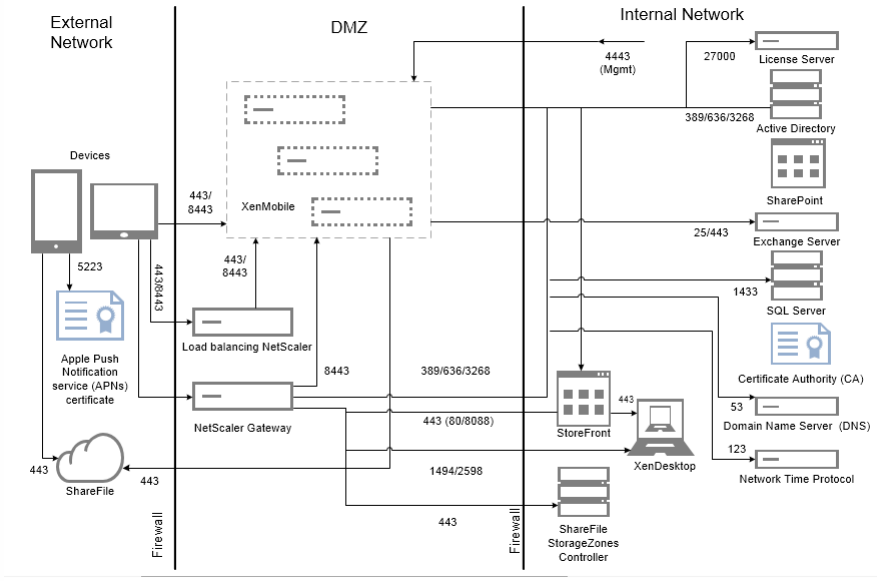


El porcentaje de error mostrado en la imagen anterior incluye errores generales obtenidos en solicitudes correspondientes a todas las operaciones, sin limitarse únicamente a los inicios de sesión. El porcentaje de error se encuentra dentro del límite aceptable del 1% para cada prueba realizada, tal y 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 MAM a través de HTTP que admite 10 000 dispositivos o más.



Las pruebas se realizaron con XenMobile Enterprise para establecer bancos de pruebas. Para ofrecer soluciones a implementaciones tanto pequeñas como grandes, se han utilizado de 1000 a 60000 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.

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

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.

Notas e hipótesis

Los casos siguientes no forman parte de las pruebas de escalabilidad. Estos casos se tendrán en cuenta para las siguientes mejoras en las pruebas de escalabilidad:

- No se ha probado la implementación de paquetes.
- No se ha probado la plataforma Windows.

En envío de directivas se ha probado para dispositivos iOS y Android.
Cada instancia de XenMobile admite un máximo de 10 000 conexiones simultáneas.

Las pruebas se realizaron en condiciones idóneas con conexión LAN para evitar problemas de latencia de red. En una situación real, la escalabilidad también depende del ancho de banda de que disponga el usuario, sobre todo para la descarga de aplicaciones.

Pruebas de reconexión

Se realizaron pruebas de reconexión por separado para Primer uso y para Usuario existente.

Las pruebas de reconexión se hicieron con un máximo de 15000 dispositivos.

La tasa de reconexión respaldada para Android es de 17 dispositivos por segundo. La tasa de reconexión respaldada para iOS es de 8 dispositivos por segundo. Para conseguirlo, el recuento de maxThread se estableció en 1000 en el archivo /opt/sas/tomcat/conf/server.xml.

TO BE ADDED: INFORMATION ON RECOMMENDED DEVICE RECONNECTION POLICIES

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 (Web, SaaS y aplicaciones MDX móviles) incluida la comprobación de estado de los dispositivos
- Envío push de directivas (para iOS)
- 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 se definen en la tabla siguiente:

Dispositivos	Registro de dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Inicios de WorxStore por dispositivo	Single Sign-On para aplicaciones Web o SaaS por dispositivo	Descargas de aplicaciones MDX por dispositivo	Descargas de aplicaciones requeridas activadas a través de XenMobile	Directivas enviadas via push por dispositivo (iOS)

1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Usuarios existentes cargas de trabajo de conexiones Worx solamente

La tabla siguiente muestra la carga de trabajo de usuarios existentes (con conexiones Worx solamente). Esta carga de trabajo simulaba un usuario que utiliza las aplicaciones WorxMail y WorxWeb. Esta simulación se utilizó para medir la escalabilidad de NetScaler Gateway en la configuración de XenMobile. Esto es posible porque al utilizar solo estas dos aplicaciones Worx, la red tiene una carga reducida. Para la aplicación WorxWeb, el usuario accede a sitios Web internos que no activan el inicio de sesión SSO en el servidor XenMobile. Las operaciones en este modo son las siguientes:

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

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

Dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Túneles VPN por dispositivo[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. La cantidad de túneles VPN corresponde a conexiones WorxMail y WorxWeb.

Los perfiles de conexión para WorxMail y WorxWeb se describen en la tabla siguiente:

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).

Estas recomendaciones se basan en perfiles de WorxMail y WorxWeb utilizados para automatizar una
carga de trabajo "media". Las modificaciones realizadas en los detalles de conexión afectan los resultados de los análisis. Por ejemplo, si se 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

Los perfiles utilizados para cada aplicación están diseñados para automatizar una carga de trabajo muy intensa. Las tablas siguientes muestran los detalles de los perfiles de WorxMail y WorxWeb.

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

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.
- El tiempo de espera de sesión de NetScaler está configurado en 60 minutos.
- Se utilizó una clave de 2048 bits en NetScaler Gateway para las transacciones SSL.

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).

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

Componente	Versión
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de datos externa	Microsoft SQL Server 2014

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

Proveedor	Genuine Intel
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).

Escalabilidad y rendimiento de XenMobile

Jul 27, 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.

Los datos de este artículo están pensados para guiarle a la hora de determinar el rendimiento y la escalabilidad de la infraestructura de XenMobile 10.3.6. 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/ dispositivos).

- 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 se define como la integración de nuevos usuarios y 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.

Escalabilidad	Hasta 45000 dispositivos	
Índices de inicios de sesión	Integración (primer uso)	Un máximo de 833 dispositivos por hora
	Usuarios existentes	Un máximo de 2,812 dispositivos por hora
Configuración	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Clúster de 6 nodos del servidor XenMobile
	Base de datos	Base de datos externa de Microsoft SQL Server

> **Important**
>
> El requisito de automatización para este informe es de 1000 a 60,000 dispositivos. Los requisitos de más de 60,000 dispositivos quedan fuera del alcance de este informe.

En esta sección se describe la configuración de Active Directory, la cantidad de directivas de XenMobile, la cantidad y el tipo de las aplicaciones, las simulaciones de acciones de usuario y las simulaciones de acciones de administrador del perfil de prueba que se usó para cada configuración de hardware y la carga que se utilizó para obtener los resultados de las pruebas descritas en este artículo.

> **Nota**
>
> Este perfil de prueba está diseñado para usar más recursos que otros perfiles utilizados para probar escalabilidad en versiones anteriores de XenMobile. Por lo tanto, estos resultados de pruebas no son directamente comparables a los resultados de escalabilidad de las versiones anteriores.

Configuración de Active Directory (AD):

- 100 000 usuarios únicos de AD
- 200 000 grupos únicos de AD
- 5 niveles de anidamiento de los grupos de AD
- 200 usuarios por cada grupo de AD

Grupos de entrega:

- 20 grupos de entrega
- 50 aplicaciones asignadas a grupos de entrega
- 10 grupos de AD por cada grupo de entrega

Directivas de dispositivo de XenMobile:

- 300 directivas de dispositivo
- 20 directivas de dispositivos por usuario

Aplicaciones:

- 200 aplicaciones nativas de una tienda pública
- 50 aplicaciones nativas de distribución empresarial
- 100 aplicaciones Web y SaaS
- 50 aplicaciones por usuario

Acciones de usuario de XenMobile:

- 50 acciones configuradas en total

- Inicios de Worx Store:
  - Usuarios nuevos (FTU): 4
  - Usuarios existentes (RU): 1
- Inicios de aplicaciones:
  - MDX: 1
  - Web/SaaS: 1
- 150 validaciones de STA por usuario

Operaciones de administrador de XenMobile:
- Enumerar dispositivos, para simular escenarios de llamadas a la asistencia técnica: 32 operaciones cada 8 horas, una cada 15-20 minutos.
- Generar informes: 2 veces cada 8 horas.

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 60000 dispositivos. Estas directrices se basan en los resultados de las pruebas y las cargas de trabajo asociadas. Las recomendaciones tienen en cuenta 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 configurados 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.
- La cantidad de conexiones por sesión de usuario en NetScaler es una consideración importante.
- Para lograr la máxima escalabilidad, los recursos de CPU y RAM se aumentaron en XenMobile.
- La configuración del clúster de 6 nodos es la configuración validada más grande. Aumentar la escalabilidad de más de 6 nodos requiere una implementación adicional de XenMobile.

En la tabla siguiente se muestran los índices de inicios de sesión recomendados para usuarios existentes y nuevos, en función de 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 de inscripción y de inicios de sesión y, por el otro, las recomendaciones del hardware apropiado.

Cantidad estimada de dispositivos	1,000	10,000	30,000	45,000
Cantidad real de dispositivos	1,000	9,998	29,977	44,991
Índice de inicios de sesión				
Integración (primer uso)	250	625	833	833
Usuarios existentes (solo Worx)	1,000	1,666	3,750	883
Configuración				
Entorno de referencia	VPX-XenMobile en modo autónomo	MPX-XenMobile en modo autónomo	MPX-XenMobile con clústeres (3)	MPX-XenMobile con clústeres (6)
NetScaler Gateway	VPX con 2 GB de RAM 2 CPU virtuales	MPX-10500	MPX-11500	MPX-11500
Modo de XenMobile	Autónomo*	Autónomo*	Clúster	Clúster
Clústeres de XenMobile	N/D	N/D	3	6
Dispositivo virtual de XenMobile	8 GB de RAM y 4 CPU virtuales	8 GB de RAM y 4 CPU virtuales	16 GB de RAM y 6 CPU virtuales	16 GB de RAM y 8 CPU virtuales
Active Directory (AD)	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 RM y 4 CPU virtuales
Base de datos	Externa	Externa - Microsoft SQL Server Memoria = 16 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 32 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 48 GB Unidades vCPU = 16

MPX-XenMobile con clústeres (3)

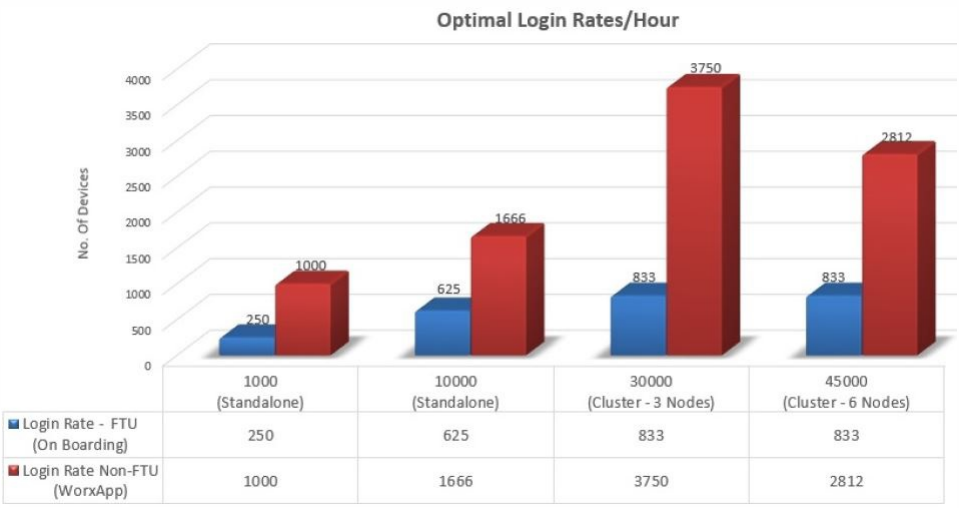
Clúster
Clúster
Clúster
Clúster
8 GB de RAM y 4 CPU virtuales
8 GB de RAM y 4 CPU virtuales

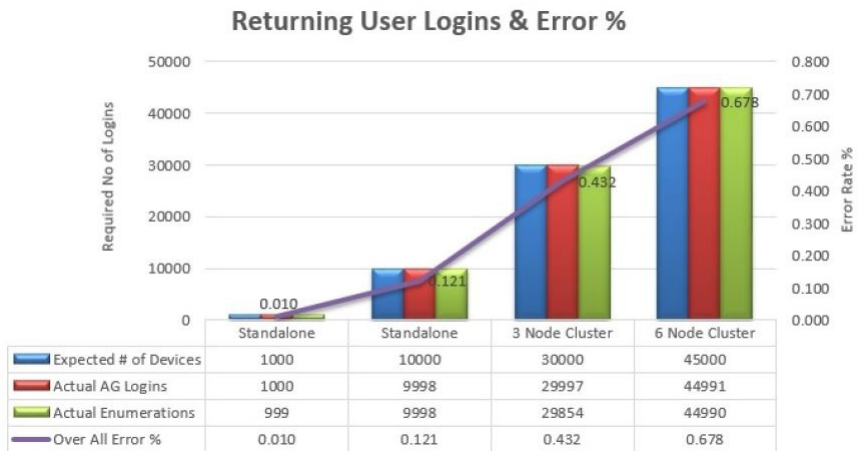
* Las implementaciones en modo autónomo no se recomiendan para aplicaciones que deben estar siempre disponibles para los usuarios. Citrix recomienda usar implementaciones en clúster, de alta disponibilidad, para la mayoría de los clientes.

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

La información siguiente ofrece puntos de datos adicionales que fueron registrados y que afectan a los resultados de la tabla anterior.

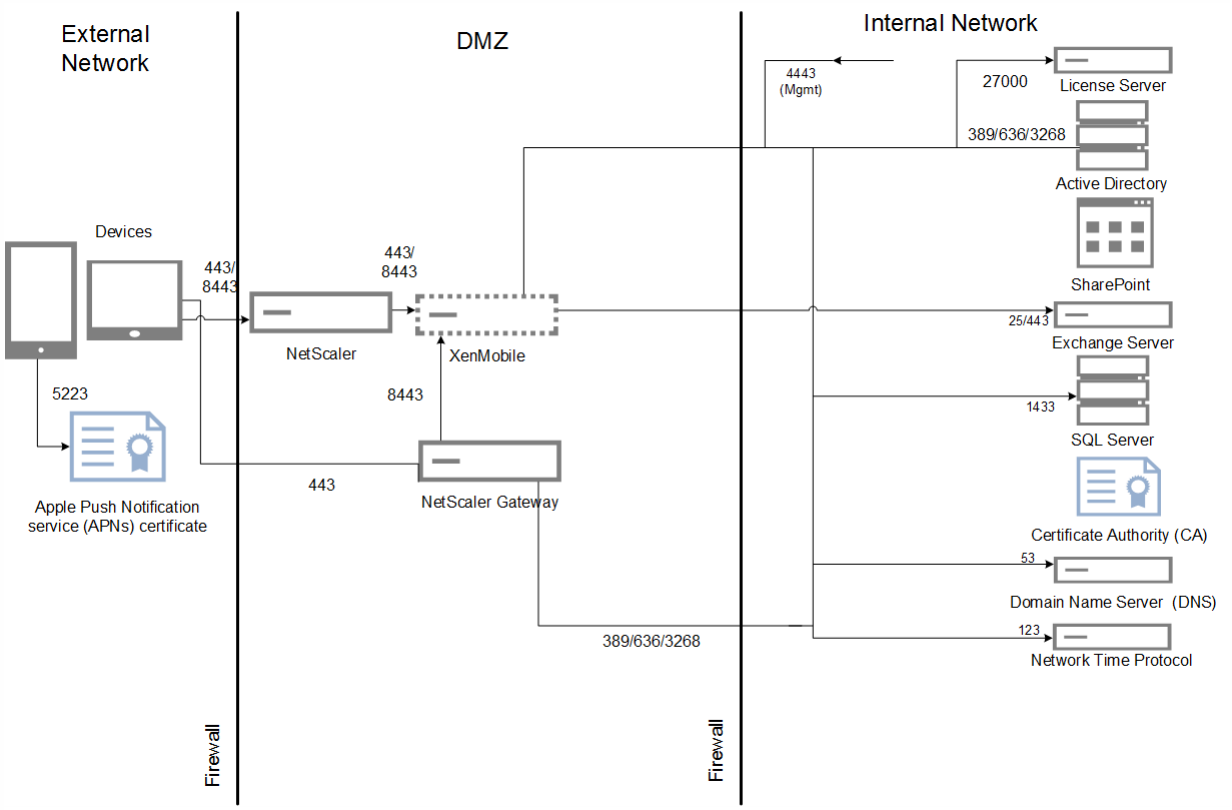
- Latencia de inscripción o de inicio de sesión (tiempo de ida y vuelta)
  - Latencia media total: de 0,5 a 1,5 segundos
  - Latencia media de un inicio de sesión de NetScaler Gateway: > 120 a 440 milisegundos
  - Latencia media de una solicitud de Worx Store: de 2 a 3 segundos
- Se ha observado una 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.
  - Respuesta lenta de la consola de XenMobile durante fases de carga alta.



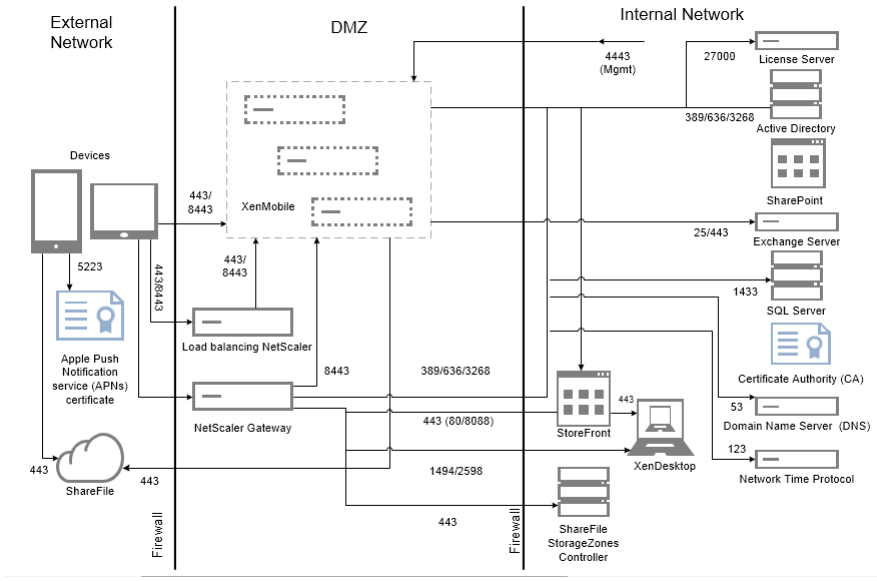


El porcentaje de error mostrado en la imagen anterior incluye errores generales obtenidos en solicitudes correspondientes a todas las operaciones, sin limitarse únicamente a los inicios de sesión. El porcentaje de error se encuentra dentro del límite aceptable del 1% para cada prueba realizada, tal y 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 MAM a través de HTTP que admite 10 000 dispositivos o más.



Las pruebas se realizaron con XenMobile Enterprise para establecer bancos de pruebas. Para ofrecer soluciones a implementaciones tanto pequeñas como grandes, se han utilizado de 1000 a 60000 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.

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

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.

Notas e hipótesis

Los casos siguientes no forman parte de las pruebas de escalabilidad. Estos casos se tendrán en cuenta para las siguientes mejoras en las pruebas de escalabilidad:

- No se ha probado la implementación de paquetes.
- No se ha probado la plataforma Windows.

En envío de directivas se ha probado para dispositivos iOS y Android.
Cada instancia de XenMobile admite un máximo de 10 000 conexiones simultáneas.

Las pruebas se realizaron en condiciones idóneas con conexión LAN para evitar problemas de latencia de red. En una situación real, la escalabilidad también depende del ancho de banda de que disponga el usuario, sobre todo para la descarga de aplicaciones.

Pruebas de reconexión

Se realizaron pruebas de reconexión por separado para Primer uso y para Usuario existente.

Las pruebas de reconexión se hicieron con un máximo de 15000 dispositivos.

La tasa de reconexión respaldada para Android es de 17 dispositivos por segundo. La tasa de reconexión respaldada para iOS es de 8 dispositivos por segundo. Para conseguirlo, el recuento de maxThread se estableció en 1000 en el archivo /opt/sas/tomcat/conf/server.xml.

TO BE ADDED: INFORMATION ON RECOMMENDED DEVICE RECONNECTION POLICIES

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 (Web, SaaS y aplicaciones MDX móviles) incluida la comprobación de estado de los dispositivos
- Envío push de directivas (para iOS)
- 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 se definen en la tabla siguiente:

Dispositivos	Registro de dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Inicios de WorxStore por dispositivo	Single Sign-On para aplicaciones Web o SaaS por dispositivo	Descargas de aplicaciones MDX por dispositivo	Descargas de aplicaciones requeridas activadas a través de XenMobile	Directivas enviadas via push por dispositivo (iOS)

1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Usuarios existentes cargas de trabajo de conexiones Worx solamente

La tabla siguiente muestra la carga de trabajo de usuarios existentes (con conexiones Worx solamente). Esta carga de trabajo simulaba un usuario que utiliza las aplicaciones WorxMail y WorxWeb. Esta simulación se utilizó para medir la escalabilidad de NetScaler Gateway en la configuración de XenMobile. Esto es posible porque al utilizar solo estas dos aplicaciones Worx, la red tiene una carga reducida. Para la aplicación WorxWeb, el usuario accede a sitios Web internos que no activan el inicio de sesión SSO en el servidor XenMobile. Las operaciones en este modo son las siguientes:

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

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

Dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Túneles VPN por dispositivo[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. La cantidad de túneles VPN corresponde a conexiones WorxMail y WorxWeb.

Los perfiles de conexión para WorxMail y WorxWeb se describen en la tabla siguiente:

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).

Estas recomendaciones se basan en perfiles de WorxMail y WorxWeb utilizados para automatizar una
carga de trabajo "media". Las modificaciones realizadas en los detalles de conexión afectan los resultados de los análisis. Por ejemplo, si se 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

Los perfiles utilizados para cada aplicación están diseñados para automatizar una carga de trabajo muy intensa. Las tablas siguientes muestran los detalles de los perfiles de WorxMail y WorxWeb.

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

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.
- El tiempo de espera de sesión de NetScaler está configurado en 60 minutos.
- Se utilizó una clave de 2048 bits en NetScaler Gateway para las transacciones SSL.

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).

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

Componente	Versión
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de datos externa	Microsoft SQL Server 2014

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

Proveedor	Genuine Intel
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).

Acerca de XenMobile Server 10.3.5

Oct 31, 2016

Se puede actualizar directamente a XenMobile 10.3.5 en la consola de XenMobile, desde las siguientes versiones:

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10.1

Para llevar a cabo la actualización, use el archivo xms_10.3.5.354.bin. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, haga clic en **Release Management**. Haga clic en **Upgrade** y cargue el archivo xms_10.3.5.354.bin. Para obtener más información acerca de actualizaciones en la consola, consulte Actualización de XenMobile.

Para completar una instalación nueva de XenMobile 10.3.5, consulte Instalación de XenMobile.

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 en XenMobile 10.3.5

XenMobile 10.3.5 ofrece soluciones de errores y las siguientes funcionalidades nuevas.

Su equipo de Cloud Services puede actualizar su implementación de XenMobile Server en la nube desde la versión 10.3 a la 10.3.5 sin interrupción de la inactividad.

Puede permitir que los usuarios de Android M habiliten o bloqueen cuatro tipos de permisos. Cuando los usuarios se inscriben en Worx Home, ven cuatro mensajes para preguntarles si quieren permitir o denegar a Worx Home los siguientes permisos:

- Acceso a la información de dispositivo para que Worx Home funcione correctamente.
- Capacidad para crear y administrar llamadas de teléfono.
- Obtener acceso a fotos, archivos multimedia y otros archivos en el dispositivo.
- Acceso a la ubicación geográfica del dispositivo.

Con esta versión, puede permitir que los usuarios de iOS vuelvan a autenticarse en Worx Home y en las aplicaciones Worx mediante Touch ID. Para dispositivos iOS 8 e iOS 9, cuando el inicio de sesión Single Sign-on está habilitado para Worx Home y Touch ID está habilitado en el dispositivo, esta combinación reemplaza al uso del PIN. Los usuarios aún tendrán que introducir un PIN cuando se requiera la autenticación en línea a través de NetScaler Gateway. Esto es necesario en los siguientes casos:

- La sesión del usuario ha caducado.
- El usuario reinicia el dispositivo.
- Worx Home no se está ejecutando y el usuario lo inicia, o inicia una aplicación MDX.

Ahora puede crear perfiles de inscripción para dispositivos iOS y Android en la nueva página **Configure > Enrollment Profiles** de la consola de XenMobile. Un perfil de inscripción se aplica a todos los modos del servidor. Puede crear varios perfiles de inscripción y asociarlos con diferentes grupos de entrega.

Nota: La página **Enrollment Profiles** no se aplica a dispositivos Windows. Para obtener información sobre la inscripción de dispositivos Windows, consulte Dispositivos Windows.

Anteriormente se establecía el límite de dispositivos por usuario mediante la propiedad del servidor **Number of Devices Per User**. Dicha propiedad del servidor está obsoleta. Ahora el límite de dispositivos se configura en la nueva página **Configure > Enrollment Profiles**. Anteriormente, se podía limitar el número de dispositivos solo para MDM. Ahora, también se puede limitar el número de dispositivos para MAM.

De forma predeterminada, la cantidad de dispositivos que un usuario puede inscribir es ilimitada. Para obtener más información, consulte Límite de inscripción de dispositivos.

XenMobile 10.3.5 ofrece soporte para hebreo y chino tradicional en Worx Store.

XenMobile 10.3.5 presenta un nuevo modo de servidor "solo MAM". Para distinguir entre el modo MAM anterior y el modo MAM nuevo, la documentación de Citrix se refiere al nuevo modo como "modo solo MAM" y se refiere al modo MAM anterior como "modo MAM antiguo". Aunque la funcionalidad del modo MAM antiguo es la misma que antes, Citrix no planea introducir mejoras en futuras versiones.

El modo solo MAM está en vigor cuando la propiedad Server Mode de XenMobile tiene el valor **MAM**. Los dispositivos se registran en el modo MAM.

La funcionalidad MAM antigua está en vigor cuando la propiedad Server Mode de XenMobile tiene el valor **ENT** y los usuarios eligen no usar administración de dispositivos. Los dispositivos se registran en el modo MDM+MAM. En el modo MDM+MAM, los usuarios que optaron por no usar la administración MDM siguen recibiendo la funcionalidad de la administración MAM antigua independientemente de si se actualiza a XenMobile 10.3.5 o no.

Nota: Anteriormente, la configuración de la propiedad Server Mode con el valor **MAM** tenía el mismo efecto que configurarla con el valor **ENT**: los dispositivos se registraban en el modo MDM+MAM y los usuarios que decidían no usar la administración MDM recibían la funcionalidad MAM antigua.

Entre las ventajas del modo solo MAM está el cifrado adicional (no solo el código de acceso del dispositivo), la red VPN móvil y una mayor privacidad del usuario final, lo que hace que el modo solo MAM sea muy adecuado para dispositivos BYOD (Bring Your Own Device).

Si el servidor XenMobile se encuentra en el modo MAM, se puede actualizar al modo solo MAM para aprovechar las ventajas de las siguientes funciones que antes solo estaban disponibles en MDM. Estas funciones no están disponibles para

Windows Phone.

- **Autenticación basada en certificados**
  El modo solo MAM respalda la autenticación con certificados. Los usuarios tienen acceso continuo a sus aplicaciones, incluso cuando su contraseña de Active Directory ha caducado .Si decide cambiar a una autenticación basada en certificados para dispositivos MAM, debe configurar NetScaler Gateway. De manera predeterminada, en XenMobile, el valor del parámetro **Settings > NetScaler Gateway**, **Deliver user certificate for authentication** es **Off**, lo que significa que se usa autenticación con nombre de usuario y contraseña. Para habilitar la autenticación con certificados es necesario cambiarlo por el valor **On**.
- **Self Help Portal**, para permitir a los usuarios lleven a cabo por si mismos las acciones de bloqueo y borrado de aplicaciones (App Lock y App Wipe). Estas acciones tienen efecto en todas las aplicaciones del dispositivo. Puede configurar las acciones App Lock y App Wipe en **Configure > Actions**.
- **Todos los modos de inscripción**, incluidos: High Security, Invitation URL y Two Factor configurados mediante **Manage > Enrollment**.
- **Límite de registro de dispositivos** para dispositivos Android e iOS. La propiedad de servidor **Number of Devices Per User** se ha movido a la nueva página **Configure > Enrollment Profiles** y ahora también se aplica al nuevo modo solo MAM.
- **API del modo solo MAM** Para dispositivos solo MAM, puede invocar los servicios REST usando cualquier cliente REST y la API de REST de XenMobile para llamar a los servicios expuestos mediante la consola de XenMobile.
- Las API de solo MAM disponibles en esta versión permiten:
  - Enviar una URL de invitación y un PIN de un solo uso
  - Emitir acciones de bloqueo y borrado de aplicaciones en los dispositivos

> ### Important
>
> Para usar el nuevo modo solo MAM, debe configurar XenMobile como se describe en el artículo y los usuarios deben volver a inscribir sus dispositivos. Asegúrese de proporcionar a los usuarios el nombre de dominio completo (FQDN) del servidor de XenMobile que necesitarán para la inscripción.
>
> En el nuevo modo solo MAM, al igual que en el modo ENT, los dispositivos se inscriben mediante el nombre FQDN de XenMobile. (En el modo MAM antiguo, los dispositivos se inscriben mediante el nombre FQDN de NetScaler Gateway).

Cómo afecta esta actualización a los dispositivos ya inscritos

La siguiente tabla resume cómo afectan las nuevas funciones a los dispositivos inscritos en XenMobile 10.3.5.

Para los dispositivos inscritos actualmente como:	XenMobile 10.3.5 ofrece	Tareas de administrador	Tareas de usuario
MDM • Modo de servidor =	• Problemas resueltos • Funciones nuevas	Instale XenMobile 10.3.5	Ninguna

MDM			
MDM+MAM • Modo de servidor = ENT • Los usuarios optaron por la administración del dispositivo	• Problemas resueltos • Funciones nuevas	Instale XenMobile 10.3.5	Ninguna.
MAM • Modo de servidor = ENT • Los usuarios rechazaron la administración del dispositivo	• Problemas resueltos • Funciones nuevas Nota: En este caso, los dispositivos se inscriben en el modo MAM antiguo. Si desea proporcionar a esos usuarios la nueva funcionalidad de MAM, configure un nuevo servidor XenMobile para ellos.	Instale XenMobile 10.3.5	Ninguna.
MAM • Modo de servidor = MAM	• Problemas resueltos • Funciones nuevas • Actualización optativa al nuevo modo solo MAM	Para continuar usando la funcionalidad de MAM antigua: Instale XenMobile 10.3.5	Ninguno.
		Para actualizar al modo solo MAM: 1. Instale XenMobile 10.3.5 2. Consulte la Vista general de la configuración del modo solo MAM, a continuación, para ver información sobre la configuración adicional requerida.	Reinscriba los dispositivos

Vista general de la configuración del modo solo MAM

El *modo solo MAM* hace referencia al modo de servidor MAM cuando se usa con licencias Enterprise o Advanced. El modo solo MAM es diferente del *modo MAM + MDM*, que se usa cuando el servidor XenMobile está en modo de servidor ENT. En el modo MDM + MAM, los usuarios que optaron por no aceptar la administración de MDM reciben las funciones antiguas de MAM independientemente de si se actualiza a XenMobile 10.3.5.

Important

La administración MAM antigua funciona igual que en las versiones anteriores y no se desarrollarán mejoras para ella en futuras versiones.

La siguiente tabla resume la configuración de modo de servidor que debe usarse para el determinado tipo de licencia y modo de dispositivo que se desee:

Tiene licencias para esta edición	Quiere que los dispositivos se registren en este modo	Defina la propiedad Server Mode con el valor
ENT / ADV / MDM	Modo MDM	MDM
ENT / ADV	Modo MAM (también llamado "modo solo MAM")	MAM
ENT / ADV	Modo MDM+MAM	ENT Los usuarios que deciden no participar en la administración de dispositivos funcionarán bajo el modo MAM antiguo.

Debe configurar el modo solo MAM *únicamente* si:

- Su servidor XenMobile tiene actualmente el parámetro **Server Mode** definido con **MAM** y si quiere cambiar al nuevo modo solo MAM para utilizar las funciones nuevas.
- Si desea configurar un servidor XenMobile para proporcionar la funcionalidad de solo MAM a todos los usuarios que se conecten con ese servidor.

Los pasos de configuración general para el modo solo MAM son los siguientes:

1. Instale o actualice a XenMobile 10.3.5.
2. En la página **Manage > Devices**, compruebe el valor de **Server Mode**. Si **Server Mode** tiene el valor **MDM** o **ENT**, no realice los pasos descritos en este procedimiento, porque al hacerlo la configuración resultante no admitirá la administración de dispositivos.
3. Abra los puertos 8443 y 443 en el servidor XenMobile y el firewall hacia Internet de forma que los dispositivos puedan conectarse directamente al servidor XenMobile. La inscripción debe tener lugar en el servidor XenMobile.
4. Si está actualizando un servidor, donde **Server Mode** tiene el valor **MAM**, vaya al paso siguiente. Si está realizando una instalación nueva de XenMobile 10.3.5, el servidor XenMobile tendrá el parámetro **Server Mode** configurado como **ENT** de manera predeterminada. Para habilitar el modo solo MAM, debe establecer la propiedad del servidor **Server Mode** con el valor **MAM**. Para obtener más información, consulte Configuración del modo de servidor solo MAM.
5. Si quiere usar la autenticación basada en certificados, configure XenMobile y NetScaler Gateway para dar respaldo a la autenticación con certificados. De manera predeterminada, en XenMobile, el valor del parámetro **Settings > NetScaler**

Gateway, **Deliver user certificate for authentication** es **Off**, lo que significa que se usa autenticación con nombre de usuario y contraseña. Debe cambiar este parámetro a **On**. Para ver información detallada de la configuración, consulte Configuración del modo de servidor solo MAM.

6. Al seleccionar o configurar una plantilla de notificaciones para usarla con el modo solo MAM, tenga en cuenta que SMTP es el único método respaldado para enviar invitaciones de inscripción.
7. Si va actualizar a los usuarios al nuevo modo solo MAM, tiene que darles el nombre de dominio completo (FQDN) del servidor XenMobile y pedirles que vuelvan a inscribirse.
   En el nuevo modo solo MAM, al igual que en el modo ENT, los dispositivos se inscriben mediante el nombre FQDN de XenMobile. (En el modo MAM antiguo, los dispositivos se inscriben mediante el nombre FQDN de NetScaler Gateway).

La siguiente tabla resume las diferencias entre la funcionalidad antigua de MAM (XenMobile 10.3 y XenMobile 10.3.5) y el nuevo modo solo MAM (XenMobile 10.3.5).

Escenarios de inscripción y otras características	XenMobile 10.3 MAM antiguo (modo de servidor = ENT)	XenMobile 10.3.5 MAM antiguo (modo de servidor = ENT)	XenMobile 10.3.5 Modo solo MAM (modo de servidor = MAM)
Autenticación con certificados	No respaldado.	No respaldado.	Respaldado. Para usar la autenticación con certificados, es necesario usar NetScaler Gateway.
Requisito de implementación	No es necesario que los dispositivos puedan acceder directamente al servidor XenMobile.	No es necesario que los dispositivos puedan acceder directamente al servidor XenMobile.	El servidor XenMobile debe ser accesible para los dispositivos.
Opción de inscripción	Usar el nombre de dominio completo (FQDN) de NetScaler Gateway u optar por no inscribirse.	Usar el nombre de dominio completo (FQDN) de NetScaler Gateway u optar por no inscribirse.	Usar el nombre de dominio completo (FQDN) del servidor XenMobile.
Métodos de inscripción	Nombre de usuario y contraseña	Nombre de usuario y contraseña	Nombre de usuario y contraseña; Alta seguridad; URL de invitación; URL de invitación y PIN, URL de invitación y contraseña, Dos factores, Nombre de usuario y PIN
Bloqueo y borrado de aplicaciones	Respaldado.	Respaldado.	Respaldado.
Opciones de Self Help Portal para			

el borrado y bloqueo de aplicaciones	No respaldado.	No respaldado.	Respaldado.
Comportamiento del borrado de aplicaciones	Las aplicaciones permanecen en el dispositivo, pero no se pueden usar. La cuenta se elimina solo en el cliente.	Las aplicaciones permanecen en el dispositivo, pero no se pueden usar. La cuenta se elimina solo en el cliente.	Las aplicaciones permanecen en el dispositivo, pero no se pueden usar. La cuenta se elimina solo en el cliente.
Acciones automatizadas para usuarios del modo solo MAM.	No respaldado.	Se respaldan las acciones de evento, propiedad de dispositivo y propiedad de usuario. No se respaldan acciones automatizadas en aplicaciones instaladas.	Se respaldan las acciones de evento, propiedad de dispositivo y propiedad de usuario. No se respaldan acciones automatizadas en aplicaciones instaladas.
Acción integrada cuando se elimina un usuario de AD	No respaldado.	Se respalda el borrado de aplicaciones.	Se respalda el borrado de aplicaciones.
Límite de inscripción	Solo se respalda en el modo MDM; configurado en una propiedad de servidor.	Respaldado; configurado en un perfil de inscripción.	Respaldado; configurado en un perfil de inscripción.
Inventario de software	Respaldado; XenMobile enumera las aplicaciones instaladas en un dispositivo	Respaldado; XenMobile enumera las aplicaciones instaladas en un dispositivo	No respaldado.

En una implementación de solo MAM de XenMobile, se puede implementar un clúster de servidores XenMobile en la zona desmilitarizada (DMZ) o dentro de la propia red interna. En cada caso, la autenticación se realiza a través de NetScaler Gateway.

Tenga en cuenta que, a diferencia de una implementación de XenMobile Enterprise, no es necesario usar XenMobile NetScaler Connector (XNC) ni XenMobile Mail Manager (XMM).

Para ver diagramas de referencia de arquitectura, consulte el artículo Reference Architecture for On-Premises Deployments

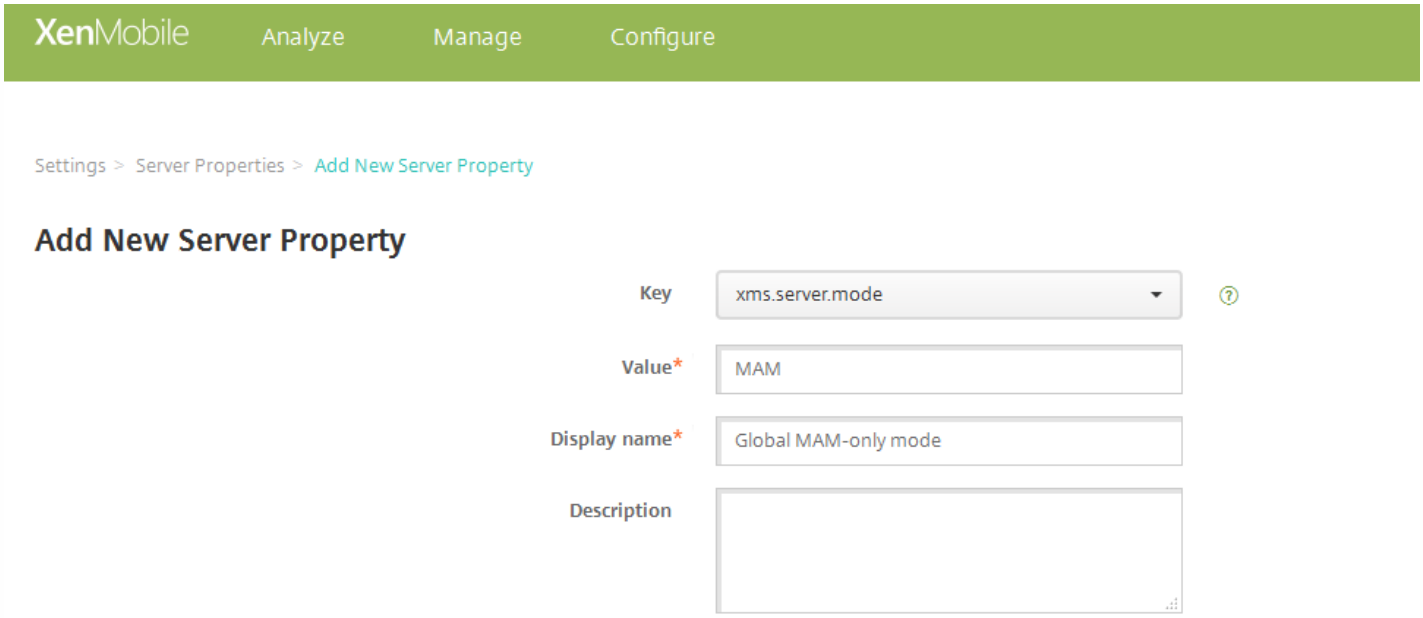
de XenMobile Deployment Handbook.

- Las aplicaciones necesarias no se instalan automáticamente. Los usuarios deben agregarlas manualmente desde Worx Store.
- Los usuarios de iOS deben confiar en el certificado de desarrollador de iOS. Los usuarios de Android deben habilitar la configuración para que se puedan instalar desde tiendas de aplicaciones de terceros.
- Los usuarios reciben notificaciones sobre actualizaciones de aplicaciones únicamente en Worx Store.
- Cuando un usuario quita Worx Home o se desinscribe de Worx Home, las aplicaciones instaladas permanecen en el dispositivo hasta que el usuario las elimina.
- El modo MAM solamente no respalda APN ni Google Cloud Messaging.
- La consola de XenMobile no incluye el estado "liberado por jailbreak o por rooting" de los dispositivos inscritos en el modo solo MAM, sin embargo, la directiva **Block jailbroken or rooted devices** funciona para esos dispositivos.

Después de una instalación nueva, el servidor está en modo de ENT de forma predeterminada. Para habilitar el modo solo MAM para XenMobile 10.3.5, configure el servidor como se indica a continuación:

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola para abrir la página **Settings**.
2. En la página **Settings**, haga clic en **Server Properties**.
3. Haga clic en **Agregar**.
4. En **Key**, haga clic en **xms.server.mode**.
5. En **Value**, introduzca **MAM**.
6. En **Display name**, introduzca una descripción para que aparezca en la tabla **Server Properties**.

Si quiere, escriba una descripción y, a continuación, haga clic en **Save**.



Important

Después de establecer la propiedad xms.server.mode con el valor solo MAM, la consola de XenMobile sigue mostrando secciones aplicables al modo MDM, como las propiedades de dispositivo. No obstante, esos parámetros no funcionarán.

Autenticación con certificados para el modo solo MAM

Jul 27, 2016

Para usar la autenticación con certificados en el modo solo MAM, debe configurar el servidor Microsoft, el servidor XenMobile y el servidor NetScaler Gateway. En este artículo se describen los siguientes pasos generales.

En el servidor Microsoft:

1. Agregue el complemento de Certificados a la consola MMC (Microsoft Management Console).
2. Agregue la plantilla a la entidad de certificación (CA).
3. Cree un certificado PFX desde el servidor de CA.

En el servidor XenMobile:

1. Cargue el certificado en XenMobile.
2. Cree una entidad PKI para la autenticación basada en certificados.
3. Configure proveedores de credenciales.
4. Configure NetScaler Gateway para entregar un certificado de usuario para la autenticación.

En NetScaler Gateway:

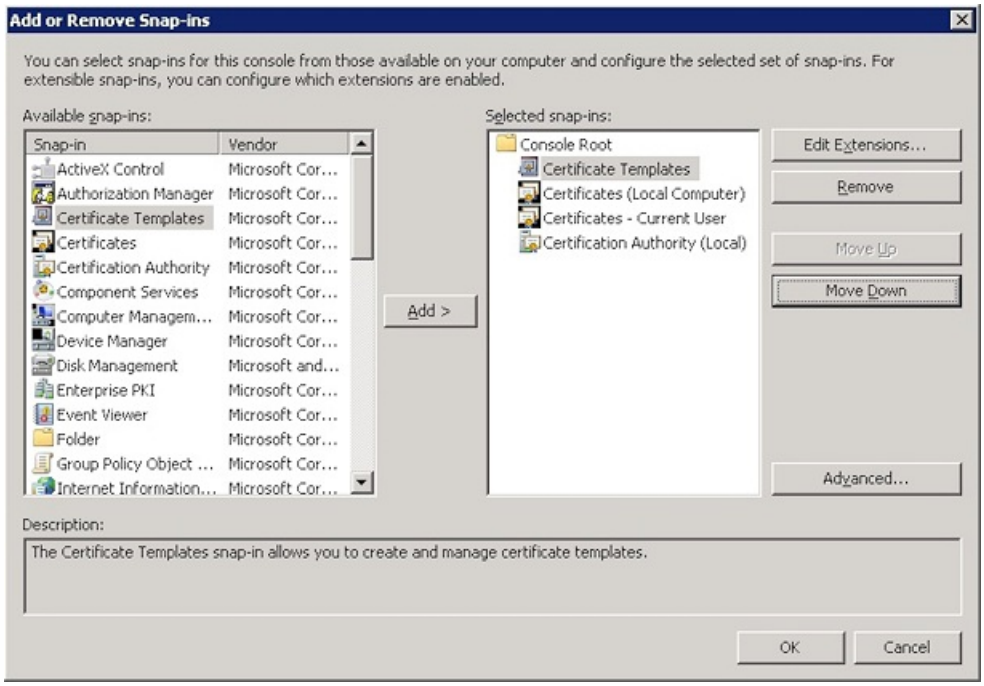
1. Configure NetScaler Gateway para la autenticación con certificados de XenMobile en modo solo MAM

Para agregar el complemento de Certificados a la consola MMC (Microsoft Management Console)

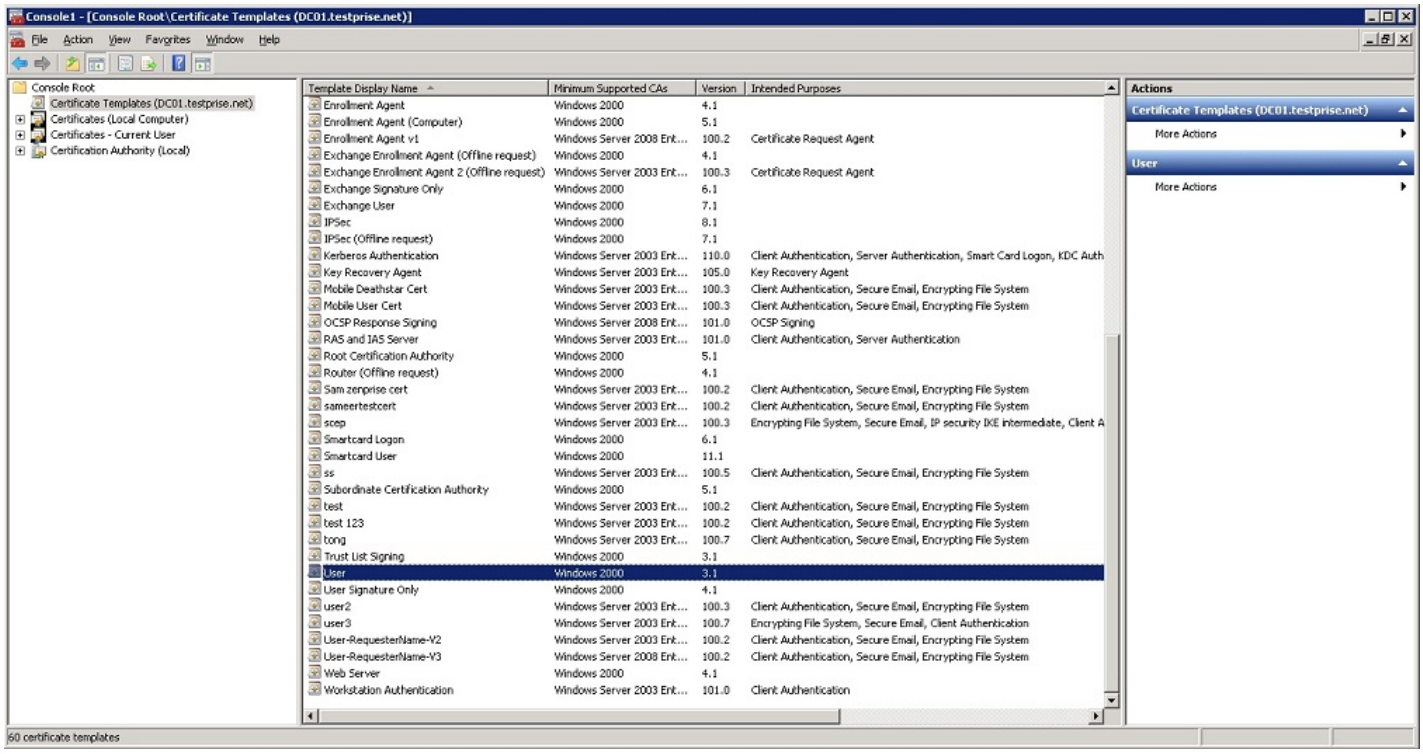
1. Abra la consola MMC y luego haga clic en **Agregar o quitar complemento**.

2. Agregue los complementos siguientes:

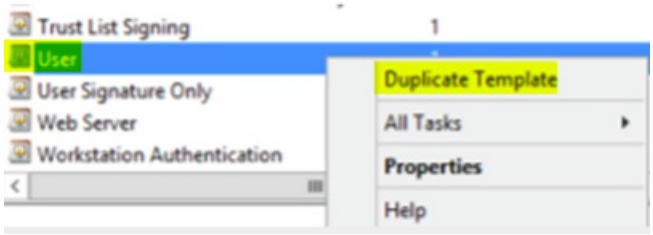
    Plantillas de certificado
    Certificados (Equipo local)
    Certificados (Usuario local)
    Entidad de certificación (Local)



3. Expanda **Plantillas de certificado**.



4. Seleccione la plantilla **Usuario** y **Plantilla duplicada**.

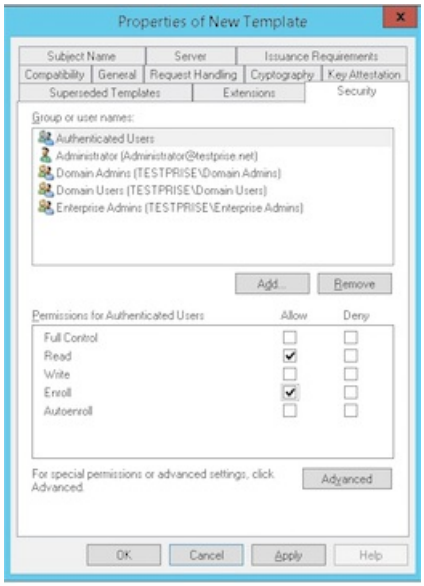


5. Suministre el nombre para mostrar de la plantilla.

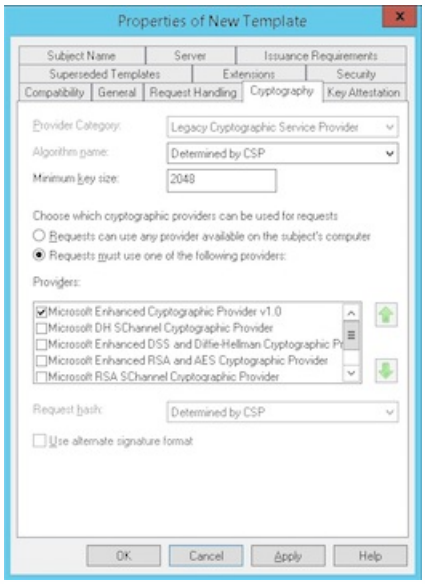
> **Importante:** No marque la casilla **Publicar certificado en Active Directory** a menos que sea necesario. Si se selecciona esta opción, todos los certificado de cliente de los usuarios se insertarán/crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

6. Seleccione Windows 2003 Server como tipo de plantilla. En Windows 2012 R2 Server, bajo **Compatibilidad**, seleccione **Entidad de certificación** y defina Windows 2003 como destinatario.

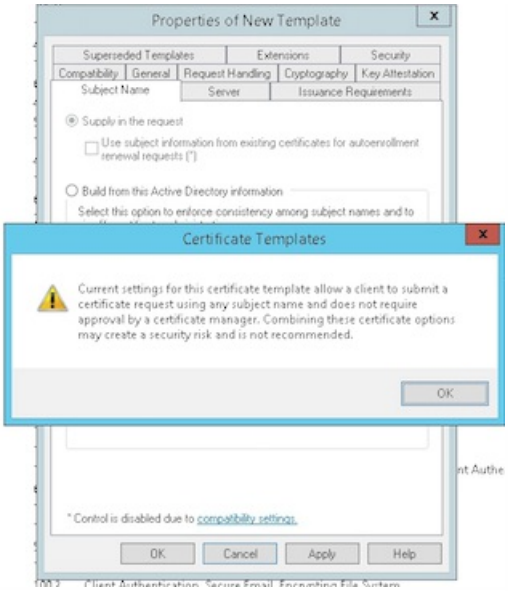
7. En **Seguridad**, seleccione la opción **Inscribir** en la columna **Permitir** para los usuarios autenticados.



8. En **Criptografía**, asegúrese de suministrar el tamaño de la clave, ya que necesitará introducirlo durante la configuración de XenMobile.



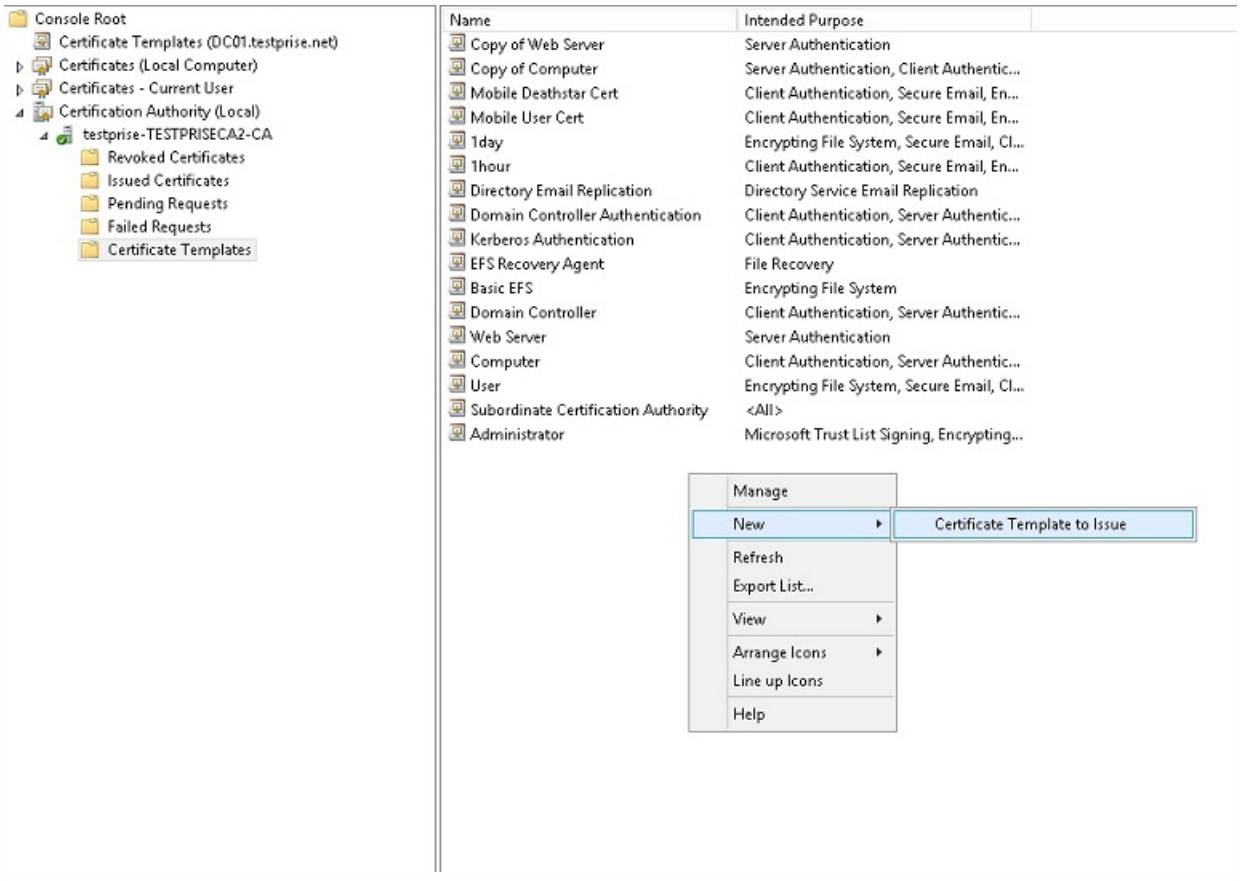
9. En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.



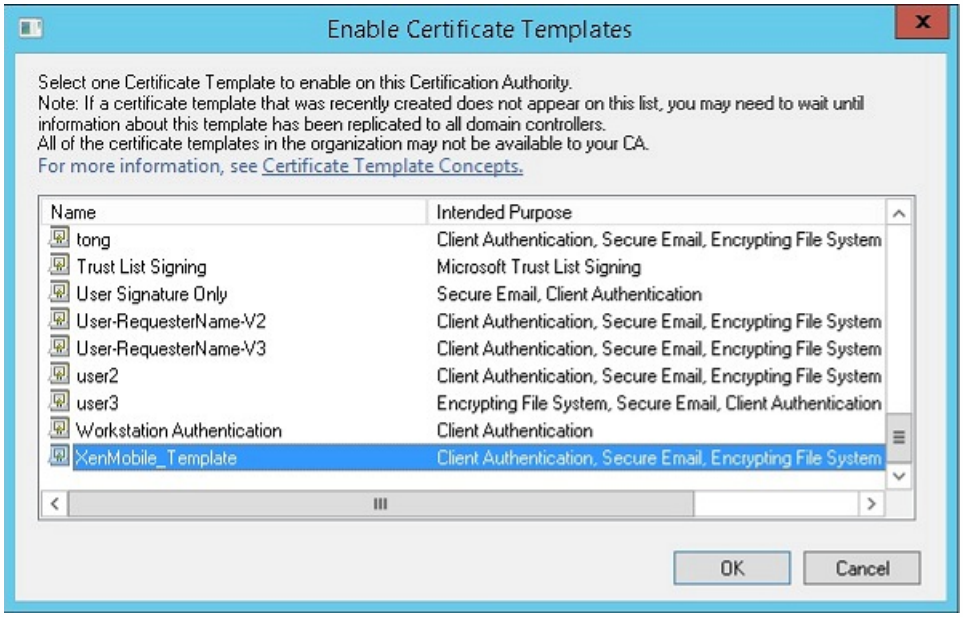
Para agregar la plantilla a la entidad de certificación

1. Vaya a **Entidad de certificación** y seleccione **Plantillas de certificado**.

2. Haga clic con el botón secundario en el panel derecho y luego seleccione **Nueva > Plantilla de certificado que se va a emitir**.



3. Seleccione la plantilla que creó en el paso anterior y luego haga clic en **Aceptar** para agregarla a la entidad de certificación.

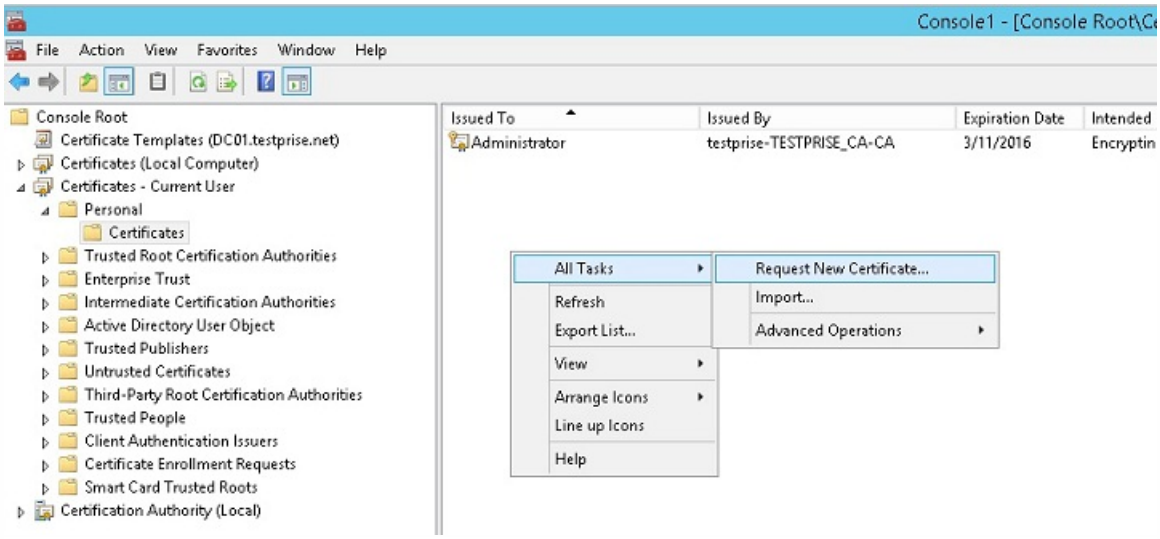


Para crear un certificado PFX desde el servidor de CA

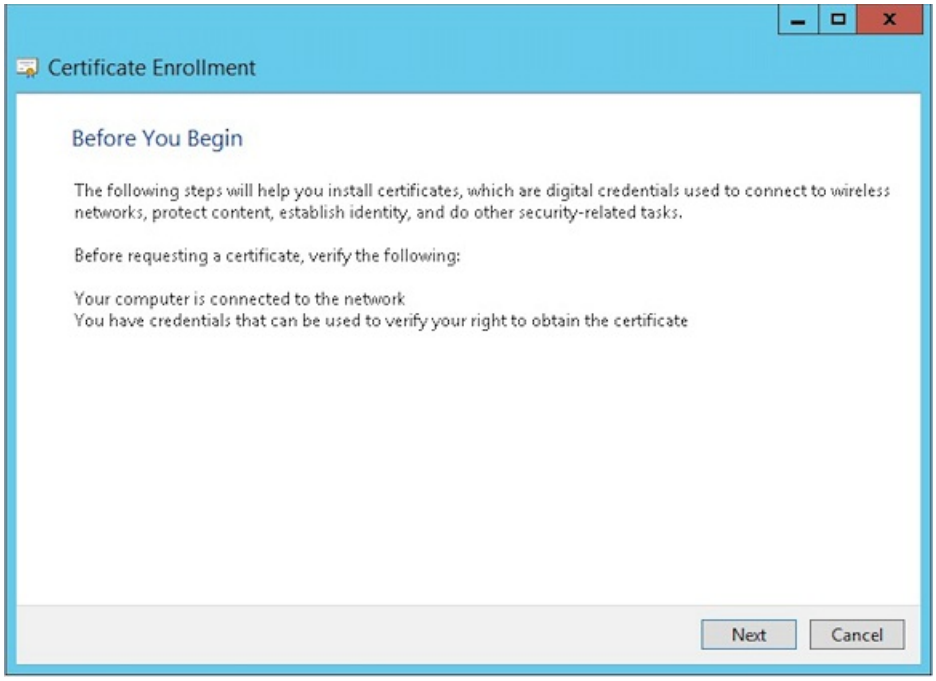
1. Cree un certificado .pfx de usuario usando la cuenta de servicio con la que inició sesión. Este .pfx se cargará en XenMobile, lo que solicitará un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.

2. En **Usuario actual**, expanda **Certificados**.

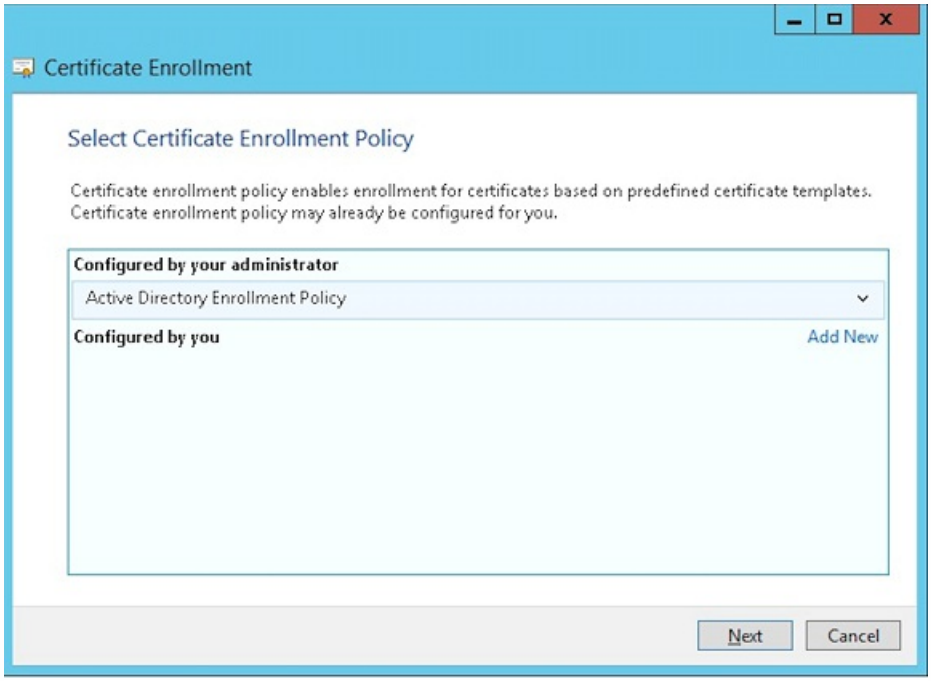
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



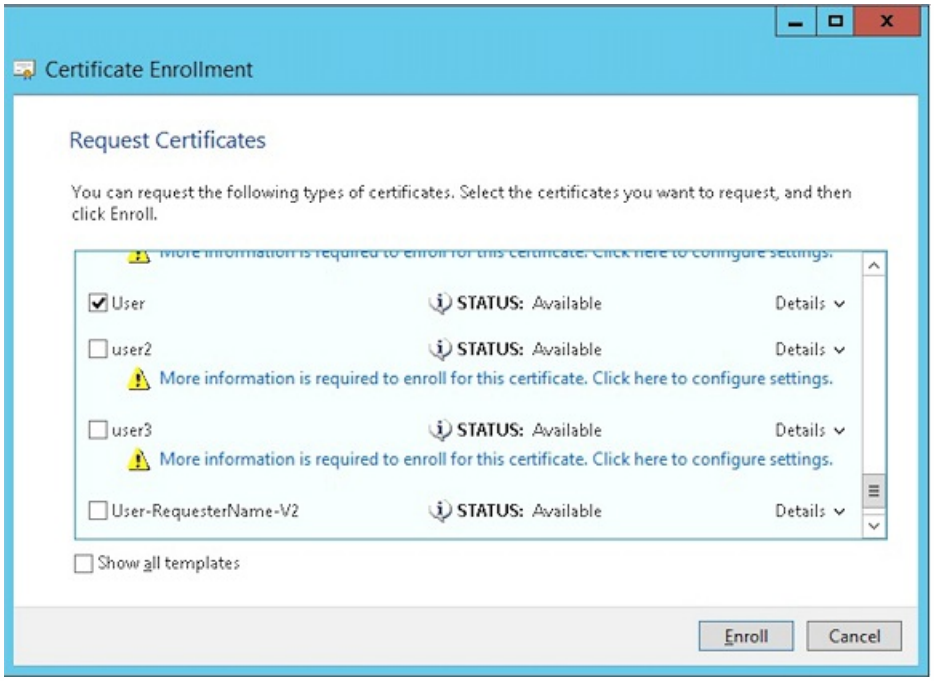
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Siguiente**.



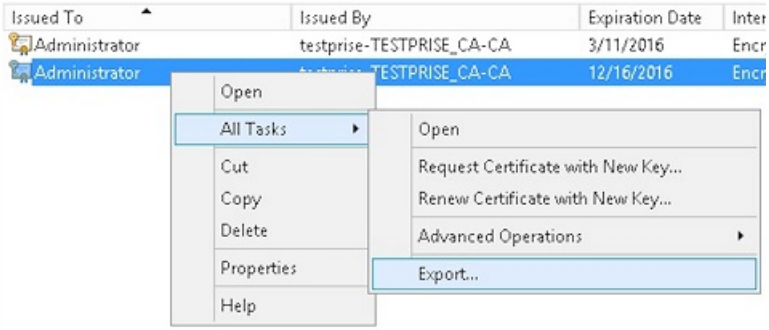
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



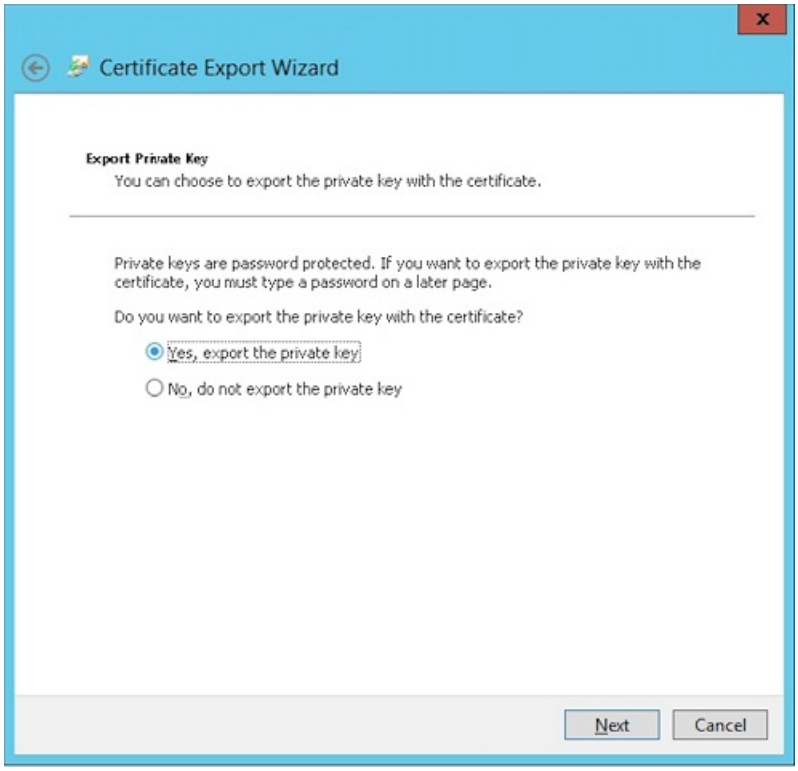
6. Seleccione la plantilla de **Usuario** y haga clic en **Inscribir**.



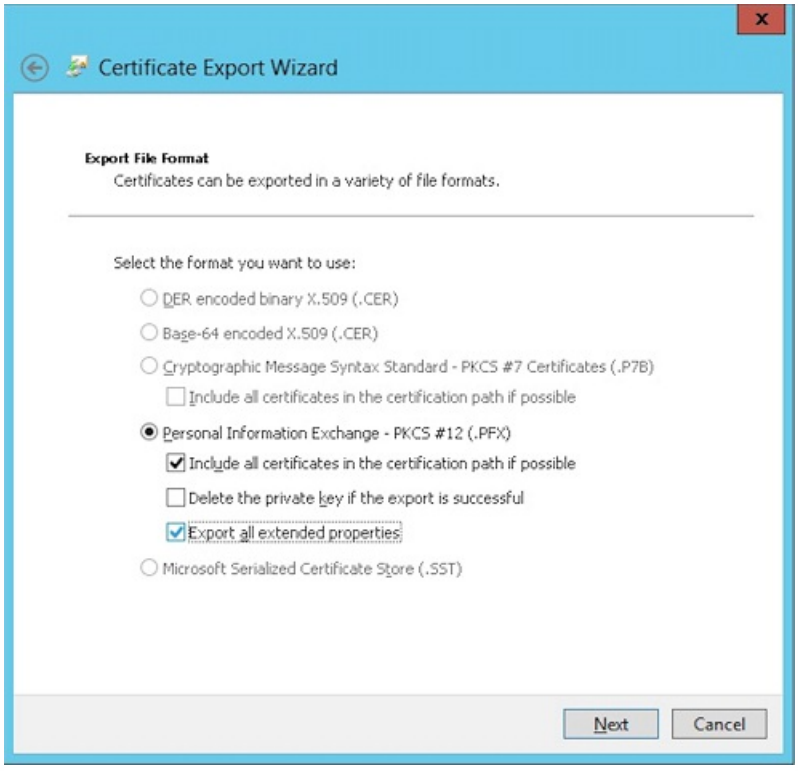
7. Exporte el archivo .pfx que creó en el paso anterior.



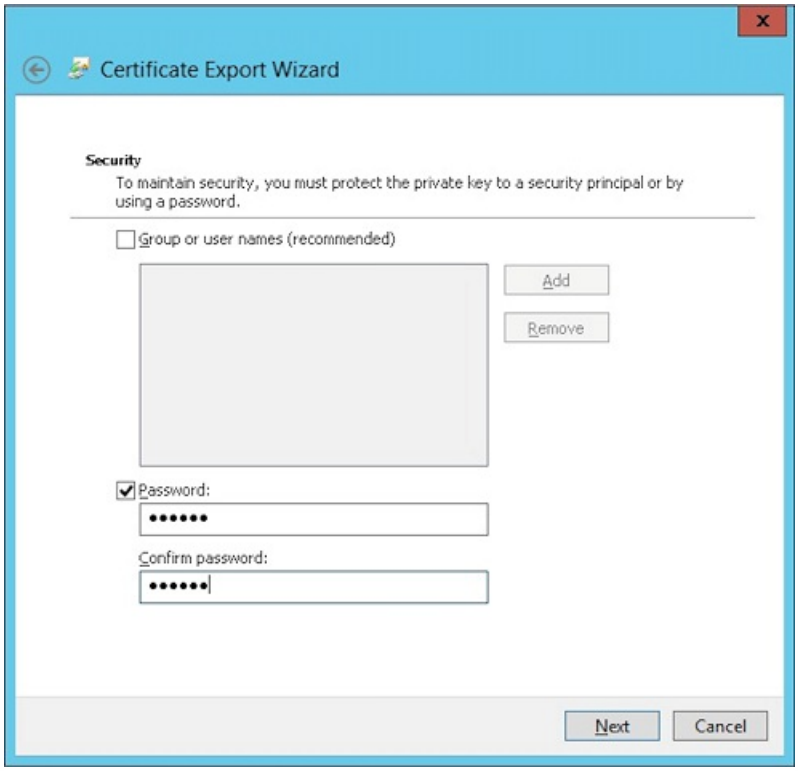
8. Haga clic en **Exportar la clave privada**.



9. Marque las casillas **Si es posible, incluir todos los certificados en la ruta de acceso de certificación** y **Exportar todas las propiedades extendidas**.



10. Defina una contraseña para usarla cuando cargue este certificado en XenMobile.



11. Guarde el certificado en su disco duro.

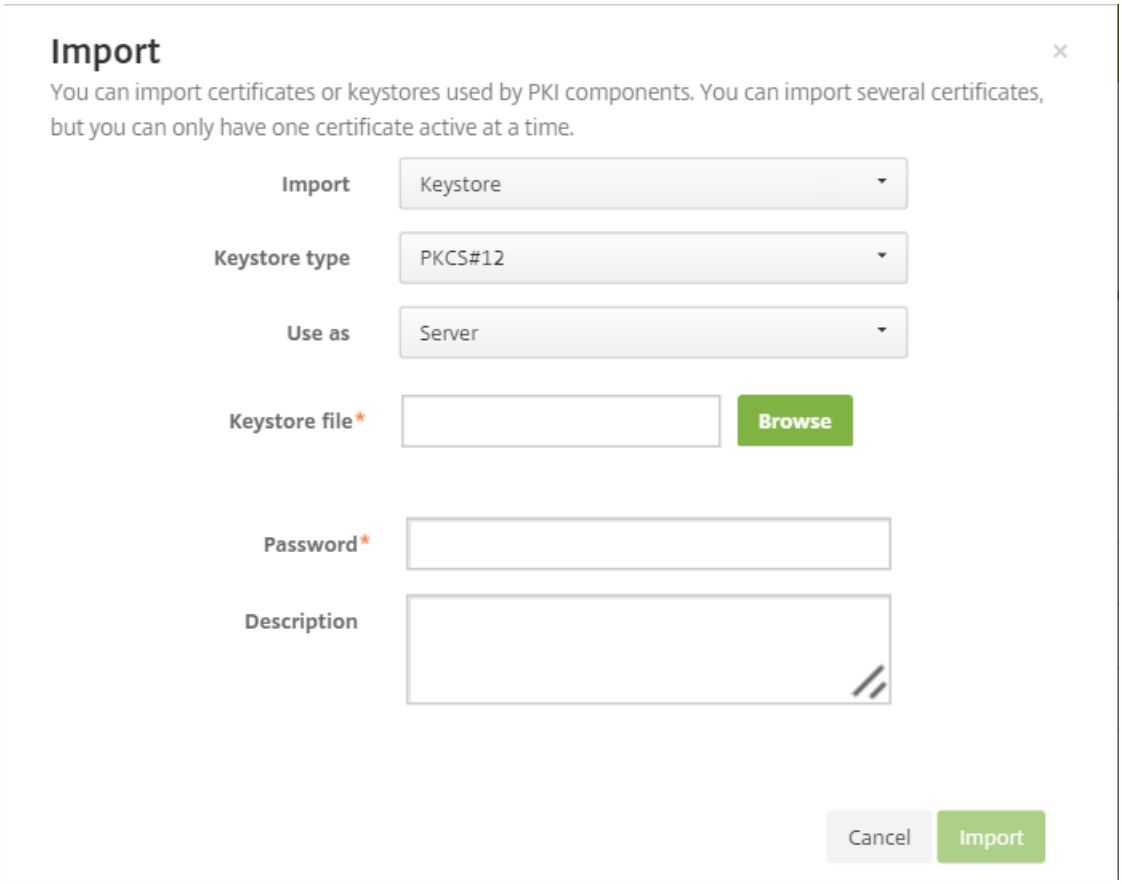
Para cargar el certificado en XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Settings**.

2. Haga clic en **Certificates** y después en **Import**.

3. Introduzca los parámetros siguientes:

- **Import**: Keystore
- **Keystore type**: PKCS#12
- **Use as**: Server
- **Keystore file**: Haga clic en **Browse** para seleccionar el certificado .pfx que acaba de crear.
- **Password**: Introduzca la contraseña que creó para este certificado.



5. Haga clic en **Import**.

6. Verifique que el certificado se instaló correctamente. Debe aparecer como User certificate.

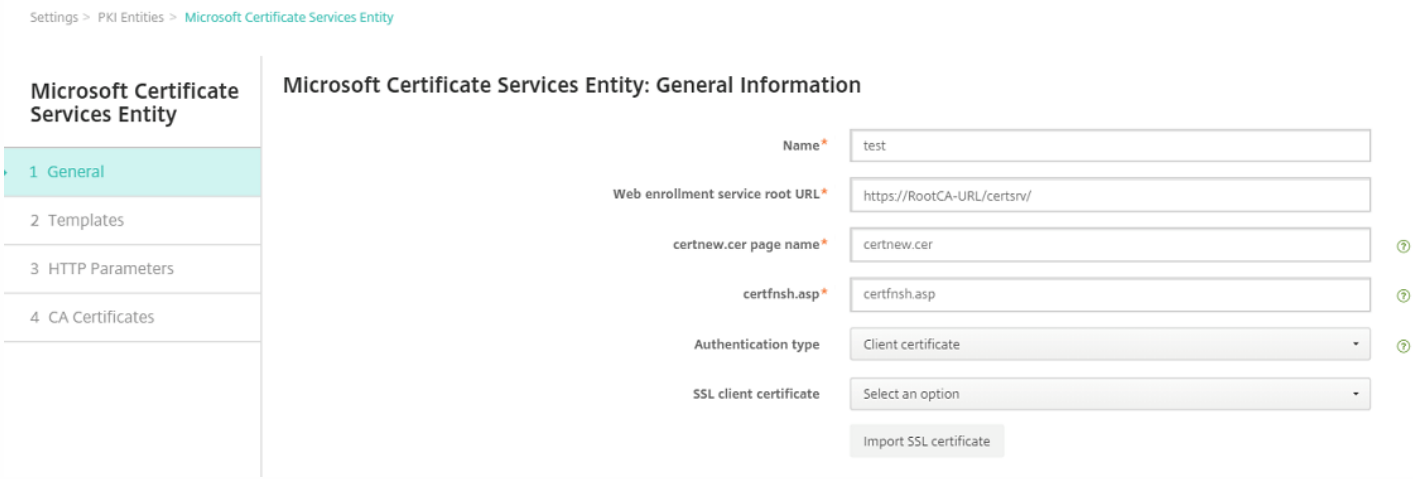
Para crear la entidad PKI para la autenticación basada en certificados

1. En **Configuración**, vaya a **Más > Administración de certificados > Entidades PKI**.

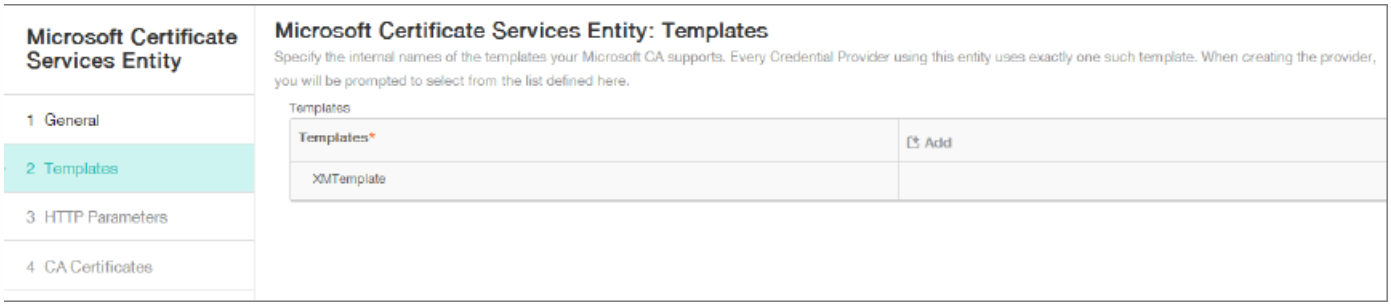
2. Haga clic en **Add** y después haga clic en **Microsoft Certificate Services Entity**. Aparece la pantalla Microsoft Certificate Services Entity: General Information.

3. Introduzca los parámetros siguientes:

- **Name**: Introduzca algún nombre
- **Web enrollment service root URL**: https://RootCA-URL/certsrv/
  Nota: Asegúrese de incluir la barra (/) al final de la ruta URL.
- **certnew.cer page name**: certnew.cer (valor predeterminado)
- **certfnsh.asp**: certfnsh.asp (valor predeterminado)
- **Authentication type**: Certificado de cliente.
- **SSL client certificate**: Seleccione la entidad raíz (RootCA) que firmó el certificado del cliente de XenMobile.

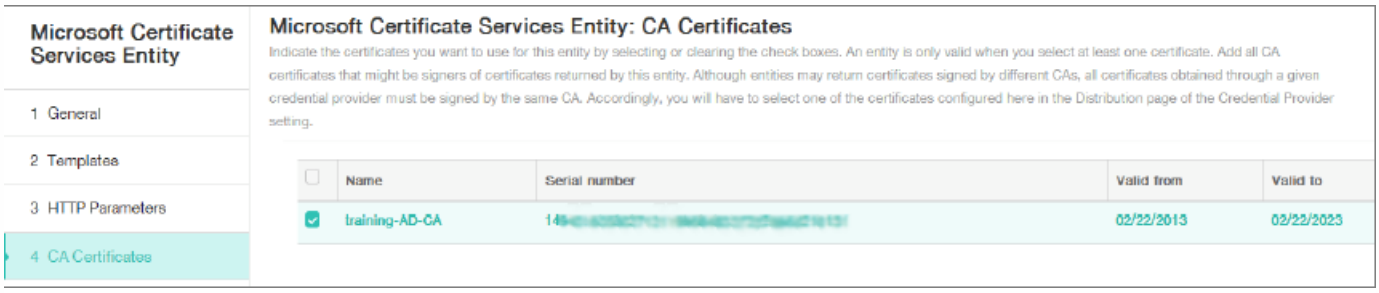


4. Bajo **Templates**, agregue la plantilla que creó cuando configuró el certificado de Microsoft. Asegúrese de no agregar espacios.



5. Omita el paso de HTTP Parameters y haga clic en **CA Certificates**.

6. Seleccione el certificado de usuario que se va a usar para emitir el certificado de cliente de XenMobile. Esto es parte de la cadena importada desde el certificado cliente de XenMobile.



7. Haga clic en **Save**.

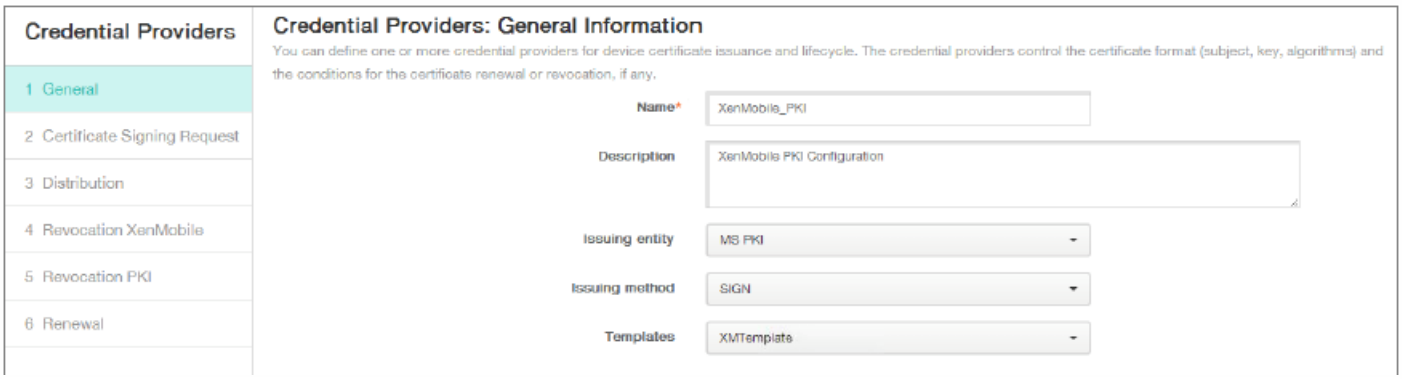
Para configurar proveedores de credenciales

1. En Settings, vaya a **More > Certificate Management > Credential Providers**.

2. Haga clic en **Add**.

3. En **General**, introduzca los parámetros siguientes:

- **Name**: Introduzca algún nombre.
- **Description**: Introduzca alguna descripción.
- **Issuing entity**: Seleccione la entidad PKI creada anteriormente.
- **Issuing method**: SIGN
- **Templates**: Seleccione la plantilla agregada bajo la entidad PKI.



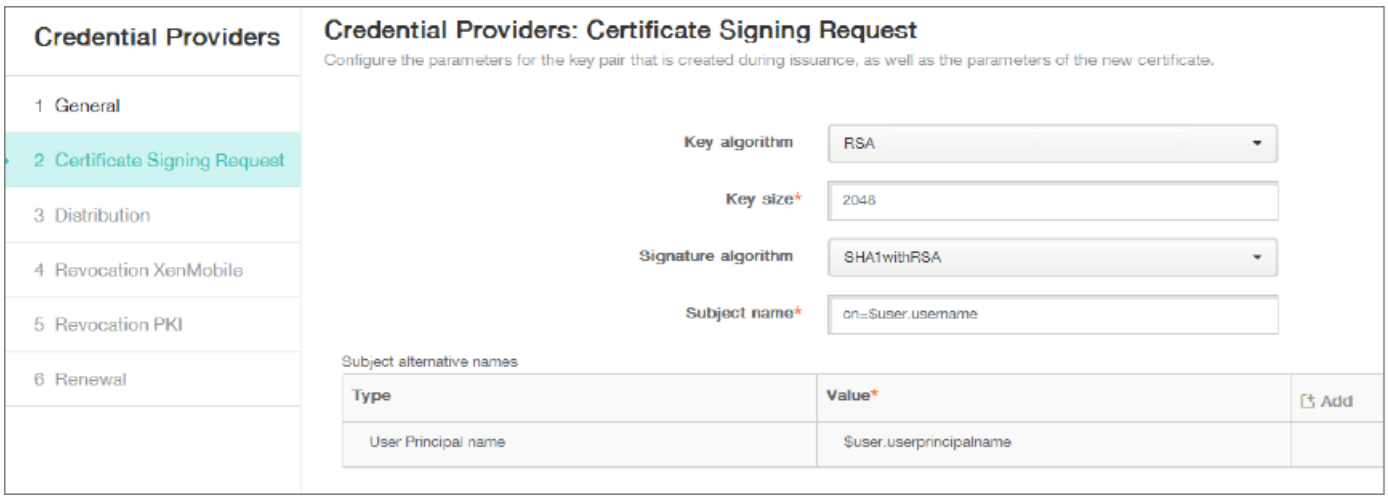
4. A continuación, haga clic en **Certificate Signing Request** e introduzca los parámetros siguientes:

- **Key algorithm**: RSA
- **Key size**: 2048
- **Signature algorithm**: SHA1withRSA
- **Subject name**: cn=$user.username

  El nombre de sujeto hace referencia al sAMAccountName. Esto permite que el dispositivo NetScaler use el campo de nombre de usuario (User Name) para la autenticación.

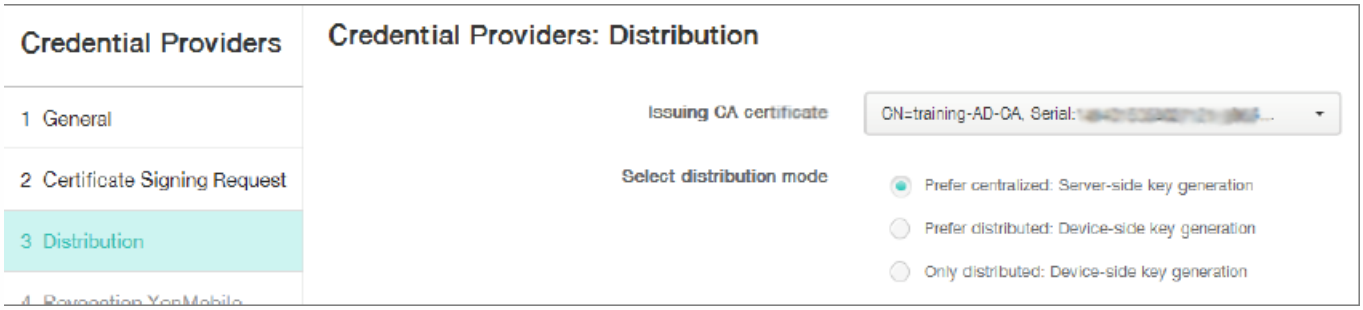
5. Para **Subject Alternative Names**, haga clic en **Add** y luego introduzca los parámetros siguientes:

- **Type**: User Principal name
- **Value**: $user.userprincipalname



6. Haga clic en **Distribution** e introduzca los parámetros siguientes:

- **Issuing CA certificate**: Seleccione la CA emisora que firmó el certificado del cliente de XenMobile.
- **Select distribution mode**: Seleccione **Prefer centralized: Server-side key generation**.

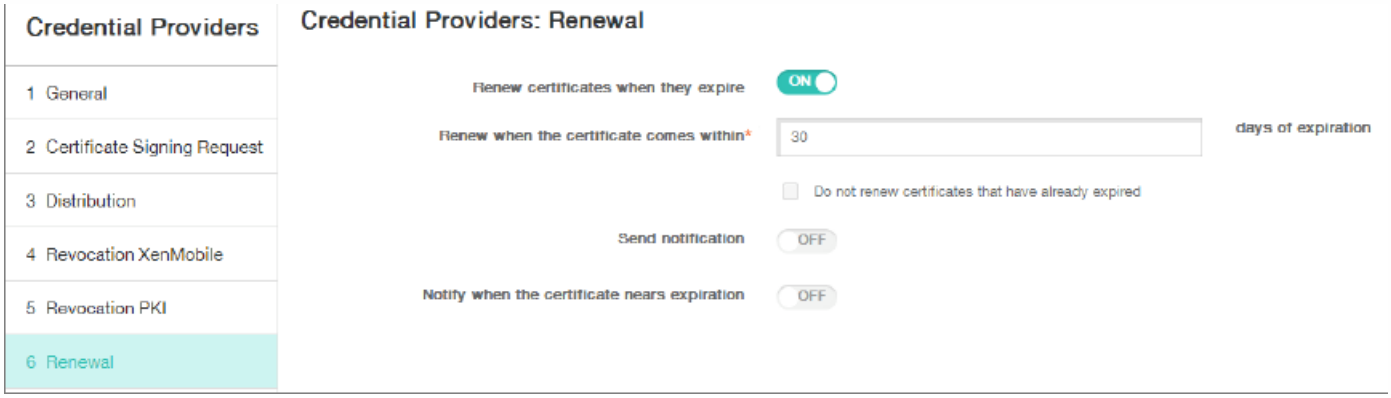


7. Para las dos secciones siguientes (**Revocation XenMobile** y **Revocation PKI**), defina los parámetros como sea necesario. Para el objetivo de este artículo, se omiten ambas opciones.

8. Haga clic en **Renewal**.

9. Para **Renew certificates when they expire**, seleccione **ON**.

10. Deje todos los demás parámetros con los valores predeterminados o cámbielos si es necesario.



11. Haga clic en **Save**.

Para configurar la entrega de certificados de NetScaler en XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Settings**.

2. En **Server**, haga clic en **NetScaler Gateway**.

3. Si NetScaler Gateway aún no fue agregado, haga clic en **Add** y especifique los parámetros:

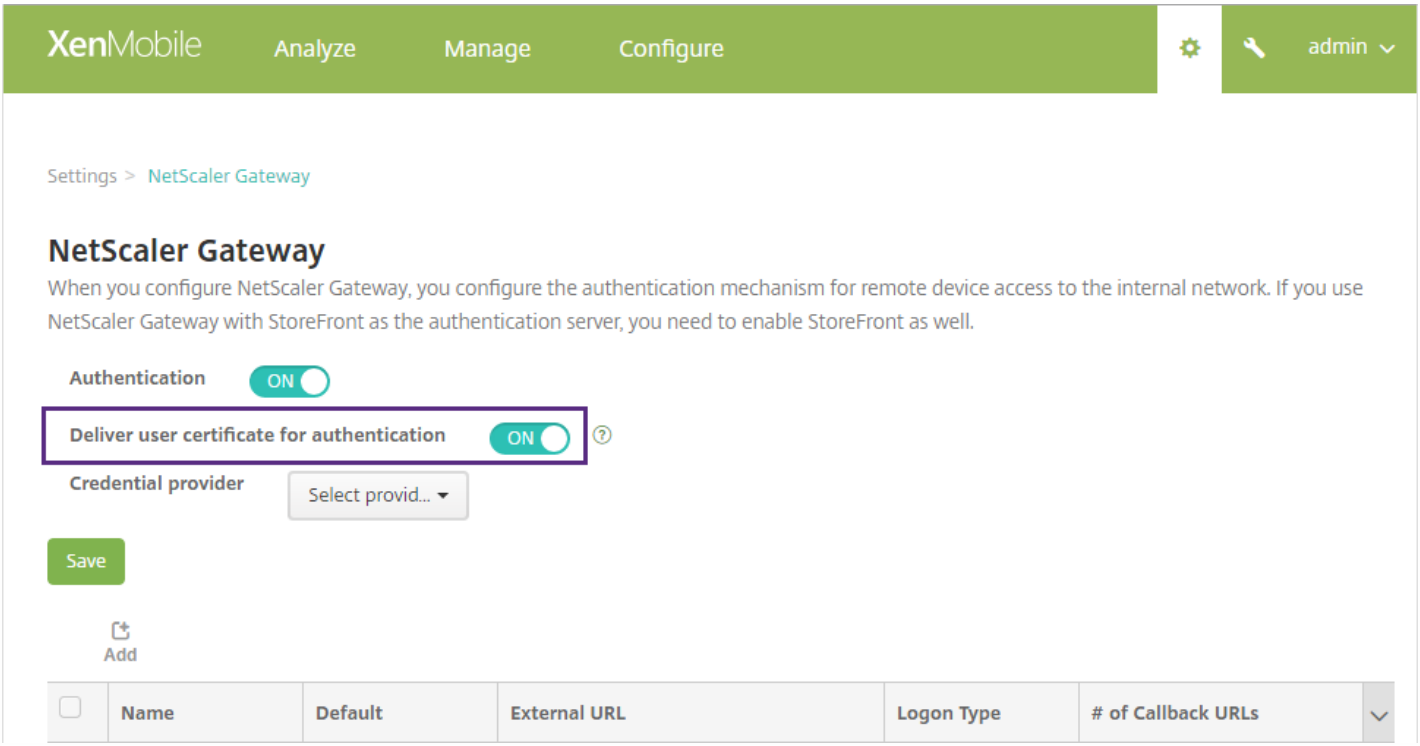
External URL: https://URLdelNetScalerGateway

Logon Type: Certificate

Password Required: OFF

Set as Default: ON

4. En **Deliver user certificate for authentication**, seleccione **On** y después haga clic en **Save**.



5. Para **Credential Provider**, seleccione un proveedor y haga clic en **Save**.

Para configurar NetScaler Gateway para la autenticación con certificados

Siga estos pasos en el dispositivo NetScaler para configurar la autenticación de certificado de XenMobile en modo MAM solamente.

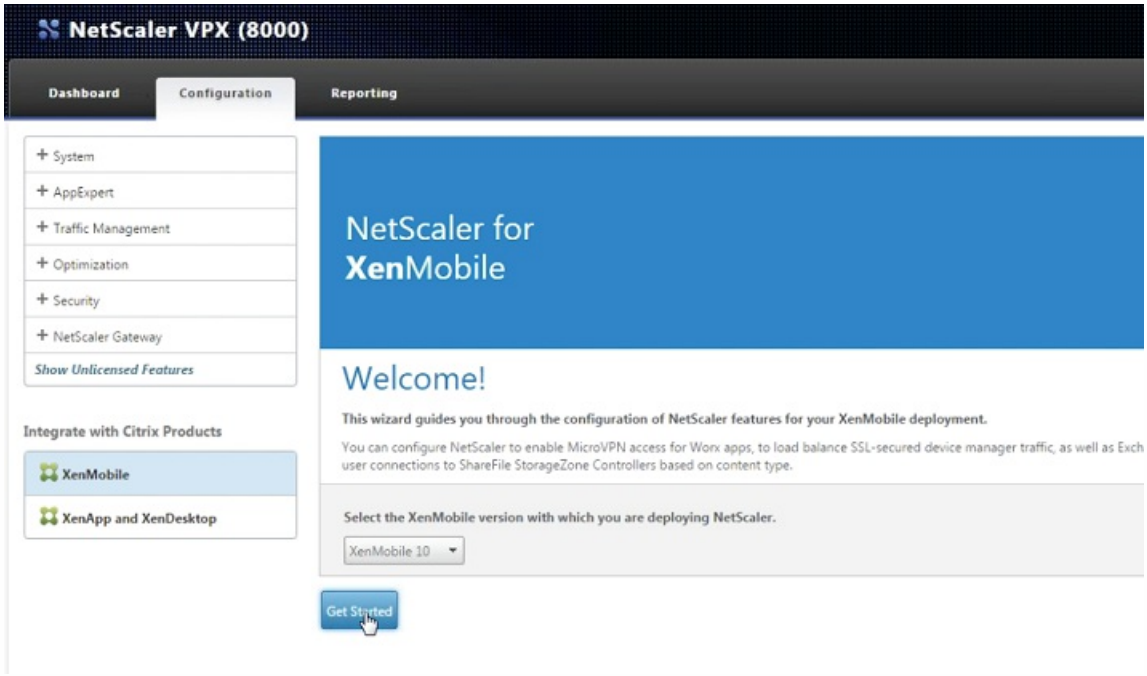
1. Inicie sesión en NetScaler.

2. Para ello, en **Configuration**, vaya a **Integrate with Citrix Products** y, a continuación, seleccione **XenMobile**.

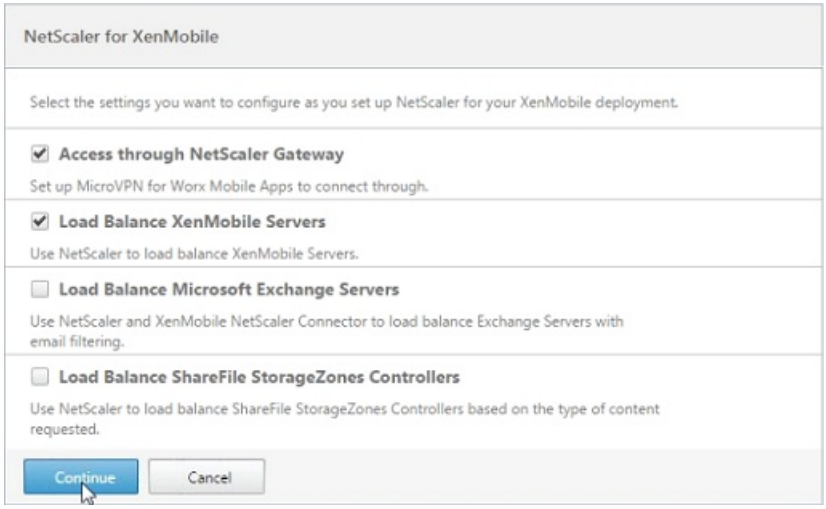
   Se abrirá un asistente para configurar las funcionalidades de NetScaler para la implementación de XenMobile.

3. Elija **XenMobile 10**.

4. Haga clic en **Get Started**.



5. En la siguiente pantalla, seleccione **Access through NetScaler Gateway** y **Load Balance XenMobile Servers** y, a continuación, haga clic en **Continue**.



6. En la siguiente pantalla, escriba la dirección IP de NetScaler Gateway externa y, a continuación, haga clic en **Continue**.

   Aparecerá la pantalla Server Certificate de NetScaler Gateway.

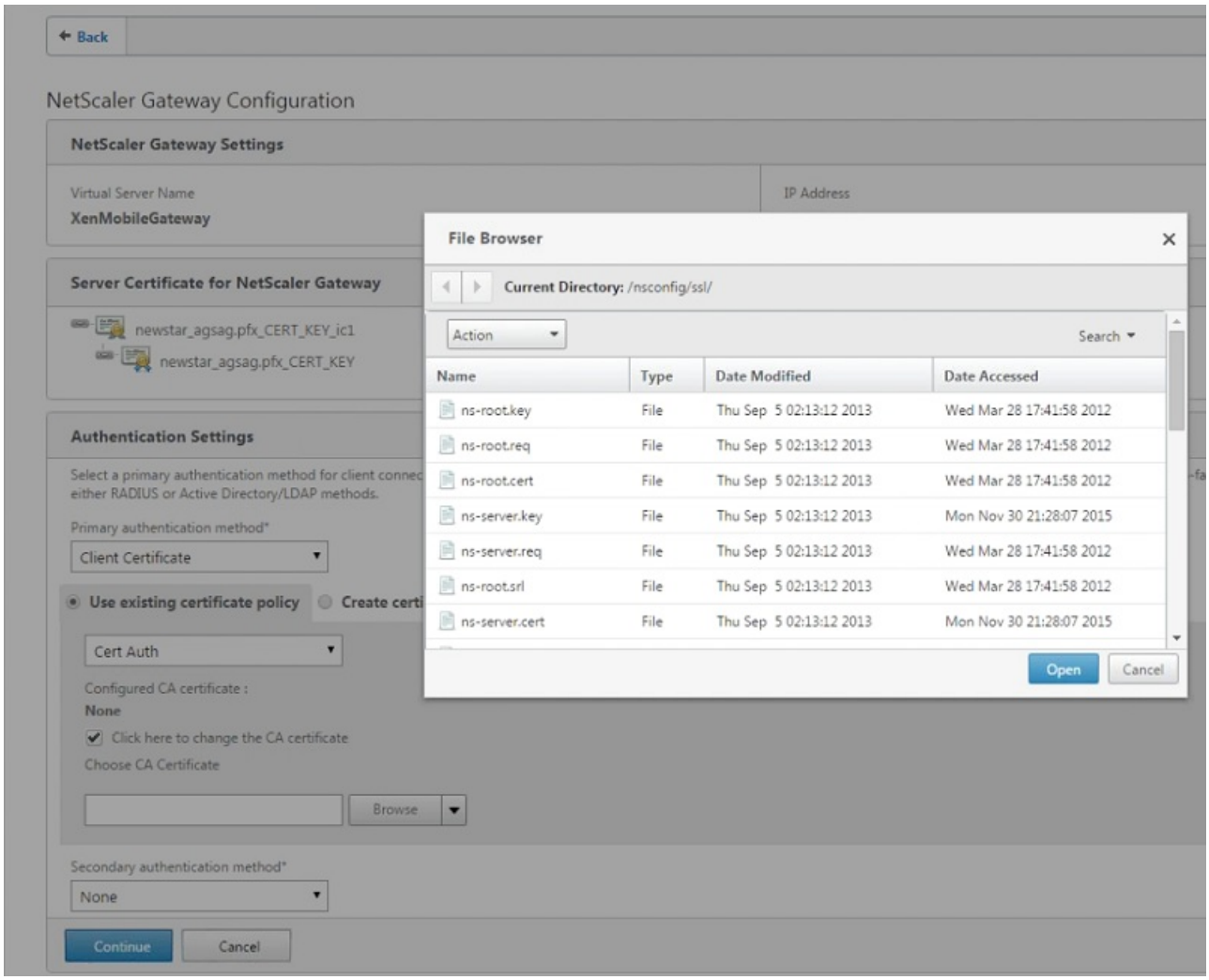
7. Debe usar un certificado existente o instalar uno. Haga clic en **Continue**.

   Aparecerá la pantalla **Authentication Settings**.

8. En el campo **Primary authentication method**, seleccione **Client Certificate**.

   Esto seleccionará automáticamente **Use existing certificate policy** y **Cert Auth** en los siguientes dos campos.

9. Seleccione **Click here to change the CA certificate** y luego, en la lista **Browse**, vaya al certificado de CA que desee.



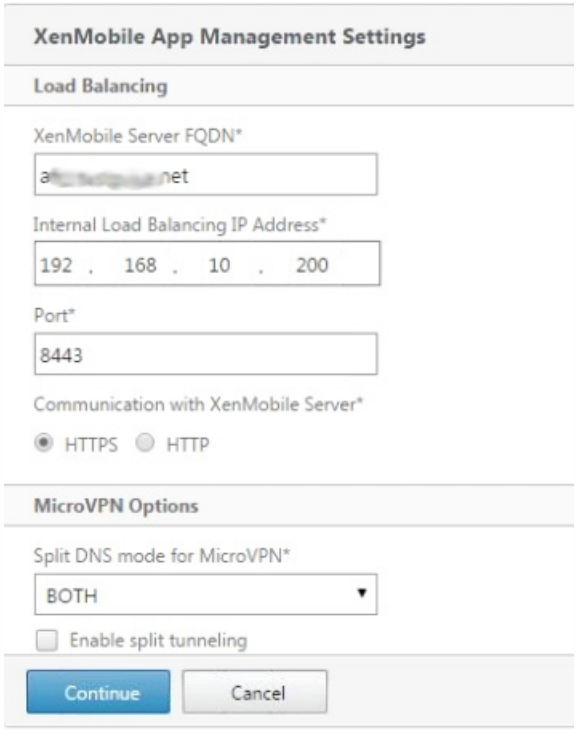
10. Mantenga **Second authentication method** como **None** y, a continuación, haga clic en **Continue**.

11. En la pantalla **Load Balancing**, especifique el nombre de dominio completo del servidor XenMobile y una dirección IP de equilibrio de carga interna de solo MAM.

12. Puesto que se trata de una implementación de descarga SSL (SSL offload), seleccione **HTTP** en **Communication with XenMobile Server**.

    El campo **Split DNS mode for MicroVPN** aparecerá como **BOTH**.

13. Haga clic en **Continue**.



14. En la pantalla **XenMobile Server Certificate**, seleccione un certificado de servidor existente o instale uno nuevo. Si ejecuta varios servidores de XenMobile, debe agregar un certificado para cada uno. Haga clic en **Continuar**.

15. En la pantalla **Device certificate**, si no se ha instalado aún, debe exportar este certificado de la consola de XenMobile. Para ello:

    a. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola para abrir la pantalla **Settings**.

    b. Haga clic en **Certificate** y, a continuación, seleccione el certificado de CA en la lista.

    c. Haga clic en **Export**.

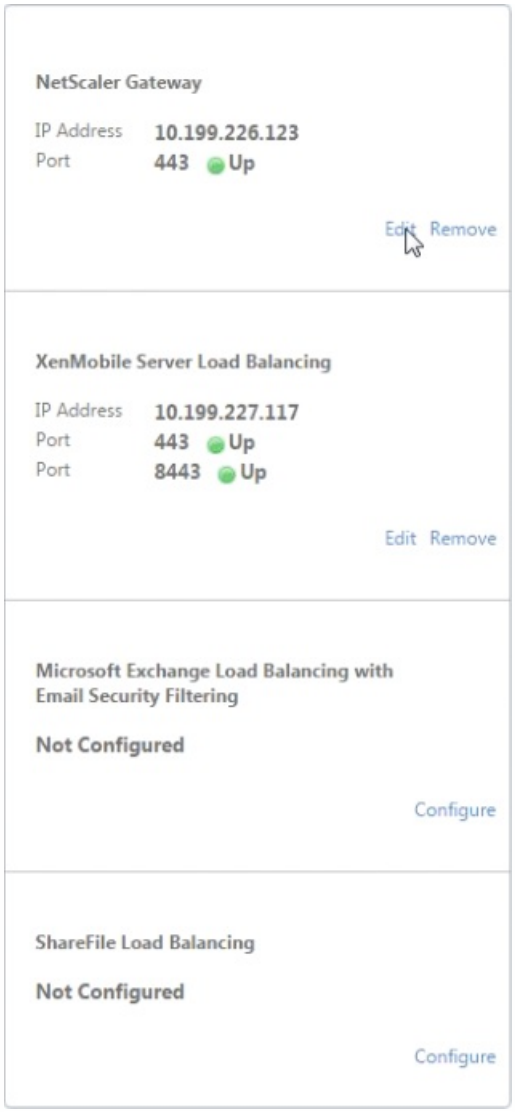
    d. Vuelva al asistente de NetScaler y seleccione el certificado que ha exportado (descargado) para instalarlo.

    e. Haga clic en **Continuar**.

Aparecerán las direcciones IP del servidor XenMobile que ha configurado.

16. Haga clic en **Continue**.

    En el panel de mandos de NetScaler, confirme que se han configurado el equilibrio de carga de XenMobile y NetScaler Gateway:



Límite de inscripción de dispositivos

Jul 27, 2016

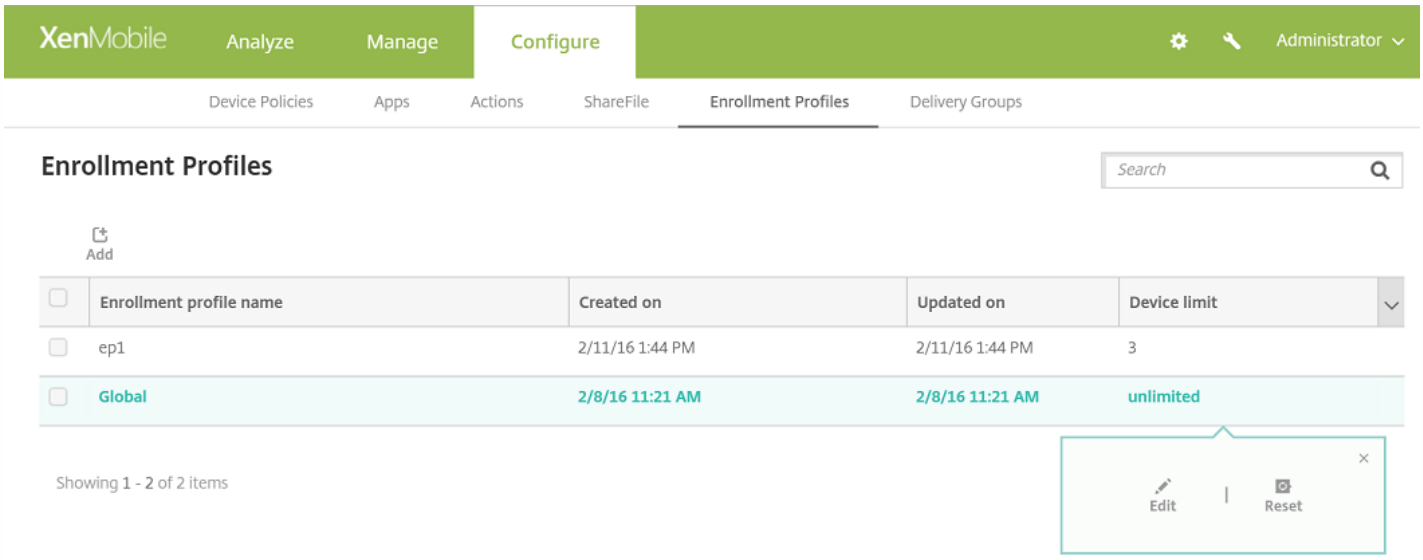
Puede limitar el número de dispositivos que un usuario puede inscribir en **Configure > Enrollment Profiles** en la consola de XenMobile, en ENT, MDM y los modos de servidor de administración de aplicaciones móviles (MAM). Las limitaciones se pueden aplicar de forma global o por grupos de entrega. Puede crear varios perfiles de inscripción y asociarlos con diferentes grupos de entrega.

Si no se configura un límite, los usuarios podrán inscribir un número ilimitado de dispositivos. Esta funcionalidad solo es compatible con dispositivos iOS y Android. Para obtener información sobre la inscripción de dispositivos Windows, consulte Dispositivos Windows.

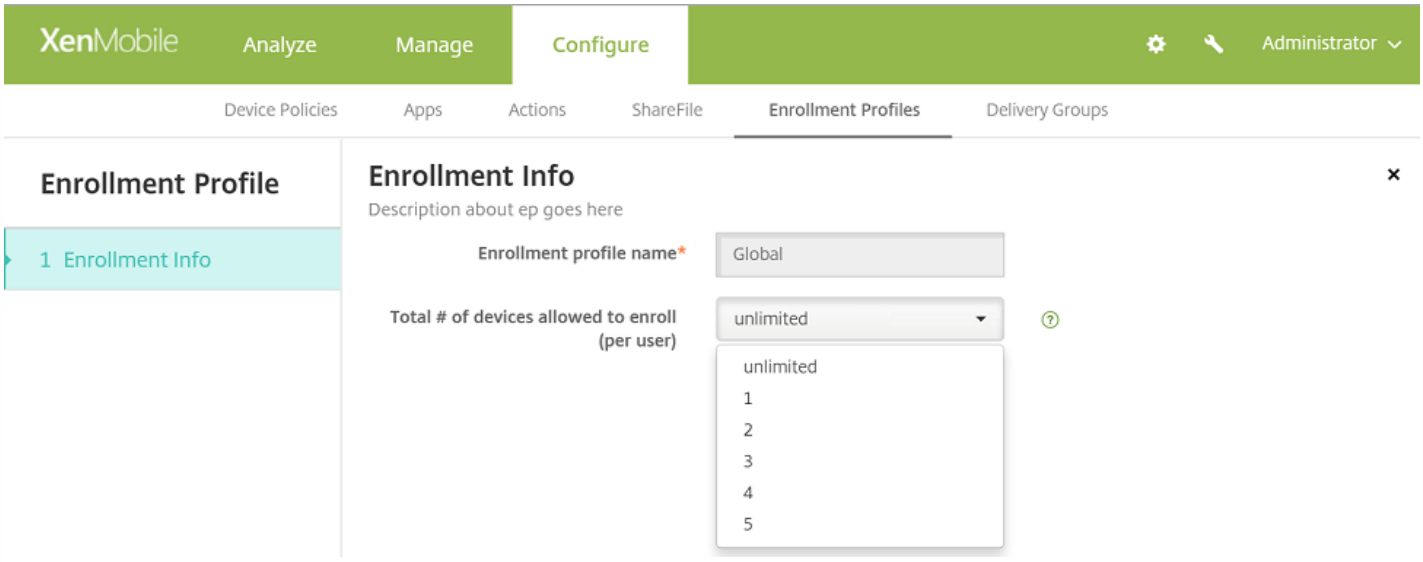
Para configurar un límite global de inscripción de dispositivos

1. Vaya a **Configurar > Perfiles de inscripción de dispositivos**.

2. Haga clic en **Global** y seleccione **Modificar**.



La información de la pantalla **Información de inscripción** aparecerá con **Global** completado automáticamente como el nombre de perfil. Desde aquí, puede seleccionar el número de dispositivos que podrán inscribir los usuarios. Esta limitación se aplicará a todos los usuarios inscritos en XenMobile.

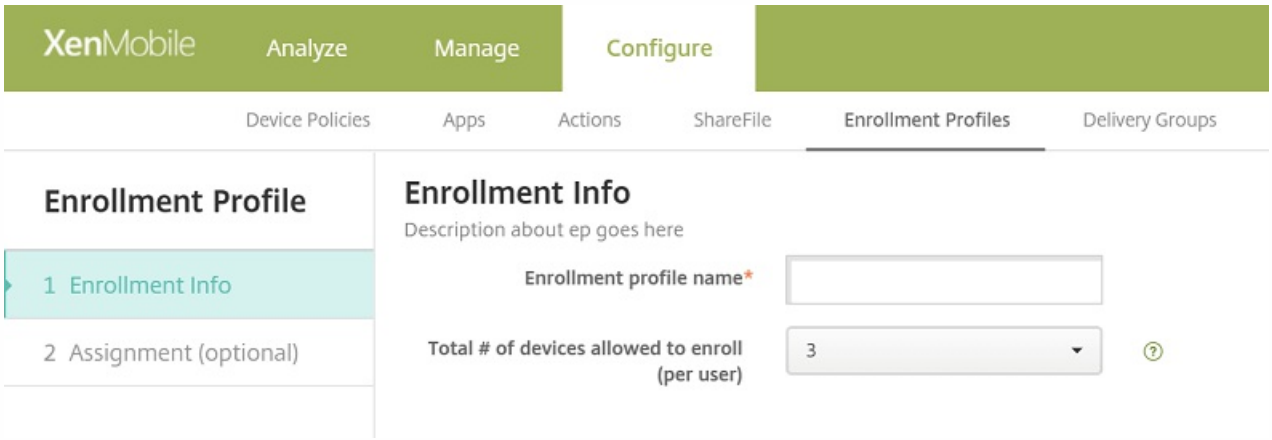


Para configurar un límite de inscripción de dispositivos para un grupo de entrega

1. Vaya a **Configurar > Perfiles de inscripción > Agregar**.

   Aparecerá la pantalla **Información de inscripción**.

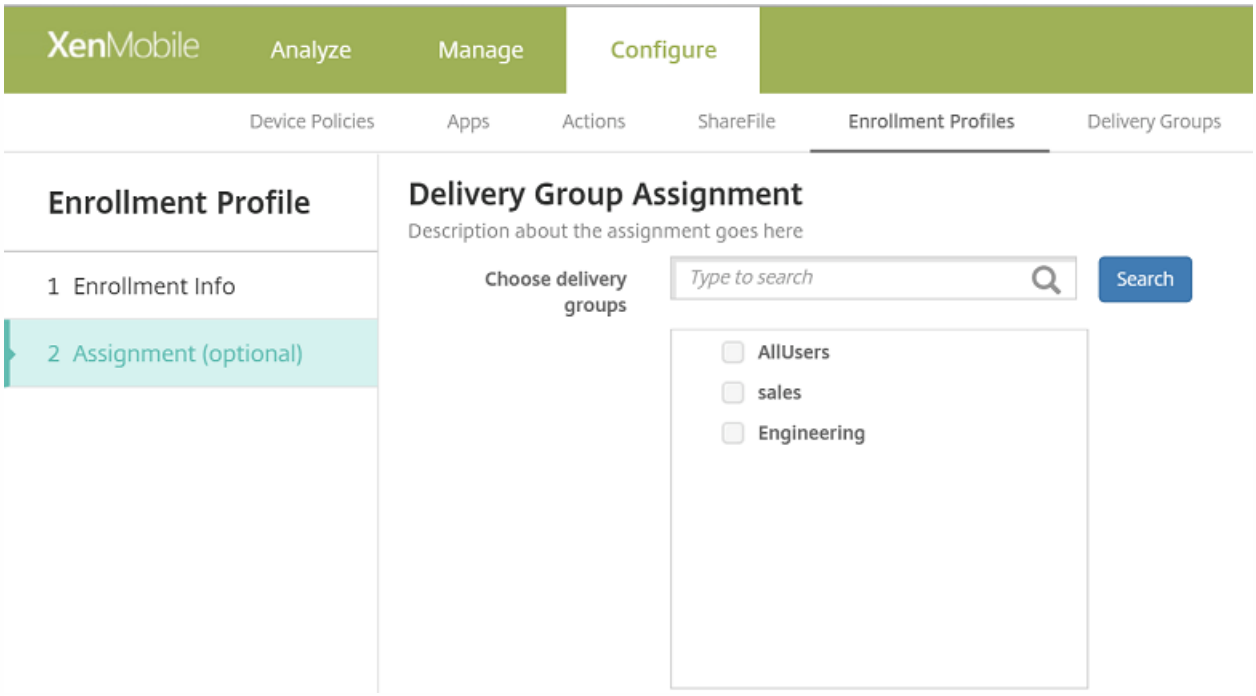
2. Escriba un nombre para el nuevo perfil de inscripción y, a continuación, seleccione el número de dispositivos que podrán inscribir los miembros de este perfil.



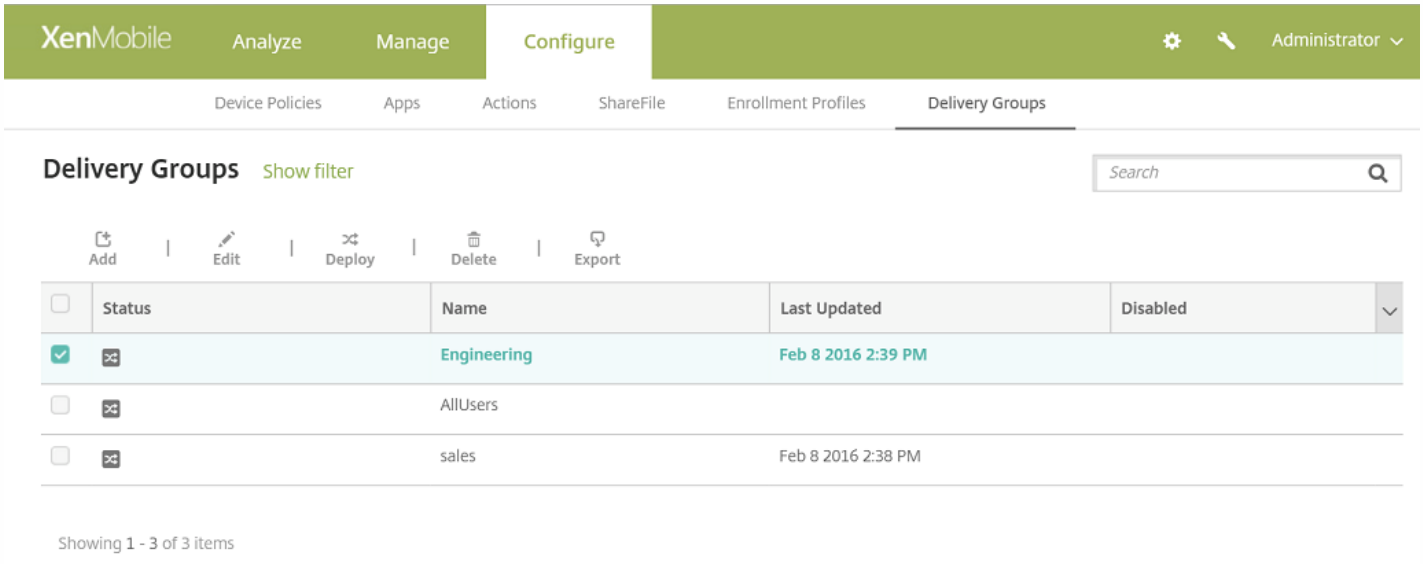
3. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Asignación de grupos de entrega**.

4. Seleccione los grupos de entrega a los que se aplicará el límite de inscripción de dispositivos y, a continuación, haga clic en **Guardar**.

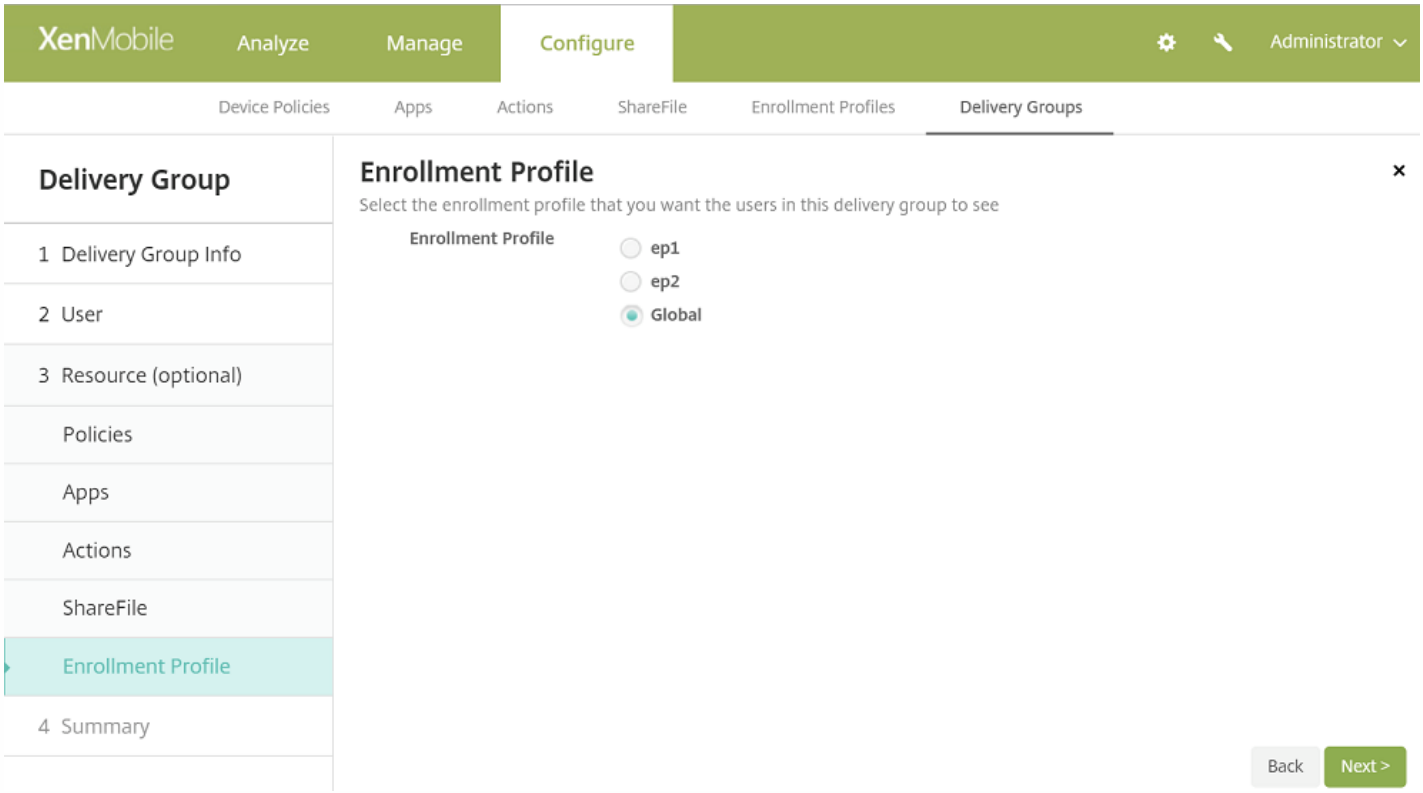


Si más adelante desea cambiar el perfil de inscripción de un grupo de entrega, vaya a **Configurar > Grupos de entrega**. Seleccione el grupo que desee y haga clic en **Modificar**.



Aparecerá la pantalla **Perfil de inscripción**.

5. Desde esta pantalla, seleccione el perfil de inscripción que desea aplicar a este grupo de entrega y, a continuación, haga clic en **Siguiente** para ver y guardar los cambios.



Experiencia del usuario con un límite de inscripción de dispositivos

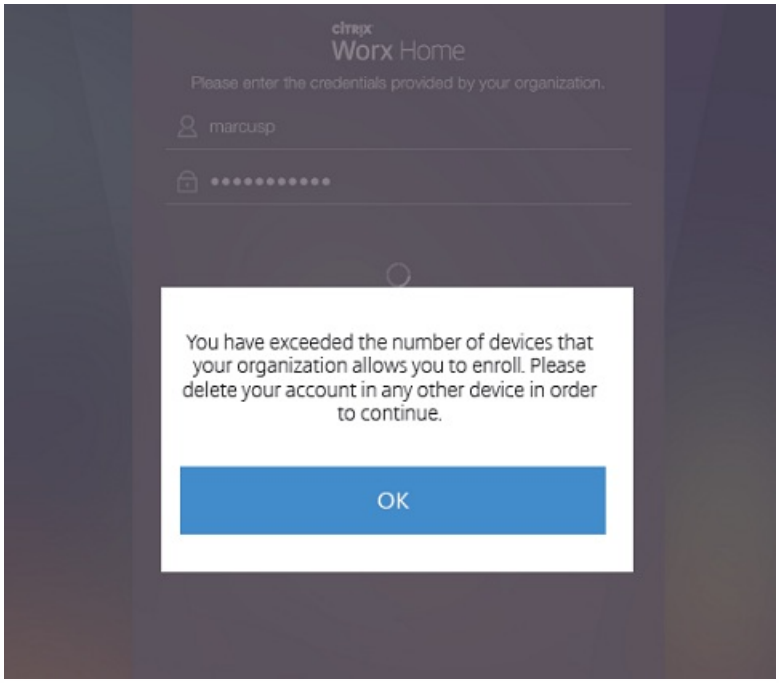
Cuando se establece el límite de inscripción de dispositivos y los usuarios intentan inscribir un dispositivo, siguen estos pasos:

1. Iniciar sesión en Worx Home.

2. Escribir la dirección de servidor que se inscribirá.

3. Escribir las credenciales.

4. Si se alcanza el límite de dispositivos, aparece un mensaje de error que indica que se ha excedido el límite de registros de dispositivos y que se debe contactar con un administrador.



La pantalla de inscripción de Worx Home aparece de nuevo.

Acciones de bloqueo de aplicaciones y borrado de aplicaciones para el modo de solo MAM

Aug 25, 2016

Al crear acciones, se establecen respuestas automáticas en un dispositivo de usuario para ciertos desencadenadores, como la instalación de una aplicación no permitida o la eliminación de un usuario de Active Directory. También puede enviar notificaciones a los usuarios para corregir un problema antes de tener que tomar medidas más severas.

A partir de XenMobile 10.3.5, puede bloquear o borrar las aplicaciones de un dispositivo en respuesta a las cuatro categorías de desencadenadores que se enumeran en la consola de XenMobile: evento, propiedad de dispositivo, propiedad de usuario y nombre de aplicación instalada. Antes, solo la categoría de evento tenía esta funcionalidad.

Para configurar el borrado o bloqueo automático de aplicaciones:

1. En la consola de XenMobile, haga clic en **Configure > Actions**.

2. En la página **Actions**, haga clic en **Add**.

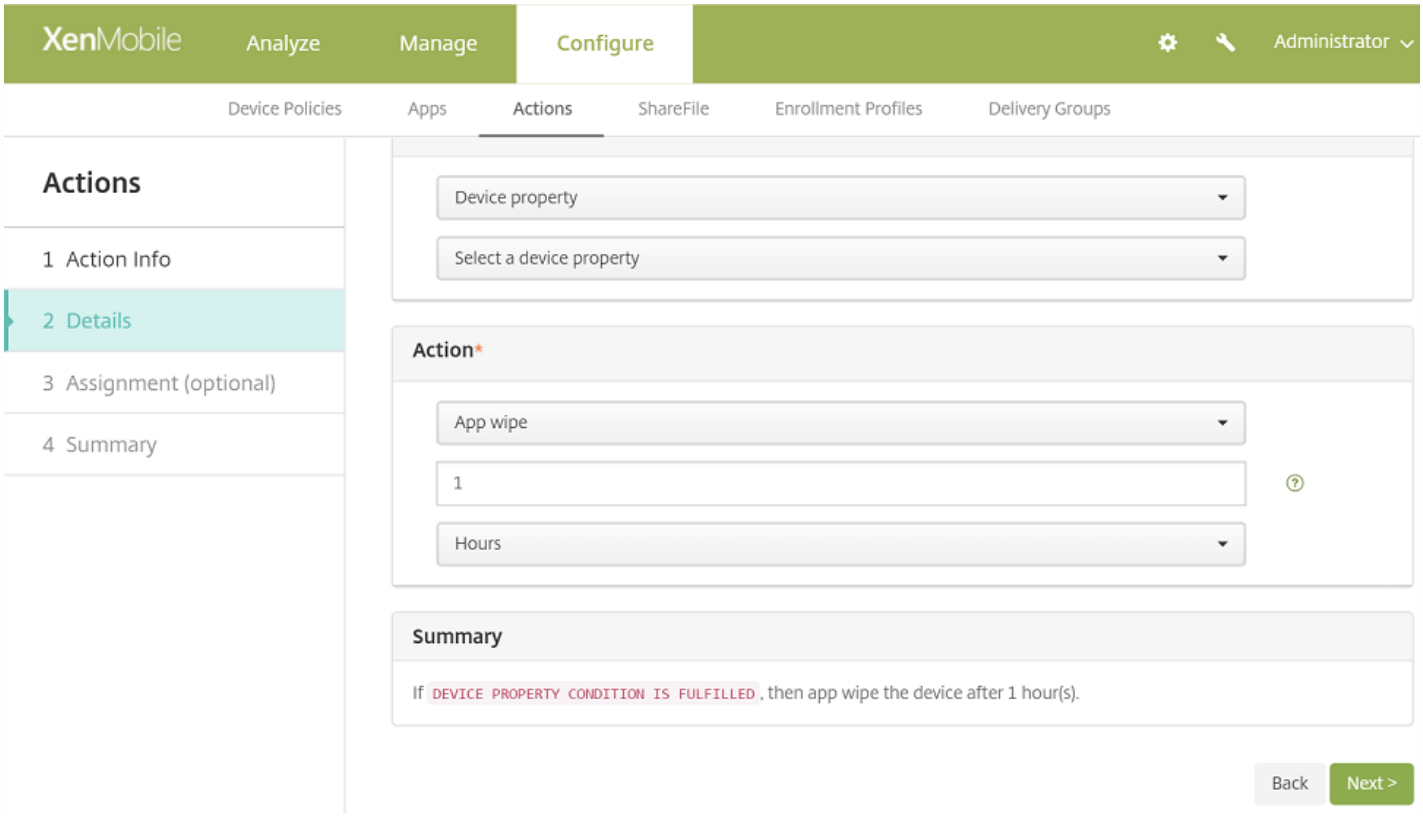
3. En la página **Action Information**, escriba un nombre para la acción y una descripción opcional.

4. En la página **Action Details**, seleccione el desencadenador que desee.

5. En **Action**, seleccione **App wipe** o **App lock**.

Para cada opción, se establece una demora de 1 hora automáticamente, pero se puede seleccionar el periodo de demora en minutos, horas o días. La demora proporciona a los usuarios tiempo para solucionar un problema, si es posible, antes de que la acción se lleve a cabo. Puede obtener más información acerca de las acciones de borrado y bloqueo de aplicaciones en el tema Permisos y roles RBAC.

> **Nota**
>
> También es posible que exista un retraso de aproximadamente una hora antes de que la acción se lleve a cabo, para permitir que la base de datos de Active Directory se sincronice con XenMobile.



6. Configure las reglas de implementación y, a continuación, haga clic en **Next**.

7. Configure las asignaciones de los grupos de entrega y una programación de implementación y, a continuación, haga clic en **Next**.

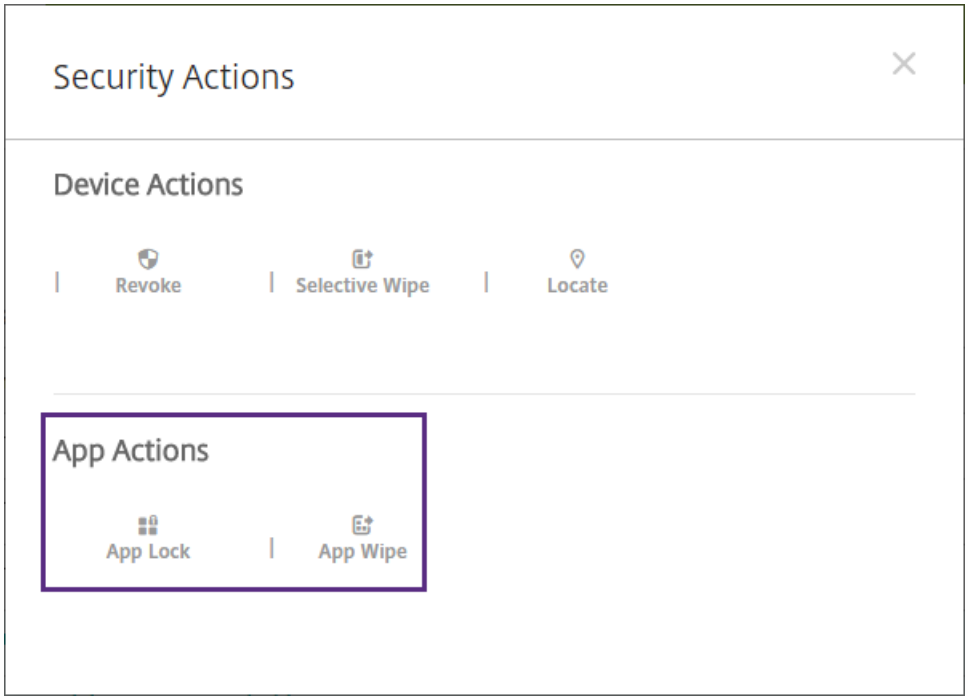
8. Haga clic en **Save**.

Para realizar un bloqueo, desbloqueo, borrado y cancelación de borrado de aplicaciones:

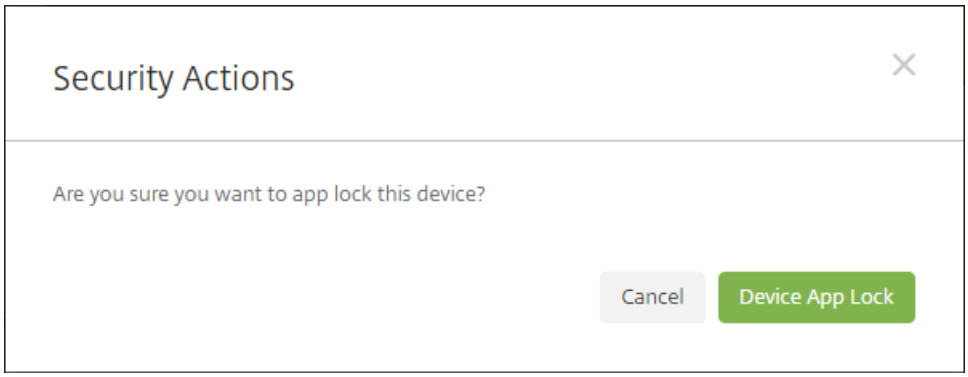
1. Vaya a **Manage > Devices**, seleccione el dispositivo y haga clic en **Secure**.

2. En el cuadro de diálogo **Security Actions**, haga clic en una acción.

> Nota: También puede utilizar este cuadro de diálogo para comprobar el estado de un dispositivo de un usuario que usted sepa que está inhabilitado o que ha sido eliminado de Active Directory. La presencia de las acciones App Unlock o App Unwipe indican que las aplicaciones de los usuarios están siendo borradas o bloquedas en ese momento.

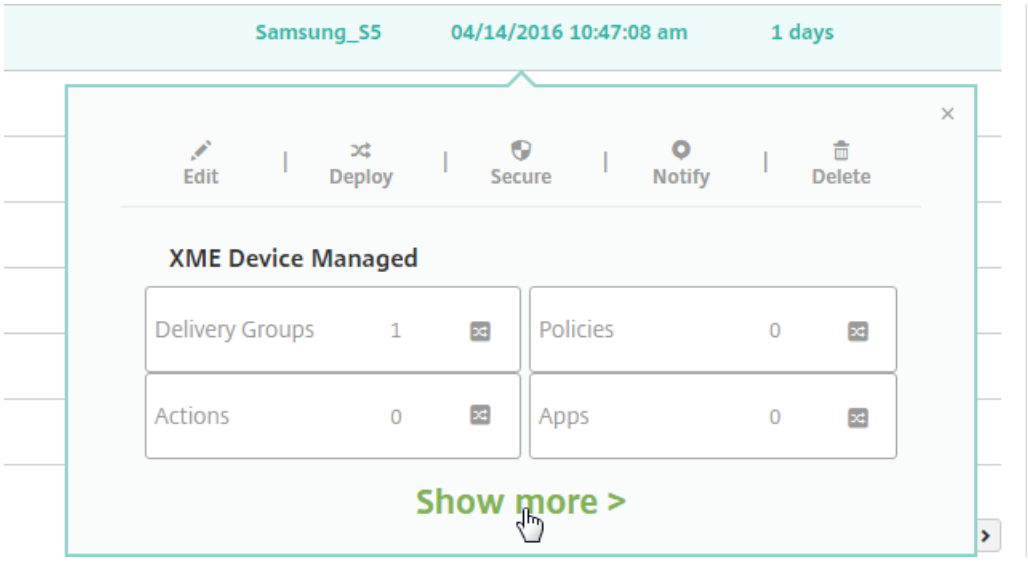


3. Confirme la acción.

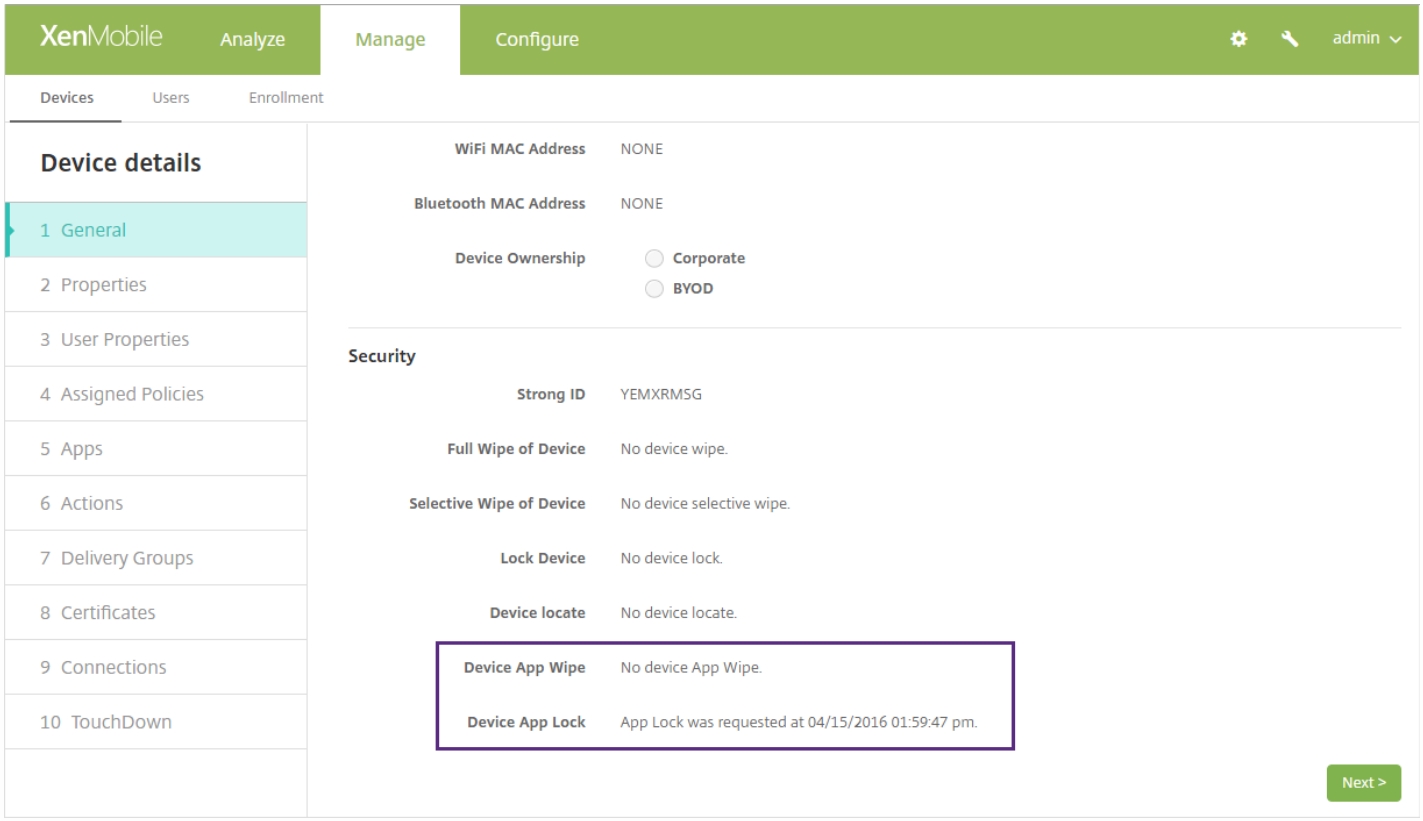


Para comprobar el estado del bloqueo o borrado de las aplicaciones

1. Vaya a **Manage > Devices**, seleccione el dispositivo y haga clic en **Show more**.



2. Vaya a **Device App Wipe** y **Device App Lock**.



API de REST Services para el modo solo MAM

Jul 27, 2016

Para dispositivos de solo MAM, puede usar cualquier cliente REST y la API de REST de XenMobile para llamar a servicios de REST que se exponen mediante la consola de XenMobile. La API no requiere el inicio de sesión en la consola de XenMobile para llamar a ningún servicio descrito en esta sección.

Puede invocar servicios de la API de REST mediante el cliente REST.

La nueva API de REST le permite:

- **Enviar una URL de invitación y un PIN de un solo uso**

  Puede usar la API de REST de XenMobile para permitir que los usuarios soliciten acceso de uso de dispositivos personales en el trabajo a través de un portal de autoservicio. Una vez aprobado, el sistema llama al servidor XenMobile y envía una solicitud para realizar las siguientes acciones:

  - Generar y enviar una URL de invitación de inscripción al usuario.

  - Generar y enviar un PIN de un solo uso al usuario.

  Nota: Esta funcionalidad es compatible con dispositivos iOS y Android, pero no con dispositivos Windows.

- **Emitir acciones de bloqueo y borrado de aplicaciones en los dispositivos**

  Puede usar la API de XenMobile para encontrar los dispositivos que pertenecen a un usuario mediante la búsqueda de todos los dispositivos para poder borrar o bloquear las aplicaciones del dispositivo, por ejemplo.

En lo que queda de este artículo, se enumeran las API de dispositivos y las API de inscripción de PIN de un solo uso disponibles en XenMobile 10.3.5. Para consultar toda la documentación sobre el conjunto actual de interfaces API disponibles, descargue el archivo PDF de Información acerca de la API de REST en XenMobile.

Interfaces API de dispositivo

- Obtener dispositivos mediante filtros
- Obtener información de dispositivos por ID
- Obtener aplicaciones de dispositivos por ID de dispositivo
- Obtener acciones de dispositivos por ID de dispositivo
- Obtener grupos de entrega de dispositivos por ID de dispositivo
- Obtener inventario de software administrado de dispositivos por ID de dispositivo
- Obtener directivas de dispositivos por ID de dispositivo
- Obtener inventario de software de dispositivos por ID de dispositivo
- Obtener coordenadas de GPS de dispositivos por ID de dispositivo
- Enviar notificación a una lista de dispositivos o usuarios
- Autorizar una lista de dispositivos
- Omisión del bloqueo de activación en una lista de dispositivos
- Bloqueo de aplicaciones en una lista de dispositivos
- Borrado de aplicaciones en una lista de dispositivos

- Bloqueo de contenedores en una lista de dispositivos
- Cancelar bloqueo de contenedores en una lista de dispositivos
- Desbloqueo de contenedores en una lista de dispositivos
- Cancelar desbloqueo de contenedores en una lista de dispositivos
- Restablecer contraseña de contenedor en una lista de dispositivos
- Cancelar el restablecimiento de contraseña de contenedor en una lista de dispositivos
- Desvincular una lista de dispositivos
- Localizar una lista de dispositivos
- Cancelar localización de una lista de dispositivos
- Seguimiento GPS de una lista de dispositivos
- Cancelar seguimiento GPS en una lista de dispositivos
- Bloquear una lista de dispositivos
- Cancelar bloqueo de una lista de dispositivos
- Desbloquear una lista de dispositivos
- Cancelar desbloqueo de una lista de dispositivos
- Implementar una lista de dispositivos
- Solicitar duplicación de AirPlay en una lista de dispositivos
- Cancelar solicitud de duplicación de AirPlay en una lista de dispositivos
- Detener duplicación de AirPlay en una lista de dispositivos
- Cancelar detención de duplicación de AirPlay en una lista de dispositivos
- Borrar las restricciones en una lista de dispositivos
- Cancelar el borrado de las restricciones en una lista de dispositivos
- Revocar una lista de dispositivos
- Llamar a una lista de dispositivos
- Cancelar llamada a una lista de dispositivos
- Borrar una lista de dispositivos
- Cancelar borrado en una lista de dispositivos
- Borrar de forma selectiva una lista de dispositivos
- Cancelar borrado selectivo de una lista de dispositivos
- Borrado de tarjeta SD en una lista de dispositivos
- Cancelar borrado de tarjeta SD en una lista de dispositivos
- Obtener todas las propiedades conocidas de dispositivos
- Obtener todas las propiedades de usuario de dispositivos
- Recuperar todas las propiedades de dispositivos por ID de dispositivo
- Actualizar todas las propiedades de dispositivos en masa por ID de dispositivo
- Agregar o actualizar una propiedad de dispositivo por ID de dispositivo
- Eliminar una propiedad de dispositivo por ID de dispositivo
- Recuperar el estado MDM de iOS de dispositivos por ID de dispositivo
- Generar código PIN

Interfaces API de inscripción con PIN de un solo uso

- Obtener modos de inscripción
- Obtener información de inscripción
- Desencadenar notificación de inscripción

- Crear invitación de inscripción
- Obtener registros de inscripción por filtro

Problemas conocidos y resueltos en XenMobile 10.3.5

Aug 25, 2016

Estos son los problemas conocidos o resueltos de XenMobile 10.3.5:

- Limitación: Las funciones para el nuevo modo solo MAM, tales como la autenticación basada en certificados, las acciones de bloqueo y borrado de aplicaciones y las API del modo solo MAM, no están disponibles para Windows Phone.
- Cuando los usuarios se reinscriben en Worx Home varias veces y, a continuación, intentan instalar una aplicación desde Worx Store, aparece un mensaje de error donde se indica que la aplicación se ha eliminado. Como solución alternativa, puede eliminar el dispositivo en la consola de XenMobile, en **Manage > Devices** y, a continuación, pedir a los usuarios que se reinscriban. [#611172]
- 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. [#618390]
- Cuando se alcanza el límite de inscripción de dispositivos en la consola de XenMobile, no aparece el mensaje de error apropiado en el dispositivo, pero los usuarios no pueden inscribirse. [#623475]
- Cuando los usuarios se inscriben en XenMobile mediante una cuenta de Azure Active Directory, incluso después de haber borrado o revocado el dispositivo, pueden inscribirse de nuevo sin autorización. Este es un problema de terceros. [#628865]
- Después de eliminar un dispositivo iOS de la consola de XenMobile, en ocasiones, cuando los usuarios vuelven a inscribir el dispositivo en modo XenMobile Enterprise (MAM y MDM), se produce un error en la inscripción en modo MAM. [#629021]
- Cuando se inhabilita la opción de renovación de certificados en el servidor XenMobile, los usuarios pueden renovar un certificado caducado en Worx Home. [#630894]
- Algunas licencias de VPP tienen ID con valores negativos, como -123441212, en cuyo caso no se pueden distribuir las aplicaciones públicas. [#631443]
- Si una credencial de Google Play está configurada con un ID de dispositivo no válido, cuando se agrega una aplicación de una tienda o almacén de aplicaciones público y se hace clic para buscar la aplicación en Google Play, la búsqueda falla o devuelve resultados incorrectos. [#633845]
- Actualmente no se puede encontrar el ID de Android introduciendo *#*#8255#*#*en el teléfono, según las instrucciones de la página **Settings > Google Play Credentials** de XenMobile. Use una aplicación de ID de dispositivo obtenida en la tienda Google Play para buscar el ID de su dispositivo. [#633854]
- En la consola de XenMobile, **Configuración > Role Based Access Control** tiene los siguientes problemas relacionados con los parámetros predeterminados.
  - En la consola de XenMobile para implementaciones en la nube, el permiso **Shared devices enroller** se configura de forma predeterminada para el rol Admin. Este permiso no debería configurarse de forma predeterminada. [#638069]
  - El permiso **Disown device** de la consola ahora es obsoleto y no debería aparecer. [#638303]
  - En la consola de XenMobile para administrar implementaciones locales, las siguientes características no se seleccionan de forma predeterminada para el rol Admin. Asegúrese de seleccionar estos parámetros según sea necesario para el rol Admin o para los roles que haya creado a partir de la plantilla Admin. [#638314]

    Lock container
    Unlock container
    Reset container password
    Bypass activation lock
    Rings the device

- En la consola de XenMobile para administrar implementaciones locales y en nube, las siguientes características no se seleccionan de forma predeterminada para el rol Admin. Asegúrese de seleccionar estos parámetros según sea necesario para el rol Admin o para los roles que haya creado a partir de la plantilla Admin. [#638322]

  Request AirPlay mirroring
  Stop AirPlay mirroring

- La autenticación SSO de ShareFile falla debido a problemas de sincronización de hora que se producen entre XenMobile y Hyper-V. [#588249]
- Cuando se habilita el anidado en la configuración de LDAP de XenMobile y se configuran los grupos de entrega y los parámetros de RBAC con los grupos de dominio correspondientes, si posteriormente se elimina el dominio de la configuración de LDAP, la información de los grupos anidados se conserva en la base de datos. [#590363]
- Cuando se elimina un usuario de Active Directory, este aún puede abrir WorxStore y suscribirse a las aplicaciones. [#592825]
- Después de comprobar si hay actualizaciones para las aplicaciones de la tienda pública de aplicaciones en la consola de XenMobile, Worx Home actualiza las aplicaciones de la tienda pública de aplicaciones a la versión más reciente, pero la aplicación sigue apareciendo en la lista de actualizaciones pendientes en el dispositivo. [#593034]
- Cuando los usuarios reciben invitaciones de calendario de la cuenta de Exchange en WorxMail, la invitación no llega al instante como se espera. [#594542]
- Cuando el dispositivo iOS se registra en el Device Enrollment Program (DEP), es posible que Worx Home no se descargue en el dispositivo iOS. [#595822]
- Puede que se produzcan problemas de variación de hora con el servidor XenMobile, como puede ser el error de Single Sign-on (SSO) de SAML para ShareFile, si no se configura un cliente NTP.

  Nota: Configure estos ajustes para habilitar la solución:

  1. Inicie sesión en la interfaz de línea de comandos de XenMobile en el hipervisor en el que se instaló XenMobile (Citrix XenServer o VMware ESXi).

  2.Vaya a **[2] System**.

  3.Vaya a **[3] Set NTP Server** y proporcione los detalles del servidor NTP.

  4. Reinicie el servidor.

  Importante: Si el sistema se ha configurado en modo de clúster, configure los ajustes anteriores en cada nodo. [#597757]

- Cuando los usuarios intentan quitar una aplicación o un enlace Web de Worx Home, aparece el siguiente error: Worx Home no pudo conectar. [#599934]
- La inscripción basada en PIN puede fallar si hay varios PIN con el estado pendiente para los usuarios. [#600264]
- Cuando se importan licencias de VPP en XenMobile, en el caso de que Apple haya reembolsado el importe de alguna de ellas, las licencias se consideran válidas en XenMobile de forma errónea. Como resultado, los usuarios no pueden instalar aplicaciones en dispositivos iOS mediante WorxStore. [#601845]
- Después de crear una acción, si se cambia el nombre de esta por el mismo nombre que el de una de las aplicaciones o las directivas del dispositivo, no se podrá eliminar la acción en un futuro. [#602958]
- Cuando se usa un dispositivo Samsung Galaxy Note 5 para acceder a WorxStore, WorxStore aparece en la vista de

tableta con una pantalla parcial, en lugar de en la vista de teléfono como se esperaba. [#604295]

- Cuando se crea una invitación de inscripción con el requisito de código PIN de un solo uso para los destinatarios del nivel superior de un grupo de Active Directory, los grupos anidados reciben la invitación, pero la inscripción falla para los grupos anidados del tercer nivel. Este problema ocurre aunque se envíe la invitación al grupo de tercer nivel. [#603434]
- Cuando se tiene un tipo de licencia Advanced y se marca la casilla de verificación Enrollment required en la consola de XenMobile, los usuarios se pueden registrar en el modo solo MAM y acceder a WorxStore. [#604113]
- Las propiedades **$user.dnsroot** y **$user.netbiosename** se usan en macros para implementar directivas mediante propiedades de usuario. Las propiedades de usuario **dnsroot** y **netbiosename** quedaron obsoletas en XenMobile 10.1. Esta solución vuelve a dar respaldo para estas propiedades en XenMobile 10.3. [#604240]
- 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. [#607143]
- En la configuración de personalización de marca de cliente de la consola de XenMobile, el nombre de la tienda solo admite caracteres alfanuméricos (ASCII); si cambia el valor predeterminado por un carácter no incluido en ASCII, los usuarios no podrán iniciar sesión en Worx Home. [#609535]
- Cuando se ha configurado LDAP con otros DN base para los usuarios y los grupos, no se podrán agregar nuevos grupos a los grupos de entrega después de actualizar a XenMobile 10.3. [#610014]
- Cuando se configura una directiva de dispositivos Wi-Fi, aunque la programación de la implementación se haya establecido como **Only when previous deployment has failed**, la directiva de Wi-Fi se enviará a los dispositivos cada vez que el dispositivo se conecte. [#610325]
- Esta solución se ocupa de la vulnerabilidad de días cero de Java de la deserialización de objetos de Apache Commons Collection. [#610427]
- Cuando se establece un rol RBAC para permitir que los usuarios inicien sesión en la consola de XenMobile con un formato de nombre de usuario sAMAccountName, se les redirigirá al portal Self Help Portal. [#610915]
- Después de instalar XenMobile 10.1 por primera vez, o de actualizar desde el modo MAM y MDM de XenMobile 9 a XenMobile MDM 10.1, en la consola de XenMobile en **Manage** > **Device**, después de actualizar los grupos de entrega y las directivas, la información es diferente; el recuento de grupos de entrega y directivas no es correcto. [#611630]
- Cuando se tienen más de 10 dominios de LDAP configurados en versiones de XenMobile anteriores a XenMobile 10.1, en XenMobile 10 y después de actualizar a XenMobile 10.1, solo aparecen 10 dominios en la consola de XenMobile. [#613502]
- No se puede agregar ni actualizar una aplicación MDX si no se establece un rol RBAC para los usuarios que incluya permisos para las aplicaciones públicas. [#614496]
- Si cambia el nombre de instancia predeterminado durante la configuración inicial de XenMobile, cuando actualice a la versión 10.3, el cambio no se conservará. Como resultado, los dispositivos inscritos no se podrán conectar. [#614604]
- Cuando se configura LDAP con un límite de bloqueo, después de actualizar a XenMobile 10.3, cuando un nuevo usuario del mismo dominio inscribe un dispositivo en Worx Home con credenciales no válidas, como una contraseña mal escrita, Worx Home deja de responder y se produce un error de SQL Server. [#615179]
- Después de actualizar de XenMobile 10.1 a XenMobile 10.3, no se puede enviar una invitación de inscripción a los usuarios mediante la opción **Add invitation**. [#616584]
- Esta solución habilita la compatibilidad con la raíz de multi-dominio de LDAP de un único bosque. Esta compatibilidad estaba disponible en XenMobile 9, pero no en XenMobile 10.x. [#616633, #618899, #620541]
- Cuando se configura una directiva de dispositivos de restricción de iOS en la consola de XenMobile, y se cambia el valor predeterminado de la opción **Allow user to remove policy**, el valor no se guarda. [#616751]
- Cuando un servidor tiene un nombre de instancia personalizado, después de actualizar de XenMobile 10.1 a XenMobile 10.3, los usuarios no pueden inscribir dispositivos. [#616954]
- Cuando los usuarios inscriben un dispositivo de DEP en modo XenMobile Enterprise, si restablecen su propio dispositivo a los valores de fábrica (borrado completo) y, a continuación, vuelven a inscribir el dispositivo, Worx Home no se implementa

en el dispositivo automáticamente como se esperaba. [#616986]

- En ocasiones, el servidor XenMobile pasa al modo de recuperación después de 20 a 30 minutos debido a un problema conocido de Java Runtime Environment (JRE). Después de reiniciar el servidor, el problema se produce de nuevo. [#616992]
- En dispositivos iOS y Android, los usuarios no pueden abrir Worx Store desde Worx Home, si se quita el nombre de almacén **Store name** en **Settings > Client Branding**. [#617003]
- Cuando se carga un archivo .ipa en la consola de XenMobile, aparece un error que indica que no se encuentra ningún icono. [#617195]
- Cuando se implementa una directiva de dispositivos de VPN con las opciones Enable per-app VPN y On demand app enabled establecidas como **ON**, y una directiva de atributos de aplicación para una aplicación administrada a la que se ha aplicado la directiva de VPN, cuando los usuarios abren la aplicación administrada, se produce el siguiente problema: la conexión VPN no se inicia automáticamente como se esperaba. Los usuarios deben habilitar el parámetro **Conectar a demanda** de forma manual en sus dispositivos. [#617803]
- En la consola de XenMobile, en **Manage** > **Users**, se produce una demora en la aparición de los usuarios existentes. Como consecuencia, no se pueden realizar operaciones de usuario local. [#618094]
- XenMobile 10.x proporciona compatibilidad con multi-dominio de LDAP en un único bosque de Active Directory. [#618375]
- Cuando se envía una invitación de inscripción y se escribe código HTML, los usuarios reciben el mensaje de correo electrónico en texto sin formato sin ningún enlace HTML. [#618504]
- Cuando los usuarios cargan un archivo .appx como una aplicación de empresa para dispositivos Windows 10, la aplicación no se implementa en el dispositivo. [#628611]
- Los usuarios no pueden inscribir dispositivos Windows 10 en XenMobile en modo MDM si contienen caracteres especiales en el ID de usuario o el campo de contraseña. [#618870]
- En iPads, XenMobile 10.3 siempre lleva a cabo primero las acciones de eliminación, independientemente del orden establecido en la consola de XenMobile. [#620459]
- Cuando se actualiza una aplicación de empresa para iOS existente en la consola de XenMobile y el archivo .ipa tiene un ID de paquete diferente, al implementar la aplicación actualizada en los dispositivos, se producirán problemas con la implementación de las aplicaciones en los dispositivos. [#621009]
- Al agregar credenciales de Google Play en el servidor XenMobile, aparece un error de "ID de dispositivo no válido" y no se puede iniciar la sesión. [#623182]
- Si elimina una aplicación de XenMobile que importó mediante VPP, la aplicación no se importará automáticamente de nuevo hasta que elimine y agregue el token otra vez. [#623403]
- Si elimina o borra un dispositivo, cualquier licencia de VPP asociada a este dispositivo no se devolverá automáticamente. Como resultado, deberá anular la asociación de la licencia de forma manual para poder usarla en otro dispositivo. [#623716]

Acerca de XenMobile Server 10.3

Oct 31, 2016

Puede actualizar XenMobile 10.1 a XenMobile 10.3 en la consola de XenMobile. Para llevar a cabo la actualización, use el archivo xms_10.3.0.824.bin. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, haga clic en **Release Management**. Haga clic en **Upgrade** y cargue el archivo xms_10.3.0.824.bin. Para obtener más información acerca de actualizaciones en la consola, consulte Actualización de XenMobile.

Para completar una instalación nueva de XenMobile 10.3, consulte Instalación de XenMobile.

> ## 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.

XenMobile 10.3 introduce las siguientes funciones nuevas.

Nueva presentación de la consola

XenMobile 10.3 tiene una nueva apariencia. La consola se actualiza con una nueva combinación de colores, fuentes y fichas, y una funcionalidad mejorada.

- La ficha Dashboard de las versiones anteriores de la consola se ha movido a la nueva ficha Analyze, que también incluye la nueva ficha Reporting. Para obtener más información, consulte Informes.
- Ahora, la ficha Manage incluye la nueva ficha Users, que permite administrar usuarios y grupos locales.
- Ahora, la ficha Configure incluye la nueva ficha ShareFile, donde puede configurar parámetros para conectarse a la cuenta de ShareFile.
- Ahora, puede acceder a la sección Settings (antes situada en la ficha Configure) si hace clic en el icono con forma de engranaje ubicado en la parte superior derecha de la consola.
- Ahora, la ficha Support se abre en la misma ficha que la consola, en lugar de abrirse en una nueva ficha.

Respaldo a plataformas nuevas

XenMobile 10.3 ahora respalda las plataformas siguientes:

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE

- Windows 10 Phone: Administración de dispositivos en los modos XenMobile MDM y Enterprise.
- Windows 10 Desktop/Tablet: Administración de dispositivos en los modos XenMobile MDM y Enterprise.

Para conocer los pasos de inscripción de dispositivos Mac OS X, consulte Dispositivos Mac OS X.

Para conocer los pasos de inscripción de dispositivos Windows 10, consulte Dispositivos Windows.

> **Nota**
>
> El respaldo a dispositivos Symbian está obsoleto en XenMobile 10.3.

Directivas de dispositivo

Estas directivas MDM nuevas están disponibles en XenMobile 10.3:

- **App lock**. Permite definir una lista de las aplicaciones que se pueden ejecutar o una lista de aquellas aplicaciones que no se pueden ejecutar en un dispositivo. Disponible para iOS y Android. Aunque la directiva de dispositivos funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N y posteriores porque Google ha dejado de respaldar la API necesaria.
- **App network usage.** Permite definir las reglas de uso de red para especificar la forma en que las aplicaciones administradas usan, por ejemplo, redes de datos móviles. Las reglas solo se aplican a aplicaciones administradas. Disponible para iOS.
- **Connection manager**. Permite configurar cómo se conectarán las aplicaciones a Internet o a una red privada. Esta configuración solo funciona en Pocket PC (dispositivos de pantalla táctil). Disponible para Windows Mobile/CE.
- **Copy apps to Samsung container**. Permite crear un contenedor SEAMS o KNOX para aplicaciones en dispositivos Samsung. Disponible para Samsung SEAMS o Samsung KNOX.
- **Delete files and folders**. Permite especificar qué archivos y carpetas se deben eliminar. Disponible para Windows Mobile/CE.
- **Device health attestation**. Permite habilitar la atestación de estado de un dispositivo, una función de seguridad y de prevención de pérdida de datos (DLP) de Windows 10 que permite determinar el estado de un dispositivo Windows 10 y tomar acciones para un mayor cumplimiento cuando sea necesario. Las cargas útiles solo se admiten en dispositivos supervisados y con Windows 10 y versiones posteriores. Disponible para Windows Phone y tabletas Windows.
- **Device name.** Permite establecer los nombres de los dispositivos iOS y Mac OS X para identificarlos fácilmente. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo.
- **Delete registry keys and values**. Permite especificar qué valores y claves de Registro se deben eliminar. Un valor vacío significa que la entrada es una clave de Registro. Disponible para Windows Mobile/CE.
- **Enterprise Data Protection.** Permite especificar las aplicaciones que requieren la protección de datos de empresa (Enterprise Data Protection o EDP) en el nivel de cumplimiento que requiera. Esta directiva se aplica a teléfonos y tabletas Windows.
- **Import iOS & Mac OS X profile**. La opción para configurar esta directiva para Mac OS X es nueva en XenMobile 10.3. Esta directiva permite importar un archivo XML de configuración de dispositivos tanto en iOS como en Mac OS X. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator.
- **Registry**. El Registro de Windows Mobile/CE almacena datos sobre las aplicaciones, los controladores, las preferencias del usuario y los parámetros de configuración. Puede definir los valores y las claves de Registro que le permitirán administrar dispositivos Windows Mobile/CE.
- **Wallpaper.** Permite agregar un archivo JPG o PNG para establecer un fondo de escritorio en un dispositivo iOS para la

pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Disponible en iOS 7.1.2 y versiones posteriores. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.
- **Windows CE certificate**. Permite crear y entregar al dispositivo un certificado desde una infraestructura de clave pública externa.

Para ver una matriz de todas las directivas nuevas y existentes clasificadas por plataformas, consulte Directivas de dispositivos de XenMobile desglosadas por plataforma.

Resumen de las nuevas funciones y mejoras por tipo de plataforma

iOS

- **Nuevas directivas de dispositivo**. App Network Usage, Device Name y Wallpaper
- **Asignación de una aplicación administrada a no administrada**. Opción de iOS 9.0 para asignar una aplicación administrada a no administrada. Al agregar y configurar los parámetros de una aplicación de tienda pública de aplicaciones para iOS en la consola de XenMobile, se puede configurar la opción **Force app to be managed**. De forma predeterminada, esta opción está establecida en **OFF**. Si selecciona **ON**, cuando la aplicación se instale como no administrada, se solicitará a los usuarios que la aplicación se administre en dispositivos no supervisados. Para obtener información más detallada, consulte Incorporación de una aplicación de tienda pública a XenMobile.
- **Nuevas opciones para las directivas de restricciones y Apple Configurator 1.7.2**. Para obtener más información, consulte Directivas de restricciones de dispositivo.
- **Respaldo para los comandos RequestMirroring y StopMirroring**. Para obtener más información, consulte Información acerca de la API de REST en XenMobile.
- **Mejoras en el asistente de instalación de dispositivos del programa Device Enrollment Program (DEP)**. Para ver más detalles, consulte Inscripción de dispositivos iOS en masa.
- **Clave OnDemandRules para redes VPN**. Para obtener más información, consulte Directivas de VPN de dispositivo.

Android

- **Configuraciones de contenedor de Samsung KNOX**. Para obtener más información, consulte Directiva de copia de aplicaciones al contenedor de Samsung.
- **Interfaces API de Samsung SAFE**. Para obtener más información, consulte Información acerca de la API de REST en XenMobile.
- **Clave ELM para dispositivos Android de Samsung**.
- **Directiva de bloqueo de aplicaciones**. Para obtener más información, consulte Directiva de bloqueo de aplicaciones.

Windows CE

- **Configuraciones de proveedor de credenciales**. Para obtener más información, consulte Directiva de credenciales de dispositivo.
- **Configuraciones de certificado de Windows CE**. Para obtener más información, consulte Directiva de certificado de Windows CE.
- **Directiva de almacenamiento de Registro**. Para obtener más información, consulte Directiva de Registro.
- **Capacidad para conectar al recibir SMS o recibir una llamada**.
- **Otras directivas nuevas**: Connection manager, Delete Files and Folders, Delete Registry Keys and Values.

Windows Phone 10 y Windows Tablet 10

- Nueva directiva de dispositivo: Enterprise Data Protection y Device Health Attestation

- Nuevas opciones de directivas de dispositivo para Windows Phone y tabletas Windows:

  App Inventory
  Credentials
  Custom XML
  Passcode
  Restrictions
  Terms & Conditions
  VPN
  WiFI

- Nuevas opciones de directivas de dispositivo para tabletas Windows:

  App Uninstall
  Sideloading Key
  Signing Certificate
  Webclip
  WorxStore

- Nuevas opcions de directiva de dispositivo para Windows Phone:

  Enterprise Hub
  Storage Encryption

Mac OS X

- Inscripción vía OTAE. Para obtener más información, consulte Mac OS X.
- Información de administración de dispositivos en la consola de XenMobile que muestra las propiedades, los certificados, los informes y los perfiles admitidos de un dispositivo.
- Acciones de seguridad en dispositivos Mac OS X: borrado selectivo o completo, bloqueo, revocación.
- Nuevas opciones de directiva de dispositivo:

  Device Name
  Import iOS and Mac OS X Profile
  AirPlay Mirroring
  App Inventory
  Calendar (CalDav)
  Contacts (CardDAV)
  Credentials
  Exchange
  Font
  LDAP
  Mail
  Passcode
  Profile Removal
  Restrictions
  SCEP
  VPN
  Webclip

WiFI

Nuevas funciones y mejoras para respaldar Android for Work

- **Respaldo para dispositivos anteriores a Android**.
- **Modo Provisioning Device Owner para Android for Work**

  Además de administrar aplicaciones de Android for Work o dispositivos Android en modo BYOD, también se pueden administrar dispositivos que son propiedad de la empresa a través del aprovisionamiento del modo Device Owner. Para ello, use un toque Near Field Communication (NFC) entre dispositivos. Un dispositivo ejecuta la aplicación Worx Provisioning Tool y toca a un dispositivo completamente nuevo o que ha sido restablecido con los valores de fábrica. El modo Device Owner es el modo de dispositivo propiedad de la empresa para la mayoría de los dispositivos que ejecutan Android 5.x.x.

- **Compra en bloque de Android for Work**

  Puede gestionar las licencias de la compra en bloque (Bulk Purchasing) en la consola de XenMobile para las aplicaciones que están habilitadas para Android for Work. El plan de compra en bloque de Android for Work simplifica el proceso de encontrar, comprar y distribuir aplicaciones y otros datos en masa para una organización. Cuando agrega una aplicación de tienda pública de aplicaciones para Android for Work a XenMobile, puede ver el estado de las licencias de Bulk Purchase y la cantidad total de licencias disponibles. Después de implementar la aplicación a los usuarios, puede consultar más adelante la cantidad de licencias que se encuentran en uso en ese momento, además de las direcciones de correo electrónico de los usuarios que están consumiendo licencias. Puede seleccionar un usuario y hacer clic en **Disassociate** para porner fin a su asignación de licencia y liberar esa licencia para otro usuario. No obstente, solo puede desasociar la licencia si el usuario no forma parte de un grupo de entrega que contiene esa aplicación en concreto.

Dispositivos compartidos

XenMobile permite configurar los dispositivos que se pueden compartir entre varios usuarios. Para obtener más información, consulte Dispositivos compartidos en XenMobile.

Respaldo para idiomas

La consola de XenMobile en XenMobile 10.3 está disponible en coreano, alemán y portugués. Ahora, las directivas MDX aparecen traducidas al verse en la consola de XenMobile. Para obtener más información, consulte Respaldo para idiomas en XenMobile.

Reports

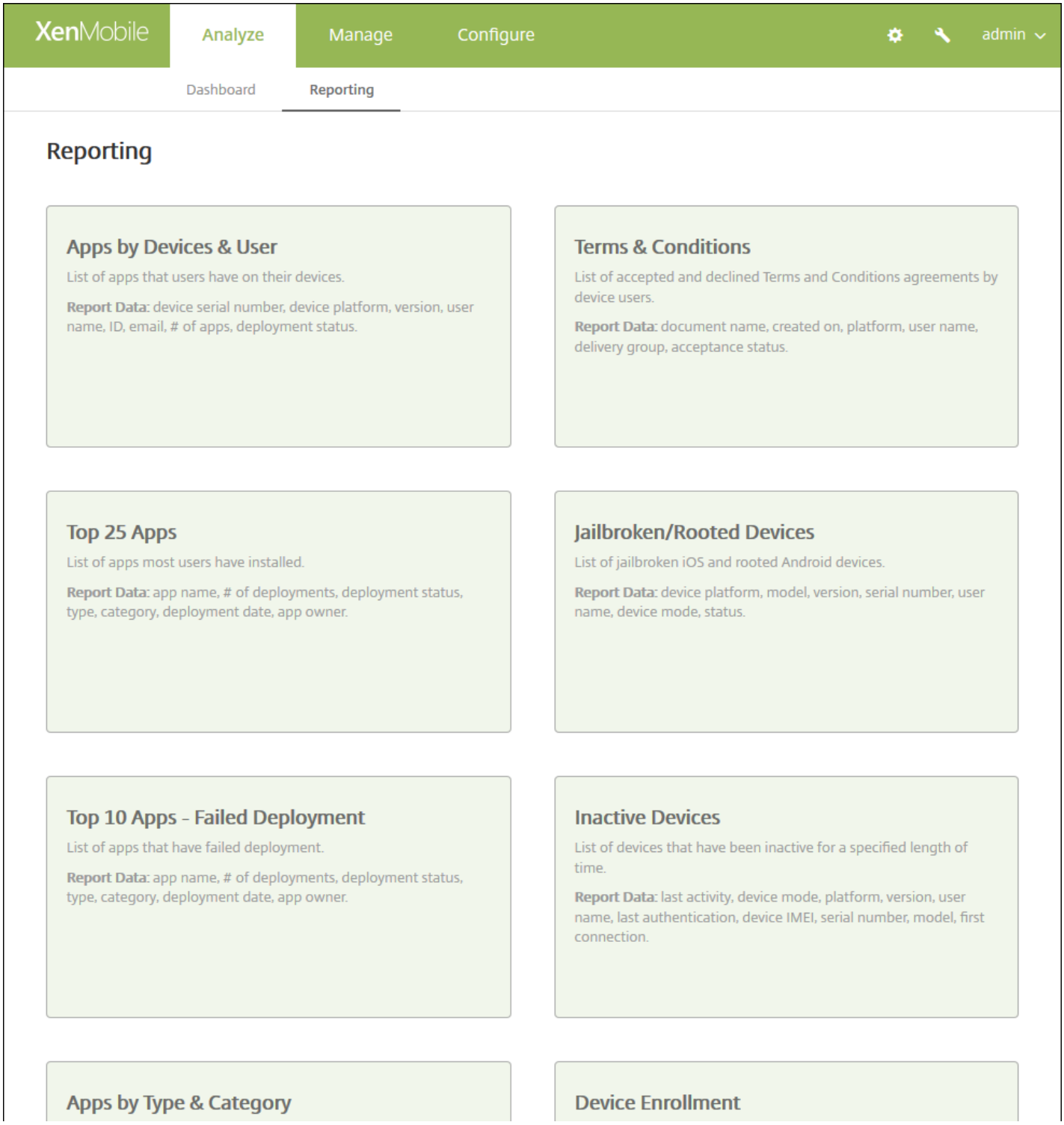
Desde la ficha **Reporting**, puede generar 10 informes predefinidos sin salir de la consola de XenMobile:

- **Apps by Devices & User**. Ofrece una lista de las aplicaciones que tienen los usuarios en sus dispositivos.
- **Terms & Conditions**. Ofrece una lista de los usuarios que hayan aceptado y rechazado los contratos de términos y condiciones.
- **Top 25 Apps**. Ofrece una lista de un máximo de 25 aplicaciones que tienen la mayoría de los usuarios en sus dispositivos.
- **Jailbroken/Rooted Devices**. Ofrece una lista de los dispositivos iOS liberados por rooting y de los dispositivos Android liberados por jailbreak.
- **Top 10 Apps – Failed Deployment**. Ofrece una lista de las aplicaciones que no se pudieron implementar.
- **Inactive Devices**. Ofrece una lista de los dispositivos que hayan estado inactivos durante un período de tiempo

especificado.

- **Apps by Type & Category**. Ofrece una lista de las aplicaciones según su versión, tipo o categoría.
- **Device Enrollment**. Ofrece una lista de los dispositivos que se han inscrito durante un período de tiempo especificado.
- **Apps by Platform**. Ofrece una lista de las aplicaciones y sus versiones según la plataforma y la versión del dispositivo.
- **Devices & Apps**. Ofrece una lista de todos los dispositivos, los datos de dispositivo y las aplicaciones instaladas.

Para ejecutar informes, haga clic en la ficha **Analyze** de la consola de XenMobile y, a continuación, haga clic en **Reporting**. Los informes se presentan en formato CSV, y se pueden abrir con programas como Microsoft Excel. Para obtener información más detallada, consulte Informes en XenMobile.



List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

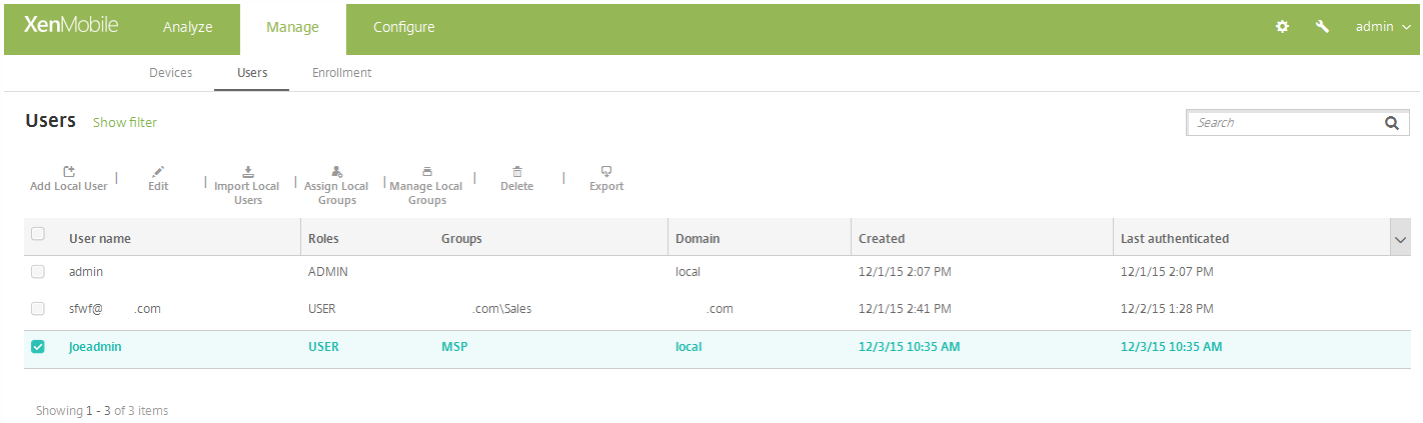
Devices & Apps

List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

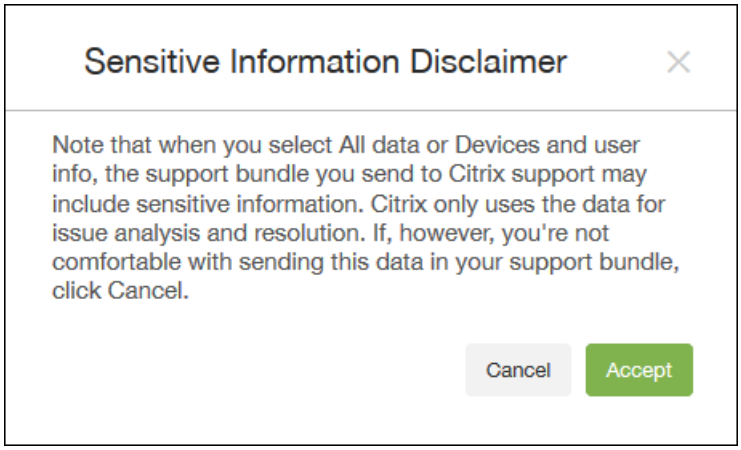
Incorporación de miembros LDAP (usuarios locales) a grupos

Muchas empresas no configuran grupos de Active Directory, pero es posible que necesiten un grupo local para un objetivo concreto, como podría ser un grupo piloto. En XenMobile 10.3, puede convertir usuarios locales LDAP en miembros de un grupo local. Luego, puede definir un grupo de entrega que contenga ese grupo local. Así, este conjunto de usuarios podrá acceder a aplicaciones y directivas asignadas al grupo de entrega sin tener que volver a inscribir sus dispositivos. Para obtener información más detallada, consulte Para agregar, modificar o eliminar usuarios locales en XenMobile.



Contrato legal referente al paquete de asistencia

La primera vez que cargue un paquete de asistencia en Citrix Insight Services (CIS), se le pedirá que acepte un contrato legal. Para obtener más información, consulte Creación de paquetes de asistencia en XenMobile.



Anonimato de datos en paquetes de asistencia

En XenMobile, cuando crea paquetes de asistencia, los datos confidenciales de usuario, red y servidor pasan a ser anónimos de forma predeterminada. Puede cambiar este comportamiento en la página Anonymization and De-anonymization. También puede descargar un archivo de asignación que XenMobile guarda cuando los datos pasan a ser anónimos. El servicio de asistencia de Citrix puede solicitar este archivo para convertir datos anónimos en no anónimos y, así, buscar los problemas que haya con un dispositivo o un usuario determinados. Para obtener más información, consulte Anonimato de datos en paquetes de asistencia.

Comprobaciones de conectividad

En la página Support de XenMobile, puede comprobar la conexión de XenMobile con NetScaler Gateway y con otros servidores y ubicaciones. Para obtener más información, consulte Realización de comprobaciones de conectividad.

Microsoft Azure

Puede unir dispositivos Windows 10 con Microsoft Azure Active Directory para permitir que los dispositivos se inscriban en Azure como un método federado de autenticación de Active Directory. Para obtener más información, consulte Configuración de Microsoft Azure.

Problemas resueltos de XenMobile Server 10.3

Jul 27, 2016

Se han resuelto los siguientes problemas en XenMobile 10.3. Para obtener información sobre los problemas resueltos de XenMobile 10.3.5, consulte Problemas conocidos y resueltos de XenMobile 10.3.5.

Un prefijo de envío de correo electrónico se puede añadir dos veces a una dirección de correo electrónico al enviar correo desde SMTP a través de una puerta de enlace SMS de operador. [#492629]

Las solicitudes de HTTP GET desde Cisco Identity Service Engine a XenMobile pueden fallar con el error 404. [#555554]

Cuando una directiva de carga de archivos está configurada para enviar por push un archivo a dispositivos Android, la operación de push puede fallar. En su lugar, puede aparecer la declaración de "Términos y condiciones" en el dispositivo. [#564144]

En algunos casos, cuando se distribuyen certificados de identidad MDM a través de SCEP y se emiten usando la infraestructura PKI integrada, al renovar estas identidades, XenMobile no revoca adecuadamente el certificado anterior. Como resultado, en algunas instancias, los dispositivos afectados pierden la funcionalidad de MDM. [#569999]

Después de configurar un servidor proxy, las comprobaciones de conectividad crean un tráfico de red que no pasa por el servidor proxy y la conexión falla. [#571467]

Si los usuarios son miembros de un dominio secundario, la conexión con aplicaciones SAML falla. [#571851]

Si una aplicación MDX de iOS está en la lista de dispositivos excluidos, la aplicación no aparece en Worx Store cuando el dispositivo está en el modo solo MAM (administración de aplicaciones móviles). [#571900]

Después de actualizar a XenMobile 10, la búsqueda de un dispositivo puede tardar hasta 30 segundos y el uso de la CPU se incrementa hasta el 100%. [#577010]

Al visitar sitios de intranet con WorxWeb en un entorno de clústeres de varios nodos, es posible que los usuarios no puedan acceder a las URL y vean el mensaje "Error Invalid OTT." [#577273]

Si configura XenMobile con un servidor proxy, es posible que fallen los intentos de agregar credenciales de Google Play o crear una aplicación Android de tienda pública. [#578727]

Aparece una página en blanco al intentar abrir la consola de XenMobile en una versión publicada de Internet Explorer 11. [#578729]

Esta versión ahora respalda WPA2 Personal y WPA2 Enterprise para iOS 8. [#579616]

Si se agrega o se carga una aplicación en la consola de XenMobile, puede ocurrir un error al cargar la aplicación en XenMobile usando el mismo nombre de archivo que el de una aplicación existente. [#580359]

Los intentos de descargar aplicaciones Worx desde Worx Store fallan en un dispositivo Android. [#582044]

Al introducir una macro con el nombre de usuario y el número de teléfono, la transformación no traduce correctamente el número de teléfono. [#589130]

El comando Bypass Activation Lock puede no funcionar en algunos dispositivos iOS. [#589991]

Si el valor de la propiedad "memberOf" excede los 255 caracteres, aparece un mensaje de error que indica que no se han encontrado grupos ("No groups found").
Si los usuarios intentan abrir una aplicación de Windows a través de Worx Home, la enumeración se realiza correctamente, pero la aplicación no se abre. Los usuarios reciben el mensaje de error: "Could not add account." [#590046]

Si se crea una directiva de Simple Certificate Enrollment Protocol (SCEP) que requiere una contraseña de desafío, no se puede guardar la directiva. Con esta versión, el campo de contraseña de desafío es optativo. [#590798]

Si configura XenMobile para usar un servidor proxy, Android for Work no puede realizar una conexión con sitios Web externos. [#591707]

El intento de cargar una aplicación IPA en App Controller falla con el mensaje de error "Invalid package type for selected app". El mensaje aparece cuando hay un error en la imagen PNG. [#592748]

Cuand los usuarios intentan inscribirse, reciben el mensaje de error "User does not exist". El error ocurre después de eliminar la inscripción de los usuarios y volver a inscribirse. Cuando esto ocurre, se vuelven a crear los usuarios en Active Directory. [#593028]

Si crea una invitación de calendario desde una cuenta de Microsoft Outlook o Microsoft Exchange, puede tardar mucho tiempo en aparecer en WorxMail. [#594542]

Si configura un flujo de trabajo y usa un número de puerto diferente del predeterminado (443), los usuarios no pueden abrir el enlace del flujo de trabajo. [#599441]

Los usuarios no pueden actualizar una aplicación Android en sus dispositivos desde XenMobile Server. [#601251]

Los usuarios no pueden iniciar una sesión en aplicaciones Worx cuando se inscriben a través de Azure Active Directory. [#608505]

A partir de diciembre de 2015, Nexmo SMS respalda solo conexiones HTTPS. En XenMobile, el parámetro predeterminado es **ON**. Si se cambia el valor a **OFF**, esto no tiene efecto alguno. Después de actualizar, el valor sigue apareciendco como **OFF**, pero las conexiones son seguras. [#609306]

Worx Store requiere un usuario del Programa de compras por volumen (VPP) incluso aunque la licencia solo sea aplicable al dispositivo. [#610338]

Problemas conocidos de XenMobile Server 10.3

Jul 27, 2016

A continuación, se describen los problemas conocidos de XenMobile 10.3. Para obtener información sobre los problemas conocidos de XenMobile 10.3.5, consulte Problemas conocidos y resueltos de XenMobile 10.3.5.

- Los problemas siguientes están relacionados con la integración entre XenMobile y NetScaler para las siguientes versiones de NetScaler cuando el protocolo de seguridad TLS 1.2 está configurado en NetScaler:
  - Versiones de NetScaler 11.x anteriores a 11.0.64
  - 10.5.59
  - 10.5.58

  Observe que el problema no ocurre cuando la implementación MAM de XenMobile incluye un equilibrador de carga de NetScaler entre el servidor XenMobile y NetScaler Gateway.

  La comunicación entre NetScaler Gateway y XenMobile en modo MAM falla debido a problemas con una sesión de backend con TLS 1.2. Como resultado, los usuarios no pueden descargar aplicaciones desde WorxStore, ni archivos desde ShareFile, cuando conectan con la red interna. [#591600, #595713, #596566, #604409]
- El envío push de aplicaciones falla después de desinstalar una aplicación corporativa. [#591450]
- Después de quitar la licencia de una aplicación, la aplicación permanece en el dispositivo del usuario. Este es un problema de terceros. [#596656]
- Cuando los usuarios intentan inscribir su dispositivo personal con una cuenta de trabajo de Microsoft, la inscripción falla. [#597037]
- La directiva Términos y condiciones no aparece con un estado 'Instalado' o 'Pendiente' en la consola de XenMobile, aunque la directiva se haya implementado correctamente en el dispositivo. [#598407]
- Las directivas de restricción tienen efecto en dispositivos Windows 10. No obstante, los usuarios no reciben un mensaje para avisarles de que una función bloqueada está inhabilitada. [#599064, #606651]
- Si agrega una categoría con aplicaciones públicas y empresariales y luego inscribe un dispositivo en XenMobile, cuando los usuarios sincronizan las aplicaciones en Worx Home, la categoría no aparece. [#599495]
- Si no agrega el permiso de borrado selectivo de dispositivo al crear un control de acceso basado en rol (RBAC) de dispositivos compartidos, cuando los usuarios intentan eliminar su cuenta en Worx Home en un dispositivo iOS (en modo XenMobile Enterprise), los usuarios deben quitar manualmente el perfil de Device Manager del dispositivo. [#600705]
- Después de implementar las directivas App Inventory y Enterprise Hub para una aplicación y luego crear una aplicación pública con un nombre y una descripción diferentes, cuando los usuarios abren la aplicación desde Worx Home, el nombre y la descripción de la aplicación son los mismos. [#600369]
- Si configura Microsoft SQL Server en modo SSL durante el primer uso, y el certificado de la entidad de certificación (CA) no corresponde al certificado de SQL Server, la conexión falla. Si vuelve a intentar conectar con el certificado de CA apropiado que se corresponde con el certificado de SQL Server, la conexión sigue fallando. Para que el certificado funcione, reinicie el servidor XenMobile para borrar la caché de truststore. [#602609]
- Los nombres de usuario en los dispositivos de usuario compartidos deben contener solo alfabeto inglés. Los dispositivos

compartidos no respaldan nombres de usuario que tengan caracteres no incluidos en ASCII. [#605544]

- Cuando los usuarios reciben invitaciones de contraseña de uso único para enlaces de IMEI (nombre de usuario y contraseña) y notificaciones SMTP y SMS, el primer perfil se instala correctamente y la instalación del segundo perfil falla con el mensaje de error "Profile Installation Fails. A connection to the server could not be established". En dispositivos iPhone 6 e iPhone 6 Plus, hay un número IMEI y un número MEID y la contraseña de un solo uso se vincula con el número MEID en lugar de hacerlo con el número IMEI. Puede reemplazar el número IMEI con el identificador único de dispositivo (UDID) de iPhone, o usar un número de teléfono normal. [#606162]
- Después de actualizar a XenMobile 10.3, la información de licencias aparece como periodo de evaluación establecido en 30 días, y con el indicador de servidor de licencias configurado establecido en 'True'. Después de actualizar el servidor XenMobile. cargue la misma licencia en el servidor, lo que quitará la licencia de periodo de evaluación. [#607939]
- En tabletas Windows 8.1, los usuarios pueden quitar correctamente aplicaciones del dispositivo. Las aplicaciones de empresa siguen apareciendo en la consola de XenMobile en las propiedades del dispositivo. [#608184]
- Las opciones de borrado de aplicaciones (App Wipe) y borrado selectivo (Selective Wipe) funcionan igual en el modo Enterprise de XenMobile. [#608715]
- El servidor XenMobile deja de responder cuando se guarda o se abre un archivo en Internet Explorer. Puede reiniciar el servidor para continuar trabajando. [#608724]
- Después de actualizar a XenMobile 10.3, Android for Work no existe en la directiva de explorador Web, aunque existan direcciones Web bloqueadas y marcadores. [#609002]
- En tabletas que ejecutan Windows 8.1 y Windows 10, después de eliminar cuentas manualmente desde el dispositivo, algunas directivas siguen presentes. [#609201]
- En tabletas Windows 10, si los usuarios cambian el parámetro de actualización automática en el dispositivo, el cambio no aparece en la sección de Información de seguridad en las propiedades del dispositivo en la consola de XenMobile. [#609254]
- El nombre de Worx Store solo respalda nombres con caracteres del alfabeto inglés (ASCII). [#609535]
- El intento de descargar una solicitud de firma de certificado (CSR) desde Internet Explorer y Firefox falla, con el error: "The Webpage cannot be displayed". La descarga de la solicitud CSR desde Chrome sí que funciona. [#609552]
- Cuando se inicia una sesión en la consola de XenMobile, y se navega a **Analyze** > **Reporting** y luego se hace clic en **Inactive Devices**, aparece una pantalla en blanco en lugar de descargarse el archivo. [#609649]
- Al configurar un espacio de trabajo en Citrix Workspace Cloud, los grupos de entrega no se actualizan con los usuarios o grupos de Active Directory que pertenecen a dominios secundarios. [#609673]
- La inscripción de un dispositivo Windows 10 falla si hay varias directivas de Términos y condiciones implementadas y ninguna de ellas es la predeterminada. [#609694]
- Si se quita una directiva de un grupo de entrega, se hace clic en el botón **Summary** y luego se guarda la directiva, el recurso permanece en el grupo de entrega. Si se hace clic en **Next** en lugar de **Summary** , la directiva se quita del grupo de entrega. [#610109]
- Para conservar la extensión de archivo original en un dispositivo Windows CE, no especifique el nombre de archivo de destino en la directiva. [#610601]

- Cuando se configura una directiva de VPN de dispositivo para Mac OS X, la opción **VPN** aparece en la lista **Connection Types**. Sin embargo, no se puede configurar esta opción para dispositivos Mac OS X. [#612846]
- Al actualizar desde XenMobile 10.1 a la versión 10.3, si WorxStore tiene un nombre personalizado, debe cambiar el nombre del almacén al valor predeterminado **Store** e implementar el parámetro en los dispositivos antes de actualizar. De lo contrario, el nombre personalizado del almacén puede causar problemas con la inscripción en XenMobile 10.3, el acceso a Worx Home y WorxStore y la implementación de aplicaciones en dispositivos iOS. [#614049]
- No se puede habilitar Android for Work en la consola de XenMobile. Cuando se configuran parámetros de cuenta de Android for Work y se introduce el ID de cuenta de servicio obtenido en Google, que contiene solo números, aparece un error al guardar la configuración. Si se introduce el ID de cuenta de servicio usando el formato anterior de Google que contenía números y caracteres, ocurre el mismo error porque este formato no corresponde al ID de cuenta de servicio en el servidor XenMobile. Este es un problema de terceros.

  Como solución temporal, para habilitar Android for Work, agregue una propiedad de servidor para el ID de cliente de Google.

  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. Haga clic en **Add**. Aparecerá la página **Add New Server Property**.

  3. En la lista **Key** , haga clic en **Custom Key**.

  4. En **Key**, introduzca **google.aw.enterprise.client.id**

  5. En **Value**, introduzca la parte numérica del ID de cliente, como por ejemplo: 3838383838388383.

  6. Introduzca un nombre en **Display name**, como "ID cliente de dominio Google".

  7. Haga clic en **Save**.

  [#615118]
- En equipos Mac OS X e iPads, XenMobile 10.3 siempre lleva a cabo primero las acciones de eliminación, independientemente del orden establecido en la consola de XenMobile. [#620459]
- Después de habilitar la inscripción de iOS en masa y actualizar la entidad de certificación (CA) raíz del certificado SSL de XenMobile, la inscripción o la reinscripción de dispositivos puede fallar. El problema puede ocurrir cuando se cambia un certificado autofirmado por un certificado público, se compra un certificado de un proveedor nuevo, o se mueve a una CA interna de la empresa. El problema no afectará a los dispositivos ya inscritos. Como solución temporal, haga lo siguiente:

  1. En la consola de XenMobile, haga clic en **Settings** > **iOS Bulk Enrollment**.
  2. En **DEP Configuration**, junto a **Allow Device Enrollment Program (DEP)**, haga clic en **NO** y luego en **Save**. Espere unos segundos. Este paso quita el perfil DEP anterior de los dispositivos DEP en el portal DEP de Apple.
  3. Haga clic en **Manage** > **Devices**. Compruebe que no aparece ningún dispositivo registrado con DEP en la columna **DEP registered**.
  4. Haga clic en **Settings** > **iOS Bulk Enrollment** de nuevo.
  5. En **DEP Configuration**, junto a **Allow Device Enrollment Program (DEP)**, haga clic en **YES** y luego en **Save**. Espere unos segundos. Este paso fuerza la aplicación de un nuevo perfil para todos los dispositivos DEP.

6. Haga clic en **Test Connection** para asegurarse de que la conexión entre el servidor XenMobile y los servidores DEP de Apple todavía funciona.
7. Haga clic en **Manage** > **Devices** de nuevo. Compruebe que todos los dispositivos DEP están de nuevo registrados en la columna **DEP registered**.

Para obtener más información acerca de Apple DEP, consulte Inscripción de dispositivos iOS en masa.
[#635699]

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. Consulte Acerca de MDX Toolkit.
- 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.

XenMobile respalda una solución integrada que ofrece la administración de dispositivos y la administración de aplicaciones

mediante la consola de XenMobile. En esta sección se describe la arquitectura de referencia para la implementación de 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.

Para obtener más información sobre cómo configurar XenMobile 10 Enterprise Edition para una implementación de recuperación ante desastres, incluido un diagrama de la arquitectura, consulte la Guía de recuperación ante desastres de XenMobile.

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 los artículos 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.

Modo de administración de dispositivos móviles (MDM)

XenMobile MDM Edition ofrece la administración de dispositivos móviles para iOS, Android, Amazon y Windows Phone (consulte Plataformas de dispositivos respaldadas en XenMobile). Implemente XenMobile en modo MDM si va a usar solo las funciones 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). Implemente XenMobile en modo MAM (también denominado modo solo MAM) si va a usar solo las funciones de MAM de XenMobile sin inscribir los dispositivos 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

Utilizando conjuntamente los modos MAM y MDM se permite la administración de aplicaciones y datos móviles además de la administración de los dispositivos móviles para iOS, Android, Amazon y Windows Phone (consulte Plataformas de dispositivos respaldadas en XenMobile). Implemente XenMobile en modo ENT si va a usar las funciones de MDM y 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.

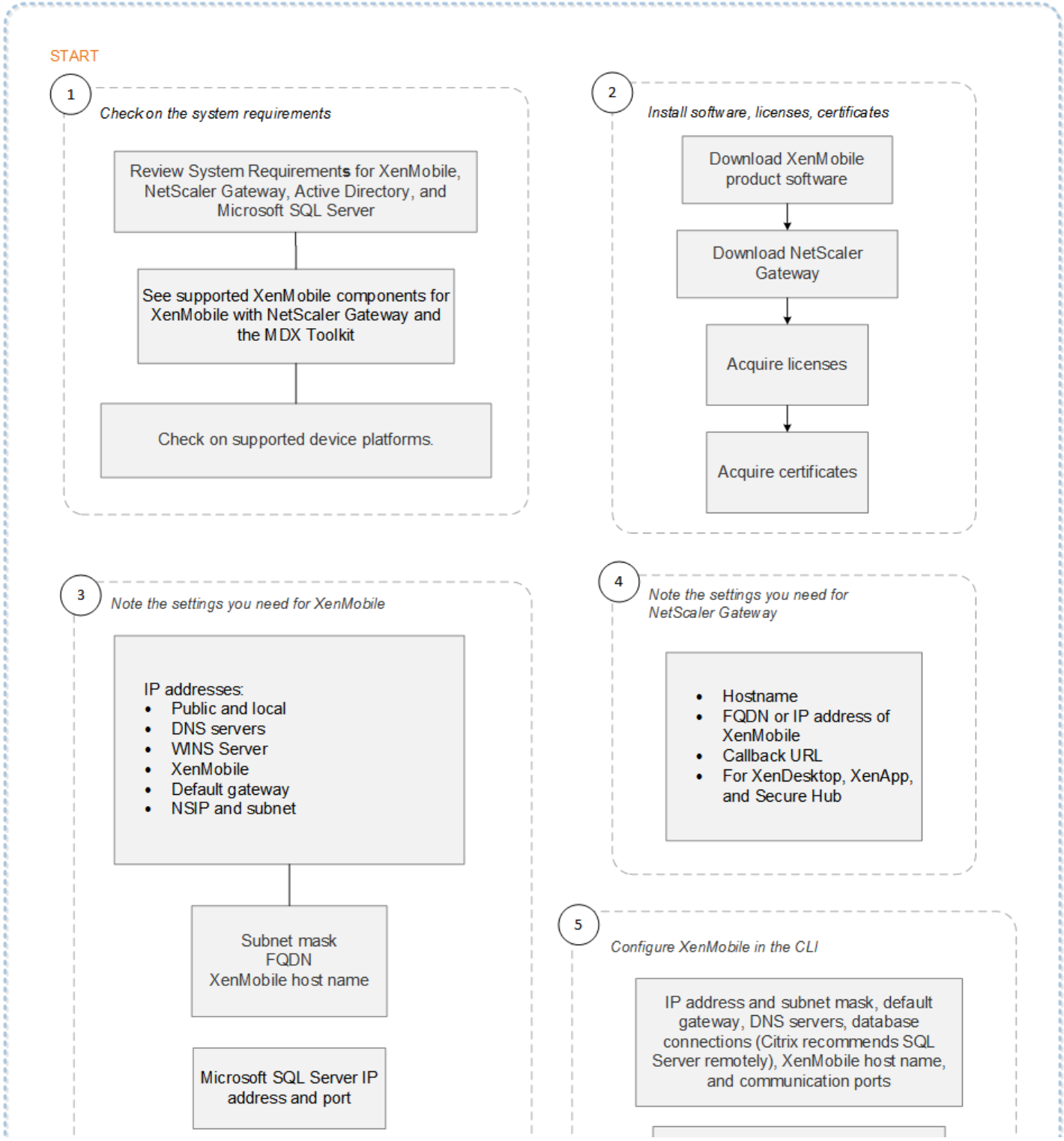
En el modelo de implementación recomendado, el servidor XenMobile se encuentra en la zona desmilitarizada (DMZ) con NetScaler Gateway en primer plano, lo que proporciona protección adicional para XenMobile.

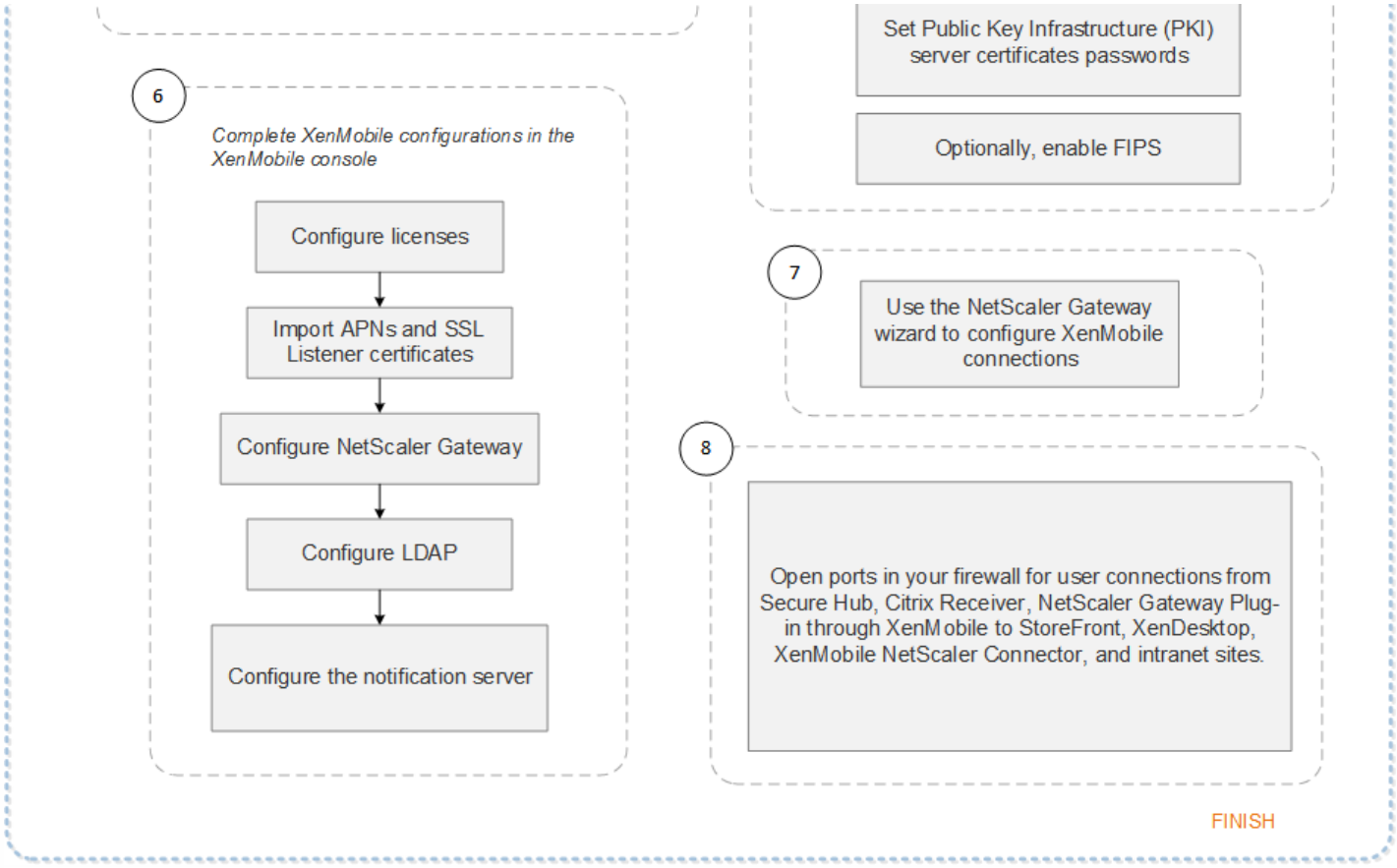
XenMobile en la red interna. Otra opción de implementación consiste en colocar el servidor XenMobile en la red interna, en lugar de la zona DMZ. Esta implementación se usa cuando las directivas de seguridad impiden colocar otros dispositivos, que no sean dispositivos de red, en la zona DMZ. Con esta implementación, ya que el servidor XenMobile no está en la zona DMZ, no es necesario abrir puertos en el firewall interno para permitir el acceso a los servidores SQL Server y PKI desde la zona DMZ.

Diagrama de flujo para la implementación de XenMobile con NetScaler Gateway

Oct 31, 2016

Puede utilizar este diagrama de flujo como guía para los pasos principales de la implementación de XenMobile 10.3 con NetScaler Gateway. Los enlaces a los temas de cada paso se muestran después de la imagen.





1

- Requisitos del sistema para XenMobile 10.3
- Compatibilidad de XenMobile
- Plataformas de dispositivos respaldados en XenMobile 10.3

2

- Instalación de XenMobile
- Certificados en XenMobile
- Licencias de XenMobile

3

- Lista de verificación de la instalación de XenMobile

4

- Lista de verificación de la instalación de XenMobile

5

- Configuración de XenMobile en la ventana del símbolo del sistema

6

- Configuración de XenMobile en un explorador Web

7

- Configuración de parámetros para el entorno de XenMobile

8

- Requisitos de puertos para XenMobile

El diagrama de flujo también está disponible en formato PDF.

Diagrama de flujo para la implementación de XenMobile

Escalabilidad de XenMobile

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.

La información incluida en este artículo está pensada para guiarle a la hora de determinar el rendimiento y la escalabilidad de la infraestructura de XenMobile 10.3. 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/ dispositivos).

- 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 se define como la integración de nuevos usuarios y 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.

Escalabilidad	Hasta 100,000 dispositivos	
Índices de inicios de sesión	Integración (primer uso)	Un máximo de 2777 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

> **Important**
>
> El requisito de automatización para este informe es de 1000 a 100000 dispositivos. Los requisitos de más de 100000 dispositivos quedan fuera del alcance de este informe.

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 configurados 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.

- La cantidad de conexiones por sesión de usuario en NetScaler es una consideración importante.
- 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.

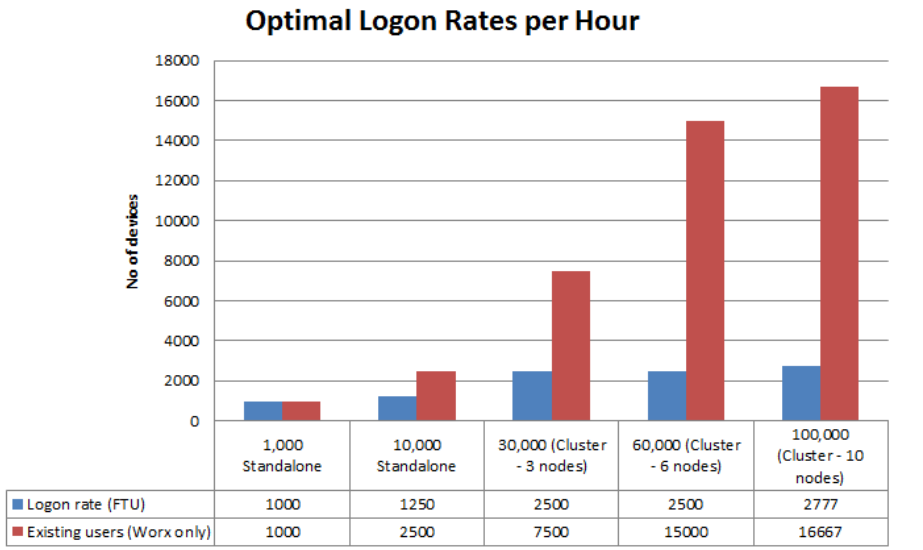
En la tabla anterior, se muestran los índices de inicios de sesión recomendados para usuarios existentes y nuevos. A su vez, esta recomendación se basa en la configuración de XenMobile, el dispositivo NetScaler Gateway, la configuración de clústeres y la base de datos. Puede utilizar los datos de esta 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 de la inscripción y de los inicios de sesión y, por el otro, las recomendaciones del hardware apropiado.

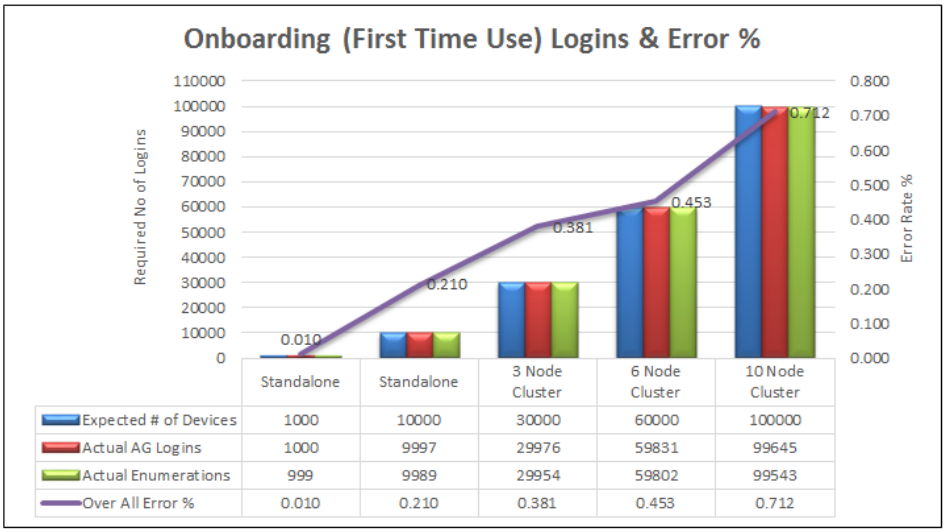
Cantidad estimada de dispositivos	1,000	10 000	30,000	60,000	100,000
Cantidad real de dispositivos	1,000	9,997	29,976	59.831	99,645
Índice de inicios de sesión					
Integración (primer uso)	125	1,250	2,500	2,500	2,777
Usuarios existentes (solo Worx)	1,000	2,500	7,500	15,000	16 667
Configuración					
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 XenMobile	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
Base de datos	Externa	Externa - Microsoft SQL Server Memoria = 16 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 16 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 32 GB Unidades vCPU = 12	Externa - Microsoft SQL Server Memoria = 32 GB Unidades vCPU = 16

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

La información siguiente ofrece puntos de datos adicionales que fueron registrados y que afectan a los resultados de la tabla anterior.

- Latencia de inscripción o de inicio de sesión (tiempo de ida y vuelta)
  - Latencia media total: de 0,5 a 1,5 segundos
  - Latencia media de un inicio de sesión de NetScaler Gateway: > 120 a 440 milisegundos
  - Latencia media de una solicitud de Worx Store: de 2 a 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.
  - Respuesta lenta de la consola de XenMobile durante fases de carga alta.



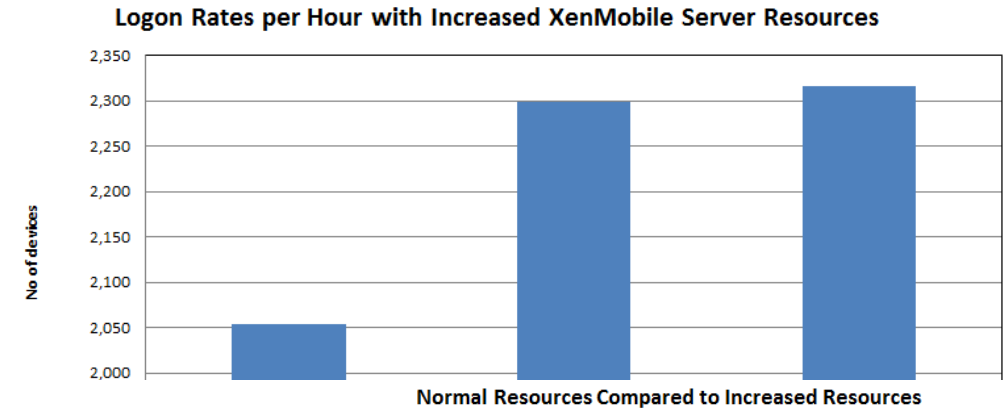


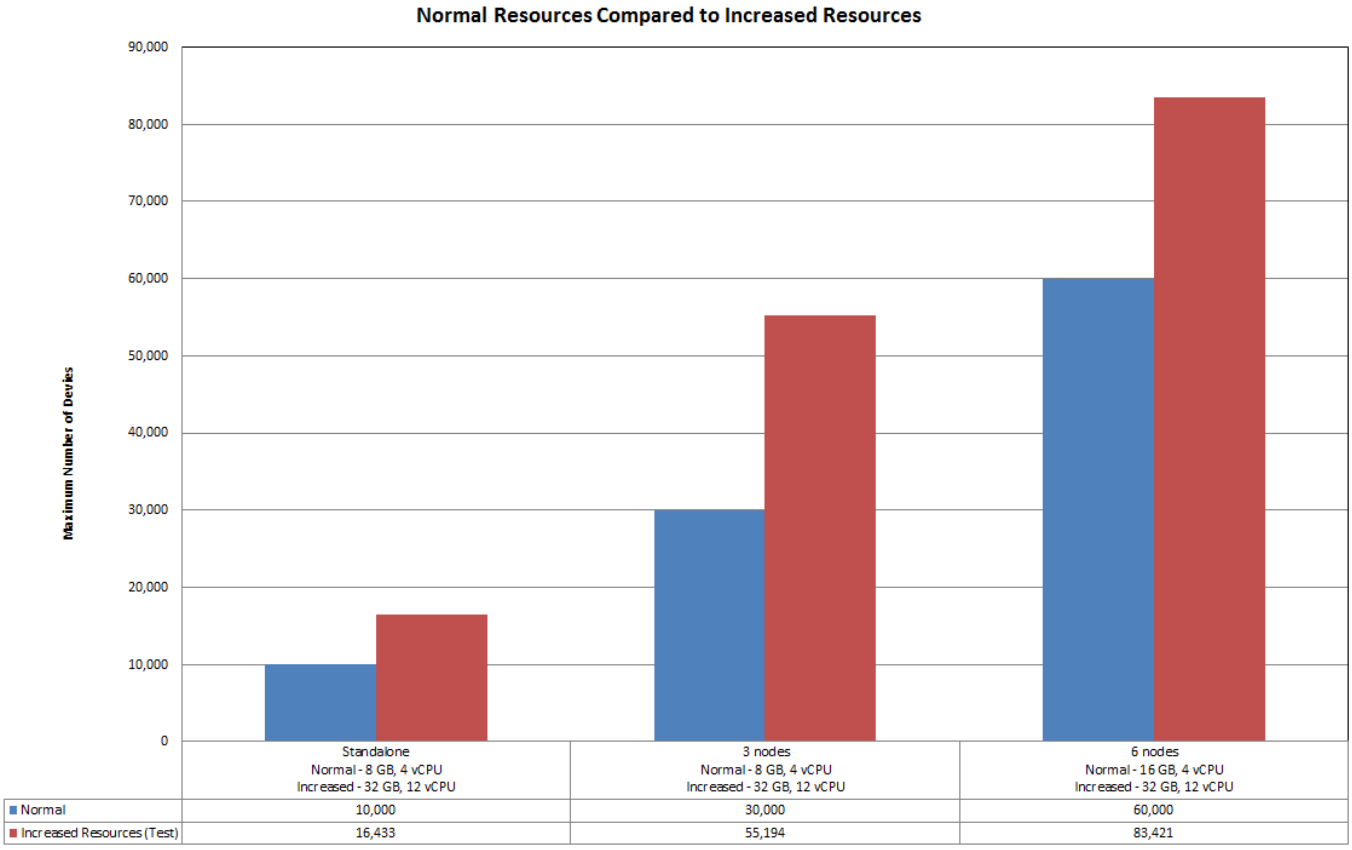
El porcentaje de error mostrado en la imagen anterior incluye errores generales obtenidos en solicitudes correspondientes a todas las operaciones, sin limitarse únicamente a los inicios de sesión. El porcentaje de error se encuentra dentro del límite aceptable del 1% para cada prueba realizada, tal y

como se define en Criterios de salida.

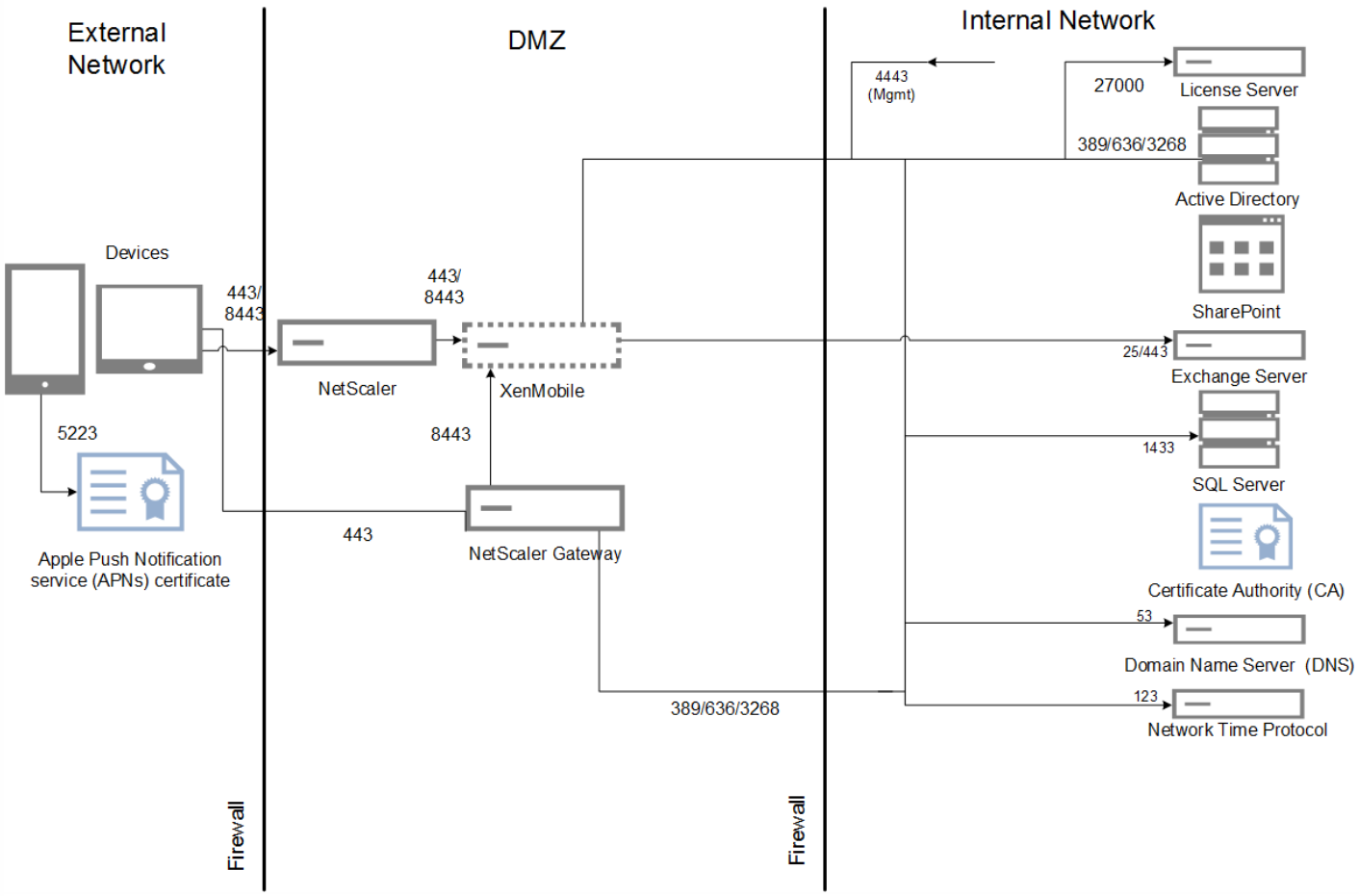
Los resultados de esta prueba ofrecen información útil para la estrategia de implementación de XenMobile Enterprise Edition con una cantidad de nodos inferior, para dar respaldo a más dispositivos. La prueba se ha ejecutado con una mayor cantidad de recursos para los componentes de hardware (CPU y memoria) de cada nodo de servidor XenMobile, para medir sus capacidades de escalabilidad. Esto resultó en un aumento de la cantidad máxima de sesiones/dispositivos respaldados por los nodos de servidor XenMobile en comparación con la prueba realizada con recursos normales y la misma cantidad de nodos.

Escalabilidad			
Cantidad máxima de dispositivos reales	16,433	55,194	83,421
Índice de inicios de sesión			
Incorporación de nuevos usuarios y primer uso	2,054	2,299	2,317
Configuración			
Entorno de referencia	VPX-XenMobile en modo autónomo	MPX-Clúster de XenMobile 3	MPX-Clúster de XenMobile 6
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
Modo de XenMobile	Autónomo	Clúster	Clúster
Clúster de XenMobile	N/D	3	6
Dispositivo virtual de XenMobile	Memoria: 32 GB Unidades vCPU: 12	Memoria: 32 GB Unidades vCPU: 12	Memoria: 32 GB Unidades vCPU: 12
Base de datos de Device Manager	Externa - Servidor SQL Memoria: 16 GB Unidades vCPU: 12	Externa: - Servidor SQL Memoria: 32 GB Unidades vCPU: 12	Externa -SQL Server Memoria: 32GB Unidades vCPU: 16
Active Directory	Memoria: 8 GB Unidades vCPU = 4	Memoria: 16 GB Unidades vCPU: 4	Memoria: 16 GB Unidades vCPU: 4

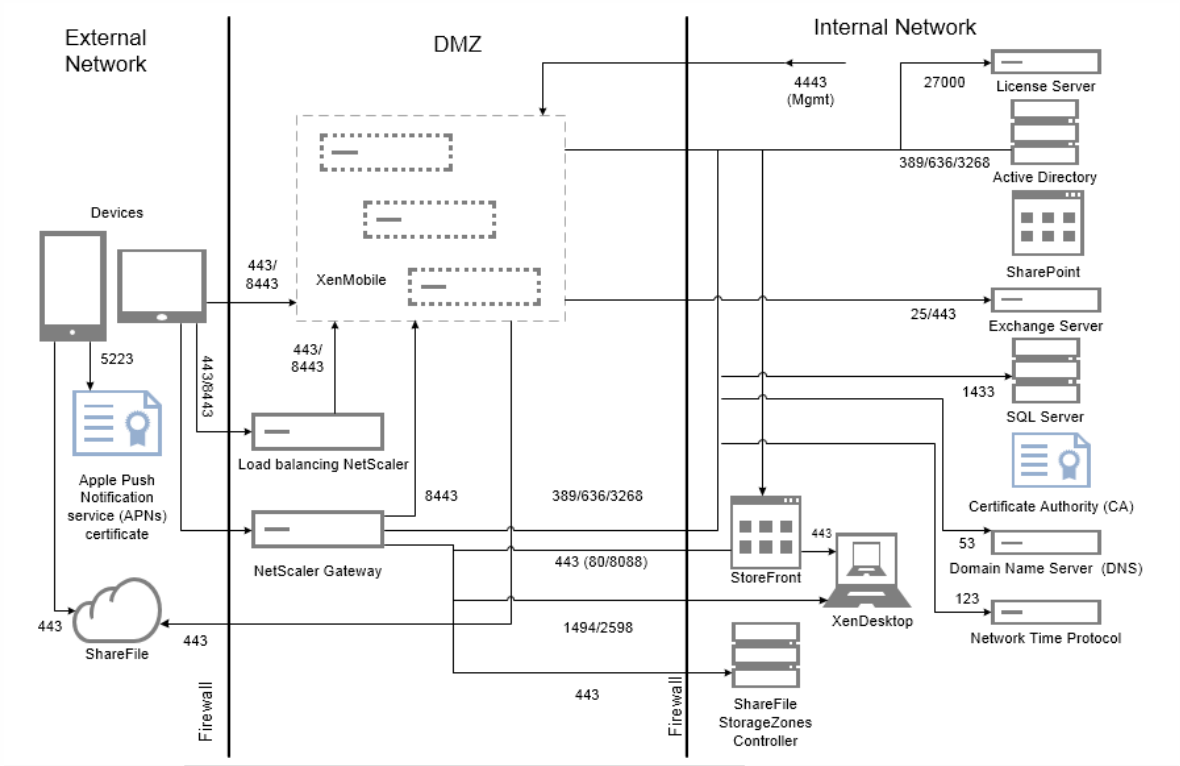




En la siguiente imagen, se muestra la arquitectura de referencia para una implementación a pequeña escala. Es una arquitectura autónoma que admite un máximo de 10 000 dispositivos.



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 MAM a través de HTTP que admite 10 000 dispositivos o más.



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 100 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.

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

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.

Notas e hipótesis

Para poder ampliar la infraestructura de XenMobile a más de 30 000 dispositivos, debe ajustar los siguientes parámetros de servidor:

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

-

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

Debe llevar a cabo estos cambios en todos los nodos de XenMobile y, una vez realizados, reiniciar el servidor.

Los casos siguientes no forman parte de las pruebas de escalabilidad. Estos casos se tendrán en cuenta para las siguientes mejoras en las pruebas de escalabilidad:

- No se han probado dispositivos Android conectados.
- No se ha probado la implementación de paquetes.
- No se ha probado la plataforma Windows.

Cada instancia de XenMobile admite un máximo de 10 000 conexiones simultáneas.

Las pruebas se realizaron en condiciones idóneas con conexión LAN para evitar problemas de latencia de red. En una situación real, la escalabilidad también depende del ancho de banda de que disponga el usuario, sobre todo para la descarga de aplicaciones.

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 (Web, SaaS y aplicaciones MDX móviles) incluida la comprobación de estado de los dispositivos
- Envío push de directivas (para iOS)
- 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 se definen en la tabla siguiente:

Dispositivos	Registro de dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Inicios de WorxStore por dispositivo	Single Sign-On para aplicaciones Web o SaaS por dispositivo	Descargas de aplicaciones MDX por dispositivo	Descargas de aplicaciones requeridas activadas a través de XenMobile	Directivas enviadas via push por dispositivo (iOS)
1000	1000	1000	14	4	4	2	2	2
10000	10000	10000	14	4	4	2	2	2
30000	30000	30000	14	4	4	2	2	2
60000	60000	60000	14	4	4	2	2	2
100000	100000	100000	14	4	4	2	2	2

Usuarios existentes cargas de trabajo de conexiones Worx solamente

La tabla siguiente muestra la carga de trabajo de usuarios existentes (con conexiones Worx solamente). 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. Esto es posible porque al utilizar solo estas dos aplicaciones Worx, la red tiene una carga reducida. Para la aplicación WorxWeb, el usuario accede a sitios Web internos que no provocan el inicio de sesión SSO en el servidor XenMobile. Las operaciones en este modo son las siguientes:

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

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

Dispositivos	Enumeraciones	Aplicaciones enumeradas por dispositivo	Túneles VPN por dispositivo[1]
1000	1000	14	4
10000	10000	14	4

30000	30000	14	4
60000	60000	14	4
100000	100000	14	4

1. La cantidad de túneles VPN corresponde a conexiones WorxMail y WorxWeb.

Los perfiles de conexión para WorxMail y WorxWeb se describen en la tabla siguiente:

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).

Estas recomendaciones se basan en perfiles de WorxMail y WorxWeb utilizados para automatizar una carga de trabajo "media". Las modificaciones realizadas en los detalles de conexión afectan los resultados de los análisis. Por ejemplo, si se 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

Los perfiles utilizados para cada aplicación están diseñados para automatizar una carga de trabajo muy intensa. Las tablas siguientes muestran los detalles de los perfiles de WorxMail y WorxWeb.

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

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.

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).

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

Componente	Versión
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
Base de datos externa	Microsoft SQL Server 2014

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

Proveedor	Genuine Intel

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).

Acerca de XenMobile Cloud

Jul 27, 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.

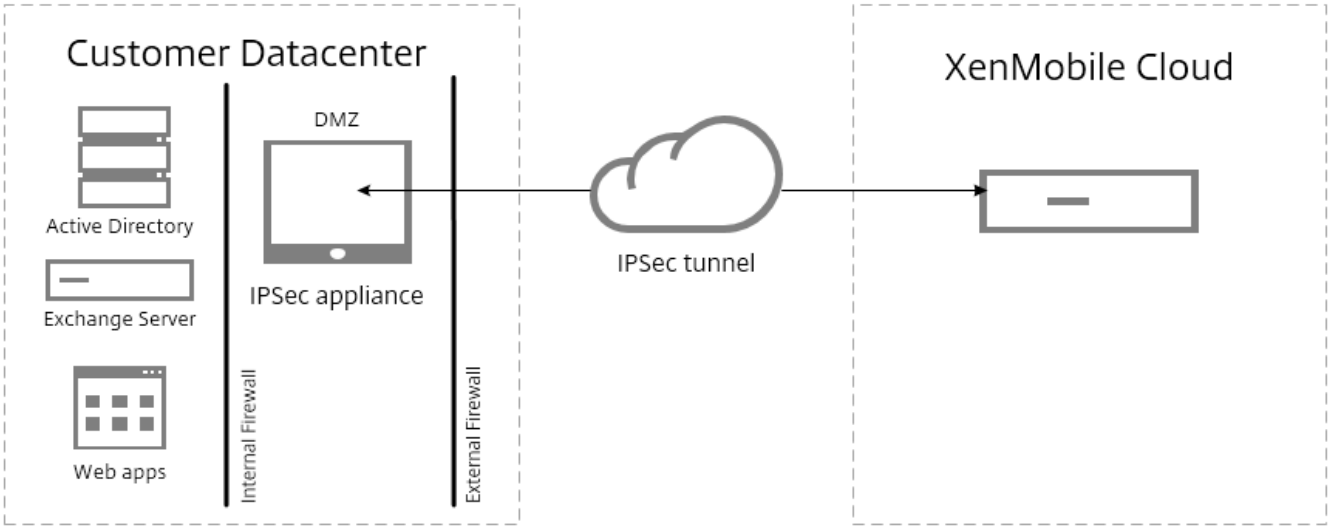
Los administradores de Cloud Operations se encargan del mantenimiento y la configuración de la conectividad de red, así como de la integración de productos Citrix como NetScaler, XenApp, XenDesktop, StoreFront y ShareFile. El entorno de Cloud se aloja en centros de datos de Amazon ubicados en todo el 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 más información, consulte Cómo ver y analizar archivos de registros en XenMobile.

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



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

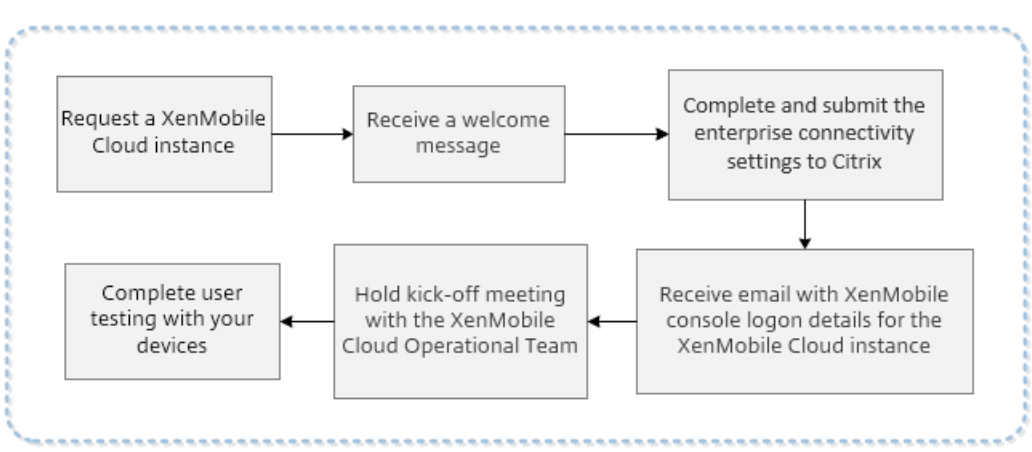
Para obtener instrucciones paso a paso acerca de la personalización de roles, consulte Configuración de roles con RBAC.

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

Jul 27, 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 (AWS) 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.

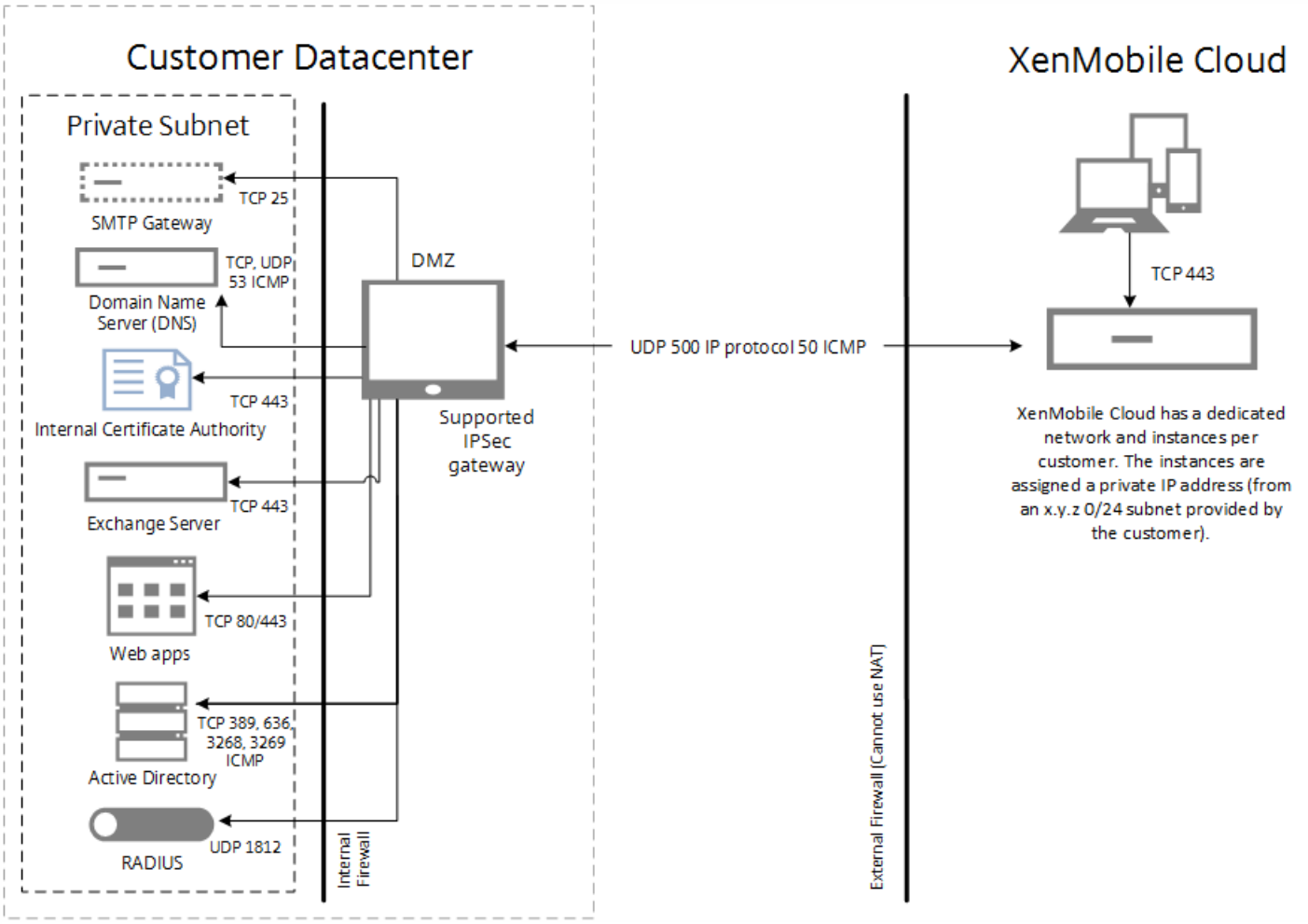
> ## Nota
>
> Si su puerta de enlace IPsec no figura en la lista aprobada, es posible que funcione de todos modos con XenMobile Cloud, pero puede tardar más en configurarse. Asimismo, puede que sea necesario usar una de las puertas de enlace IPSec respaldadas oficialmente como plan de reserva.

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 conexión VPN de AWS requiere una conexión Keep-Alive (permanente) iniciada desde el lado del cliente. Configure un ping permanente desde su entorno a la subred de Amazon VPC para garantizar la continuidad del servicio.

La conexión VPN de AWS no admite la configuración de varias asociaciones de seguridad en la puerta de enlace IPsec. Está limitado a un par único de asociación de seguridad en cada túnel, uno de entrada y otro de salida. Consolide las reglas y los filtros para garantizar que impiden el tráfico no deseado.

La siguiente ilustración muestra cómo se configura el túnel IPsec en XenMobile Cloud para conectarse a los servicios de su 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 públicas de VPN IPCSEC de XenMobile Cloud (AWS) [1]	Dispositivo IPSec del cliente	ID de protocolo IP	50	Protocolo ESP de IPSec.
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	LDAP(TCP)	389, 636 3268, 3269	Para la autenticación de usuarios en Active Directory y consultas de directorio a los controladores de

	centro de datos del cliente			dominio.
Subred /24 de cliente, no utilizada y enrutable [2]	Controladores de dominio de Active Directory en el centro de datos del cliente	ICMP		Para la solución de problemas (puede quitarse después de completarse la instalación entera).
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, no utilizada y enrutable [2]	Servidor RADIUS	UDP	1812	Optativo (no utilizado para pruebas 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 Activación de 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

Jul 27, 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.

- 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.

- 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.

- 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 10.3, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.5.x o 6.2.x); para obtener información más detallada, consulte XenServer.
  - VMware (versiones compatibles: ESXi 5.1, ESXi 5.5 o ESXi 6.0). Para obtener información más detallada, consulte VMware. Tenga en cuenta que ESXi 6.0 solo recibe respaldo en XenMobile 10.3.x.
  - 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
- Cuatro unidades CPU vittuales
- 8 GB de RAM
- 50 GB de espacio en disco

La configuración recomendada para 10 000 o más dispositivos es la siguiente:

- Procesador de cuatro núcleos con 8 GB de RAM para cada nodo.

XenMobile 10.3.x requiere el servidor de licencias de Citrix 11.12.1 o una versión posterior.

Requisitos del sistema para NetScaler Gateway

Para ejecutar NetScaler Gateway con XenMobile 10.3, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.2.x, 6.1.x o 6.0.x)
  - VMware (versiones respaldadas: ESXi 4.1, ESXi 5.1, ESXi 5.5 o ESXi 6.0)
  - Hyper-V (versiones respaldadas: Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2)
- 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 10.3

XenMobile requiere una de las siguientes bases de datos:

- Microsoft SQL Server

  El repositorio de XenMobile admite una base de datos de Microsoft SQL Server que se ejecute en alguna de las siguientes versiones compatibles (para obtener más información acerca de las bases de datos de Microsoft SQL Server, consulte Microsoft SQL Server):

  Microsoft SQL Server 2016
  Microsoft SQL Server 2014
  Microsoft SQL Server 2012
  Microsoft SQL Server 2008 R2

Microsoft SQL Server 2008

XenMobile 10.1 admite grupos de disponibilidad AlwaysOn de SQL Server.

Citrix recomienda usar Microsoft SQL de forma remota.

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 usa otra versión de servidor, 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

- PostgreSQL

  PostgreSQL se incluye con XenMobile. Puede usarlo de forma local o remota.

  Nota: Todas las ediciones de XenMobile admiten Remote PostgreSQL 9.3.11 para Windows, con las siguientes limitaciones:

  - Respaldo para un máximo de 300 dispositivos

    Utilice instalaciones de SQL Server locales si tiene más de 300 dispositivos.

  - No hay respaldo para clústeres

Compatibilidad de StoreFront

StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Interfaz Web 5.4
XenApp y XenDesktop 7.9
XenApp y XenDesktop 7.8
XenApp y XenDesktop 7.7
XenApp y XenDesktop 7.6
XenApp y XenDesktop 7.5
XenApp 6.5

Requisitos de servidor de correo de XenMobile 10.3

XenMobile 10.3 respalda el uso de los siguientes servidores de correo:

- Exchange 2016
- Exchange 2013
- Exchange 2010

Compatibilidad de XenMobile

Jul 27, 2016

Para ver un resumen de los componentes de XenMobile que se pueden integrar, consulte Compatibilidad de XenMobile.

Plataformas de dispositivos respaldados

Jul 27, 2016

Encontrará la lista completa de dispositivos que XenMobile 10.x respalda para la administración de la movilidad empresarial en Plataformas de dispositivos respaldados en XenMobile.

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
389	Se usa para conexiones de protocolo LDAP no seguras.	XenMobile	Servidor de autenticación LDAP o Active Directory
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 notificaciones push de Apple (APNs) a gateway.push.apple.com para notificaciones de dispositivos iOS y la inserción de directivas de dispositivo.	XenMobile	Internet (hosts APNs con la 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)
8081	Se utiliza para los túneles de aplicaciones desde el cliente optativo Remote Support Client para MDM. El valor predeterminado es 8081.	Remote Support Client	Internet, para túneles de aplicaciones hacia dispositivos de usuario (Android y Windows solamente)
8443	Utilizado para la inscripción de dispositivos iOS y Windows Phone.	Internet Red LAN y Wi-Fi	XenMobile

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 y 10.3 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 del servicio ADS.

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

Los clientes que quieran habilitar la fijación de certificados, deben cumplir los requisitos siguientes:

- **Obtener 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	IP address
discovery.mdm.zenprise.com	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
	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

Jul 27, 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

Oct 31, 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. Para obtener más información sobre el respaldo para globalización para todos los productos Citrix, consulte http://support.citrix.com/article/CTX119253.

Respaldo para idiomas en aplicaciones móviles Worx

Una "X" indica que la aplicación está disponible en ese idioma concreto. Actualmente, Secure Forms solo está disponible en inglés.

iOS						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
Japonés	X	X	X	X	X	X
Chino simplificado	X	X	X	X	X	X
Chino tradicional	X	X	X	X	X	X
Francés	X	X	X	X	X	X
Alemán	X	X	X	X	X	X
Español	X	X	X	X	X	X
Coreano	X	X	X	X	X	X
Portugués	X	X	X	X	X	X
Neerlandés	X	X	X	X	X	X
Italiano	X	X	X	X	X	X
Danés	X	X	X	X	X	X

Sueco	X	X	X	X	X	X
Hebreo	X	X	X	X	X	X
Árabe	X	X	X	X	X	X

Android						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
Japonés	X	X	X	X	X	X
Chino simplificado	X	X	X	X	X	X
Chino tradicional	X	X	X	X	X	
Francés	X	X	X	X	X	X
Alemán	X	X	X	X	X	X
Español	X	X	X	X	X	X
Coreano	X	X	X	X	X	X
Portugués	X	X	X	X	X	X
Neerlandés	X	X	X	X	X	X
Italiano	X	X	X	X	X	X
Danés	X	X	X	X	X	X
Sueco	X	X	X	X	X	X

Hebreo	X	X	X	X	X	
Árabe	X	X	X	X	X	

Windows			
	Worx Home	**WorxMail**	**WorxWeb**
Francés	X	X	X
Alemán	X	X	X
Español	X	X	X
Italiano	X	X	X
Danés	X	X	X
Sueco	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 consola de XenMobile está disponible en chino simplificado, francés, coreano, alemán y portugués.

Compatibilidad con Right-to-Left

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

Jul 27, 2016

Puede usar esta lista de verificación para anotar los requisitos previos y los parámetros de la instalación de XenMobile. 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 nombre 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	

Licencia

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 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	

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 10.3 y Lista de verificación previa a la instalación de XenMobile.

> ### Nota
>
> Compruebe que el hipervisor está configurado con la hora correcta (ya sea mediante un servidor NTP o una configuración manual) porque XenMobile utiliza esa hora.

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 a través de 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.
- - Elimine el archivo Virtual Machines/.xml
  - Mueva el archivo Legacy/.exp a Virtual Machines

Para instalar Windows Server 2008 R2 o Windows Server 2012, lleve a cabo lo siguiente:

Estos pasos son necesarios porque hay dos versiones diferentes del archivo de manifiesto de Hyper-V que representa la configuración de máquina virtual (.exp y .xml). Las versiones Windows Server 2008 R2 y Windows Server 2012 solo admiten .exp. Para esas versiones, solo debe tener el archivo de manifiesto EXP en la ubicación adecuada antes de la instalación.

Windows Server 2012 R2 no requiere estos pasos adicionales.

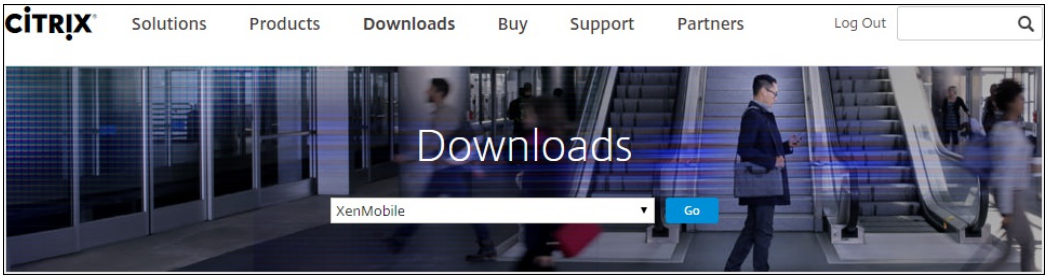
Modo FIPS 140-2: Si tiene pensado instalar el servidor XenMobile en modo FIPS, necesitará completar una serie de requisitos previos, según se describe en Configuración de FIPS con XenMobile.

Descarga del software del producto XenMobile

Puede descargar el software del producto desde el sitio Web de Citrix. Tiene que iniciar sesión primero en el sitio y después usar el enlace de Descargas en la página Web de Citrix para ir a la página que contiene el software que quiera descargar.

Cómo descargar el software de XenMobile

1. Vaya al sitio Web de Citrix.
2. Junto al cuadro de búsqueda, haga clic en Iniciar sesión e inicie una sesión con su cuenta.
3. Haga clic en la ficha Descargas.
4. En la página Descargas, en la lista de selección de productos, haga clic en XenMobile.



5. Haga clic en Go. Aparecerá la página XenMobile.
6. Expanda XenMobile 10.
7. Haga clic en XenMobile 10.0 Server.
8. En la página XenMobile 10.0 Server, haga clic en Download, situado junto a la imagen virtual apropiada que hay que usar para instalar XenMobile en XenServer, VMware o Hyper-V.
9. 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. Si todavía no ha iniciado sesión en el sitio Web de Citrix, haga clic en Iniciar sesión junto al cuadro de búsqueda e inicie una sesión con su cuenta.
3. Haga clic en la ficha Descargas.
4. En la página Descargas, en la lista de productos, haga clic en NetScaler Gateway.
5. Haga clic en Go. Aparecerá la página NetScaler Gateway.
6. En la página NetScaler Gateway, expanda la versión de NetScaler Gateway que se está ejecutando.
7. Debajo de Firmware, haga clic en la versión del software de dispositivo que desea descargar.
   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.
8. Haga clic en la versión de software del dispositivo que desea descargar.
9. En la página de software del dispositivo correspondiente a la versión que quiere descargar, haga clic en Download para descargar el dispositivo virtual.
10. 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. Configure la dirección IP y la máscara de subred, la puerta de enlace predeterminada, los servidores DNS, etcétera, para

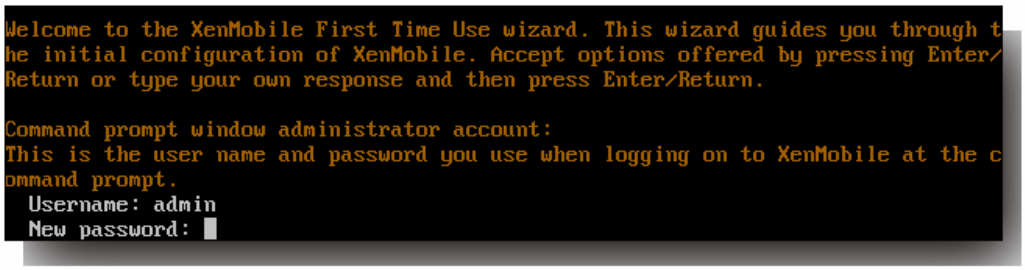
XenMobile mediante la consola de línea de comandos de XenCenter o vSphere.

2. Inicie sesión en la consola de administración de XenMobile y siga 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. Para ello, introduzca el nombre de usuario y la contraseña del administrador.
   Importante:
   Al crear o modificar las contraseñas de la cuenta de administrador del símbolo del sistema, de los certificados del servidor de infraestructura de clave pública (PKI) y de FIPS, XenMobile impone las siguientes reglas para todos los usuarios excepto para los usuarios de Active Directory cuyas contraseñas están administradas fuera de XenMobile:
   - La contraseña debe tener al menos 8 caracteres y debe satisfacer al menos tres de los siguientes criterios de complejidad:
     - Letras mayúsculas (de la 'A' a la 'Z')
     - Letras minúsculas (de la 'a' a la 'z')
     - Números (del 0 al 9)
     - Caracteres especiales (tales como: !, #, $, %)



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

4. Facilite la siguiente información de red y, a continuación, escribay; para confirmar la configuración:
   1. IP address
   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)

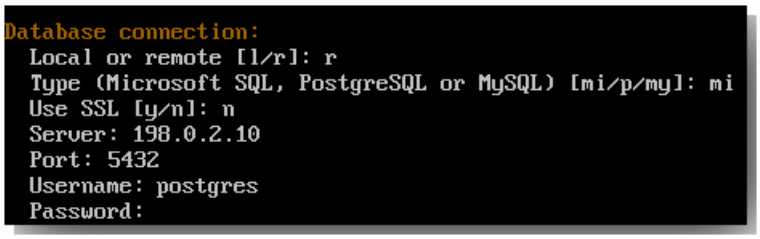
Nota: Las direcciones que se muestran en esta imagen y las imágenes siguientes no son operativas; se proporcionan simplemente como ejemplos.

5. Escribay; para aumentar la seguridad mediante la generación de una frase secreta aleatoria. También puede escribirn para proporcionar 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. La frase secreta no se puede ver.

   Nota: Si quiere ampliar el entorno y configurar servidores adicionales, debe facilitar 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 obtener información más detallada acerca del estándar 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. Proporcione la siguiente información para configurar la conexión con la base de datos:



1. La base de datos puede ser local o remota. Escribal para la local o bien-r para la remota.
2. Seleccione el tipo de base de datos. Escribami para Microsoft SQL, o bien escribap para PostgreSQL.
   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.

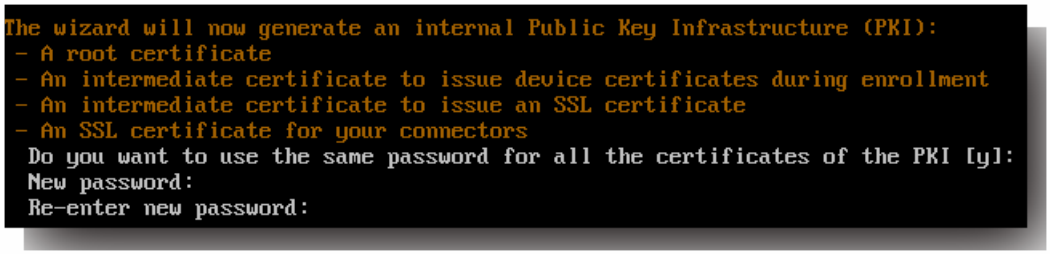
- No se respalda la migración de la base de datos. Las bases de datos creadas en un entorno de prueba no se pueden mover a un entorno de producción.

3. Si lo prefiere, escribay; para usar autenticación SSL en la base de datos.
4. 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.
5. Introduzca el número de puerto de la base de datos si es diferente del número de puerto predeterminado. El puerto predeterminado para Microsoft SQL es 1433 y el puerto predeterminado para PostgreSQL es 5432.
6. Introduzca el nombre de usuario del administrador de la base de datos.
7. Introduzca la contraseña del administrador de la base de datos.
8. Introduzca el nombre de la base de datos.
9. Presione Entrar para confirmar los parámetros de la base de datos.

8. Si lo prefiere, escribay; para habilitar la organización en clúster de nodos o instancias de XenMobile.
   Importante: Si habilita un clúster de XenMobile, después de completarse la configuración del sistema, abra el puerto 80 para habilitar la comunicación en tiempo real entre miembros del clúster. Esto debe hacerse en todos los nodos del clúster.
9. Introduzca el nombre de dominio completo (FQDN) del servidor XenMobile.

10. Presione Entrar para confirmar los parámetros.
11. 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).

12. Omita la siguiente pregunta acerca de la actualización de una versión anterior de XenMobile ya que está instalando XenMobile por primera vez.
13. Escribay; si quiere usar la misma contraseña para cada certificado de infraestructura de clave pública (PKI). Para obtener información más detallada acerca de la función PKI de XenMobile, consulte Carga de certificados en XenMobile.

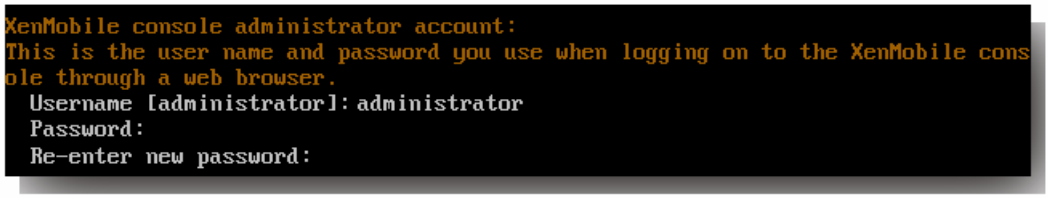


    Importante: Si va a agrupar nodos o instancias de XenMobile en clúster, debe proporcionar contraseñas idénticas para los nodos subsiguientes.

14. Introduzca la nueva contraseña y, a continuación, vuelva a introducir la nueva contraseña para confirmarla.

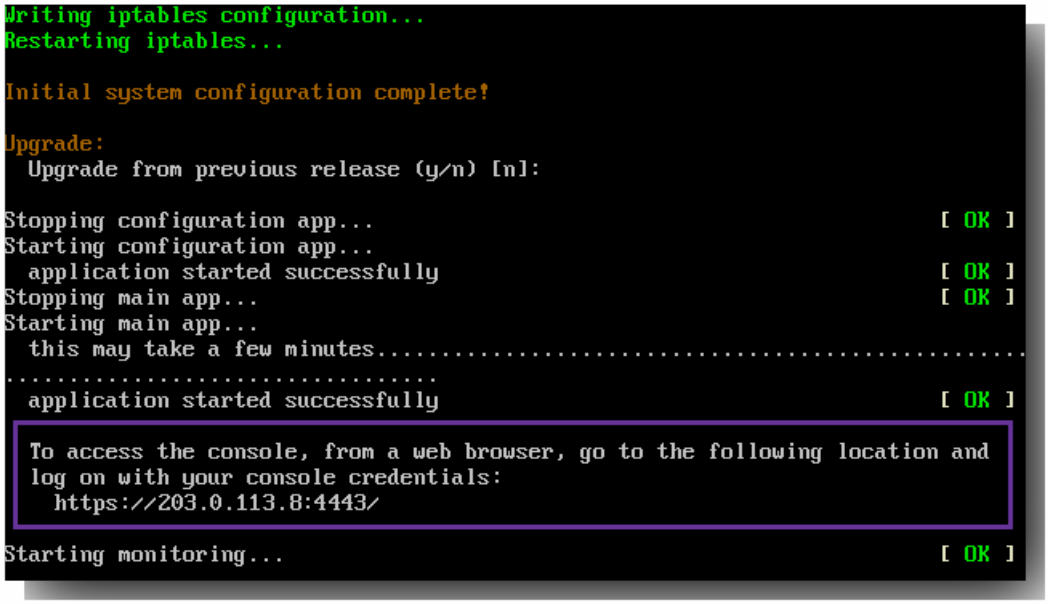
Nota: No aparecerá ningún carácter (como, por ejemplo, asteriscos) cuando escriba la nueva contraseña. No aparece nada.

15. Presione Entrar para confirmar los parámetros.
16. 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.

17. Presione Entrar para confirmar los parámetros. La configuración inicial del sistema se guardará.
18. Cuando se le pregunte si se trata de una actualización, escriban porque es una instalación nueva.
19. Copie toda la URL que aparece en pantalla, y continúe la siguiente configuración inicial de XenMobile con 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 al final de la configuración en la ventana del símbolo del sistema.
2. Introduzca 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: Este paso 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.
   - 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

Jul 27, 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.

Actualización de XenMobile

Oct 31, 2016

Cuando hay disponibles nuevas versiones o actualizaciones importantes de XenMobile, se publican en Citrix.com y se envía un aviso al contacto registrado de cada cliente. Existen tres opciones principales para actualizar XenMobile, dependiendo de la versión que se esté utilizando:

- **Para actualizar desde XenMobile 9.0**: MDM Edition, App Edition y Enterprise Edition
  Primero debe actualizar a XenMobile 10.1, mediante la herramienta Upgrade Tool. Puede descargar la herramienta desde la página de descargas de Citrix.com. Para obtener información detallada sobre la herramienta Upgrade Tool, consulte Actualización de XenMobile.

  Con la versión más reciente de la herramienta Upgrade Tool, ahora puede migrar los datos de los siguientes tipos de dispositivos, cuando actualiza desde XenMobile 9 a XenMobile 10.1 y luego instala una actualización a la versión XenMobile 10.3.x:

  Windows CE
  Windows 10 Phone
  Windows 10 Tablet

  En la versión actual de la herramienta Upgrade Tool, cuando la consola multiarrendatario o MTC (Multi-Tenant Console) está habilitada en XenMobile 9.0, puede migrar instancias de XenMobile 9 administradas con MTC a instancias independientes de XenMobile 10. XenMobile 10 no respalda la consola MTC, de modo que debe administrar estas instancias individualmente. Para ver más información, consulte Actualización del servidor de consola multiarrendatario (MTC) a XenMobile 10.1.
- **Para actualizar desde XenMobile 10.1 a XenMobile 10.3.x**
  Puede utilizar la página **Release Management** en la consola de XenMobile, tal y como se describe en el artículo. No use la herramienta Upgrade Tool para instalaciones de XenMobile 10.3.x.
- **Para instalar nuevas versiones del software de XenMobile 10.3.x, Service Packs y revisiones del sistema**
  Puede utilizar la página **Release Management** en la consola de XenMobile, tal y como se describe en el artículo.

Important

- Al actualizar desde XenMobile 10.1 a la versión 10.3.x, si WorxStore tiene un nombre personalizado, debe cambiar el nombre del almacén al valor predeterminado **Store** e implementar el parámetro en los dispositivos antes de actualizar. De lo contrario, el nombre personalizado del almacén puede causar problemas con la inscripción en XenMobile 10.3, el acceso a Worx Home y WorxStore y la implementación de aplicaciones en dispositivos iOS. Para ver información detallada sobre cómo configurar la personalización de WorxStore, consulte Para crear marcas personalizadas de Worx Store en dispositivos iOS.
- Después de actualizar a XenMobile 10.3.x, cuando se actualizan las aplicaciones móviles de Worx en XenMobile 10.3.x que configuró en una versión anterior, los parámetros de las aplicaciones ya no aparecen en la consola de XenMobile. Es necesario editar y configurar de nuevo los parámetros de estas aplicaciones. No tendrá que volver a instalar las aplicaciones. Solo tiene que hacer esto una vez: los valores permanecerán intactos en futuras versiones del producto si actualiza la aplicación o si actualiza el servidor.

Resumen de la ruta de actualización

Versión de XenMobile Server	Número de versión	Actualizar a	Número de versión	Ruta de actualización	Ubicación
XenMobile Server 9 con App Controller Patch 5	9.0.0.97582	XenMobile Server 10.1	10.1.0.63030	De XenMobile Server 9 a XenMobile Server 10.1	Descargar (App Controller Patch 5 y Upgrade Tool)
XenMobile Server 10 o 10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	Actualizar de XenMobile Server 10 o 10.1 a la versión 10.3	Descargar
XenMobile Server 10.3	10.3.0.10004, 10.3.0.10008, 10.3.0.10010, 10.3.0.10014, 10.3.0.10016, 10.3.0.10032, 10.3.0.10036	XenMobile Server 10.3 Rollup Patch 3	10.3.0.10048	Actualizar de XenMobile Server 10.3 a la versión 10.3 Rolling Patch 3	Descargar
XenMobile Server 10.3	10.3.0.x	XenMobile Server 10.3.5	10.3.5.354	Actualizar de XenMobile Server 10.3 a la versión 10.3.5	Descargar
XenMobile Server 10.3.5	10.3.5.354	XenMobile Server 10.3.6 (Service Pack)	10.3.6.310	Actualizar de XenMobile Server 10.3.5 a la versión 10.3.6	Descargar

Para actualizar desde XenMobile 10.1 o desde XenMobile 10.3.x

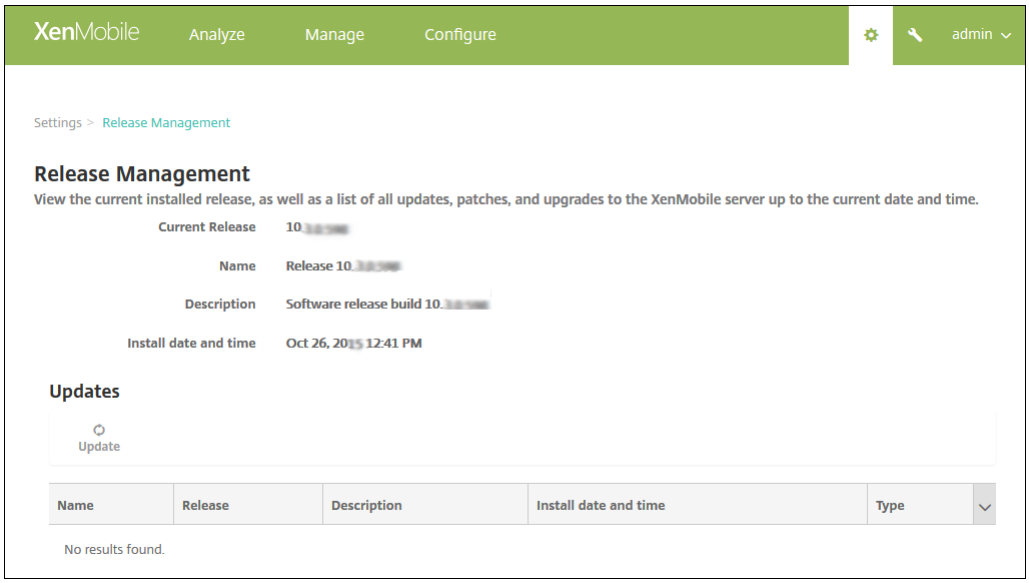
Requisitos previos:

- 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.
- Consulte los Requisitos del sistema de la versión a la que está actualizando. Para XenMobile 10.3, consulte Requisitos del sistema.

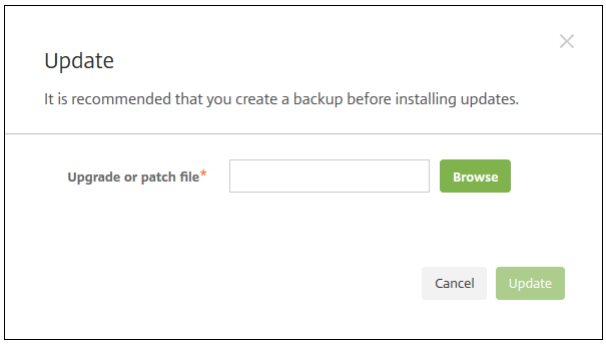
1. Inicie sesión con su cuenta en el sitio Web de Citrix y descargue el archivo de actualización (.bin) de XenMobile a una ubicación apropiada.

2. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

3. Haga clic en **Release Management**. Aparecerá la página **Release Management**.



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



4. Seleccione el archivo de actualización de XenMobile que descargó de Citrix.com. Para ello, haga clic en **Browse** y vaya a la ubicación del 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. Es importante que borre la caché del explorador Web después de reiniciarse el sistema.

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

1. Cargue el archivo .bin en todos los nodos de **Settings** > **Release Management**.

2. Cierre todos los nodos de **Settings** en la interfaz de línea de comandos.

3. Inicie un nodo y compruebe que el servicio se está ejecutando.

4. Inicie los otros nodos uno tras otro.

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.

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 embar

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

1. Apague todos los nodos menos uno.
2. Actualice ese nodo.
3. 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.

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 embar

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

1. Apague todos los nodos menos uno.
2. Actualice ese nodo.
3. 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.

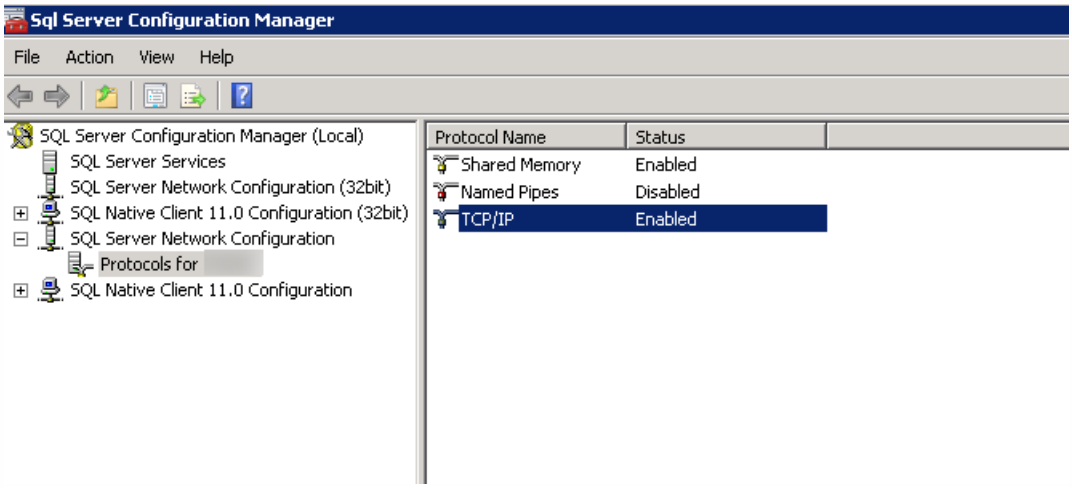
Respaldo para instancias de SQL con nombre

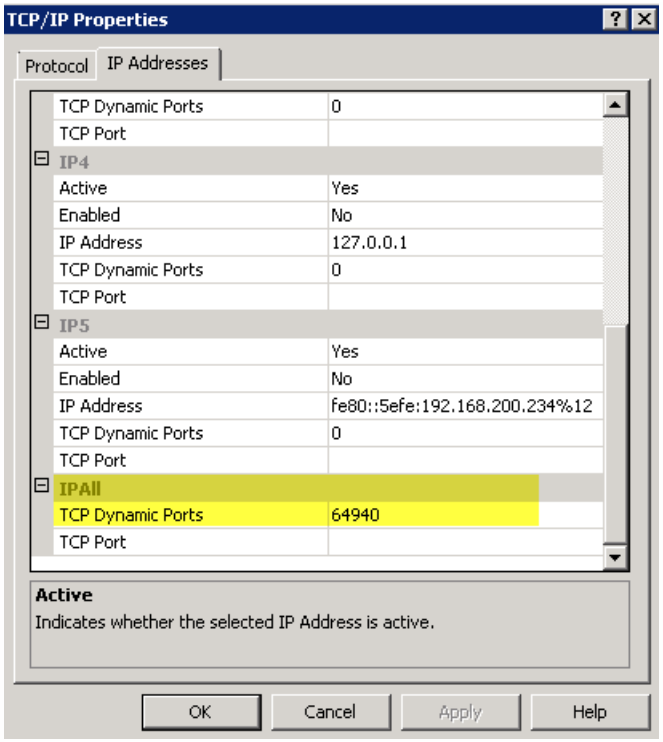
Jul 27, 2016

Puede usar Upgrade Tool para actualizar el producto desde XenMobile 9 a XenMobile 10 y desde XenMobile 9 a XenMobile 10.1. Si la configuración de XenMobile 9 utiliza instancias de SQL con nombre, debe seguir los pasos específicos para este caso. 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.

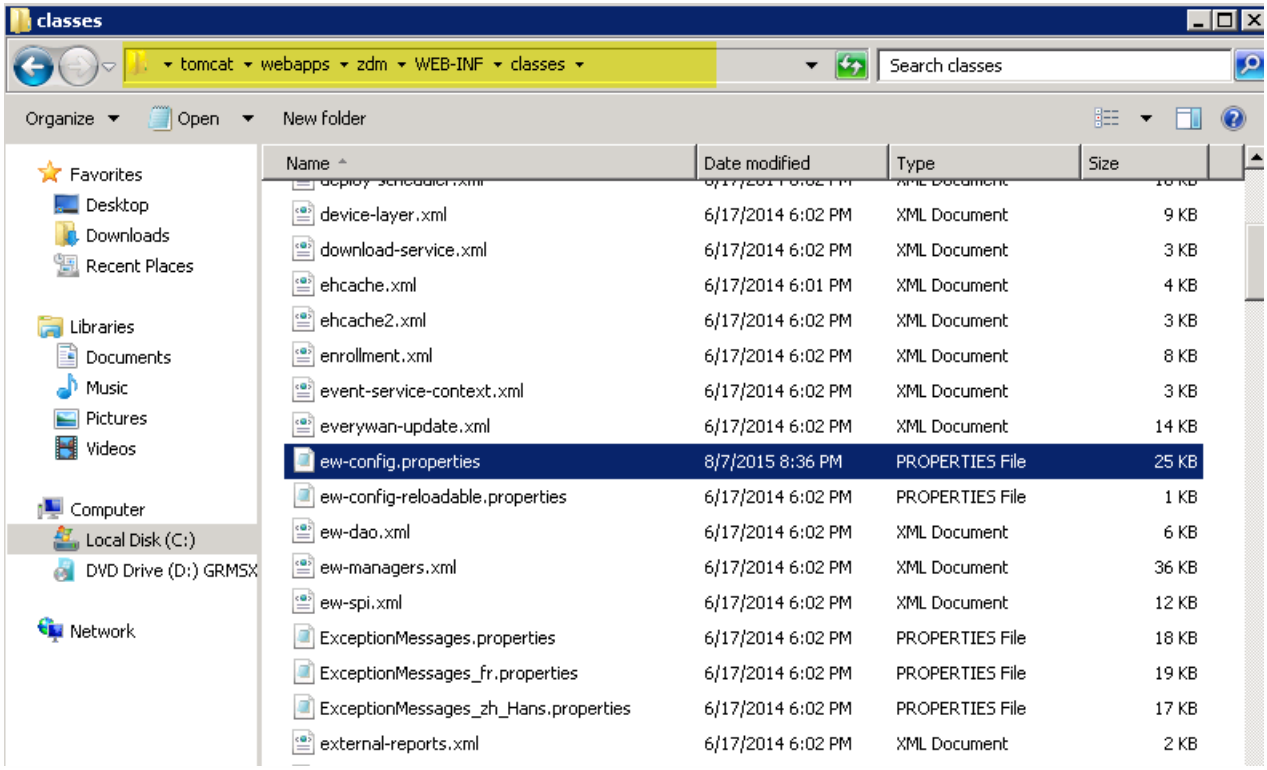
> ## Nota
>
> Citrix recomienda que la instancia de la base de datos de SQL Server se ejecute siempre en un puerto estático, porque el servidor XenMobile necesita acceso continuo a la base de datos. Esta conexión, por lo general, atraviesa un firewall. Como resultado de ello, necesita abrir el puerto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





Pasos para actualizar XenMobile con una instancia SQL Server con nombre

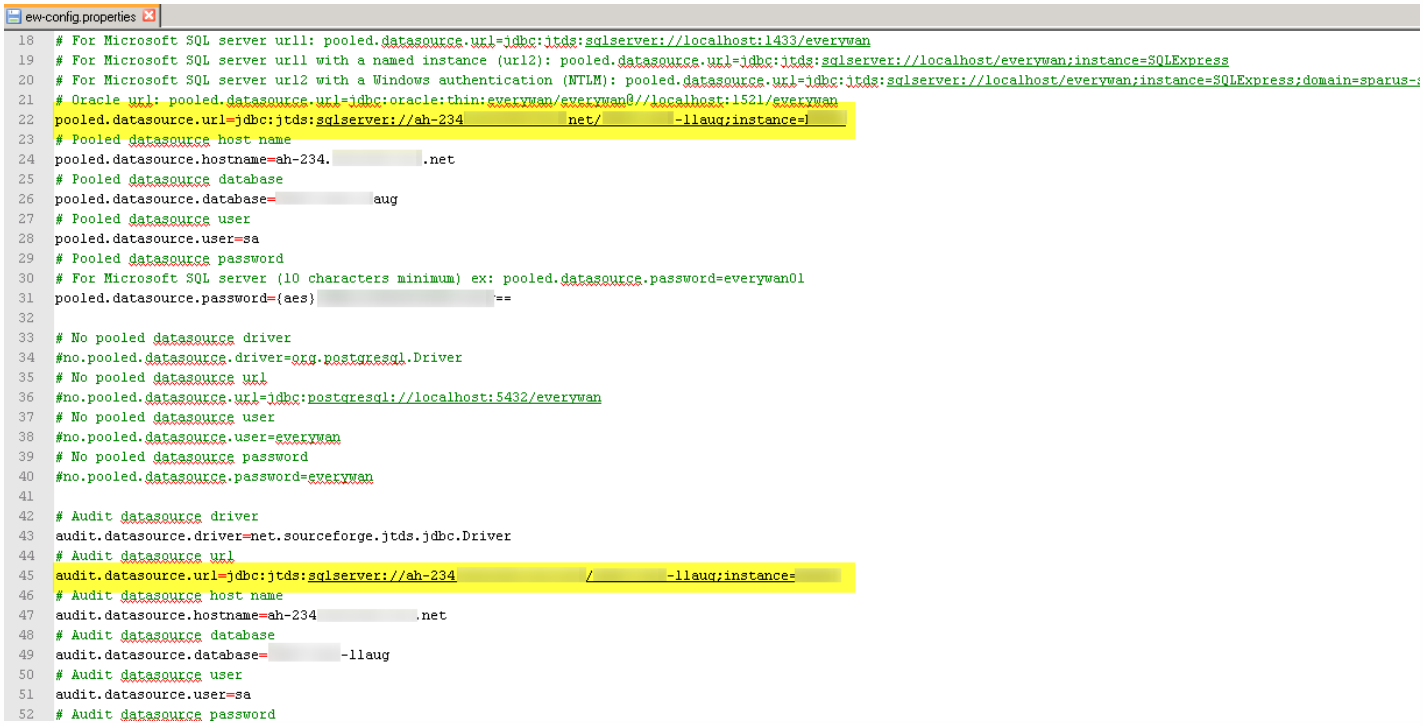
1. Vaya al directorio de instalación de Device Manager y abra el archivo ew-config.properties. Este se encuentra en tomcat\webapps\zdm\WEB-INF\classes.



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/

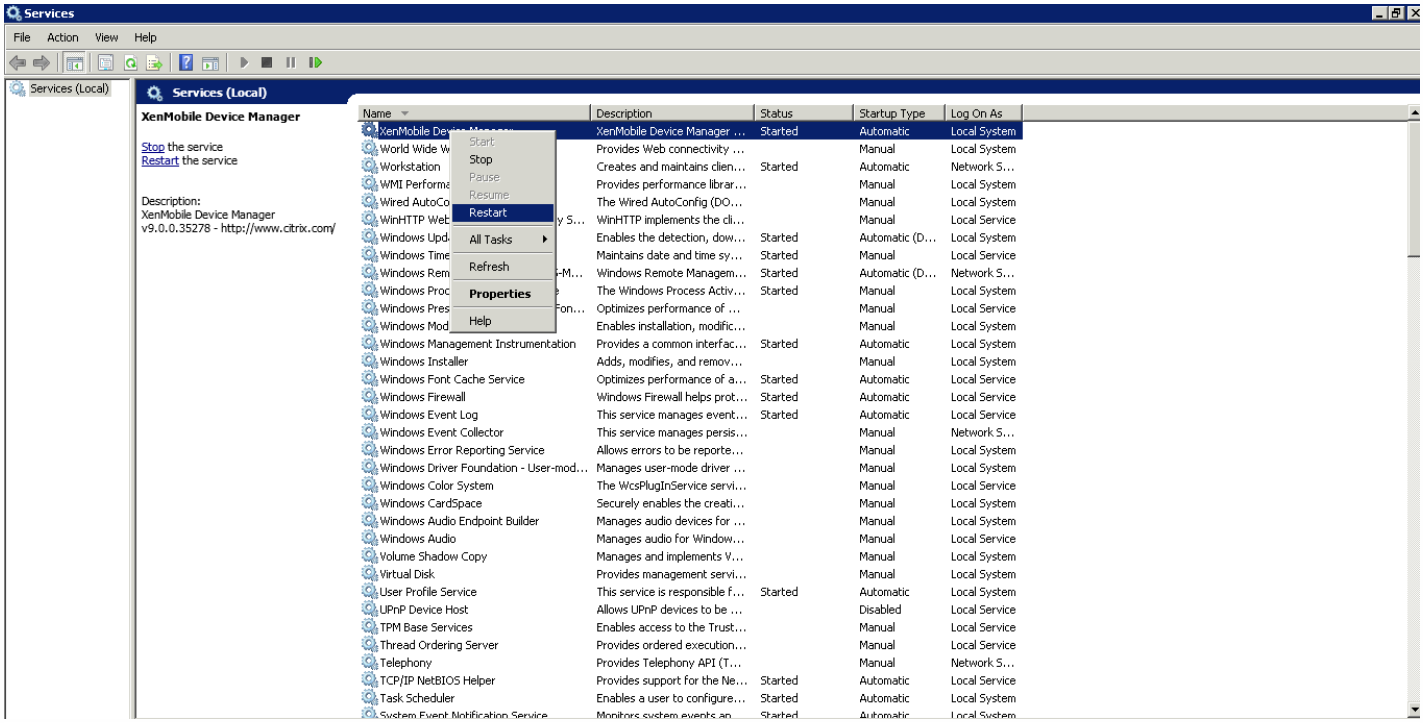
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

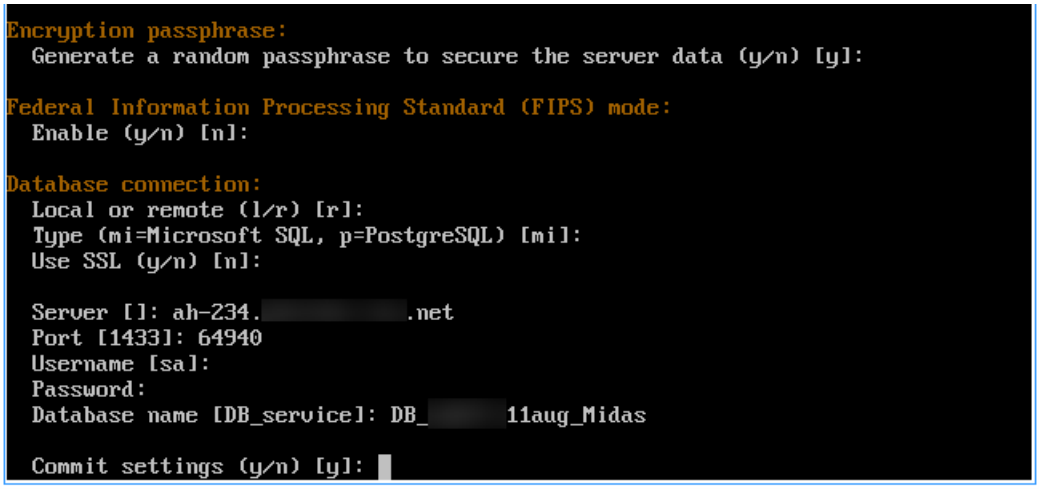
ew-config.properties

```
# 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 estos pasos para continuar la actualización del entorno de XenMobile:

Para actualizar desde XenMobile 9.0 - MDM Edition, App Edition y Enterprise Edition - a XenMobile 10.1, use la herramienta de actualización (Upgrade Tool). Puede descargar la herramienta de actualización desde la página de descargas de Citrix.com. Para obtener información más detallada, consulte Actualización de XenMobile.

Configuración de clústeres en XenMobile 10

Jul 27, 2016

En versiones de XenMobile anteriores a 10, se configuraba Device Manager como clúster y App Controller como par de alta disponibilidad. XenMobile 10 ha integrado Device Manager y App Controller de XenMobile 9. A partir de la versión 10, la alta disponibilidad ya no se aplica a XenMobile. Por tanto, para configurar la agrupación en clústeres, deberá configurar las dos siguientes direcciones IP virtuales de 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.
- Una dirección IP pública para la banda L de MDM y un dirección IP privada para MAM.
- Certificados de servidor.
- Una dirección IP libre para la dirección IP virtual de NetScaler Gateway.

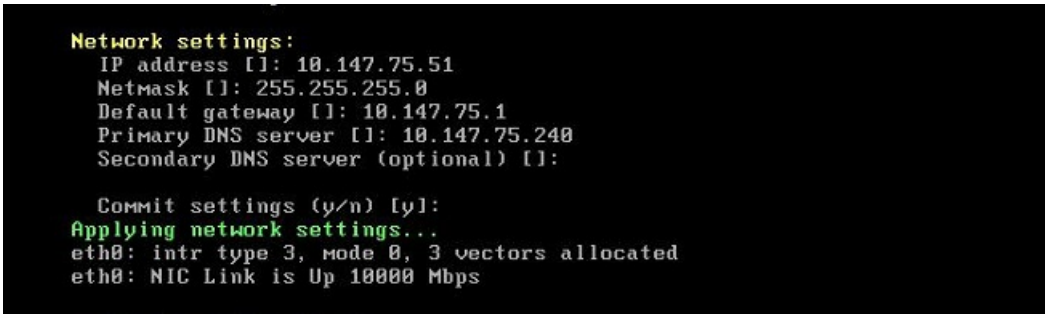
Para ver gráficos de referencia con las arquitecturas de XenMobile 10.x en configuraciones en clúster, consulte Descripción de la arquitectura.

Instalación de nodos de clúster en XenMobile

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.

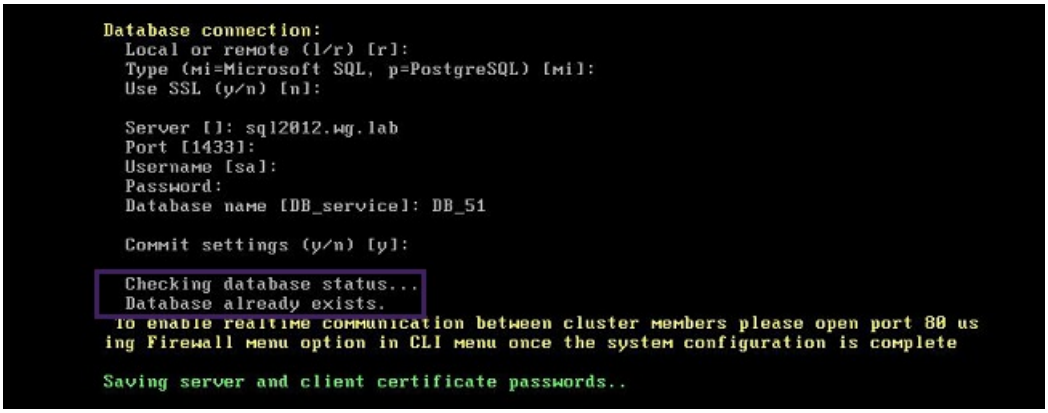
2. Facilite los datos de la configuración de red tal y como se muestra en la imagen siguiente.



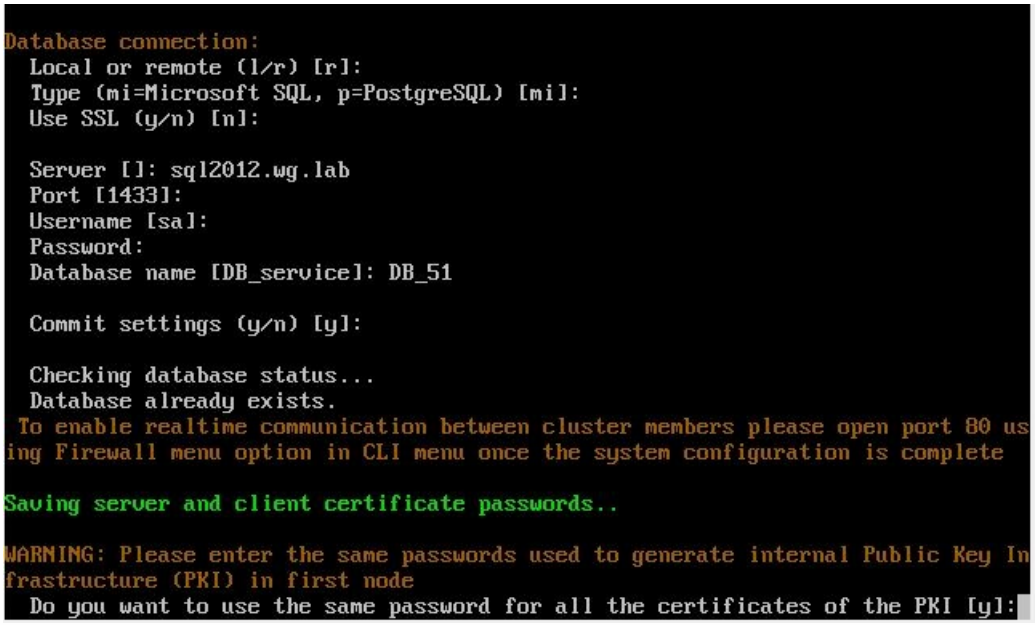
3. Si quiere usar la contraseña predeterminada para la protección de datos, escribay;, o bienn e introduzca una nueva contraseña.

4. Si quiere usar el estándar FIPS, escribay;, o bienn.

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".

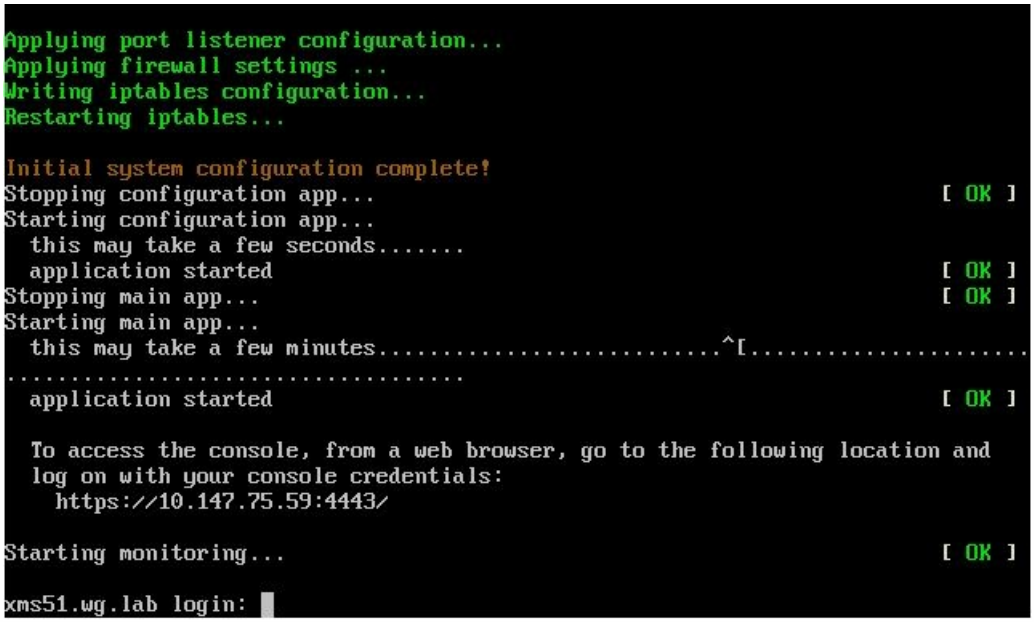


6. Introduzca las mismas contraseñas para los certificados proporcionados a la primera máquina virtual.



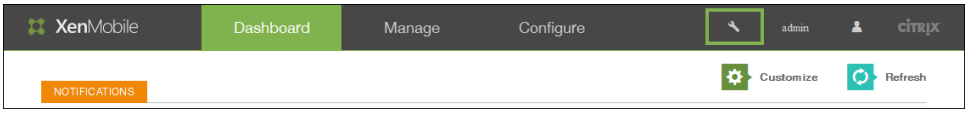
Una vez introducida la contraseña, se completará la configuración inicial del segundo nodo.

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

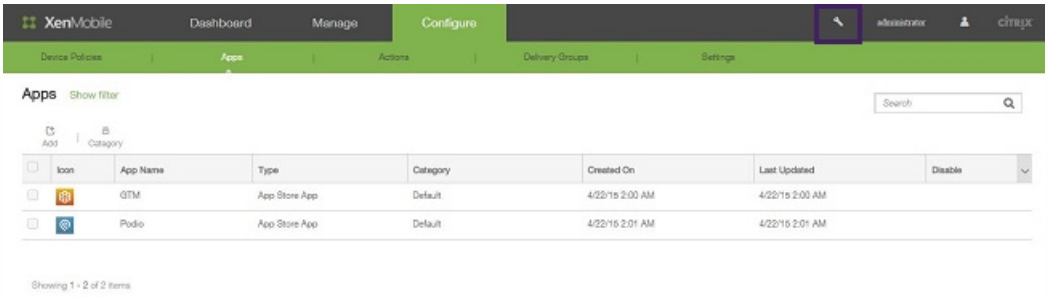


Nota: Este cuadro de diálogo de inicio de sesión es idéntico al cuadro de diálogo del inicio de sesión de la primera máquina virtual. Esta coincidencia sirve para confirmar que ambas máquinas virtuales utilizan el mismo servidor de base de datos.

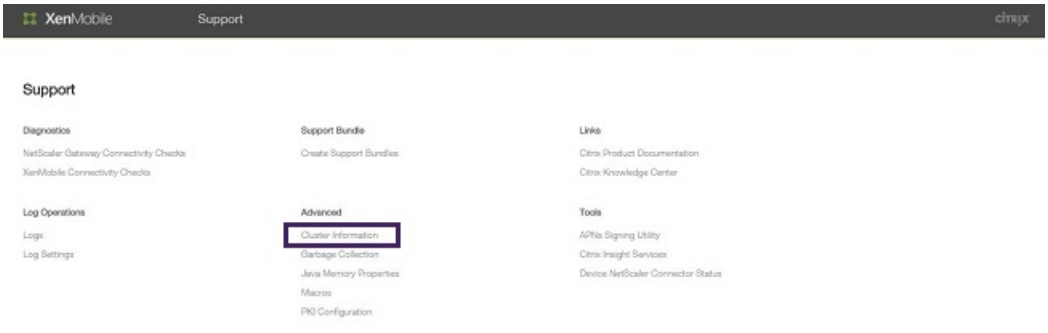
8. Use el nombre de dominio completo (FQDN) de XenMobile para abrir la consola de XenMobile en un explorador Web.
9. En el panel de mandos, haga clic en el icono de herramienta, situado en la parte superior derecha de la pantalla.



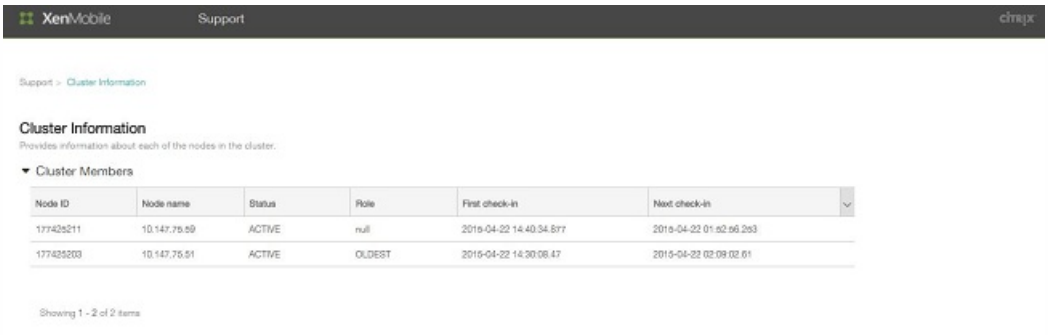
Se abrirá la página Support.



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.



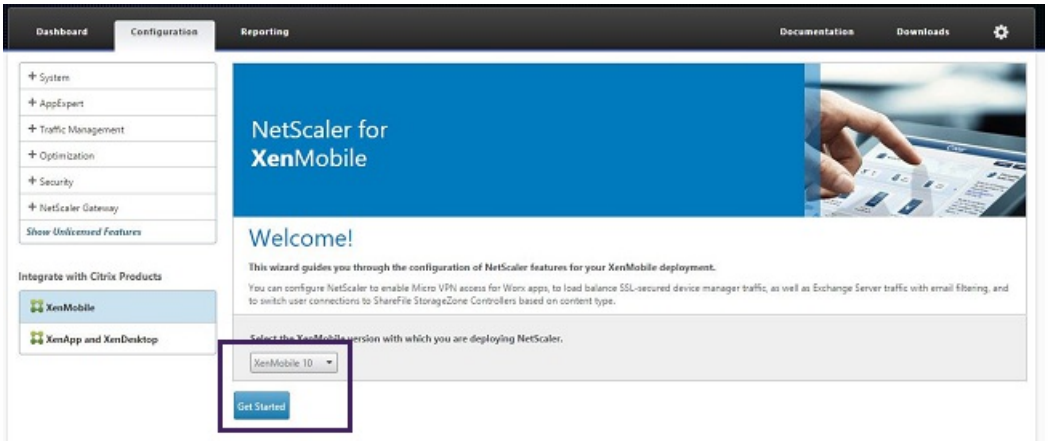
Ahora, el nuevo nodo es miembro del clúster. Puede agregar otros nodos siguiendo los mismos pasos.

Para configurar el equilibrio de carga para el clúster de XenMobile en NetScaler

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.

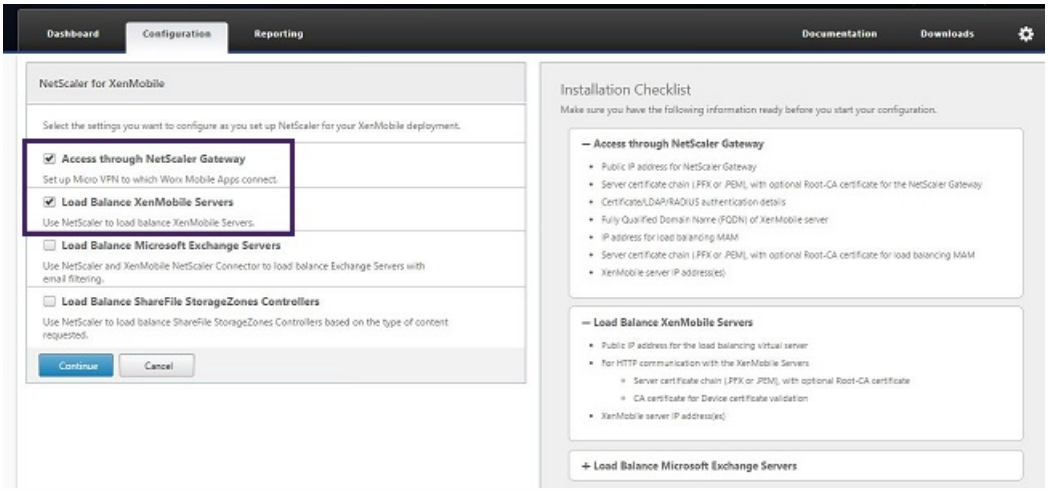
1. Inicie sesión en NetScaler.

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

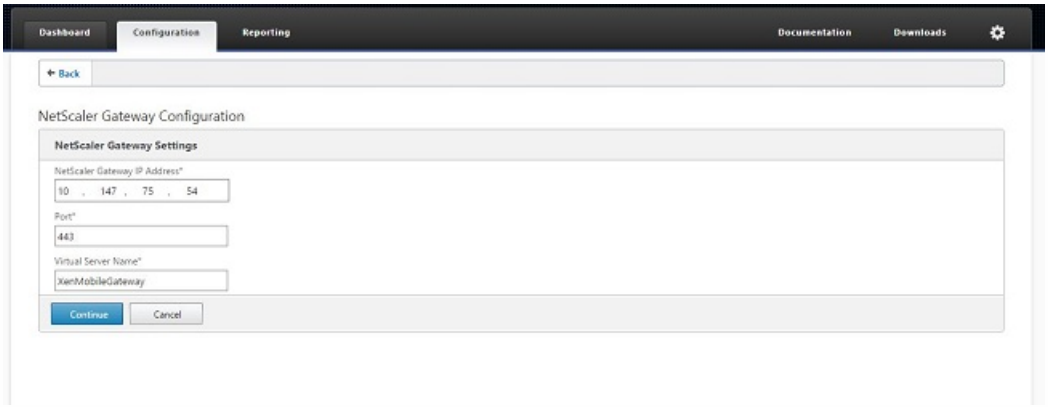


3. Marque las casillas Access through NetScaler Gateway y Load Balance XenMobile Servers. A continuación, haga clic en

Continue.

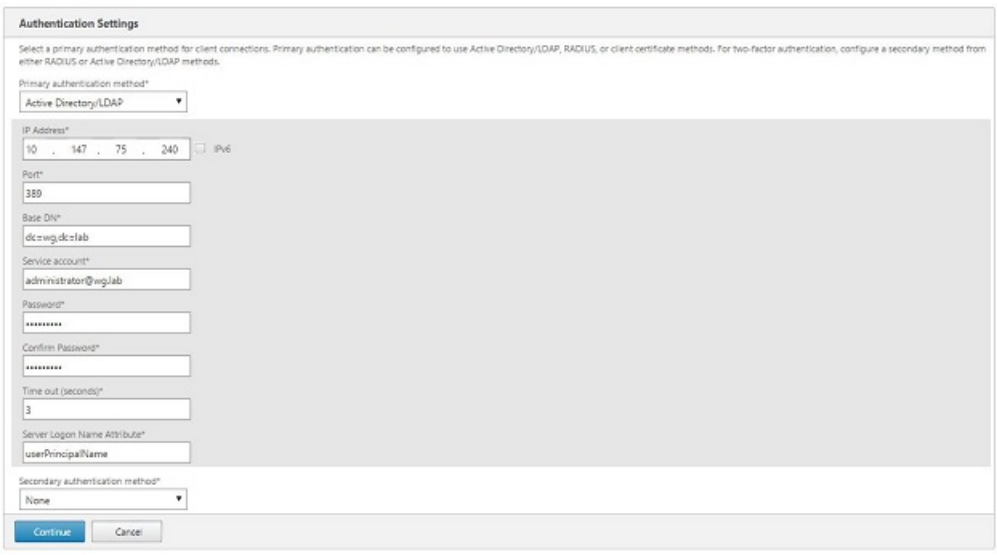


4. Introduzca la dirección IP de NetScaler Gateway y haga clic en Continue.



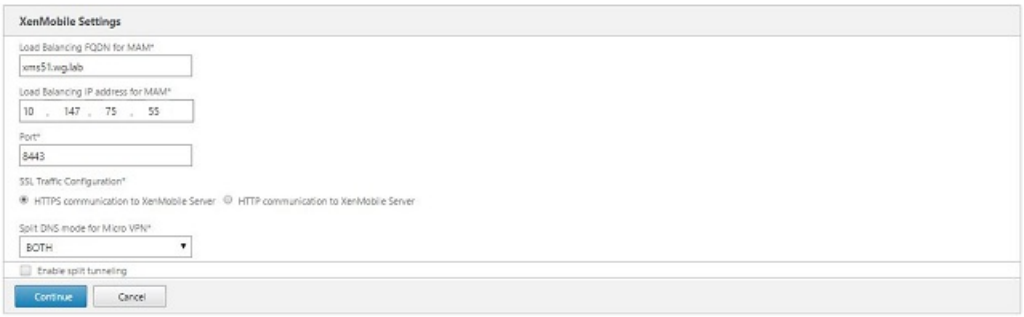
5. Vincule el certificado del servidor a la dirección IP virtual de NetScaler Gateway. Para ello, lleve a cabo una de las siguientes acciones y, a continuación, haga clic en Continue.
   - En Use existing certificate, elija el certificado del servidor de la lista.
   - Haga clic en la ficha Install Certificate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

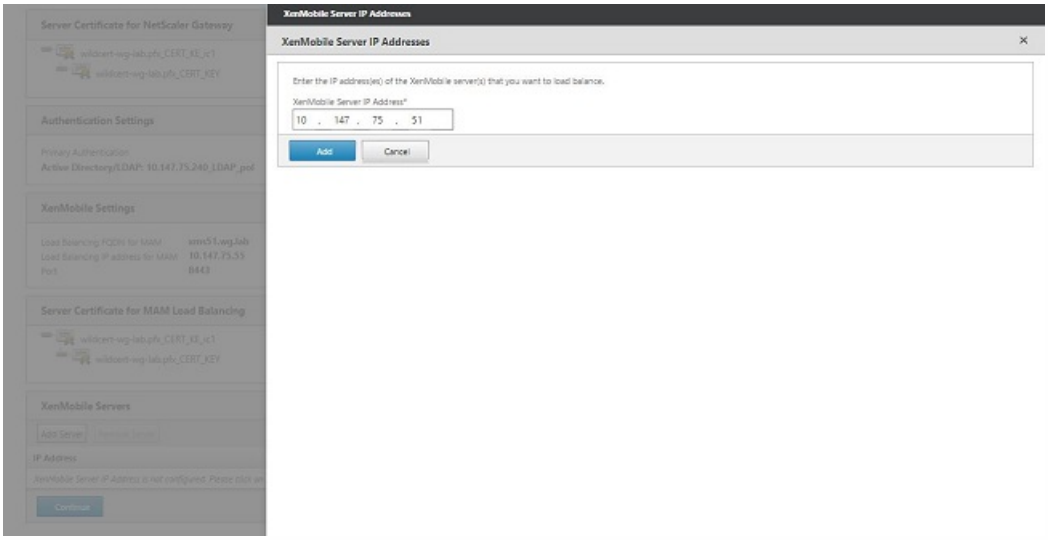


Nota: Compruebe que el nombre de dominio completo perteneciente a la dirección IP virtual de equilibrio de carga para MAM y el nombre de dominio completo de XenMobile coinciden.

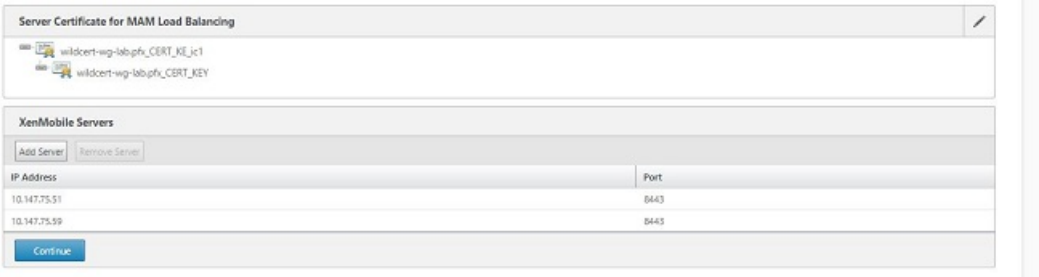
8. Si quiere usar el modo de puente SSL (HTTPS), marque HTTPS communication to XenMobile Server. En cambio, si quiere usar la descarga de SSL, marque HTTP communication to XenMobile Server, como se muestra en la imagen anterior. Dada la finalidad de este artículo, se opta por el modo de puente SSL (HTTPS).
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.

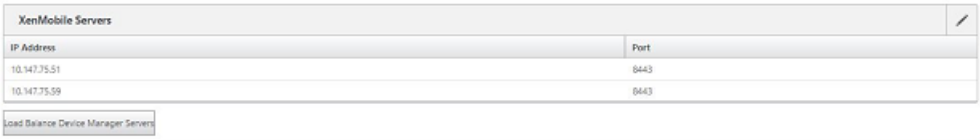
11. Introduzca la dirección IP del nodo de XenMobile y, a continuación, haga clic en Add.



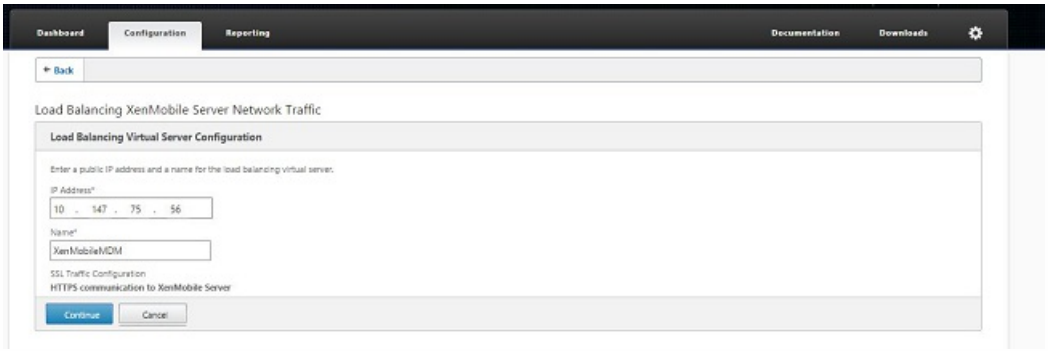
12. Repita los pasos 10 y 11 para agregar nodos de XenMobile adicionales que formen parte del clúster de XenMobile. Verá todos los nodos de XenMobile que haya agregado. Haga clic en Continuar.



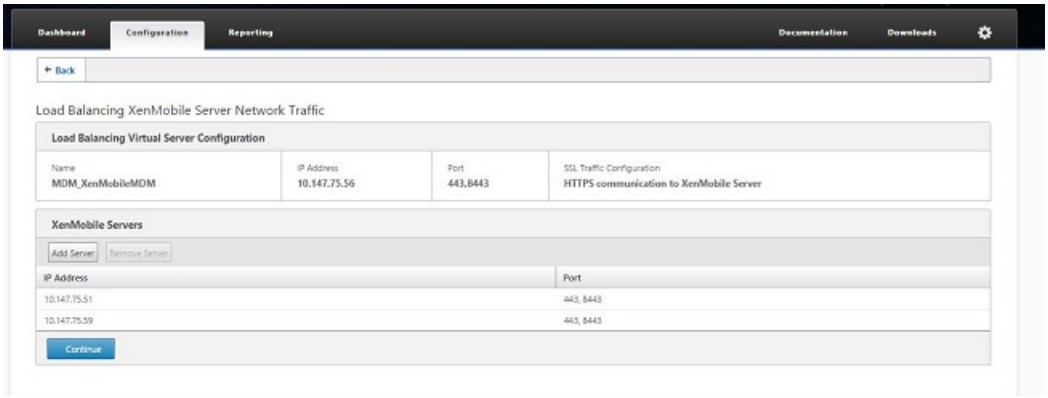
13. Haga clic en Load Balance Device Manager Servers para continuar con la configuración del equilibrio de carga para MDM.



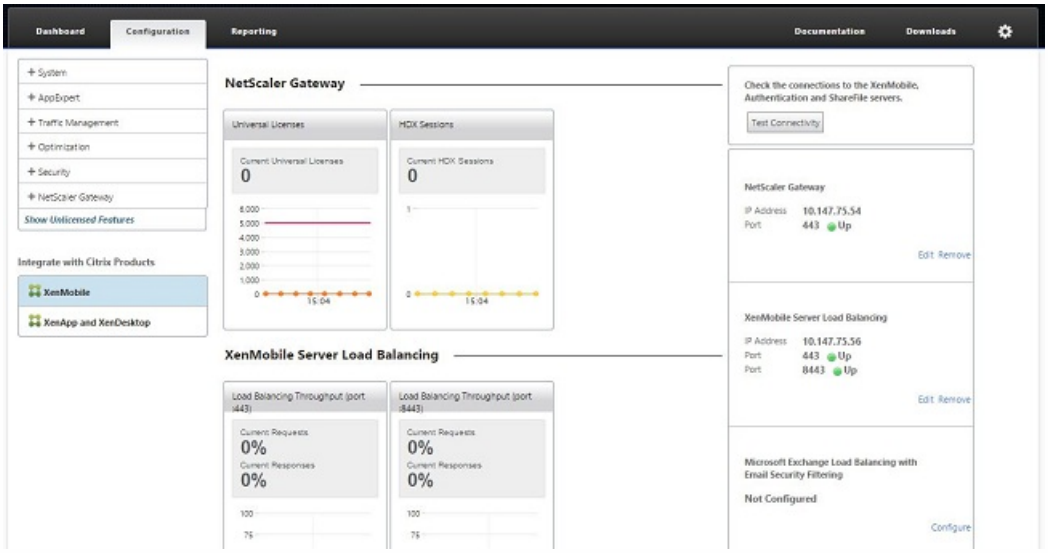
14. Introduzca la dirección IP que se utilizará como la IP de equilibrio de carga para MDM y, a continuación, haga clic en Continue.



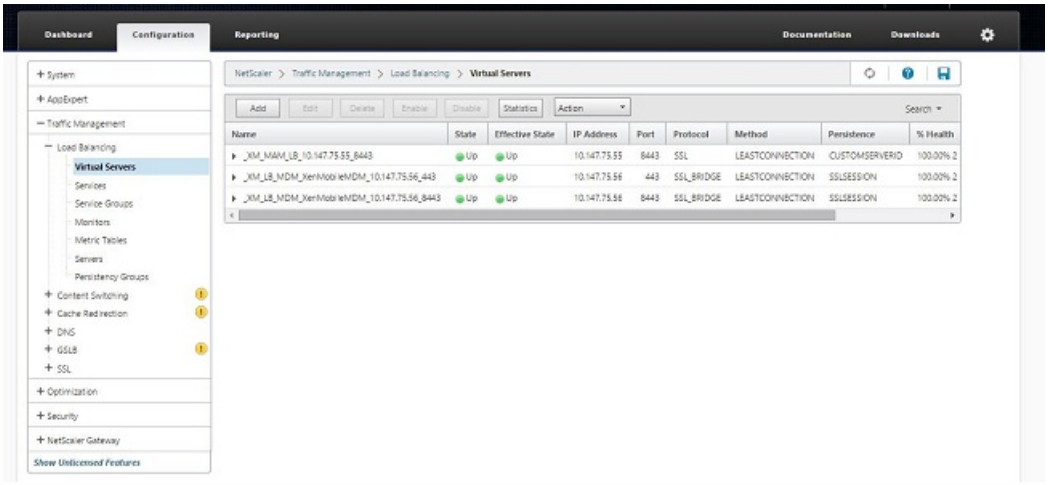
15. Una vez que vea los nodos de XenMobile en la lista, haga clic en Continue y, a continuación, en Done para finalizar el proceso.



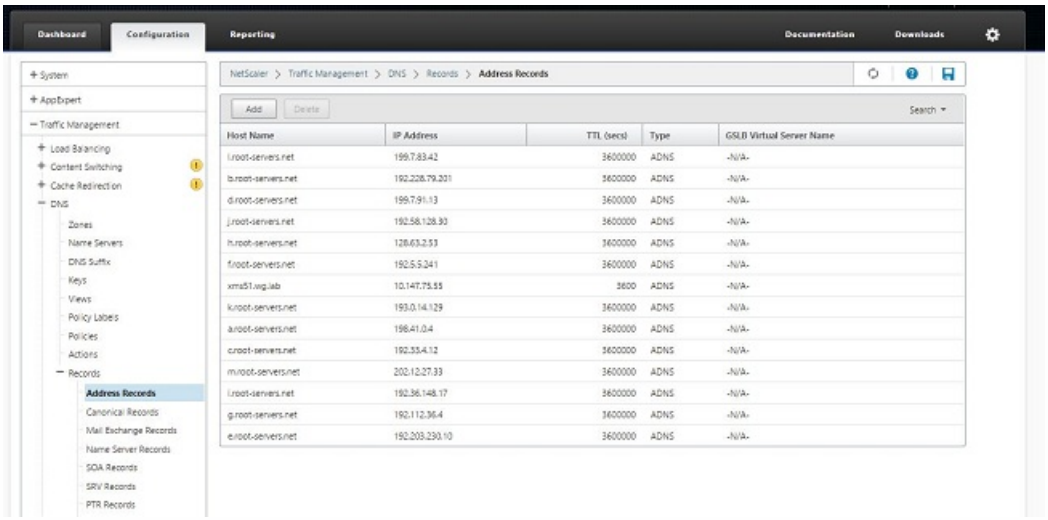
Verá el estado de la dirección IP virtual en la página XenMobile.



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.

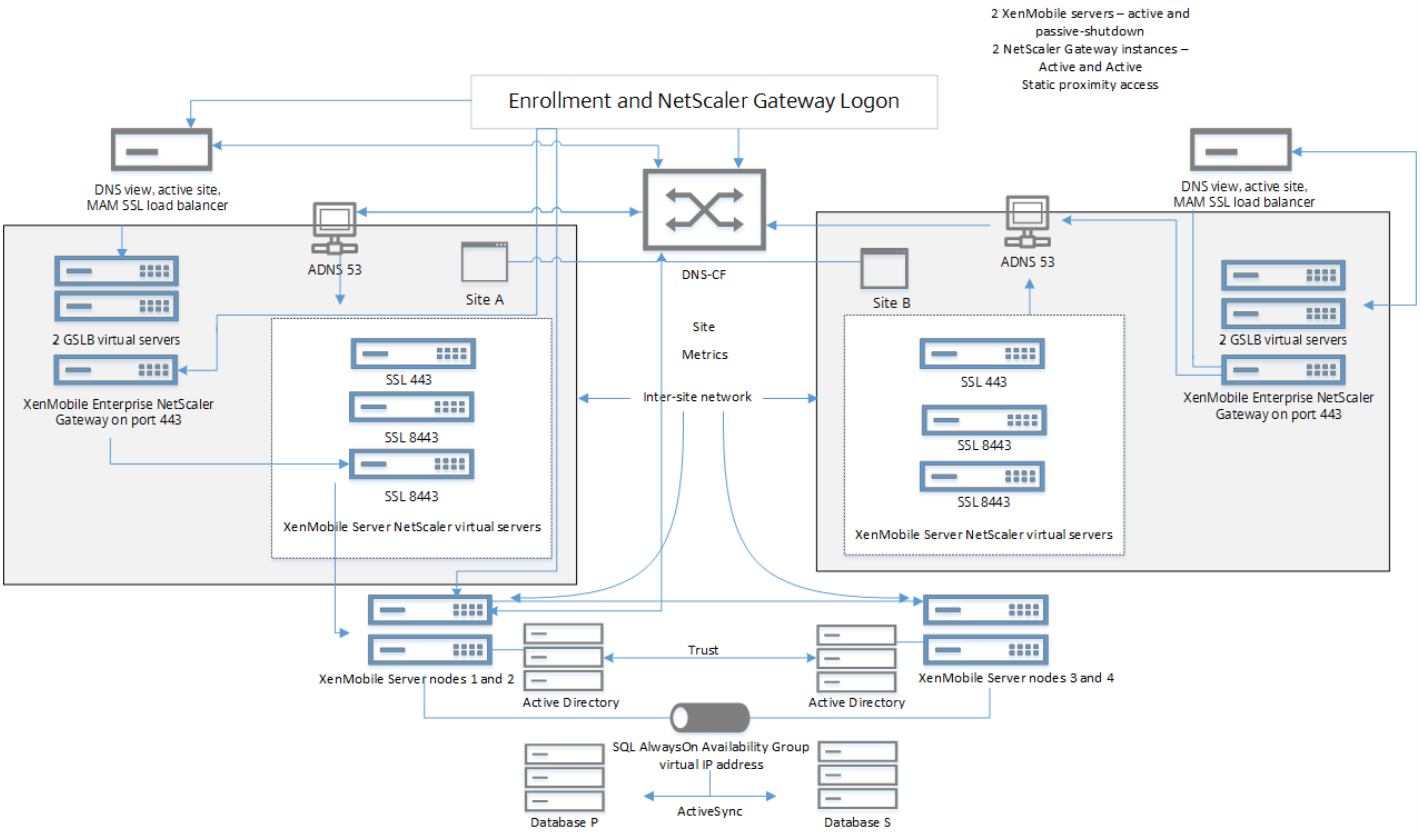


Guía de recuperación ante desastres de XenMobile

Jul 27, 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.



PDF Guía de recuperación ante desastres de XenMobile

PDF Diagrama de la arquitectura para recuperación ante desastres de XenMobile

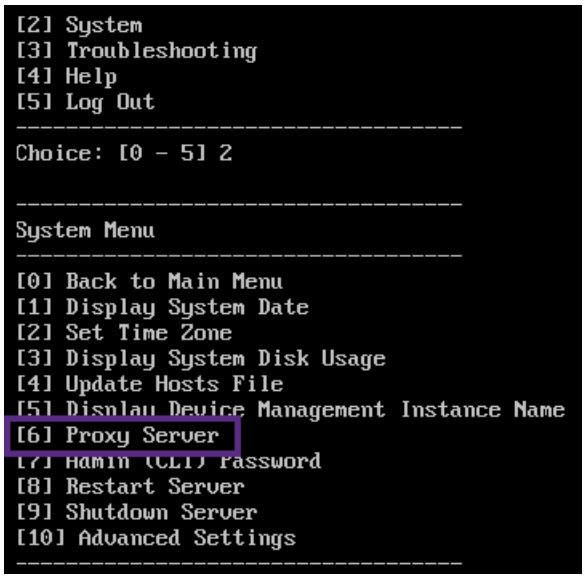
Habilitación de servidores proxy en XenMobile

Jul 27, 2016

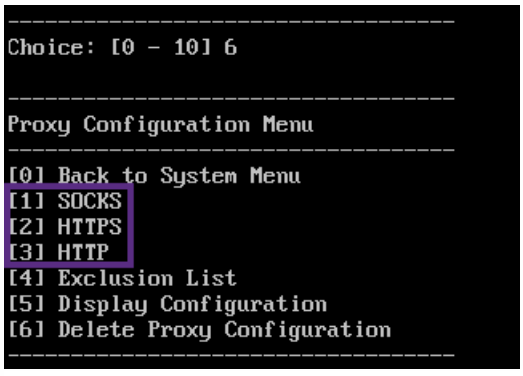
Si desea controlar el tráfico saliente a Internet, puede configurar un servidor proxy en XenMobile para transportar dicho tráfico. Para ello, debe configurar el servidor proxy mediante la interfaz de línea de comandos (CLI). Tenga en cuenta que la configuración del servidor proxy requiere reiniciar el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



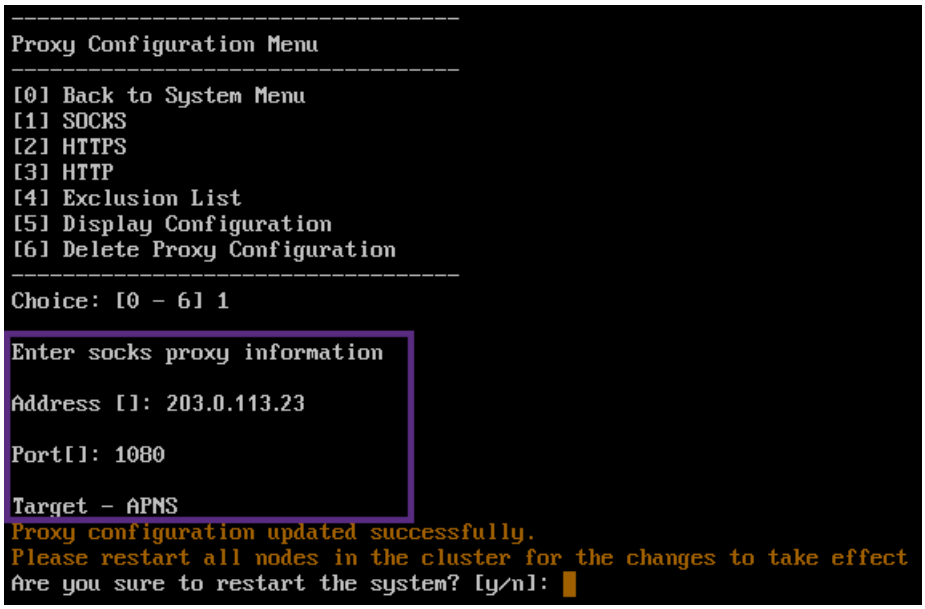
3. En el menú de configuración de proxy, introduzca **1** para seleccionar SOCKS, **2** para seleccionar HTTPS, o **3** para seleccionar HTTP.



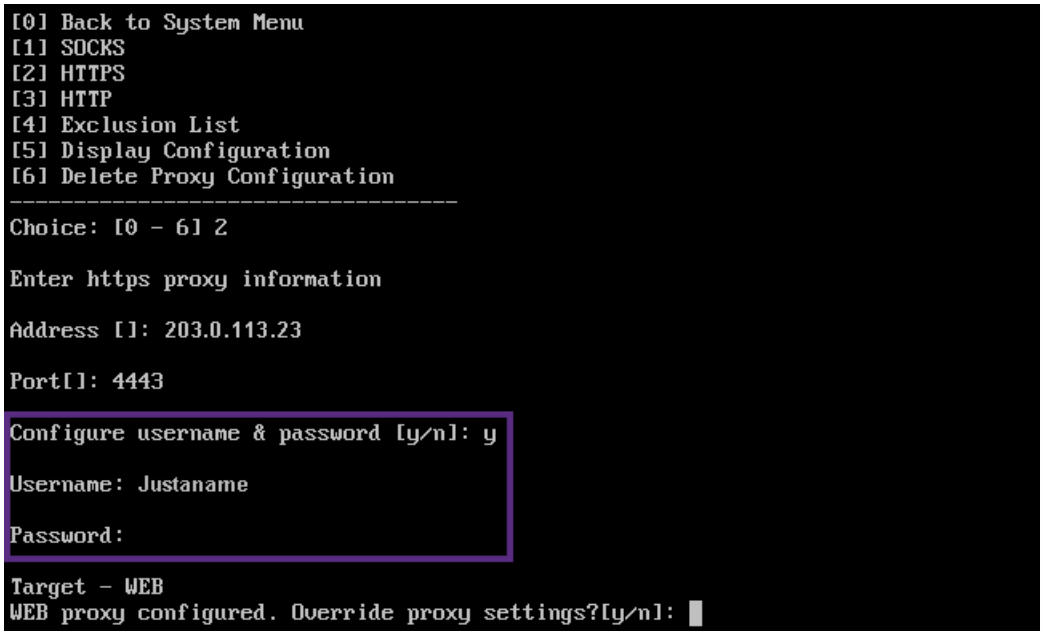
4. Introduzca la dirección IP del servidor proxy, el número de puerto y el destino. Consulte la tabla siguiente para ver los tipos de destino admitidos para cada tipo de servidor proxy.

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.

Licencia

Oct 31, 2016

XenMobile y NetScaler Gateway requieren licencias. Para ver una hoja de datos con las funciones de XenMobile disponibles en cada edición, consulte este documento PDF.

Para obtener más información sobre el sistema de licencias de NetScaler Gateway, consulte Licencias de NetScaler Gateway. 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 Licencia 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 10.3.x requiere Citrix License Server 11.12.1 o una versión posterior; las versiones anteriores del servidor de licencias no funcionan con XenMobile 10.3.x.

> **Important**
>
> 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.

Aspectos a tener en cuenta sobre el sistema de licencias de XenMobile

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 de XenMobile. El acceso a la consola Web de XenMobile no se bloquea nunca, independientemente de si hay disponible una licencia válida de XenMobile. En la consola de XenMobile, puede ver la cantidad de días que le quedan del periodo de evaluación.

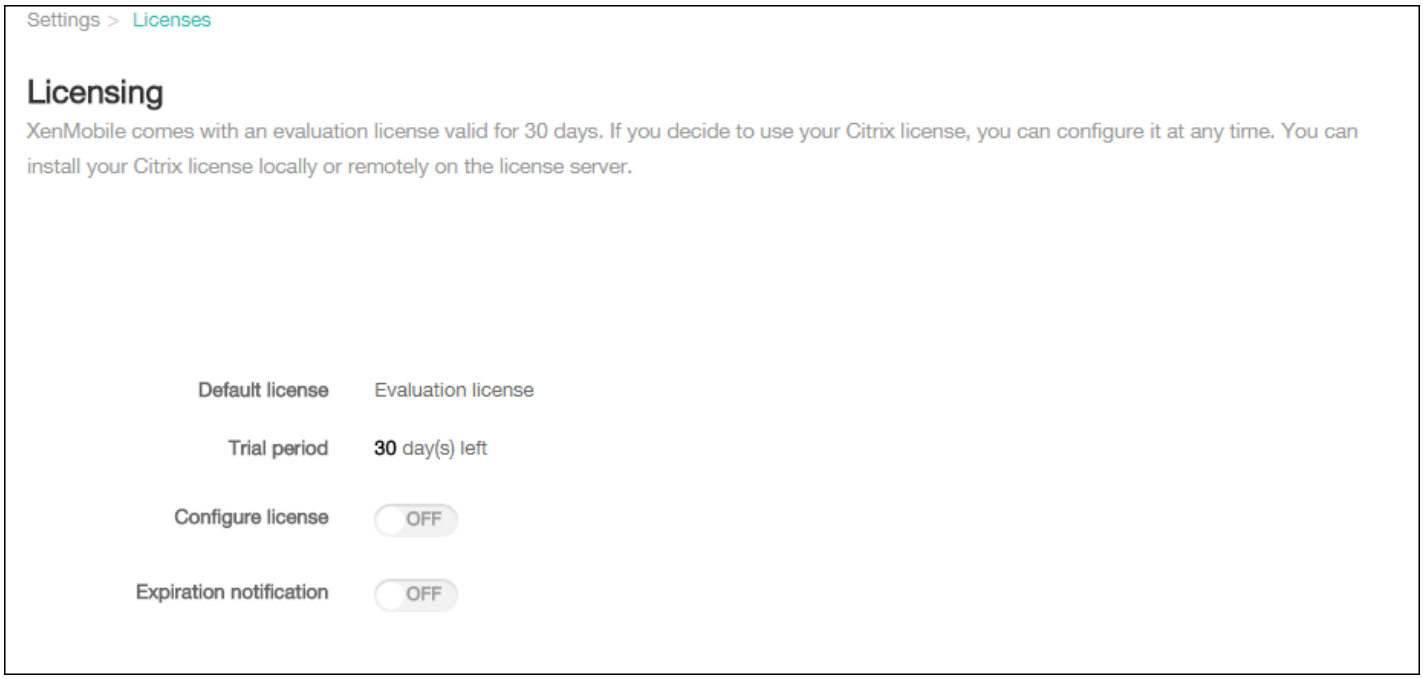
Aunque XenMobile permite cargar varias licencias, solo se puede activar una licencia en un momento dado.

Cuando caduca una licencia de XenMobile, ya no se puede utilizar ninguna de las funciones de administración de

dispositivos. 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. Para obtener más información acerca de los programas y los modelos de licencia de XenMobile, consulte las licencias de XenMobile.

Para encontrar la página Licensing en la consola de XenMobile

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 el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

2. Haga clic en **Licensing**. Aparecerá la página **Licensing**.

Para agregar una licencia local

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.

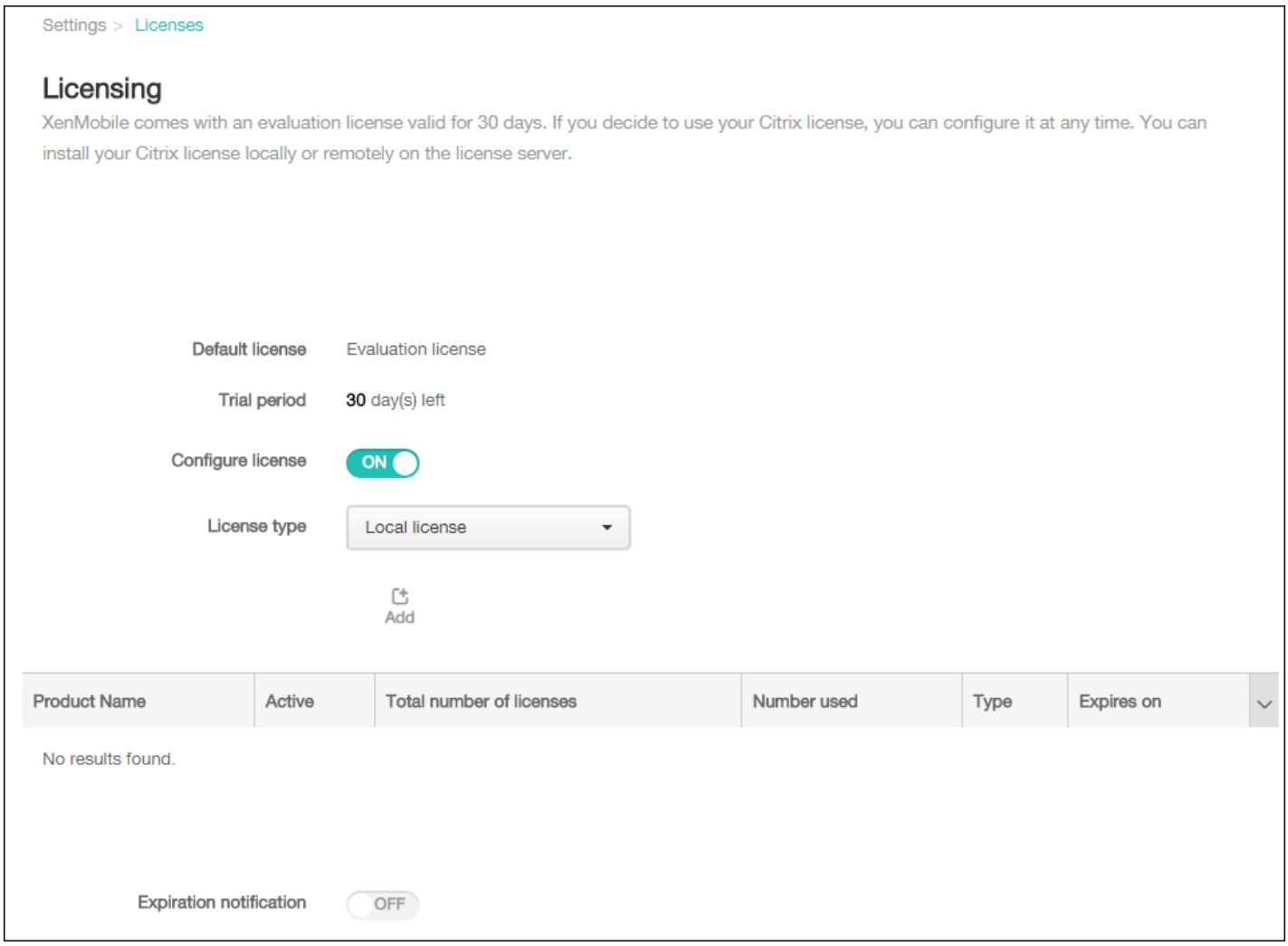
Puede administrar todas las licencias locales a través de la consola de XenMobile.

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.

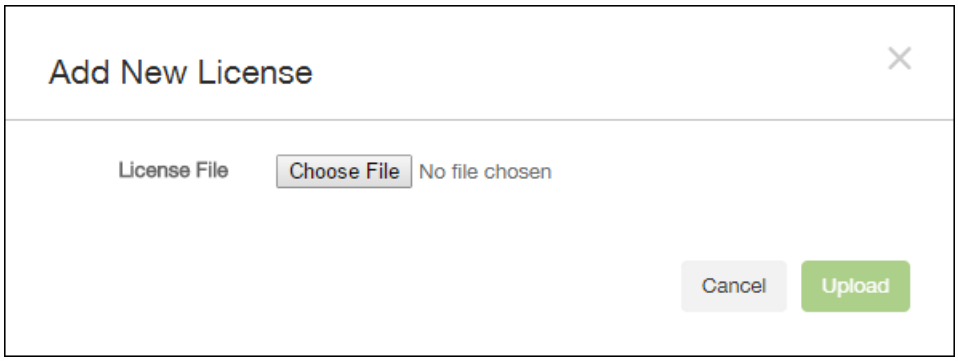
2. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

3. Haga clic en **Licensing**. Aparecerá la página **Licensing**.

4. 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.



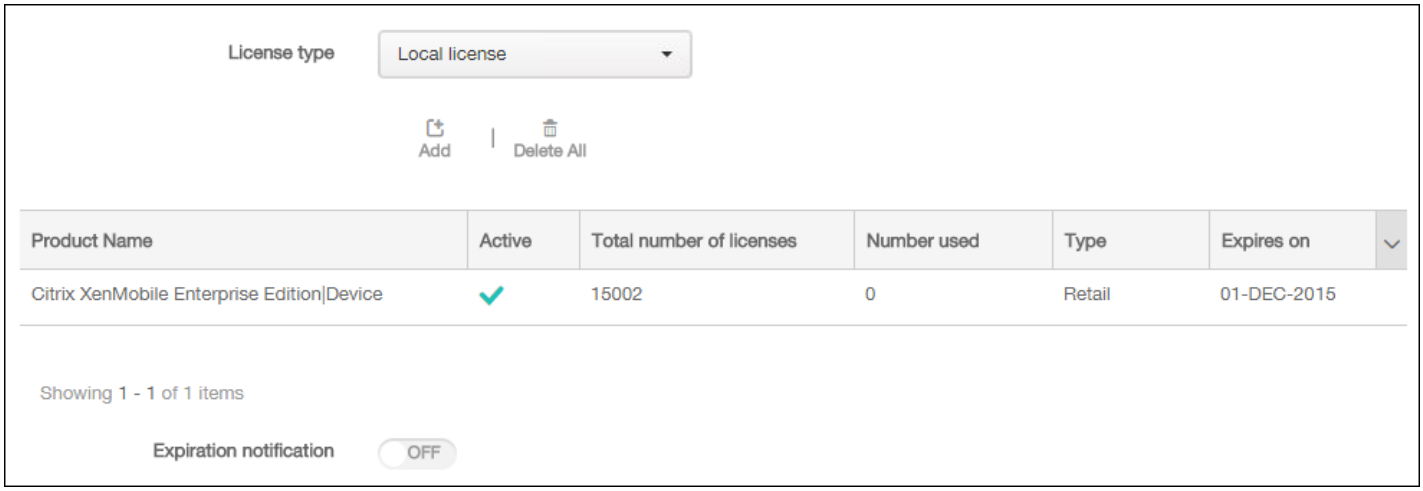
5. Compruebe que **License type** está establecido en **Local license** y, a continuación, haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New License**.



6. En el cuadro de diálogo **Add New License**, haga clic en **Choose File** y, a continuación, vaya a la ubicación del archivo de

su licencia.

7. Haga clic en **Upload**. La licencia se cargará de forma local y aparecerá en la tabla.



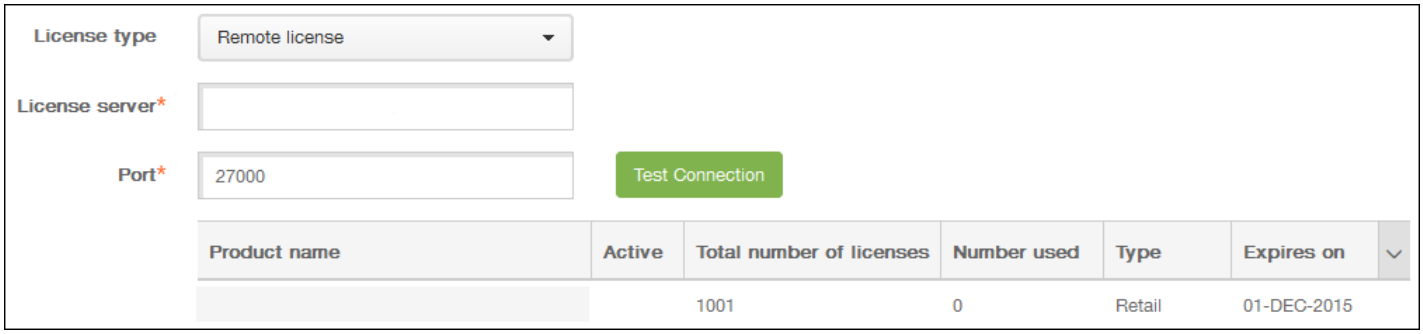
8. Cuando la licencia aparezca en la tabla de la página **Licensing**, actívela. Si se trata de la primera licencia de la tabla, la licencia se activa automáticamente.

Para agregar una licencia remota

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.

3. Establezca **License type** en **Remote license**. El botón **Add** se reemplaza por los campos **License server**, **Port** y el botón **Test Connection**.



4. Configure los siguientes parámetros:

- **License server**. Escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor de licencias remoto.
- **Port**. Acepte el puerto predeterminado o escriba el número de puerto utilizado para comunicarse con el servidor de licencias.

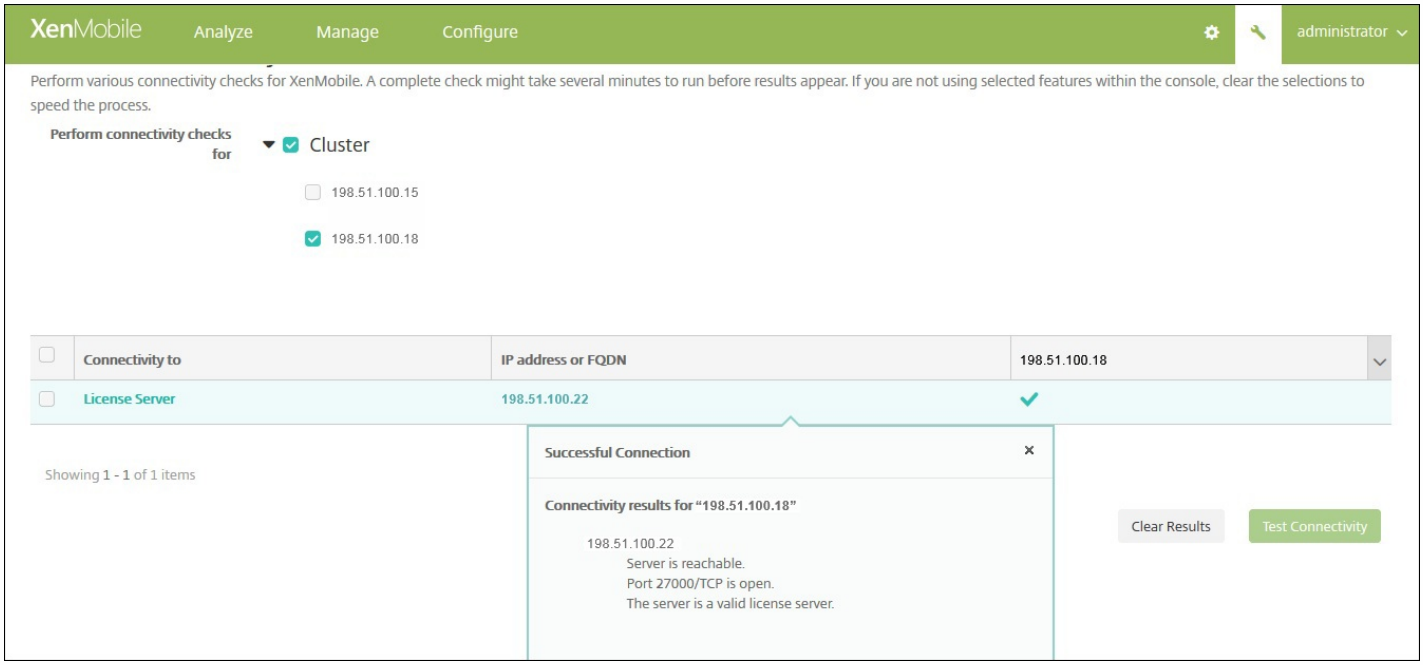
5. Haga clic en **Test Connection**. Si la conexión es satisfactoria, XenMobile se conecta al servidor de Citrix Licensing, y la

tabla Licensing se rellena con las licencias disponibles. Si solo hay una licencia, esta se activa automáticamente.

Cuando haga clic en **Test Connection**, XenMobile confirma la siguiente:

- XenMobile puede comunicarse con el servidor de licencias.
- Las licencias del servidor de licencias son válidas.
- El servidor de licencias es compatible con XenMobile.

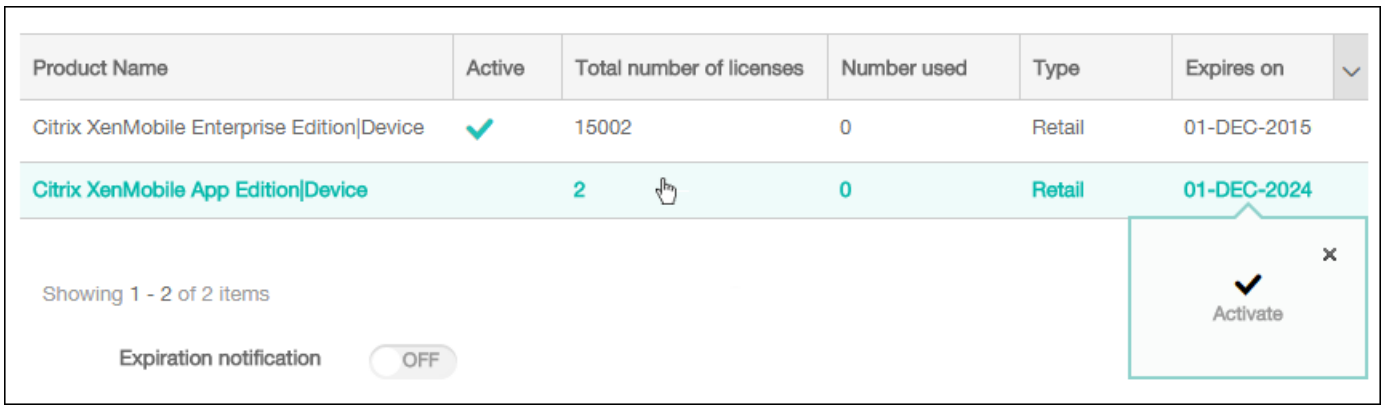
Si no se puede establecer la conexión, revise el mensaje de error que se muestra, realice las correcciones necesarias y, a continuación, haga clic en **Test Connection**.



Para activar una licencia diferente

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**.

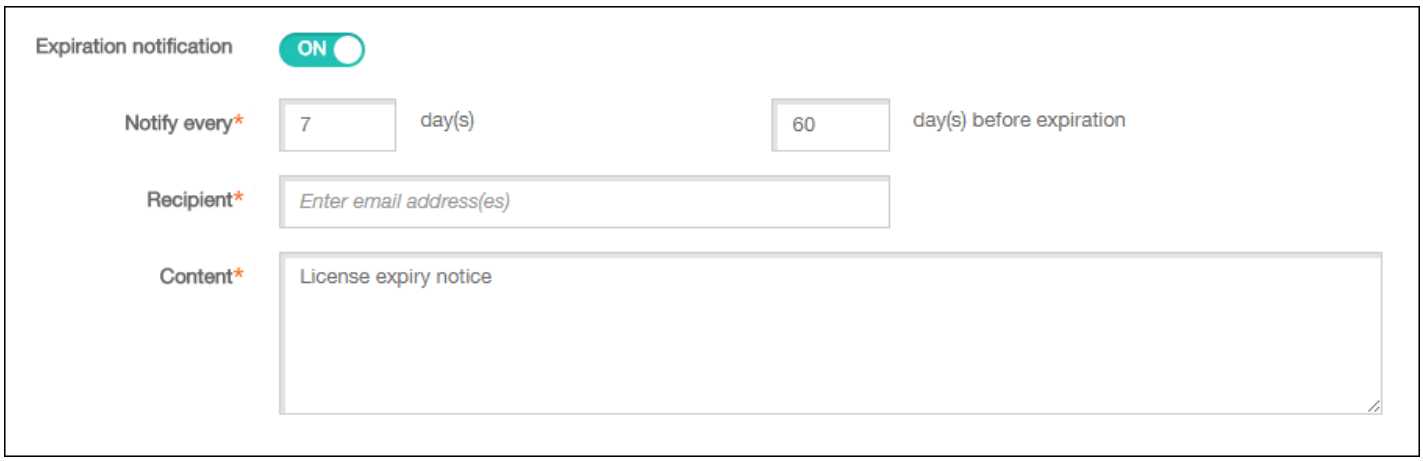
3. Haga clic en **Activate**. Se activa la licencia seleccionada.

> **Important**
>
> Si activa la licencia seleccionada, la licencia actualmente activa se desactiva.

Para automatizar una notificación de caducidad

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. Configure los siguientes parámetros:

- En **Notify every**, escriba:
  - La frecuencia con 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.
- **Recipient**. Escriba su dirección de correo electrónico o la de la persona responsable de la licencia.
- **Content**. Escriba el mensaje de notificación de caducidad que el destinatario verá en la notificación.

3. Haga clic en **Save**. En la cantidad de días antes de la caducidad que haya definido, XenMobile comienza a enviar mensajes de correo electrónico con el texto que haya proporcionado en **Content** al destinatario que haya indicado en **Recipient**. Las notificaciones se envían con la frecuencia que haya establecido.

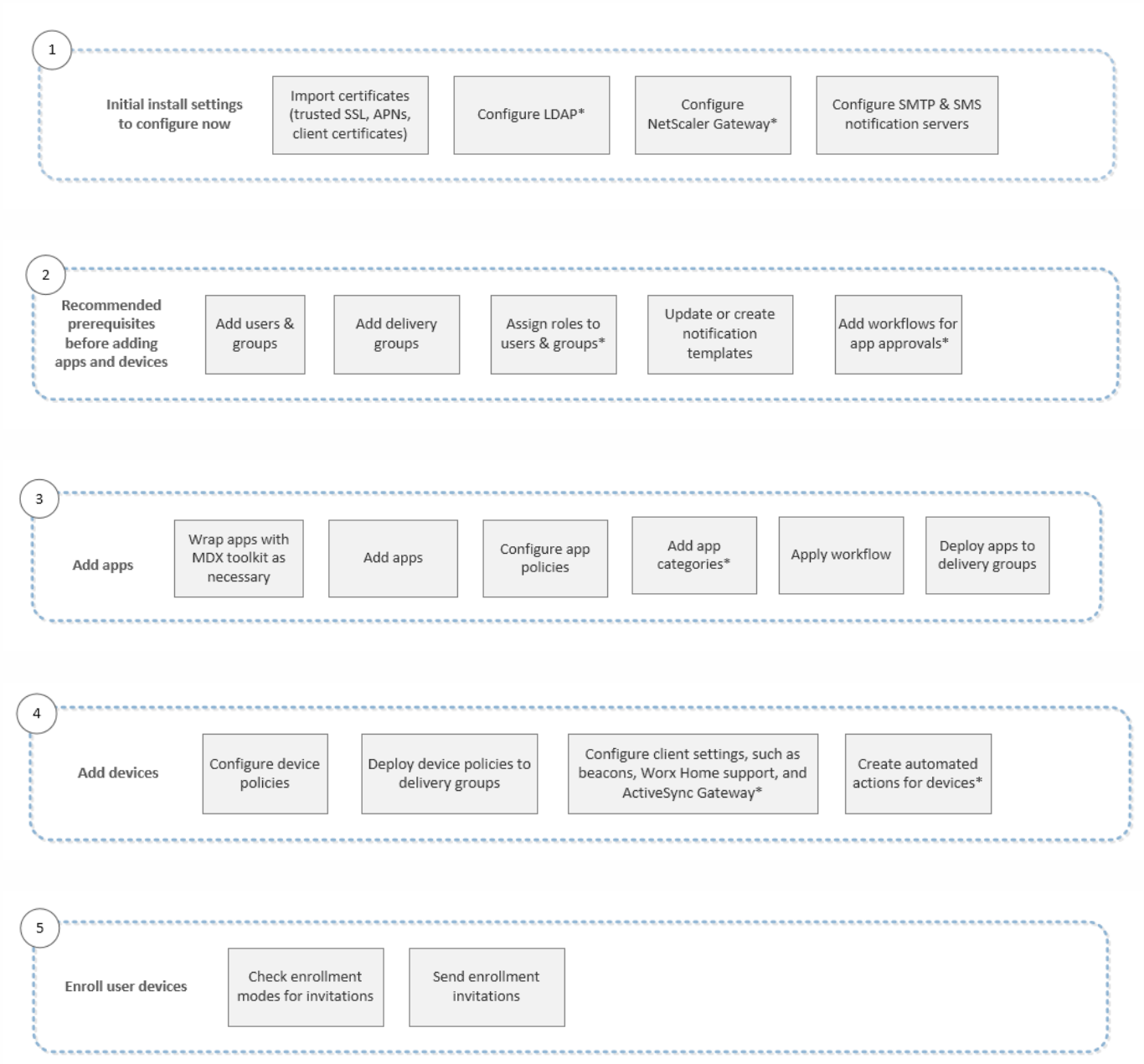
Introducción a la consola de XenMobile

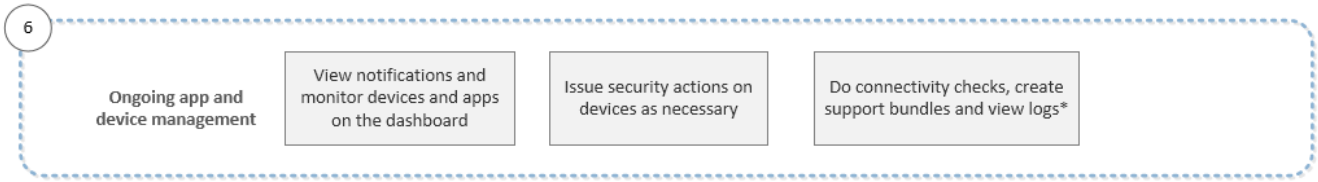
Jul 27, 2016

La consola de XenMobile es la herramienta de administración unificada para XenMobile. 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. Para obtener detalles sobre el respaldo de exploradores Web para la consola de XenMobile, consulte Repaldo para exploradores Web en el artículo de compatibilidad de XenMobile.

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.

Nota: Los elementos con un asterisco son optativos.



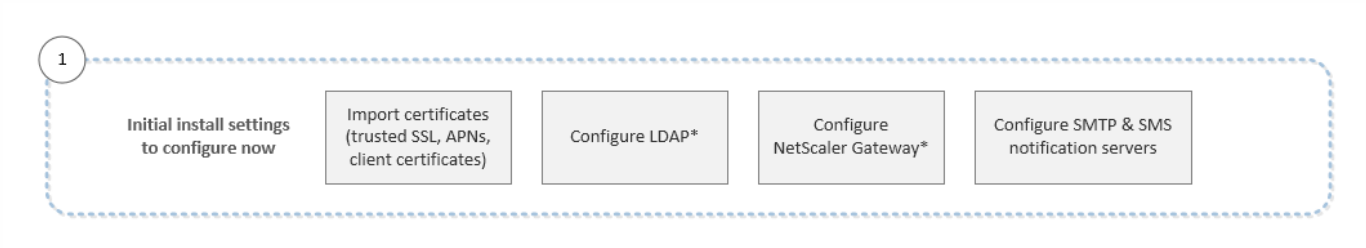


Flujo de trabajo para la configuración inicial

Jul 27, 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 empezar, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. 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 acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

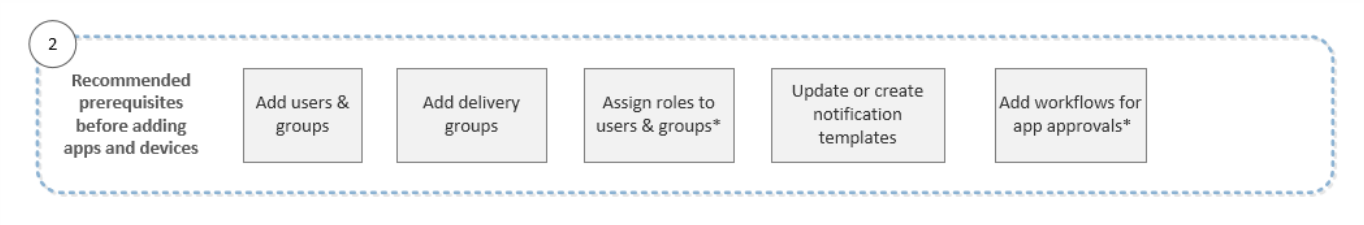
- Certificados en XenMobile
- Configuración de LDAP
- XenMobile y NetScaler Gateway
- Notificaciones en XenMobile

Flujo de trabajo para los requisitos previos de consola

Oct 31, 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 acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- Configuración de cuentas de usuario, roles y parámetros de inscripción
- Administración de grupos de entrega en XenMobile
- Configuración de roles 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

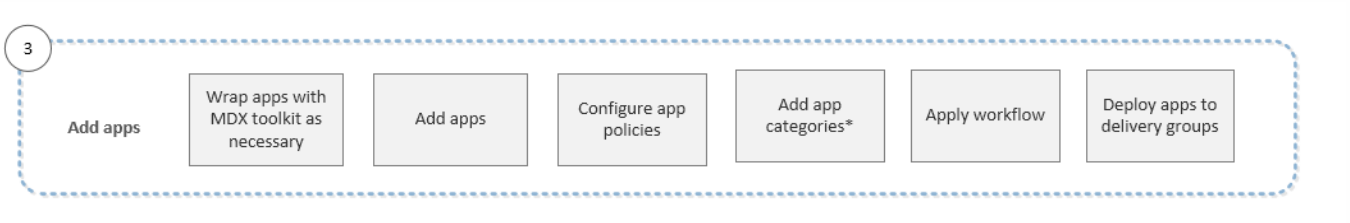
Oct 31, 2016

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 acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- Acerca del MDX Toolkit
- Incorporación de aplicaciones a XenMobile
- Vista general de las directivas MDX
- 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

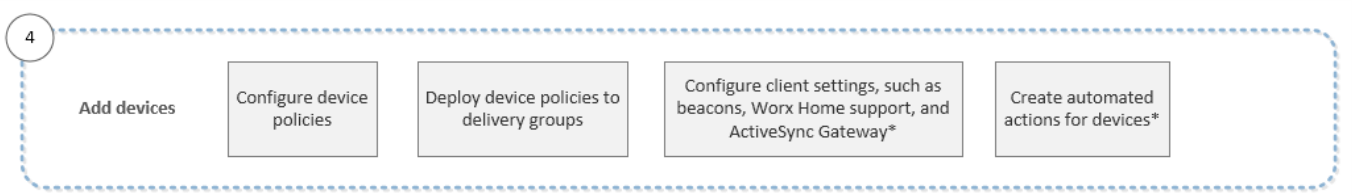
Jul 27, 2016

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 acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- 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

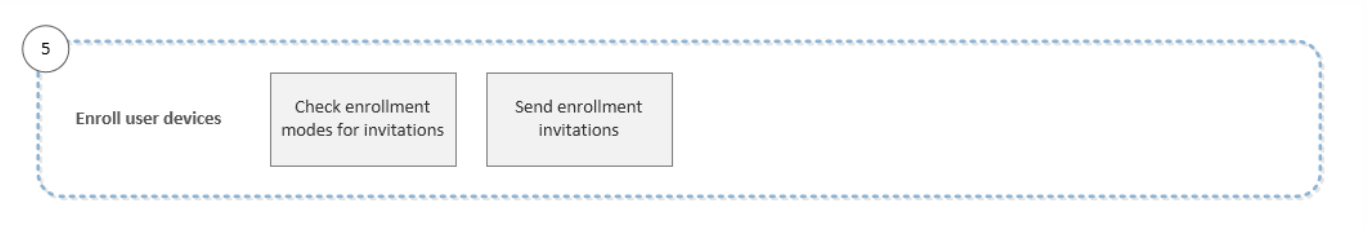
Flujo de trabajo para inscribir dispositivos de usuario

Jul 27, 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 acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- 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

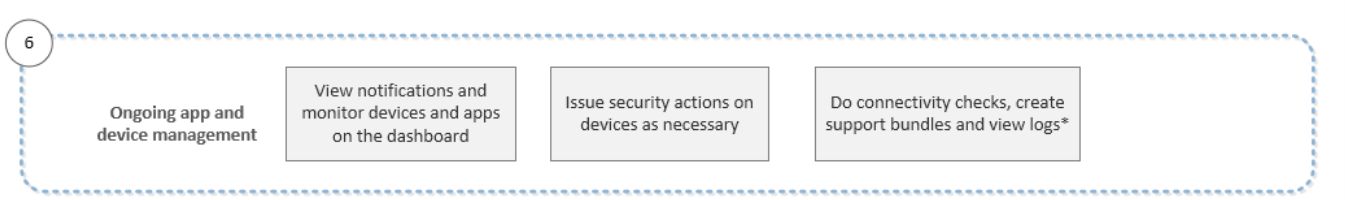
Jul 27, 2016

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

Jul 27, 2016

Existen filtros y tablas en toda la consola de XenMobile. Los puede ver en las fichas Devices, Enrollment, Device Policies, Apps, Actions y Delivery Groups, así como en la mayoría de las páginas de Settings. Con los filtros, puede limitar la información de cualquier área de la consola para localizar la información exacta que quiera ver o sobre la que quiera realizar una acción. Con las tablas, puede hacer clic en uno o varios elementos para ver las opciones de acciones que puede llevar a cabo en los elementos seleccionados. Las opciones pueden cambiar según la cantidad de elementos que seleccione.
En la siguiente tabla, se ofrecen algunas de las opciones más comunes, así como dónde las puede encontrar.

Opción de menú	**Acción**	**Tabla en que aparece la opción**
Agregue un	Agregar un elemento nuevo a la tabla.	All
Categoría	Agregar y administrar categorías de aplicaciones.	Apps
Copy URL	Copiar una dirección URL al Portapapeles.	Inscripción
Delete o Delete All	Eliminar permanentemente los elementos seleccionados.	All
Deploy	Implementar recursos para usuarios y dispositivos.	Devices y Delivery Groups
Inhabilitar	Inhabilitar una aplicación o el grupo de entrega AllUsers.	Apps y Delivery Groups
Edit	Realizar cambios en un elemento existente.	Todas excepto Enrollment
Export	Enviar el contenido de la tabla a un archivo CSV.	All
Import	Agregar dispositivos desde un archivo de aprovisionamiento.	Dispositivos
	Agregar grupos y usuarios locales a partir de un archivo.	Grupos y usuarios locales
Manage Local Groups	Agregar un grupo local para la administración.	Grupos y usuarios locales
Notify	Enviar una notificación a los usuarios y dispositivos seleccionados.	Enrollment y Devices
Refresh	Actualizar la tabla.	Dispositivos
Seguridad	Invocar acciones de seguridad en el dispositivo seleccionado.	Dispositivos

Opción de menú	Acción	Tabla en que aparece la opción
Self Help Portal	Habilitar el Self Help Portal como modo de inscripción.	Inscripción
Update	Actualizar los valores de la tabla.	Administración de versiones

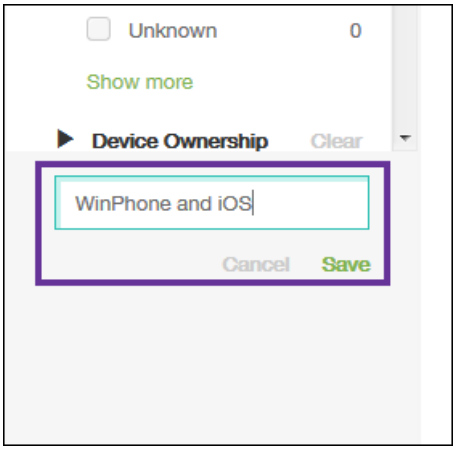
A continuación, se presentan varias maneras de ver las distintas opciones disponibles de llevar a cabo acciones basadas en la información de las tablas de la consola:

- Puede marcar la casilla de verificación ubicada junto a un elemento para que el menú de opciones aparezca sobre la lista.
- Puede marcar la casilla de verificación ubicada junto a más de un elemento para realizar una acción en todos los elementos a la vez. Lo que pueda llevar a cabo con varios elementos depende de la tabla que tenga en pantalla.
- Puede hacer clic en un elemento de la lista para que el menú de opciones aparezca a la derecha de la lista. Cuando haga clic en Show More, aparecerán datos detallados sobre el elemento. Lo que vea depende de la tabla que tenga en pantalla.
- Puede escribir el nombre completo o parcial en el cuadro de búsqueda para limitar la cantidad de elementos de la lista.

Solo se muestran 10 elementos por página en el área Device Policies de la consola. Haga clic en los triángulos situados en la esquina inferior derecha de la página para pasar páginas hacia delante y hacia atrás.

Si quiere ver un subconjunto específico de la información en un área de la consola (como Devices, Enrollment, Device Policies, Apps, Actions, Delivery Groups, Delivery Groups y Local Users and Groups), puede filtrar la lista en función de los criterios que seleccione. En este procedimiento, se utiliza la página Devices como ejemplo, pero los pasos para filtrar información son los mismos en toda la consola.

1. En la página Devices, haga clic en Show Filter.
   Aparece el panel de filtrado con los criterios mediante los que puede filtrar la lista Devices. Al mostrar el filtro por primera vez, todos los criterios aparecen contraídos.
2. Haga clic en el triángulo situado a la izquierda de un filtro para ver las opciones disponibles de ese filtro. Los números situados a la derecha de cada criterio representan la cantidad de dispositivos que incluye ese criterio.
3. Seleccione los criterios de filtrado que se van a utilizar. La lista Devices está limitada a los dispositivos que cumplen 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.
   - Haga clic en Clear, situado junto a un criterio concreto para eliminar ese filtro y quitar los elementos de la lista filtrada.
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 Save. Si decide no guardar el filtro, haga clic en Cancel.



6. Después de guardar el filtro, puede seleccionarlo en la parte inferior del panel Filter para filtrar la información de la tabla.
   Nota: Si hace clic en el triángulo ubicado a la derecha del nombre del filtro, puede eliminarlo o cambiarle el nombre.

Informes en XenMobile

Jul 27, 2016

XenMobile ofrece 10 informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones:

- **Apps by Devices & User**. Ofrece una lista de las aplicaciones que tienen los usuarios en sus dispositivos.
- **Terms & Conditions**. Ofrece una lista de los usuarios que hayan aceptado y rechazado los contratos de términos y condiciones.
- **Top 25 Apps**. Ofrece una lista de un máximo de 25 aplicaciones que tienen la mayoría de los usuarios en sus dispositivos.
- **Jailbroken/Rooted Devices**. Ofrece una lista de los dispositivos iOS liberados por jailbreak y de los dispositivos Android liberados por root.
- **Top 10 Apps – Failed Deployment**. Ofrece una lista de las aplicaciones que no se pudieron implementar.
- **Inactive Devices**. Ofrece una lista de los dispositivos que hayan estado inactivos durante un período de tiempo especificado.
- **Apps by Type & Category**. Ofrece una lista de las aplicaciones según su versión, tipo y categoría.
- **Device Enrollment**. Ofrece una lista de los dispositivos que se han inscrito durante un período de tiempo especificado.
- **Apps by Platform**. Ofrece una lista de las aplicaciones y sus versiones según la plataforma y la versión del dispositivo.
- **Devices & Apps**. Ofrece una lista de todos los dispositivos, los datos de dispositivo y las aplicaciones instaladas.

Los informes se presentan en formato CSV, y se pueden abrir con programas como Microsoft Excel. En la tabla siguiente, se muestran los encabezados y los informes en que se usan.

Encabezado	Descripción	Dónde se usa
ACCEPTANCE_STATUS	Estado de aceptación de los términos y condiciones	Terms & Conditions
APP_CATEGORY	Categoría en que se muestra la aplicación en los dispositivos (por ejemplo, aplicaciones de empresa o aplicaciones provenientes de tiendas públicas de aplicaciones)	Top 10 Apps – Failed Deployment, Apps by Type & Category, Devices & Apps
APP_ID	Identificador único de la aplicación	Devices & Apps
APP_NAME	Nombre de la aplicación	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Devices & Apps
APP_OWNER	Propietario de la aplicación (p. ej., Citrix.com en caso de aplicaciones Worx)	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Apps by Platform, Devices & Apps

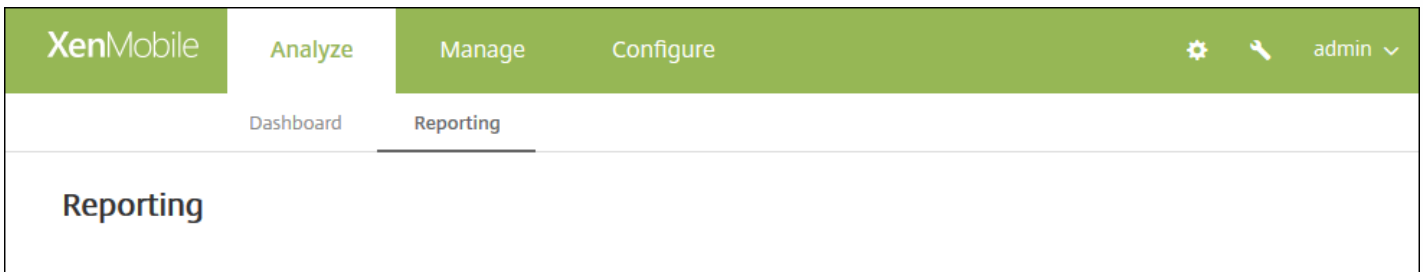
APP_TYPE	Tipo de aplicación (p. ej., de empresa o de tienda pública de aplicaciones)	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Devices & Apps
APP_VERSION	Versión de la aplicación	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Apps by Platform, Devices & Apps
APPS_ON_DEVICE	Cantidad de aplicaciones instaladas en el dispositivo	Apps by Devices & User
CERTIFICATE_EXPIRATION	Fecha de caducidad del certificado del dispositivo	Devices & Apps
CREATION_DATE	Fecha en que se creó el archivo de términos y condiciones	Terms & Conditions
DELIVERY_GROUP	Grupo de entrega asociado al recurso implementado	Terms & Conditions
DEPLOYMENT_DATE	Fecha en que se implementó el recurso	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Devices & Apps
DEPLOYMENT_SUCCESS, DEPLOYMENT_FAILED, DEPLOYMENT_PENDING	Estado de implementación	Apps by Devices & User, Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Apps by Platform, Devices & Apps
DEPLOYMENT_TOTAL	Cantidad total de implementaciones que se han intentado	Top 25 Apps, Top 10 Apps – Failed Deployment, Apps by Type & Category, Apps by Platform, Devices & Apps
DEVICE_MODE	Modo del dispositivo (administrado o no administrado)	Jailbroken/Rooted Devices, Inactive Devices, Device Enrollment, Devices & Apps, Devices & Apps
DEVICE_OWNERSHIP	Categorías referentes a la pertenencia del	Devices & Apps

	dispositivo (BYOD, de la empresa o pertenencia desconocida)	
DEVICE_PLATFORM	La plataforma del dispositivo	Apps by Platform
DEVICE_STATUS	Estado de cumplimiento del dispositivo	Devices & Apps
DEVICE_VERSION	Número de versión del sistema operativo del dispositivo	Apps by Platform
DOCUMENT_NAME	Nombre del archivo de términos y condiciones	Terms & Conditions
EMAIL	Dirección de correo electrónico del usuario	Devices & Apps
ENROLLMENT_DATE	Fecha en que el dispositivo se inscribió en XenMobile	Devices & Apps
ENROLLMENT_STATUS	Estado de inscripción del dispositivo (inscrito o no inscrito)	Devices & Apps
FIRST_CONNECTION_DATE	La fecha en que el dispositivo se conectó por primera vez a XenMobile	Inactive Devices, Device Enrollment
IMEI	Número IMEI (Device International Mobile Station Equipment Identity)	Dispositivos inactivos
LAST_ACTIVITY	Fecha de la última actividad de dispositivo	Dispositivos inactivos
LAST_AUTH_DATE	La fecha de la última vez que el dispositivo se autenticó en XenMobile	Inactive Devices, Device Enrollment, Devices & Apps
LAST_USERNAME	Último nombre asociado al dispositivo	Jailbroken/Rooted Devices, Inactive Devices, Device Enrollment
LOCATION	Ubicación geográfica del dispositivo	Devices & Apps
MANAGED	Indica si el dispositivo está administrado o no	Jailbroken/Rooted Devices

MODEL	Modelo del dispositivo	Jailbroken/Rooted Devices, Inactive Devices, Device Enrollment, Apps by Platform
MODEL_NAME	Modelo del dispositivo	Devices & Apps
OS_VERSION	Versión del sistema operativo en el dispositivo	Apps by Devices & User, Inactive Devices, Device Enrollment, Devices & Apps
PHONE_NUMBER	Número de teléfono del usuario	Device Enrollment
PLATFORM	La plataforma del dispositivo	Apps by Devices & User, Terms & Conditions, Jailbroken/Rooted Devices, Inactive Devices, Device Enrollment, Devices & Apps
SERIAL_NUMBER	Número de serie del dispositivo	Apps by Devices & User, Jailbroken/Rooted Devices, Inactive Devices, Devices & Apps
USER EMAIL	Dirección de correo electrónico del usuario	Apps by Devices & User
USER_ID	Número único del usuario	Devices & Apps
USER_NAME	User name	Apps by Devices & User, Terms & Conditions, Devices & Apps
USERID	ID de usuario	Apps by Devices & User

Siga estos pasos para crear un informe:

1. En la consola de XenMobile, haga clic en la ficha **Analyze** y, a continuación, haga clic en **Reporting**. Aparecerá la página **Reporting**.



Apps by Devices & User

List of apps that users have on their devices.

Report Data: device serial number, device platform, version, user name, ID, email, # of apps, deployment status.

Terms & Conditions

List of accepted and declined Terms and Conditions agreements by device users.

Report Data: document name, created on, platform, user name, delivery group, acceptance status.

Top 25 Apps

List of apps most users have installed.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Jailbroken/Rooted Devices

List of jailbroken iOS and rooted Android devices.

Report Data: device platform, model, version, serial number, user name, device mode, status.

Top 10 Apps - Failed Deployment

List of apps that have failed deployment.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Inactive Devices

List of devices that have been inactive for a specified length of time.

Report Data: last activity, device mode, platform, version, user name, last authentication, device IMEI, serial number, model, first connection.

Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

Devices & Apps

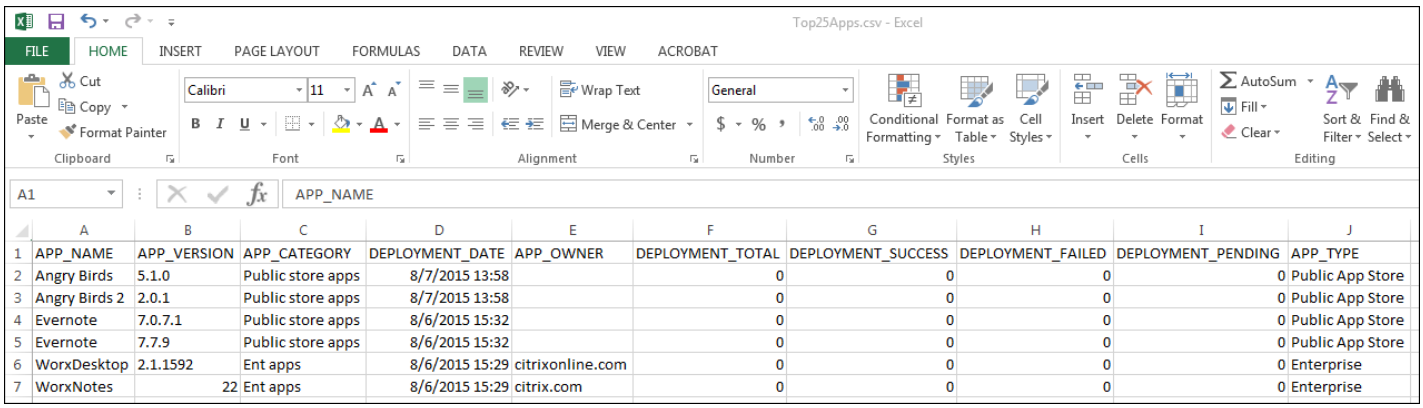
List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

2. Haga clic en el informe que quiere crear. En función del explorador Web que utilice, el archivo se descargará automáticamente o se le pedirá que lo guarde.

3. Repita el paso 2 para cada informe que quiera crear.

A continuación, se ofrece un ejemplo del informe Top 25 Apps abierto en Microsoft Excel:



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

Notificaciones

Jul 27, 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 Acciones automatizadas.

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 de 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.

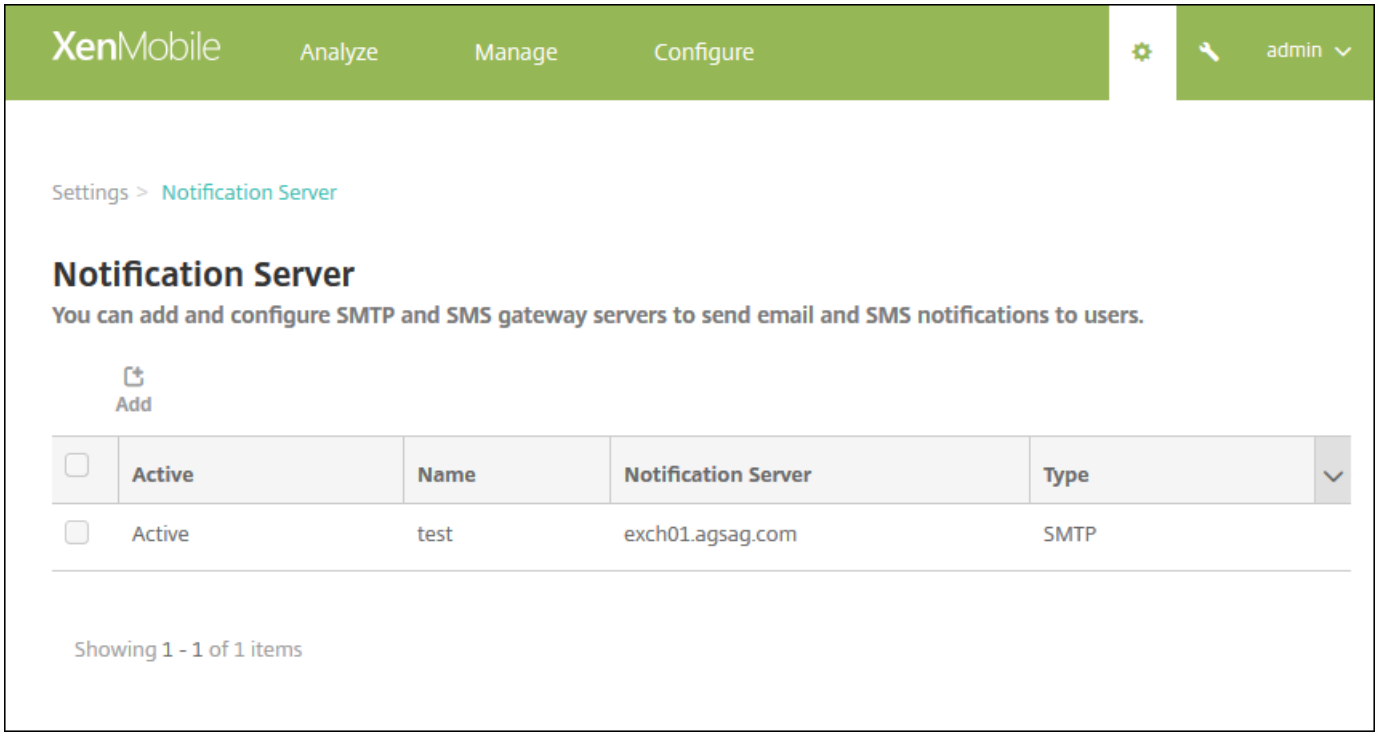
En los procedimientos de este artículo se describe la forma de configurar un servidor SMTP, una puerta de enlace SMS y una puerta de enlace SMS de operador.

- 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.

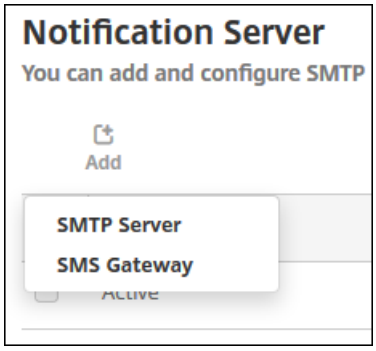
- Solo hay activo un solo servidor SMTP y un solo servidor SMS a la vez.
- Debe abrir el puerto 25 desde XenMobile (ubicado en la zona DMZ de la red) para apuntarlo al servidor SMTP de la red interna para que las notificaciones se envíen correctamente.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

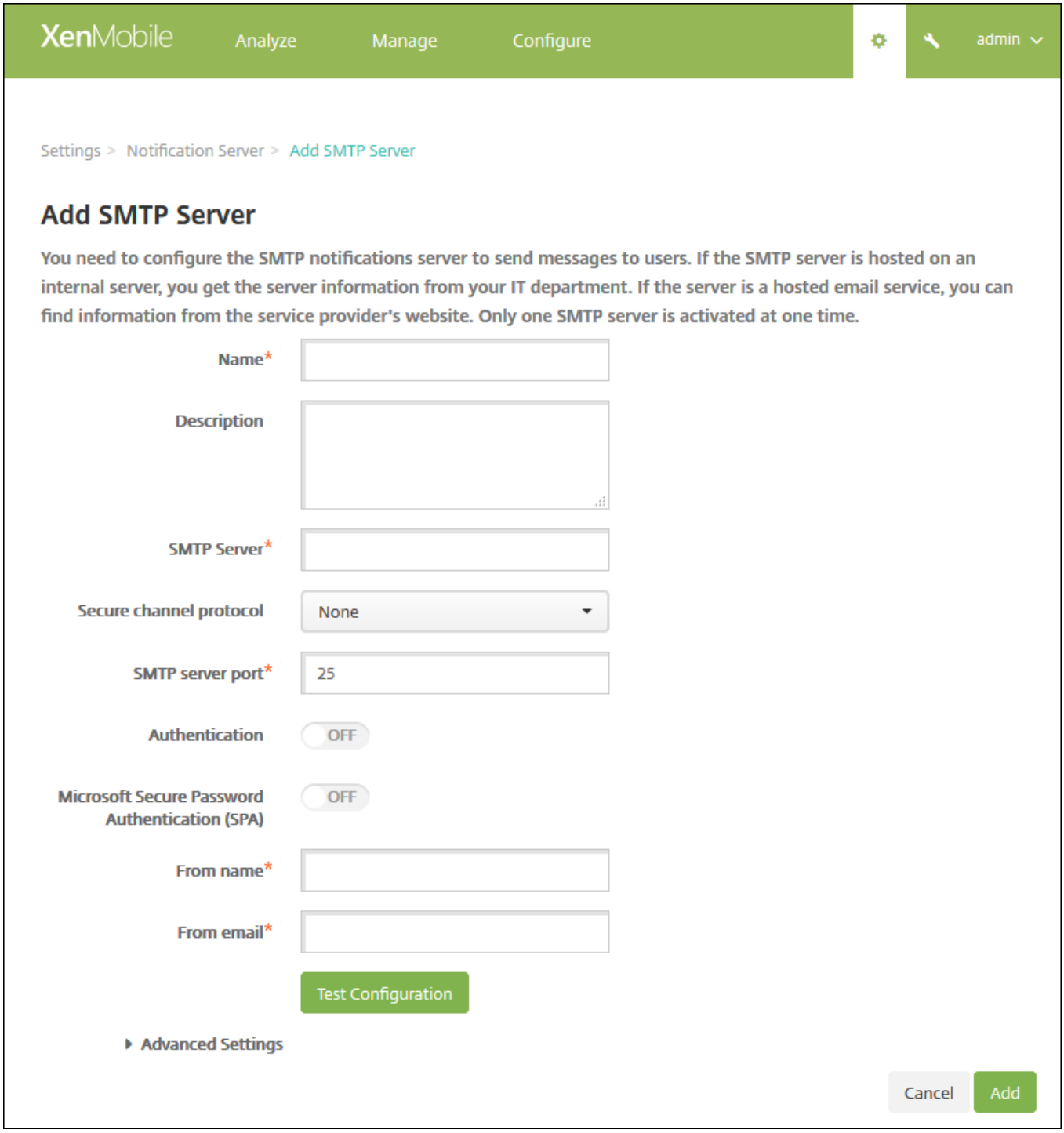
2. En **Notifications**, haga clic en **Notification Server**. Aparecerá la página **Notification Server**.



2. Haga clic en **Add**. Aparece un menú con las opciones para configurar un servidor SMTP o una puerta de enlace SMS.



- Para agregar un servidor SMTP, haga clic en **SMTP Server**. A continuación, vaya a Para agregar un servidor SMTP y consulte los pasos que se deben seguir para configurar este parámetro.
- Para agregar una puerta de enlace SMS, haga clic en **SMS Gateway**. A continuación, vaya a Para agregar una puerta de enlace SMS y consulte los pasos que se deben seguir para configurar este parámetro.



1. 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 **SSL**, **TLS** o **None** para definir el protocolo de canal seguro que utiliza el

servidor (si el servidor está configurado para usar la autenticación segura). El valor predeterminado es **None**.

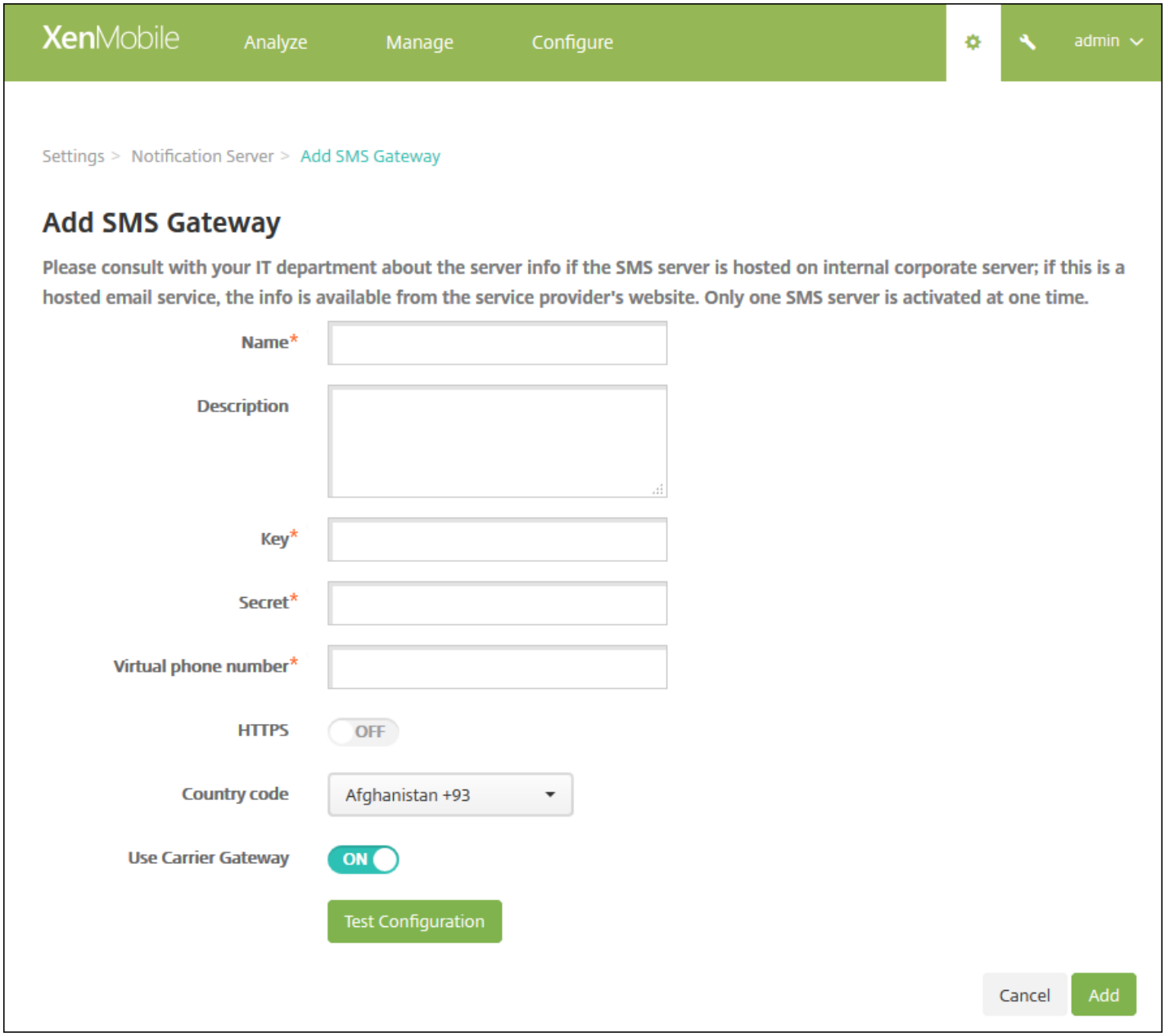
- **SMTP server port**. Escriba el puerto que usa el servidor SMTP. De forma predeterminada, el puerto definido es el 25. En cambio, si las conexiones SMTP usan el protocolo SSL de canal seguro, el puerto definido es 465.
- **Authentication**. Seleccione **ON** u **OFF**. El valor predeterminado es **OFF**.
- Si habilita **Authentication**, configure los siguientes parámetros:
  - **User name**. Escriba el nombre de usuario que se usará para la autenticación.
  - **Password**. Escriba la contraseña de autenticación del usuario.
- **Microsoft Secure Password Authentication (SPA)**. Si el servidor SMTP usa la autenticación SPA, haga clic en **ON**. El valor predeterminado es **OFF**.
- **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.

2. Haga clic en **Test Configuration** para enviar una notificación de prueba por correo electrónico.

3. Expanda **Advanced Settings** y, a continuación, configure estos parámetros:

- **Number of SMTP retries**. Escriba el número de reintentos de envío de un mensaje fallido enviado desde el servidor SMTP. El valor predeterminado es 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. El valor predeterminado es de 30 segundos.
- **Maximum number of SMTP recipients**. Escriba la cantidad máxima de destinatarios por mensaje de correo electrónico enviado por el servidor SMTP. El valor predeterminado es 100.

4. Haga clic en **Add**.



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. Configure los siguientes parámetros:

- **Name**. Escriba un nombre para la configuración de la puerta de enlace SMS. Este campo es obligatorio.
- **Description**. Si quiere, escriba una descripción de la configuración.
- **Key**. Escriba el identificador numérico proporcionado por el administrador del sistema para la activación de la cuenta. Este campo es obligatorio.
- **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. Este campo es obligatorio.

- **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 si quiere utilizar HTTPS para la transmisión de solicitudes de SMS a Nexmo. El valor predeterminado es **OFF**.
- **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 +. El valor predeterminado es **Afghanistan +93**.

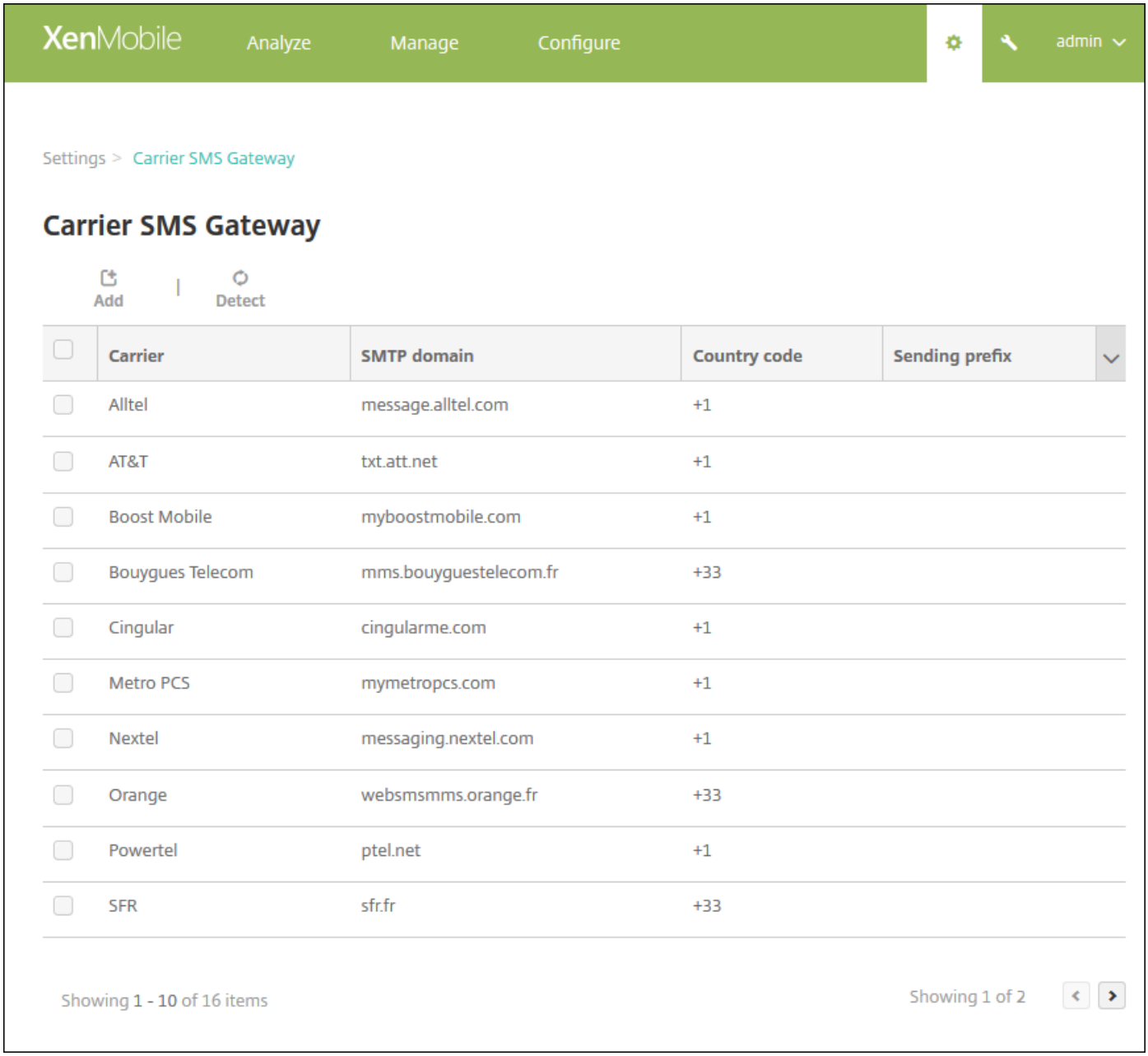
2. Haga clic en **Test Configuration** para enviar un mensaje de prueba con la configuración actual. Los errores de conexión, como aquellos relacionados con errores de autenticación o de números de teléfono virtual, se detectan y aparecen inmediatamente. Los mensajes se reciben en el mismo período de tiempo que los que se envían entre teléfonos móviles.

2. Haga clic en **Add**.

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.

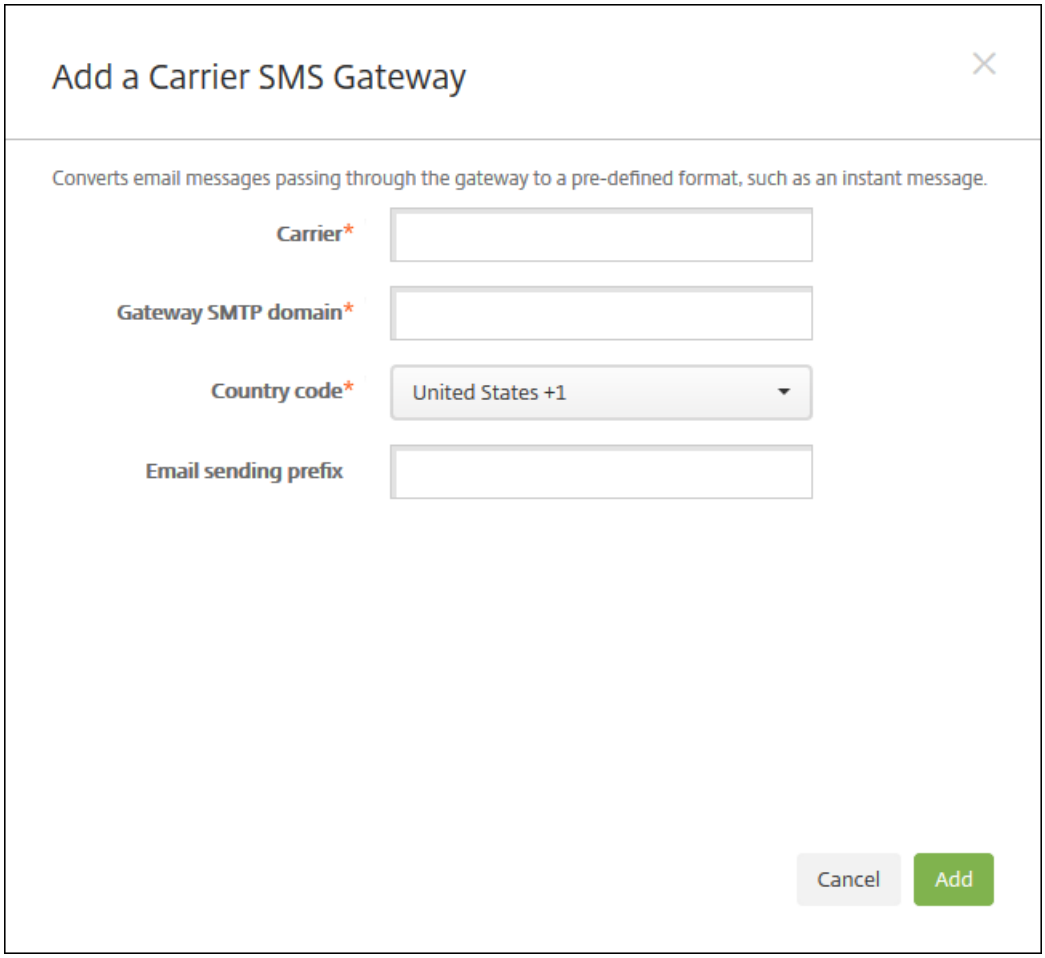
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. En **Notifications**, haga clic en **Carrier SMS Gateway**. Se abrirá la página **Carrier SMS Gateway**.



3. Lleve a cabo una de las siguientes acciones:

- Haga clic en **Detect** para detectar automáticamente una puerta de enlace. Aparecerá un cuadro de diálogo en el que se indicará que no hay nuevos operadores detectados, o bien se mostrarán los nuevos operadores detectados de los dispositivos inscritos.
- Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a Carrier 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.

4. Configure los siguientes parámetros:

- **Carrier**. Escriba el nombre del operador.
- **Gateway SMTP domain**. Escriba el dominio asociado a la puerta de enlace SMTP.
- **Country code**. En la lista, haga clic en el código del país del operador.
- **Email sending prefix**. Si lo prefiere, puede especificar un prefijo de envío de correo electrónico.

5. Haga clic en **Add** para agregar el nuevo operador, o bien haga clic en **Cancel** para no agregarlo.

XenMobile y NetScaler Gateway

Oct 31, 2016

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

Nota: Para ver cuáles son las versiones de NetScaler Gateway respaldadas con XenMobile, consulte Compatibilidad con XenMobile. Para obtener información sobre cómo configurar NetScaler Gateway para XenMobile en NetScaler, consulte Configuring Settings for Your XenMobile Environment.

Autenticación

Existen varios componentes que desempeñan un papel en la autenticación durante las operaciones de XenMobile:

- **Servidor XenMobile**. La seguridad de la inscripción, así como la experiencia de la inscripción, se definen desde servidor XenMobile. Desde aquí también puede definir opciones para los nuevos usuarios; por ejemplo, puede decidir si la inscripción va a ser para todos o solo se va a obtener por invitación y si requerir la autenticación de dos o tres factores. A través de las propiedades de cliente en XenMobile, puede habilitar la autenticación con PIN de Worx y configurar la complejidad y el tiempo de caducidad de ese PIN.
- **NetScaler**. Con NetScaler, puede finalizar sesiones SSL de micro VPN, proteger la seguridad de los datos en tránsito en la red y definir la experiencia de autenticación cada vez que un usuario accede a una aplicación.
- **Worx Home**. Worx Home funciona con el servidor XenMobile en las operaciones de inscripción. Presente en el dispositivo, Worx Home es la entidad que se comunica con NetScaler. Si una sesión caduca, Worx Home obtiene un tíquet de autenticación de NetScaler y lo envía a las aplicaciones MDX. Citrix recomienda usar la fijación de certificados, que impide ataques de intermediarios (ataque de tipo "Man in the middle"). Para obtener más información, consulte la sección sobre la fijación de certificados en el artículo Worx Home.

  Asimismo, Worx Home favorece a la seguridad del contenedor MDX, ya que envía directivas, crea sesiones nuevas con NetScaler cuando se agota el tiempo de espera de una aplicación y define el tiempo de espera y la experiencia de autenticación MDX. Worx Home también es responsable de detectar la liberación por jailbreak, comprobar la geolocalización y las directivas que se apliquen.
- **Directivas MDX**. Las directivas MDX crean la caja fuerte de datos en el dispositivo. Las directivas MDX dirigen las conexiones de micro VPN de nuevo a NetScaler, aplican las restricciones del modo desconectado y las directivas de cliente (como los tiempos de espera).

Para obtener más información sobre la autenticación (incluidos los métodos de autenticación de uno o dos factores), las directivas, las configuraciones y las propiedades de cliente que intervienen en la autenticación; para ver ejemplos de tres configuraciones de XenMobile de menor a mayor seguridad, consulte Autenticación.

Para obtener información acerca de la configuración, consulte los siguientes artículos:

Configuración de la autenticación de dominios y tokens de seguridad

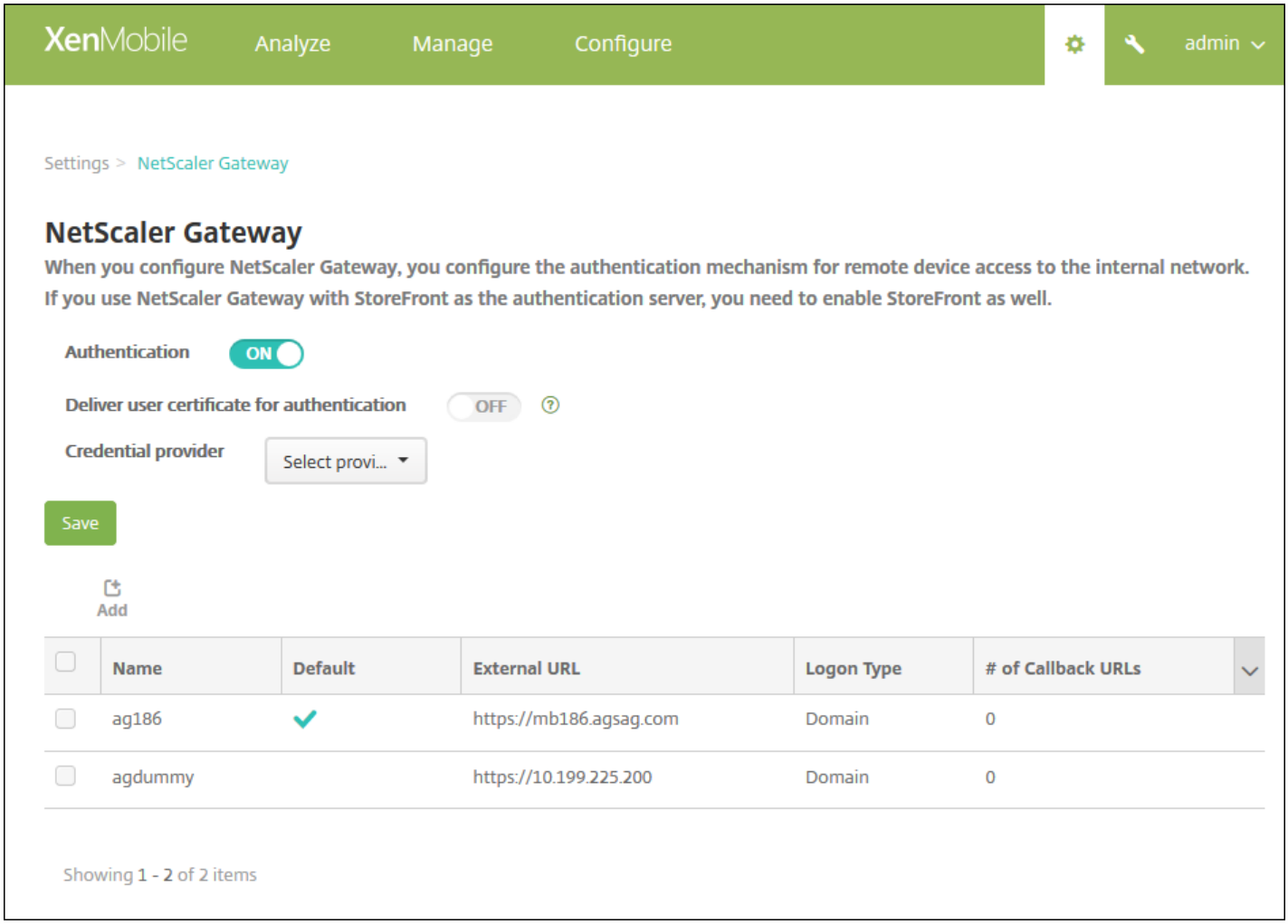
Configuración de la autenticación con certificados del cliente

Configuración de XenMobile para la autenticación con certificado y token de seguridad

Configuración de XenMobile y de la aplicación de ShareFile para Single Sign-On mediante SAML

1. En la consola Web de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **NetScaler Gateway**. Aparecerá la página **NetScaler Gateway**.



Configure estos parámetros:

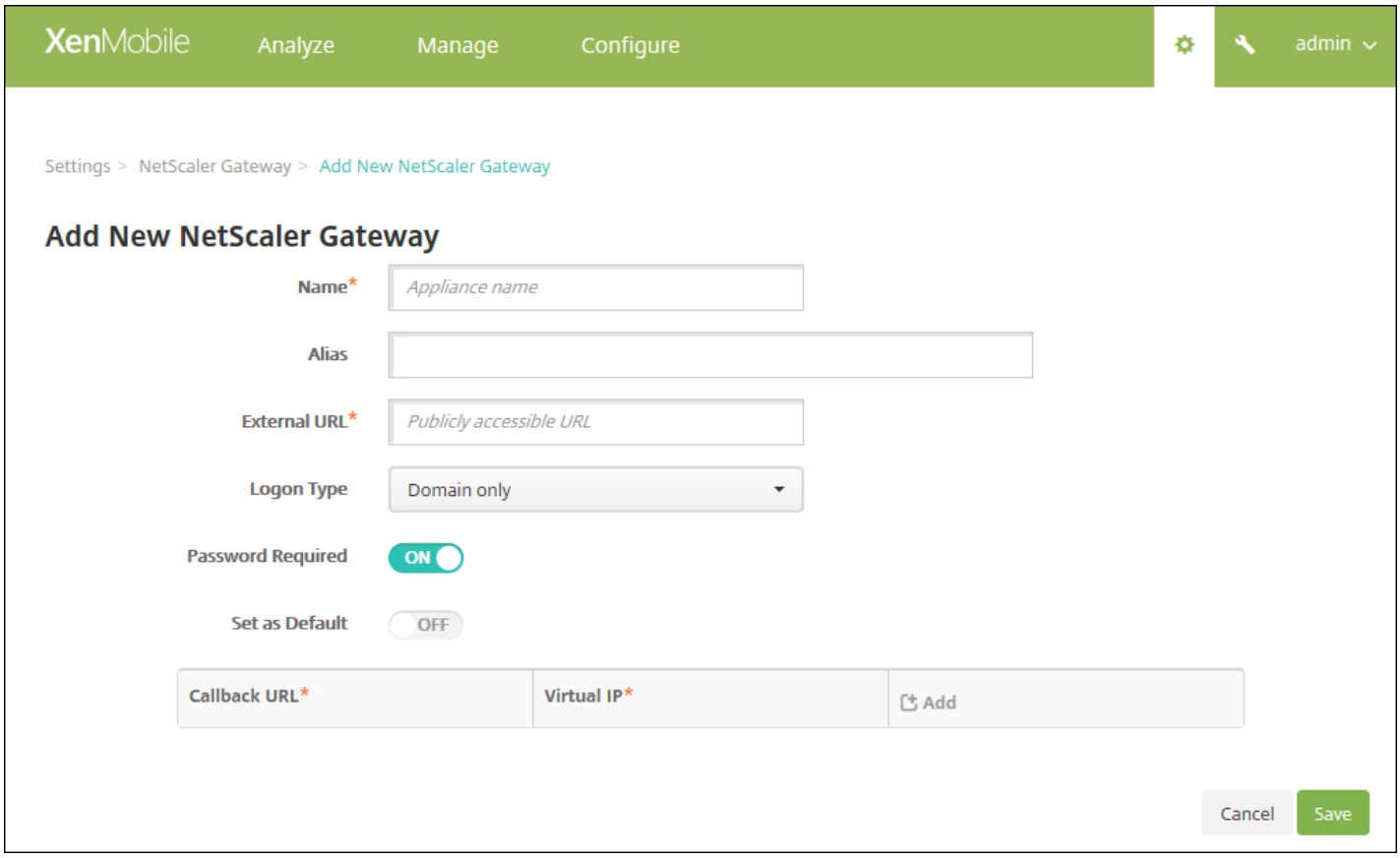
- **Authentication**. Seleccione si quiere habilitar la autenticación. El valor predeterminado es **ON**.
- **Deliver user certificate for authentication**. Seleccione si quiere que XenMobile comparta el certificado de autenticación con Worx Home para que NetScaler Gateway gestione la autenticación de certificados de cliente. El valor predeterminado es **OFF**.
- **Credential Provider**. En la lista, haga clic en el proveedor de credenciales que se va a utilizar. Para obtener más información, consulte Proveedores de credenciales.

3. Haga clic en **Save**.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **NetScaler Gateway**. Aparecerá la página **NetScaler Gateway**.

3. Haga clic en **Add**. Aparecerá la página **Add New NetScaler Gateway**.



4. Configure los siguientes parámetros:

- **Name**. Escriba un nombre para la instancia de NetScaler Gateway.
- **Alias**. Puede incluir un alias.
- External URL. Escriba la URL de acceso público de NetScaler Gateway. Por ejemplo, https://receiver.com.
- **Logon Type**. En la lista, 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**. El valor predeterminado es **Domain only**.

  Si dispone de varios dominios, la opción **Domain only** no funcionará, por lo que deberá utilizar **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.

  Si utiliza la opción **Certificate and security token**, se necesita configuración adicional en NetScaler Gateway para que

admita Worx Home. Para obtener más información, consulte Configuring XenMobile for Certificate and Security Token Authentication.

- **Password Required**. Seleccione si quiere que se solicite la contraseña para la autenticación. El valor predeterminado es **ON**.
- **Set as Default**. Seleccione si quiere usar esta instancia de NetScaler Gateway como predeterminada. El valor predeterminado es **OFF**.

5. Haga clic en **Save**. 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**. Aparecerá la página **Add New NetScaler Gateway**.

2. 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 y haga clic en **Guardar**.

Configuración de LDAP

Aug 25, 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 para 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.

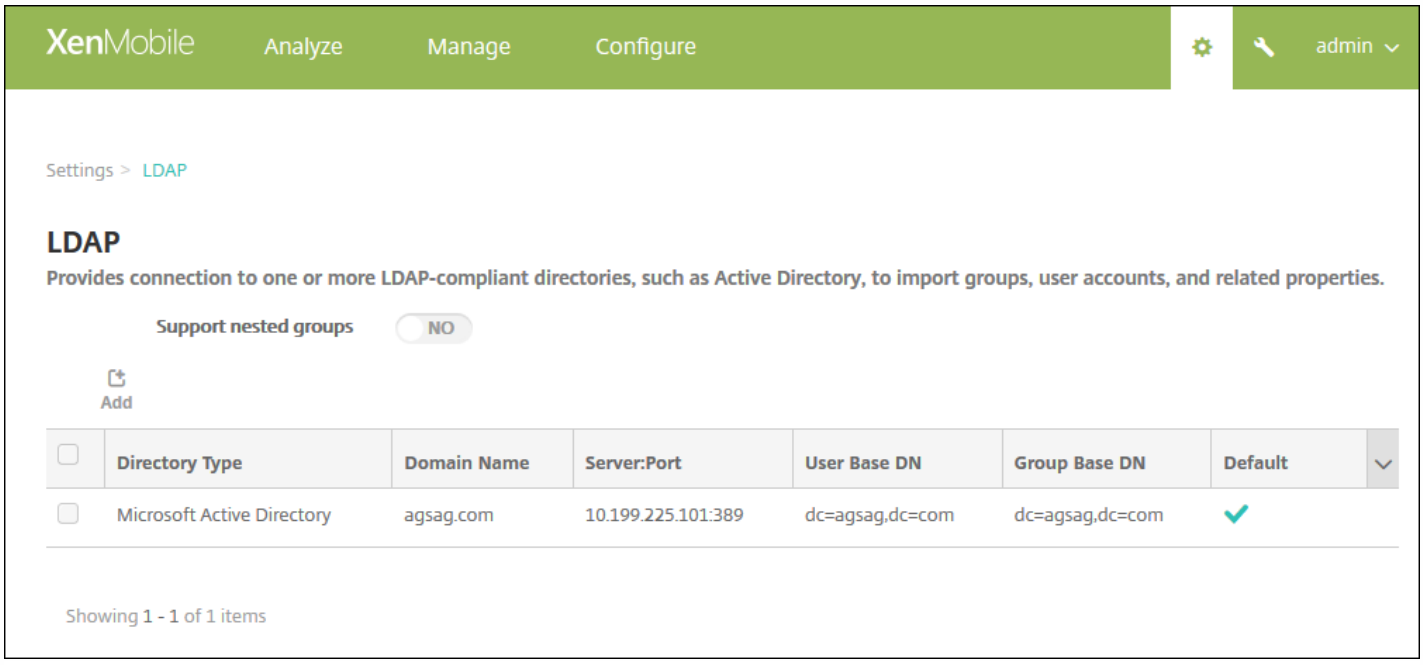
Cómo funciona el protocolo LDAP

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.

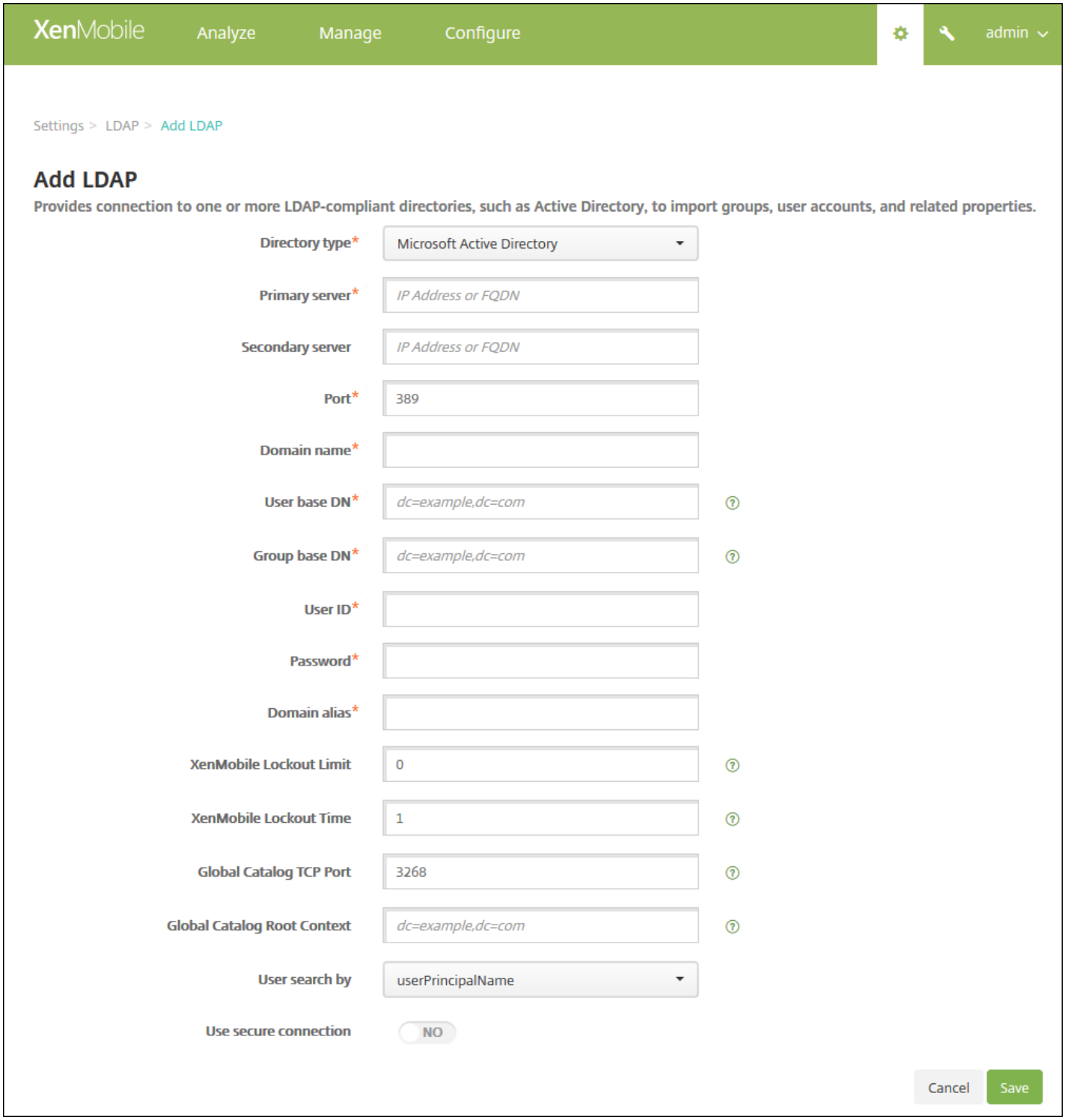
Para agregar conexiones LDAP a XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **LDAP**. Aparecerá la página **LDAP**. Puede agregar, modificar o eliminar directorios compatibles con el protocolo LDAP desde esta página.



1. En la página **LDAP**, haga clic en **Add**. Aparecerá la página **Add LDAP**.



2. Configure los siguientes parámetros:

- **Directory type**. En la lista, haga clic en el tipo de directorio correspondiente. El valor predeterminado es **Microsoft Active Directory**.
- **Primary server**. Escriba 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).

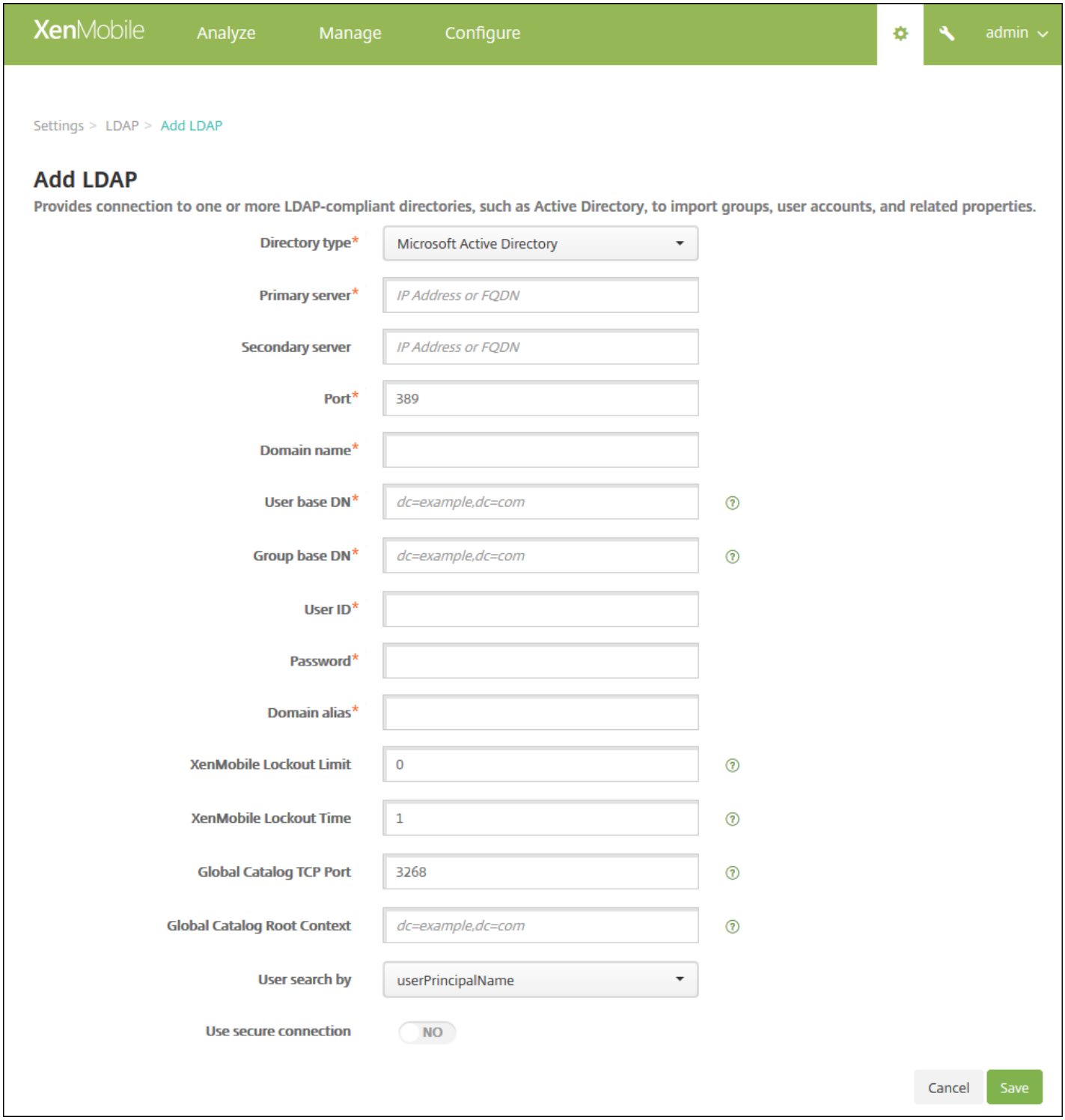
- **Port**. Escriba el número de puerto que utiliza el servidor LDAP. De forma predeterminada, el número de puerto es 389 para conexiones LDAP no protegidas. Use el número de puerto 636 para conexiones LDAP protegidas, el 3268 para conexiones LDAP no protegidas de Microsoft o el 3269 para conexiones LDAP protegidas de Microsoft.
- **Domain name**. Introduzca el nombre de dominio.
- **User base DN**. Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Algunos ejemplos de sintaxis: ou=usuarios, dc=ejemplo, dc=com.
- **Group base DN**. Escriba 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 nombre del servidor que ejecuta Active Directory.
- **User ID**. Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Password**. Escriba la contraseña asociada al usuario.
- **Domain alias**. Escriba un alias del nombre de dominio.
- **XenMobile Lockout Limit**. Escriba un número comprendido entre 0 y 999 para la cantidad de intentos fallidos de inicio de sesión. Si escribe 0 en este campo, XenMobile no bloqueará nunca a un usuario por intentos fallidos de inicio de sesión.
- **XenMobile Lockout Time**. Escriba 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, el usuario no deberá esperar después de un bloqueo.
- **Global Catalog TCP Port**. Escriba 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 escribir 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**. El valor predeterminado es **userPrincipalName**.
- **Use secure connection**. Seleccione si utilizar conexiones protegidas. El valor predeterminado es **NO**.

3. Haga clic en **Save**.

1. En la tabla **LDAP**, seleccione el directorio a modificar.

> **Nota**: Si marca la casilla situada junto a un directorio, el menú de opciones aparecerá encima de la lista LDAP. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.

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



3. Cambie la siguiente información como corresponda:

- **Directory type**. En la lista, haga clic en el tipo de directorio correspondiente.
- **Primary server**. Escriba 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**. Escriba 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**. No puede cambiar este campo.
- **User base DN**. Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Algunos ejemplos de sintaxis: ou=usuarios, dc=ejemplo, dc=com.
- **Group base DN**. Escriba 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 nombre del servidor que ejecuta Active Directory.
- **User ID**. Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Password**. Escriba la contraseña asociada al usuario.
- **Domain alias**. Escriba 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**. Escriba 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, el usuario no deberá esperar después de un bloqueo.
- **Global Catalog TCP Port**. Escriba 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 escribir 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**. Seleccione si utilizar conexiones protegidas.

4. Haga clic en **Save** para guardar los cambios o en **Cancel** para no realizar cambios en la propiedad.

1. En la tabla **LDAP**, seleccione el directorio a 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**.

Configuración de la autenticación de dominios y tokens de seguridad

Oct 31, 2016

Puede configurar XenMobile para exigir a los usuarios que se autentiquen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso.

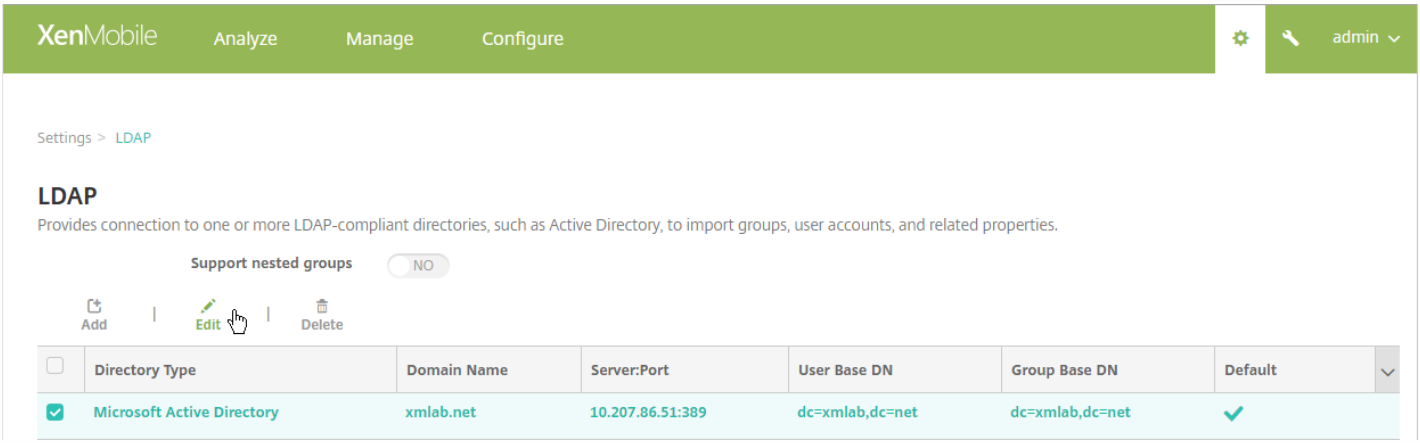
Para disfrutar de una usabilidad óptima, puede combinar esta configuración con un PIN de Worx y el almacenamiento en caché de contraseñas de Active Directory, de modo que los usuarios no tengan que escribir continuamente su nombre de usuario y su contraseña de Active Directory. Los usuarios necesitarán escribir su nombre de usuario y su contraseña para la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

Configuración de parámetros de LDAP

El uso del protocolo LDAP para la autenticación exige que se instale un certificado SSL desde una autoridad certificadora en XenMobile. Para obtener más información, consulte Carga de certificados en XenMobile.

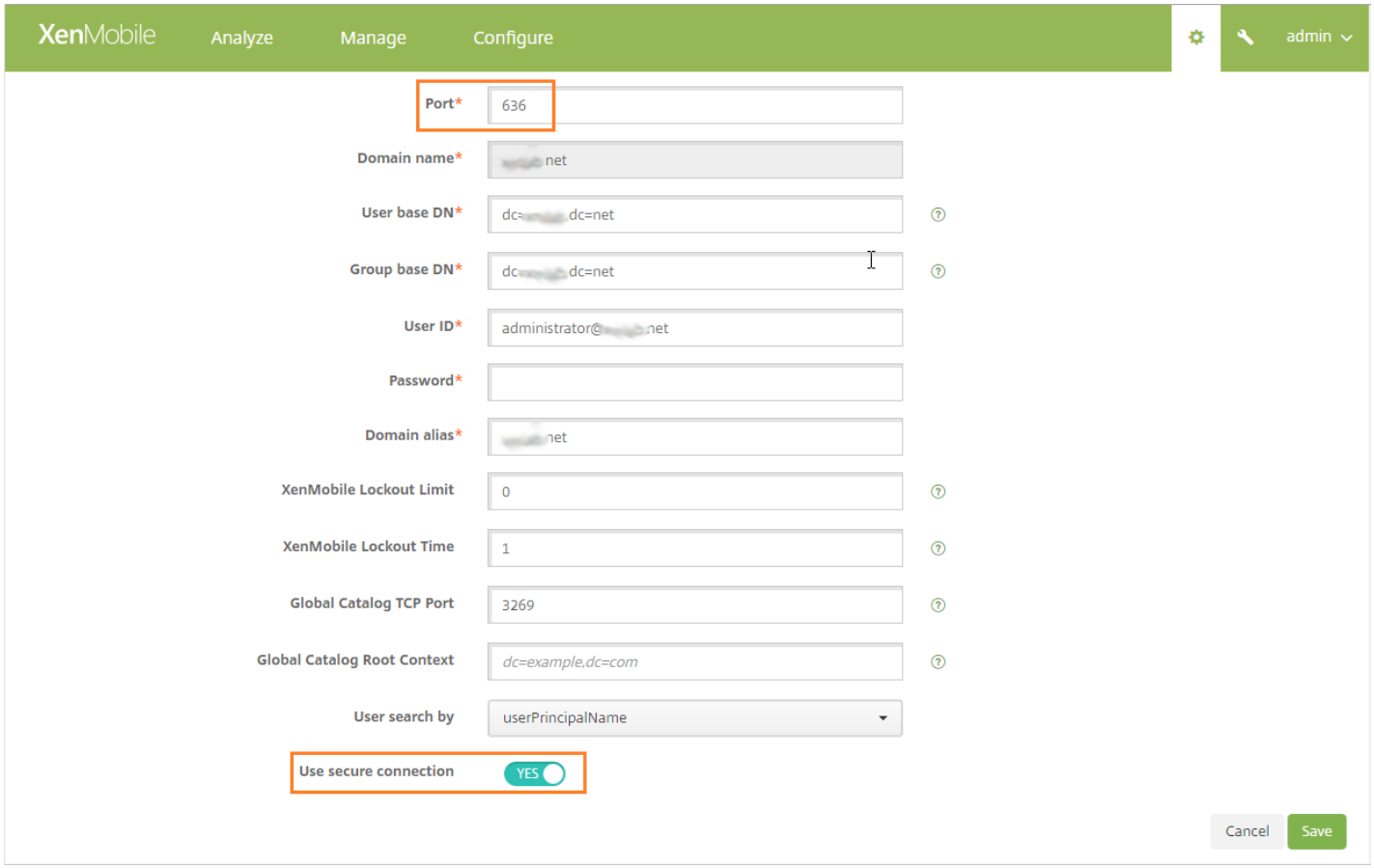
1. En **Settings**, haga clic en **LDAP**.

2. Seleccione **Microsoft Active Directory** y, a continuación, haga clic en **Edit**.



3. Verifique que el campo **Port** es **636** para conexiones LDAP seguras, o bien **3269** para conexiones LDAP seguras de Microsoft.

4. Cambie **Use secure connection** a **Yes.**



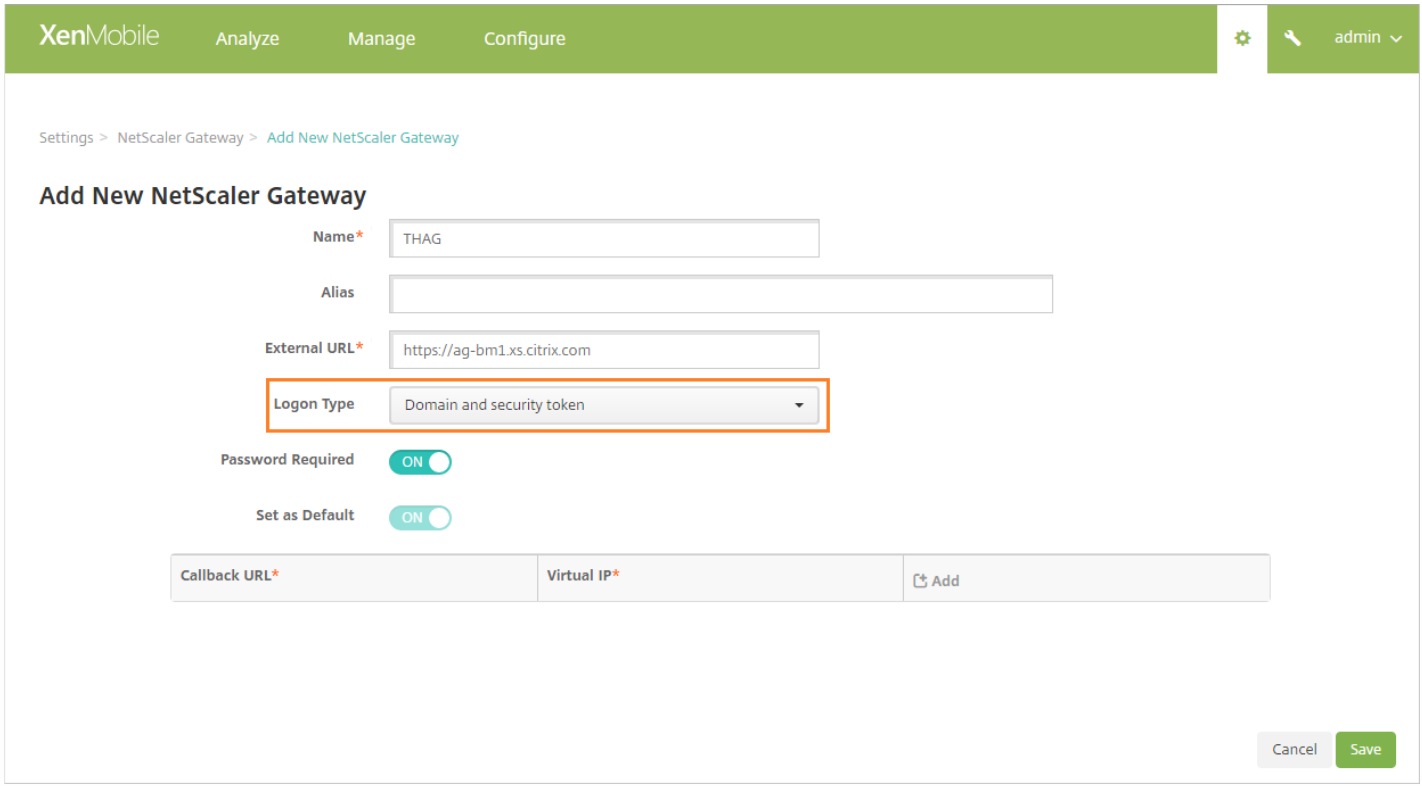
Configuración de los parámetros de NetScaler Gateway

En los siguientes pasos se supone que ya ha agregado una instancia de NetScaler Gateway a XenMobile. Para agregar una instancia de NetScaler Gateway, consulte NetScaler Gateway y XenMobile.

1. En **Settings**, haga clic **NetScaler Gateway**.

2. Seleccione NetScaler Gateway y, a continuación, haga clic en **Edit**.

3. En **Logon Type**, seleccione **Domain and security token**.



Cómo habilitar el PIN de Worx y el almacenamiento en caché de contraseñas de Active Directory

Para habilitar el PIN de Worx y el almacenamiento en caché de contraseñas de Active Directory, vaya a **Settings > Client Properties** y seleccione las casillas de verificación de **Enable Worx PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte Referencia de propiedades de cliente.

Configuración de NetScaler Gateway para la autenticación de dominios y tokens de seguridad

Configure directivas y perfiles de sesión de NetScaler Gateway para los servidores virtuales que utilice con XenMobile. Para obtener más información, consulte Configuración de la autenticación de dominios y tokens de seguridad en la documentación de NetScaler Gateway.

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.

La autenticación con certificados de cliente proporciona una capa de seguridad adicional para las aplicaciones móviles y permite que los usuarios pueden acceder sin problemas a aplicaciones HDX. Cuando se configura la autenticación con certificados de cliente, el usuario introduce su PIN de Worx para acceder con inicio de sesión único (Single Sign-on) a las aplicaciones habilitadas para Worx. El PIN de Worx también simplifica la experiencia de autenticación del usuario. El PIN de Worx se usa para proteger la seguridad de un certificado de cliente o para guardar las credenciales de Active Directory localmente en el dispositivo.

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. El servidor XenMobile no respalda el uso de certificados con la extensión .pem. Use el comando openssl para generar un archivo PFX desde un 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.

En el entorno de XenMobile, una combinación de certificado de cliente y autenticación LDAP es la mejor solución para la seguridad y la experiencia de usuario, al combinar las mejores capacidades de Single Sign-on con un nivel de seguridad de autenticación de dos factores en NetScaler. Al usar certificados de cliente y LDAP conjuntamente, la seguridad se basa en algo que los usuarios conocen (sus contraseñas de Active Directory y en algo que poseen (certificados de cliente en sus dispositivos). WorxMail (y otras aplicaciones Worx) puede configurar y proporcionar automáticamente una experiencia de primer uso perfecta junto con autenticación de certificados de cliente, con un entorno de acceso al servidor Exchange configurado correctamente. Para una experiencia de uso óptima, puede combinar esta opción con el PIN de Worx y el almacenamiento en caché de contraseñas de Active Directory.

La autenticación con certificados del cliente se basa en los atributos del certificado del cliente que se presenta al servidor virtual. Es necesario vincular un certificado raíz al servidor virtual de NetScaler Gateway. Cuando los usuarios inician sesiones en NetScaler Gateway, 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.

Notas:

- La autenticación con certificados del cliente también puede utilizarse con otro tipo de autenticación como, por ejemplo, RADIUS.
- 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.
- WorxMail (y otras aplicaciones Worx) puede configurar y proporcionar automáticamente una experiencia de primer uso perfecta junto con autenticación de certificados de cliente, con un entorno de acceso al servidor Exchange configurado correctamente. Para una experiencia de uso óptima, puede combinar esta opción con el PIN de Worx y el almacenamiento en caché de contraseñas de Active Directory.
- La autenticación de dispositivos con Netscaler Gateway no recibe respaldo para certificados obtenidos a través de una entidad de certificación (CA) discrecional.
- XenMobile no admite la autenticación con certificado de cliente en dispositivos compartidos.

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 de Worx Home en el servidor XenMobile
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* con 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.

El almacén de claves es un archivo que contiene certificados utilizados para firmar las aplicaciones Android. Cuando la validez de una clave caduca, los usuarios ya no pueden actualizar la aplicación a una nueva versión.

Symantec es el proveedor exclusivo de certificados de firma de código para el servicio App Hub de Microsoft. Los desarrolladores y publicadores de software se unen a App Hub para distribuir aplicaciones para Windows Phone y Xbox 360 para descargarlas desde Windows Marketplace. 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 cuál sea el certificado que haya 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

Oct 31, 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 ubicación de almacenamiento de 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.

Esta sección ofrece instrucciones generales para cargar certificados. Para obtener más información acerca de la creación, la carga y la configuración de certificados de cliente, consulte Configuración de la autenticación con certificados del cliente.

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.

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)

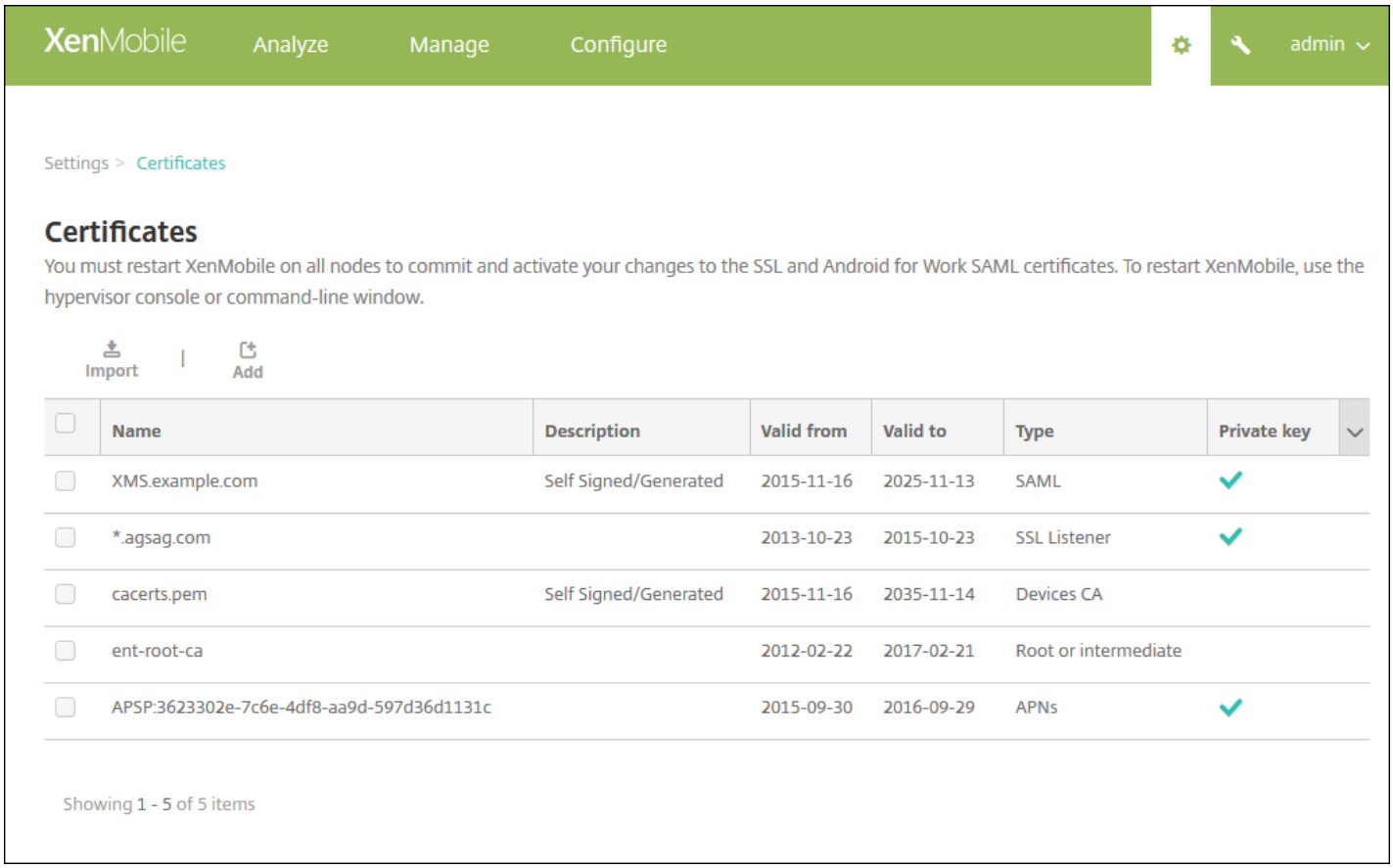
Importante: El servidor XenMobile no respalda el uso de certificados con la extensión .pem. Use el comando openssl para generar un archivo PFX desde un archivo PEM:

```
openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
```

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 el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

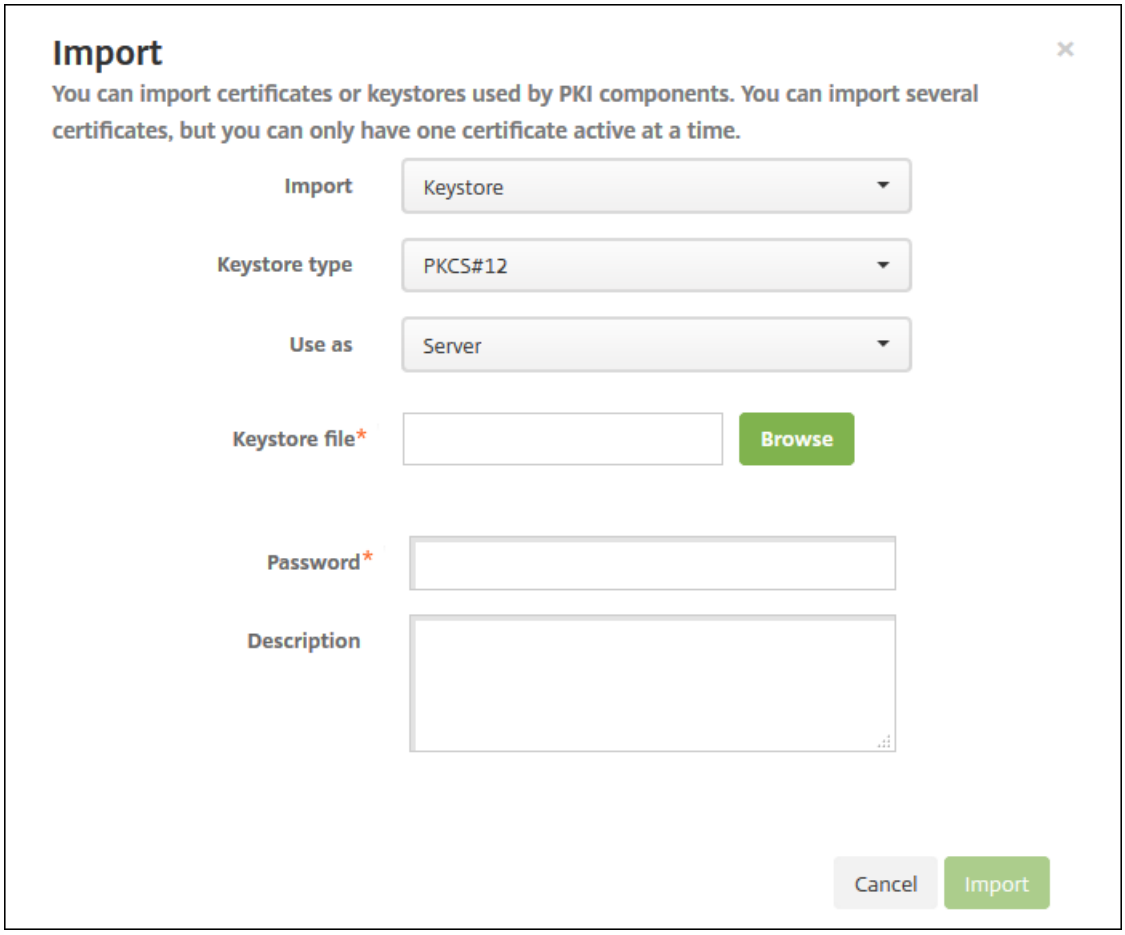
2. Haga clic en **Certificates**. Aparecerá la página **Certificates**.



3. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.

4. Configure los siguientes parámetros:

- **Import**. Seleccione **Keystore** en la lista. El cuadro de diálogo **Import** cambiará para reflejar las opciones de almacén de claves disponibles.



- **Keystore type**: Seleccione **PKCS#12** en la lista.
- **Use as**. En la lista, 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 (APNs) 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.
- **Keystore file**. Seleccione el archivo de almacén de claves que quiere importar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Password**. Escriba la contraseña asignada al certificado.
- **Description**. Si quiere, escriba una descripción del almacén de claves que le ayude a distinguirlo de otros almacenes.

5. 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 el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, haga clic en **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**.

4. El cuadro de diálogo **Import** cambiará para reflejar las opciones de certificado disponibles. 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 que quiere importar.

6. Si quiere, busque el archivo de clave privada 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 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.

La forma más eficaz de actualizar los certificados es la siguiente: en la consola de XenMobile, haga clic en el icono con forma de engranaje, ubicado en la esquina superior derecha, y abra la página Settings; a continuación, haga clic en 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.

Configuración de la autenticación con certificados del cliente

Jul 27, 2016

Para usar la autenticación de certificado de cliente en los modos ENT y MAM de XenMobile, debe configurar el servidor Microsoft, el servidor XenMobile y, a continuación, NetScaler Gateway. En este artículo se describen los siguientes pasos generales.

En el servidor Microsoft:

1. Agregue el complemento de Certificados a la consola MMC (Microsoft Management Console).
2. Agregue la plantilla a la entidad de certificación (CA).
3. Cree un certificado PFX desde el servidor de CA.

En el servidor XenMobile:

1. Cargue el certificado en XenMobile.
2. Cree una entidad PKI para la autenticación basada en certificados.
3. Configure proveedores de credenciales.
4. Configure NetScaler Gateway para entregar un certificado de usuario para la autenticación.

En NetScaler Gateway:

1. Configure NetScaler Gateway para la autenticación con certificados de XenMobile en modo MAM

Requisitos previos

- Para dispositivos Windows Phone 8.1 que usan autenticación de certificados de cliente y descarga SSL, debe inhabilitar la reutilización de sesiones SSL para el puerto 443 en los dos servidores virtuales de equilibrio de carga en NetScaler. Para ello, ejecute el siguiente comando para el puerto 443 en los servidores virtuales:

  set ssl vserver sessReuse DISABLE

  Nota: Si inhabilita la reutilización de sesiones SSL, se inhabilitan algunas de las optimizaciones que NetScaler ofrece, lo que puede ocasionar una disminución del rendimiento en NetScaler.

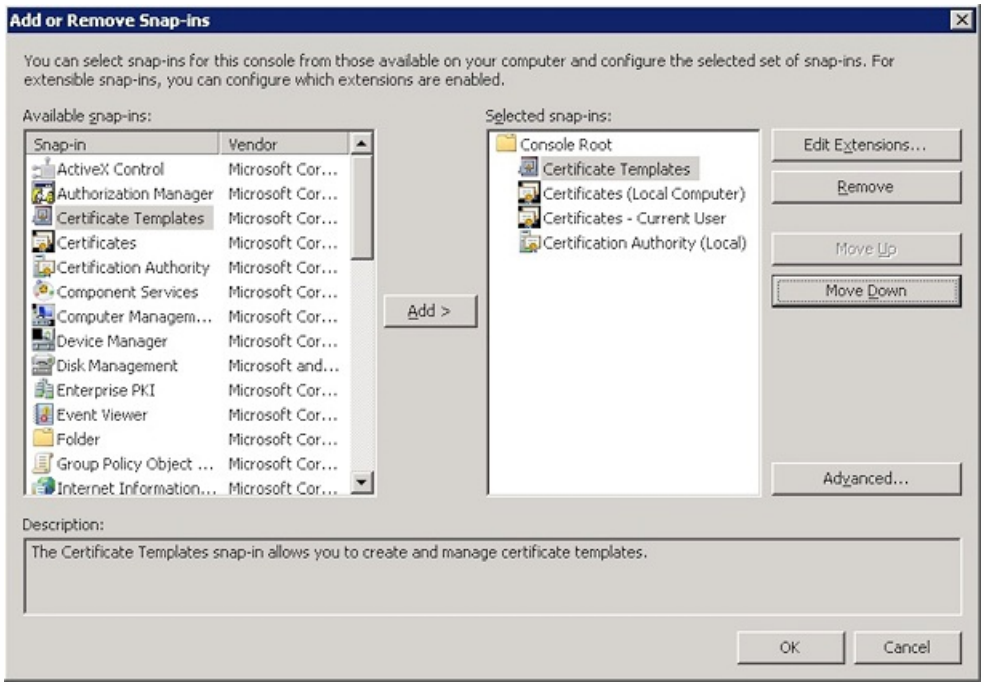
- Para configurar la autenticación basada en certificados para Exchange ActiveSync, consulte este blog de Microsoft.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync hacia el servidor Exchange Server, asegúrese de que los dispositivos móviles tienen todos los certificados raíz e intermedios. De lo contrario, la autenticación basada en certificados fallará durante la configuración de buzones de correo en WorxMail. En la consola IIS de Exchange, debe:
  - Agregar un sitio Web para que XenMobile lo use con Exchange y enlazar el certificado de servidor Web.
  - Usar el puerto 9443.
  - Para ese sitio Web, debe agregar dos aplicaciones, una para "Microsoft-Server-ActiveSync" y otra para "EWS". En ambas aplicaciones, bajo **SSL Settings**, seleccione **Require SSL**.
- Asegúrese de que WorxMail para iOS, Android y Windows Phone está empaquetado con el MDX Toolkit más reciente.

Cómo agregar el complemento de Certificados a la consola MMC (Microsoft Management Console).

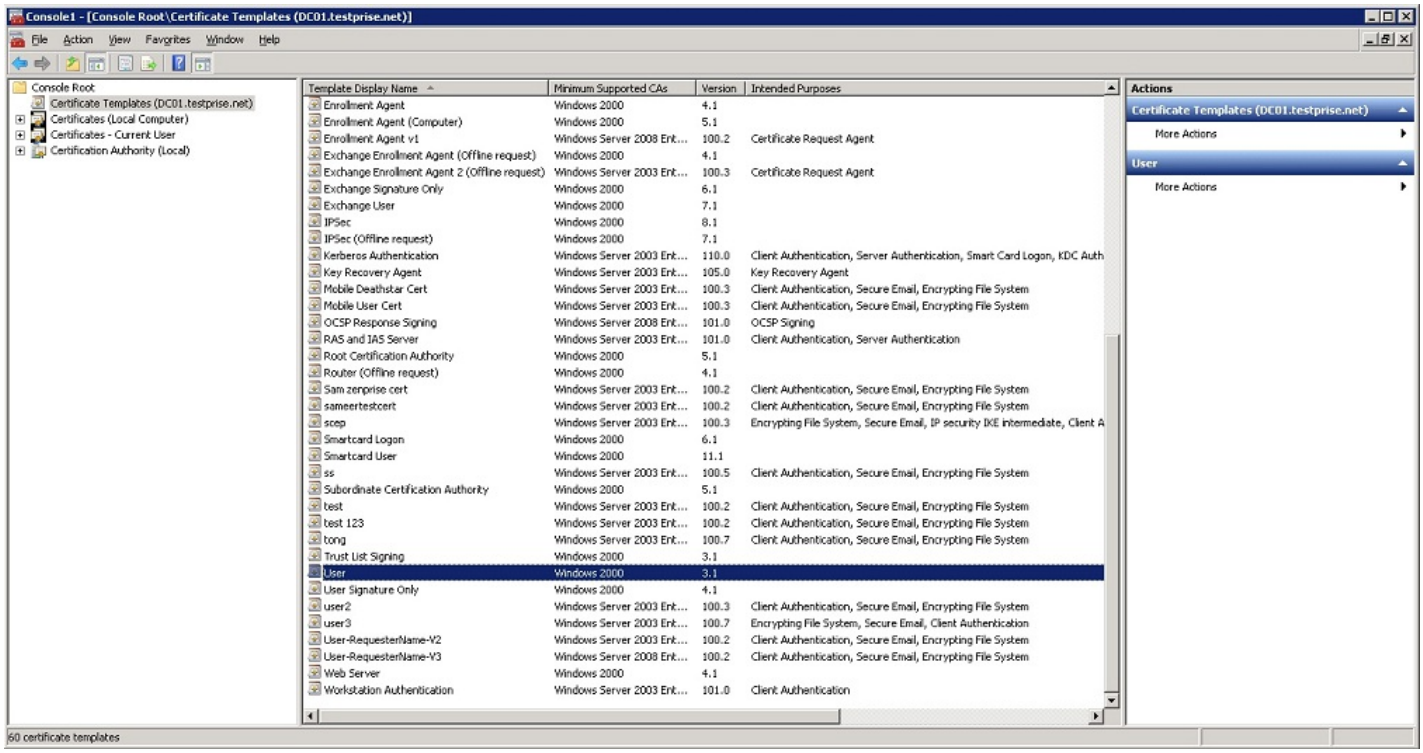
1. Abra la consola MMC y luego haga clic en **Agregar o quitar complemento**.

2. Agregue los complementos siguientes:

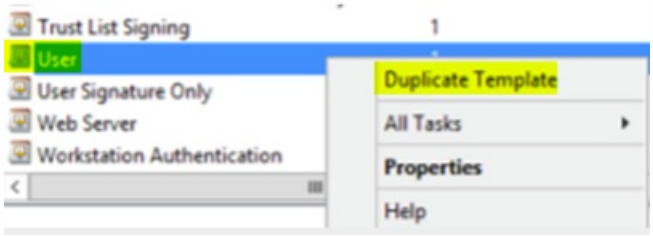
   Plantillas de certificado
   Certificados (Equipo local)
   Certificados (Usuario local)
   Entidad de certificación (Local)



3. Expanda **Plantillas de certificado**.



4. Seleccione la plantilla **Usuario** y **Plantilla duplicada**.

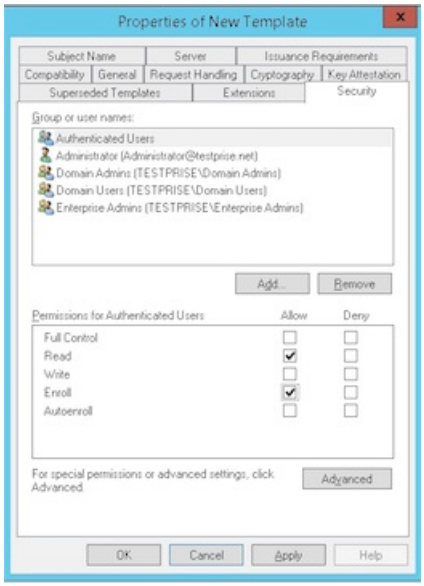


5. Suministre el nombre para mostrar de la plantilla.

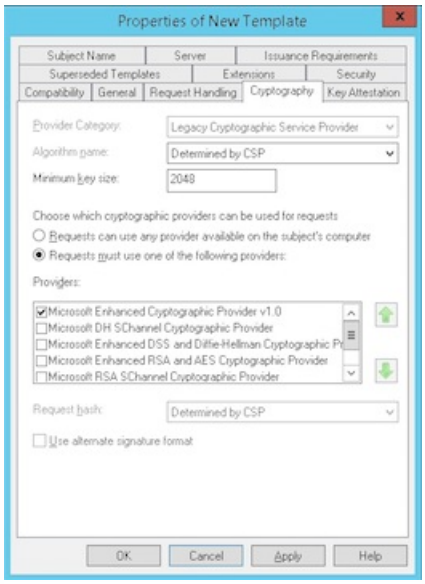
> **Importante:** No marque la casilla **Publicar certificado en Active Directory** a menos que sea necesario. Si se selecciona esta opción, todos los certificado de cliente de los usuarios se insertarán/crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

6. Seleccione **Windows 2003 Server** como tipo de plantilla. En Windows 2012 R2 Server, bajo **Compatibilidad**, seleccione **Entidad de certificación** y como destinatario elija **Windows 2003**.

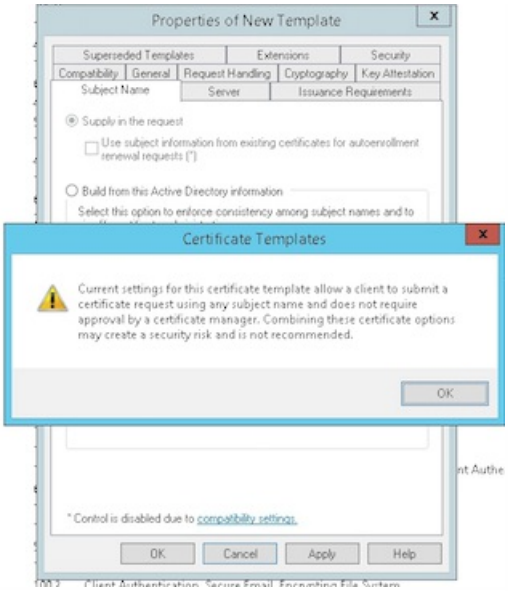
7. En **Seguridad**, seleccione la opción **Inscribir** en la columna **Permitir** para los usuarios autenticados.



8. En **Criptografía**, asegúrese de suministrar el tamaño de la clave, ya que necesitará introducirlo durante la configuración de XenMobile.



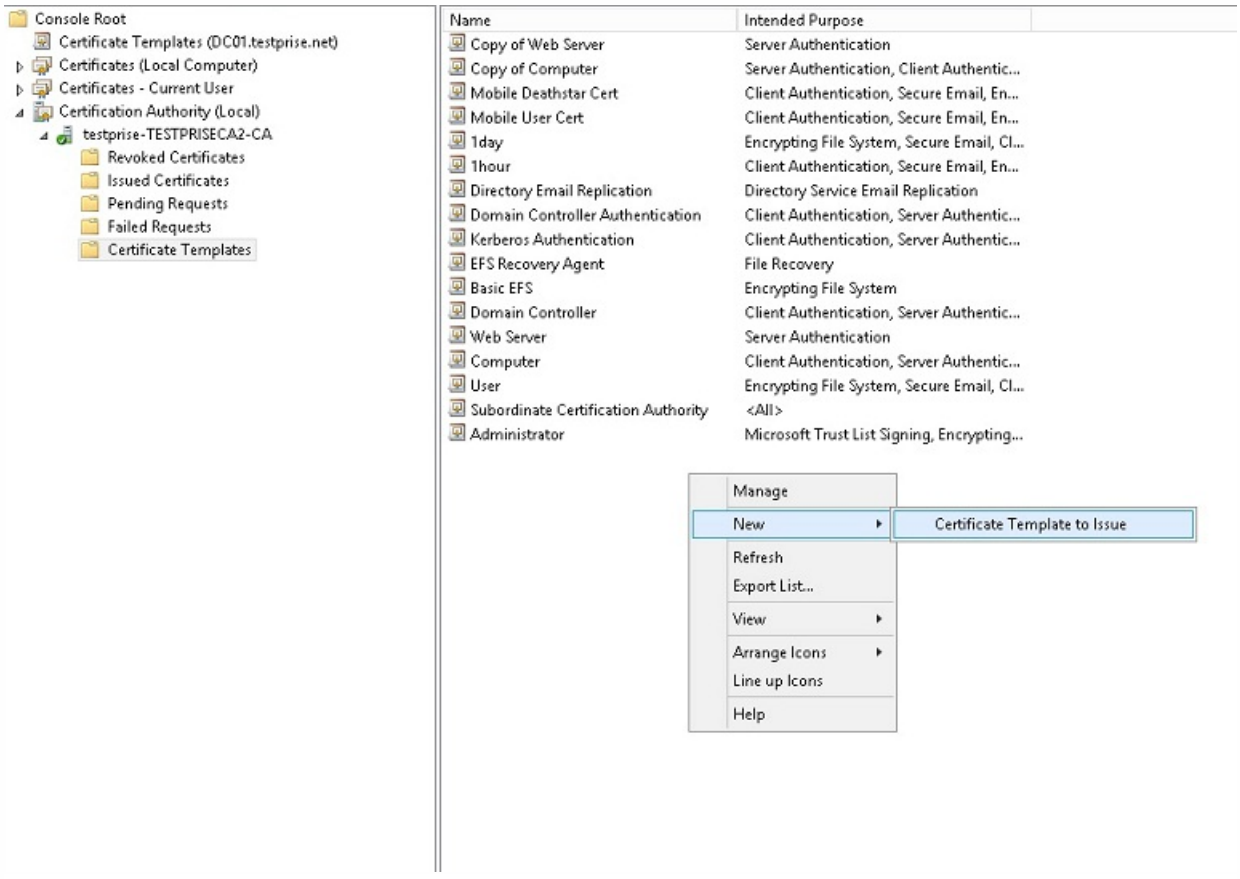
9. En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.



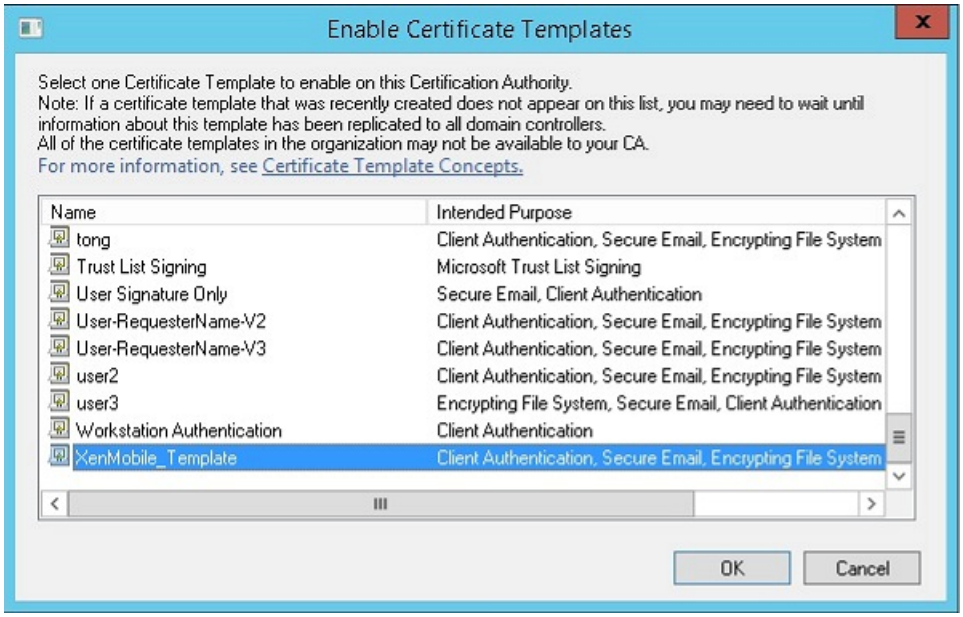
Cómo agregar la plantilla a la entidad de certificación

1. Vaya a **Entidad de certificación** y seleccione **Plantillas de certificado**.

2. Haga clic con el botón secundario en el panel derecho y luego seleccione **Nueva > Plantilla de certificado que se va a emitir**.



3. Seleccione la plantilla que creó en el paso anterior y luego haga clic en **Aceptar** para agregarla a la **Entidad de certificación**.

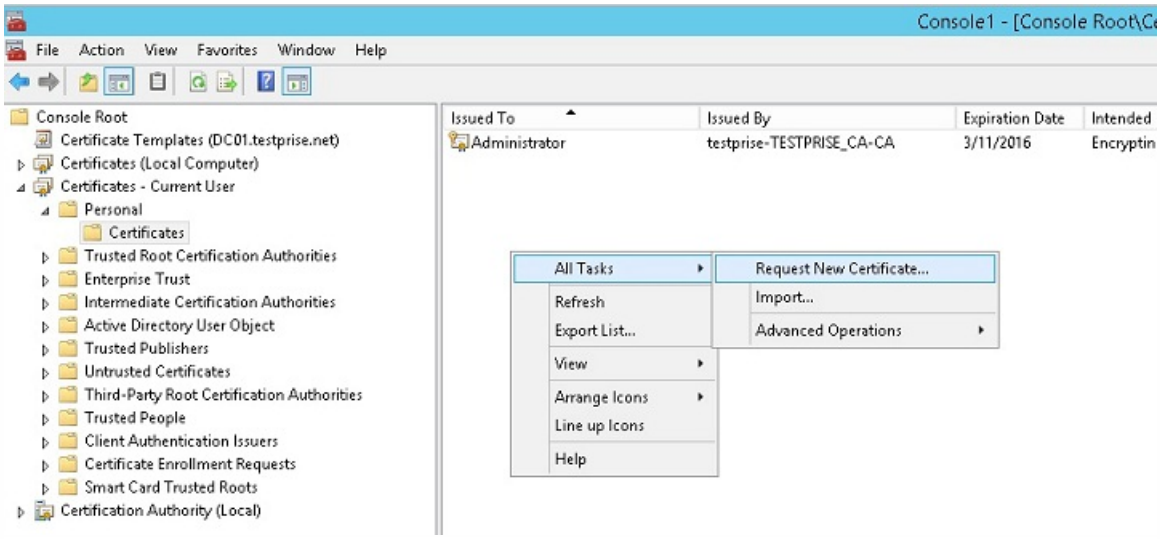


Creación de un certificado PFX desde el servidor de CA

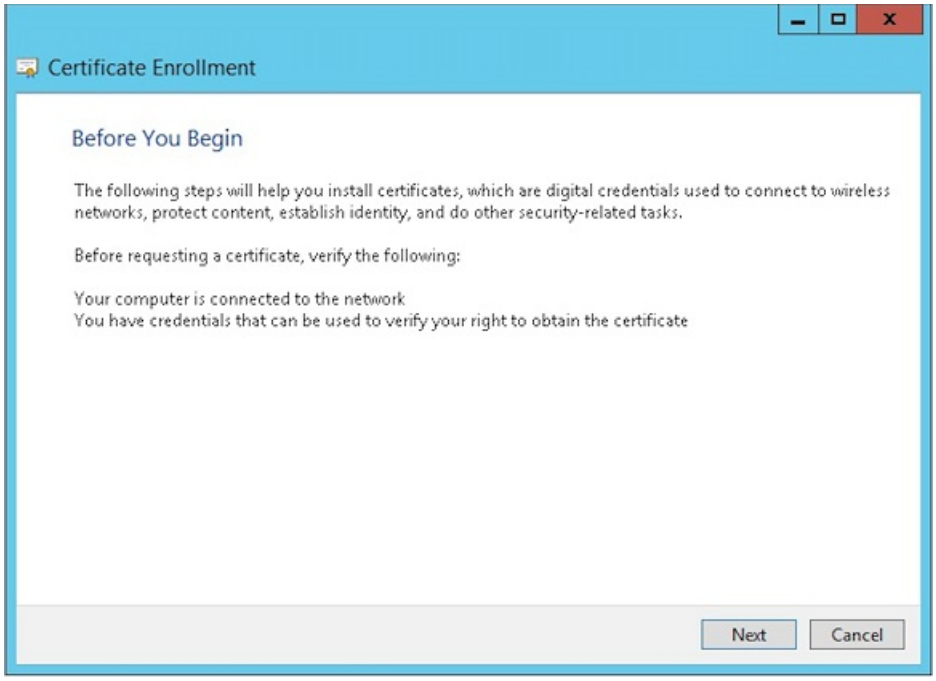
1. Cree un certificado .pfx de usuario usando la cuenta de servicio con la que inició sesión. Este .pfx se cargará en XenMobile, lo que solicitará un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.

2. En **Usuario actual**, expanda **Certificados**.

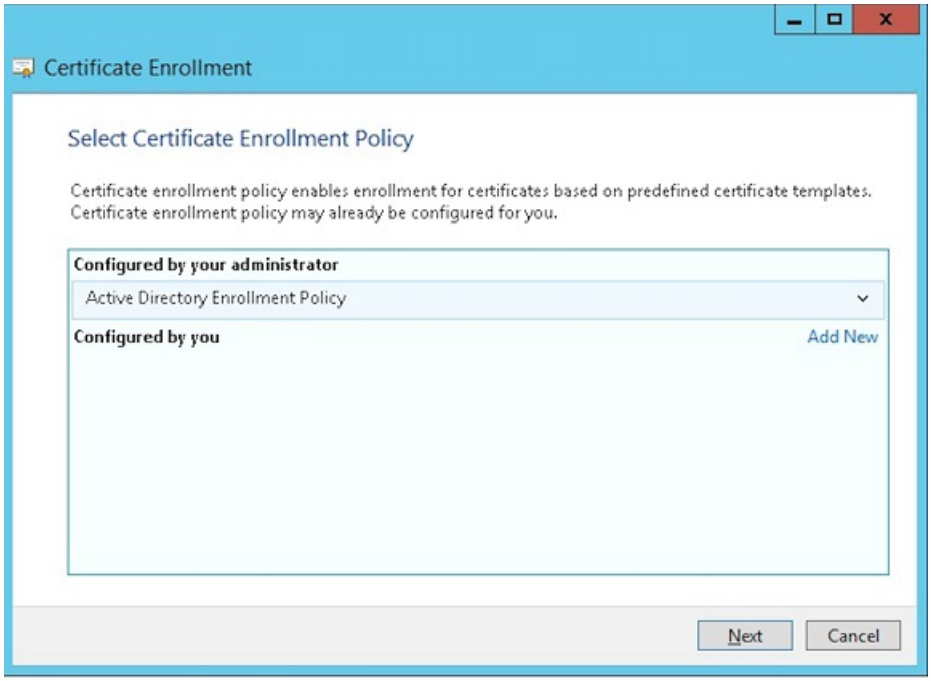
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



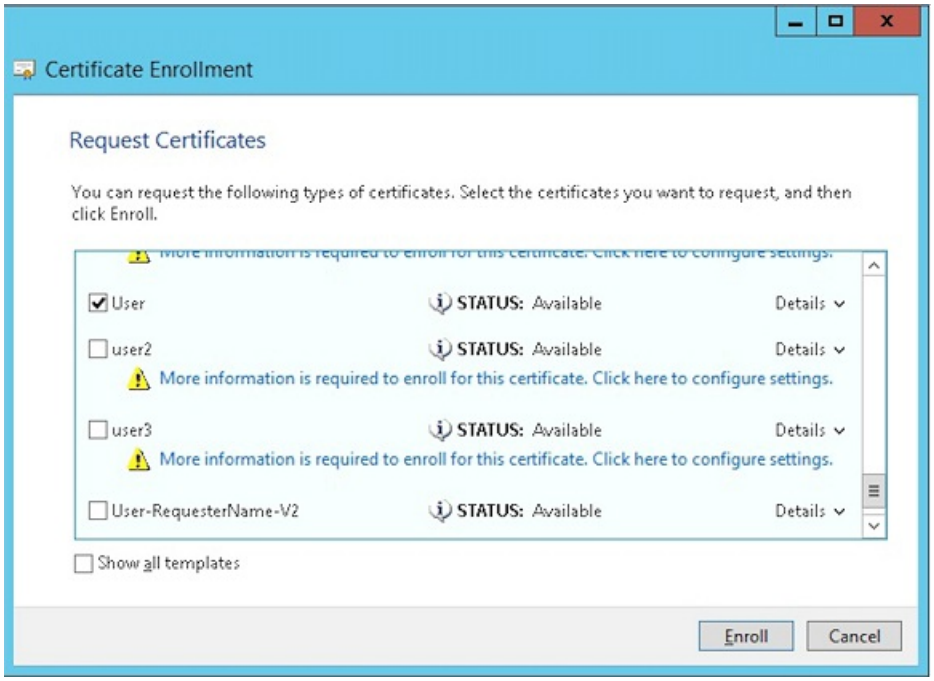
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Next**.



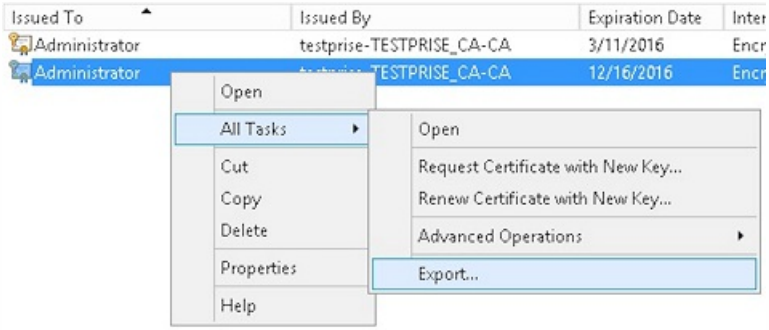
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



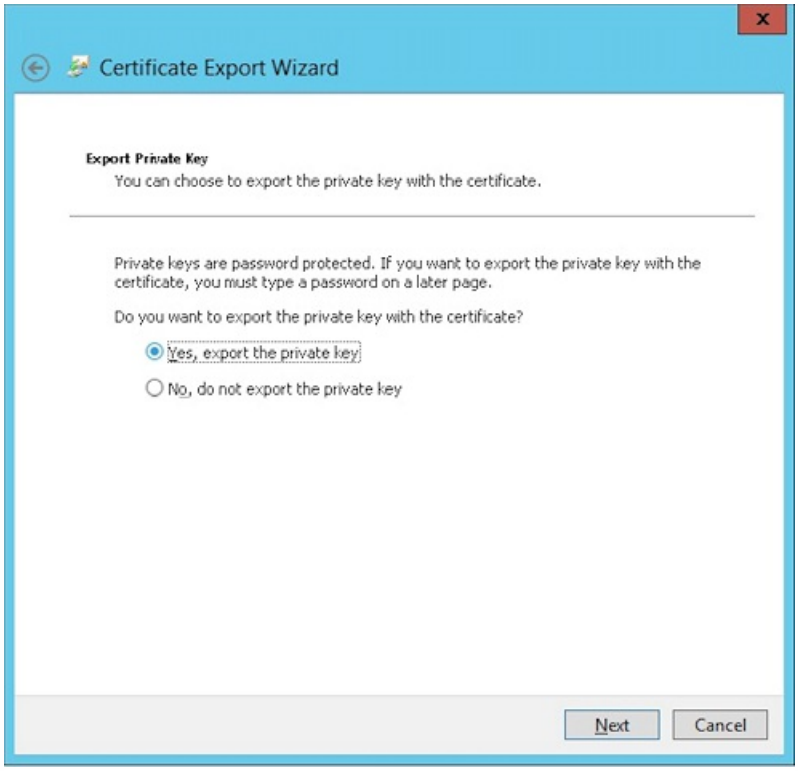
6. Seleccione la plantilla de **Usuario** y haga clic en **Inscribir**.



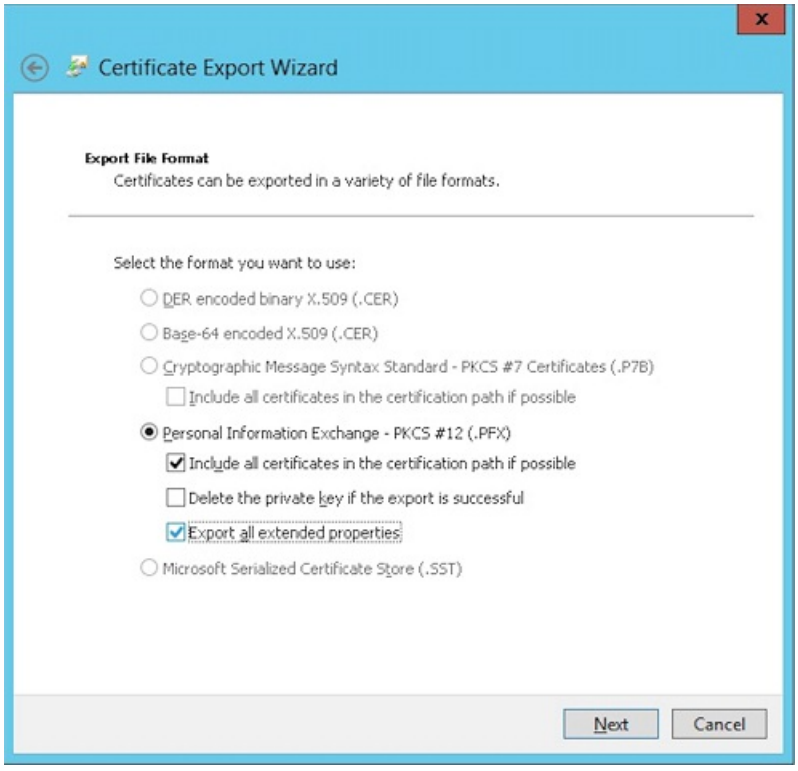
7. Exporte el archivo .pfx que creó en el paso anterior.



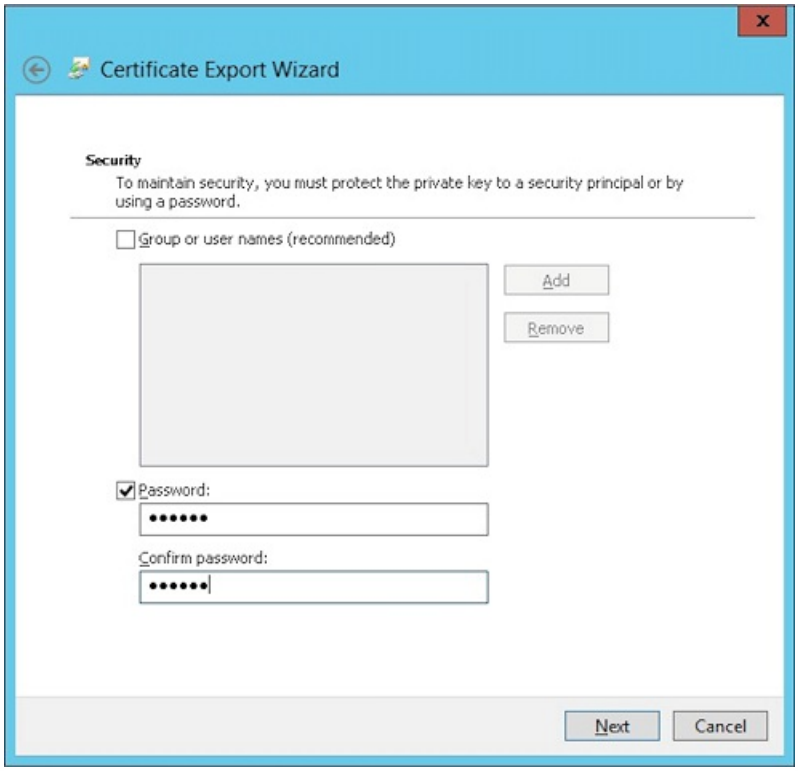
8. Haga clic en **Exportar la clave privada**.



9. Marque las casillas **Si es posible, incluir todos los certificados en la ruta de acceso de certificación** y **Exportar todas las propiedades extendidas**.



10. Defina una contraseña para usarla cuando cargue este certificado en XenMobile.



11. Guarde el certificado en su disco duro.

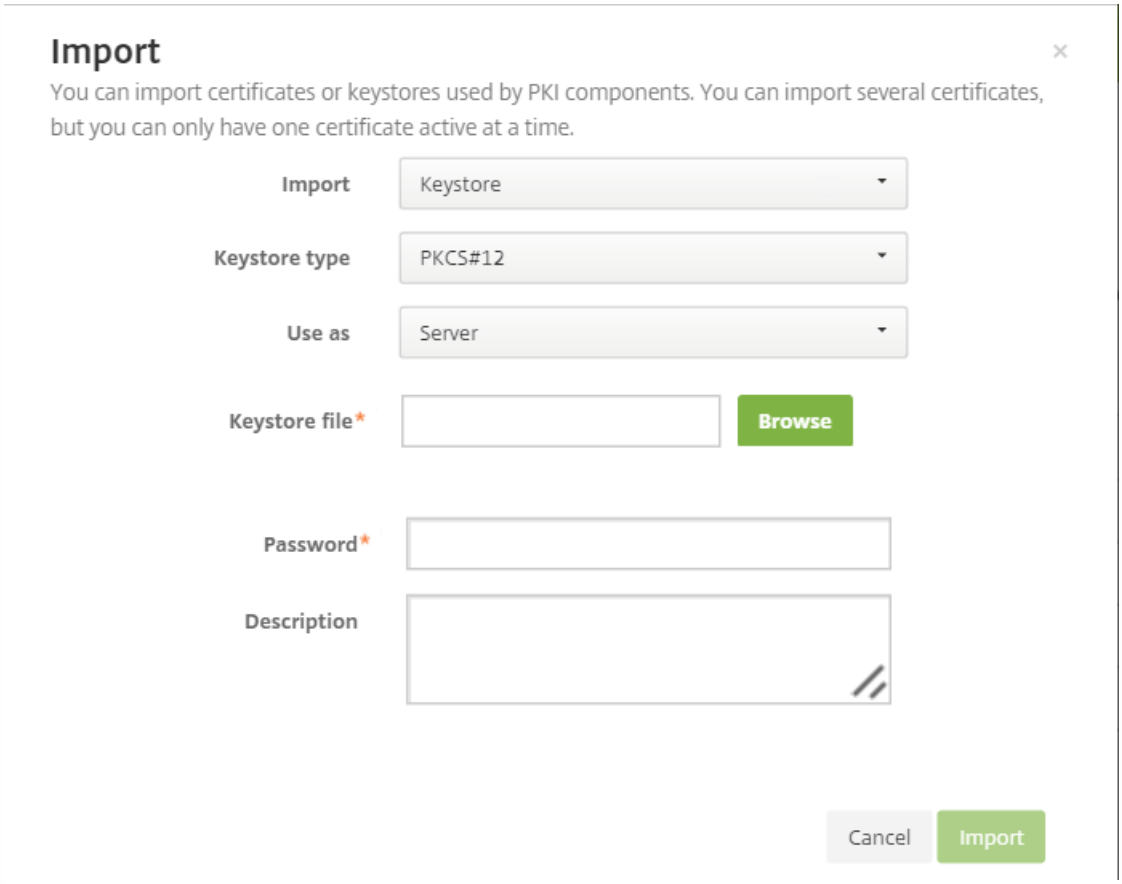
Cómo cargar el certificado en XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Settings**.

2. Haga clic en **Certificates** y después en **Import**.

3. Introduzca los parámetros siguientes:

- **Import**: Keystore
- **Keystore type**: PKCS#12
- **Use as**: Server
- **Keystore file**: Haga clic en Browse para seleccionar el certificado .pfx que acaba de crear.
- **Password**: Introduzca la contraseña que creó para este certificado.



4. Haga clic en **Import**.

5. Verifique que el certificado se instaló correctamente. Debe aparecer como User certificate.

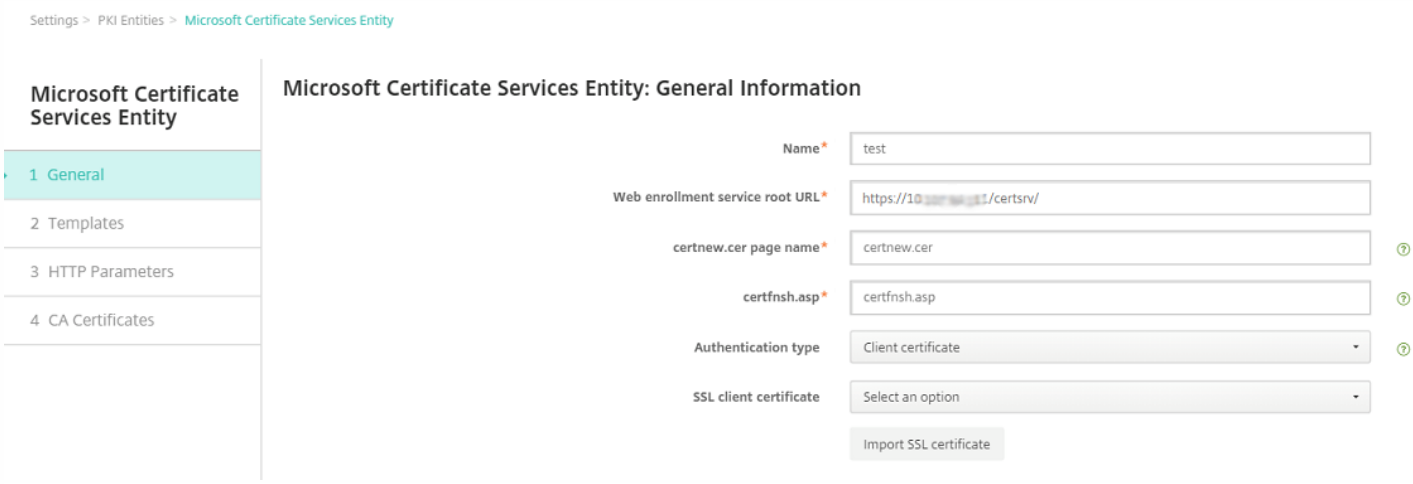
Creación de una entidad PKI para la autenticación basada en certificados

1. En **Settings**, vaya a **More > Certificate Management > PKI Entities**.

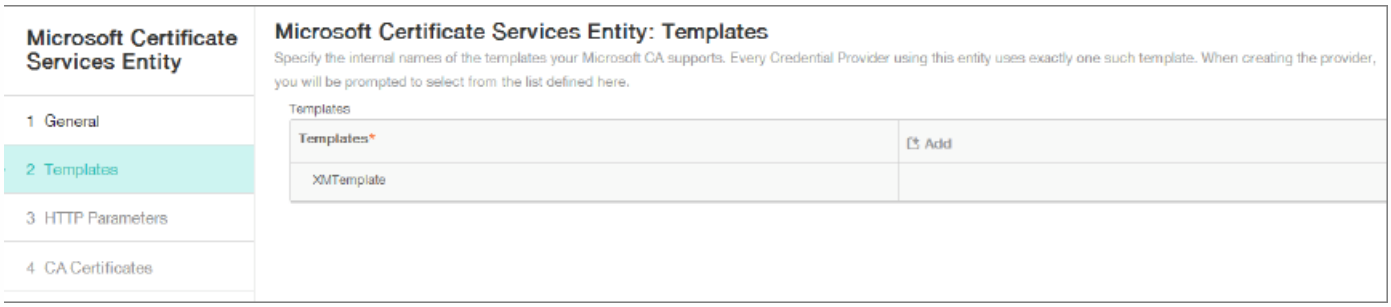
2. Haga clic en **Add** y después haga clic en **Microsoft Certificate Services Entity**. Aparecerá la pantalla **Microsoft Certificate Services Entity: General Information**.

3. Introduzca los parámetros siguientes:

- **Name**: Introduzca algún nombre
- **Web enrollment service root URL**: https://RootCA-URL/certsrv/
  Asegúrese de incluir la barra (/) al final de la ruta URL.
- **certnew.cer page name**: certnew.cer (valor predeterminado)
- **certfnsh.asp**: certfnsh.asp (valor predeterminado)
- **Authentication type**: Certificado de cliente.
- **SSL client certificate**: Seleccione el certificado de usuario que se va a usar para emitir el certificado de cliente de XenMobile.

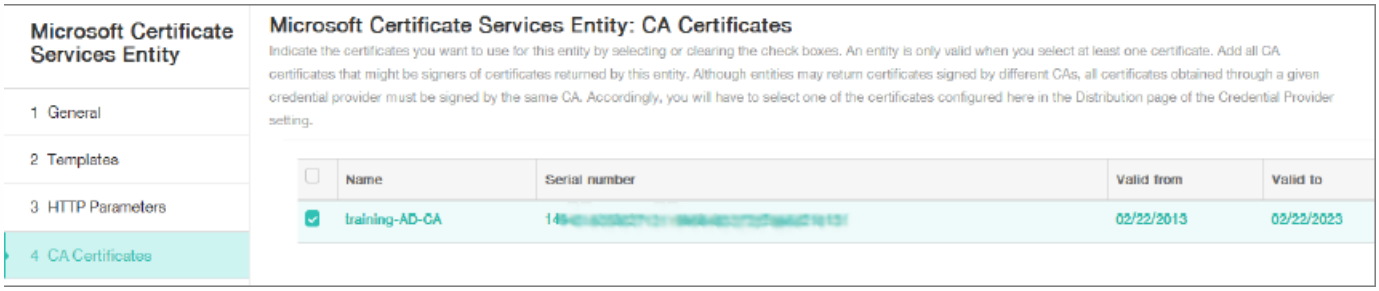


4. Bajo **Templates**, agregue la plantilla que creó cuando configuró el certificado de Microsoft. Asegúrese de no agregar espacios.



5. Omita el paso de HTTP Parameters y haga clic en **CA Certificates**.

6. Seleccione el nombre de la CA raíz que corresponda con su entorno. Esta CA raíz es parte de la cadena importada desde el certificado cliente de XenMobile.



7. Haga clic en **Save**.

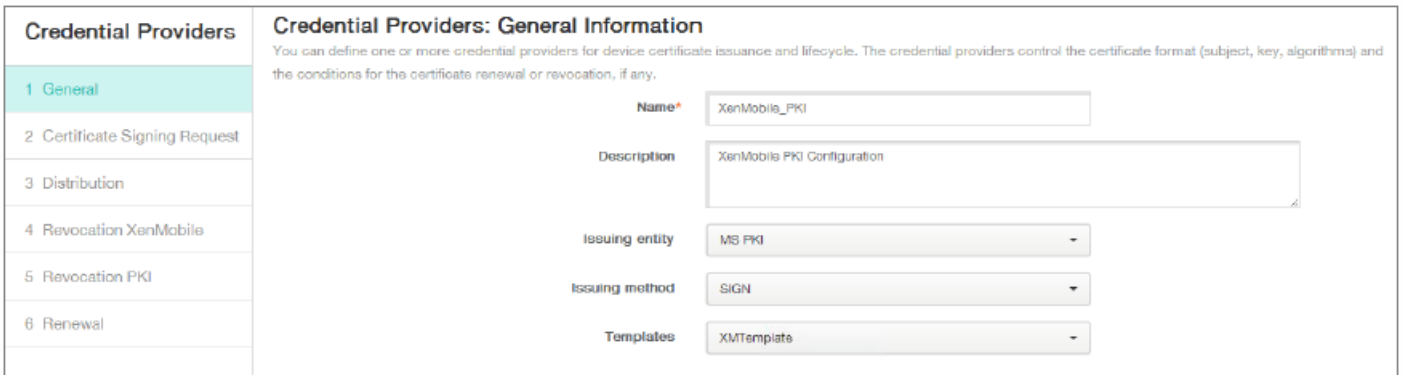
Configuración de proveedores de credenciales

1. En **Settings**, vaya a **More > Certificate Management > Credential Providers**.

2. Haga clic en **Add**.

3. En **General**, introduzca los parámetros siguientes:

- **Name**: Introduzca algún nombre.
- **Description**: Introduzca alguna descripción.
- **Issuing entity**: Seleccione la entidad PKI creada anteriormente.
- **Issuing method**: SIGN
- **Templates**: Seleccione la plantilla agregada bajo la entidad PKI.

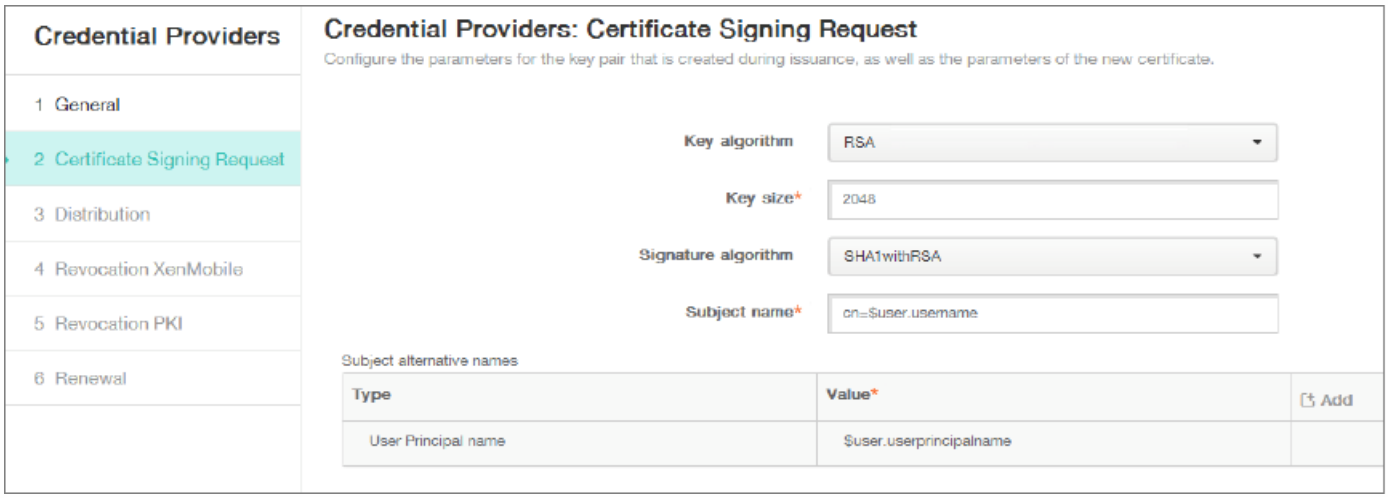


4. Haga clic en **Certificate Signing Request** e introduzca los parámetros siguientes:

- **Key algorithm**: RSA
- **Key size**: 2048
- **Signature algorithm**: SHA1withRSA
- **Subject name**: cn=$user.username

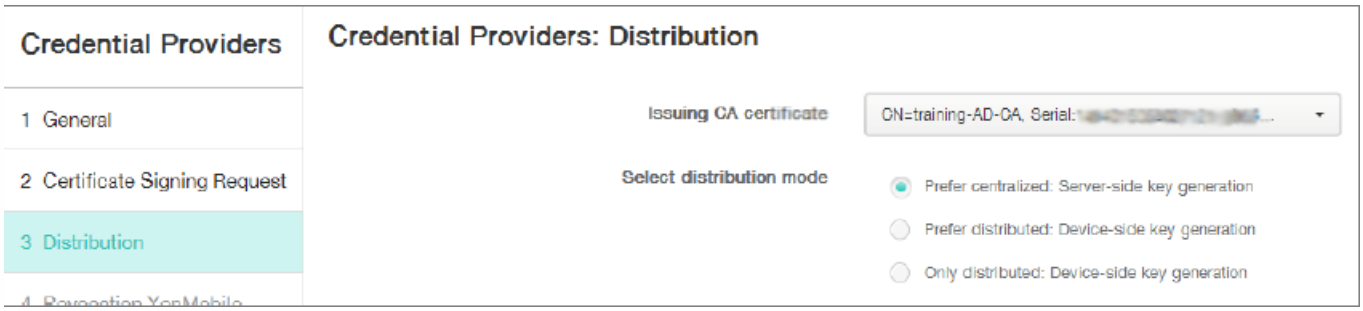
Para **Subject Alternative Names**, haga clic en **Add** y luego introduzca los parámetros siguientes:

- **Type**: User Principal name
- **Value**: $user.userprincipalname



5. Haga clic en **Distribution** e introduzca los parámetros siguientes:

- **Issuing CA certificate**: Seleccione la CA emisora que firmó el certificado del cliente de XenMobile.
- **Select distribution mode**: Seleccione **Prefer centralized: Server-side key generation**.

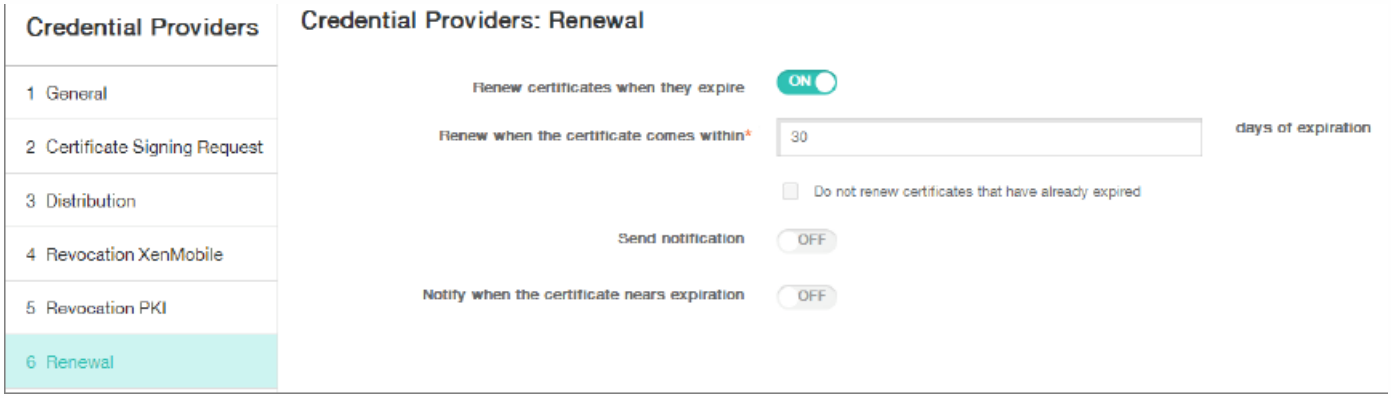


6. Para las dos secciones siguientes—**Revocation XenMobile** y **Revocation PKI**—defina los parámetros como sea necesario. Para el objetivo de este artículo, se omiten ambas opciones.

7. Haga clic en **Renewal**.

8. Para **Renew certificates when they expire**, seleccione **ON**.

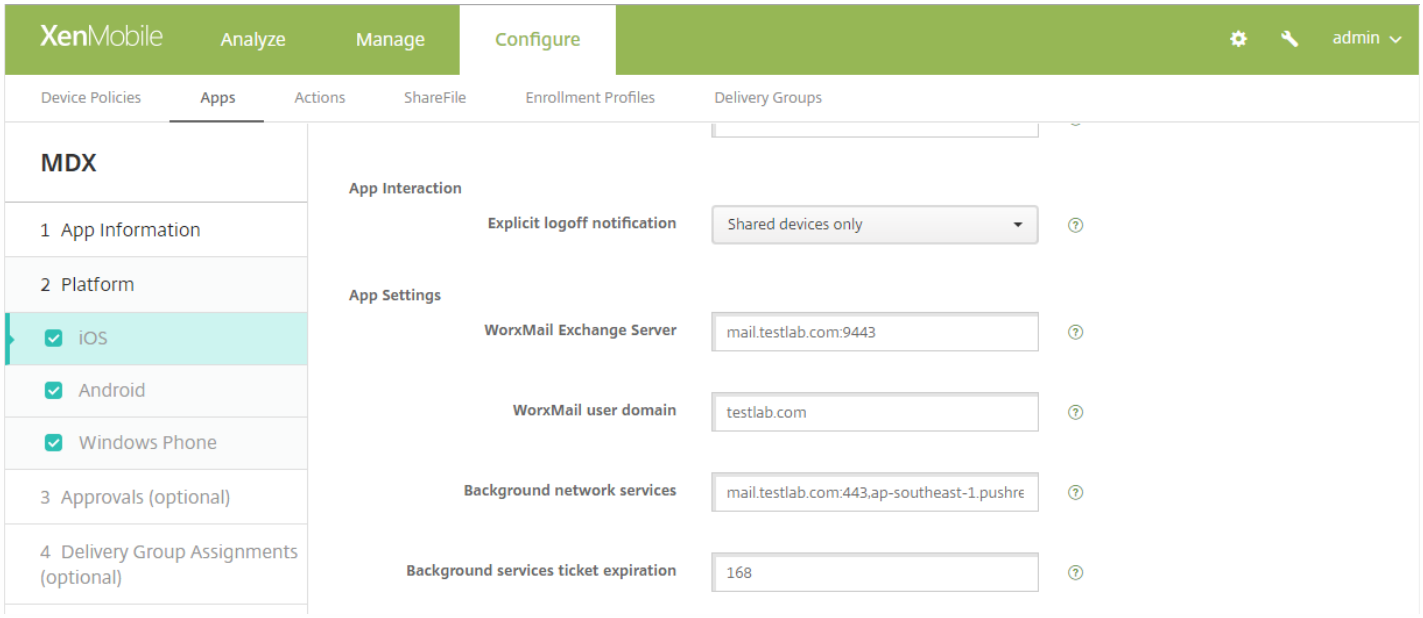
9. Deje todos los demás parámetros con los valores predeterminados o cámbielos si es necesario.



10. Haga clic en **Save**.

Configuración de WorxMail para usar autenticación basada en certificados

Cuando agregue WorxMail a XenMobile, asegúrese de configurar los parámetros de Exchange en **Parámetros de aplicación**.



Configuración de la entrega de certificados de NetScaler en XenMobile

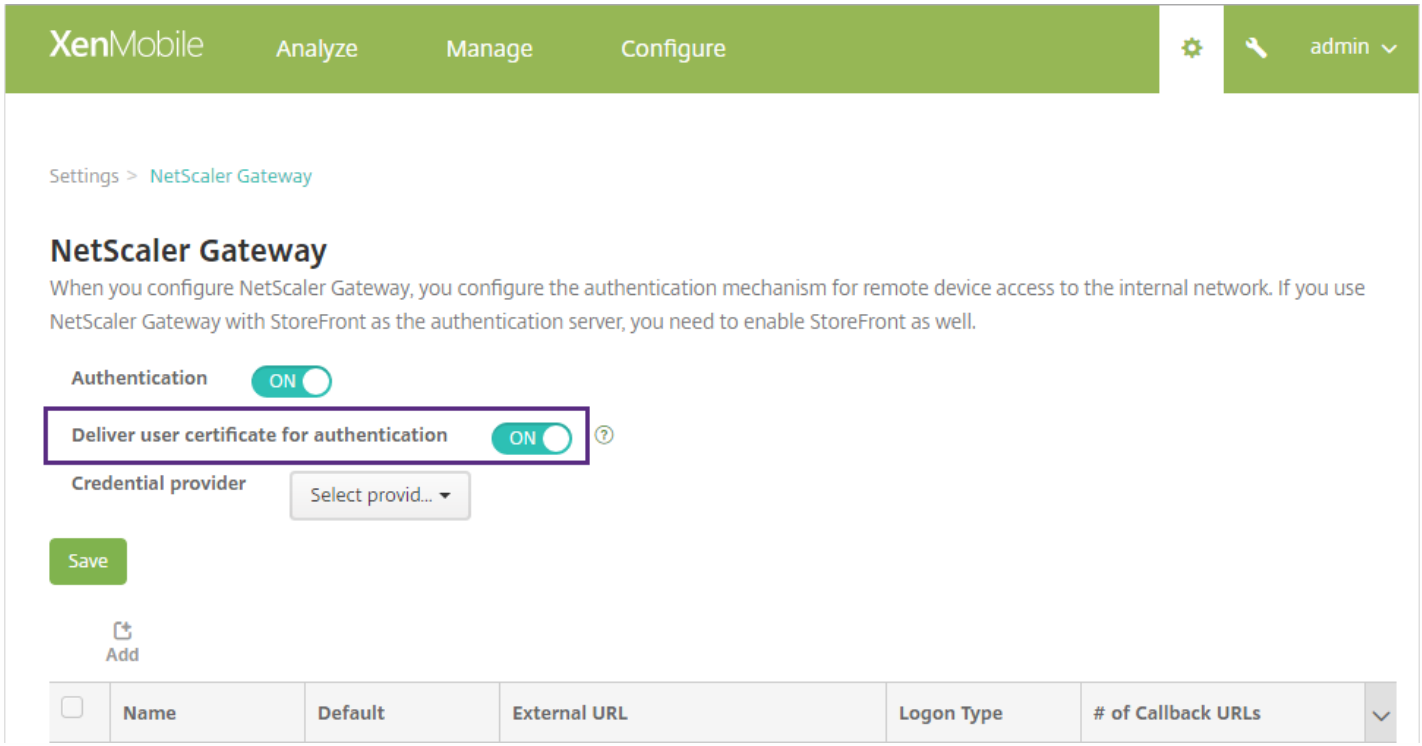
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Settings**.

2. En **Server**, haga clic en **NetScaler Gateway**.

3. Si NetScaler Gateway aún no fue agregado, haga clic en **Add** y especifique los parámetros:

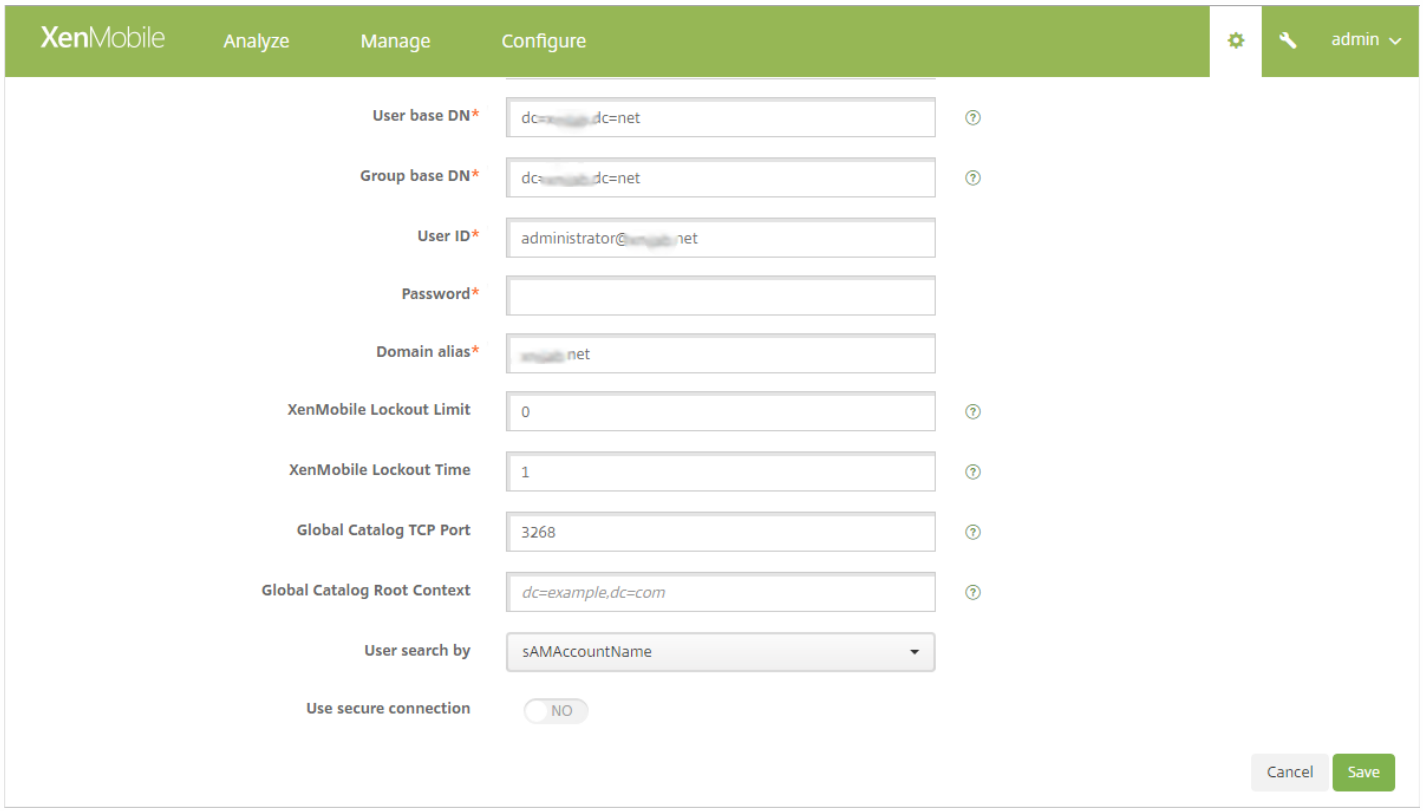
- **External URL**: https://URLdelNetScalerGateway
- **Logon Type**: Certificate
- **Password Required**: OFF
- **Set as Default**: ON

4. Parar **Deliver user certificate for authentication**, seleccione **On**.



5. Para **Credential Provider**, seleccione un proveedor y haga clic en **Save**.

6. Si va a usar atributos de sAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el conector de LDAP en XenMobile, de este modo: vaya **Settings > LDAP**, seleccione el directorio y haga clic en **Edit**, y seleccione **sAMAccountName** en **User search by**.



Creación de una directiva Enterprise Hub para Windows Phone 8.1

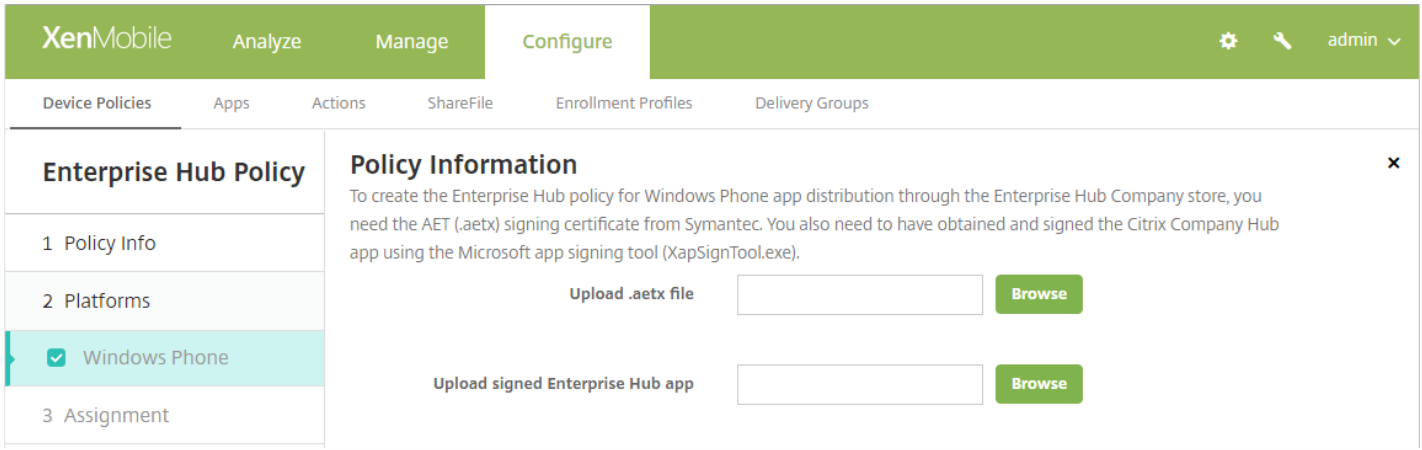
Para dispositivos Windows Phone 8.1, es necesario crear una directiva Enterprise Hub para distribuir el archivo AETX y el cliente Worx Home.

> **Nota**
>
> Asegúrese de que ambos archivos, AETX y Worx Home, utilicen el mismo certificado de empresa del proveedor de certificados y el mismo ID de publicador de la cuenta de desarrollador de Tienda Windows.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.

2. Haga clic en **Add** y, a continuación, bajo **More > XenMobile Agent**, haga clic en **Enterprise Hub**.

3. Después de dar un nombre a la directiva, seleccione el archivo .AETX correcto y la aplicación Worx Home firmada para Enterprise Hub.



4. Asigne la directiva a grupos de entrega y guárdela.

Con el asistente de NetScaler para XenMobile, configure NetScaler Gateway para la autenticación con certificados

> **Nota**
>
> Puede ejecutar el asistente de NetScaler para XenMobile solamente una vez. Si ya usó el asistente, siga las instrucciones indicadas

en "Para configurar NetScaler Gateway para la autenticación con certificados", a continuación.

Siga estos pasos en el dispositivo NetScaler para configurar la autenticación con certificados en XenMobile.

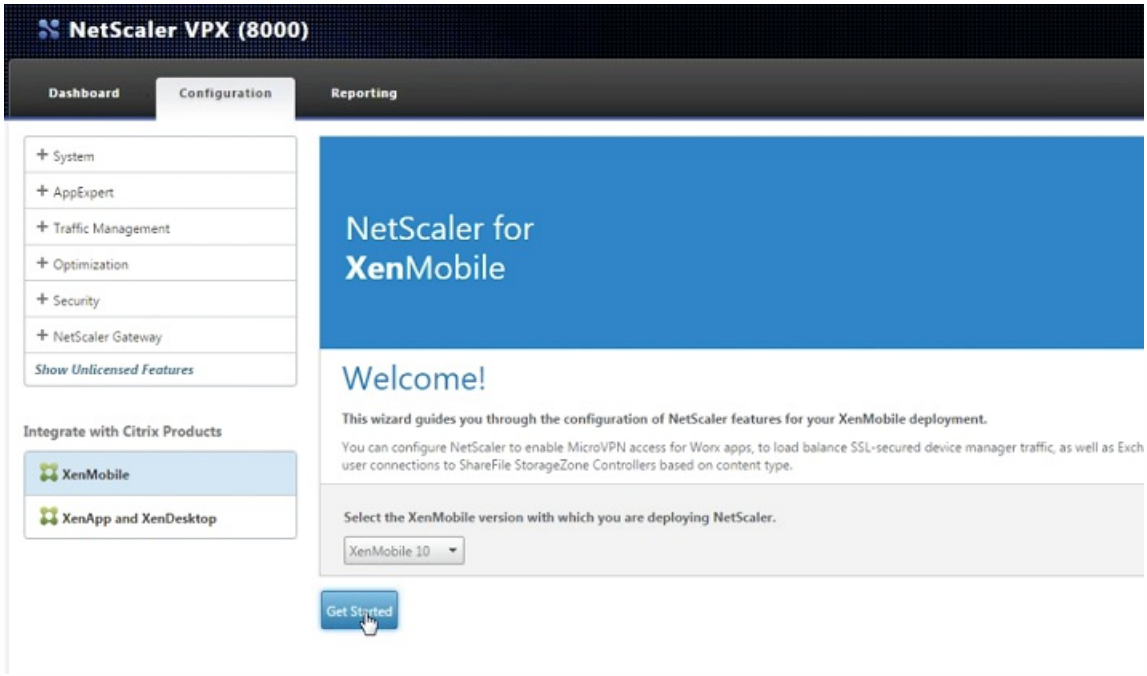
1. Inicie sesión en NetScaler.

2. Para ello, en **Configuration**, vaya a **Integrate with Citrix Products** y, a continuación, seleccione **XenMobile**.

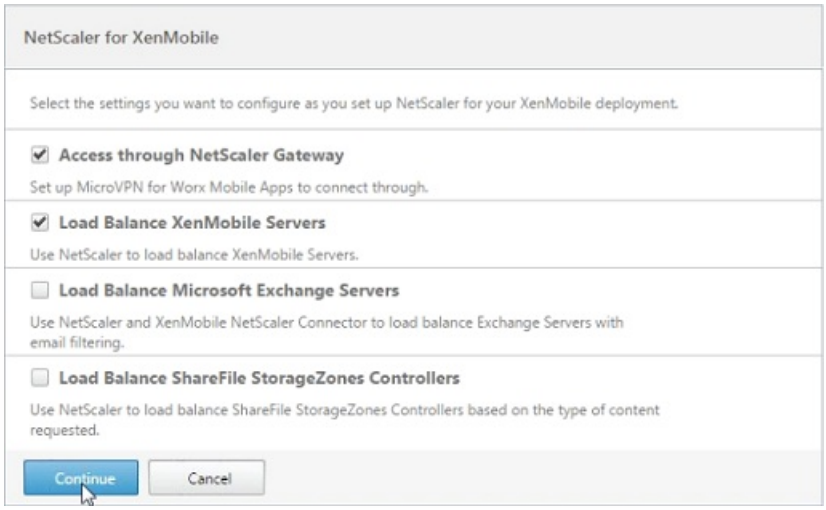
Se abrirá un asistente para configurar las funcionalidades de NetScaler para la implementación de XenMobile.

3. Elija **XenMobile 10**.

4. Haga clic en **Get Started**.



5. En la pantalla siguiente, seleccione **Access through NetScaler Gateway** (para los modos ENT y MAM) y **Load Balance XenMobile Servers**, y luego haga clic en **Continue**.



6. En la siguiente pantalla, escriba la dirección IP de NetScaler Gateway externa y, a continuación, haga clic en **Continue**.

Aparecerá la pantalla Server Certificate de NetScaler Gateway.

7. Debe usar un certificado existente o instalar uno. Haga clic en **Continuar**.

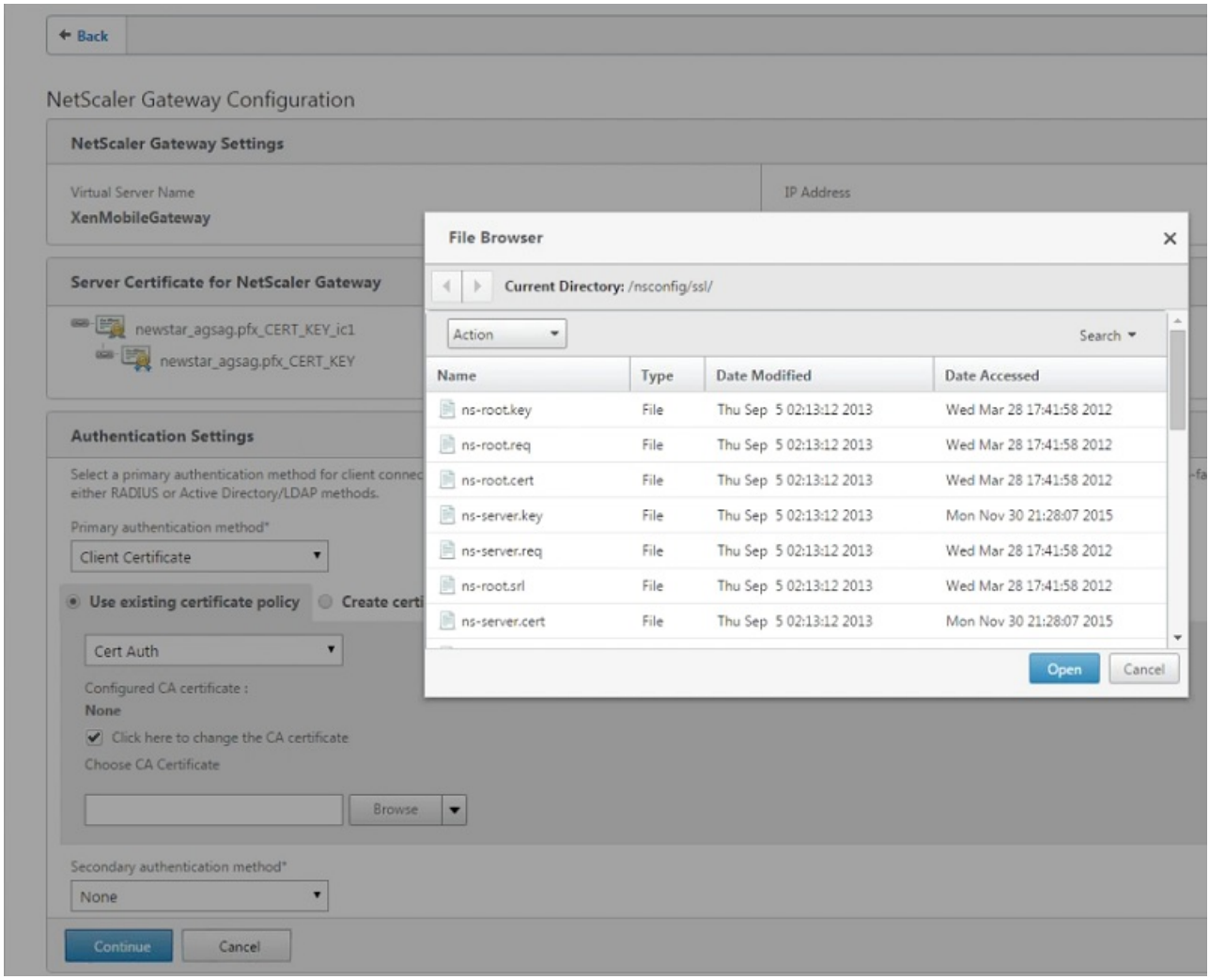
Aparecerá la pantalla **Authentication Settings**.

8. En el campo **Primary authentication method**, seleccione **Client Certificate**.

Esto seleccionará automáticamente **Use existing certificate policy** y **Cert Auth** en los siguientes dos campos. El siguiente procedimiento presupone que ya dispone de una directiva de certificados.

Si desea crear una directiva de certificados, haga clic en **Create certificate policy** y complete la configuración. En la pantalla **XenMobile Server Certificate**, seleccione un certificado de servidor existente o instale uno nuevo. Si ejecuta varios servidores de XenMobile, debe agregar un certificado para cada uno. En **Server Logon Name Attribute** especifique **userPrincipalName** o **samAccountName.**

9. Seleccione **Click here to change the CA certificate** y luego, en la lista **Browse**, vaya al certificado de CA que desee.



10. Mantenga **Second authentication method** como **None** y, a continuación, haga clic en **Continue**.

11. En la pantalla **Device certificate**, si el certificado aún no está instalado, debe exportar este certificado desde la consola de XenMobile. Para ello:

a. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola para abrir la pantalla **Settings**.

b. Haga clic en **Certificate** y, a continuación, seleccione el certificado de CA en la lista.

c. Haga clic en **Export**.

d. Vuelva al asistente de NetScaler y seleccione el certificado que ha exportado (descargado) para instalarlo.

e. Haga clic en **Continuar**.

Aparecerán las direcciones IP del servidor XenMobile que ha configurado.

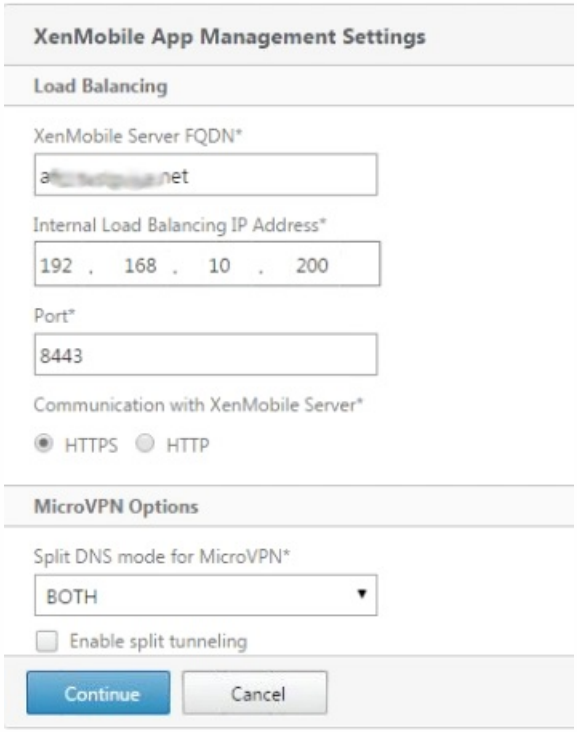
12. En la pantalla **Load Balancing**, especifique el nombre de dominio completo del servidor XenMobile y una dirección IP de equilibrio de carga interna de solo MAM.

13. Puesto que se trata de una implementación de descarga SSL (SSL offload), seleccione **HTTP** en **Communication with**

XenMobile Server.

El campo **Split DNS mode for MicroVPN** aparecerá como **BOTH**.

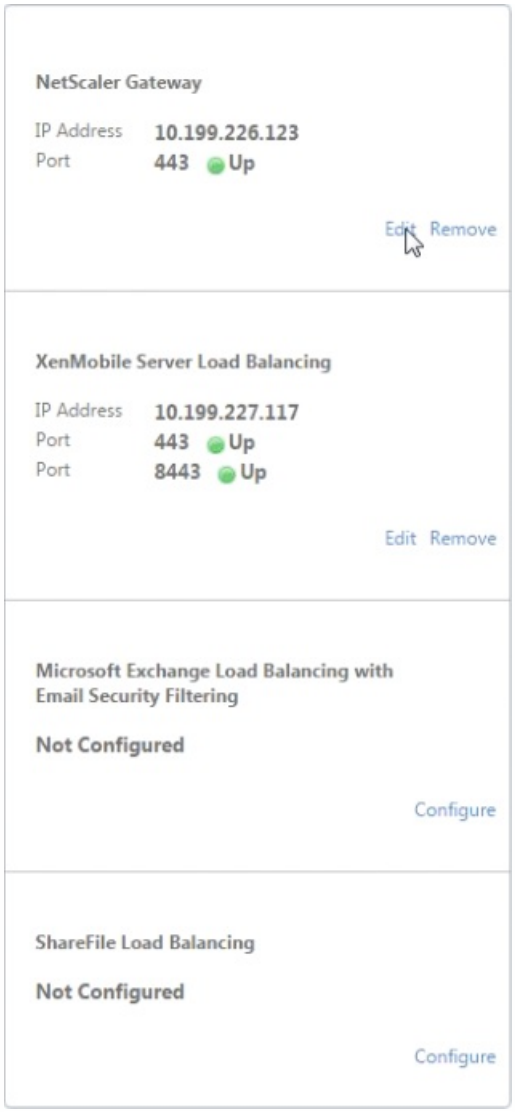
14. Haga clic en **Continue**.



Aparecerán las direcciones IP del servidor XenMobile que ha configurado.

15. Haga clic en **Continue**.

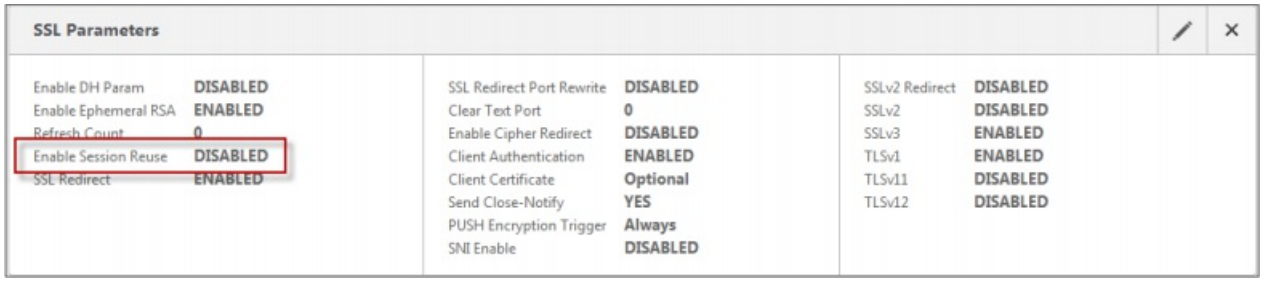
En el panel de mandos de NetScaler, confirme que el equilibrio de carga de XenMobile y NetScaler Gateway está configurado de este modo:



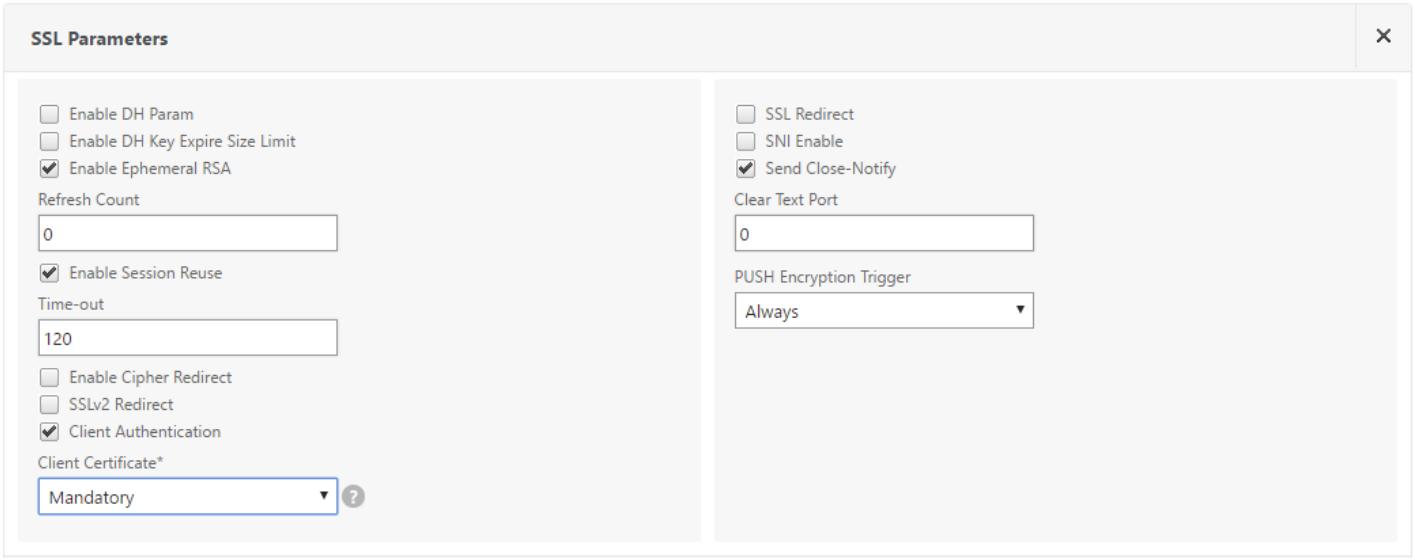
16. Si va a usar atributos de sAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el perfil de certificado como se describe en la sección siguiente.

Configuración manual de NetScaler Gateway para la autenticación con certificados

1. En **Traffic Management > Load Balancing > Virtual Servers**, vaya a cada servidor virtual (ambos 443 y 8443), actualice los parámetros en **SSL Parameters**, y defina **Enable Session Reuse** como **DISABLED**.



2. En el servidor virtual de NetScaler Gateway, en **Enable Client Authentication -> Client Certificate**, seleccione **Client Authentication** y, en **Client Certificate**, seleccione **Mandatory**.



3. Cree una nueva directiva de certificado para la autenticación de forma que XenMobile pueda extraer el **User Principal Name** o el **sAMAccount** del certificado del cliente suministrado por Worx Home a NetScaler Gateway.

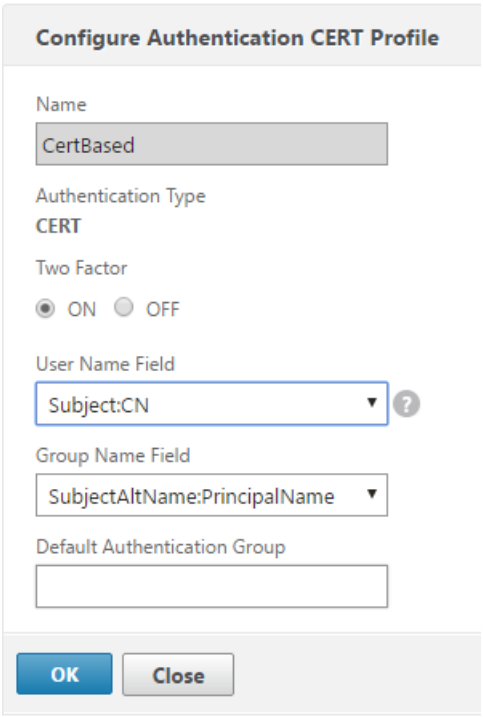
4. Configure los siguientes parámetros para el perfil de certificado:

Authentication Type: **CERT**

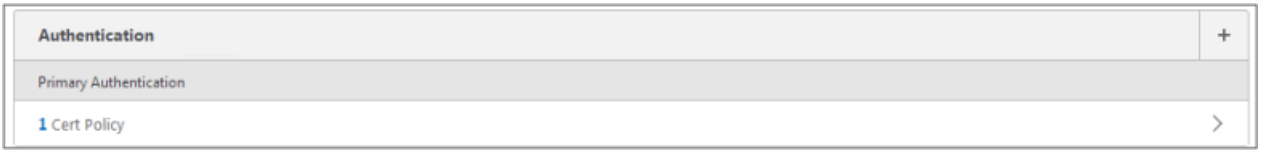
Two Factor: **ON** o **OFF**

User Name Field: **Subject:CN**

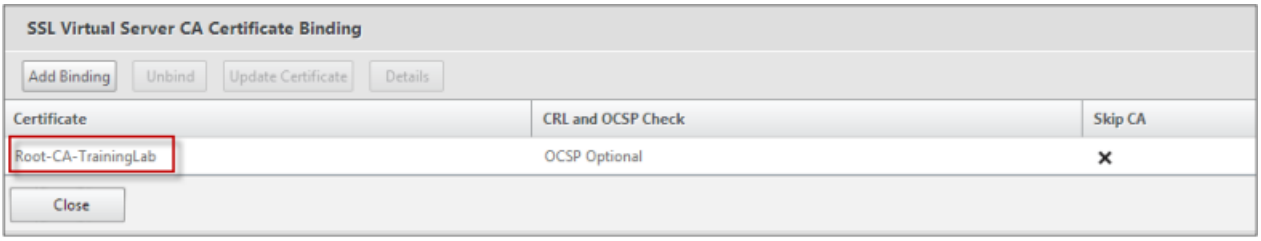
Group Name Field: **SubjectAltName:PrincipalName**

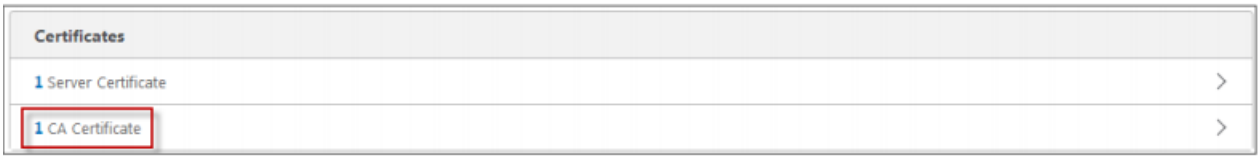


5. Vincule solo la directiva de autenticación con certificados como **Primary Authentication** en el servidor virtual de NetScaler Gateway.



6. Vincule el certificado de CA raíz para validar la confianza del certificado de cliente presentado a NetScaler Gateway.





Solución de problemas de la configuración de certificado de cliente

Después de la configuración, el flujo de trabajo de usuarios es el siguiente:

1. Los usuarios inscriben sus dispositivos móviles.

2. XenMobile solicita a los usuarios que creen un PIN de Worx.

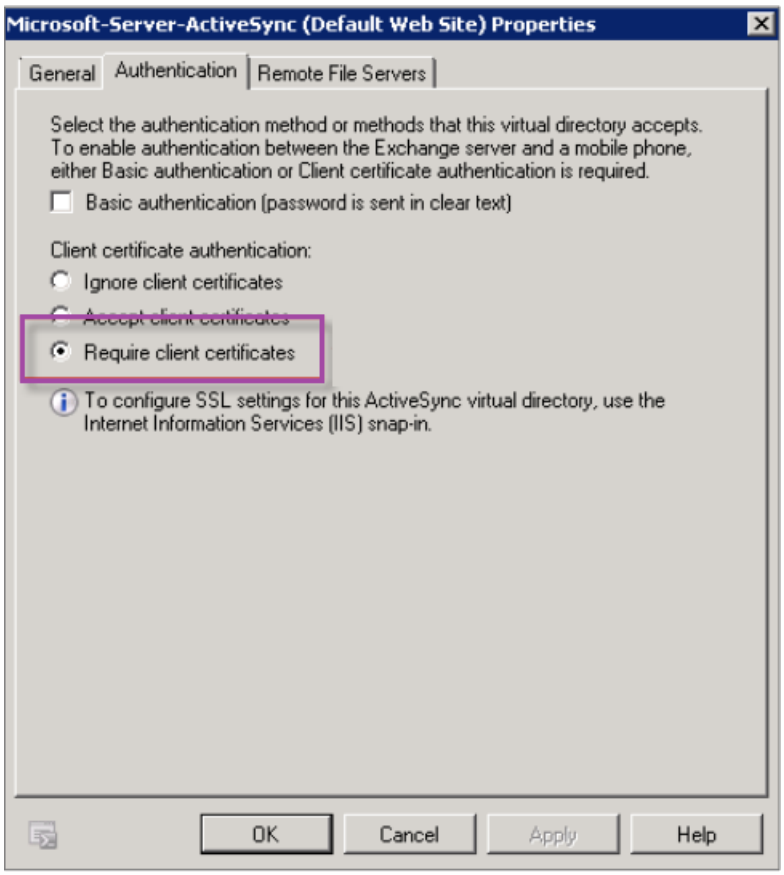
3. Los usuarios, a continuación, son dirigidos a Worx Store.

4. Cuando los usuarios ejecutan WorxMail para iOS, Android y Windows Phone 8.1, XenMobile no les pedirá credenciales de usuario para configurar su buzón. En su lugar, WorxMail solicita el certificado de cliente desde Worx Home y lo envía a Microsoft Exchange Server para la autenticación. Si XenMobile pide credenciales cuando los usuarios inician WorxMail, verifique si ha configurado todo correctamente.

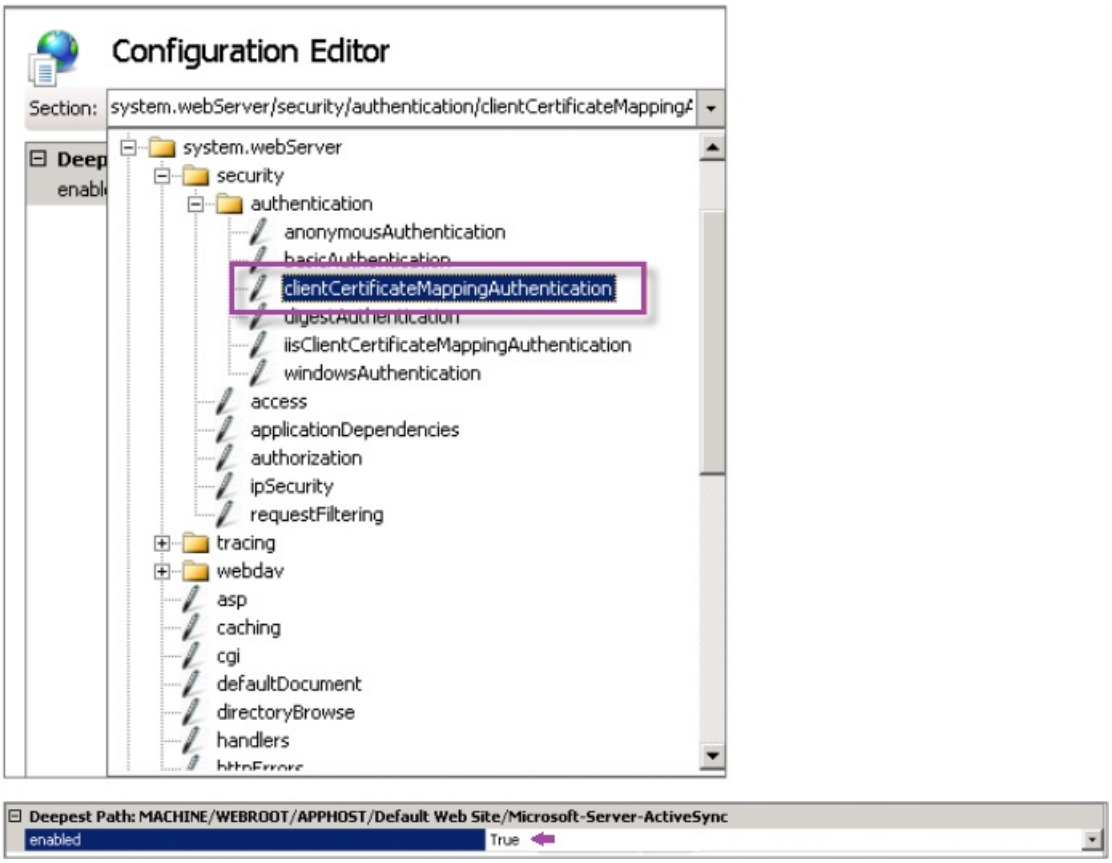
Si los usuarios pueden descargar e instalar WorxMail, pero durante la configuración de buzones WorxMail no puede finalizar la configuración:

1. Si el servidor de Microsoft Exchange ActiveSync está usando certificados de servidor SSL privados para proteger el tráfico, compruebe que los certificados raíz e intermedios están instalados en el dispositivo móvil.

2. Compruebe que el tipo de autenticación seleccionado para ActiveSync es **Require client certificates**.



3. En Microsoft Exchange Server, compruebe el sitio de **Microsoft-Server-ActiveSync** para ver si tiene habilitada la autenticación con asignación de certificados de cliente (que está inhabilitada de manera predeterminada). La opción está en **Editor de configuración > Seguridad > Autenticación**.



Nota: Después de seleccionar **Verdadero**, asegúrese de hacer clic en **Aplicar** para que los cambios tengan efecto.

4. Compruebe la configuración de NetScaler Gateway en la consola de XenMobile: Asegúrese de que **Deliver user certificate for authentication** tiene el valor **ON** y que en **Credential provider** está seleccionado el perfil correcto, como se describió anteriormente en "Para configurar la entrega de certificados de NetScaler en XenMobile".

Para determinar si el certificado de cliente se ha entregado a un dispositivo móvil:

1. En la consola de XenMobile, vaya a **Manage > Devices** y seleccione el dispositivo.

2. Haga clic en **Edit** o **Show More**.

3. Vaya a la sección **Delivery Groups** y busque esta entrada:

    NetScaler Gateway Credentials : Requested credential, CertId=

Para validar si está habilitada la negociación de certificados de cliente:

1. Ejecute este comando de netsh para mostrar la configuración del certificado SSL que está vinculada en el sitio Web de IIS:

    netsh http show sslcert

2. Si el valor de **Negotiate Client Certificate** es **Disabled**, ejecute el siguiente comando para habilitarlo:

    netsh http delete sslcert ipport=0.0.0.0:443

netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable

Por ejemplo:

netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable

Si no puede entregar certificados raíz e intermedios a un dispositivo Windows Phone 8.1 a través de XenMobile:

- Envíe los archivos .cer de certificados raíz/intermedios por correo electrónico al dispositivo Windows Phone 8.1 e instálelos directamente.

Si WorxMail no se puede instalar correctamente en Windows Phone 8.1:

- Compruebe que el token de inscripción de la aplicación (.AETX) se entrega a través de XenMobile usando la directiva de dispositivo Enterprise Hub.
- Compruebe que el token de inscripción de la aplicación se creó usando el mismo certificado de empresa del proveedor de certificados utilizado para empaquetar WorxMail y firmar las aplicaciones de Worx Home.
- Compruebe que se usa el mismo ID de publicador para firmar y empaquetar Worx Home, WorxMail y el token de inscripción de la aplicación.

Entidades de infraestructura PKI

Oct 31, 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)
- PKIs genéricas (GPKIs)
- 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:

- **Name**. Escriba un nombre descriptivo para la entidad de infraestructura PKI.
- **WSDL URL**. Escriba la ubicación del archivo WSDL que describe el adaptador.
- **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.

5. Haga clic en **Next**.

Aparecerá la página Generic PKI Entity: Adapter Capabilities.

6. 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**.

7. 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.

8. 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 el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **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:

- 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.
- 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.
- 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.
- 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.
- 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.

5. Haga clic en **Next**.

Aparecerá 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.

Para conocer los requisitos de plantillas de Microsoft Certificate Services, consulte la documentación de Microsoft referente a su versión de servidor Microsoft. XenMobile no presenta requisitos para los certificados que distribuye, salvo los formatos de certificado indicados en Certificados.

6. 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.

7. 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.

8. 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.

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

10. Haga clic en **Save**.

La entidad se muestra en la tabla PKI Entities.

XenMobile respalda la lista de revocación de certificados (CRL) solo para una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, XenMobile utiliza NetScaler para administrar la revocación. Al configurar la autenticación basada en certificados de cliente, tenga en cuenta si es necesario configurar el parámetro de lista de revocación de certificados (CRL), **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse usando un certificado existente en el dispositivo; XenMobile vuelve a emitir un certificado nuevo, porque no impide a un usuario generar un certificado de usuario si se revoca otro. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

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 el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **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**.

Aparecerá la página **Discretionary CA: General Information**.

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

- **Name**. Escriba un nombre descriptivo para la entidad de certificación discrecional.
- **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**.

5. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Parameters**.

6. En la página **Discretionary CA: Parameters**, lleve a cabo lo siguiente:
- **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.
- **Next serial number**. Escriba un valor para determinar el siguiente número a emitir.
- **Certificate valid for**. Escriba la cantidad de días durante los que el certificado será válido.
- **Key usage**. Debe identificar el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, establezca las claves apropiadas en **On**. Una vez establecidas, la entidad de certificación está limitada a la emisión de certificados para esos fines.
- **Extended key usage**. Para agregar parámetros adicionales, haga clic en **Add**, escriba el nombre de la clave y, a continuación, haga clic en **Save**.

7. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Distribution**.

8. 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 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.

9. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Online Certificate Status Protocol (OCSP)**.

En la página **Discretionary CA: Online Certificate Status Protocol (OCSP)**, lleve a cabo lo siguiente:

- 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.
- 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.

10. Haga clic en **Save**.

La entidad de certificación discrecional se muestra en la tabla PKI Entitites.

Proveedores de credenciales

Jul 27, 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 admite el método de inicio de sesión para las tres entidades PKI (la entidad de servicios de certificado de Microsoft, el protocolo PKI genérico y la CA discrecional).
- fetch. Con este método, la emisión de certificados, para los fines de XenMobile, es la recuperación de un par de claves existente. XenMobile solo admite el método de recuperación para el protocolo PKI genérico.

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 el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **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:

- **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.
- **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.
- **Issuing entity**. Haga clic en la entidad emisora de certificados.
- **Issuing method**: Haga clic en **Sign** o **Fetch** para elegir el método que el sistema usará para obtener los certificados desde la entidad configurada. Para la autenticación con certificados de cliente, elija **Sign**.
- Si la lista de plantillas está disponible, seleccione una plantilla para el proveedor de credenciales.

4. Haga clic en **Next**.

Nota: Estas plantillas pasan a estar disponibles cuando las entidades de Microsoft Certificate Services se agregan a **Settings** > **More** > **PKI Entities**.

Aparecerá la página **Credential Providers: Certificate Signing Request**.

5. En la página **Credential Providers: Certificate Signing Request**, lleve a cabo lo siguiente:

- **Key algorithm**. Haga clic en el algoritmo de clave para el nuevo par de claves. Los valores disponibles son: **RSA**, **DSA** y **ECDSA**.
- **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.

- **Signature algorithm**. Haga clic en un valor para el nuevo certificado. Los valores dependen del algoritmo de clave.
- **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.

  Por ejemplo, para la autenticación con certificados de cliente, use los parámetros siguientes:

  Key algorithm: RSA
  Key size: 2048
  Signature algorithm: SHA1withRSA
  Subject name: cn=$user.username

6. 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.

Para la autenticación con certificados de cliente, especifique:

Type: User Principal name
Value: $user.userprincipalname

Nota: Al igual que para el nombre del sujeto (Subject Name), puede hacer uso de las macros de XenMobile en el campo del valor.

7. Haga clic en **Next**.

Aparecerá la página **Credential Providers: Distribution**.

8. En la página **Credential Providers: Distribution**, lleve a cabo lo siguiente:

- 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.
- 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**, 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. Aparecerán campos nuevos para esos certificados.

9. Haga clic en **Next**.

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.

12. En la página **Credential Providers: Revocation XenMobile**, lleve a cabo lo siguiente:

- En **Revoke issued certificates**, seleccione una de las opciones que indican el momento en que se deben revocar los certificados.
- 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.

- 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.

13. Haga clic en **Next**.

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.

14. En la página **Credential Providers: Revocation PKI**, lleve a cabo lo siguiente si quiere revocar certificados procedentes de la infraestructura de clave pública:

- Cambie la opción **Enable external revocation checks** a **On**. Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
- 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
- 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.

- 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.

15. Haga clic en **Next**.

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).

16. En la página **Credential Providers: Renewal**, haga lo siguiente si quiere renovar los certificados cuando caduquen: Defina **Renew certificates** cuando caduquen con el valor **On**.

Aparecerán campos adicionales.

- 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.
- 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.

17. 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.

18. 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.

19. 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.

20. Haga clic en **Save**.

El proveedor de credenciales se agregará a la tabla Credential Providers.

Solicitud de un certificado APNs

Jul 27, 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).
- Pida a Citrix que firme 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 como administrador en la consola de XenMobile.
9. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
10. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
11. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
12. En el menú **Import**, elija **Keystore**.
13. En **Use as**, elija **APNs**.
14. En **Keystore file**, seleccione el archivo de almacén de claves que quiere importar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
15. En **Password**, escriba la contraseña asignada al certificado.
16. Haga clic en **Import**.

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. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
2. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
3. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
4. En el menú **Import**, elija **Keystore**.
5. En **Use as**, elija **APNs**.
6. Busque el archivo .p12 en su equipo.
7. 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 la consola de XenMobile. Haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
7. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
8. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
9. En el menú **Import**, elija **Keystore**.
10. En **Use as**, elija **APNs**.
11. Busque el archivo .p12 en su equipo.
12. Escriba la contraseña y, a continuación, haga clic en **Import**.

Parámetros de inscripción, cuentas de usuario y roles

Jul 27, 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. Para abrir la página **Settings**, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola.

En la página **Settings**, puede realizar lo siguiente:

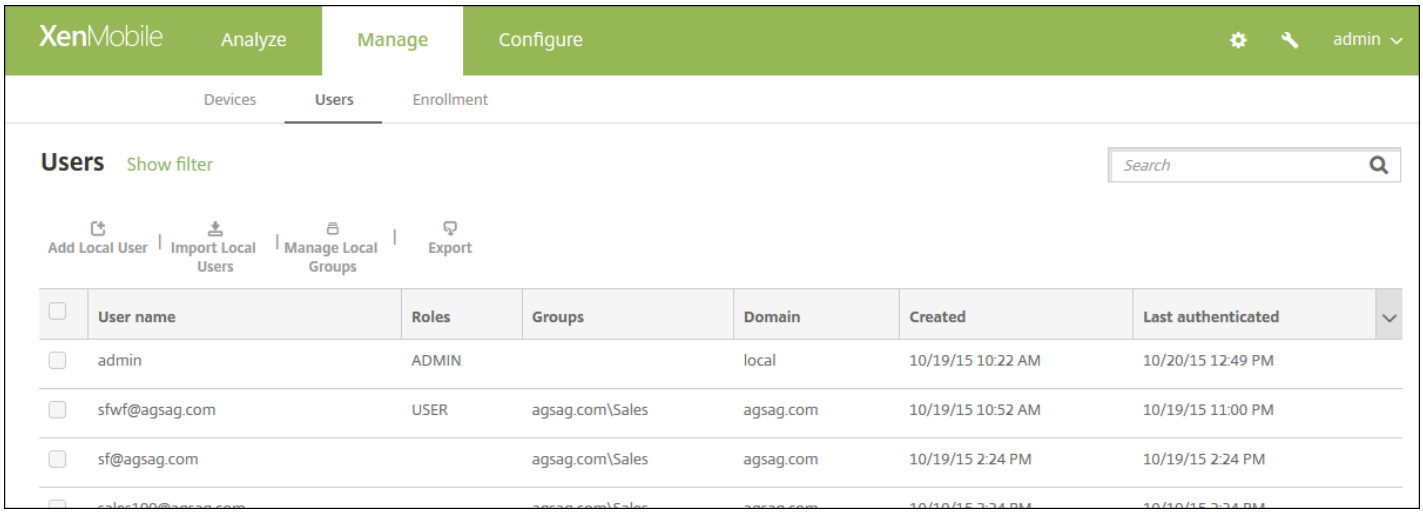
- Haga clic en **Local Users and Groups** para agregar cuentas de usuario de forma manual. También puede usar un archivo CSV de aprovisionamiento para importar las cuentas y administrar grupos locales. Para obtener más detalles, consulte:
  - Para agregar, modificar o eliminar usuarios locales en XenMobile
  - 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. Para obtener más detalles, consulte:
  - Para configurar modos de inscripción y habilitar el portal Self Help Portal
  - Activación de 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. Para obtener más detalles, consulte:
  - Configuración de roles con RBAC y Permisos y roles de 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. Para obtener más detalles, consulte:
  - Creación y actualización de plantillas de notificaciones

Para agregar, modificar o eliminar usuarios locales en XenMobile

Jul 27, 2016

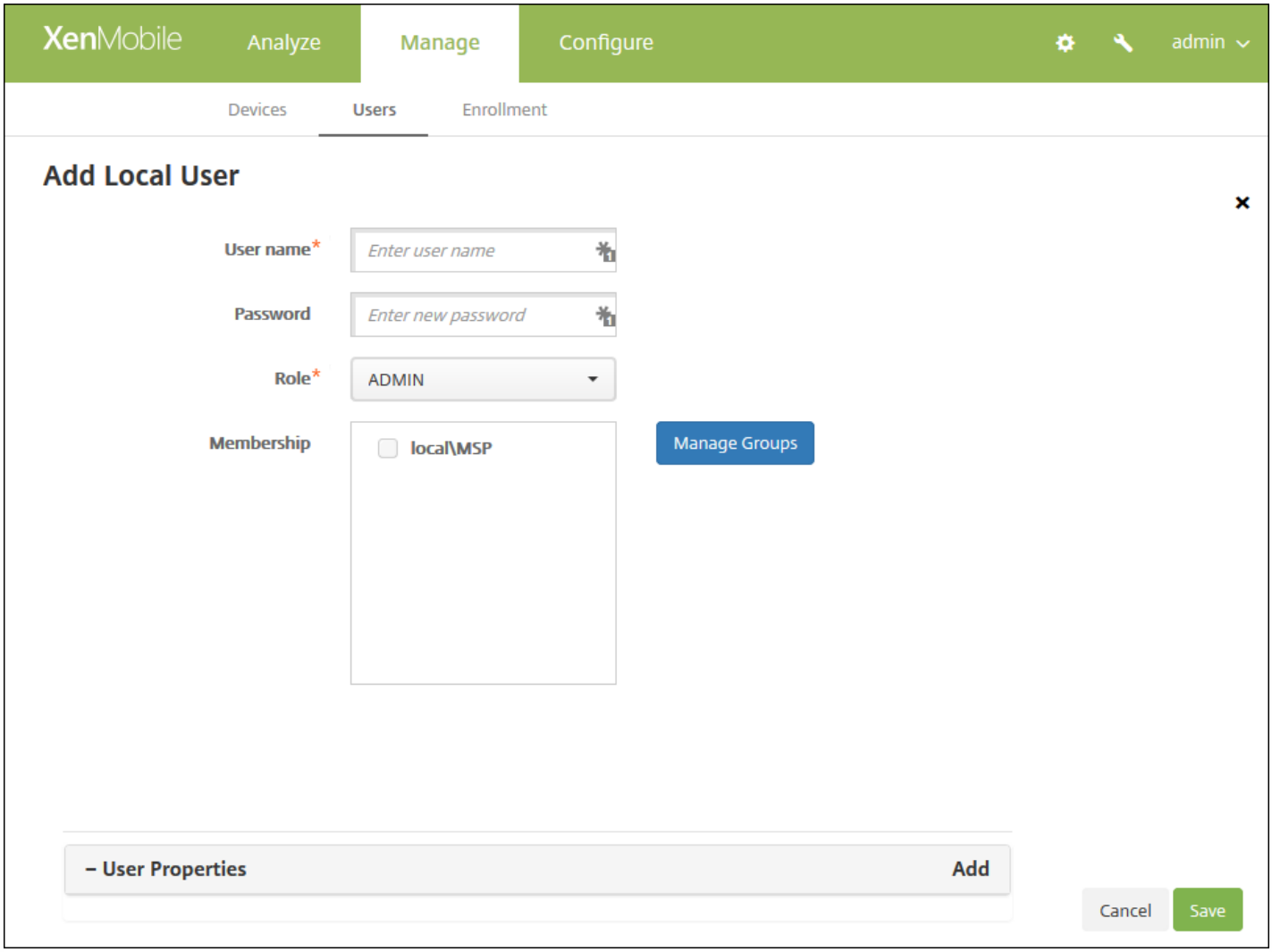
Puede agregar cuentas de usuario local a XenMobile de forma manual, o bien puede usar un archivo de aprovisionamiento para importar las cuentas. Consulte Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV para obtener información acerca de los pasos necesarios para importar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

1. En la consola de XenMobile, haga clic en **Manage > Users**. Aparecerá la página **Users**.



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 **Users**, haga clic en **Add Local User**. Aparecerá la página **Add Local User**.



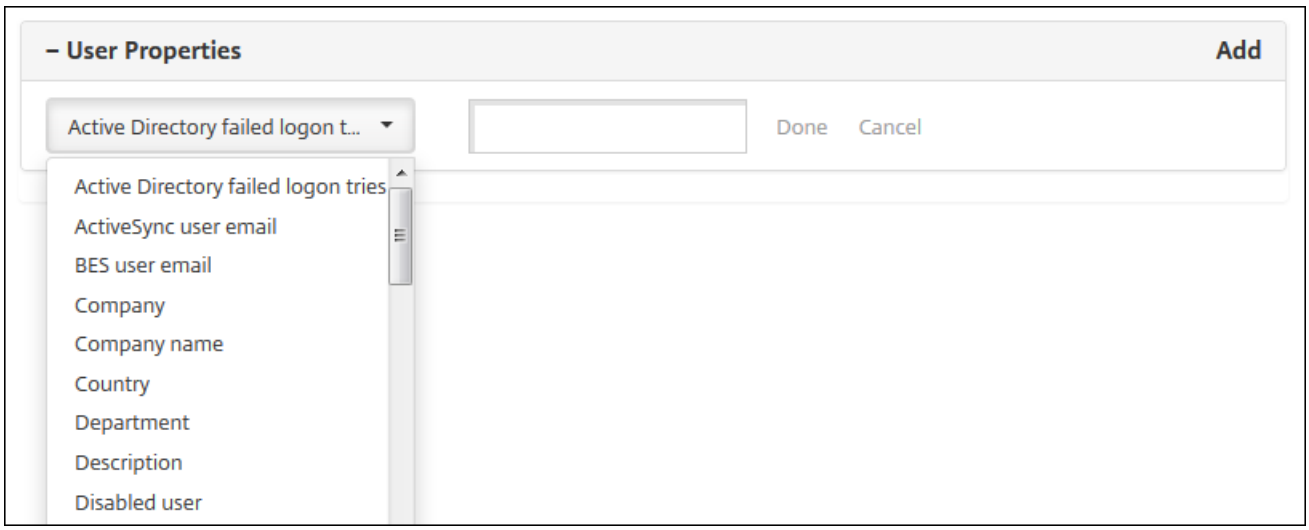
2. Configure los siguientes parámetros:

- **User name**. Escriba el nombre del usuario. Este campo es obligatorio. Puede incluir espacios en los nombres, además de letras mayúsculas y minúsculas.
- **Password**. Escriba una contraseña opcional de usuario.
- **Role**. En la lista, haga clic en el rol del usuario. Para obtener más información acerca de los roles, consulte Configuración de roles con RBAC y Permisos y roles de RBAC. Las opciones posibles son:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Membership**. En la lista, haga clic en el grupo o en los grupos a los que agregar el usuario.
- **User Properties**. Agregue propiedades de usuario opcionales. Para cada propiedad de usuario que quiera agregar, haga clic en **Add** y haga lo siguiente:
  - **User Properties**. En la lista, haga clic en una propiedad y, a continuación, escriba el atributo de la propiedad de usuario en el campo que hay junto a la propiedad.
  - Haga clic en **Done** para guardar la propiedad de usuario o haga clic en **Cancel** para no guardarla.

    Nota: Para eliminar una propiedad de usuario existente, coloque el cursor sobre la línea que la contiene y, a

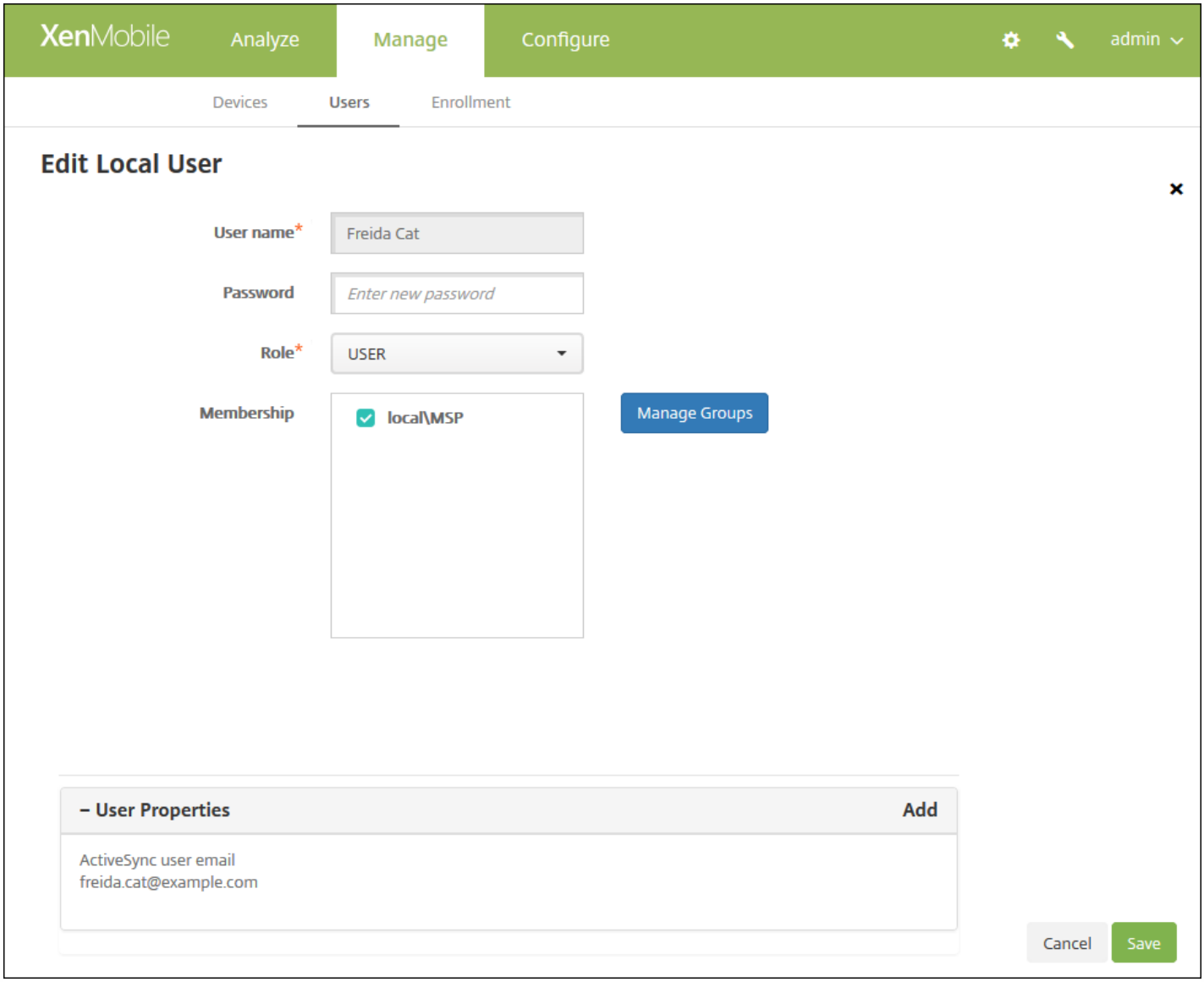
continuación, haga clic en la X situada a la derecha. La propiedad se elimina inmediatamente.

Para modificar una propiedad de usuario, haga clic en la propiedad y realice los cambios. Haga clic en **Done** para guardar los cambios de la lista o haga clic en **Cancel** para no realizar cambios en la lista.



3. Haga clic en **Save**.

1. En la página **Users**, en la lista de usuarios, haga clic para seleccionar un usuario y, a continuación, haga clic en **Edit**. Aparecerá la página **Edit Local User**. Consulte Filtros y tablas en la consola de XenMobile para obtener más información sobre cómo seleccionar elementos en tablas.



2. Cambie la siguiente información como corresponda:

- **User name**. No se puede cambiar el nombre de usuario.
- **Password**. Cambie o agregue una contraseña de usuario.
- **Role**. En la lista, haga clic en el rol del usuario.
- **Membership**. En la lista, haga clic en el grupo o en los grupos a los que agregar el usuario. Para quitar al usuario de un grupo, desmarque la casilla de verificación situada junto al nombre del grupo.
- **User properties**. Realice una de las siguientes acciones:
  - Para cambiar cada propiedad de usuario, haga clic en ella y realice los cambios. Haga clic en **Done** para guardar los cambios de la lista o haga clic en **Cancel** para no realizar cambios en la lista.
  - Para cada propiedad de usuario que quiera agregar, haga clic en **Add** y haga lo siguiente:
    - **User Properties**. En la lista, haga clic en una propiedad y, a continuación, escriba el atributo de la propiedad de usuario en el campo que hay junto a la propiedad.
    - Haga clic en **Done** para guardar la propiedad de usuario o haga clic en **Cancel** para no guardarla.
  - Para eliminar cada propiedad de usuario, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la X situada a la derecha. La propiedad se elimina inmediatamente.

3. Haga clic en **Save** para guardar los cambios o en **Cancel** para no guardarlos.

1. En la página **Users**, en la lista de usuarios, seleccione al usuario.

   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.

3. Haga clic en **Delete** para eliminar al usuario o en **Cancel** para no eliminarlo.

Importación de cuentas de usuario

Oct 31, 2016

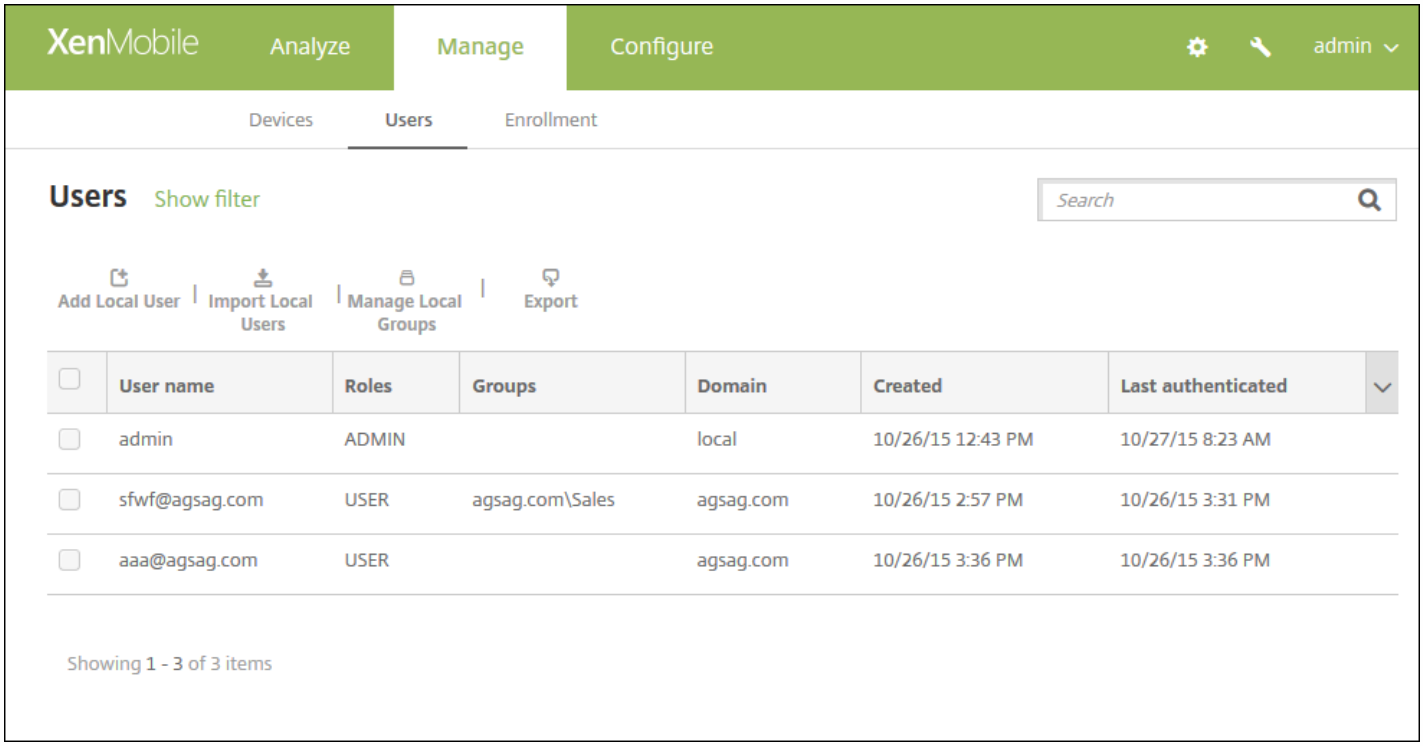
Puede importar propiedades y cuentas de usuario desde un archivo de formato CSV llamado "archivo de aprovisionamiento", el cual puede crear manualmente. Para obtener información acerca de los formatos de los archivos de aprovisionamiento, consulte Formatos de archivo de aprovisionamiento.

Nota:

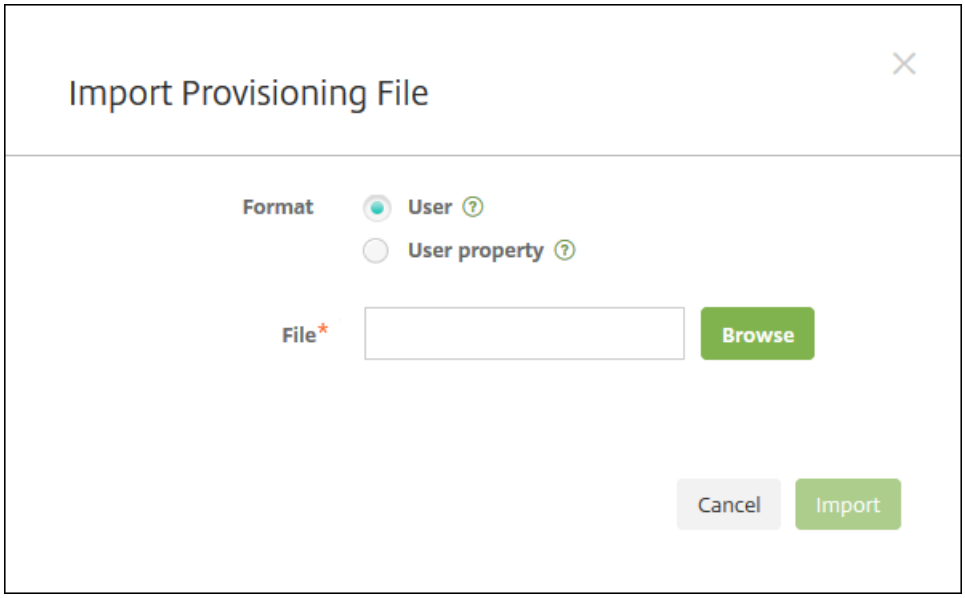
- Si importa los usuarios desde un directorio LDAP, utilice el nombre de dominio, junto con el nombre de usuario en el archivo de importación. Por ejemplo, nombredeusuario@dominio.com. Esta sintaxis evitará búsquedas adicionales que pueden reducir la velocidad de importación.
- Si importa usuarios al 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 este 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 **Manage > Users**. Aparecerá la página **Users**,



2. Haga clic en **Import Local Users**. Aparece el cuadro de diálogo **Import Provisioning File**.



3. Seleccione **User** o **Property** para el formato del archivo de aprovisionamiento que va a importar.

4. Para seleccionar el archivo de aprovisionamiento que quiere usar, haga clic en **Browse** y vaya a la ubicación de ese archivo.

5. Haga clic en **Import**.

Formatos de archivo de aprovisionamiento

Aug 25, 2016

El archivo de aprovisionamiento que se crea manualmente y se usa para importar en XenMobile propiedades y cuentas de usuario debe tener uno de los siguientes formatos:

- Campos de archivo de aprovisionamiento de usuarios: usuario;contraseña;rol;grupo1;grupo2
- Campos de archivo de aprovisionamiento de atributos de usuario: usuario;nombrePropiedad1;valorPropiedad1;nombrePropiedad2;valorPropiedad2

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\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01 significa:

- Usuario: user01
- Contraseña: pwd;01
- Rol: USER
- Grupos:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

Este otro ejemplo, AUser0;1.password;USER;ActiveDirectory.test.net, significa:

- Usuario: AUser0
- Contraseña: 1.password
- Rol: USER
- Grupo: ActiveDirectory.test.net

Esta 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

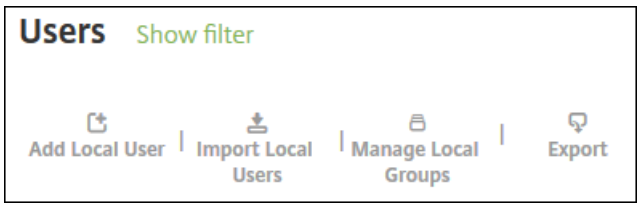
Cómo agregar o quitar grupos

Jul 27, 2016

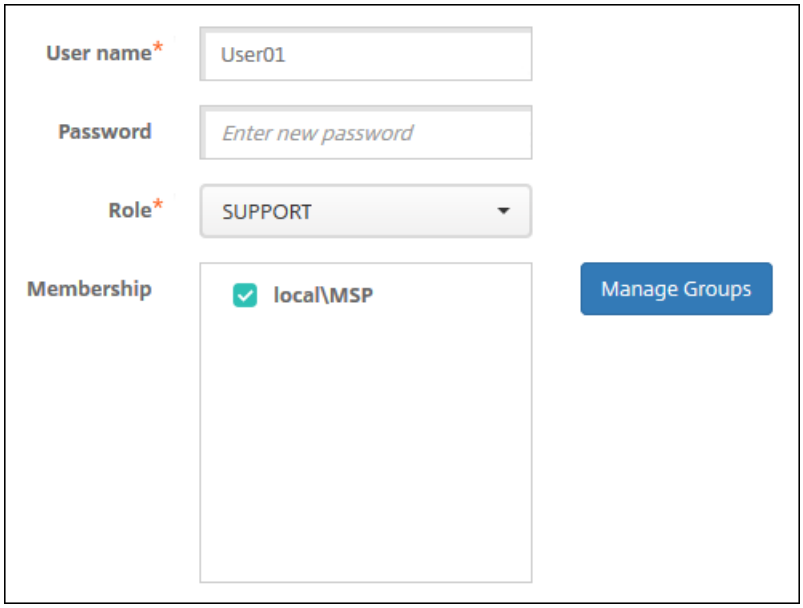
Puede administrar grupos en el cuadro de diálogo Manage Groups de la consola de XenMobile, que encontrará en las páginas **Users**, **Add Local User** o **Edit Local User**. No hay ningún comando de modificación de grupos. Si quita un grupo, tenga en cuenta que quitar un grupo no tiene ningún efecto 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:

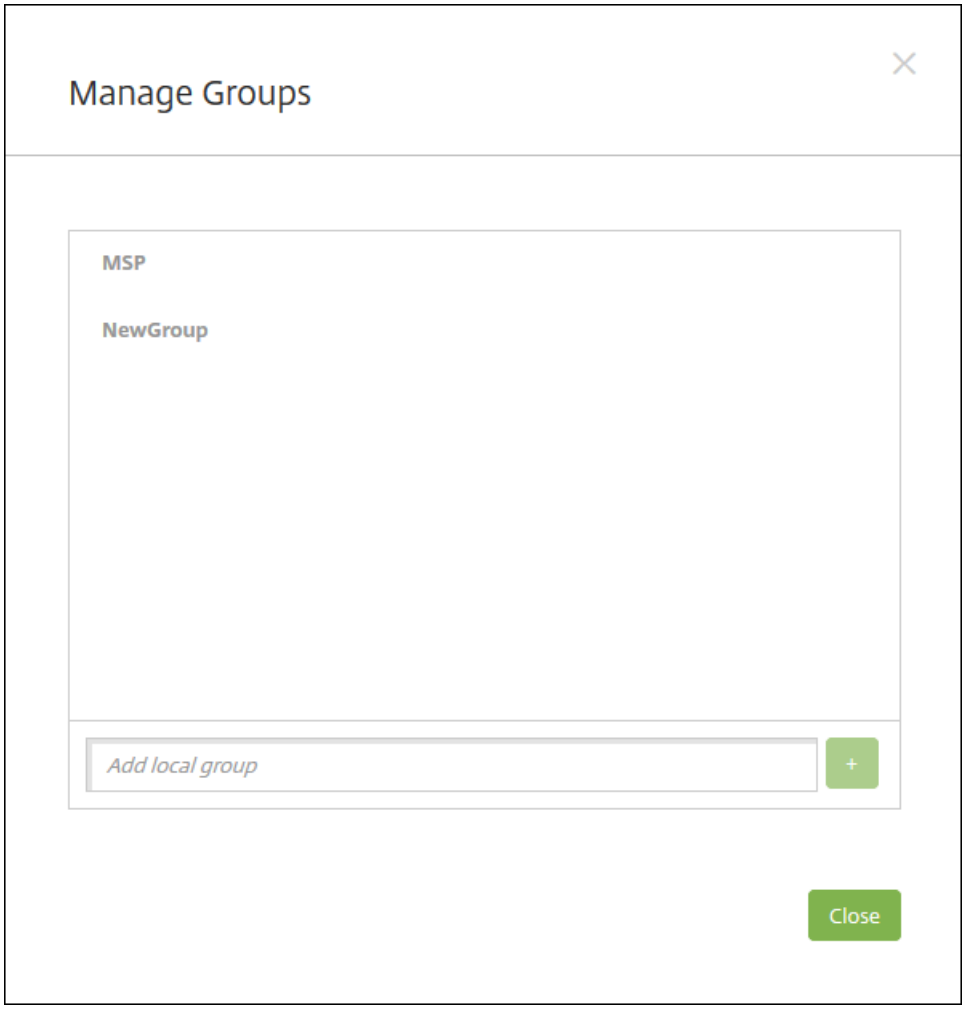
- En la página **Users**, haga clic en **Manage Local Groups**.



- Ya sea en la página **Add Local User** o **Edit Local User**, haga clic en **Manage Groups**.



Aparecerá el cuadro de diálogo **Manage Groups**.



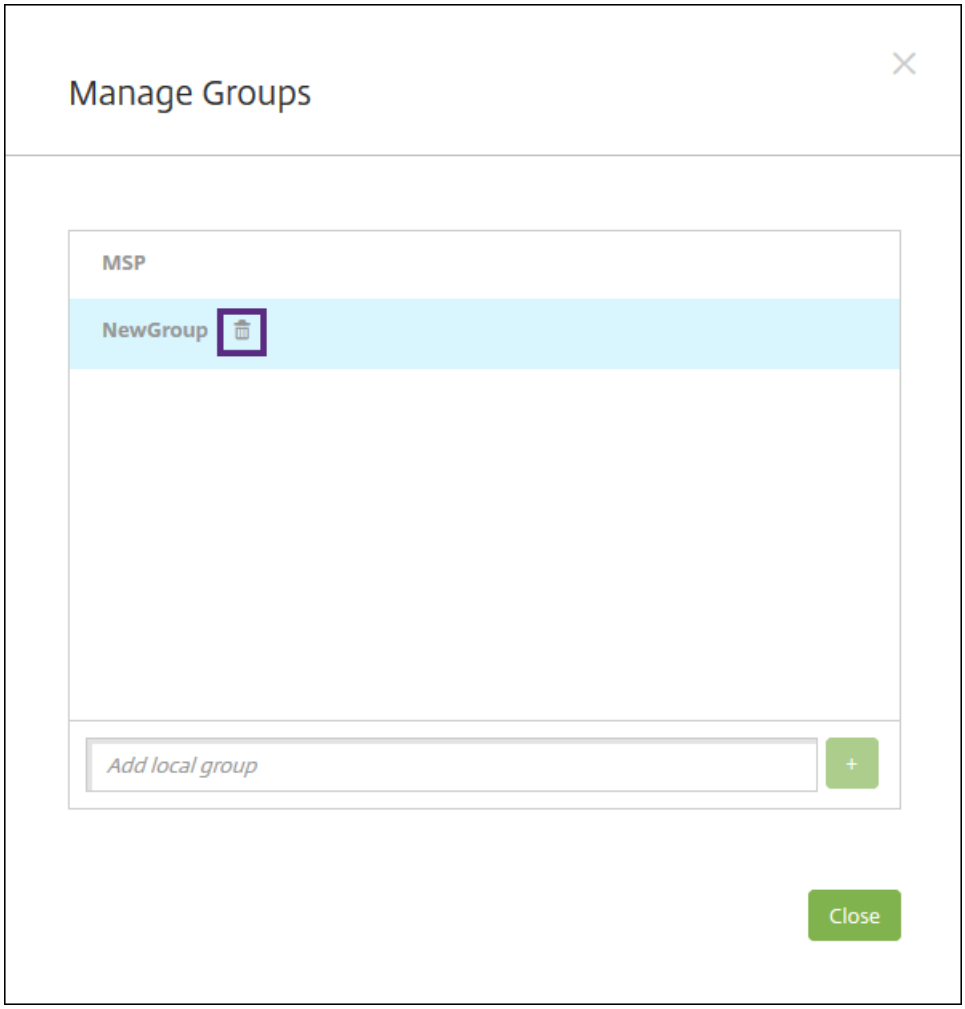
2. Bajo la lista de grupos, escriba un nuevo nombre de grupo y, a continuación, haga clic en el signo más (+). El grupo de usuarios se agrega a la lista.

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 Users, 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**.

Configuración de roles con RBAC

Oct 31, 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.
- **Device Provisioning**. Concede acceso a tareas básicas de administración de dispositivos para dispositivos Windows CE.
- **Support**. Concede acceso para la asistencia remota.
- **User**. Rol utilizado por los usuarios que pueden inscribir dispositivos y acceder al portal Self Help Portal.

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.

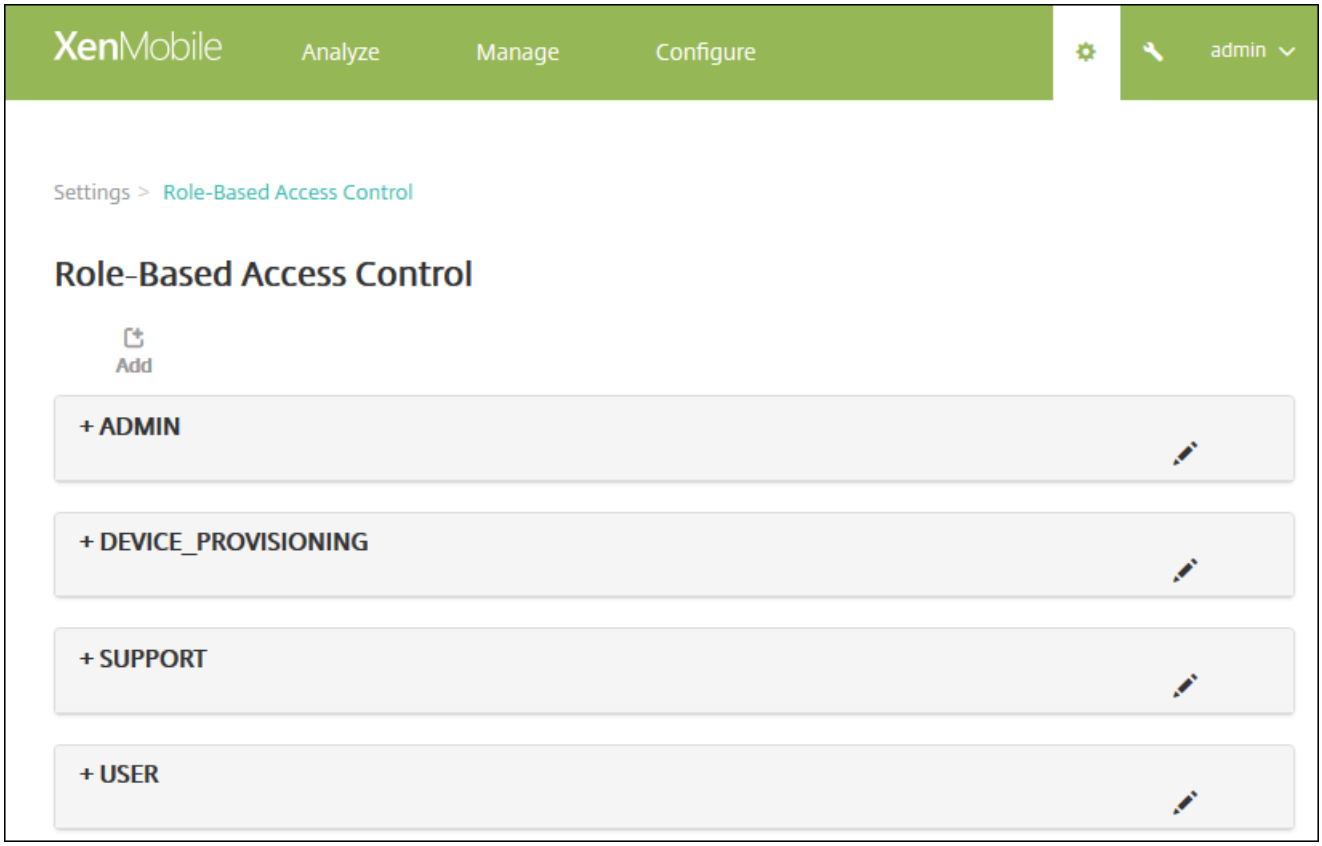
Nota: Los usuarios locales solo pueden tener un rol asignado.

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.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. Haga clic en **Role-Based Access Control**. Aparecerá la página **Role-Based Access Control** con los cuatro roles de usuario predeterminados, además de los roles que haya agregado antes.



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 ilustración.

3. 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.

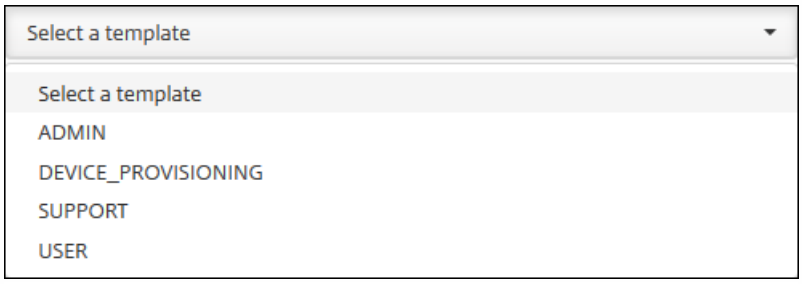
4. Escriba la siguiente información para crear un nuevo rol de usuario o para modificar un rol de usuario existente:

- **RBAC name**. Indique un nombre descriptivo para el nuevo rol de usuario. No se puede cambiar el nombre de un rol

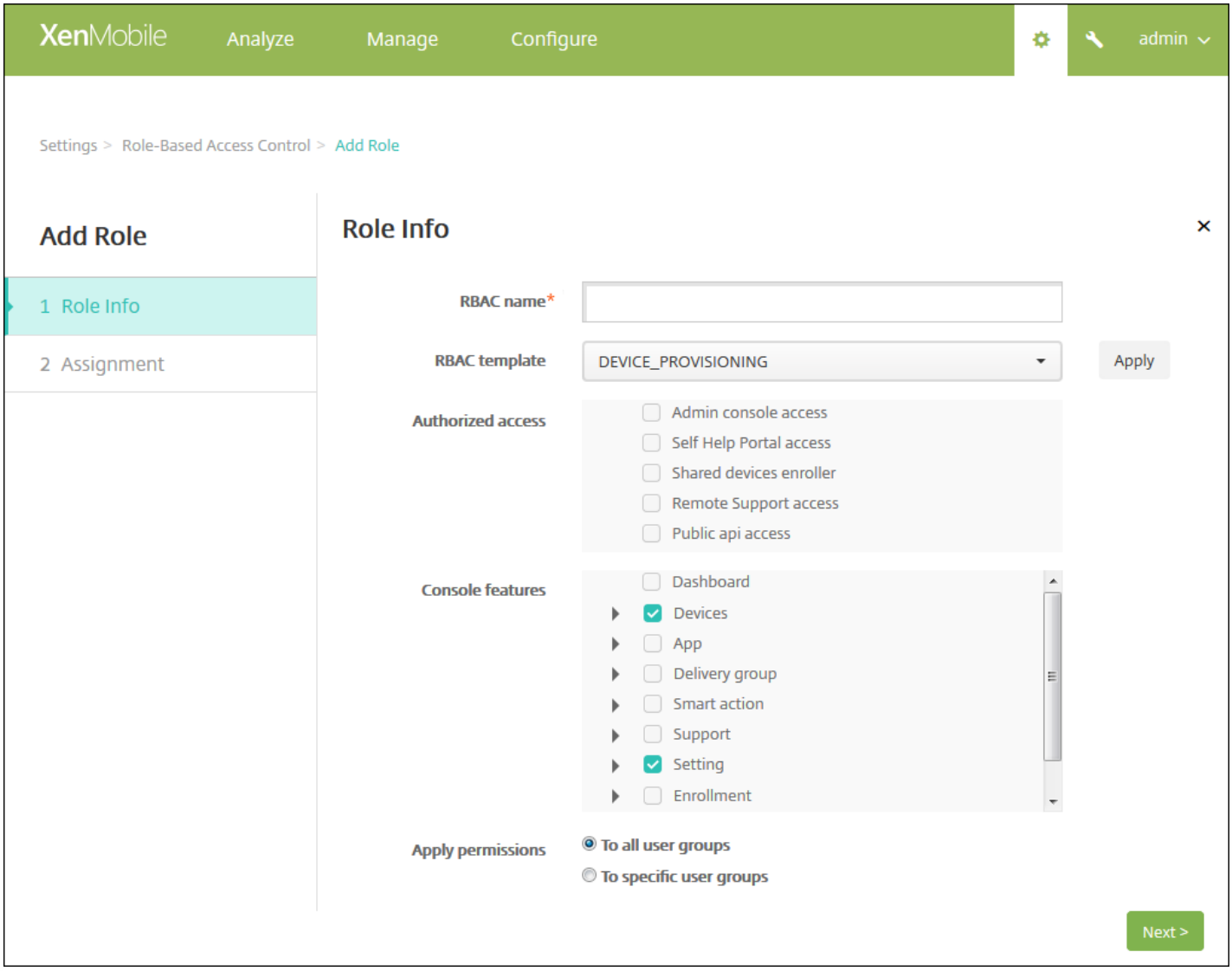
existente.

- **RBAC template**. Puede hacer clic en una plantilla como punto de partida para el nuevo rol. No puede seleccionar una plantilla si está modificando un rol existente.

  Las plantillas RBAC son los roles de usuario predeterminados. 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**.

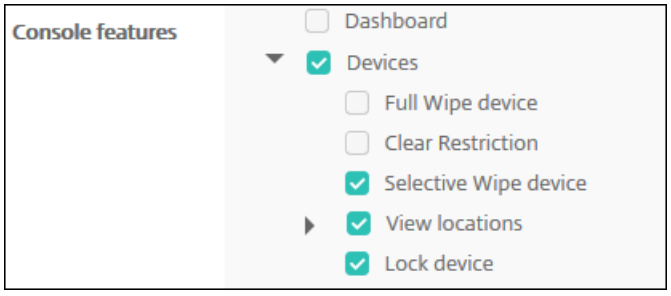


5. Haga clic en **Apply**, situado a la derecha del campo **RBAC template**, para rellenar las casillas **Authorized access** y **Console features** con los permisos concedidos de funciones y acceso predefinidos para la plantilla seleccionada.



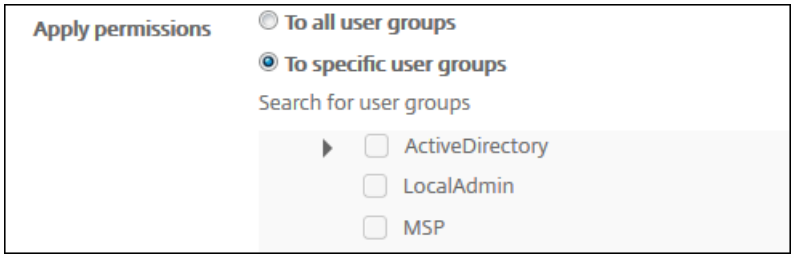
6. Marque y desmarque las casillas de verificación **Authorized access** y **Console features** para personalizar el rol.

Si hace clic en el triángulo situado junto a Console feature, aparecerán los permisos específicos de esa función y puede marcarlos o desmarcarlos. Si marca la casilla del nivel superior de la lista, impedirá el acceso a esa parte de la consola. Debe marcar de forma individual las opciones situadas por debajo de la casilla del nivel superior para habilitar el acceso a esas opciones. Por ejemplo, en la figura siguiente, las opciones **Full Wipe device** y **Clear Restrictions** no aparecen en la consola para los usuarios asignados a ese rol, mientras que las opciones marcadas sí aparecen.

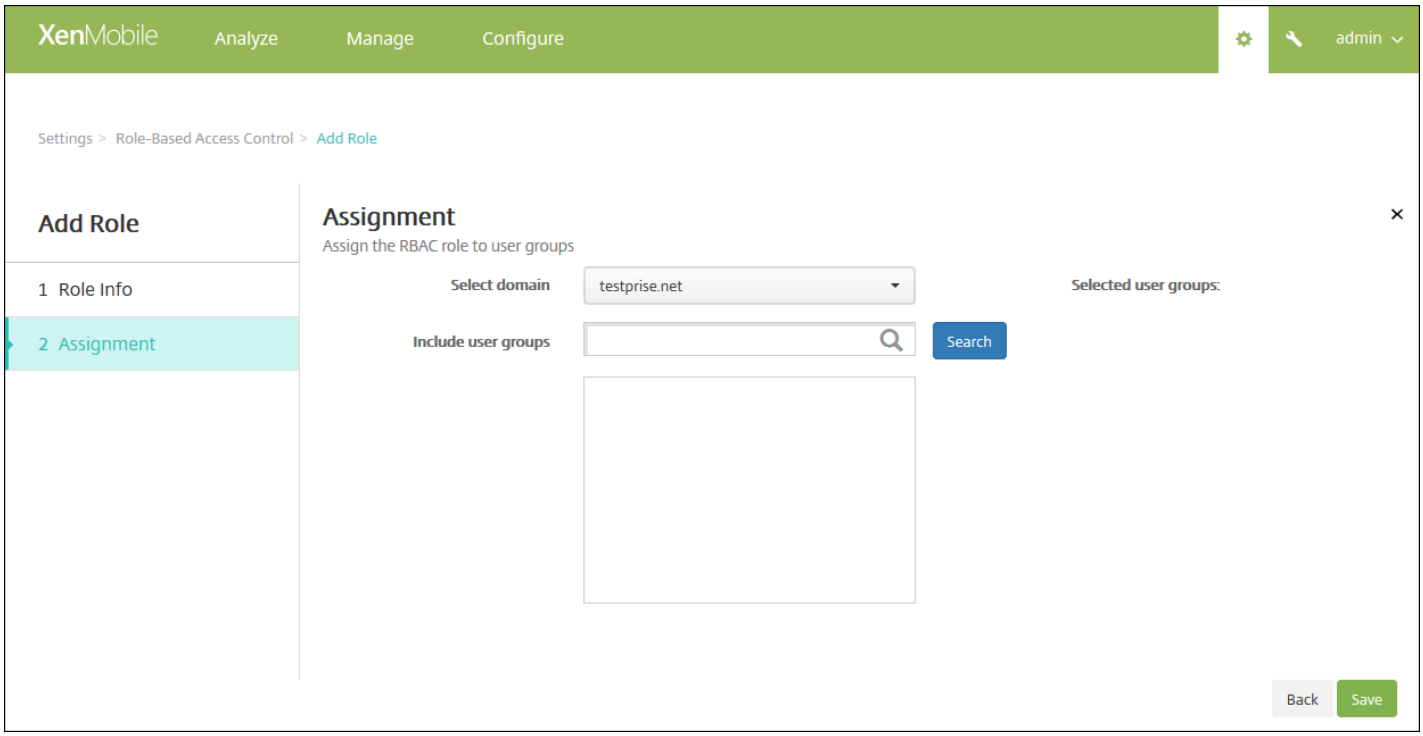


7. **Apply permissions**. Marque los grupos a los que aplicar los permisos seleccionados. Si hace clic en **To specific user**

groups, aparecerá una lista de grupos. De esa lista, puede seleccionar un grupo o varios.

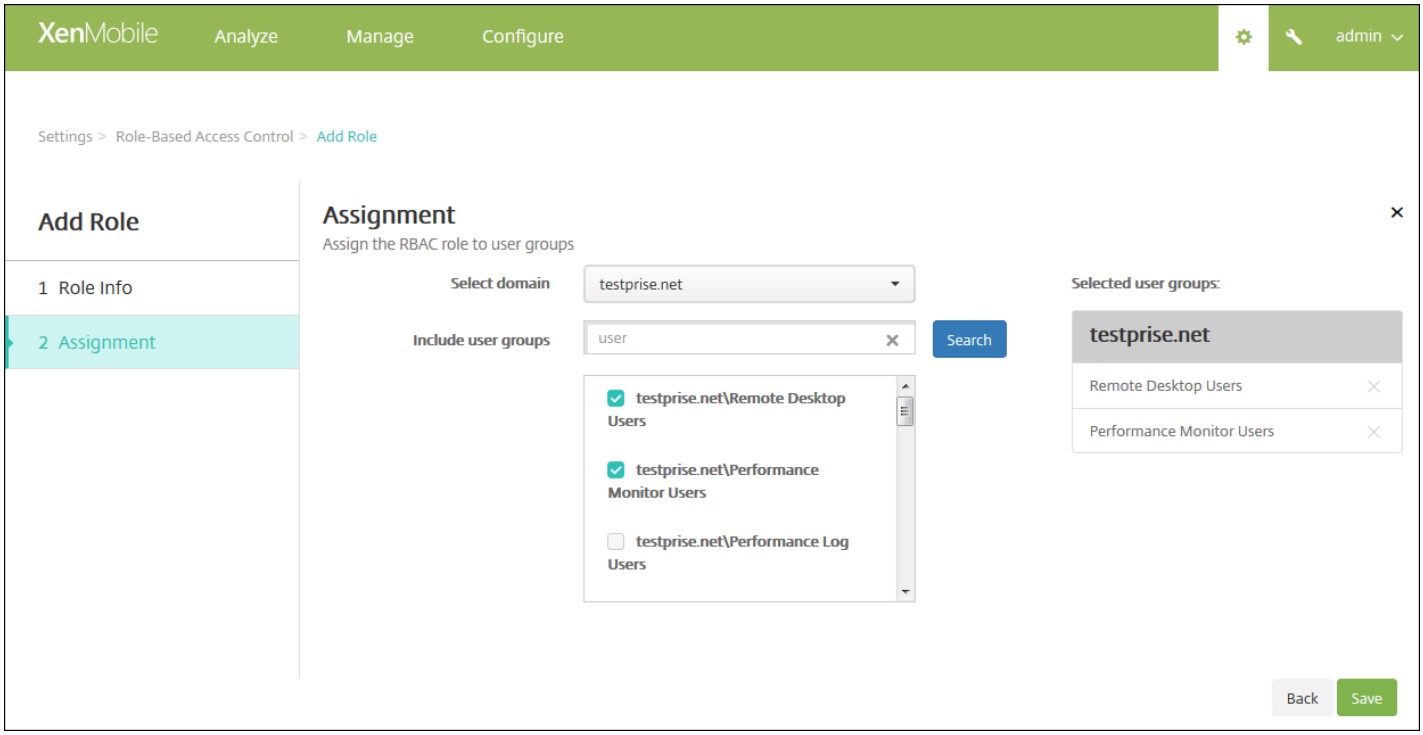


8. Haga clic en **Siguiente**. Aparecerá la página **Assignment**.



9. Escriba la siguiente información para asignar el rol a los grupos de usuarios.

- **Select domain**. En la lista, haga clic en un dominio.
- **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.
- En la lista que aparezca, seleccione los grupos de usuarios a los que asignar el rol. Cuando se selecciona un grupo de usuarios, el grupo aparece en la lista **Selected user groups**.



Nota: Para quitar un grupo de usuarios de la lista **Selected user groups**, haga clic en la X situada junto al nombre del grupo de usuarios.

10. Haga clic en **Save**.

Permisos y roles de RBAC

Aug 25, 2016

Cada rol del control de acceso basado en roles (RBAC) tiene ciertos permisos de funciones y de acceso asociados a cada uno de ellos. En este artículo, se describe para qué sirve cada uno de esos permisos. Para obtener una lista completa de permisos predeterminados para cada rol integrado, descargue Role-Based Access Control Defaults.

Para obtener más información acerca de los roles de RBAC, consulte Configuración de roles con RBAC.

Para configurar modos de inscripción y habilitar el portal Self Help Portal

Jul 27, 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).

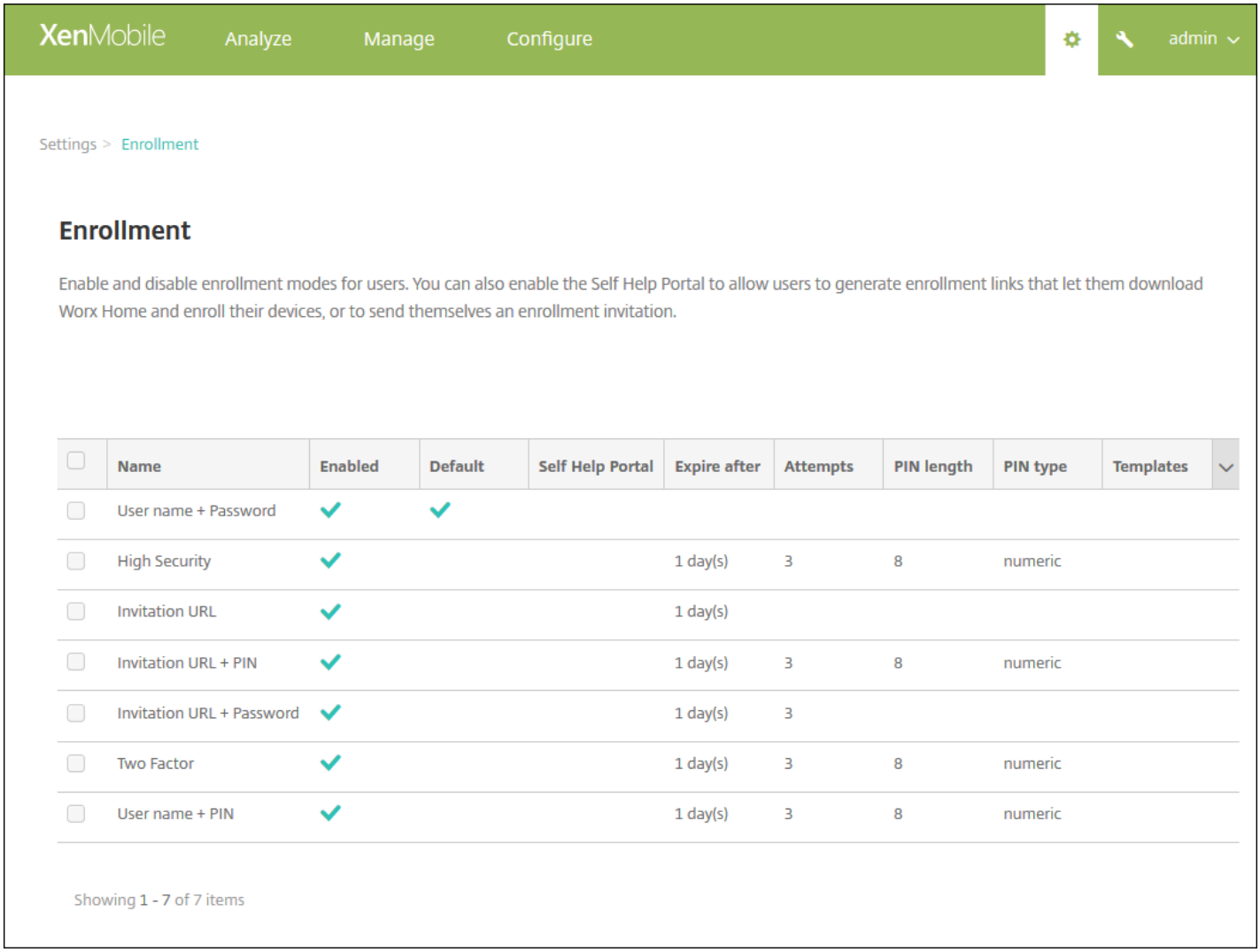
Nota: Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Creación o actualización de plantillas de notificaciones.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. Haga clic en **Enrollment**. Aparecerá la página **Enrollment**, que contiene una tabla de todos los modos de inscripción disponibles. De manera predeterminada, están habilitados todos los modos de inscripción.

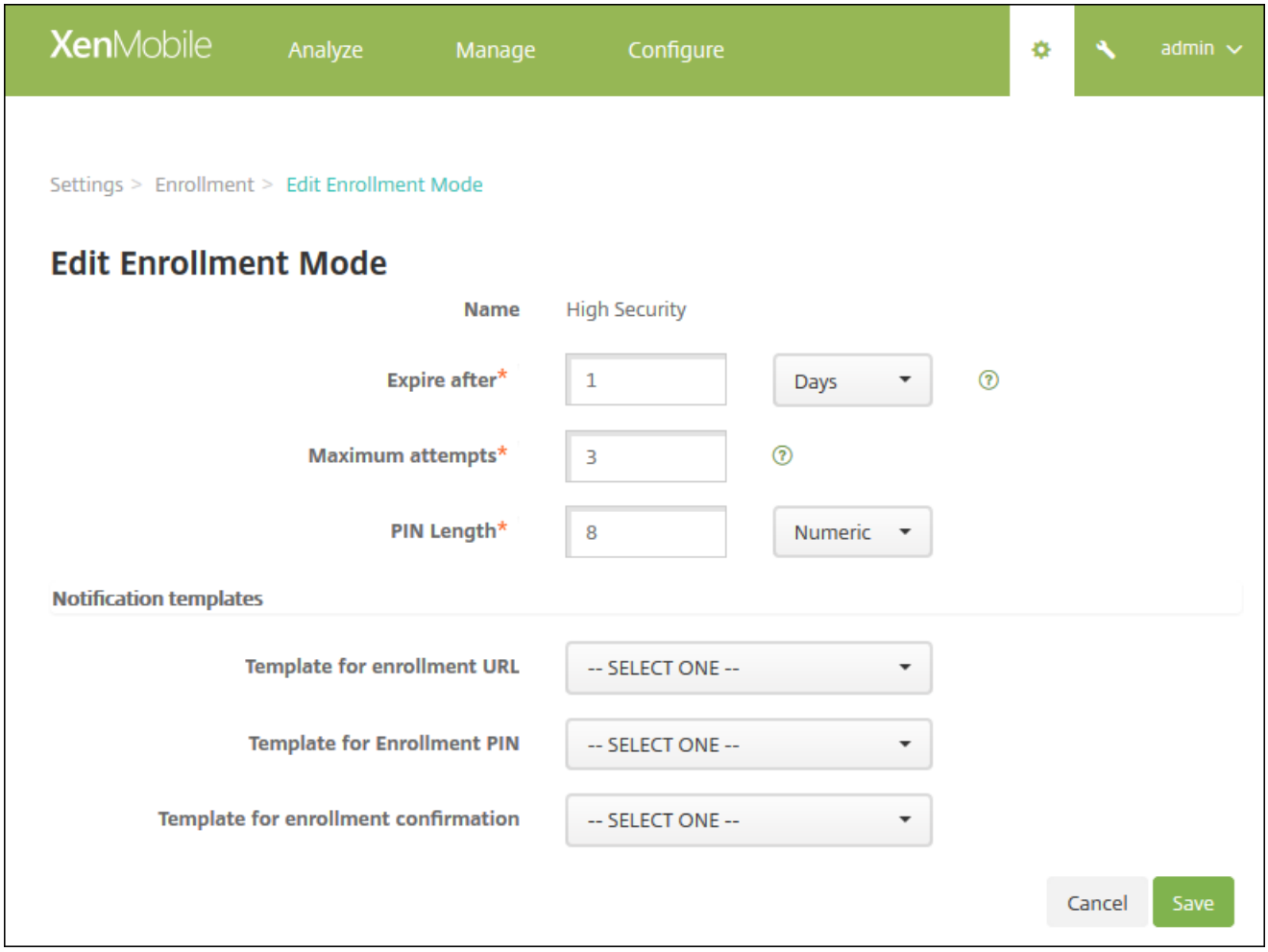
3. Seleccione un modo de inscripción de la lista para modificarlo y, a continuación, establezca ese modo como predeterminado, elimínelo, o bien permita a los usuarios acceder a él a través del portal Self Help Portal.

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 a la derecha de la lista.



Para modificar un modo de inscripción

1. En la lista **Enrollment**, seleccione un modo de inscripción y, a continuación, haga clic en Edit. Aparecerá la página **Edit Enrollment Mode**. Las opciones que verá dependerán del modo que seleccione.



2. Cambie la siguiente información como corresponda:

- **Expire after**. Introduzca una fecha límite de caducidad, después de la cual, los usuarios no podrán inscribir sus dispositivos. Este valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.
  Nota: Escriba 0 para evitar que la invitación caduque.

- **Days**. En la lista, haga clic en **Days** o **Hours**, de acuerdo con la fecha límite de caducidad que ha introducido en **Expire after**.
- **Maximum Attempts**. Escriba la cantidad de intentos de inscripción que un usuario puede llevar a cabo antes de que se bloquee el proceso de inscripción. Este valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.
  Nota: Escriba 0 para permitir una cantidad ilimitada de intentos.

- **PIN length**. Escriba un número para indicar la cantidad de dígitos o caracteres que contendrá el PIN generado.
- **Numeric**. En la lista, haga clic en **Numeric** o **Alphanumeric** para indicar el tipo de PIN.
- **Plantillas de notificaciones**:
  - **Template for Enrollment URL**. En la lista, 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 plantillas de notificaciones, consulte Creación o actualización de plantillas de notificaciones.
  - **Template for Enrollment PIN**. En la lista, seleccione una plantilla para el PIN de inscripción.

- **Template for enrollment confirmation**. En la lista, seleccione la plantilla a utilizar para informar al usuario de que la inscripción se ha realizado correctamente.

3. Haga clic en **Save**.

Para establecer un modo de inscripción como predeterminado

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 puede establecer como modo de inscripción predeterminado **Username + Password**, **Two Factor** o **Username + PIN**.
1. Seleccione uno de los modos, ya sea **Username + Password**, **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.

Para inhabilitar un modo de inscripción

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.

Activación de la detección automática en XenMobile para la inscripción de usuarios

Jul 27, 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 activar la detección automática, puede acceder al portal Autodiscovery Service en https://xenmobiletools.citrix.com. Para obtener más información sobre el portal Autodiscovery Service, consulte la sección Servicio de detección automática de XenMobile.

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 usando el portal Autodiscovery Service en https://xenmobiletools.citrix.com, abra un caso de asistencia técnica en el portal de Citrix Support y déles 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:

- Obtenga un certificado SSL firmado públicamente y sin comodines para enterpriseenrollment.miempresa.com, donde miempresa.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.
- Cree un registro de nombre canónico (CNAME) en su DNS y asigne la dirección de su certificado SSL (enterpriseenrollment.miEmpresa.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 para dominios múltiples, en caso de que quiera inscribir dispositivos usando varios dominios. 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

Jul 27, 2016

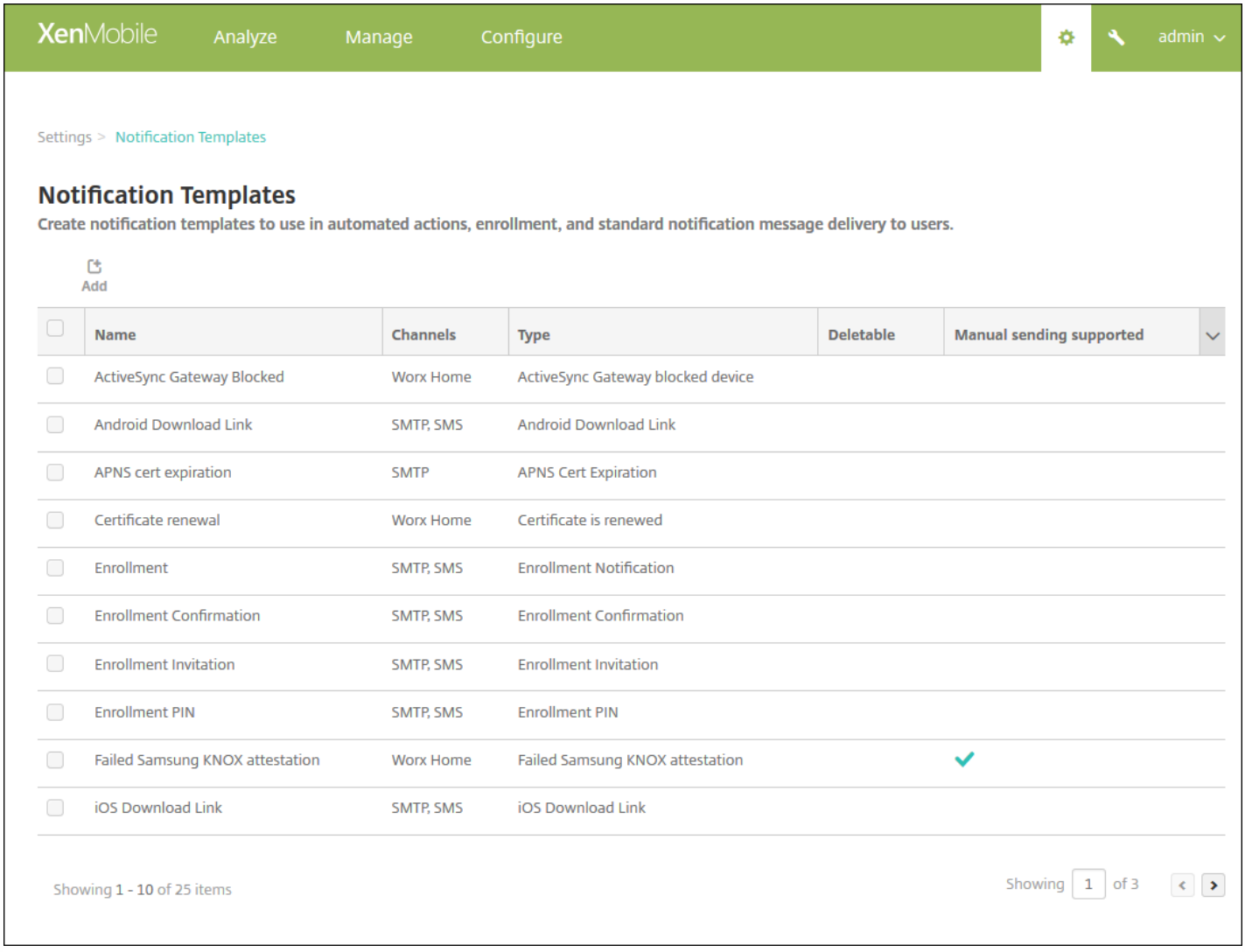
En XenMobile, puede crear o actualizar plantillas de notificaciones que se van a usar en acciones automatizadas, inscripciones y el envío de mensajes de notificación estándar a los usuarios. Puede configurar plantillas de notificaciones para enviar mensajes a través de tres canales diferentes: Worx Home, SMTP o SMS.

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.

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 más información, consulte Notificaciones en XenMobile.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. Haga clic en **Notification Templates**. Aparecerá la página **Notification Templates**.



Para agregar una plantilla de notificación

1. Haga clic en **Add**. 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. Aparecerá la página **Add Notification Template**.

Si elige configurar el servidor SMTP o SMS ahora, se le redirigirá a la página **Notification Server**, en la página **Settings**. Después de configurar los canales que se van a utilizar, puede volver a la página **Notification Template** para continuar agregando o modificando plantillas de notificación.

> ## Important
>
> 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.

2. Configure los siguientes parámetros:

- **Name**. Escriba un nombre descriptivo para la plantilla.
- **Description**. Escriba una descripción para la plantilla.
- **Type**. En la lista, haga clic en el tipo de notificación. Solo se muestran los canales admitidos para el tipo de notificación seleccionado. Solo se permite la plantilla predefinida de caducidad APNS Cert Expiration. Esto significa que no se puede agregar una nueva plantilla de este tipo.

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 utilicen las siguientes macros en los campos Subject o Message:

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

3. En **Channels**, indique 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 **SMTP**, la mayoría de los usuarios deben recibir el mensaje porque se habrán inscrito con sus direcciones de correo electrónico.
- Si elige **SMS**, solo los usuarios con dispositivos dotados de una tarjeta SIM recibirán las notificaciones.

Worx Home:

- **Activate**. Haga clic para habilitar el canal de notificación.
- **Message**. Escriba el mensaje que se enviará al usuario. Este campo es obligatorio si está usando Worx Home.
- **Sound File**. Seleccione el sonido de notificación que oirá el usuario cuando reciba la notificación.

SMTP:

- **Activate**. Haga clic para habilitar el canal de notificación.

Importante: Solo se puede activar la notificación de SMTP si ya se ha configurado el servidor SMTP.

- **Sender**. Escriba un remitente optativo para la notificación, que puede consistir en un nombre, una dirección de correo electrónico o ambos.
- **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.
- **Subject**. Escriba un asunto descriptivo para la notificación. Este campo es obligatorio.
- **Message**. Escriba el mensaje que se enviará al usuario.

SMS:

- **Activate**. Haga clic para habilitar el canal de notificación.

Importante: Solo se puede activar la notificación de SMS si ya se ha configurado una puerta de enlace SMS.

- **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 SMS. 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**.
- **Message**. Escriba el mensaje que se enviará al usuario. Este campo es obligatorio.

5. Haga clic en **Add**. 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.

Para modificar una plantilla de notificación

1. Seleccione una plantilla de notificaciones. Aparecerá la página de modificación de la plantilla en cuestión. En ella, podrá realizar cambios a todos los campos salvo a **Type**; tampoco podrá activar ni desactivar canales.

2. Haga clic en **Save**.

Para eliminar una plantilla de notificación

Nota: Solo puede eliminar las plantillas de notificación que haya agregado; no puede eliminar plantillas de notificación predeterminadas.

1. Seleccione una plantilla de notificación existente.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.

3. Haga clic en **Delete** para eliminar la plantilla de notificación o en **Cancel** para no eliminarla.

Administración de grupos de entrega

Jul 27, 2016

La configuración y la administración de dispositivos suele implicar la creación de recursos (directivas y aplicaciones) y acciones en la consola de XenMobile y, posteriormente, su empaquetado mediante grupos de entrega. El orden en que XenMobile envía los recursos y las acciones de un grupo de entrega a los dispositivos se conoce como *orden de implementación*. Este artículo describe cómo agregar, administrar e implementar grupos de entrega; cómo cambiar el orden de implementación de los recursos y las acciones de los grupos de entrega; y cómo determina XenMobile el orden de implementación cuando un usuario está incluido en varios grupos de entrega que tienen directivas duplicadas o en conflicto.

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, y tabletas Windows 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.

Orden de implementación

El orden de implementación es la secuencia con la que XenMobile envia recursos a los dispositivos. El orden de implementación solo se admite en el modo MDM.

Al determinar el orden de implementación, XenMobile aplica filtros y criterios de control, tales como las reglas de implementación y la programación de la implementación, en las directivas, las aplicaciones, las acciones y los grupos de entrega. Antes de agregar grupos de entrega, tenga en cuenta la información de esta sección que pueda ser relevante para los objetivos de su implementación.

Est es un resumen de los conceptos principales relacionados con el orden de implementación:

- **Orden de implementación:** La secuencia en la que XenMobile transfiere los recursos (directivas y aplicaciones) y las acciones a un dispositivo. El orden de implementación de algunas directivas, tales como Terms and Conditions y Software Inventory, no tiene ningún efecto en otros recursos. El orden en el que se implementan las acciones no tiene ningún efecto en otros recursos, por lo que su posición se ignora cuando XenMobile implementa los recursos.
- **Reglas de implementación:** XenMobile utiliza las reglas de implementación que se especifican para las propiedades de los dispositivos con el fin de filtrar las directivas, las aplicaciones, las acciones y los grupos de entrega. Por ejemplo, una regla de implementación puede especificar que debe enviarse el paquete de implementación cuando el nombre de dominio coincida con un valor determinado.

- **Programación de la implementación:** XenMobile utiliza la programación de la implementación especificada para acciones, aplicaciones y directivas de dispositivo con el fin de controla 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 siguiente tabla muestra estos y otros criterios que se pueden asociar con objetos específicos o recursos para filtrarlos o controlar su implementación.

Objeto/Recurso	Criterios de control/filtro
Directiva de dispositivo	Plataforma del dispositivo Regla de implementación (basada en las propiedades del dispositivo) Programación de la implementación
Aplicación	Plataforma del dispositivo Regla de implementación (basada en las propiedades del dispositivo) Programación de la implementación
Acción	Regla de implementación (basada en las propiedades del dispositivo) Programación de la implementación
Grupo de entrega	Usuario/Grupos Regla de implementación (basada en las propiedades del dispositivo)

Es muy probable que, en un entorno típico, varios grupos de entrega queden asignados a un mismo usuario, y estos son los resultados posibles:

- Pueden existir objetos duplicados dentro de los grupos de entrega.
- Una misma directiva está configurada de distinta forma en grupos de entrega diferentes asignados a un mismo usuario.

Cuando ocurre alguna de estas circunstancias, XenMobile calcula un orden de implementación para todos los objetos que debe entregar a un dispositivo o sobre los que debe realizar alguna acción. Los pasos para realizar este cálculo son independientes de la plataforma del dispositivo.

Pasos para el cálculo:

1. Identificar todos los grupos de entrega de un usuario específico, en función de los filtros de usuario/grupos y las reglas de implementación.
2. Crear una lista ordenada de todos los recursos (directivas, acciones y aplicaciones) de los grupos de entrega seleccionados, en función de los filtros de plataforma de dispositivo, reglas de implementación y programación de la implementación. El algoritmo para ordernarlos es la siguiente:

a. Colocar los recursos de los grupos de entrega que tengan una orden de implementación definida por el usuario por delante de aquellos que no la tengan. La razón para hacer esto se describe después de los pasos.

b. En caso de haber dos grupos de entrega en las mismas circunstancias, ordenar los recursos de los grupos de entrega por nombre de grupo. Por ejemplo, se colocan los recursos del grupo de entrega A por delante de los del grupo de entrega B.

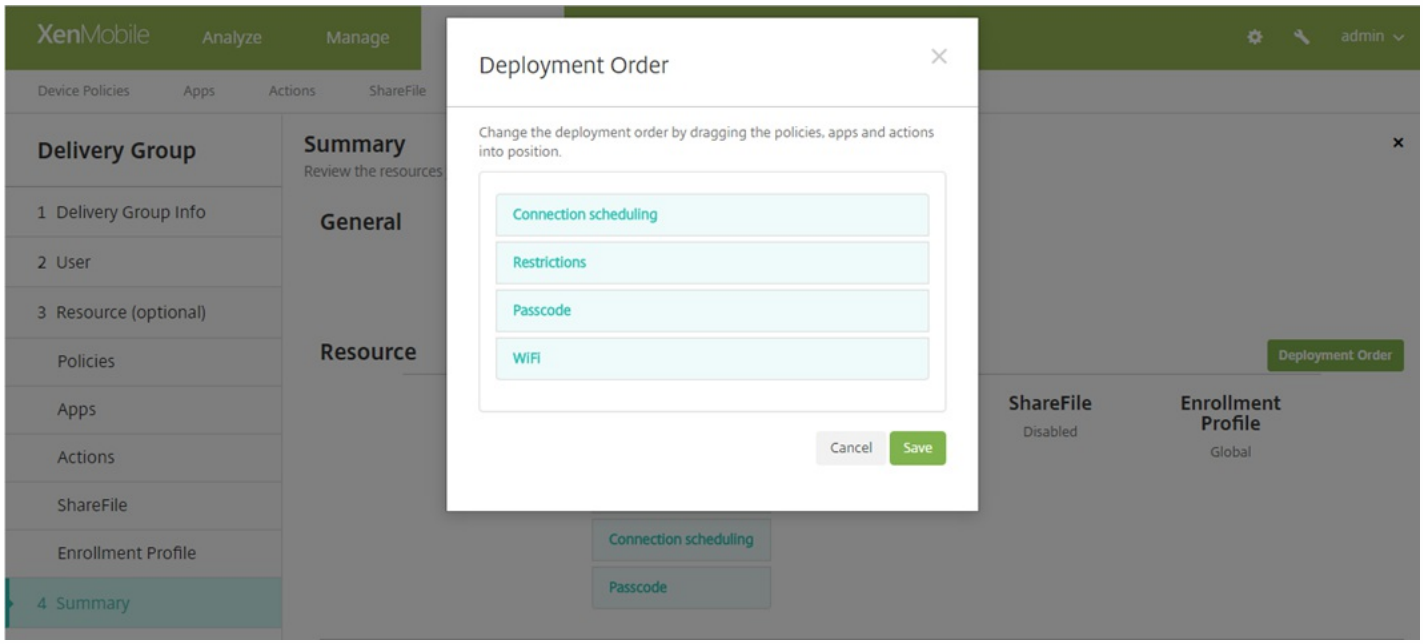
c. Durante el proceso de ordenamiento, si hay una orden de implementación especificada para los recursos de un grupo de entrega, se mantiene ese orden. Si no la hay, los recursos del grupo de entrega se ordenan por nombre de recurso.

d. Si el mismo recurso aparece más de una vez, quitar el recurso duplicado.

Los recursos que tienen un orden definido por el usuario asociado con ellos se implementan antes de los recursos que no tienen un orden definido por el usuario. Un recurso puede existir en varios grupos de entrega asignados al usuario. Tal como se indica en los pasos anteriores, el algoritmo de cálculo elimina recursos duplicados y solo entrega el primer recurso de la lista. Quitando los recursos duplicados de ese modo, XenMobile aplica el orden definido por el administrador de XenMobile.

Por ejemplo, suponga que tiene dos grupos de entrega de la siguiente manera:

- Grupo de entrega, Gestores de cuentas 1: Con un orden no especificado (**unspecified**) para los recursos; contiene las directivas **WiFi** y **Passcode**.
- Grupo de entrega, Gestores de cuentas 2: Con un orden especificado (**specified**) para los recursos; contiene las directivas **Connection scheduling**, **Restrictions**, **Passcode** y **WiFi**. En este caso, se desea entregar la directiva **Passcode** antes que la directiva **WiFi**.



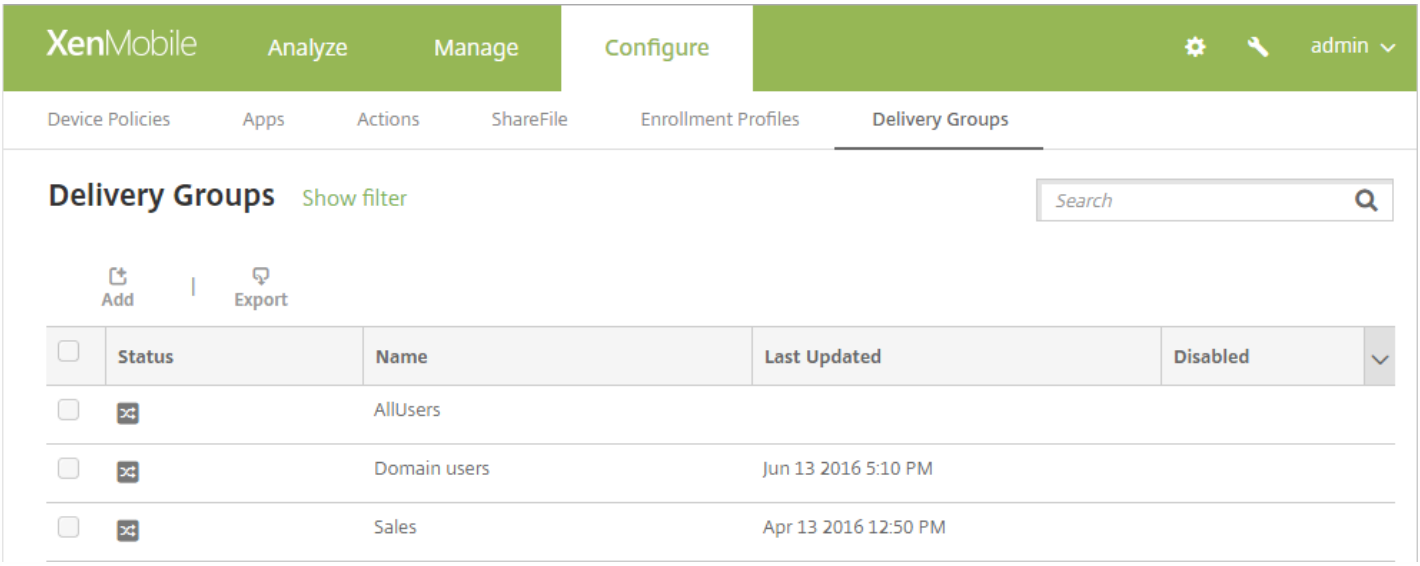
Si el algoritmo de cálculo ordena los grupos de implementación solo por nombre, XenMobile realizaría la implementación en este orden, empezando con el grupo de entrega Gestores de cuentas 1: **WiFi**, **Passcode**, **Connection scheduling** y **Restrictions**. XenMobile omitiría **Passcode** y **WiFi**, por ser duplicados, del grupo de entrega Gestores de cuentas 2.

Sin embargo, debido a que el grupo Gestores de cuentas 2 tiene un orden de implementación especificado por el

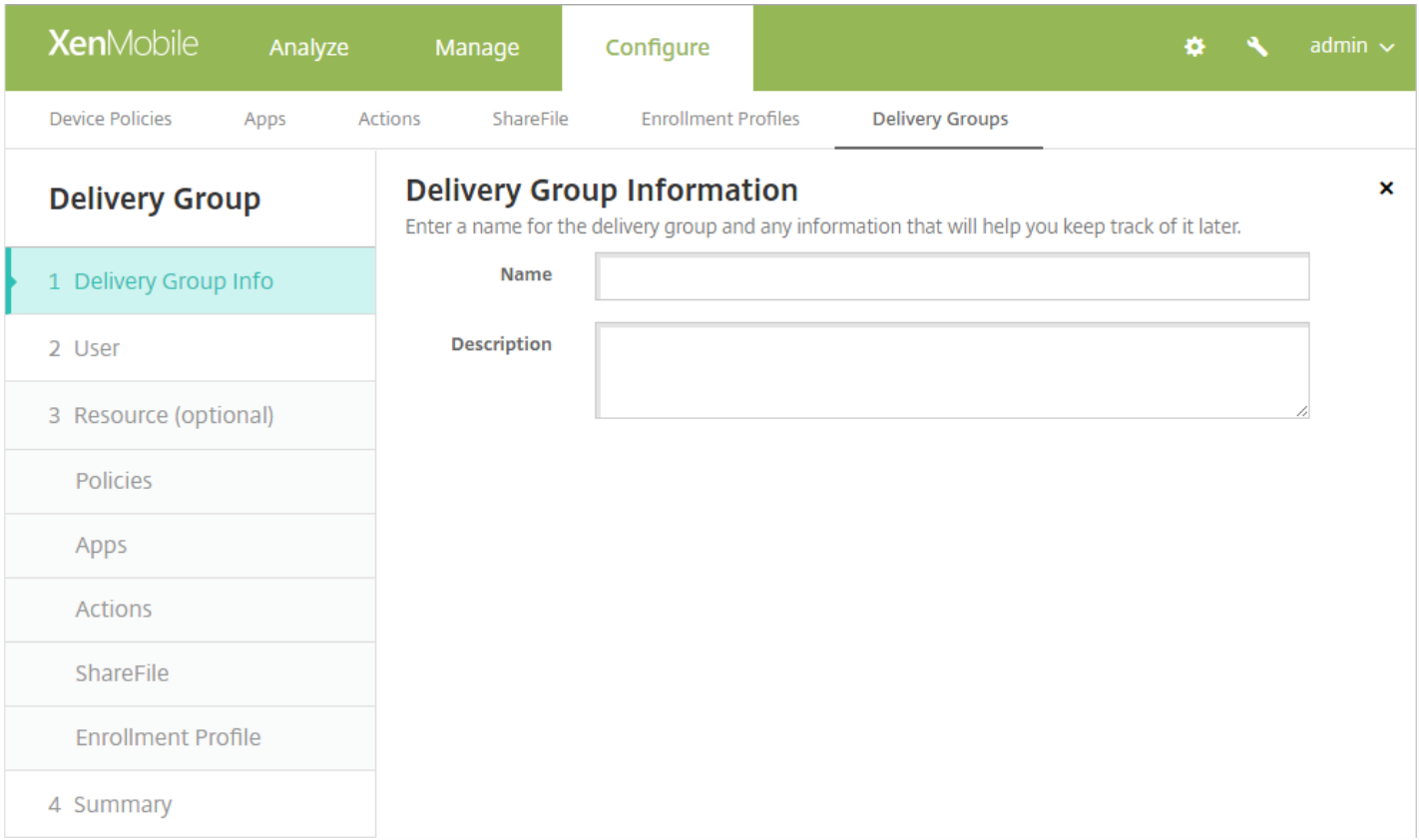
administrador, el algoritmo de cálculo coloca los recursos del grupo de entrega Gestores de cuentas 2 por encima de los recursos del grupo de entrega Gestores de cuentas 1 en la lista. Como resultado de ello, XenMobile implementa las directivas en este orden: **Connection scheduling**, **Restrictions**, **Passcode** y **WiFi**. XenMobile omite las directivas **WiFi** y **Passcode** del grupo de entrega Gestores de cuentas 1, por ser duplicados. El algoritmo, por lo tanto, respeta el orden especificado por el administrador de XenMobile.

Para agregar un grupo de entrega

1. En la consola de XenMobile, haga clic en **Configure > Delivery Groups**. Aparecerá la página **Delivery Groups** .



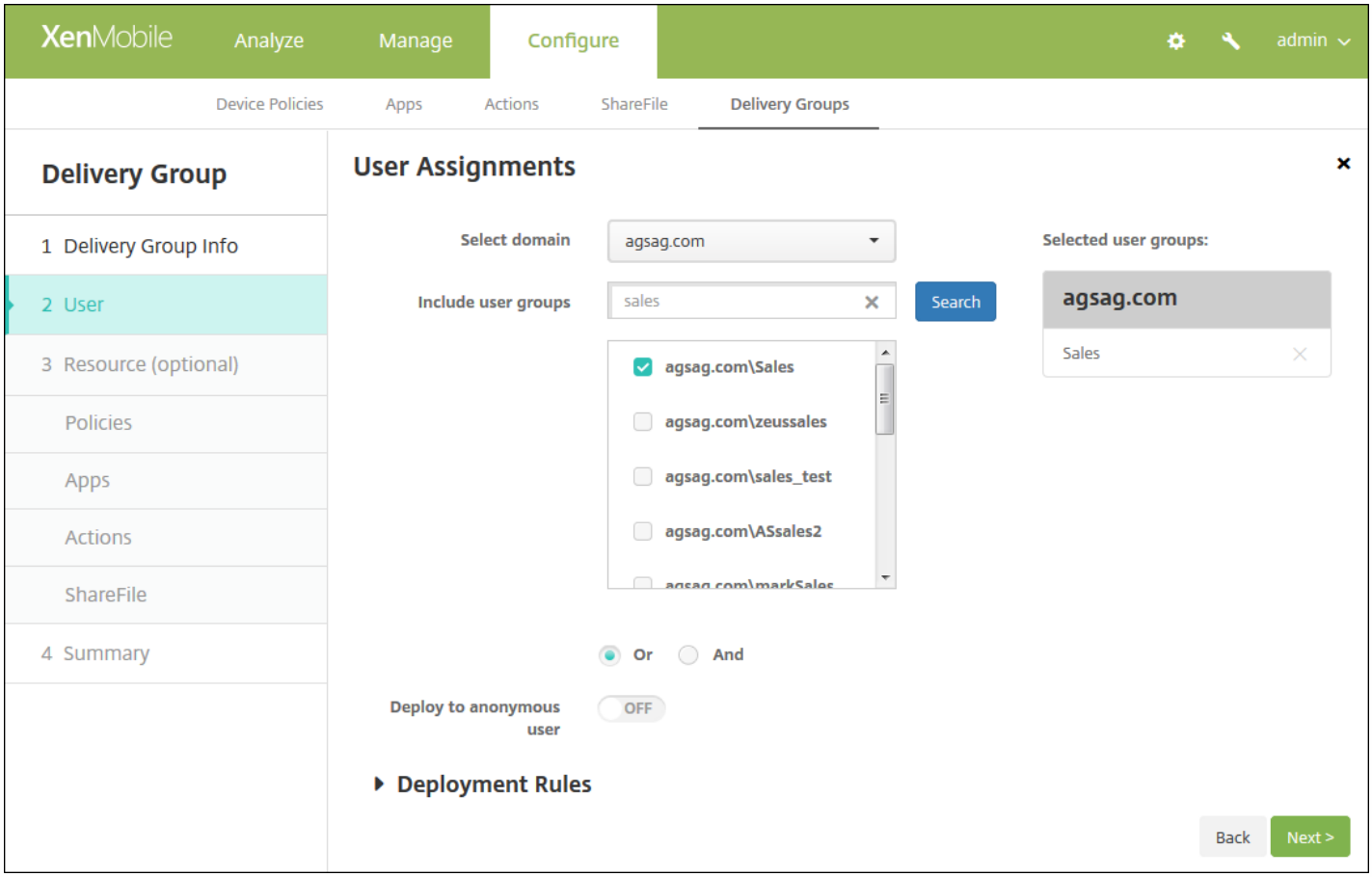
2. En la página **Delivery Groups** , haga clic en **Add**. Aparecerá la página **Delivery Group Information** .



3. En la página **Delivery Group Information** , introduzca la información siguiente:

- **Name**. Indique un nombre descriptivo para el grupo de entrega.
- **Description**. Escriba, si quiere, una descripción del grupo de entrega.

4. Haga clic en **Next**. Aparecerá la página **User Assignments** .



5. Configure los siguientes parámetros:

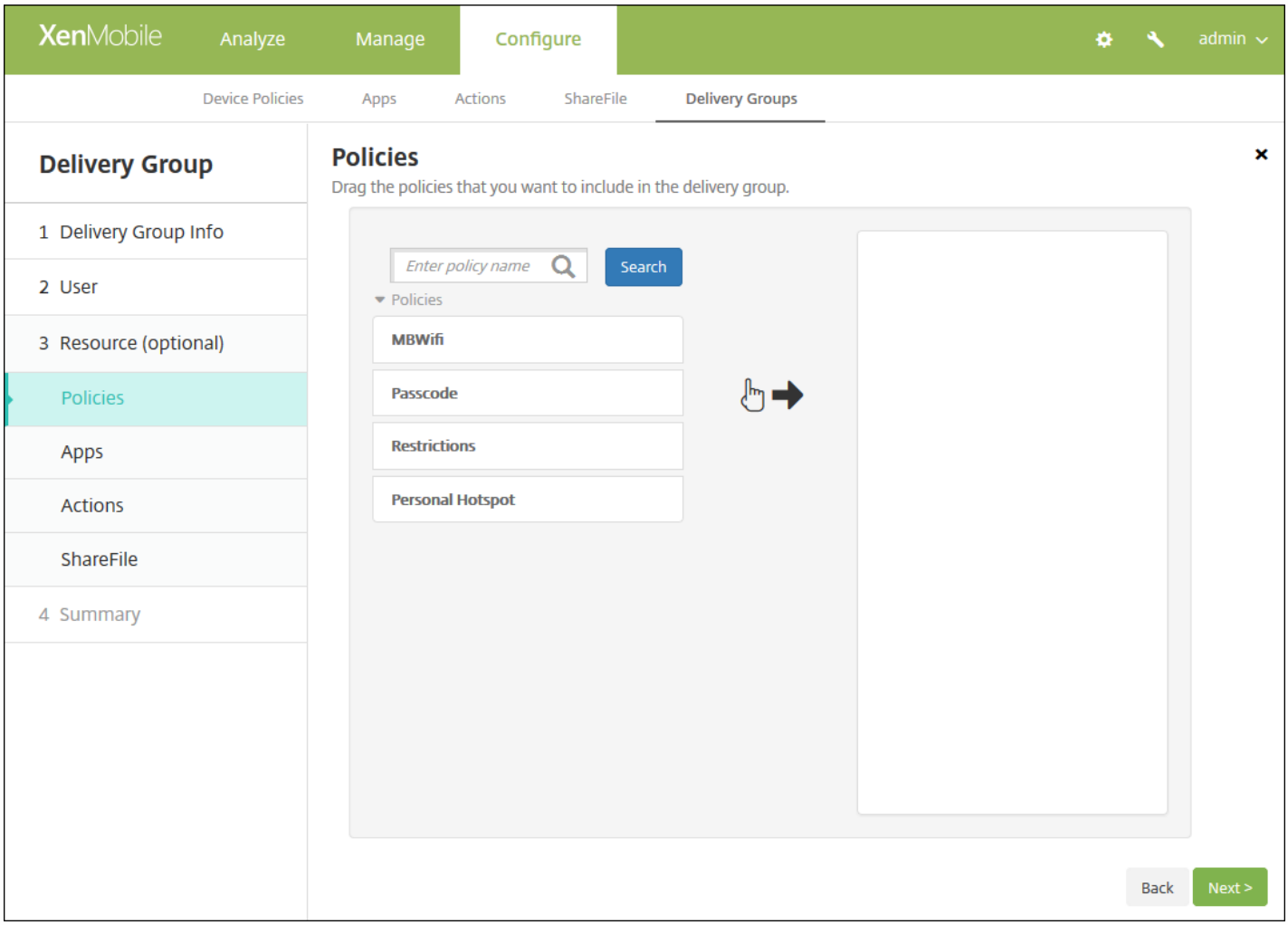
- **Select domain**. En la lista, seleccione el dominio del que se elegirá a los usuarios.
- **Include user groups**. Realice una de las siguientes acciones:
  - En la lista de grupos de usuarios, haga clic en los grupos que desee agregar. Los grupos seleccionados aparecen en la lista **Selected user groups** .
  - 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.
    - Para quitar un grupo de usuarios de la lista **Selected user groups**, realice una de las siguientes acciones:
      - En la lista **Selected user groups** , haga clic en la **X** junto a cada uno de los grupos que quiera quitar.
      - Haga clic en **Search** para ver una lista de todos los grupos de usuarios en el dominio seleccionado. Desplácese por la lista y deje sin marcar las casillas de los grupos que quiera quitar.
      - 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. Desplácese por la lista y desmarque la casilla de cada grupo que quiera quitar.
- **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 a ellos.
- **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.

Para agregar recursos opcionales a grupos de entrega

Puede agregar recursos opcionales a grupos de entrega con el fin de aplicar directivas específicas, proporcionar aplicaciones obligatorias y opcionales, agregar acciones automatizadas y habilitar ShareFile para el inicio Single Sign-On en contenido y datos. En los siguientes apartados, se describe cómo agregar directivas, aplicaciones y acciones, y cómo habilitar ShareFile. Puede agregar cualquiera, todos o ninguno de estos recursos al grupo de entrega. Para omitir el paso de agregar un recurso, haga clic en el recurso que quiera agregar o haga clic en **Summary**.

Incorporación de directivas



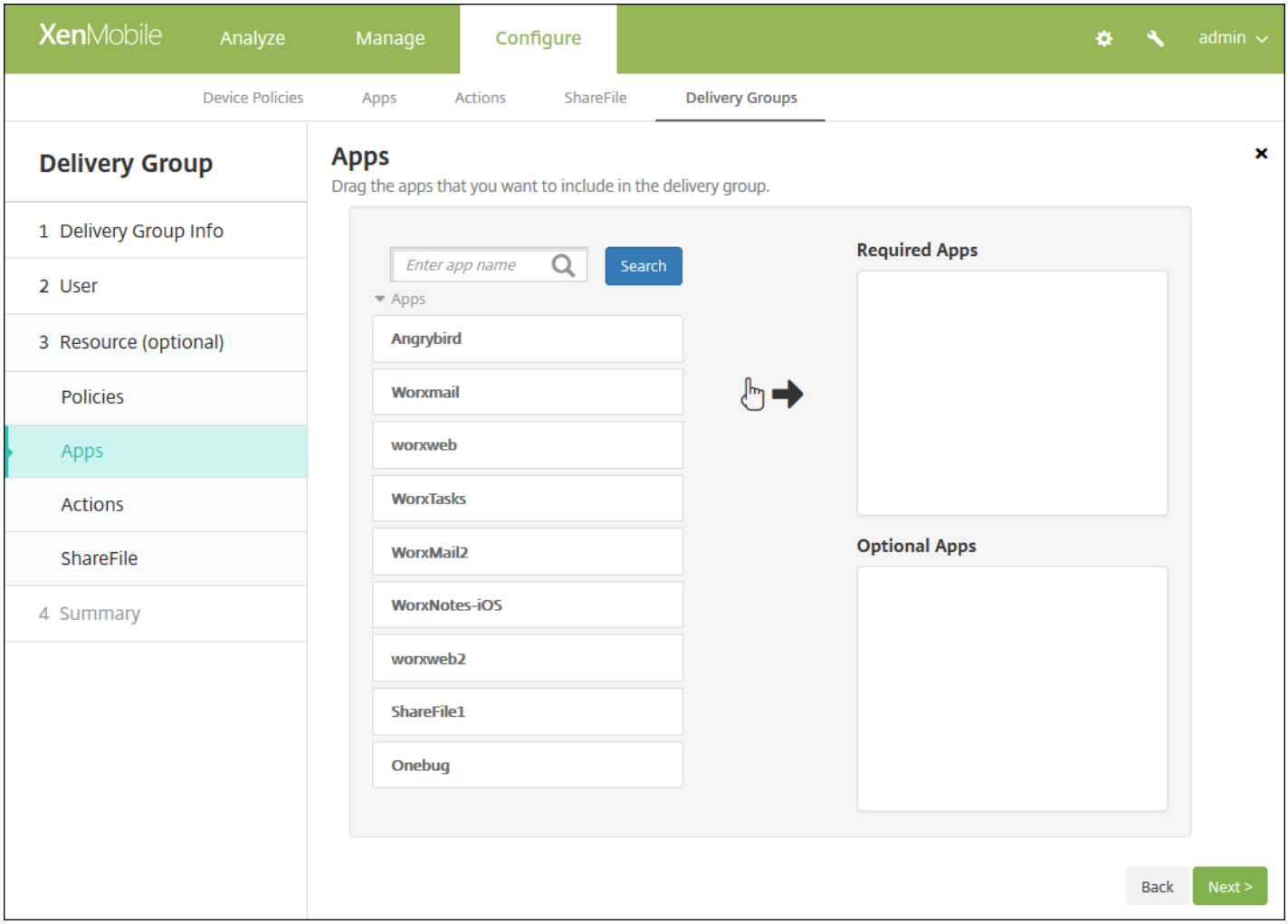
1. Para cada directiva que quiera agregar, lleve a cabo lo siguiente:

- Busque la directiva que quiera agregar en la lista de las directivas disponibles.
- O bien, para limitar la cantidad de directivas de la lista, escriba el nombre completo o parcial de la directiva en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la directiva que quiera agregar y arrástrela al cuadro de la derecha.

Nota: Para quitar una directiva, haga clic en la **X** situada junto al nombre de esa directiva en el cuadro de la derecha.

2. Haga clic en **Next**. Aparecerá la página **Apps**.

Incorporación de aplicaciones



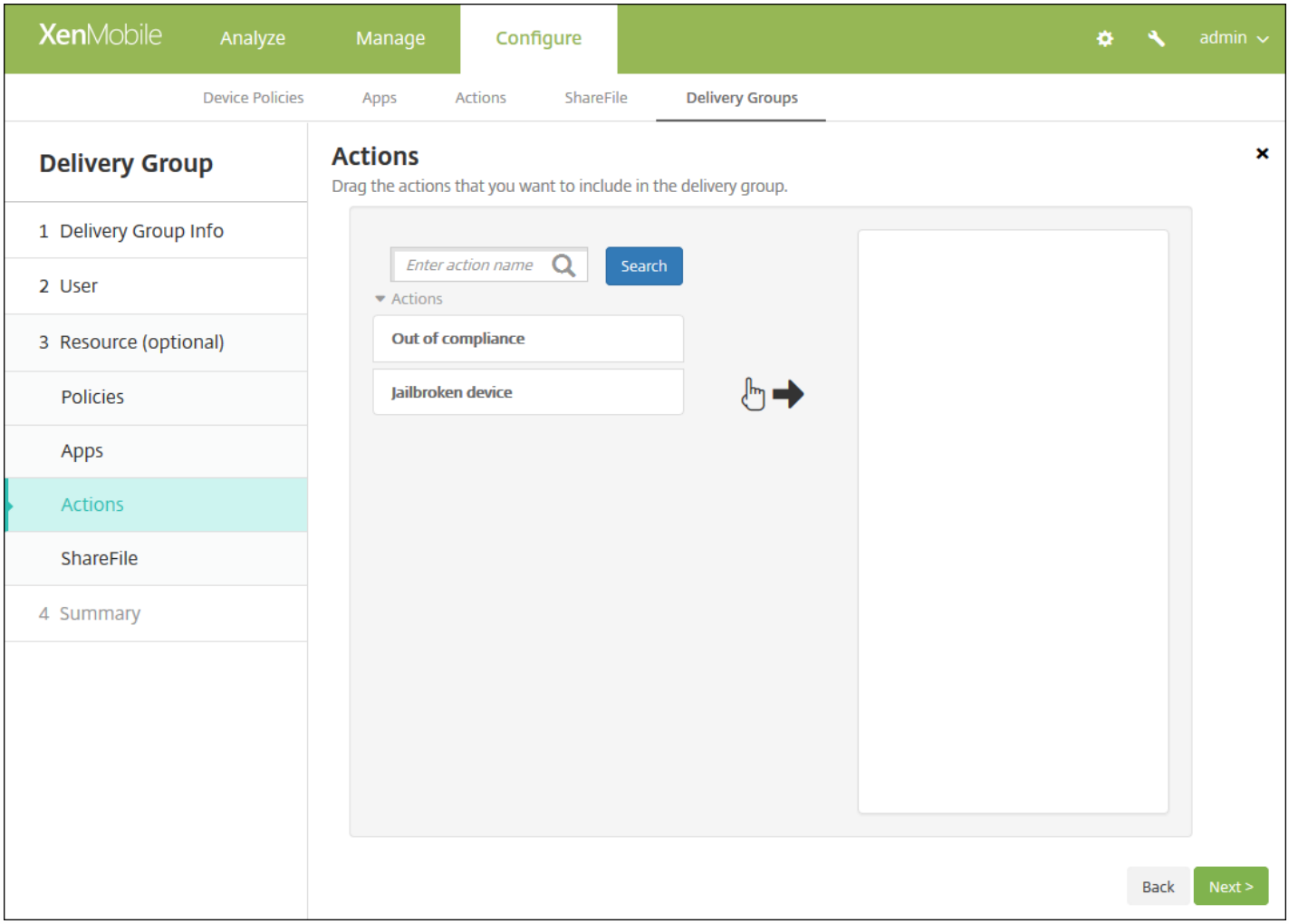
1. Para cada aplicación que quiera agregar, lleve a cabo lo siguiente:

- Busque la aplicación que quiera agregar en la lista de las aplicaciones disponibles.
- O bien, para limitar la cantidad de aplicaciones de la lista, escriba el nombre completo o parcial de la aplicación en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la aplicación que quiera agregar y arrástrela al cuadro **Required Apps** o al cuadro **Optional Apps**.

Nota: Para quitar una aplicación, haga clic en la **X** situada junto al nombre de esa aplicación en el cuadro de la derecha.

2. Haga clic en **Next**. Aparecerá la página **Actions**.

Incorporación de acciones



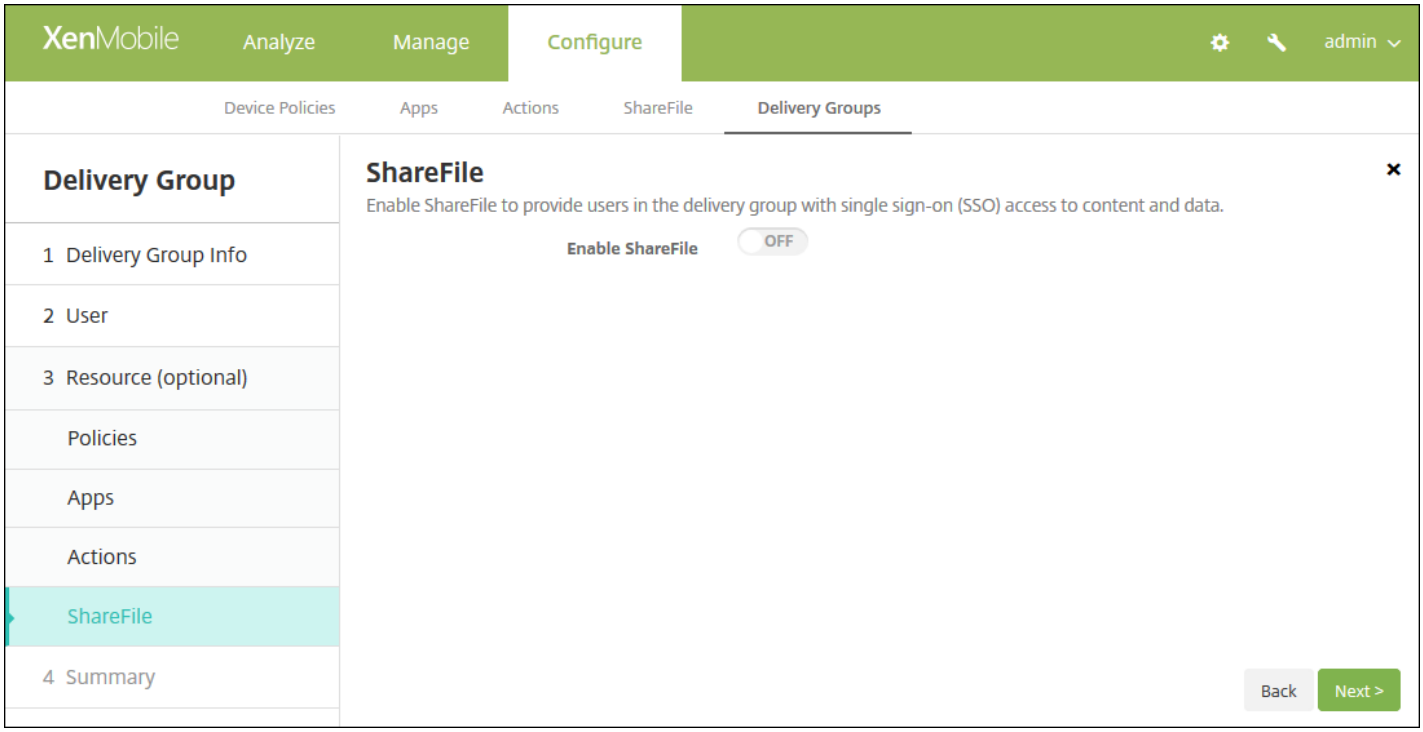
1. Para cada acción que quiera agregar, haga lo siguiente:

- Busque la acción que quiera agregar en la lista de las acciones disponibles.
- O bien, para limitar la cantidad de acciones de la lista, escriba el nombre completo o parcial de la acción en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la acción que quiera agregar y arrástrela al cuadro de la derecha.

Nota: Para quitar una acción, haga clic en la **X** situada junto al nombre de esa acción en el cuadro de la derecha.

2. Haga clic en **Next**. Aparecerá la página **ShareFile**.

Habilitar ShareFile

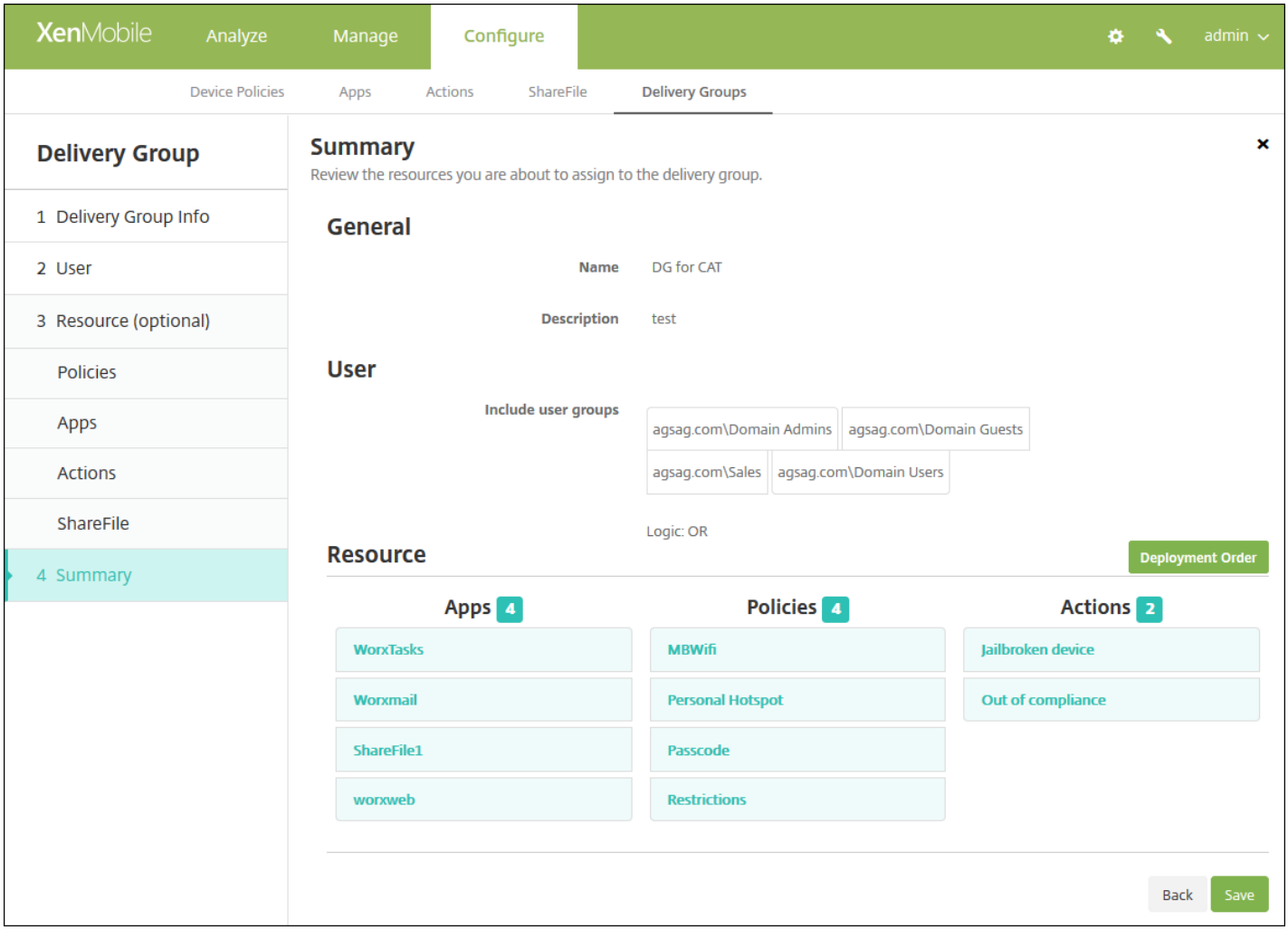


1. Configure este parámetro:

- **Enable ShareFile**. Haga clic en **ON** para habilitar el acceso Single Sign-On de ShareFile a contenido y datos.

2. Haga clic en **Next**. Aparece la página **Summary**.

Revisión de las opciones configuradas y cambio del orden de implementación



En la página **Summary**, puede revisar las opciones que haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos. La página Summary muestra los recursos por categoría; no refleja el orden de implementación.

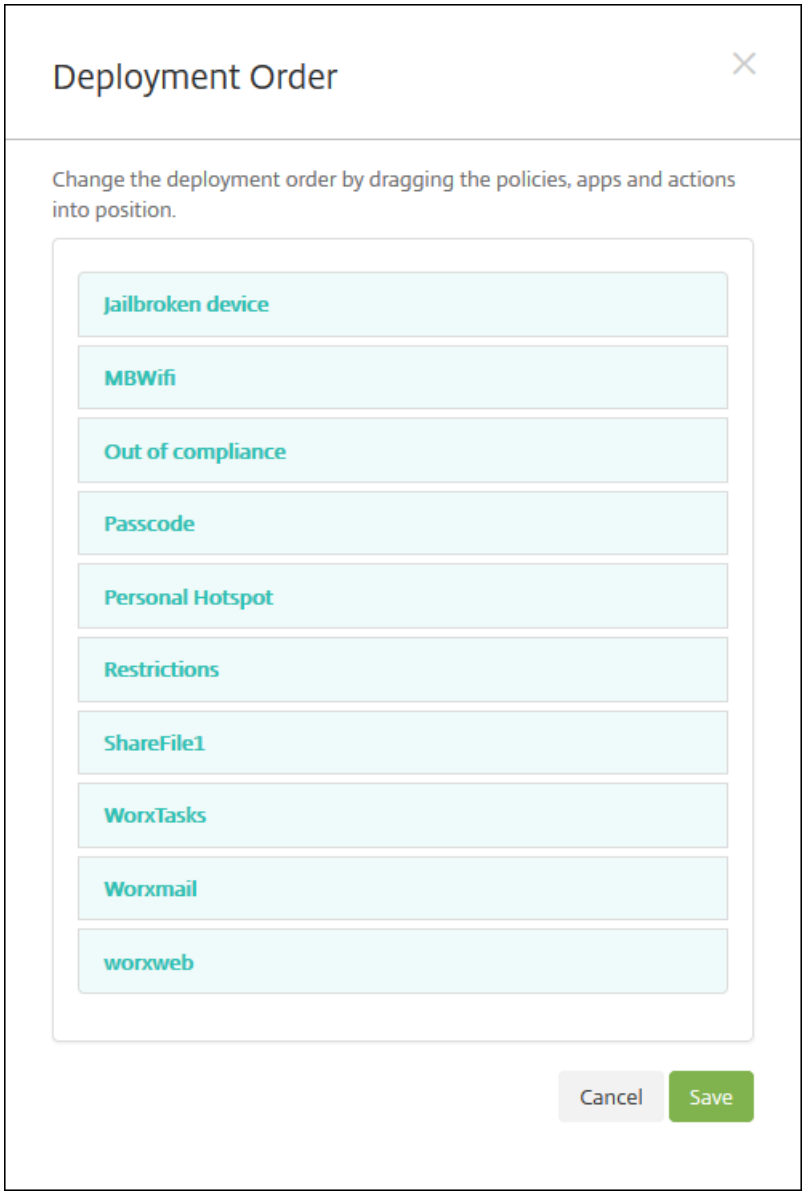
1. Haga clic en **Back** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.

2. Haga clic en **Deployment Order** para ver el orden de implementación o para cambiarlo.

3. Haga clic en **Save** para guardar el grupo de entrega.

Para cambiar el orden de implementación

1. Haga clic en el botón **Deployment Order**. Aparecerá el cuadro de diálogo **Deployment Order**.



2. Haga clic en un recurso y arrástrelo a la ubicación desde donde quiere implementarlo. Después de cambiar el orden de implementación, XenMobile implementa los recursos de la lista de arriba a abajo.

3. Haga clic en **Save** para guardar el orden de implementación.

Para modificar un grupo de entrega

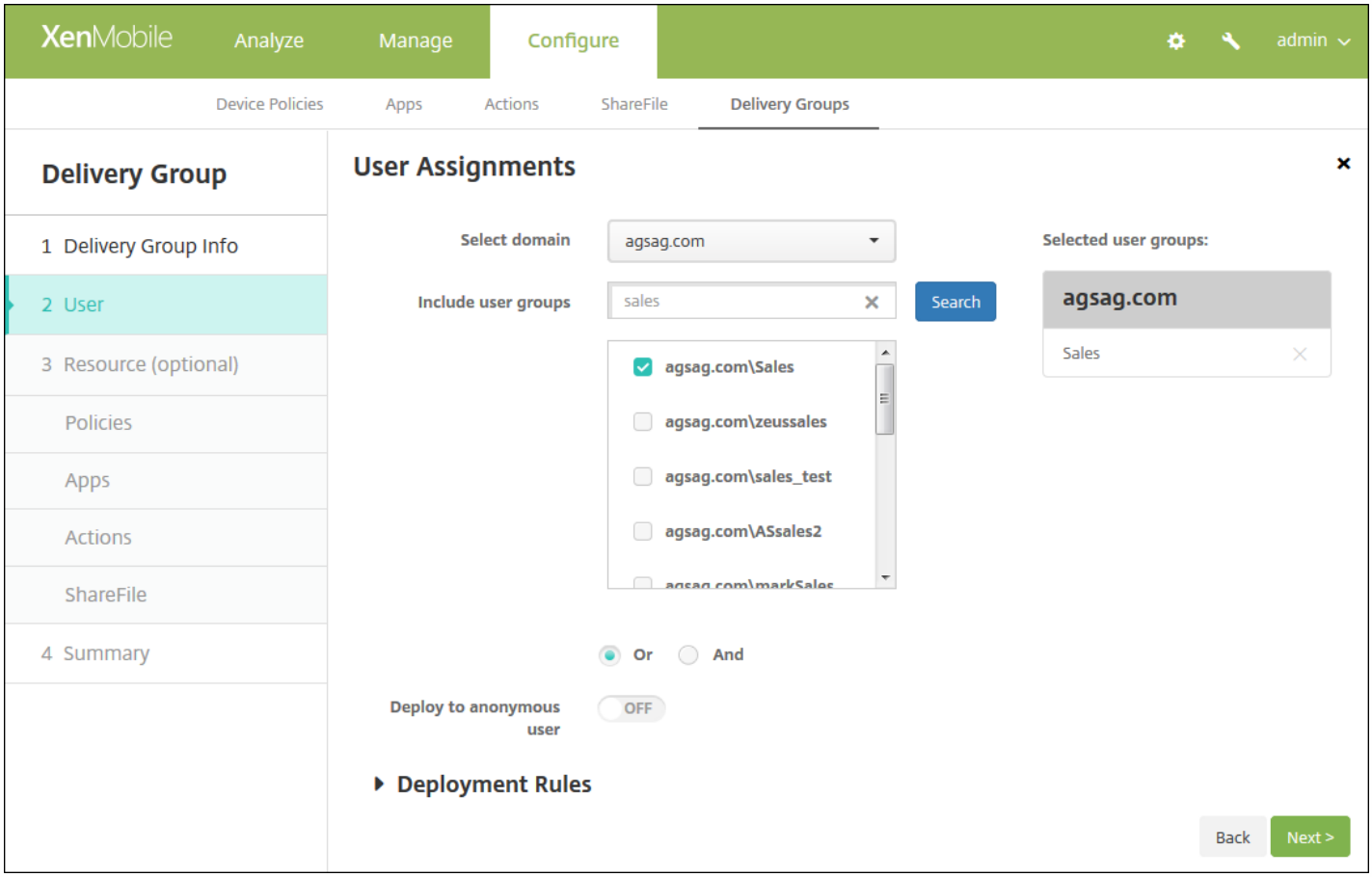
En la página **Delivery Groups**, seleccione el grupo de entrega que quiera modificar. Puede seleccionarlo de dos maneras: marcando la casilla de verificación que aparece junto a su nombre o haciendo clic en la línea que contiene su nombre. y luego en **Edit**. Aparecerá la página para modificar la información de grupos de entrega **Delivery Group Information**.

> **Nota**
>
> Según cómo haya seleccionado el grupo de entrega, el comando **Edit** aparece encima o a la derecha del grupo de entrega.

2. Agregue o cambie el campo **Description**.

Nota: No se puede cambiar el nombre de un grupo existente.

3. Haga clic en **Next**. Aparecerá la página **User Assignments**.



4. En el panel **Select User Groups**, escriba o cambie la información siguiente:

- **Select domain**. En la lista, seleccione el dominio del que se elegirán los usuarios.
- **Include user groups**. Realice una de las siguientes acciones:
  - En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista **Selected user groups**.
  - 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.

    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.

- **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.
- **Deploy to anonymous user**. Seleccione si implementar recursos para los 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.

5. Expanda **Deployment Rules** y, a continuación, configure los parámetros como hizo en el paso 5 de este procedimiento.

6. Haga clic en **Next**. 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.

7. Cuando termine de modificar un recurso, haga clic en **Next**, o bien, en **Delivery Group**, haga clic en **Summary**.

8. En la página **Summary**, puede revisar las opciones que haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos.

9. Haga clic en **Back** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.

10. Haga clic en **Deployment Order** para reorganizar el orden de implementación de los recursos; para obtener más información sobre cómo cambiar el orden de implementación, consulte Para cambiar el orden de implementación.

11. Haga clic en **Save** para guardar el grupo de entrega.

Para habilitar e inhabilitar el grupo de entrega AllUsers

> **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 a **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 la etiqueta **Disabled** bajo el encabezado **Disabled** en la tabla de grupos 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 la etiqueta **Disabled** del encabezado **Disabled** de la tabla de grupos de entrega.

Para implementar en grupos de entrega

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS, Windows Phone y Windows Tablet que pertenezcan a ese grupo de entrega para que se vuelvan a conectar a XenMobile. De esta manera, puede volver a evaluar los dispositivos e implementar aplicaciones, directivas y acciones. Los usuarios de dispositivos de otras plataformas reciben los recursos inmediatamente si ya están conectados; o, en función de la directiva de programación, la próxima vez que se conecten.

Nota: Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de Worx Store 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.

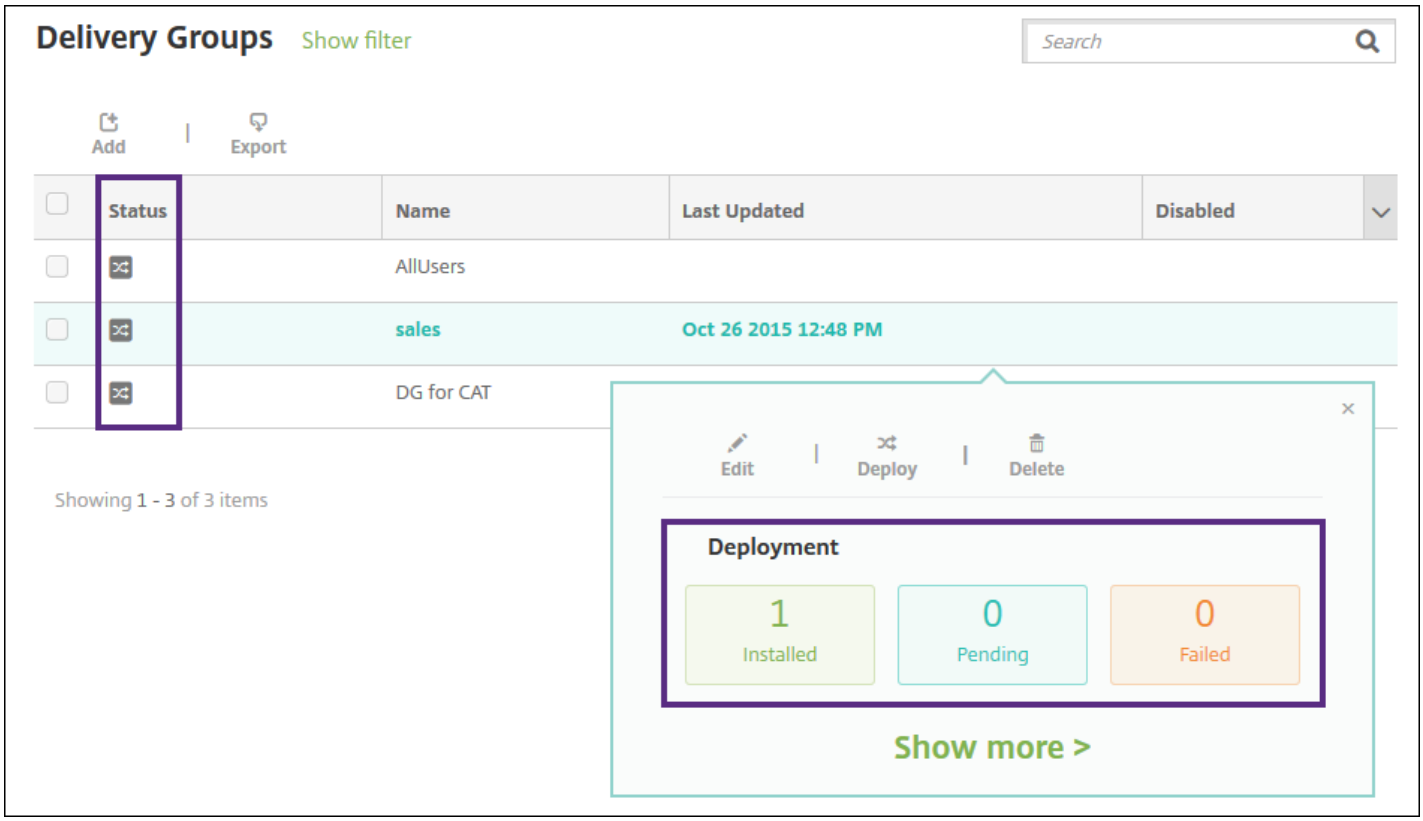
2. Haga clic en **Deploy**.

Nota: Según cómo seleccione el grupo de entrega, el comando **Deploy** aparecerá encima o a la derecha del grupo de entrega.

Compruebe que los grupos en los que desea implementar aplicaciones, directivas y acciones aparezcan enumerados 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 dispositivo y la directiva de programación.

Puede comprobar el estado de la implementación en la página **Delivery Groups** de alguna de las siguientes maneras:

- Mire el icono de implementación, en el encabezado **Status** del grupo de entrega, que indicará si ha habido algún error en la implementación.
- Haga clic en la línea que contiene el grupo de entrega para mostrar una etiqueta superpuesta donde se indica si la implementación fue instalada (**Installed**), está pendiente (**Pending**) o falló (**Failed**).



Para eliminar grupos de entrega

> **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**. Aparecerá el cuadro de diálogo **Delete**.

Nota: Según cómo seleccione el grupo de entrega, el comando **Delete** aparecerá encima o a la derecha del grupo de entrega.

3. Haga clic en **Delete**.

> **Important**
>
> No se puede deshacer esta acción.

Para exportar la tabla de grupos de entrega

1. Haga clic en el botón **Export** situado encima de la tabla **Delivery Groups**. XenMobile extrae la información de la tabla **Delivery Groups** y la convierte a un archivo CSV.

2. Abra o guarde el archivo CSV. El modo de hacer esto dependerá del explorador Web que se esté utilizando. También puede cancelar la operación.

Inscripción de usuarios y dispositivos

Aug 25, 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 y el usuario debe haberse autenticado. Entonces, se instalan ambos, XenMobile y el perfil del usuario. 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.

Nota: Antes de poder inscribir usuarios de dispositivos iOS, debe solicitar un certificado APNs. 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

Jul 27, 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. Deberá introducir su PIN de Worx dos veces. 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. Worx Home se abre. En ese momento, puede acceder a Worx Store para ver las aplicaciones que puede instalar en el dispositivo Android.
9. 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.

Para desinscribir y volver a inscribir un dispositivo Android

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

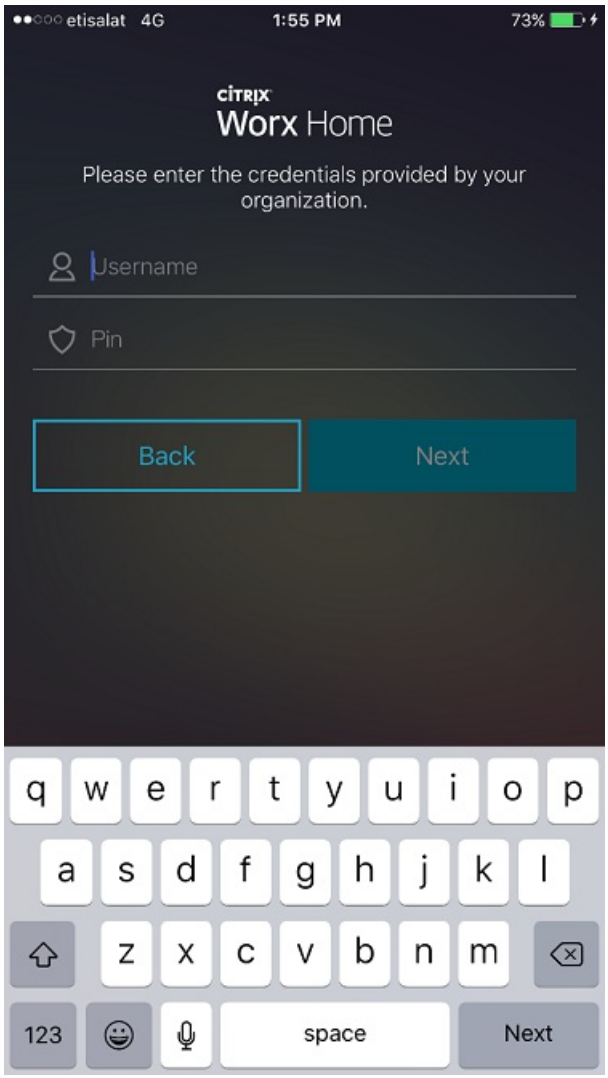
Jul 27, 2016

1. Descargue la aplicación Worx Home desde el App Store de Apple, iTunes, al dispositivo y, a continuación, instale la aplicación en el dispositivo.

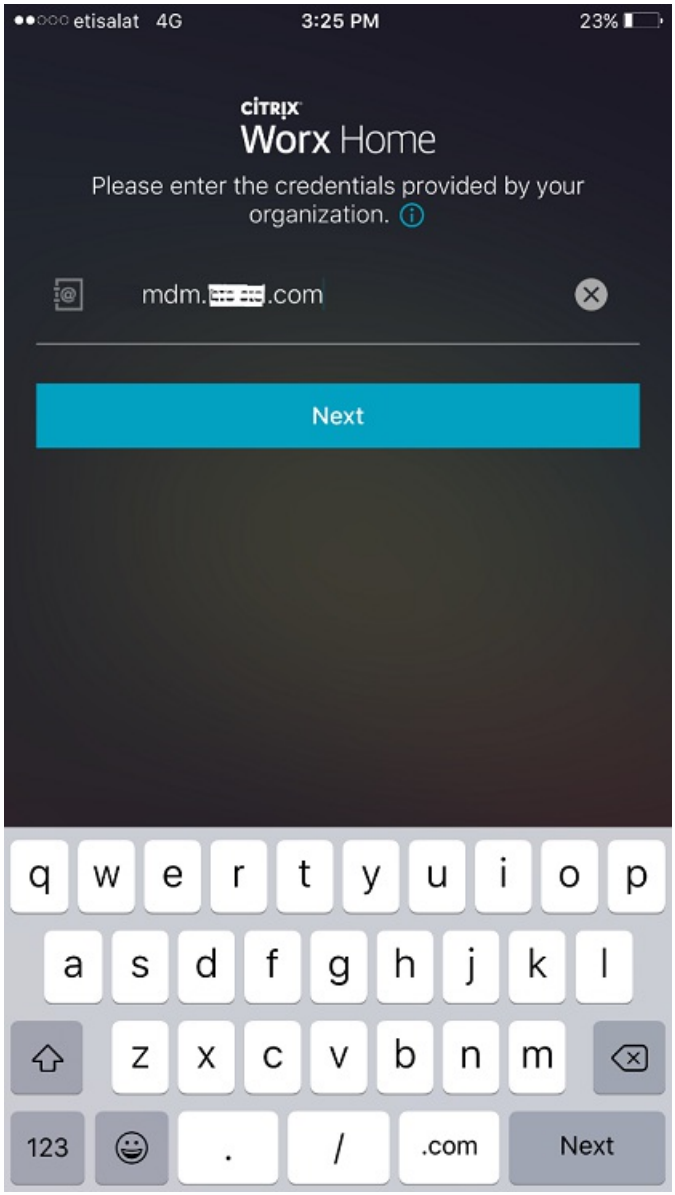
En la pantalla de inicio del dispositivo iOS, toque la aplicación Worx Home.

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**.

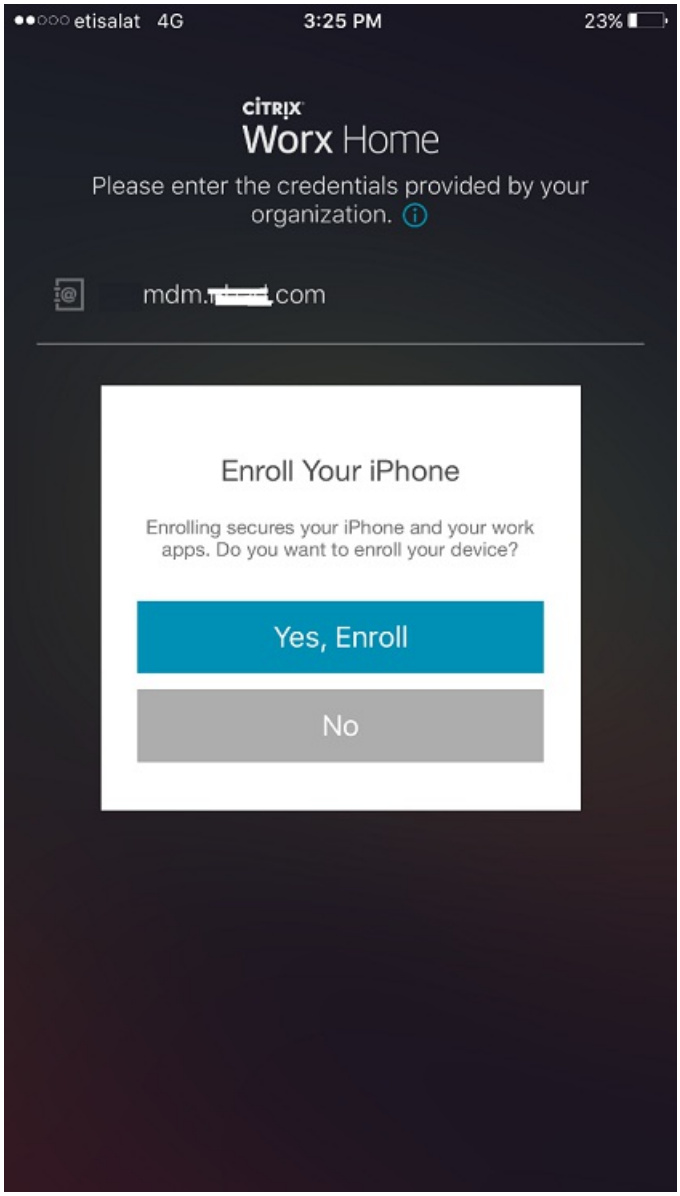
Las pantallas mostradas pueden ser distintas de estos ejemplos, en función de cómo esté configurado XenMobile.

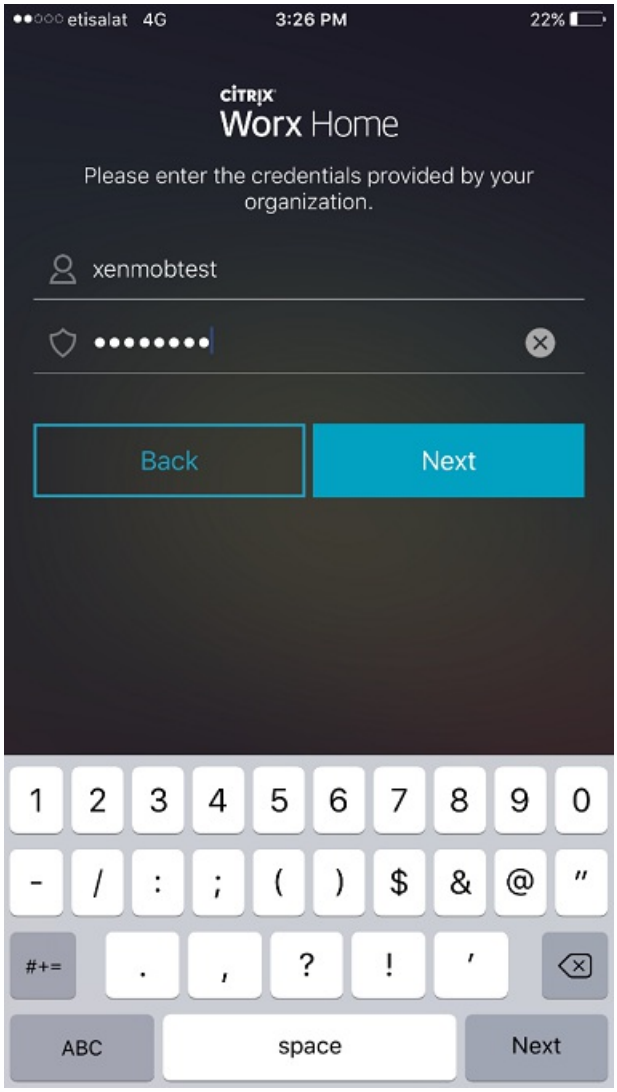


4. Especifique la dirección suministrada por su servicio de asistencia técnica.



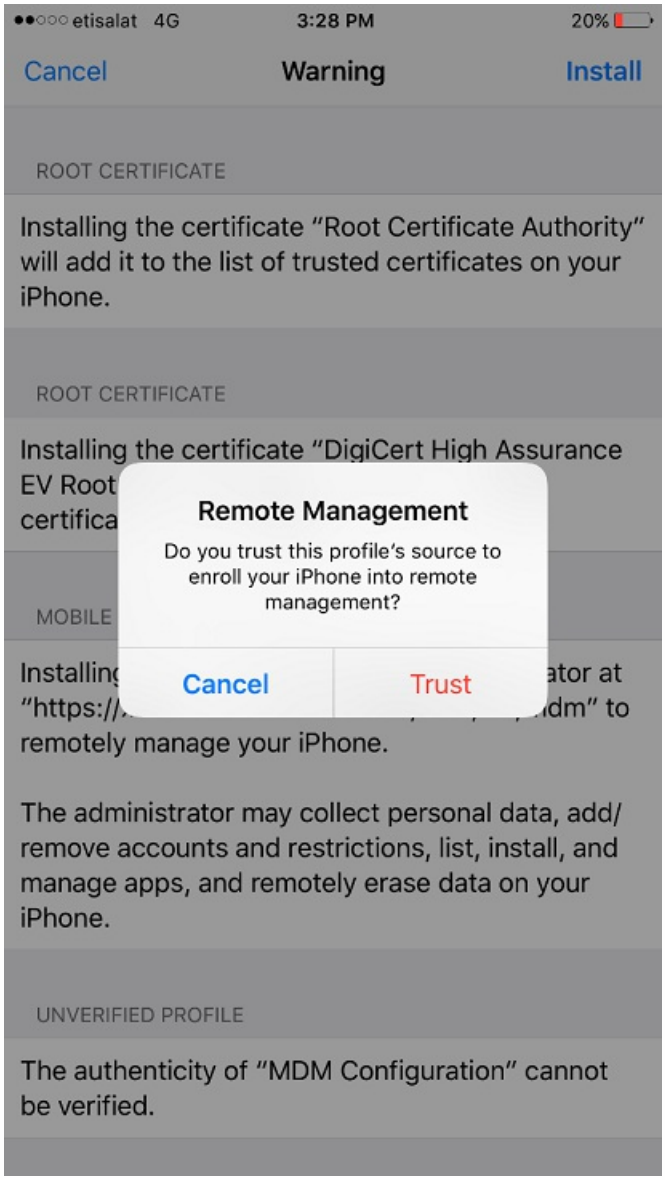
5. Cuando se le solicite la inscripción, haga clic en **Sí, inscribirlo** y, a continuación, introduzca sus credenciales cuando se le pidan.



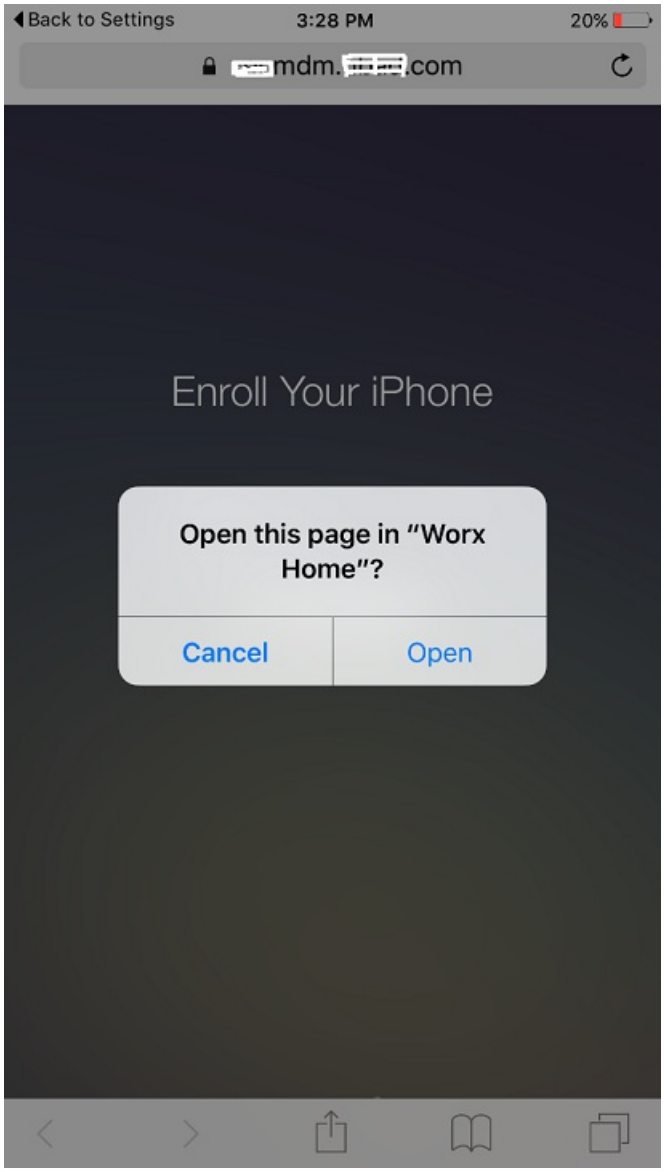


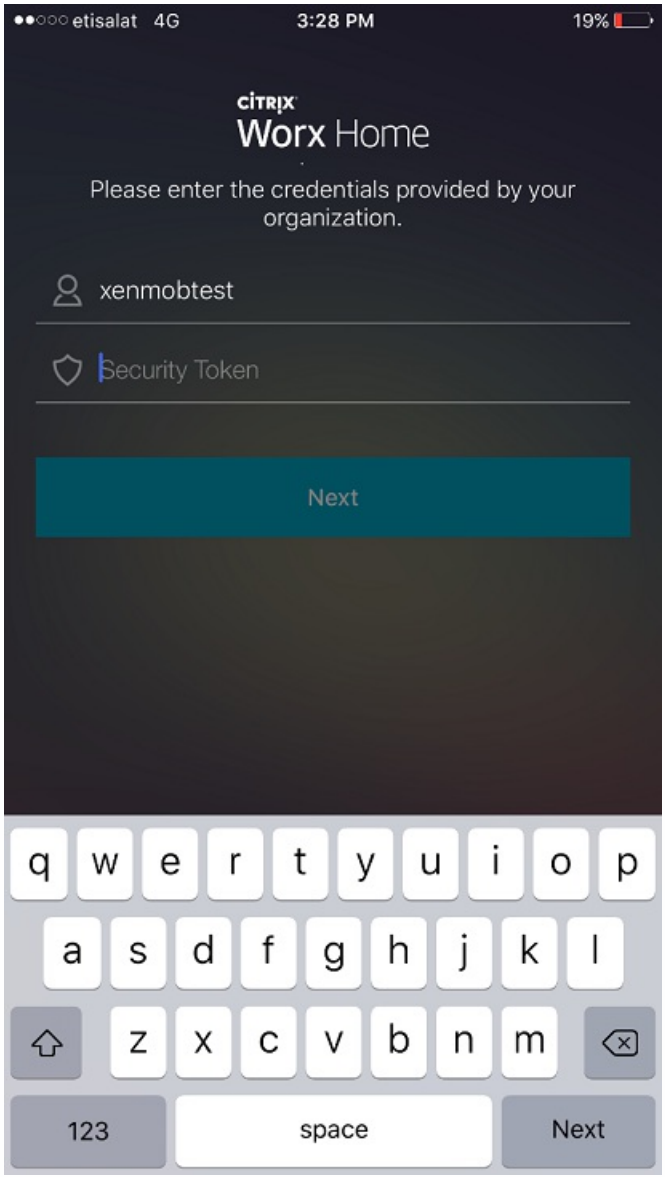
6. Toque en **Instalar** para instalar el servicio de perfiles (Citrix Profile Services).

7. Toque en **Trust**.



8. Toque en **Abrir** e introduzca sus credenciales.





Dispositivos Mac OS X

Jul 27, 2016

Puede inscribir en XenMobile equipos Mac que ejecutan OS X. Los usuarios de Mac se inscriben directamente desde sus dispositivos.

Los pasos a seguir para inscribir equipos Mac son:

1. Si quiere, puede configurar directivas para Mac en la consola de XenMobile. Consulte Directivas de dispositivos para obtener más información acerca de las directivas de dispositivos. Para saber qué directivas se pueden configurar para Mac, consulte Directivas de dispositivos de XenMobile desglosadas por plataforma.

2. Envíe el enlace de inscripción https://serverFQDN:8443/zdm/macos/otae, que los usuarios abrirán en Safari. Donde

- serverFQDN es el nombre de dominio completo del servidor que ejecuta XenMobile.
- El puerto 8443 es el puerto seguro predeterminado; si ha configurado otro puerto, indique ese en lugar de 8443.
- zdm es el nombre de la instancia utilizada durante la instalación del servidor.

Para obtener más información acerca del envío de enlaces de instalación, consulte Para enviar un enlace de instalación.

3. Los usuarios deben instalar certificados según sea necesario. La solicitud a los usuarios de instalar certificados depende de si ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para iOS y Mac OS. Para obtener más información acerca de certificados, consulte Certificados.

4. Los usuarios inician sesión en su Mac.

5. Se instalan las directivas de dispositivos Mac.

Ahora ya puede iniciar la administración de equipos Mac con XenMobile del mismo modo en que administra dispositivos móviles.

Dispositivos Windows

Jul 27, 2016

En XenMobile, puede inscribir dispositivos que ejecuten los siguientes sistemas operativos Windows:

- Windows 8.1 y 10
- Windows Phone 8.1 y 10

Los usuarios de Windows y Windows Phone se inscriben directamente a través de sus dispositivos.

Debe configurar la detección automática y el servicio de detección de Windows 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

Para inscribir dispositivos Windows con detección automática

Los usuarios pueden inscribir dispositivos que ejecutan Windows RT 8.1, versiones de 32 y 64 bits de Windows 8.1 Pro y Windows 8.1 Enterprise, así como Windows 10. Para habilitar la administración de dispositivos Windows, Citrix recomienda configurar la detección automática y el servicio de detección de Windows. Para obtener más información, consulte Para habilitar 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 en **Configuración** y luego:

- En Windows 8.1, toque en **Red** > **Área de trabajo**.
- En Windows 10, toque en **Cuentas** > **Acceso al trabajo** > **Inscribir en administración de dispositivos (MDM)**.

3. Introduzca su correo electrónico de la empresa y toque en **Activar** en Windows 8.1, o en **Continuar** en Windows 10. 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 le permite omitir una limitación conocida de Microsoft, por la que la inscripción se realiza en la Administración de dispositivos nativa de Windows; 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 Windows 8.1, en el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique si está de acuerdo con que su dispositivo sea administrado y luego toque en **Activar**. En Windows 10, en el cuadro de diálogo **Términos de uso**, indique que está de acuerdo con que su dispositivo sea administrado y toque en **Aceptar**.

Para inscribir dispositivos Windows sin detección automática

Puede inscribir dispositivos Windows sin detección automática. Sin embargo, Citrix recomienda configurar la detección automática. La inscripción sin la detección automática consiste en una llamada al puerto 80 antes de conectarse a la URL pertinente, por lo que 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 en **Configuración** y luego:

- En Windows 8.1, toque en **Red** > **Área de trabajo**.
- En Windows 10, toque en **Cuentas** > **Acceso al trabajo** > **Inscribir en administración de dispositivos (MDM)**.

3. Introduzca la dirección de correo electrónico de empresa.

4. En Windows 10, si no se ha configurado la detección automática, aparecerá una opción donde podrá introducir datos del servidor, como se describe en el paso 5. En Windows 8.1, si la opción **Automatically detect server address** está activada, tóquela para desactivarla.

5. En el campo **Indicar dirección del servidor**:

- Para Windows 8.1, 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 ese puerto en lugar de *8443* en esta dirección.
- Para Windows 10, use esta dirección: https://beta.managedm.com:8443/zdm/wpe. Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice ese puerto en lugar de *8443* en esta dirección.

6. Introduzca la contraseña.

7. En Windows 8.1, en el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique si está de acuerdo con que su dispositivo sea administrado y luego toque en **Activar**. En Windows 10, en el cuadro de diálogo **Términos de uso**, indique que está de acuerdo con que su dispositivo sea administrado y toque en **Aceptar**.

Para inscribir dispositivos Windows Phone en XenMobile

Para inscribir dispositivos Windows Phone 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 un almacén o tienda de 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 para cada plataforma a la que quiera dar respaldo).
1. En la pantalla principal del teléfono Windows, toque el icono **Configuración**.

2. En Windows Phone 8.1, toque en **Sistema** > **Área de trabajo** y luego toque en **Agregar cuenta**. Para Windows 10 Phone, toque en **Cuentas** > **Acceso al trabajo** > **Inscribir en administración de dispositivos (MDM)**.

3. 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.

4. En la pantalla siguiente, escriba la dirección Web del servidor XenMobile, tal 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.

5. 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**.

6. 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**.

7. En Windows Phone 8.1, 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, deberá volver a inscribir el dispositivo para recibir la tienda de aplicaciones de empresa.

8. En Windows Phone 8.1, en la pantalla **Cuenta agregada**, toque en **listo**.

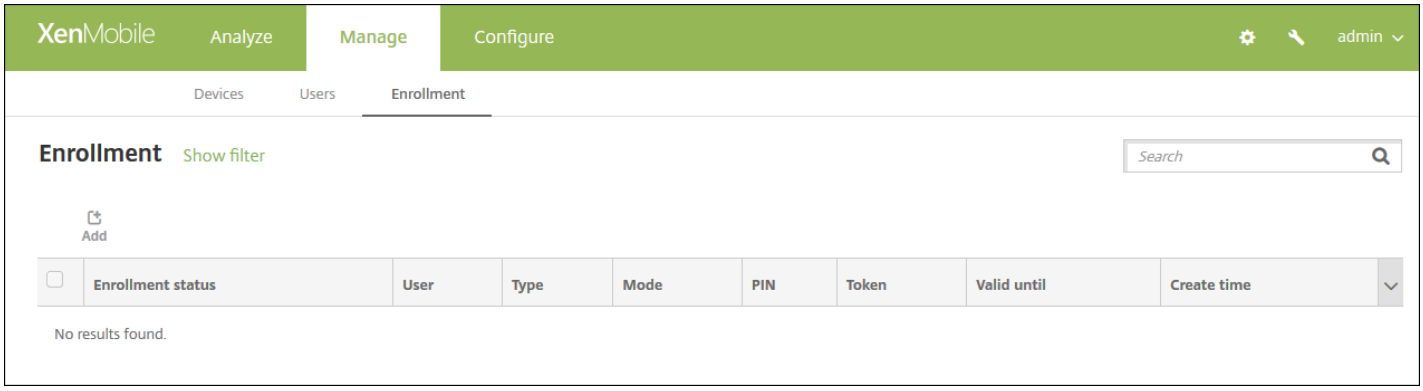
9. Para forzar la conexión con el servidor, toque el icono de actualización. Si el dispositivo no se conecta manualmente al servidor, XenMobile intenta reconectarse. XenMobile se conecta al dispositivo cada 3 minutos 5 veces sucesivas; después, se conecta cada 2 horas. Puede modificar este intervalo de conexión en Windows **WNS Heartbeat Interval** en **Server properties**. Una vez finalizada la inscripción, Worx Home se inscribe de fondo. No aparece ningún indicador tras completarse la instalación. Abra Worx Home desde la pantalla **Todas las aplicaciones**.

Envío de una invitación de inscripción en XenMobile

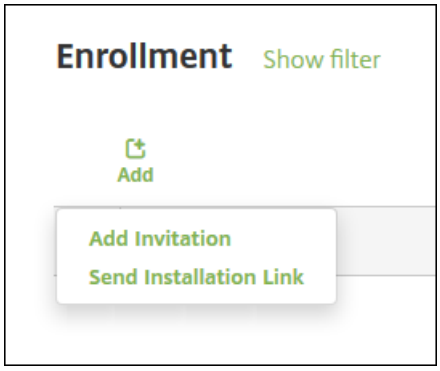
Oct 31, 2016

Desde la consola de XenMobile, puede enviar a los usuarios una invitación para la inscripción de dispositivos iOS o Android. También puede enviar un enlace de instalación a los usuarios con dispositivos iOS, Android, Windows o Mac.

1. En la consola de XenMobile, haga clic en **Manage > Enrollment**. Aparecerá la página **Enrollment**.



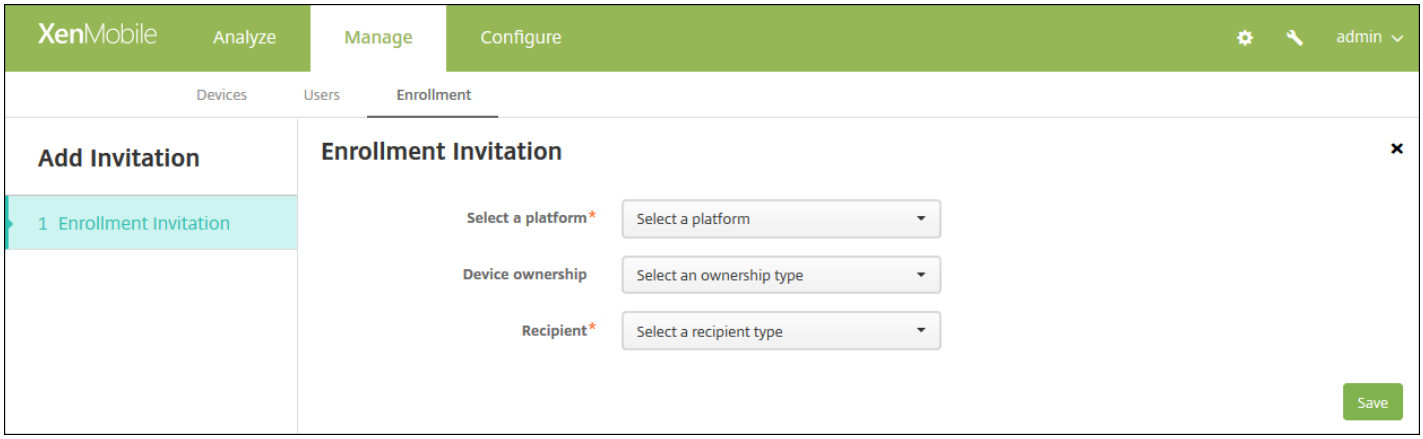
2. Haga clic en **Add**. Aparecerá un menú con opciones de inscripción.



- Para enviar una invitación de inscripción a un usuario o grupo, haga clic en **Add Invitation** y, a continuación, consulte Para enviar una invitación y siga los pasos ahí indicados para configurar este parámetro.
- Para enviar un enlace de instalación para la inscripción a una lista de destinatarios a través de SMTP o SMS, haga clic en **Send Installation Link** y, a continuación, consulte Para enviar un enlace de instalación y siga los pasos ahí indicados para configurar este parámetro.

Para enviar una invitación

1. Haga clic en **Add Invitation**. Aparecerá la pantalla **Enrollment Invitation**.

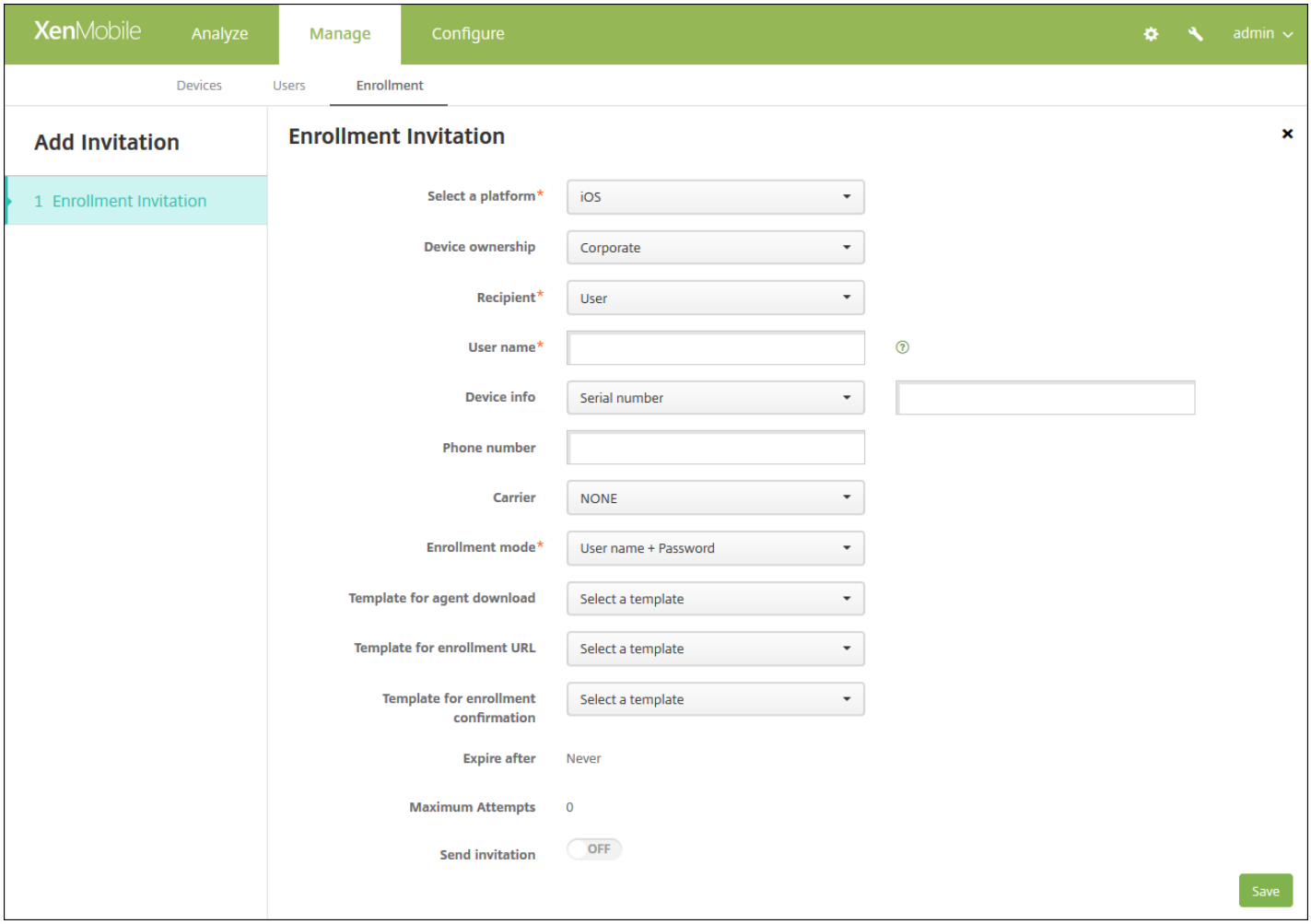


2. Configure los siguientes parámetros:

- **Select a platform**. En la lista, haga clic en **iOS** o **Android**.
- **Device ownership**. En la lista, haga clic en **Corporate** o **Employee**.
- **Recipient**. En la lista, haga clic en **User** o **Group**.

Podrá ver más opciones para configurar según el destinatario que seleccione. Para la configuración de **User**, consulte Para enviar una invitación de inscripción a un usuario; para la configuración de **Group**, consulte Para enviar una invitación de inscripción a un grupo.

Para enviar una invitación de inscripción a un usuario



1. Configure estos parámetros de **User**:

- **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 enviarle notificaciones. Si se trata de un usuario de Active Directory, compruebe que el protocolo LDAP está configurado.
- **Device info**. En la lista, haga clic en **Serial number**, **UDID** o **IMEI**. Después de elegir una opción, aparece un campo en el que puede escribir el valor correspondiente del dispositivo.
- **Phone number**. Si lo prefiere, escriba el número de teléfono del usuario.
- **Carrier**. En la lista, seleccione un operador al que asociar el número de teléfono del usuario.
- **Enrollment mode**. En la lista, haga clic en la forma en que quiere que los usuarios se inscriban. El valor predeterminado es **User name + Password**. Las opciones posibles son:
  - High Security (Nivel de seguridad alto)
  - Invitation URL (URL de invitación)
  - Invitation URL + PIN (URL de invitación + PIN)
  - Invitation URL + Password (URL de invitación + contraseña)
  - Two Factor (Autenticación de dos factores)
  - Nombre de usuario + PIN

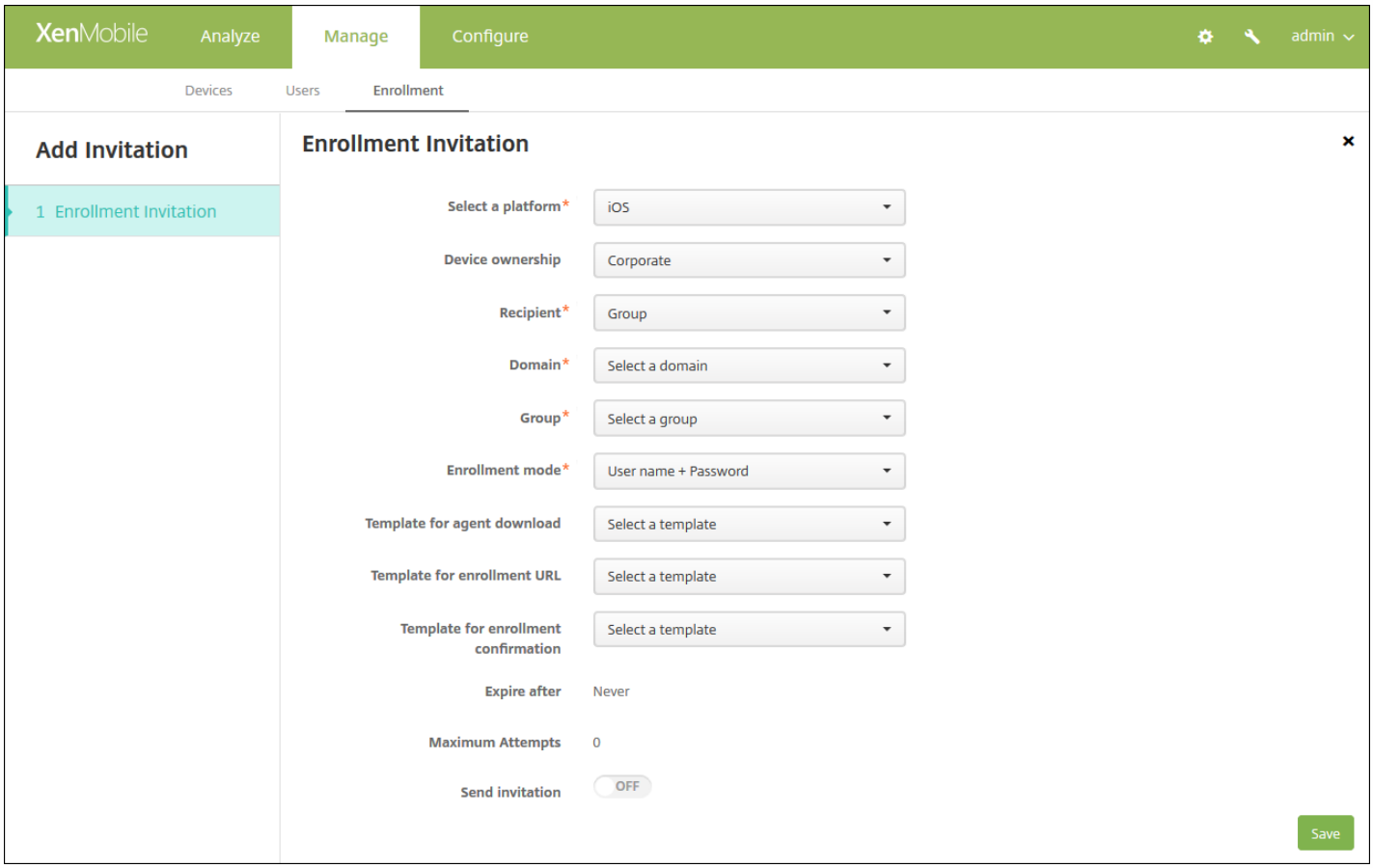
  Nota: Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment**

PIN, donde deberá hacer clic en **Enrollment PIN**.

- **Template for agent download**. En la lista, haga clic en la plantilla que se utilizará para la invitación a la inscripción. Las variantes de esta opción dependen del tipo de plataforma. Por ejemplo, aparecerá **iOS Download Link** como opción si ha seleccionado **iOS** como plataforma.
- **Template for enrollment URL**. En la lista, haga clic en **Enrollment Invitation**.
- **Template for enrollment confirmation**. En la lista, haga clic en **Enrollment Confirmation**.
- **Expire after**. Este campo se establece cuando se configura el modo de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte Para configurar modos de inscripción.
- **Maximum Attempts**. Este campo se establece cuando se configura el modo de inscripción e indica la cantidad máxima de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte Para configurar modos de inscripción.
- **Send invitation**. Seleccione **ON** para enviar la invitación inmediatamente, o bien haga clic en **OFF** para agregarla solamente a la tabla de la página **Enrollment**.

2. Haga clic en **Save and Send** si ha indicado **Send invitation**; de lo contrario, haga clic en **Save**. La invitación aparecerá en la tabla de la página **Enrollment**.

Para enviar una invitación de inscripción a un grupo



1. Configure los siguientes parámetros:

- **Domain**. En la lista, haga clic en el dominio del que se seleccionará el grupo.

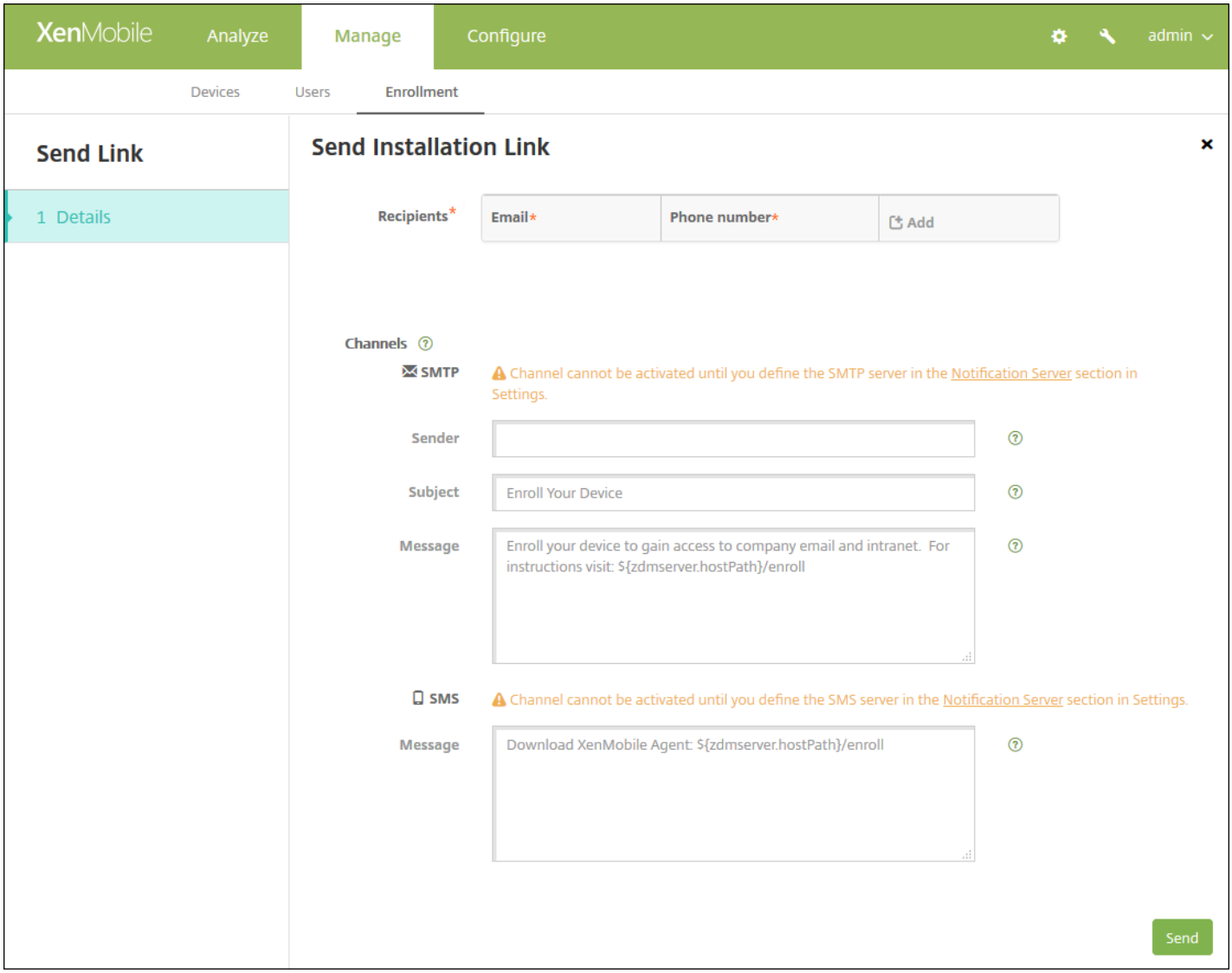
- **Group**. En la lista, haga clic en el grupo que recibirá la invitación.
- **Enrollment mode**. En la lista, haga clic en la forma en que quiere que los usuarios del grupo se inscriban. El valor predeterminado es **User name + Password**. Las opciones posibles son:
  - High Security (Nivel de seguridad alto)
  - Invitation URL (URL de invitación)
  - Invitation URL + PIN (URL de invitación + PIN)
  - Invitation URL + Password (URL de invitación + contraseña)
  - Two Factor (Autenticación de dos factores)
  - Nombre de usuario + PIN

  Nota: Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment PIN**, donde deberá hacer clic en **Enrollment PIN**.

- **Template for agent download**. En la lista, haga clic en la plantilla que se utilizará para la invitación a la inscripción. Las variantes de esta opción dependen del tipo de plataforma. Por ejemplo, aparecerá **iOS Download Link** como opción si ha seleccionado **iOS** como plataforma.
- **Template for enrollment URL**. En la lista, haga clic en **Enrollment Invitation**.
- **Template for enrollment confirmation**. En la lista, haga clic en **Enrollment Confirmation**.
- **Expire after**. Este campo se establece cuando se configura el modo de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte Para configurar modos de inscripción.
- **Maximum Attempts**. Este campo se establece cuando se configura el modo de inscripción e indica la cantidad máxima de veces que se da el proceso de inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte Para configurar modos de inscripción.
- **Send invitation**. Seleccione **ON** para enviar la invitación inmediatamente, o bien haga clic en **OFF** para agregarla solamente a la tabla de la página **Enrollment**.

2. Haga clic en **Save and Send** si ha indicado **Send invitation**; de lo contrario, haga clic en **Save**. La invitación aparecerá en la tabla de la página **Enrollment**.

Para enviar un enlace de instalación



Antes de enviar un enlace de instalación para la inscripción, debe configurar canales (SMTP o SMS) en el servidor de notificaciones. Puede hacerlo desde la página **Settings**. Para obtener más información, consulte Notificaciones.

1. Configure los siguientes parámetros:

- **Recipient**. Para cada destinatario que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Email**. Escriba la dirección de correo electrónico del destinatario. Este campo es obligatorio.
  - **Phone number**. Escriba el número de teléfono del destinatario. Este campo es obligatorio.
  - Haga clic en **Guardar**.

    Nota: Para eliminar un destinatario existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. 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 destinatario existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Channels**. Seleccione el canal que se va a usar para enviar el enlace de instalación para la inscripción. Puede enviar notificaciones a través de SMTP o SMS. Estos canales no se pueden activar hasta que se configuren los parámetros de servidor en la página **Settings**, en **Notification Server**. Para obtener más información, consulte Notificaciones.
  - **SMTP**. Si quiere, configure estos parámetros. Si no escribe nada en estos campos, se utilizarán los valores predeterminados que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
    - **Sender**. Si lo prefiere, escriba un remitente.
    - **Subject**. Aquí puede escribir un asunto para el mensaje. Por ejemplo: "Inscriba su dispositivo".
    - **Message**. Si quiere, escriba el mensaje que se enviará al destinatario. Por ejemplo: "Inscriba su dispositivo para tener acceso a las aplicaciones y al correo electrónico de la organización".
  - **SMS**. Configure este parámetro. Si no escribe nada en este campo, se utilizará el valor predeterminado que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
    - **Message**. Escriba el mensaje que se enviará a los destinatarios. 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.

2. 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 de nombre_de_dominio de SAMAccountName@nombre_de_dominio.com.

Dispositivos compartidos en XenMobile

Jul 27, 2016

XenMobile permite configurar los dispositivos que se pueden compartir entre varios usuarios. La función de dispositivos compartidos permite, por ejemplo, que los médicos, en los hospitales, usen cualquier dispositivo cercano para acceder a las aplicaciones y a los datos, en lugar de tener que llevar encima un dispositivo concreto. También puede interesarle intercambiar dispositivos en ámbitos judiciales, comerciales y de fabricación para compartir los dispositivos entre sí y, de esta manera, reducir costes de equipamiento.

Puntos clave sobre dispositivos compartidos

Modo MDM

- Disponible en teléfonos y tabletas iOS y Android. No se admite la inscripción básica del Device Enrollment Program (DEP) para dispositivos compartidos de XenMobile Enterprise. Debe utilizar una inscripción autorizada de DEP para inscribir un dispositivo compartido en este modo.
- No se admiten la autenticación de certificados de cliente, el PIN de Worx, Touch ID ni la entropía de usuario.

Modo MDM+MAM

- Disponible solo en tabletas iOS y Android.
- Compatible solo con el cliente y el servidor XenMobile 10.3.x.
- No se admite el modo solo MAM. Los dispositivos deben inscribirse en MDM.
- Solo se respaldan WorxMail, WorxWeb y la aplicación móvil de ShareFile (versión 4.4). No se admiten las aplicaciones HDX.
- Los usuarios de Active Directory son los únicos usuarios admitidos; los grupos y los usuarios locales no se admiten.
- Los dispositivos compartidos existentes que están en modo solo MDM que quieran actualizarse a MDM+MAM deben reinscribirse.
- Los usuarios solo pueden compartir aplicaciones Worx y aplicaciones empaquetadas MDX; no pueden compartir aplicaciones nativas en los dispositivos.
- Una vez se hayan descargado durante la primera inscripción, las aplicaciones Worx no se vuelven a descargar cada vez que un nuevo usuario inicia sesión en el dispositivo. El nuevo usuario puede coger el dispositivo, iniciar sesión y utilizarlo.
- En Android, para aislar los datos de cada usuario por motivos de seguridad, la directiva **Disallow rooted devices** de la consola de XenMobile debe establecerse como **On**.

Requisitos previos para la inscripción de dispositivos compartidos

Antes de inscribir dispositivos compartidos, debe realizar lo siguiente:

- Crear un rol de usuario de inscripción de dispositivos compartidos. Consulte Configuración de roles con RBAC.
- Crear un usuario de dispositivos compartidos. Consulte Para agregar, modificar o eliminar usuarios locales en XenMobile.
- Crear un grupo de entrega que contenga las aplicaciones, las acciones y las directivas base que quiera que se apliquen al usuario de inscripción de dispositivos compartidos. Consulte Administración de grupos de entrega.

Requisitos previos para el modo MDM+MAM

1. Crear un grupo de Active Directory con un nombre parecido a **Shared Device Enrollers**.
2. Agregar a este grupo usuarios de Active Directory que inscribirán dispositivos compartidos. Si quiere una nueva cuenta para este fin, cree un nuevo usuario de Active Directory (por ejemplo, **sdenroll**) y agréguelo al grupo de Active Directory.

Requisitos de los dispositivos compartidos

Para una experiencia del usuario mejorada, incluida la instalación silenciosa y la eliminación de aplicaciones, Citrix recomienda configurar dispositivos compartidos en las siguientes plataformas:

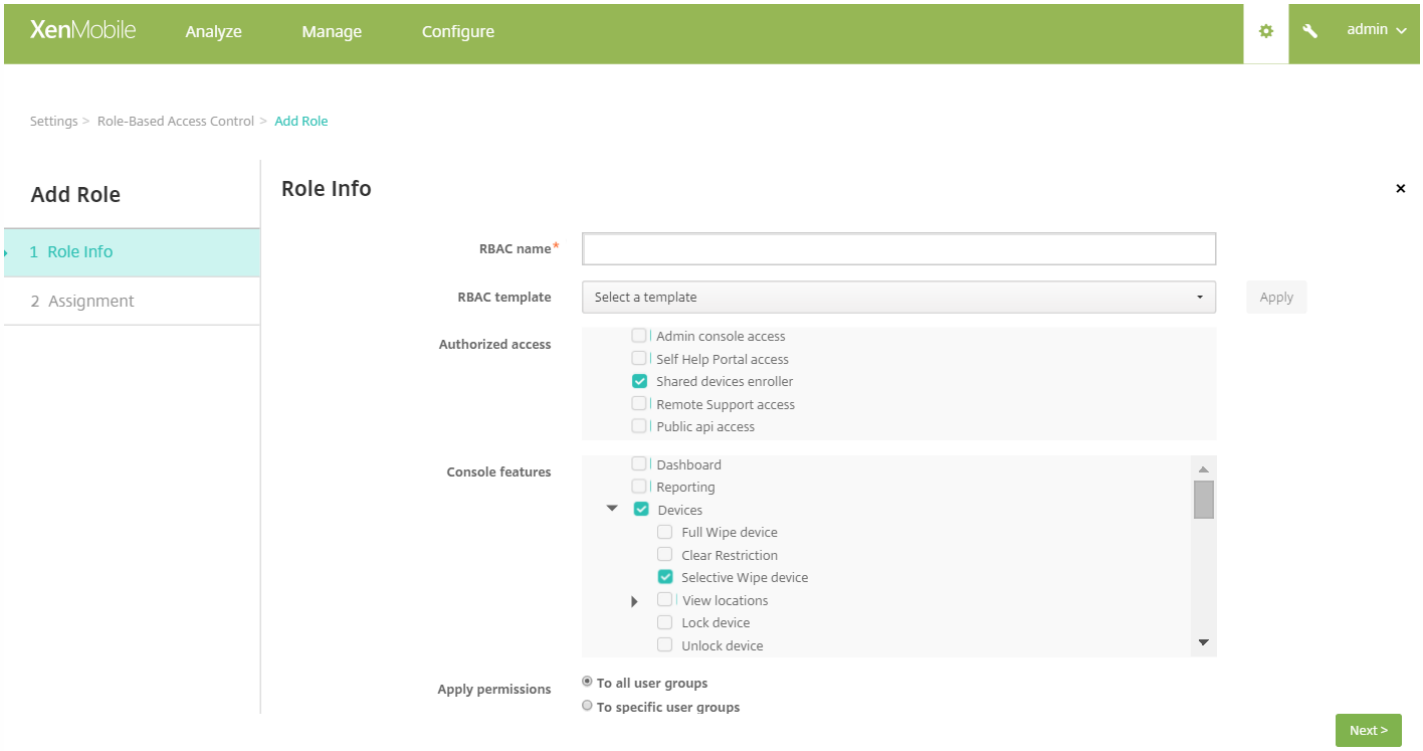
- iOS 9
- iOS 8
- Android M
- Android 5.x
- Android 4,4.x
- Android 4.0.x (modo solo MDM)

Configuración de un dispositivo compartido

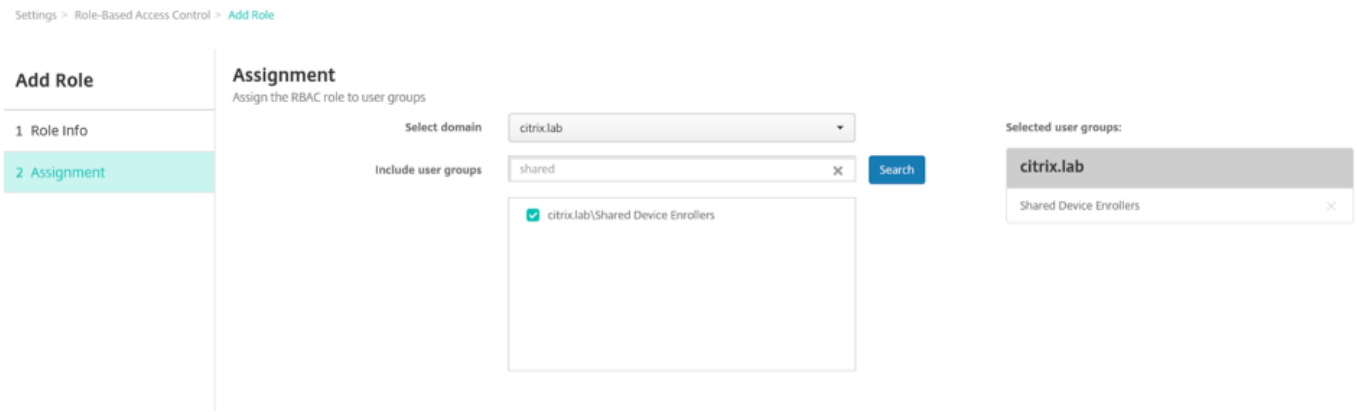
Siga estos pasos para configurar un dispositivo compartido.

1. Desde la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página Settings.
2. Haga clic en **Role-Based Access Control** y, a continuación, haga clic en **Add**. Aparece la pantalla **Add Role**.
3. Cree un rol de usuario de inscripción de dispositivo compartido denominado **Shared Device Enrollment User** con permisos de **Shared devices enroller** en **Authorized Access**. Expanda **Devices**, en la sección **Console features** y, a continuación, seleccione **Selective Wipe device**. Esta configuración garantiza que las aplicaciones y las directivas aprovisionadas mediante la cuenta de inscripción de dispositivos compartidos se eliminen a través de Worx Home, cuando se anule la inscripción del dispositivo.

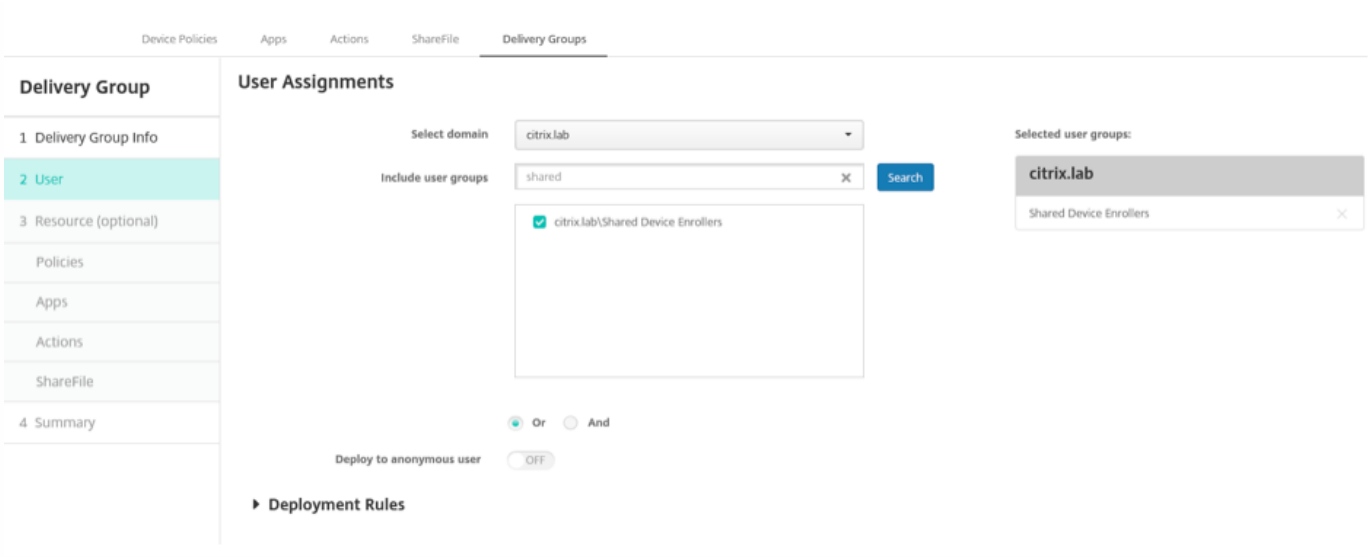
   Para **Apply Permissions**, conserve la configuración predeterminada, **To all user groups**, o asigne permisos a grupos de usuarios de Active Directory específicos con **To specific user groups**.



Haga clic en **Next** para pasar a la pantalla **Assignment**. Asigne el rol de inscripción de dispositivo compartido que acaba de crear al grupo de Active Directory que ha creado para los usuarios de inscripción de dispositivos compartidos en el paso 1 de requisitos previos. En la siguiente imagen, **citrix.lab** es el dominio de Active Directory y **Shared Device Enrollers** es el grupo de Active Directory.



4. Cree un grupo de entrega que contenga las directivas base, las aplicaciones y las acciones que quiere que se apliquen al dispositivo cuando un usuario no haya iniciado sesión. A continuación, asocie ese grupo de entrega al grupo de Active Directory de usuario de inscripción de dispositivos compartidos.



5. Instale Worx Home en el dispositivo compartido e inscríbalo en XenMobile con la cuenta de usuario de inscripción de dispositivos compartidos. Ahora, puede ver y administrar el dispositivo a través de la consola XenMobile. Para obtener más información, consulte Inscripción de dispositivos.

6. Si quiere aplicar directivas diferentes u ofrecer aplicaciones adicionales a los usuarios autenticados, cree un grupo de entrega asociado a esos usuarios y que se haya implementado solo en dispositivos compartidos. Al crear los grupos, configure reglas de implementación para que los paquetes se implementen en dispositivos compartidos. Para obtener más información, consulte Configuración de reglas de implementación.

7. Si quiere dejar de compartir el dispositivo, realice un borrado selectivo para quitar la cuenta del usuario de inscripción de dispositivos compartidos del dispositivo, junto con las aplicaciones y las directivas que se han implementado en él.

Experiencia de usuario de dispositivos compartidos

Modo MDM

Los usuarios solo ven los recursos disponibles para ellos, y obtienen la misma experiencia en cada dispositivo compartido. Las aplicaciones y las directivas de inscripción de dispositivos compartidos permanecen en el dispositivo. Cuando un usuario que no se ha inscrito en dispositivos compartidos inicia sesión en Worx Home, las aplicaciones y las directivas de esa persona se implementan en el dispositivo. Cuando dicho usuario cierra la sesión, se eliminan las directivas y las aplicaciones que son diferentes de las de la inscripción de dispositivos compartidos, mientras los recursos de inscripción de dispositivos compartidos permanecen intactos.

Modo MDM+MAM

WorxMail y WorxWeb se implementan en el dispositivo cuando los inscribe el usuario de inscripción de dispositivos compartidos. Los datos de usuario se conservan de forma segura en el dispositivo. Los datos no se expondrán a otros usuarios cuando estos inicien sesión en WorxMail o WorxWeb.

Solo un usuario a la vez puede iniciar sesión en Worx Home. El usuario anterior debe finalizar la sesión antes de que el siguiente pueda iniciarla. Por motivos de seguridad, Worx Home no almacena credenciales de usuario en dispositivos compartidos, de modo que los usuarios deben introducir sus credenciales cada vez que inicien sesión. Con el fin de que el

usuario nuevo no pueda acceder a los recursos pensados para el usuario anterior, Worx Home no permite que los nuevos usuarios inicien sesión mientras se quitan las directivas, las aplicaciones y los datos asociados al usuario anterior.

La inscripción de dispositivos compartidos no cambia el proceso de actualización de aplicaciones. Puede insertar actualizaciones en los usuarios de dispositivos compartidos como siempre, y estos pueden actualizar las aplicaciones directamente en sus dispositivos.

Directivas de WorxMail recomendadas

- Para asegurar el mejor funcionamiento de WorxMail, configure **Max sync period** en función de la cantidad de usuarios que compartirán el dispositivo. No se recomienda permitir una sincronización ilimitada.

Cantidad de usuarios que comparten el dispositivo	Periodo de sincronización máximo recomendado
De 21 a 25	1 semana o menos
De 6 a 20	2 semanas o menos
Hasta 5	1 mes o menos

- Bloquee **Enable contact export** para evitar exponer los contactos de un usuario a los demás usuarios que comparten el dispositivo.

- En iOS, solo se pueden definir los siguientes parámetros para cada usuario. Todos los demás parámetros serán comunes a todos los usuarios que compartan el dispositivo:

  Notificaciones
  Firma
  Fuera de la oficina
  Período de sincronización de correo
  S/MIME
  Comprobar ortografía

Administración de dispositivos con Android for Work en XenMobile

Oct 31, 2016

Android for Work es un espacio de trabajo seguro, disponible en dispositivos Android con Android 5.0 y versiones posteriores, que aísla datos, aplicaciones y cuentas de empresa de los datos, aplicaciones y cuentas personales. En XenMobile, se administran tanto los dispositivos personales (BYOD) como los dispositivos Android que sean propiedad de la empresa, haciendo que los usuarios creen un perfil de trabajo aparte en sus dispositivos el cual, combinado con el cifrado del hardware y las directivas que usted implemente, se encarga de separar de manera segura el espacio personal y el espacio de trabajo en el dispositivo. Se pueden administrar de forma remota todas las directivas, las aplicaciones y los datos empresariales; también se pueden borrar directivas, aplicaciones y datos del dispositivo sin que ello afecte al área personal del usuario. Para obtener más información acerca de los dispositivos Android compatibles, consulte la página de dispositivos de Google.

En XenMobile, también se pueden administrar dispositivos que ejecutan Android 4.0 - 4.4. Para ello, los usuarios deben descargar e instalar la aplicación Android for Work, que ofrece la misma función de espacio de trabajo seguro que existe integrada en los dispositivos con Android 5.0 y versiones posteriores.

Se utiliza Google Play for Work para agregar, comprar y aprobar aplicaciones para su implementación en el espacio de trabajo de Android for Work del dispositivo. Se puede utilizar Google Play for Work para implementar aplicaciones privadas de Android, así como aplicaciones públicas o de terceros. Cuando se agrega una tienda de aplicaciones de pago pública a XenMobile para Android for Work, se puede revisar el estado de la licencia de compra en bloque: la cantidad total de licencias disponibles y la cantidad de licencias en uso actualmente, además de la dirección de correo electrónico de cada uno de los usuarios que está consumiendo una licencia. Para obtener más información, consulte Para agregar una aplicación de tienda pública de aplicaciones a XenMobile.

Requisitos para Android for Work:

- Un dominio accesible públicamente
- Una cuenta de administrador de Google
- Dispositivos con Android 5.0 Lollipop y versiones posteriores con respaldo para perfiles administrados, o bien dispositivos que dispongan entre la versión 4.0 y la 4.4 de Android (Ice Cream Sandwich, Jelly Bean y KitKat) con la aplicación Android for Work
- Una cuenta de Google con Google Play instalado en el perfil personal del usuario
- Un perfil de Work instalado en el dispositivo

Antes de establecer las restricciones de la aplicación Android for Work, deberá llevar a cabo lo siguiente:

- Complete, en Google, las tareas de configuración de Android for Work.
- Cree un conjunto de credenciales de Google Play.
- Configure el servidor Android for Work.
- Cree al menos una directiva de dispositivo Android for Work.
- Agregue, compre y apruebe aplicaciones de Android for Work en la tienda de aplicaciones Google Play for Work.

Cuando administre Android for Work, puede utilizar los siguientes enlaces:

- Consola de administración de Google: https://admin.google.com/AdminHome

- Consola de administración Google Play for Work: https://play.google.com/work/apps
- Publicar en Google Play aplicaciones alojadas en servidores propios y de canal privado: https://play.google.com/apps/publish
- Google Developers Console para crear cuentas de servicio: https://console.developers.google.com

Requisitos previos de Android for Work

Para poder administrar Android for Work en XenMobile, debe hacer lo siguiente:

- Cree una cuenta de Android for Work.
- Configurar una cuenta de servicio.
- Descargar un certificado de Android for Work.
- Habilitar y autorizar las API de MDM y Admin SDK de Google.
- Autorizar a la cuenta de servicio para que use el directorio y Google Play
- Obtener un token de vinculación.

En los siguientes apartados, se describe cómo llevar a cabo cada una de esas tareas. Después de completar esas tareas, puede crear un conjunto de credenciales de Google Play, configurar opciones de Android for Work y administrar aplicaciones de Android for Work en XenMobile.

> **Advertencia**
>
> Existe un problema conocido de terceros que impide usar la consola de XenMobile para habilitar Android for Work. Para ver más información sobre este problema y cómo configurar una propiedad de servidor como solución temporal, consulte el apartado #615118 de los Problemas conocidos de XenMobile Server 10.3.

Cómo crear una cuenta de Android for Work

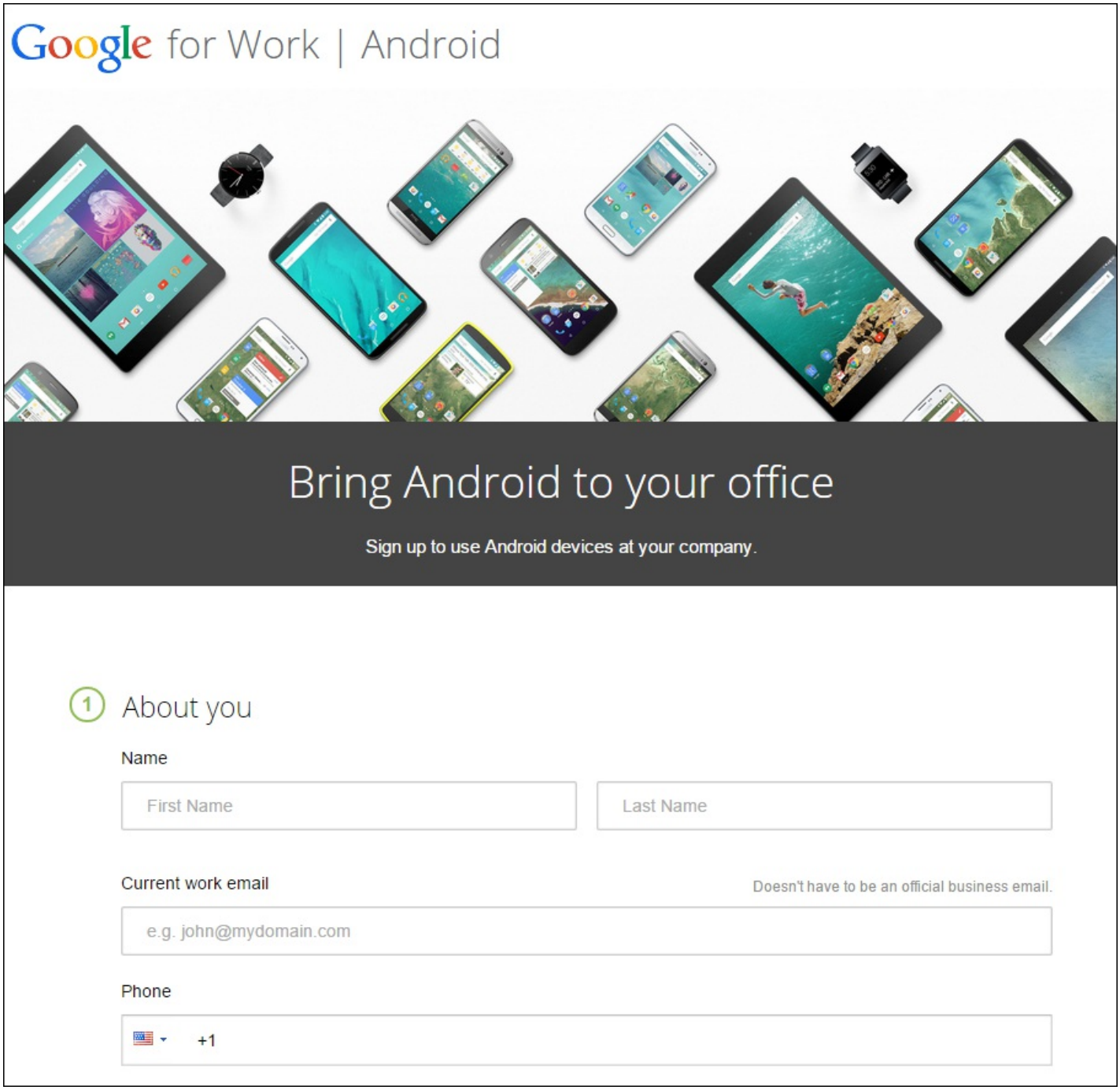
Antes de configurar una cuenta de Android for Work, debe cumplir los siguientes requisitos previos:

- Debe disponer de un nombre de dominio; por ejemplo, ejemplo.com.
- Debe permitir que Google verifique que usted es el propietario del dominio.
- Debe habilitar y administrar Android for Work a través de un proveedor de administración de movilidad empresarial (EMM), como XenMobile 10.1 o una versión posterior.

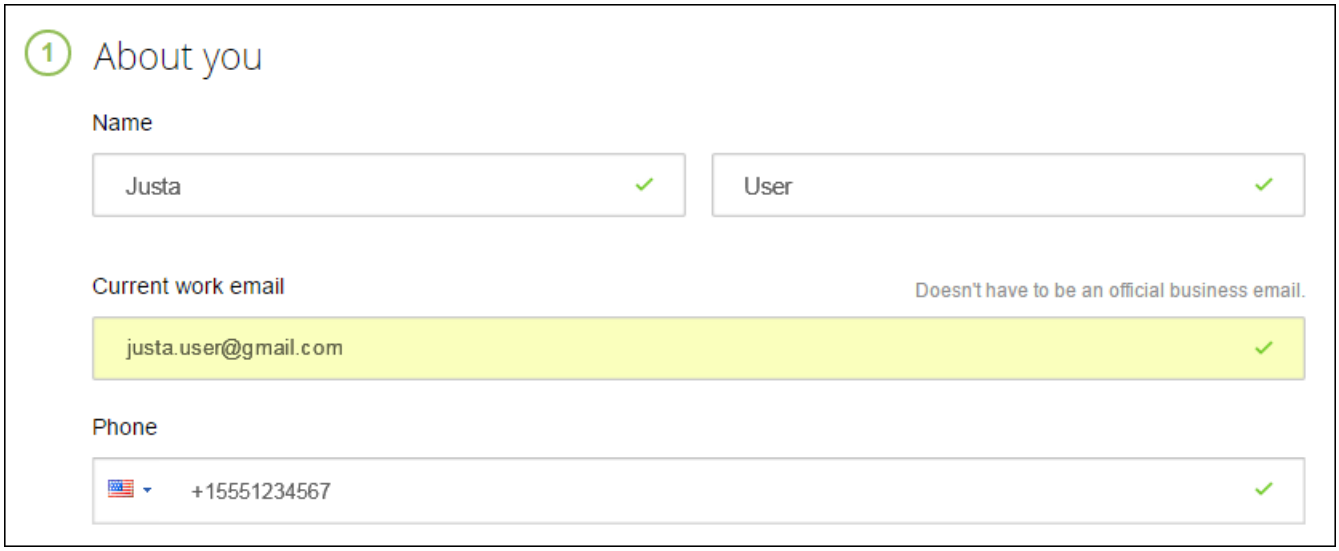
Si ya ha verificado el nombre de su dominio con Google, puede pasar a Cómo configurar una cuenta de servicio de Android for Work y descargar un certificado de Android for Work.

1. Vaya a https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

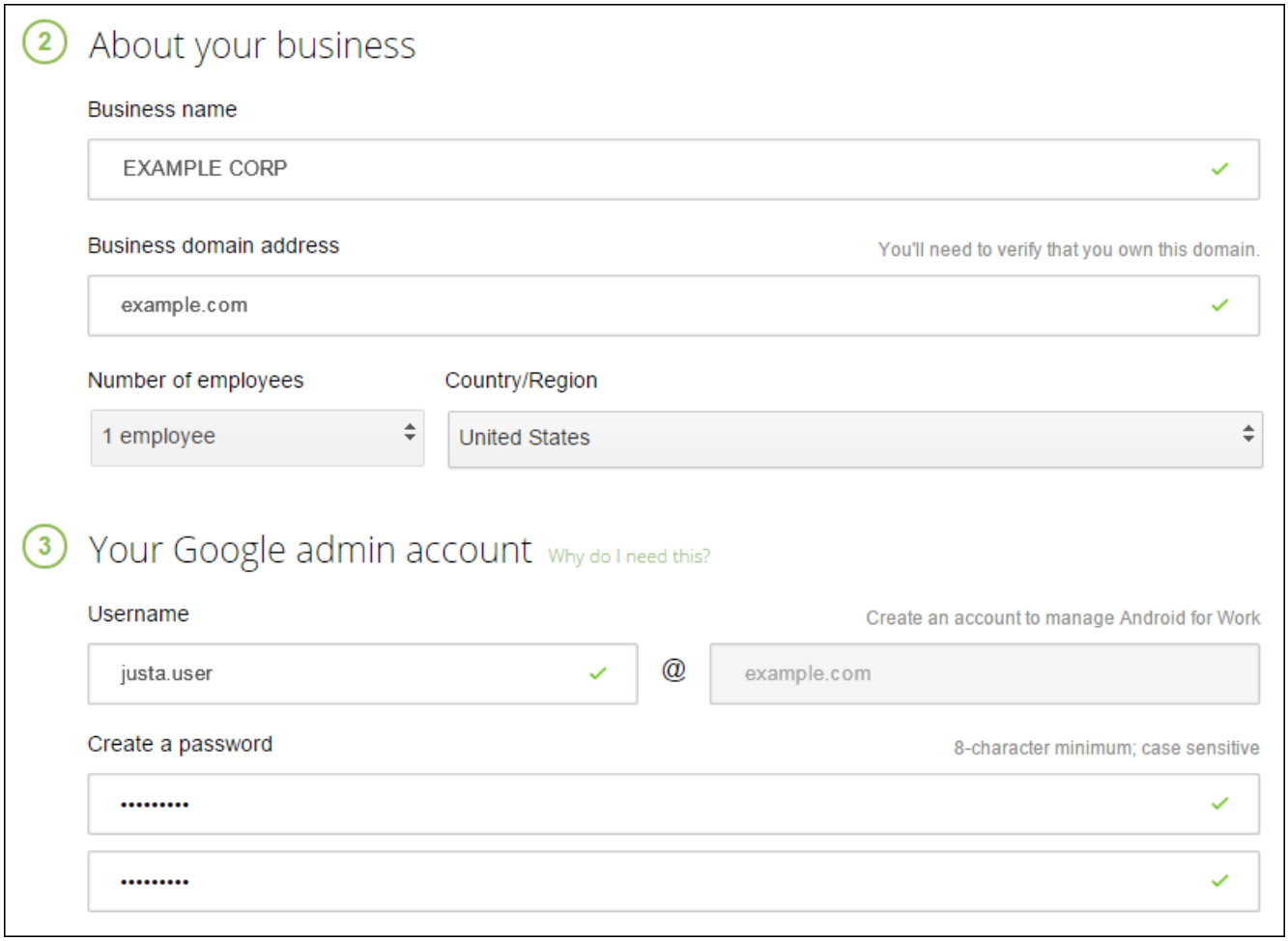
Se le redirige a la siguiente página, donde puede introducir su información de administrador y la información acerca de la empresa.



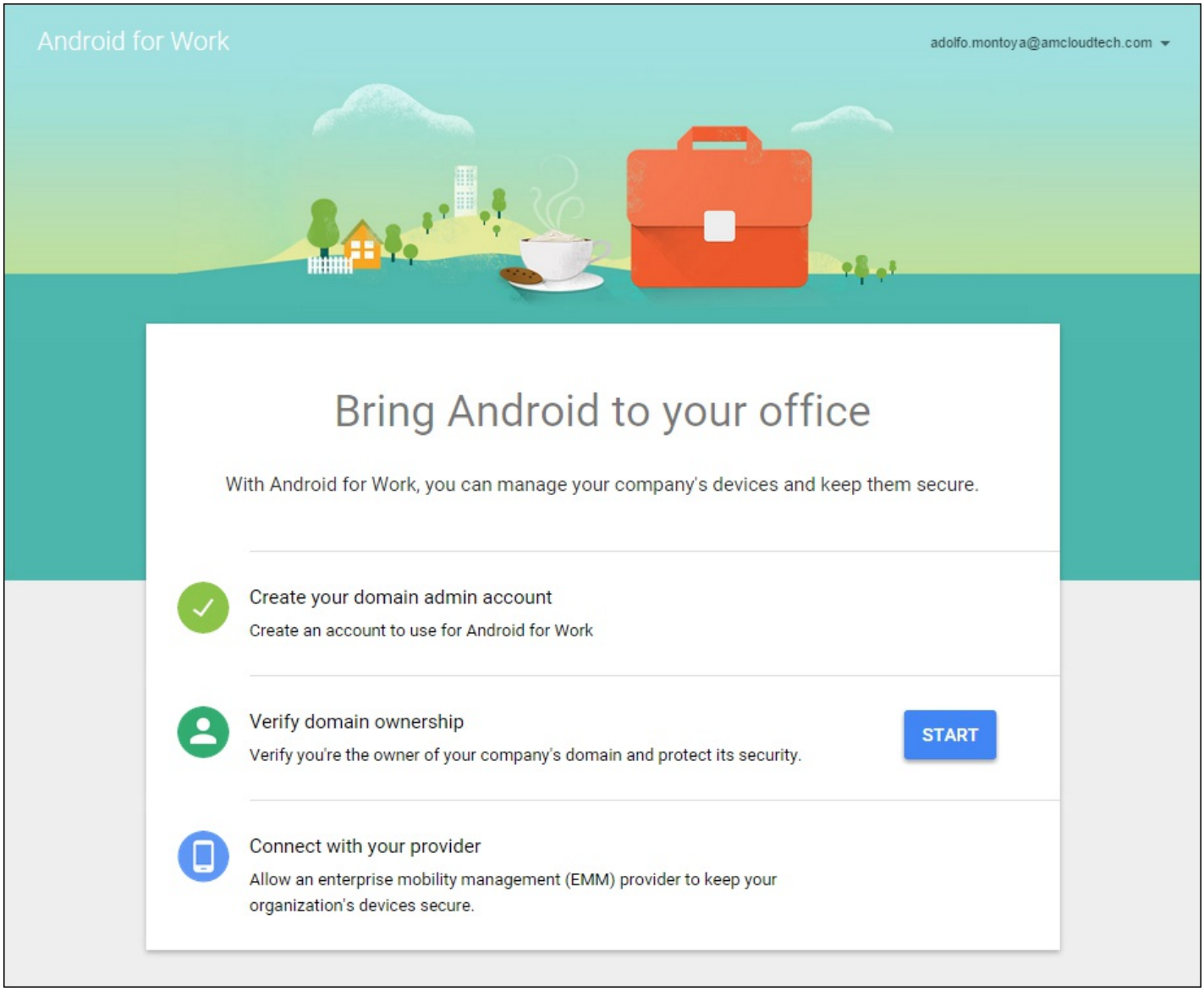
2. Introduzca la información de usuario del administrador.



3. Introduzca información sobre la empresa y la cuenta de administrador.



Una vez completado el primer paso, verá la página siguiente.

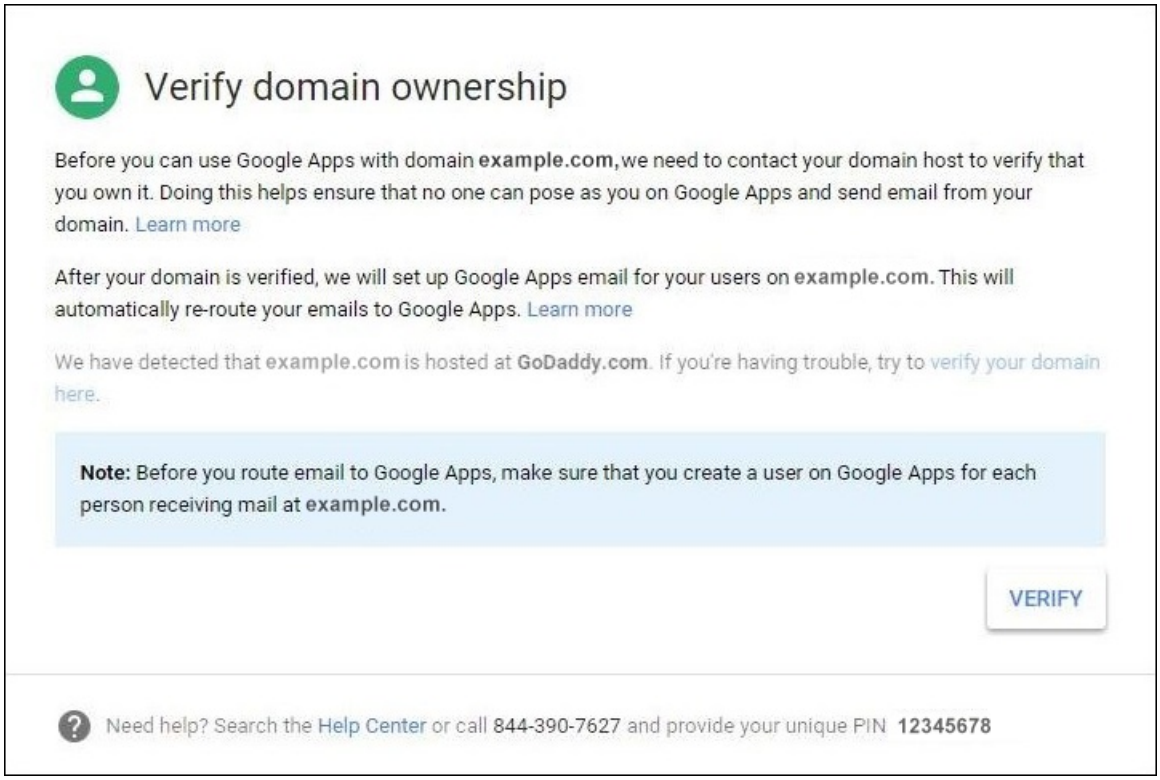


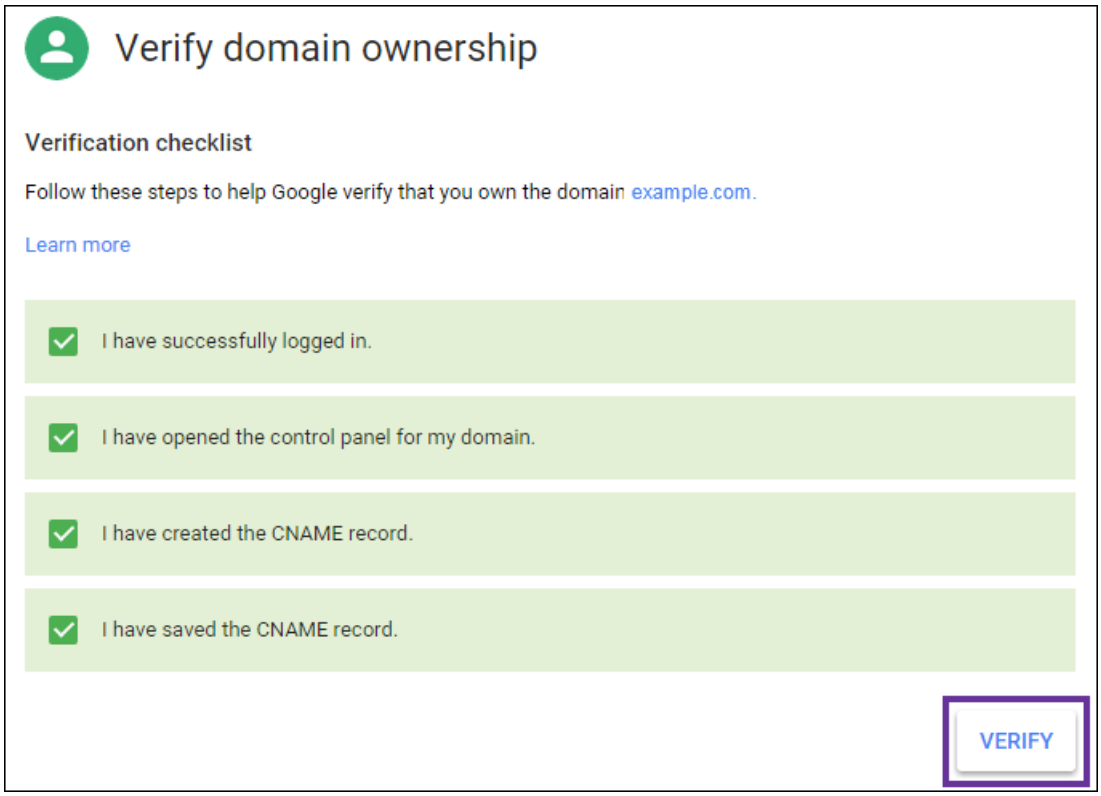
Verificación de la propiedad del dominio

Debe permitir que Google verifique su dominio. Existen tres métodos para verificar el dominio: agregue un registro TXT o un registro CNAME al sitio Web del host del dominio, cargue un archivo HTML en el servidor Web de su dominio, o agregue una etiqueta a su página principal. Google recomienda el primer método. Los pasos para comprobar que usted es el propietario del dominio no se describen en este artículo, pero puede encontrar esta información aquí: https://support.google.com/a/answer/6095407/.

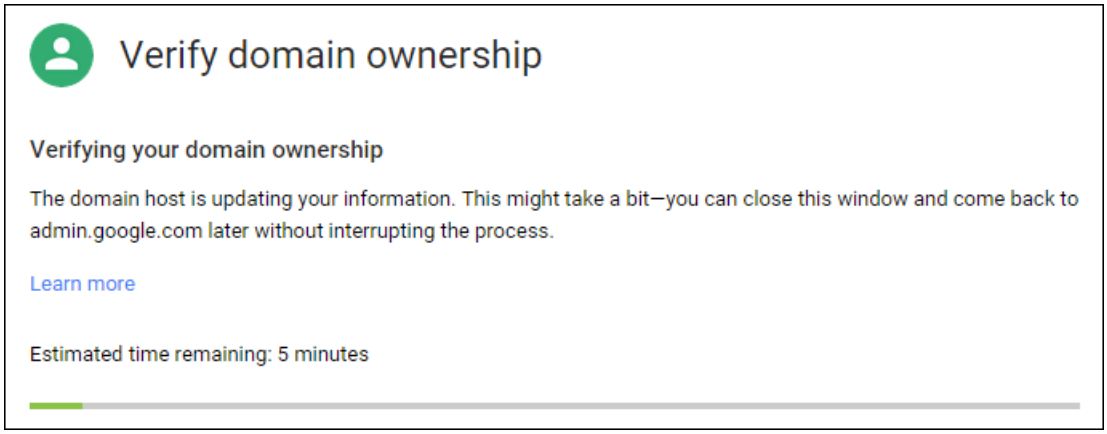
1. Haga clic en **Start** para iniciar la verificación de su dominio. Verá la página **Verify domain ownership**. Siga las instrucciones de esta página para verificar su dominio.

2. Cuando termine, haga clic en **Verify**.

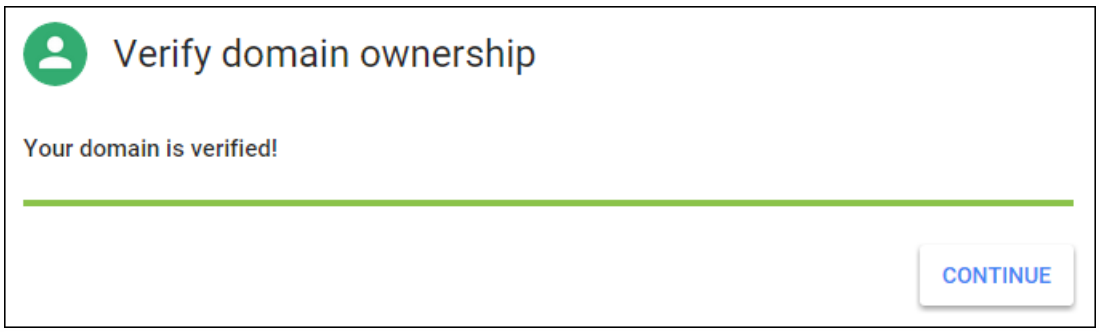




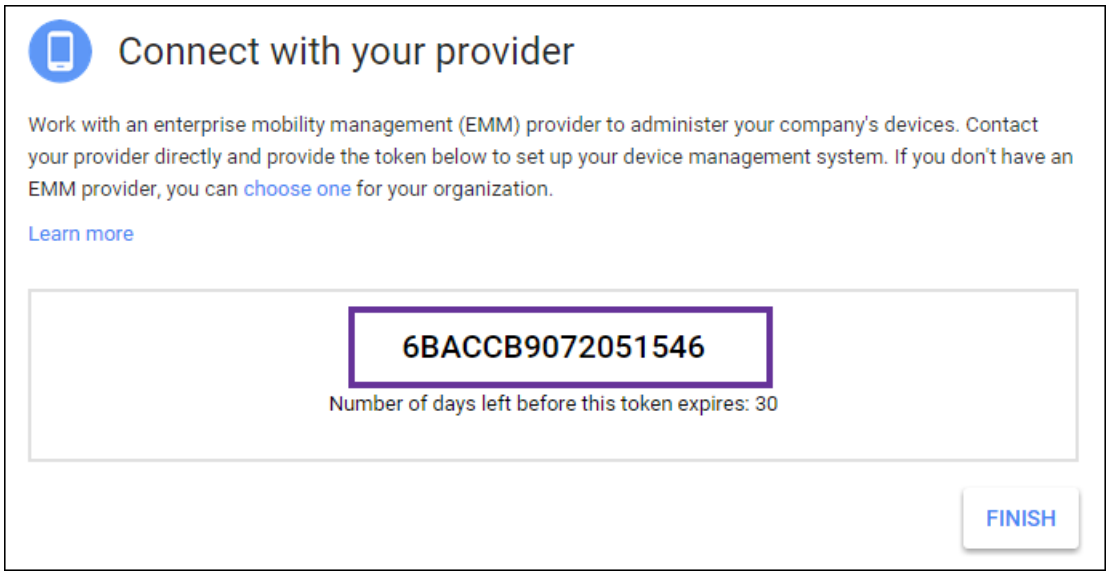
3. Google verifica que usted es el propietario del dominio.



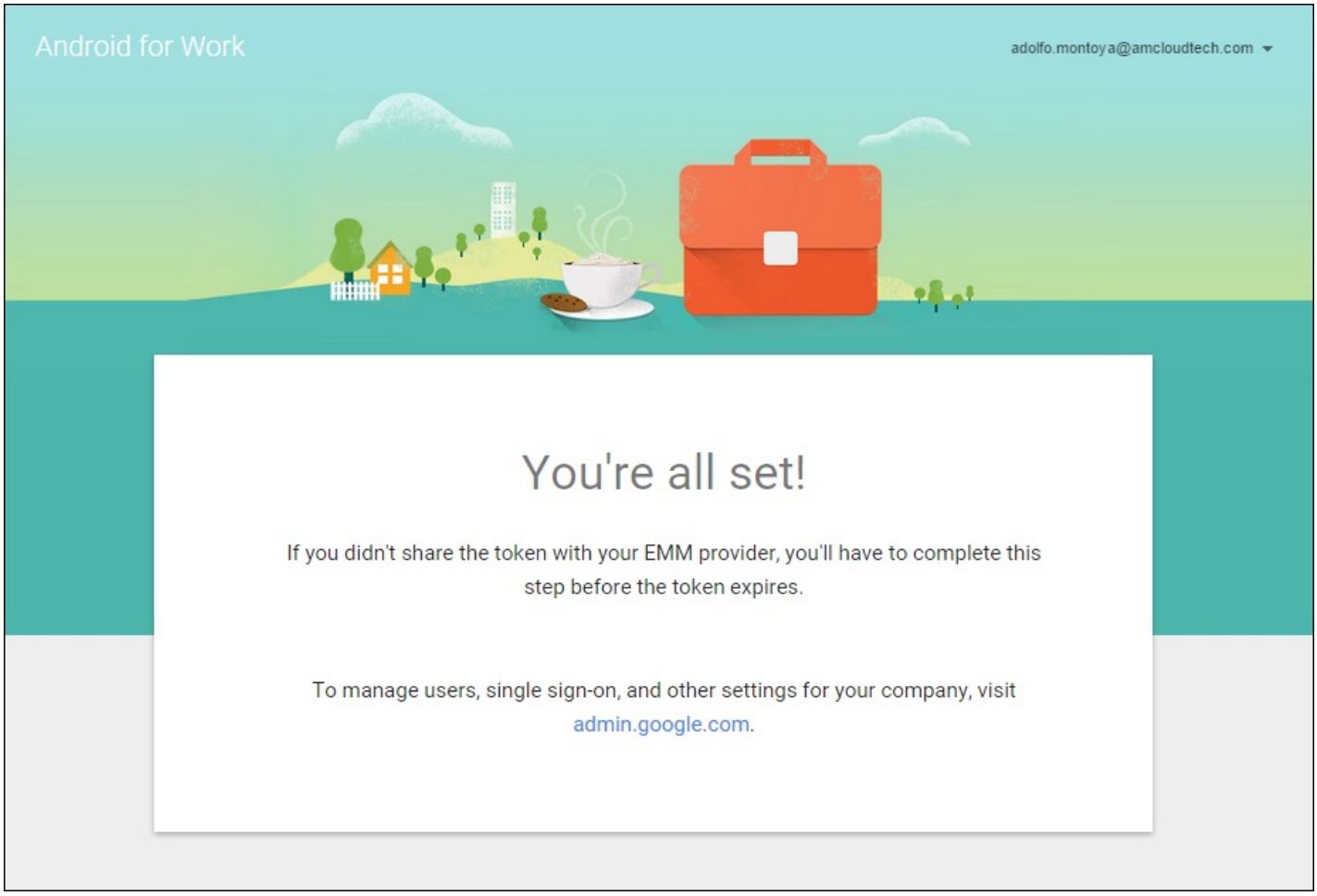
4. Aparecerá la siguiente página tras una verificación correcta. Haga clic en **Continuar**.



5. Google crea un token de vinculación de EMM que usted debe suministrar a Citrix y usarlo para configurar los parámetros de Android for Work. Copie y guarde el token, porque lo necesitará más adelante durante el procedimiento de configuración.



6. Haga clic en **Finish** para completar la configuración de Android for Work.



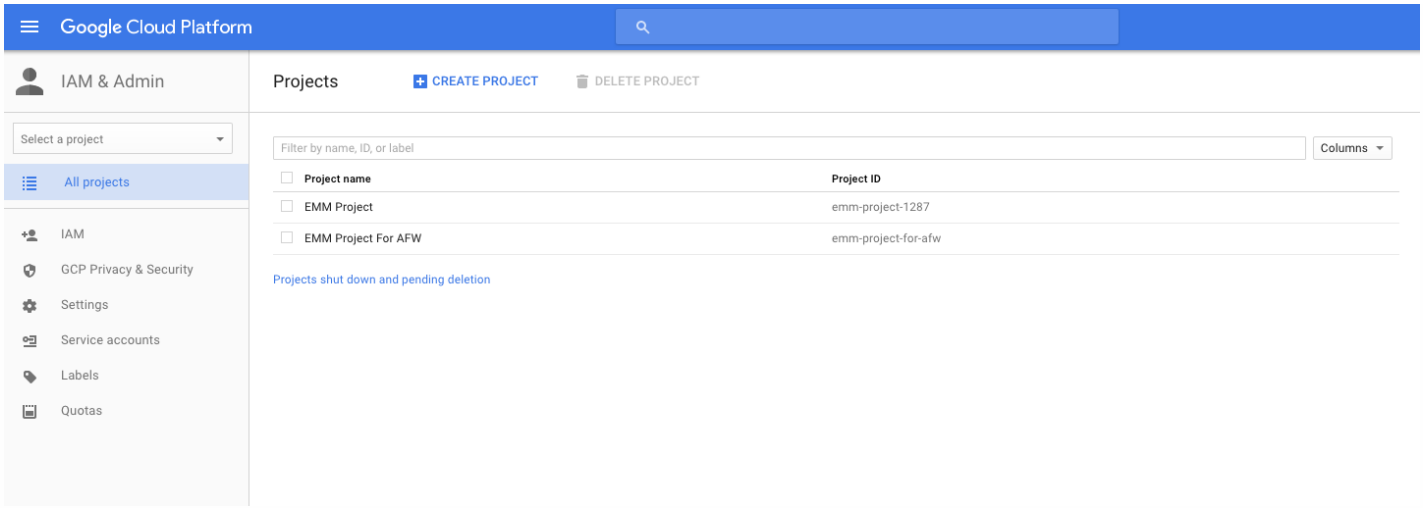
Después de crear una cuenta de servicio de Android for Work, puede iniciar sesión en la consola de administración de Google para administrar las opciones de movilidad de Android for Work.

Cómo configurar una cuenta de servicio de Android for Work y descargar un certificado de Android for Work

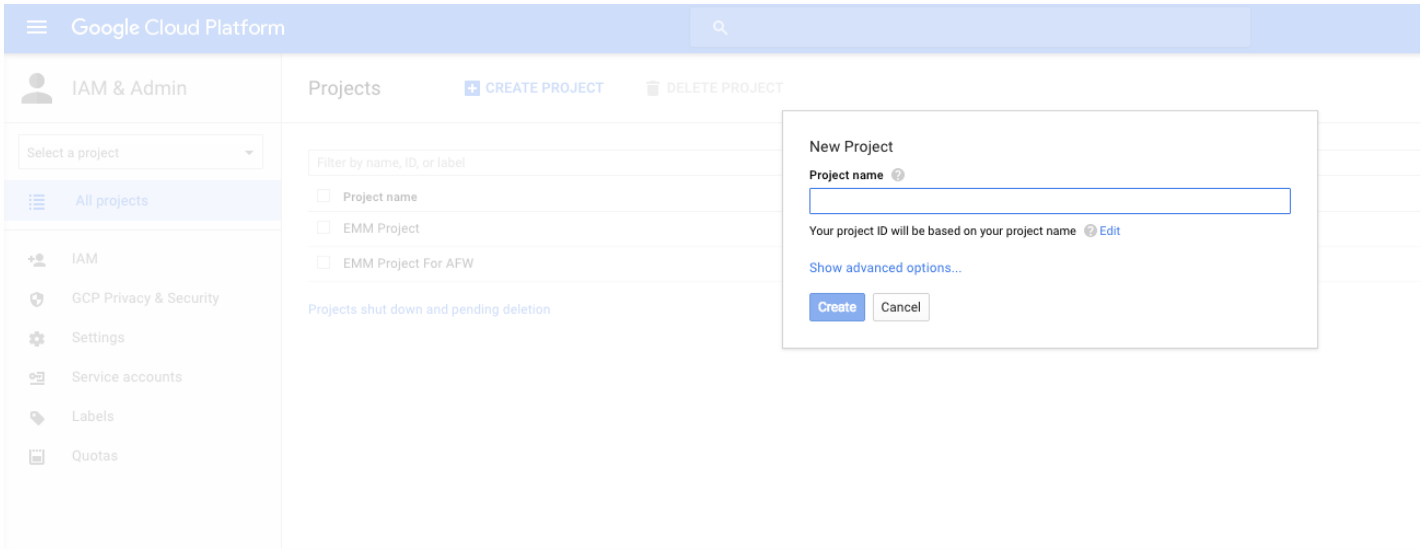
Para permitir que XenMobile establezca contacto con los servicios de Google Play y Google Directory, debe crear una nueva cuenta de servicio con la ayuda del portal de proyectos de Google para desarrolladores. Esta cuenta de servicio se utiliza para la comunicación de servidor a servidor entre XenMobile y los servicios de Google para Android for Work. Para obtener más información acerca del protocolo de autenticación que se utiliza, vaya a https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. En un explorador Web, vaya a https://console.cloud.google.com/project e inicie sesión con las credenciales de administración de Google.

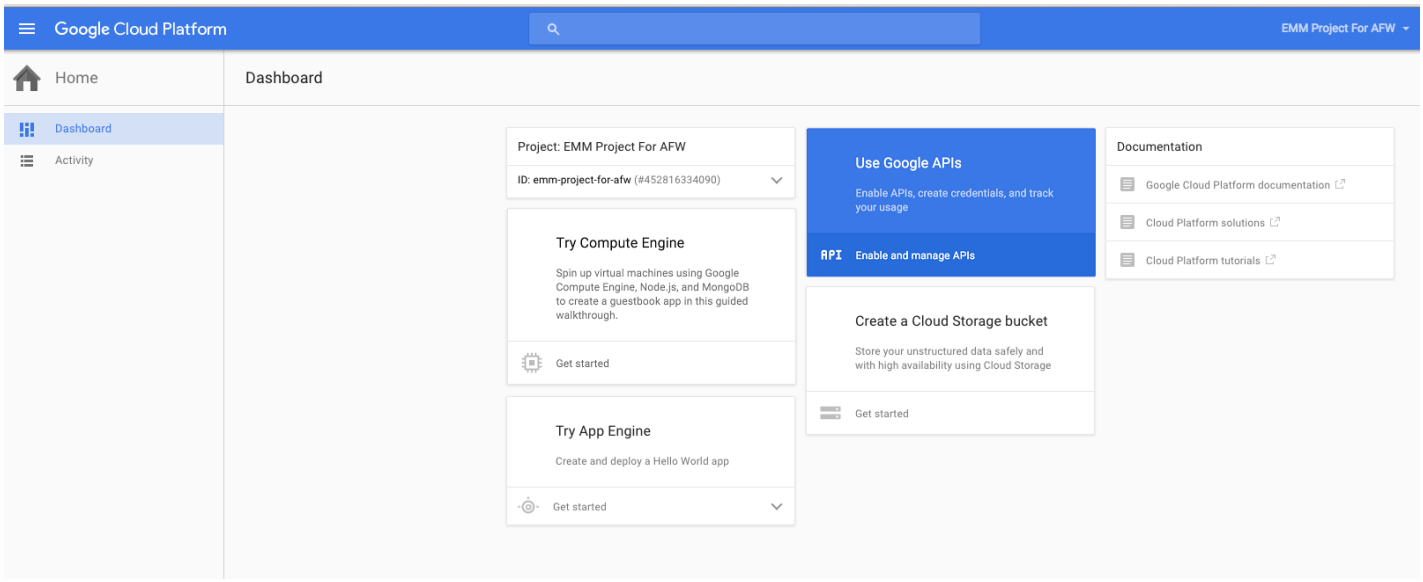
2. En la lista **Projects** , haga clic en **Create Project**.



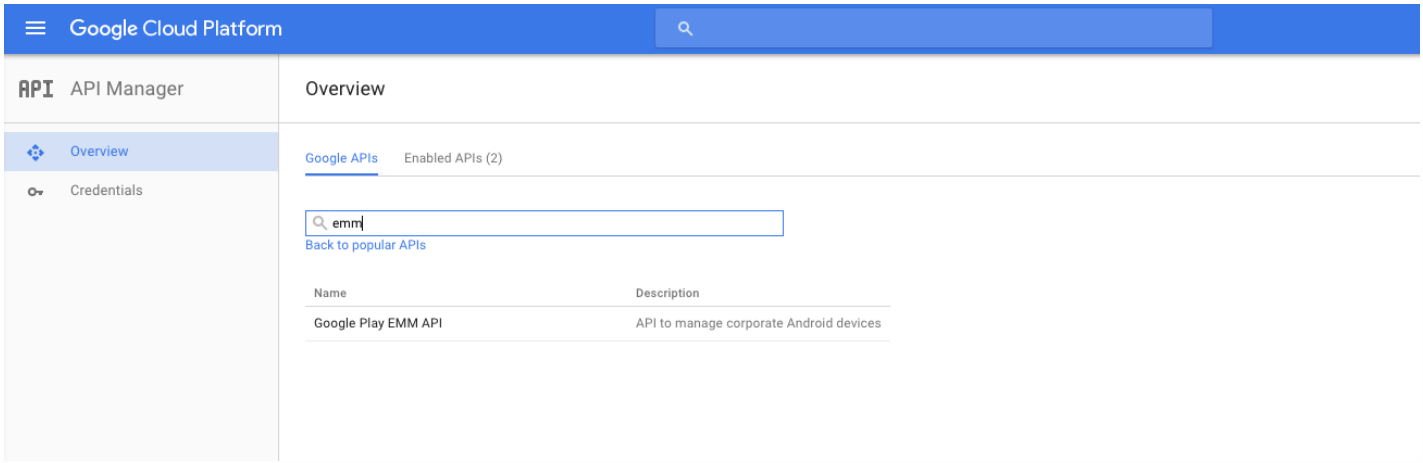
3. En **Project name**, introduzca un nombre para el proyecto.



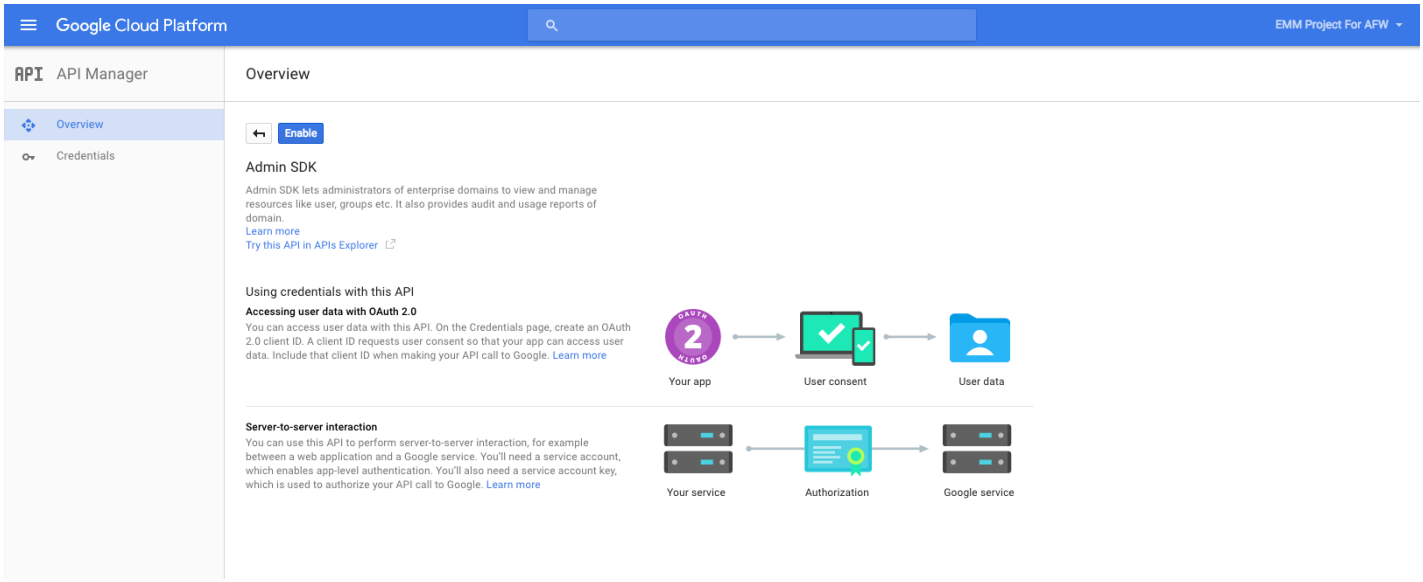
4. En el panel de mandos, haga clic en **Use Google APIs**.



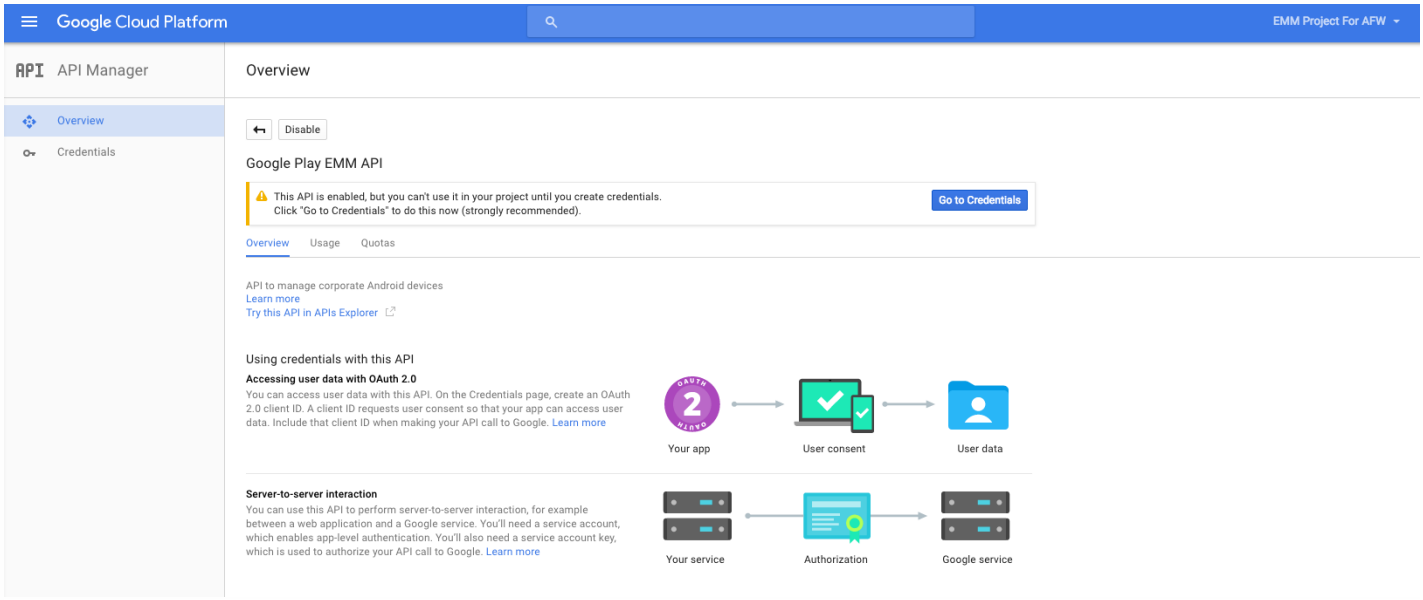
5. En la página Google APIs, en **Search**, introduzca **EMM** y luego haga clic en el resultado de la búsqueda.



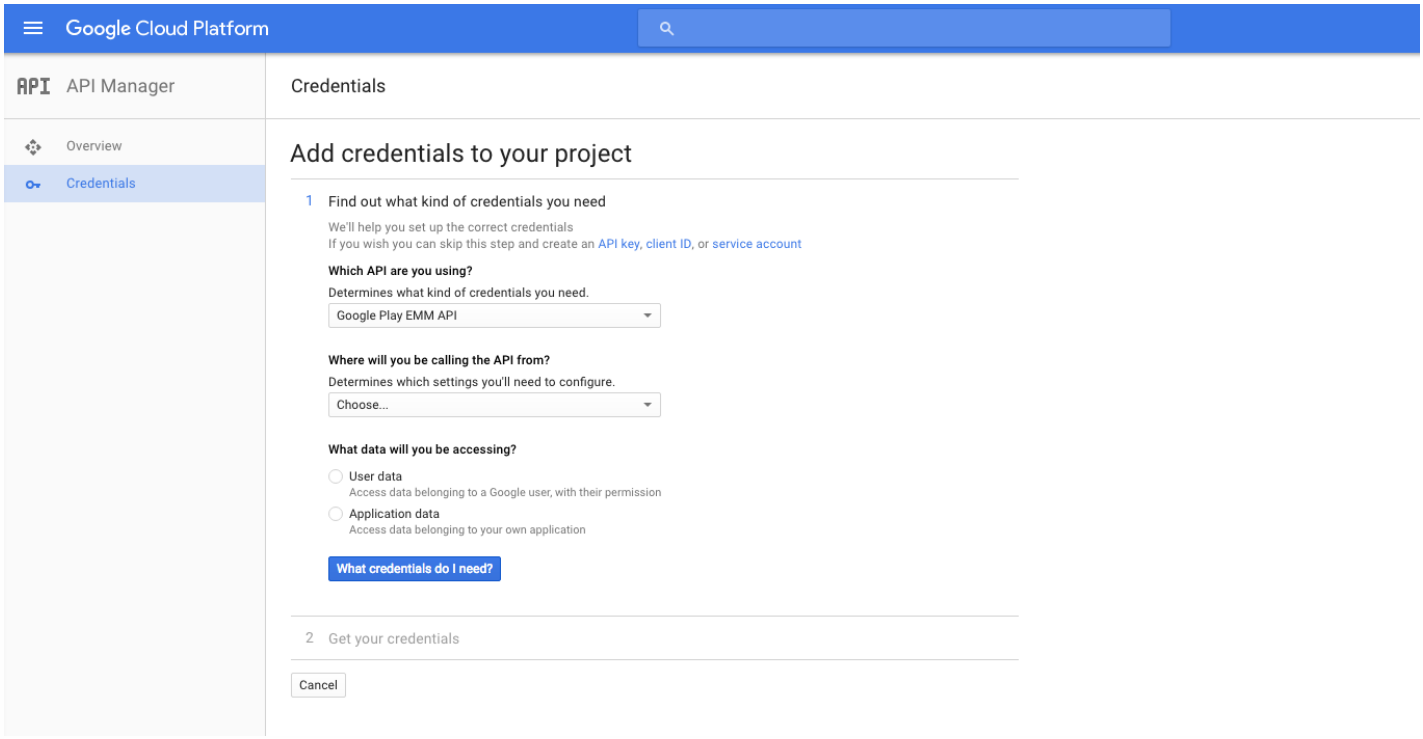
6. En la página Overview, haga clic en **Enable**.



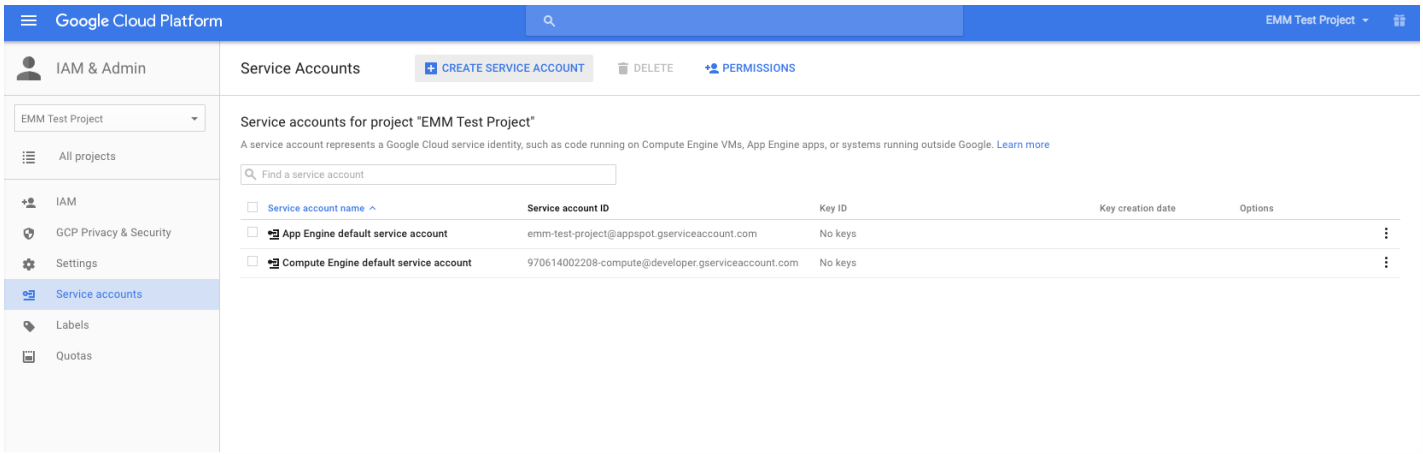
7. Junto a **Google Play EMM API**, haga clic en **Go to Credentials**.



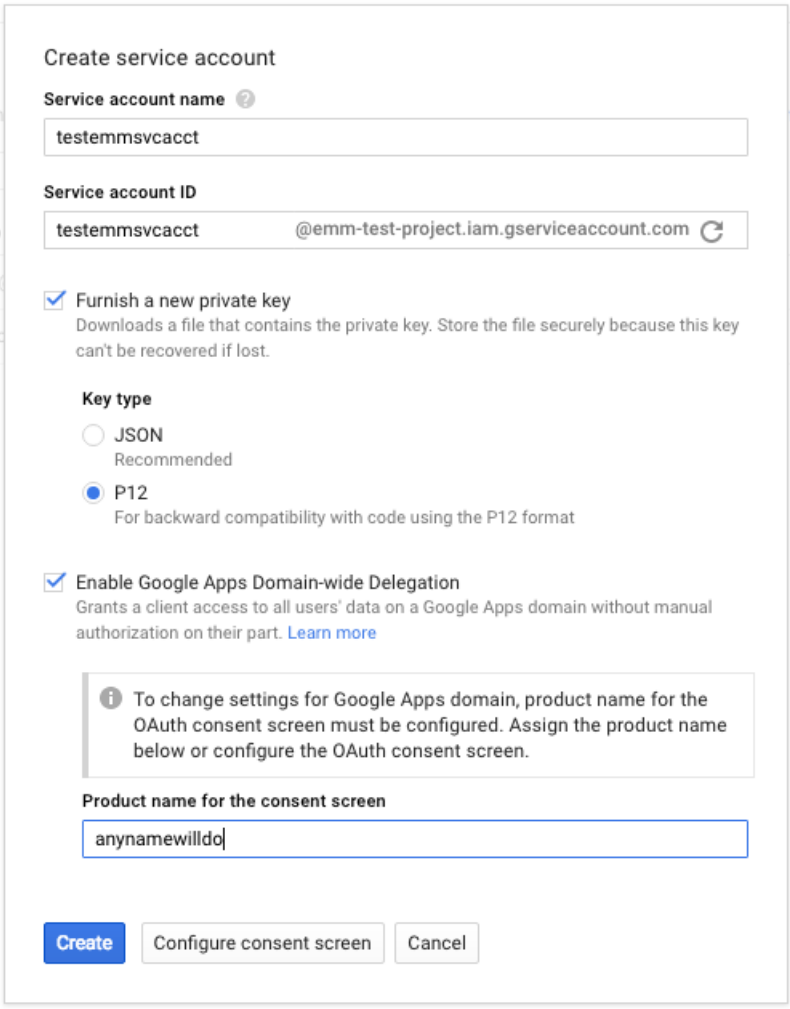
8. En la lista **Add credentials to our project**, en el paso 1, haga clic en **service account**.



9. En la página **Service Accounts** , haga clic en **Create Service Account**.

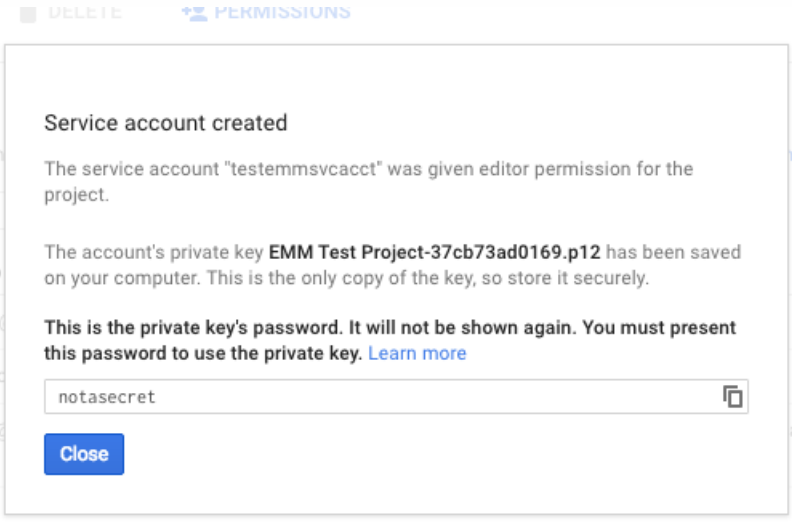


10. En **Create service account key** dé un nombre a la cuenta, marque la casilla **Furnish a new private key**, haga clic en **P12**, marque la casilla **Enable Google Apps Domain-wide Delegation** y haga clic en **Create.**

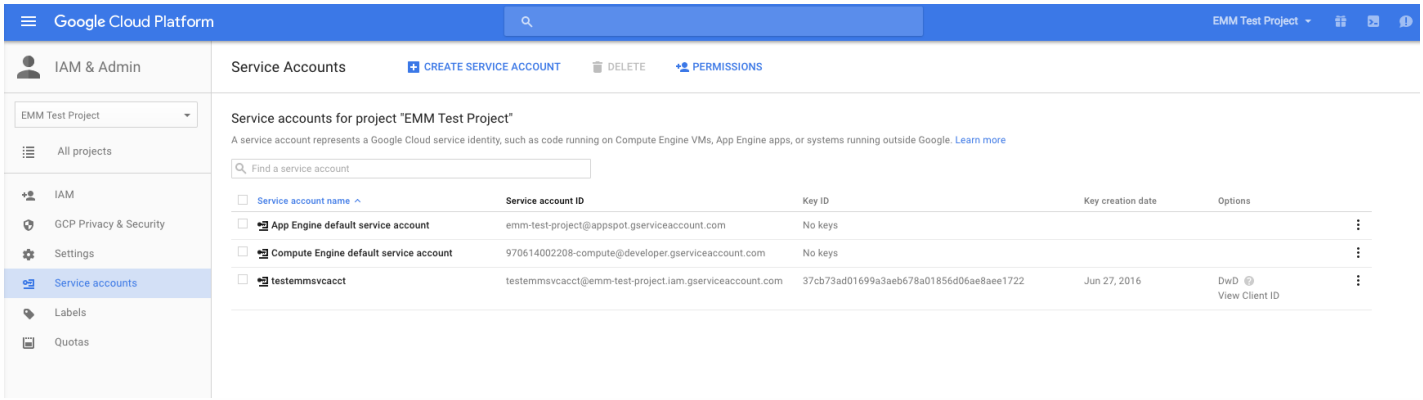


El archivo de certificado (P12) se descargará en su equipo. Asegúrese de guardar el certificado en una ubicación segura.

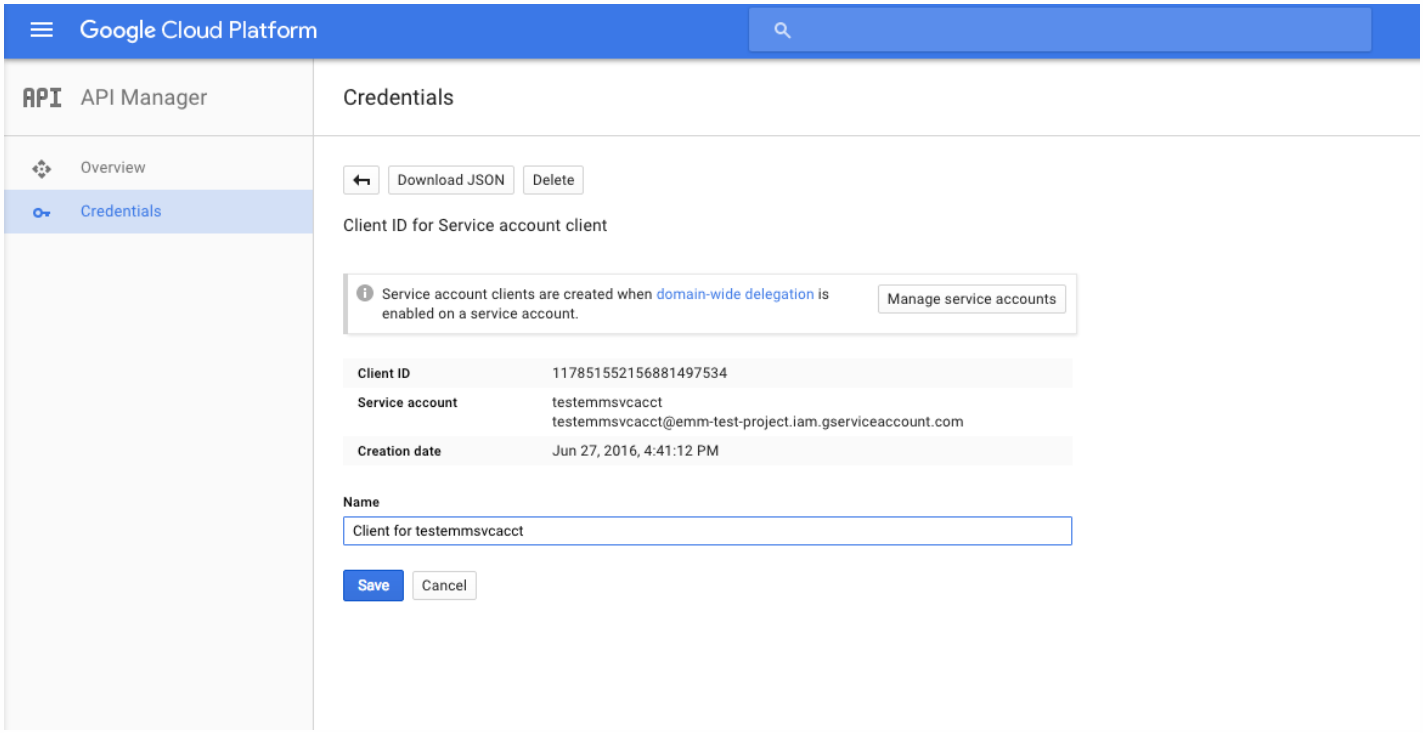
11. En la pantalla de confirmación **Service account created**, haga clic en **Close**.



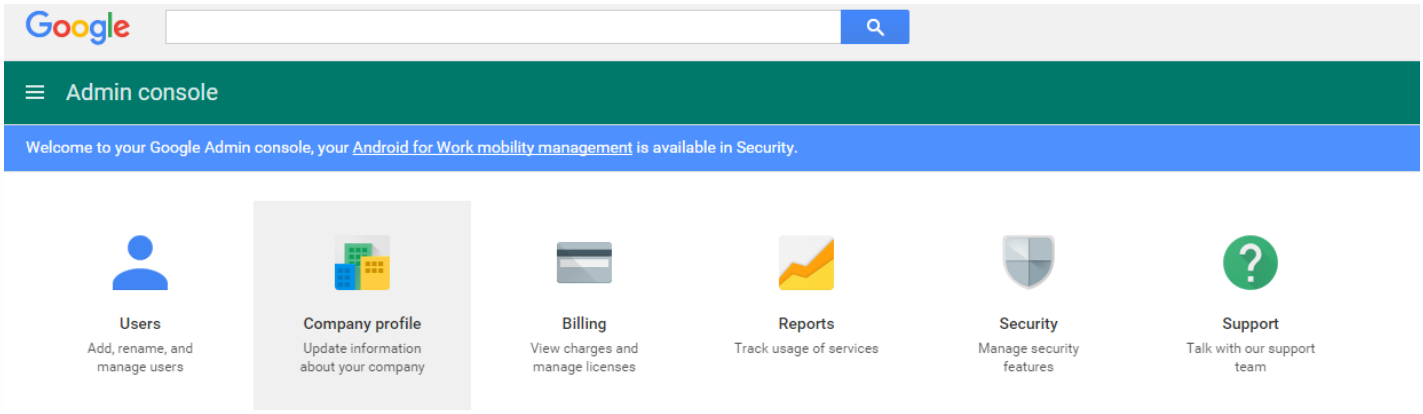
12. En **Permissions**, haga clic en **Service accounts** y después, bajo **Options**, para su cuenta de servicio, haga clic en **View Client ID**.



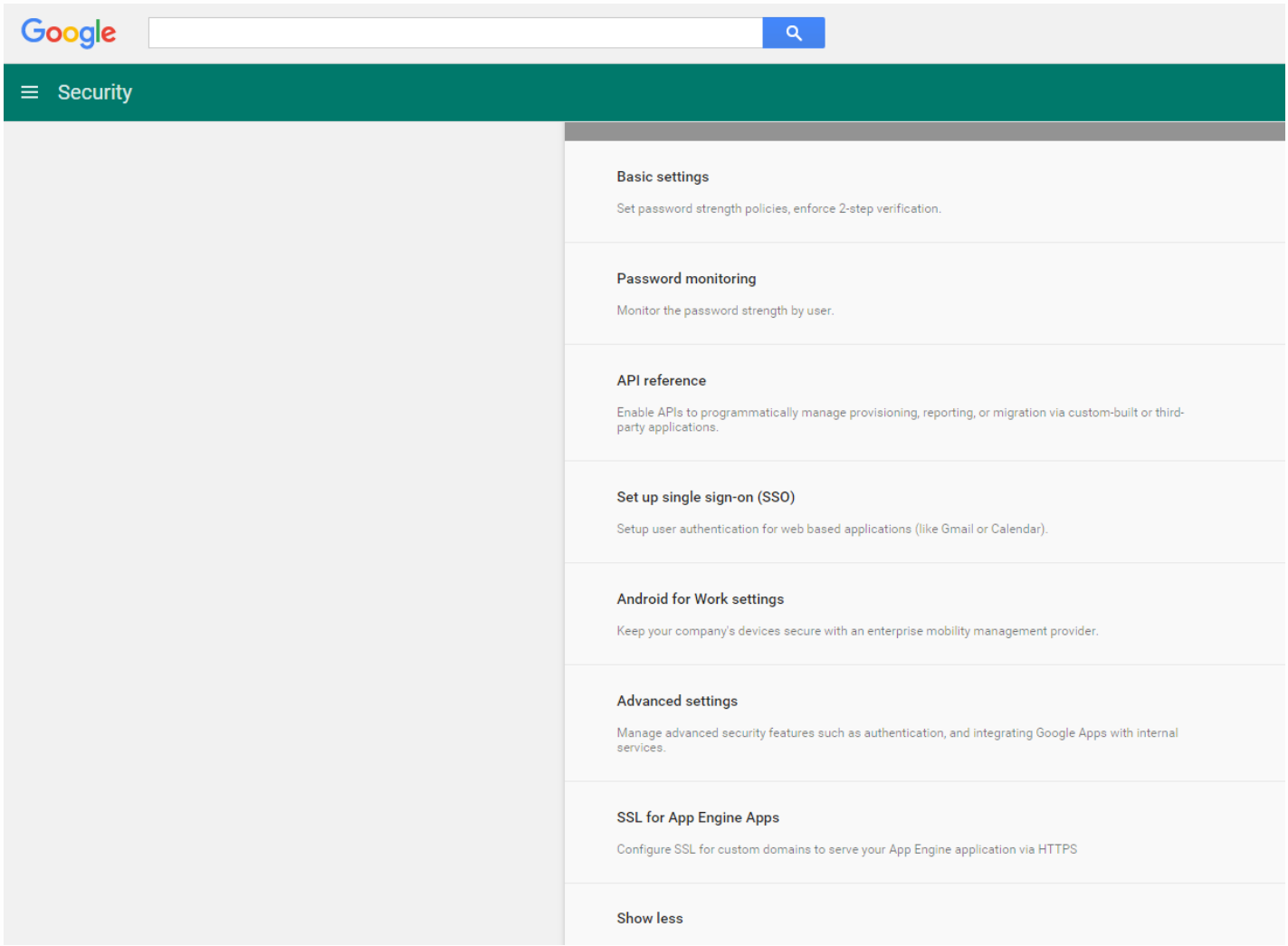
13. Aparecerán los detalles requeridos para la autorización de cuentas en la consola de administración de Google. Copie los valores de **Client ID** y **Service account ID** en una ubicación donde pueda encontrarlos más adelante. Necesitará esta información, junto con el nombre de dominio, para enviarla a Citrix para su inclusión en una lista blanca.



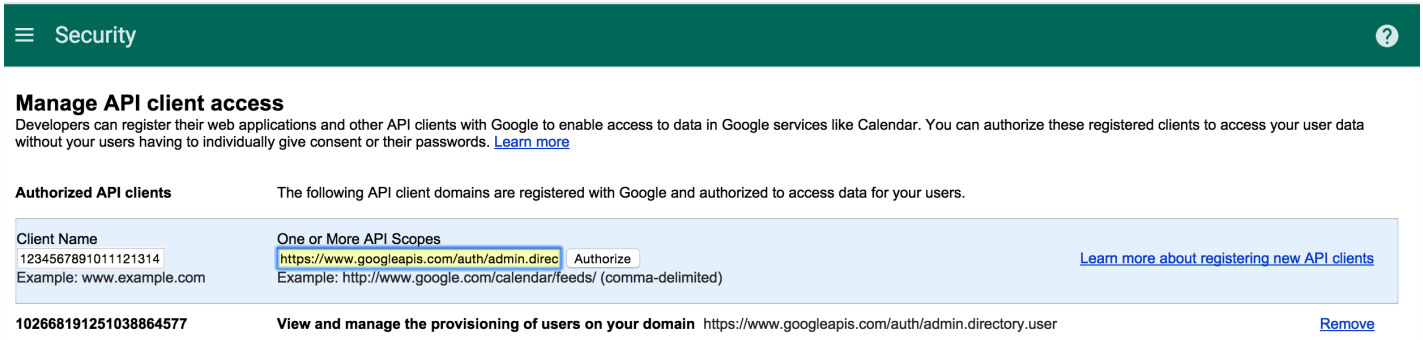
14. Abra la consola de administración de Google para su dominio y haga clic en **Security**.



15. Haga clic en **Android for Work settings**.



16. En **Client Name**, introduzca el ID de cliente que guardó previamente, en **One or More API Scopes**, introduzca https://www.googleapis.com/auth/admin.directory.user y haga clic en **Authorize**.

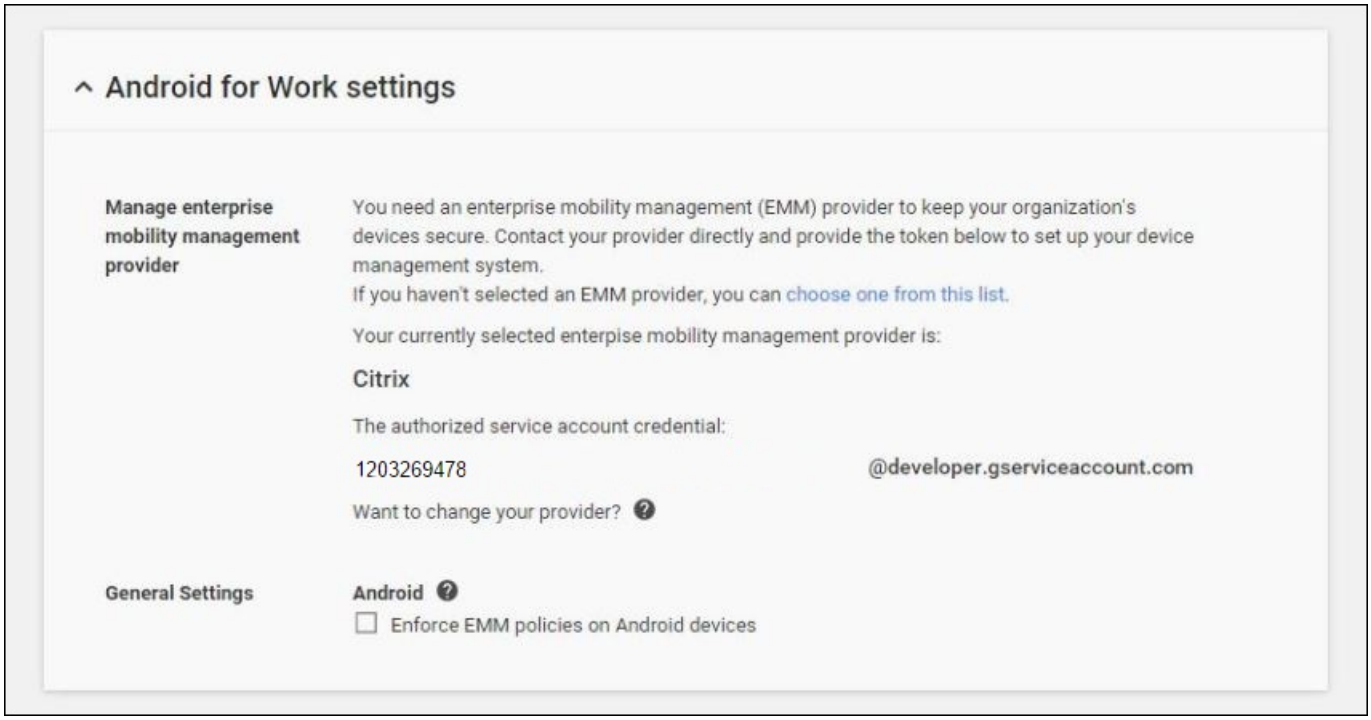


Vinculación a EMM

Antes de utilizar XenMobile para administrar los dispositivos Android for Work, debe ponerse en contacto con el servicio de asistencia técnica de Citrix (https://www.citrix.com/contact/technical-support.html) y proporcionarles su nombre de dominio, cuenta de servicio y token de vinculación. Citrix vinculará el token con XenMobile como proveedor de administración de movilidad empresarial (EMM).

1. Para confirmar la vinculación, inicie sesión en el portal de administración de Google y haga clic en **Security**.

2. Haga clic en **Android for Work settings**. Verá que su cuenta de Google Android for Work aparece vinculada a Citrix como su proveedor EMM.



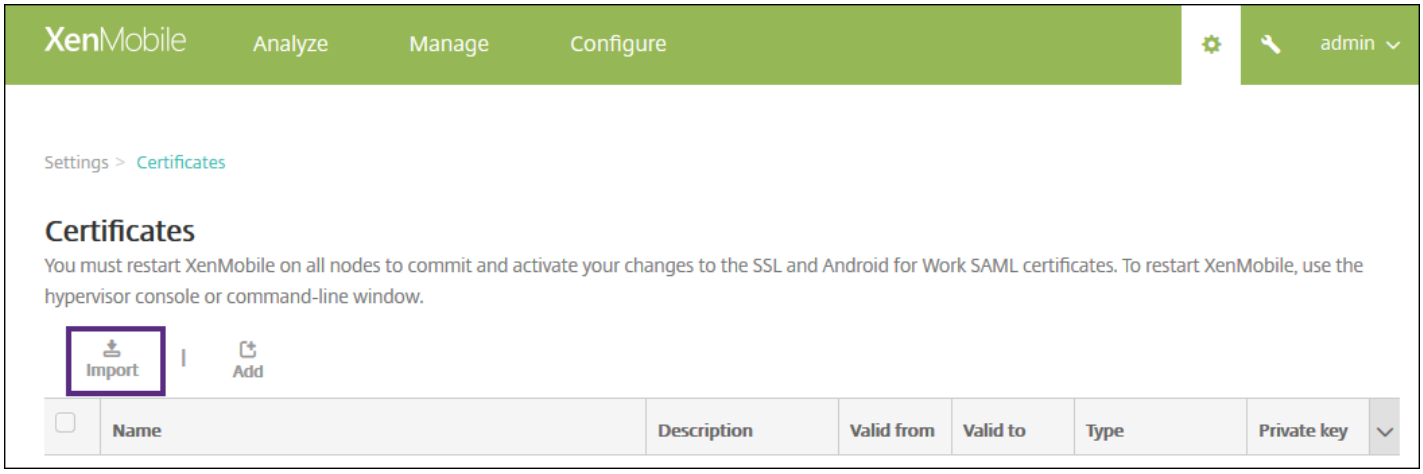
Después de confirmar la vinculación con el token, ya puede empezar a usar XenMobile para administrar sus dispositivos Android for Work. Debe importar el certificado P12 que generó en el paso 14, configurar los parámetros del servidor de Android for Work, habilitar el inicio de sesión Single Sign-on basado en SAML y definir al menos una directiva de dispositivo para Android for Work.

Importación del certificado P12

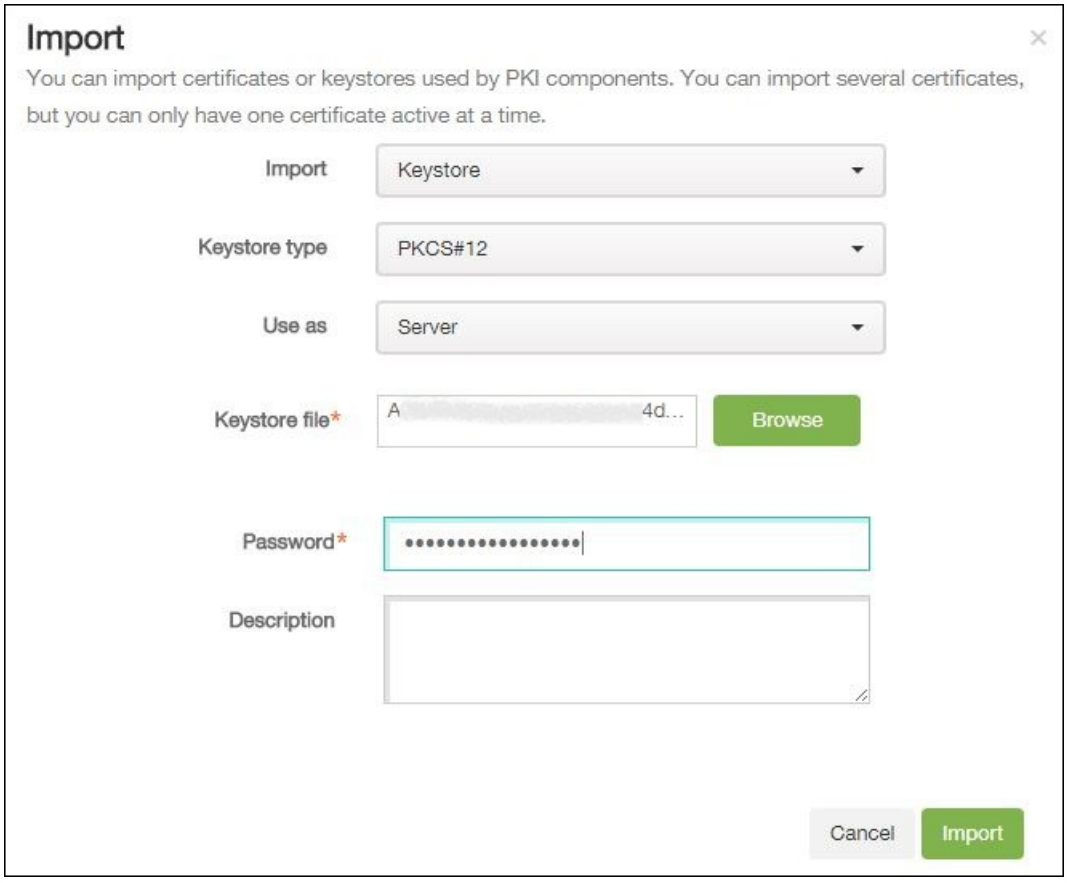
Siga estos pasos para importar el certificado P12 de Android for Work:

1. Inicie sesión en la consola de XenMobile.

2. Haga clic en el icono con forma de engranaje ubicado en la esquina superior derecha de la consola para abrir la página **Settings** y, a continuación, haga clic en **Certificates**. Aparecerá la página **Certificates**.



3. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.



Configure los siguientes parámetros:

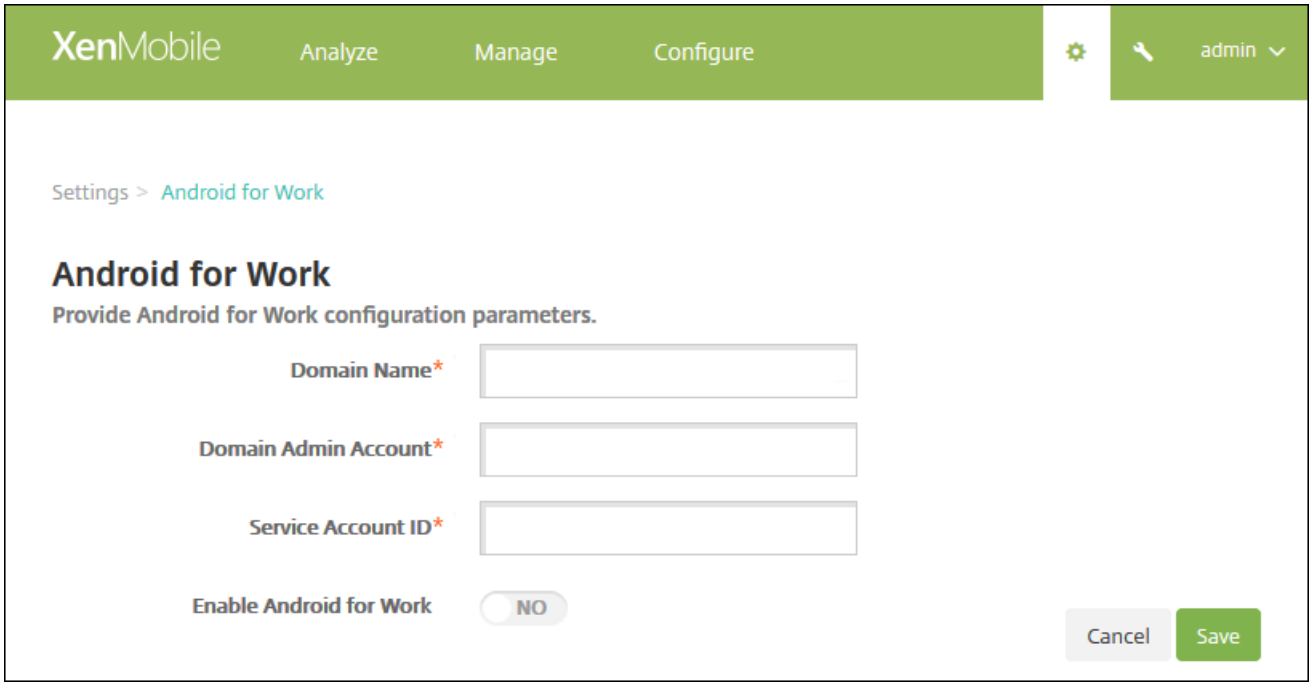
- **Import**. Seleccione **Keystore** en la lista.
- **Keystore type**. Seleccione **PKCS#12** en la lista.
- **Use as**. Seleccione **Server** en la lista.
- **Keystore file**. Haga clic en **Browse** y vaya al certificado P12.
- **Password**: Escriba la contraseña del almacén de claves.
- **Description**. Si quiere, escriba una descripción del certificado.

4. Haga clic en **Import**.

Configuración de los parámetros de servidor de Android for Work

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **Android for Work**. Aparecerá la página **Android for Work**.



Configure los siguientes parámetros:

- **Domain name**. Introduzca el nombre de dominio de Android for Work. Por ejemplo: dominio.com
- **Domain Admin Account**: Introduzca el nombre de usuario del administrador del dominio; por ejemplo la cuenta de correo electrónico utilizada en el portal Google Developer Portal.
- **Service Account ID**: Introduzca el ID de cuenta de servicio. Por ejemplo, el correo electrónico asociado a la cuenta de servicio de Google (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com).
- **Enable Android for Work**. Haga clic para habilitar o inhabilitar Android for Work.

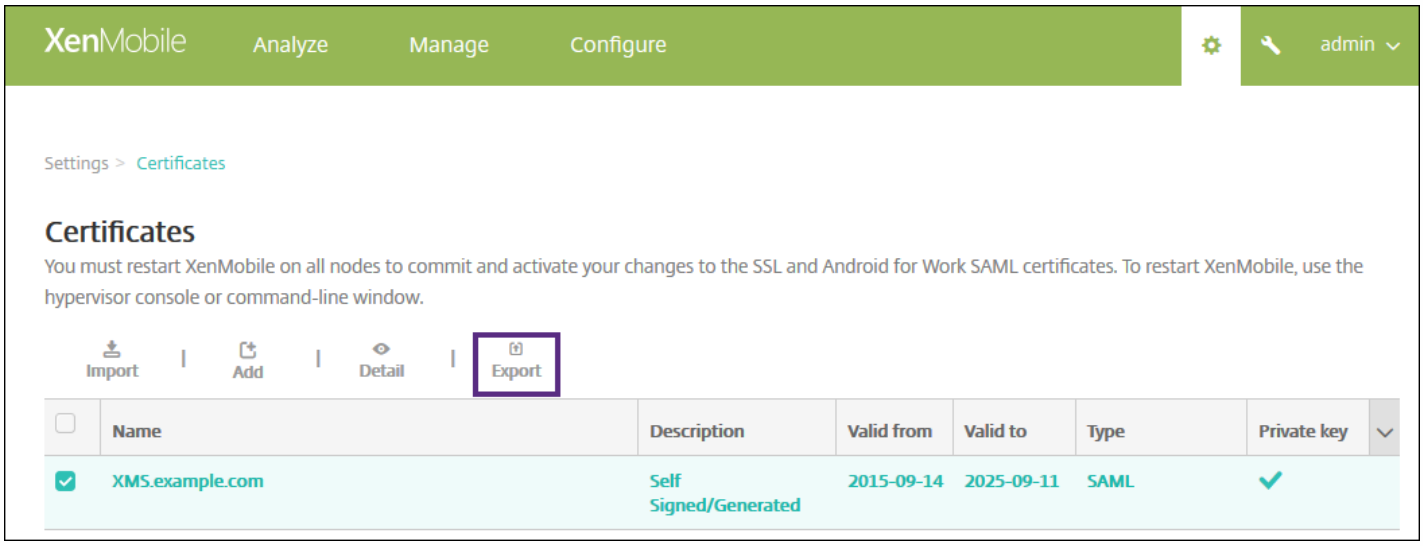
3. Haga clic en **Save**.

Habilitación del inicio de sesión Single Sign-on basado en SAML

1. Inicie sesión en la consola de XenMobile.

2. Haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

3. Haga clic en **Certificates**. Aparecerá la página **Certificates**.

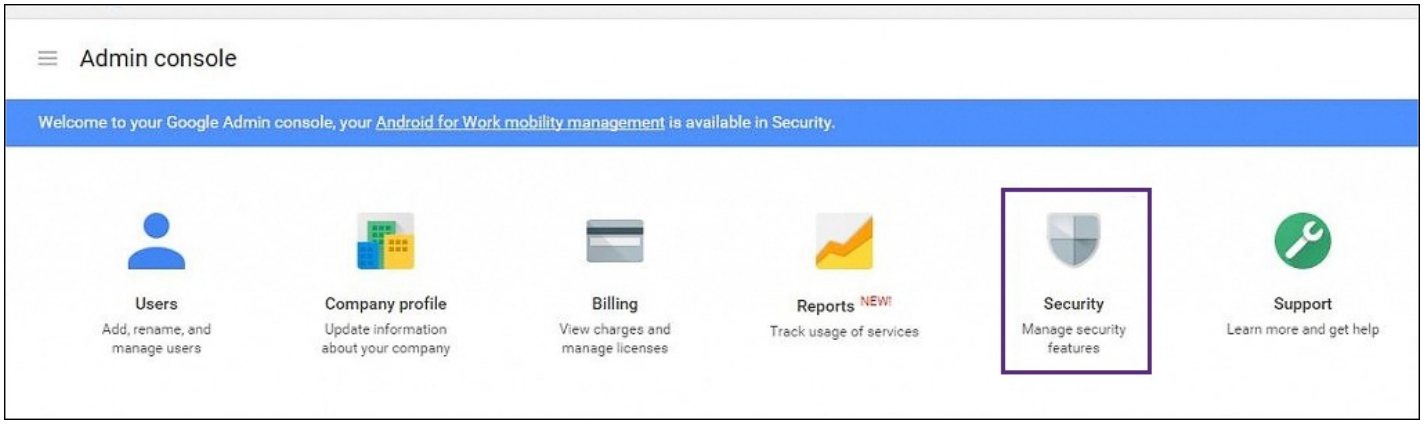


3. En la lista de certificados, haga clic en el certificado SAML.

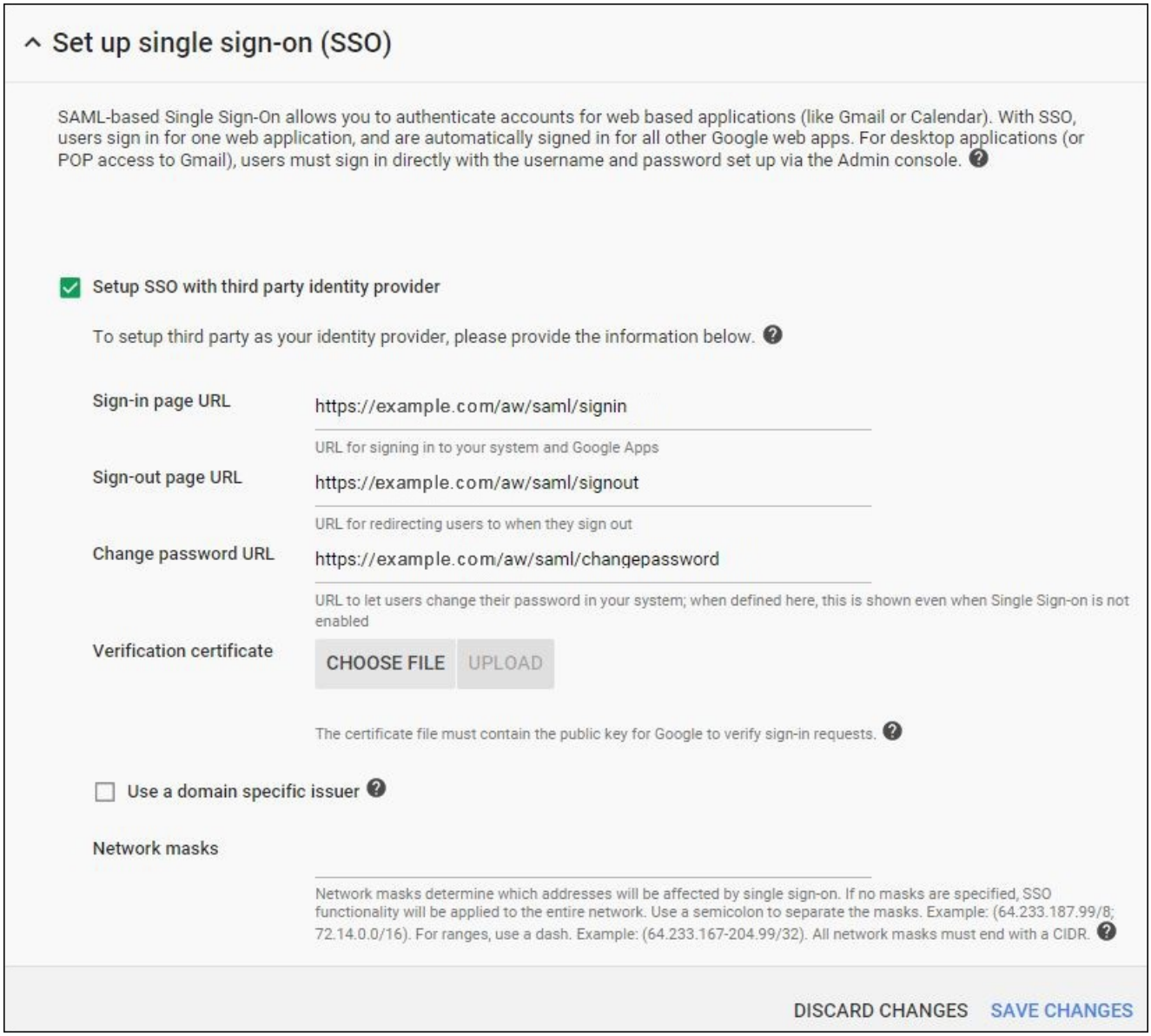
4. Haga clic en **Export** y guarde el certificado en su equipo.

5. Inicie sesión en el portal de administración de Google (https://admin.google.com) con las credenciales de administrador de Android for Work.

6. Haga clic en **Security**.



7. En **Security**, haga clic en **Set up single sign-on (SSO)** y configure los parámetros siguientes:

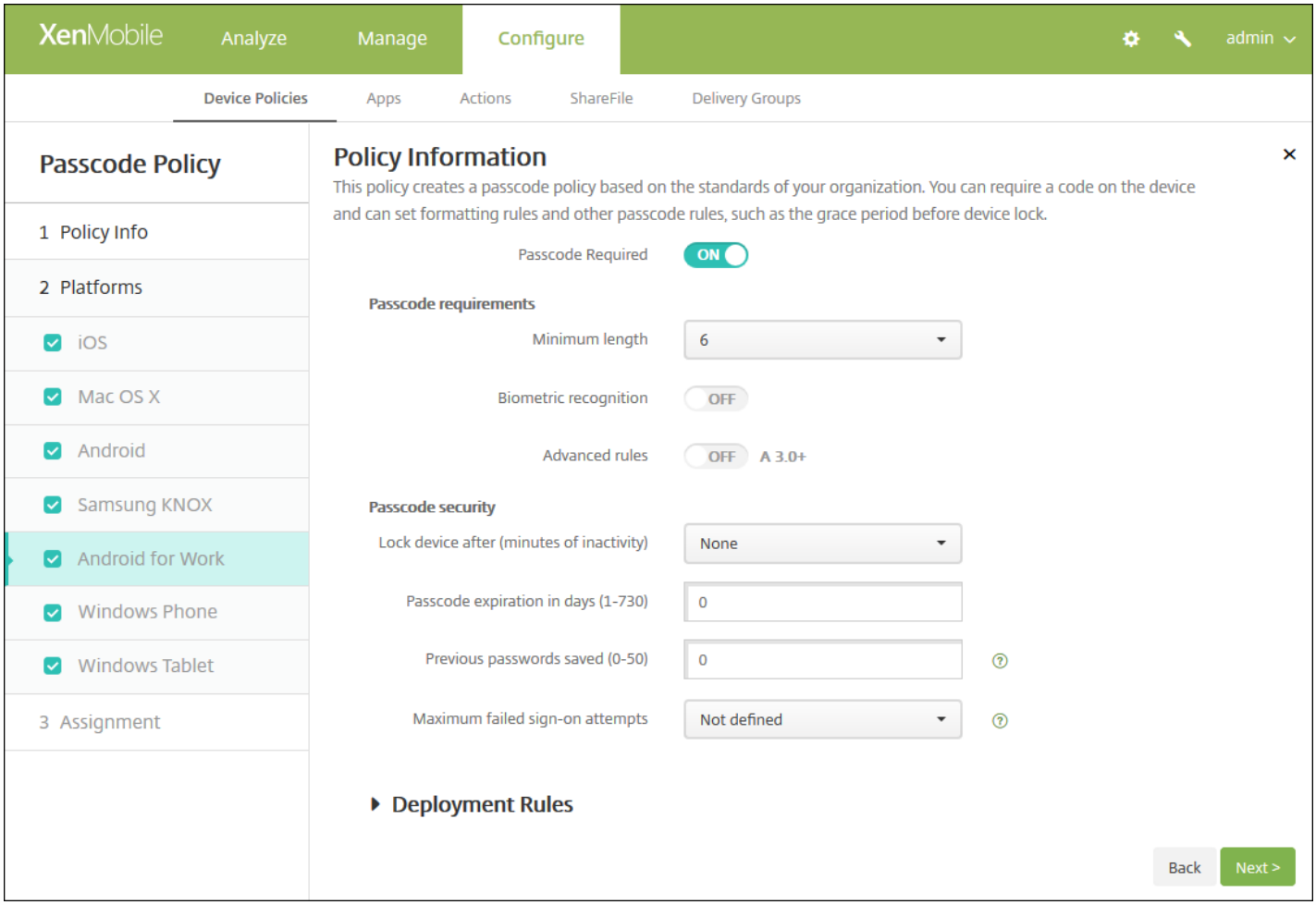


- **Sign-in page URL**: Introduzca la URL para que los usuarios inicien sesiones en el sistema y Google Apps. Por ejemplo: https:///aw/saml/signin.
- **Sign-out page URL**: Introduzca la dirección URL a la que se redirige a los usuarios cuando cierran la sesión. Por ejemplo: https:///aw/saml/signout.
- **Change password URL**: Introduzca la dirección URL para permitir que los usuarios cambien su contraseña en el sistema. Por ejemplo: https:///aw/saml/changepassword. Si esto está definido aquí, los usuarios ven esto aunque SSO no esté disponible.
- **Verification certificate**: Haga clic en CHOOSE FILE y busque el certificado SAML exportado desde XenMobile.

8. Haga clic en **SAVE CHANGES** para guardar los cambios.

Configuración de una directiva de dispositivo para Android for Work

Puede configurar cualquier directiva de dispositivo que desee, pero es conveniente configurar una directiva de código de acceso, para requerir que los usuarios definan un código de acceso en sus dispositivos la primera vez que los inscriben.



Estos son los pasos básicos para configurar una directiva de dispositivo:

1. Inicie sesión en la consola de XenMobile.

2. Haga clic en **Configure->Device Policies**.

3. Haga clic en **Add** y seleccione la directiva que desee agregar desde el cuadro de diálogo **Add a New Policy** (en este ejemplo, tendría que seleccionar **Passcode**).

4. Complete la página **Policy Information**.

5. Haga clic en **Android for Work** y configure los parámetros de la directiva.

6. Asigne la directiva a un grupo de entrega.

Para obtener más información sobre cómo definir otras directivas de dispositivo que están disponibles para Android for Work, consulte Directivas de dispositivos de XenMobile desglosadas por plataforma.

Configuración de parámetros de cuenta para Android for Work

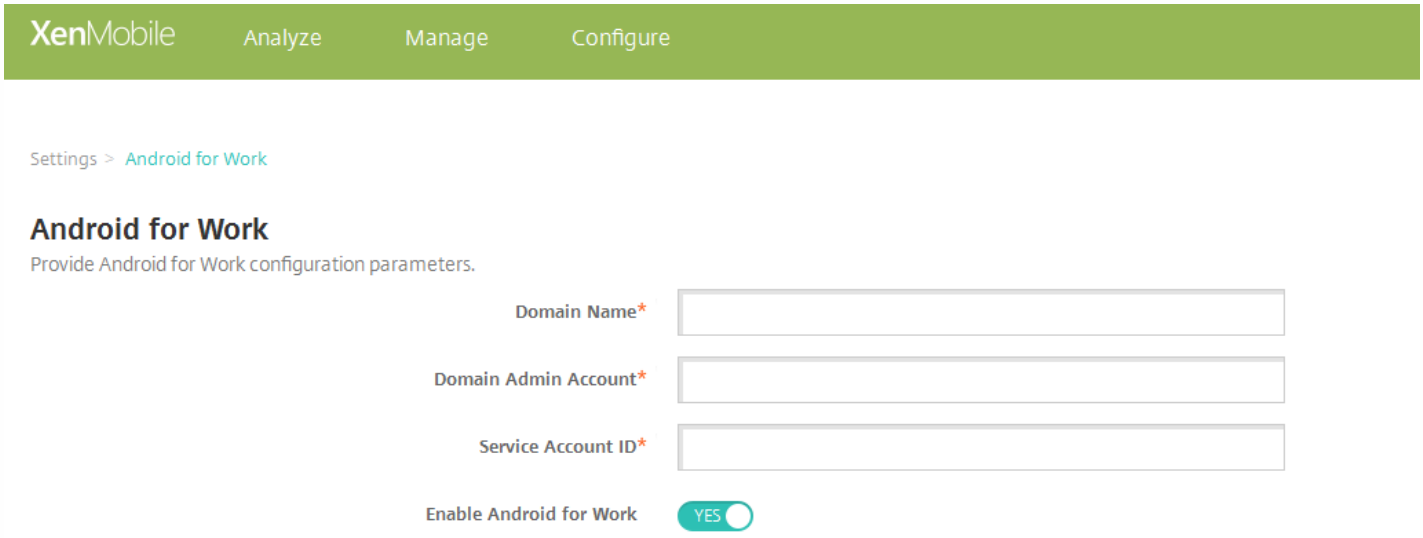
Jul 27, 2016

> ## Advertencia
>
> Existe un problema conocido de terceros que impide usar la consola de XenMobile para habilitar Android for Work. Para ver más información sobre este problema y cómo configurar una propiedad de servidor como solución temporal, consulte el apartado #615118 de los Problemas conocidos de XenMobile Server 10.3.

En XenMobile, antes de empezar a administrar aplicaciones y directivas Android for Work en los dispositivos de los usuarios, debe configurar la información de la cuenta y del dominio de Android for Work. Antes de ello, debe completar las tareas de configuración de Android for Work en Google para definir un administrador de dominio y obtener un ID de cuenta de servicio, así como un token de enlace. Para obtener más información acerca de las tareas de configuración de Android for Work en Google, consulte Managing Devices with Android for Work.

1. En la consola Web de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. Aparecerá la página **Settings**.

2. En **Server**, haga clic en **Android for Work**. Aparecerá la página de configuración **Android for Work**.



3. En la página **Android for Work**, configure los siguientes parámetros:

- **Domain Name**. Introduzca el nombre de dominio.
- **Domain Admin Account**. Escriba el nombre de usuario del administrador de dominio.

- **Service Account ID**. Escriba el ID de la cuenta de servicio de Google.
- **Enable Android for Work**. Seleccione si habilitar Android for Work.

4. Haga clic en **Save**.

Aprovisionamiento de Android for Work con el modo Device Owner

Jul 27, 2016

Para aprovisionar Android for Work en modo Device Owner, debe transferir datos a través de una conexión NFC (Near-Field Communications) entre dos dispositivos, uno que ejecuta la herramienta Worx Provisioning Tool, y otro restaurado con sus parámetros de fábrica, siguiendo los pasos descritos en este documento. El modo Device Owner está disponible solo para dispositivos que son propiedad de la empresa.

¿Por qué usar NFC? Bluetooth, WiFi y otros modos de comunicación están inhabilitados en un dispositivo que ha sido restablecido a sus parámetros de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede comprender en ese estado.

Para ver una descripción general de la implementación de Android for Work en el entorno de XenMobile, consulte Administración de dispositivos con Android for Work en XenMobile.

Requisitos previos

- Un servidor XenMobile habilitado para Android for Work, versiones 10.1 y 10.3.
- Un dispositivo con parámetros de fábrica, aprovisionado para Android for Work en modo Device Owner. Los pasos para hacer esto se describen abajo.
- Otro dispositivo con capacidades de comunicación NFC, ejecutando la herramienta Worx Provisioning Tool configurada. La herramienta Worx Provisioning Tool está disponible en Worx Home 10.3 en la página de descargas de Citrix.

Cada dispositivo solo puede tener un único perfil de Android for Work, administrado por una aplicación EMM de administración de movilidad empresarial (Enterprise Mobility Management). En XenMobile, Worx Home es la aplicación EMM. Solo se permite un perfil para cada dispositivo. Si se intenta agregar una segunda aplicación EMM, se eliminará la primera.

Puede iniciar el modo Device Owner en dispositivos totalmente nuevos sin configurar, o en dispositivos que han sido restaurados a sus parámetros de fábrica. Podrá administrar por completo el dispositivo con XenMobile.

Conexión NFC en modo Device Owner

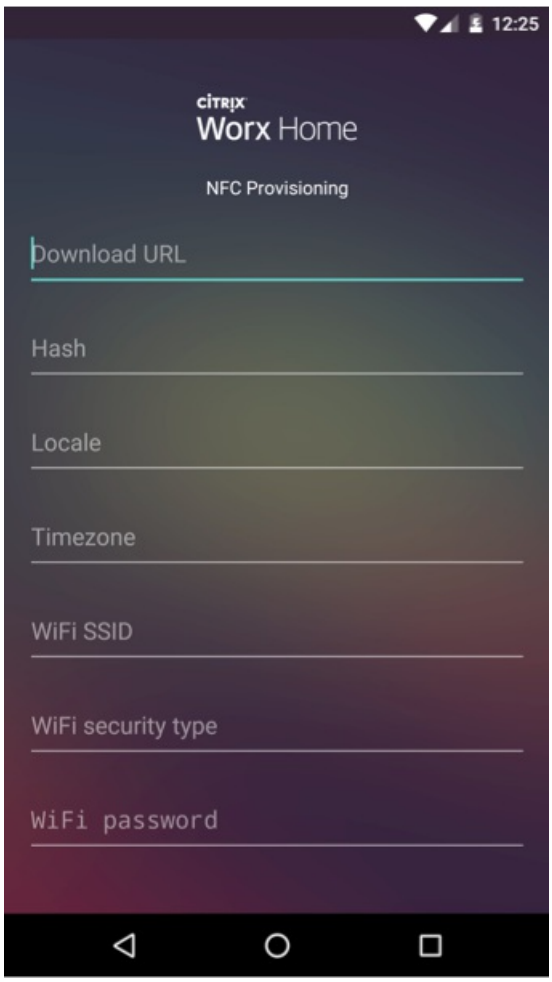
El aprovisionamiento de un dispositivo restablecido con parámetros de fábrica requiere que usted envíe los siguientes datos vía conexión NFC para activar Android for Work:

- Nombre del paquete de la aplicación de proveedor EMM que actuará como Device Owner (Worx Home).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación de proveedor EMM.
- Valor hash SHA1 de la aplicación de proveedor EMM para verificar si la descarga fue correcta.
- Detalles de conexión WiFi para que un dispositivo restablecido con parámetros de fábrica pueda conectar y descargar la aplicación de proveedor EMM. (Android no respalda actualmente WiFi 802.1x para este flujo de trabajo).
- Zona horaria del dispositivo (optativo).
- Ubicación geográfica del dispositivo (optativo).

Cuando los dos dispositivos se conectan por NFC, los datos de la herramienta Worx Provisioning Tool se envían al dispositivo restablecido con parámetros de fábrica. Esos datos se utilizan para descargar Worx Home con los parámetros del administrador. Si no introduce valores para la zona horaria y la ubicación geográfica, Android los configurará automáticamente en el nuevo dispositivo.

Configuración de la herramienta Worx Provisioning Tool

Antes de hacer una conexión NFC, es necesario configurar la herramienta Worx Provisioning Tool. Esta configuración se transfiere, a continuación, al dispositivo restablecido con parámetros de fábrica durante la conexión NFC.



Puede introducir los datos en los campos requeridos o rellenar los campos mediante un archivo de texto. La aplicación no guarda información una vez introducida ésta, por lo que puede ser conveniente crear un archivo de texto para conservar esa información para el futuro.

Configuración mediante un archivo de texto

Nombre el archivo **nfcprovisioning.txt** y colóquelo en la tarjeta SD del dispositivo en la carpeta /sdcard/Downloads. La aplicación leerá el archivo de texto y rellenará los valores.

El archivo de texto debe contener los datos siguientes:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
Esta es la ubicación de la intranet o de Internet donde se encuentra la aplicación de proveedor EMM. Después de que el dispositivo restablecido con parámetros de fábrica se conecta a la red WiFi a continuación de la conexión NFC (usando el SSID, tipo de seguridad y contraseñas introducidos en la pantalla anterior), debe tener acceso a esta ubicación para la descarga. La dirección URL es una dirección URL normal, sin formato especial.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=

Esta es la suma de comprobación de la aplicación de proveedor EMM. Se usa para verificar que la descarga se realizó correctamente. Los pasos para obtenerla se describen a continuación.

android.app.extra.PROVISIONING_WIFI_SSID=
Este es el SSID del dispositivo conectado por WiFi donde se está ejecutando la herramienta Worx Provisioning Tool.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
Los valores admitidos son WEP y WPA2. Si la red WiFi no está protegida, este campo debe estar vacío.

android.app.extra.PROVISIONING_WIFI_PASSWORD=
Si la red WiFi no está protegida, este campo debe estar vacío.

android.app.extra.PROVISIONING_LOCALE=
Introduzca códigos de idioma y país. Los códigos de idioma son códigos ISO de dos letras minúsculas (por ejemplo, "es" para español), según se definen en ISO 639-1. Los códigos de país son códigos ISO de dos letras mayúsculas (por ejemplo, "ES" para España), según se definen en ISO 3166-1. Por ejemplo, introduzca es_ES para el español hablado en España. Si no introduce ningún código, el país y el idioma se rellenan automáticamente.

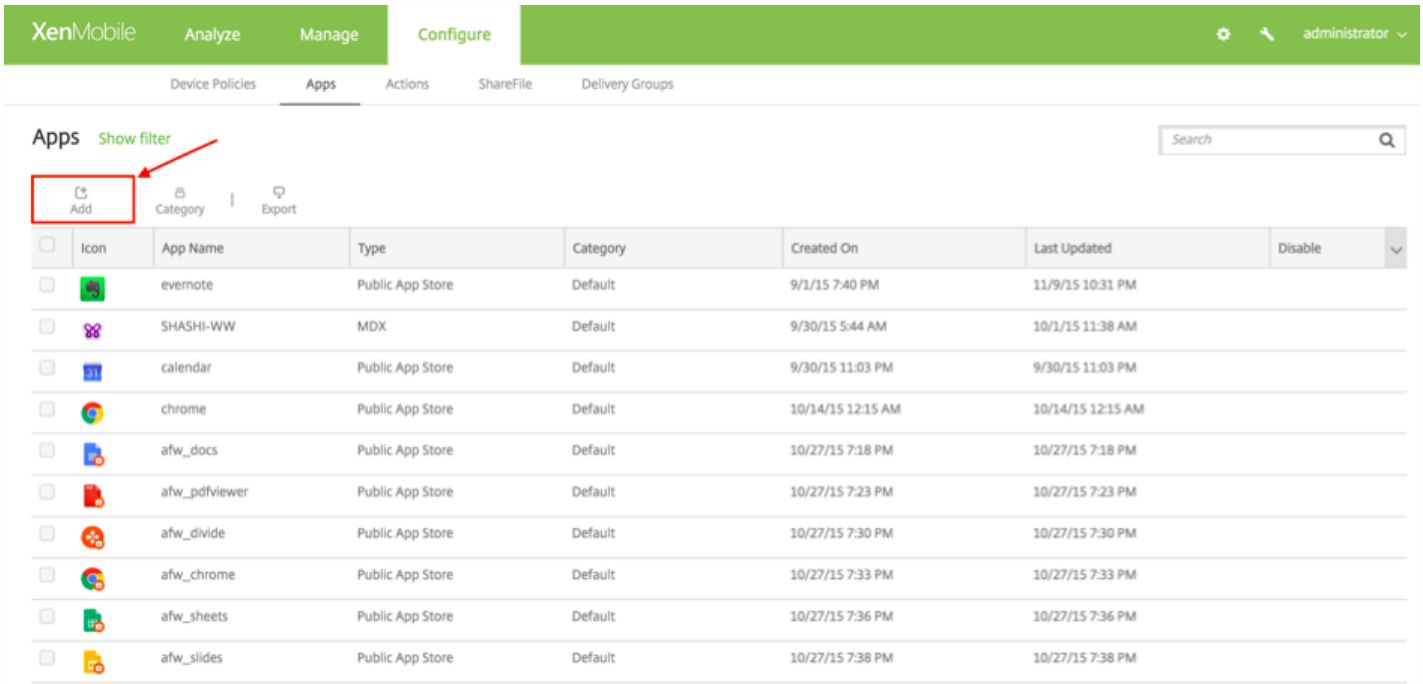
android.app.extra.PROVISIONING_TIME_ZONE=
La zona horaria en que se ejecuta el dispositivo. Introduzca un nombre Olson con el formato área/ciudad. Por ejemplo: America/Los_Angeles para la zona horaria del Pacífico en Estados Unidos. Si no introduce ninguno, la zona horaria se rellena automáticamente.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
Esto no es necesario, porque el valor está codificado en la aplicación como "Worx Home". Se menciona aquí a título meramente informativo.

Obtención de la suma de comprobación de Worx Home

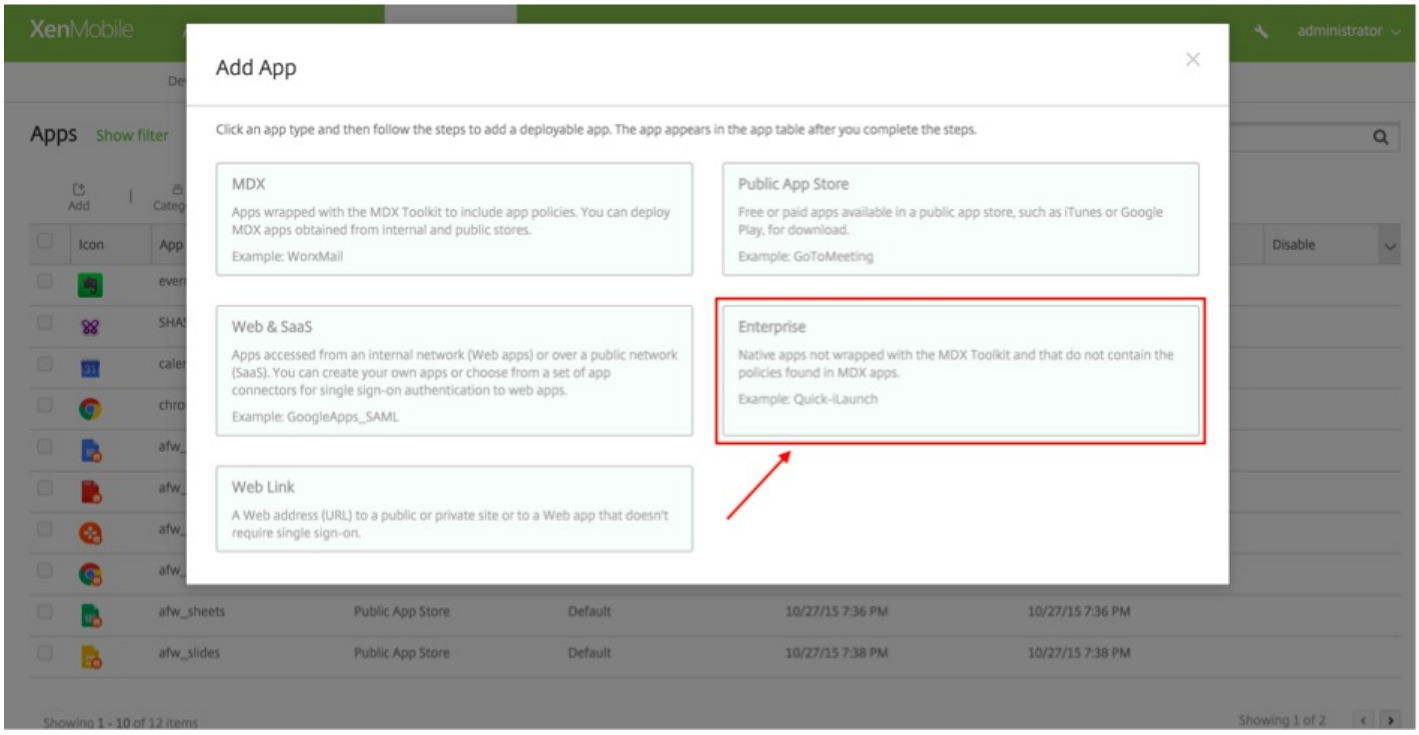
Para obtener la suma de comprobación de cualquier aplicación, agregue la aplicación como aplicación de empresa.

1. En la consola de XenMobile, vaya a **Configure > Apps > Add**.



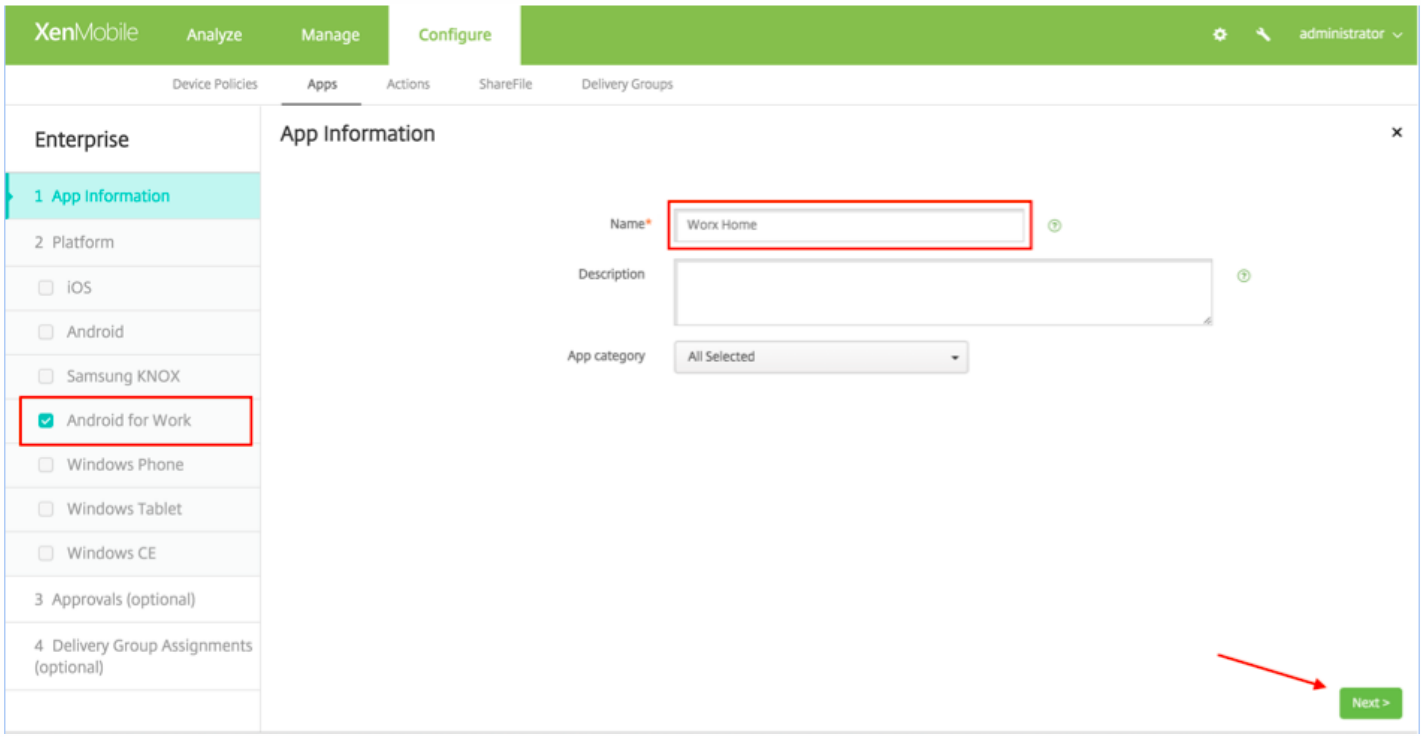
Aparecerá la ventana Add App.

2. Haga clic en **Enterprise**.



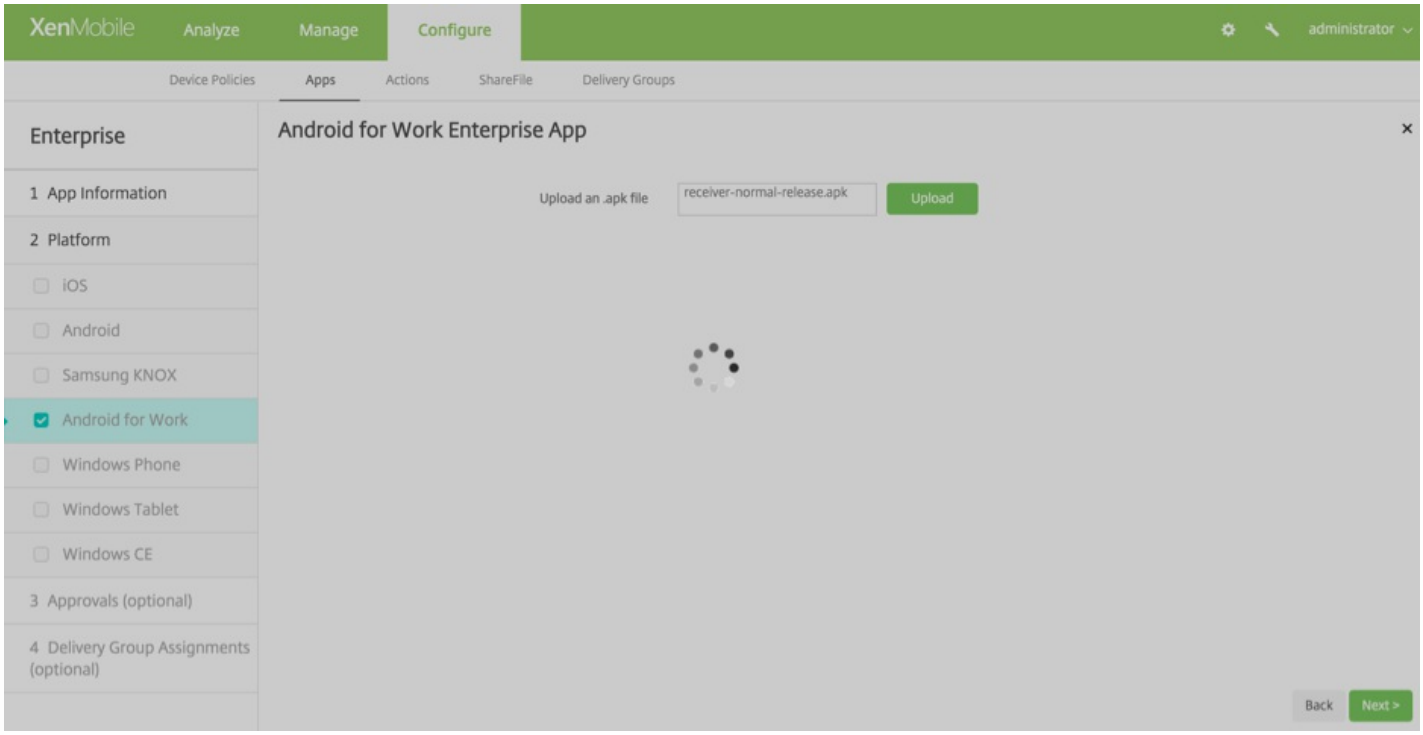
Aparecerá la pantalla **App information**.

3. Seleccione la configuración siguiente y haga clic en **Next**.

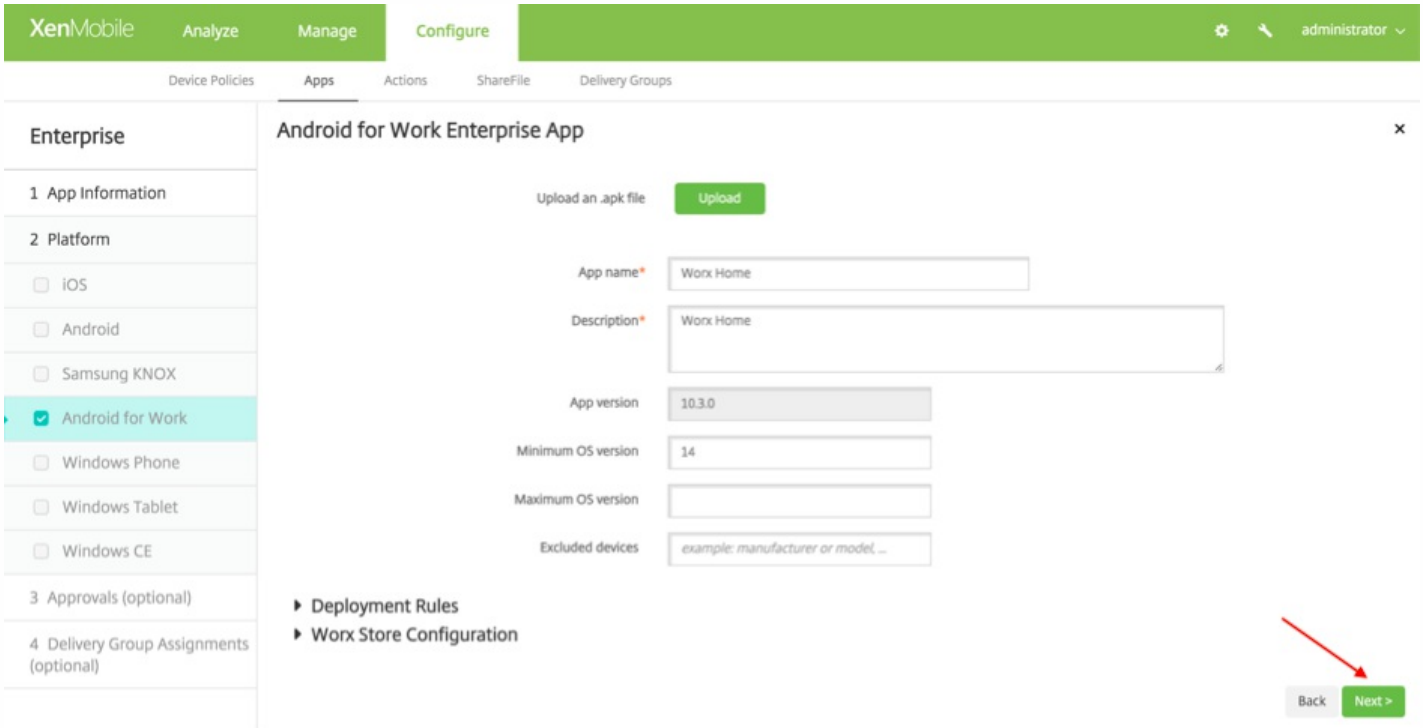


Aparecerá la pantalla **Android for Work Enterprise App** .

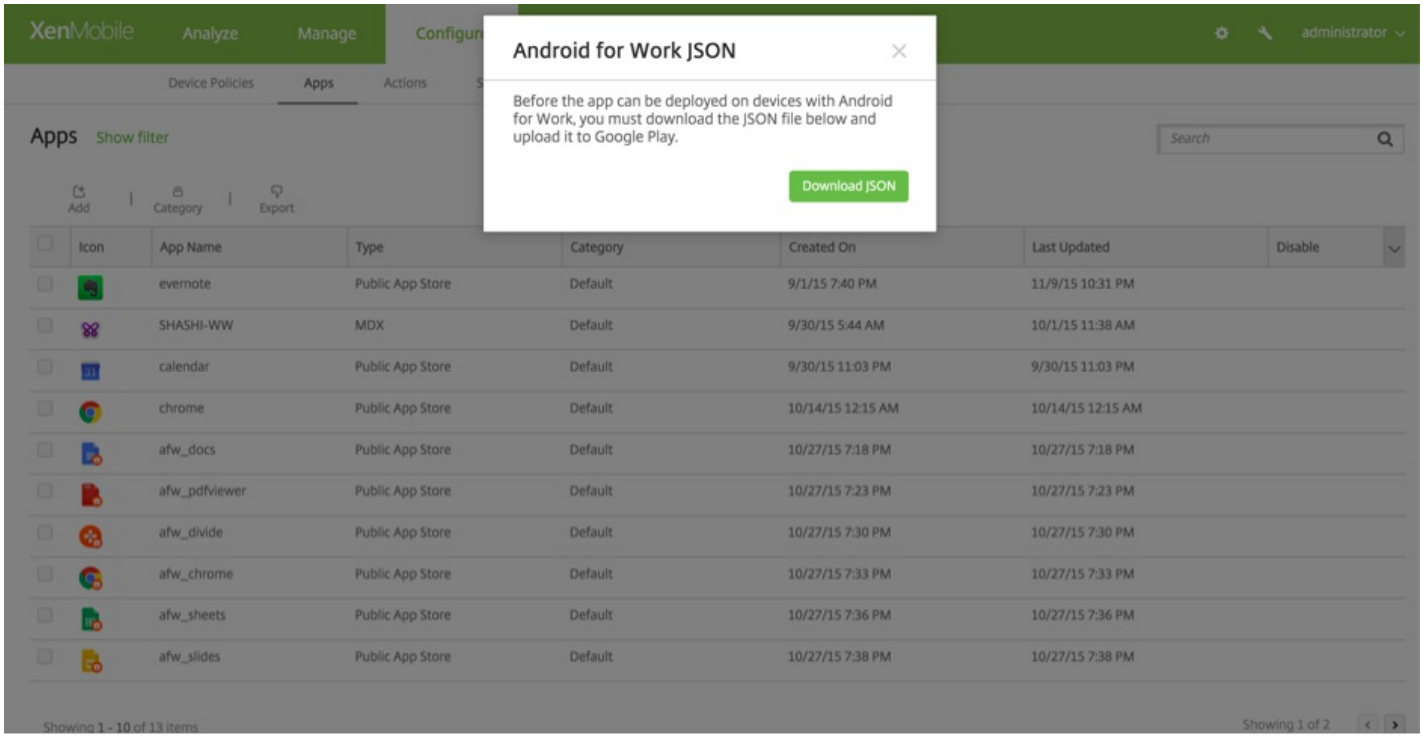
4. Suministre la ruta para el archivo .apk y haga clic en **Next** para cargar el archivo.



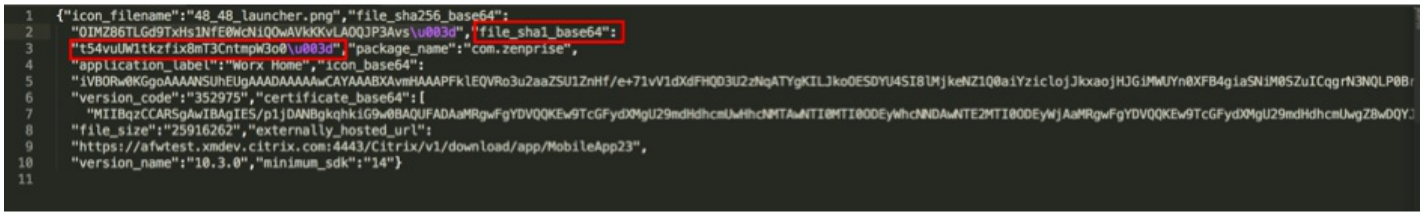
Una vez completada la carga, verá los datos del paquete cargado.



5. Haga clic en **Next** para ver la pantalla donde descargar el archivo JSON, que podrá utilizar para hacer cargas en Google Play. Para Worx Home, la carga en Google Play no es obligatoria, pero necesita el archivo JSON para leer el valor SHA1 en él.



Un archivo JSON típico es similar al siguiente:



6. Copie el **valor file_sha1_base64** y úselo en el campo **Hash** de la herramienta Worx Provisioning Tool. **Nota:** El hash debe ser compatible con direcciones URL.

- Convierta los símbolos **+** a **-**
- Convierta los símbolos **/** a **_**
- Sustituya las secuencias **\u003d** al final con **=**

La aplicación hará la conversión de manera segura si guarda el hash en el archivo nfcprovisioning.txt en la tarjeta SD del dispositivo. Sin embargo, si opta por introducir el hash manualmente, tendrá que asegurarse usted mismo de que el valor puede utilizarse de manera segura en la URL.

Bibliotecas utilizadas

La herramienta Worx Provisioning Tool hace uso de las bibliotecas siguientes en su código fuente:

- Biblioteca v7 appcompat de Google bajo la licencia de Apache 2.0
- Biblioteca Design Support de Google bajo la licencia de Apache 2.0

- Biblioteca v7 Palette de Google bajo la licencia de Apache 2.0
- Butter Knife de Jake Wharton **bajo la licencia de Apache** 2.0

Configuración de reglas de implementación

Oct 31, 2016

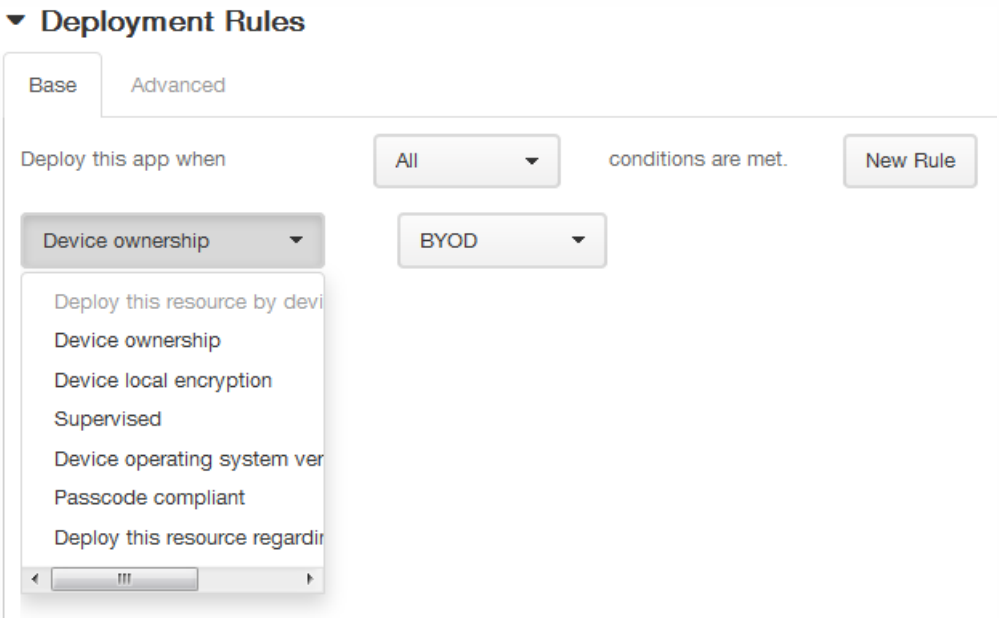
Esta sección describe:

- 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

Las reglas de implementación son parámetros que afectan al resultado de la implementación de un paquete. Puede especificar reglas de implementación para propiedades de un dispositivo, aplicaciones y acciones. XenMobile utiliza las reglas de implementación que se especifican para las propiedades de los dispositivos con el fin de filtrar las directivas, las aplicaciones, las acciones y los grupos de entrega para determinar el orden de implementación de un paquete. Para obtener más información, consulte Orden de implementación.

Puede basar la implementación de un paquete en una versión de sistema operativo específica, en una plataforma de hardware concreta, o en alguna otra combinación. En el asistente utilizado para agregar y editar las propiedades de un dispositivo, aplicaciones y acciones, hay un editor de reglas básico (**Base**) y otro avanzado (**Advanced**). 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**, aparece el editor **Advanced Rule Editor**.

En este modo, puede especificar la relación entre las reglas. Se pueden usar los operadores **AND**, **OR** y **NOT**.

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 connection**, que no se aplicará para iOS. iOS usa APNs.

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: El valor predeterminado es **Now**. Para especificar el momento de la implementación, seleccione **Later** y, a continuación, elija una fecha y una hora.

Deployment condition: El valor predeterminado es **On every connection**. Para limitar las implementaciones, cambie esta opción a **Only when previous deployment has failed**.

Deploy for always-on connections: El valor predeterminado es **OFF**. Esta directiva solo se aplica a dispositivos Android. La propiedad del servidor XenMobile, **Background Deployment** requiere establecer **Deploy for always-on connections** en **ON** para cada directiva implementada en dispositivos Android. Para obtener más información acerca de las conexiones permanentes (always-on), consulte los artículos de "XenMobile Deployment Handbook", así como las secciones "Other Server Optimizations" y "Optimizing Deployment Scheduling for Android Devices" en Tuning XenMobile Operations y "Scheduling policy" en Device and App Policies.

Cómo agregar dispositivos y ver información de los mismos

Jul 27, 2016

La base de datos del servidor XenMobile almacena una lista de dispositivos móviles. Cada dispositivo móvil está definido por un número de serie exclusivo 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. Para obtener más información acerca de formatos del archivo de aprovisionamiento de dispositivos, consulte Formatos del archivo de aprovisionamiento de dispositivos.

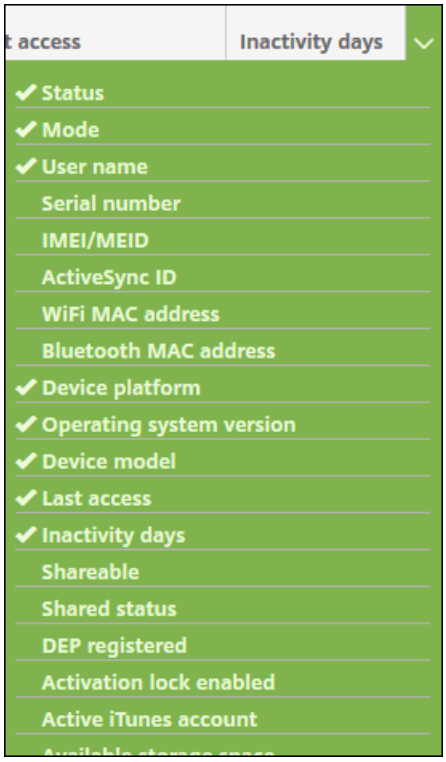
En la página **Devices** de la consola de XenMobile, verá una tabla con todos los dispositivos y la siguiente información relativa a ellos: **Status** para el estado del dispositivo (iconos que representan los dispositivos liberados por jailbreak, si están administrados, si Active Sync Gateway está disponible y su estado de implementación), **Mode** (si es MDM, MAM o ambos modos), **User name** para el nombre de usuario, **Device platform** para la plataforma del dispositivo, **Operating system version** para la versión del sistema operativo, **Device model** para el modelo del dispositivo, **Last access** para el último acceso y **Inactivity days** para los días de inactividad.

Puede agregar dispositivos manualmente, importar dispositivos desde un archivo de aprovisionamiento de dispositivos, modificar los detalles de los dispositivos, enviar notificaciones a dispositivos y eliminar dispositivos. También puede exportar todos los datos de la tabla de dispositivos a un archivo .csv, lo que le permite generar un informe personalizado. El servidor exporta todos los atributos de dispositivo y, si se aplican filtros, los filtros se tienen en cuenta al crear el archivo .csv.

Nota: Los encabezados mencionados son los predeterminados. Puede personalizar lo que aparece en la tabla **Devices**. Para ello, haga clic en la flecha hacia abajo del último encabezado y, a continuación, haga clic en los encabezados adicionales que quiera mostrar en la tabla o elimine los que no.

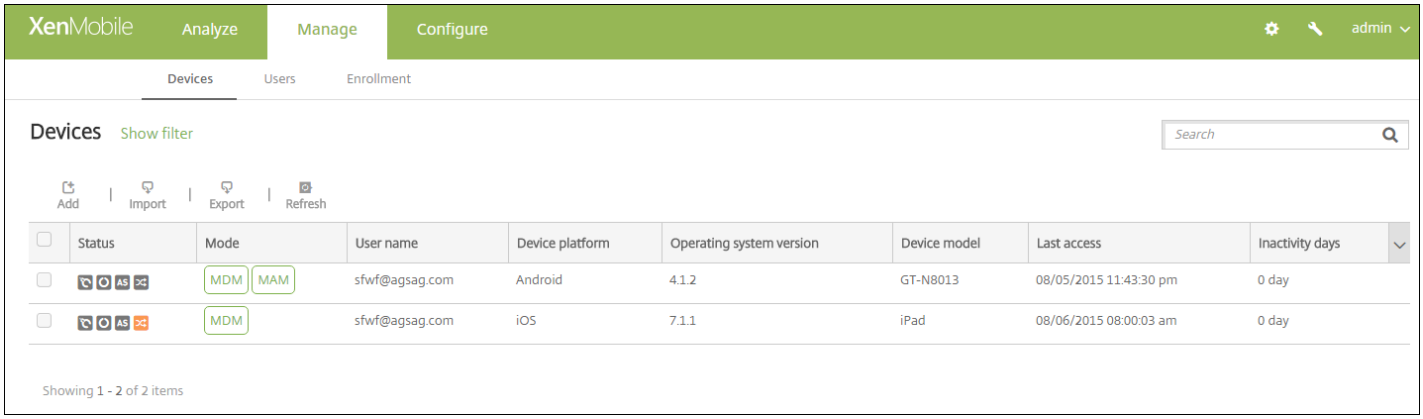
Consulte las secciones siguientes para ver los pasos incluidos en las acciones de la tabla **Devices**:

- Agregar dispositivos manualmente
- Importar dispositivos desde un archivo de aprovisionamiento de dispositivos
- Modificar dispositivos
- Enviar notificaciones a dispositivos
- Eliminar dispositivos
- Exportar la tabla **Devices** a un archivo CSV

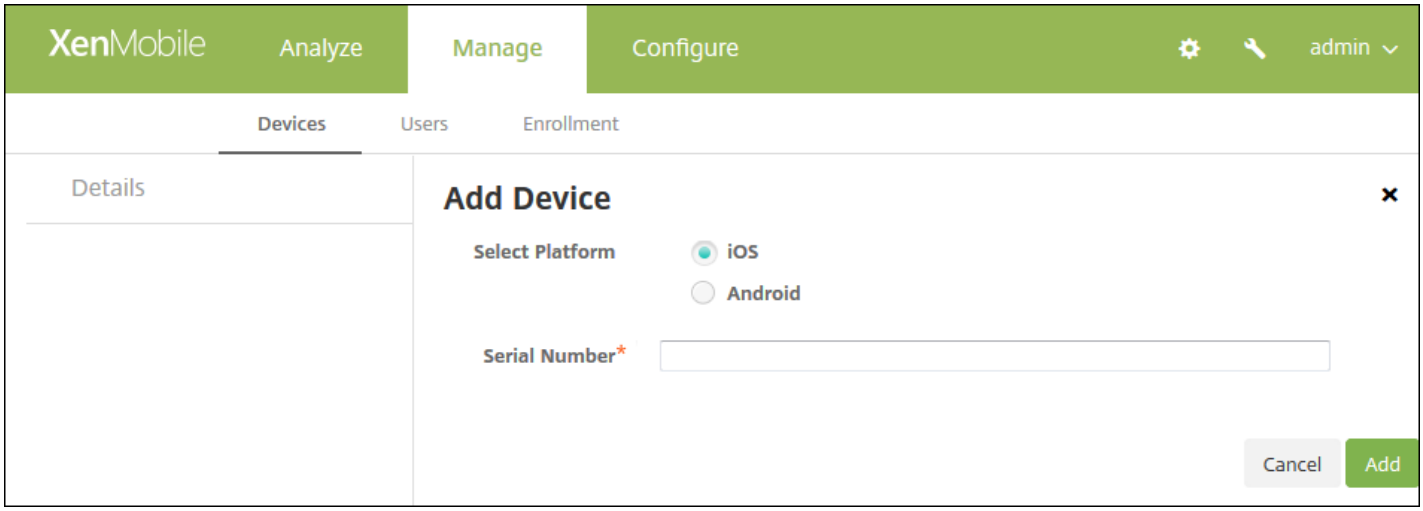


Para agregar dispositivos manualmente

1. En la consola de XenMobile, haga clic en **Manage > Devices**. Aparecerá la página **Devices**.



2. Haga clic en **Add**. Aparecerá la página **Add Device**.

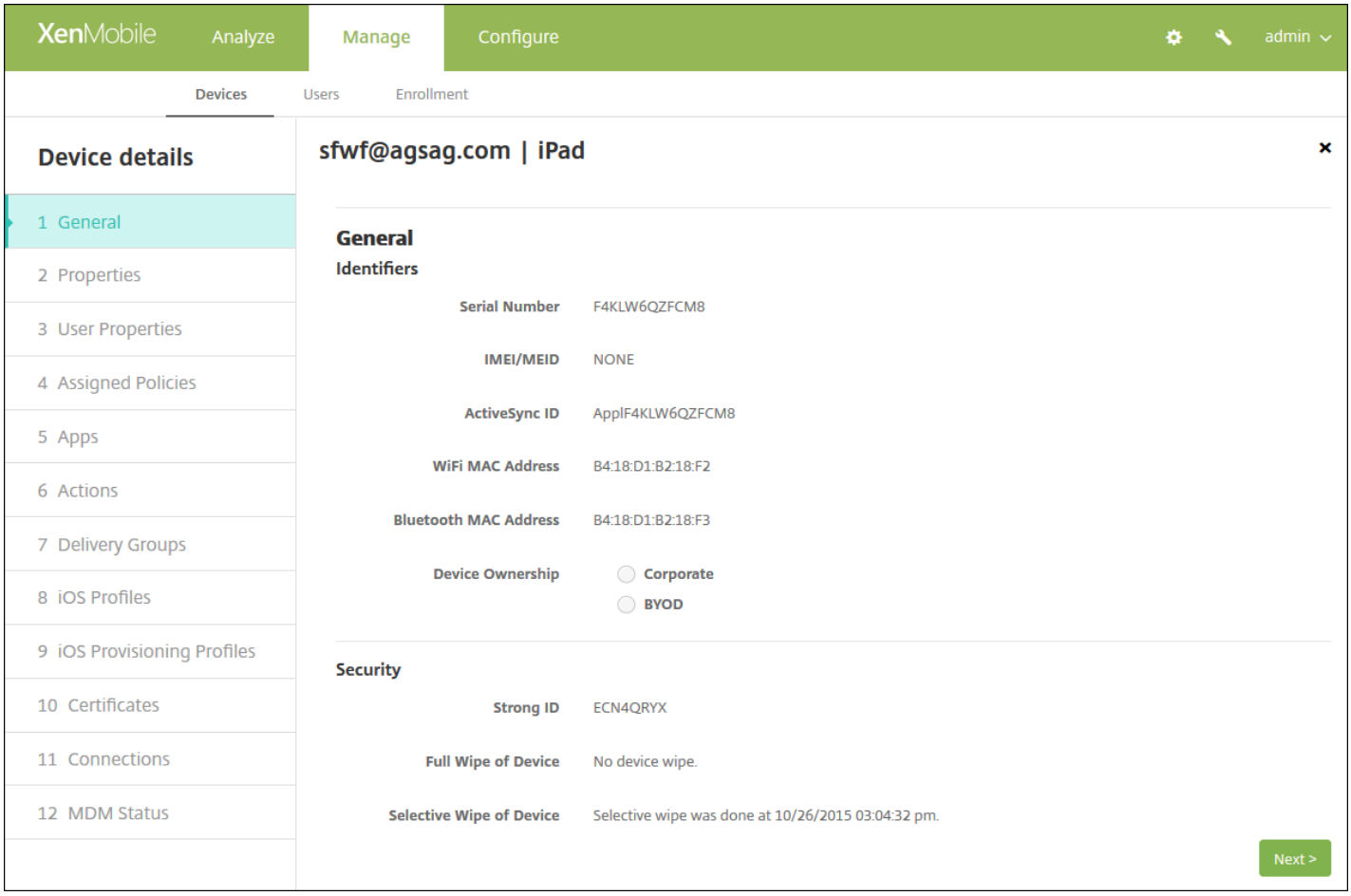


3. Configure los siguientes parámetros:

- **Select platform**. Haga clic en **iOS** o **Android**.
- **Serial Number**. Escriba el número de serie del dispositivo.
- **IMEI/MEID**. Si quiere, solo para dispositivos Android, escriba información referente al identificador IMEI/MEID del dispositivo.

4. Haga clic en **Add**. La tabla **Devices** aparecerá con el dispositivo agregado al final de la lista. 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 a la derecha de la lista.



5. En **General Identifiers**, confirme la información mostrada (la lista exacta varía según el tipo de plataforma):

- Número de serie
- IMEI/MEID
- ActiveSync ID
- WiFi MAC Address
- Bluetooth MAC Address
- Device Ownership

6. En **Security**, confirme la información mostrada (la lista exacta varía según el tipo de plataforma):

- Strong ID
- Full Wipe of Device
- Selective Wipe of Device
- Lock Device
- Device Unlock
- Device locate
- Device Enable Tracking
- Device Disown
- Activation Lock Bypass
- Device Clear Restrictions
- Request AirPlay Mirroring

- Stop AirPlay Mirroring

Nota: El bloqueo de dispositivo (Lock Device) para iOS está disponible para iOS 7 y versiones posteriores.

7. Haga clic en **Next**. Aparecerá la página **Properties**. Desde ella, puede agregar propiedades al dispositivo.

8. Haga clic en **Add**. Aparecerá la lista de las propiedades disponibles.

9. Para cada propiedad que quiera agregar, lleve a cabo lo siguiente:

- Haga clic en la propiedad que se va a aprovisionar y, a continuación, establezca su valor. Por ejemplo, puede seleccionar la propiedad **Activation lock enabled** y establecer el valor en **Yes** o en **No**.
- Haga clic en **Done**.

10. Haga clic en **Next**.

Nota: A medida que se agregan las propiedades, todas ellas aparecen 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, la pertenencia, la versión, el autor, el tamaño, el estado de su instalación, el identificador y el tipo.
- En el caso de aplicaciones **pendientes y erróneas**, 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.

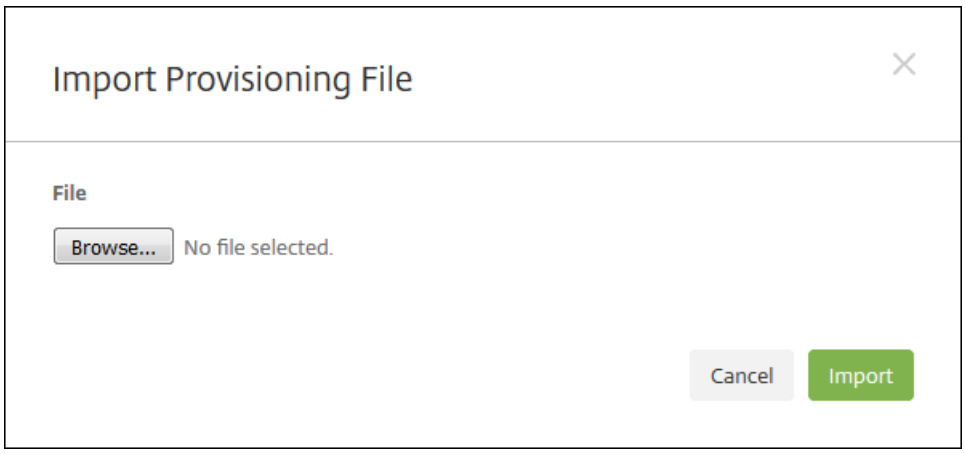
12. Haga clic en **Save**.

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**. Aparecerá el cuadro de diálogo **Import Provisioning**

File.

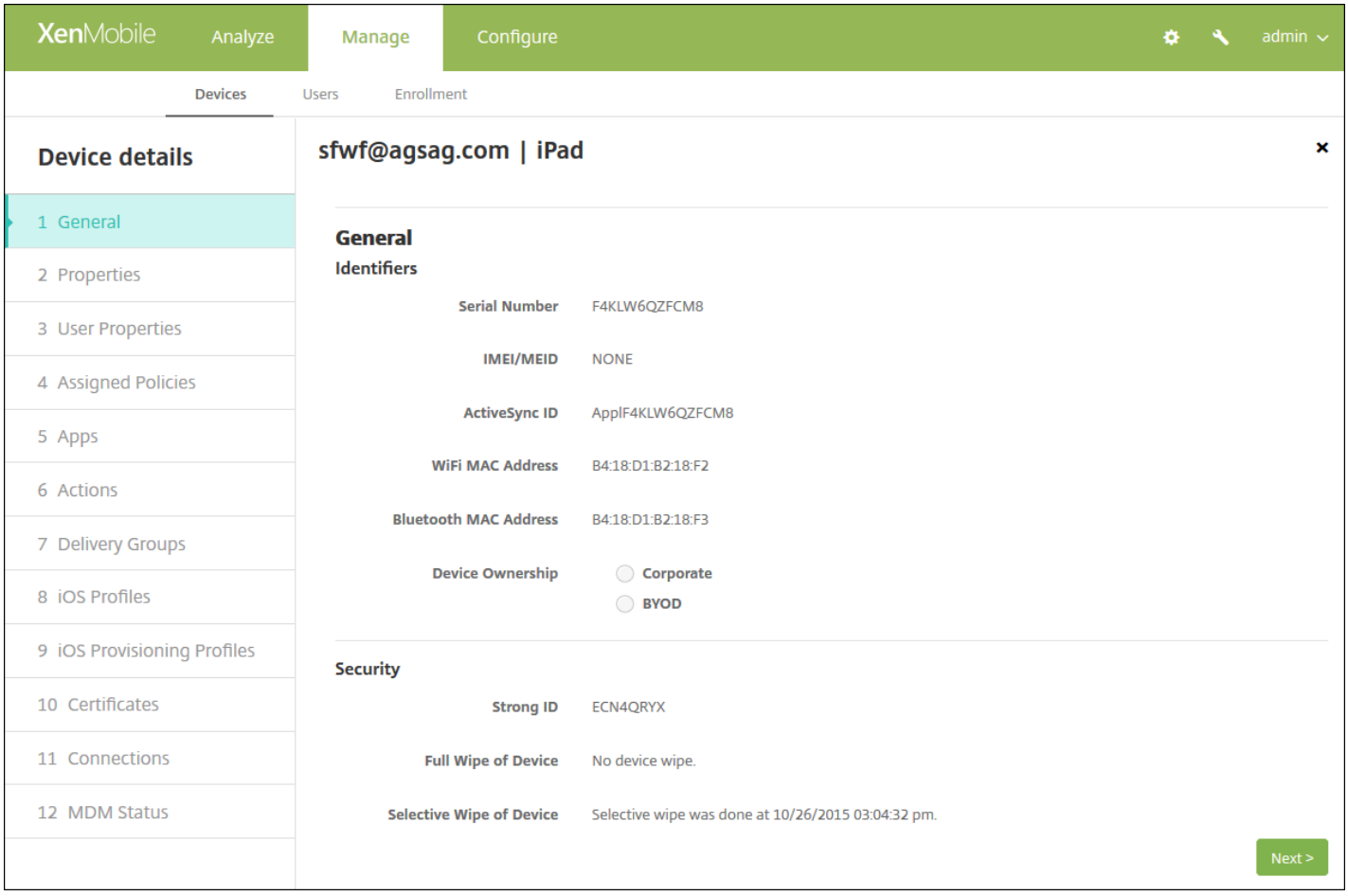


2. Para seleccionar el archivo a importar, haga clic en **Browse** y vaya a la ubicación de ese archivo.

3. Haga clic en **Import**. Los archivos importados se agregarán a la tabla **Devices**.

Cómo modificar dispositivos

1. Seleccione el dispositivo que quiere 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**. Aparece la página **Properties** .

4. En la página **Properties**, puede agregar, modificar o eliminar propiedades.

- Para agregar una propiedad, haga clic en Add en la categoría a la que quiera agregar una propiedad. A continuación, haga clic en la propiedad en la lista que se muestra y agregue el valor que le corresponde. Haga clic en **Done**.
- 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 Policies**.

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 esas páginas, consulte Para agregar dispositivos manualmente.

Nota: La parte superior de la página **User Properties** no se puede modificar.

- Para agregar cada propiedad de usuario, haga clic en **Add** y lleve a cabo lo siguiente:
  - En la lista que aparece, haga clic en la propiedad que quiera agregar, especifique el valor de la propiedad y, a continuación, haga clic en **Done** o en **Cancel**.
- 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. En cada una de las páginas siguientes, puede ver información resumida y hacer clic en **Next**.

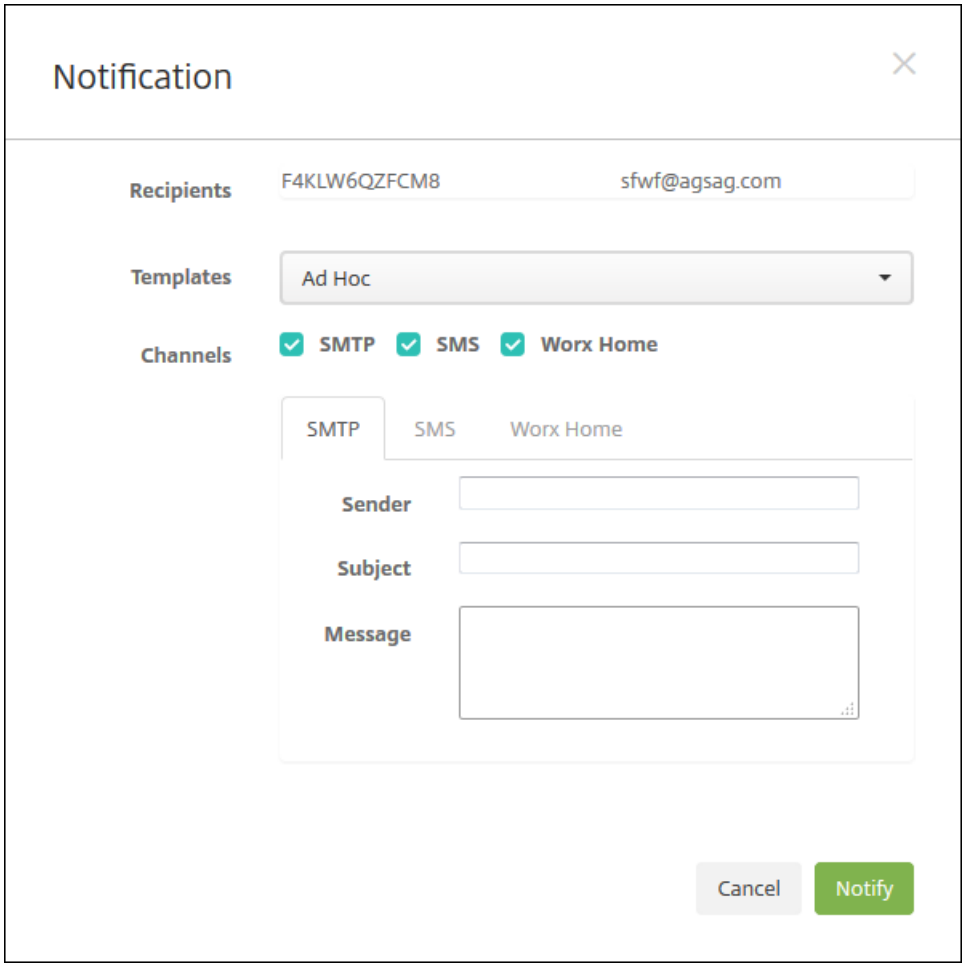
8. En la página final, haga clic en **Save** para guardar los cambios realizados en el dispositivo.

Cómo enviar una notificación a los dispositivos

Puede enviar notificaciones a los dispositivos desde la página Devices. Para obtener más información acerca de las notificaciones, consulte Para crear o actualizar plantillas de notificaciones 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 el campo **Recipients**, se ofrece una lista de todos los dispositivos que van a recibir la notificación.



3. Configure los siguientes parámetros:

- **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**.
- **Channels**. Seleccione cómo enviar el mensaje. El valor predeterminado es **SMTP**, **SMS** y **Worx Home**. Puede hacer clic en las fichas **SMTP**, **SMS** y **Worx Home** para ver el formato del mensaje de cada canal.
- **Sender**. Escriba un remitente opcional.
- **Subject**. Escriba un asunto para un mensaje **Ad Hoc**.
- **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.

Para exportar la tabla Devices

1. Haga clic en el botón **Export** situado sobre la tabla **Devices**. XenMobile extrae la información de la tabla Devices y la convierte a un archivo CSV.

2. Abra o guarde el archivo CSV. El modo de hacer esto dependerá del explorador Web que se esté utilizando. También puede cancelar la operación.

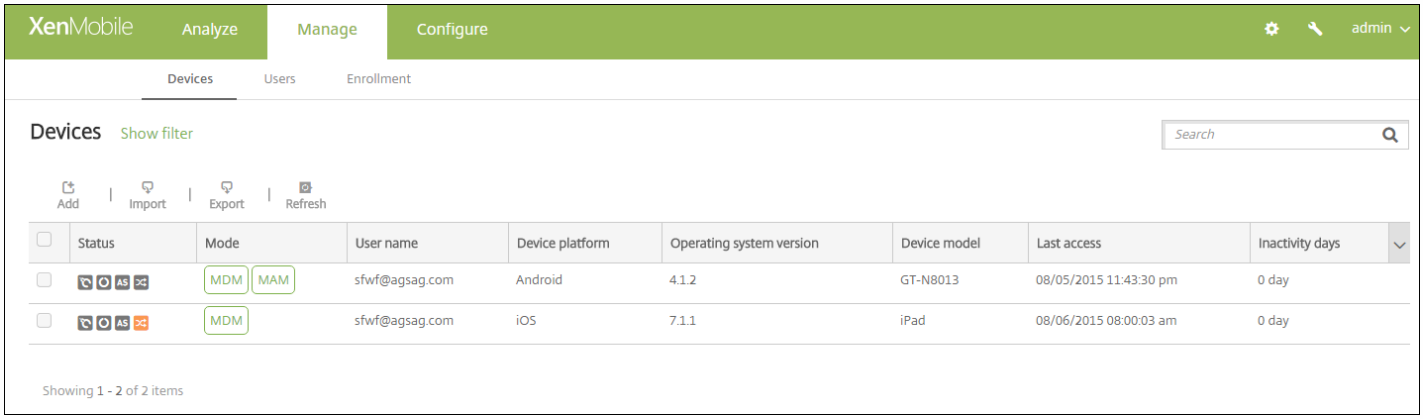
Bloqueo de dispositivos iOS

Jul 27, 2016

Puede bloquear un dispositivo iOS y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo. Esta función está respaldada en dispositivos iOS 7 y 8.

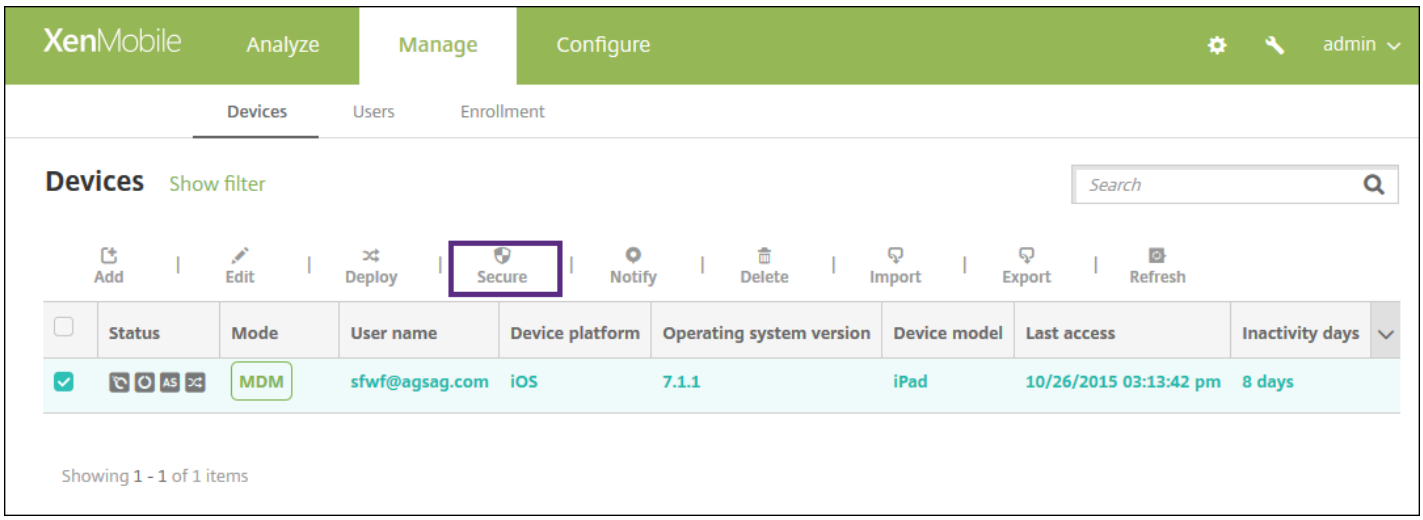
Si opta por incluir un mensaje y un número de teléfono en la pantalla de bloqueo, estos solo aparecerán en dispositivos bloqueados si también se ha configurado la directiva de códigos de acceso en la consola de XenMobile o si los usuarios han habilitado manualmente un código de acceso en el dispositivo.

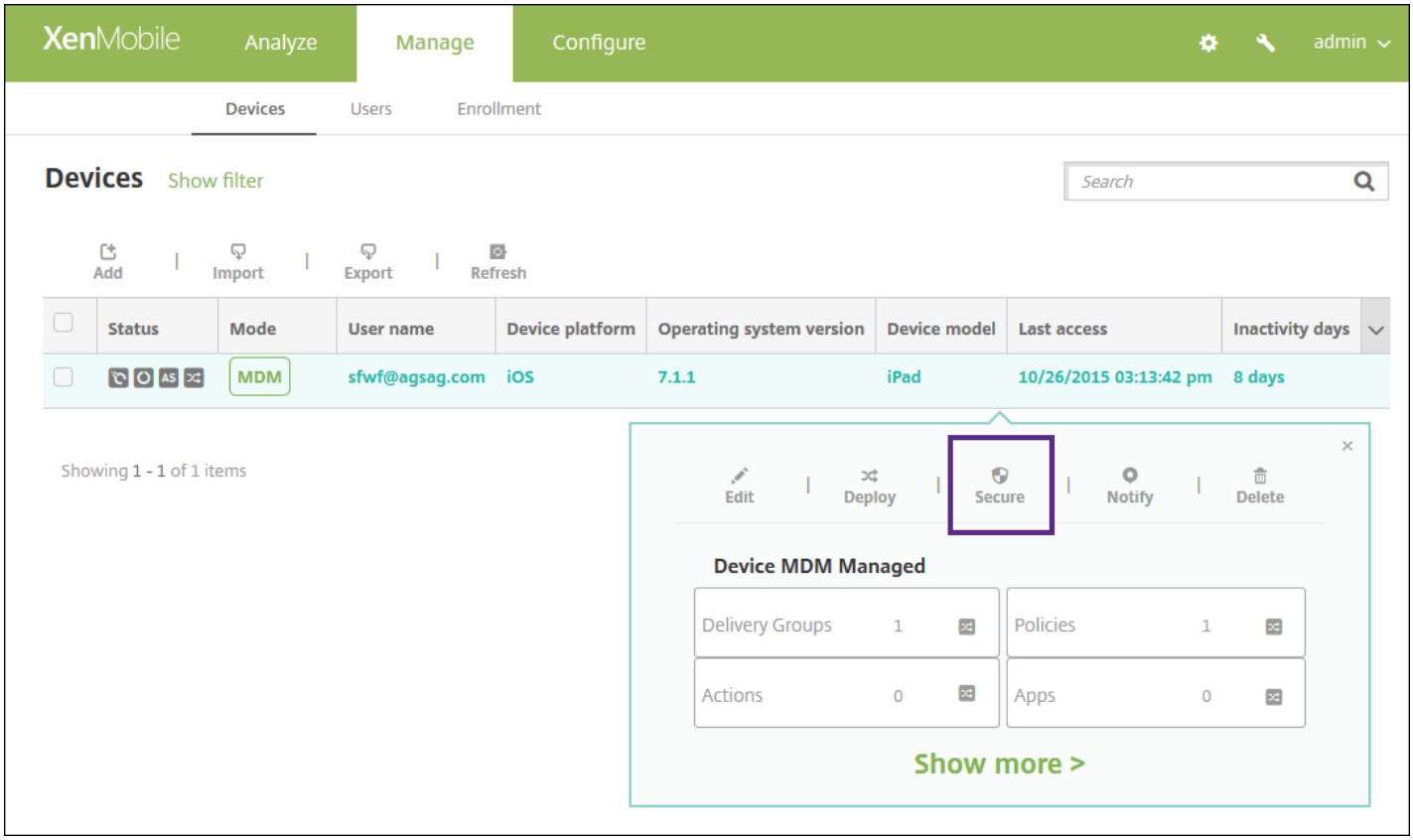
1. En la consola de XenMobile, haga clic en **Manage > Devices**. Aparecerá la página **Devices**.



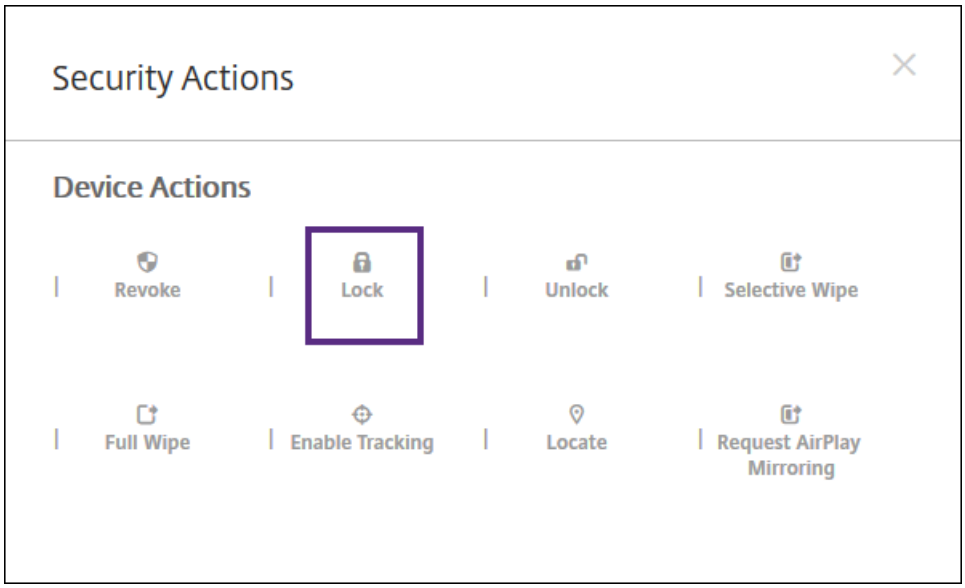
2. Seleccione el dispositivo iOS que quiere bloquear.

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.

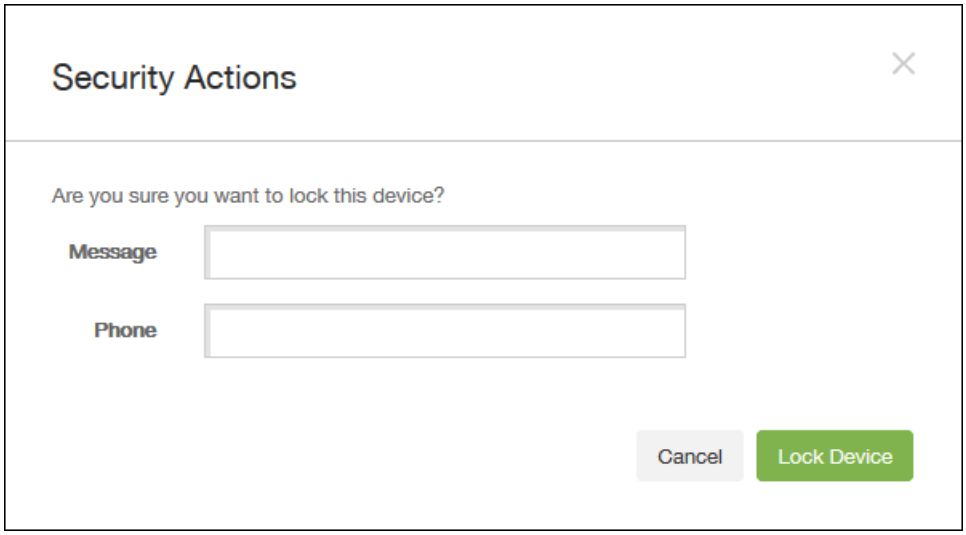




3. En el menú de opciones, seleccione **Secure**. Aparecerá el cuadro de diálogo **Security Actions**.



4. Seleccione **Lock**. Aparecerá el cuadro de diálogo de confirmación **Security Actions**.



5. Si lo prefiere, puede introducir el mensaje y el número de teléfono que aparecerán en la pantalla de bloqueo del dispositivo.

6. Haga clic en **Lock Device**.

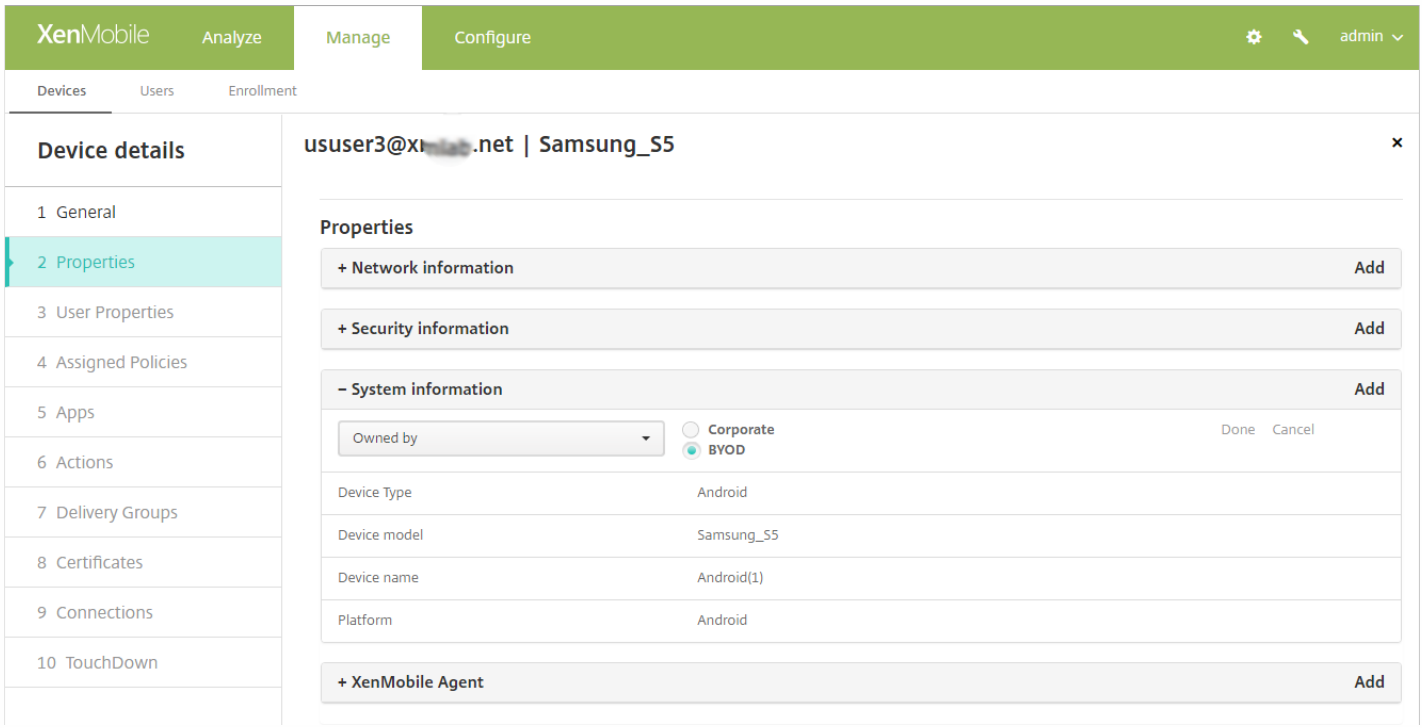
Etiquetado manual de dispositivos de usuario

Jul 27, 2016

En XenMobile, puede etiquetar manualmente un dispositivo en XenMobile de una de las siguientes maneras:

- Durante el proceso de inscripción por invitación.
- Durante el proceso de inscripción mediante el portal Self Help Portal.
- Agregando el propietario del dispositivo a las propiedades del mismo.

Tiene la opción de etiquetar el dispositivo como propiedad de la empresa o del empleado. Cuando usa el portal Self-Help Portal para inscribir un dispositivo, también puede etiquetarlo como propiedad de la empresa o del empleado. Tal y como se muestra en la siguiente imagen, también puede etiquetar un dispositivo manualmente si agrega la propiedad **Owned by** al dispositivo desde la ficha **Devices** de la consola de XenMobile y elige entre **Corporate** (propiedad de la empresa) o **BYOD** (propiedad del empleado).



Formatos del archivo de aprovisionamiento de dispositivos

Jul 27, 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

Directivas de dispositivo

Oct 31, 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. Para ver una matriz de directivas por plataforma, consulte Directivas de dispositivos de XenMobile desglosadas por plataforma.

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).

Puede configurar las siguientes directivas de dispositivo en XenMobile.

Nombre de directiva de dispositivo	**Descripción de directiva de dispositivo**
AirPlay Mirroring	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.
AirPrint	La directiva AirPrint de dispositivo permite agregar impresoras AirPrint a la lista de impresoras AirPrint que aparecen en 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.
Android for Work App Restrictions	Puede modificar las restricciones asociadas a aplicaciones Android for Work. Sin embargo, antes de modificarlas, debe cumplir los siguientes requisitos previos: • Complete, en Google, las tareas de configuración de Android for Work. Para obtener más información, consulte Administración de dispositivos con Android for Work. • Cree un conjunto de credenciales de Google Play. Para obtener más información,

	consulte Credenciales de Google Play. • Cree una cuenta de Android for Work. Para obtener más información, consulte Creación de una cuenta de Android for Work. • Agregue aplicaciones Android for Work a XenMobile. Para obtener más información, consulte Cómo agregar aplicaciones a XenMobile.
APN	Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. 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.
App Access	La directiva de dispositivo App Access permite definir una lista de las aplicaciones que deben estar instaladas en el dispositivo obligatoriamente, que pueden estar instaladas en el dispositivo o que no deben instalarse en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento del dispositivo con los requisitos de dicha lista de aplicaciones.
App Attributes	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.
App Configuration	Con esta directiva, puede configurar de manera remota una aplicación de App Store que respalde una configuración administrada, implementando un archivo XML de configuración (llamado lista de propiedades o plist) en los dispositivos iOS de los usuarios, para configurar varios parámetros y comportamientos de la aplicación.
App Inventory	La directiva App Inventory 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.
App Lock	En XenMobile, puede crear una directiva para definir una lista de aquellas aplicaciones cuya ejecución se permite en un dispositivo o una lista de aquellas aplicaciones cuya ejecución debe bloquearse en un dispositivo. Puede configurar esta directiva para dispositivos Android e iOS, pero su funcionamiento difiere según la plataforma. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS. Nota: Aunque la directiva de dispositivos funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N y posteriores porque Google ha dejado de respaldar la API necesaria.

	En dispositivos iOS, solo se puede seleccionar una aplicación iOS por cada directiva. Esto significa ue los usuarios solo pueden usar el dispositivo para ejecutar una sola aplicación. Los usuarios no pueden realizar ninguna otra actividad en el dispositivo, excepto las opciones que usted permita específicamente cuando aplique la directiva de bloqueo de aplicaciones.
App Network Usage	Puede definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas usan, por ejemplo, redes de datos móviles en dispositivos iOS. Las reglas solo se aplican a aplicaciones administradas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de XenMobile. No se incluyen en este grupo aquellas aplicaciones que los usuarios descargan directamente en sus dispositivos (sin que se implementen por medio de XenMobile) ni aquellas aplicaciones que ya estaban instaladas en los dispositivos cuando estos se inscribieron en XenMobile.
Restricciones de aplicaciones	Puede crear una lista negra de las aplicaciones que quiera impedir que los usuarios instalen en sus dispositivos Samsung KNOX. También puede crear listas blancas de las aplicaciones que quiere permitir que los usuarios instalen.
App Tunneling	Puede configurar la directiva App Tunneling para aumentar la continuidad del servicio y la fiabilidad de la transferencia de datos para las aplicaciones móviles. 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 pasará por XenMobile antes de redirigirse al servidor que ejecuta la aplicación.
App Uninstall	La directiva App Uninstall permite quitar aplicaciones de los dispositivos de los 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.
App Uninstall Restrictions	Con esta directiva, puede especificar las aplicaciones que los usuarios pueden o no pueden desinstalar.
Explorador Web	Con las directivas de explorador, puede definir si los dispositivos de los usuarios pueden usar el explorador Web o limitar las funciones del explorador que se puedan usar. En dispositivos Samsung, puede inhabilitar completamente el explorador, puede habilitar o inhabilitar los elementos emergentes, JavaScript, las cookies, la función de completado automático, y también puede decidir si forzar advertencias de fraude. En dispositivos Android for Work, puede incluir direcciones URL específicas en listas de URL permitidas o prohibidas; también

	puede agregar marcadores de explorador concretos y seguros.
Calendar (CalDav)	En XenMobile, puede agregar una directiva de dispositivos si quiere agregar una cuenta de calendarios (CalDAV) a los dispositivos iOS o Mac OS X de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de planificación con cualquier servidor que admita CalDAV.
Cellular	Esta directiva permite configurar los parámetros de red de telefonía móvil.
Connection Manager	En XenMobile, puede especificar la configuración de conexión de las aplicaciones que se conectan automáticamente a Internet y a redes privadas. Esta directiva solo está disponible para dispositivos Pocket PC de Windows.
Connection Scheduling	Esta directiva es necesaria para que los dispositivos Android y Windows Mobile se conecten de vuelta con el servidor XenMobile para la administración MDM, el envío de aplicaciones y la implementación de directivas. Si no envía esta directiva y no ha habilitado Google GCM, un dispositivo no podrá conectarse al servidor. Por lo tanto, es importante enviar esta directiva en el paquete base para los dispositivos que se inscriben.
Contacts (CardDAV)	En XenMobile, puede agregar una directiva de dispositivos para agregar una cuenta de contactos iOS (CardDAV) a los dispositivos iOS o Mac OS X de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de contacto con cualquier servidor que admita CardDAV.
Copy apps to Samsung Container	Puede especificar que las aplicaciones que ya están instaladas en un dispositivo se copien en un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles. Las aplicaciones que se copien al contenedor SEAMS estarán disponibles en las pantallas de inicio de los usuarios, mientras que las aplicaciones que se copien al contenedor KNOX solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.
Credentials	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. Cada plataforma de dispositivo requiere un conjunto diferente de valores, que se describen en el artículo sobre la directiva de credenciales. Nota: Antes de crear esta directiva, necesitará la información de credenciales que vaya a utilizar para cada plataforma, además de los certificados en sí y las contraseñas.
Copy apps to Samsung Container	Puede especificar que las aplicaciones que ya están instaladas en un dispositivo se copien en un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles. Para

	obtener más información sobre los dispositivos respaldados, consulte Dispositivos Samsung KNOX respaldados. Las aplicaciones que se copien al contenedor SEAMS estarán disponibles en las pantallas de inicio de los usuarios, mientras que las aplicaciones que se copien al contenedor KNOX solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.
Credentials	A menudo se usa conjuntamente con una directiva de Wi-Fi. Esta directiva permite a las empresas implementar certificados para la autenticación en recursos internos que requieren autenticación mediante certificado.
Custom XML	Puede crear directivas XML personalizadas en XenMobile cuando desee personalizar las siguientes características: • 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 XML personalizada mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows. 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.
Delete Files and Folders	En XenMobile, puede crear una directiva para eliminar archivos o carpetas específicas de los dispositivos Windows Mobile/CE.
Delete Registry Keys and Values	En XenMobile, puede crear una directiva para eliminar de los dispositivos Windows Mobile/CE claves y valores específicos del Registro.
Device Health Attestation	En XenMobile, puede crear una directiva para requerir que los dispositivos Windows 10 informen de su estado, haciendo que dichos dispositivos envíen ciertos datos e información de tiempo de ejecución al servicio Health Attestation Service (HAS) para su posterior análisis. El servicio HAS crea y devuelve un certificado de atestación de estado que el dispositivo envía a XenMobile. Cuando XenMobile recibe el certificado de atestación de estado, según el contenido de este, puede implementar las acciones automatizadas que haya configurado previamente. Los datos que se comprueban en el servicio HAS son: • AIKPresent

	• BitLockerStatus • BootDebuggingEnabled • BootManagerRevListVersion • CodeIntegrityEnabled • CodeIntegrityRevListVersion • DEPPolicy • ELAMDriverLoaded • IssuedAt • KernelDebuggingEnabled • PCR • ResetCount • RestartCount • SafeModeEnabled • SBCPHash • SecureBootEnabled • TestSigningEnabled • VSMEnabled • WinPEEnabled Para obtener más información, consulte la página HealthAttestation CSP de Microsoft.
Device Name	Con la directiva de nombre de dispositivo, puede definir los nombres de dispositivos iOS y Mac OS X para poder identificarlos fácilmente. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Para obtener más información acerca de las macros, consulte Macros en XenMobile.
Enterprise Hub	Una directiva Enterprise Hub para dispositivos Windows Phone 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) Nota: XenMobile solo admite una directiva Enterprise Hub por modo de Windows Phone Worx Home. Por ejemplo, para cargar Windows Phone Worx Home en XenMobile Enterprise Edition, no debe crear varias directivas Enterprise Hub con versiones diferentes de Worx Home para XenMobile Enterprise Edition. Puede implementar la directiva Enterprise Hub inicial durante la inscripción del dispositivo.
Exchange	Con XenMobile tiene dos opciones para entregar el correo electrónico. Puede entregar correo electrónico ActiveSync usando la aplicación WorxMail en contenedor, o bien puede usar esta directiva Exchange de MDM para habilitar el correo electrónico ActiveSync para el cliente de correo nativo del dispositivo.

Files	Con esta directiva, puede agregar archivos de script a XenMobile para realizar algunas funciones para los usuarios. También puede agregar documentos a los que quiera que los usuarios de los dispositivos Android puedan acceder desde sus dispositivos. Cuando agregue el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo. Por ejemplo, si quiere que los usuarios de Android reciban un documento de empresa o archivo PDF, puede implementar el archivo en el dispositivo y permitir que los usuarios sepan dónde se encuentra el archivo. Puede agregar los siguientes tipos de archivo con esta directiva: • Archivos de texto (XML, HTML, PY, etc.) • Otros archivos, como documentos, imágenes, hojas de cálculo o presentaciones • Solo para Windows Mobile y Windows CE: archivos de script creados con MortScript
Font	En XenMobile, puede agregar esta directiva de dispositivo para agregar fuentes de texto adicionales a los dispositivos iOS y Mac OS X 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.
Import iOS and Mac OSx Profile	Puede importar en XenMobile archivos XML de configuración de dispositivos iOS y OS X. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator. Para obtener más información sobre cómo usar Apple Configurator para crear un archivo de configuración, consulte la página de ayuda de Apple Configurator.
Kiosk	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 quiosco. Nota: • Todas las aplicaciones que especifique para el modo quiosco deben estar ya instaladas en los dispositivos de los usuarios. • Algunas opciones solo se aplican a Samsung Mobile Device Management (MDM) API 4.0 y versiones posteriores.
LDAP	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.
Ubicación	Esta directiva de ubicación se puede usar para ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado GPS para Worx Home. Una vez que esta directiva se envía al dispositivo, los administradores pueden emitir un comando de localización geográfica desde el servidor XenMobile y el dispositivo responderá con las coordenadas de su ubicación. También se pueden aplicar directivas de geocerca y seguimiento geográfico.
Mail	En XenMobile, puede agregar una directiva de dispositivos para configurar una cuenta de correo electrónico en los dispositivos iOS o Mac OS X de los usuarios.
Managed Domains	Con esta directiva puede definir los dominios administrados que se aplicarán al correo electrónico y al explorador Web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari. Así, puede especificar las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador Web. Esta directiva solo está disponible para dispositivos supervisados con iOS 8 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte Cómo colocar un dispositivo iOS en modo supervisado mediante Apple Configurator. Cuando un usuario envía un correo electrónico a un destinatario cuyo dominio no consta en la lista de dominios administrados de correo electrónico, el mensaje se marca en el dispositivo del usuario para avisarle de que envía un mensaje a una persona fuera del dominio empresarial. Cuando un usuario intente abrir un elemento (documento, adjunto o descarga) con Safari desde un dominio que no conste en la lista de dominios Web administrados, la aplicación de empresa correspondiente abrirá el elemento. Si el elemento no es de un dominio Web que conste en la lista de dominios Web administrados, el usuario no podrá abrir el elemento con la aplicación de empresa, y deberá usar una aplicación personal no administrada.
Microsoft Exchange ActiveSync	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. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en el artículo Microsoft Exchange ActiveSync de esta sección.
MDM Options	En XenMobile, puede crear una directiva de dispositivo para administrar la función Bloqueo de activación de Buscar mi iPhone/iPad en los dispositivos supervisados iOS 7.0 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 o Inscripción masiva de iOS.

	Bloqueo de activación es una función de Buscar mi iPhone o iPad que está diseñada para evitar la reactivación de dispositivos perdidos o robados porque se necesita el ID de Apple y la contraseña del usuario para poder desactivar Buscar Mi iPhone, borrar los datos del dispositivo o reactivarlo y usarlo. En XenMobile, puede omitir el requisito de ID de Apple y contraseña si habilita el bloqueo de activación en la directiva de opciones de MDM. Así, cuando un usuario devuelva un dispositivo con la función Buscar Mi iPhone activada, podrá administrar el dispositivo desde la consola de XenMobile sin sus credenciales de Apple.
Organization Info	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.
Passcode	Una directiva de código de acceso permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Con esta directiva se puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.
Personal Hotspot	Con esta directiva puede permitir que los usuarios se conecten a Internet aunque estén fuera del alcance de una red Wi-Fi, utilizando la conexión de datos móviles a través de la función Compartir Internet de sus dispositivos iOS. Disponible en iOS 7.0 y versiones posteriores.
Profile Removal	En XenMobile, puede crear una directiva de eliminación de perfiles de aplicaciones. Una vez implementada, la directiva elimina el perfil de aplicación de los dispositivos iOS o Mac OS X de los usuarios.
Provisioning Profile	Por regla general, cuando se desarrolla y se firma con código una aplicación empresarial iOS, se incluye un perfil de aprovisionamiento de distribución empresarial, que requiere Apple para que la aplicación funcione en dispositivos iOS. Si falta o ha caducado un perfil de aprovisionamiento, la aplicación se bloquea cuando un usuario toca para abrirla. El problema principal con los perfiles de aprovisionamiento es que caducan al año de generarse en el portal de desarrolladores de Apple, por lo que se debe hacer un seguimiento de la fecha de caducidad de todos los perfiles de aprovisionamiento en todos los dispositivos iOS que inscriban los usuarios. El seguimiento de las fechas de caducidad no solo implica estar al día de las fechas de caducidad en sí, sino también saber qué usuarios utilizan qué versión de la aplicación. Existen dos soluciones: enviar por correo electrónico los perfiles de aprovisionamiento a los usuarios o ponerlos en un portal Web para que se puedan descargar e instalar desde allí. Estas soluciones funcionan, pero no son infalibles, puesto que los usuarios deben actuar siguiendo las instrucciones de un correo o visitar el portal Web para descargar e instalar el perfil en cuestión. Si quiere que este proceso sea transparente para los usuarios, en XenMobile puede instalar y quitar perfiles de aprovisionamiento con directivas de dispositivo. Se quitan los perfiles que falten o hayan caducado y se instalan perfiles actualizados en los dispositivos de los usuarios, por lo que tocar una aplicación solo la abre para su uso.

Provisioning Profile Removal	Puede eliminar perfiles de aprovisionamiento iOS con la ayuda de directivas de dispositivo. Para obtener más información acerca de los perfiles de aprovisionamiento, consulte cómo agregar un perfil de aprovisionamiento.
Proxy	En XenMobile, puede agregar una directiva de dispositivos para especificar la configuración global de proxy HTTP en dispositivos con Windows Mobile/CE y 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.
Registro del sistema	El Registro de Windows Mobile/CE almacena datos sobre las aplicaciones, los controladores, las preferencias del usuario y los parámetros de configuración. En XenMobile, puede definir los valores y las claves del Registro que permitirán administrar dispositivos Windows Mobile/CE.
Remote Support	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.
Restricciones	La directiva de restricciones ofrece al administrador diversas opciones para bloquear y controlar las características y la funcionalidad de los dispositivos administrados. Existen cientos de opciones de restricción para los dispositivos respaldados, que van desde inhabilitar la cámara o el micrófono del dispositivo móvil, a imponer reglas de roaming y acceso a servicios externos como, por ejemplo, tiendas de aplicaciones. 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. 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". Las excepciones principales son la función "Security - Force" de iOS y todas las funciones de tabletas Windows, que tienen el valor predeterminado "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.
Roaming	En XenMobile, puede agregar una directiva de dispositivos para configurar si se permite el roaming de voz y de datos en los dispositivos iOS o Windows Mobile/CE de los usuarios. Si se inhabilita la movilidad de voz, la movilidad de datos se inhabilita automáticamente. En el caso de iOS, esta directiva solo está disponible para iOS 5.0 y versiones posteriores.
Samsung SAFE Firewall	Esta directiva permite configurar los parámetros del firewall para dispositivos Samsung. Puede escribir las direcciones IP, los puertos y los nombres de host a los que quiera permitir o bloquear el acceso de los dispositivos. También puede configurar el proxy y las opciones de reenrutado de este.
Samsung MDM License Key	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 se implementa la clave de Samsung ELM, el parámetro "Samsung MDM API available" se establece en "True".

SCEP	Esta directiva permite configurar dispositivos iOS y Mac OS X 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.
Sideloading Key	En XenMobile, la instalación de aplicaciones mediante "sideloading" permite implementar en dispositivos Windows 8.1 aplicaciones no adquiridas en la Tienda Windows. Por regla general, se realiza una instalación sideloading 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 sideloading de las aplicaciones, configure la clave de sideloading 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 de producto de carga lateral, 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 de producto de sideloading
Signing Certificate	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.
Single Sign On (SSO) Account	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.
Storage Encryption	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 Samsung SAFE, Windows Phone y Android Sony. Cada plataforma requiere un conjunto diferente de valores, que se describen en el artículo referente a la directiva Encryption en esta sección.

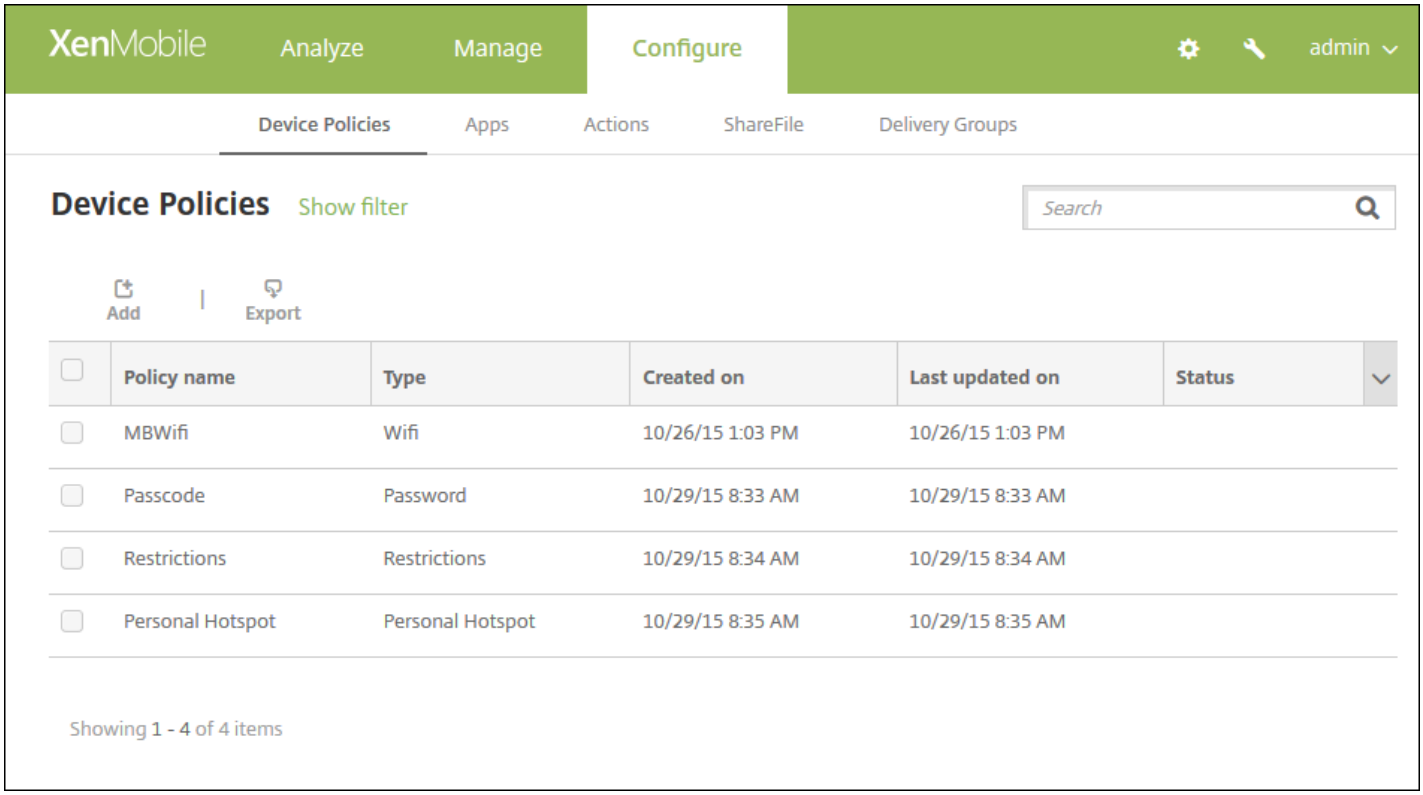
Subscribed Calendars	En XenMobile, puede agregar una directiva de dispositivos para agregar un calendario suscrito a la lista de calendarios en los dispositivos iOS de los usuarios. La lista de los calendarios públicos a los que se puede suscribir está disponible en www.apple.com/downloads/macosx/calendars. Nota: Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.
Terms and Conditions	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. Debe suministrar un archivo para cada combinación de plataforma e idioma que quiera implementar. Para dispositivos Android y iOS, debe proporcionar archivos PDF. Para dispositivos Windows, debe suministrar archivos de texto (.txt) y los archivos de imagen correspondientes.
VPN	Para los clientes que quieran ofrecer acceso a sistemas backend con tecnología antigua de VPN Gateway, esta directiva de VPN se puede usar para enviar los datos de la conexión de puerta de enlace VPN al dispositivo. Se da respaldo a varios proveedores de VPN a través de esta directiva, incluidos Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y habilitar VPN a demanda (siempre que la puerta de enlace VPN respalde esta opción). 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. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en el artículo VPN de esta sección.
Wallpaper	Puede agregar un archivo JPG o PNG para establecer un fondo de escritorio en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Disponible en iOS 7.1.2 y versiones posteriores. Para usar fondos de pantalla diferentes en dispositivos iPad y iPhone, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.
Web Content Filter	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.

Webclip	Con esta directiva, puede colocar los accesos directos a sitios Web o clips Web de forma que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips Web en dispositivos iOS, Mac OS X y Android; las tabletas Windows solo requieren una etiqueta y una URL.
WiFi	La directiva WiFi permite que los administradores puedan enviar datos de enrutadores de Wi-Fi a los dipositivos administrados: SSID y datos de autenticación y configuración. Mediante las directivas de redes WiFi, puede administrar el modo en que los usuarios conectan sus dispositivos a redes inalámbricas WiFi. 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 WiFi de manera uniforme para todos los usuarios de las plataformas de dispositivo que seleccione. Puede configurar los parámetros de Wi-Fi para los usuarios de las plataformas que se indican a la izquierda, pero cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en el artículo WiFi en esta sección.
Windows CE Certificate	Agregue esta directiva de dispositivo para crear y entregar certificados de Windows Mobile/CE desde una infraestructura PKI externa a los dispositivos de los usuarios. Para obtener más información acerca de los certificados y las entidades de infraestructura PKI, consulte Certificados.
Worx Store	En XenMobile, puede crear una directiva para especificar si los dispositivos iOS, Android o tabletas Windows mostrarán un clip Web de Worx Store en la pantalla de inicio.
XenMobile Options	Puede agregar una directiva de opciones de XenMobile para configurar el comportamiento de Worx Home al conectarse a XenMobile desde dispositivos Android y Windows Mobile/CE.
XenMobile Uninstall	En XenMobile, puede agregar esta directiva de dispositivo para desinstalar XenMobile de dispositivos Android y Windows Mobile/CE. Cuando se implementa, esta directiva elimina XenMobile de todos los dispositivos que contenga el grupo de implementación.

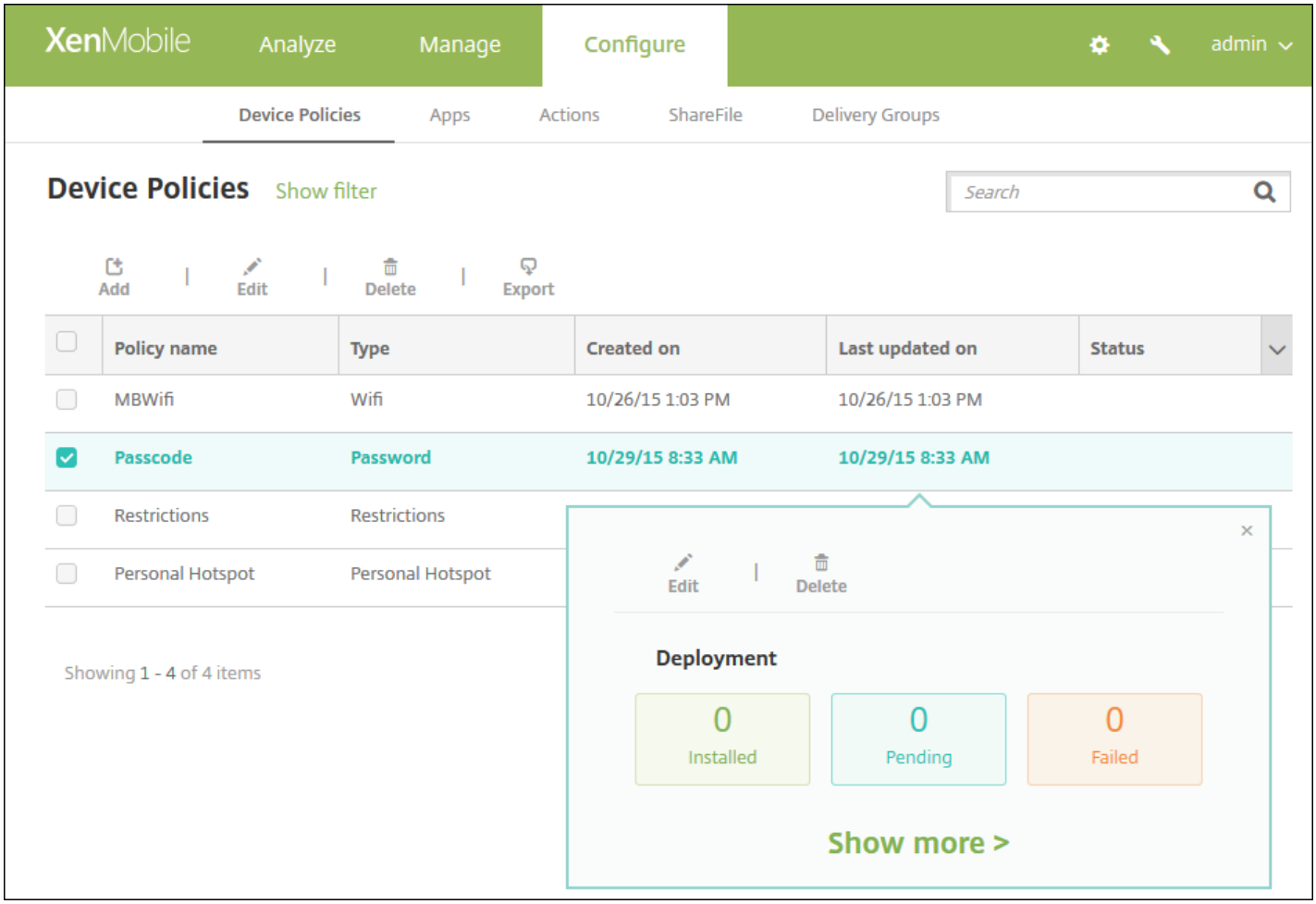
La página de directivas de dispositivos en la consola

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 a la derecha 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**.

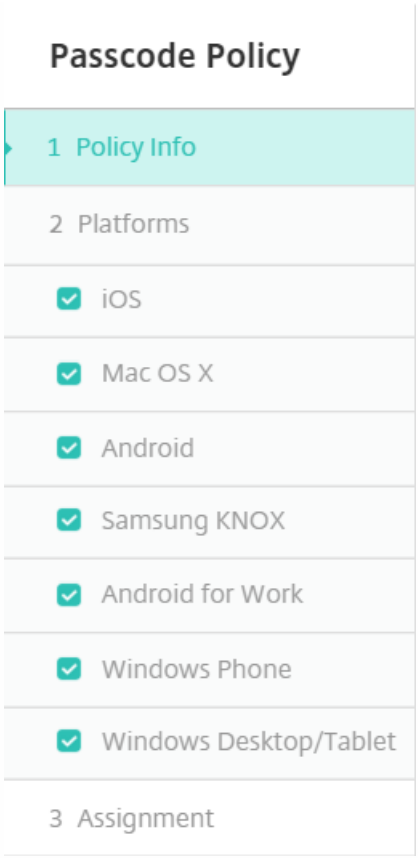
Aparecerá el cuadro de diálogo **Add a New Policy**. Puede expandir **More** para ver más directivas.

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.

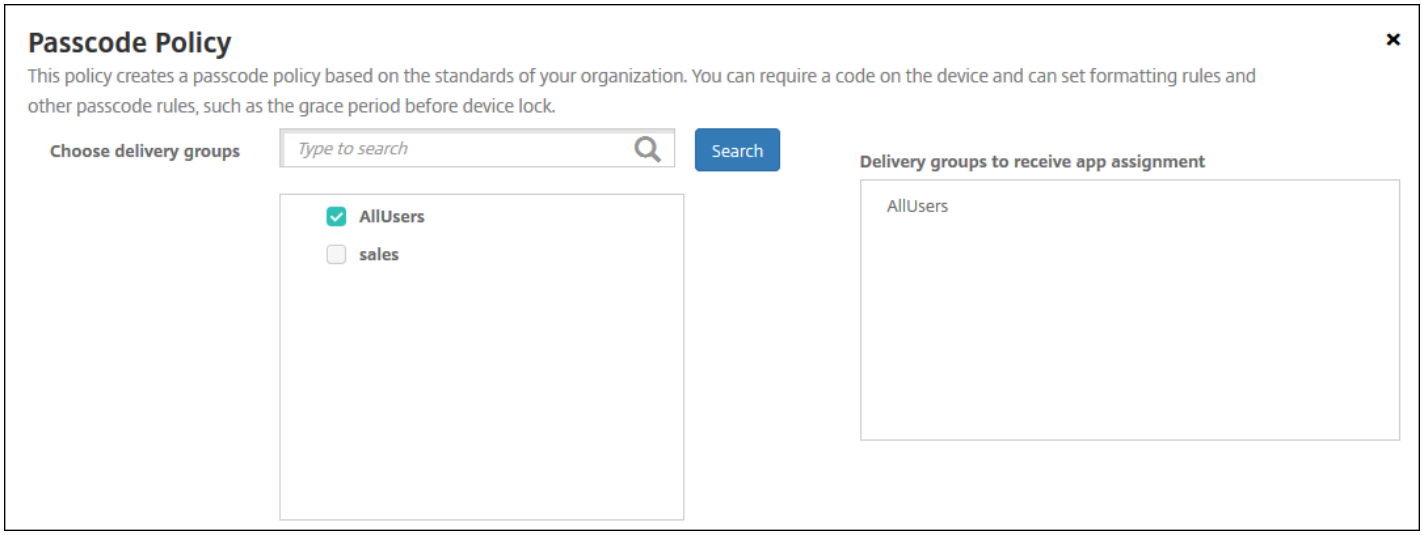


4. Complete los datos de la página **Policy Information** y haga clic en **Next**. La página **Policy Information** recopila información (como el nombre de la directiva) para ayudarle a identificar sus directivas y realizar un seguimiento de ellas. Esta página es similar para todas las directivas.

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

Aug 25, 2016

Para ver las directivas clasificadas por plataforma, descargue el documento Device Policies by Platform Matrix en formato PDF.

Puede agregar y configurar las directivas de dispositivos en la consola de XenMobile, desde **Configure > Device Policies**. XenMobile 10.3 admite las directivas de dispositivo para las plataformas siguientes:

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Phone 8/Windows 10 Mobile
- Windows 8 y Windows 10 de escritorio o tableta (.86)

> ## Nota
>
> El respaldo a dispositivos Symbian está obsoleto en XenMobile 10.3.

Directivas de duplicación de AirPlay

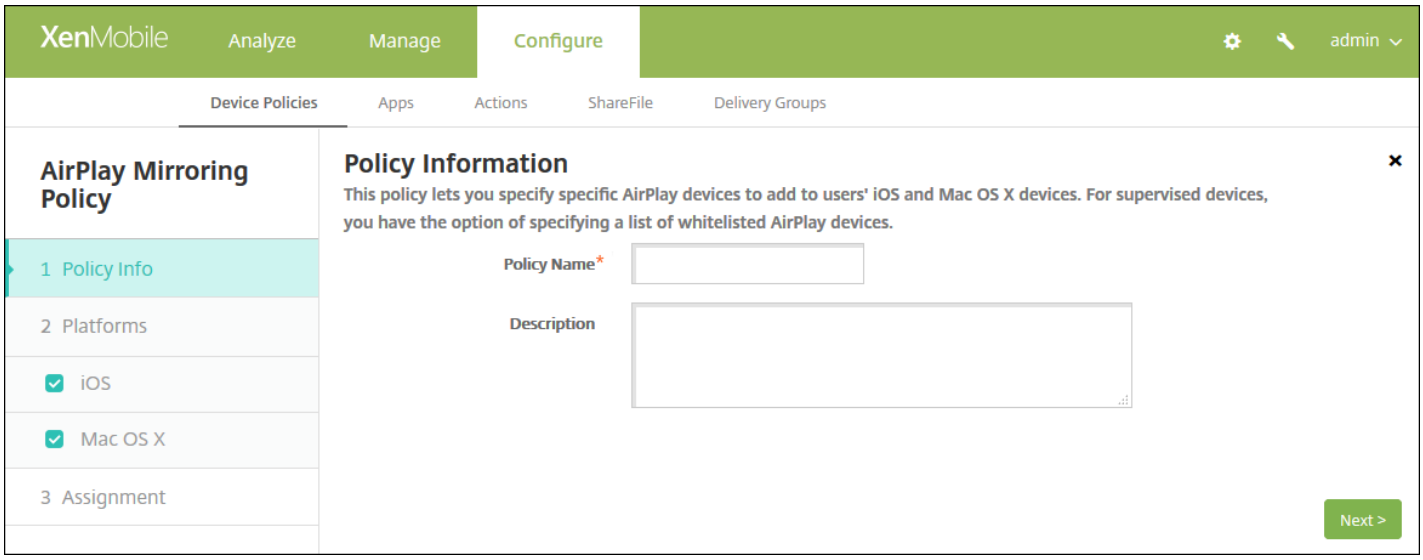
Aug 25, 2016

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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **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:

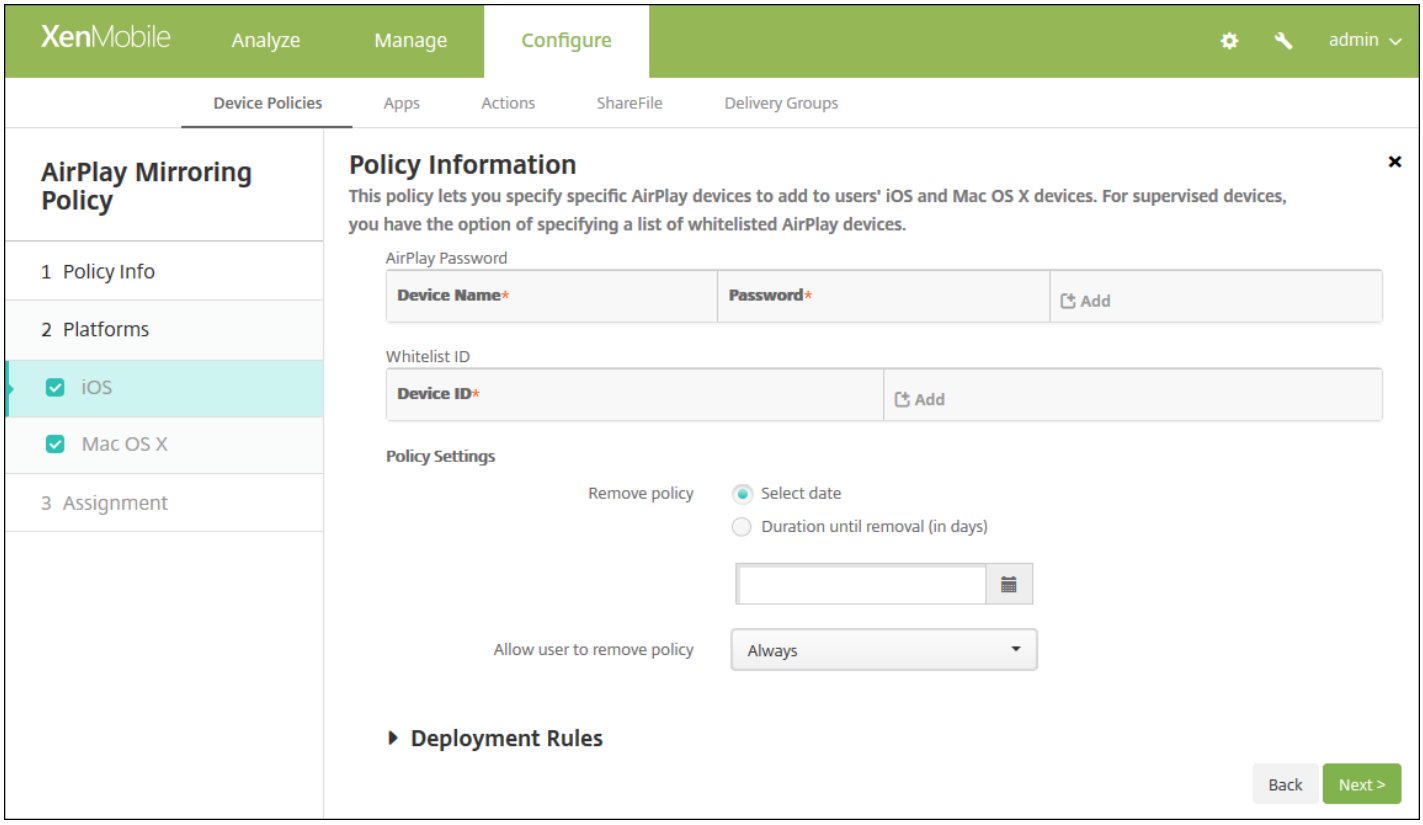
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure estos parámetros:

- **AirPlay Password**. Para cada dispositivo que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID**. Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Password**. Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.
- **Whitelist ID**. Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID**. Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.

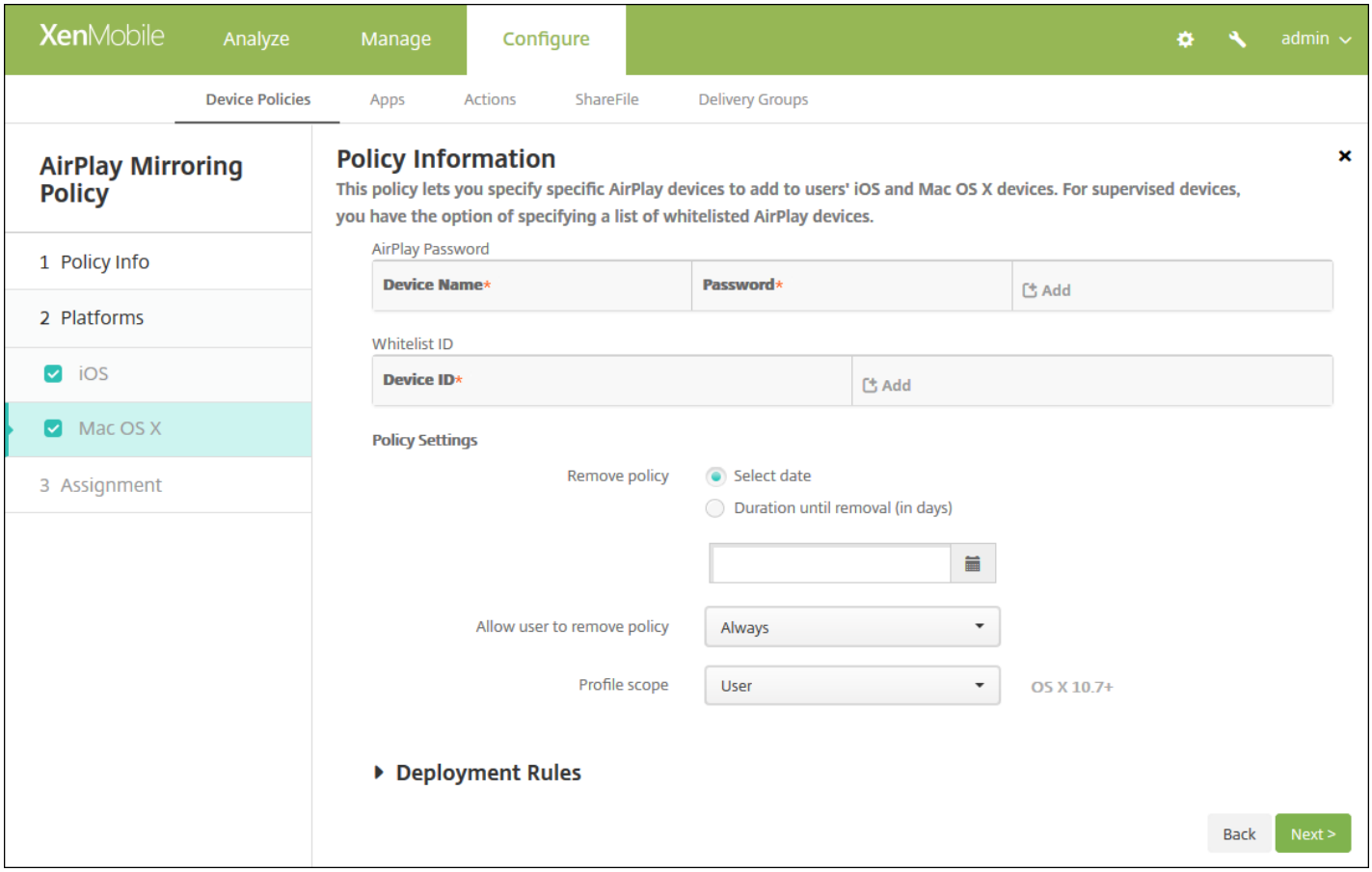
    Nota: Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.

- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure estos parámetros:

- **AirPlay Password**. Para cada dispositivo que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID**. Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Password**. Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.
- **Whitelist ID**. Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID**. Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.

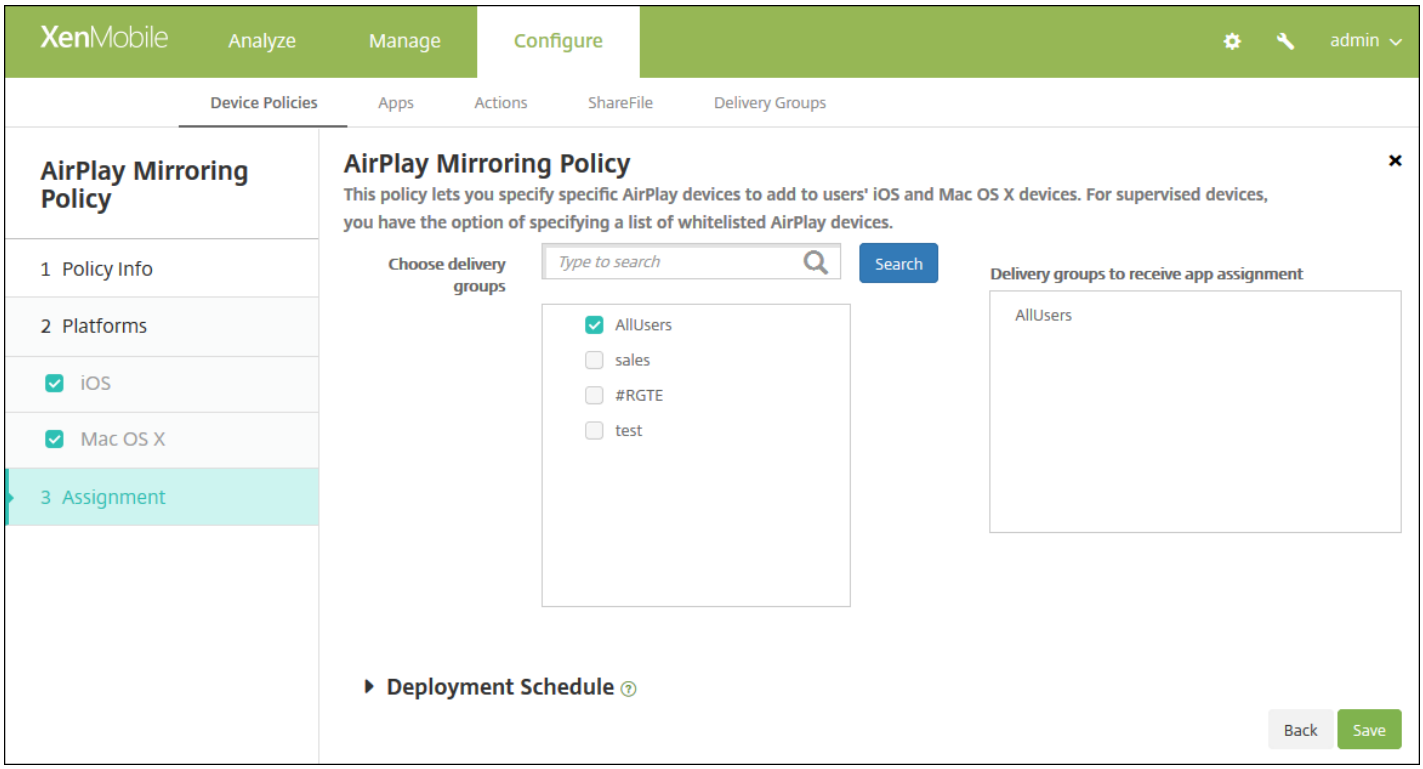
    Nota: Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **AirPlay Mirroring 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.

- 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.
- 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 aplica para iOS.

11. Haga clic en **Save**.

Directiva de AirPrint

Jul 27, 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.

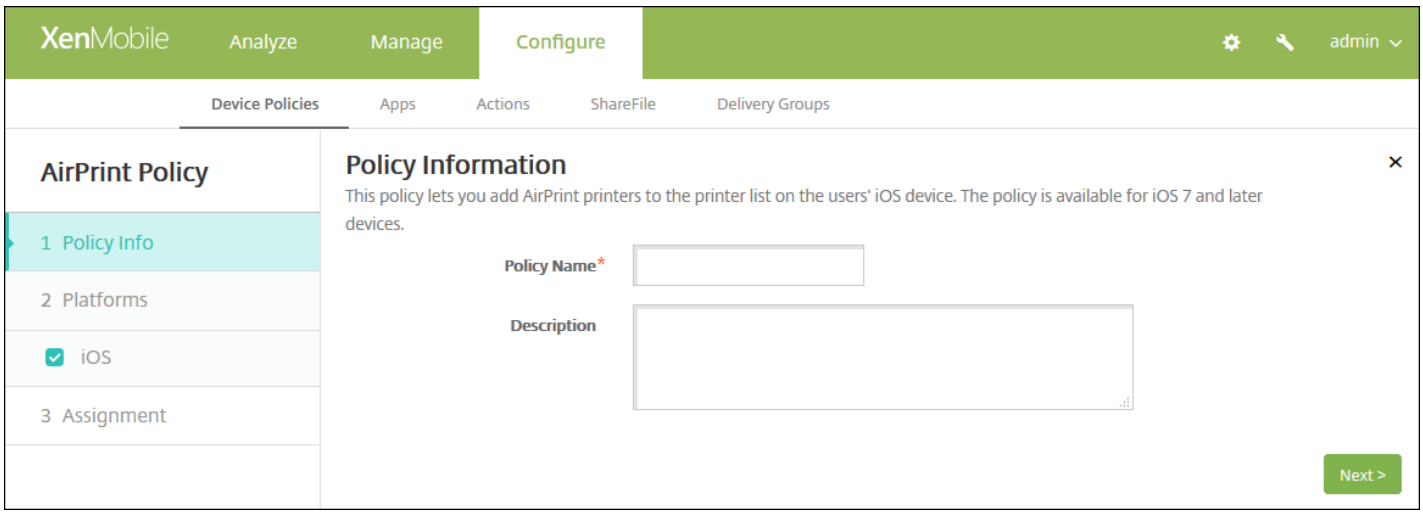
Nota:

- 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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

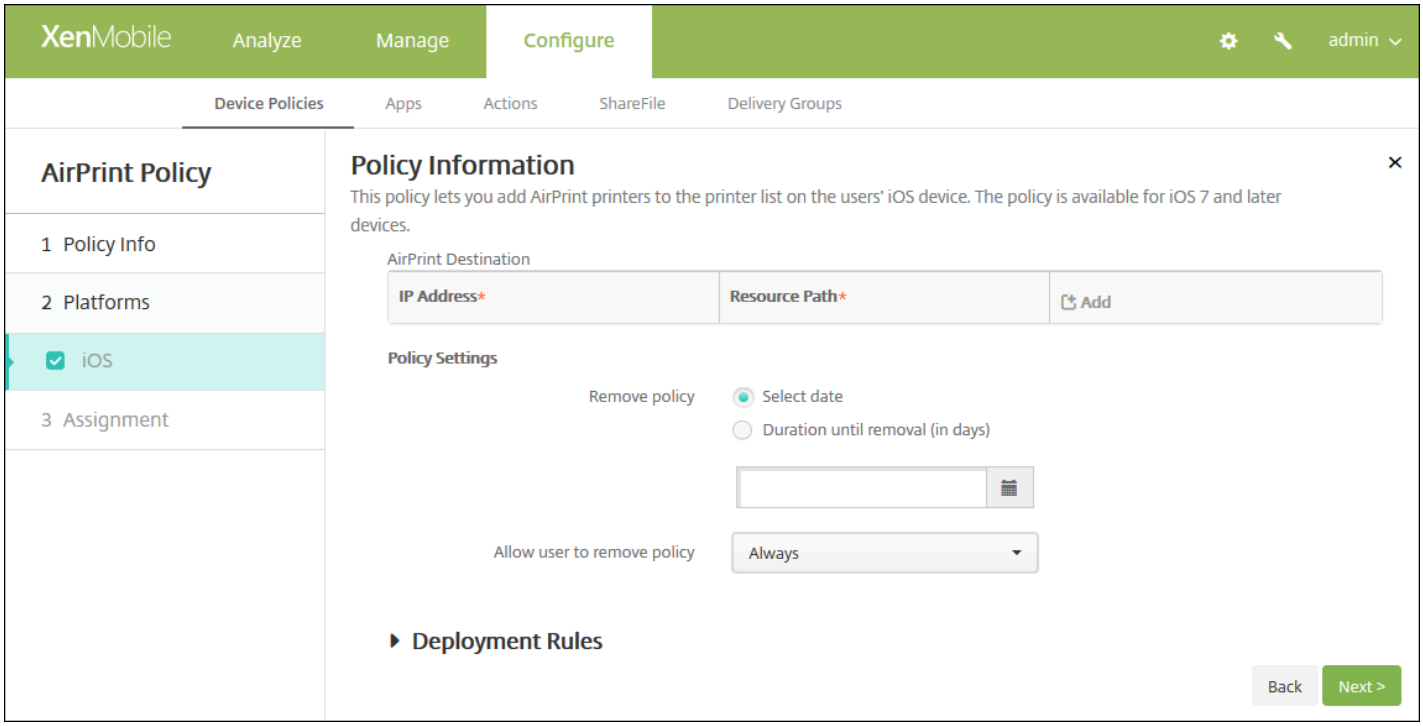
3. Haga clic en **More** y, en **End user**, haga clic en **AirPrint**. Aparecerá la página **AirPrint Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **iOS Platform Information**.



6. Configure los siguientes parámetros:

- **AirPrint Destination**. Para cada destino de AirPrint que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **IP Address**. Escriba la dirección IP de la impresora AirPrint.
  - **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.
  - Haga clic en **Save** para agregar la impresora, o bien haga clic en **Cancel** para no agregarla.

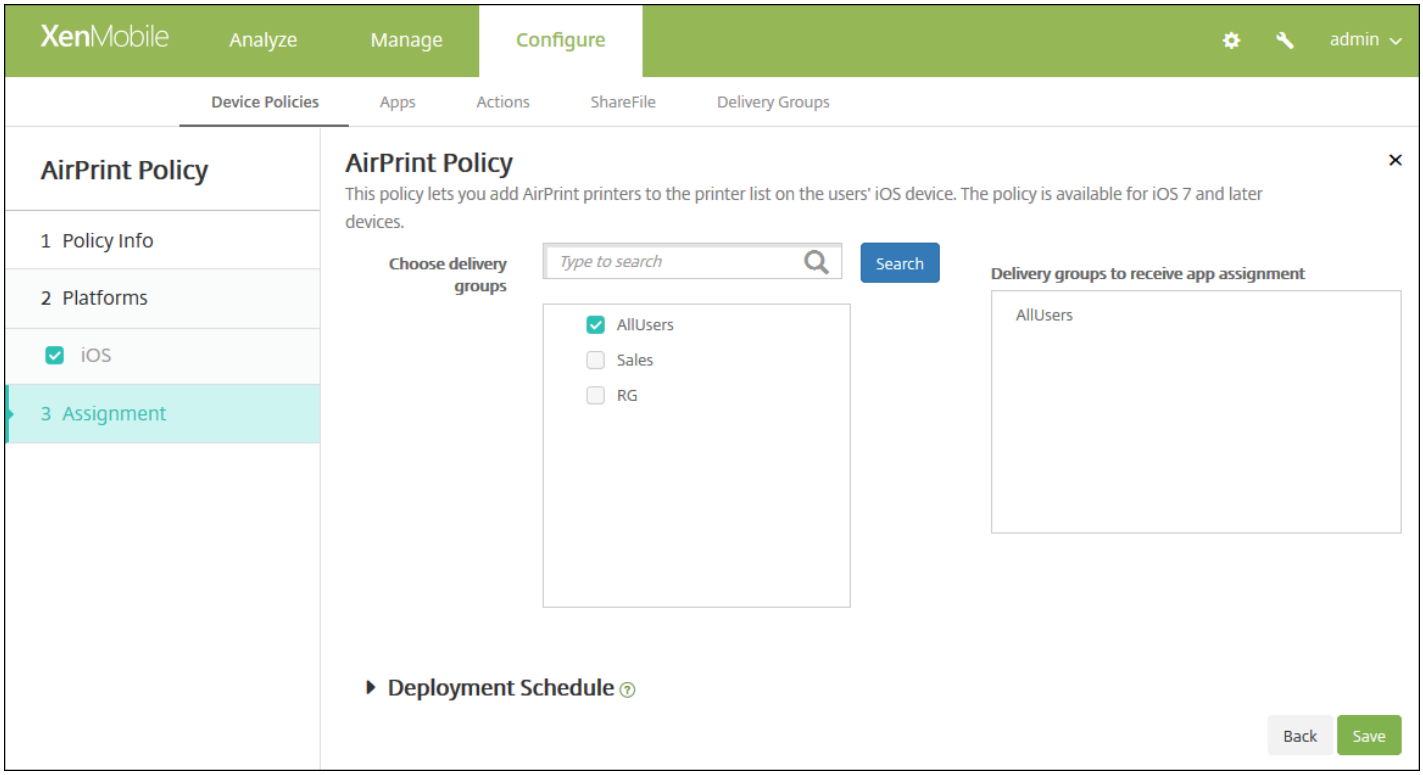
    Nota: Para eliminar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para 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.

- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **AirPrint 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de restricción de aplicaciones Android for Work

Jul 27, 2016

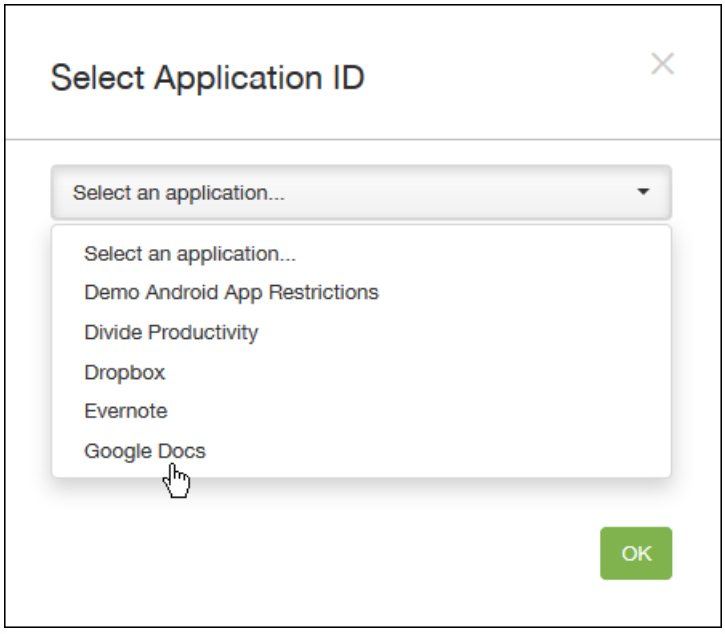
Puede modificar las restricciones asociadas a aplicaciones Android for Work. Sin embargo, antes de modificarlas, debe cumplir los siguientes requisitos previos:

- Complete, en Google, las tareas de configuración de Android for Work. Para obtener más información, consulte Managing Devices with Android for Work.
- Cree un conjunto de credenciales de Google Play. Para obtener más información, consulte Credenciales de Google Play.
- Cree una cuenta de Android for Work. Para obtener más información, consulte Creación de una cuenta de Android for Work.
- Agregue aplicaciones Android for Work a XenMobile. Para obtener más información, consulte Incorporación de aplicaciones a XenMobile.

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 la página **Add a New Policy**.

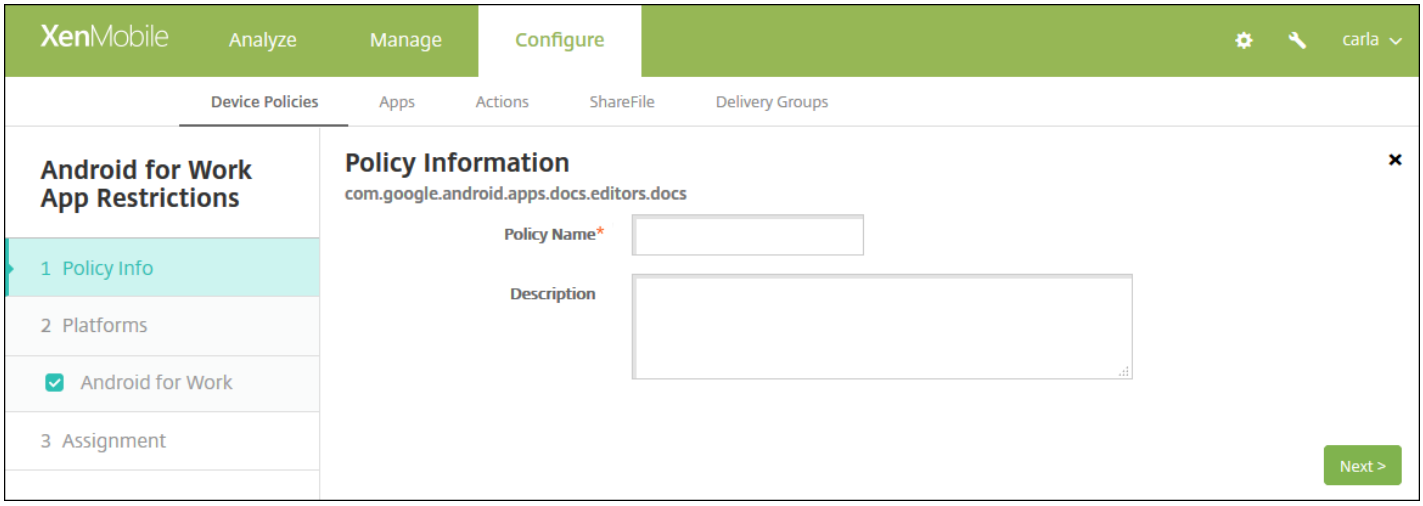
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Android for Work App Restrictions**. Aparecerá un cuadro de diálogo que le pedirá que seleccione una aplicación.



4. En la lista, seleccione la aplicación a la que quiere aplicar restricciones y, a continuación, haga clic en **OK**.

- Si no hay aplicaciones Android for Work que agregar a XenMobile, no podrá continuar. Para obtener más información sobre cómo agregar aplicaciones a XenMobile, consulte Incorporación de aplicaciones a XenMobile.
- Si la aplicación no tiene restricciones asociadas a ella, aparece una notificación a ese respecto. Haga clic en **OK** para cerrar el cuadro de diálogo.
- Si la aplicación tiene restricciones asociadas a ella, aparecerá la página de información **Android for Work App**

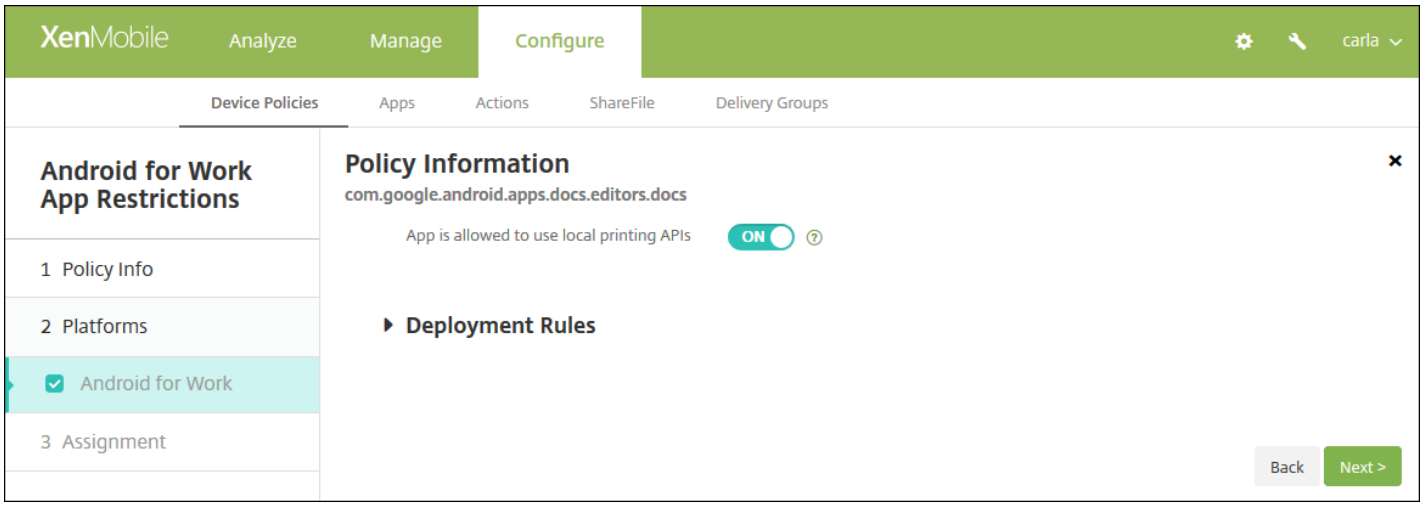
Restrictions Policy.



5. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

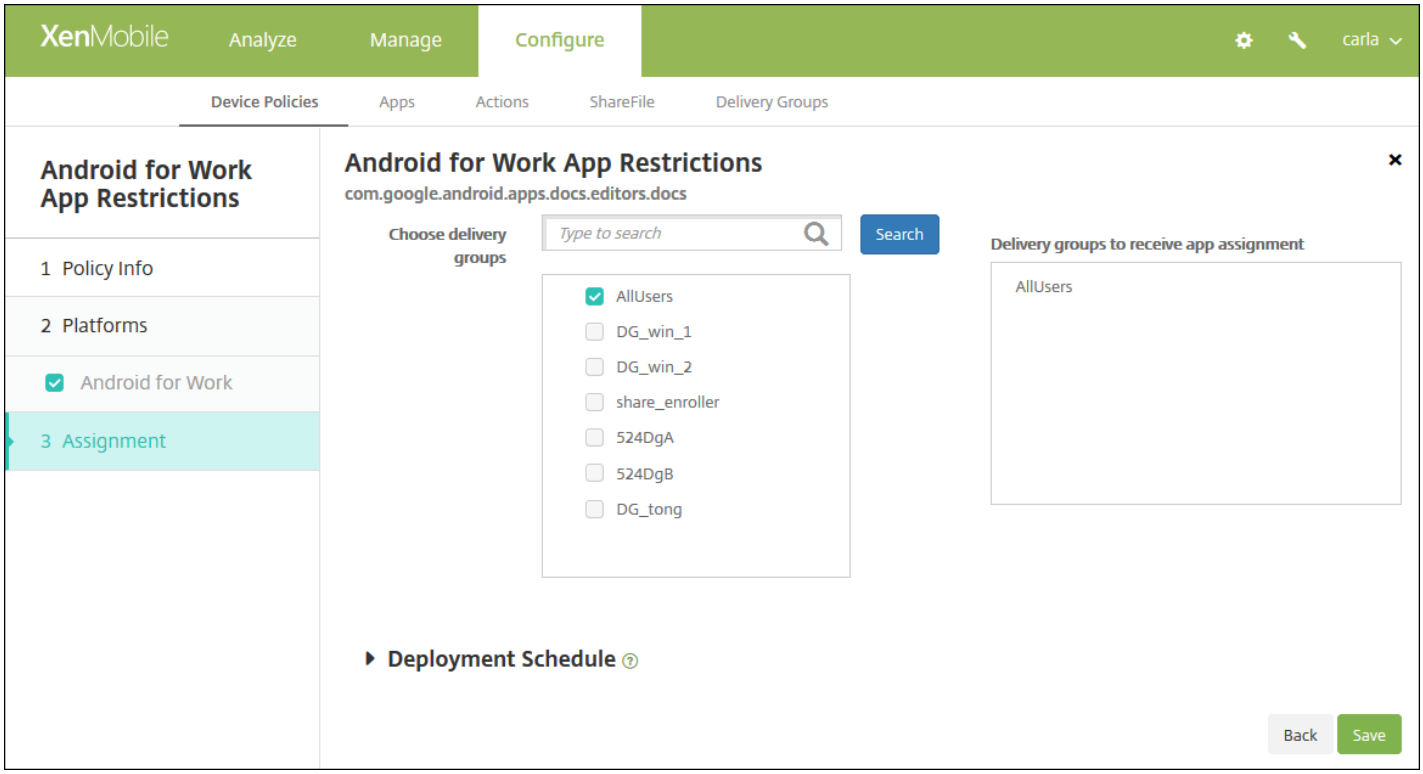
6. Haga clic en **Next**. Aparecerá la página referente a la plataforma **Android for Work**.



7. Configure los parámetros para la aplicación seleccionada. Los parámetros que aparecen dependen de las restricciones asociadas a la aplicación seleccionada.

8. Configure las reglas de implementación.

9. Haga clic en **Next**. Aparecerá la página de asignación **Android for Work App Restrictions 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 es aplicable en este caso.

12. Haga clic en **Save**.

Directivas APN de dispositivos

Jul 27, 2016

Puede agregar una directiva de nombres de punto de acceso (APN) personalizada para dispositivos iOS, Android y Windows Mobile/CE. Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. 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.

Configuración de iOS

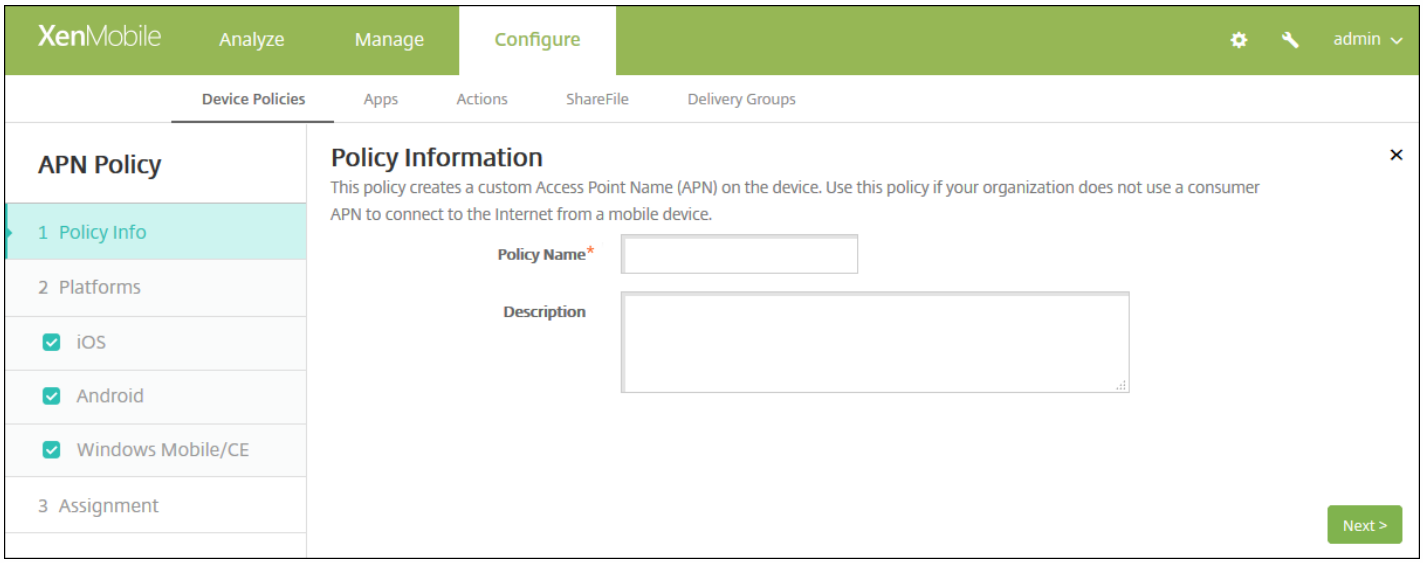
Configuración de Android

Configuración de Windows Mobile/CE

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Haga clic en **More** y, en **Network access**, haga clic en **APN**. Aparecerá la página de información **APN Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

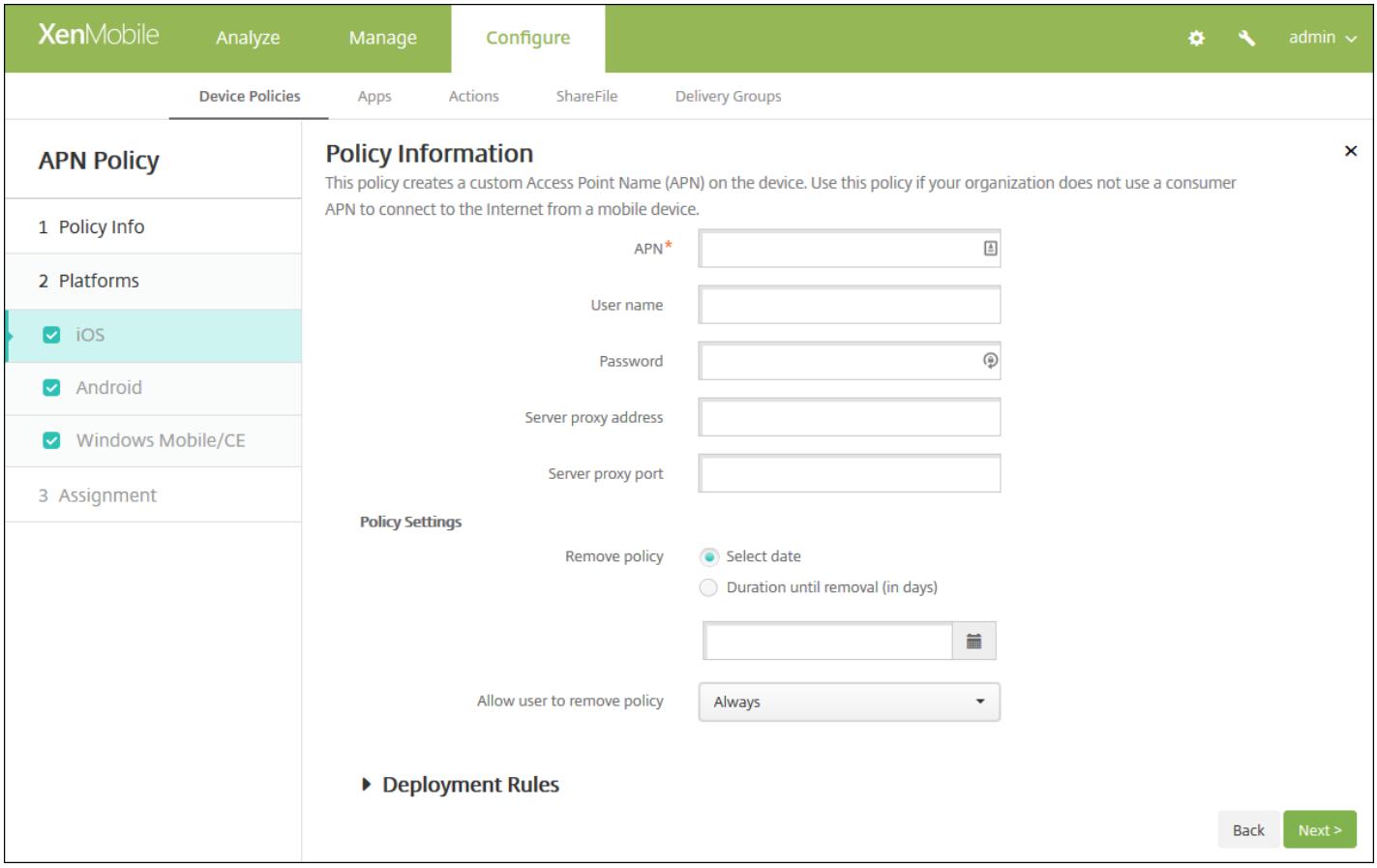
5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

Nota: Al aparecer la página **Policy Platforms**, todas las plataformas están seleccionadas, y verá en primer lugar la plataforma de iOS.

6. En **Platforms**, seleccione las plataformas que quiera agregar.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

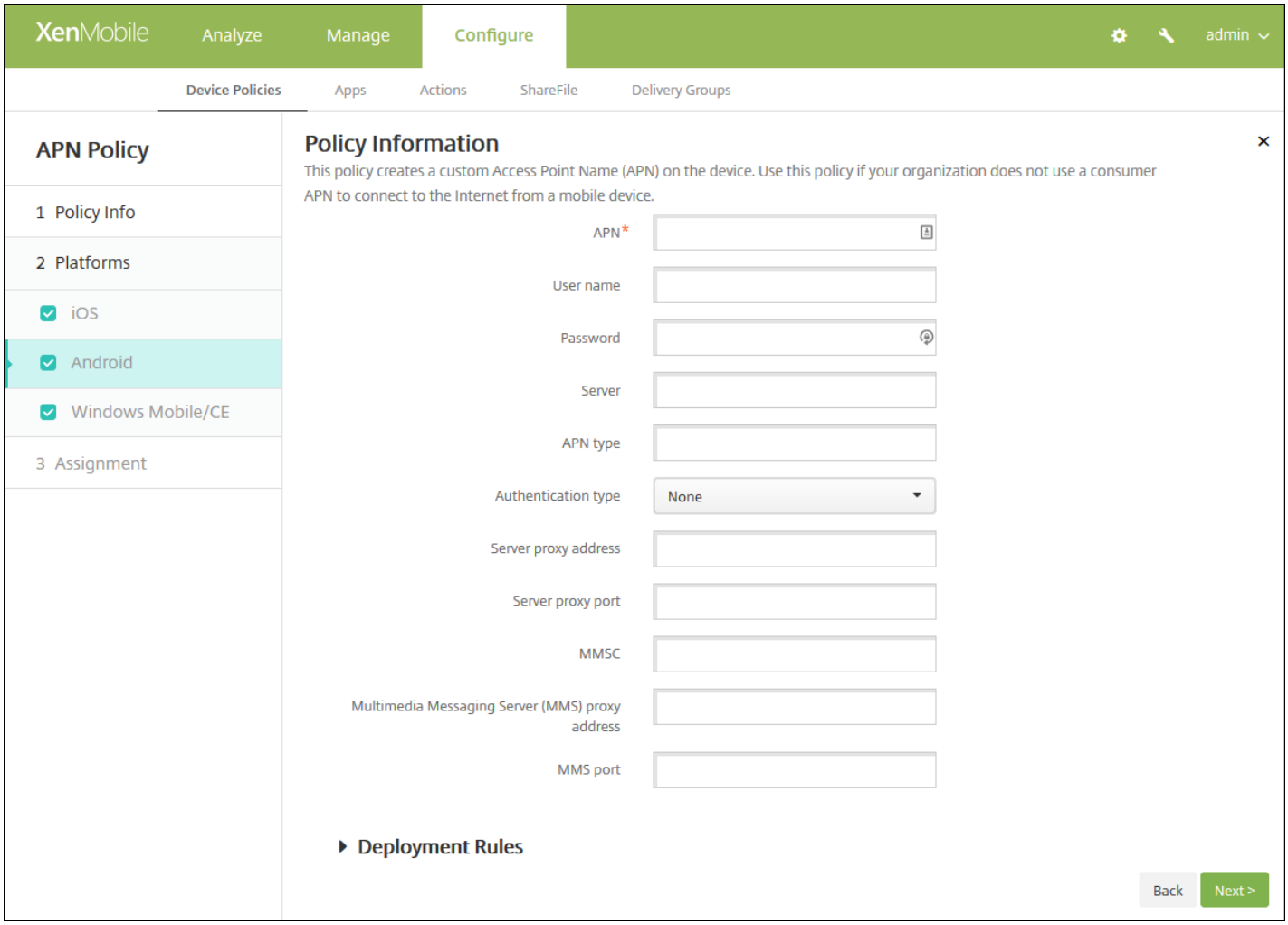
Configuración de los parámetros de iOS



Configure estos parámetros:

- **APN**: Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de IOS aceptado. De lo contrario, la directiva fallará.
- **User name**: Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.
- **Password**: La contraseña del usuario para este 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.
- **Server proxy address**: La dirección IP o dirección URL del proxy de APN.
- **Server proxy port**: El número de puerto del proxy de APN. Esto es necesario si especificó una dirección de servidor proxy.
- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Android



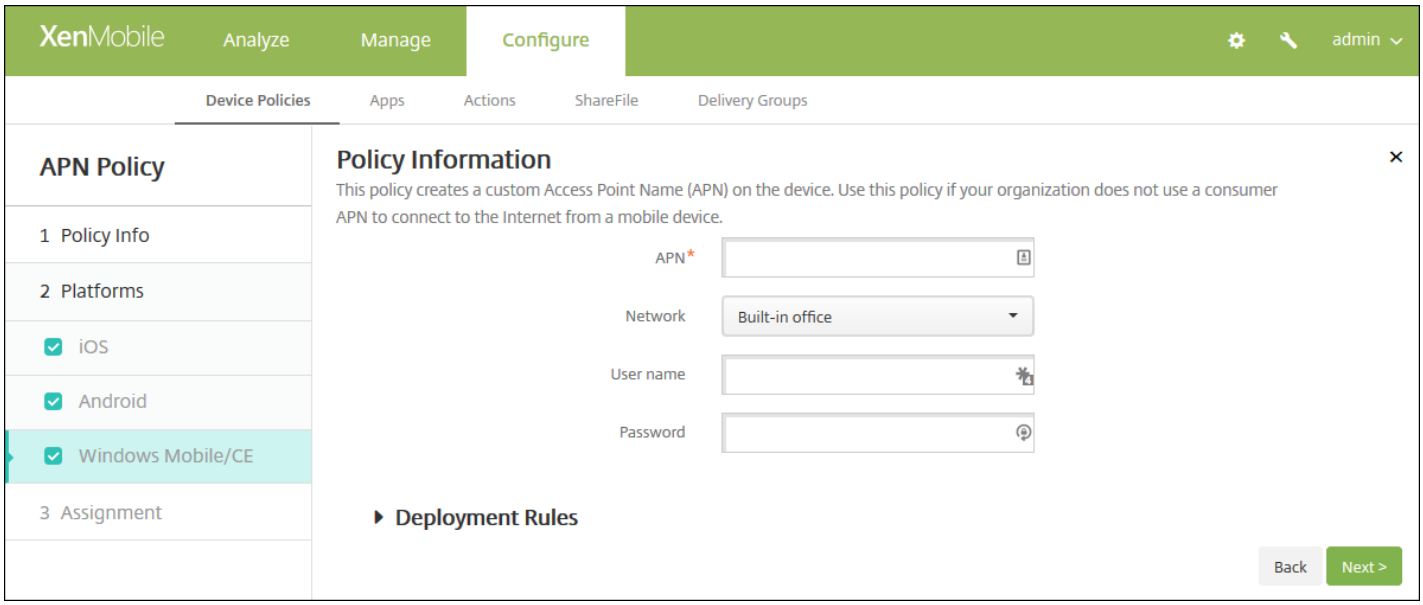
Configure estos parámetros:

- **APN**: Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de Android aceptado. De lo contrario, la directiva fallará.
- **User name**: Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.
- **Password**: La contraseña del usuario para este 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.
- **Server**: Este parámetro es anterior a los smartphones y normalmente queda 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.
- **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 (Dial Up Networking) está obsoleto y no se usa con frecuencia.
  - hipri. Redes de alta prioridad.

- fota. El firmware over-the-air se usa para recibir actualizaciones de firmware.

- **Authentication type**. En la lista, haga clic en el tipo de autenticación que se va a usar. El valor predeterminado es None.
- **Server proxy address**: La dirección IP o dirección URL del proxy HTTP de APN del operador.
- **Server proxy port**: El número de puerto del proxy de APN. Esto es necesario si especificó una dirección de servidor proxy.
- **MMSC**: La dirección del servidor de puerta de enlace MMS suministrada por el operador.
- **Multimedia Messaging Server (MMS) proxy address**: Este es el servidor de MMS para el tráfico de mensajes multimedia. 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).
- **MMS port**: El puerto utilizado para el proxy MMS.

Configuración de los parámetros de Windows Mobile/CE

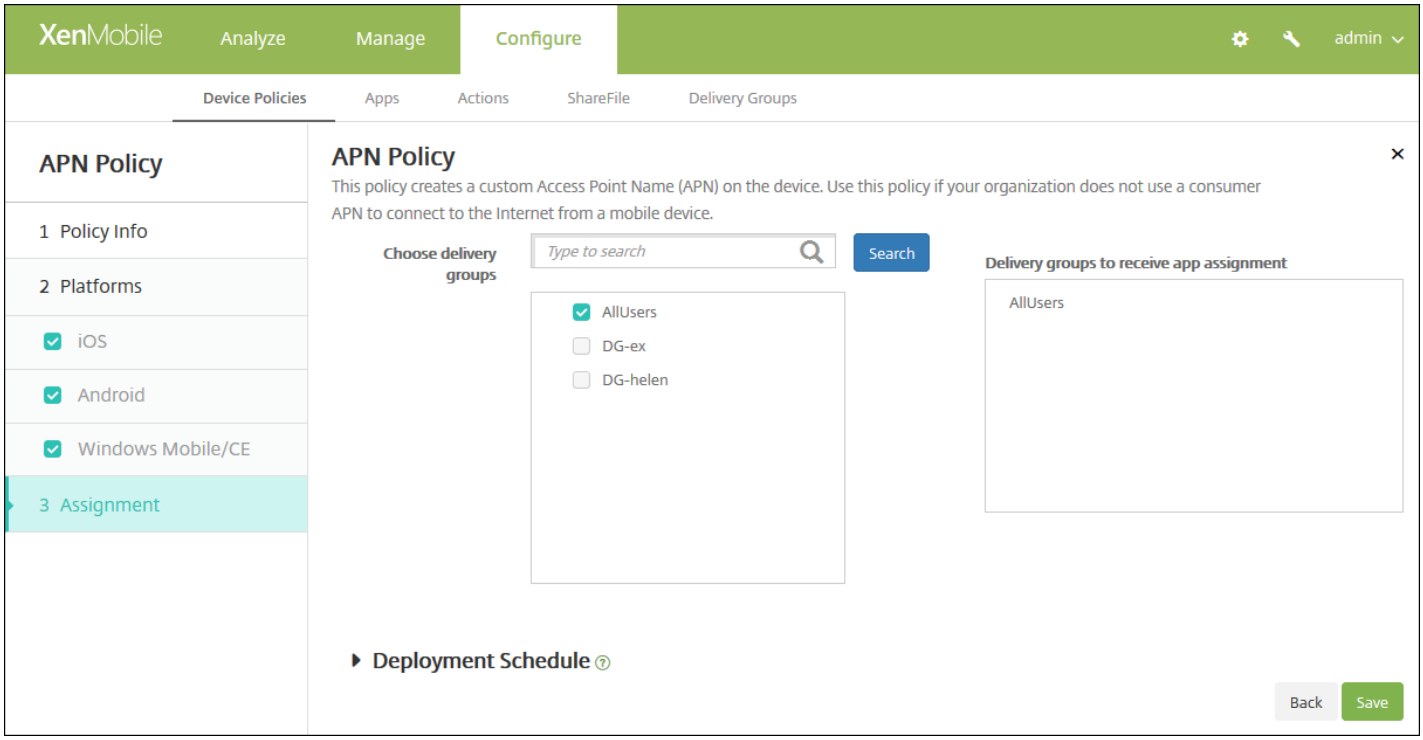


Configure los siguientes parámetros:

- **APN**: Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de Android aceptado. De lo contrario, la directiva fallará.
- **Network**. En la lista, haga clic en el tipo de red que quiere usar. El valor predeterminado es **Built-in office**.
- **User name**: Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación del perfil.
- **Password**: La contraseña del usuario para este 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.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **APN 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

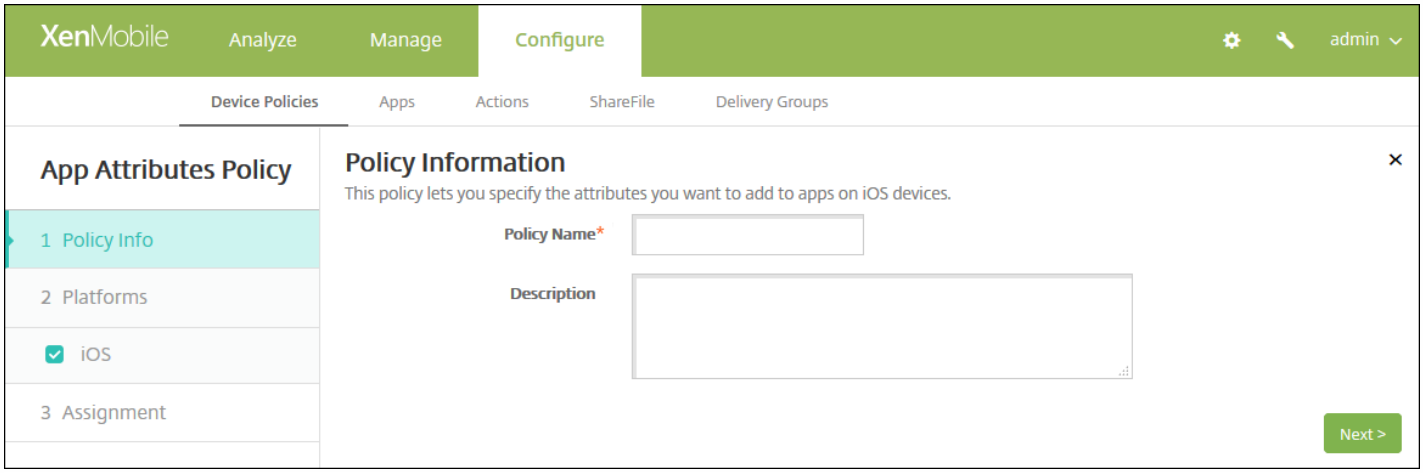
Nota:

- 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.
- 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 aplica para iOS.

11. Haga clic en **Save** para guardar la directiva.

Directiva de atributos de aplicaciones

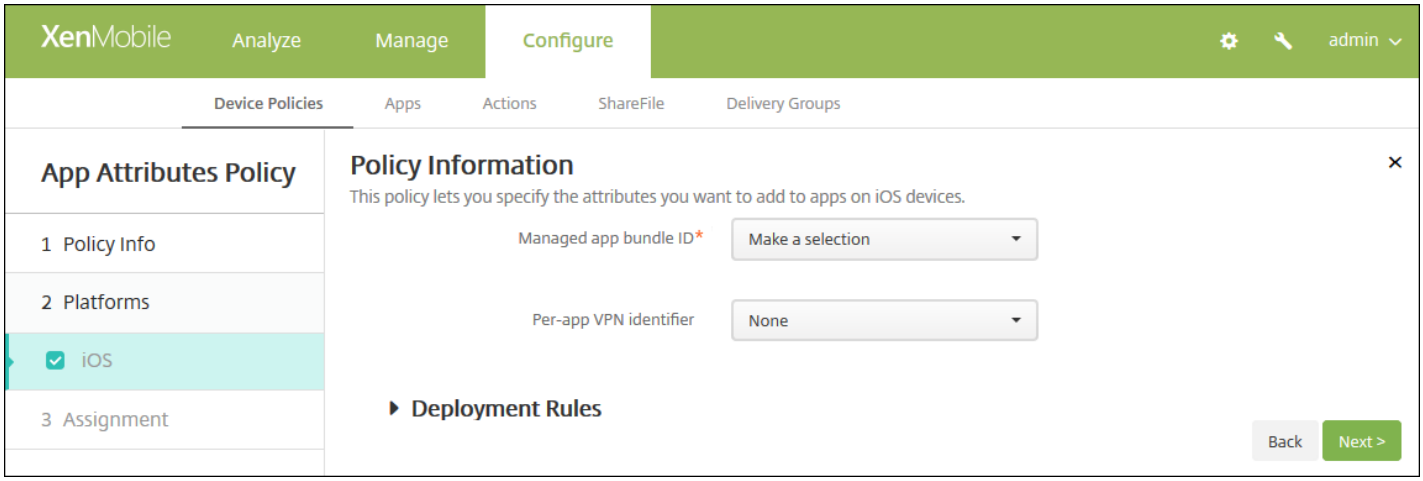
Jul 27, 2016



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información referente a los atributos de las aplicaciones de plataforma **App Attributes**.

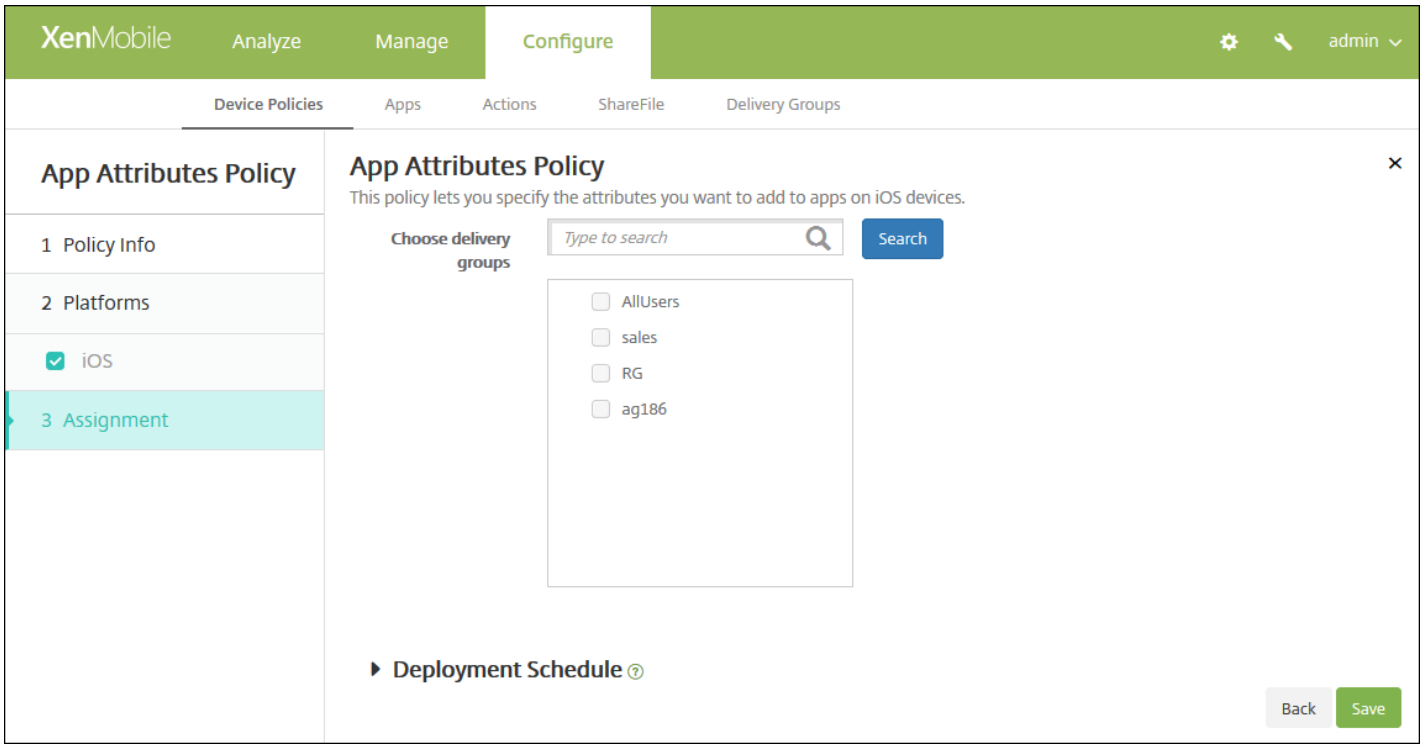


6. Configure los siguientes parámetros:

- **Managed app bundle ID**. En la lista, haga clic en un ID de paquete de aplicación o en **Add new**.
  - Si hace clic en **Add new**, escriba el ID del paquete de aplicación en el campo que aparece.
- **Per-app VPN identifier**. En la lista, haga clic en el identificador de red VPN para cada aplicación.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación App Attributes 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 acceso de aplicaciones

Jul 27, 2016

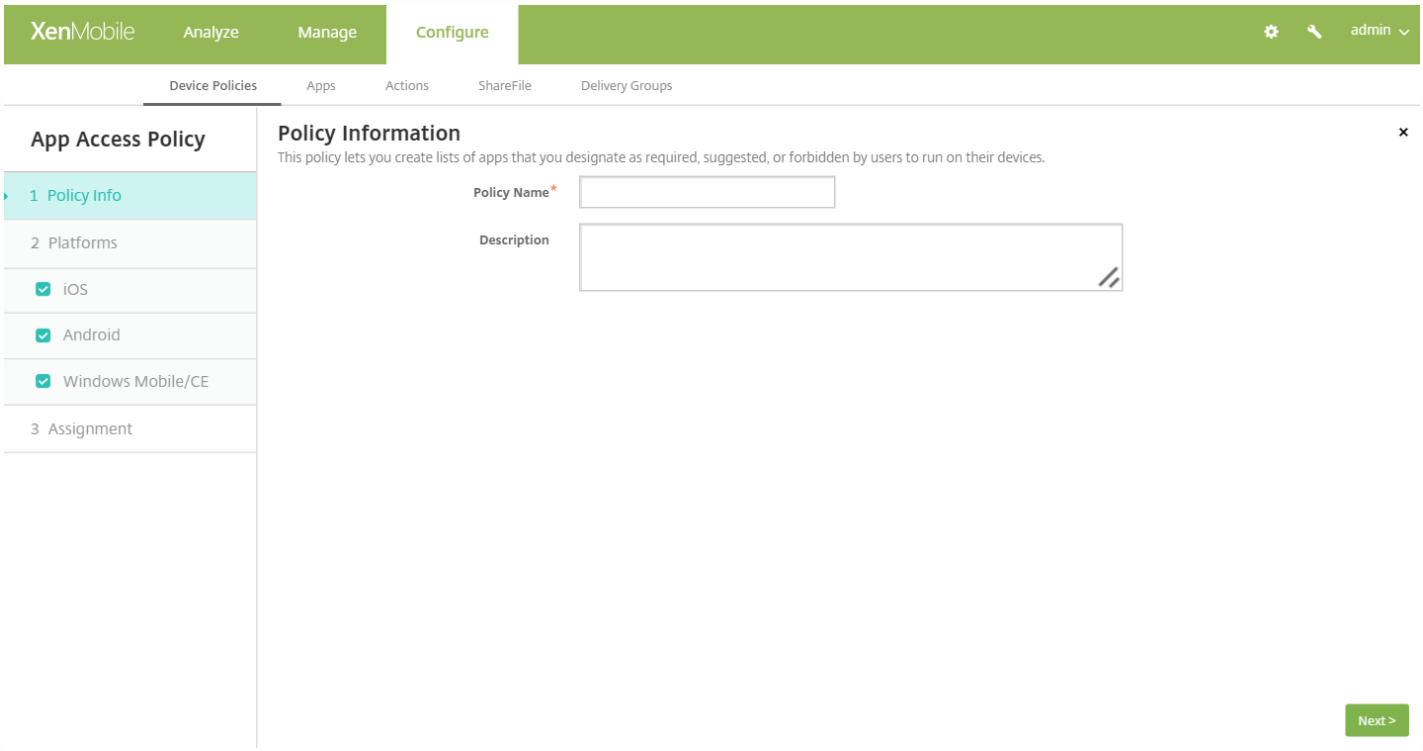
En XenMobile, la directiva de acceso de aplicaciones permite definir una lista de las aplicaciones que deben estar instaladas en el dispositivo, pueden estar instaladas en el dispositivo o no deben estar instaladas en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento del dispositivo con los requisitos de dicha lista de aplicaciones. Puede crear directivas de acceso a aplicaciones para dispositivos iOS, Android y Windows Mobile/CE.

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 **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Haga clic en **More** y, a continuación, en **Apps**, haga clic en **App Access**. Aparecerá la página de información **App Access Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

6. Configure los siguientes parámetros para cada una de las plataformas seleccionadas.

- **Access policy**. Haga clic en Required, Suggested o Forbidden. El valor predeterminado es Required.
- Para agregar una o varias aplicaciones a la lista, haga clic en **Add** y, a continuación, lleve a cabo lo siguiente:
  - **App name**. Escriba un nombre de aplicación.
  - **App Identifier**. Escriba un identificador opcional de la aplicación.
  - Haga clic en **Save** o **Cancel**.
  - Repita estos pasos 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 a la derecha. 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. Configure las reglas de implementación.

8. Haga clic en Next. Aparecerá la página de la plataforma siguiente o bien la página de asignación **App Access 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de configuración de aplicaciones

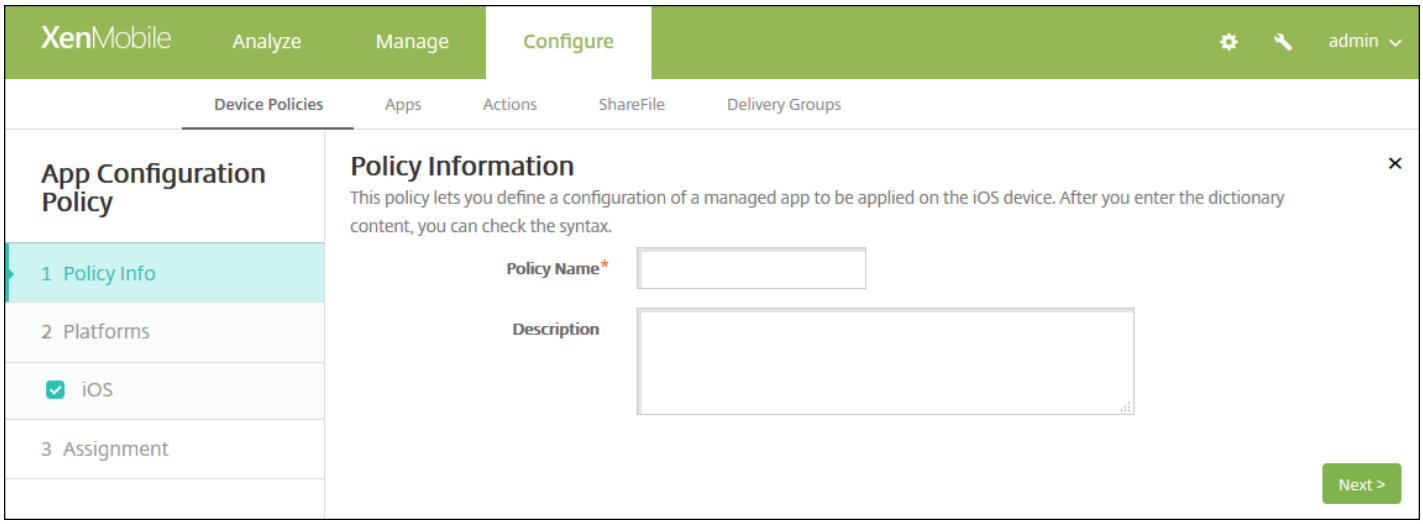
Jul 27, 2016

Puede configurar de manera remota una aplicación de App Store que respalde una configuración administrada, implementando un archivo XML de configuración (llamado lista de propiedades o plist) en los dispositivos iOS de los usuarios, para configurar varios parámetros y comportamientos de la aplicación. Los parámetros y los comportamientos que se puedan configurar dependen de la aplicación y no forman parte del ámbito de este artículo.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá la página **Add a New Policy**.

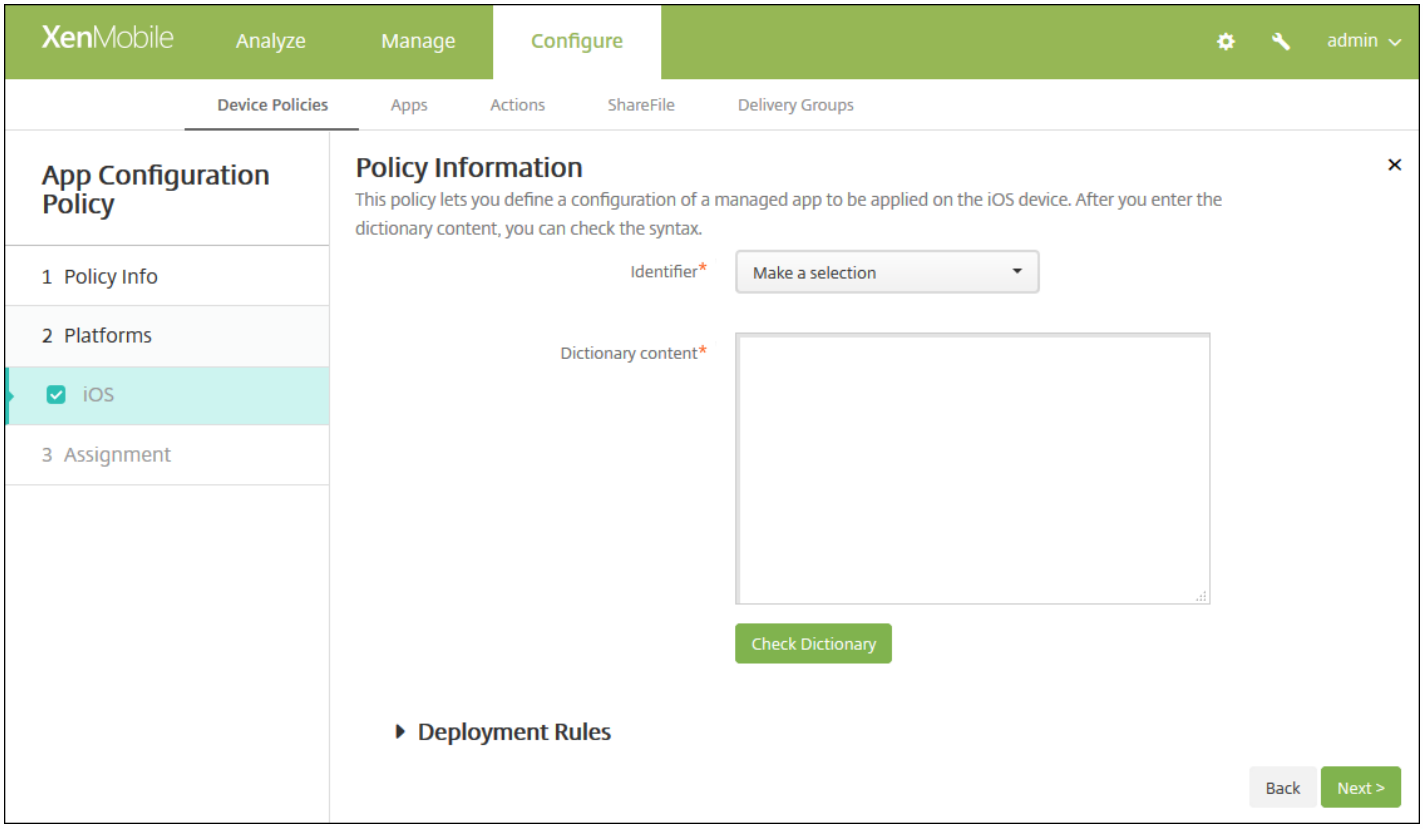
3. Haga clic en **More** y, a continuación, en **Apps**, haga clic en **App Configuration**. Aparecerá la página de información **App Configuration Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **iOS Platform**.

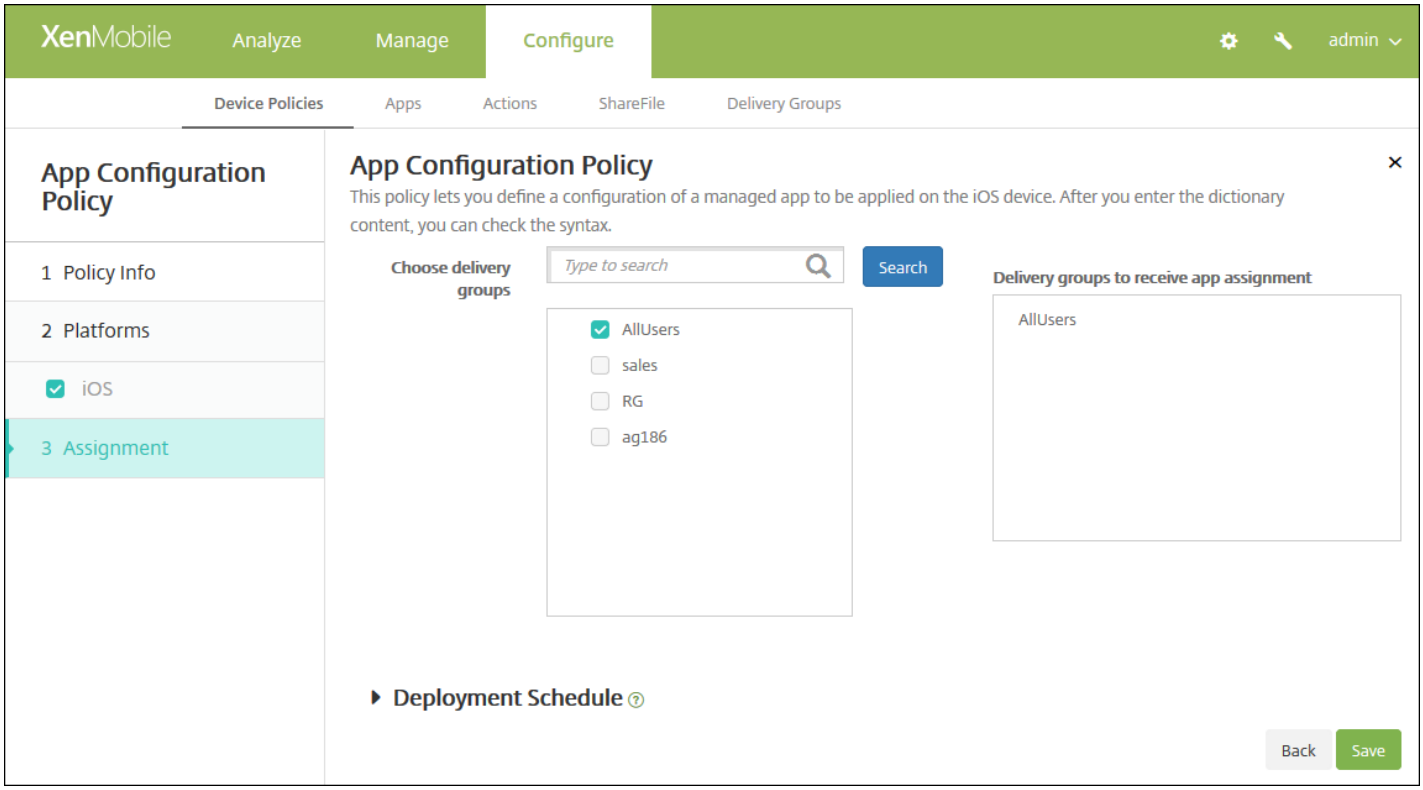


6. Configure los siguientes parámetros:

- **Identifier**. En la lista, haga clic en la aplicación que quiera configurar, o bien haga clic en **Add** para agregar una nueva aplicación a la lista.
  - Si hace clic en **Add new**, escriba el identificador de la aplicación en el campo que aparece.
- **Dictionary content**. Escriba, o copie y pegue, la información de configuración de la lista de propiedades XML (plist).
- Haga clic en **Check Dictionary**. XenMobile verifica el archivo XML. Si no hay errores, verá **Valid XML** bajo el cuadro de contenido. Si apareciera algún error de sintaxis bajo el cuadro de contenido, deberá corregirlo antes de continuar.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App Configuration 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 inventario de aplicaciones

Jul 27, 2016

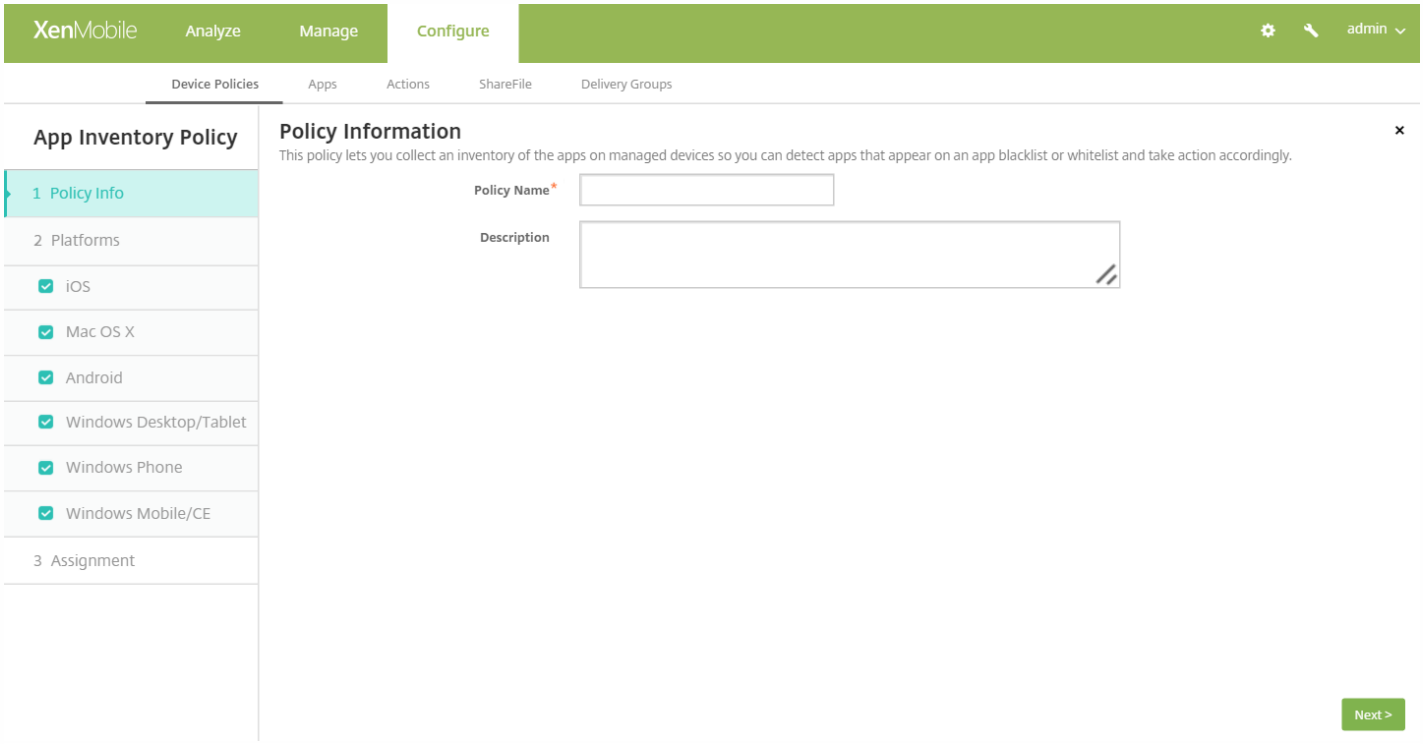
En XenMobile, una directiva de inventario de aplicaciones permite obtener un inventario de las aplicaciones presentes en los dispositivos administrados. A continuación, el inventario se compara con las directivas de acceso de aplicaciones implementadas en esos dispositivos. De esta forma, podrá detectar 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. Puede crear directivas de acceso de aplicaciones para dispositivos iOS, Mac OS X, Android (incluidos los dispositivos habilitados para Android for Work) y escritorios y tabletas Windows, Windows Phone y Windows Mobile/CE.

> ## Important
>
> Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de la instancia de WorxStore 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 **Add**. Aparecerá la página **Add a New Policy**.

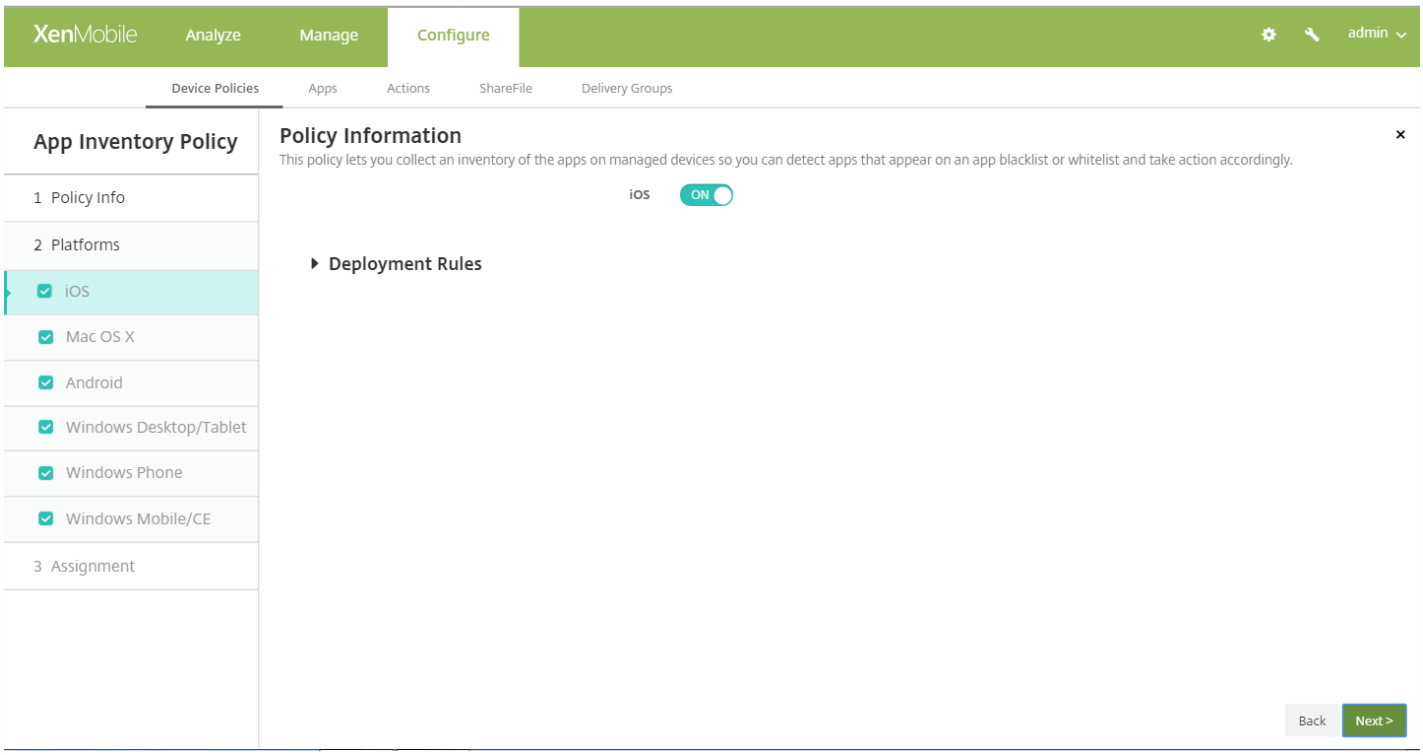
3. Expanda **More** y, en **Apps**, haga clic en **App Inventory**. Aparecerá la página **App Inventory Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



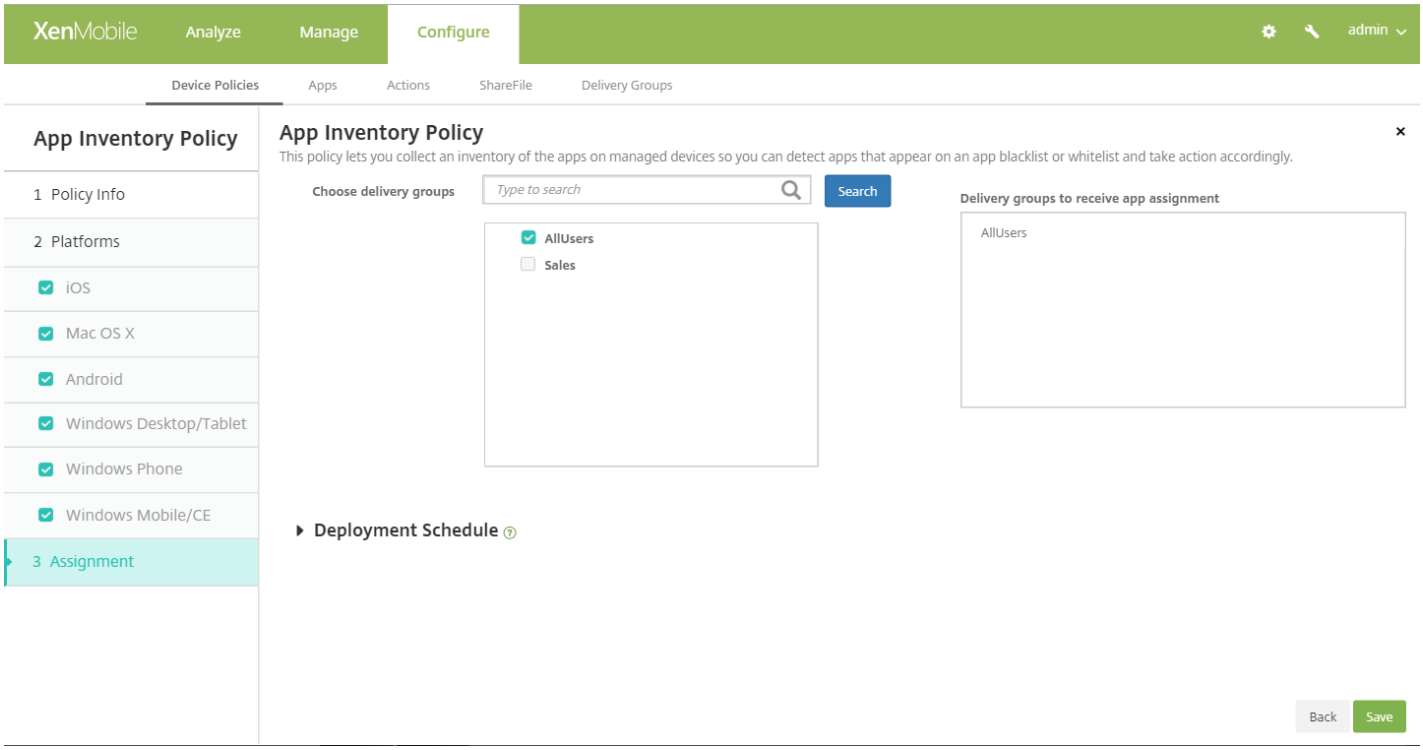
En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

6. Para cada plataforma que seleccione, deje el valor predeterminado o cambie la opción a **OFF**. El valor predeterminado es **ON**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App Inventory 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:

- 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.
- Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
- Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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.
- Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.

Nota:

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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 a iOS.

11. Haga clic en **Save**.

Directiva de bloqueo de aplicaciones

Aug 25, 2016

Puede crear una directiva en XenMobile para definir una lista de las aplicaciones que se permite ejecutar en un dispositivo, o una lista de las aplicaciones cuya ejecución debe bloquearse en un dispositivo. Puede configurar esta directiva para dispositivos Android e iOS, pero su funcionamiento difiere según la plataforma. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS.

Análogamente, en dispositivos iOS, solo se puede seleccionar una aplicación iOS por cada directiva. Esto significa ue los usuarios solo pueden usar el dispositivo para ejecutar una sola aplicación. Cuando hay una directiva de bloqueo de aplicaciones en vigor, los usuarios no pueden realizar ninguna actividad en el dispositivo, excepto las opciones que usted permita específicamente.

Además, los dispositivos iOS deben supervisarse para insertar las directivas de bloqueo de aplicaciones.

Aunque la directiva de dispositivos funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N y posteriores porque Google ha dejado de respaldar la API necesaria.

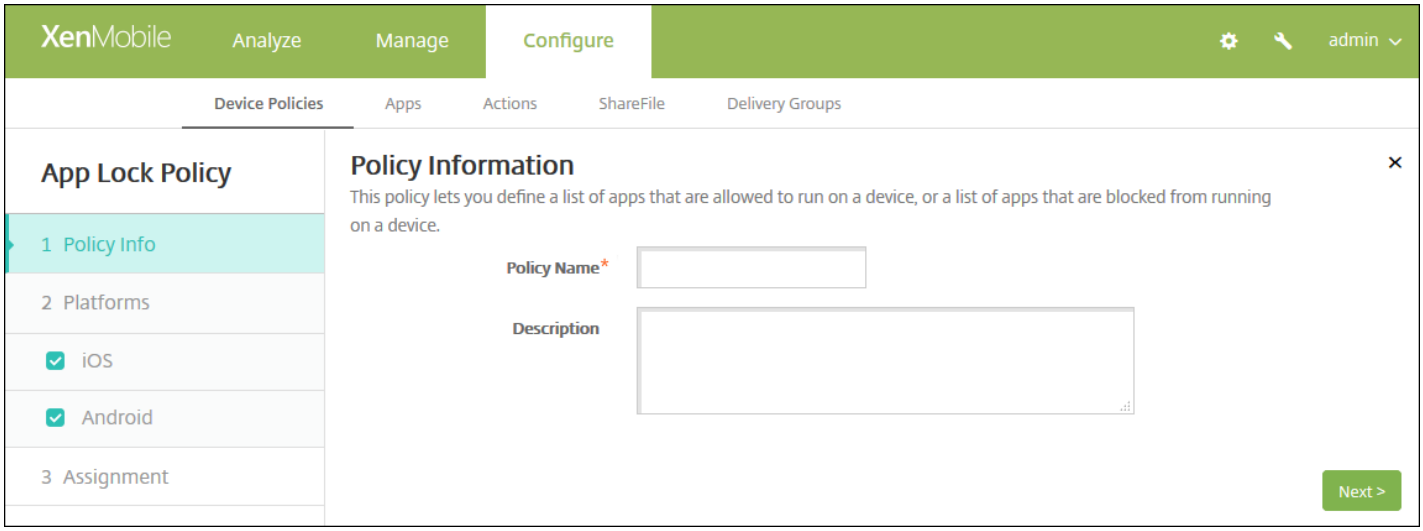
Configuración de iOS

Configuración de Android

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **More** y, a continuación, en **Security**, haga clic en **App Lock**. Aparecerá la página **App Lock Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

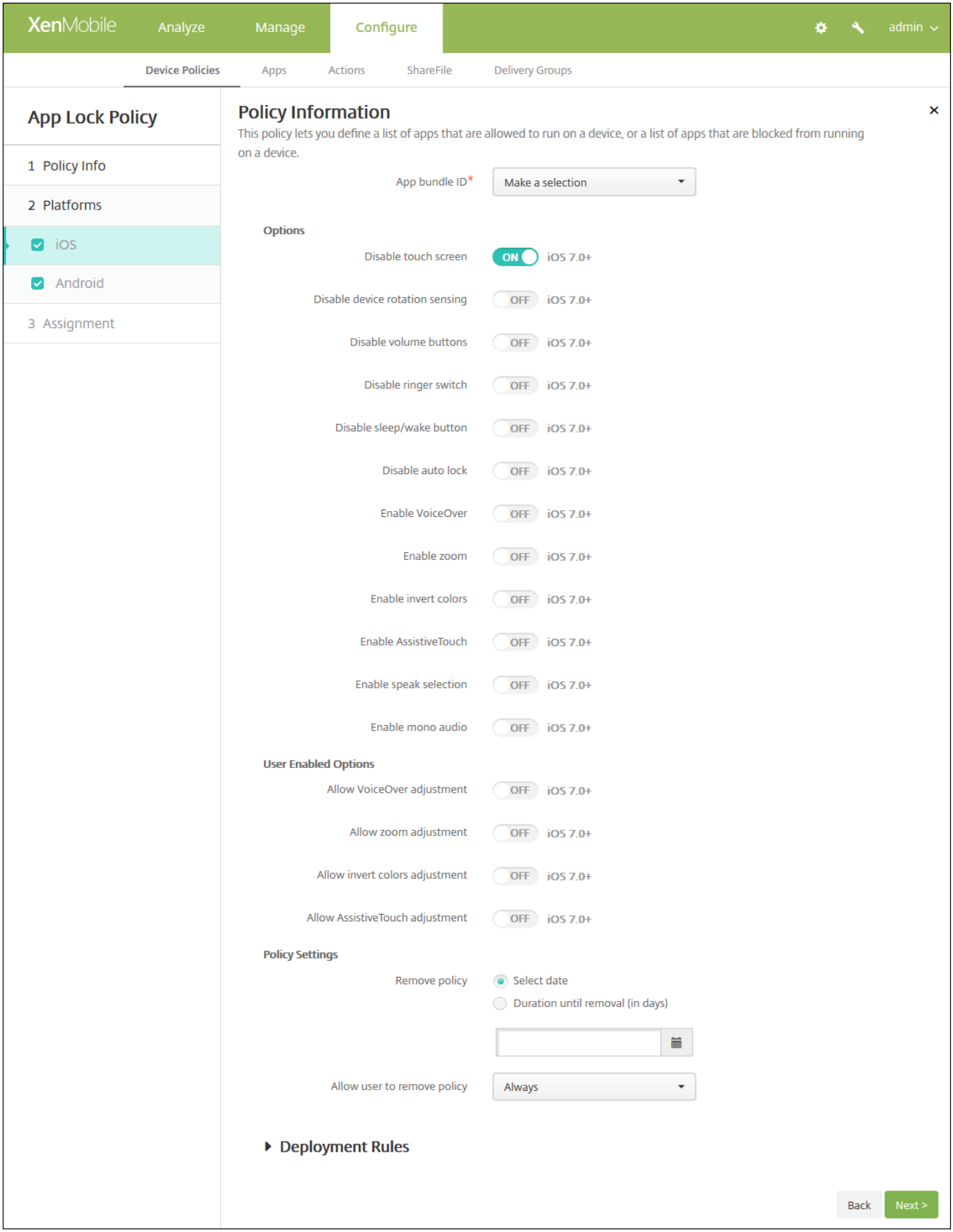
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

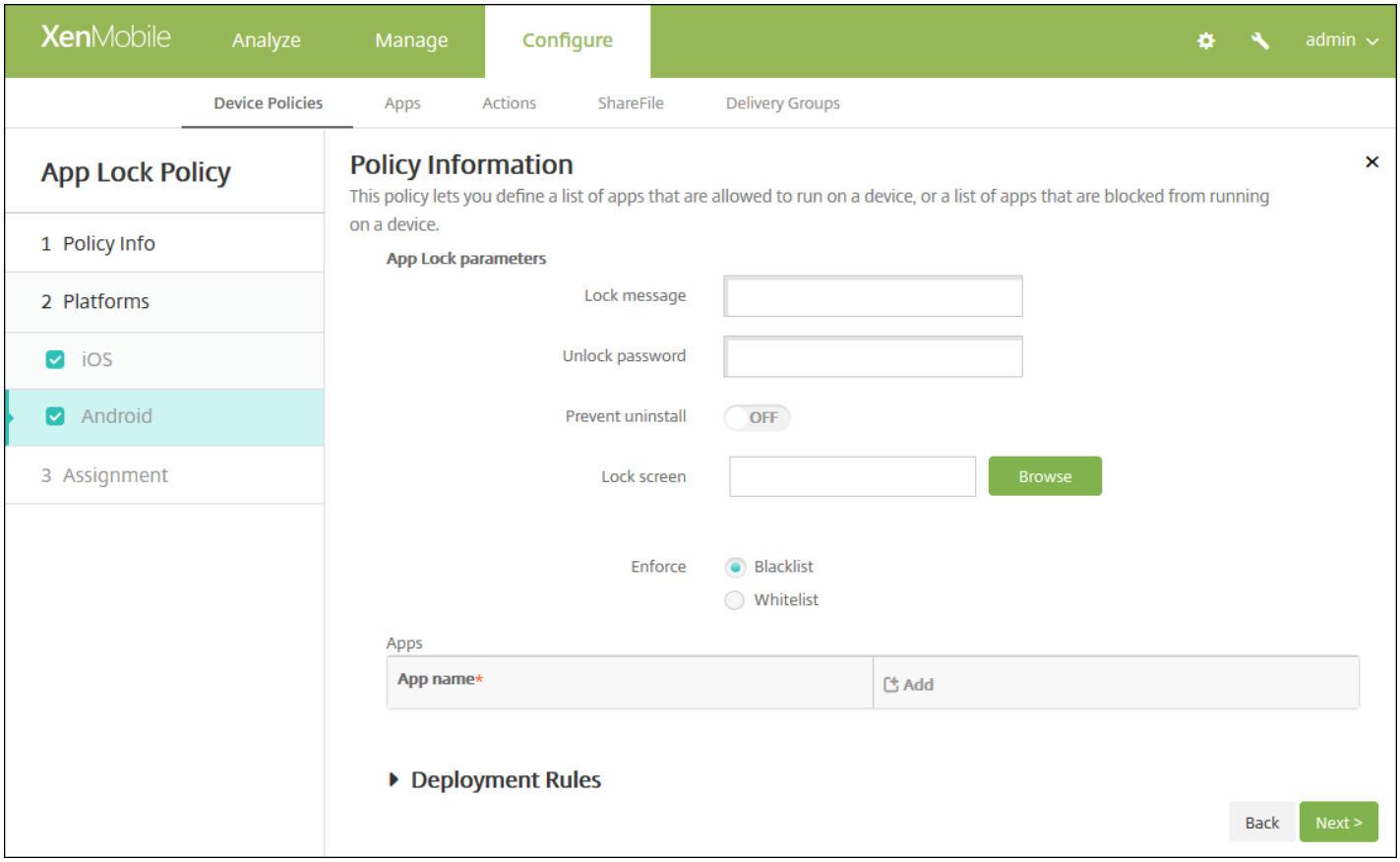
Configuración de los parámetros de iOS



Configure estos parámetros:

- **App bundle ID**. En la lista, haga clic en la aplicación a la que se aplica esta directiva, o bien haga clic en **Add new** para agregar una nueva aplicación a la lista. Si selecciona **Add new**, escriba el nombre de la aplicación en el campo que aparece.
- **Options**. Todas las siguientes opciones solo se aplican a iOS 7.0 o versiones posteriores. El valor predeterminado de todas ellas es **OFF**, excepto para Disable touch screen, cuyo valor predeterminado es **ON**.
  - Disable touch screen (Inhabilitar la pantalla táctil)
  - Disable device rotation sensing (Inhabilitar la detección de giro)
  - Disable volume buttons (Inhabilitar los botones de volumen)
  - Disable ringer switch (Inhabilitar modificador de tono) **Nota**: Si esta opción está inhabilitada, los tonos dependen de la posición que tenía el modificador cuando se inhabilitó.
  - Disable sleep/wake button (Inhabilitar el botón de suspensión o reactivación)
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom (Habilitar zoom)
  - Enable invert colors (Habilitar la inversión de colores)
  - Habilitar AssistiveTouch
  - Enable Speak Selection (Habilitar la función Speak Selection)
  - Enable mono audio (Habilitar el ajuste Audio mono)
- **Opciones habilitadas por los usuarios**. Todas las siguientes opciones solo se aplican a iOS 7.0 o versiones posteriores. El valor predeterminado de todas ellas es **OFF**.
  - Allow VoiceOver adjustment (Permitir ajuste de VoiceOver)
  - Allow zoom adjustment (Permitir ajuste de zoom)
  - Allow invert colors adjustment (Permitir ajuste de inversión de colores)
  - Allow AssistiveTouch adjustment (Permitir ajuste de AssistiveTouch)
- **Configuraciones de directivas**
  - o Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - o Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - o En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - o Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Android



Configure estos parámetros:

- **App Lock parameters**
  - **Lock message**. Escriba el mensaje que verán los usuarios cuando intenten abrir una aplicación bloqueada.
  - **Unlock password**. Escriba la contraseña para desbloquear la aplicación.
  - **Prevent uninstall**. Seleccione si permitir a los usuarios desinstalar aplicaciones. El valor predeterminado es **OFF**.
  - **Lock screen**. Seleccione la imagen que aparecerá en la pantalla de bloqueo del dispositivo. Para ello, haga clic en Browse y vaya a la ubicación del archivo.
  - **Enforce**. Haga clic en **Blacklist** para crear una lista de aplicaciones que no se pueden ejecutar en los dispositivos, o bien haga clic en **Whitelist** para crear una lista de aplicaciones que se pueden ejecutar en los dispositivos.
- **Apps**. Haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name**. En la lista, haga clic en el nombre de la aplicación que se va a agregar a la lista de aplicaciones permitidas o a la lista de aplicaciones prohibidas. También puede hacer clic en **Add new** para agregar una nueva aplicación a la lista de las aplicaciones disponibles.
  - Si selecciona **Add new**, escriba el nombre de la aplicación en el campo que aparece.
  - Haga clic en **Save** o **Cancel**.
  - Repita estos pasos para cada aplicación que quiera agregar a las listas de aplicaciones permitidas o prohibidas.

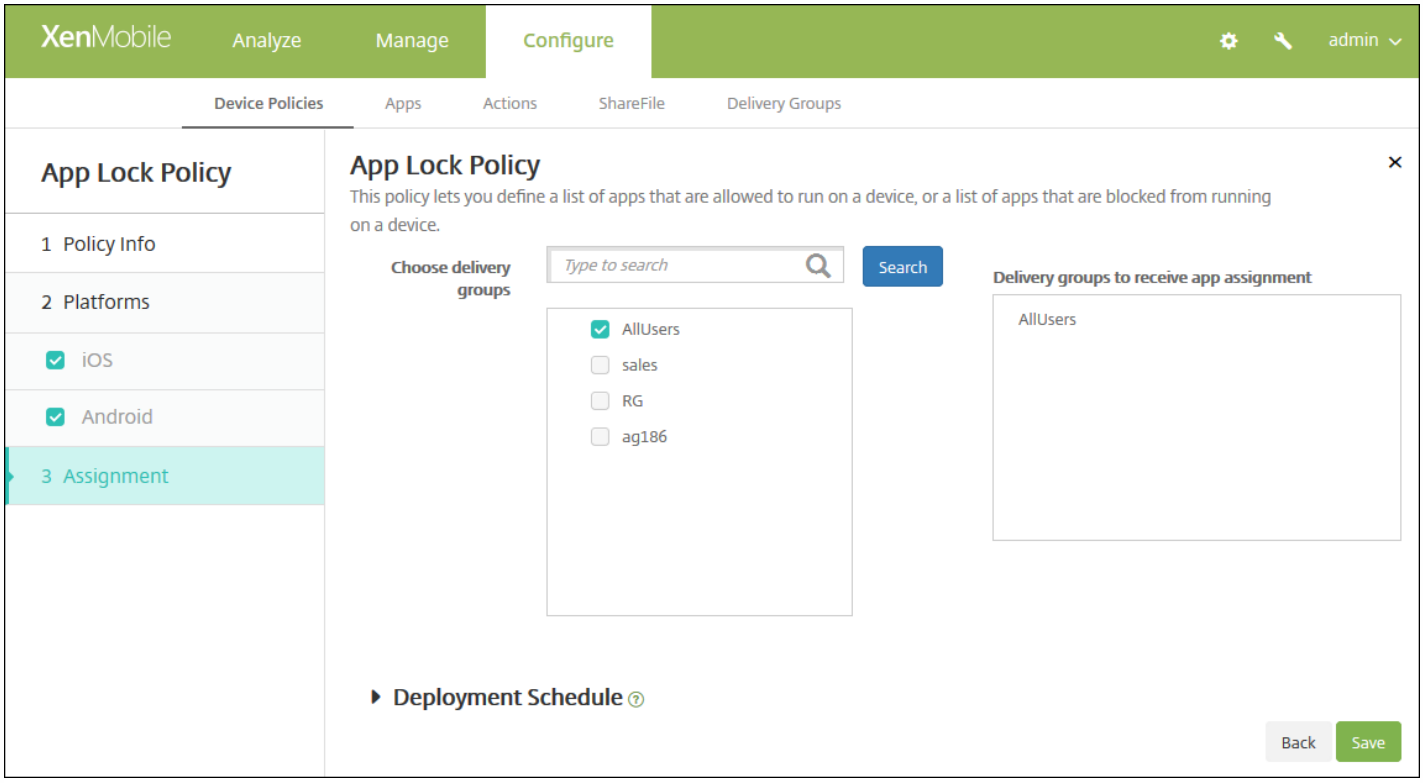
    Nota: Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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. Configure las reglas de implementación.

8. Haga clic en **Next** y aparecerá la página de asignación **App Lock 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de uso de red por parte de aplicaciones

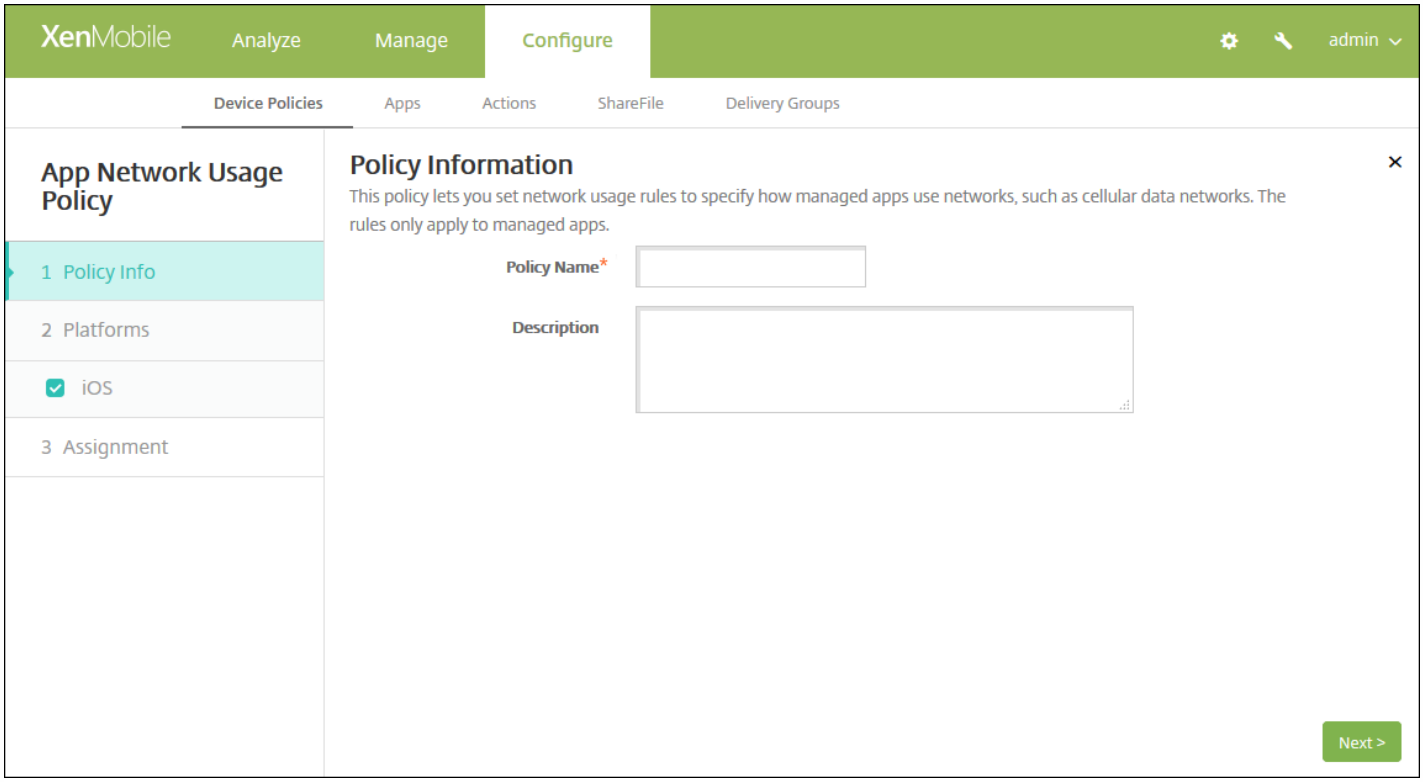
Jul 27, 2016

Puede definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas usan, por ejemplo, redes de datos móviles en dispositivos iOS. Las reglas solo se aplican a aplicaciones administradas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de XenMobile. No se incluyen en este grupo aquellas aplicaciones que los usuarios descargan directamente a sus dispositivos (sin que se implementen por medio de XenMobile) ni aquellas aplicaciones ya instaladas en los dispositivos cuando estos se inscribieron en XenMobile.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

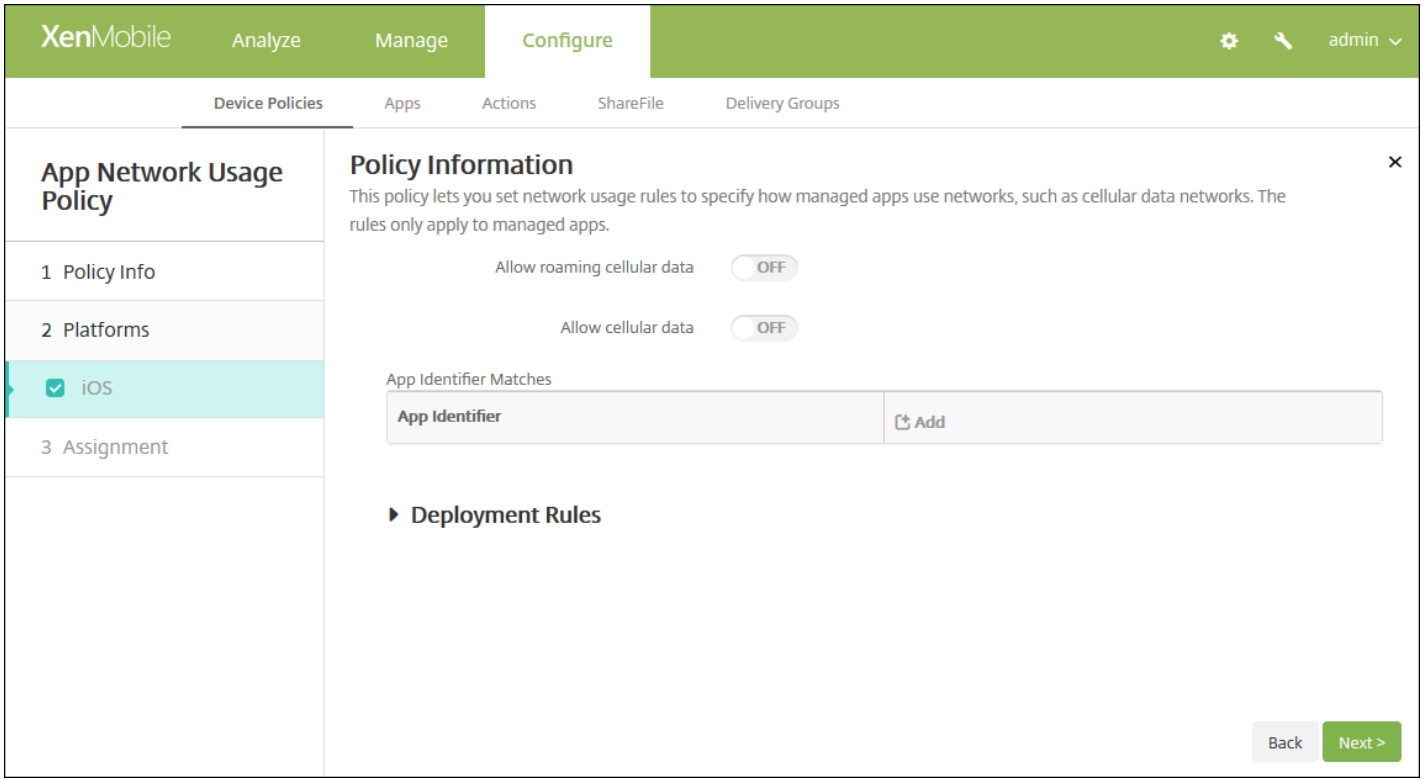
3. Expanda **More** y luego, en **Apps**, haga clic en **App Network Usage**. Aparecerá la página de información **App Network Usage Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. Configure estas opciones.

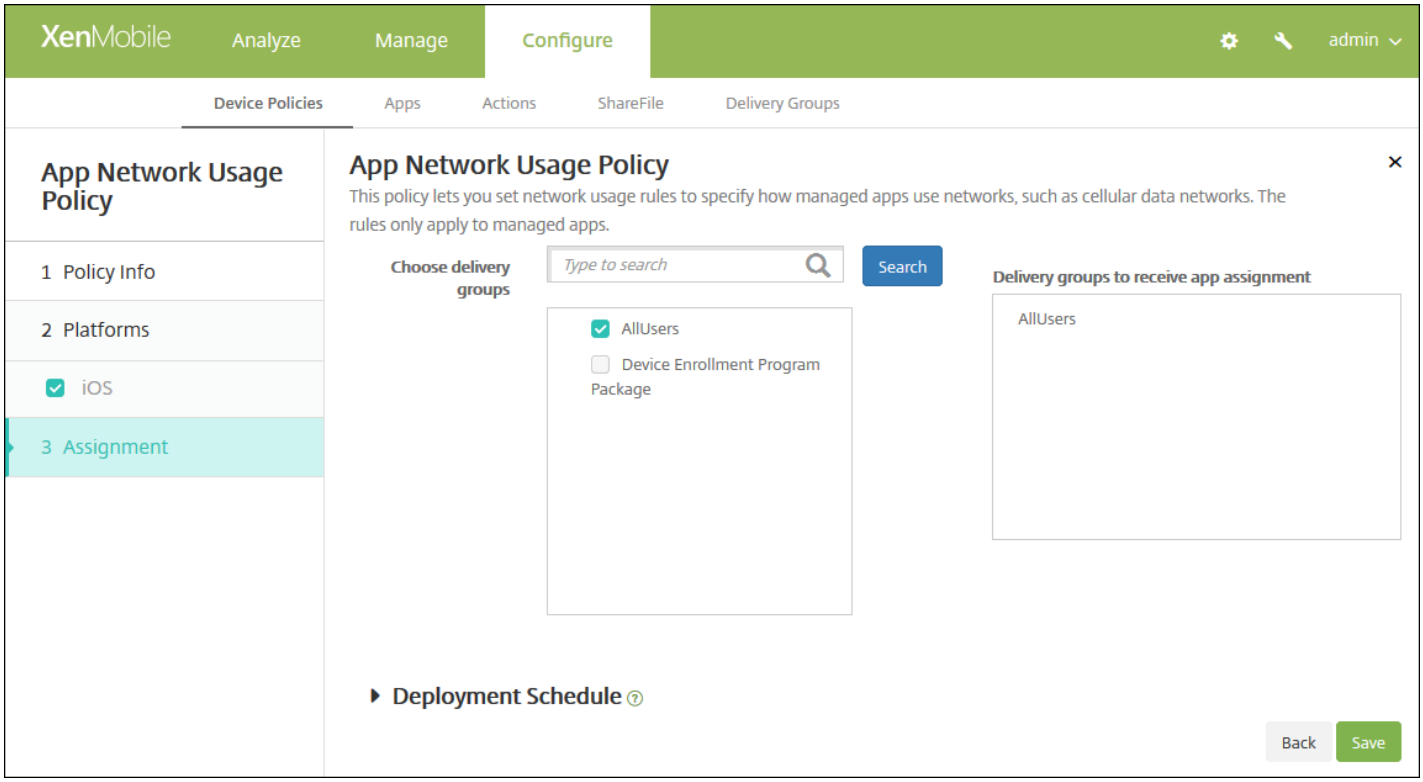
- **Allow roaming cellular data**. Seleccione si las aplicaciones indicadas pueden usar una conexión de datos móviles durante el roaming. El valor predeterminado es **OFF**.
- **Allow cellular data**. Seleccione si las aplicaciones especificadas pueden usar la conexión de datos móviles. El valor predeterminado es **OFF**.
- **App Identifier Matches**. Para cada aplicación que quiera agregar a la lista, haga clic en **Add** y haga lo siguiente:
  - **App Identifier**. Escriba un identificador de la aplicación.
  - Haga clic en **Save** para guardar la aplicación en la lista, o bien haga clic en **Cancel** para no guardarla.

    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 a la derecha. 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. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App Network Usage 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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.

Directiva de restricciones de aplicaciones

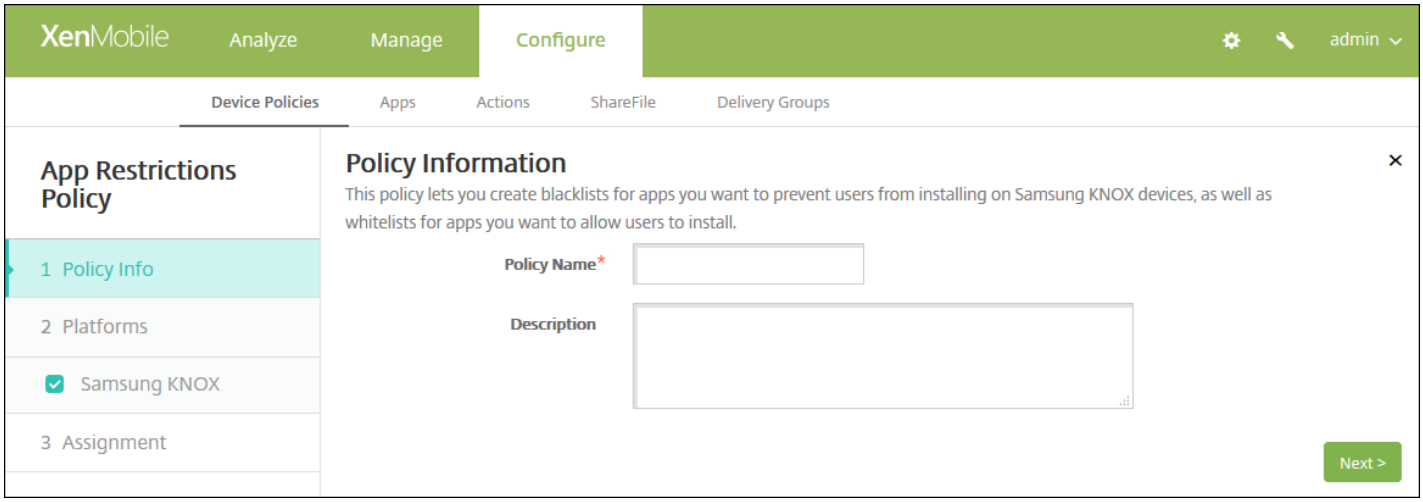
Jul 27, 2016

Puede crear una lista negra de las aplicaciones que quiera impedir que los usuarios instalen en sus dispositivos Samsung KNOX. También puede crear listas blancas de las aplicaciones que quiere permitir que los usuarios instalen.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

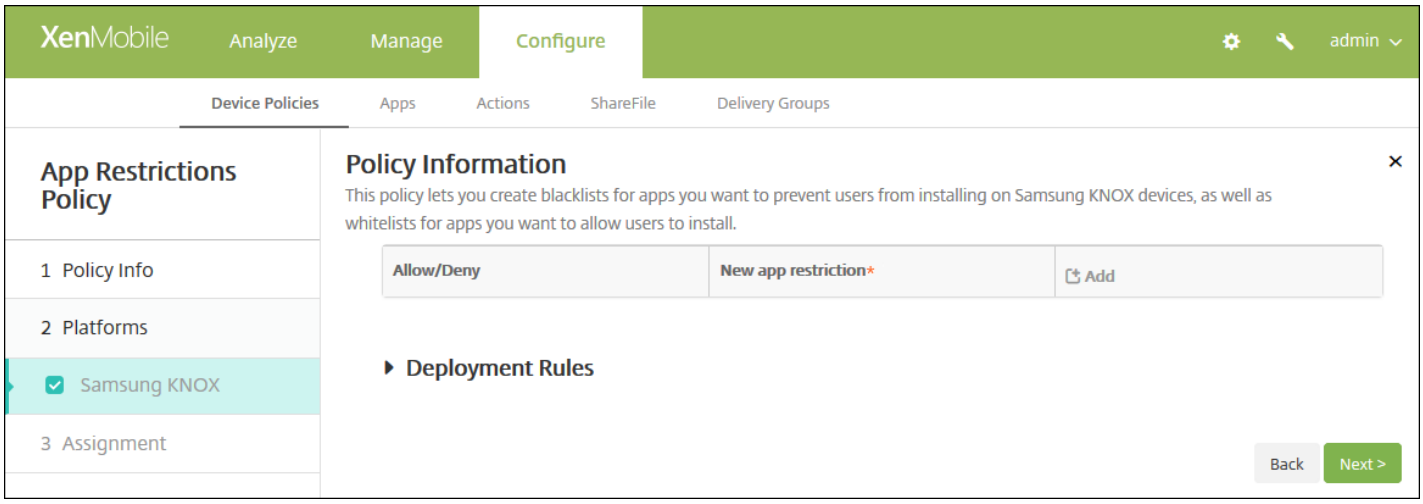
3. Expanda **More** y, a continuación, en **Security**, haga clic en **App Restrictions**. Aparecerá la página de información **App Restrictions Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Samsung KNOX**.



6. Para cada aplicación que quiera agregar a la lista Allow/Deny, haga clic en **Add** y lleve a cabo lo siguiente:

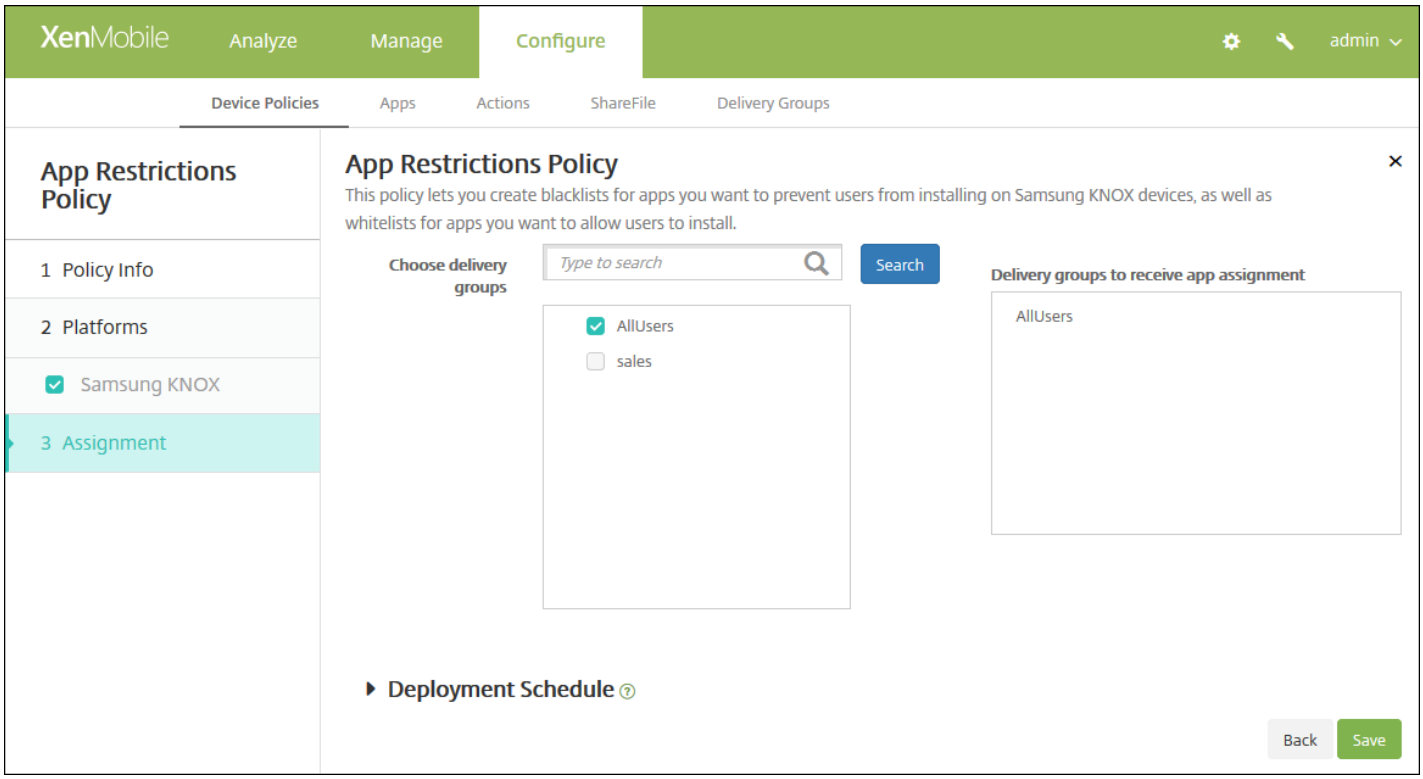
- **Allow/Deny**. Seleccione si permitir a los usuarios instalar la aplicación.
- **New app restriction**. Escriba el ID del paquete de la aplicación; por ejemplo, com.kmdm.af.crackle.
- Haga clic en **Save** para guardar la aplicación en la lista Allow/Deny, o bien haga clic en **Cancel** para no guardarla.

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 a la derecha. 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. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App Restrictions 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

- 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**.
- 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.
- 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 tunelización de aplicaciones

Jul 27, 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. Puede configurar la directiva de tunelización de aplicaciones para dispositivos Android y Windows Mobile/CE.

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.

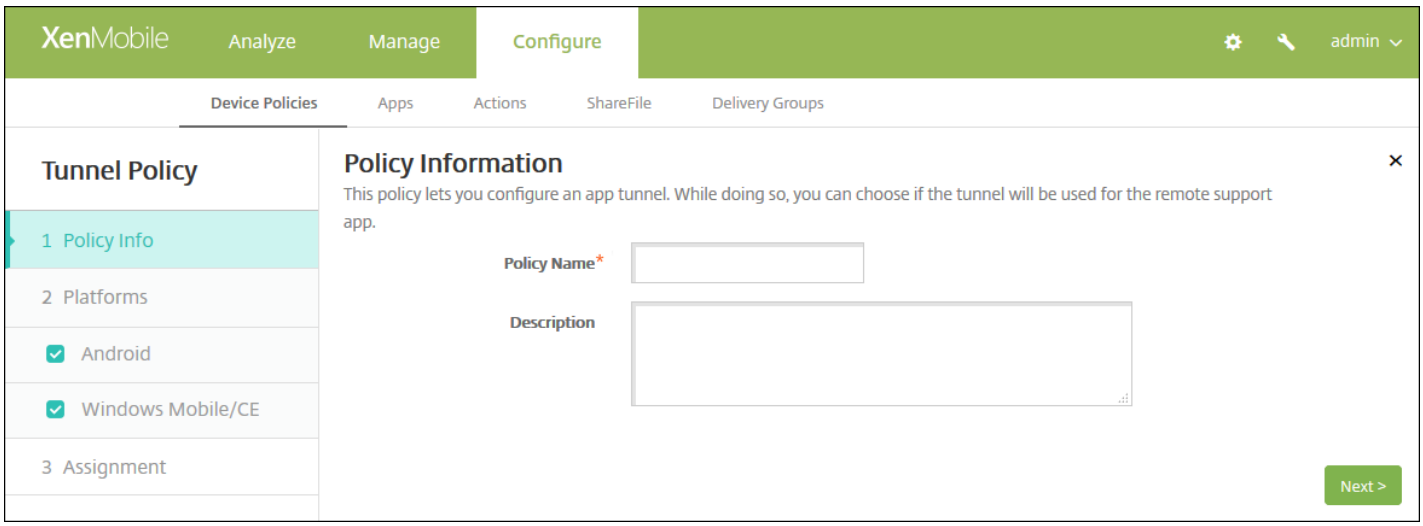
Configuración de Android

Configuración de Windows Mobile/CE

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. 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:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

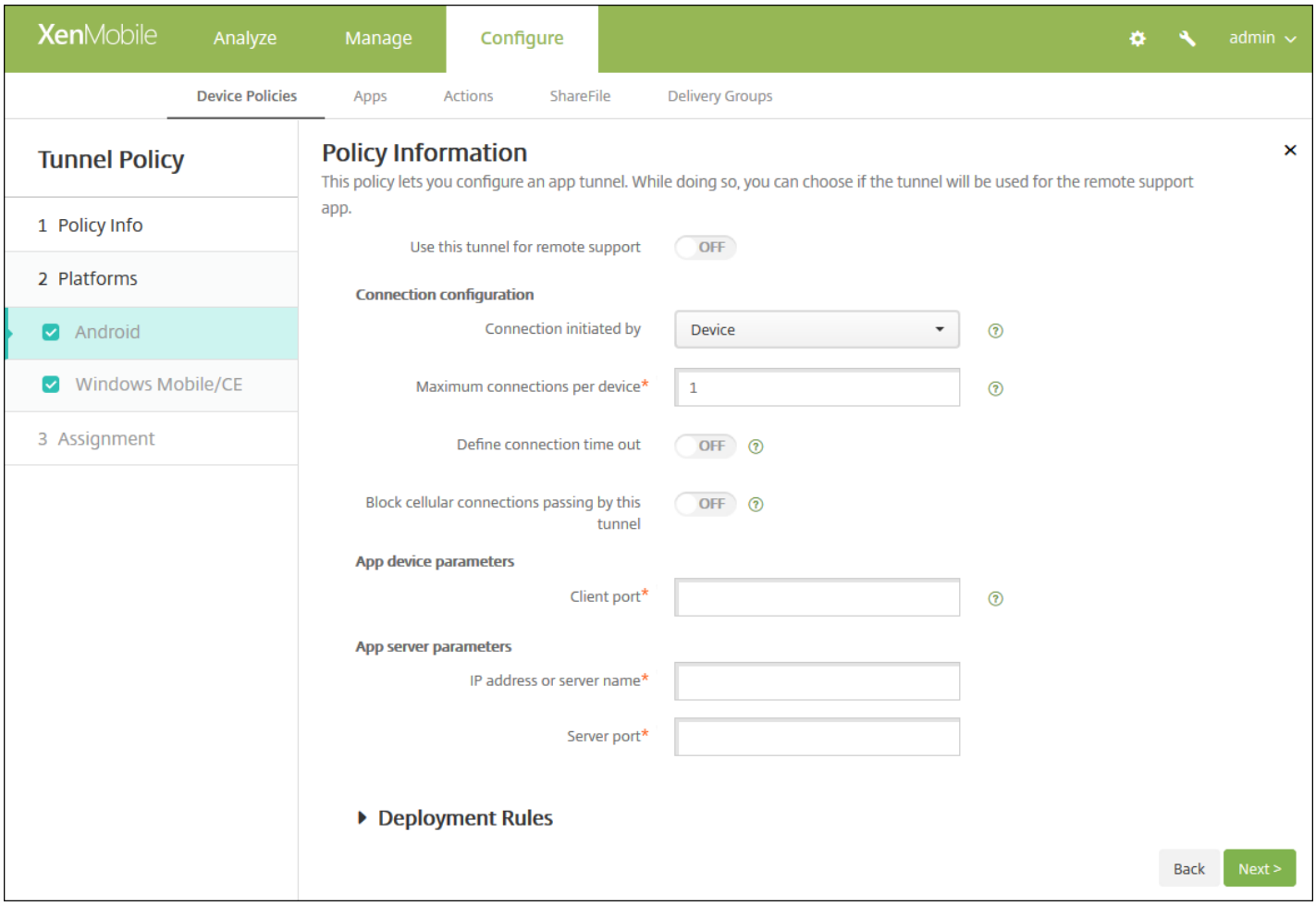
5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la

configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de Android



Configure estos parámetros:

- **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:
  - **Connection initiated by**. Haga clic en **Device** o **Server** para indicar el origen de la conexión.
  - **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.
  - **Define connection time out**. Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **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.
  - **Block cellular connections passing by this tunnel**. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.
    Nota: Las conexiones WiFi y USB no se bloquearán.

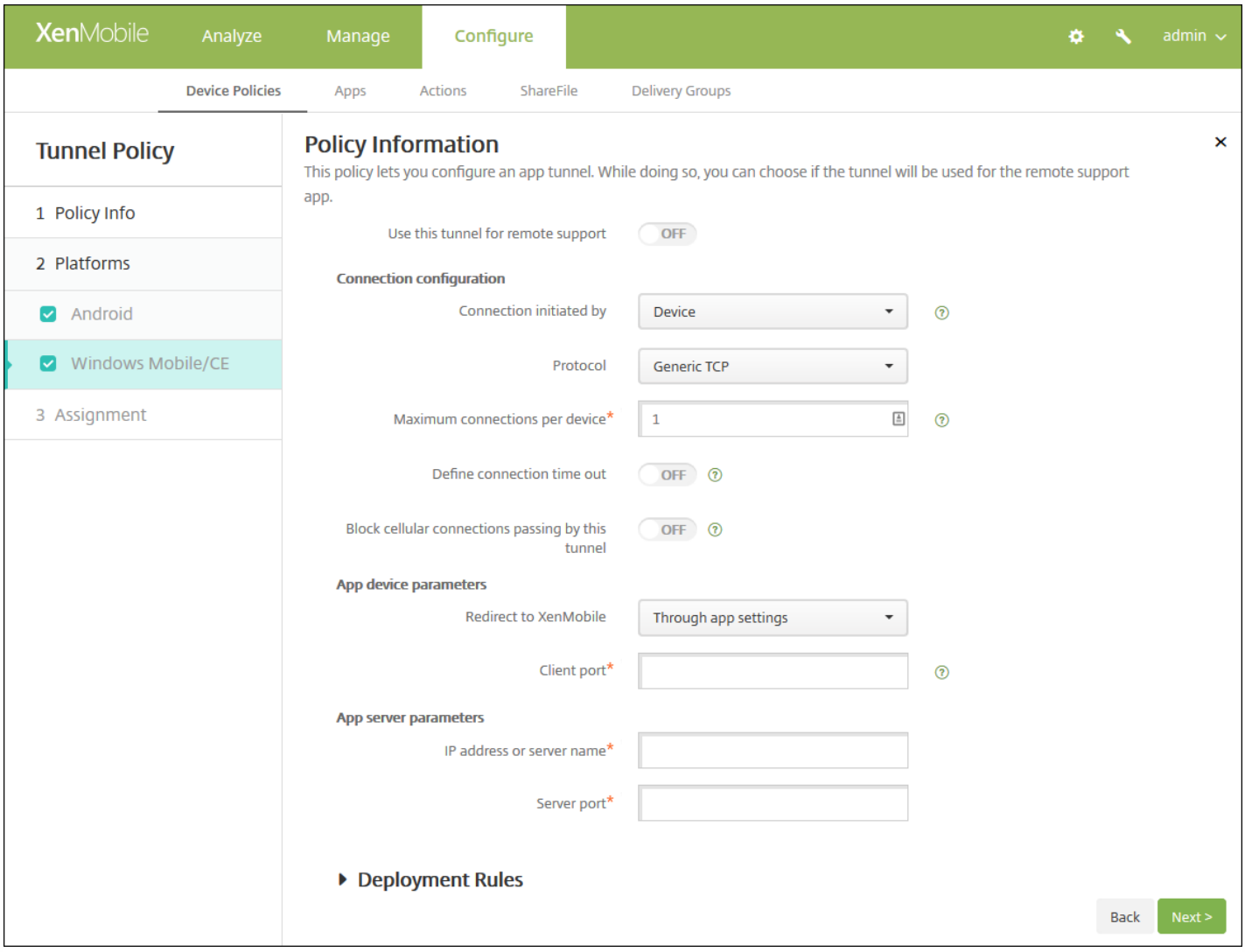
- **Client port**. Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del

puerto del servidor.

- **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.
- **Server port**. Escriba el número de puerto del servidor.

- Si selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Use this tunnel for remote support**. Establecido en **On**.
  - **Define connection time out**. Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Connection time out**. Si activa **Define connection time out**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Use SSL connection**. Seleccione si usar una conexión SSL segura para este túnel.
  - **Block cellular connections passing by this tunnel**. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.
    Nota: Las conexiones WiFi y USB no se bloquearán.

Configuración de los parámetros de Windows Mobile/CE



Configure estos parámetros:

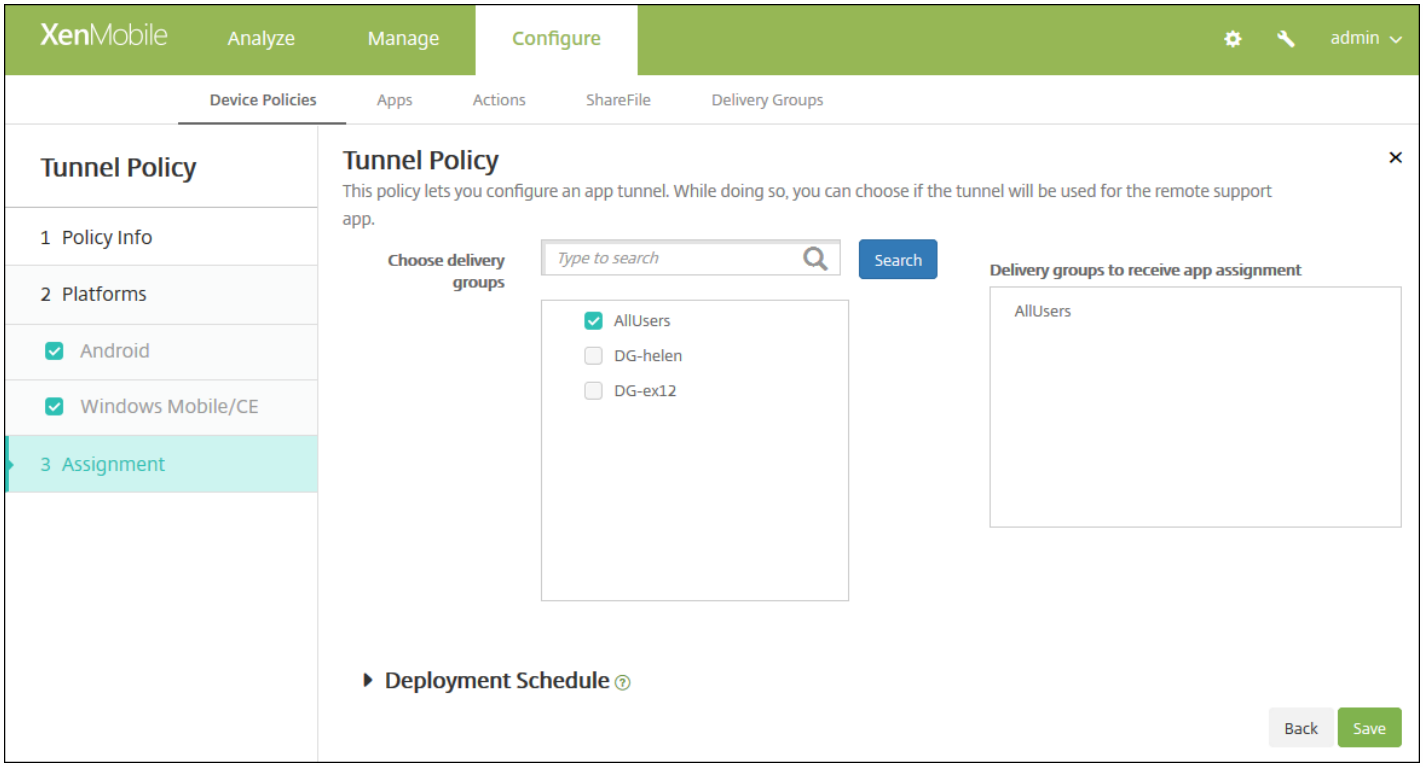
- **Use this tunnel for remote support**. Seleccione si el túnel se usará para la asistencia remota.

  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:
  - C**onnection initiated by**: Haga clic en **Device** o **Server** para especificar el origen de la conexión.
  - **Protocol**. En la lista, haga clic en el protocolo que se va a utilizar. El valor predeterminado es **Generic TCP**.
  - **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.
  - **Define connection time out**. Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **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.
  - **Block cellular connections passing by this tunnel**. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.
    Nota: Las conexiones WiFi y USB no se bloquearán.
  - **Redirect to XenMobile**. En la lista, haga clic en la forma en que se conecta el dispositivo a XenMobile. El valor predeterminado es **Through app settings**.
    - Si selecciona **Using a local alias**, escriba el alias en **Local alias**. El valor predeterminado es **localhost**.
    - Si selecciona **An IP address range**, escriba la dirección IP inicial del intervalo en **IP address range from** y la dirección IP final del intervalo en **IP address** range to.
  - **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.
  - **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.
  - **Server port**. Escriba el número de puerto del servidor.
- Si selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Use this tunnel for remote support**. Establecido en **On**.
  - **Define connection time out**. Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Connection time out**. Si establece la opción 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.
  - **Use SSL connection**. Seleccione si usar una conexión SSL segura para este túnel.
  - **Block cellular connections passing by this tunnel**. Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.
    Nota: Las conexiones WiFi y USB no se bloquearán.

7. Configure las reglas de implementación.

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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 dispositivo para desinstalación de aplicaciones

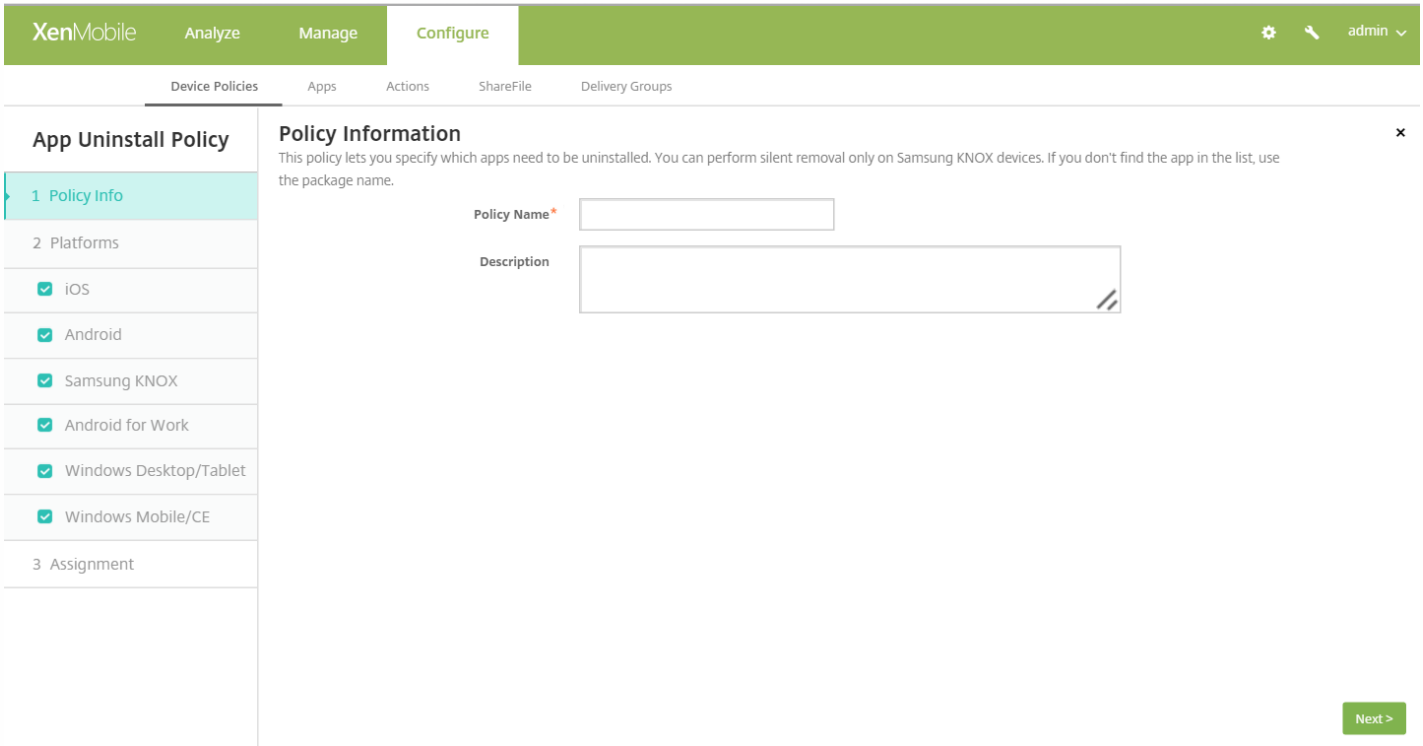
Jul 27, 2016

Puede crear una directiva de desinstalación de aplicaciones para las plataformas iOS, Android, Samsung KNOX, Android for Work, escritorios y tabletas Windows y Windows Mobile/CE. 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**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **More** y luego, en **Apps**, haga clic en **App Uninstall**. Aparecerá la página **App Uninstall Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

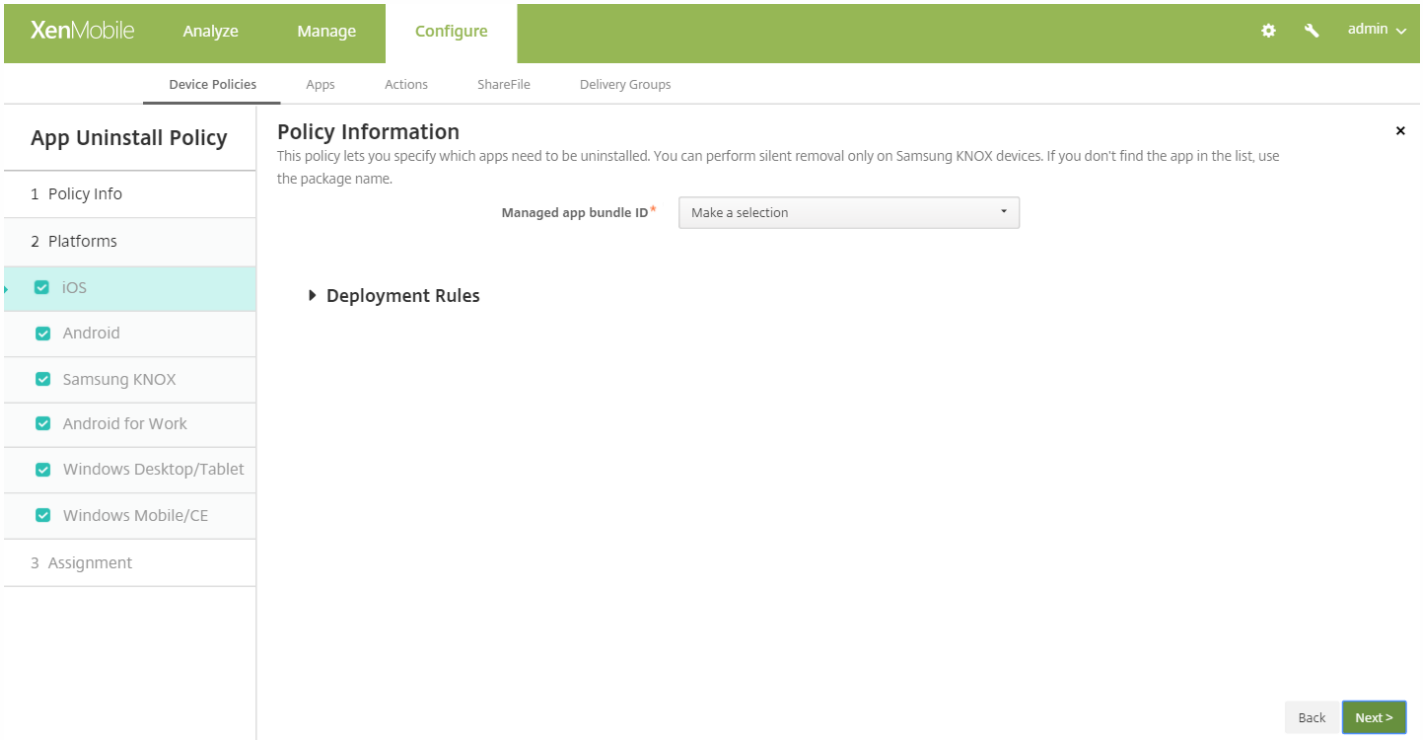
5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las

demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

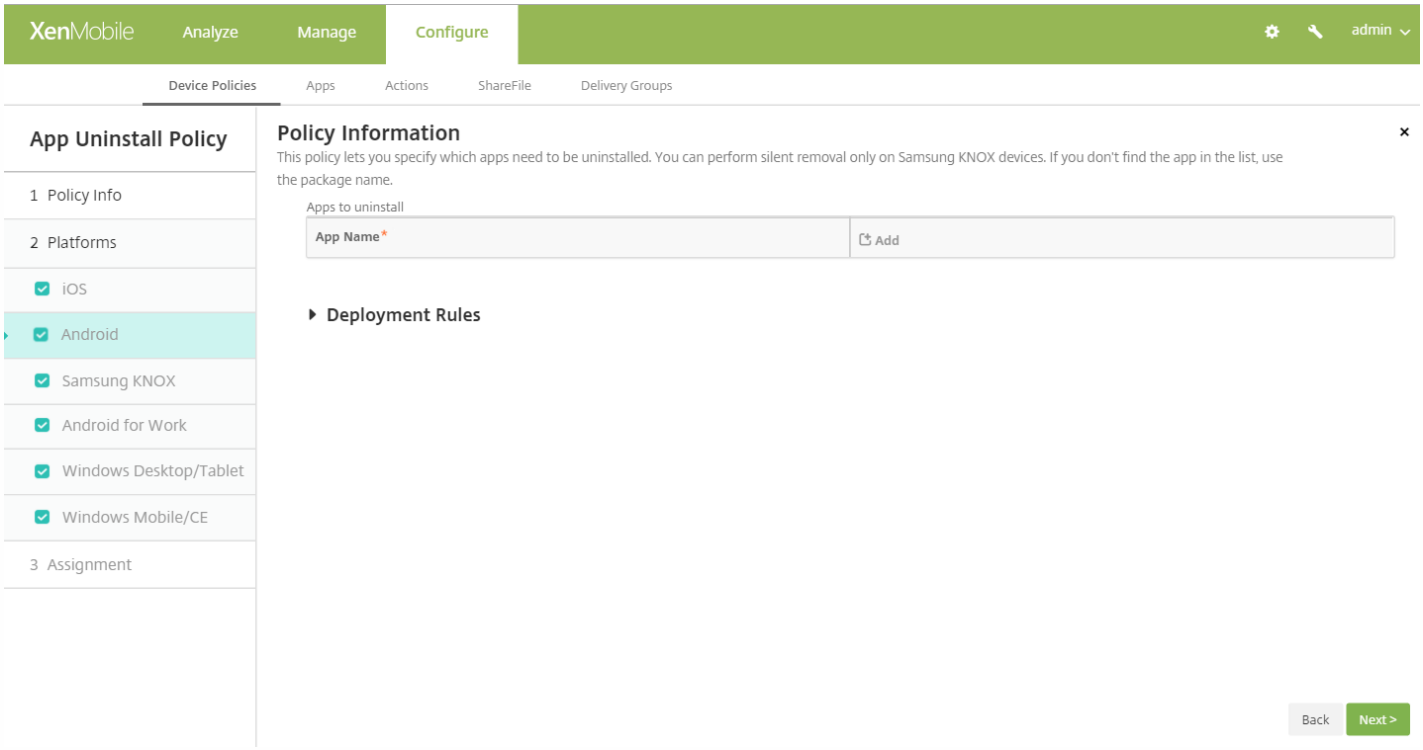
Configuración de los parámetros de iOS



Configure este parámetro:

- **Managed app bundle ID**, En la lista, haga clic en una aplicación existente, o bien haga clic en **Add new**. 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.

Configuración de los parámetros de todas las demás plataformas



Configure este parámetro:

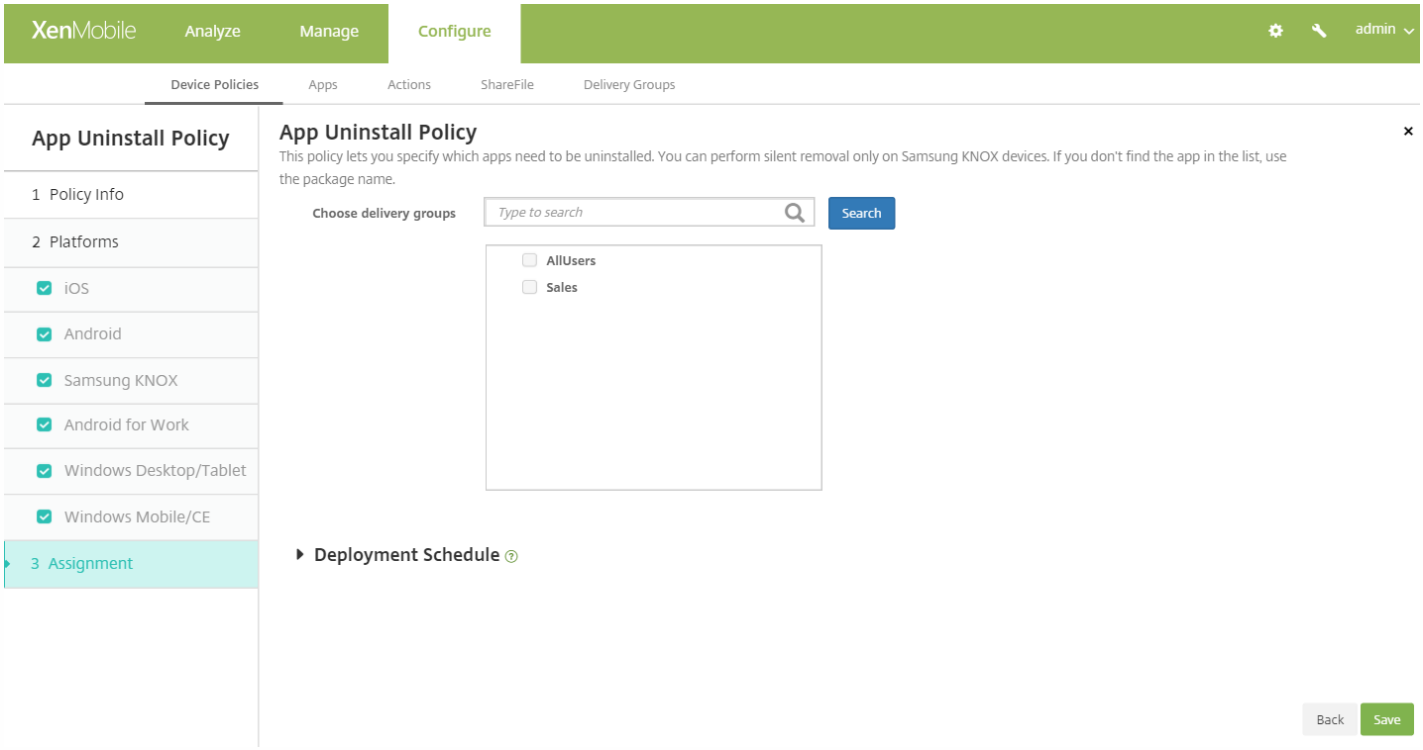
- **Apps to uninstall**. Para cada aplicación que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name**. En la lista, haga clic en una aplicación existente, o bien haga clic en **Add new** para introducir un nuevo nombre de aplicación. Si no hay ninguna aplicación configurada para esta plataforma, la lista estará vacía y deberá agregar aplicaciones nuevas.
  - Haga clic en **Add** para agregar la aplicación, o bien haga clic en **Cancel** para no agregarla.

    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.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 restricciones para desinstalación de aplicaciones

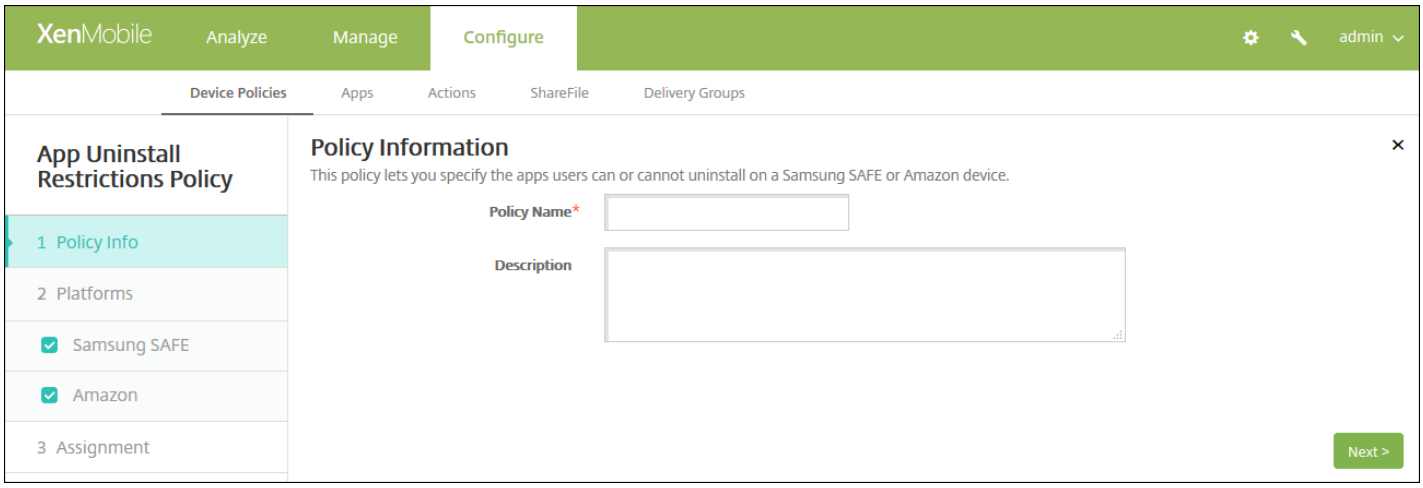
Jul 27, 2016

Puede especificar las aplicaciones que los usuarios pueden o no pueden instalarse en un dispositivo Amazon o Samsung SAFE.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

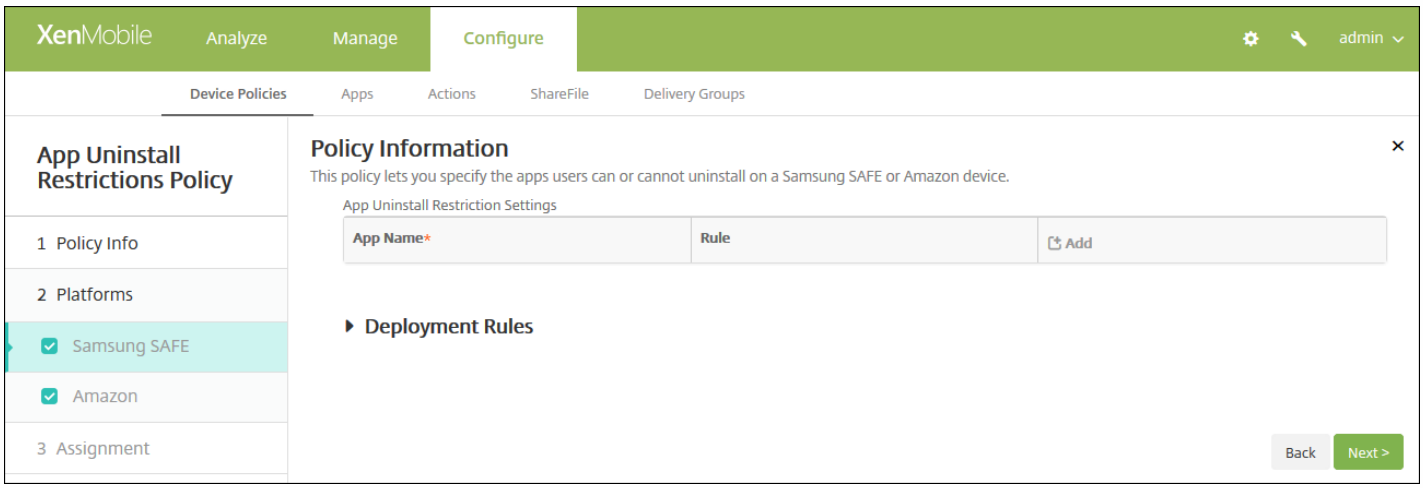
3. Expanda **More** y luego, en **Apps**, haga clic en **App Uninstall Restrictions**. Aparecerá la página de información **App Uninstall Restrictions Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas:

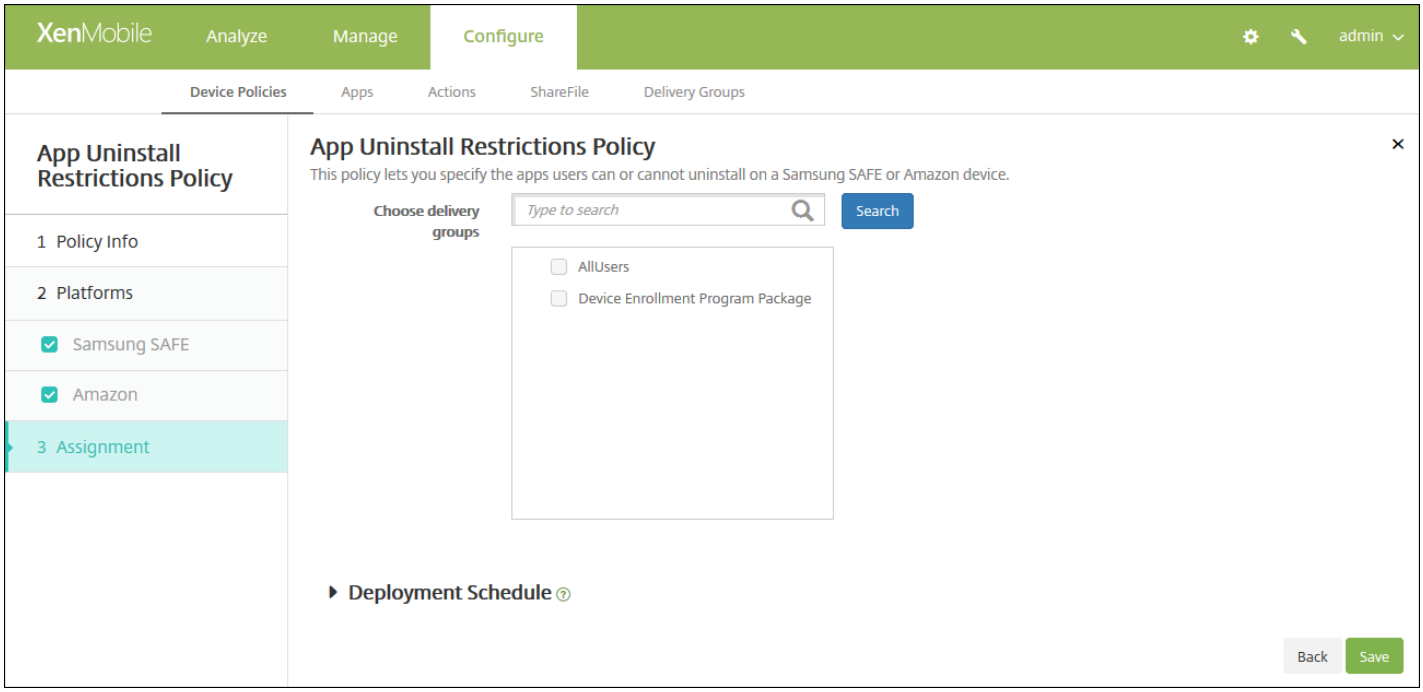
- **App Uninstall Restrictions Settings**. Para cada regla que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name**. En la lista, haga clic en una aplicación, o bien haga clic en **Add new** para introducir una nueva.
  - **Rule**. Seleccione si los usuarios pueden desinstalar la aplicación. De forma predeterminada, se permite la desinstalación.
  - Haga clic en **Save** o **Cancel**.

    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 a la derecha. 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.

8. Configure las reglas de implementación.

9. Haga clic en **Next**. Aparecerá la página de asignación **App Uninstall Restrictions 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 exploradores

Jul 27, 2016

Puede crear directivas de exploradores Web para dispositivos Samsung SAFE, Samsung KNOX y Android for Work, con el objetivo de definir si se puede usar el explorador Web en los dispositivos de los usuarios, o para limitar las funciones del explorador que pueden usarse en los dispositivos de los usuarios. En dispositivos Samsung, puede inhabilitar completamente el explorador, puede habilitar o inhabilitar los elementos emergentes, JavaScript, las cookies, la función de completado automático, y también puede decidir si forzar advertencias de fraude. En dispositivos Android for Work, puede incluir direcciones URL específicas en listas de URL permitidas o prohibidas; también puede agregar marcadores de explorador concretos y seguros.

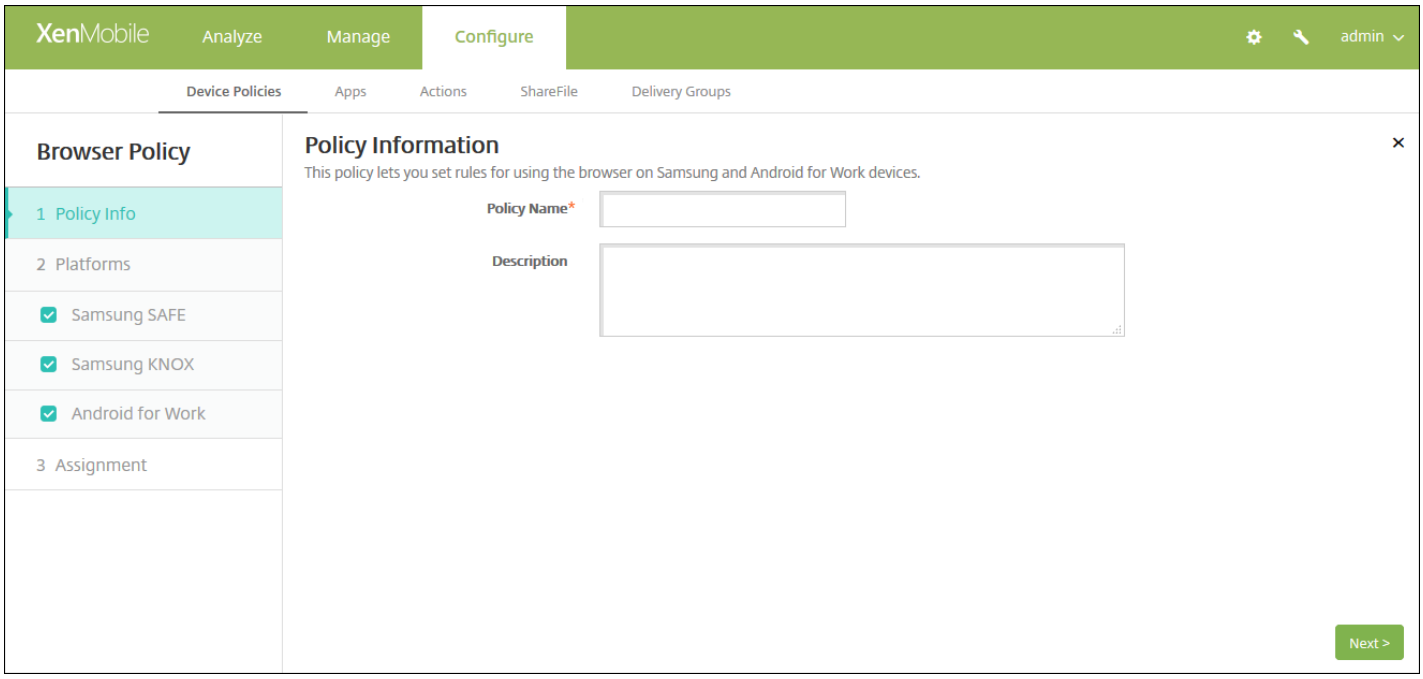
Configuración de Samsung SAFE y Samsung KNOX

Configuración de Android for Work

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 **Apps**, haga clic en **Browser**. Aparecerá la página de información **Browser Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

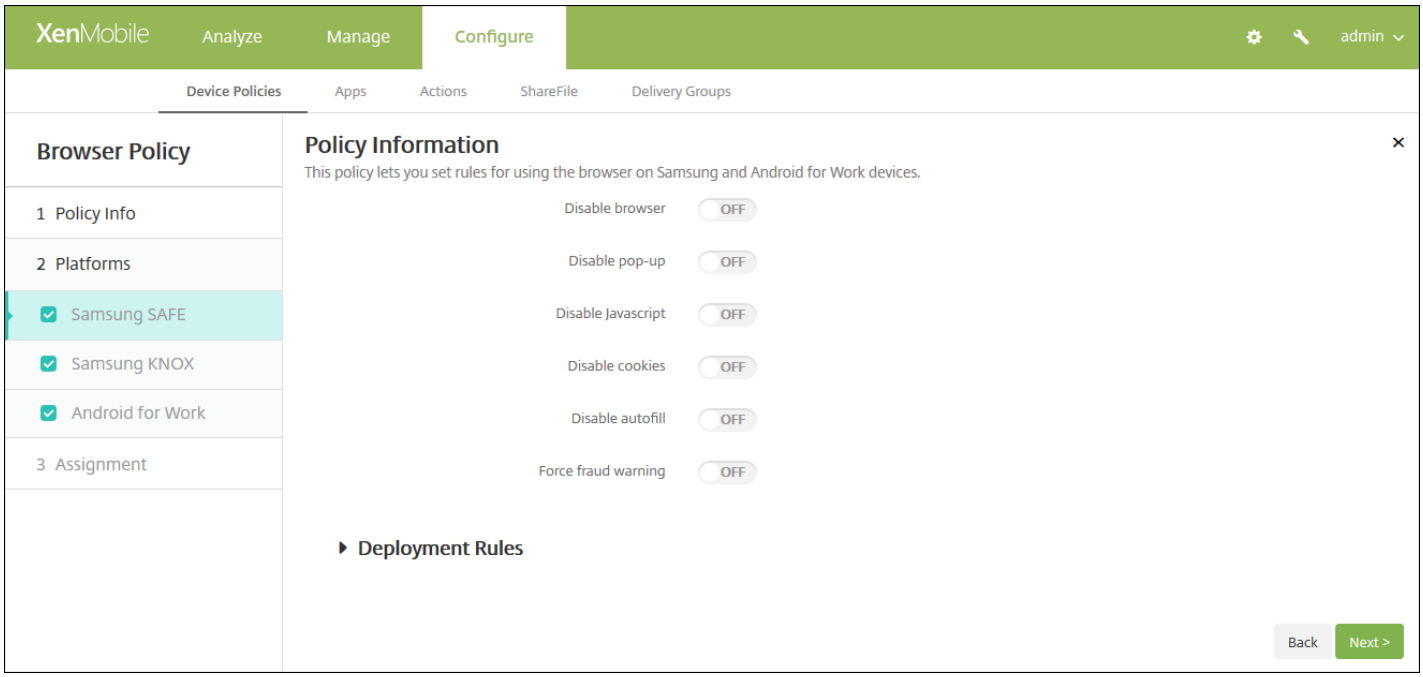
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

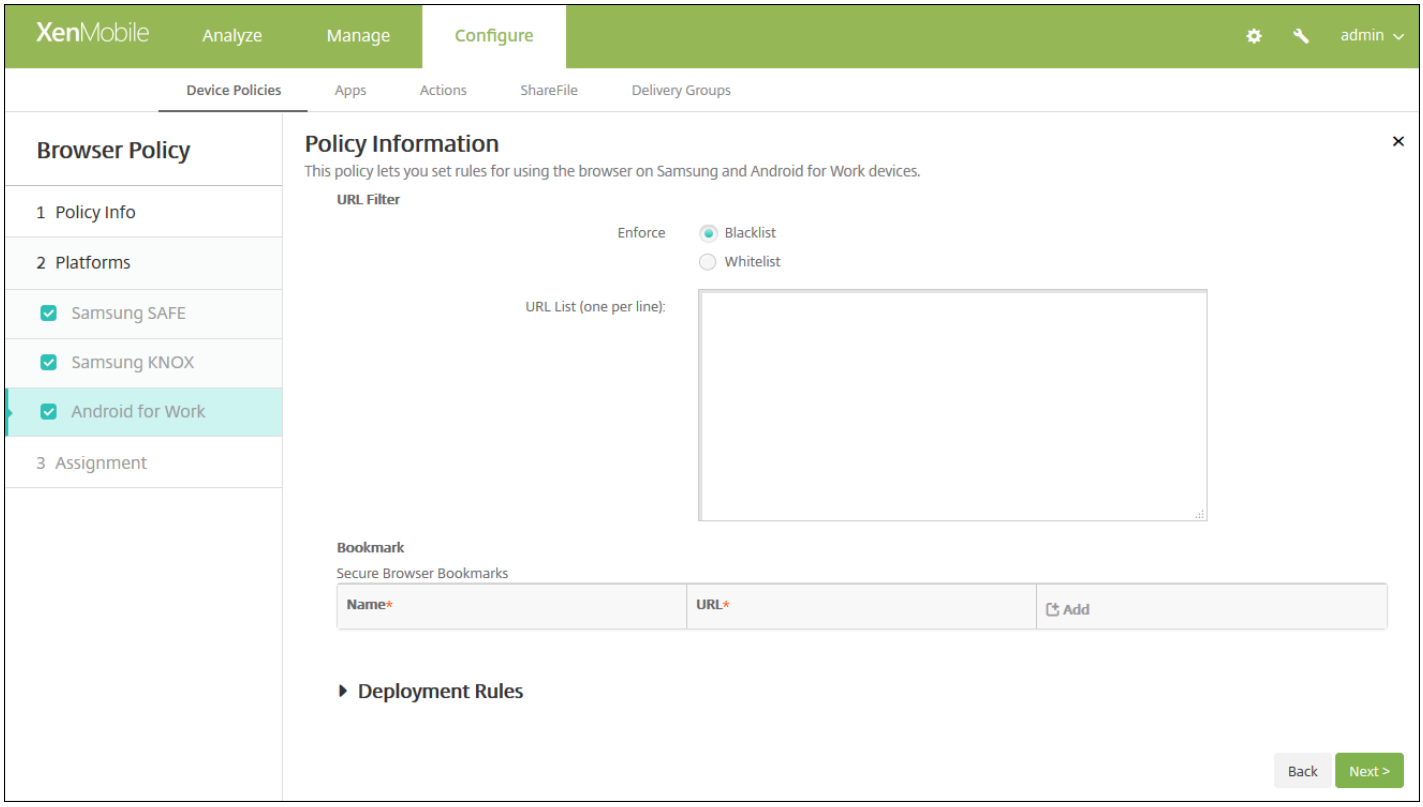
Configuración de los parámetros de Samsung SAFE y Samsung KNOX



Configure estos parámetros:

- **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.
- **Disable pop-up**. Seleccione si permitir o no los mensajes emergentes en el explorador.
- **Disable Javascript**. Seleccione si permitir o no que se ejecute JavaScript en el explorador.
- **Disable cookies**. Seleccione si permitir o no las cookies.
- **Disable autofill**. Seleccionar si permitir a los usuarios activar la función de completado automático del explorador.
- **Force fraud warning**. Seleccione si mostrar una advertencia cuando los usuarios visiten un sitio Web fraudulento o no seguro.

Configuración de los parámetros de Android for Work

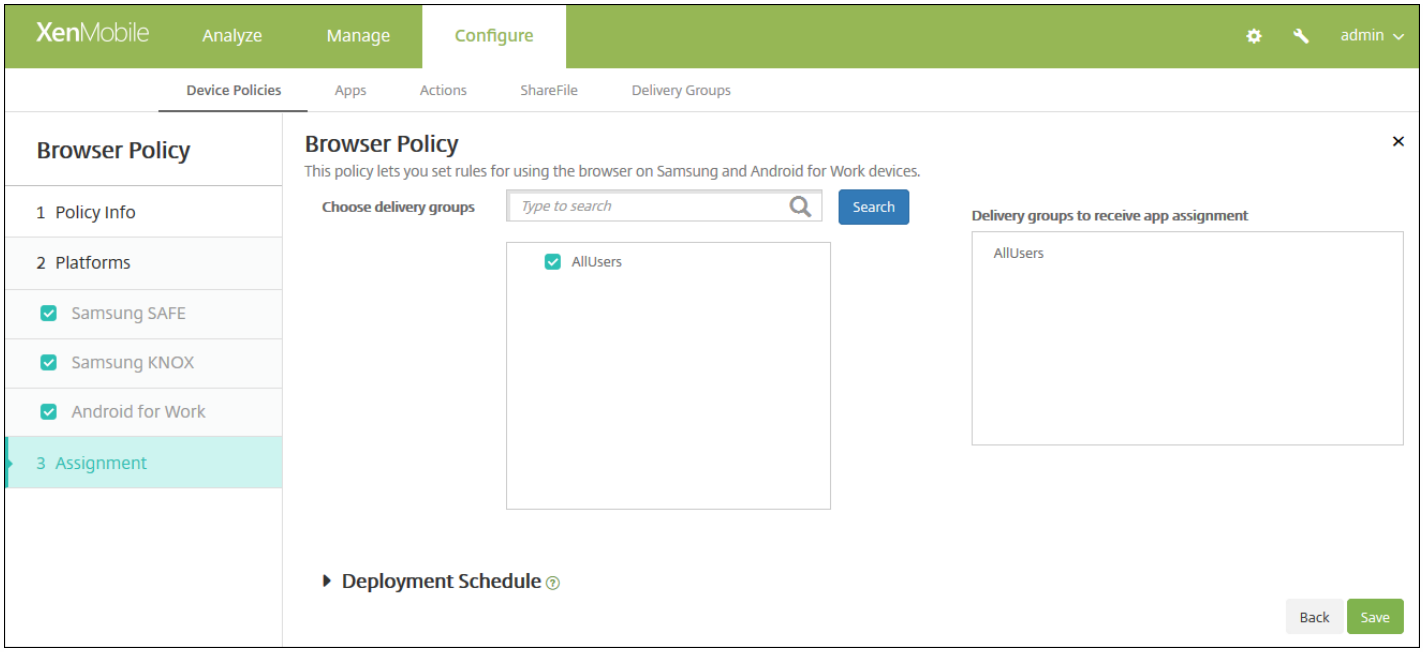


Configure estos parámetros:

- En **URL Filter**, configure los siguientes parámetros:
  - **Enforce**. Seleccione **Blacklist** o **Whitelist**. Si selecciona **Blacklist**, los usuarios podrán acceder a todas las direcciones URL *excepto* a aquellas que especifique aquí. Si selecciona **Whitelist**, los usuarios *solo* podrán acceder a las direcciones URL que especifique aquí.
  - **URL List**. Escriba las direcciones URL (una por línea) para el tipo de lista que haya escogido en **Enforce**.
- En **Bookmark**, haga clic en **Add** y, en **Name** y **URL**, escriba el nombre y la dirección URL de los marcadores que aparecerán en los exploradores seguros de los usuarios.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Browser 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta opción se configura en **Settings** > **Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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 calendarios (CalDAV)

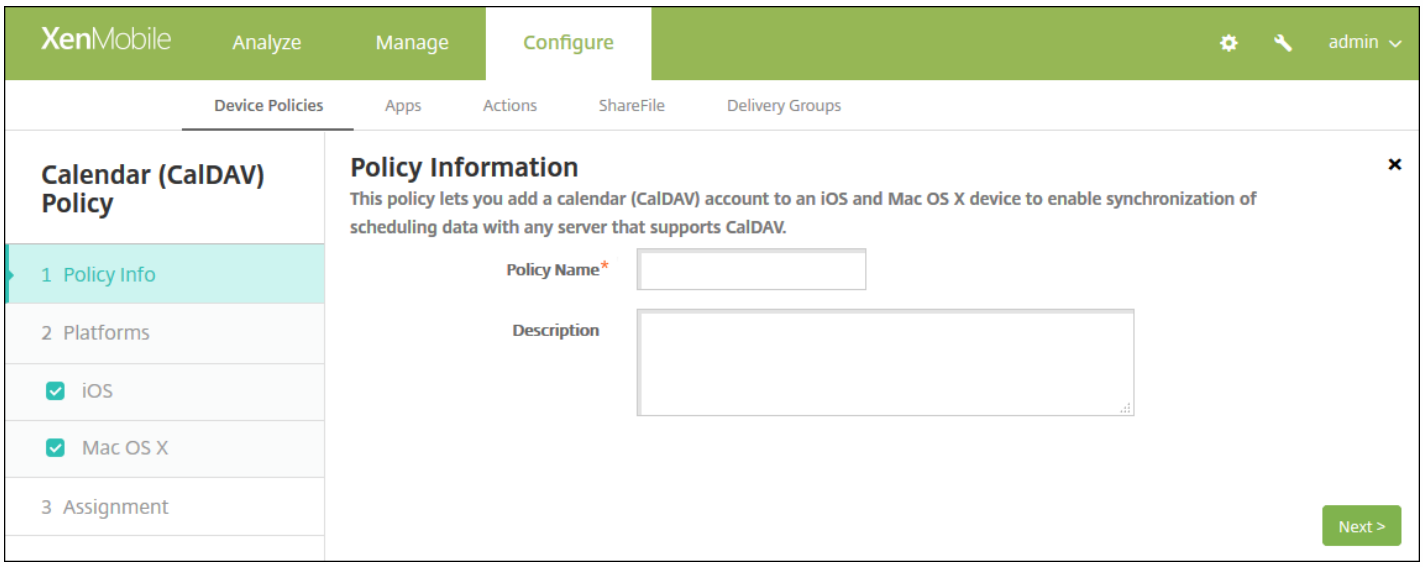
Jul 27, 2016

En XenMobile, puede agregar una directiva de dispositivos si quiere agregar una cuenta de calendarios (CalDAV) a los dispositivos iOS o Mac OS X 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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **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:

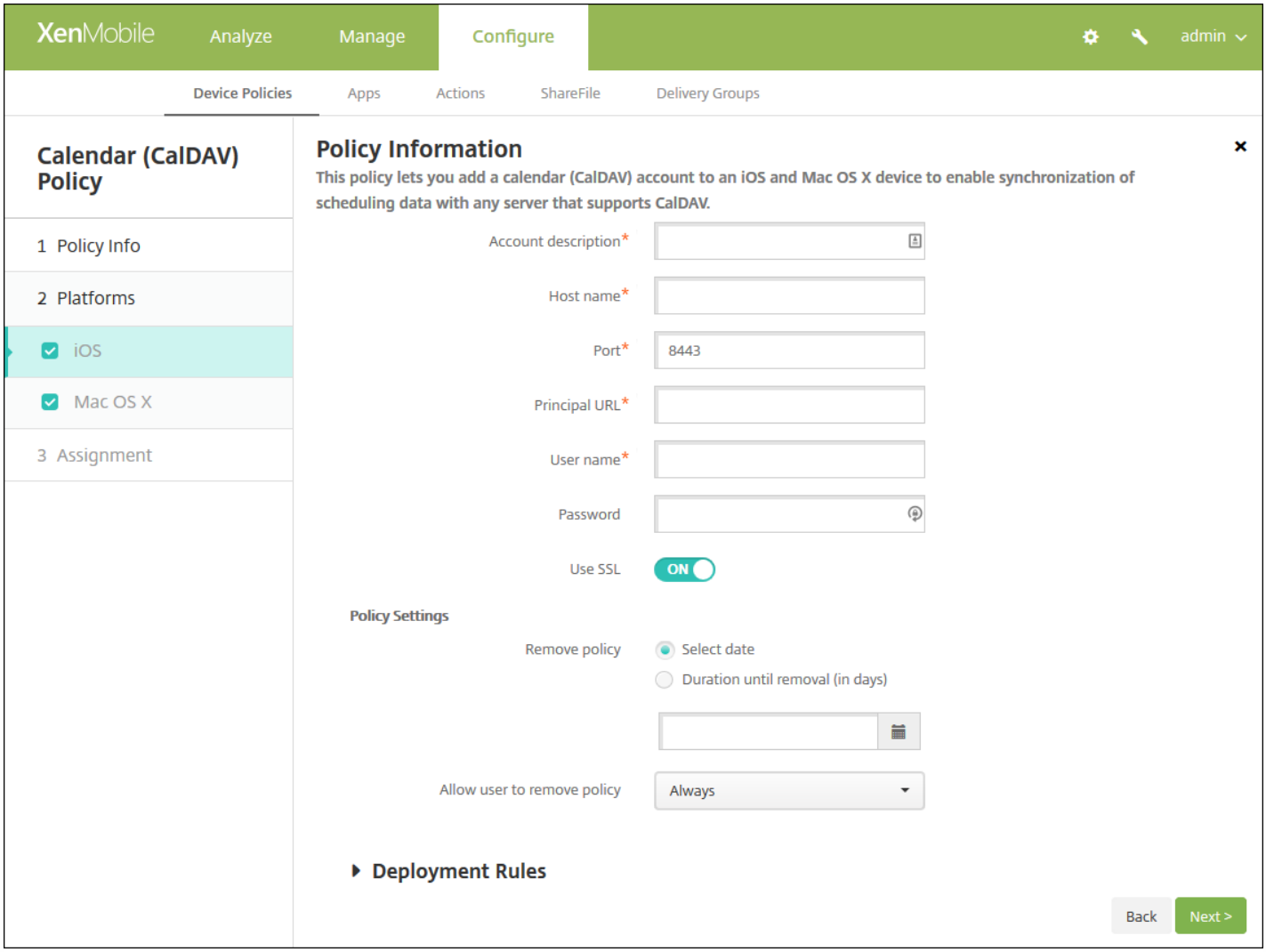
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

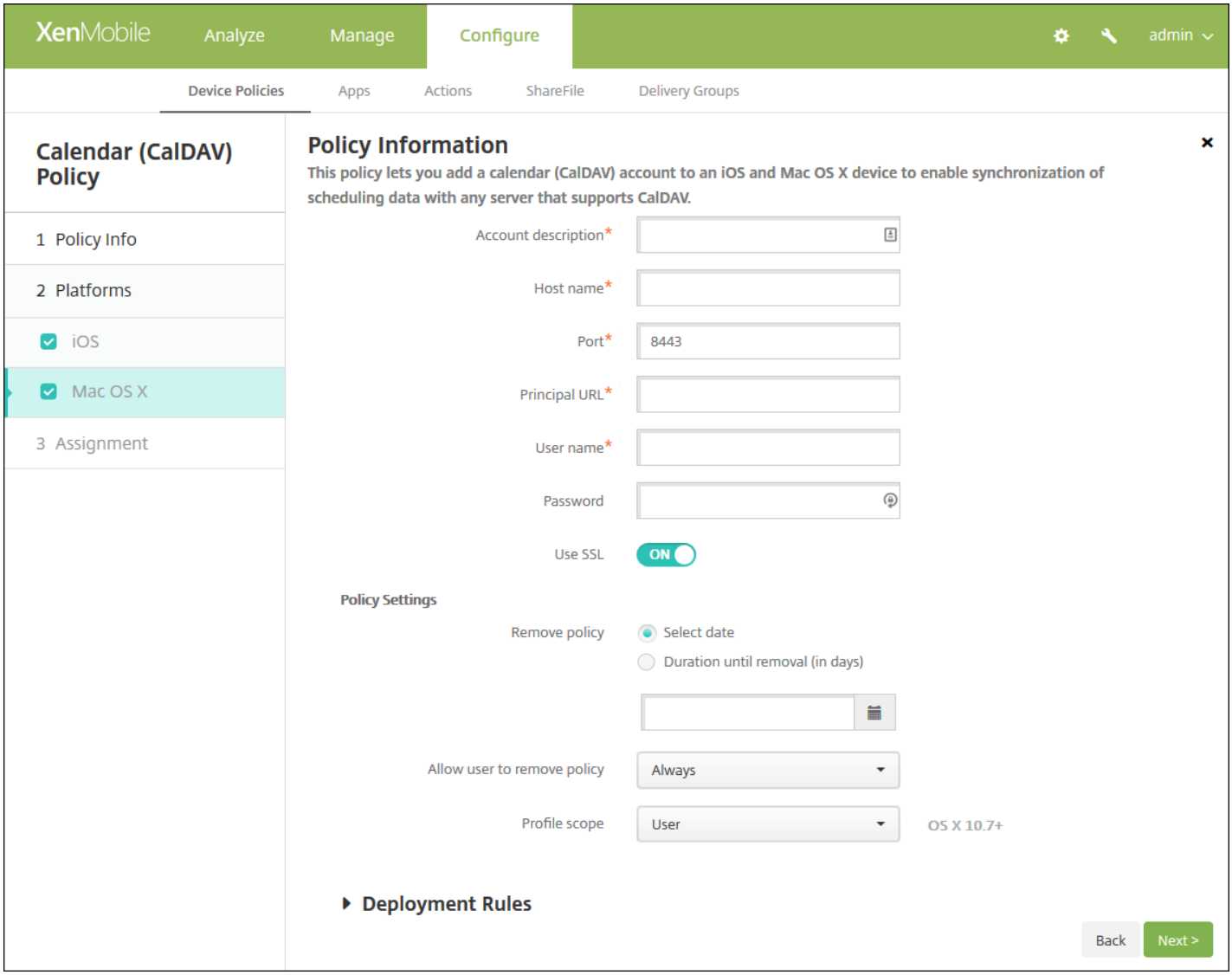
Configuración de los parámetros de iOS



Configure los siguientes parámetros:

- **Account description**. Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name**. Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Port**. Especifique el puerto con el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL**. Indique la URL base del calendario del usuario.
- **User name**. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password**. Escriba una contraseña opcional de usuario.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



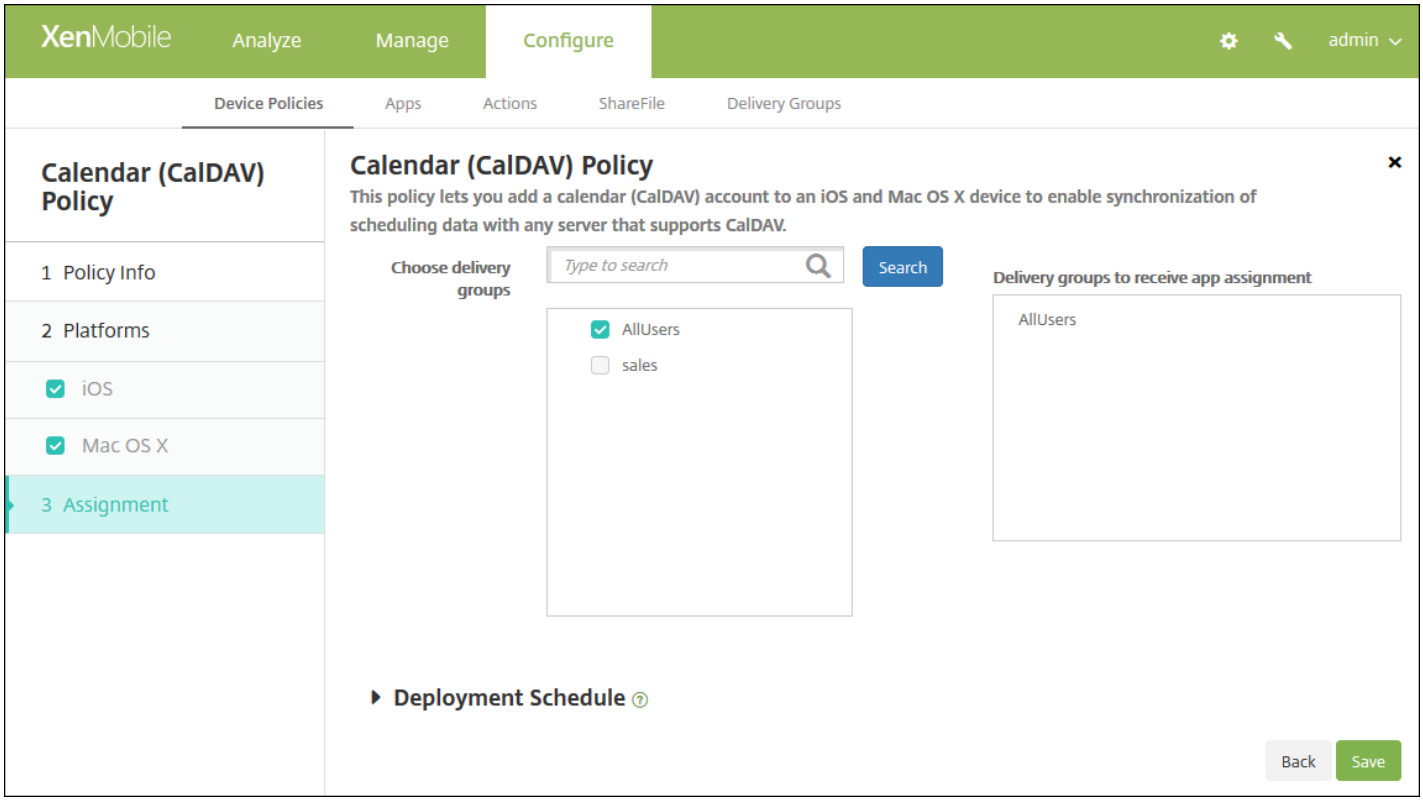
Configure los siguientes parámetros:

- **Account description**. Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name**. Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Port**. Especifique el puerto con el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL**. Indique la URL base del calendario del usuario.
- **User name**. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password**. Escriba una contraseña opcional de usuario.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está

disponible para OS X 10.7 y versiones posteriores.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Calendar (CalDAV) 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta opción se configura en **Settings** > **Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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**.

Directiva de redes de telefonía móvil

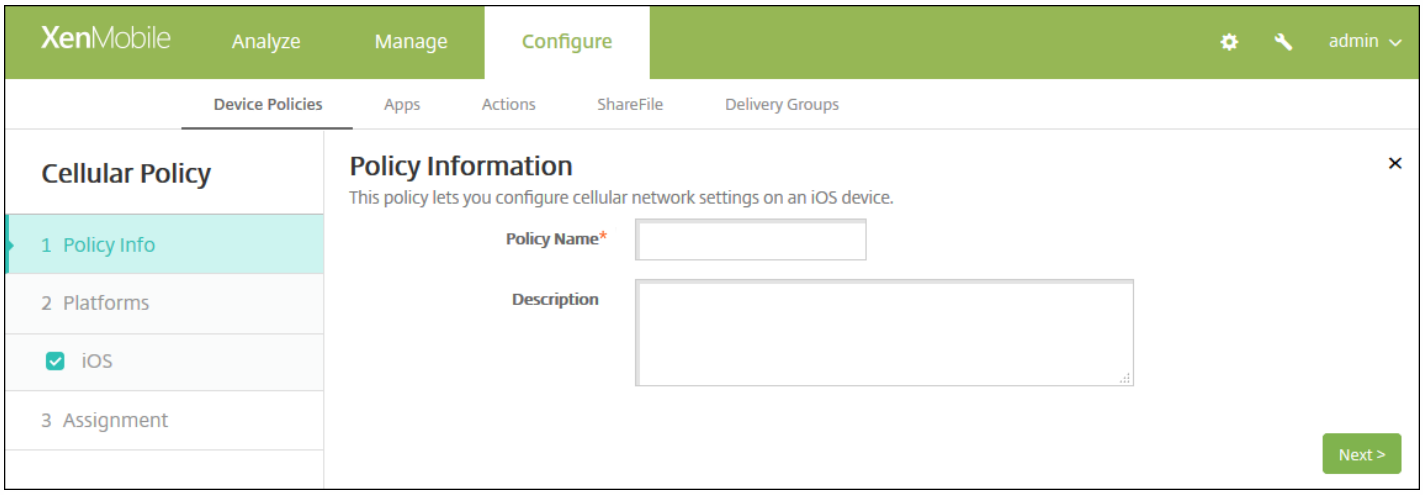
Jul 27, 2016

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**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá la página **Add a New Policy**.

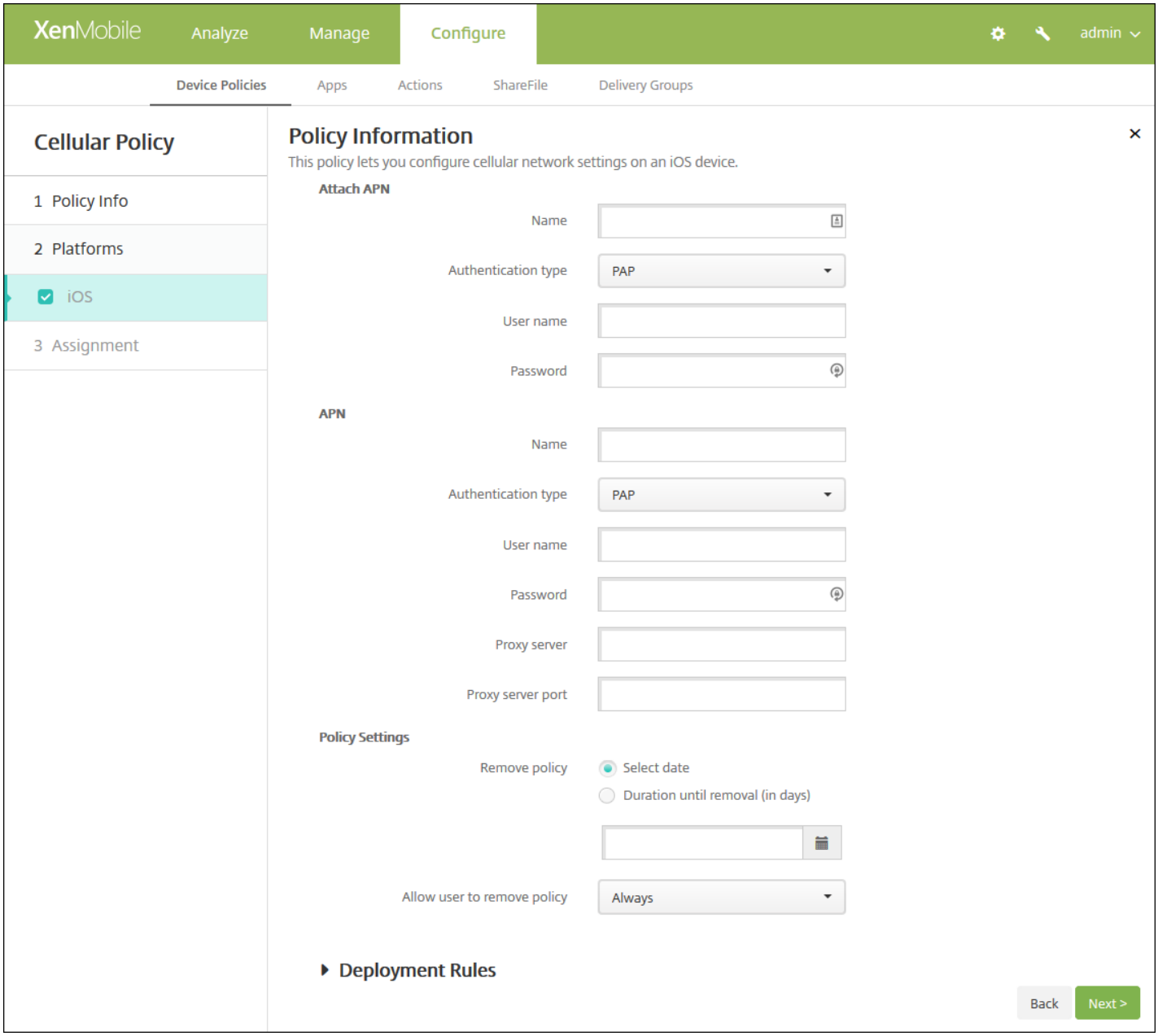
3. Expanda **More** y, a continuación, en **Network Access**, haga clic en **Cellular**. Aparecerá la página de información **Cellular Network Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **iOS Platform**.



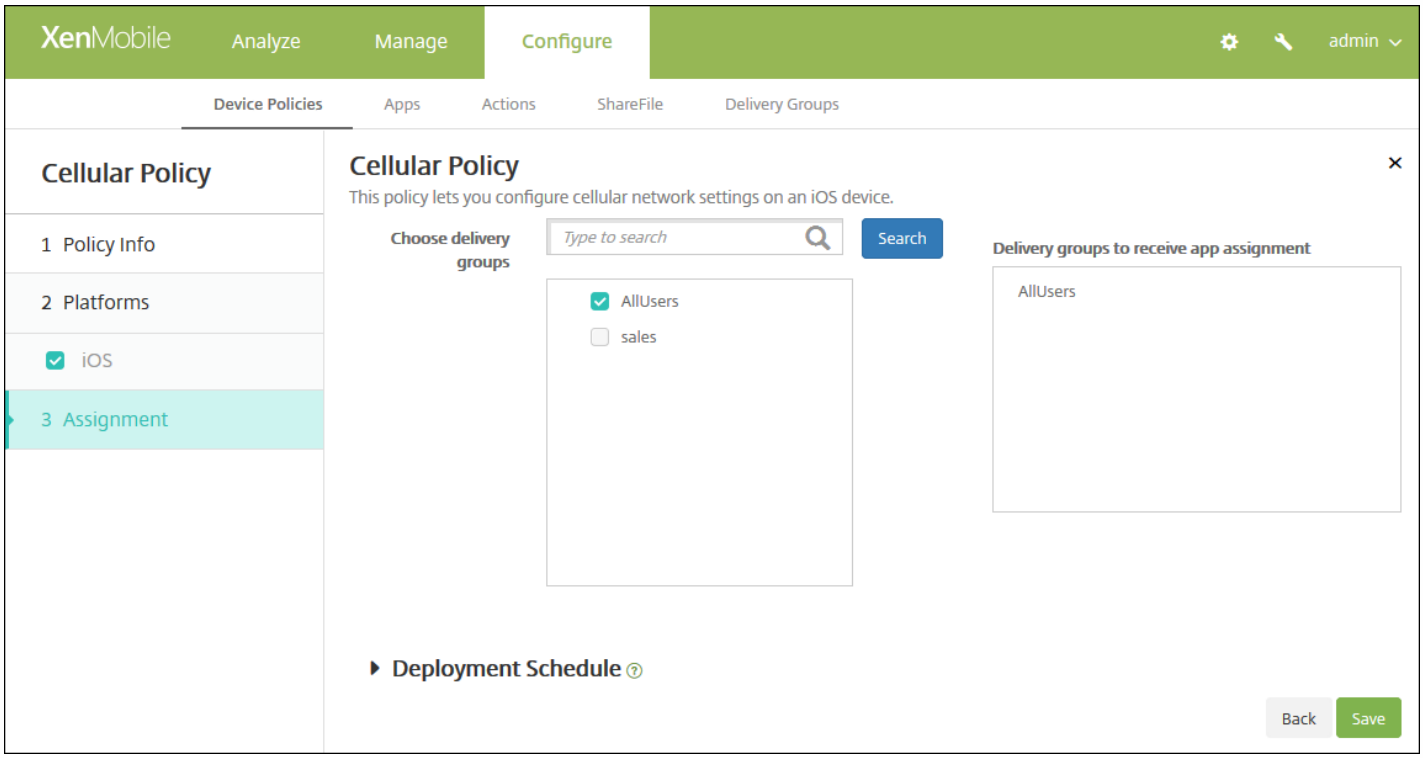
6. Configure los siguientes parámetros:

- **Attach APN**
  - **Name**. Escriba un nombre para esta configuración.
  - **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**.
  - **User name**. Escriba el nombre de usuario que se usará para la autenticación.
- **APN**
  - **Name**. Escriba un nombre para la configuración del nombre de punto de acceso (APN).
  - **Authentication type**. En la lista, haga clic en **CHAP** o **PAP**. El valor predeterminado es **PAP**.
  - **User name**. Escriba el nombre de usuario que se usará para la autenticación.
  - **Password**. Escriba una contraseña para la autenticación.
  - **Proxy server**. Escriba la dirección de red del servidor proxy.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Cellular Network 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.

- 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**.

Directiva de administrador de conexiones

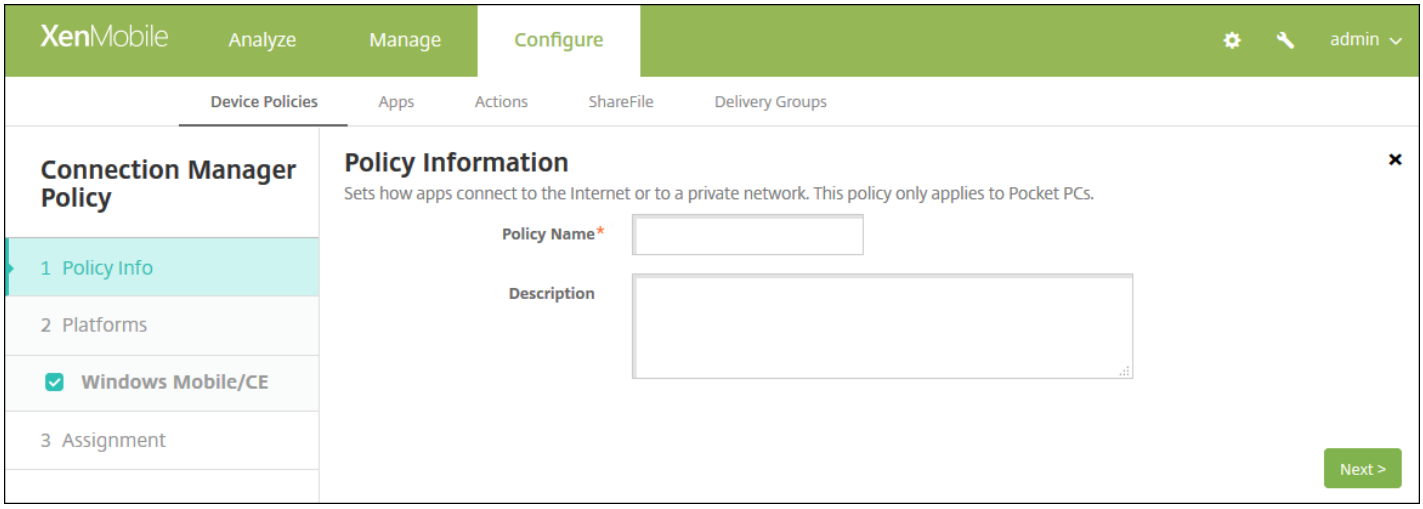
Jul 27, 2016

En XenMobile, puede especificar la configuración de conexión de las aplicaciones que se conectan automáticamente a Internet y a redes privadas. Esta directiva solo está disponible para dispositivos Pocket PC de Windows.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

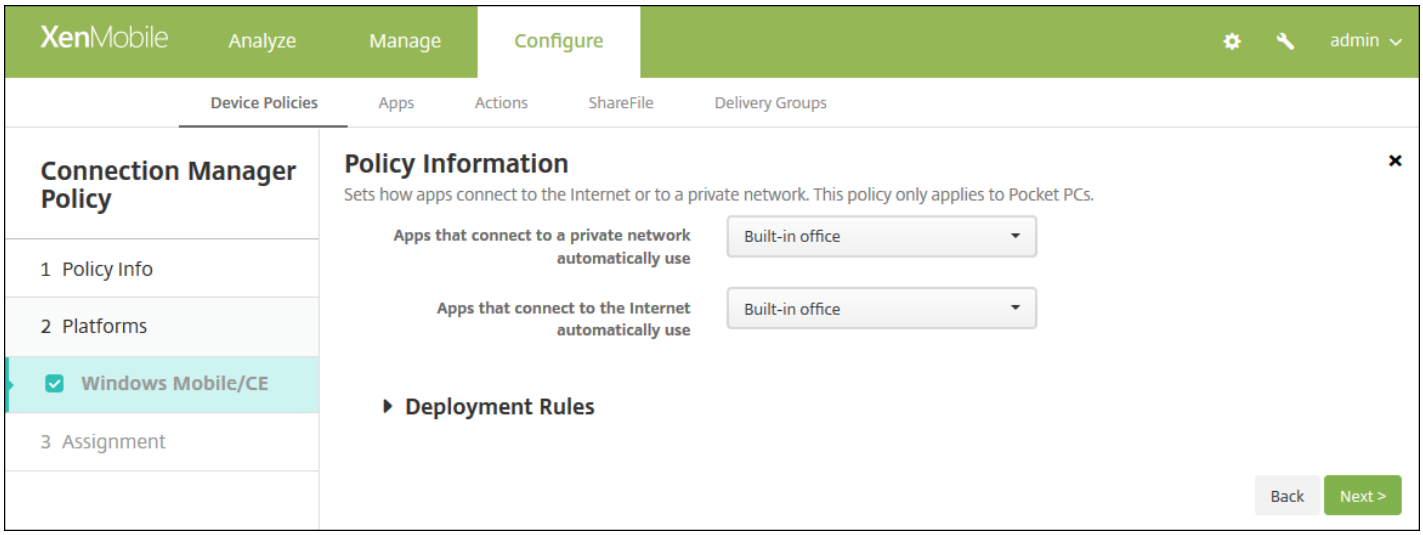
3. Haga clic en **More** y, en **Network access**, haga clic en **Connection Manager**. Aparecerá la página de información **Connection Manager Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



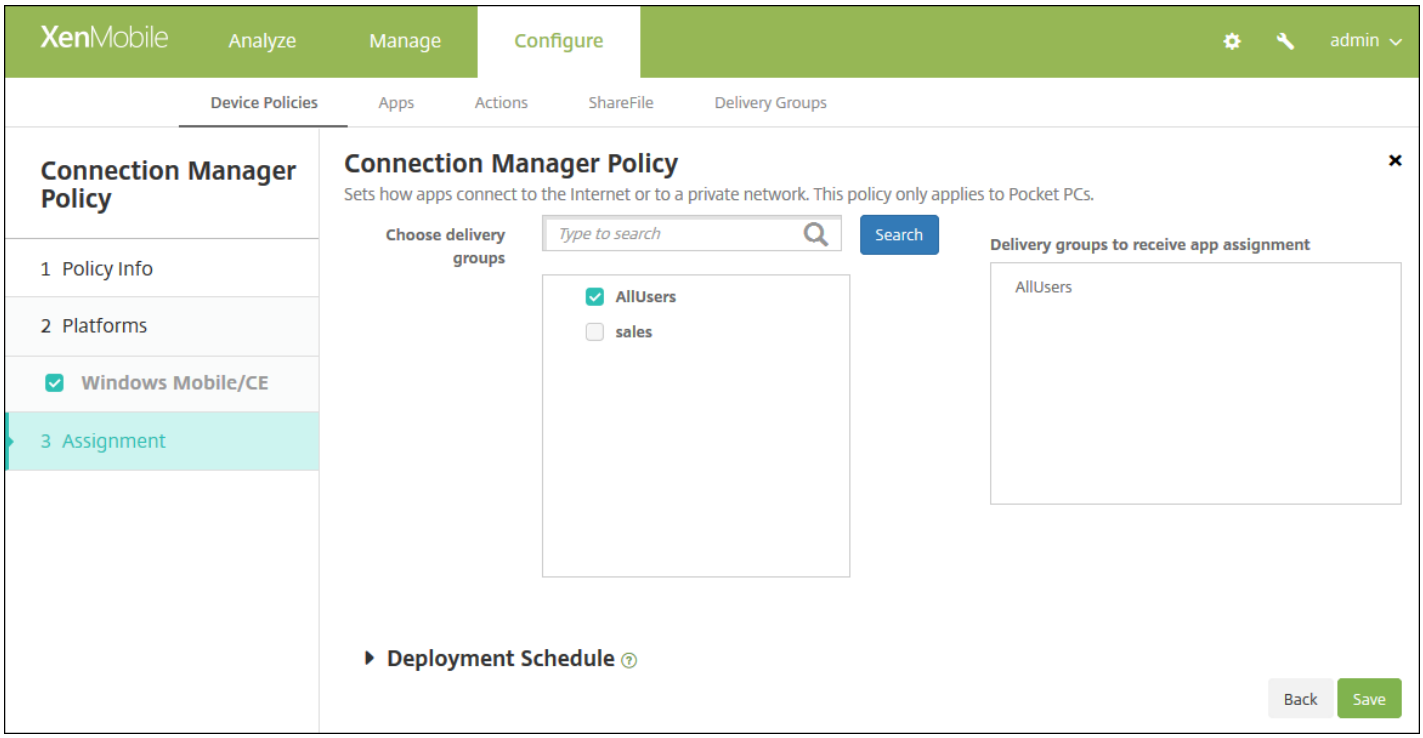
6. Configure estas opciones.

Nota: La opción **Built-in office** significa que todas las conexiones se realizan a la intranet de la empresa, mientras que **Built-in Internet** significa que todas las conexiones se realizan a Internet.

- **Apps that connect to a private network automatically use**. En la lista, haga clic en **Built-in office** o **Built-in Internet**. El valor predeterminado es **Built-in office**.
- **Apps that connect to the Internet automatically use**. En la lista, haga clic en **Built-in office** o **Built-in Internet**. El valor predeterminado es **Built-in office**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Connection Manager**.



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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 programación de conexiones

Jul 27, 2016

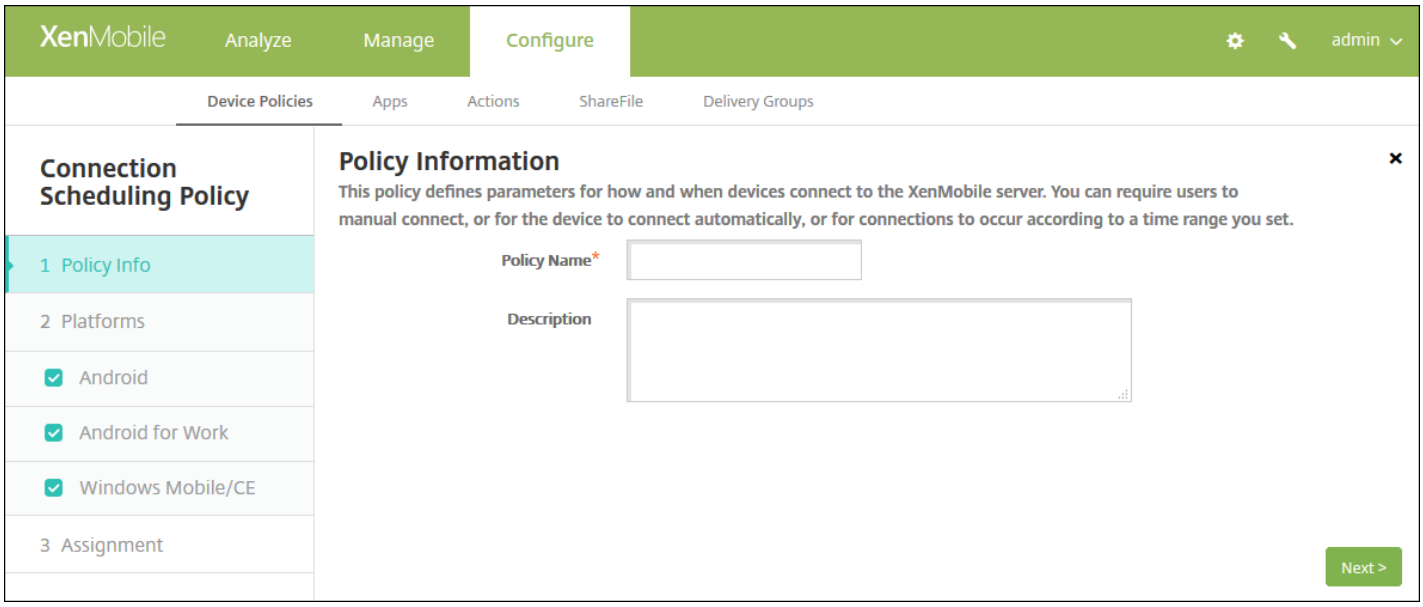
Puede crear directivas de programación de conexiones para controlar cómo y cuándo los usuarios de los dispositivos se conectan a XenMobile. Tenga en cuenta que también puede configurar esta directiva para dispositivos habilitados para Android for Work.

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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

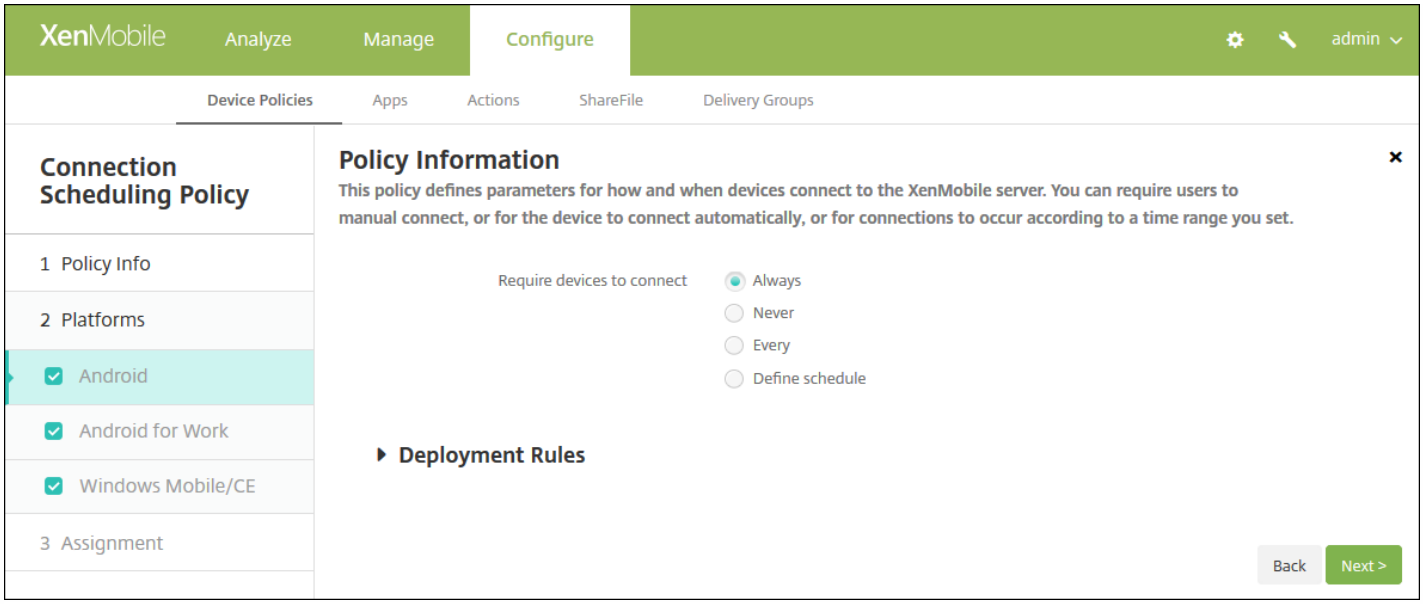
3. Haga clic en **Scheduling**. Aparecerá la página de información **Connection Scheduling Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

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. Citrix recomienda esta opción para maximizar la seguridad. Cuando seleccione **Always**, use también la opción **Tunnel Policy** del dispositivo, con el valor **Define connection time-out** para asegurarse de que la conexión no gaste toda la batería. Manteniendo la conexión activa, puede enviar comandos de seguridad, tales como borrado o bloqueo del dispositivo, a demanda. También debe seleccionar la opción **Deployment Schedule**, **Deploy for always-on connections** en cada directiva implementada en el dispositivo.
  - **Never**. Se conecta manualmente. Los usuarios deben iniciar la conexión desde XenMobile en sus dispositivos. Citrix no recomienda esta opción para las implementaciones de producción, ya que impide la implementación de directivas de seguridad en los dispositivos y, por lo tanto, los usuarios nunca reciben nuevas aplicaciones o directivas.
  - **Every**. Se conecta en el intervalo predeterminado. Cuando esta opción está activa y usted envía una directiva de seguridad, como un bloqueo o un borrado, XenMobile procesa la acción en el dispositivo la próxima vez que el dispositivo se conecta. 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**. Cuando se habilita, 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 a intervalos regulares en el período de tiempo que usted defina. Consulte Definición de un período de tiempo de conexión para configurar un período de tiempo de conexión.
    - **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

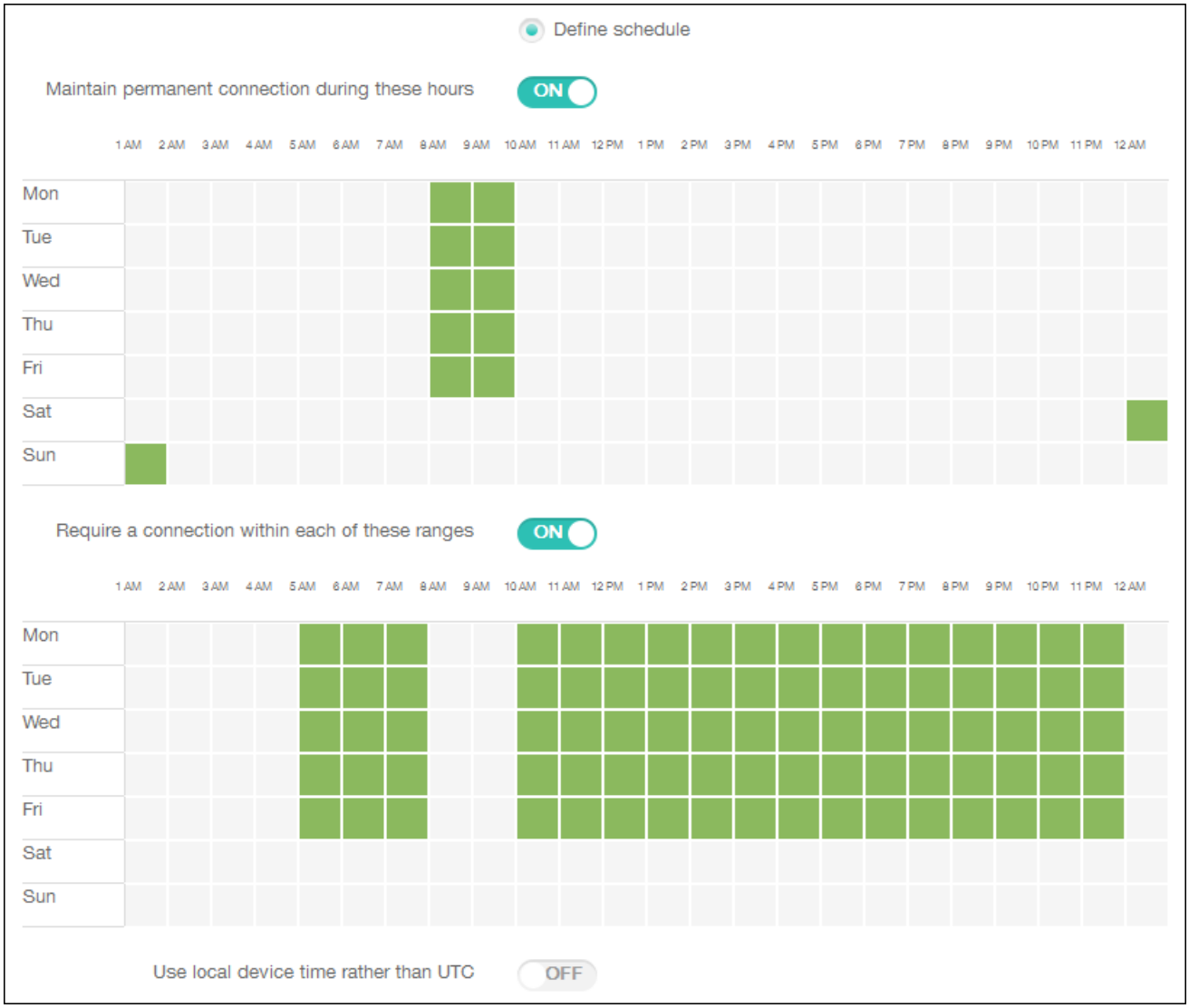
vez en cualquier período de tiempo definido.

- **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).

Definición de un período de tiempo de conexión

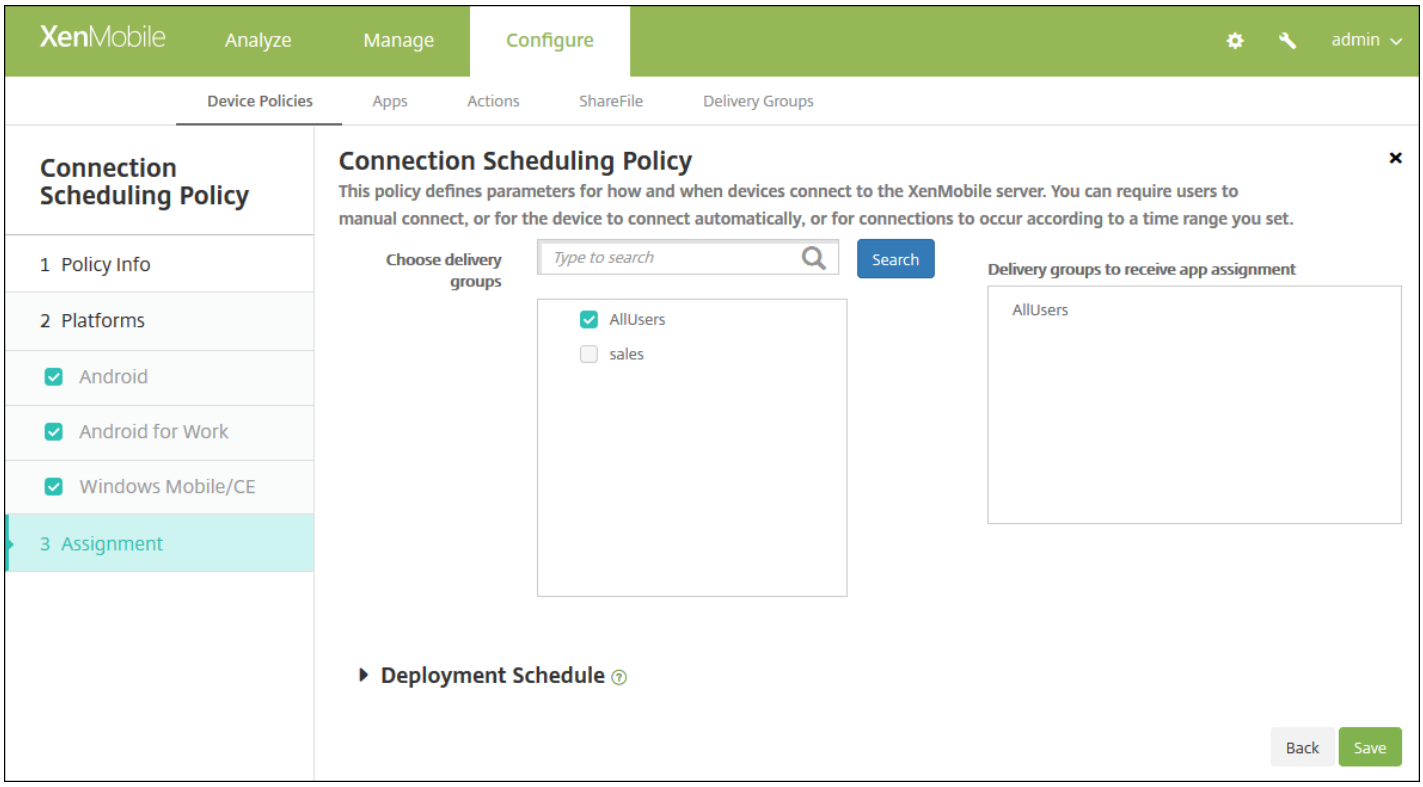
Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. 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.



8. Configure las reglas de implementación.

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**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directivas de contactos (CardDAV)

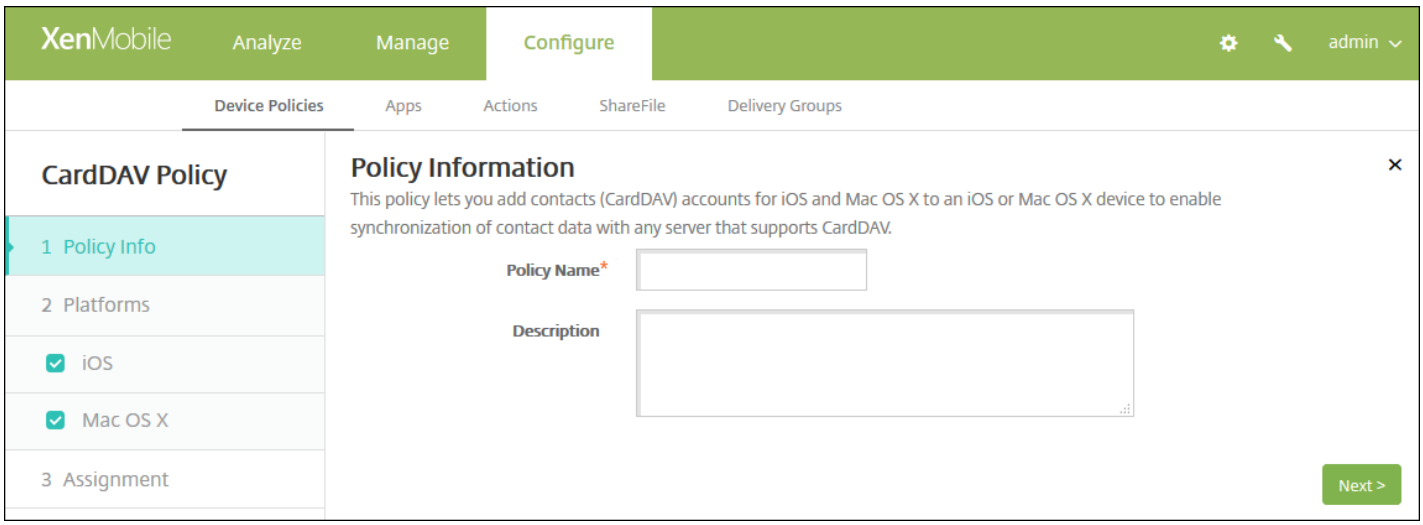
Jul 27, 2016

En XenMobile, puede agregar una directiva de dispositivos para agregar una cuenta de contactos iOS (CardDAV) a los dispositivos iOS o Mac OS X 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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **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:

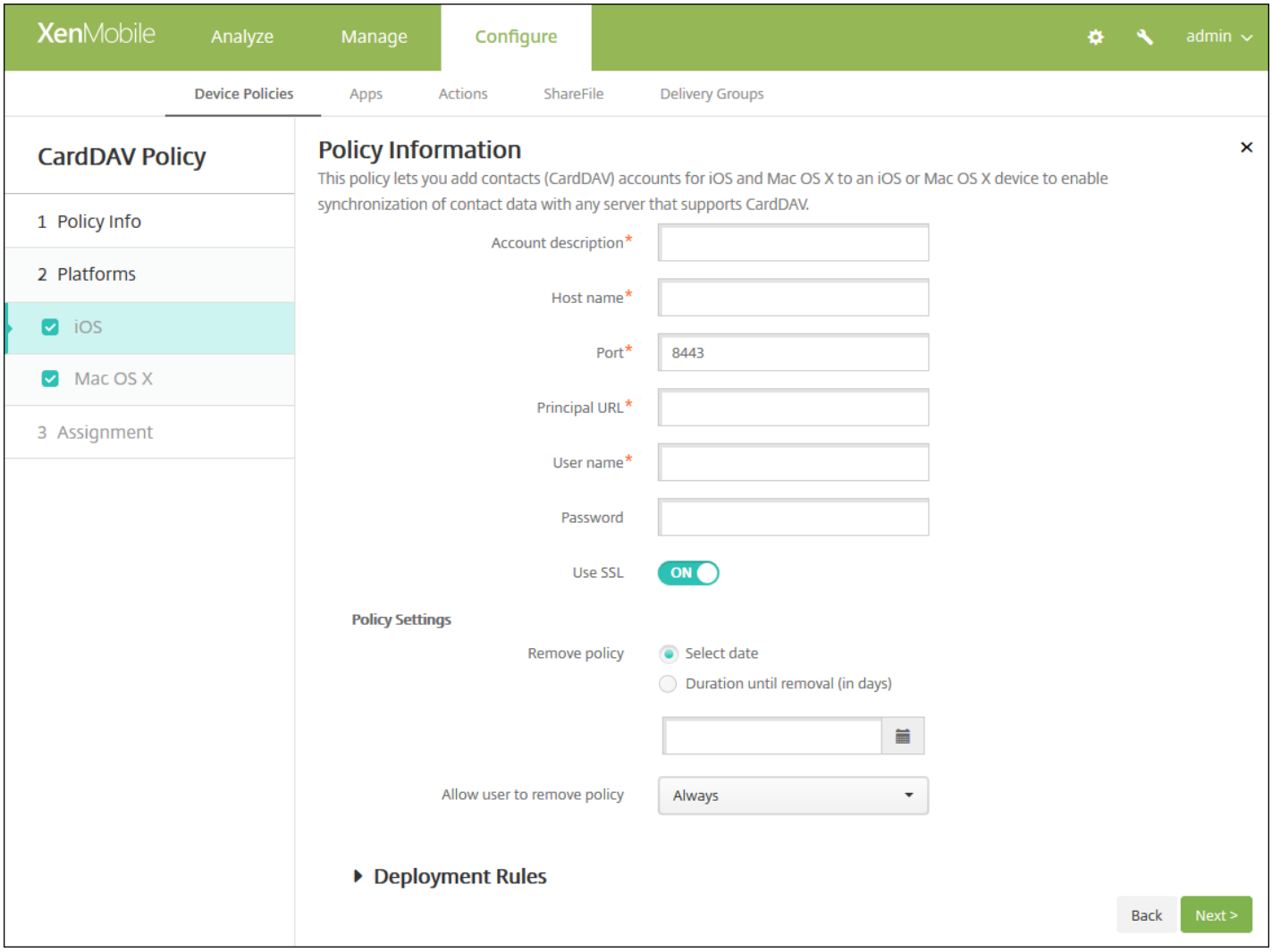
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

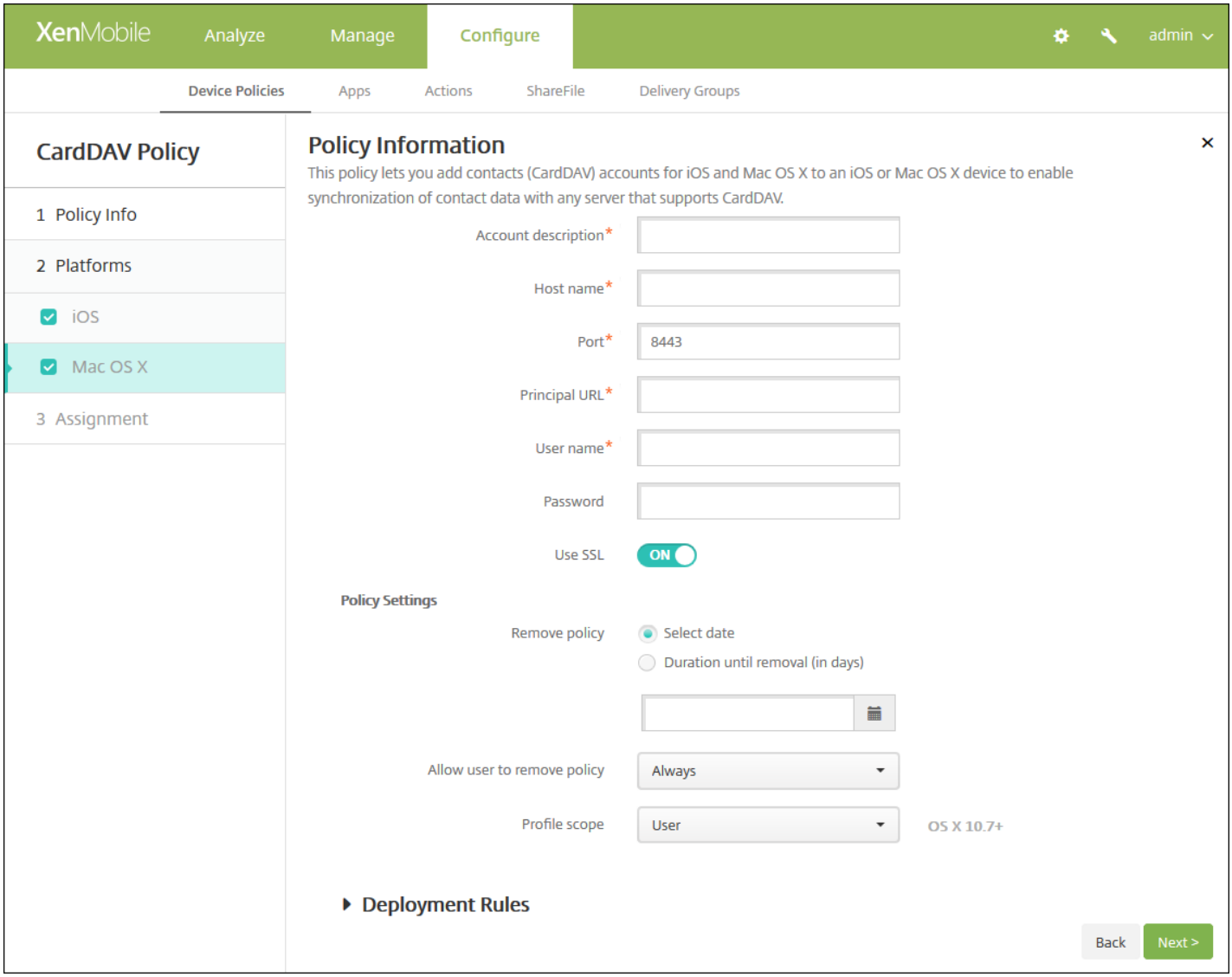
Configuración de los parámetros de iOS



Configure estos parámetros:

- **Account description**. Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name**. Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Port**. Especifique el puerto con el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL**. Indique la URL base del calendario del usuario.
- **User name**. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password**. Escriba una contraseña opcional de usuario.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



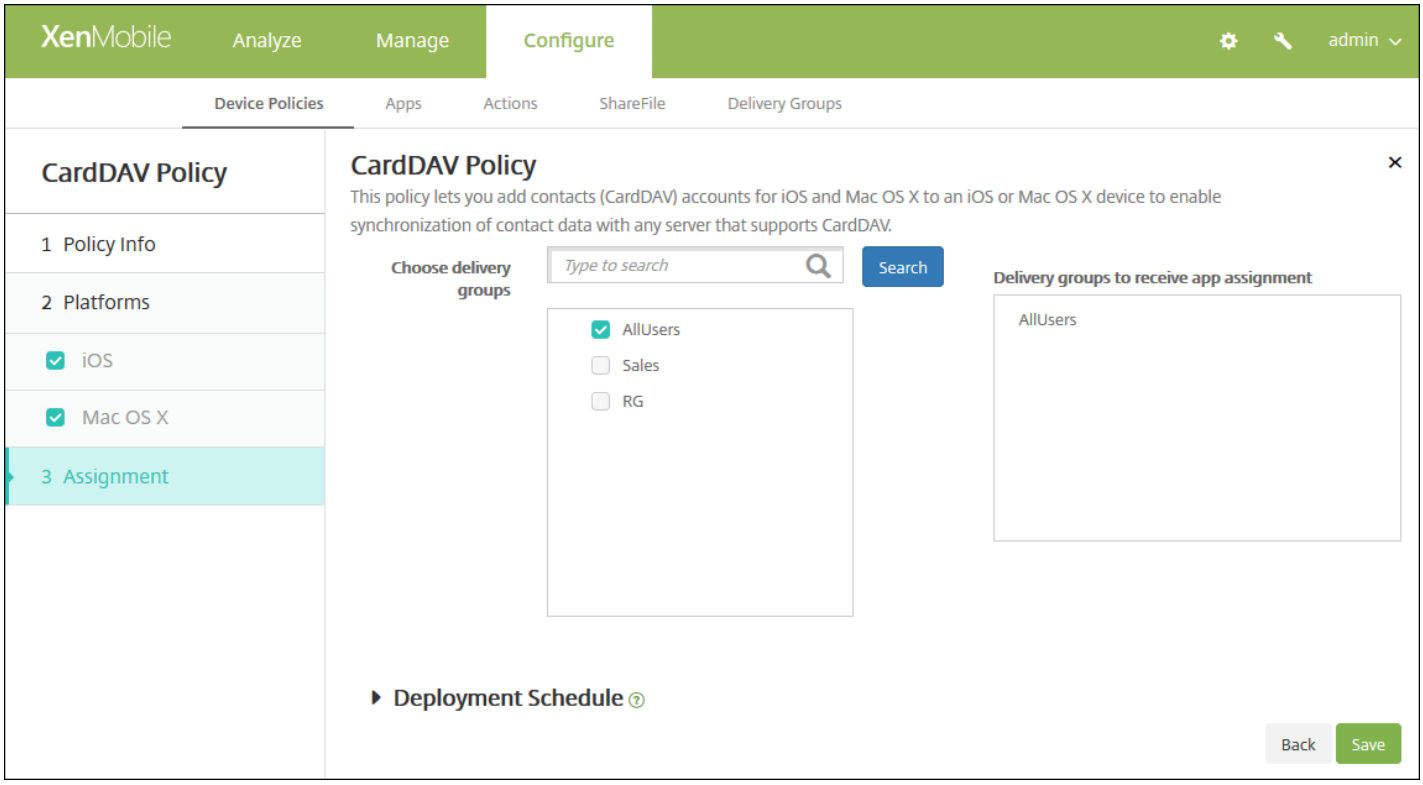
Configure estos parámetros:

- **Account description**. Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name**. Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Port**. Especifique el puerto con el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL**. Indique la URL base del calendario del usuario.
- **User name**. Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password**. Escriba una contraseña opcional de usuario.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está

disponible para OS X 10.7 y versiones posteriores.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **CardDAV 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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 en **Settings** > **Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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**.

Copiado de aplicaciones a directivas de contenedores Samsung

Jul 27, 2016

Puede especificar que las aplicaciones que ya estén instaladas en un dispositivo se copien a un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles (para obtener más información acerca de los dispositivos compatibles, consulte la página de Samsung Dispositivos compatibles con Samsung KNOX). Las aplicaciones que se copien al contenedor SEAMS estarán disponibles en las pantallas de inicio de los usuarios, mientras que las aplicaciones que se copien al contenedor KNOX solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.

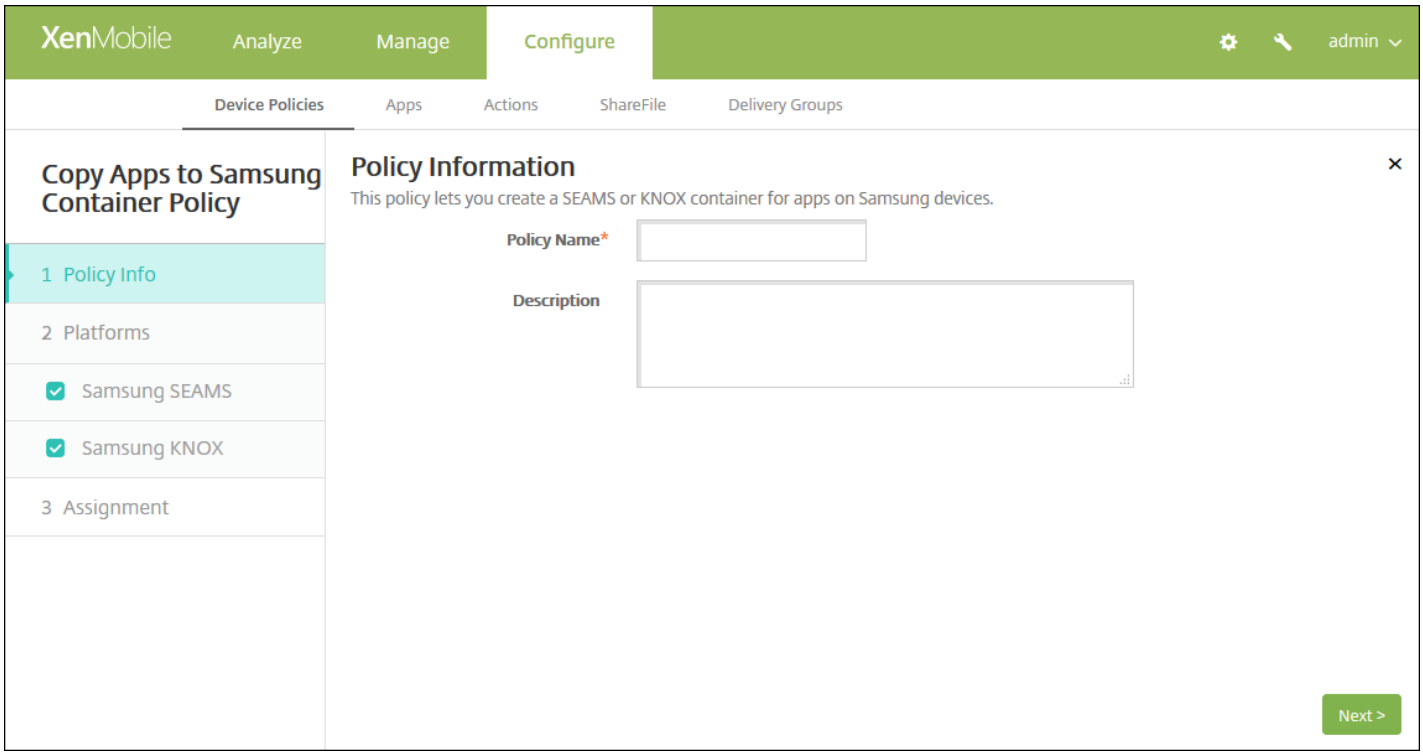
Requisitos previos:

- Los dispositivos deben estar inscritos en XenMobile.
- Las claves MDM de Samsung (ELM y KLM) deben estar implementadas (para obtener información sobre cómo llevarlo a cabo, consulte las directivas de claves de licencia para Samsung MDM).
- Las aplicaciones deben estar ya instaladas en el dispositivo.
- Inicialice KNOX en el dispositivo para copiar las aplicaciones al contenedor KNOX.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

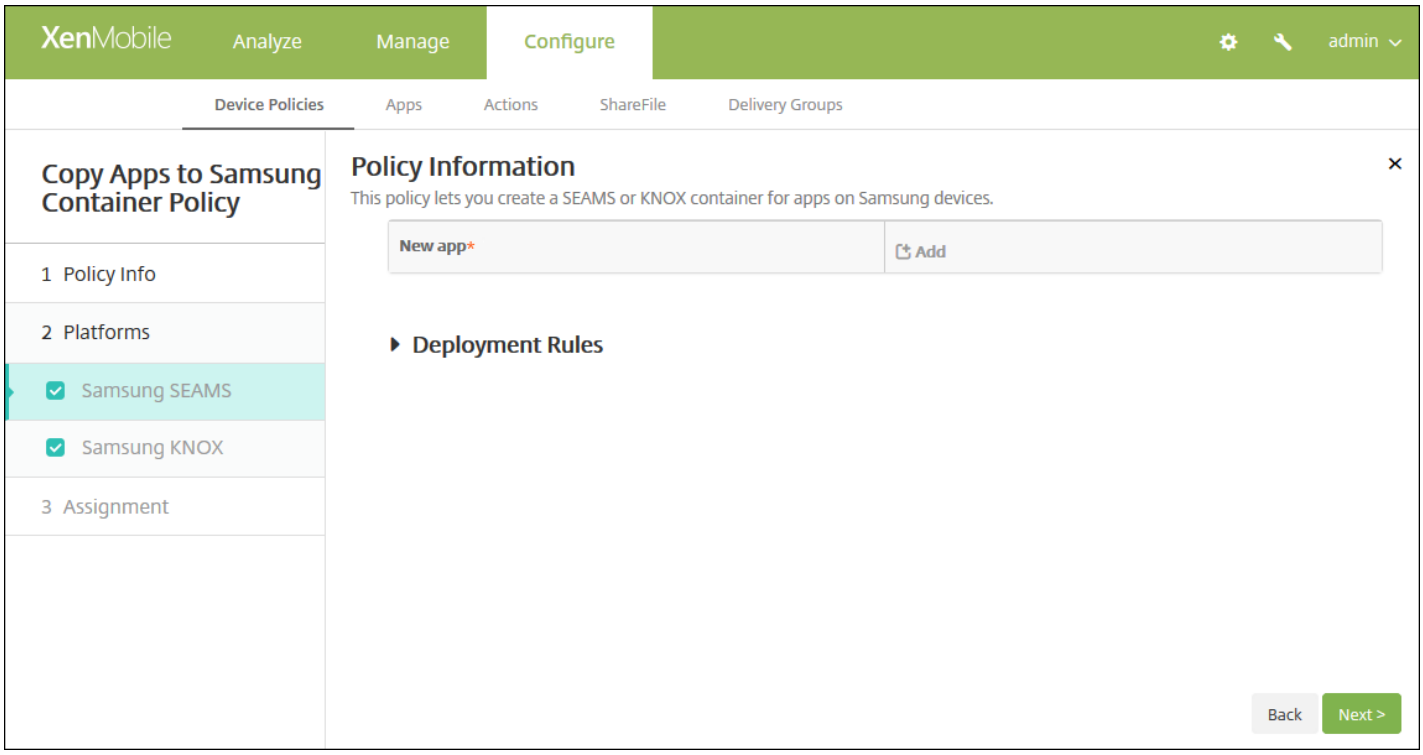
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Copy Apps to Samsung Container**. Aparecerá la página de información acerca de la directiva **Copy Apps to Samsung Container Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En Platforms, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

7. Configure el siguiente parámetro para cada una de las plataformas seleccionadas.

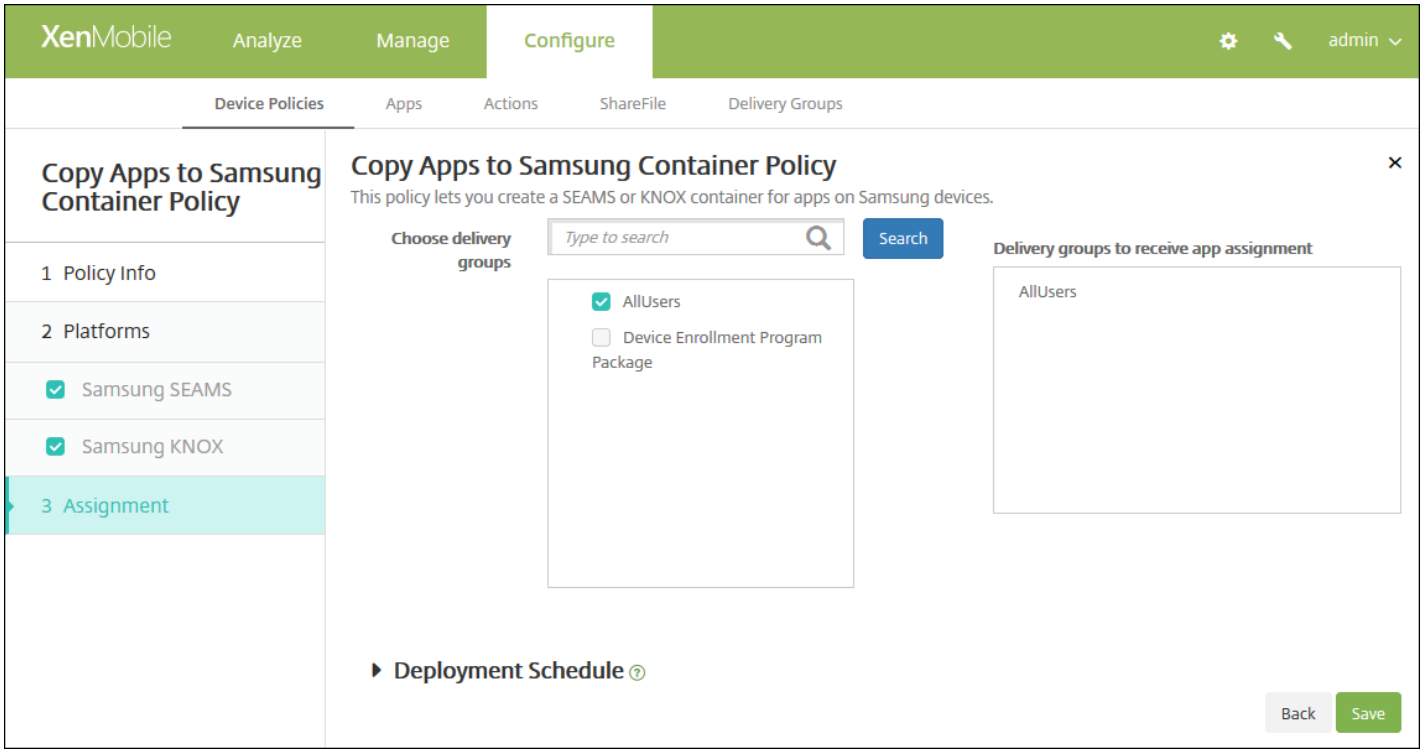
- **New App**. Para agregar cada aplicación a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - Escriba un ID de paquet, por ejemplo: com.mobiwolf.lacingart para la aplicación LacingArt.
  - Haga clic en **Save** o **Cancel**.

    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 a la derecha. 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.

8. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de la plataforma siguiente, o bien la página de asignación **Copy Apps to Samsung Container 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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.

Una vez que la directiva esté implementada correctamente, las aplicaciones SEAMS aparecerán en la página **Device details**, bajo el encabezado **Location: Enterprise SEAMS Location**, mientras que las aplicaciones KNOX aparecerán bajo el encabezado **Location: Enterprise Location**.

Directivas de credenciales

Jul 27, 2016

En XenMobile, puede crear directivas de credenciales de dispositivo para habilitar la autenticación integrada con la configuración de PKI en XenMobile, tal como una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor. Para obtener más información acerca de las credenciales, consulte Certificados.

Puede crear directivas de credenciales para dispositivos iOS, Mac OS X, Android, Android for Work, tabletas y escritorios Windows, Windows Mobile/CE y Windows Phone. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

Configuración de iOS

Configuración de Mac OS X

Configuración de Android y Android for Work

Parámetros para escritorios y tabletas Windows

Configuración de Windows Mobile/CE

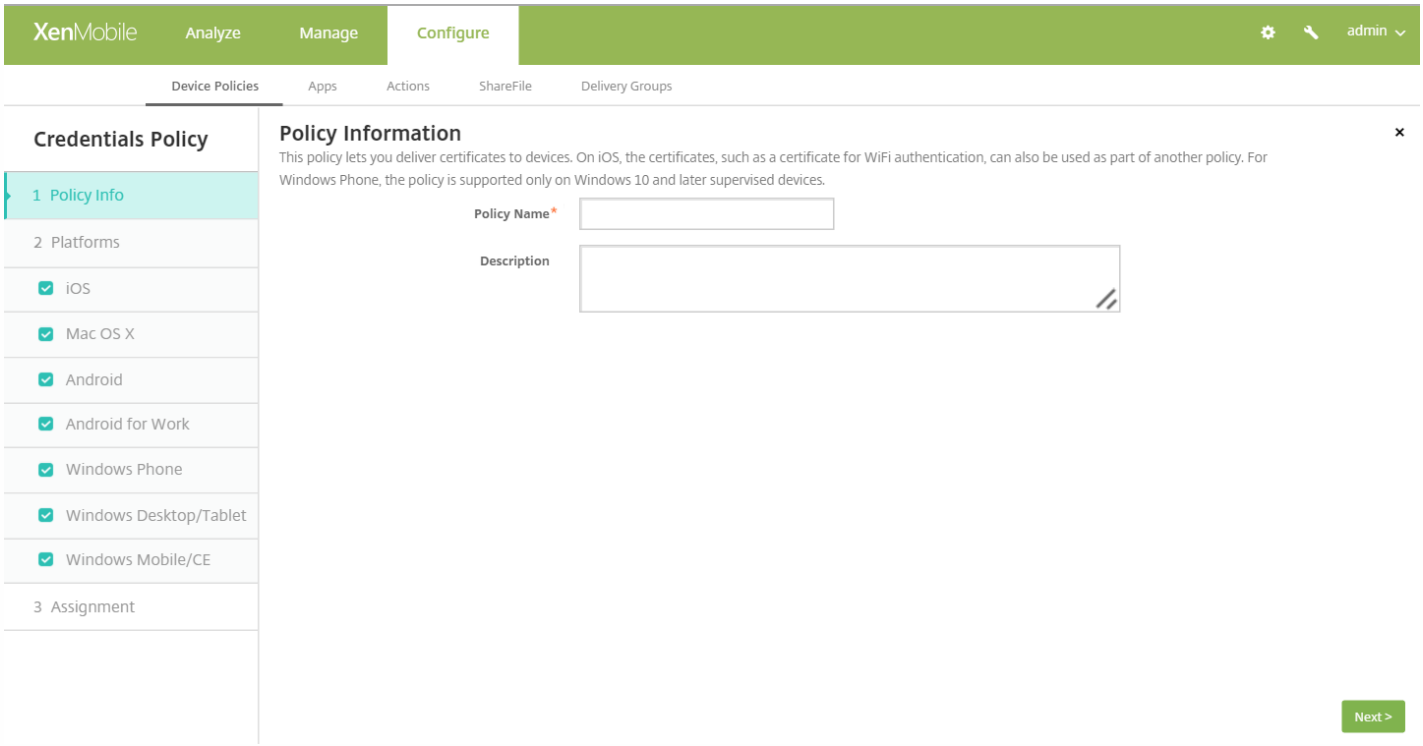
Configuración de Windows Phone

Antes de crear esta directiva, se necesita la información de credenciales que vaya a utilizar para cada plataforma, además de los certificados en sí y las contraseñas.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

3. Expanda **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:

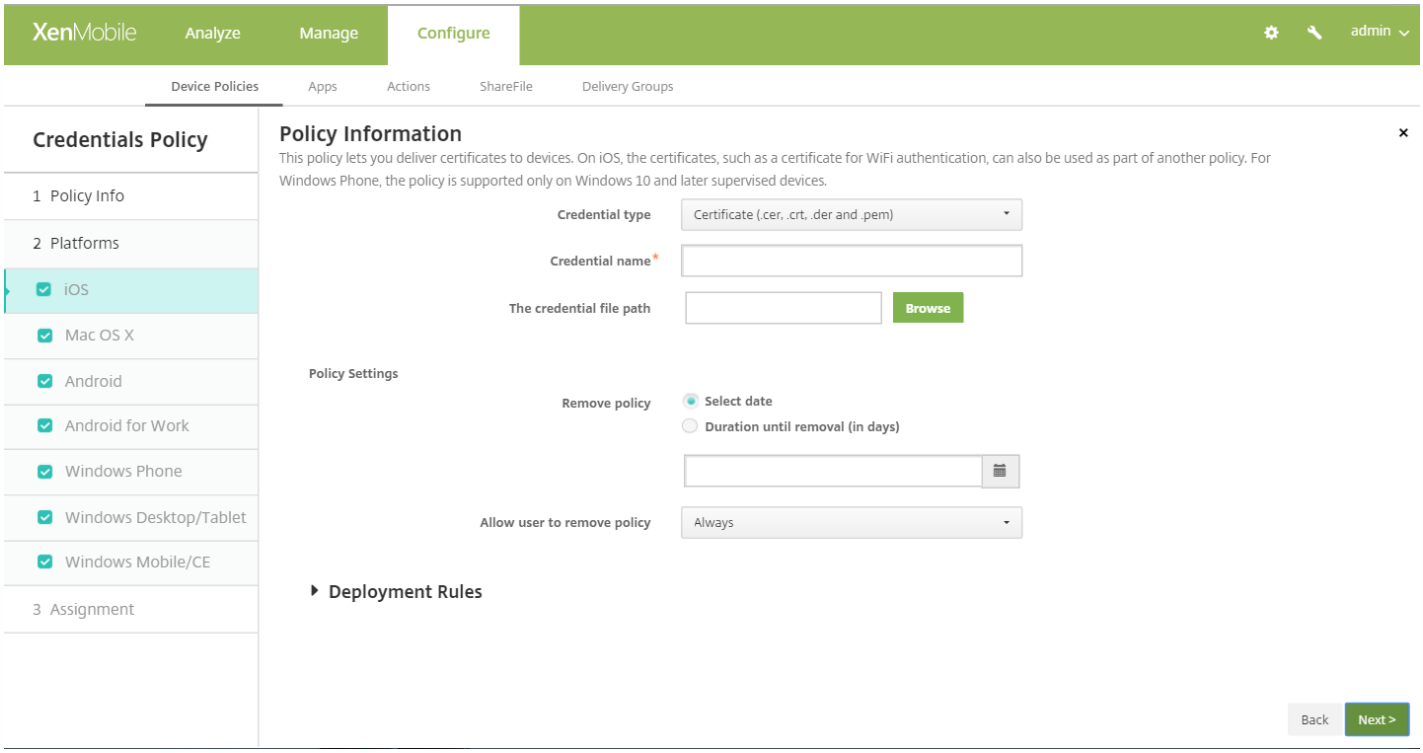
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

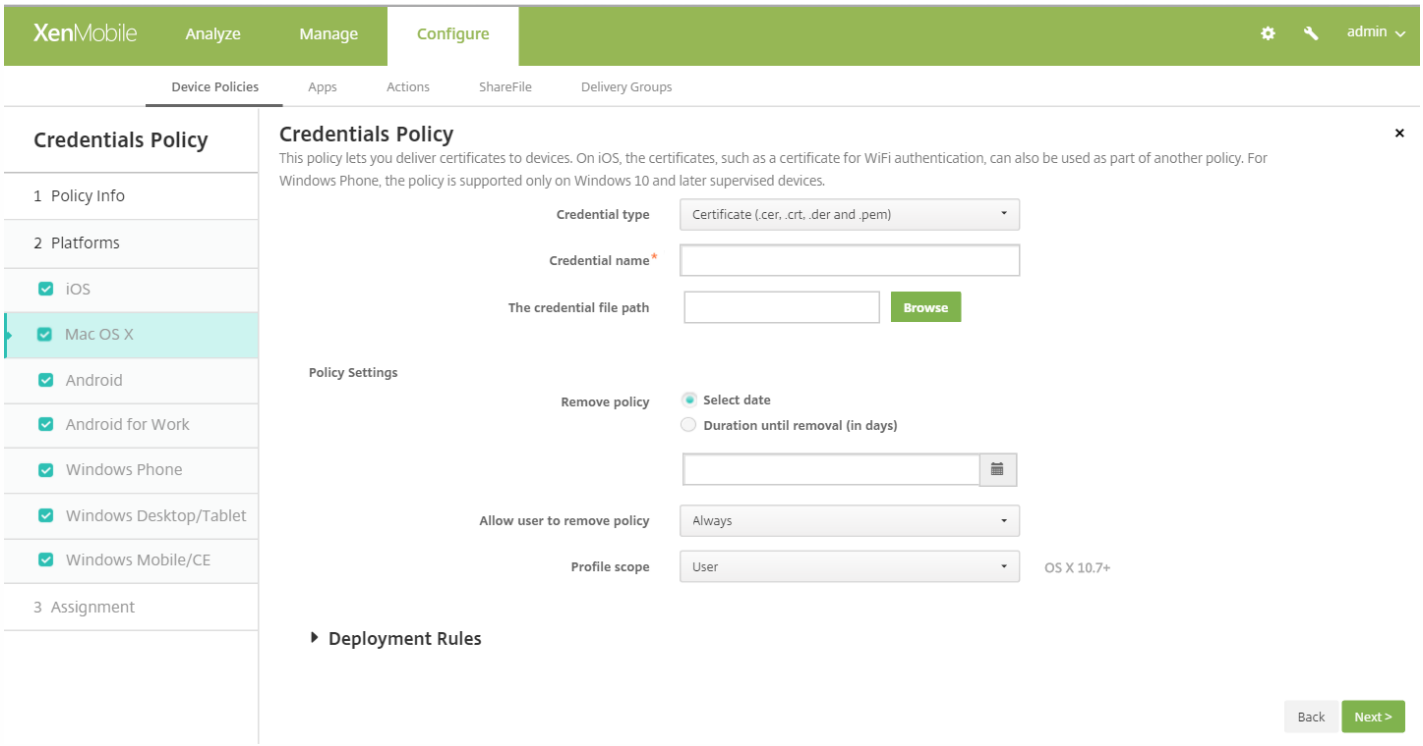
Configuración de los parámetros de iOS



Configure los siguientes parámetros:

- **Credential type**. En la lista, haga clic en el tipo de credencial que se va a utilizar con esta directiva y, a continuación, escriba la siguiente información referente a 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**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la **lista Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

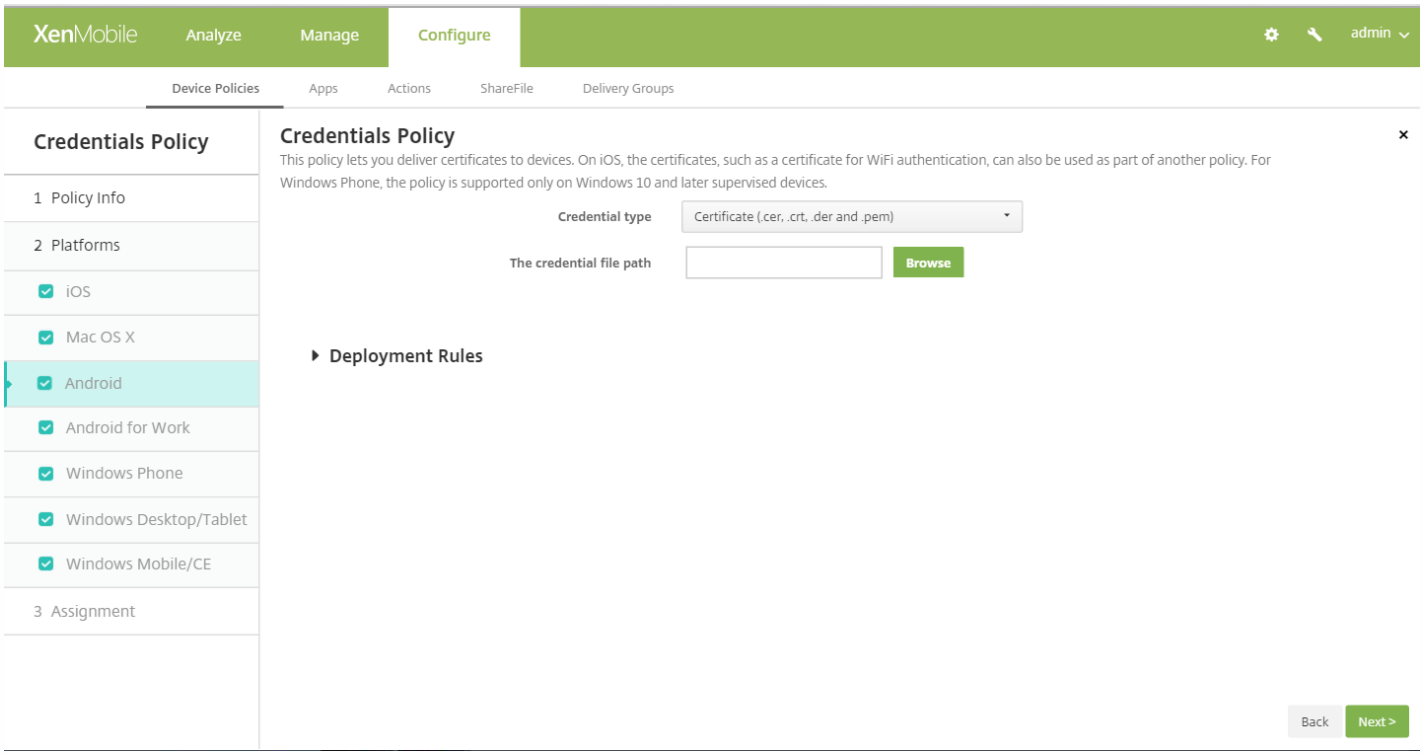
Configuración de los parámetros de Mac OS X



Configure los siguientes parámetros:

- **Credential type**. En la lista, haga clic en el tipo de credencial que se va a utilizar con esta directiva y, a continuación, escriba la siguiente información referente a 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**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la **lista Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Policy scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

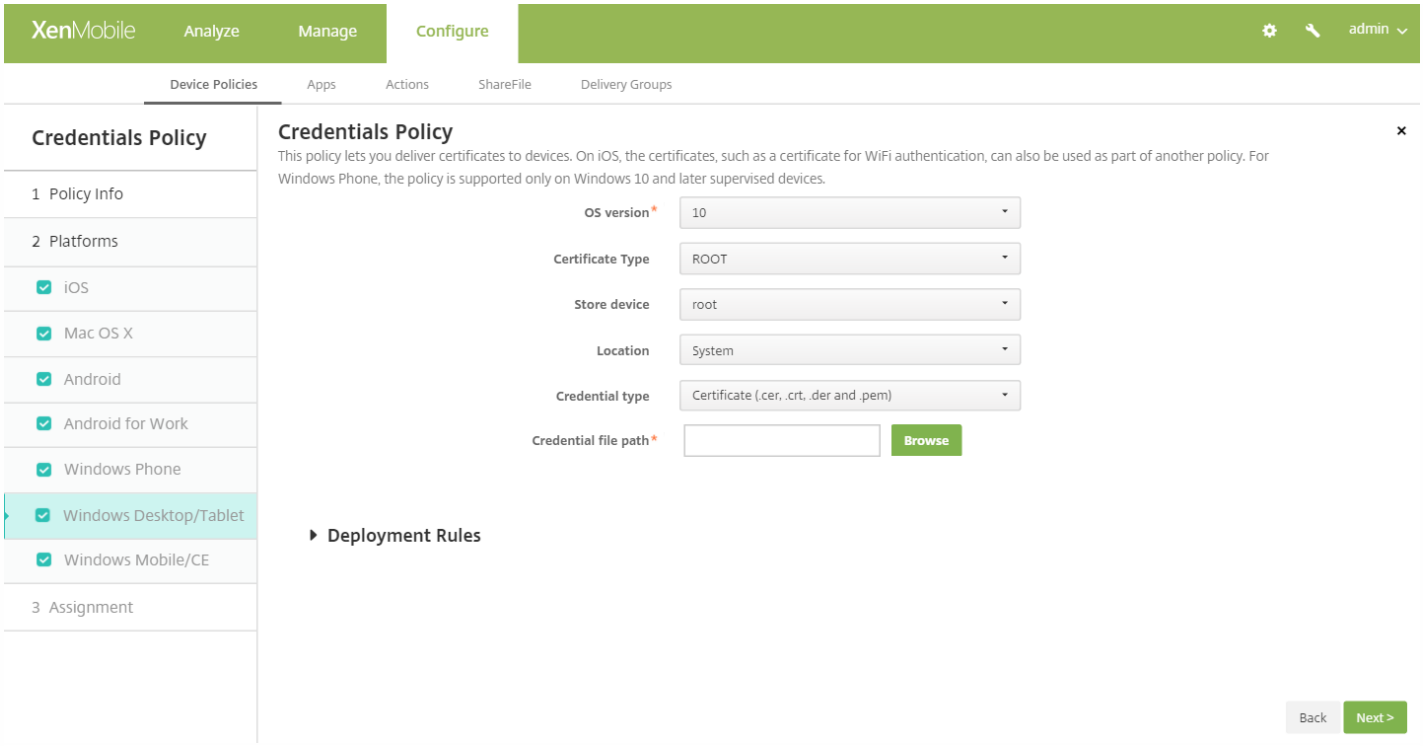
Configuración de los parámetros de Android y Android for Work



Configure los siguientes parámetros:

- **Credential type**. En la lista, haga clic en el tipo de credencial que se va a utilizar con esta directiva y, a continuación, escriba la siguiente información referente a 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 la 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.

Configuración de los parámetros de escritorios o tabletas Windows



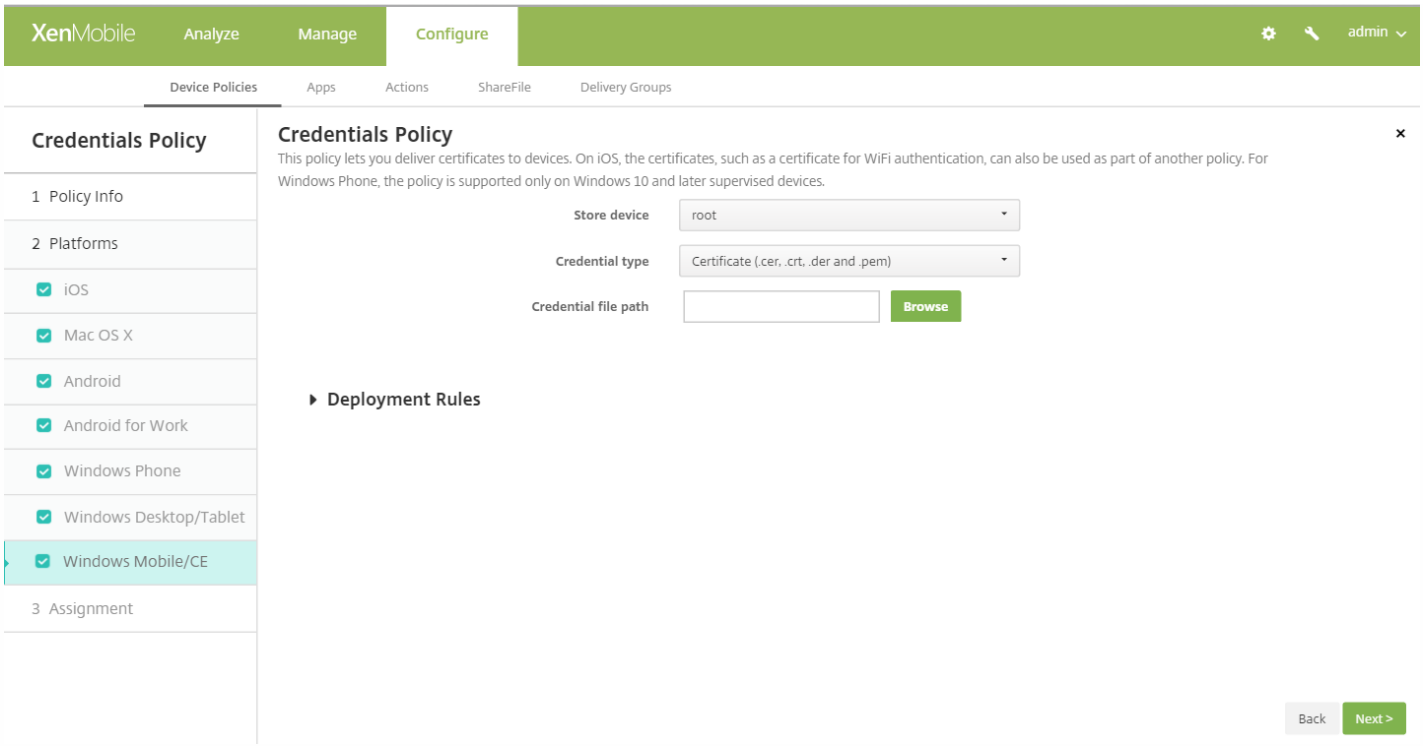
Configure los siguientes parámetros:

- **OSVersion**. En la lista, haga clic en **8.1** para Windows 8.1 o **10** para Windows 10. El valor predeterminado es **10**.

Configuración de Windows 10

Configuración de Windows 8,1

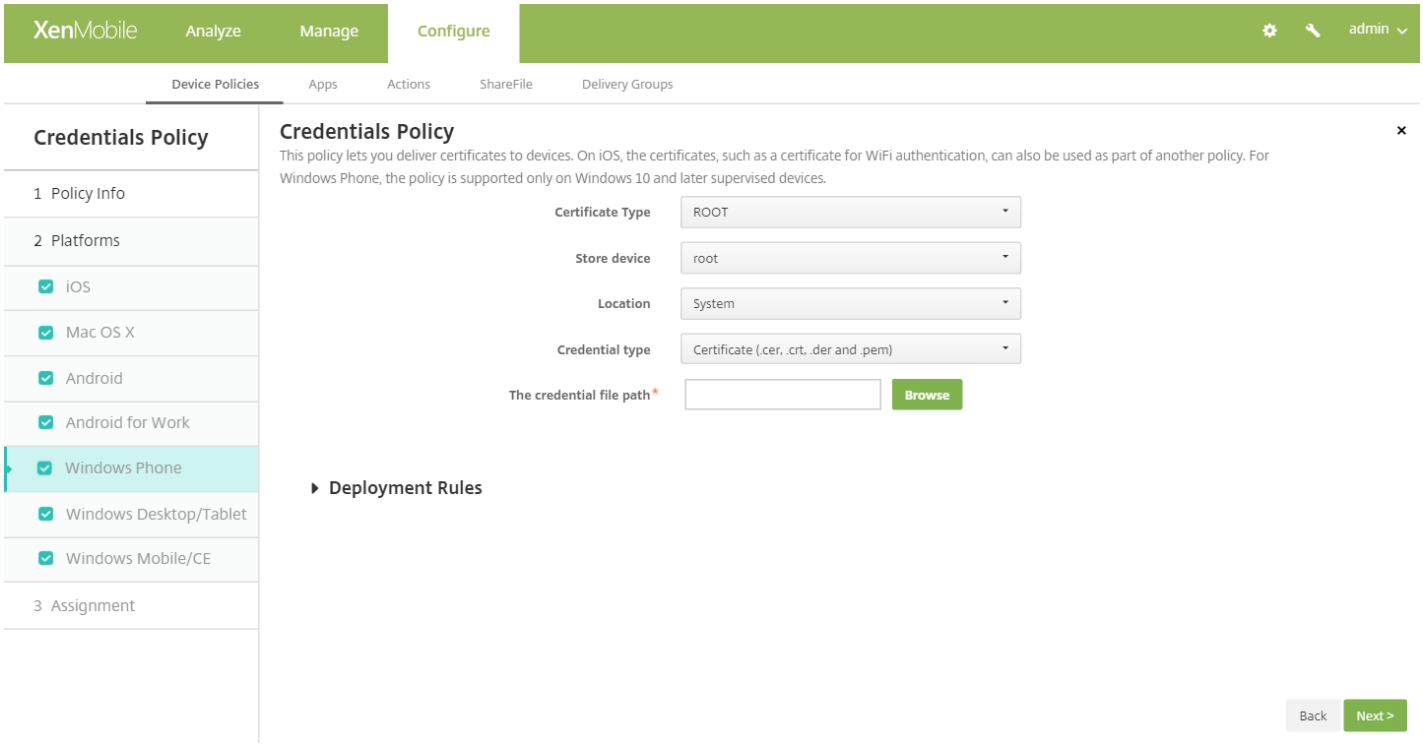
Configuración de los parámetros de Windows Mobile/CE



Configure los siguientes parámetros:

- **Store device**. En la lista, haga clic en la ubicación del almacén de certificados de la credencial. El valor predeterminado es **root**. Las opciones son:
  - **Privileged execution trust authorities**. Las aplicaciones firmadas con un certificado perteneciente a este almacén se ejecutarán con un nivel de confianza con privilegios.
  - **Unprivileged execution trust authorities**. Las aplicaciones firmadas con un certificado perteneciente a este almacén se ejecutarán con un nivel de confianza normal.
  - **SPC (Software Publisher Certificate)**. El Certificado de publicación de software (SPC) se usa para firmar archivos CAB.
  - **root**. Un almacén de certificado que contiene certificados raíz o autofirmados.
  - **CA**. Un almacén de certificados que contiene información de cifrado, incluidas las entidades de certificación intermedia.
  - **MY**. Un almacén de certificados que contiene los certificados personales del usuario final.
- **Credential type**. El certificado es el único tipo de credencial para dispositivos Windows Mobile/CE.
- **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.

Configuración de los parámetros de Windows Phone

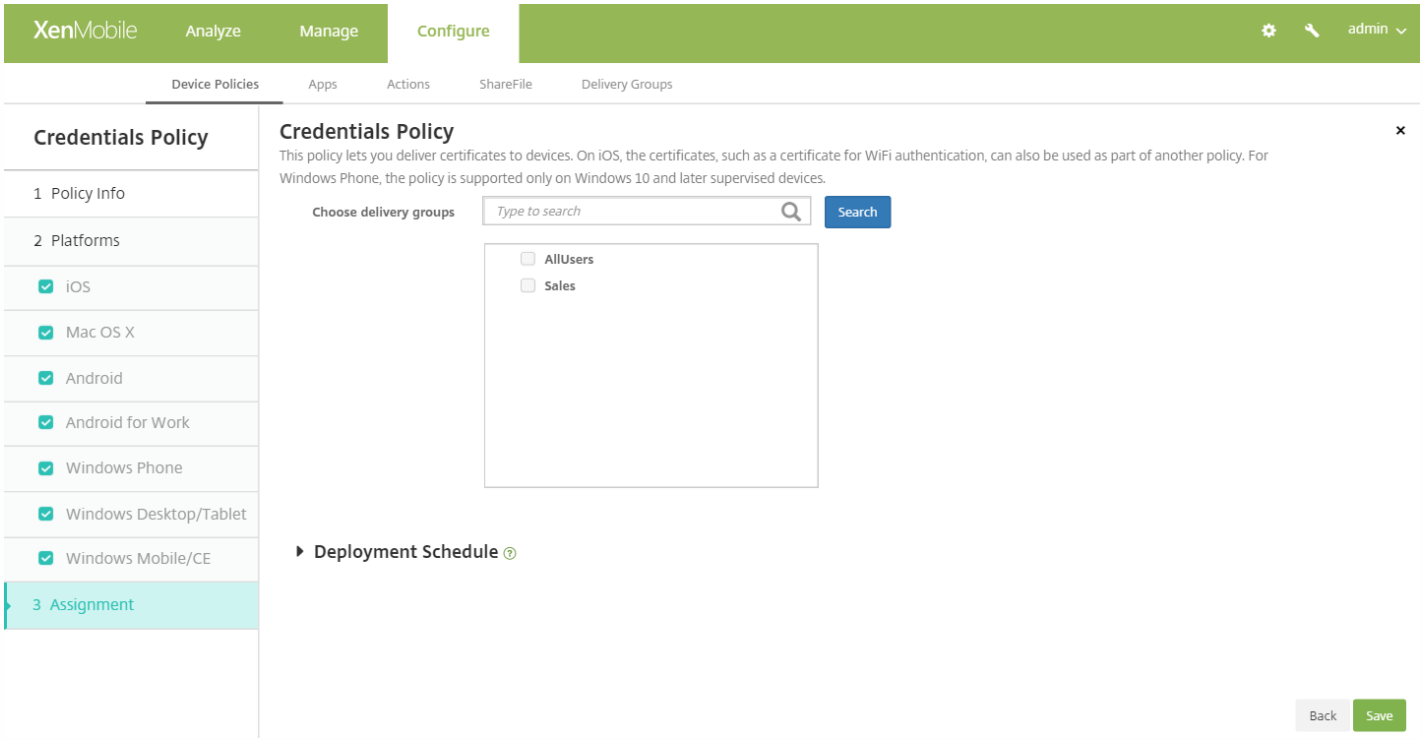


Configure los siguientes parámetros:

- **Certificate Type**. En la lista, haga clic en ROOT o CLIENT.
- Si hace clic en **ROOT**, 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**, el certificado se guarda en los almacenes de certificados de los usuarios.
  - **Location**. System es la única ubicación para teléfonos Windows.
  - **Credential type**. Certificate es el único tipo de credencial para teléfonos Windows.
  - **Credential file path**. Seleccione el archivo de certificado. Para ello, deberá hacer clic en **Browse** y, a continuación, ir a la ubicación del archivo.
- Si hace clic en **CLIENT**, configure los siguientes parámetros:
  - **Location**. **System** es la única ubicación para teléfonos Windows.
  - **Credential type**. **Keystore** es el único tipo de credencial para teléfonos Windows.
  - **Credential name**. Escriba el nombre de la credencial. Este campo es obligatorio.
  - **Credential file path**. Seleccione el archivo de certificado. Para ello, deberá hacer clic en Browse y, a continuación, ir a la ubicación del archivo.
  - **Password**. Escriba la contraseña asociada a la credencial. Este campo es obligatorio.

7. Configure las reglas de implementación.

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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 contenido XML personalizado

Jul 27, 2016

En XenMobile, puede crear sus propias directivas de contenido XML para personalizar las siguientes funciones en tabletas Windows y dispositivos de escritorio de Windows, Windows Phone y Windows Mobile/CE:

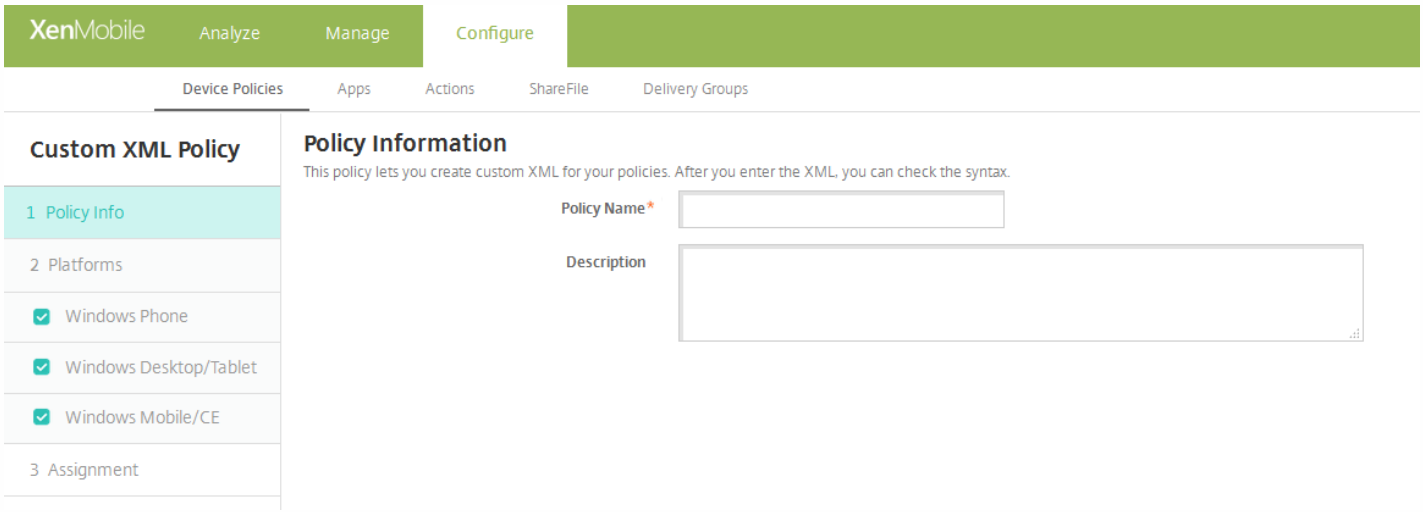
- El aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o inhabilitación de las funciones.
- La configuración de dispositivos, que incluye la capacidad para permitir a los usuarios cambiar la configuración y los parámetros de sus dispositivos.
- Las actualizaciones de software, 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 XML personalizada mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows. La creación de contenido XML personalizado con la API de OMA DM no se cubre en esta sección. 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**. Aparecerá el cuadro de diálogo **Add New Policy**.

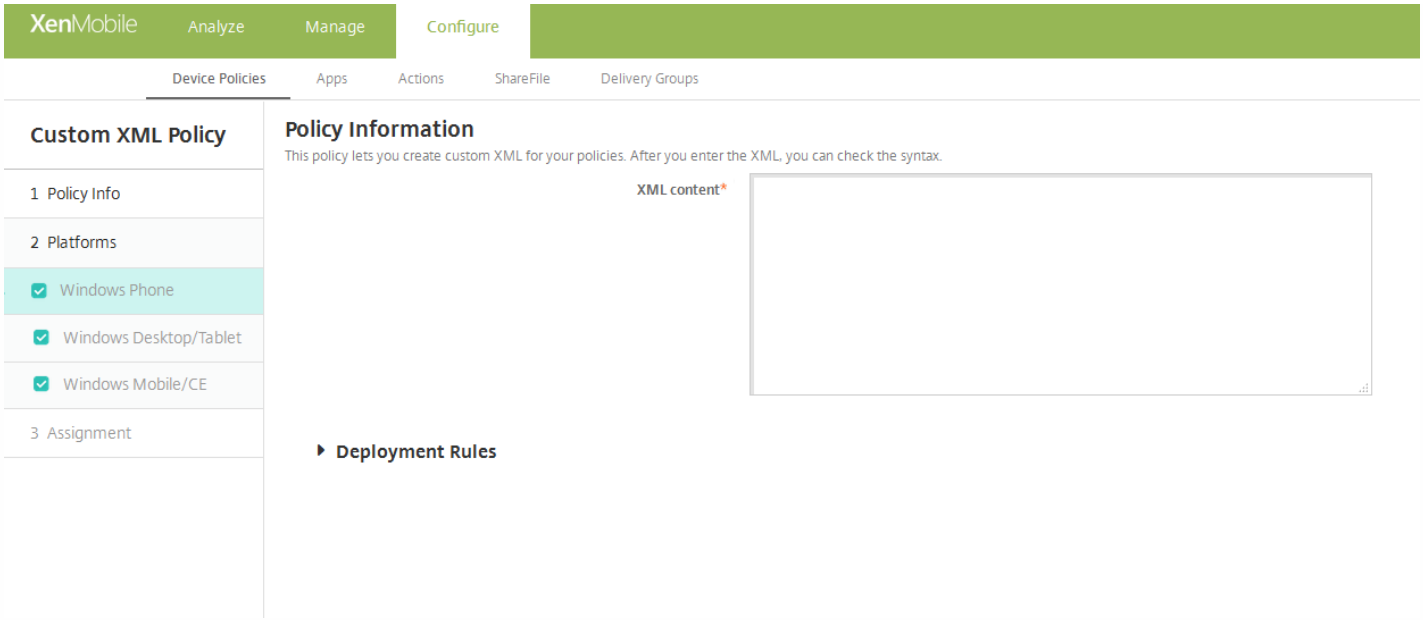
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Custom XML**. Aparecerá la página de información **Custom XML Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

7. Configure el siguiente parámetro para cada una de las plataformas seleccionadas:

- **XML content**. Escriba o copie y pegue el código XML personalizado que se va a agregar a la directiva.

8. Configure las reglas de implementación.

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**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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 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**.

Directiva de eliminación de archivos y carpetas

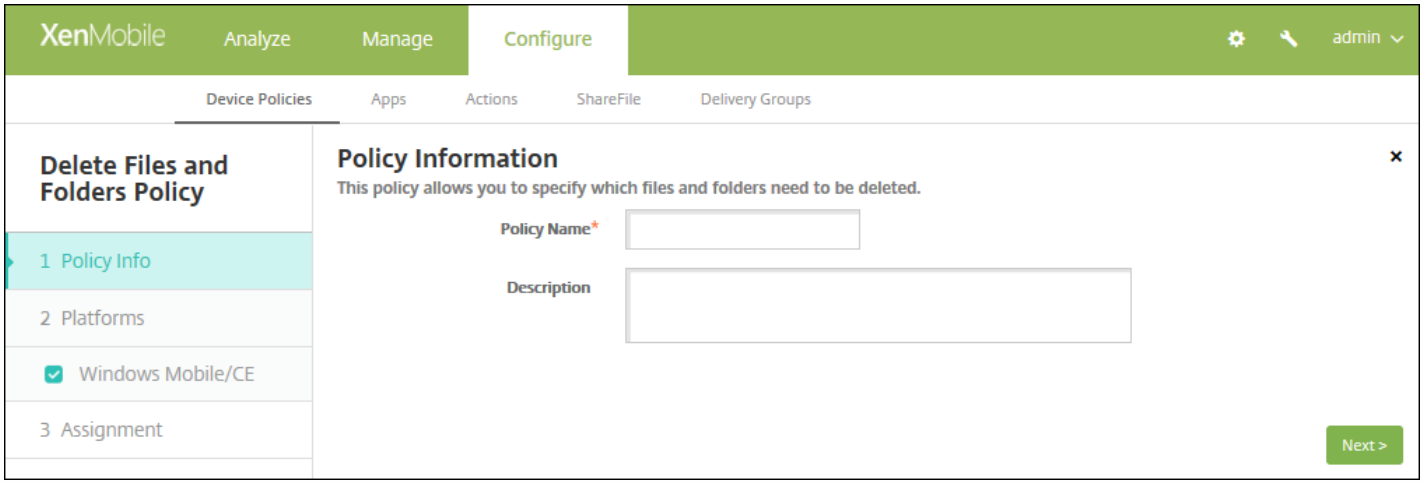
Jul 27, 2016

En XenMobile, puede crear una directiva para eliminar archivos o carpetas específicas de los dispositivos Windows Mobile/CE.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

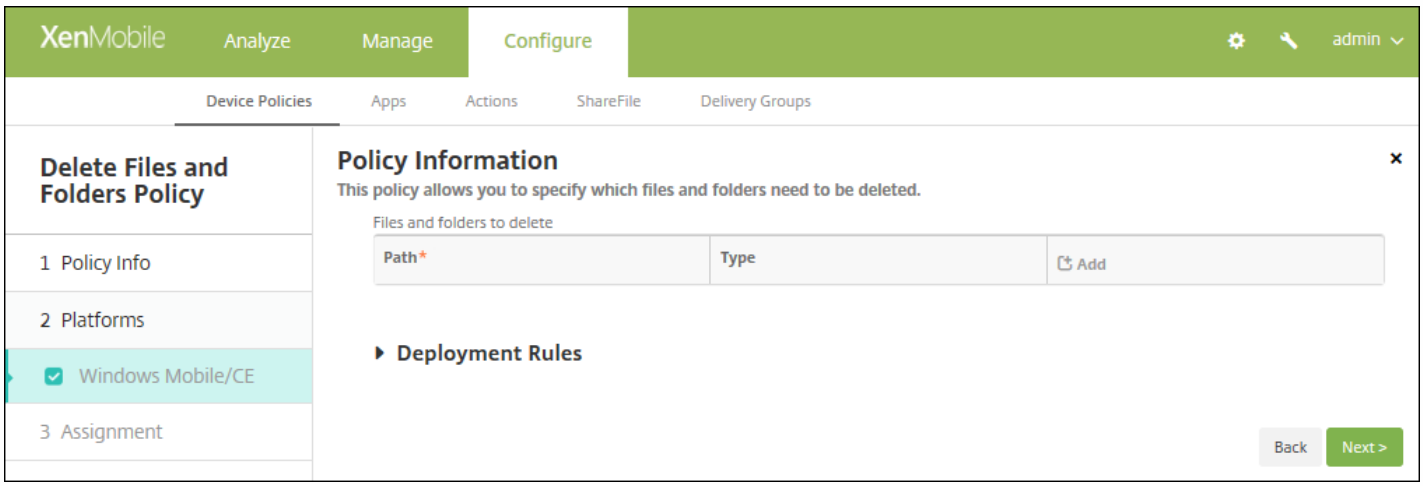
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Delete Files and Folders**. Aparecerá la página de información **Delete Files and Folders Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



6. Configure los siguientes parámetros:

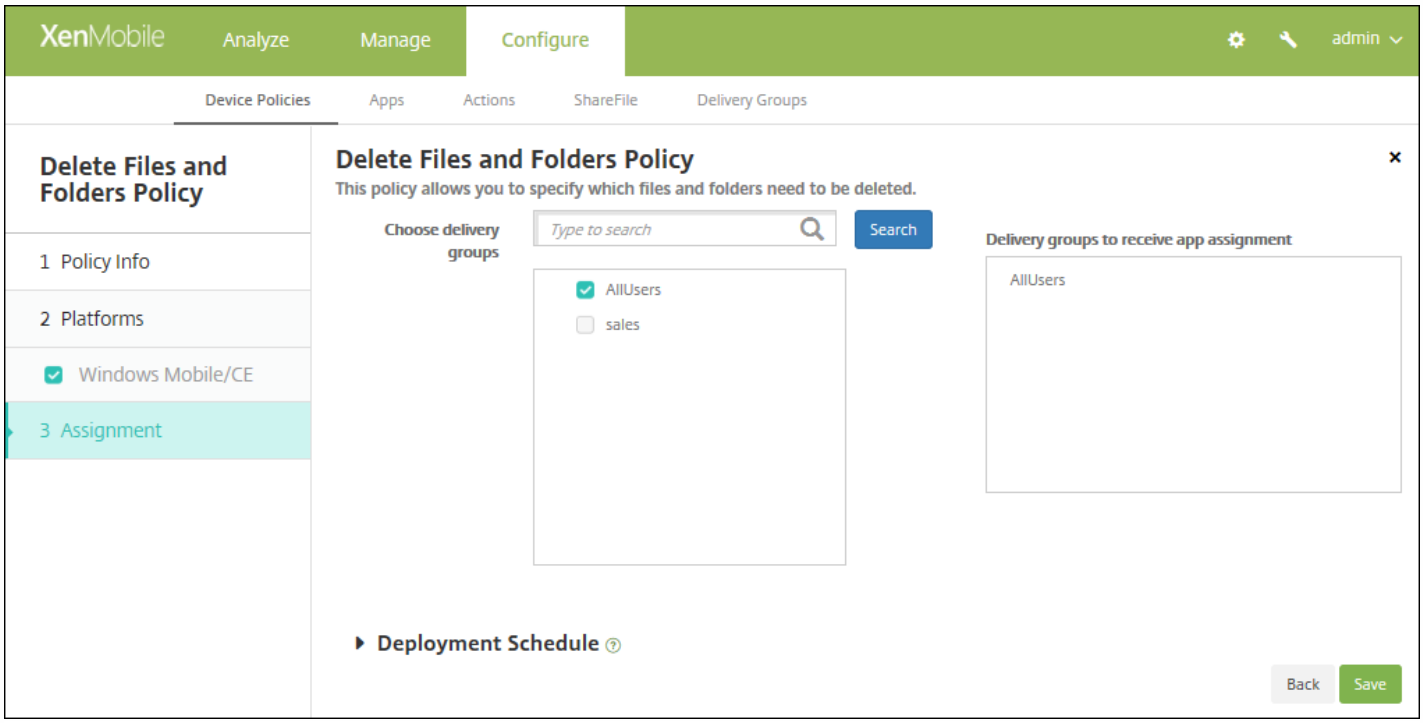
- **Files and folders to delete**. Para cada archivo o carpeta que quiera eliminar, haga clic en Add y lleve a cabo lo siguiente:
  - **Path**. Escriba la ruta al archivo o carpeta.
  - **Type**. En la lista, haga clic en File o Folder. El valor predeterminado es File.
  - Haga clic en **Save** para guardar el archivo o carpeta, o bien haga clic en **Cancel** para no guardarlos.

    Nota: Para eliminar un elemento 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 elemento 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. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Delete Files and Folders 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

- 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**.
- 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.
- 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**.

Directiva de eliminación de valores y claves de Registro

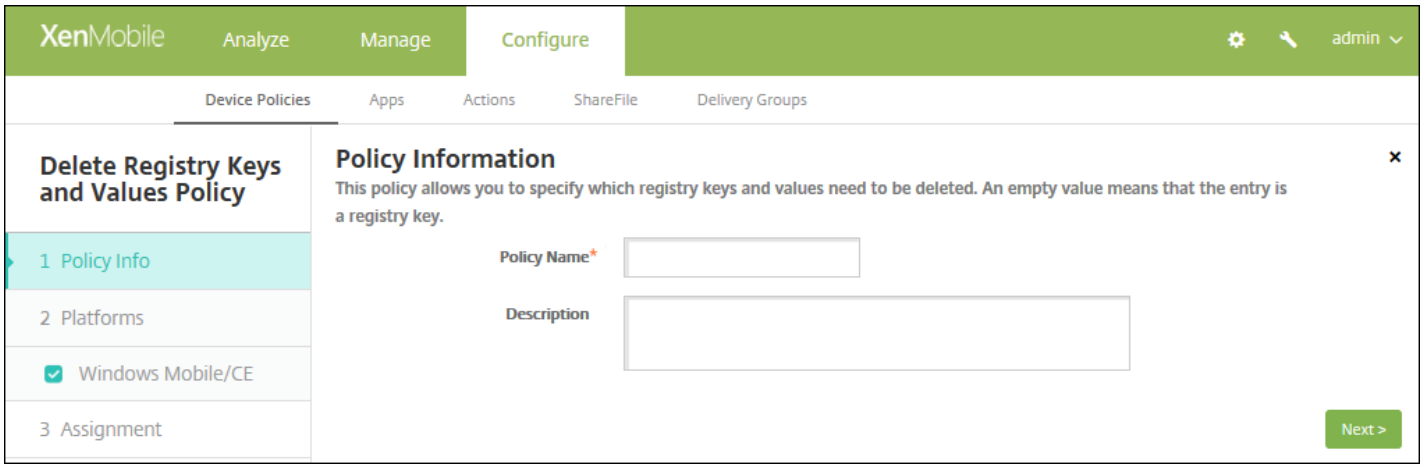
Jul 27, 2016

En XenMobile, puede crear una directiva para eliminar de los dispositivos Windows Mobile/CE claves y valores específicos del Registro.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

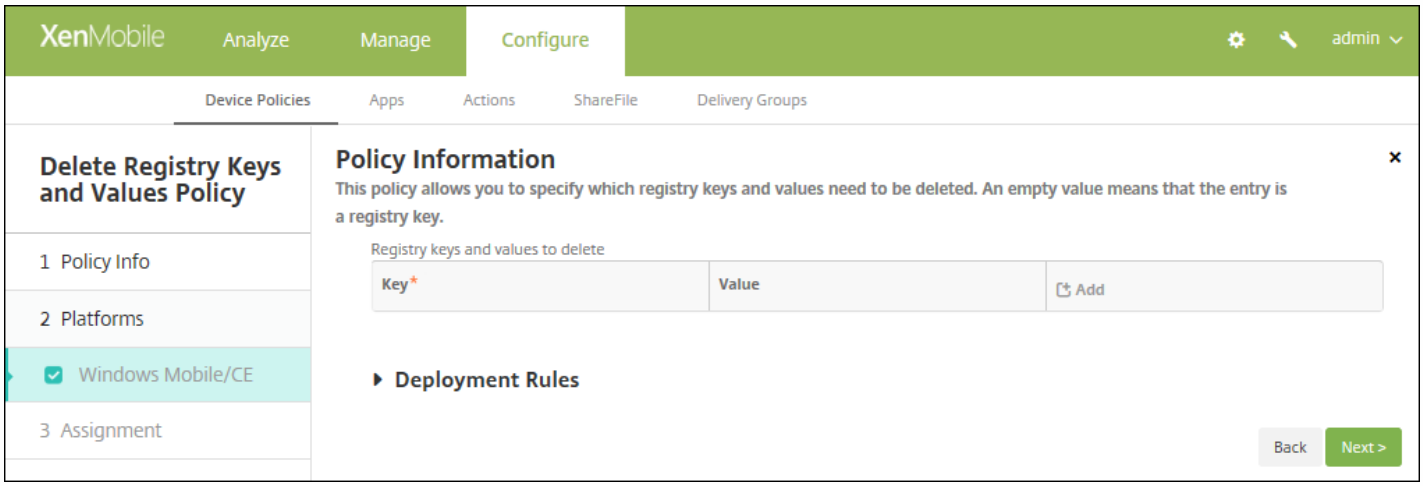
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Delete Registry Keys and Values**. Aparecerá la página de información **Delete Registry Keys and Values Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



6. Configure los siguientes parámetros:

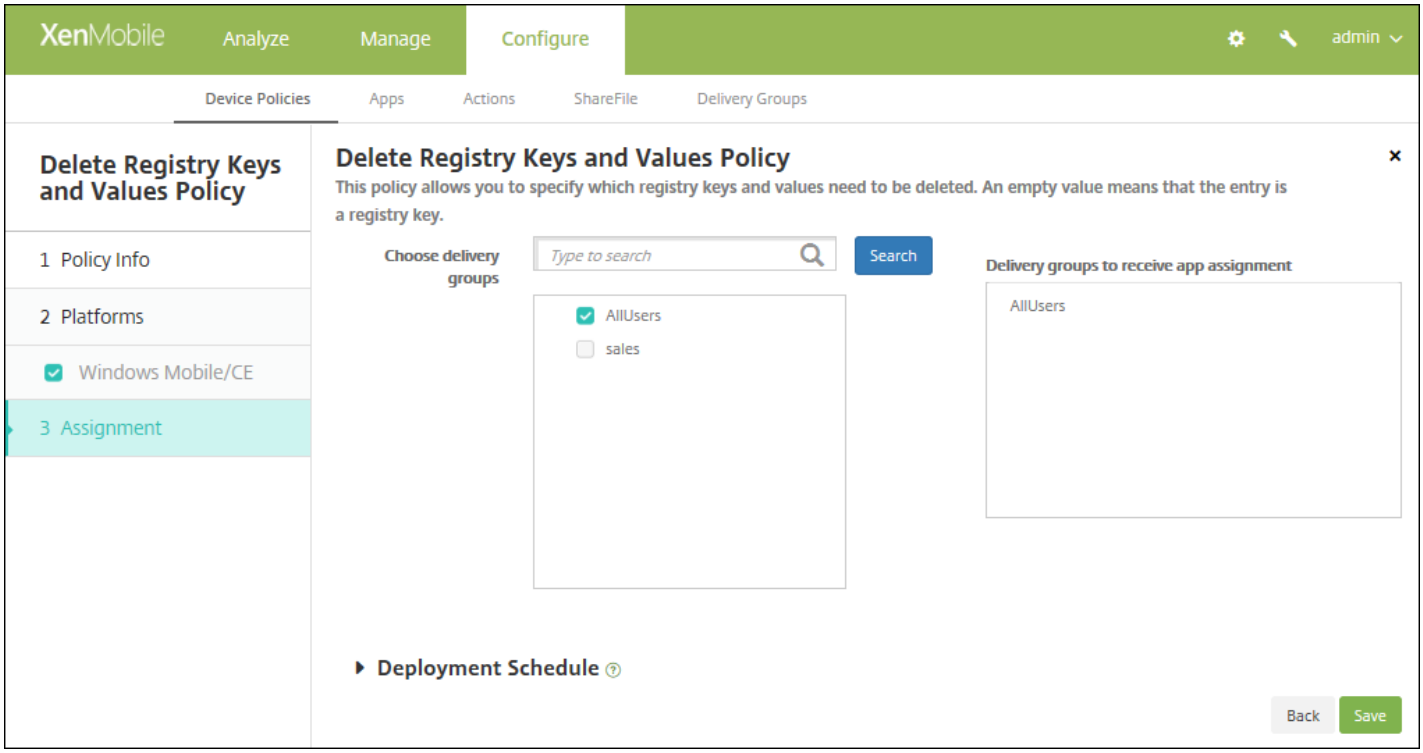
- **Registry keys and values to delete**. Para cada valor y clave del Registro que quiera eliminar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Key**. Escriba la ruta de la clave del Registro. Este campo es obligatorio. La ruta de la clave del Registro debe empezar por HKEY_CLASSES_ROOT\, HKEY_CURRENT_USER\, HKEY_LOCAL_MACHINE\ o HKEY_USERS\.
  - **Value**. Escriba el nombre del valor que se va a eliminar, o bien deje el campo en blanco para eliminar toda la clave del Registro.
  - Haga clic en **Save** para guardar la clave y el valor, o bien haga clic en **Cancel** para no guardarlos.

    Nota: Para eliminar un elemento 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 elemento 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. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Delete Registry Keys and Values 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de atestación de estado de dispositivos

Jul 27, 2016

En XenMobile, puede requerir que los dispositivos Windows 10 informen de su estado. Así, estos dispositivos enviarán datos concretos e información sobre tiempos de ejecución al servicio Health Attestation Service (HAS) para su posterior análisis. El servicio HAS crea y devuelve un certificado de atestación de estado que el dispositivo envía a XenMobile. Cuando XenMobile recibe el certificado de atestación de estado, según el contenido de este, puede implementar las acciones automatizadas que haya configurado previamente.

Los datos que se comprueban en el servicio HAS son:

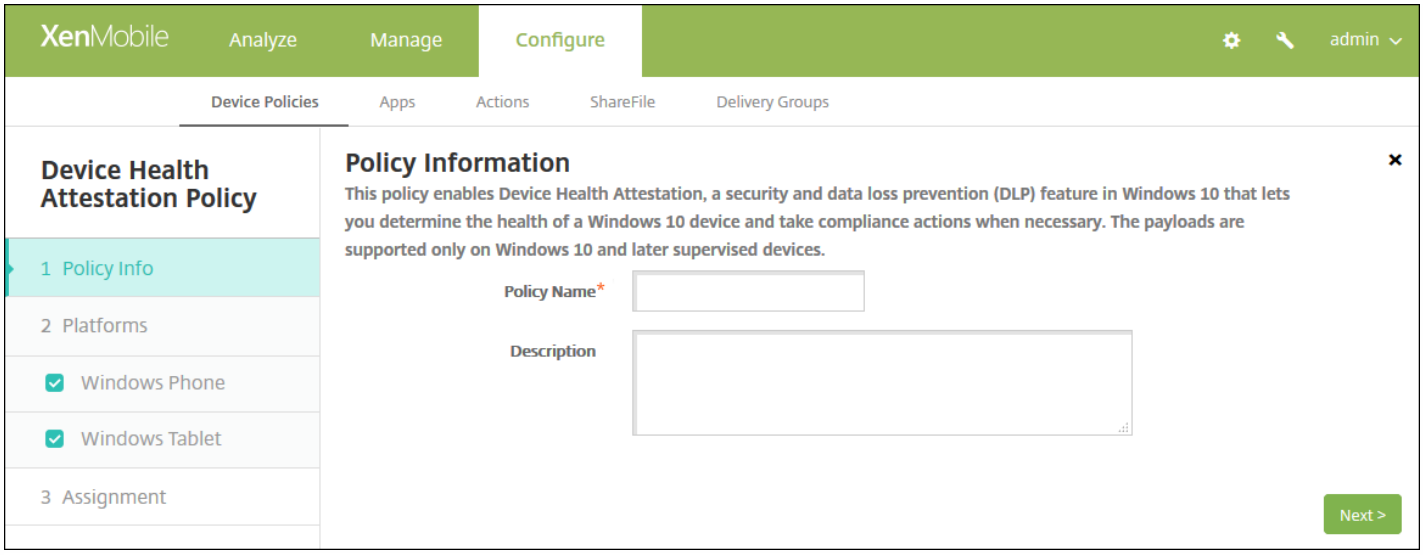
- AIKPresent
- BitLockerStatus
- BootDebuggingEnabled
- BootManagerRevListVersion
- CodeIntegrityEnabled
- CodeIntegrityRevListVersion
- DEPPolicy
- ELAMDriverLoaded
- IssuedAt
- KernelDebuggingEnabled
- PCR
- ResetCount
- RestartCount
- SafeModeEnabled
- SBCPHash
- SecureBootEnabled
- TestSigningEnabled
- VSMEnabled
- WinPEEnabled

Para obtener más información, consulte la página HealthAttestation CSP de Microsoft.

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 **Custom**, haga clic en **Device Health Attestation policy**. Aparecerá la página de información **Device Health Attestation policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

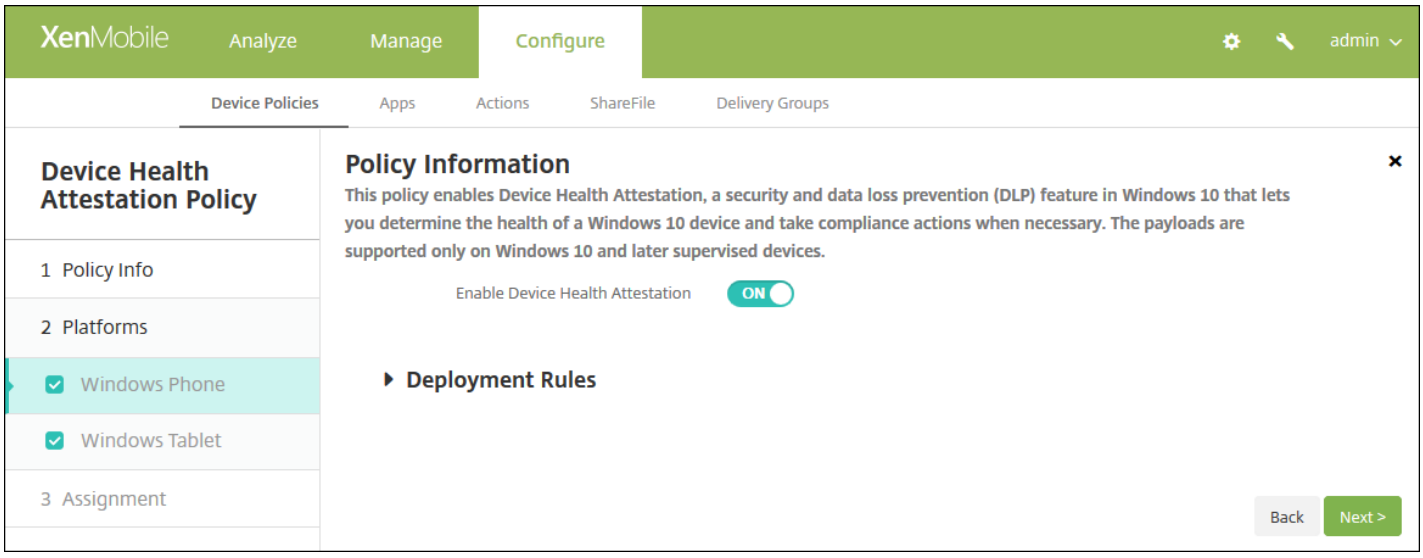
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de Windows Phone y de tabletas Windows



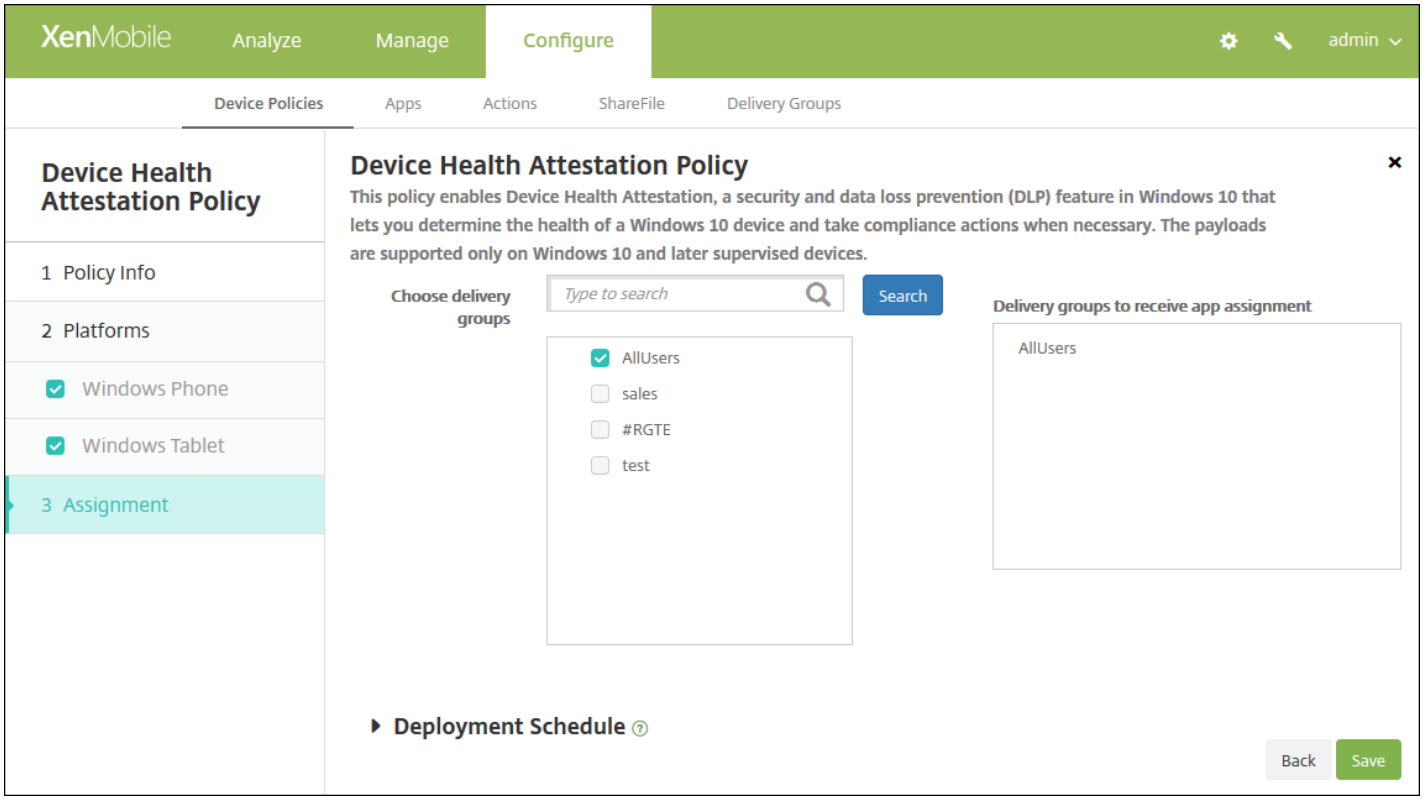
Configure este parámetro para cada plataforma seleccionada:

- **Enable Device Health Attestation Policy**. Seleccione si se debe requerir la atestación de estado de los dispositivos. El

valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de la directiva **Device Health Attestation**.



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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de nombres de dispositivos

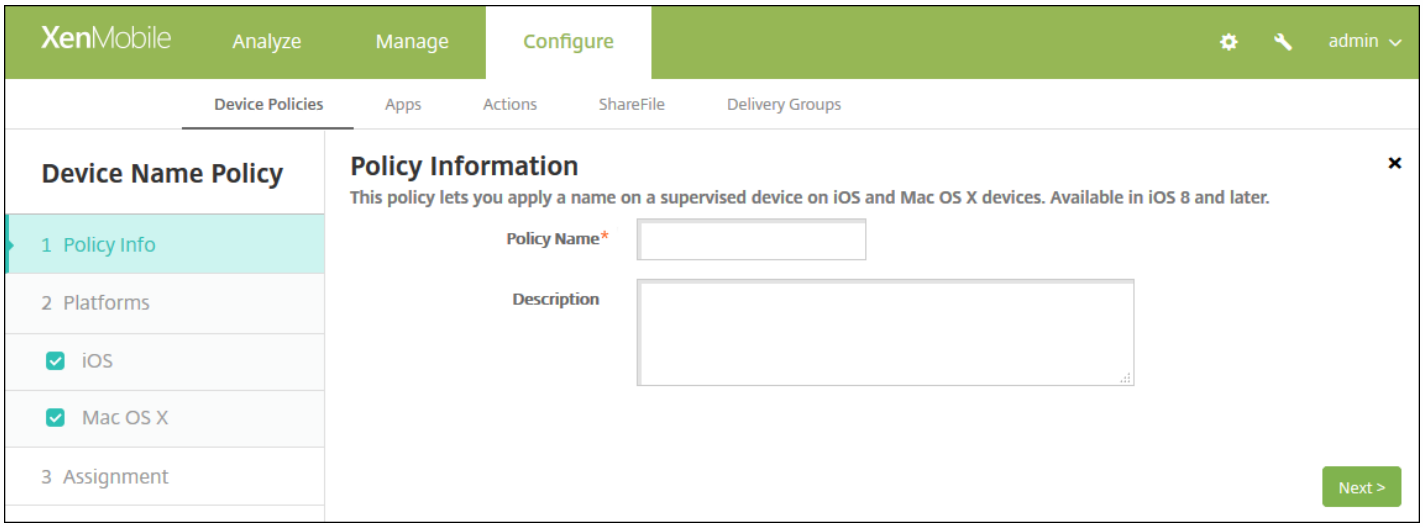
Jul 27, 2016

Puede definir nombres para dispositivos iOS y Mac OS X de forma que pueda reconocerlos fácilmente. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Por ejemplo, para establecer el número de serie del dispositivo como nombre, puede utilizar ${device.serialnumber}. Para establecer el nombre del dispositivo como una combinación del nombre de usuario y el dominio, puede utilizar ${user.username}@ejemplo.com. Consulte Macros en XenMobile para obtener más información acerca de las macros.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá la página **Add a New Policy**.

3. Expanda **More** y, en **End user**, haga clic en **Device name**. Aparecerá la página de información **Device Name Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

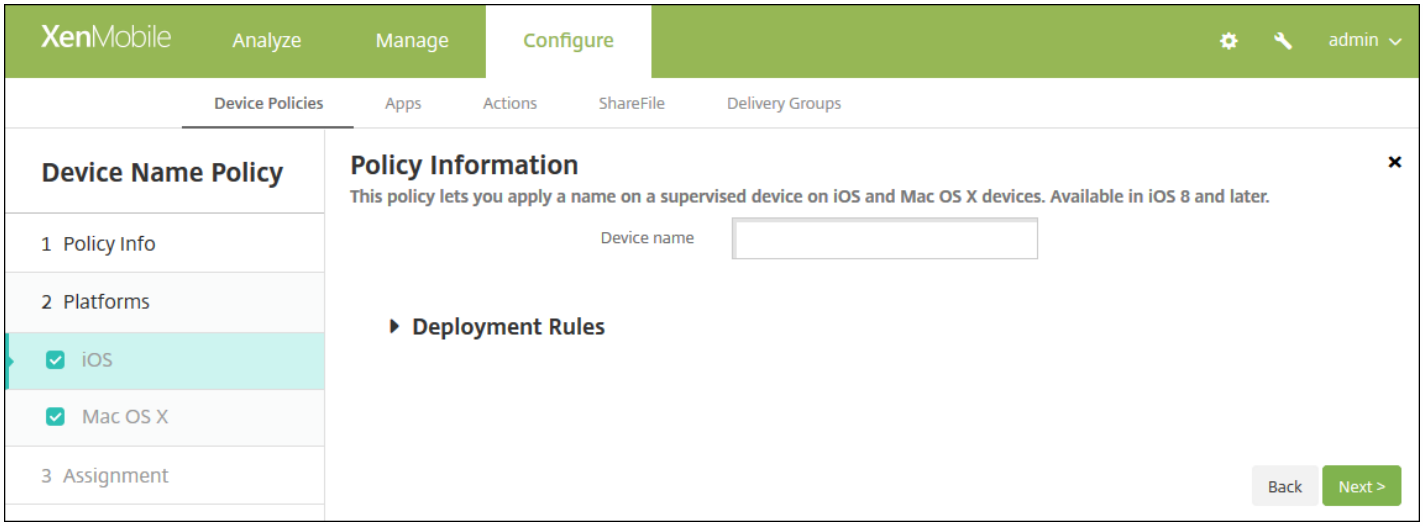
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS y Mac OS X

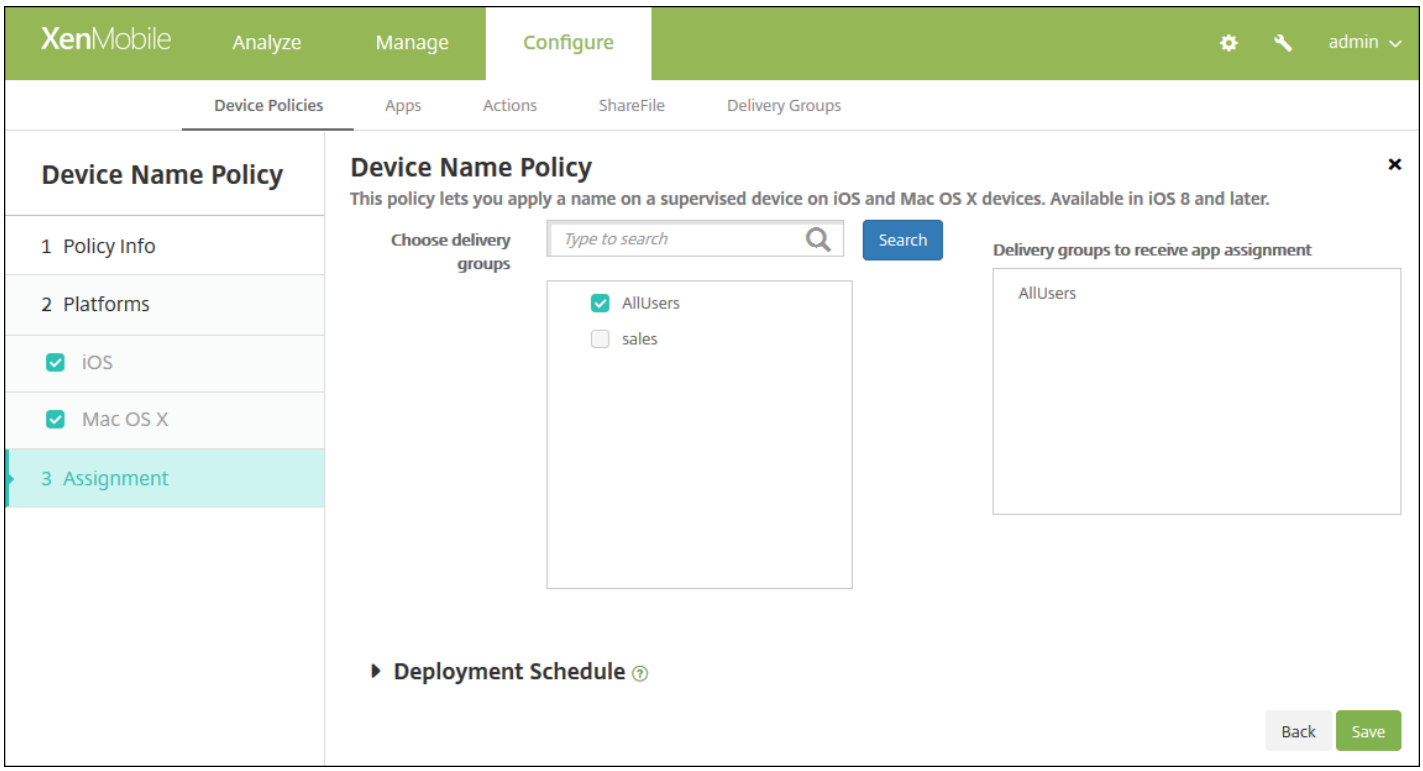


Configure este parámetro para las plataformas que elija:

- **Device name**. Escriba la macro, una combinación de ellas o una combinación de macros y texto para darle a cada dispositivo un nombre único. Por ejemplo, use ${device.serialnumber} para establecer el número de serie de cada dispositivo como su nombre, o bien utilice ${device.serialnumber} ${user.username} para incluir el nombre de usuario en el nombre del dispositivo.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Device Name 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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.

Directiva Enterprise Hub para dispositivos

Jul 27, 2016

Una directiva Enterprise Hub para dispositivos Windows Phone permite distribuir aplicaciones a través del almacén Enterprise Hub de la empresa.

Antes de crear la directiva, necesita lo siguiente:

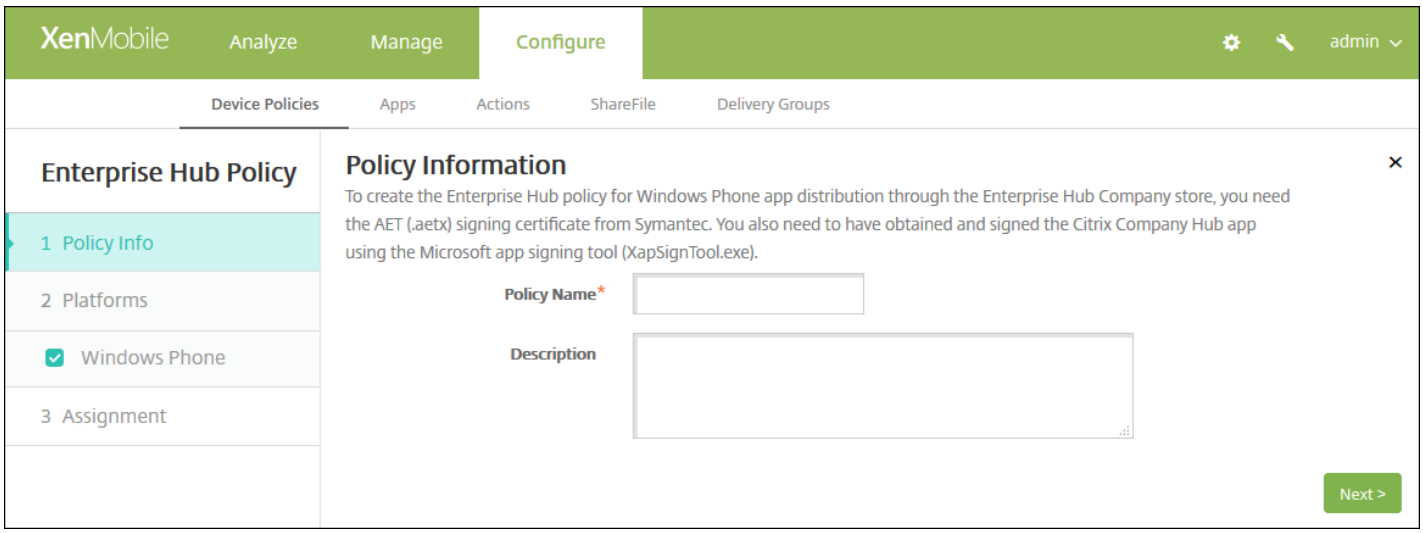
- Un certificado de firma AET (.aetx) de Symantec
- La aplicación Citrix Company Hub firmada mediante la herramienta de firma de aplicaciones de Microsoft (XapSignTool.exe)

Nota: XenMobile solo admite una directiva Enterprise Hub por modo de Windows Phone Worx Home. Por ejemplo, para cargar Windows Phone Worx Home en XenMobile Enterprise Edition, no debe crear varias directivas Enterprise Hub con versiones diferentes de Worx Home para XenMobile Enterprise Edition. Puede implementar la directiva Enterprise Hub inicial durante la inscripción del dispositivo.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

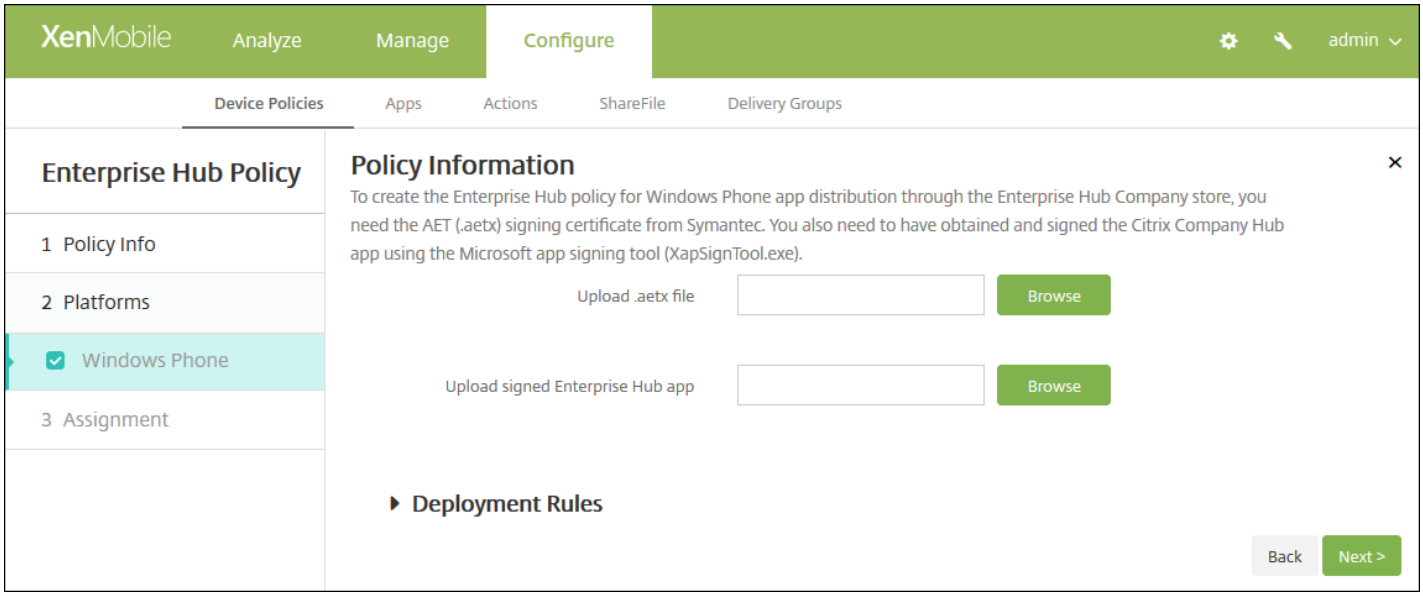
3. Haga clic en **More** y, en **XenMobile agent**, haga clic en **Enterprise Hub**. Aparecerá la página **Enterprise Hub Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de la plataforma **Windows Phone**.

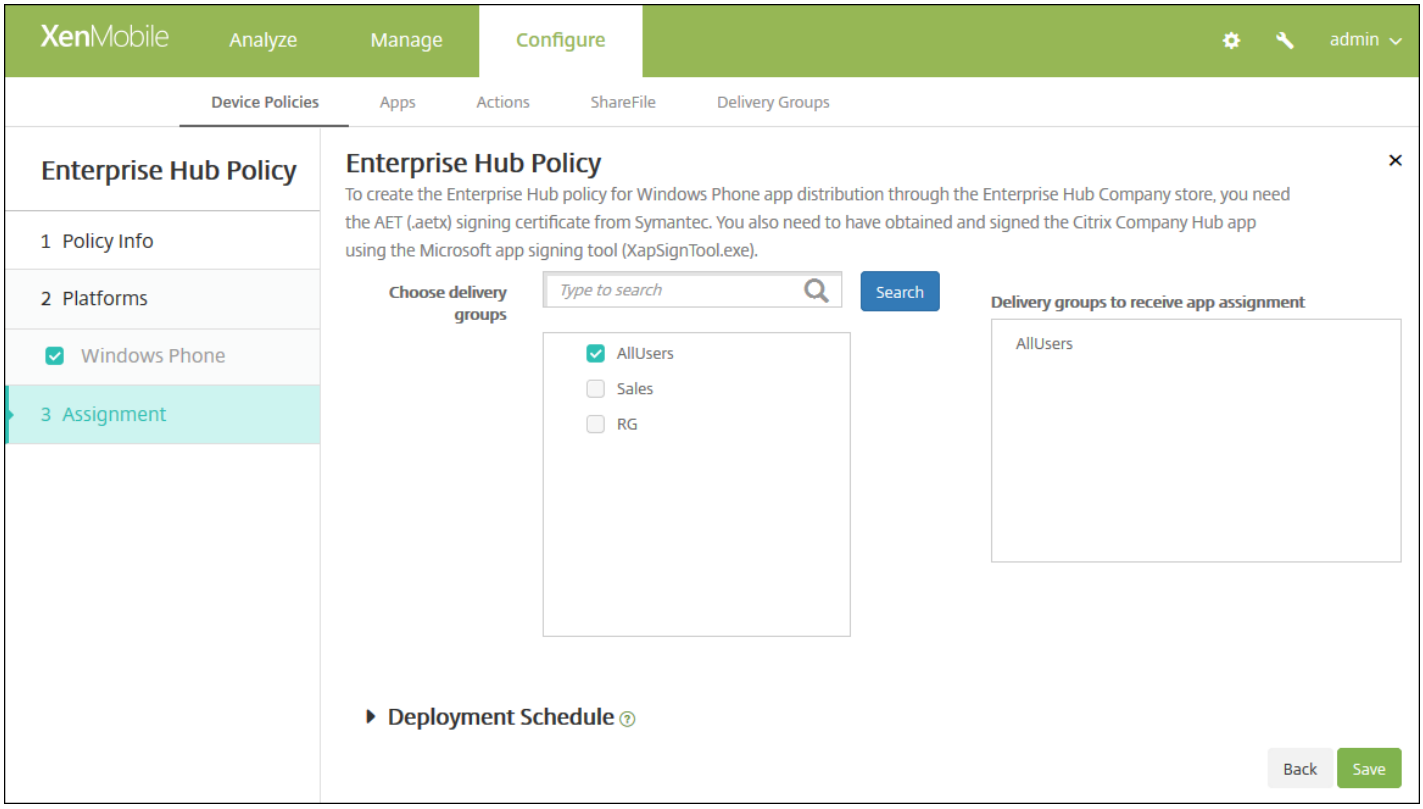


6. Configure los siguientes parámetros:

- **Upload .aetx file**. Seleccione el archivo AETX. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Upload signed Enterprise Hub app**. Seleccione la aplicación Enterprise Hub. Para ello, haga clic en **Browse** y vaya a la ubicación de la aplicación.

7. Configure las reglas de implementación.

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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 archivos

Jul 27, 2016

Puede agregar archivos de script a XenMobile para realizar algunas funciones para los usuarios. También puede agregar documentos a los que quiera que los usuarios de los dispositivos Android puedan acceder desde sus dispositivos. Cuando agregue el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo. Por ejemplo, si quiere que los usuarios de Android reciban un documento de empresa o archivo PDF, puede implementar el archivo en el dispositivo y permitir que los usuarios sepan dónde se encuentra el archivo.

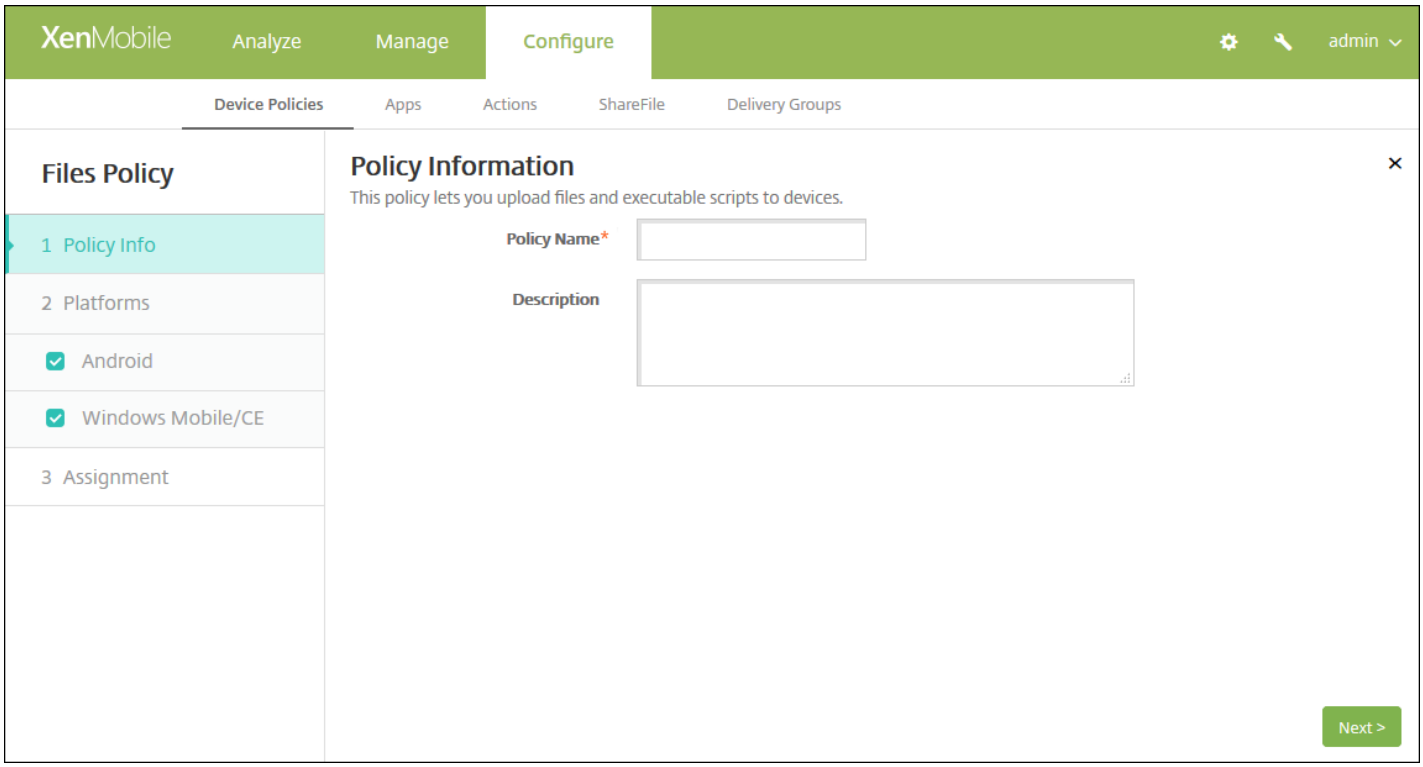
Puede agregar los siguientes tipos de archivo con esta directiva:

- Archivos de texto (XML, HTML, PY, etc.)
- Otros archivos, como documentos, imágenes, hojas de cálculo o presentaciones
- Solo para Windows Mobile y Windows CE: archivos de script creados con MortScript

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy** .

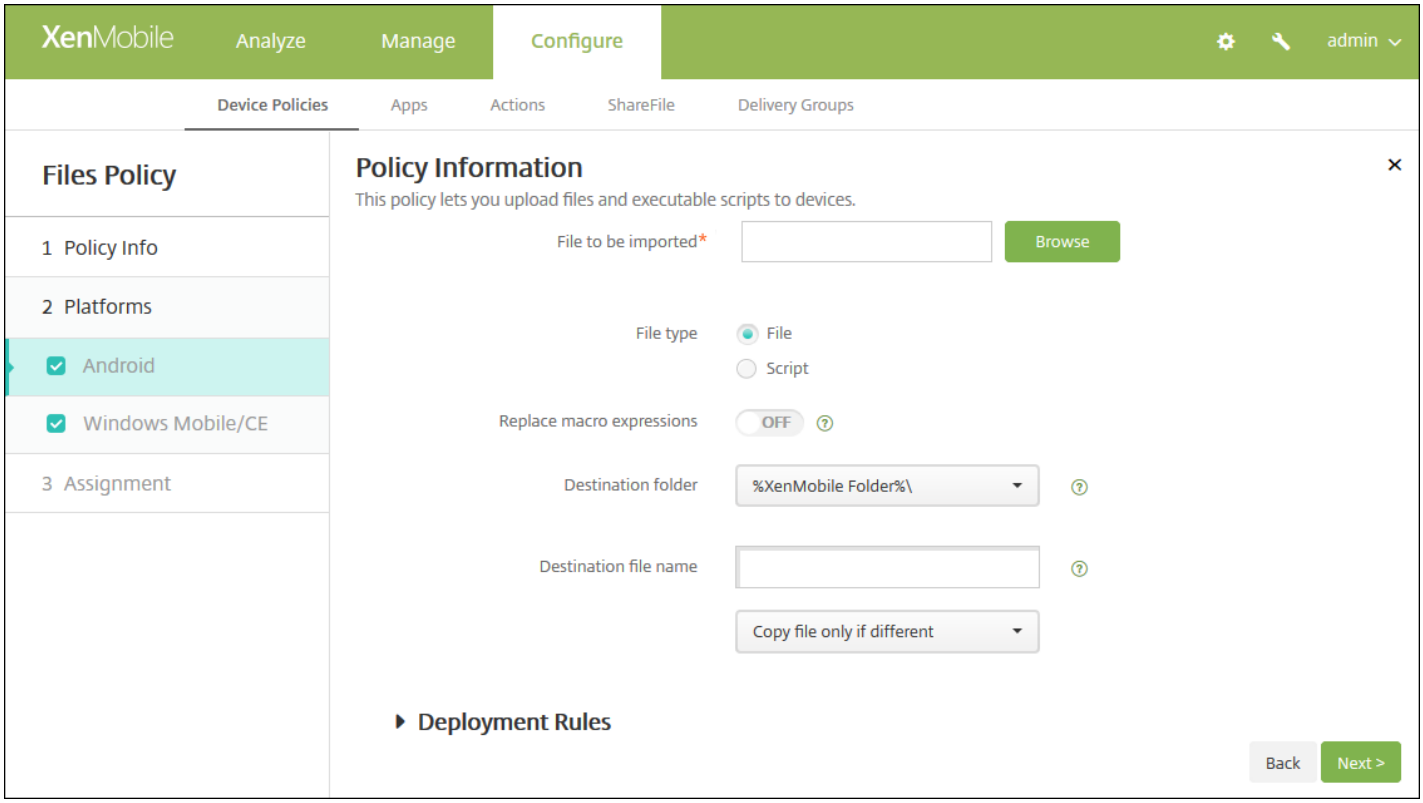
3. Expanda **More** y luego, en **Apps**, haga clic en **Files**. Aparecerá la página de información **Files Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

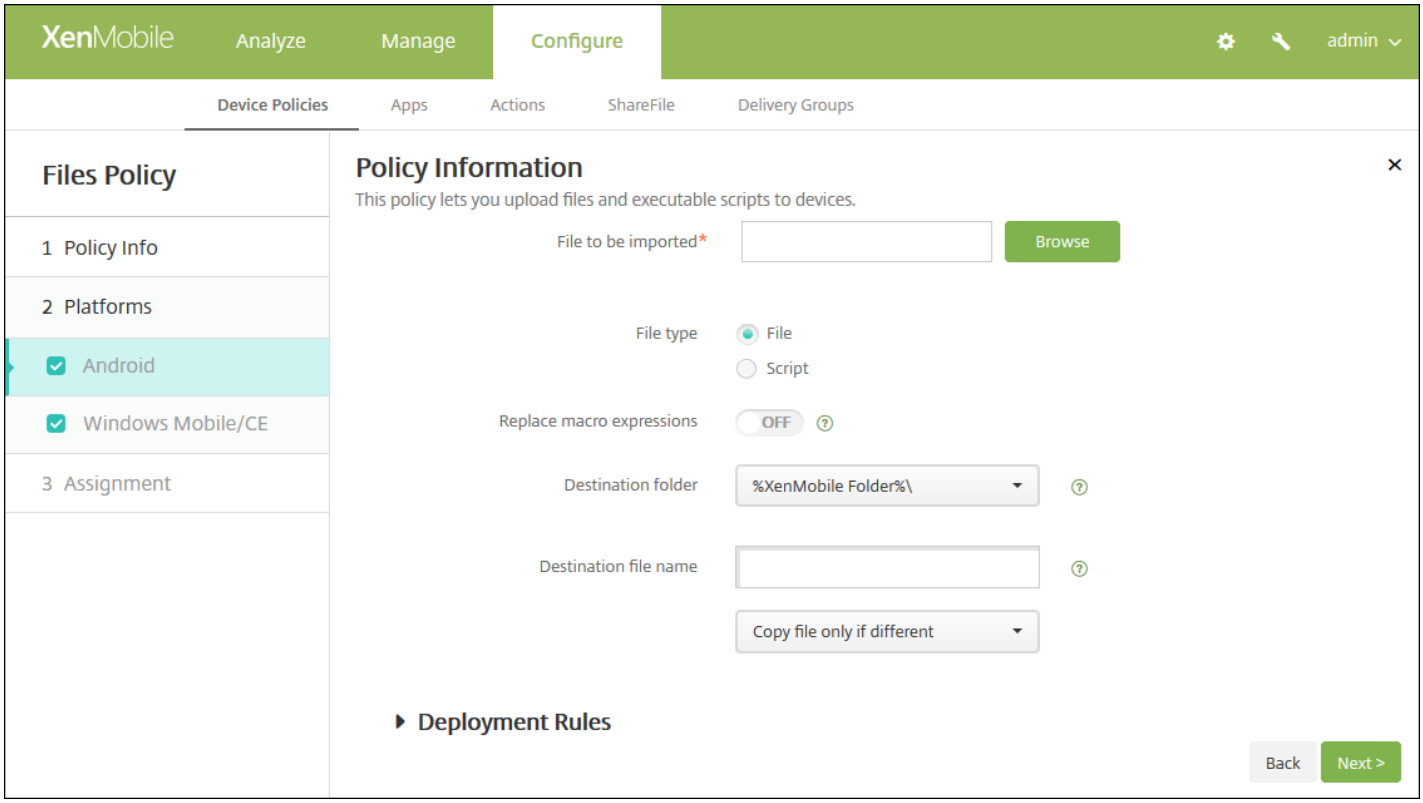
5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

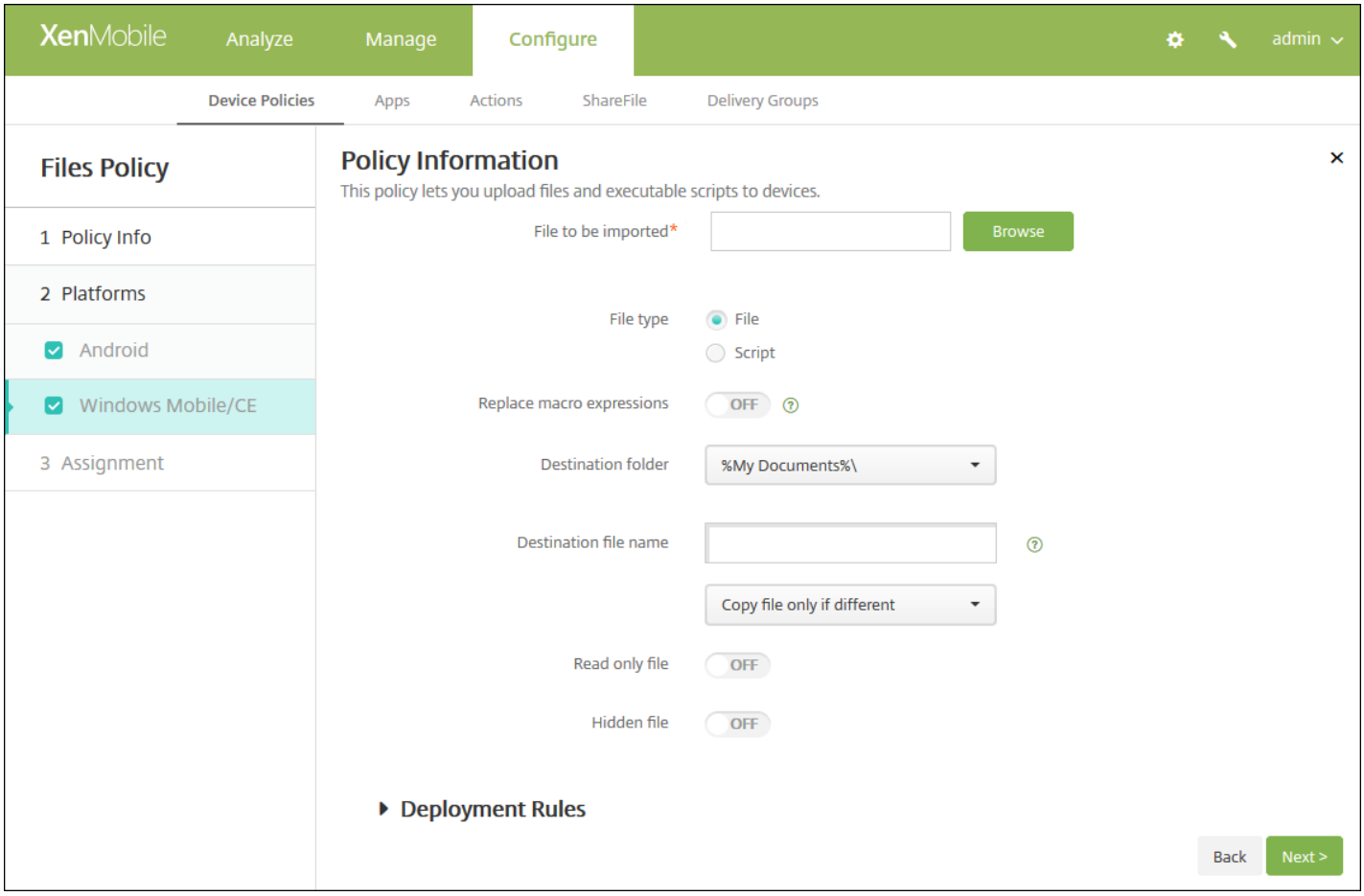
Configuración de los parámetros de Android



Configure los siguientes parámetros:

- **File to be imported**. Seleccione el archivo a importar; para ello, haga clic en Browse y, a continuación, vaya a la ubicación del archivo.
- **File type**. Seleccione **File** o **Script**. Si selecciona **Script**, aparecerá la opción **Execute immediately**. Seleccione si quiere que el script se ejecute tan pronto como el archivo se cargue. El valor predeterminado es **OFF**.
- **Replace macro expressions**: Seleccione si quiere reemplazar nombres de token de macro en un script con una propiedad de usuario o de dispositivo. El valor predeterminado es **OFF**.
- **Destination folder**. En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Add new** para elegir una ubicación de archivo no incluida en la lista. Además, puede usar las macros %XenMobile Folder%\ o %Flash Storage%\ como inicio del identificador de ruta.
- **Destination file name**: Si lo desea, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copy file only if different**. Seleccione en la lista si quiere copiar el archivo cuando sea diferente del archivo existente. La opción predeterminada es copiar el archivo solo si es diferente.

Configuración de los parámetros de Windows Mobile/CE



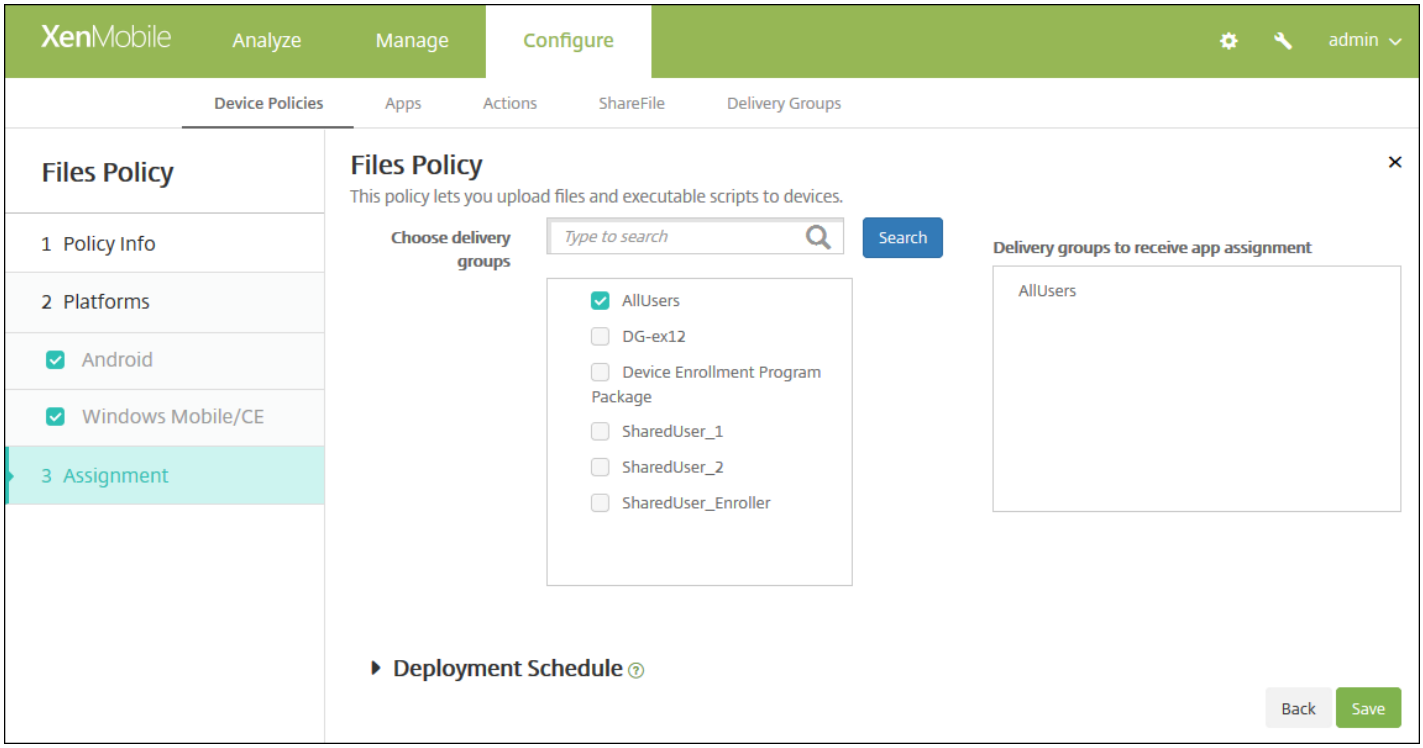
Configure los siguientes parámetros:

- **File to be imported**. Seleccione el archivo a importar; para ello, haga clic en Browse y, a continuación, vaya a la ubicación del archivo.
- **File type**. Seleccione **File** o **Script**. Si selecciona **Script**, aparecerá la opción **Execute immediately**. Seleccione si quiere que el script se ejecute tan pronto como el archivo se cargue. El valor predeterminado es **OFF**.
- **Replace macro expressions**: Seleccione si quiere reemplazar nombres de token de macro en un script con una propiedad de usuario o de dispositivo. El valor predeterminado es **OFF**.
- **Destination folder**. En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Add new** para elegir una ubicación de archivo no incluida en la lista. Además, puede utilizar cualquiera de las siguientes macros como inicio del identificador de ruta:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**: Si lo desea, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copy file only if different**. Seleccione en la lista si quiere copiar el archivo cuando sea diferente del archivo existente. La opción predeterminada es copiar el archivo solo si es diferente.
- **Read only file**. Seleccione si el archivo será de solo lectura. El valor predeterminado es **OFF**.
- **Hidden file**. Seleccione esta opción si no quiere que el archivo se muestre en la lista de archivos. El valor predeterminado

es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Files 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 a iOS.

11. Haga clic en **Save** para guardar la directiva.

Directiva de fuentes

Jul 27, 2016

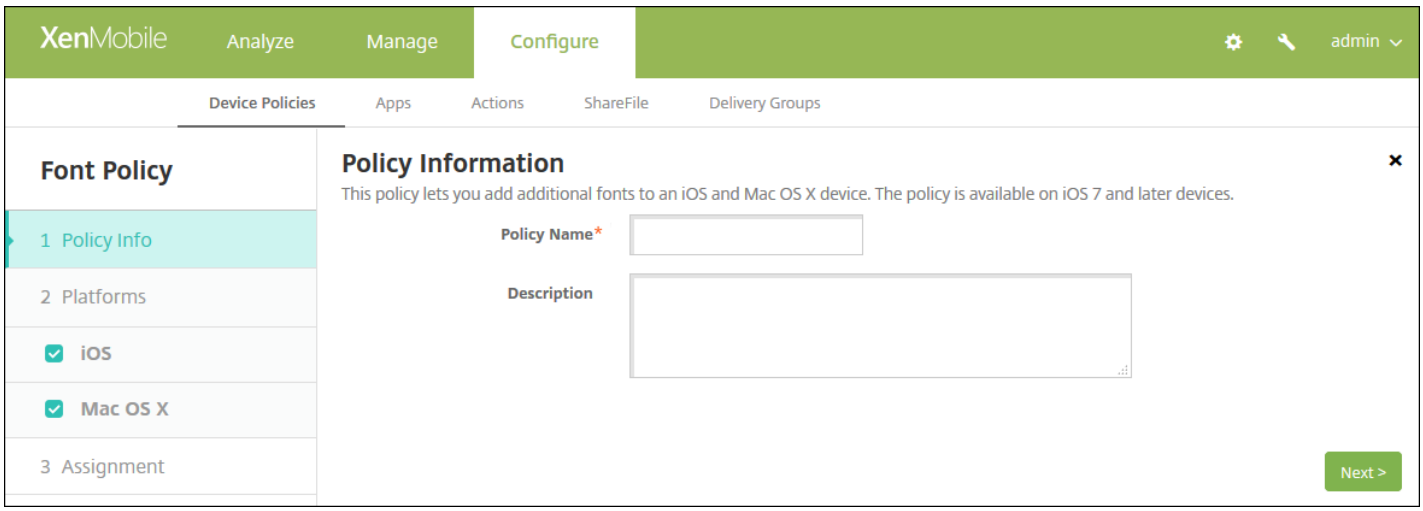
En XenMobile, puede agregar una directiva de dispositivos para agregar fuentes de texto adicionales a los dispositivos iOS y Mac OS X de los usuarios. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.oft). No se admiten las colecciones de fuentes (.ttc o .otc).

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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **More** y, en **End user**, haga clic en **Font**. Aparecerá la página **Font Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

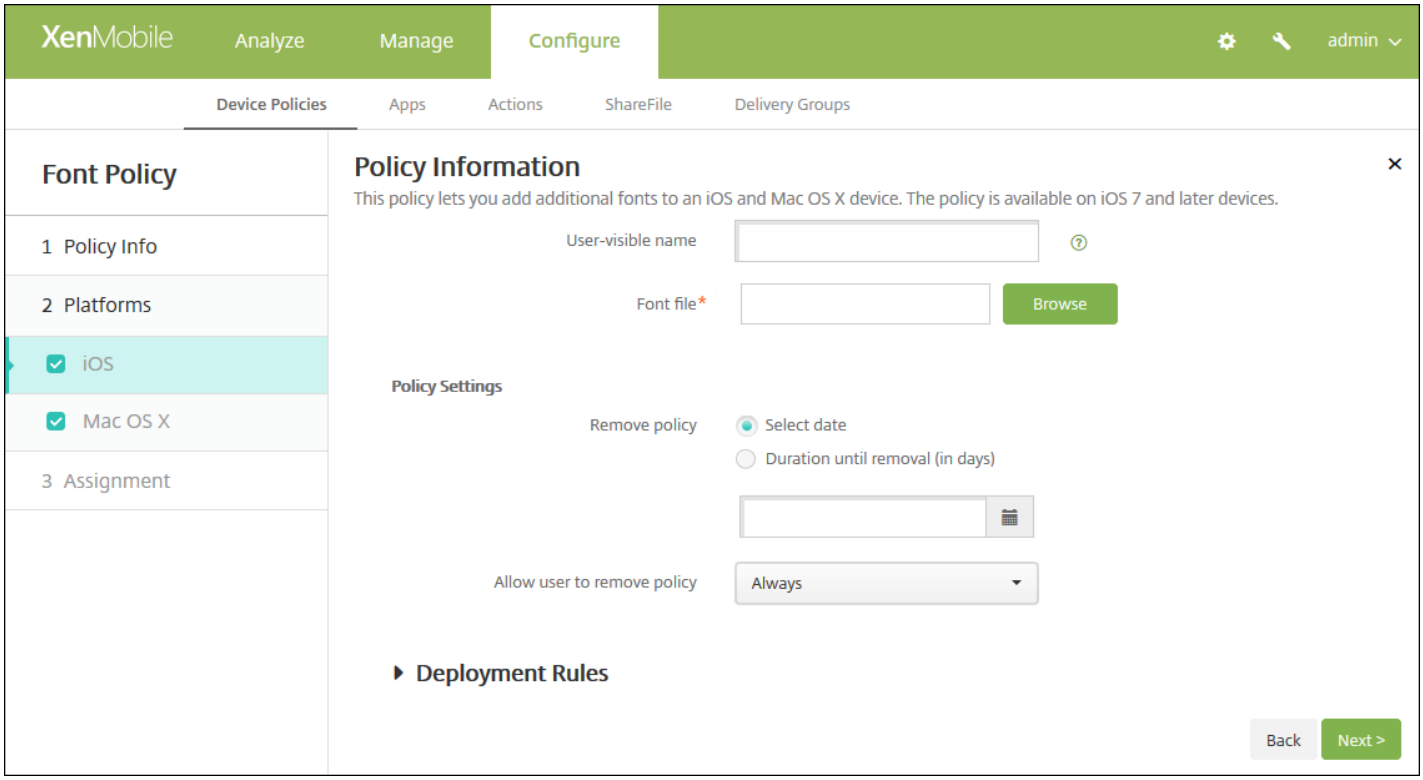
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

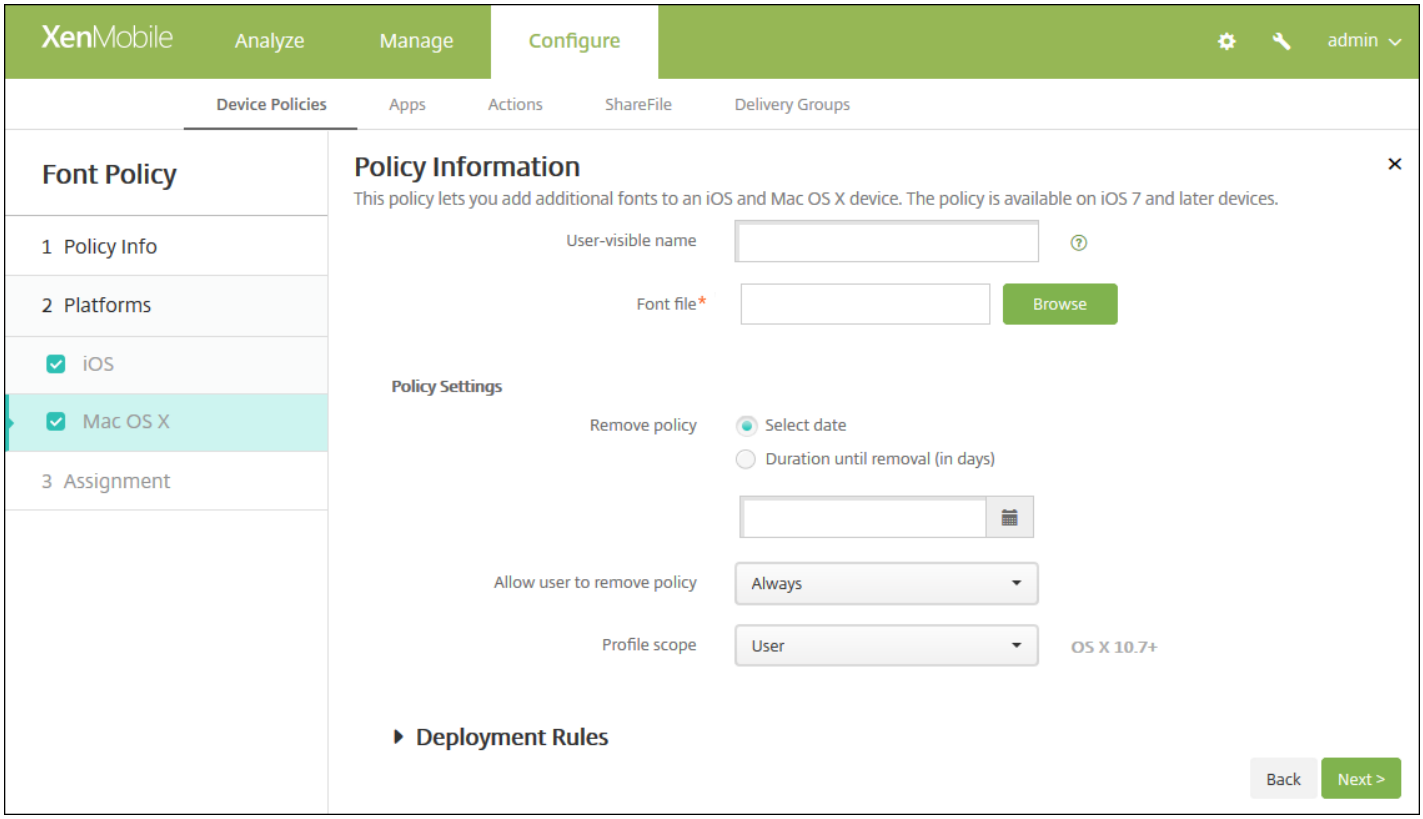
Configuración de los parámetros de iOS



Configure los siguientes parámetros:

- **User-visible name**. Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **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.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

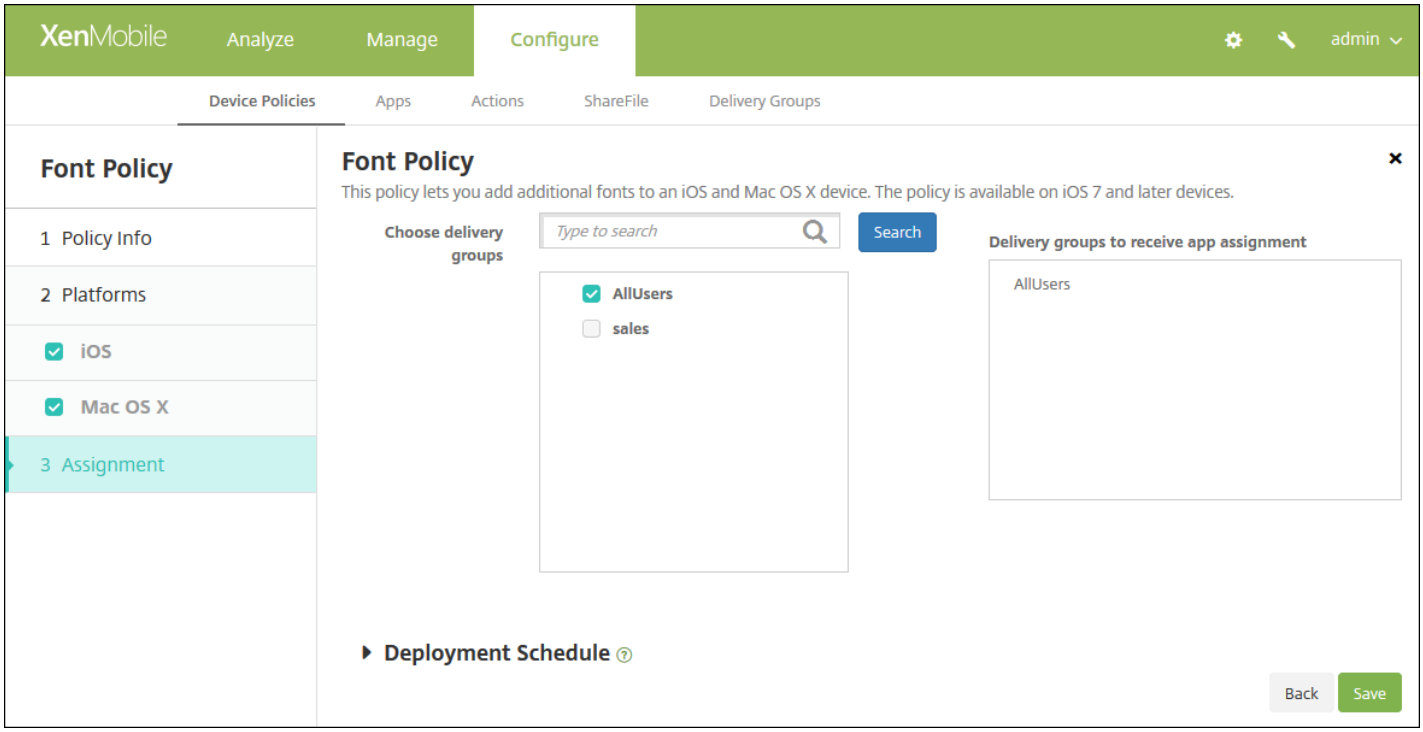


Configure los siguientes parámetros:

- **User-visible name**. Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **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.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Font 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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 en **Settings** > **Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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 importación de perfiles de iOS y Mac OS X

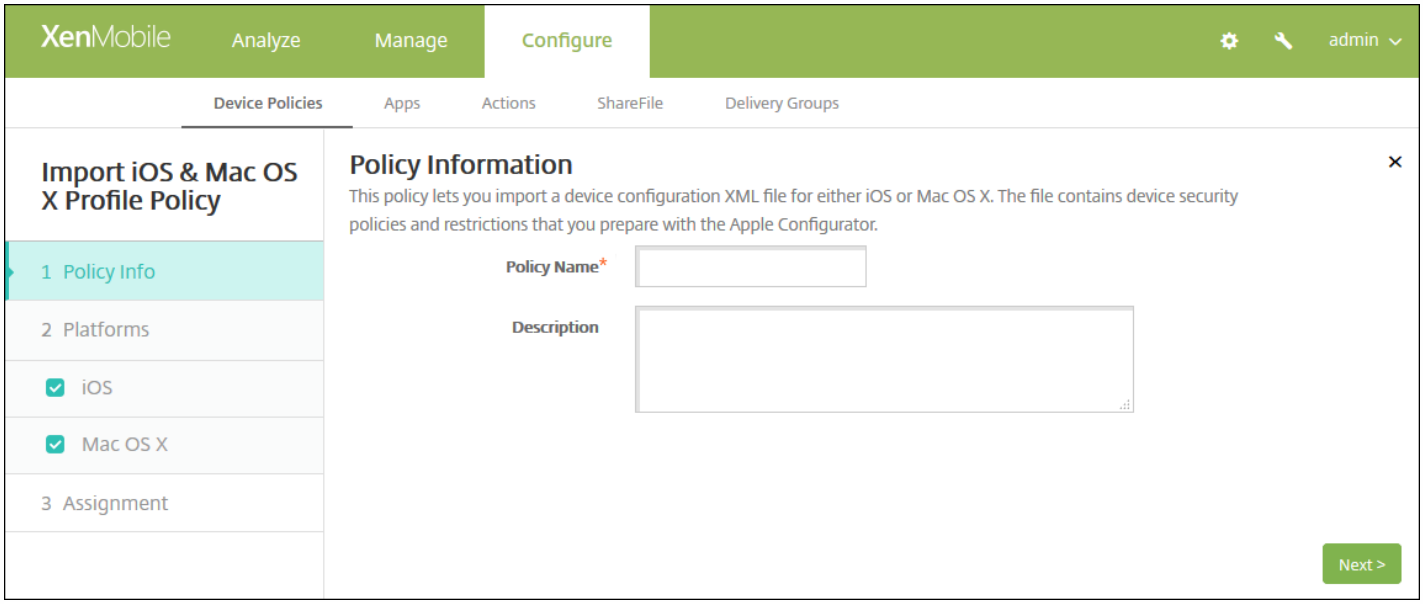
Jul 27, 2016

Puede importar en XenMobile archivos XML de configuración de dispositivos iOS y OS X. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator. Para obtener más información sobre cómo usar Apple Configurator para crear un archivo de configuración, consulte la página de ayuda de Apple Configurator.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

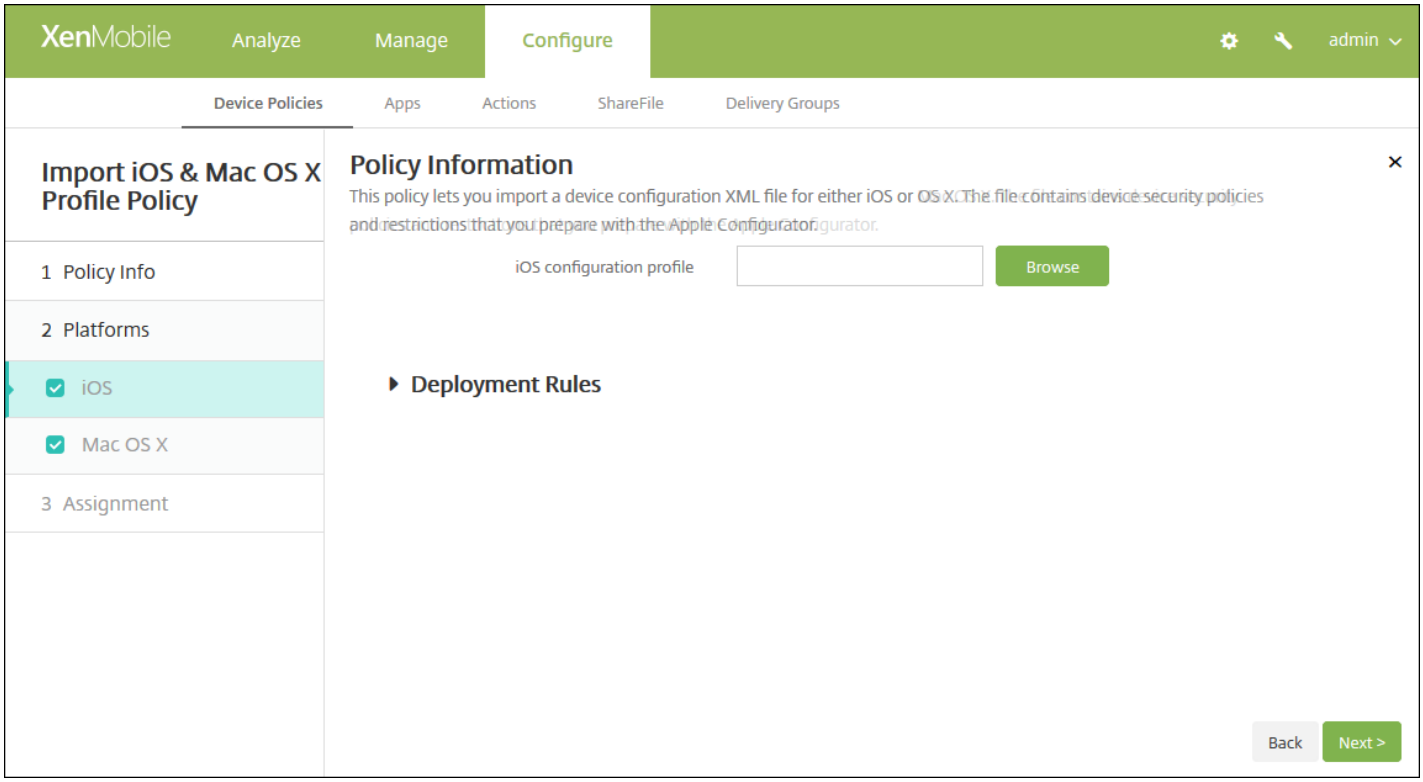
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Import iOS & Mac OS X Profile**. Aparecerá la página de información **Import iOS & Mac OS X Profile Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

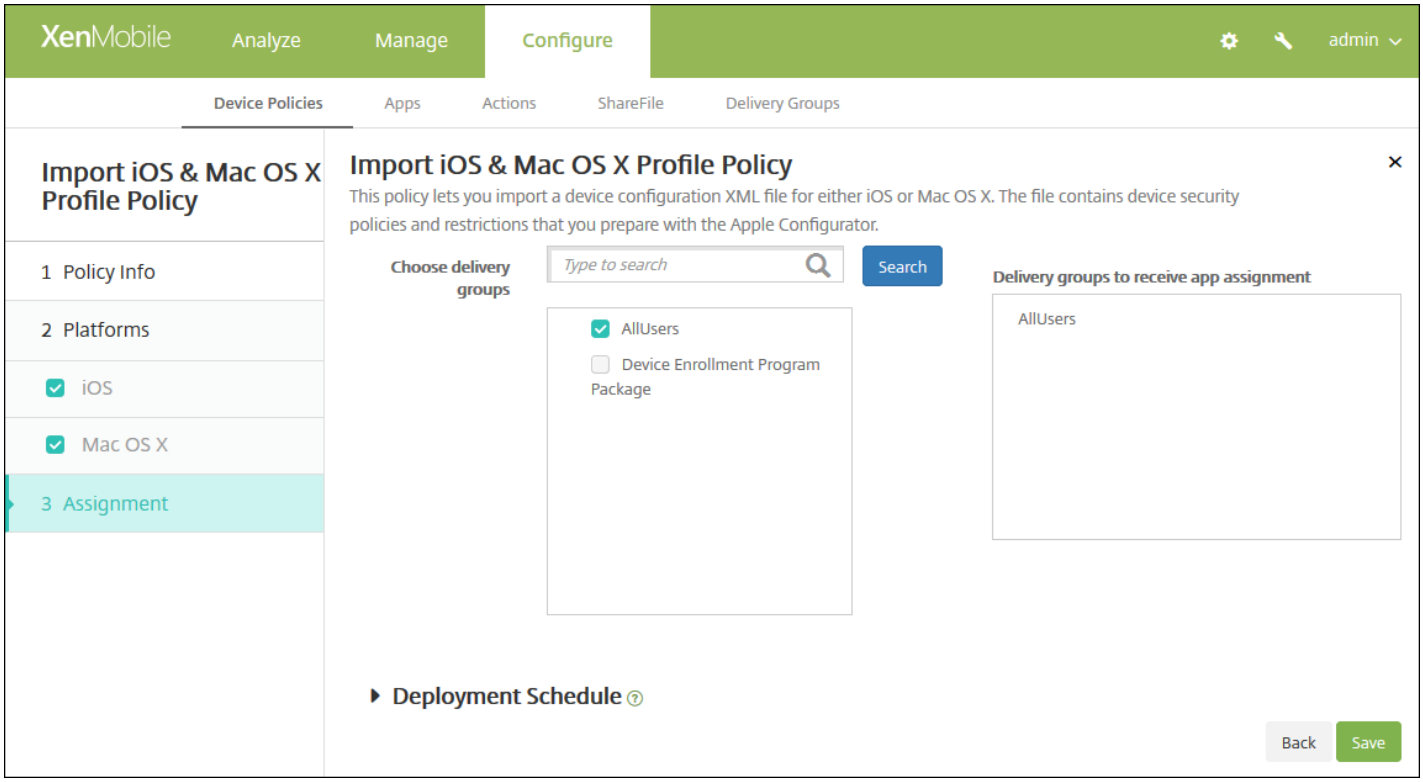
Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma. .

7. Configure esta opción para cada plataforma seleccionada:

- **iOS configuration profile** o **Mac OS X configuration profile**. Seleccione el archivo de configuración que quiera importar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

8. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Import iOS & Mac OS X Profile 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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.

Directiva de quiosco

Jul 27, 2016

En XenMobile, puede crear una directiva de quiosco 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 quiosco.

Para colocar un dispositivo Samsung SAFE en modo quiosco

1. Habilite la clave API de Samsung SAFE, en el dispositivo móvil, como se describe en Directivas de dispositivo de clave de licencia MDM de Samsung. Este paso le permite habilitar directivas en dispositivos Samsung SAFE.

2. Habilite la directiva Connection Scheduling para dispositivos Android, según se describe en Directivas de dispositivo de programación de conexiones. Este paso permite que los dispositivos Android se conecten con XenMobile.

3. Agregue una directiva de dispositivo Kiosk, como se describe en la sección siguiente.

4. Asigne esas tres directivas de dispositivo a los grupos de entrega adecuados. Decida si quiere incluir otras directivas, como App Inventory, en esos grupos de entrega.

Si más adelante desea quitar los dispositivos del modo quiosco, cree una nueva directiva de dispositivo Kiosk que tenga el parámetro **Kiosk mode** configurado con **Disable**. Actualice los grupos de entrega para quitar la directiva Kiosk que habilitaba el modo quiosco y agregue la directiva Kiosk que lo inhabilita.

Para agregar una directiva de dispositivo Kiosk

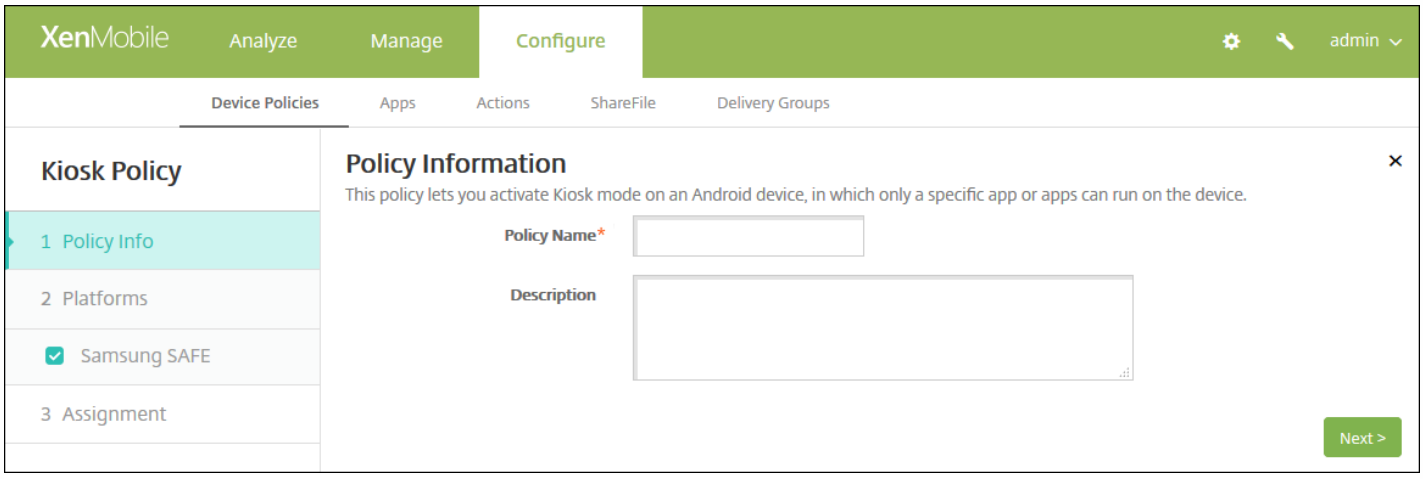
Nota:

- Todas las aplicaciones que especifique para el modo quiosco deben estar ya instaladas en los dispositivos de los usuarios.
- Algunas opciones solo se aplican a Samsung Mobile Device Management (MDM) 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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

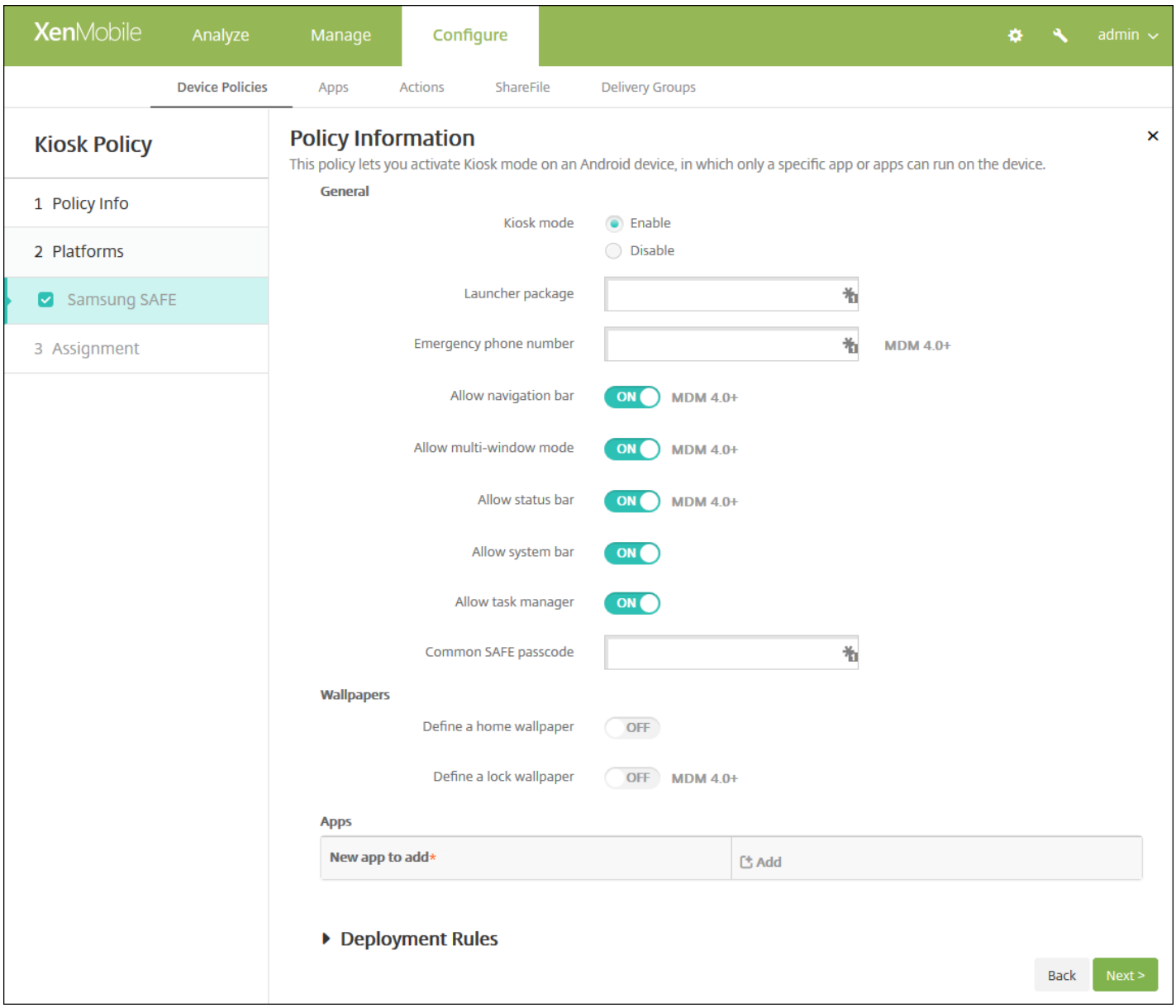
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Kiosk**. Aparecerá la página **Kiosk Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Samsung SAFE**.



6. Configure los siguientes parámetros:

- **Kiosk mode**. Haga clic en **Enable** o **Disable**. El valor predeterminado es **Enable**. Si hace clic en **Disable**, desaparecerán todas las opciones siguientes.
- **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 quiosco. Si está usando un programa interno de inicio, escriba el nombre completo del paquete de aplicaciones de ese programa.

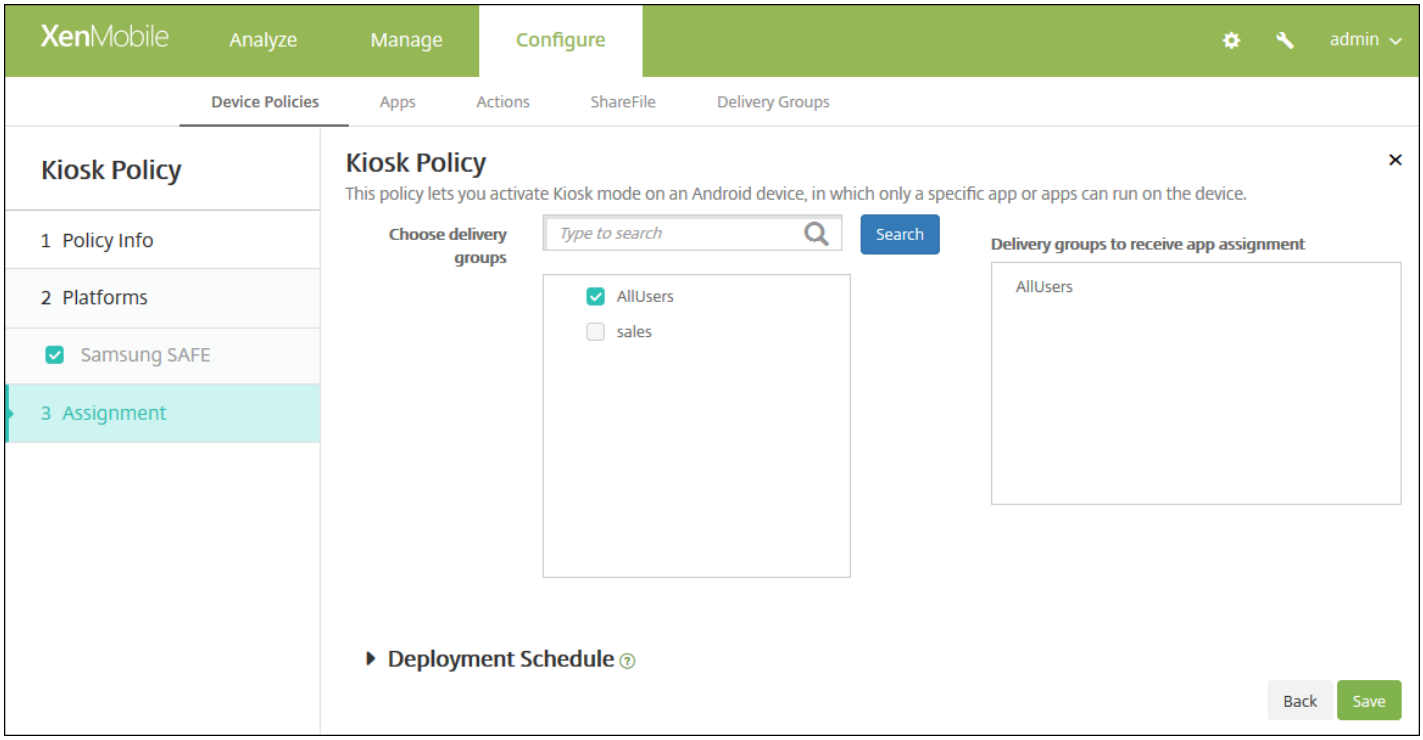
- **Emergency phone number**. Escriba un número de teléfono opcional. Una persona que encuentre un dispositivo perdido podrá usar este número para ponerse en contacto con su empresa. Se aplica solo a MDM 4.0 y versiones posteriores.
- **Allow navigation bar**. Seleccione si permitir que los usuarios vean y usen la barra de navegación en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow multi-window mode**. Seleccione si permitir que los usuarios usen varias ventanas en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow status bar**. Seleccione si permitir que los usuarios vean la barra de estado en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow system bar**. Seleccione si permitir que los usuarios vean la barra del sistema en el modo de quiosco. El valor predeterminado es **ON**.
- **Allow task manager**. Seleccione si permitir que los usuarios vean y usen el Administrador de tareas en el modo de quiosco. El valor predeterminado es **ON**.
- **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.
- **Fondos de pantalla**
  - **Define a home wallpaper**. Seleccione si utilizar una imagen personalizada para la pantalla de inicio en el modo de quiosco. El valor predeterminado es **OFF**.
    - **Home image**. Cuando habilite **Define a home wallpaper**, seleccione un archivo de imagen. Para ello, podrá hacer clic en **Browse** e ir a la ubicación del archivo.
  - **Define a lock wallpaper**. Seleccione si utilizar una imagen personalizada para la pantalla de bloqueo en el modo quiosco. El valor predeterminado es **OFF**. Se aplica solo a MDM 4.0 y versiones posteriores.
    - **Lock image**. Cuando habilite **Define a lock wallpaper**, seleccione un archivo de imagen. Para ello, podrá hacer clic en **Browse** e ir a la ubicación del archivo.
- **Apps**. Para agregar cada aplicación al modo quiosco, haga clic en **Add** y lleve a cabo lo siguiente:
  - **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.
  - Haga clic en **Save** para agregar la aplicación, o bien haga clic en **Cancel** para no agregarla.

    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 a la derecha. 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. Configure las reglas de implementación.

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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 a iOS.

11. Haga clic en **Save**.

Directivas LDAP de dispositivos

Jul 27, 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.

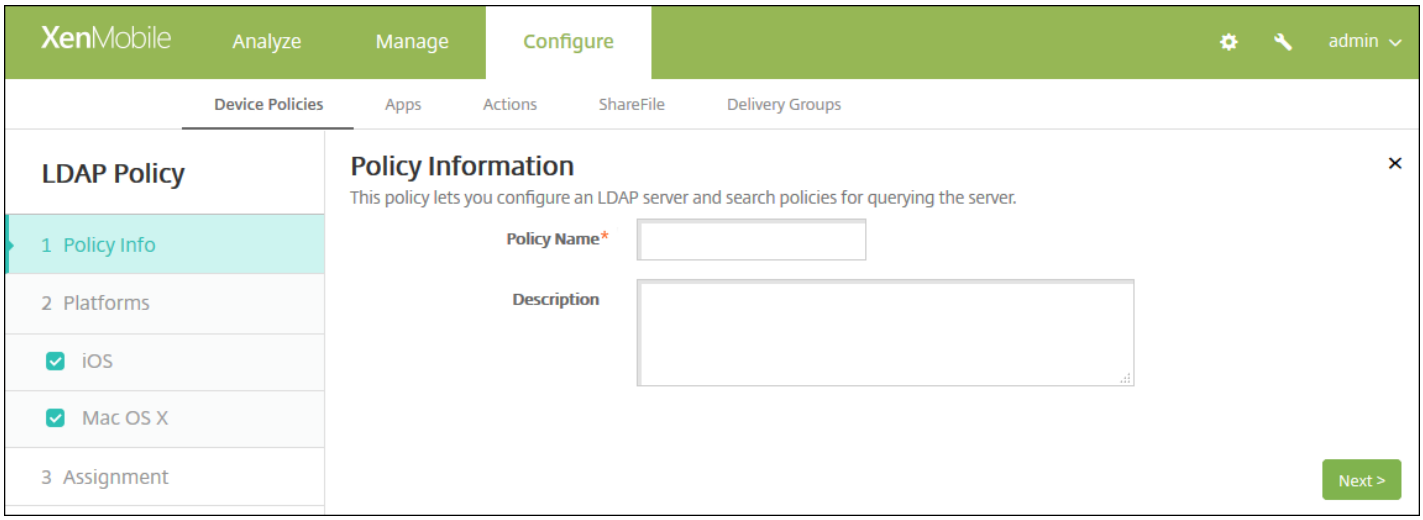
Configuración de iOS

Configuración de Mac OS X

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. Expanda **More** y, en **End user**, haga clic en **LDAP**. Aparecerá la página **LDAP Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

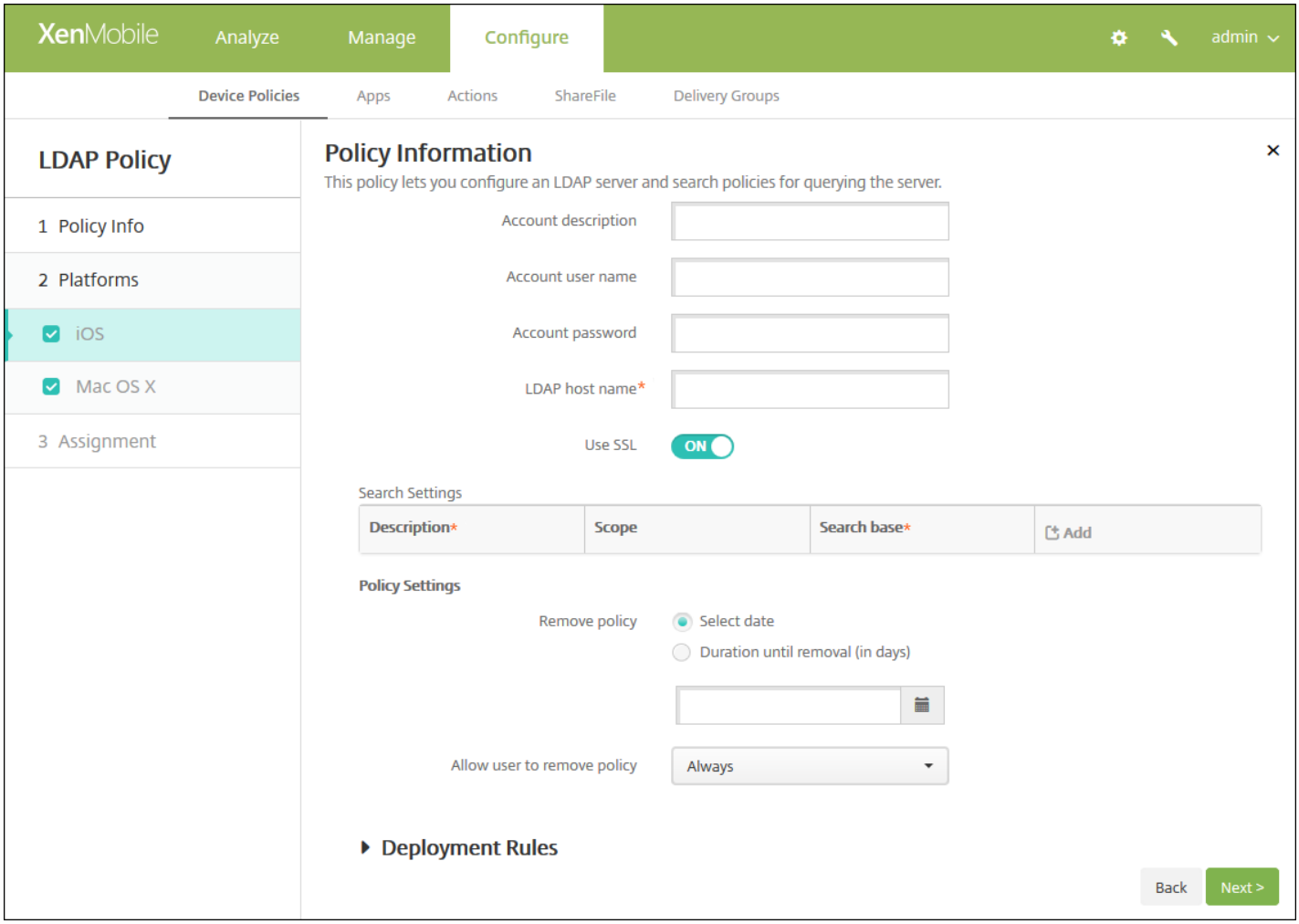
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure los siguientes parámetros:

- **Account description**. Indique una descripción opcional de la cuenta.
- **Account user name**. Escriba un nombre de usuario opcional.
- **Account password**. Escriba una contraseña opcional. Use esta opción solo con perfiles cifrados.
- **LDAP host name**. Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor LDAP. El valor predeterminado es **ON**.
- **Search Settings**. Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Add** y lleve a cabo lo siguiente:
  - **Description**. Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
  - **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.
  - **Search base**. Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o 0=empresa de ejemplo. Este campo es obligatorio.

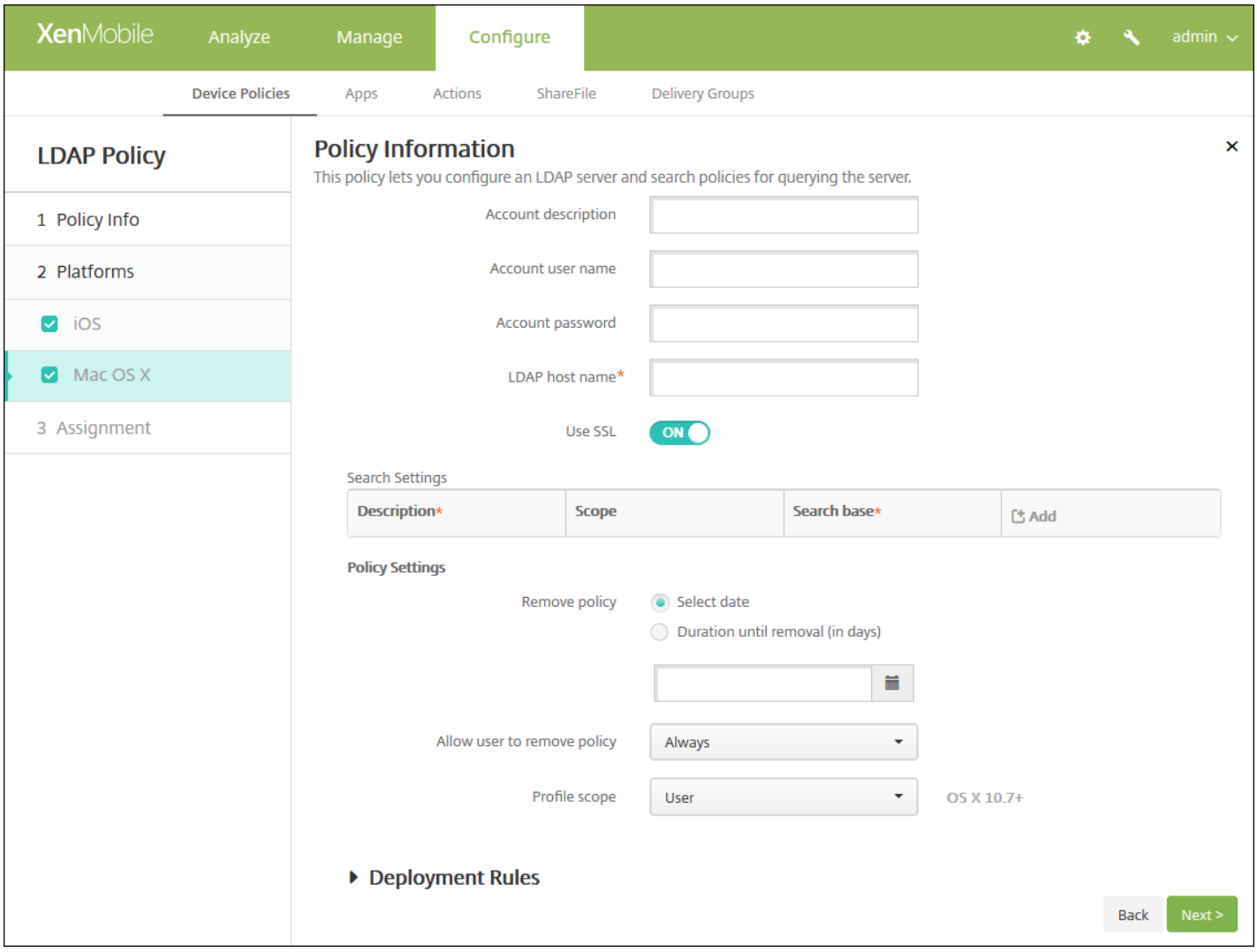
- Haga clic en **Save** para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
- Repita estos pasos para cada opción de búsqueda que quiera agregar.

  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.

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure los siguientes parámetros:

- **Account description**. Indique una descripción opcional de la cuenta.
- **Account user name**. Si quiere, escriba un nombre de usuario.
- **Account password**. Escriba una contraseña opcional. Use esta opción solo con perfiles cifrados.
- **LDAP host name**. Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Use SSL**. Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor LDAP. El valor predeterminado es **ON**.
- **Search Settings**. Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Add** y lleve a cabo lo siguiente:
  - **Description**. Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
  - **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.
  - **Search base**. Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o 0=empresa de ejemplo. Este campo es obligatorio.
  - Haga clic en **Save** para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
  - Repita estos pasos para cada opción de búsqueda que quiera agregar.

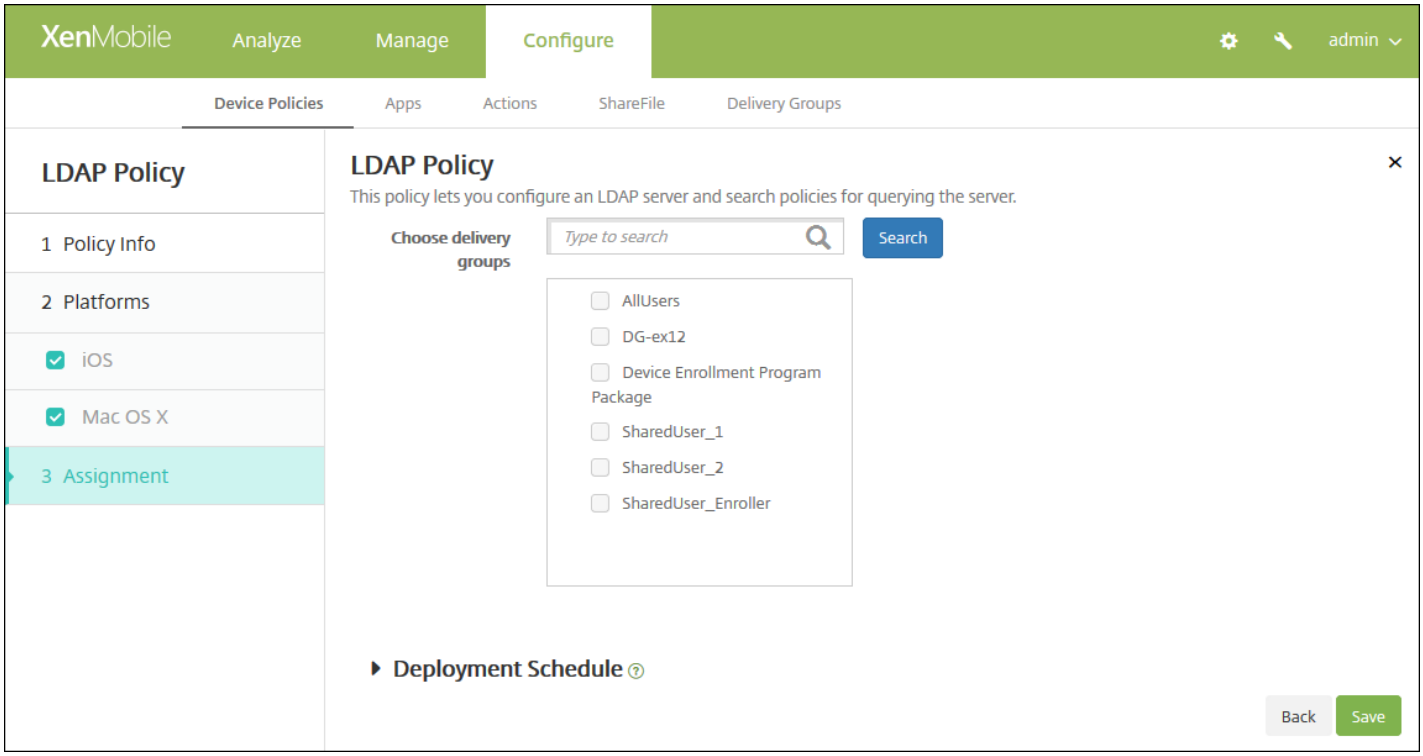
    Nota: Para eliminar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel 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.

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
- En **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **LDAP 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 ubicación

Jul 27, 2016

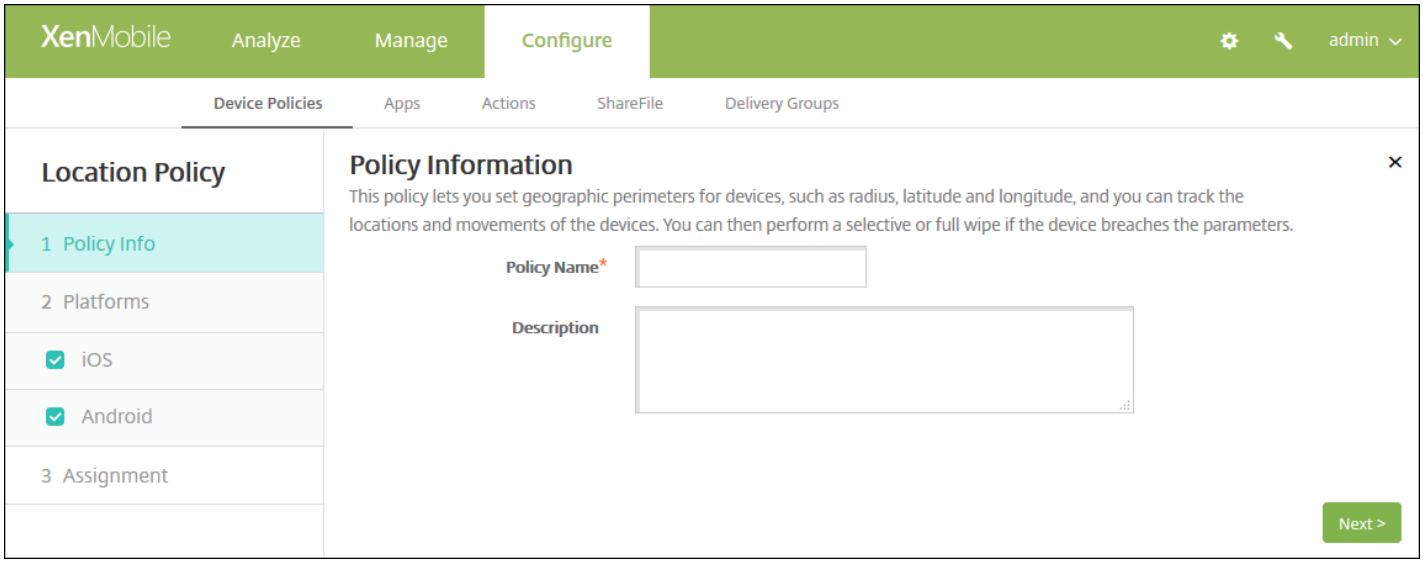
En XenMobile, puede crear directivas de ubicación para aplicar límites geográficos y realizar un seguimiento de la ubicación y del movimiento de los dispositivos de los usuarios. Cuando los usuarios abandonen el perímetro definido (también conocido como *geocerca*), XenMobile puede realizar un borrado 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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Haga clic en **Location**. Aparecerá la página de información **Location Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

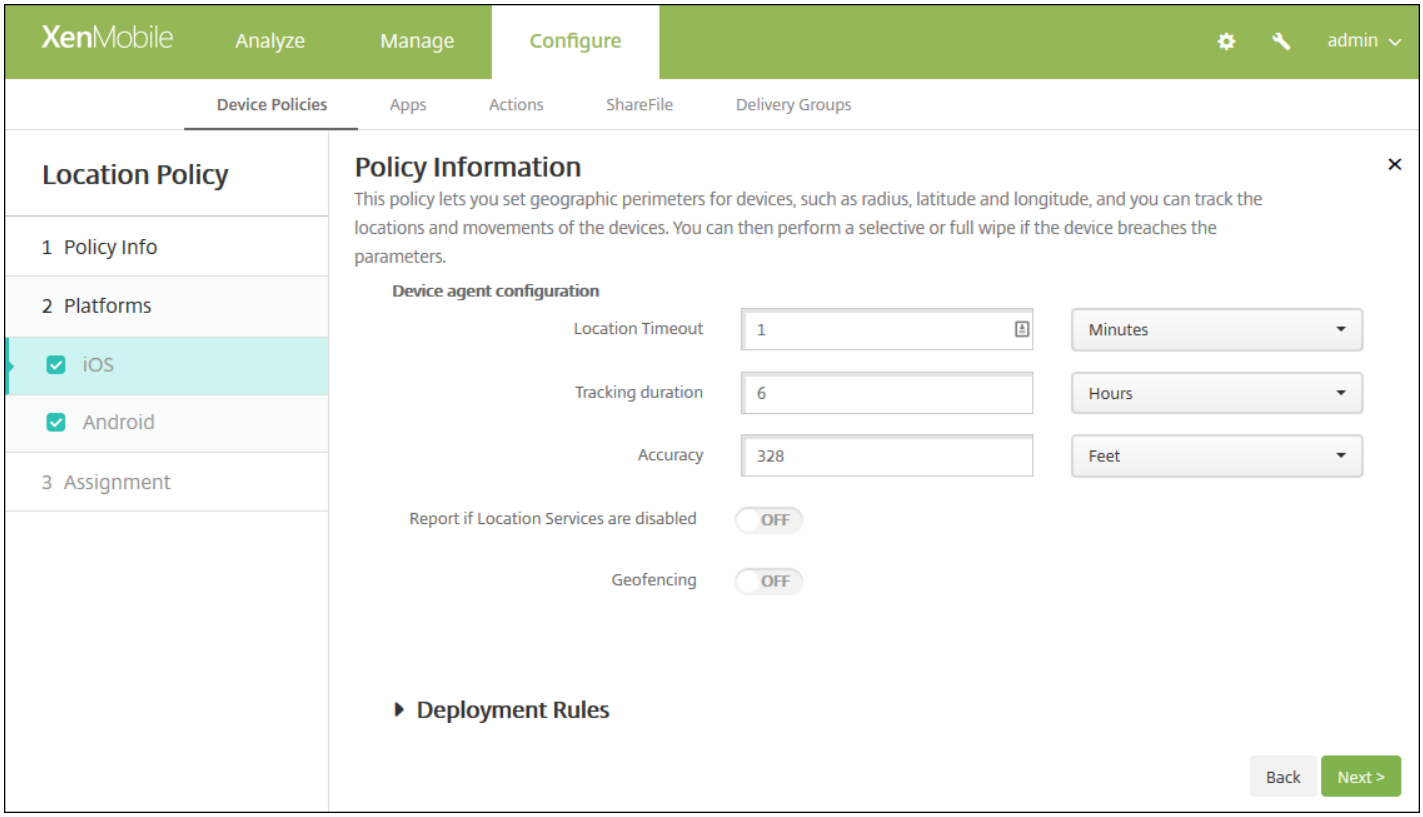
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

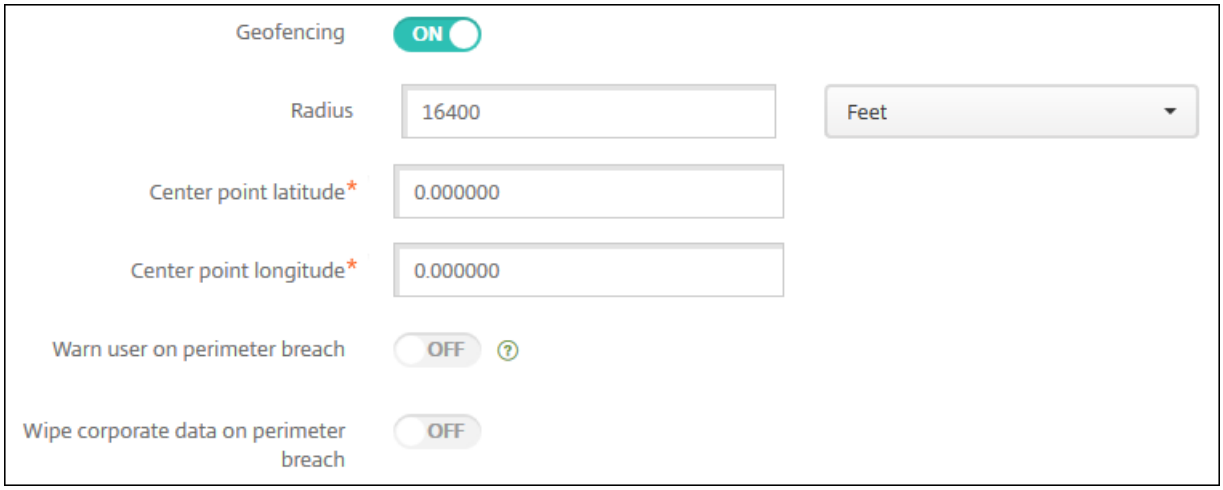
Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure estos parámetros:

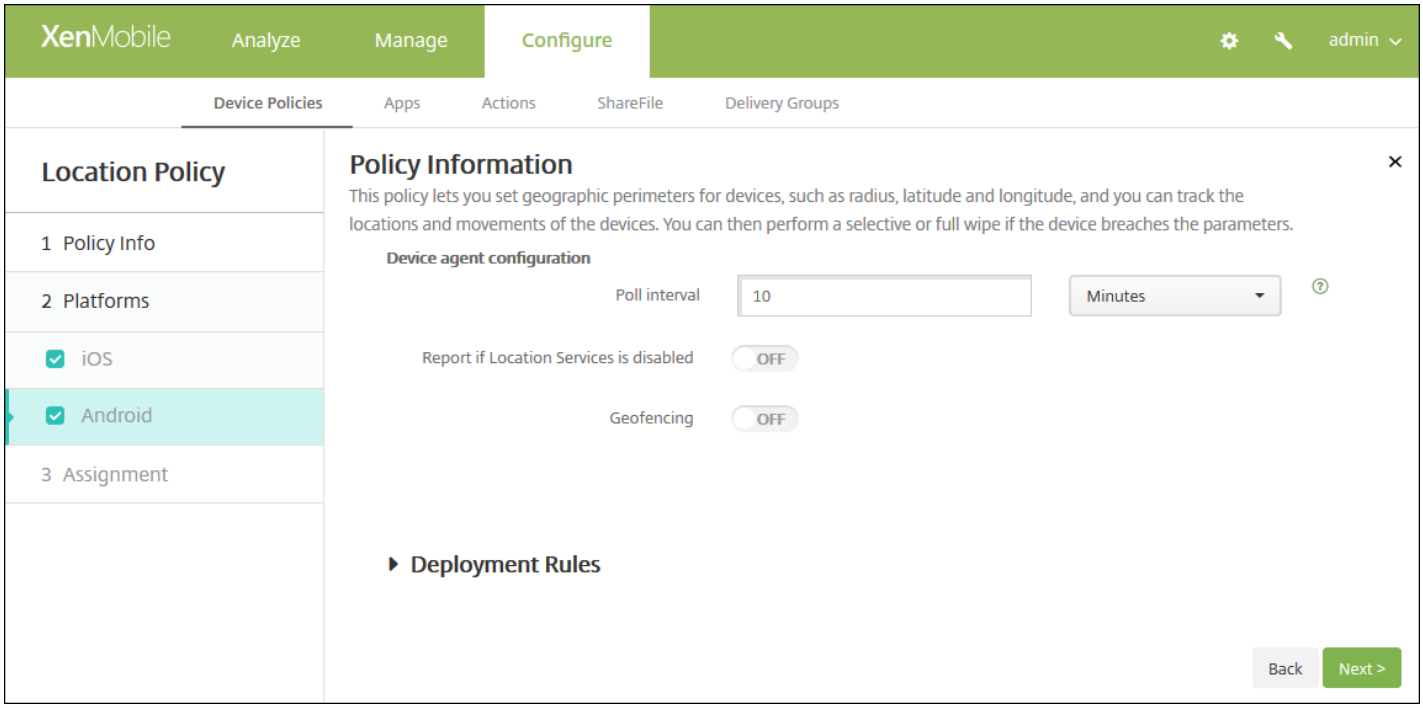
- **Location timeout**. Escriba un número y, en la lista, haga clic en **Seconds** o **Minutes** para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es de 1 minuto.
- **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**.
- **Geocercas**



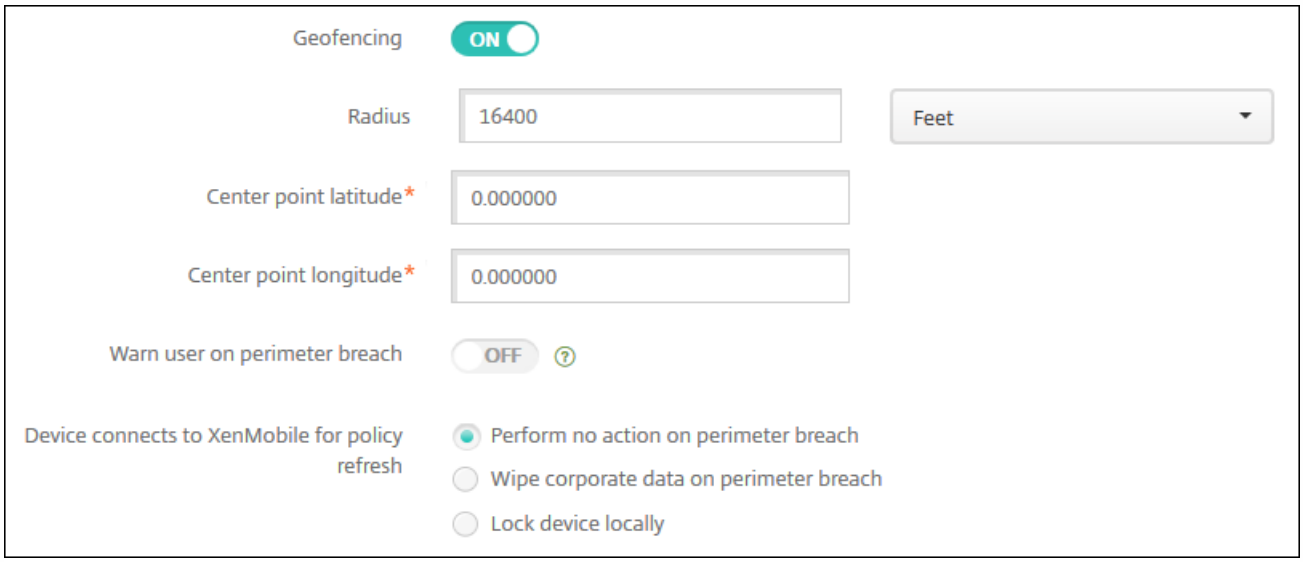
Al habilitar geocercas, configure los siguientes parámetros:

- **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 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, aparecerá 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.

Configuración de los parámetros de Android



- **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. Si este valor es 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**.
- **Geocercas**



Al habilitar geocercas, configure los siguientes parámetros:

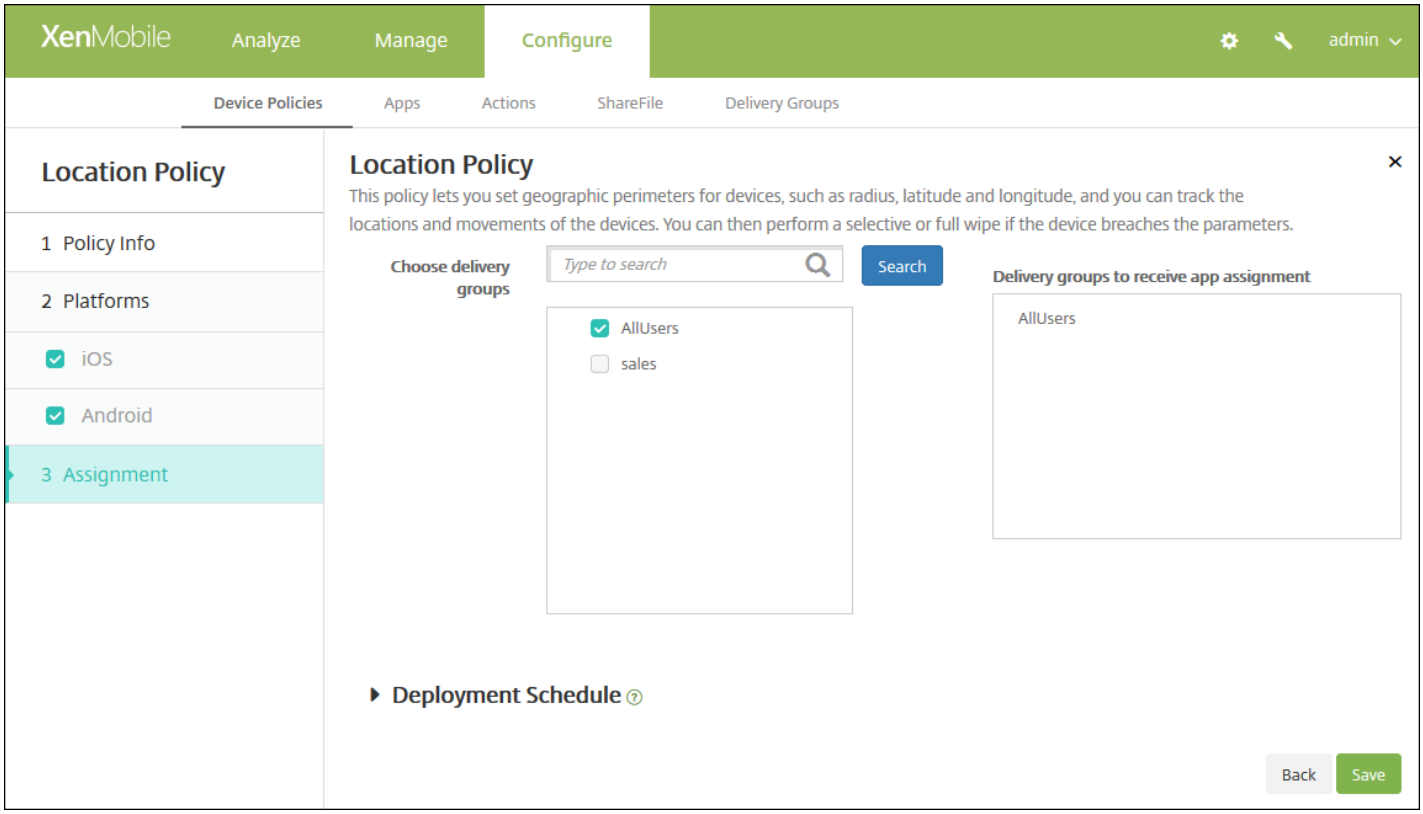
- **Radius**. Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies. Los valores válidos para el radio del perímetro son:

- 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, aparecerá 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. Configure las reglas de implementación.

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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 correos electrónicos

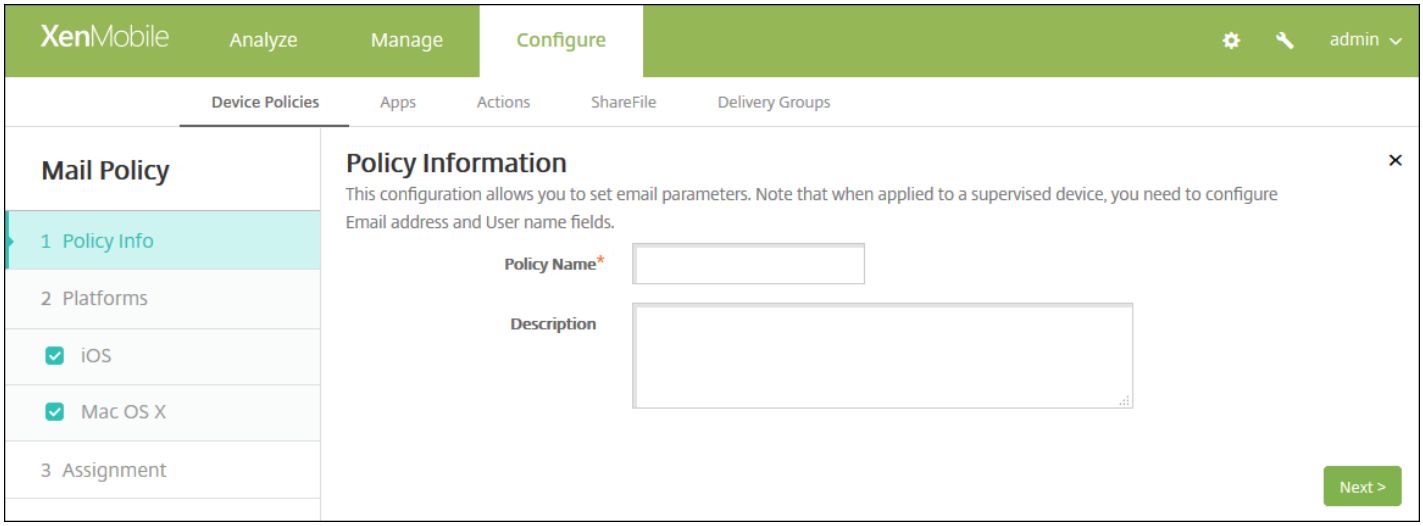
Jul 27, 2016

En XenMobile, puede agregar una directiva de dispositivos para configurar una cuenta de correo electrónico en los dispositivos iOS o Mac OS X 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**.

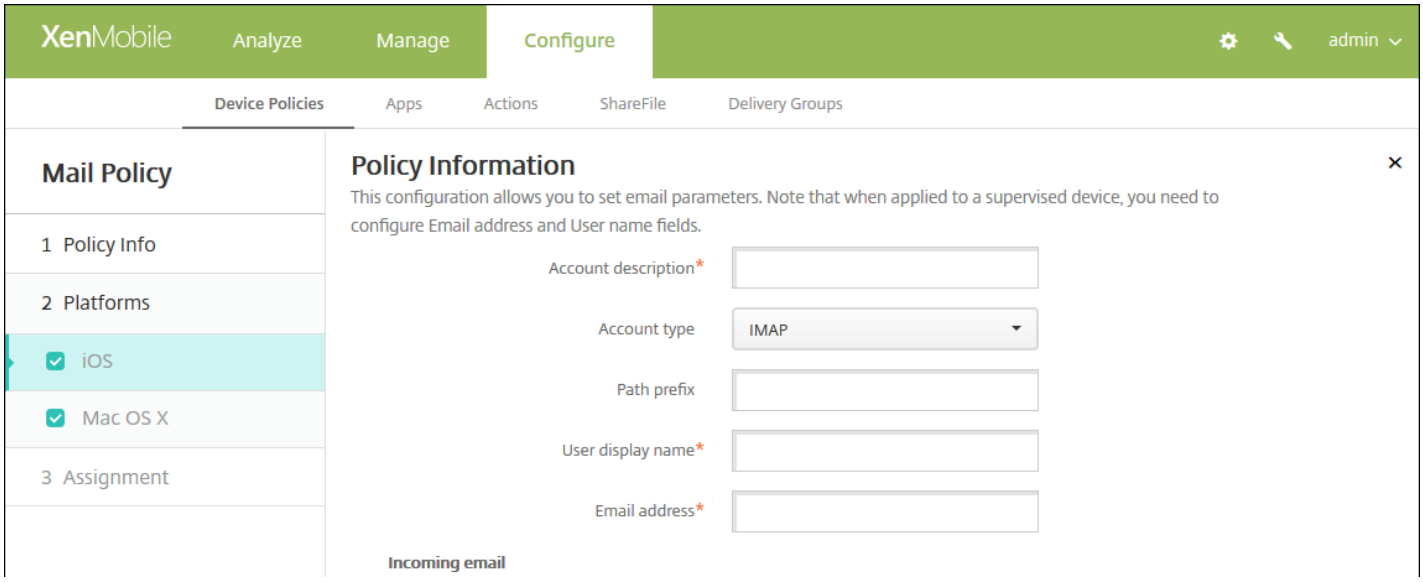
3. Haga clic en **More** y, en **End user**, haga clic en **Mail**. Aparecerá la página **Mail Policy**.

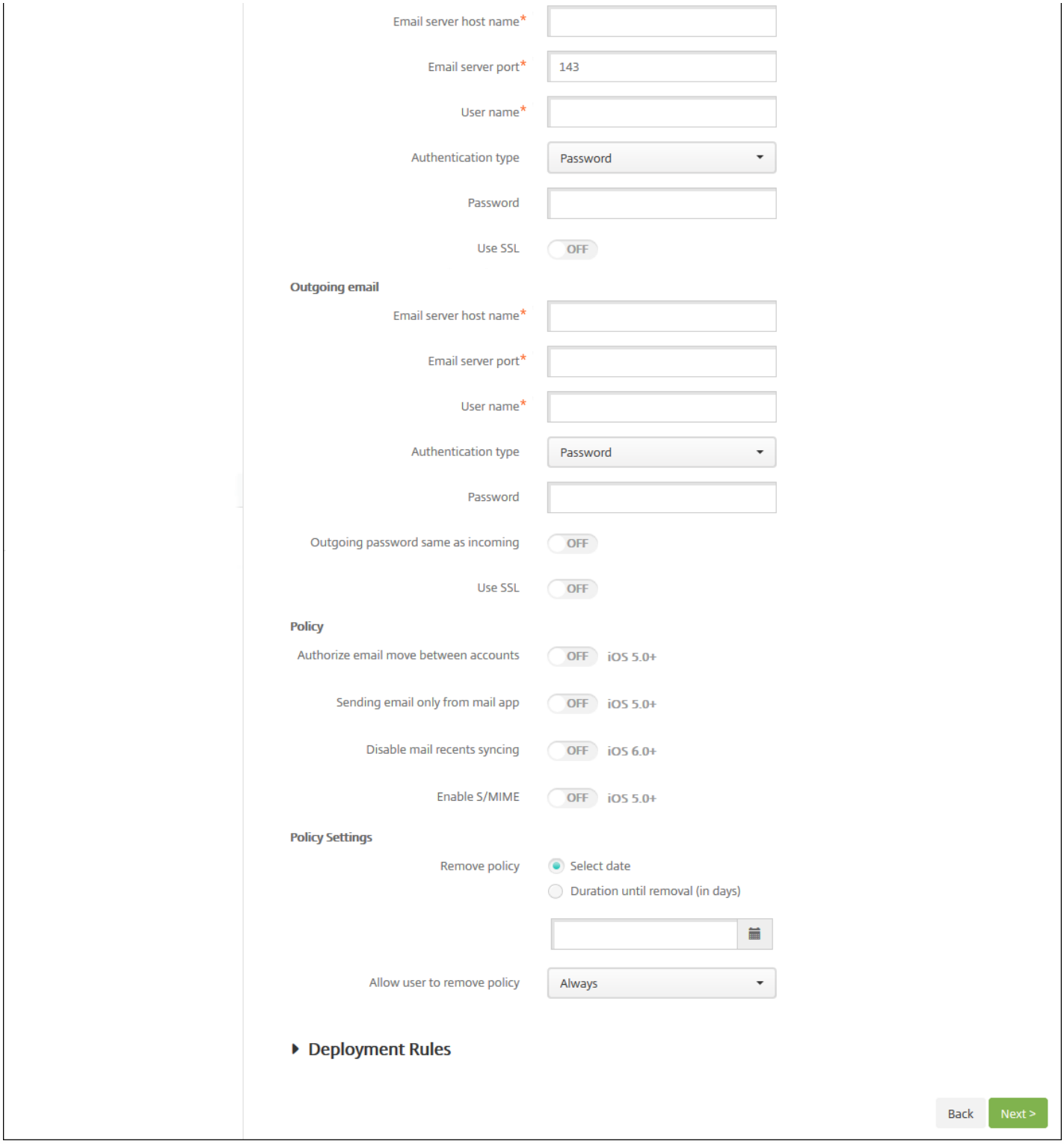


4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de Mail Policy.





6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas.

- **Account description**. Indique una descripción de la cuenta. Esta descripción aparece en las aplicaciones Correo y Ajustes. Este campo es obligatorio.
- **Account type**. En la lista, haga clic en **IMAP** o **POP** para seleccionar el protocolo que se va a usar para las cuentas de usuario. El valor predeterminado es **IMAP**. Si selecciona **POP**, desaparece la opción **Path prefix**.
- **Path prefix**. Escriba **INBOX** o introduzca el prefijo de la ruta de su cuenta de correo electrónico IMAP (si no es **INBOX**). Este campo es obligatorio.
- **User display name**. Escriba el nombre de usuario completo que se va a usar para los mensajes, entre otros. Este campo es obligatorio.
- **Email address**. Escriba la dirección de correo electrónico completa de la cuenta. Este campo es obligatorio.
- **Configuración de correos electrónicos entrantes**
  - **Email server host name**. Escriba el nombre del host o la dirección IP del servidor de correos entrantes. Este campo es obligatorio.
  - **Email server port**. Escriba el número de puerto del servidor de correos entrantes. El valor predeterminado es **143**. Este campo es obligatorio.
  - **User name**. Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico del usuario hasta el carácter @. Este campo es obligatorio.
  - **Authentication type**. En la lista, haga clic para seleccionar el tipo de autenticación que se va a usar. El valor predeterminado es **Authentication type**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password**. Si quiere, escriba una contraseña para el servidor de correos entrantes.
  - **Use SSL**. Seleccione esta opción si el servidor de correos entrantes utiliza la autenticación de capa de sockets seguros (SSL). El valor predeterminado es **OFF**.
- **Configuración de correos electrónicos salientes**
  - **Email server host name**. Escriba el nombre del host o la dirección IP del servidor de correos salientes. Este campo es obligatorio.
  - **Email server port**. Escriba el número de puerto del servidor de correos salientes. Si no indica ningún número de puerto, se utiliza el puerto predeterminado para el protocolo especificado.
  - **User name**. Escriba el nombre de usuario de la cuenta de correo electrónico. Suele ser el mismo que la dirección de correo electrónico del usuario hasta el carácter @. Este campo es obligatorio.
  - **Authentication type**. En la lista, haga clic para seleccionar el tipo de autenticación que se va a usar. El valor predeterminado es **Authentication type**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password**. Si quiere, escriba una contraseña para el servidor de correos salientes.
  - **Outgoing password same as incoming**. Seleccione si las contraseñas entrantes y salientes son iguales. El valor predeterminado es OFF, lo que significa que las contraseñas son diferentes. Si se establece en **ON**, desaparece el campo anterior **Password**.
  - **Use SSL**. Seleccione esta opción si el servidor de correos salientes utiliza la autenticación de capa de sockets seguros (SSL). El valor predeterminado es **OFF**.
- **Directiva**
  - **Nota**: Al configurar parámetros de iOS, estas opciones solo se aplican a iOS 5.0 y versiones posteriores; no hay restricciones cuando se configure Mac OS X.
  - **Authorize email move between accounts**. Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta y reenviarlos y responderlos desde otra cuenta. El valor predeterminado es **OFF**.
  - **Sending email only form mail app**. Seleccione esta opción para obligar a los usuarios a utilizar la aplicación de correo de iOS para enviar correos electrónicos.
  - **Disable mail recents syncing**. Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes. El valor predeterminado es **OFF**. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.
  - **Enable S/MIME**. Seleccione si esta cuenta es compatible con el cifrado y la autenticación S/MIME. El valor

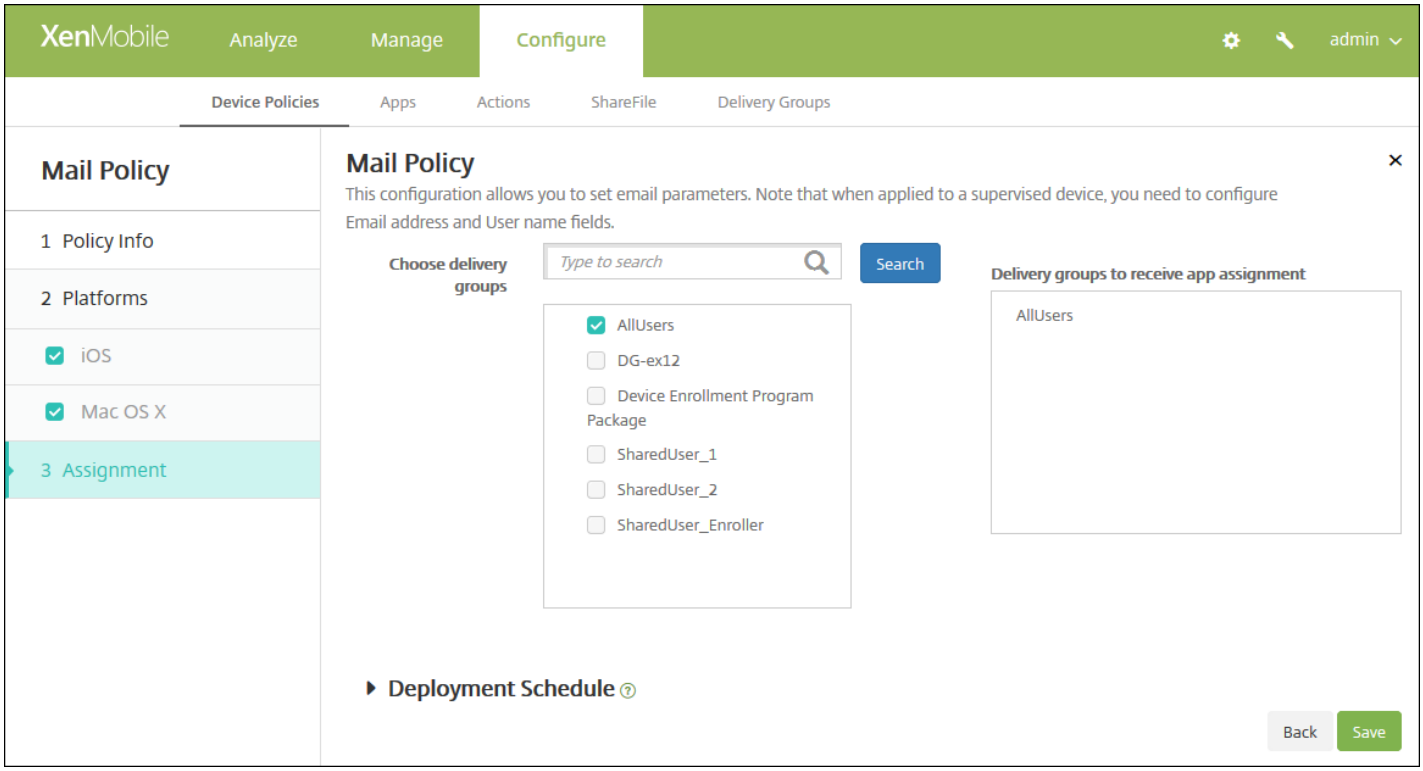
predeterminado es **OFF**. Si se establece en ON, aparecen los dos siguientes campos.

- **Signing identity credential**. En la lista, seleccione la credencial de firma que se va a usar.
- **Encryption identity credential**. En la lista, seleccione la credencial de cifrado que se va a usar.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, en la lista, haga clic en **User** o **System**. El valor predeterminado es **User**. Esta opción solo está disponible para Mac OS X 10.7 y versiones posteriores.

8. Configure las reglas de implementación.

9. Haga clic en **Next**. Aparecerá la página de asignación **Mail 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.

- 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.
- 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.

Directiva de dominios administrados

Jul 27, 2016

Puede definir los dominios administrados que se aplicarán al correo electrónico y al explorador Web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari. Así, puede especificar las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador Web. Esta directiva solo está disponible para dispositivos supervisados con iOS 8 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.

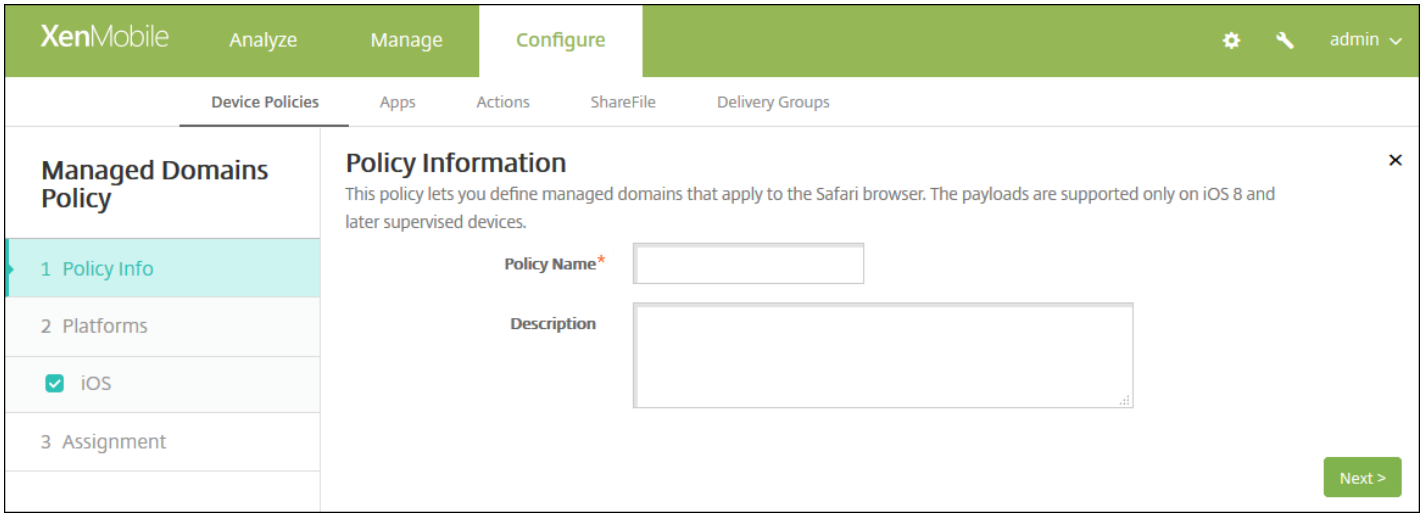
Cuando un usuario envía un correo electrónico a un destinatario cuyo dominio no consta en la lista de dominios administrados de correo electrónico, el mensaje se marca en el dispositivo del usuario para avisarle de que envía un mensaje a una persona fuera del dominio empresarial.

Cuando un usuario intente abrir un elemento (documento, adjunto o descarga) con Safari desde un dominio que no conste en la lista de dominios Web administrados, la aplicación de empresa correspondiente abrirá el elemento. Si el elemento no es de un dominio Web que conste en la lista de dominios Web administrados, el usuario no podrá abrir el elemento con la aplicación de empresa, y deberá usar una aplicación personal no administrada.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

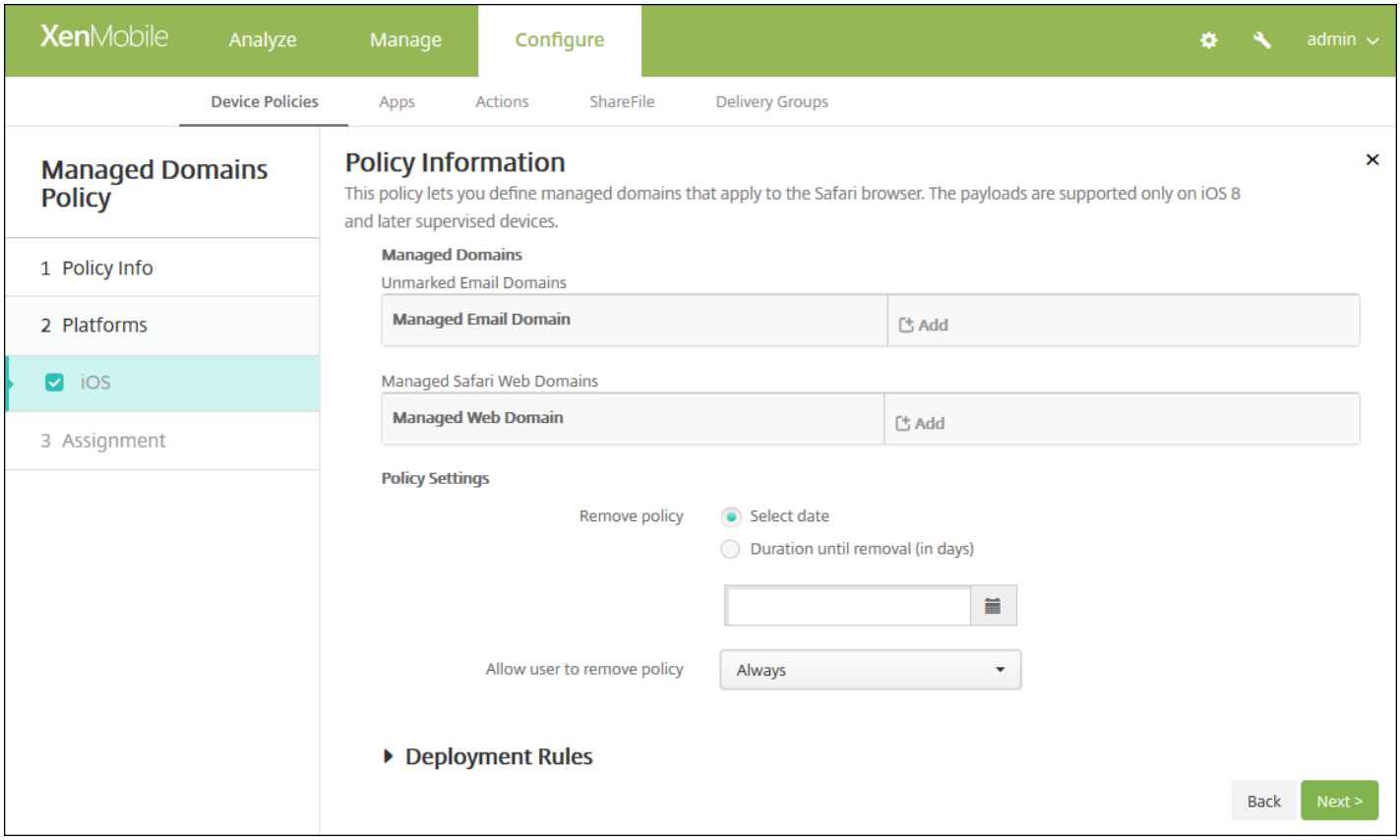
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Managed domains**. Aparecerá la página de información **Managed Domains Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **iOS Platform**.



Cómo especificar dominios

6. Configure los siguientes parámetros:

- **Managed Domains**
  - **Unmarked Email Domains**. Para cada dominio de correo electrónico que quiera incluir en la lista, haga clic en **Add** y lleve a cabo lo siguiente:
    - **Managed Email Domain**. Escriba el dominio de correo electrónico.
    - Haga clic en **Save** para guardar el dominio de correo electrónico, o bien haga clic en **Cancel** para no guardarlo.
  - **Managed Safari Web Domains**. Para cada dominio Web que quiera incluir en la lista, haga clic en **Add** y lleve a cabo lo siguiente:
    - **Managed Web Domain**. Escriba el dominio Web.
    - Haga clic en **Save** para guardar el dominio Web, o bien haga clic en **Cancel** para no guardarlo.

      Nota: Para eliminar un dominio 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.

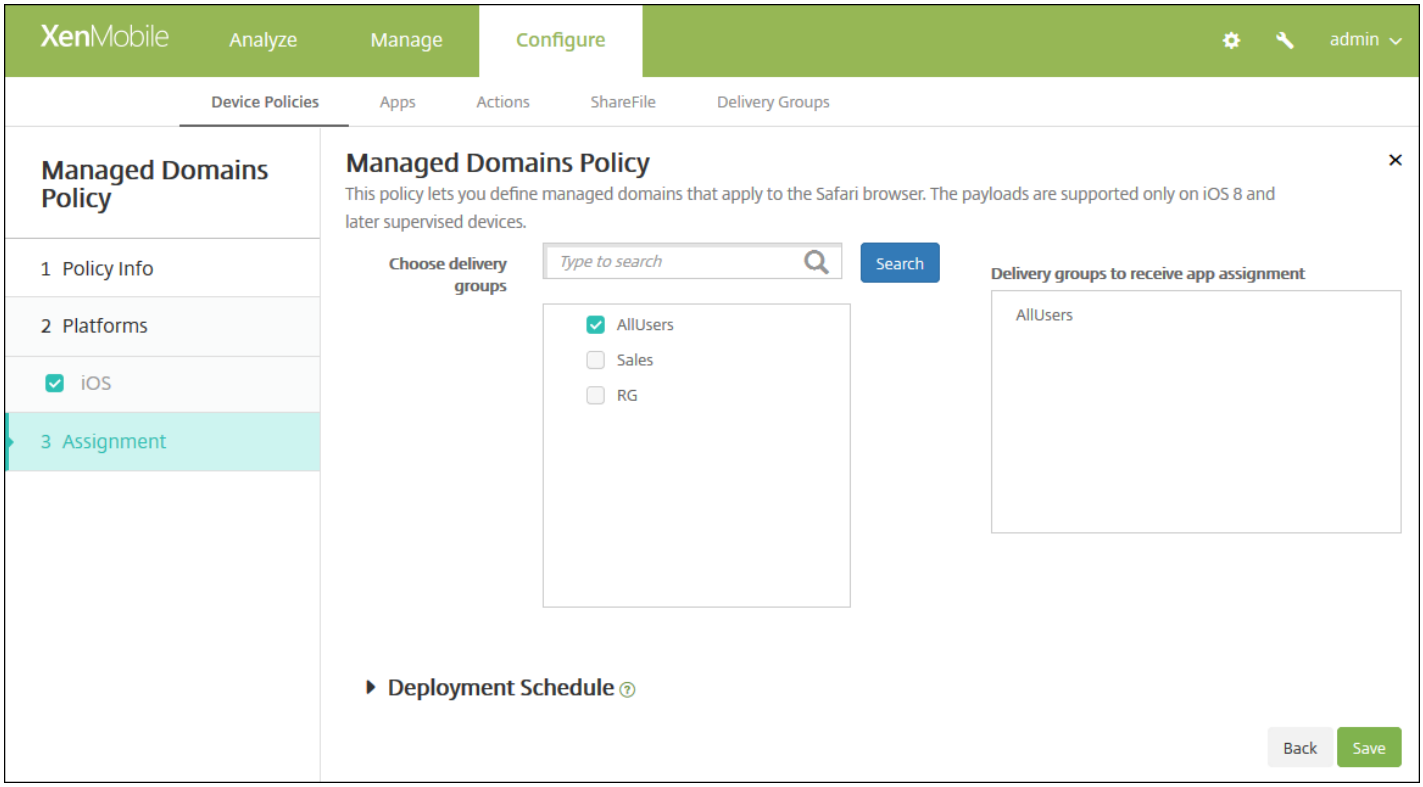
      Para modificar un dominio existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Managed Domains 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de opciones de MDM

Jul 27, 2016

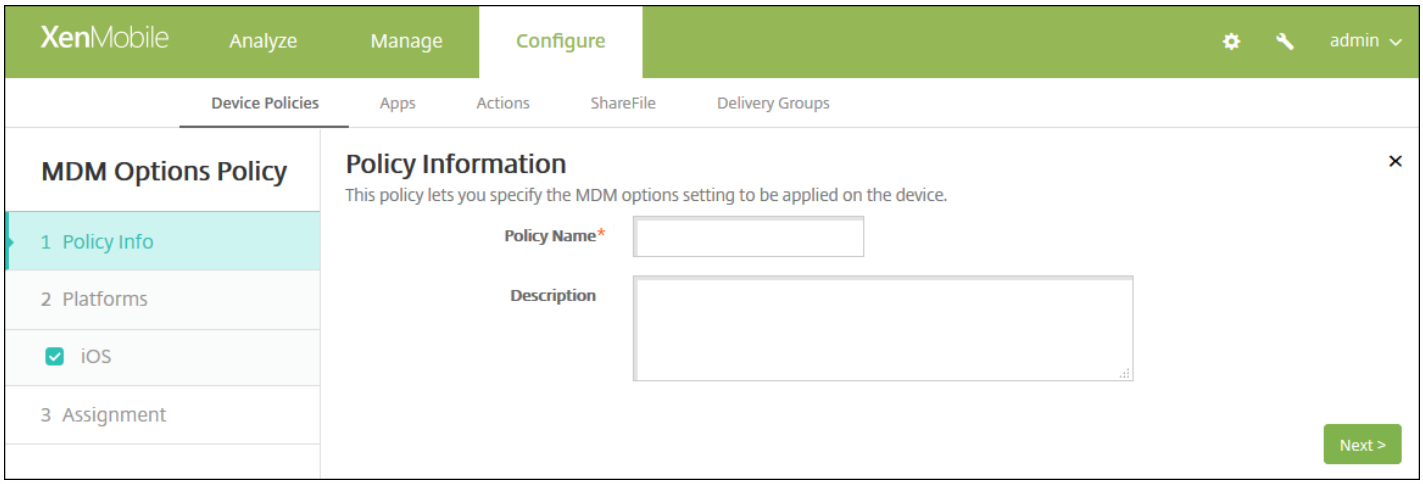
En XenMobile, puede crear una directiva de dispositivo para administrar la función Bloqueo de activación de Buscar mi iPhone/iPad en los dispositivos supervisados iOS 7.0 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator o Inscripción masiva de iOS.

Bloqueo de activación es una función de Buscar mi iPhone o iPad que está diseñada para evitar la reactivación de dispositivos perdidos o robados porque se necesita el ID de Apple y la contraseña del usuario para poder desactivar Buscar Mi iPhone, borrar los datos del dispositivo o reactivarlo y usarlo. En XenMobile, puede omitir el requisito de ID de Apple y contraseña si habilita el bloqueo de activación en la directiva de opciones de MDM. Así, cuando un usuario devuelva un dispositivo con la función Buscar Mi iPhone activada, podrá administrar el dispositivo desde la consola de XenMobile sin sus credenciales de Apple.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

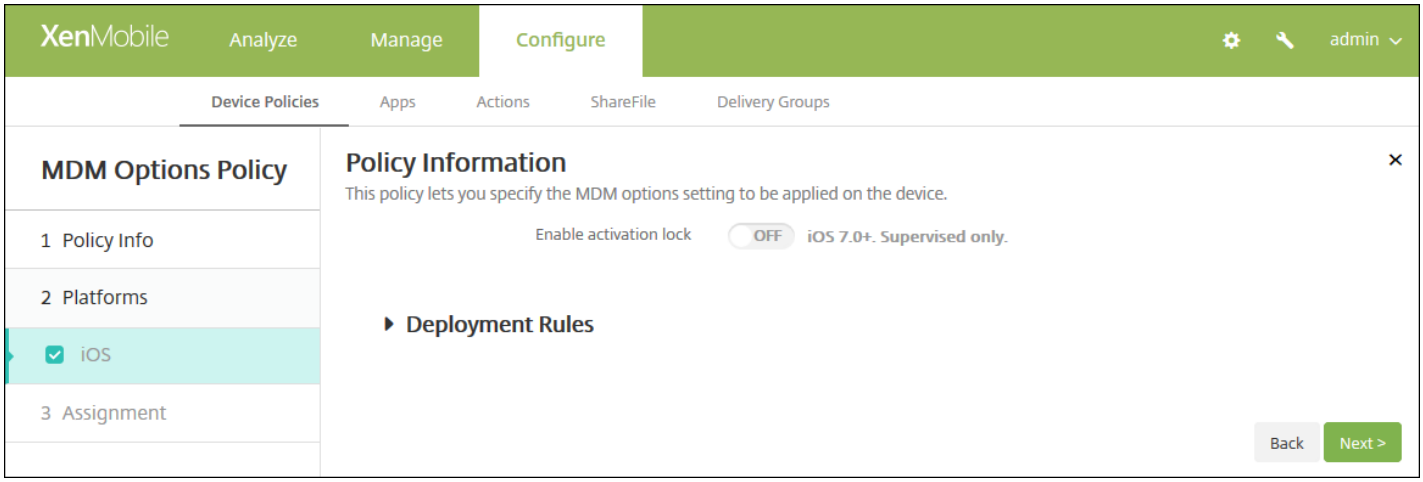
3. Expanda **More** y, en **End user**, haga clic en **MDM Options**. Aparecerá la página de información **MDM Options Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **iOS MDM Policy Platform**.

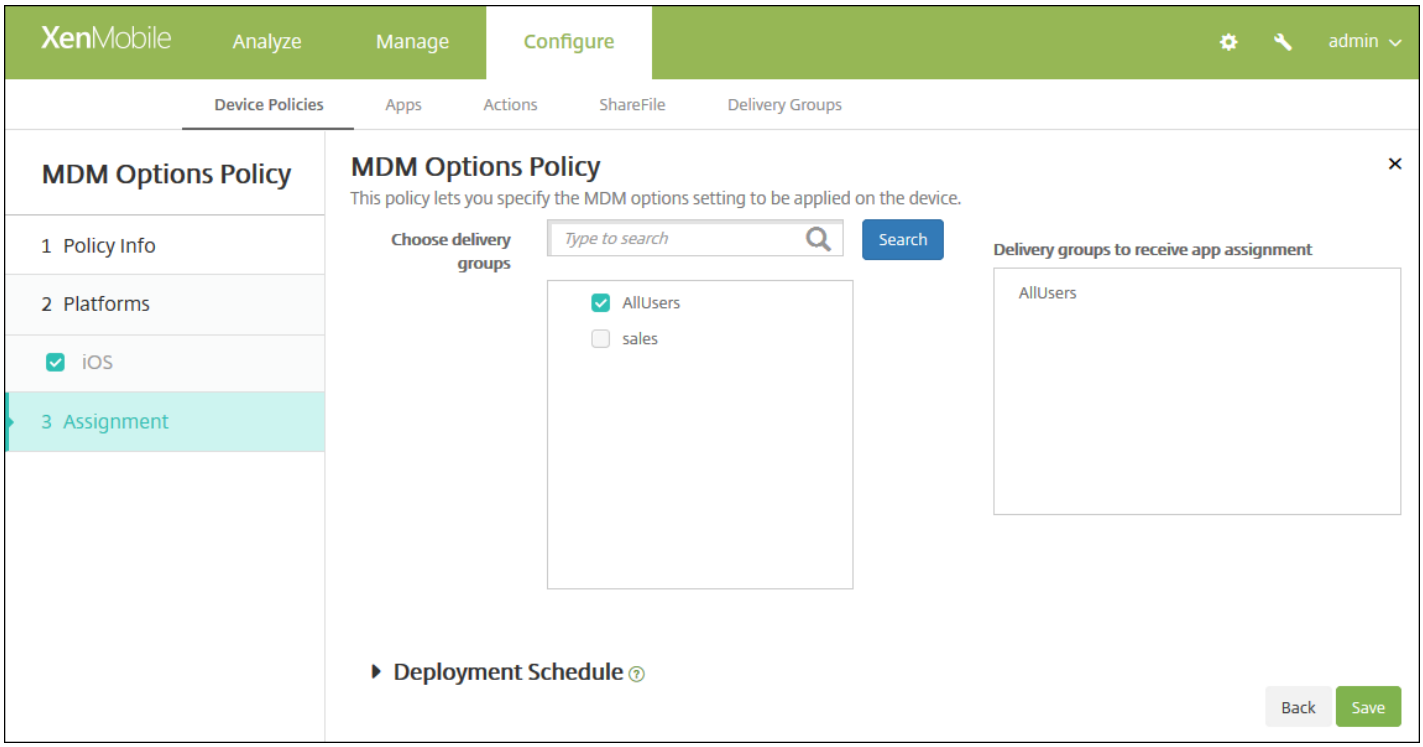


6. Configure este parámetro:

- **Enable Activation Lock**. Seleccione si quiere habilitar la función Bloqueo de activación en los dispositivos a los que se implementará esta directiva. El valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **MDM Options 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 Microsoft Exchange ActiveSync

Jul 27, 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, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX y Windows Phone. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en los siguientes apartados.

Configuración de iOS

Configuración de Mac OS X

Configuración de Android HTC

Configuración de Android TouchDown

Configuración de Android for Work

Configuración de Samsung SAFE y Samsung KNOX

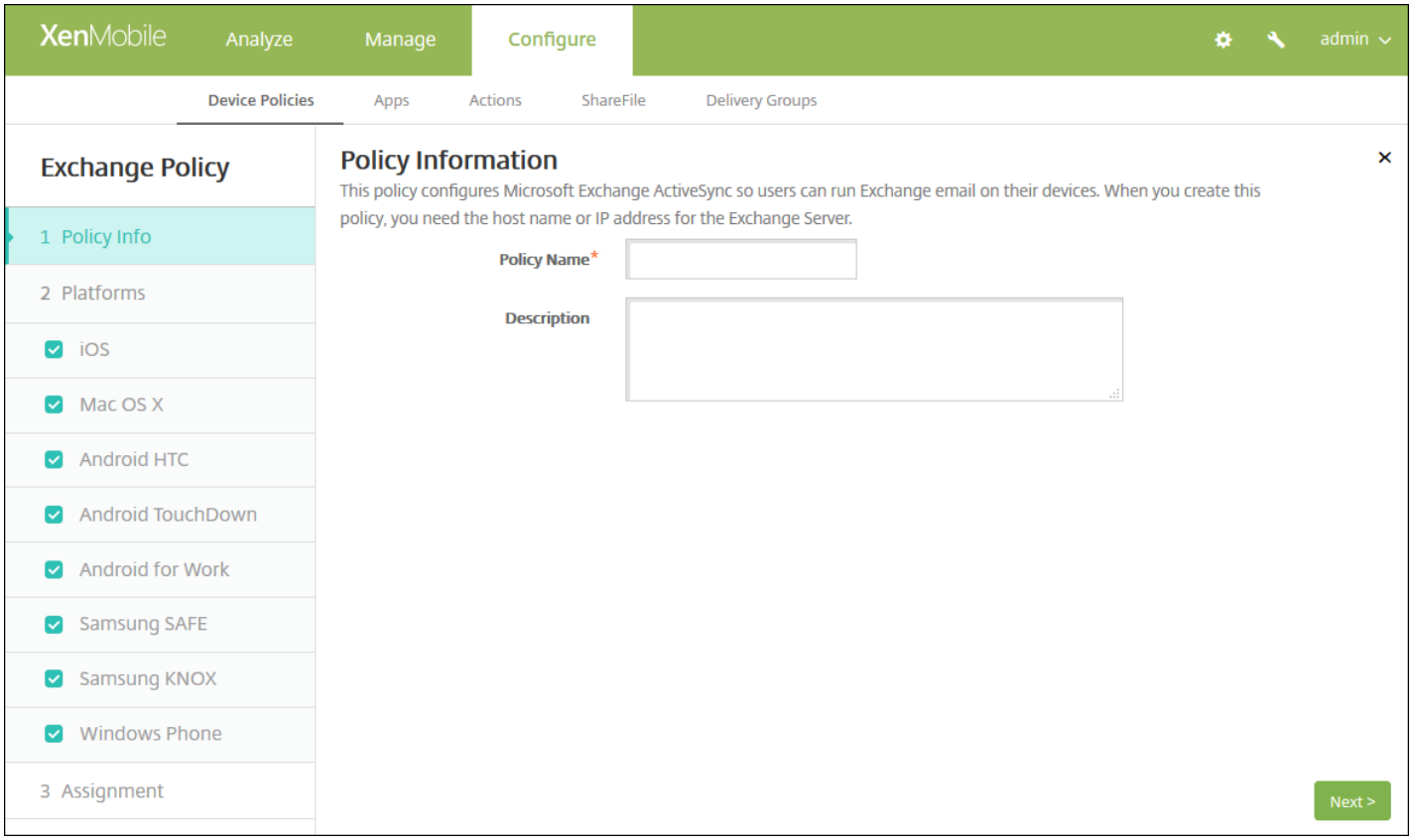
Configuración de Windows Phone

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**. Aparecerá el cuadro de diálogo **Add a New Policy**:

3. Haga clic en **Exchange**. Aparecerá la página de información **Exchange Policy**.



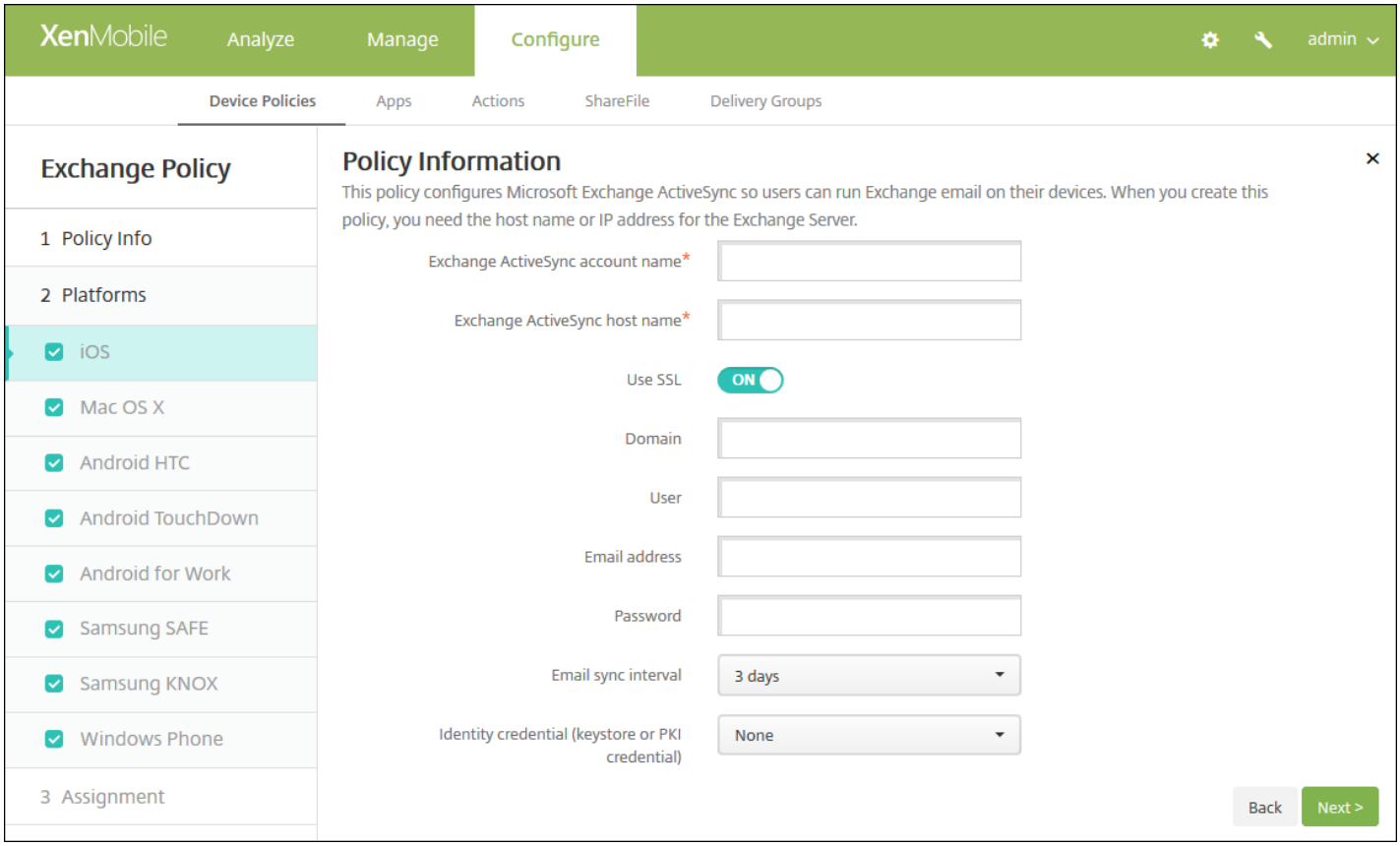
4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



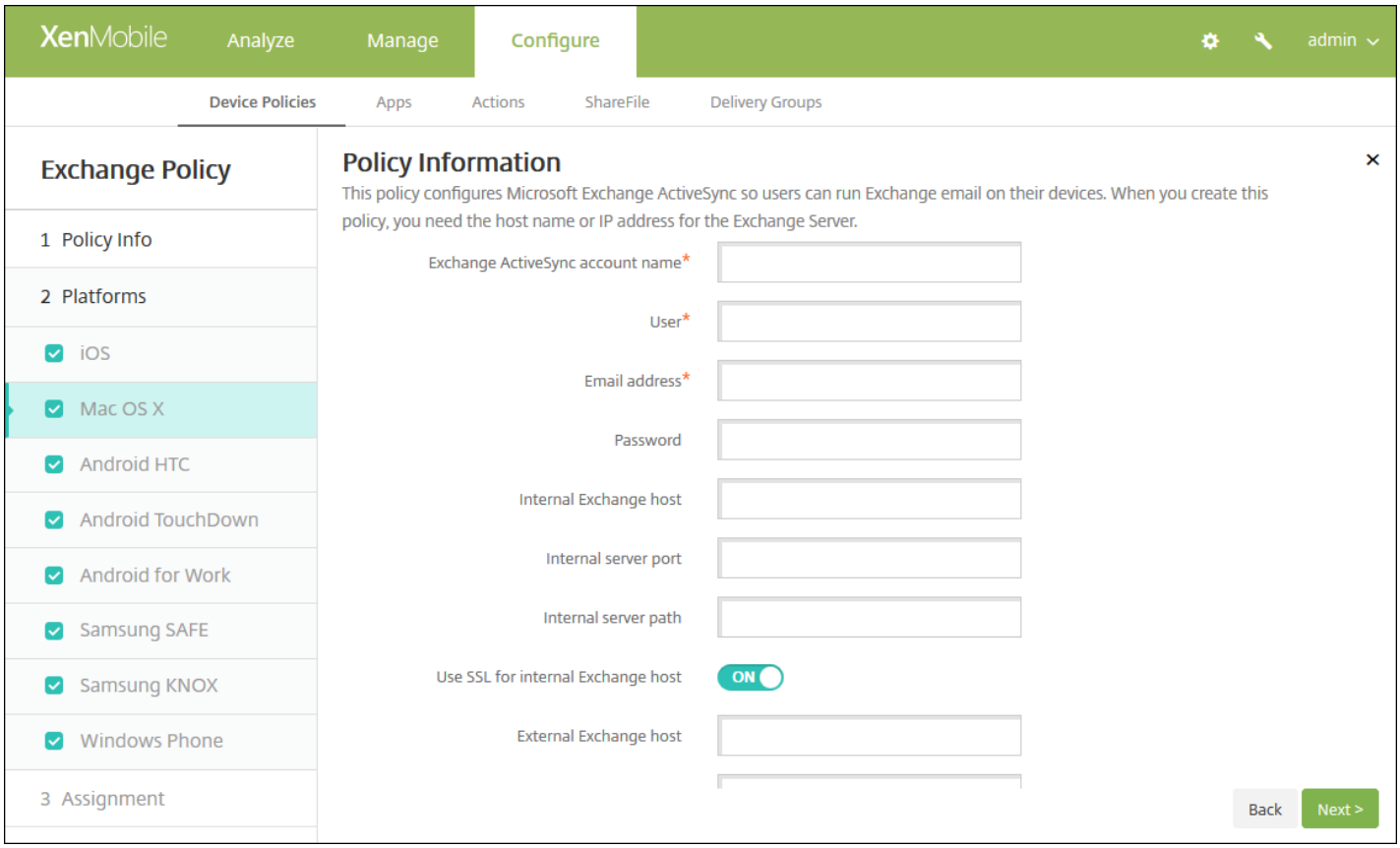
Configure estos parámetros:

- **Exchange ActiveSync account name**. Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Exchange ActiveSync host name**: Escriba la dirección del servidor de correo electrónico.
- **Use SSL**. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **ON**.
- **Domain**. Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema ${user.domainname} en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User**. Especifique el nombre de usuario de la cuenta de usuario de Exchange. 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. Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Password**. Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Email sync interval**. En la lista, seleccione la frecuencia de sincronización del correo electrónico con el servidor Exchange Server. El valor predeterminado es de **3 días**.
- **Identity credential (keystore or PKI)**. En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.
- **Authorize email move between accounts**. Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta y reenviarlos y responderlos desde otra cuenta. El valor predeterminado es **OFF**.
- **Send email only from email app**. Seleccione esta opción para obligar a los usuarios a utilizar la aplicación Correo de iOS para enviar correos electrónicos. El valor predeterminado es **OFF**.
- **Disable email recent syncing**. Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes.

El valor predeterminado es **OFF**. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.

- **Enable S/MIME**. Seleccione si esta cuenta admite el cifrado y la autenticación S/MIME. El valor predeterminado es **OFF**. Si se establece en **ON**, aparecen los dos campos siguientes:
  - **Signing identity credential**. El valor predeterminado es **None**.
  - **Encryption identity credential**. El valor predeterminado es **None**.
- **Enable per message S/MIME switch**. Seleccione si permitir que los usuarios cifren cada correo electrónico saliente. El valor predeterminado es **OFF**.

Configuración de los parámetros de Mac OS X



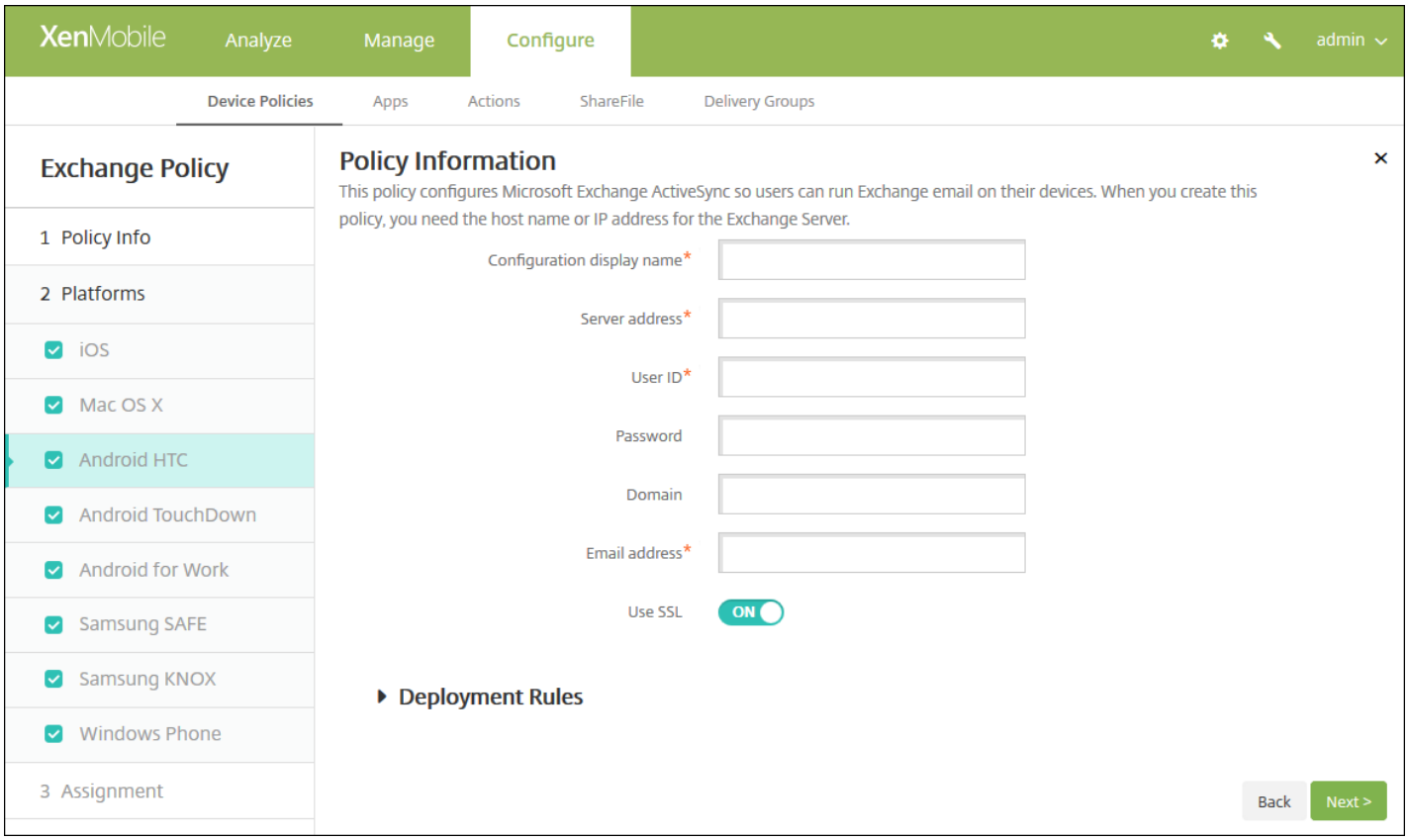
Configure estos parámetros:

- **Exchange ActiveSync account name**. Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **User**. Especifique el nombre de usuario de la cuenta de usuario de Exchange. 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. Puede utilizar la macro de sistema ${user.mail} en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Password**. Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Internal Exchange host**. Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host interno de Exchange.
- **Internal server host**. Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto interno de Exchange Server.
- **Internal server path**. Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta

de servidor interno de Exchange.

- **Use SSL for internal Exchange host**. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **ON**.
- **External Exchange host**. Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host externo de Exchange.
- **External server host**. Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto externo de Exchange Server.
- **External server path**. Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor externo de Exchange.
- **Use SSL for external Exchange host**. Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **ON**.
- **Allow Mail Drop**. Seleccione si permitir que los usuarios compartan archivos entre dos equipos Mac de forma inalámbrica (sin tener que conectarse a una red existente). El valor predeterminado es **OFF**.

Configuración de los parámetros de Android HTC

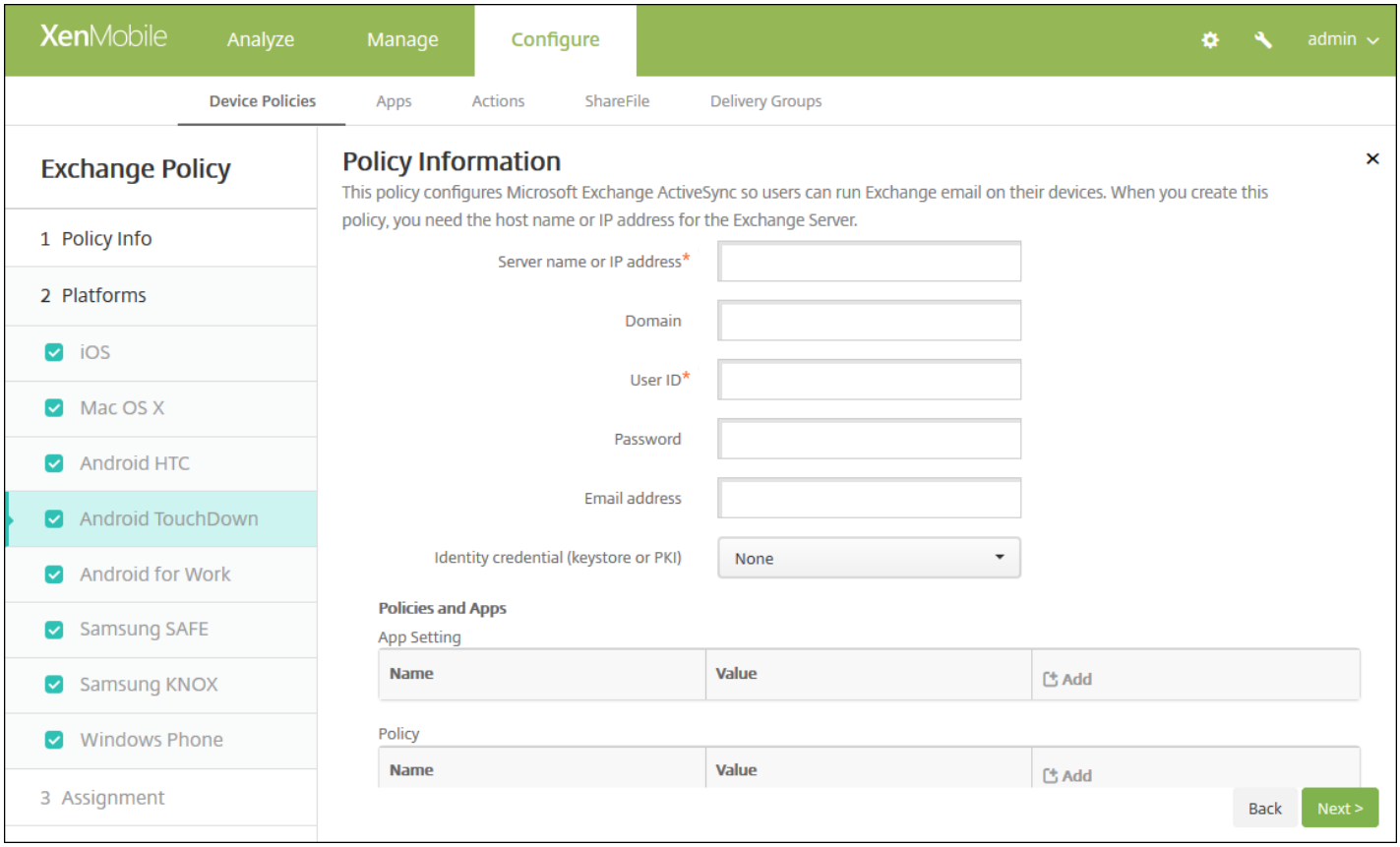


Configure estos parámetros:

- **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. 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. 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. 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**.

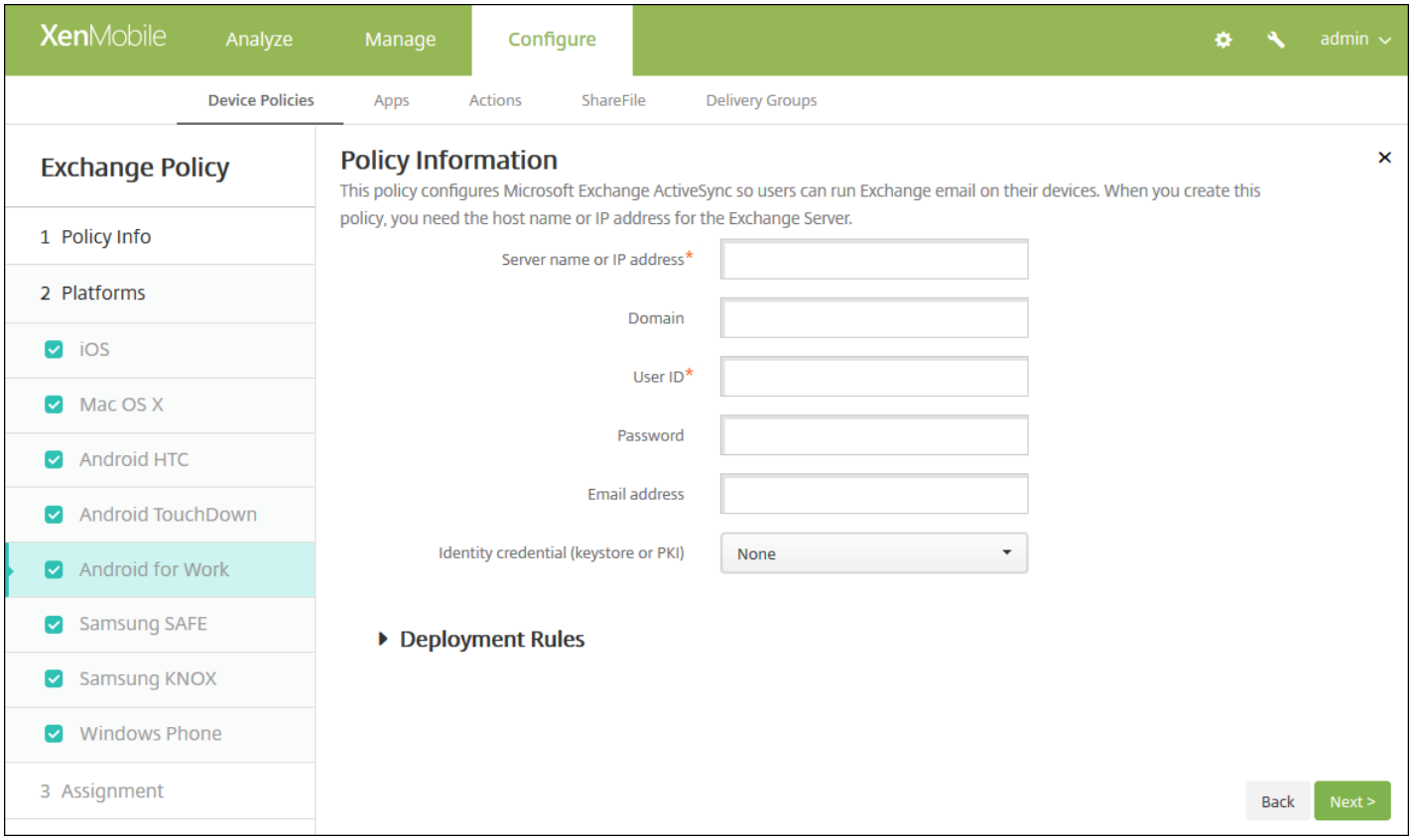
Configuración de los parámetros de Android TouchDown



Configure estos 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. 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. 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. 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 identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.
- **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.

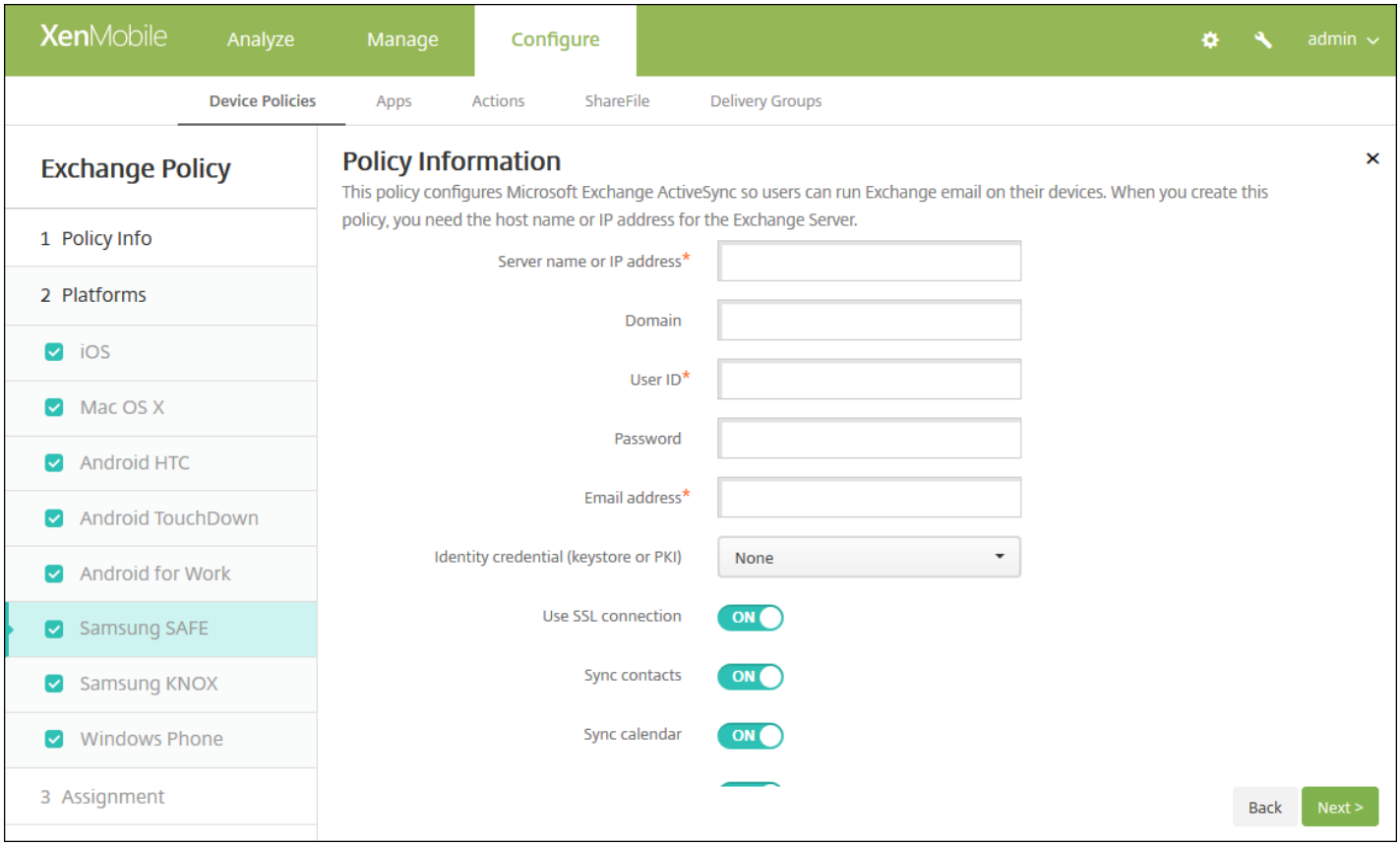
Configuración de los parámetros de Android for Work



Configure estos 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. 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. 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. 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 identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.

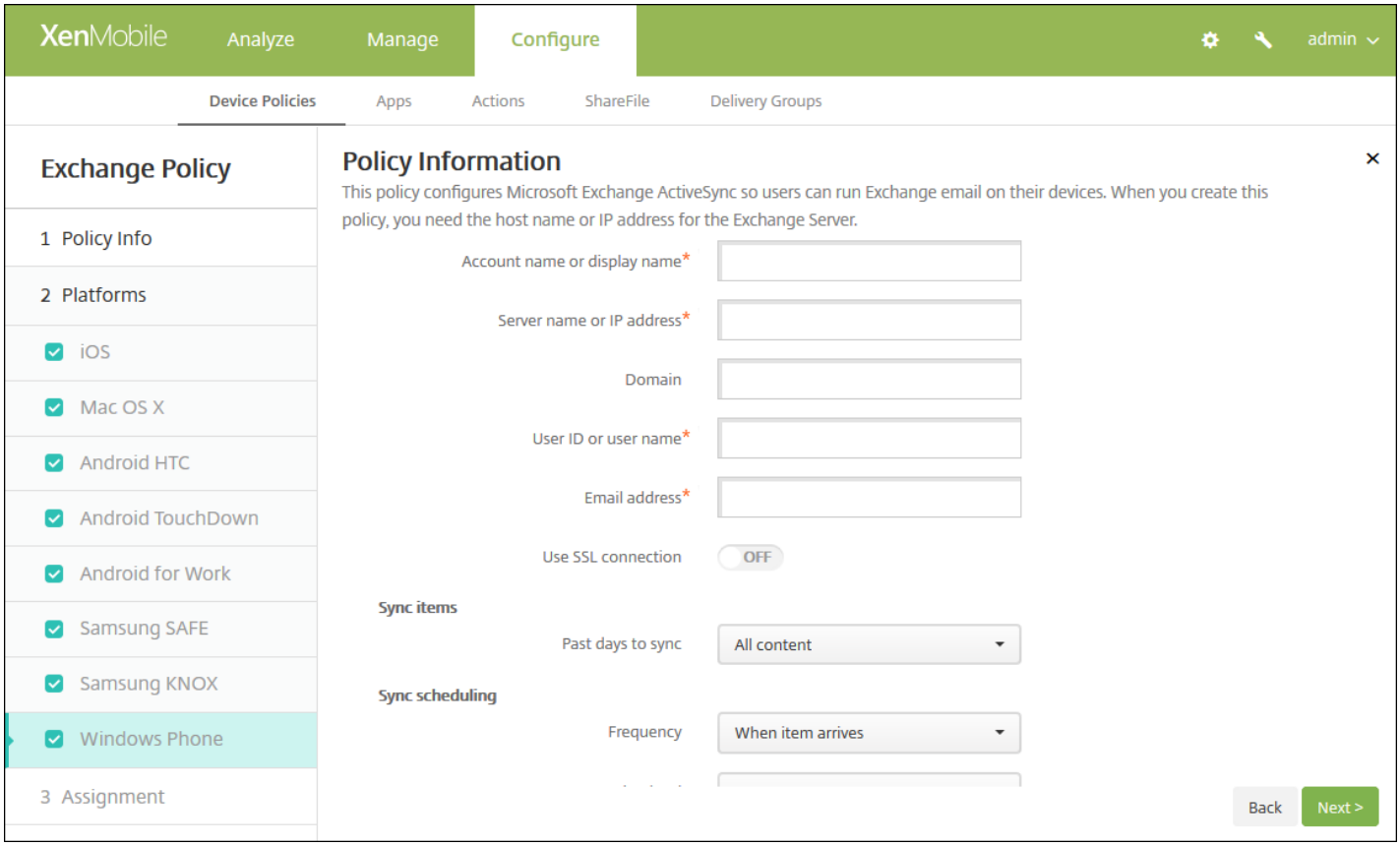
Configuración de los parámetros de Samsung SAFE y Samsung KNOX



Configure estos 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. 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. 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. 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 identidades 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**.

Configuración de los parámetros de Windows Phone



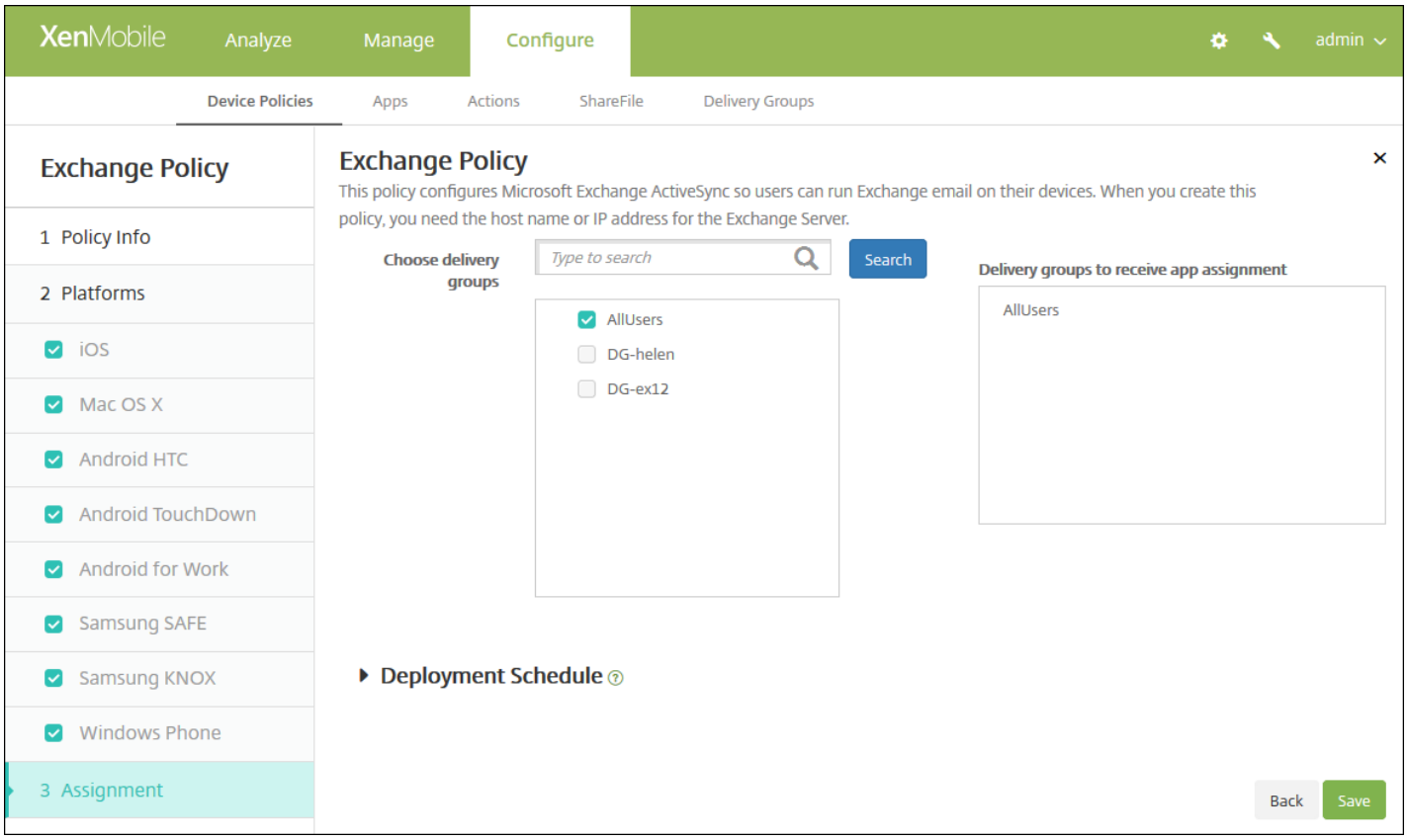
Configure estos parámetros:

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. 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. 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. 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. El valor predeterminado es **All content**.
- **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. El valor predeterminado es **When it arrives**.
- **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. El valor predeterminado es **Disabled**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Exchange 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

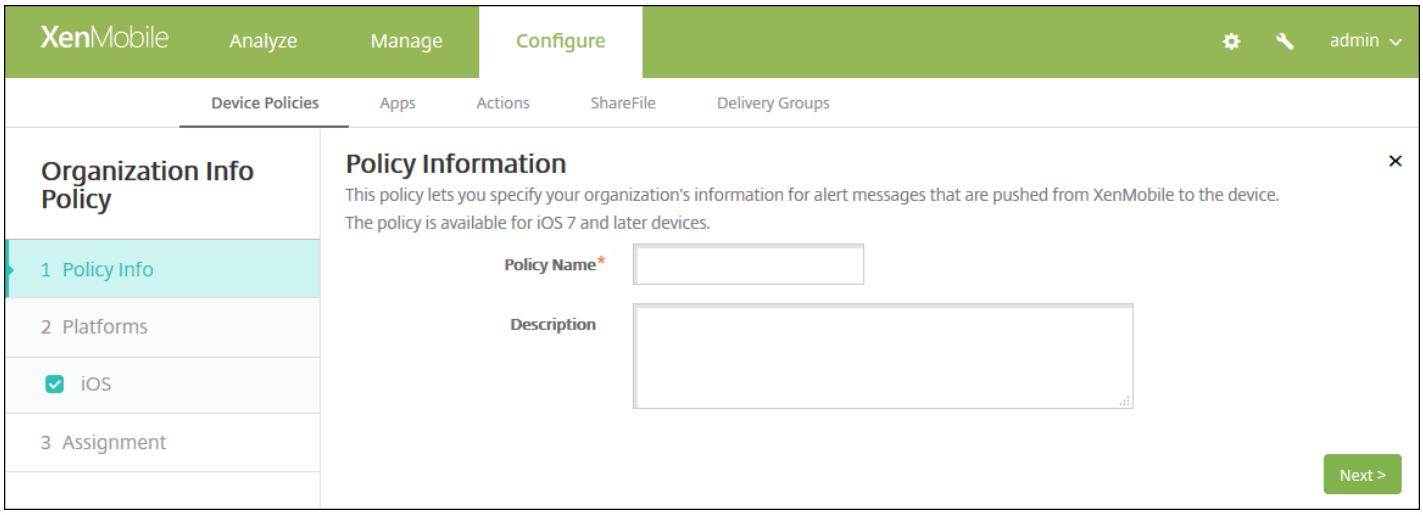
10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

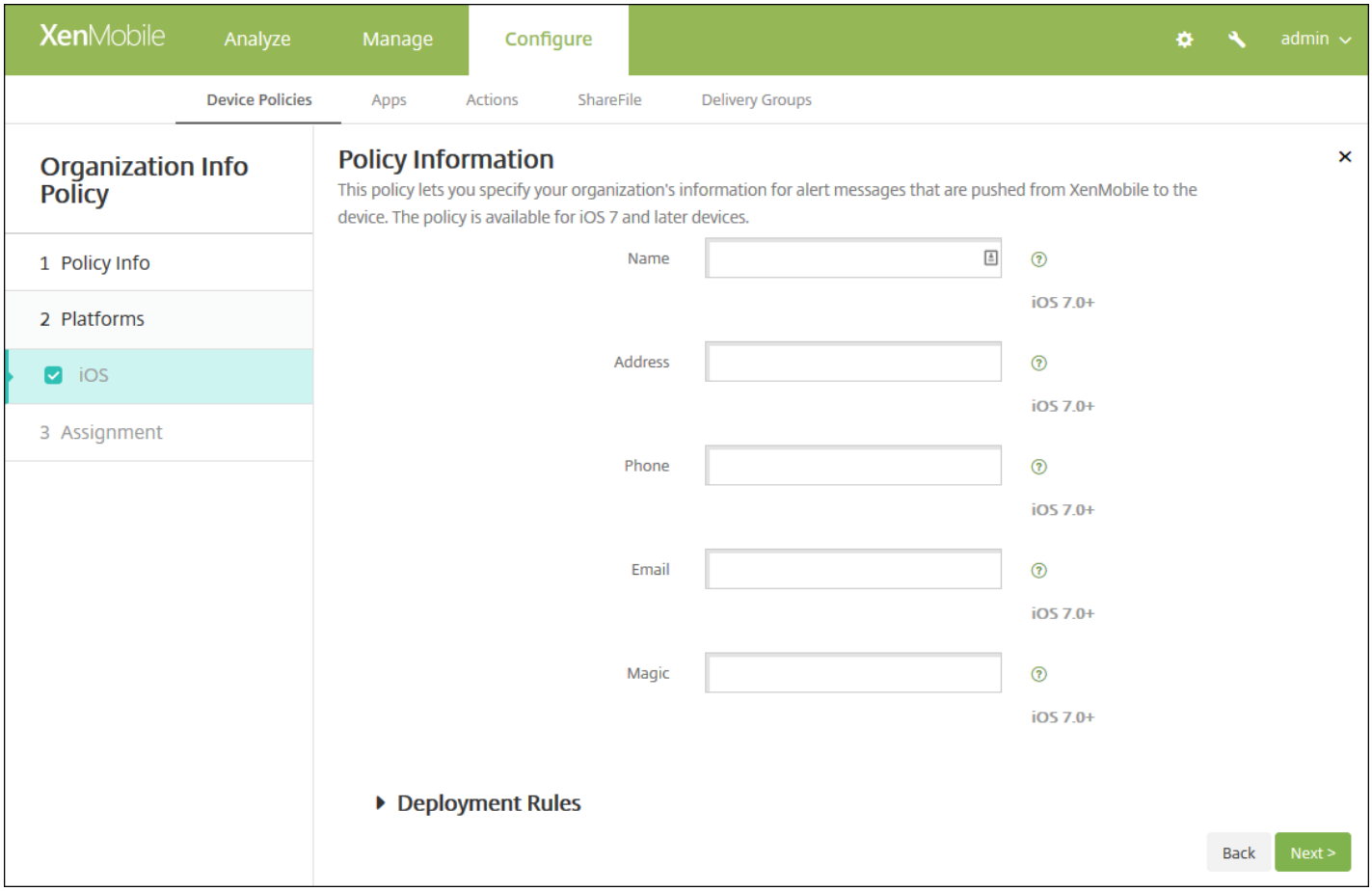
Nota:

- 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.
- 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.

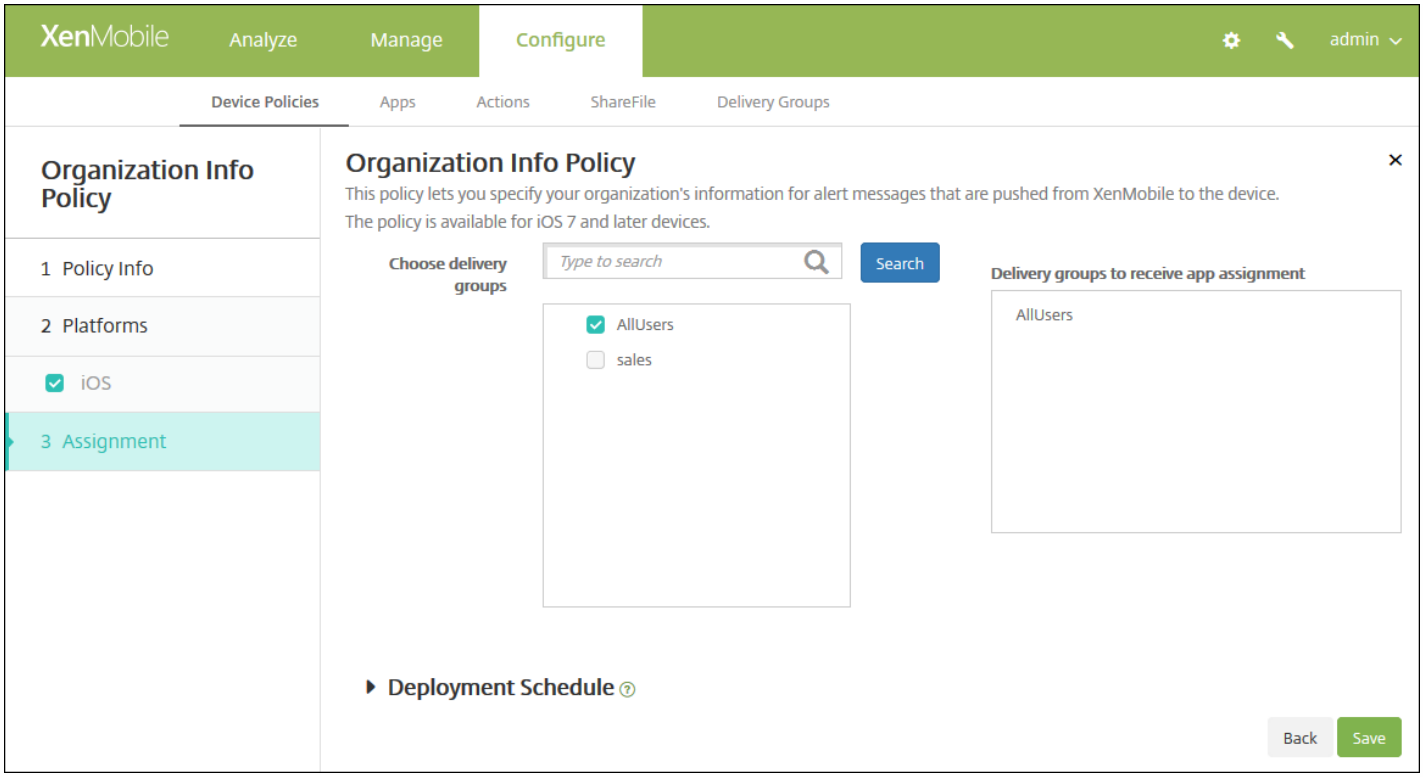
11. Haga clic en **Save**.

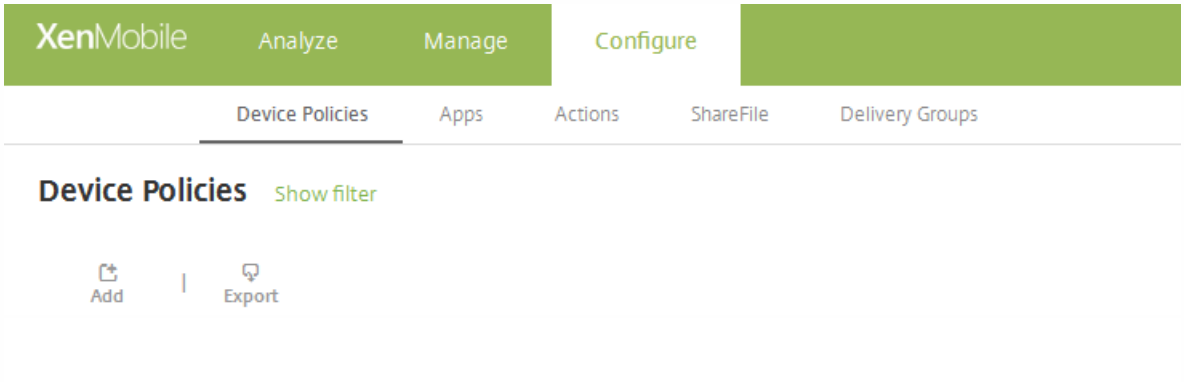


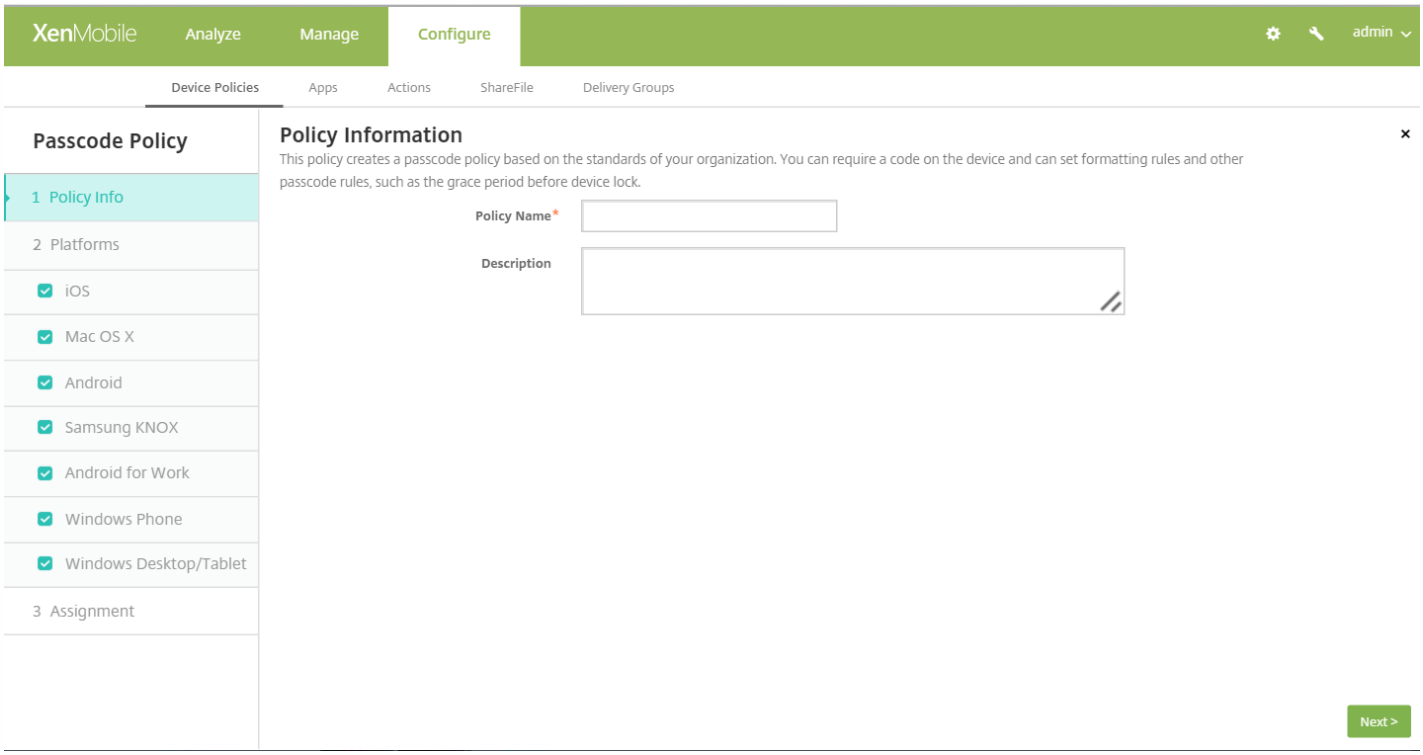
-
-



-
-
-
-
-

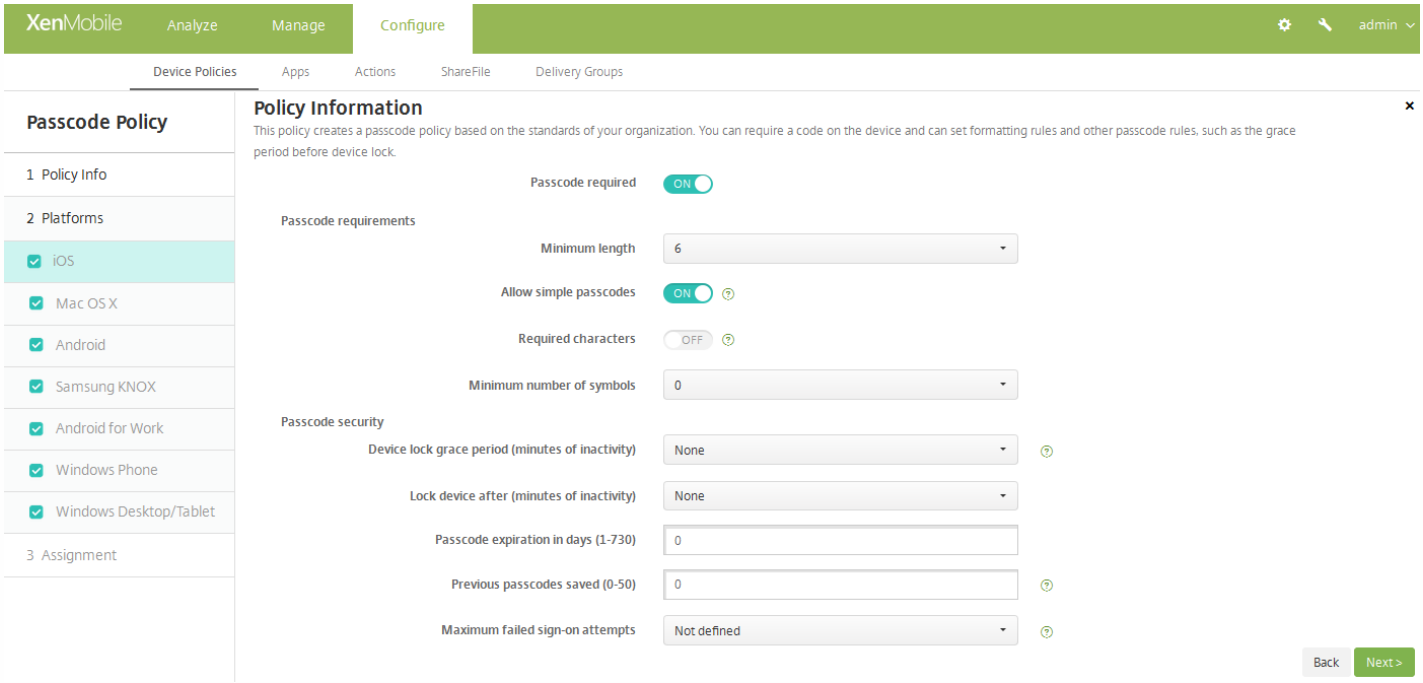






-
-

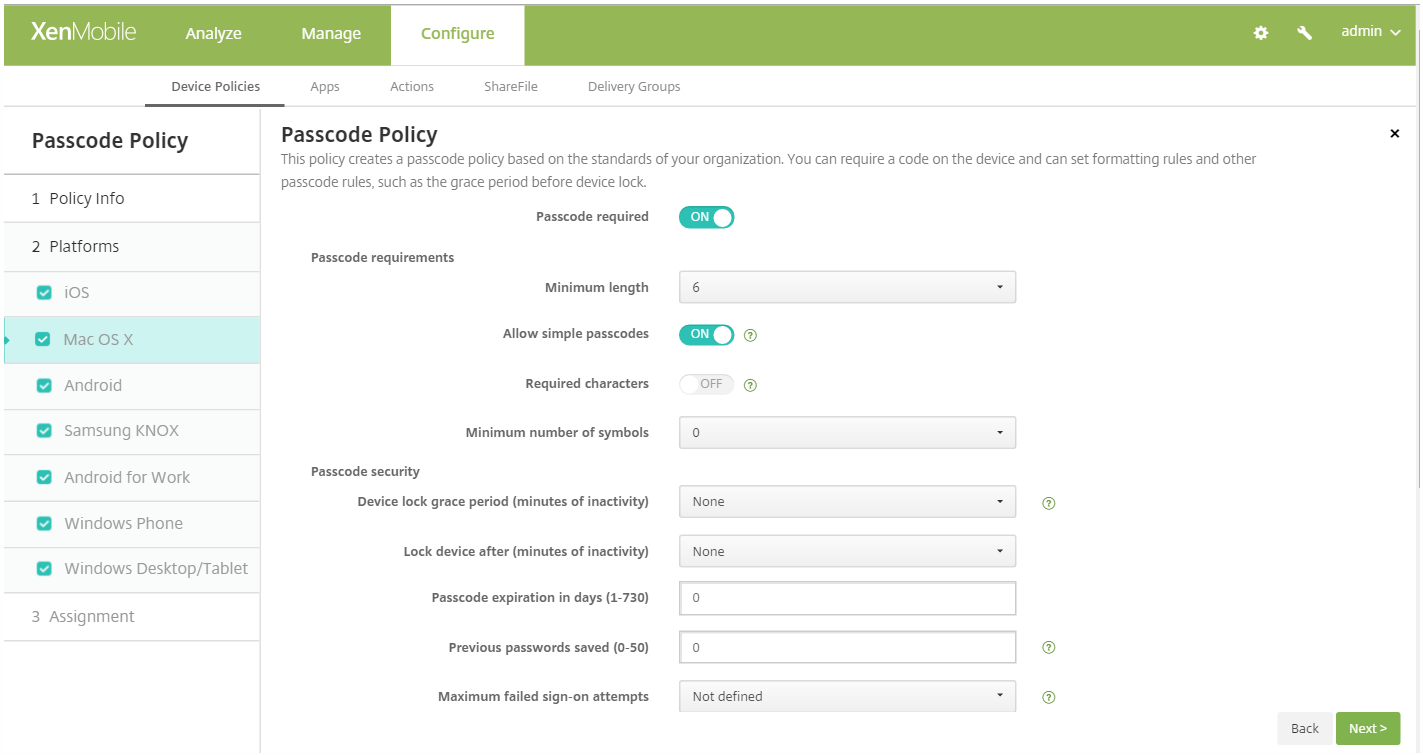
Configuración de los parámetros de iOS



-
-
  -
  -
  -
  -
-
  -
  -
  -
  -

-
-
  -
  -
  -
  -

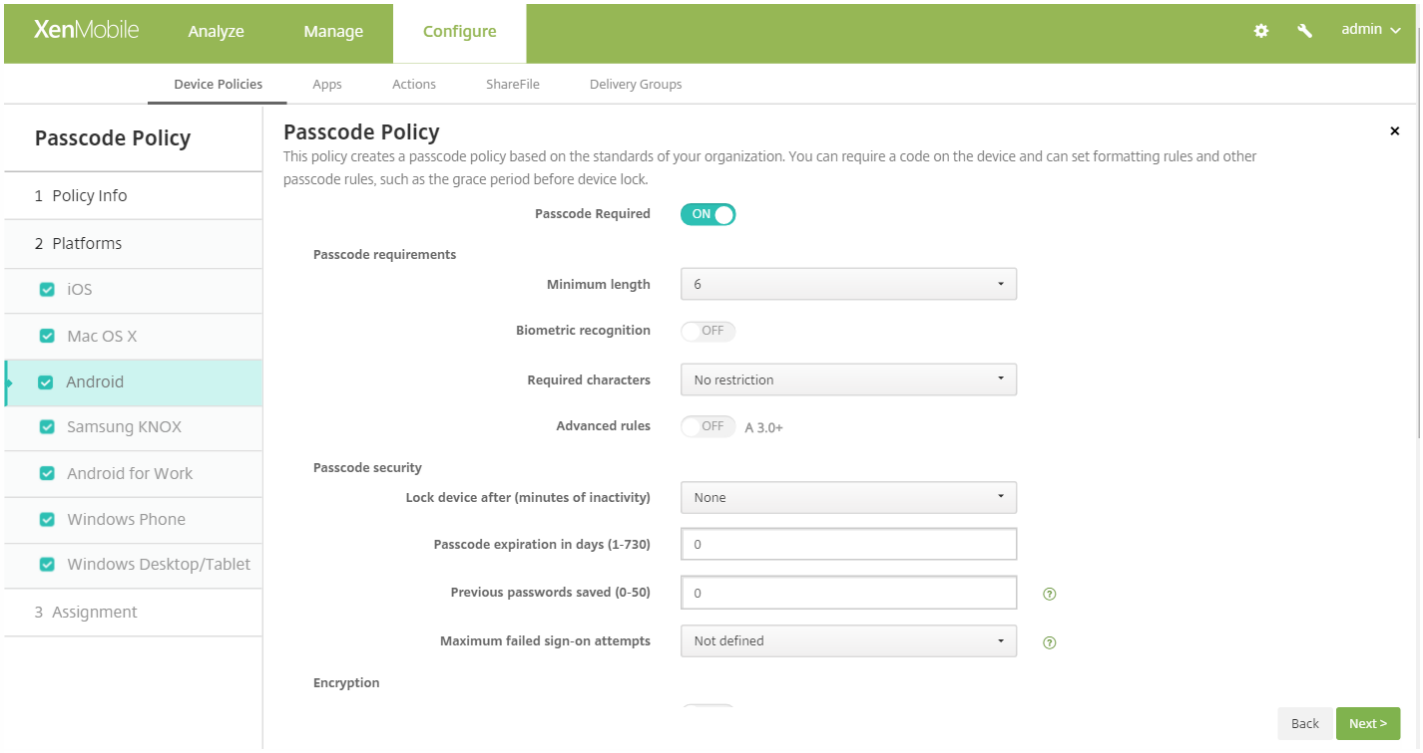
Configuración de los parámetros de Mac OS X



-
-
-
-
  -
  -

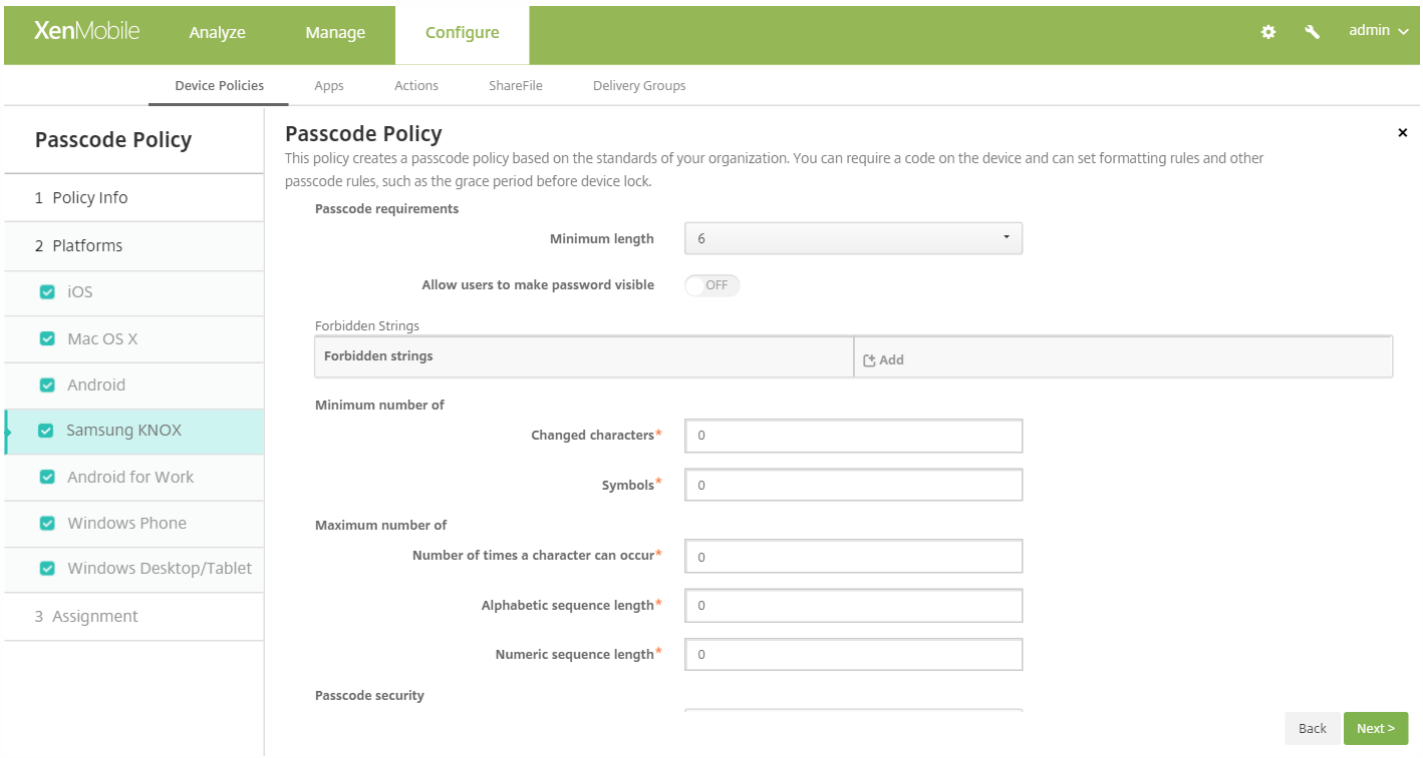
-
-
-
  -
  -
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
  -
  -

Configuración de los parámetros de Android



-
-
  -
  -
  -
  -
  -
    -
    -
    -
    -
    -
    -
    -
-

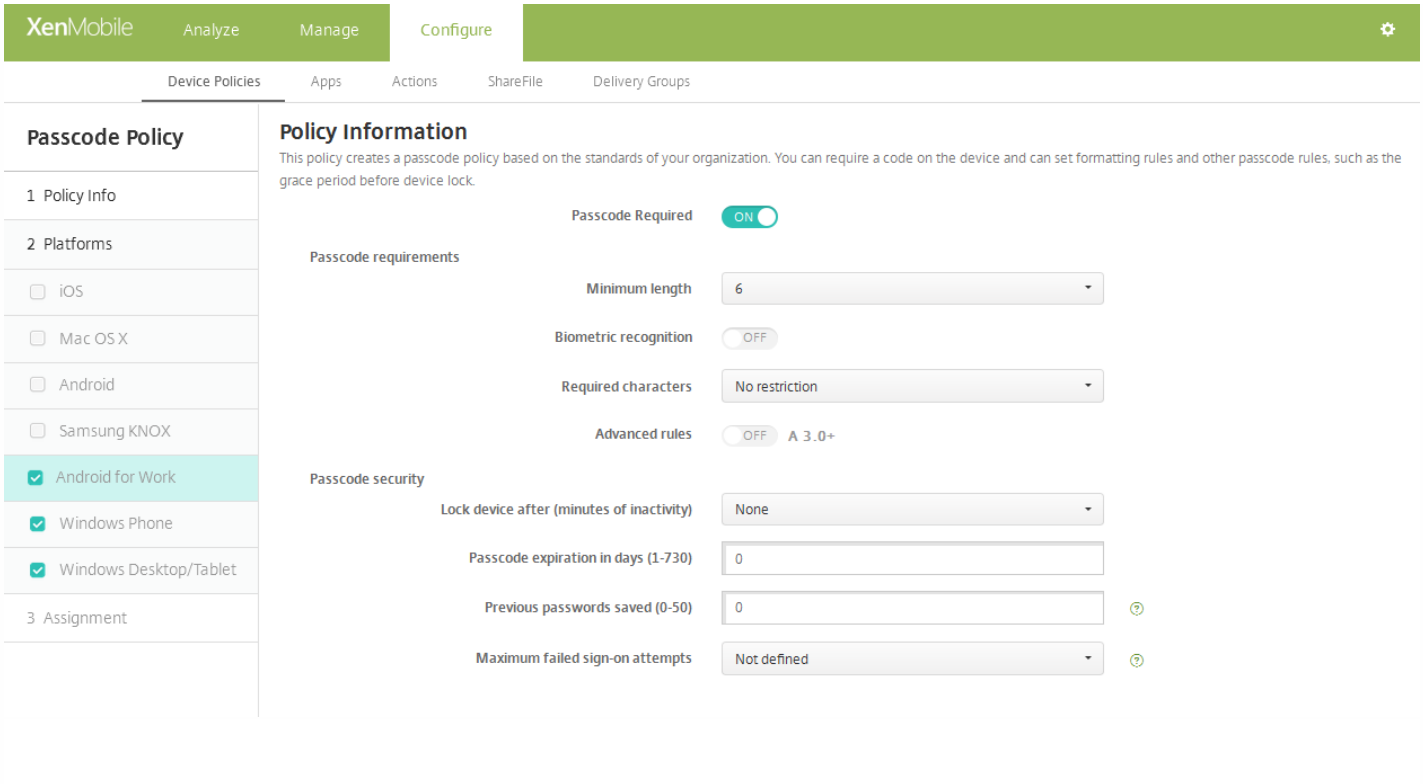
Configuración de los parámetros de Samsung KNOX



-
  -
  -
  -
    -
    -

-
  -
  -
-
  -
  -
  -
-
  -
  -
  -
  -
  -

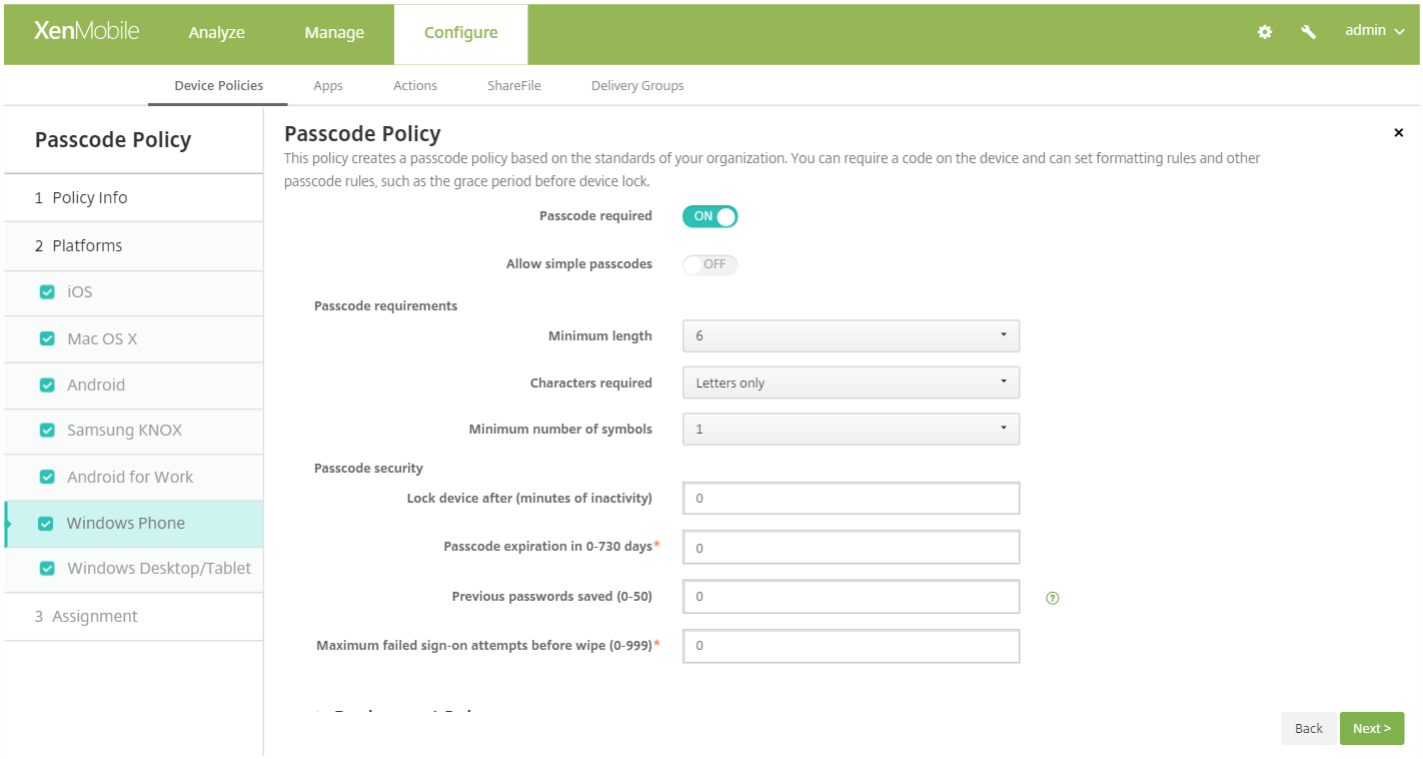
Configuración de los parámetros de Android for Work



-
-
  -
  -
  -
  -
  -
    -
    -
    -
    -
    -
    -
-

-
-
-
-

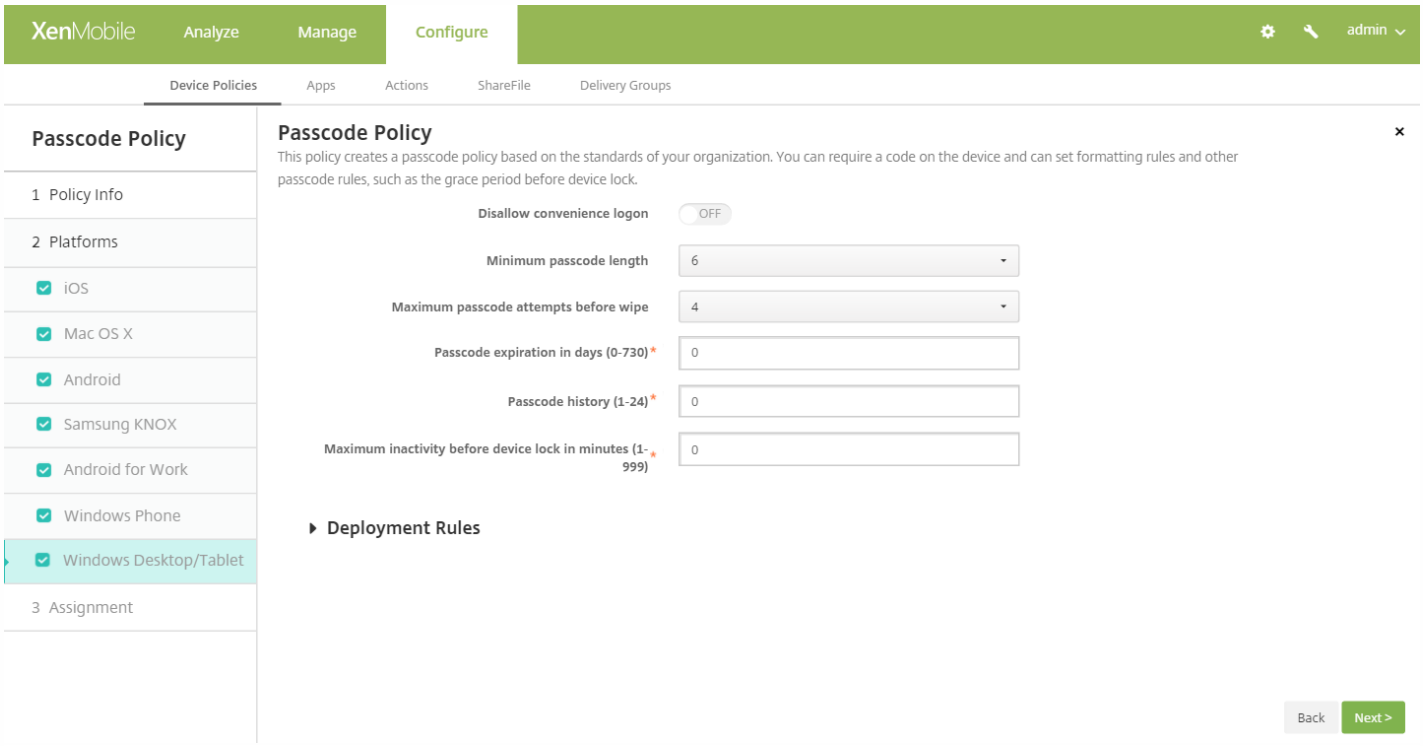
Configuración de los parámetros de Windows Phone



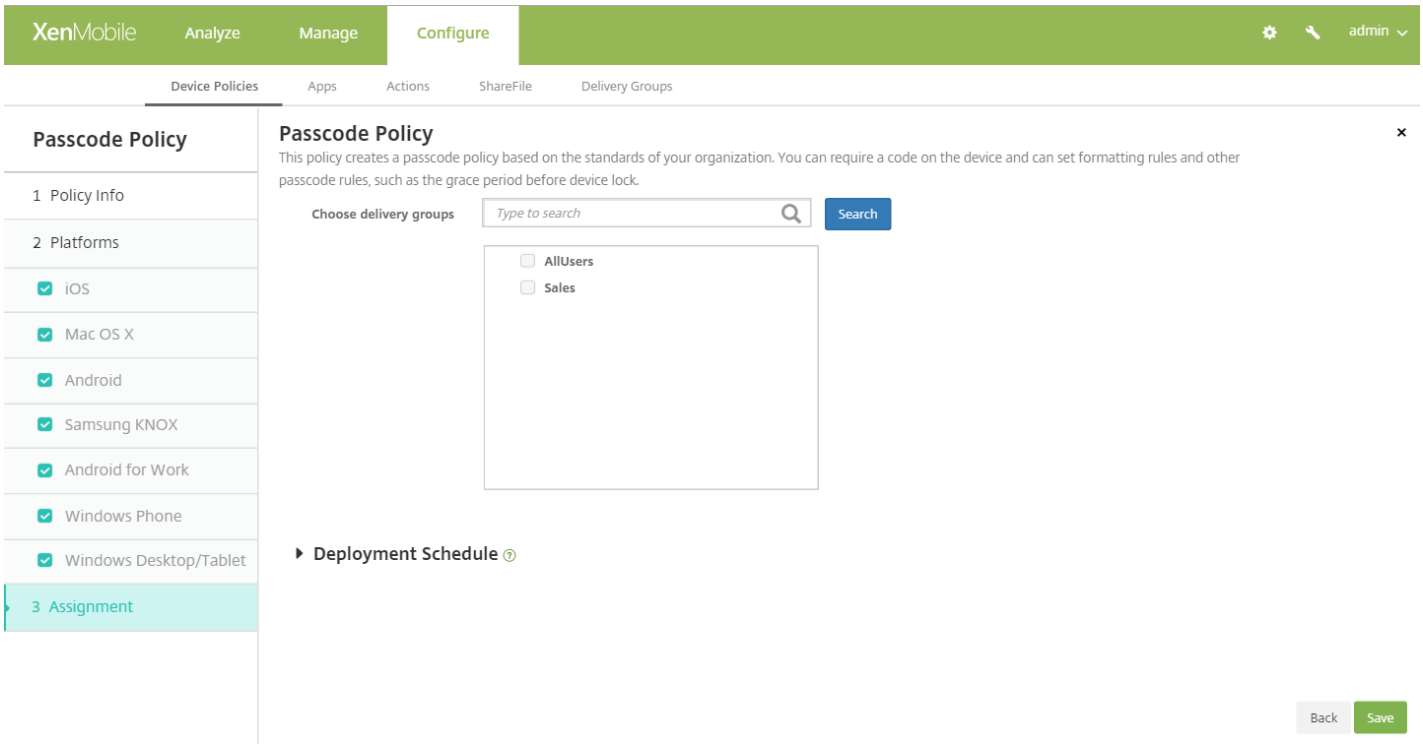
-
-
-
-
-

-
-
-
-
-
-

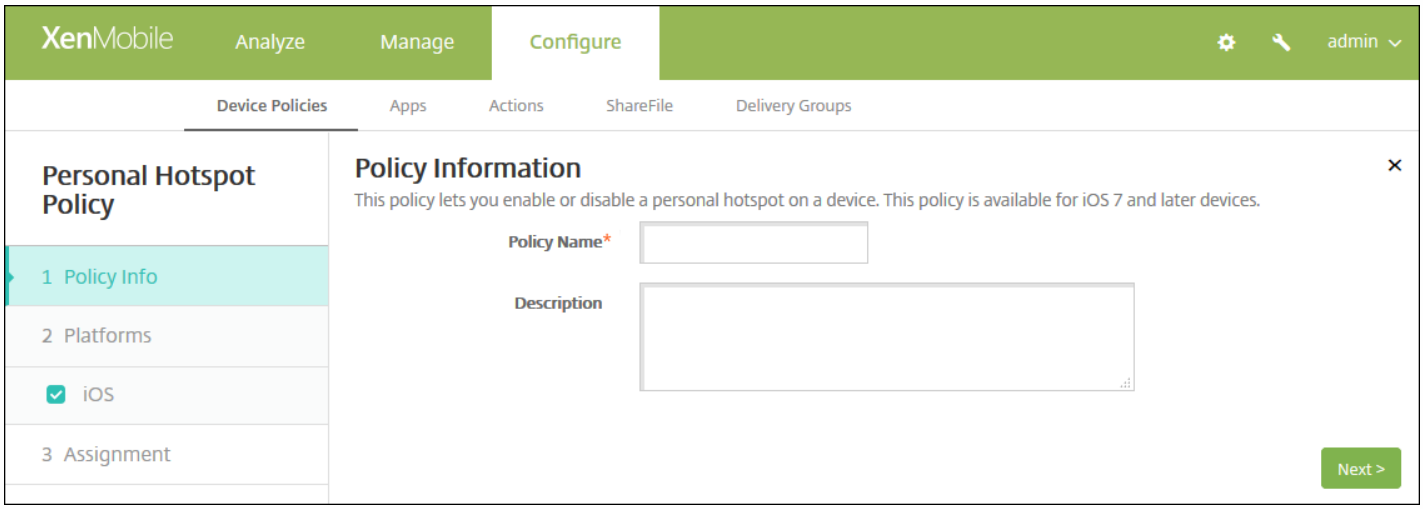
Configuración de los parámetros de escritorios o tabletas Windows



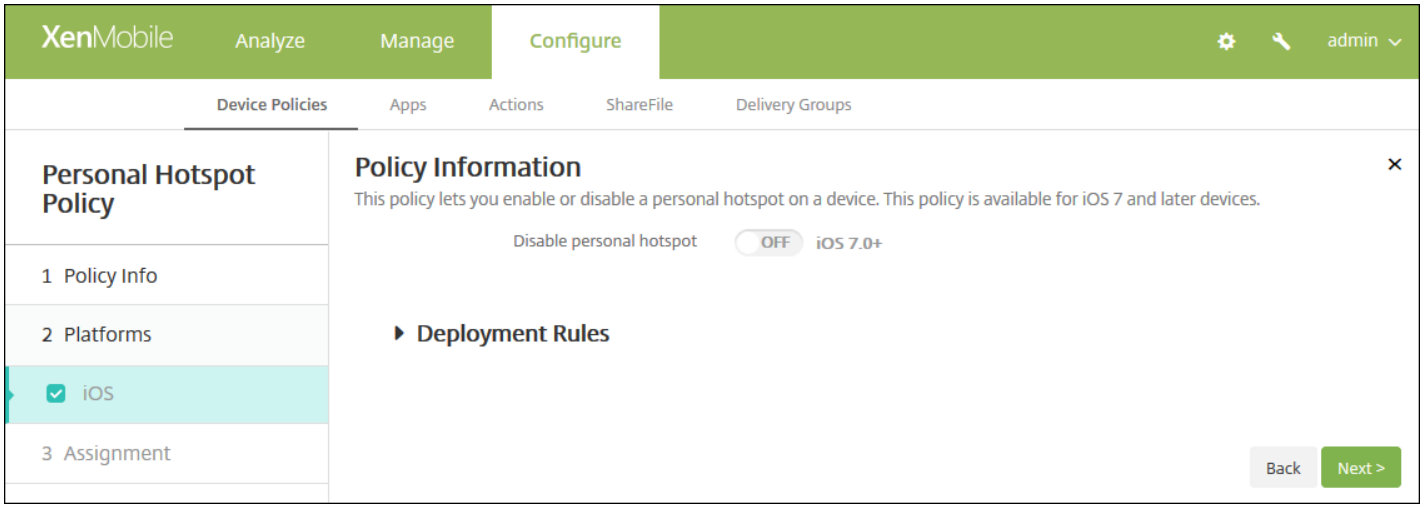
-
-
-

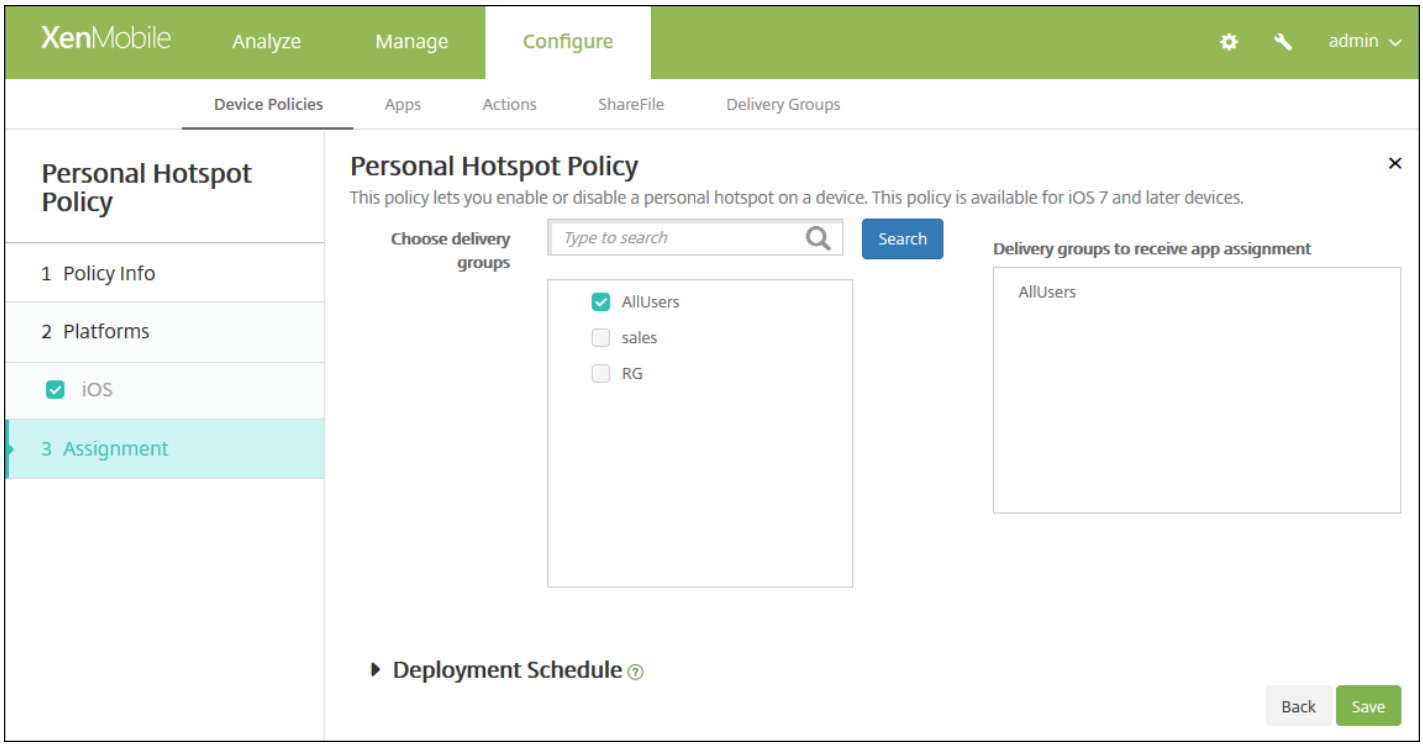


-
-
-

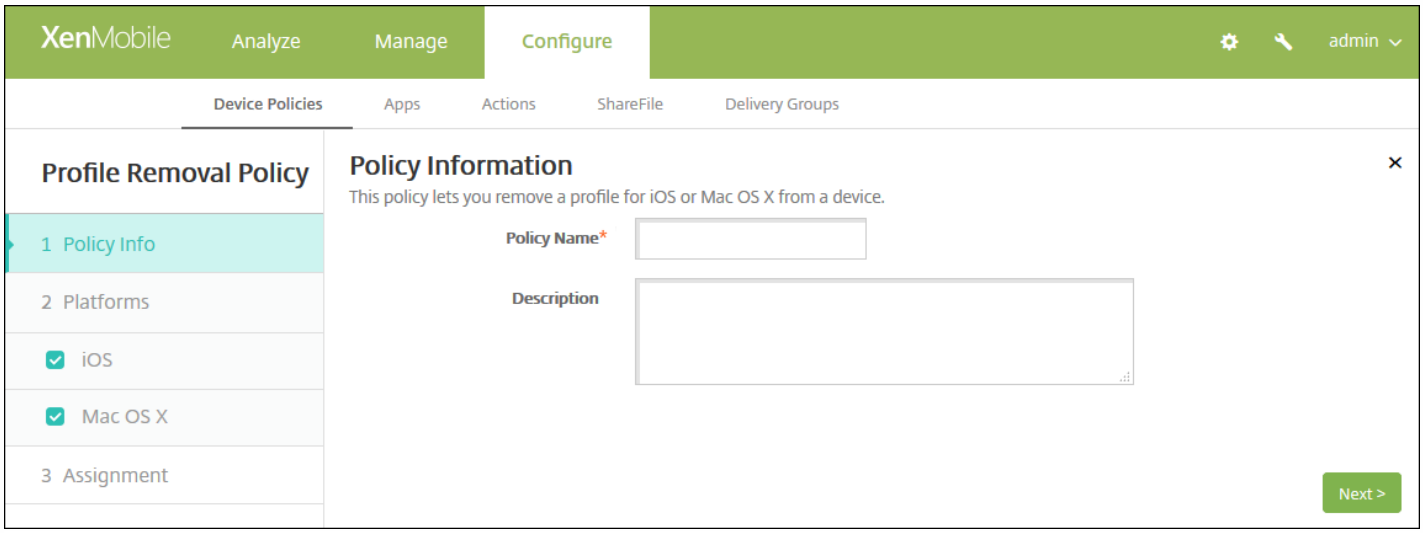


-
-



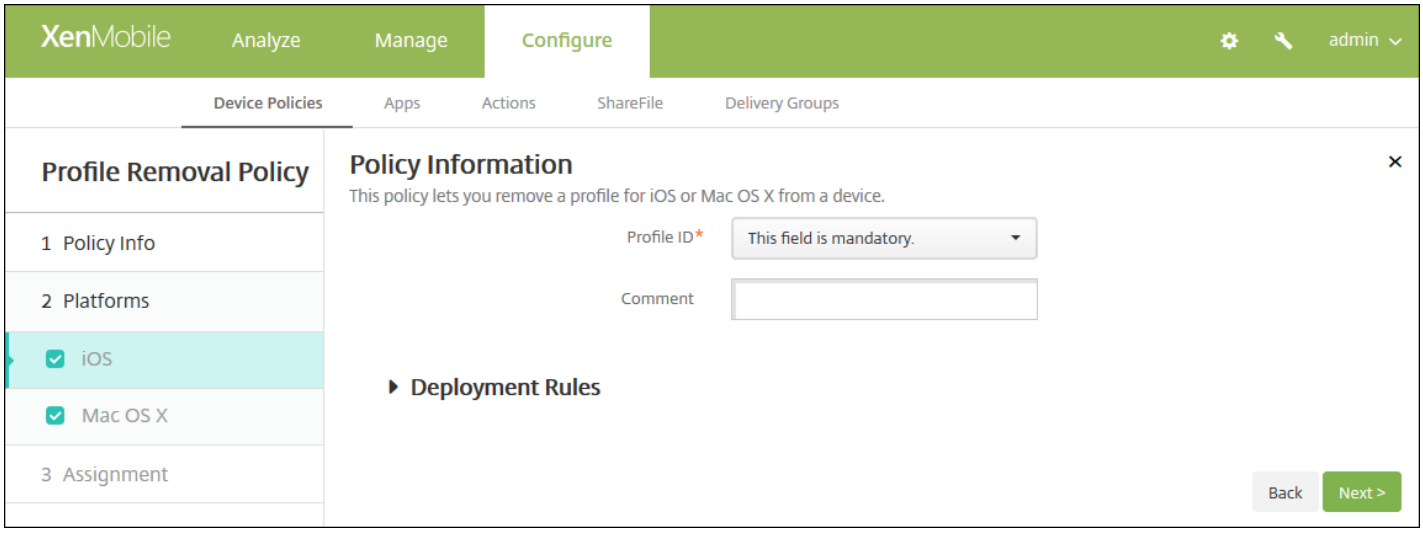


-
-
-
-
-
-
-



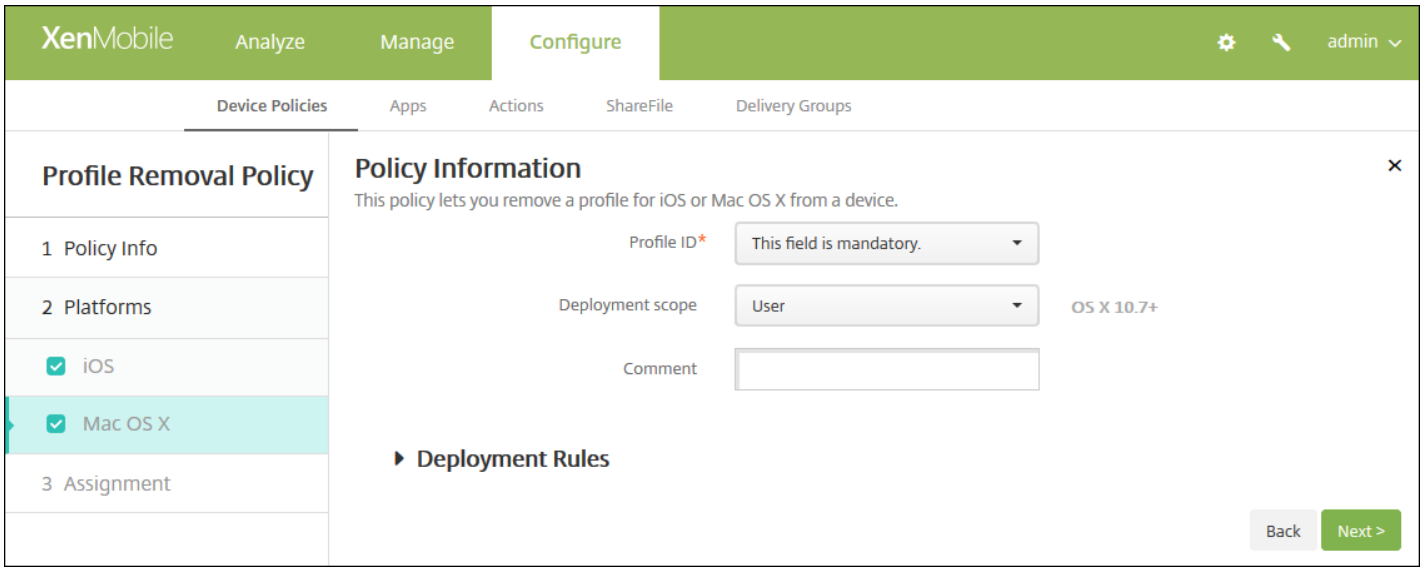
-
-

Configuración de los parámetros de iOS

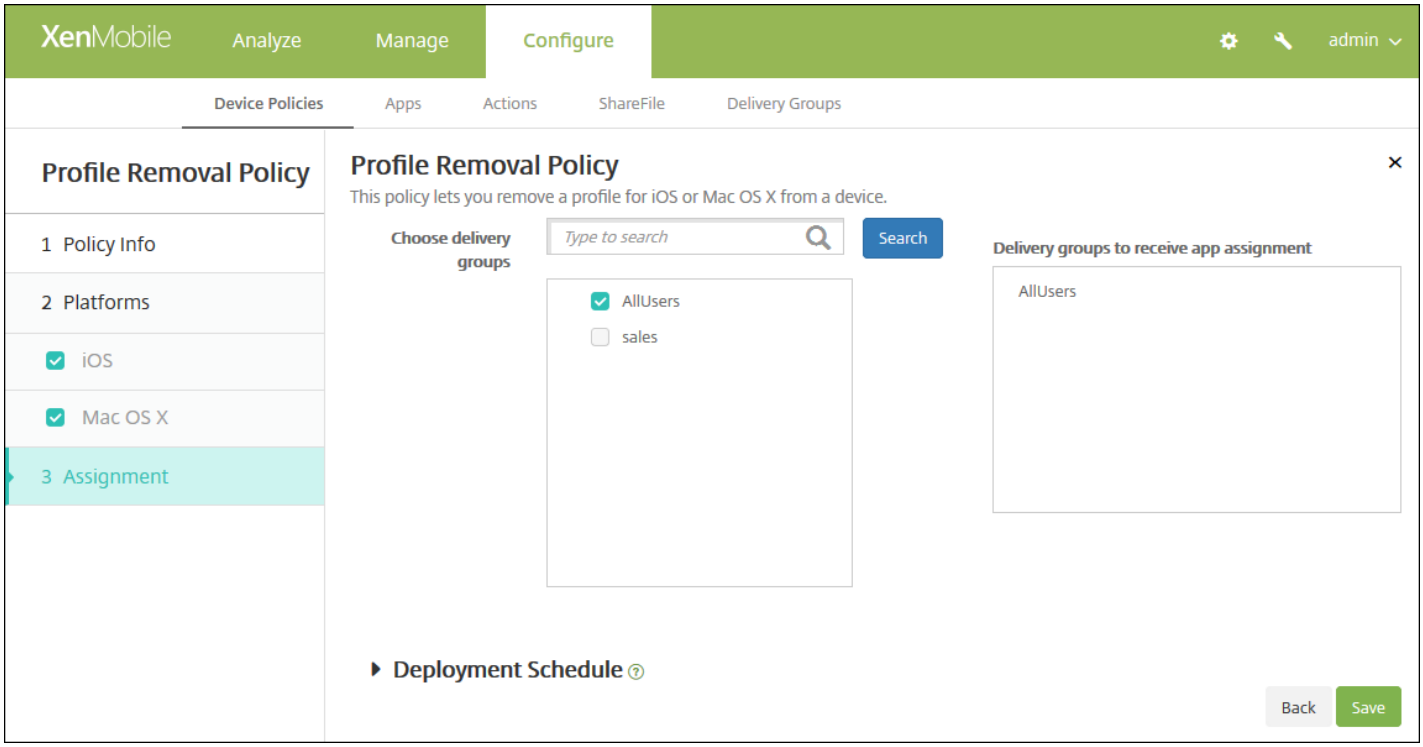


-
-

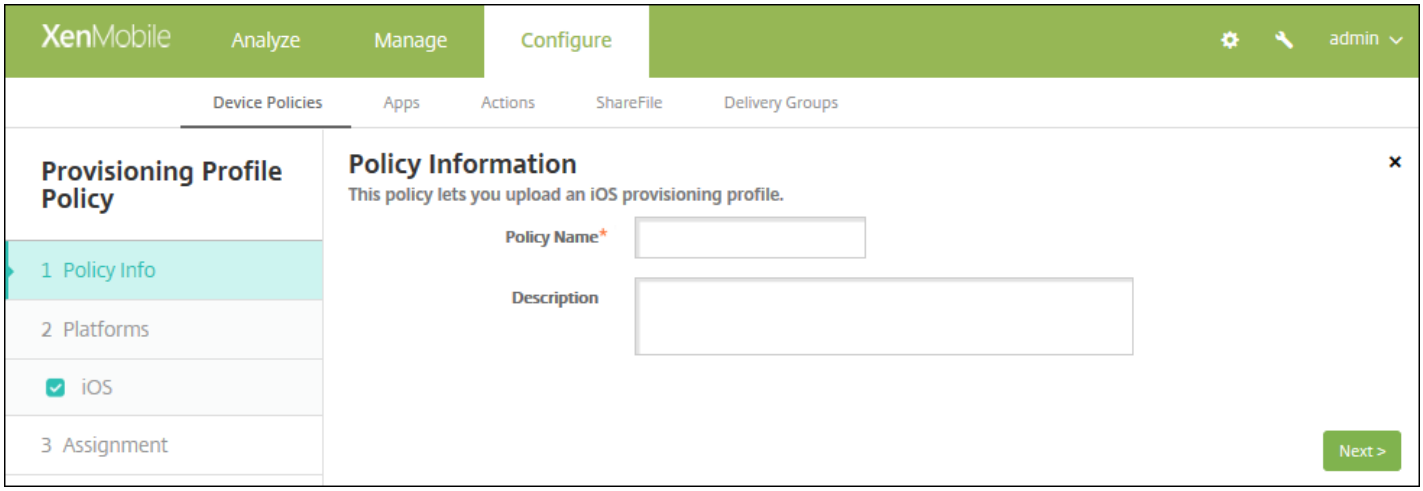
Configuración de los parámetros de Mac OS X



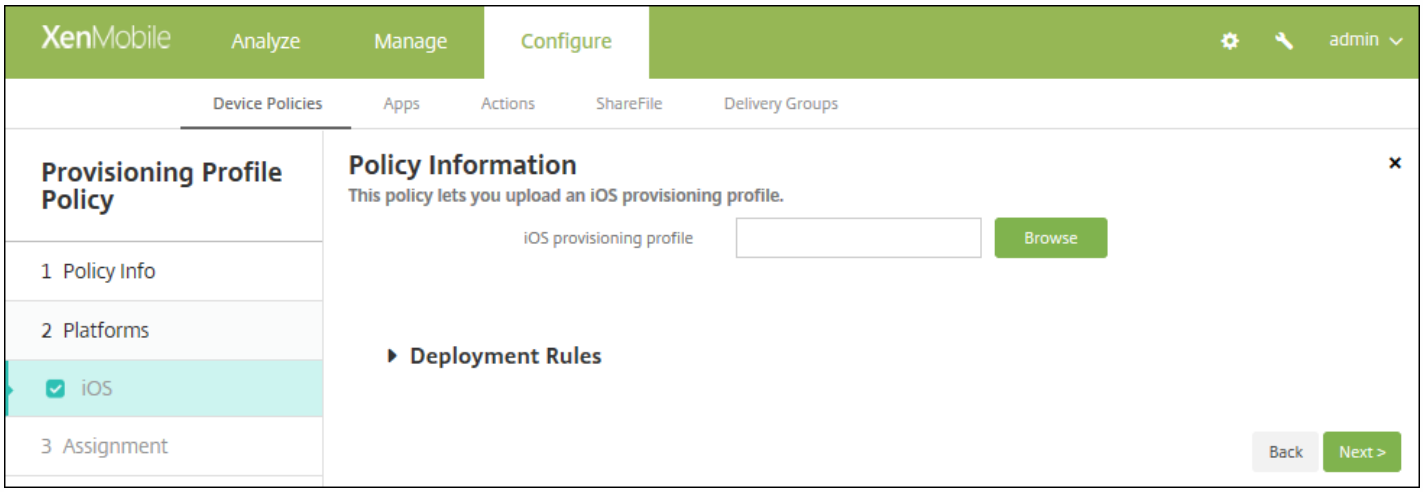
-
-
-



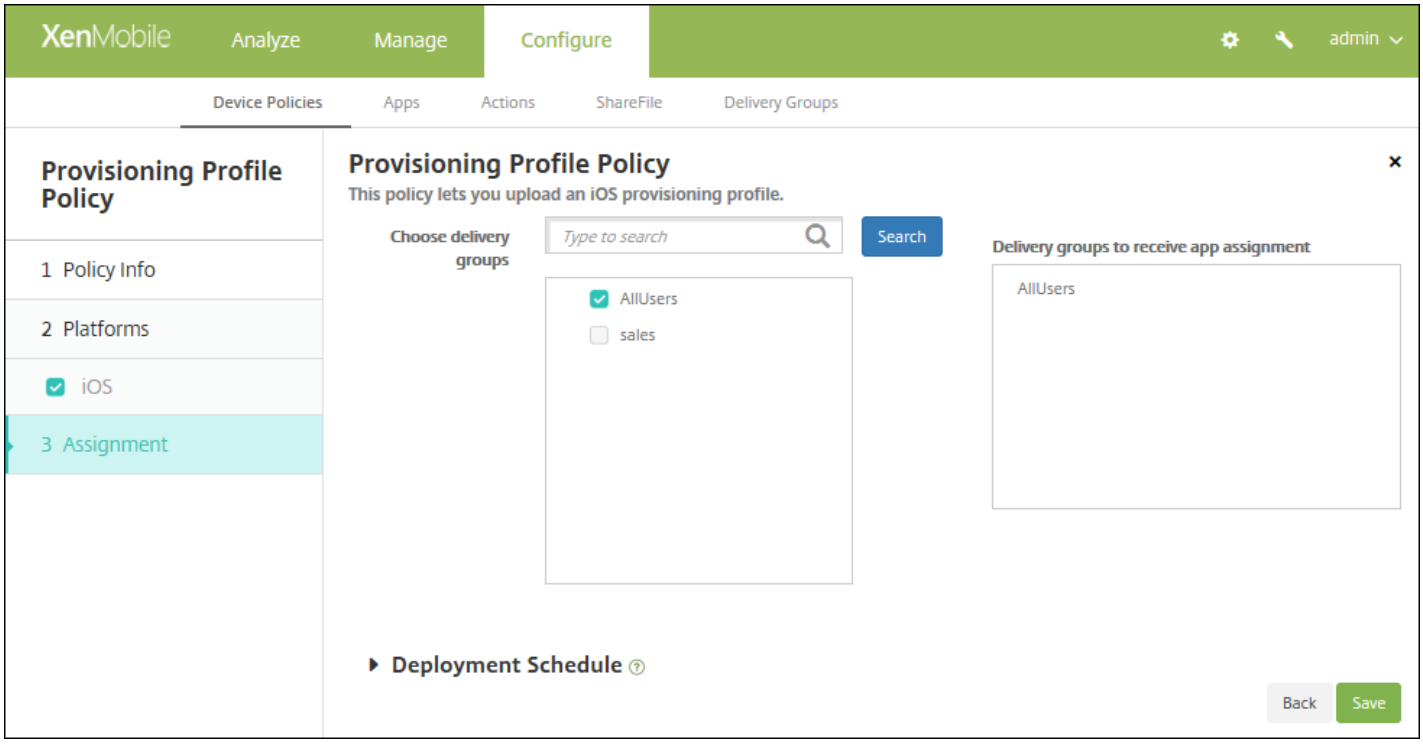
-
-
-
-
-
-
-



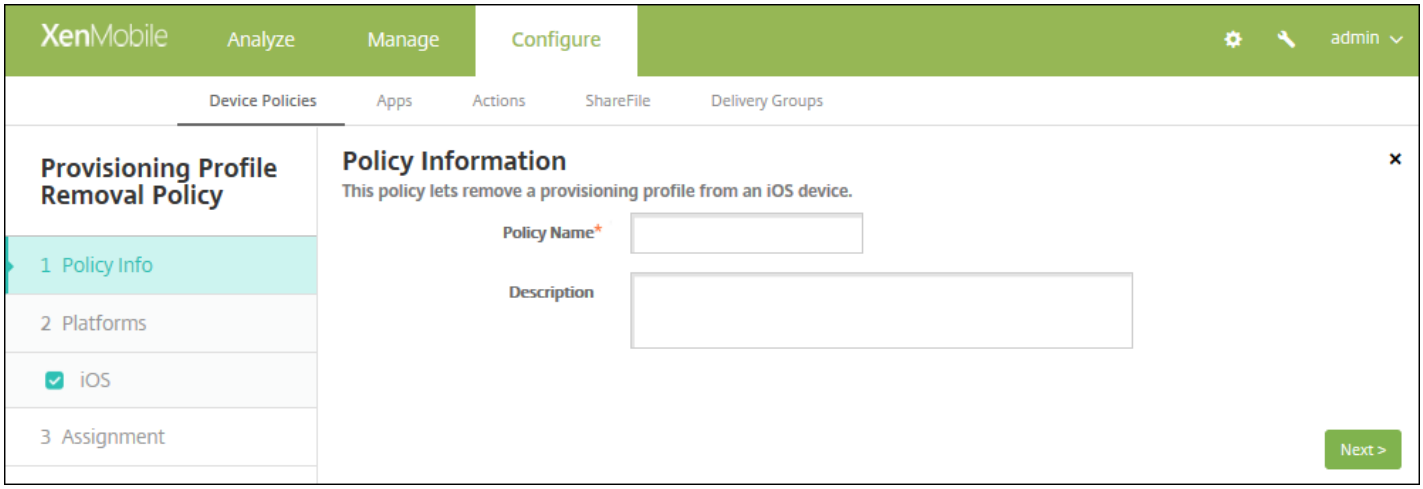
-
-



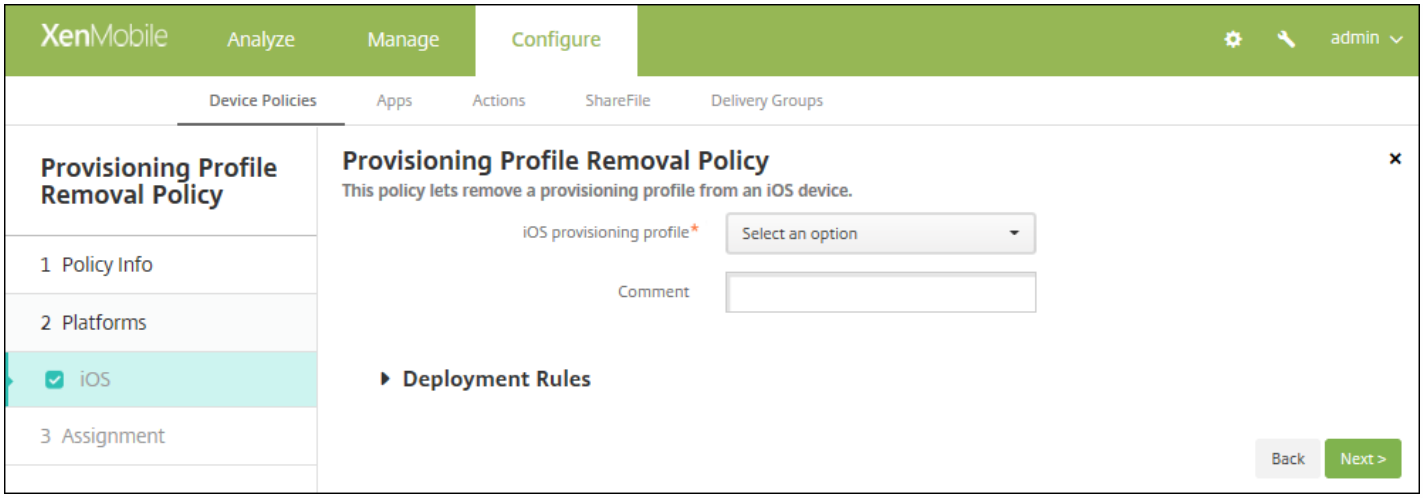
-



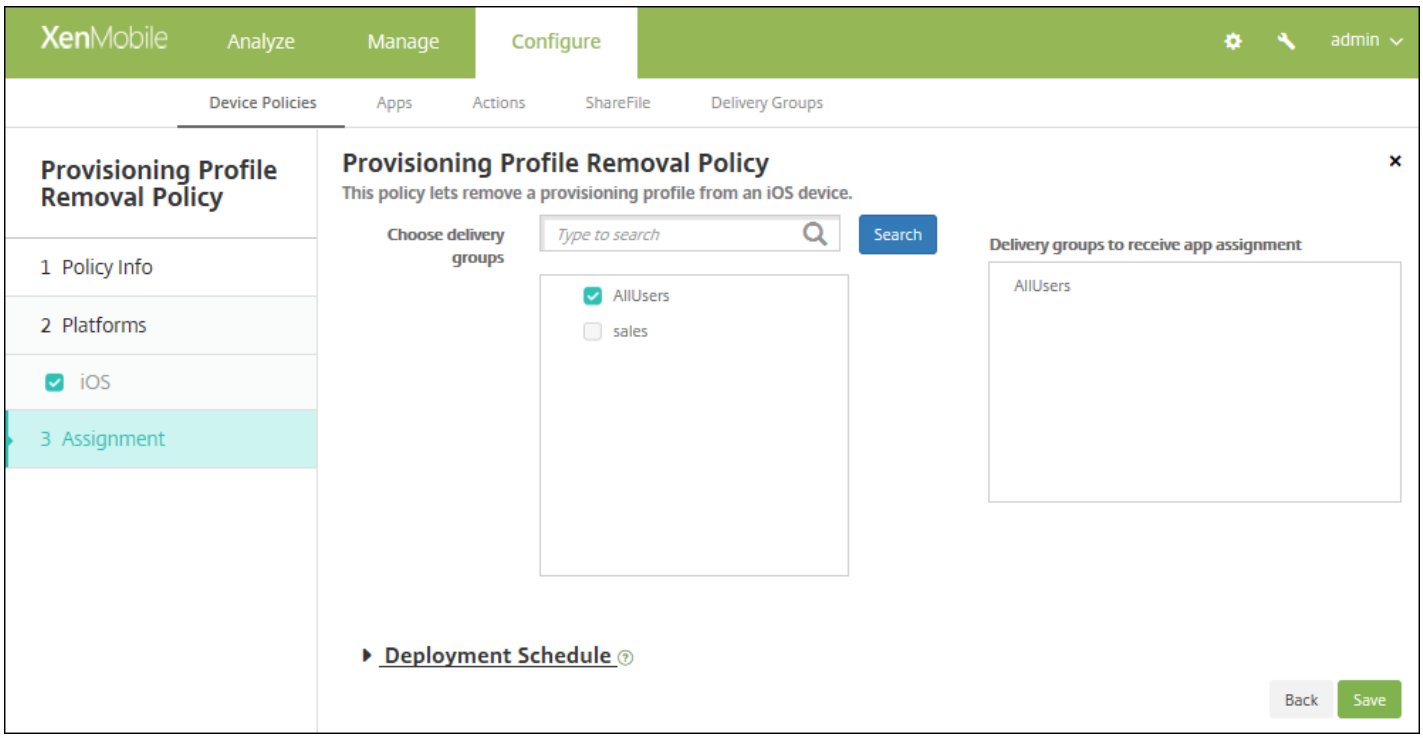
-
-
-
-
-
-
-



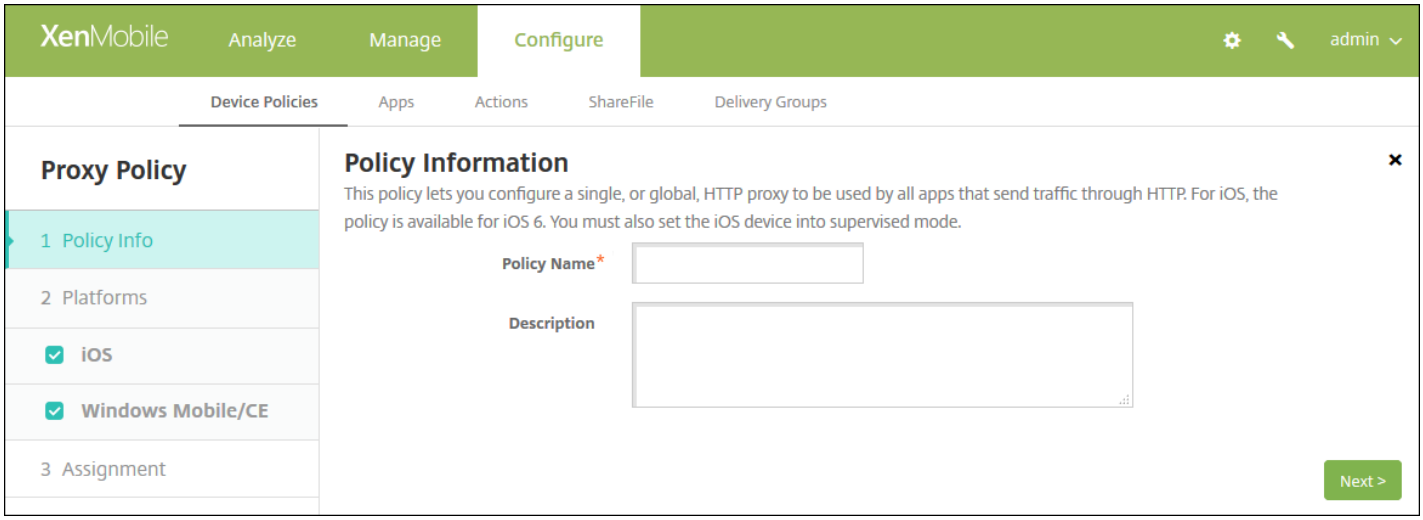
-
-



-
-

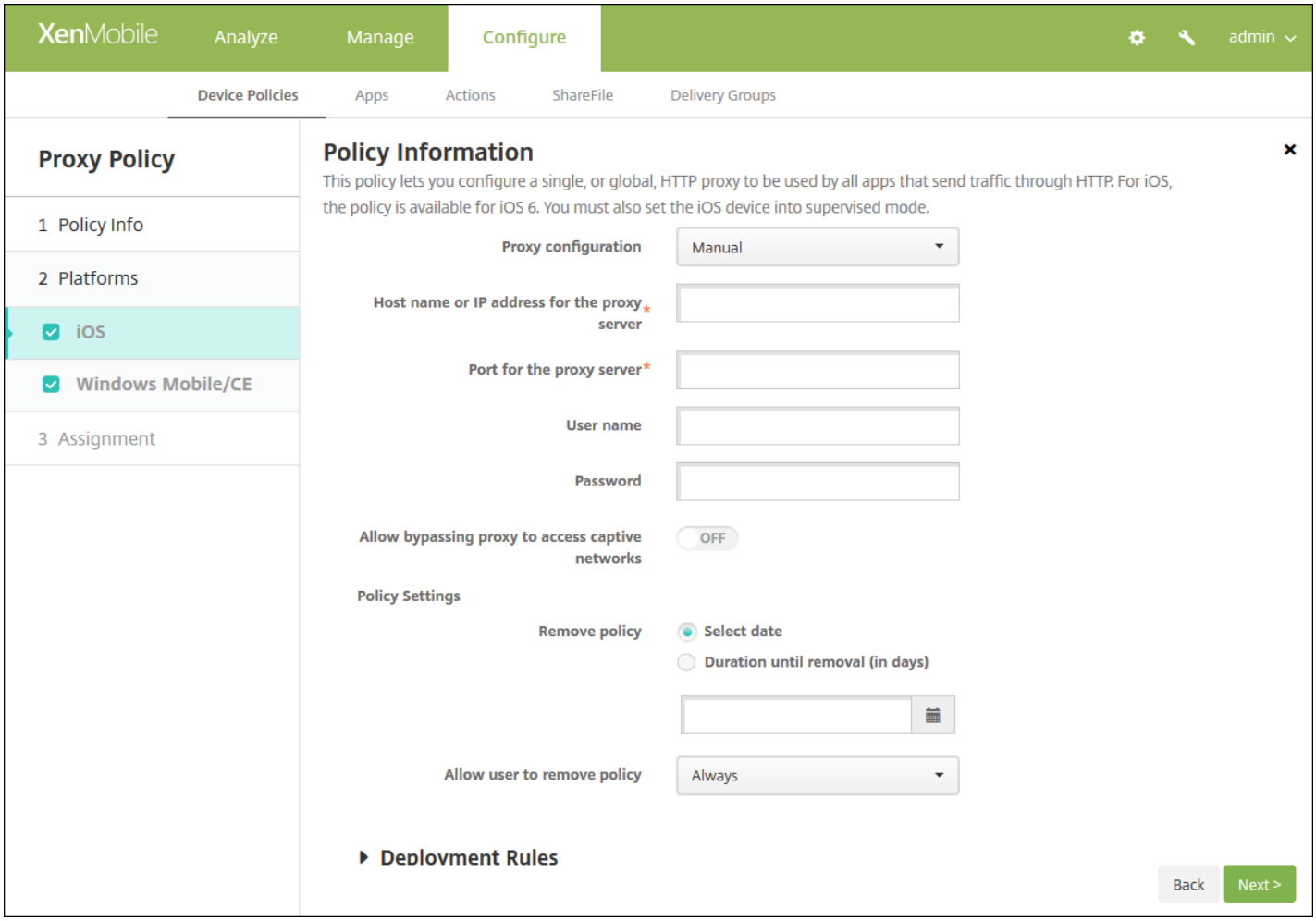


-
-
-
-
-
-
-



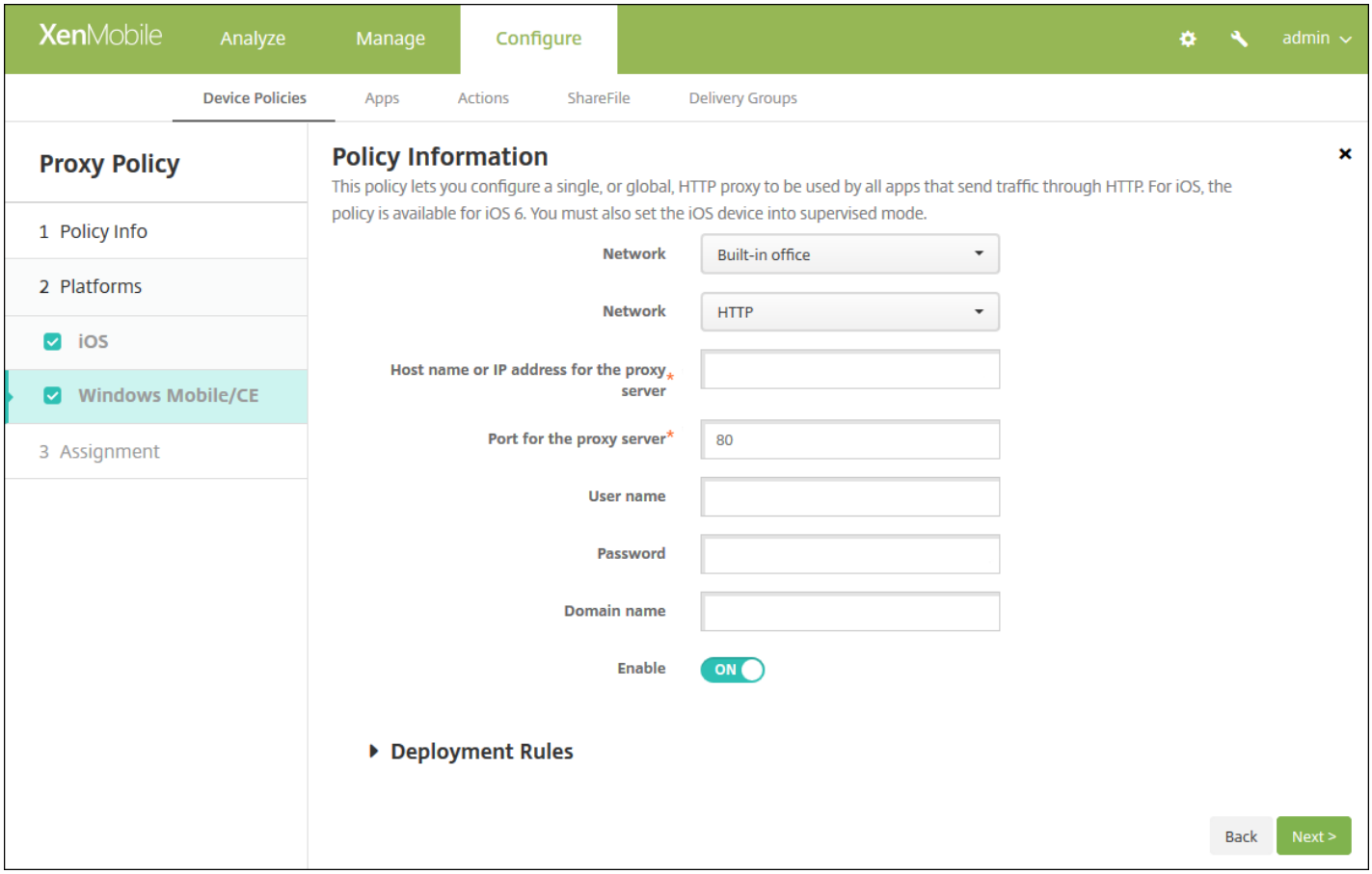
-
-

Configuración de los parámetros de iOS

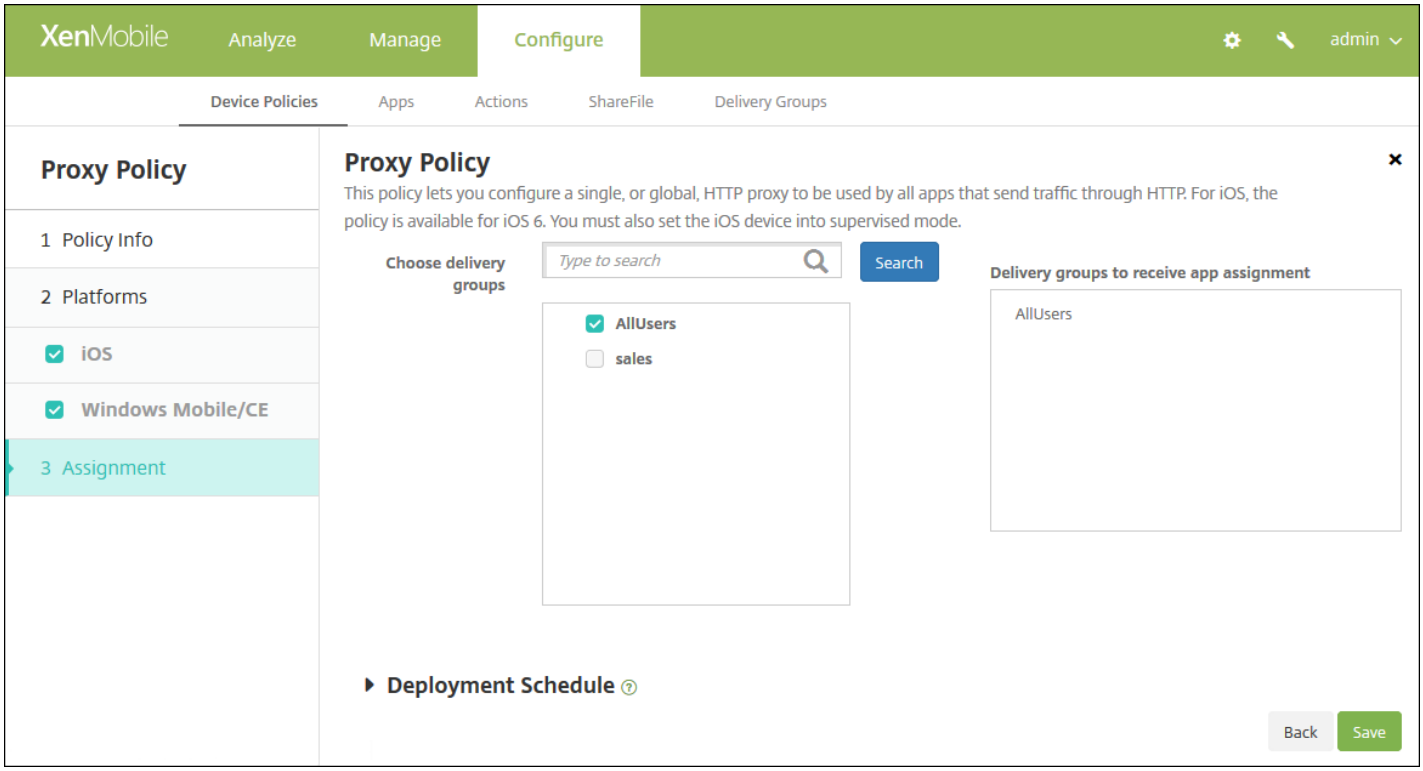


-
  -
    -
    -
    -
    -
  -
    -
    -
-
-
  -

Configuración de los parámetros de Windows Mobile/CE

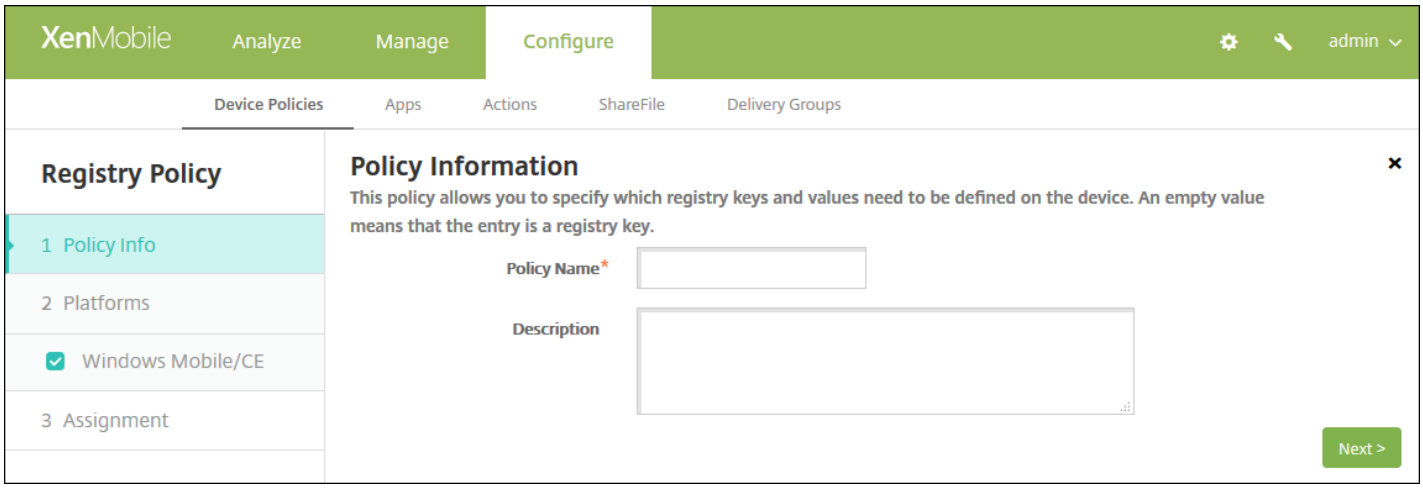


-
-
-
-
-

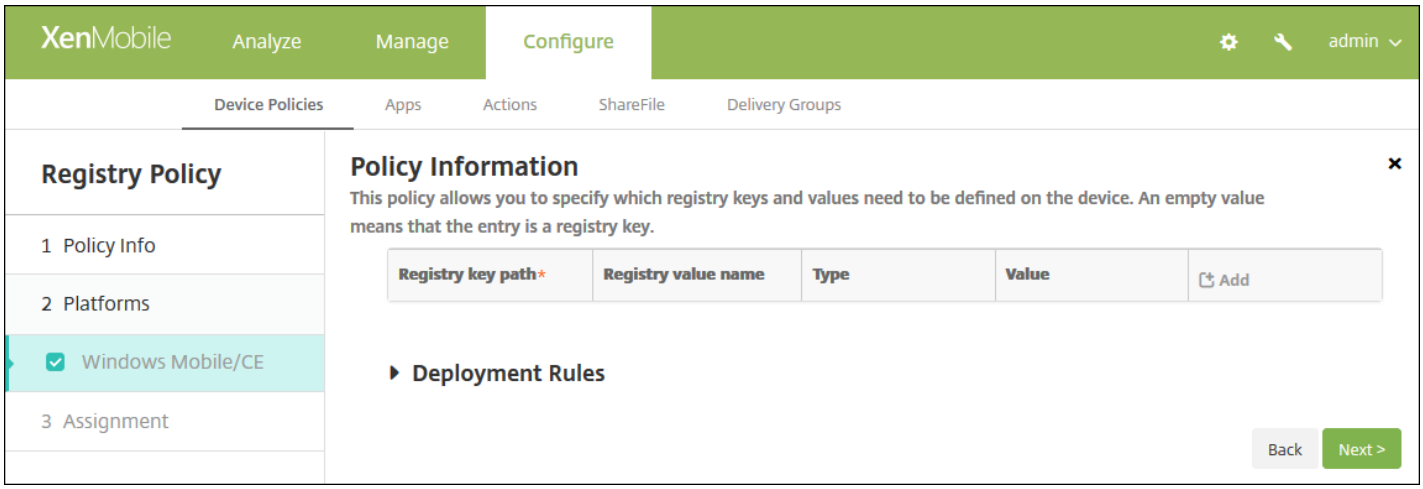


-
-
-
-

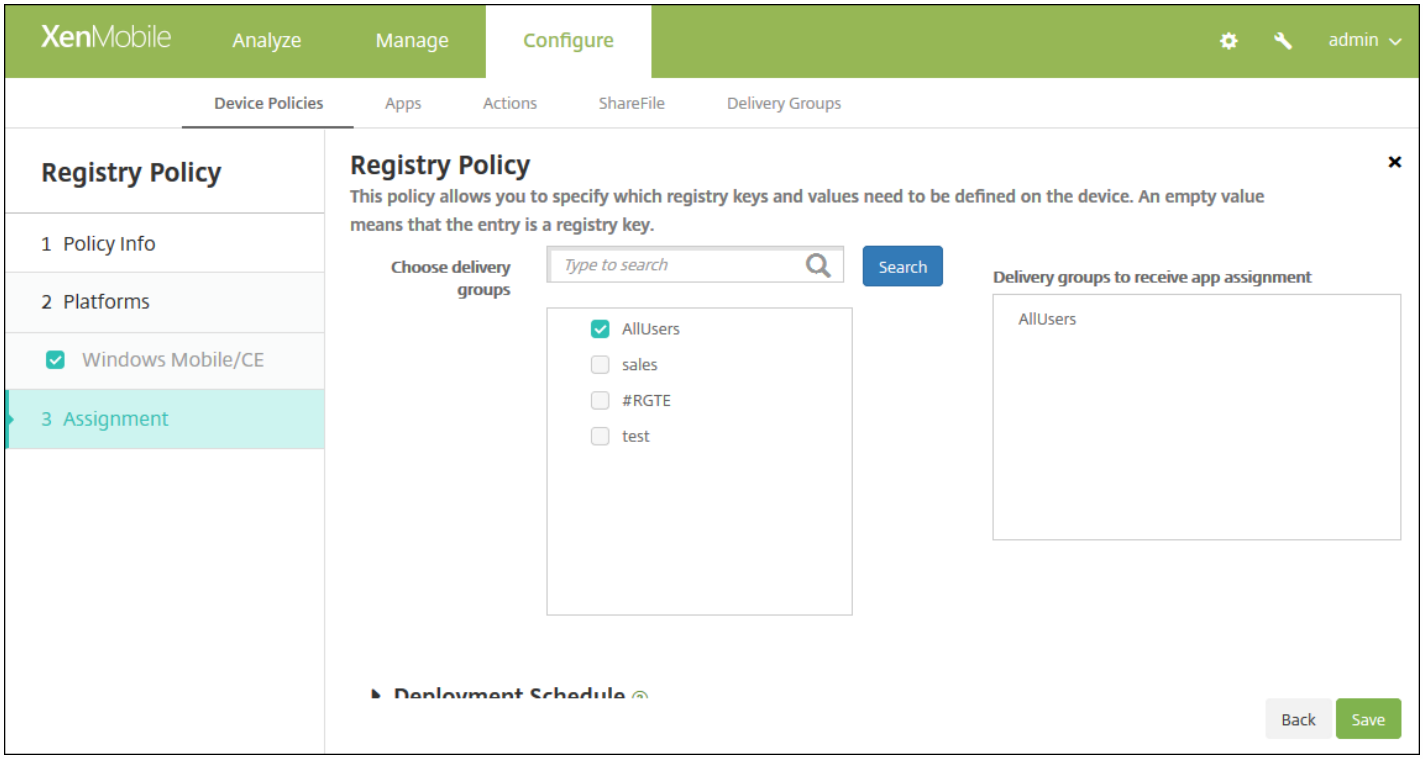
-
-



-
-

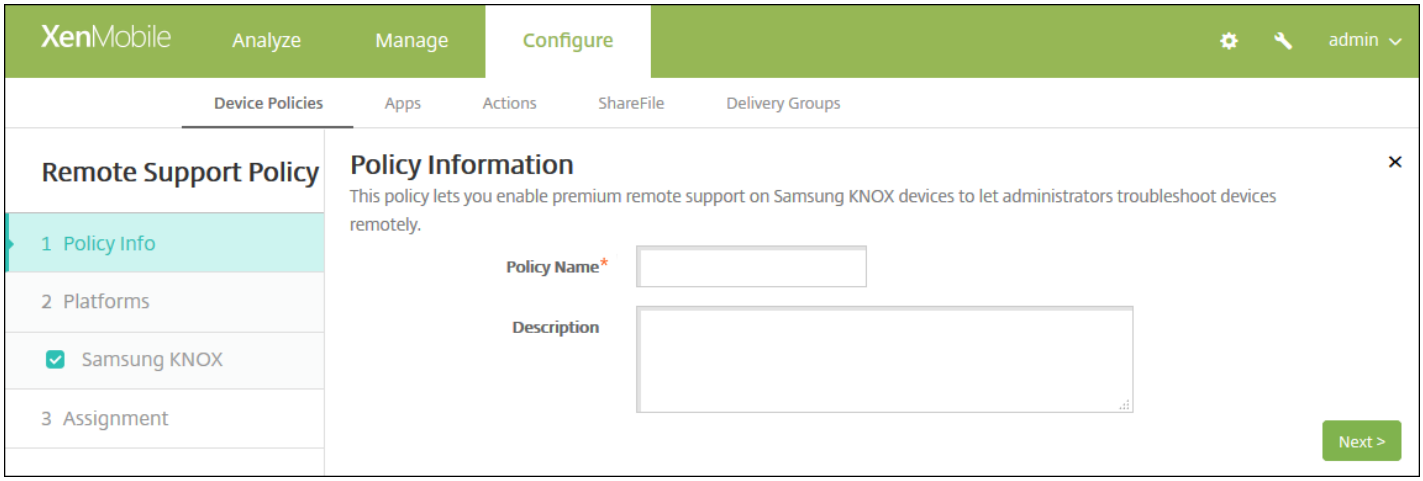


-
-
-
-
  -
  -
  -
  -
-
-

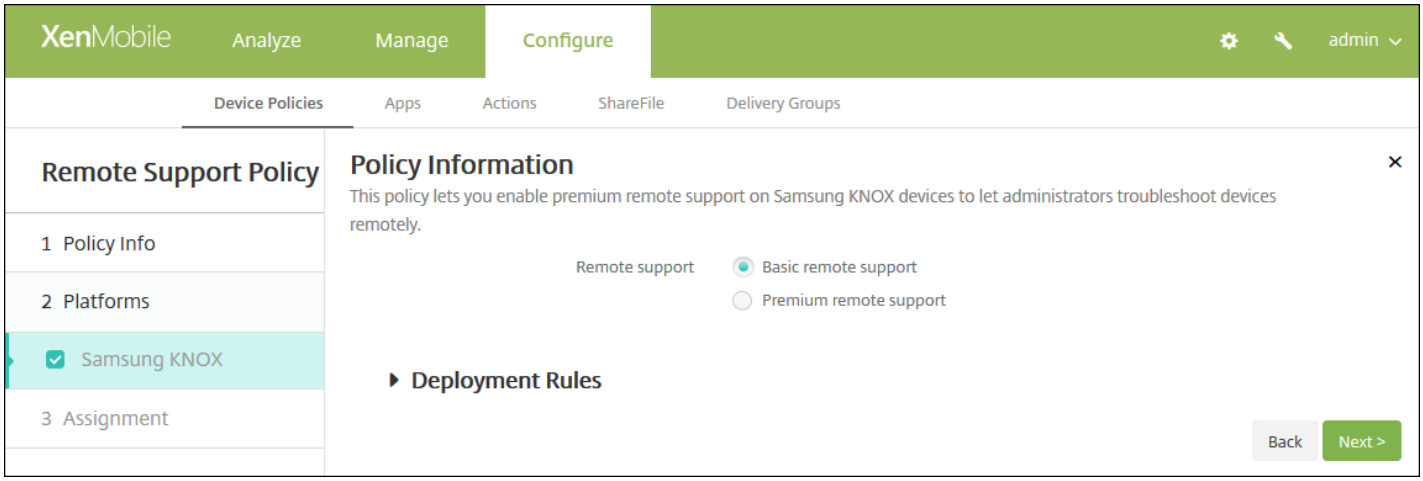


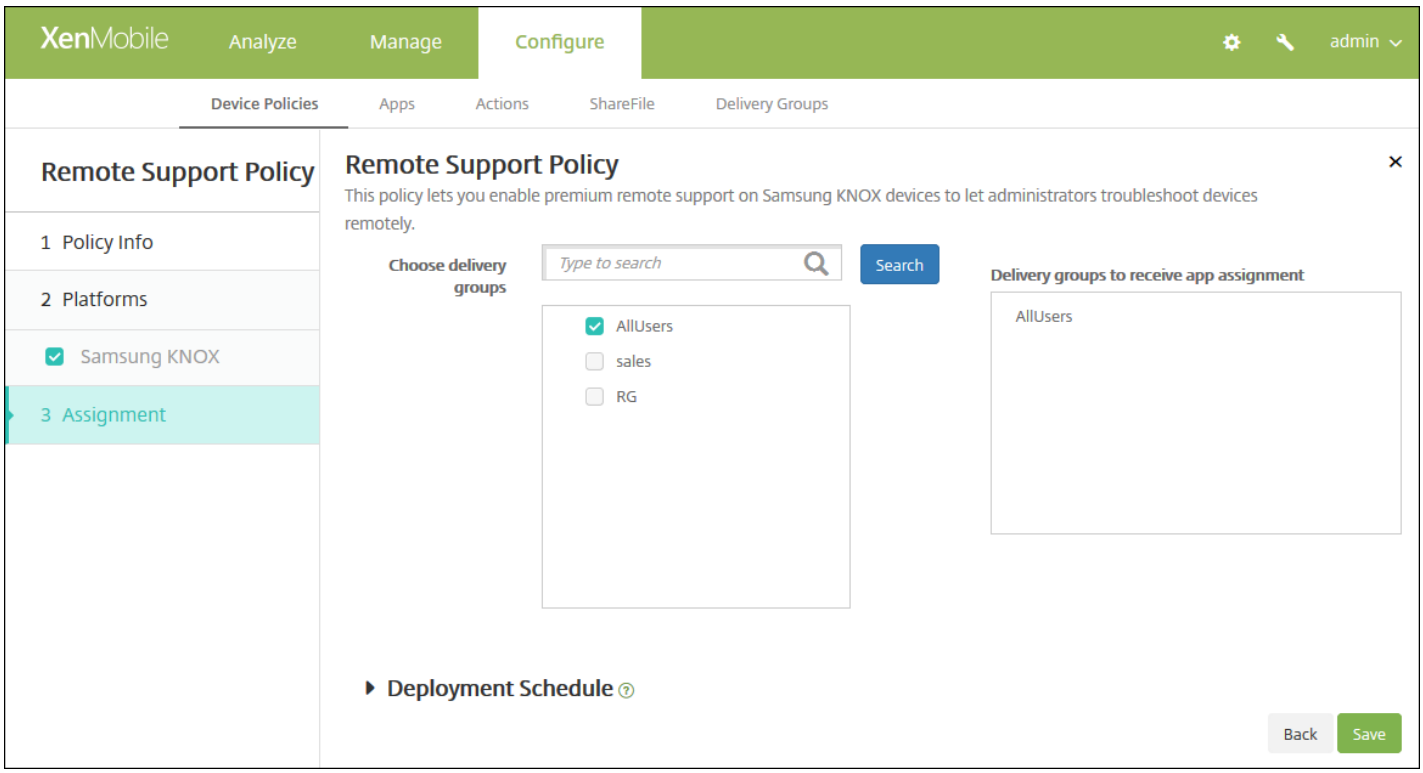
-
-
-
-
-
-
-

-
-
-
-
-
-



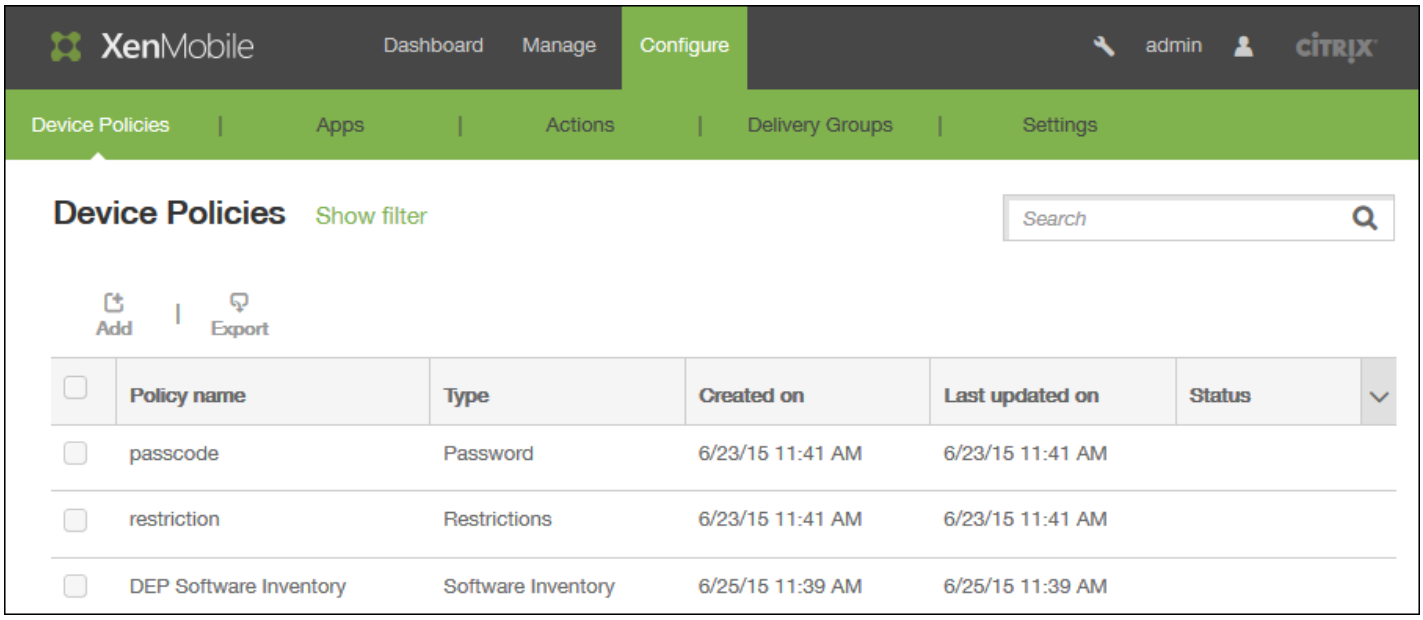
-

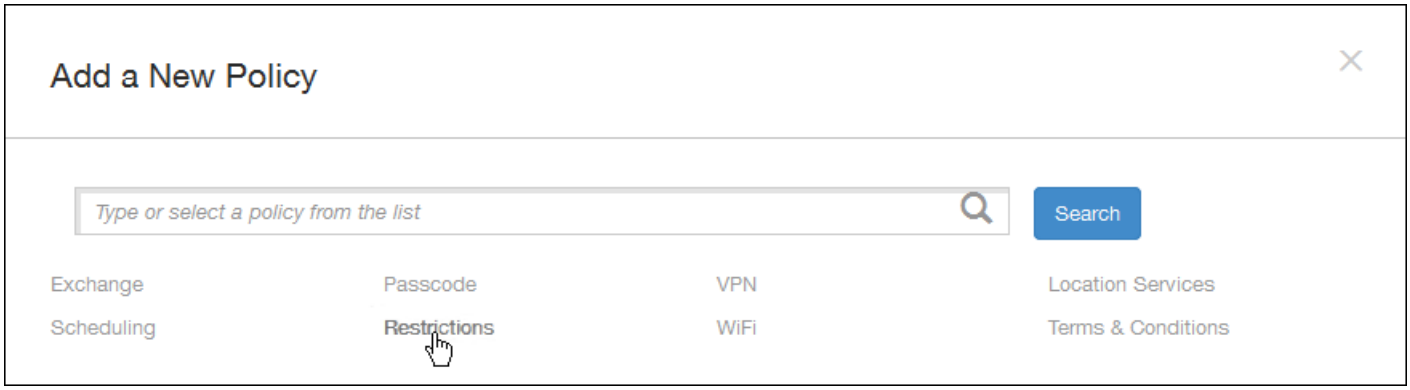
- 

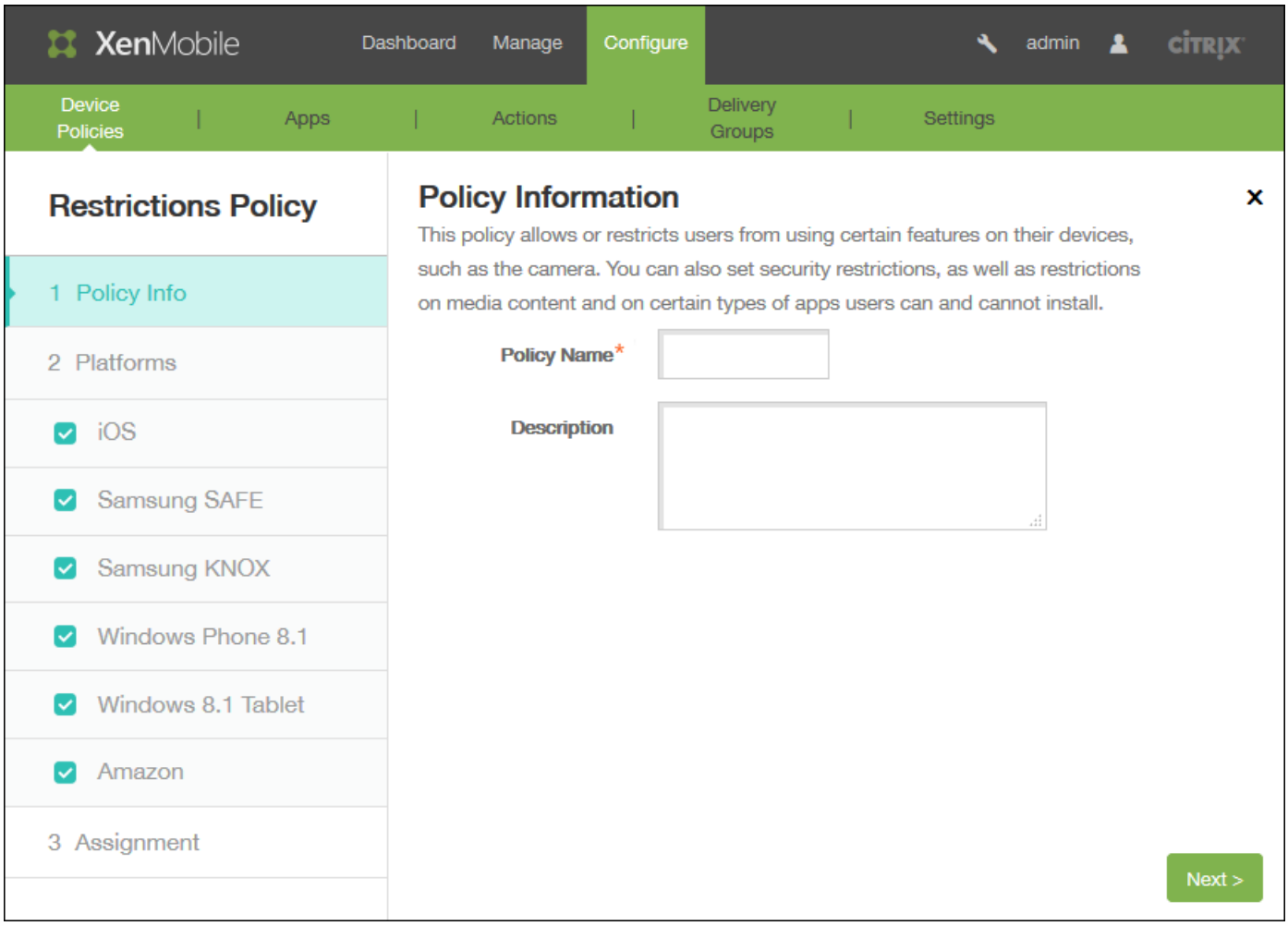
- 

-
-
-
-
-
-
-

-
-

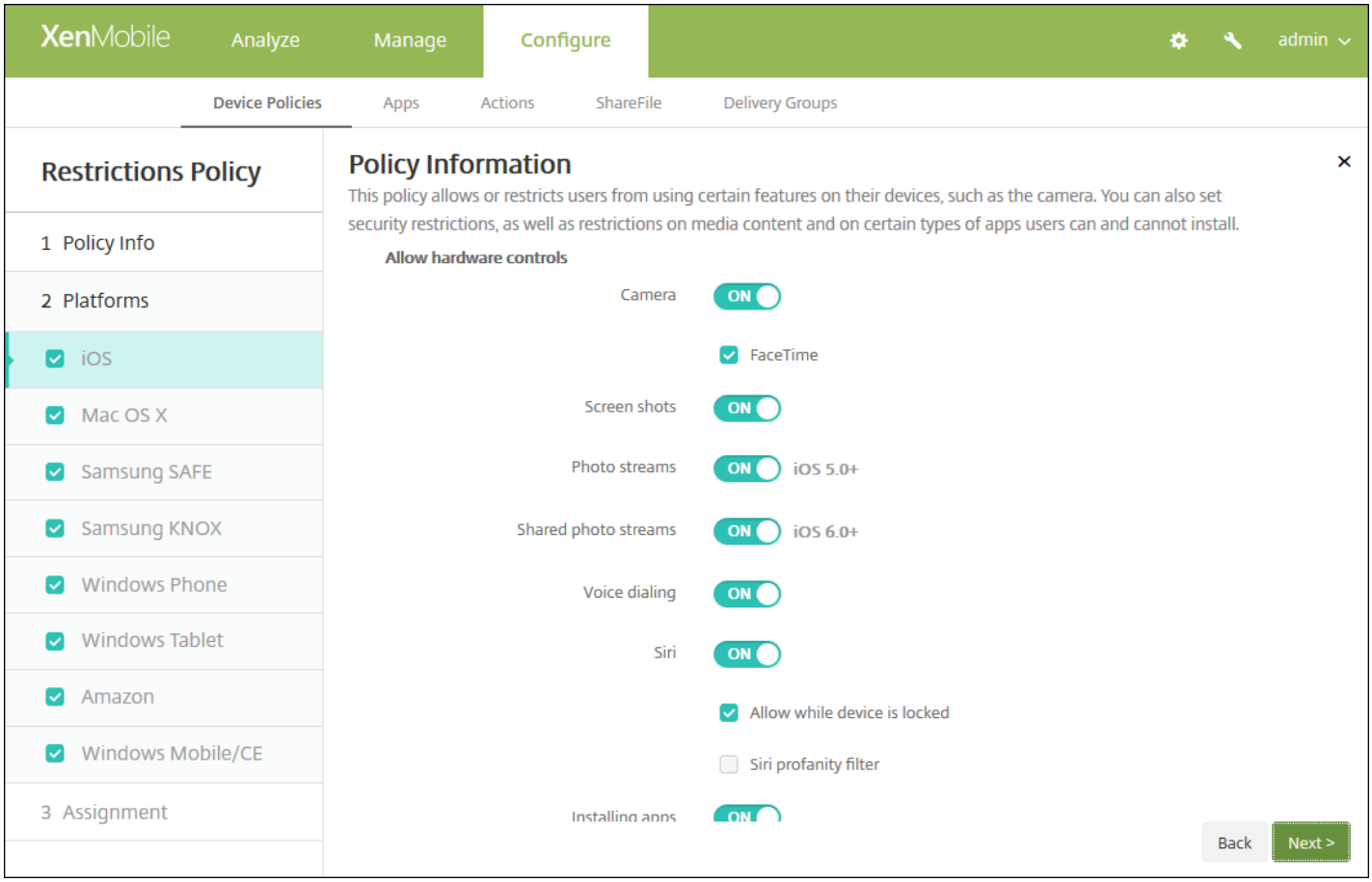




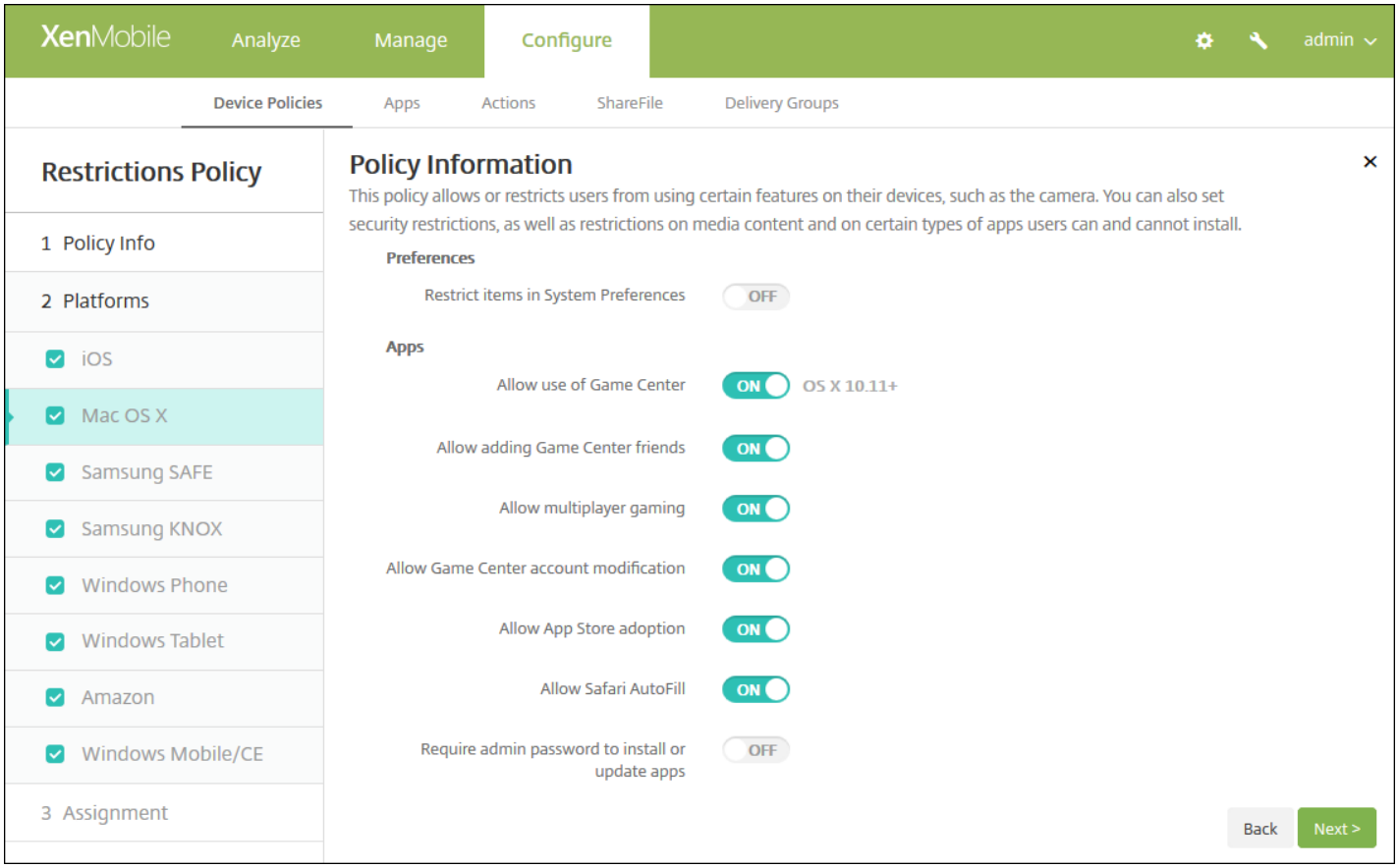


-
-

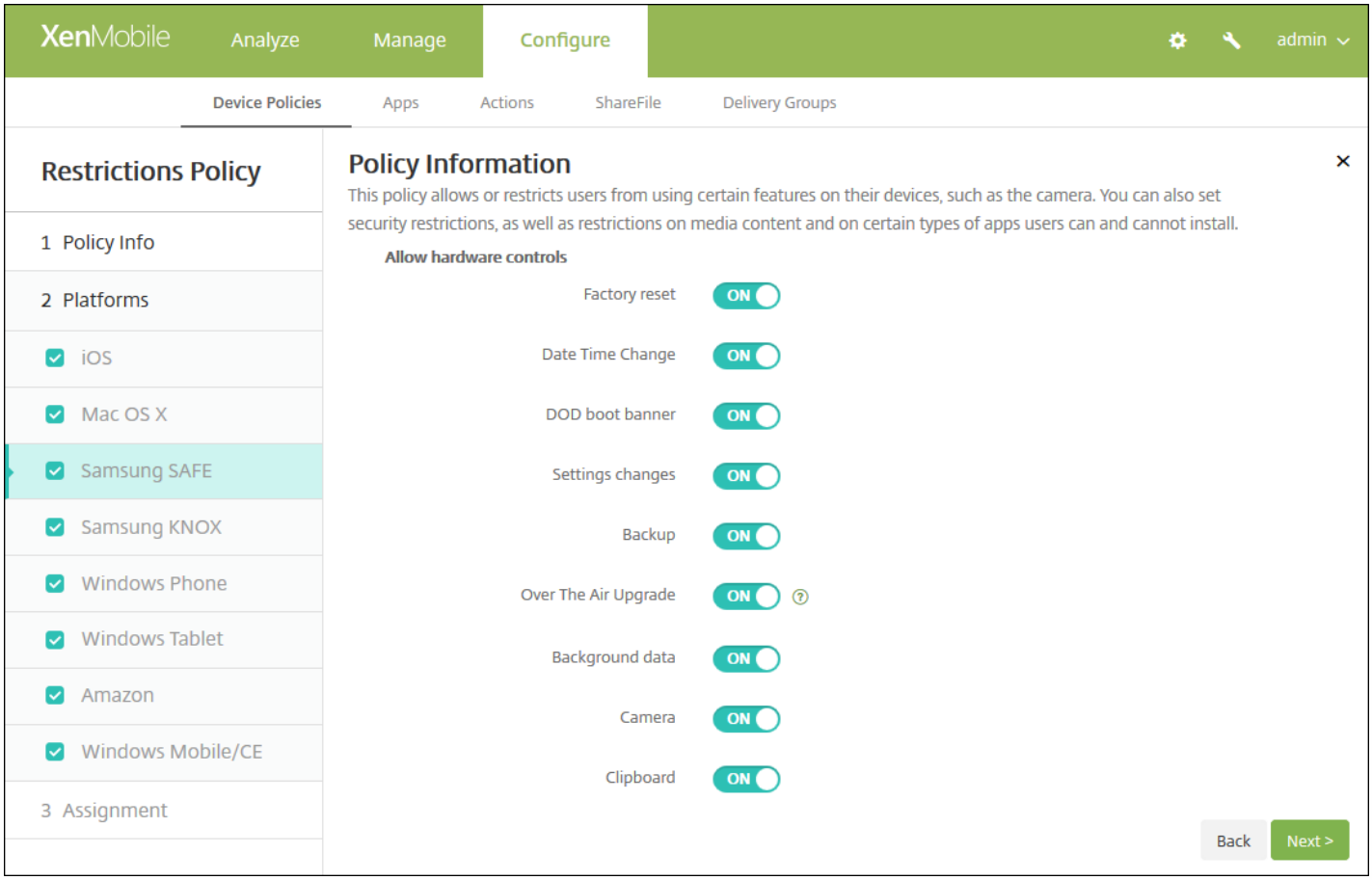
Si ha seleccionado iOS, configure los siguientes parámetros:



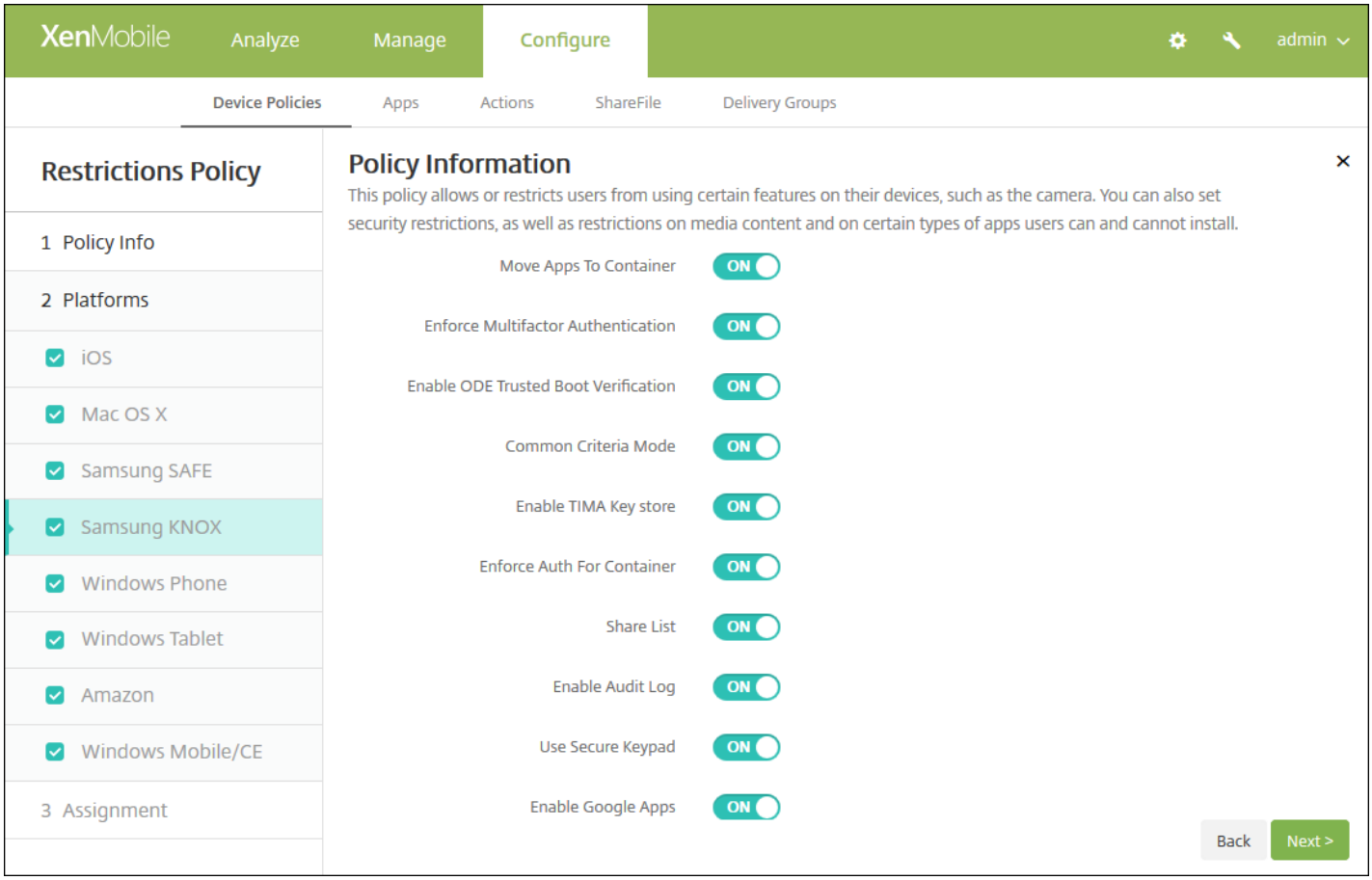
Configuración de los parámetros de Mac OS X



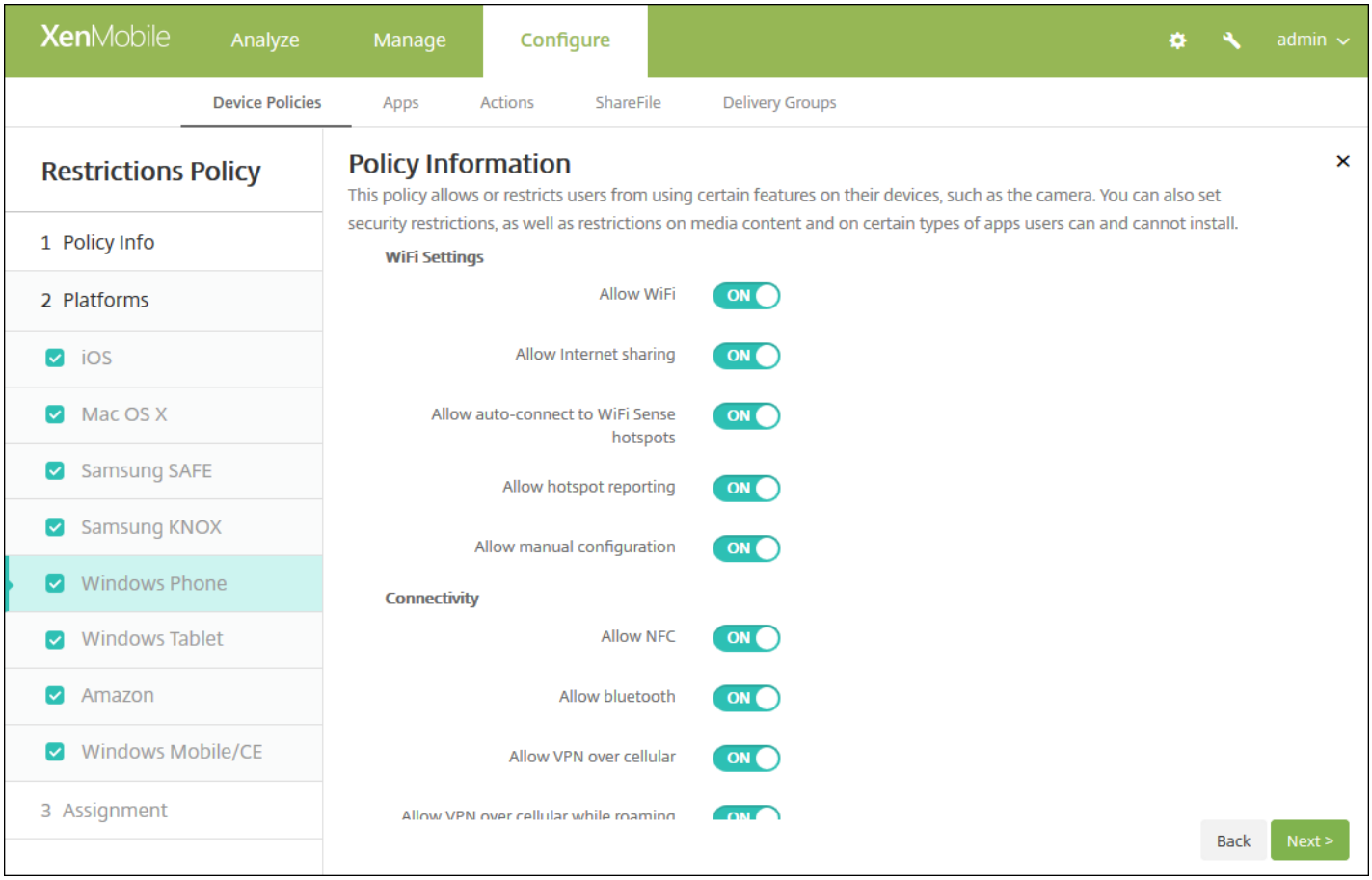
Configuración de los parámetros de Samsung SAFE



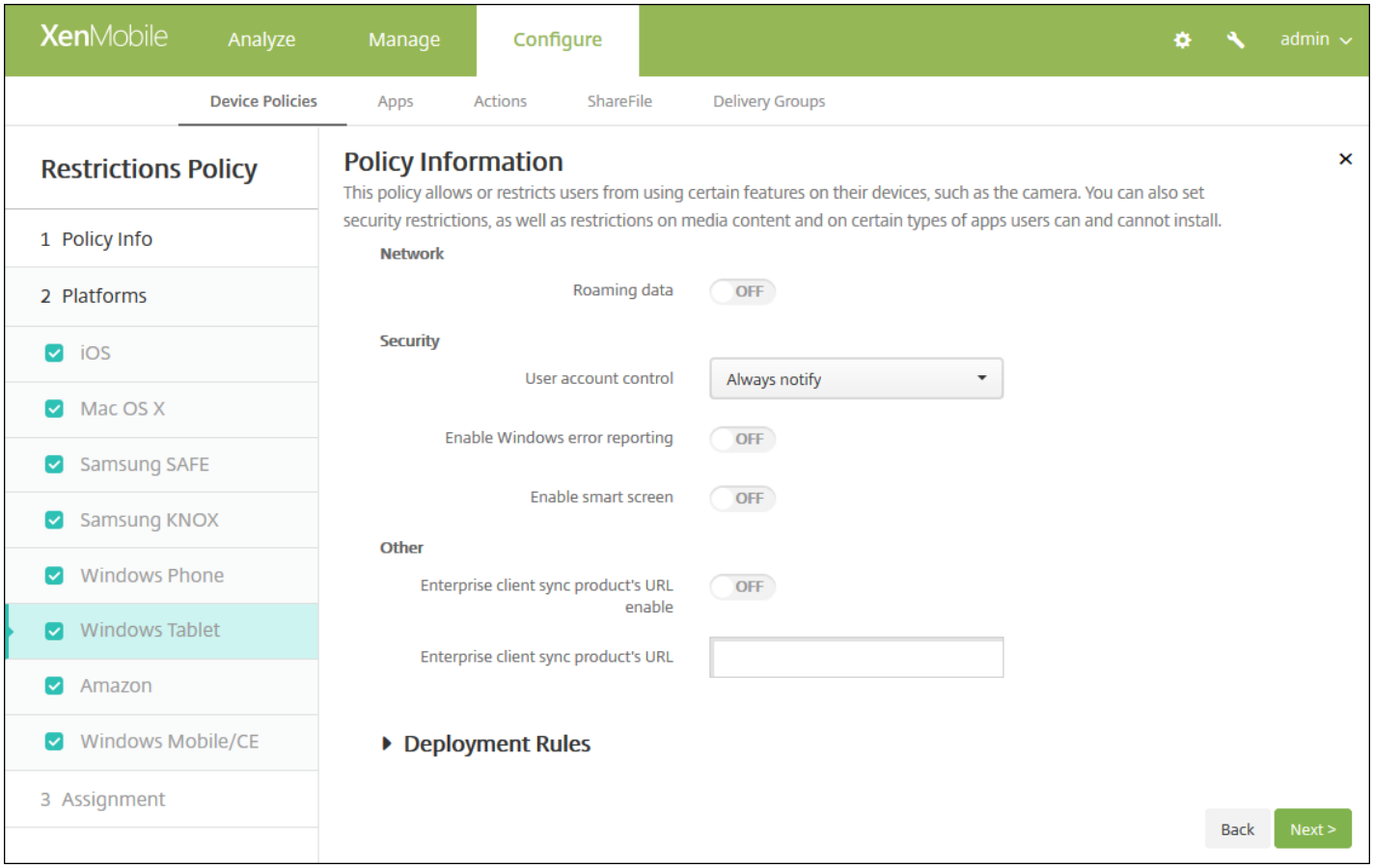
Configuración de los parámetros de Samsung KNOX



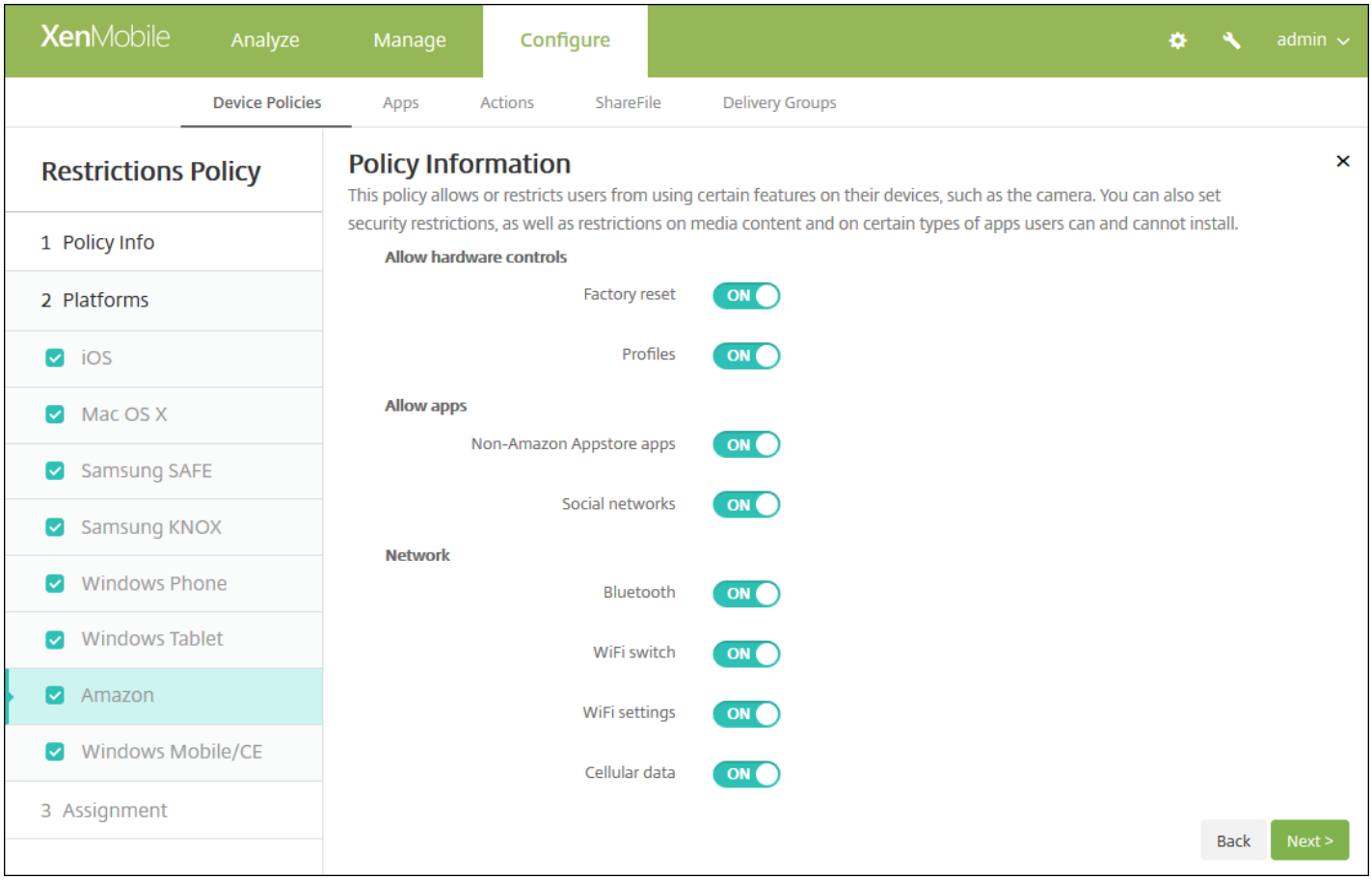
Configuración de los parámetros de Windows Phone



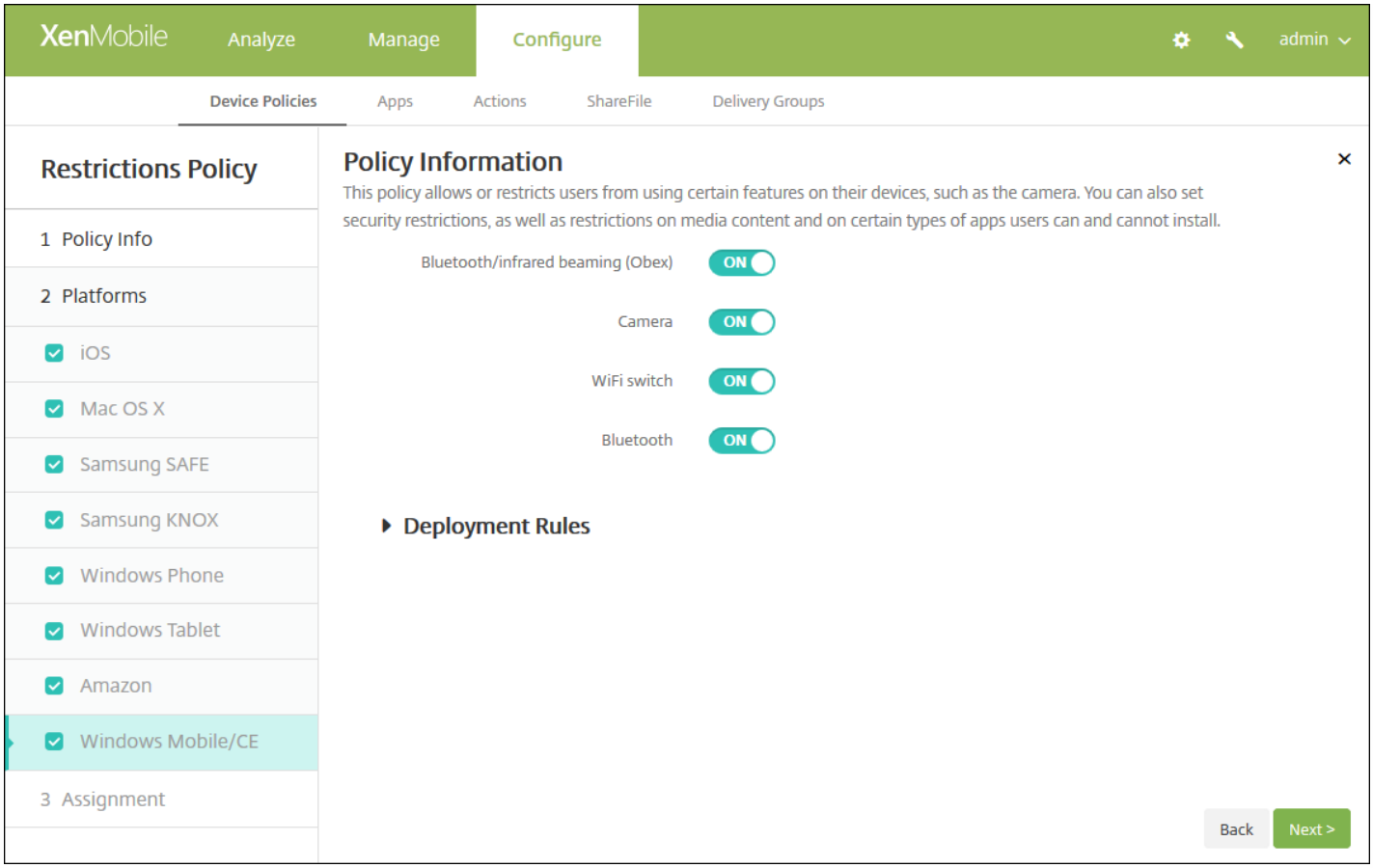
Configuración de los parámetros de tabletas Windows

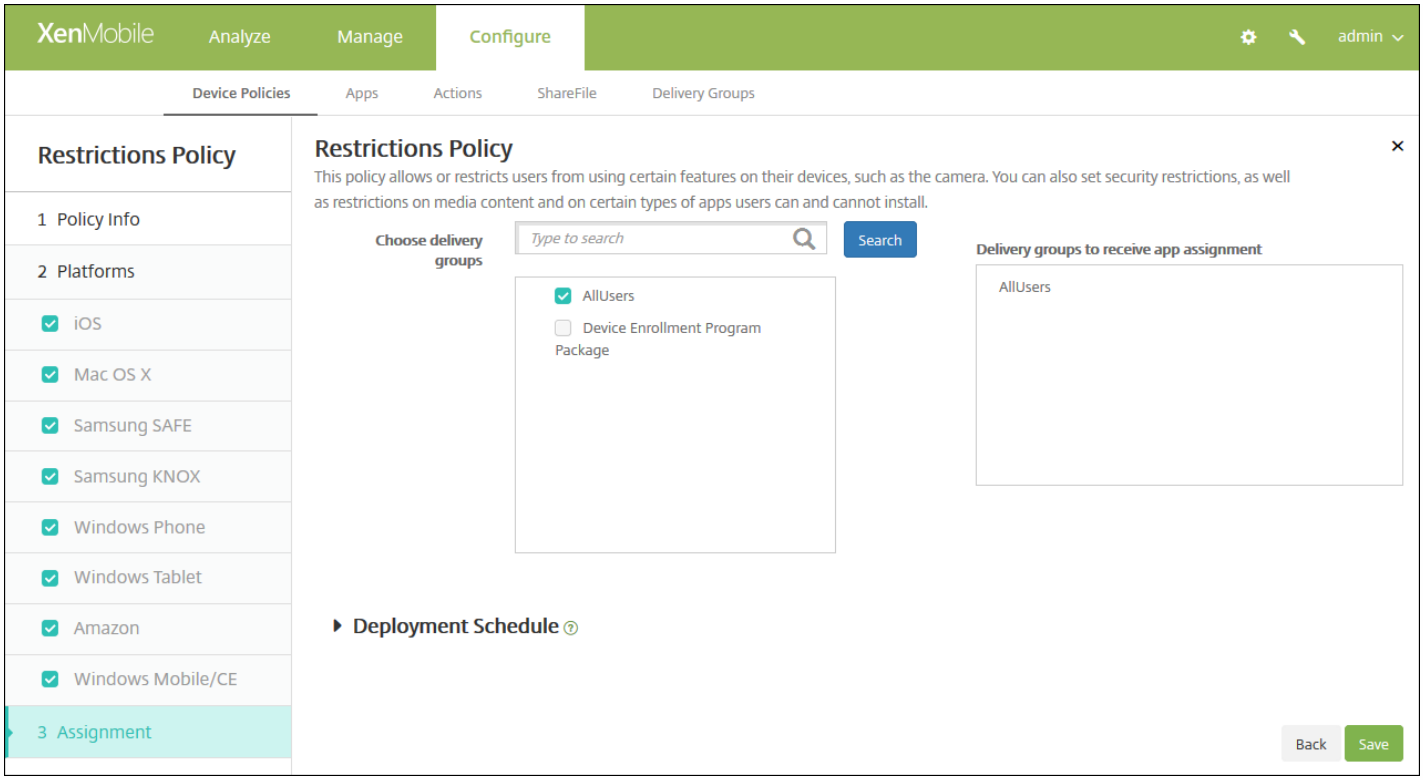


Configuración de los parámetros de Amazon

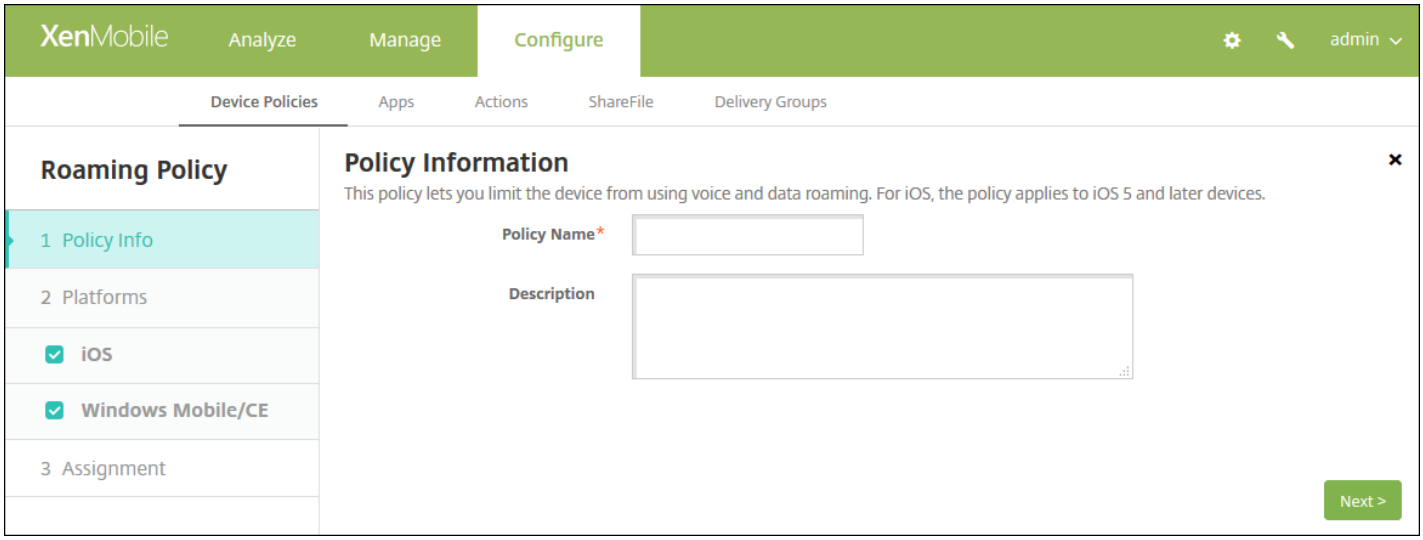


Configuración de los parámetros de Windows Mobile/CE



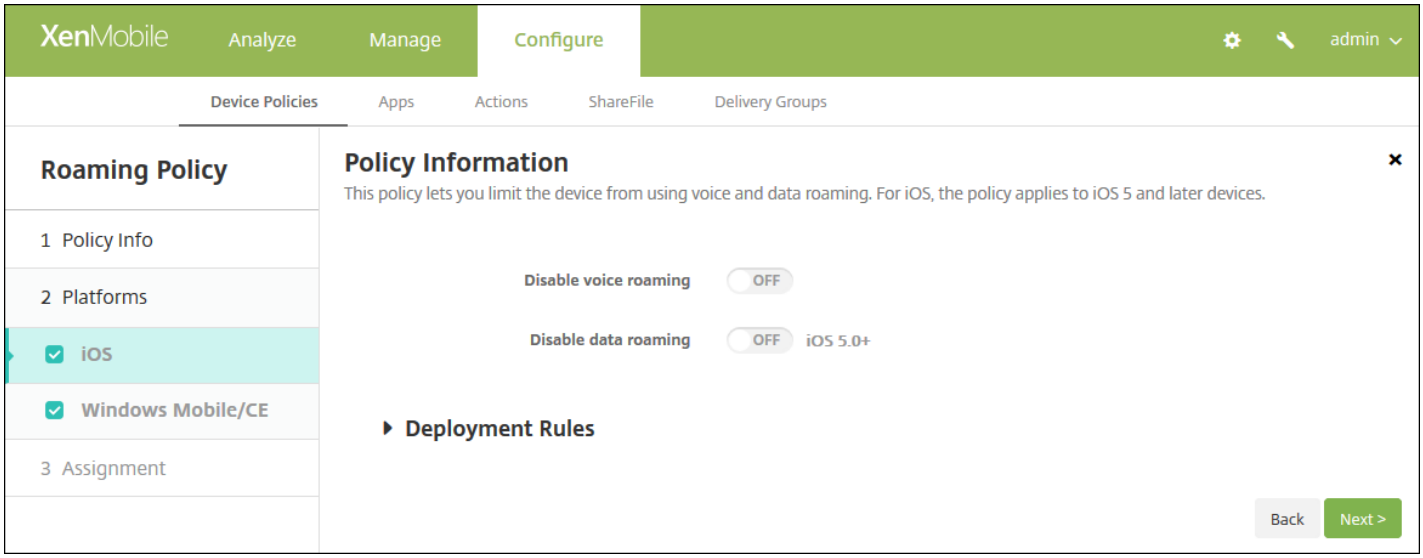


-
-
-
-
-
-
-



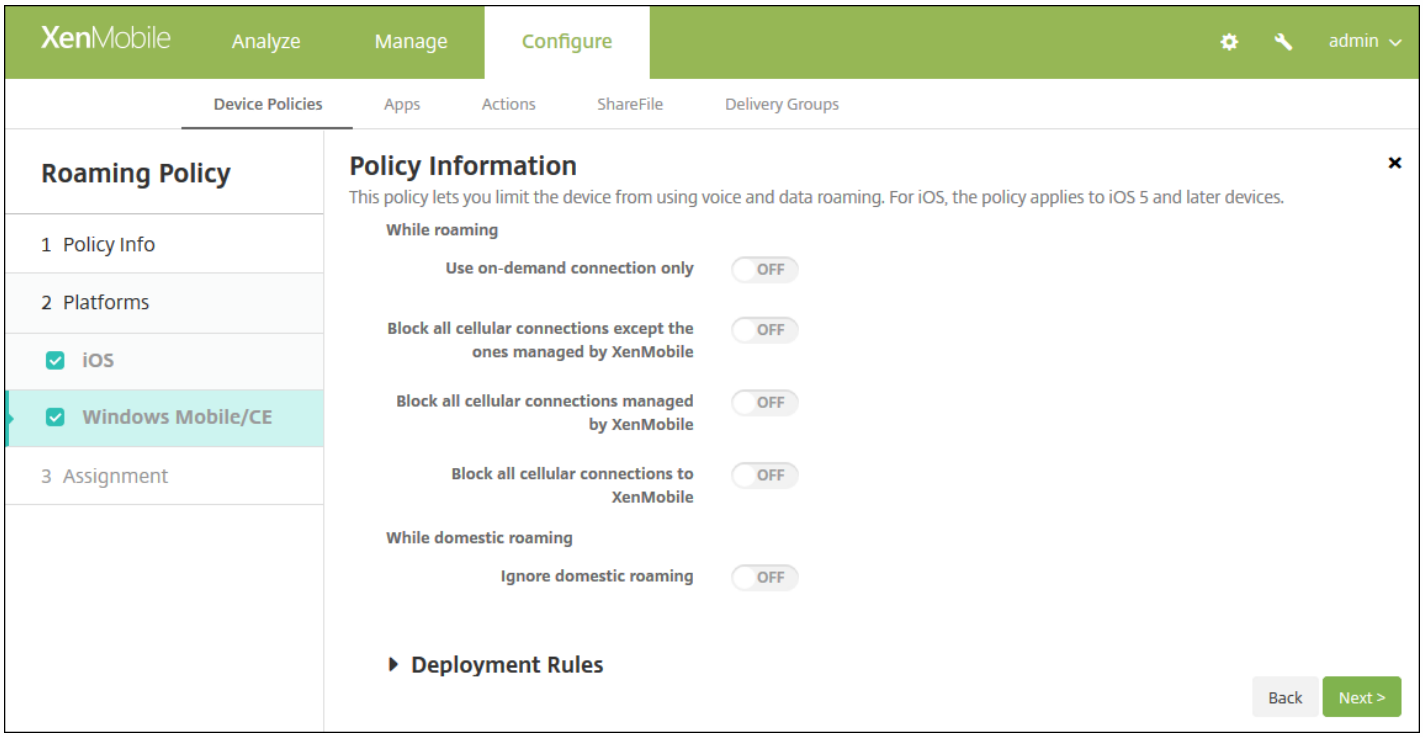
-
-

Configuración de los parámetros de iOS

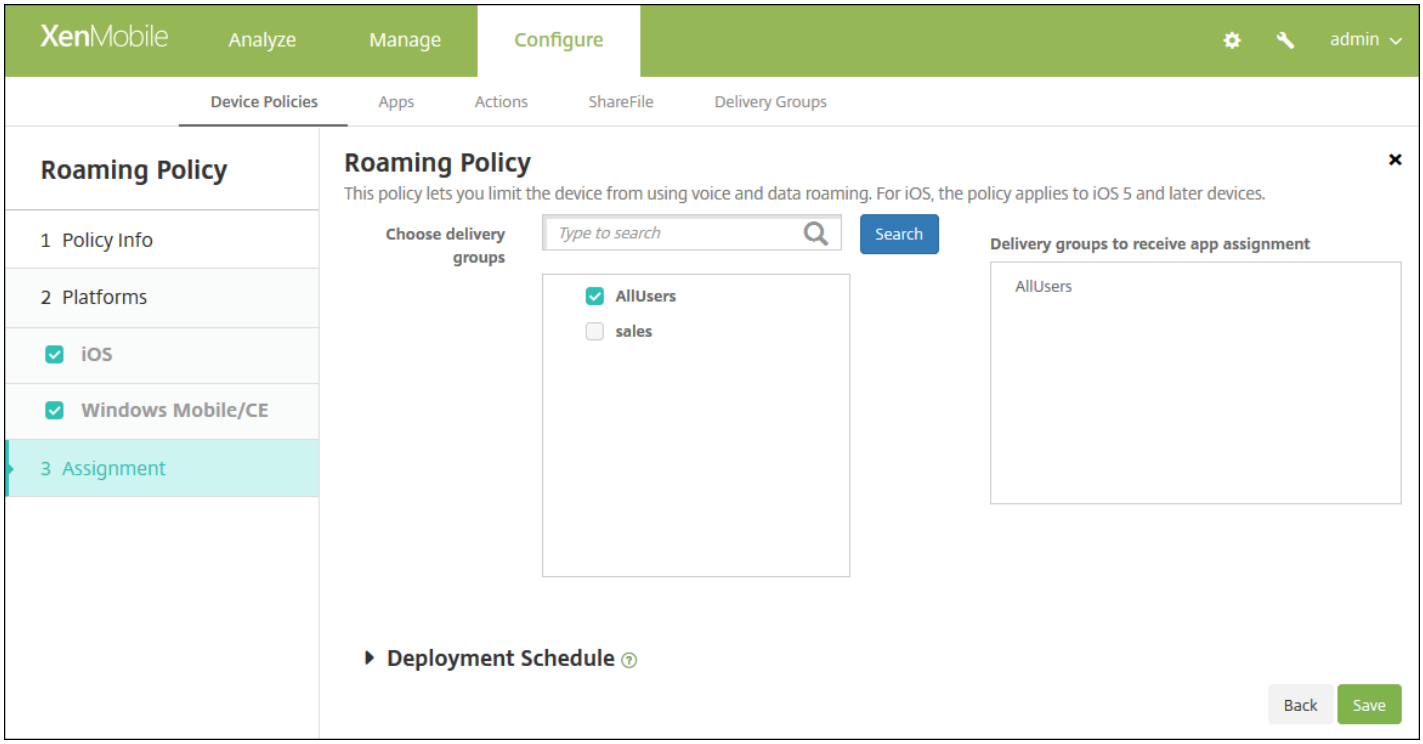


-
-

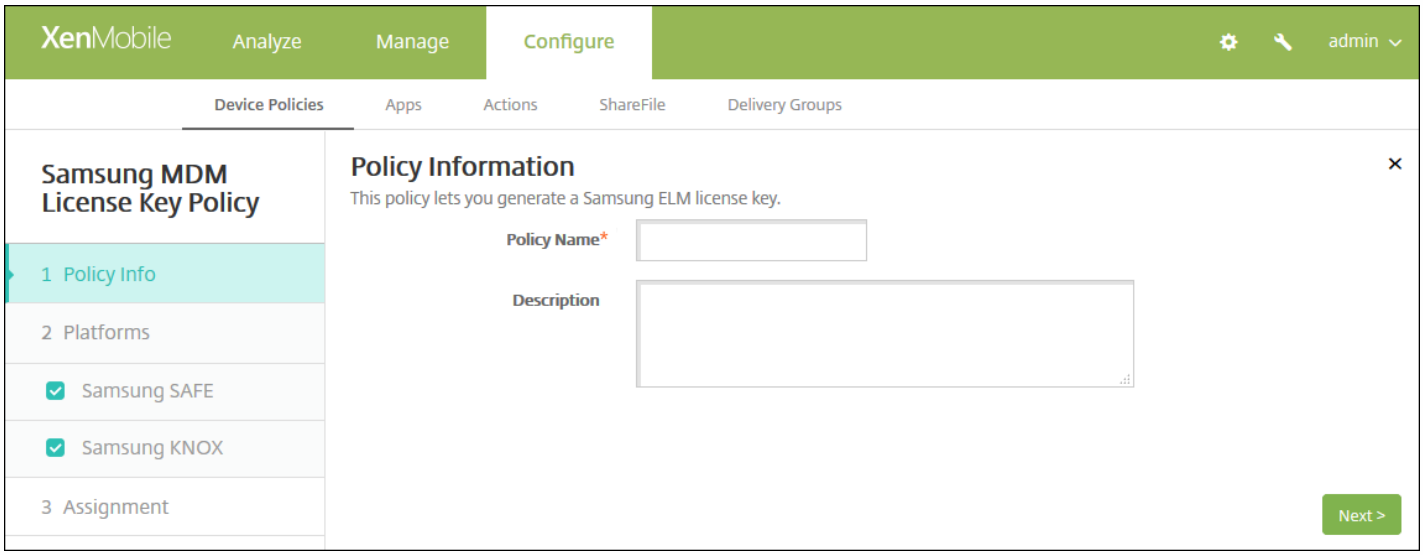
Configuración de los parámetros de Windows Mobile/CE



-
  -
  -
  -
  -
-
  -

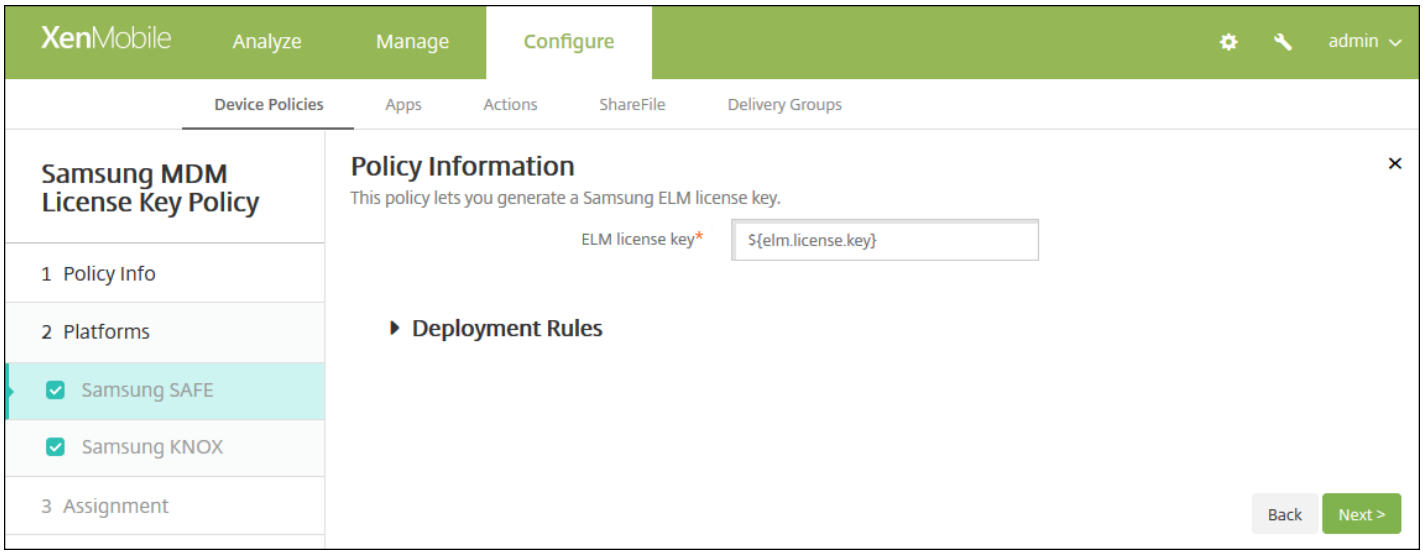


-
-
-
-
-
-
-



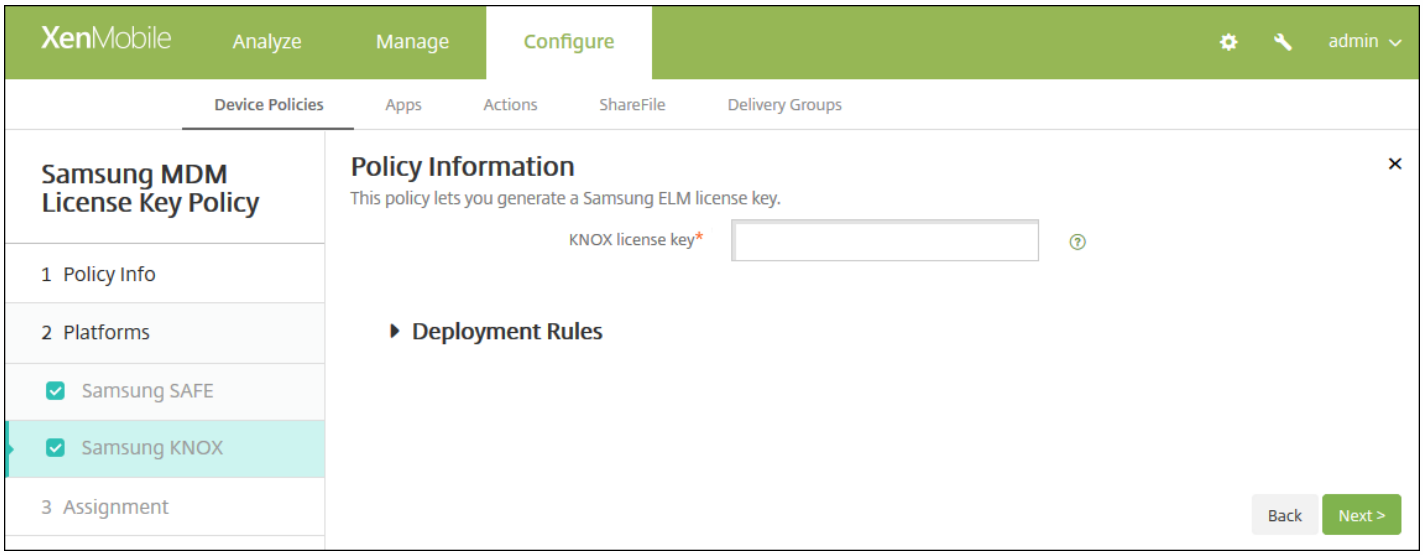
-
-

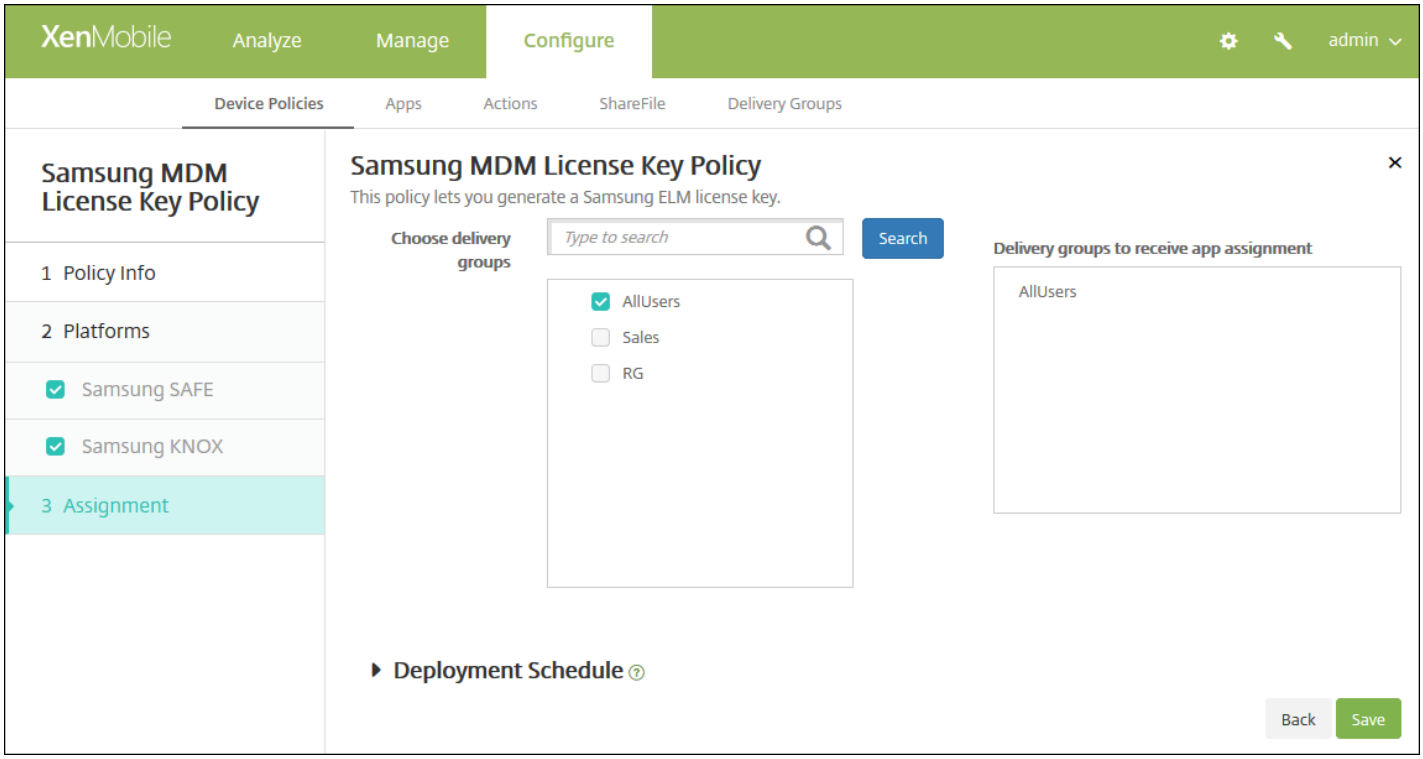
Configuración de los parámetros de Samsung SAFE



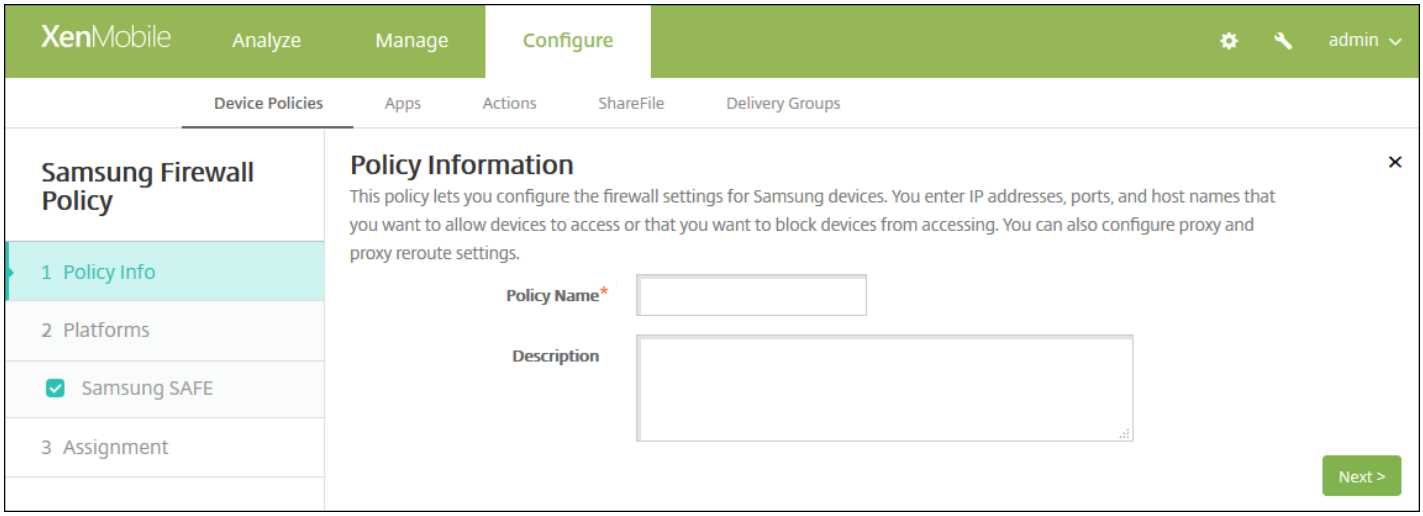
-

Configuración de los parámetros de Samsung KNOX

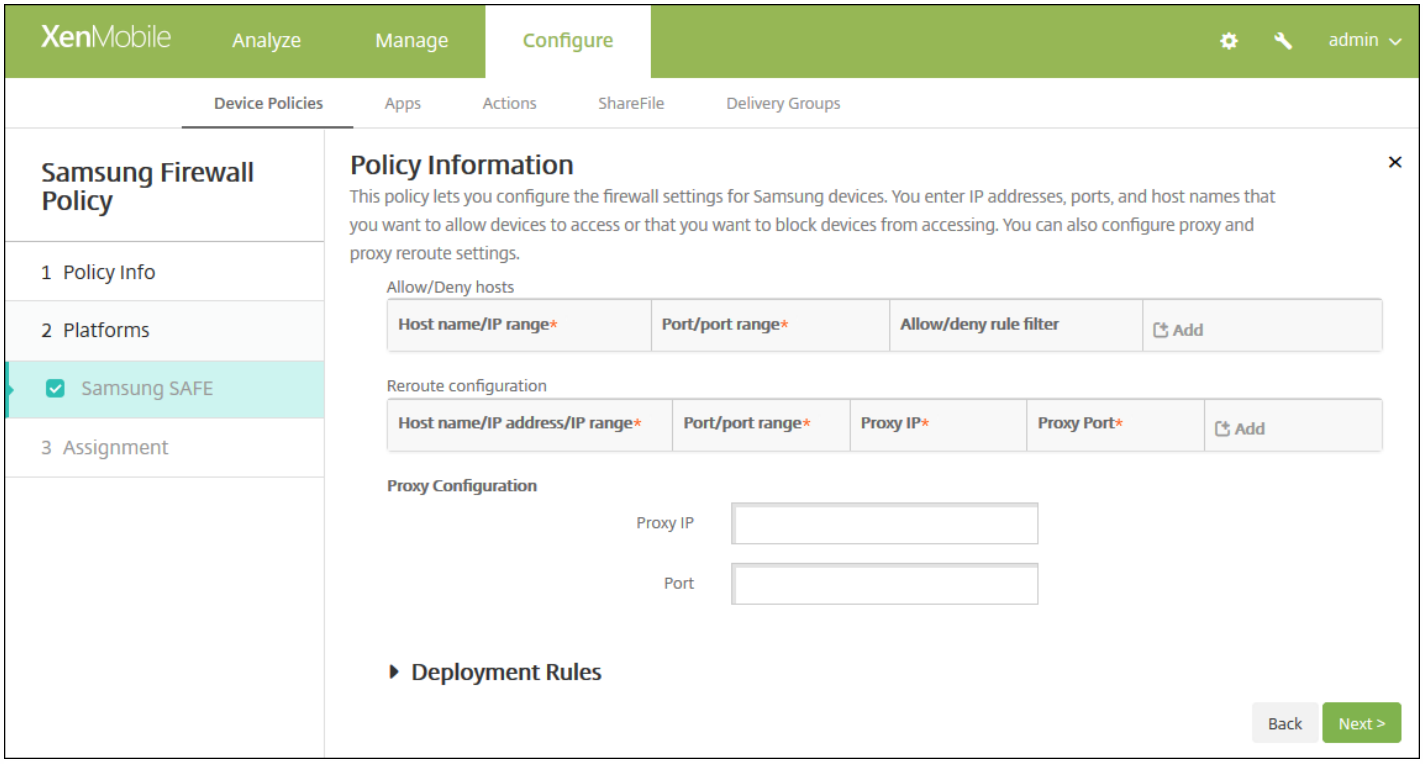




-
-

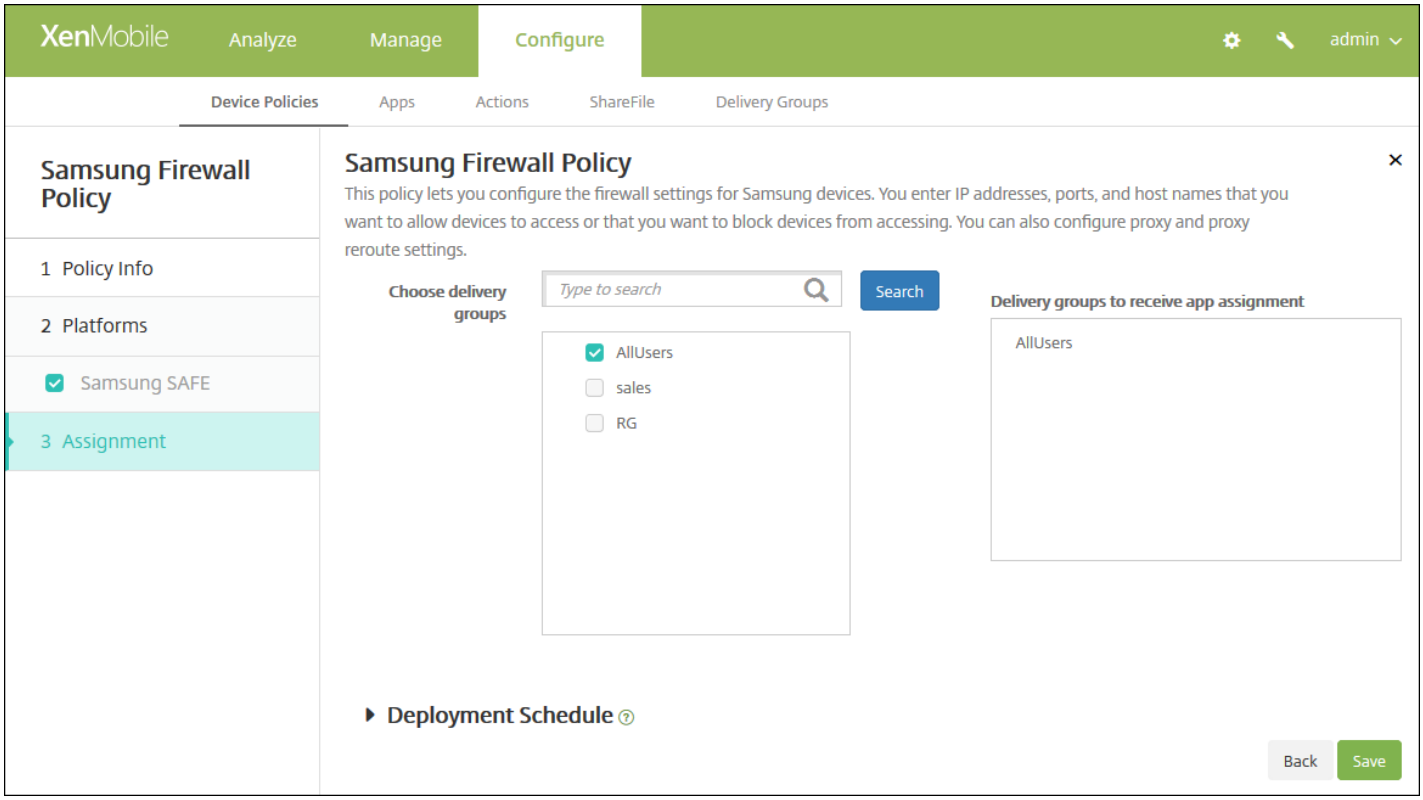


-
-



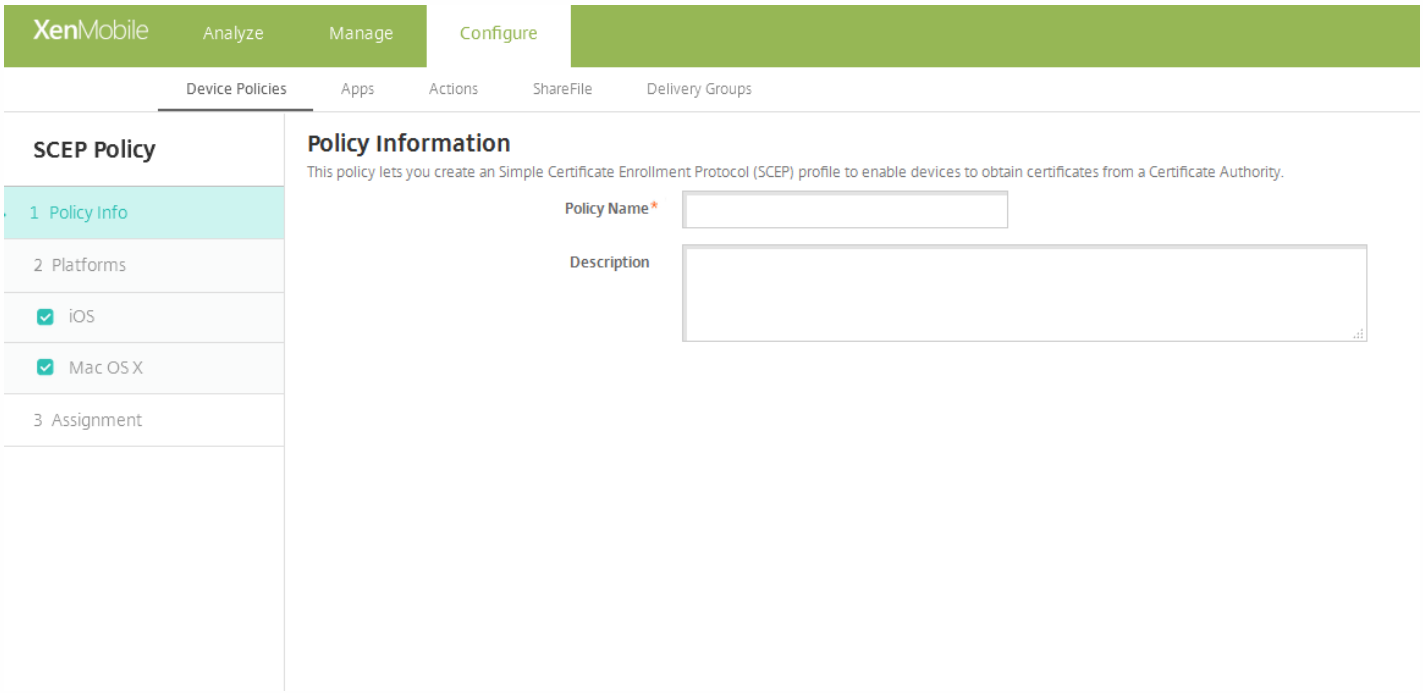
-
  -
    -
    -
    -
    -
-
  -
    -
    -
    -
    -

-
  -
  -



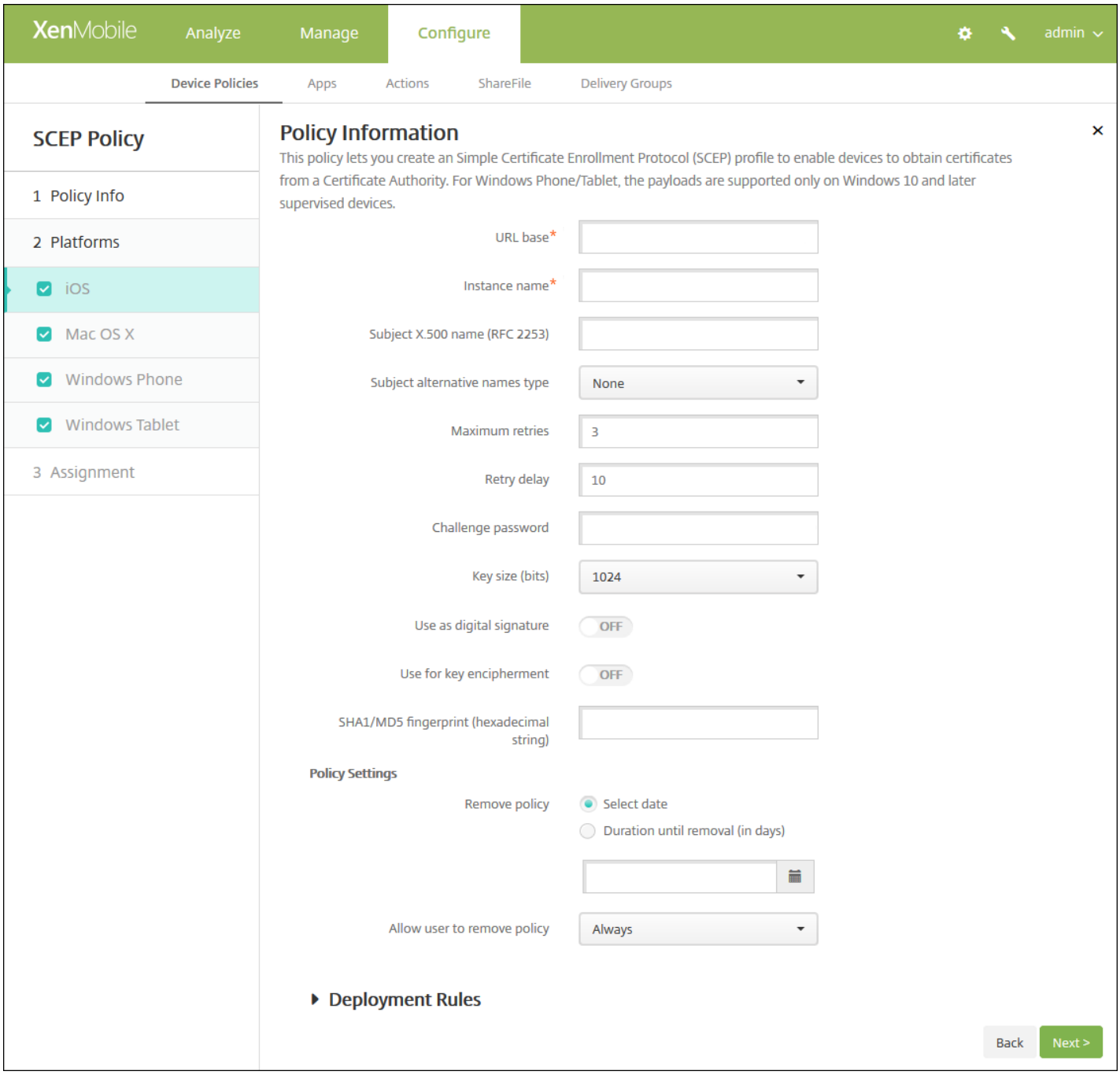
-
-
-
-

-
-



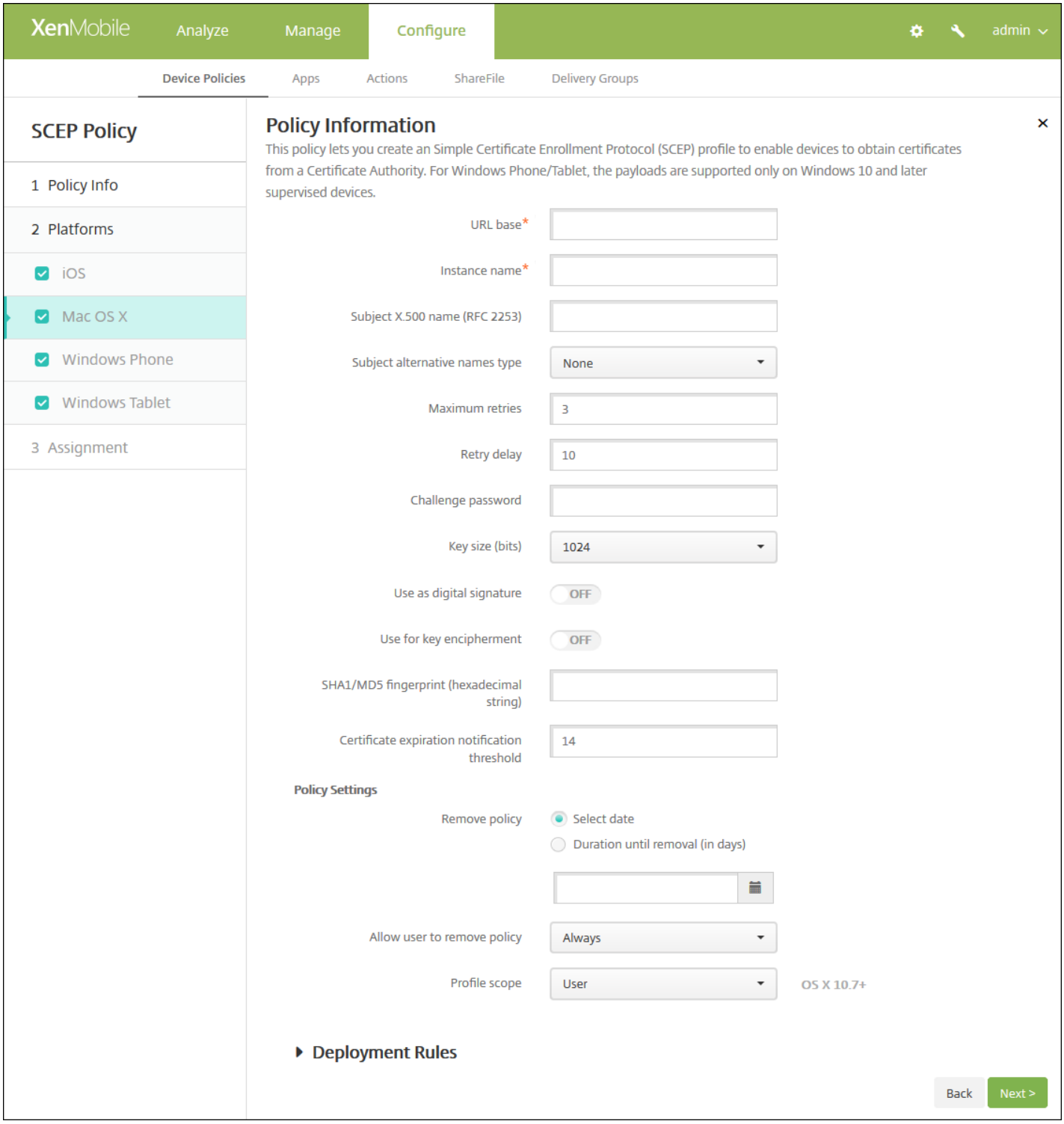
-
-

Configuración de los parámetros de iOS



-
-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -

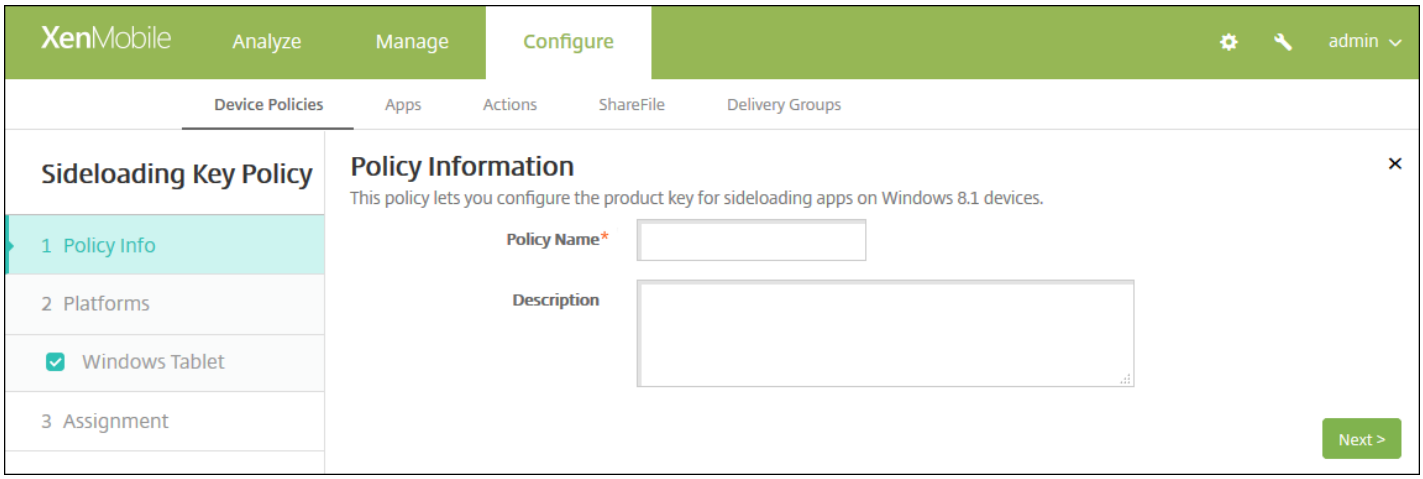
Configuración de los parámetros de Mac OS X



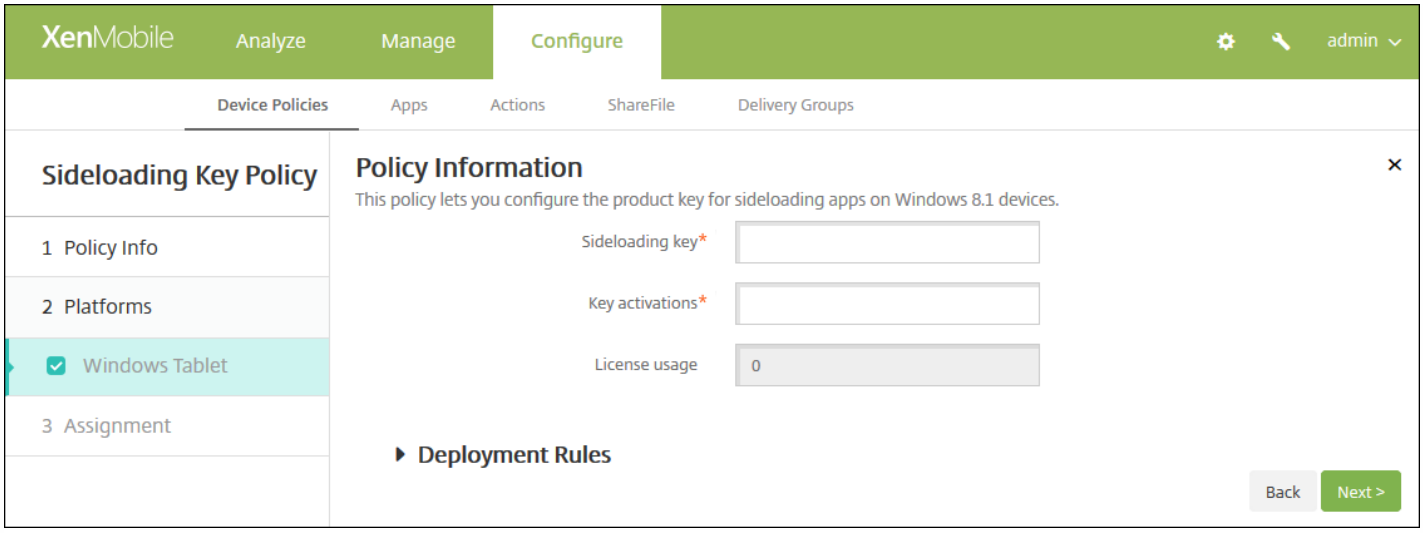
-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -
  -

-
-
-
-
-
-
-

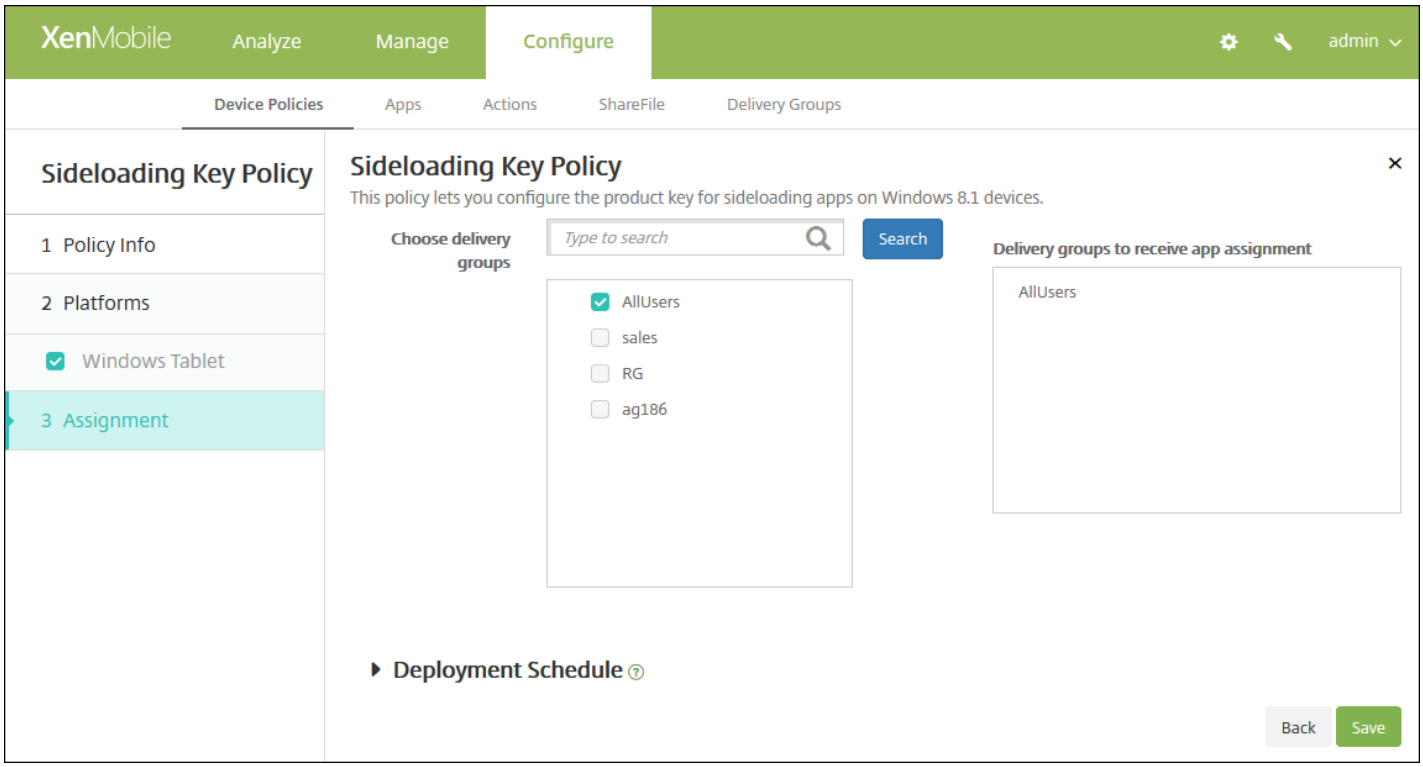
-
-



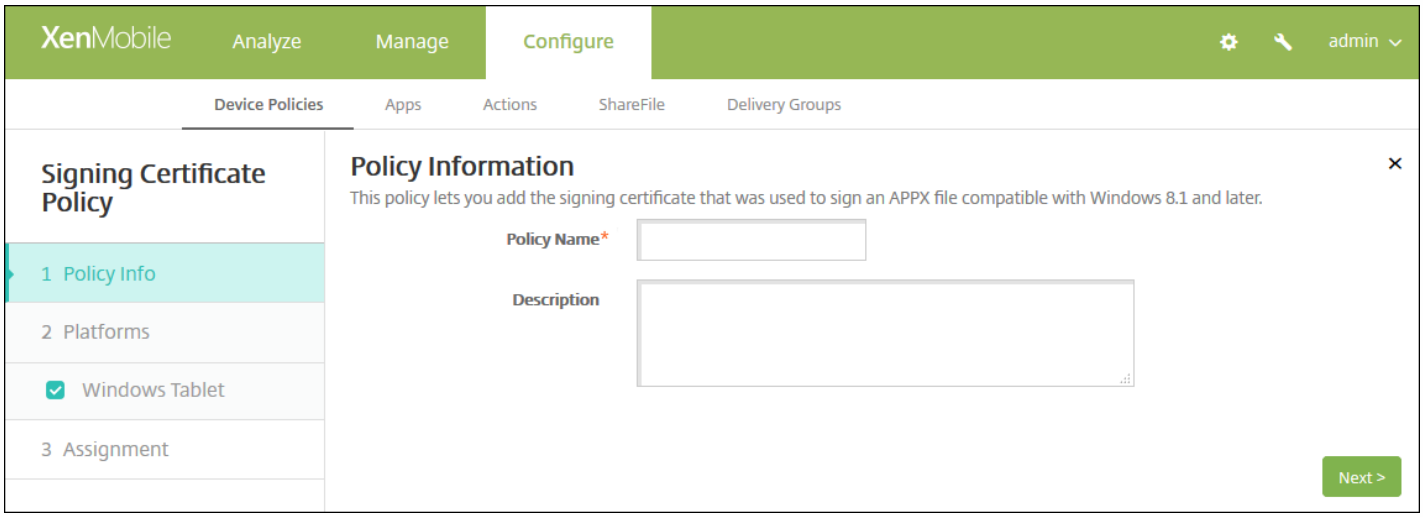
-
-



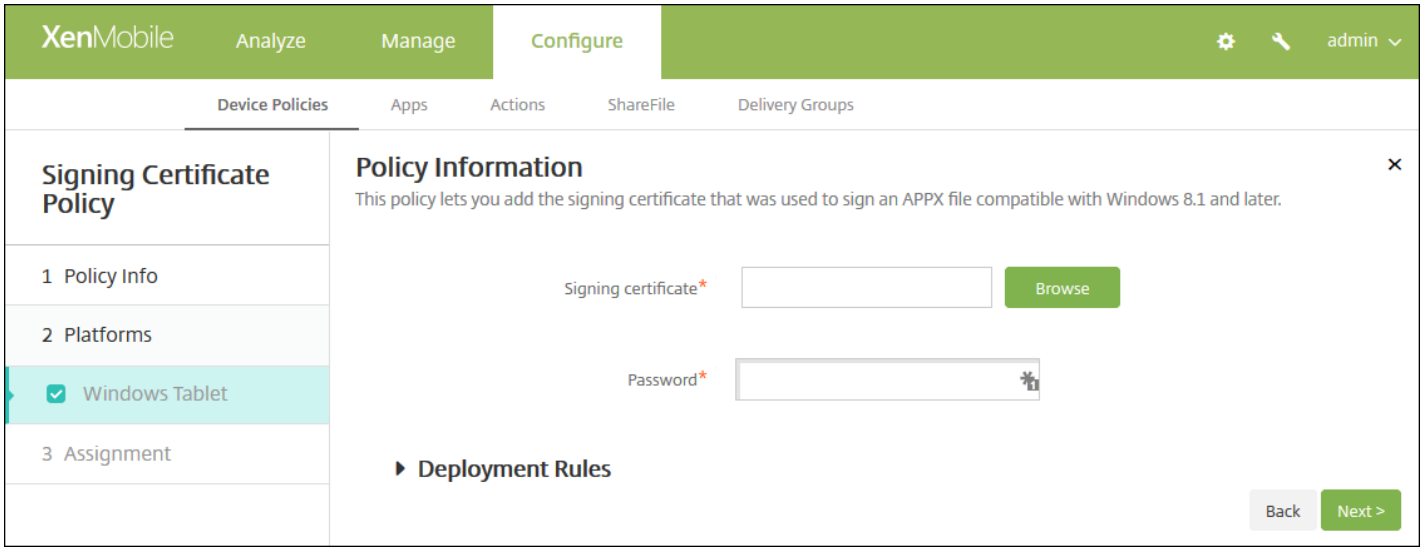
-
-
-



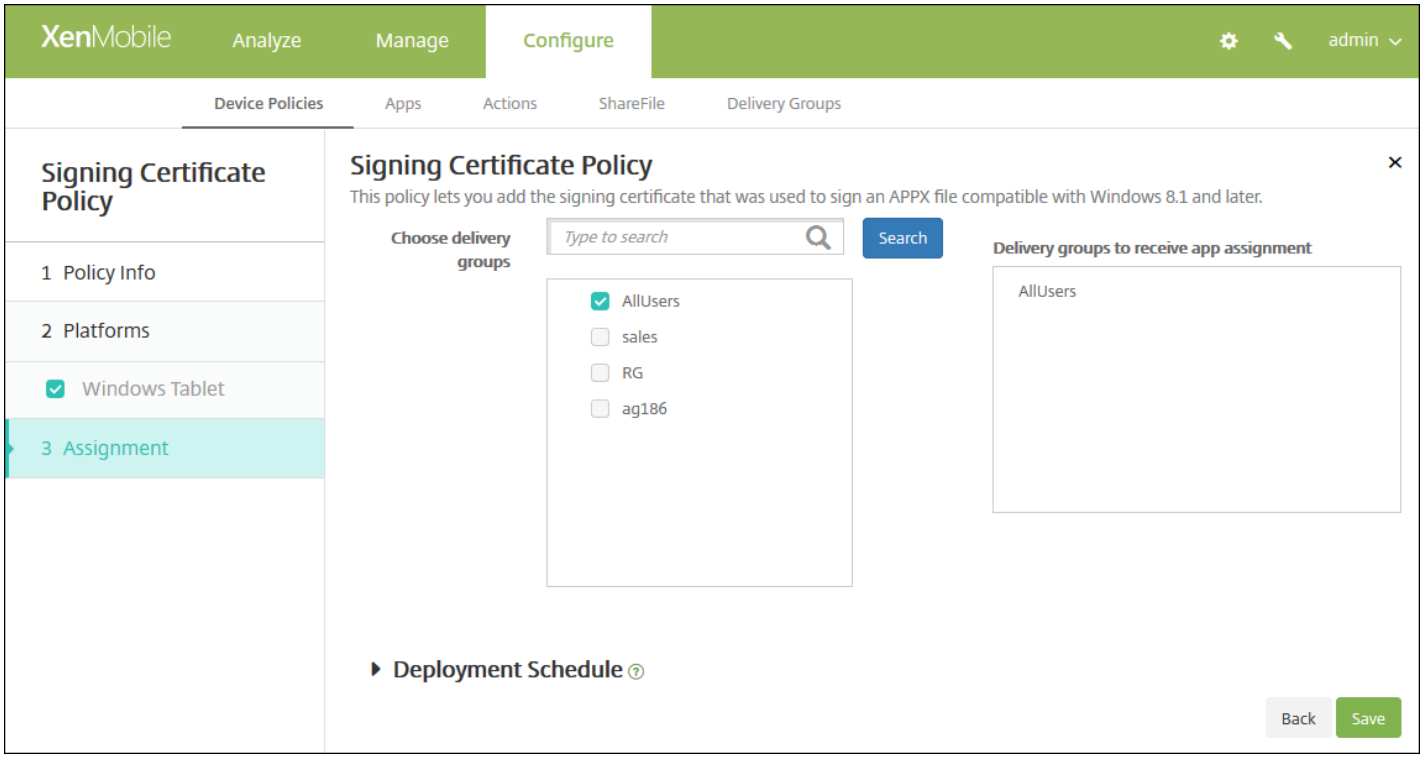
-
-
-
-
-
-
-



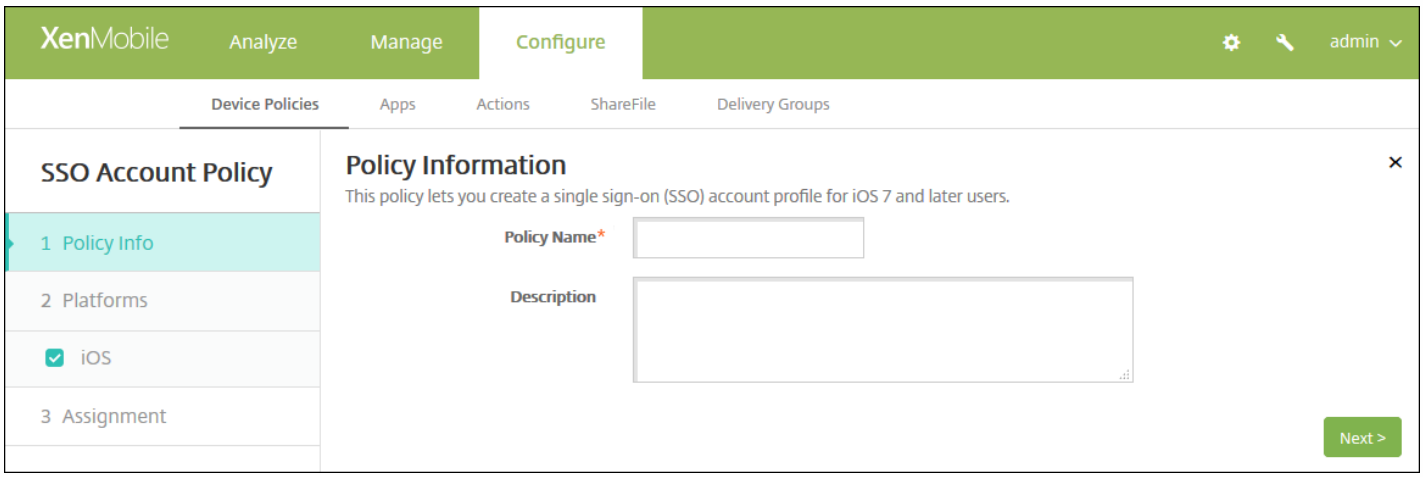
-
-



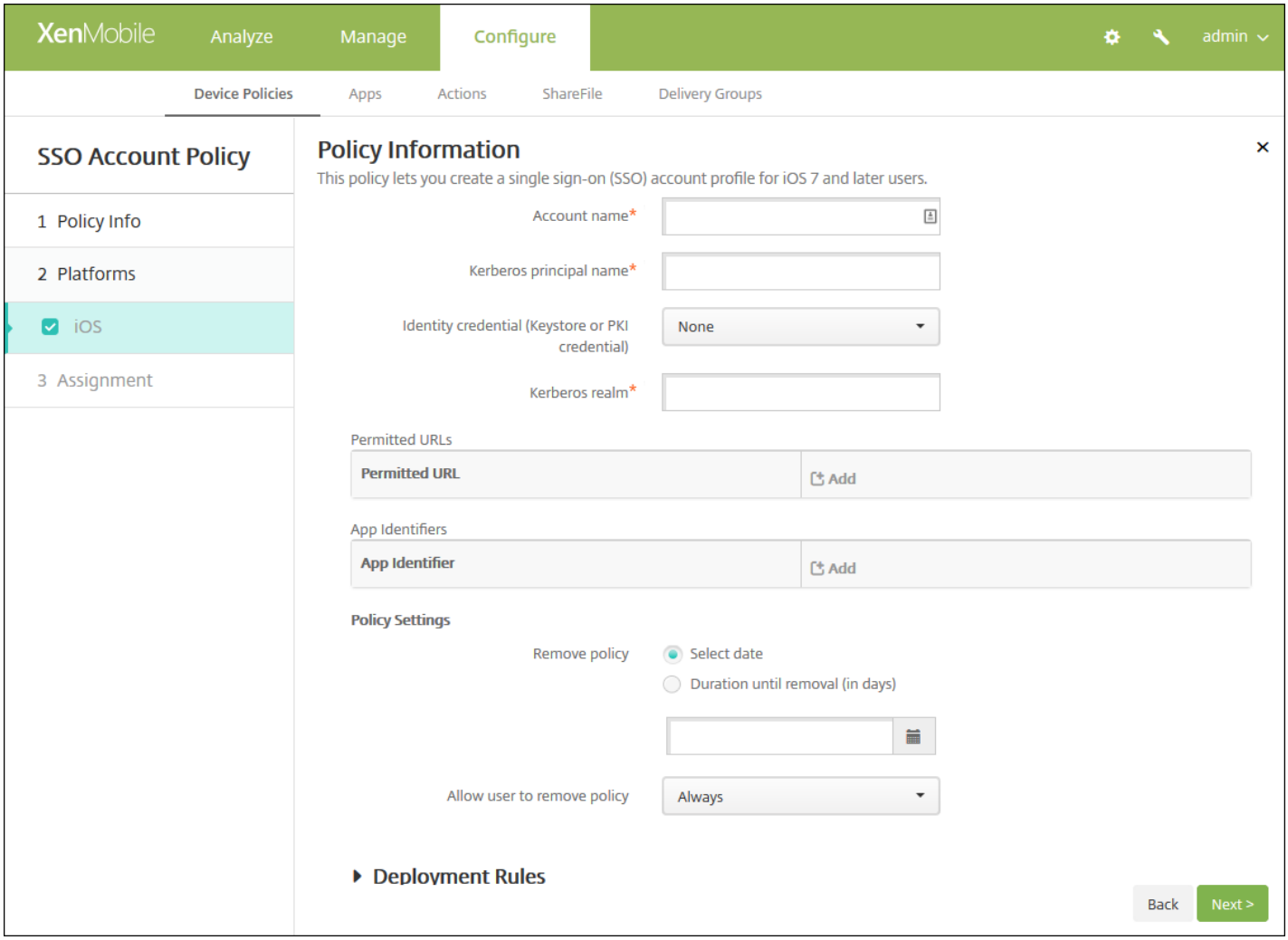
-
-



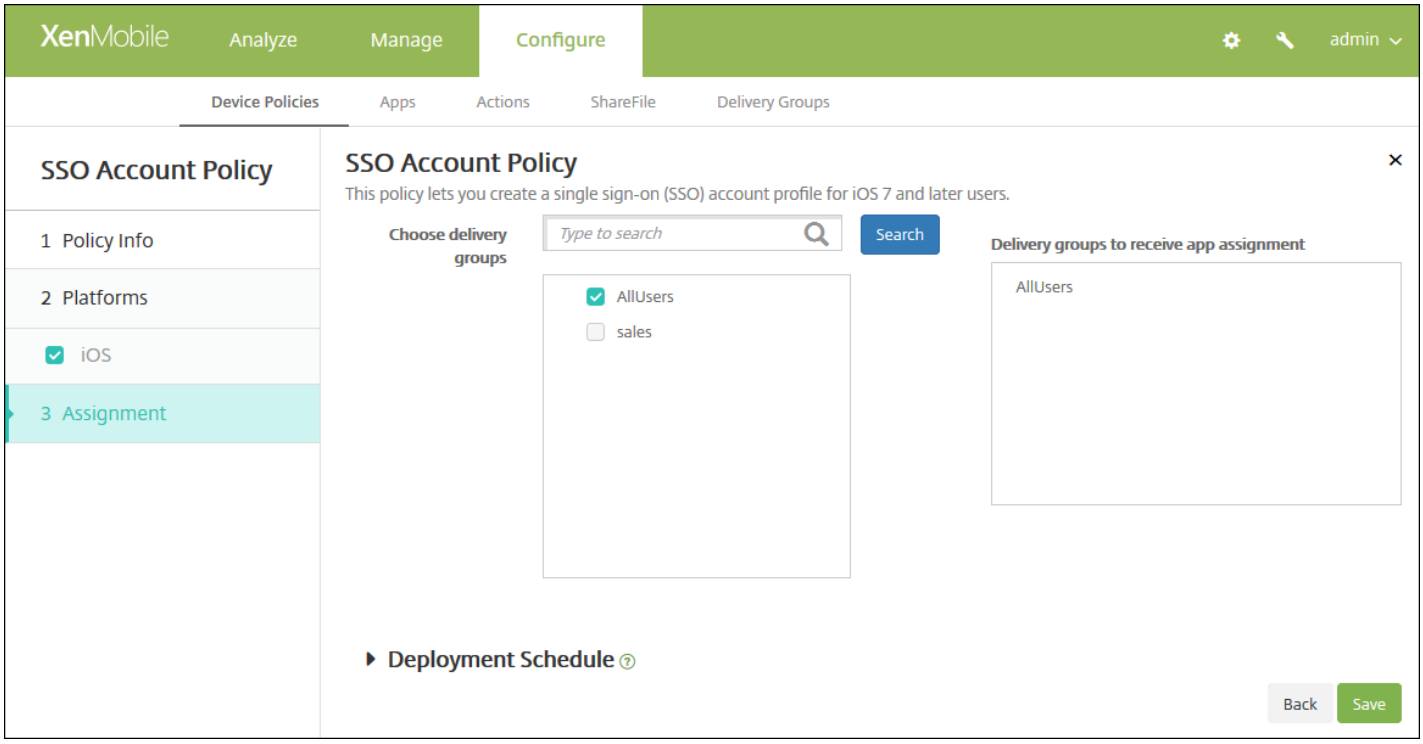
-
-
-
-
-
-
-



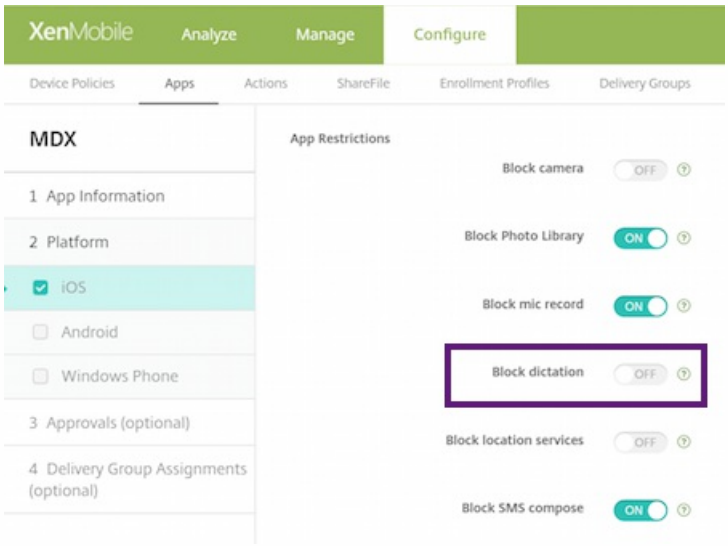
-
-

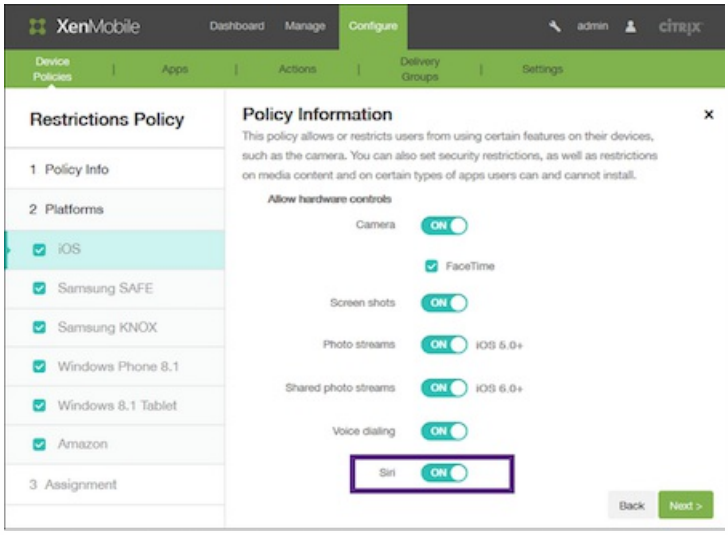


-
-
-
-
-
-



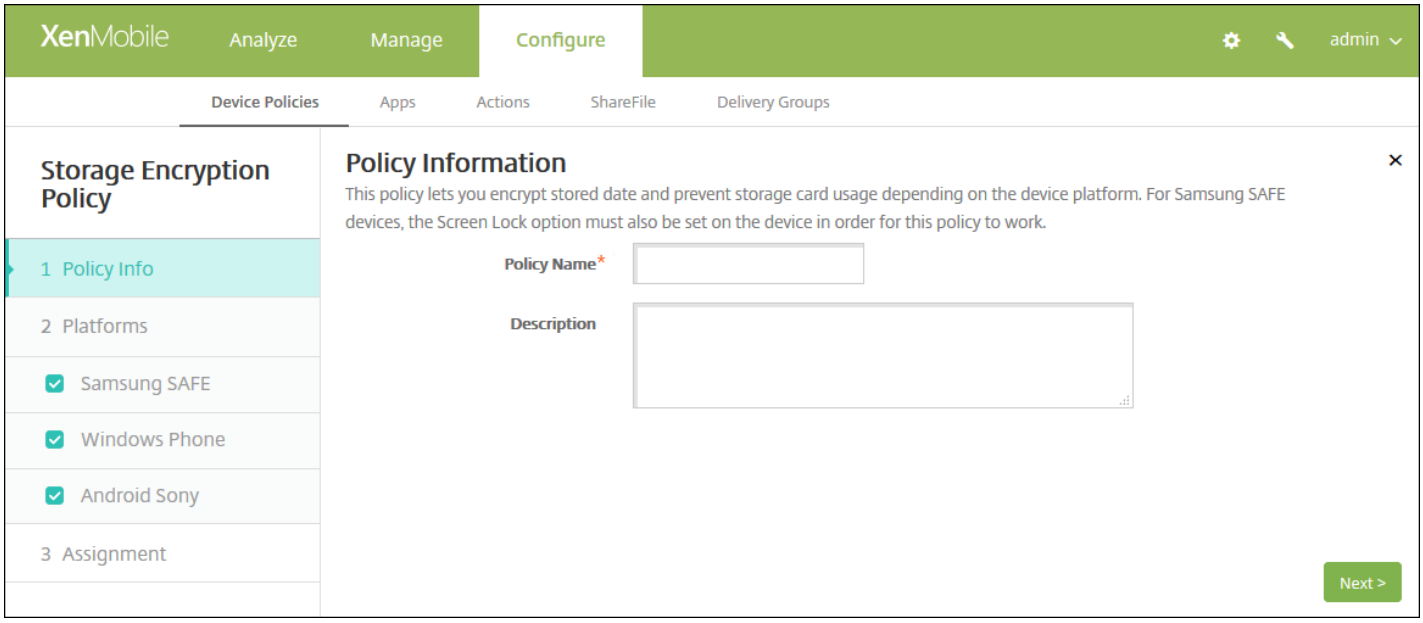
-
-
-
-
-
-
-





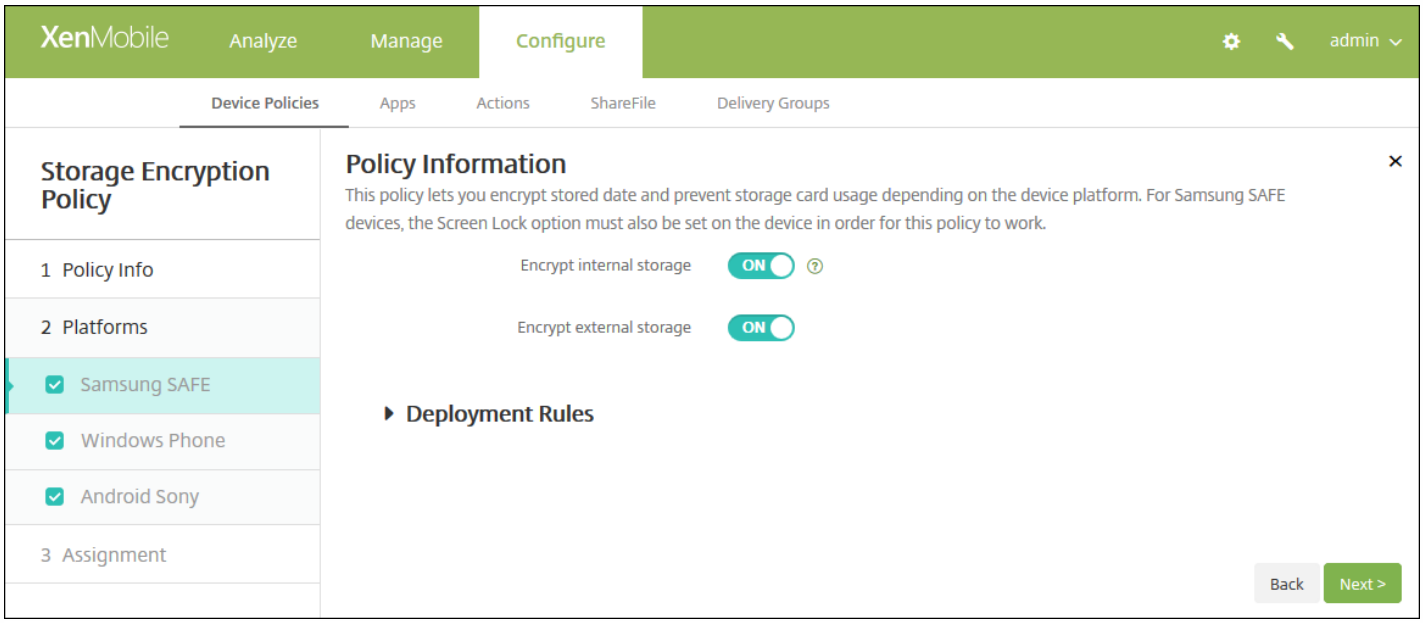
-
-

-
-
-



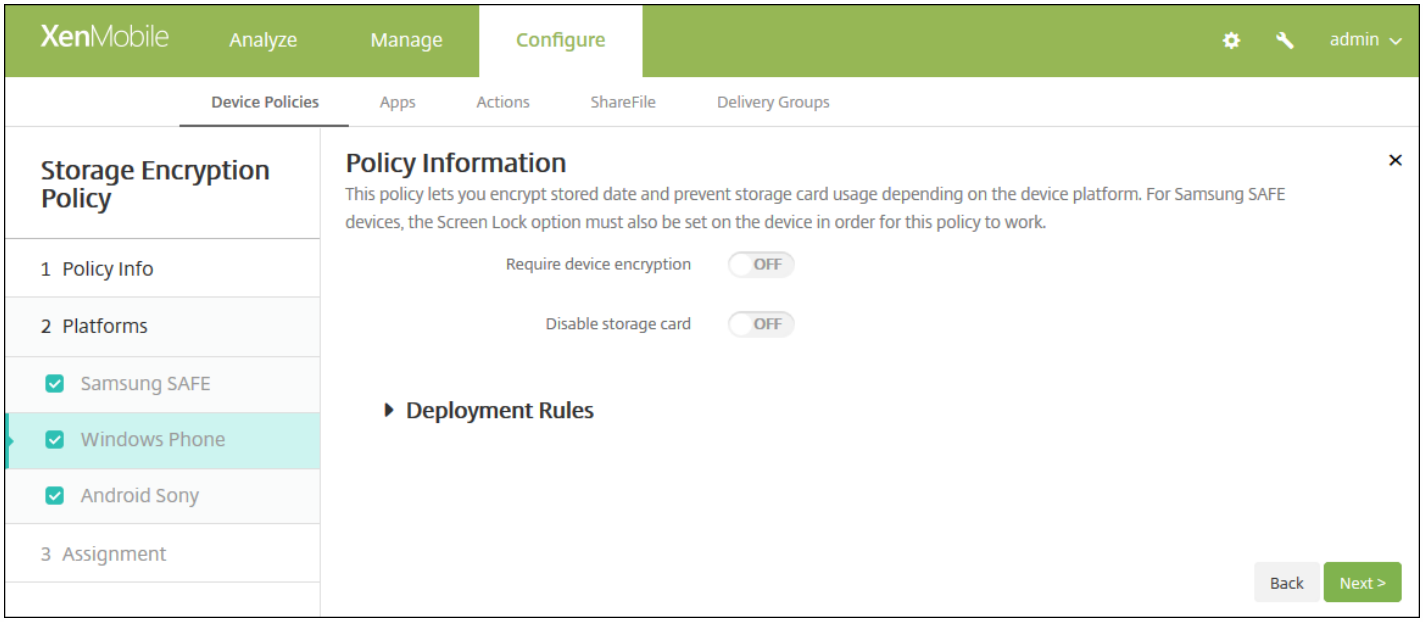
-
-

Configuración de los parámetros de Samsung SAFE



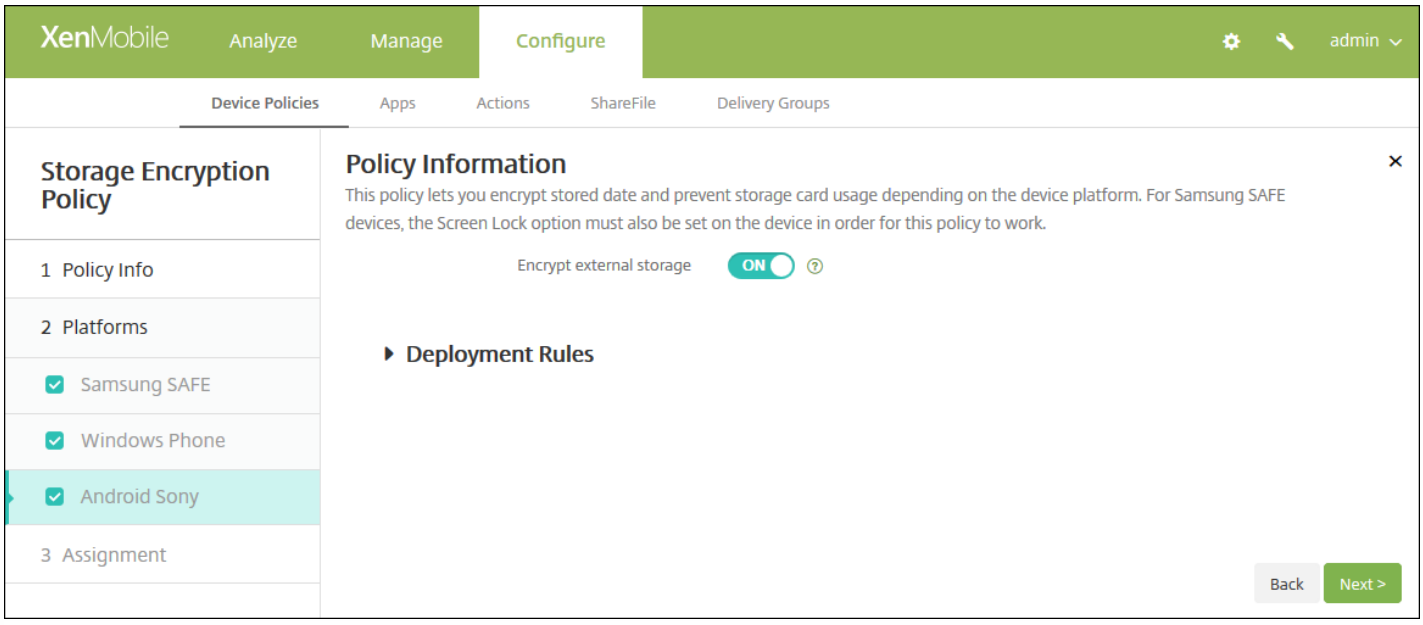
-
-

Configuración de los parámetros de Windows Phone

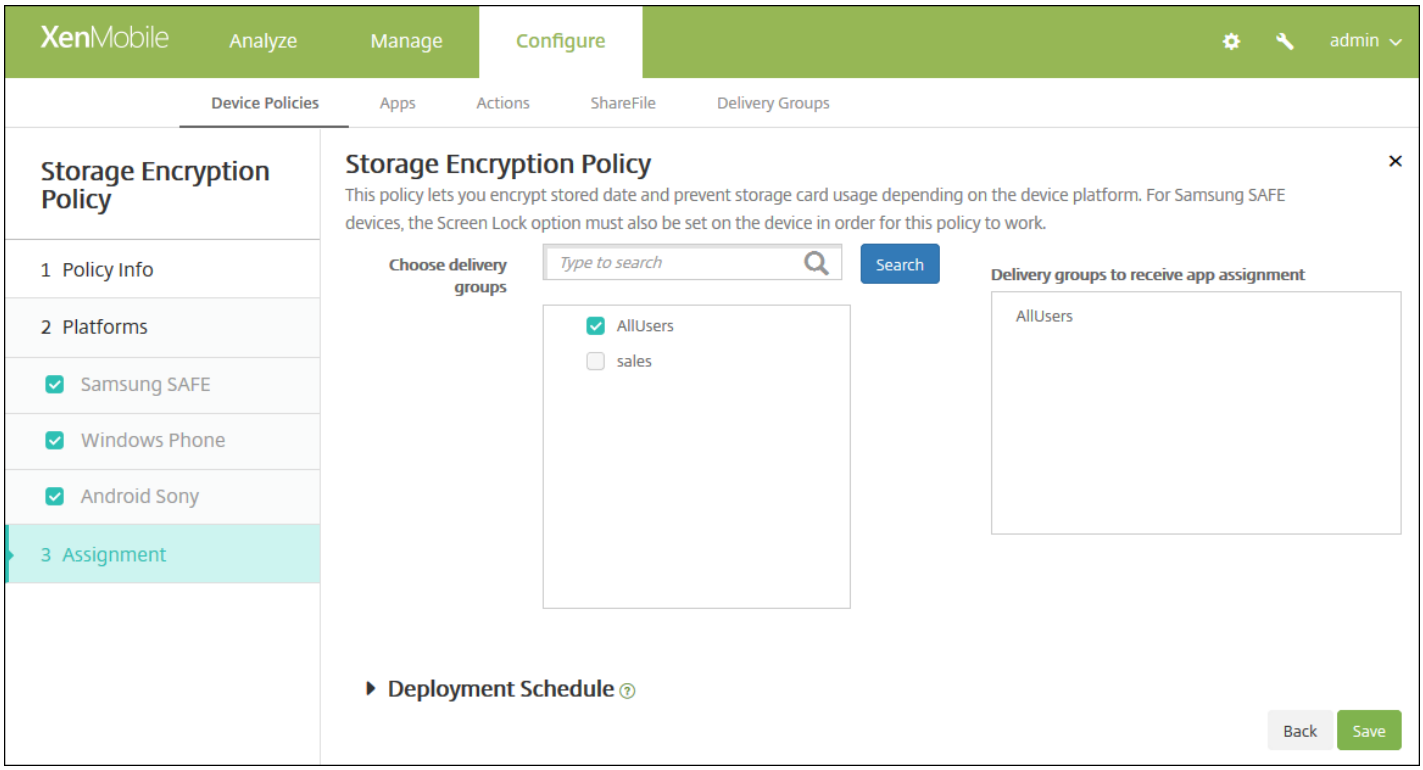


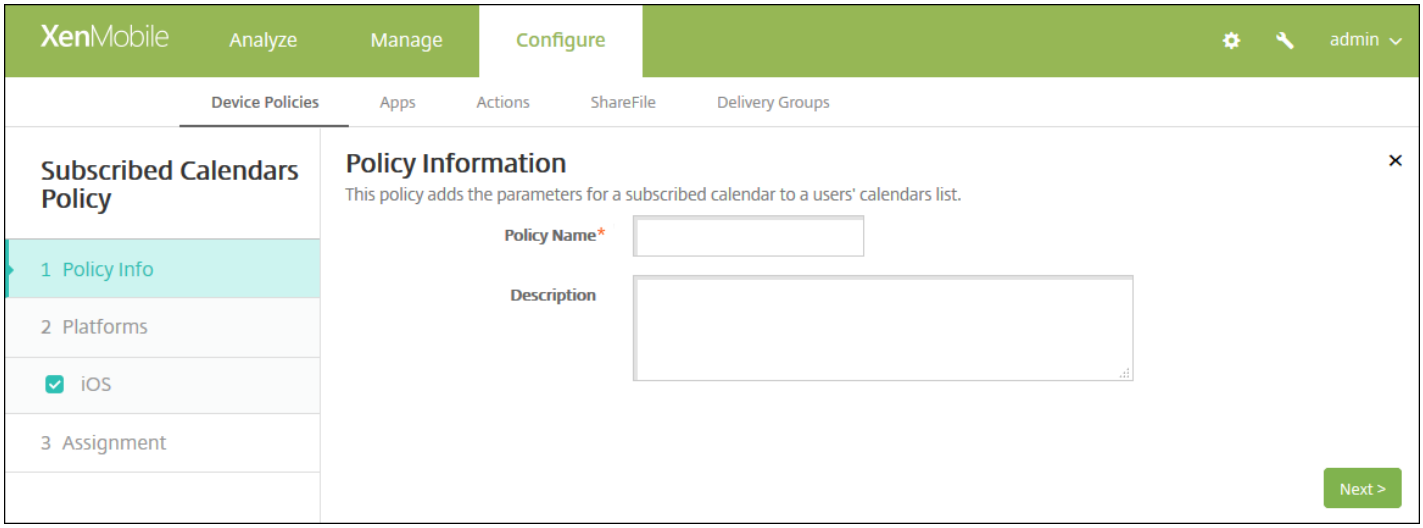
-
-

Configuración de los parámetros de Android Sony

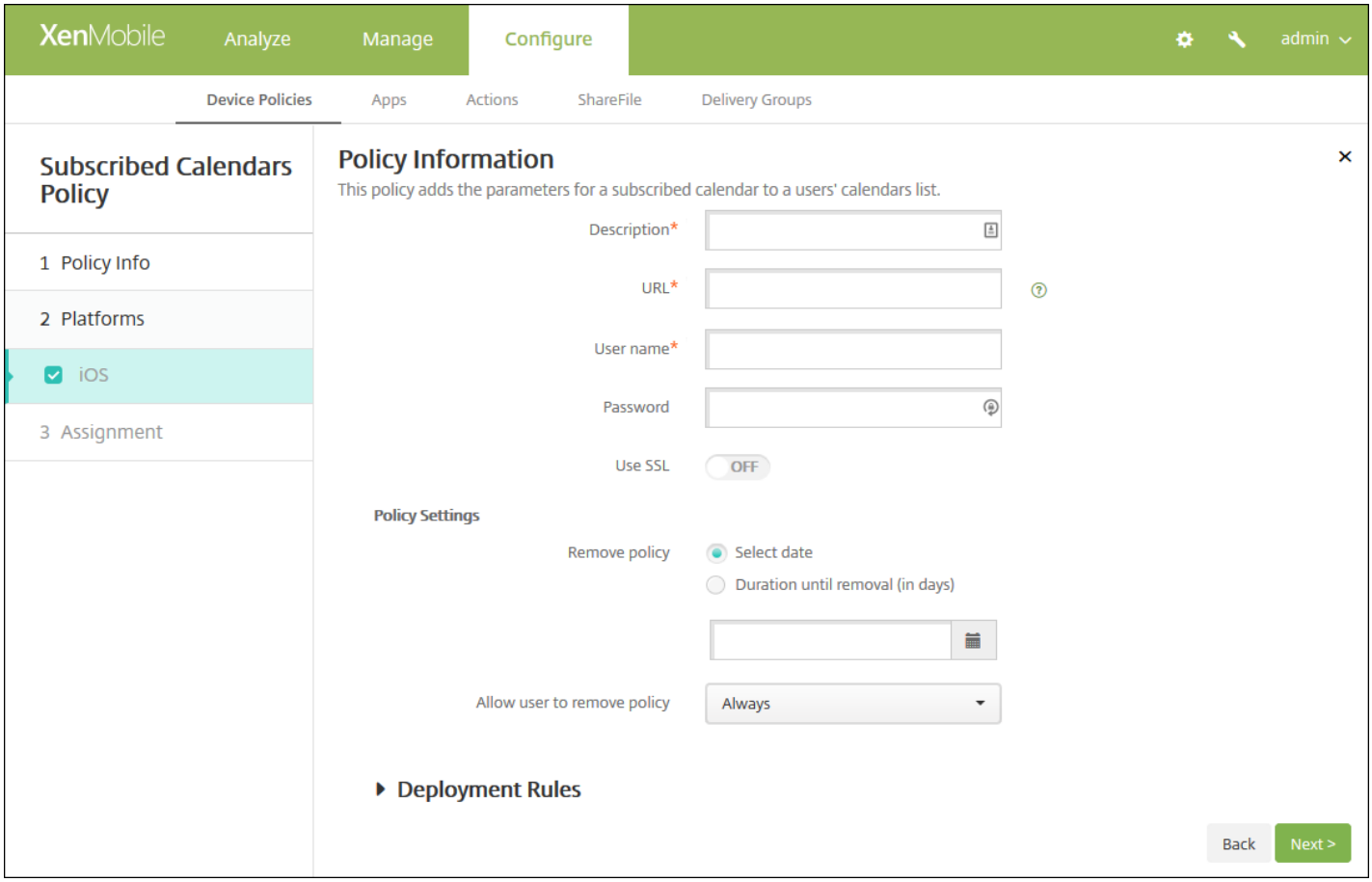


-





-
-

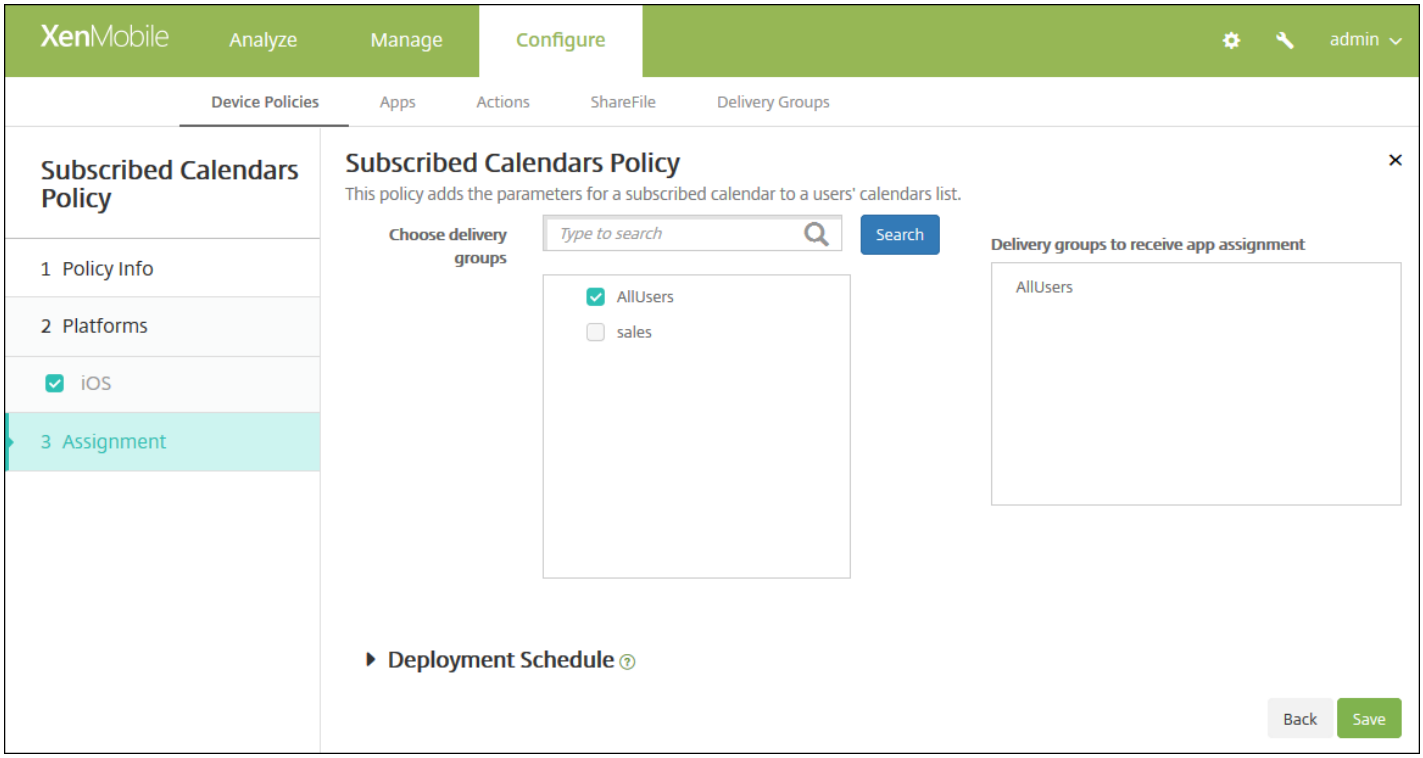


-
-

-
-
-

-
  -
  -

  -
  -



-
-
-
-
-
-
-

Directivas de términos y condiciones

Jul 27, 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. Debe suministrar un archivo para cada combinación de plataforma e idioma que quiera implementar. Para dispositivos Android y iOS, debe proporcionar archivos PDF. Para dispositivos Windows, debe suministrar archivos de texto (.txt) y los archivos de imagen correspondientes.

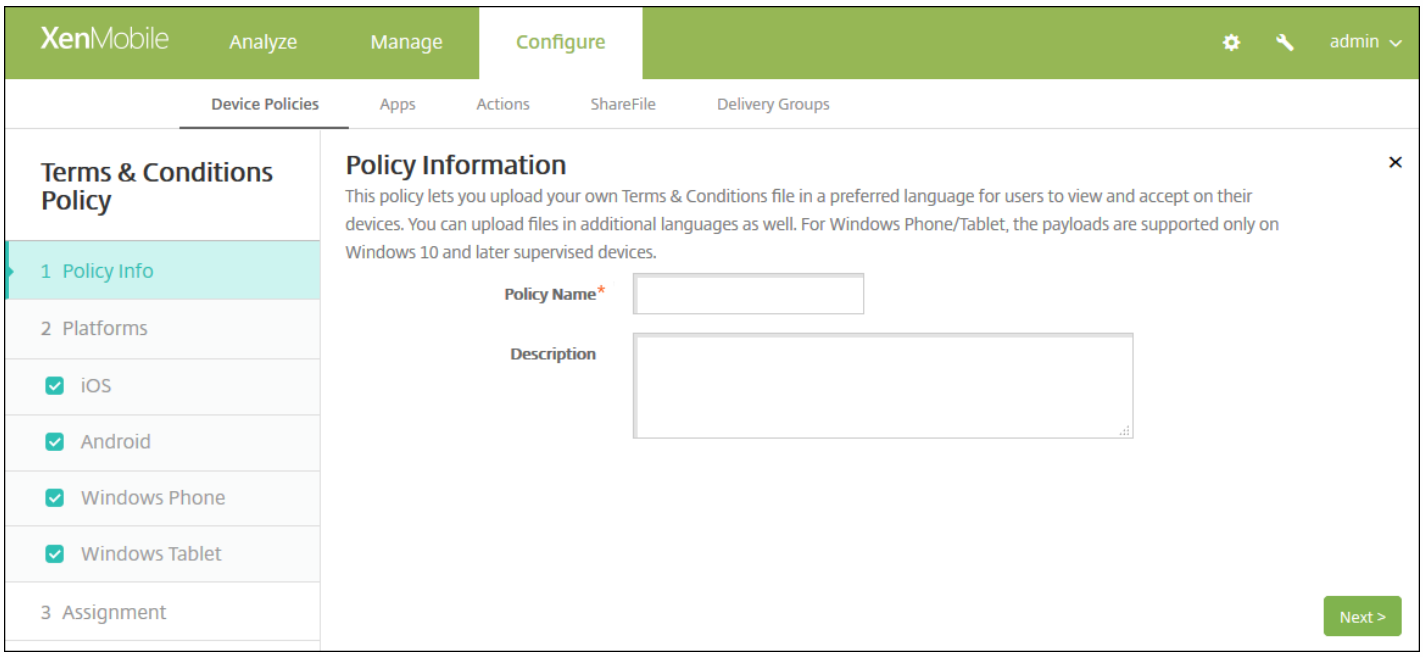
Configuración de iOS y Android

Configuración de Windows Phone y tabletas Windows

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

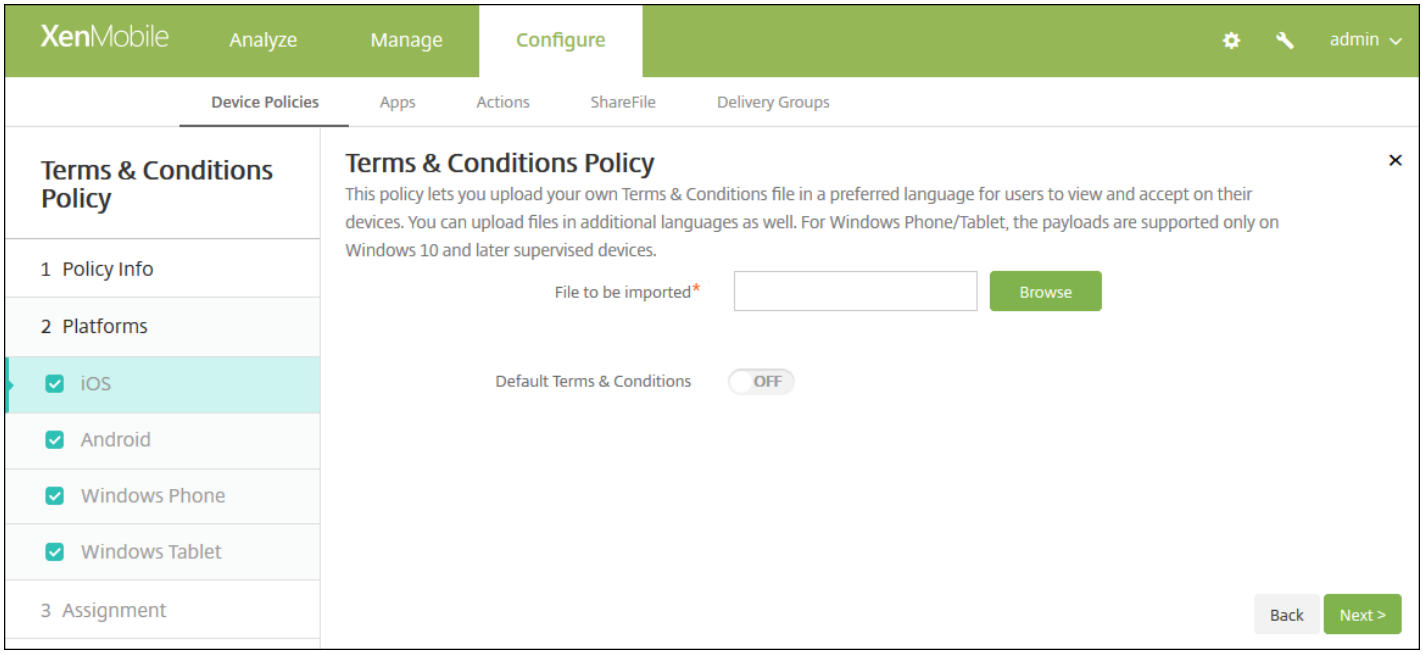
3. Haga clic en **Terms & Conditions**. Aparecerá la página **Terms & Conditions Policy**.



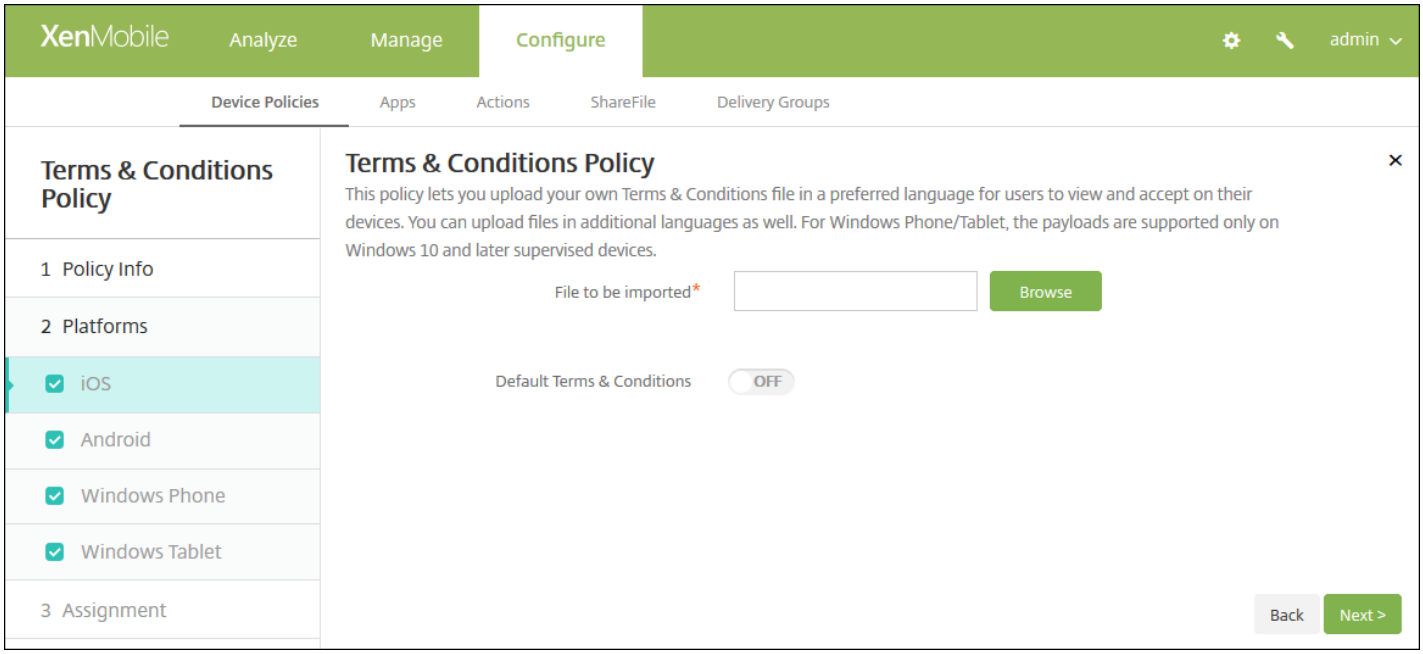
4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de asignación**Terms & Conditions Policy**.



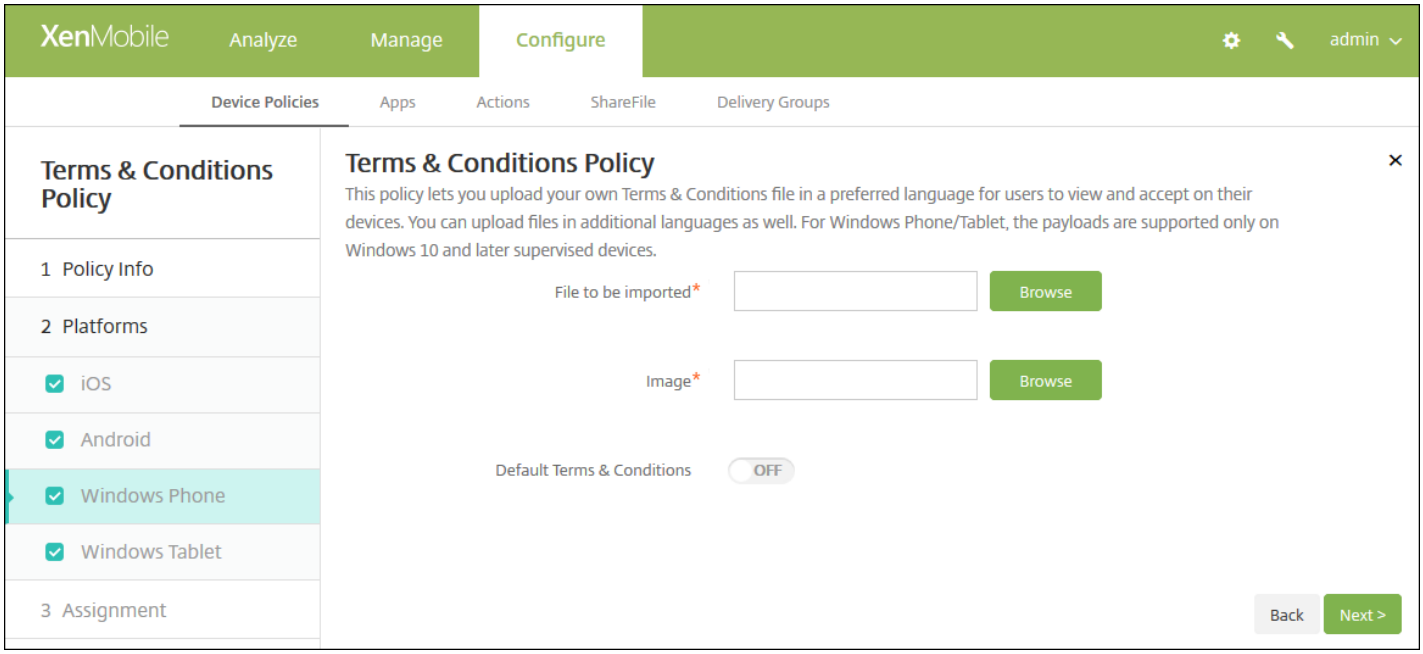
Configuración de iOS y Android



Configure estos parámetros:

- **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.
- **Default Terms & Conditions**. 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**.

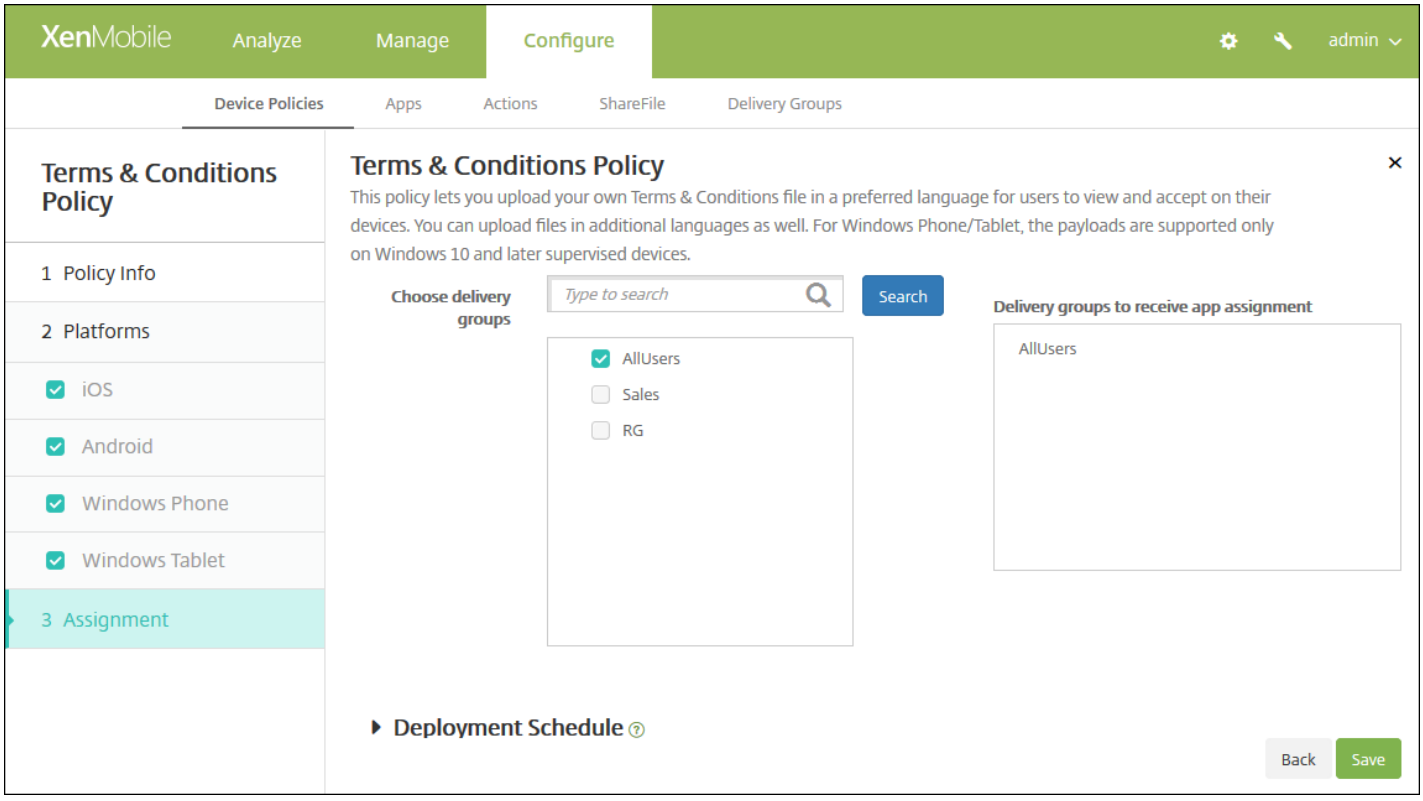
Configuración de Windows Phone y tabletas Windows



Configure estos parámetros:

- **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.
- **Image**. Para seleccionar el archivo de imagen a importar, haga clic en **Browse** y vaya a la ubicación de ese archivo.
- **Default Terms & Conditions**. 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**.

6. Haga clic en **Next**. Aparecerá la página de asignación **Terms & Conditions 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. Haga clic en **Save**.

Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

Jul 27, 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.

Directivas VPN de dispositivos

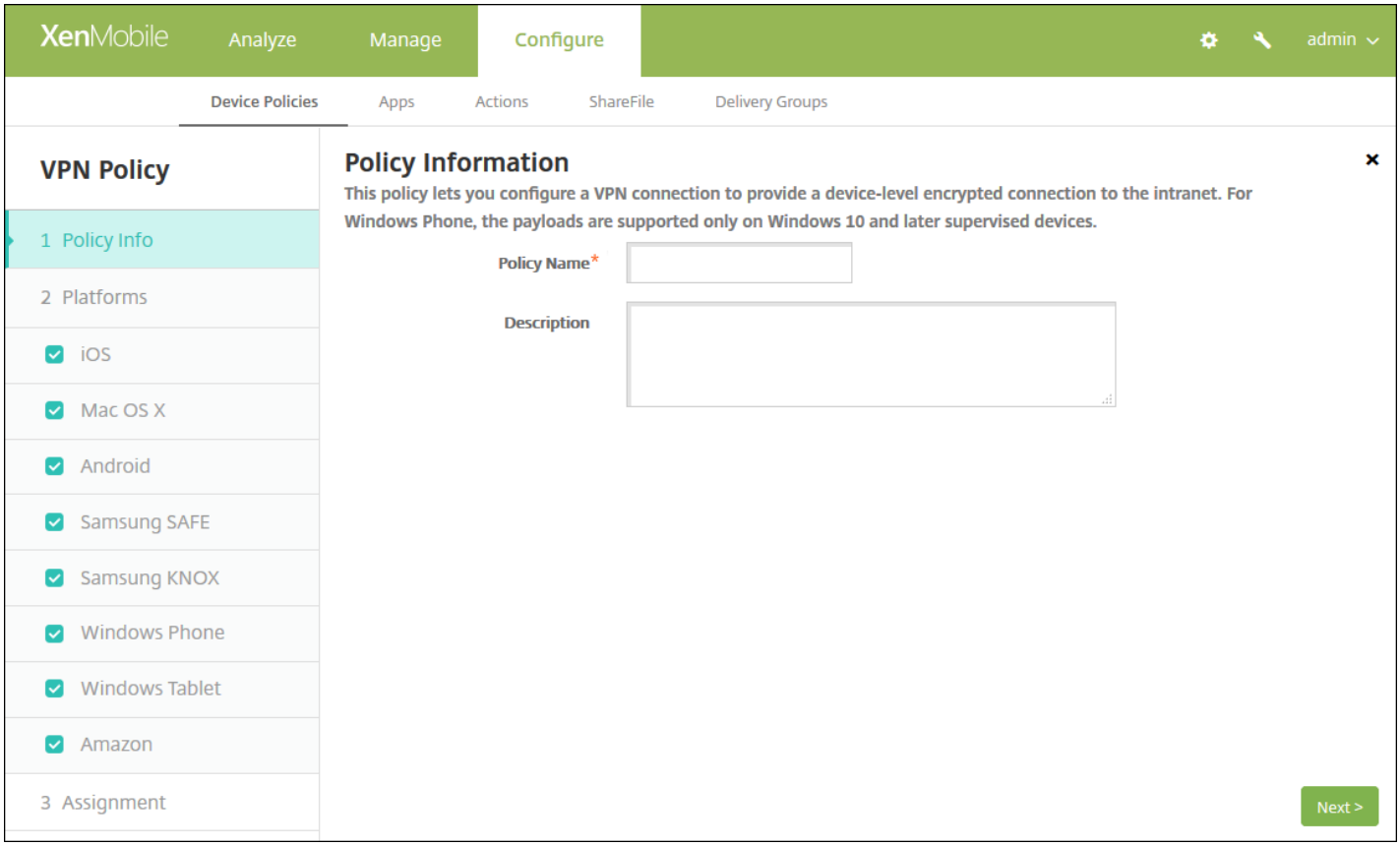
Oct 31, 2016

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 (incluidos los dispositivos habilitados para Android for Work), Samsung SAFE, Samsung KNOX, tabletas Windows, Windows Phone y Amazon. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente 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**. 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:

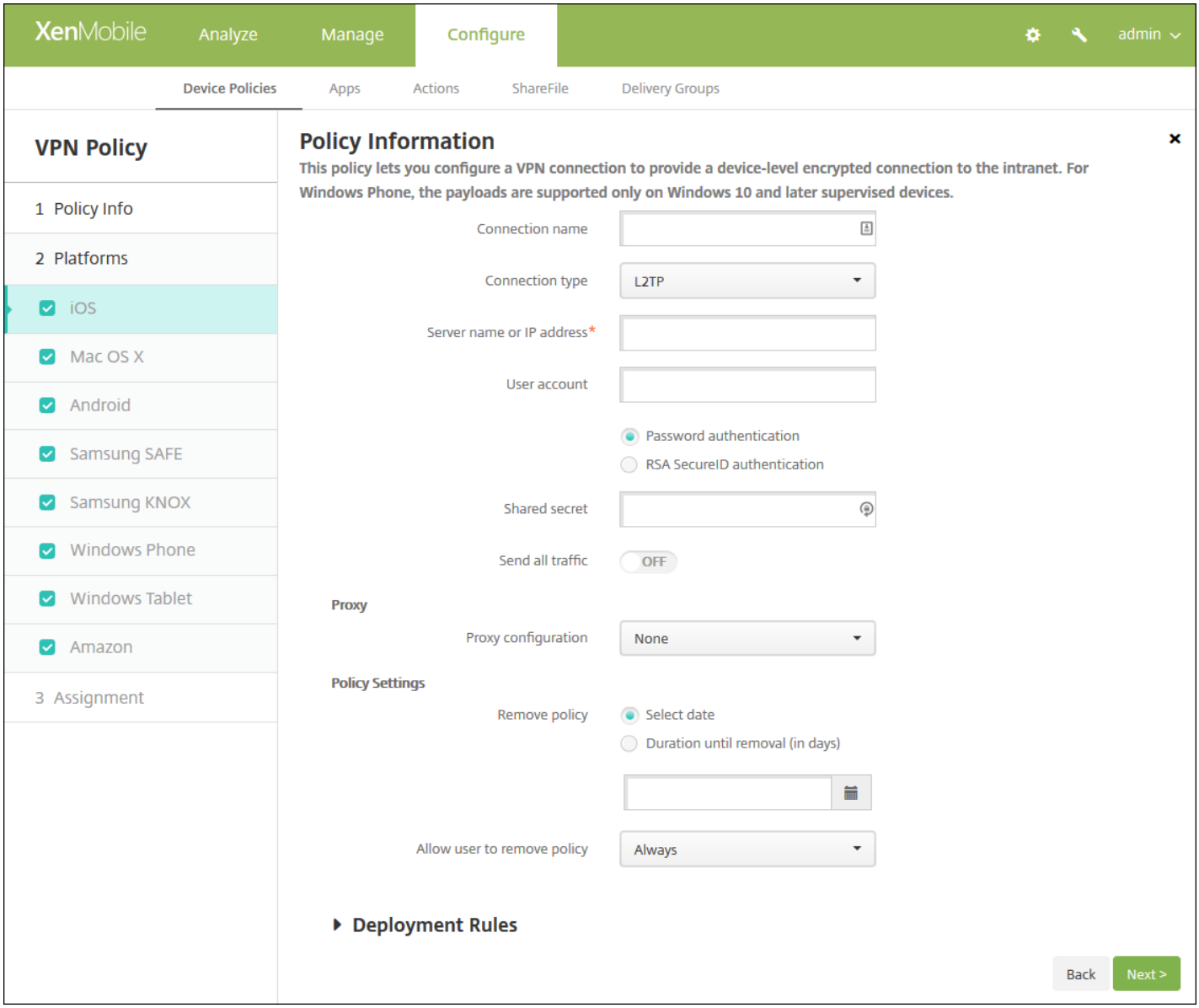
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**. Al aparecer la página **Policy Platforms**, todas las plataformas están seleccionadas, y verá en primer lugar la plataforma de iOS.

6. En **Platforms**, seleccione la plataforma o las plataformas que quiere agregar. Borre aquellas plataformas que no quiera configurar.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure estos parámetros:

- **Connection name**. Escriba un nombre para la conexión.
- **Connection type**. En la lista, haga clic en el protocolo que se va a usar para esta conexión. El valor predeterminado es **L2TP**.
  - **L2TP**. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP**. Túnel punto a punto.
  - **IPsec**. La conexión VPN de su empresa.
  - **Cisco AnyConnect**. Cliente VPN AnyConnect de Cisco.
  - **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.
  - **Citrix VPN**. Cliente VPN de Citrix 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.

Configuración del protocolo L2TP

Configuración del protocolo PPTP

Configuración del protocolo IPsec

Configuración del protocolo AnyConnect de Cisco

Configuración del protocolo SSL de Juniper

Configuración del protocolo SSL de F5

Configuración del protocolo SonicWALL

Configuración del protocolo VIA de Ariba

Configuración del protocolo IKEv2

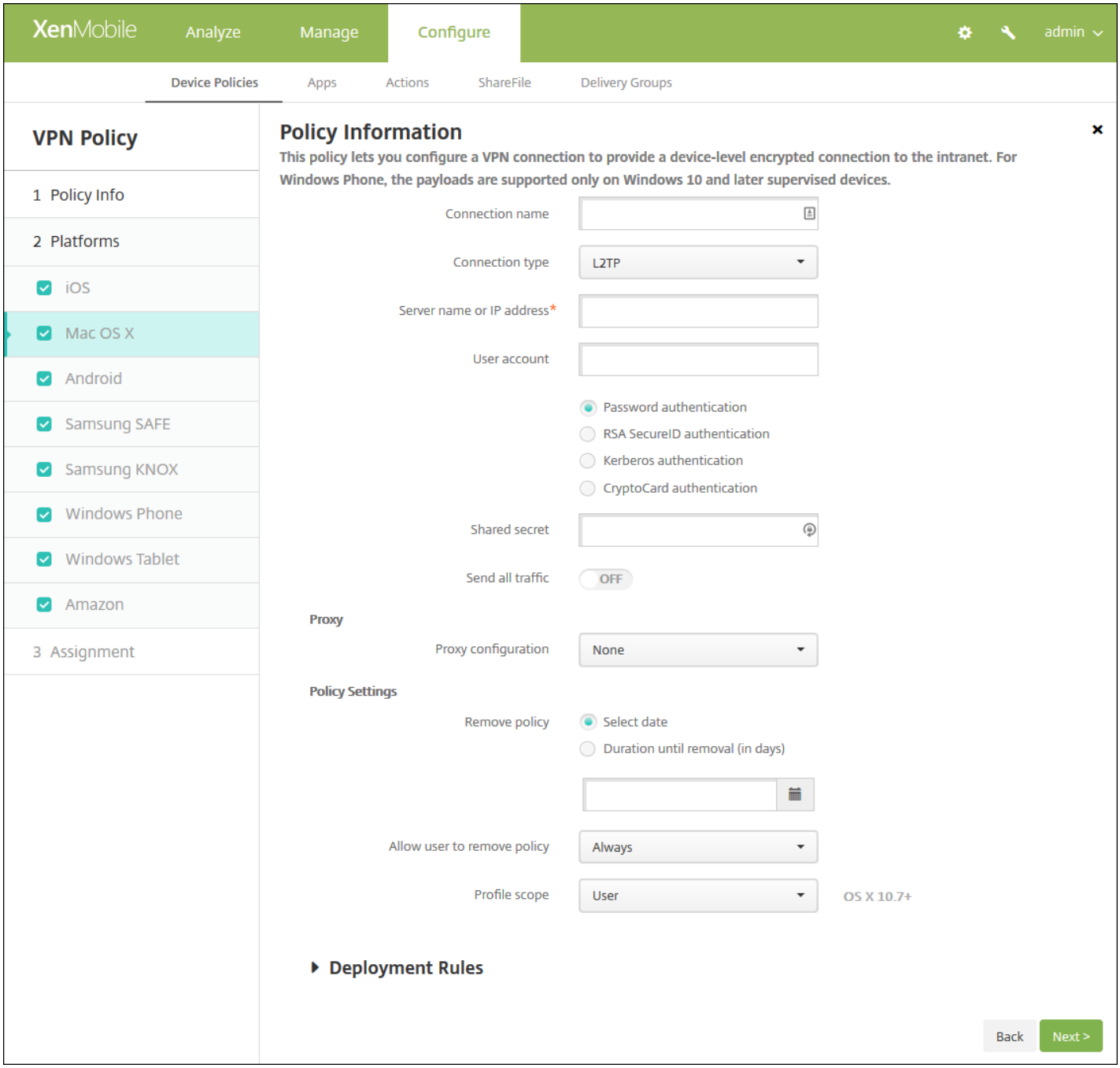
Configuración del protocolo VPN de Citrix

Configuración del protocolo SSL personalizado

Configuración de las opciones de Enable VPN on demand

- **Proxy**
  - **Proxy configuration**. En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **None**.
    - Si habilita **Manual**, configure los siguientes parámetros:
      - **Host name or IP address for the proxy server**. Escriba el nombre o la dirección IP de host del servidor proxy. Este campo es obligatorio.
      - **Port for the proxy server**. Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
      - **User name**. Si quiere, escriba un nombre de usuario para el servidor proxy.
      - **Password**. Si quiere, escriba una contraseña de servidor proxy.
    - Si selecciona **Automatic**, configure este parámetro:
      - **Proxy server URL**. Escriba la URL del servidor proxy. Este campo es obligatorio.
- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure estos parámetros:

- **Connection name**. Escriba un nombre para la conexión.
- **Connection type**. En la lista, haga clic en el protocolo que se va a usar para esta conexión. El valor predeterminado es L2TP.
  - **L2TP**. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP**. Túnel punto a punto.
  - **IPsec**. La conexión VPN de su empresa.
  - **Cisco AnyConnect**. Cliente VPN AnyConnect de Cisco.
  - **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.
- **Citrix VPN**. Cliente VPN de Citrix.
- **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.

Configuración del protocolo L2TP

Configuración del protocolo PPTP

Configuración del protocolo IPsec

Configuración del protocolo AnyConnect de Cisco

Configuración del protocolo SSL de Juniper

Configuración del protocolo SSL de F5

Configuración del protocolo SonicWALL

Configuración del protocolo VIA de Ariba

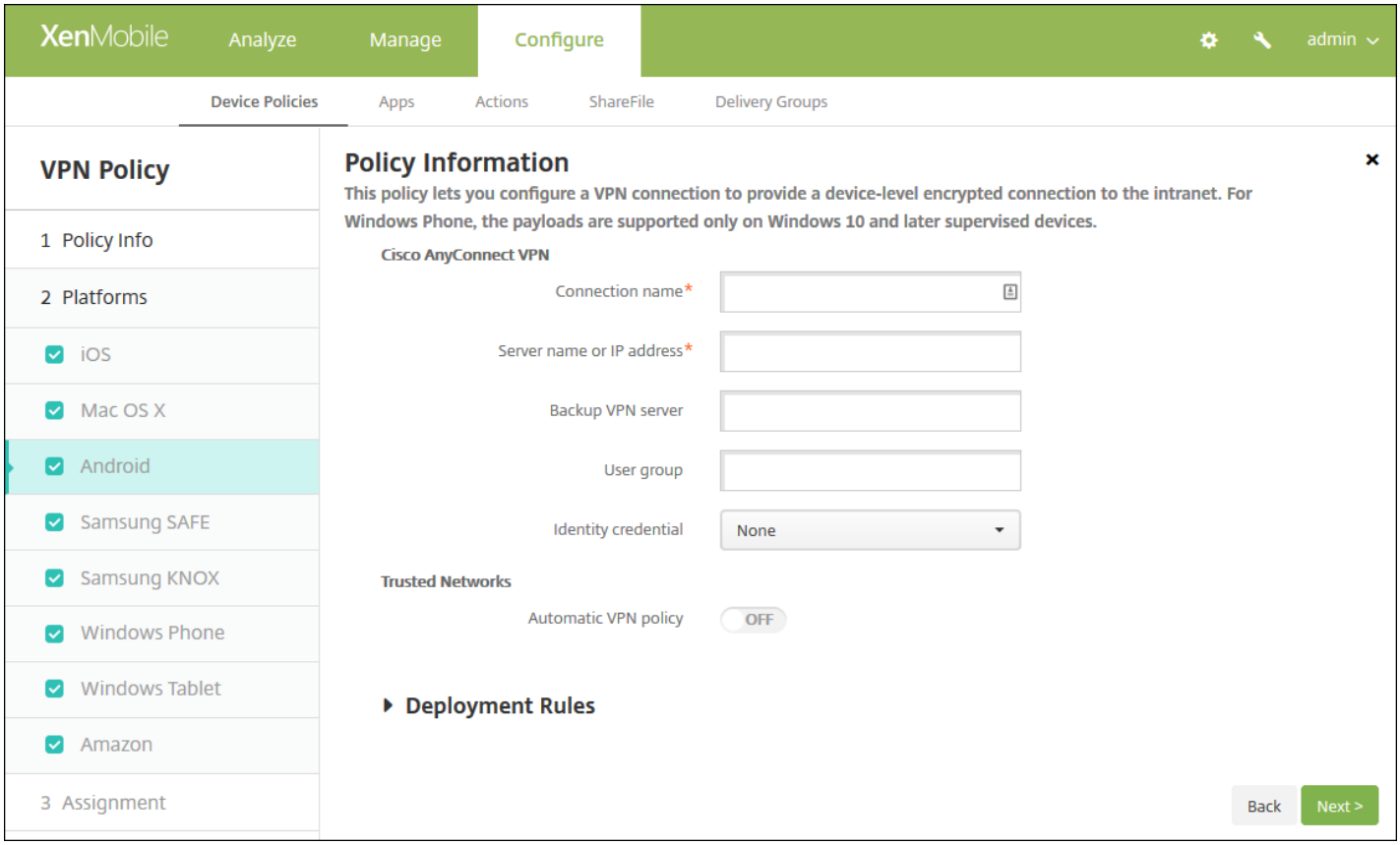
Configuración del protocolo VPN de Citrix

Configuración del protocolo SSL personalizado

Configuración de las opciones de Enable VPN on demand

- **Proxy**
  - **Proxy configuration**. En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **None**.
    - Si habilita **Manual**, configure los siguientes parámetros:
      - **Host name or IP address for the proxy server**. Escriba el nombre o la dirección IP de host del servidor proxy. Este campo es obligatorio.
      - **Port for the proxy server**. Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
      - **User name**. Si quiere, escriba un nombre de usuario para el servidor proxy.
      - **Password**. Si quiere, escriba una contraseña de servidor proxy.
    - Si selecciona **Automatic**, configure este parámetro:
      - **Proxy server URL**. Escriba la URL del servidor proxy. Este campo es obligatorio.
- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

Configuración de los parámetros de Android



Configure estos parámetros:

- **Cisco AnyConnect VPN**
  - **Connection name**. Escriba un nombre para la conexión VPN de Cisco AnyConnect. Este campo es obligatorio.
  - **Server name or IP address**. Escriba el nombre o la dirección IP del servidor VPN. Este campo es obligatorio.
  - **Backup VPN server**. Escriba la información del servidor VPN de respaldo.
  - **User group**. Escriba la información del grupo de usuarios.
  - **Identity credential**. En la lista, seleccione una credencial de identidad.
- **Trusted Networks**
  - **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 habilita esta opción, configure los siguientes parámetros:
    - **Trusted network policy**. En la lista, haga clic en la directiva pertinente. El valor predeterminado es **Disconnect**. Las opciones posibles son:
      - **Disconnect**. El cliente cierra la conexión VPN en la red de confianza. Ésta es la opción predeterminada.
      - **Connect**. El cliente inicia una conexión VPN en la red de confianza.
      - **Do Nothing**. El cliente no lleva a cabo ninguna acción.
      - **Pause**. Suspende la sesión VPN (en lugar de desconectarla) cuando un usuario introduce una red configurada como red de confianza después de establecer una sesión VPN fuera de la red de confianza. Cuando el usuario abandona esa red de confianza, la sesión se reanuda. Esto elimina la necesidad de establecer una nueva sesión VPN después de abandonar una red de confianza.
    - **Untrusted network policy**. En la lista, haga clic en la directiva pertinente. El valor predeterminado es **Connect**. Las

opciones posibles son:

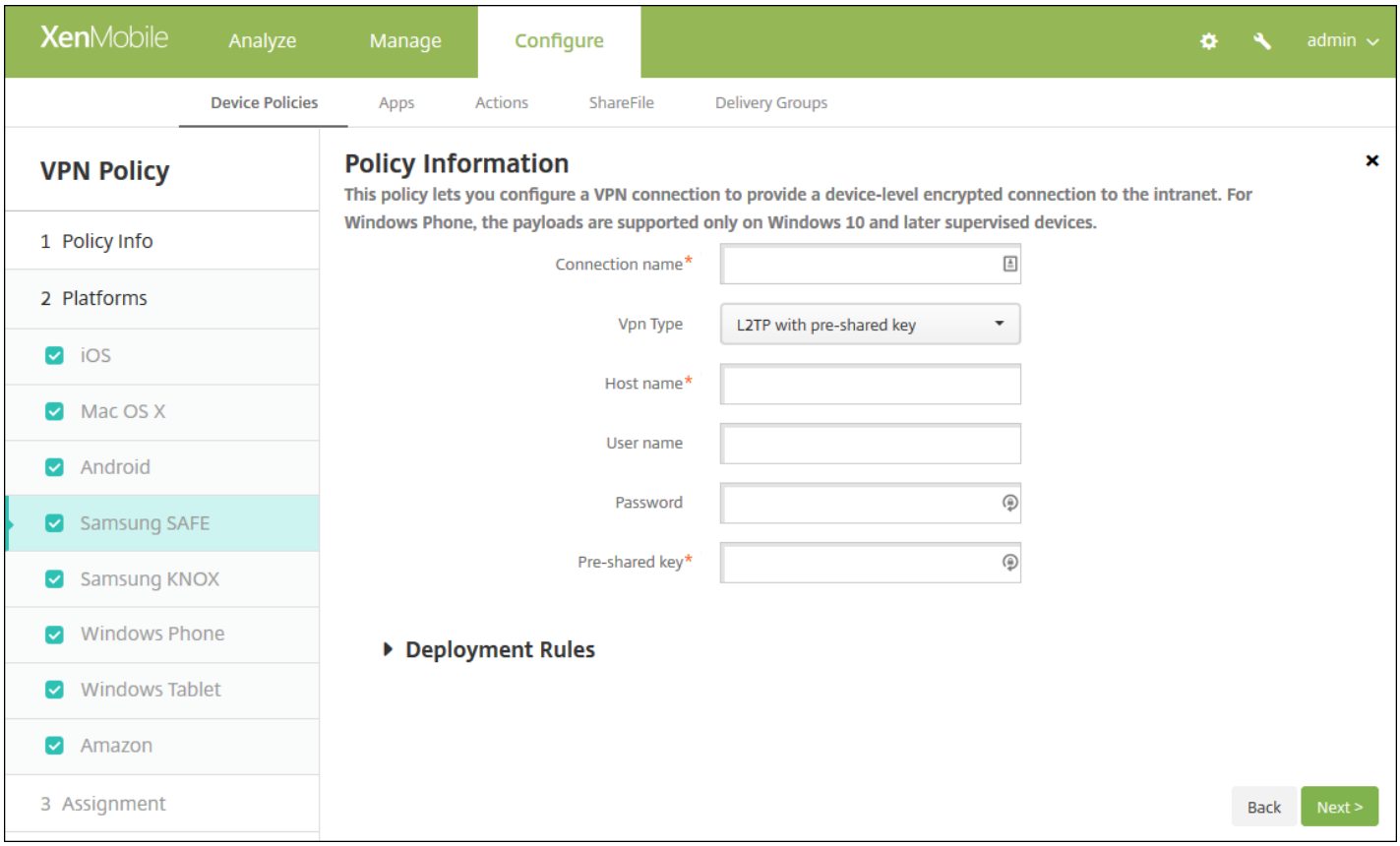
- **Connect**. El cliente inicia una conexión VPN en una red que no es de confianza.
- **Do Nothing**. El cliente inicia una conexión VPN en una red que no es de confianza. Esta opción inhabilita la opción Always-on VPN.

- **Trusted domains**. Para agregar cada sufijo de dominio que puede tener la interfaz de red cuando el cliente se encuentra en la red de confianza, haga clic en **Add** y realice lo siguiente:
  - **Domain**. Escriba el dominio que se va a agregar.
  - Haga clic en **Save** para guardar el dominio, o bien haga clic en **Cancel** para no guardarlo.
- **Trusted servers**. Para agregar cada dirección de servidor que puede tener la interfaz de red cuando el cliente se encuentra en la red de confianza, haga clic en **Add** y realice lo siguiente:
  - **Servers**. Escriba el servidor que se va a agregar.
  - Haga clic en **Save** para guardar el servidor, o bien haga clic en **Cancel** para no guardarlo.

Nota: Para eliminar un servidor existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. 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 servidor existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

Configuración de los parámetros de Samsung SAFE



Configure estos parámetros:

- **Connection name**. Escriba un nombre para la conexión.
- **Vpn type**. En la lista, haga clic en el protocolo que se va a usar para esta conexión. El valor predeterminado es **L2TP with pre-shared key**. Las opciones posibles son:
  - **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. Se aplica a versiones SAFE anteriores a 2.0.
  - **Generic**. Una conexión VPN genérica. Se aplica a SAFE 2.0 o versiones posteriores.

En las siguientes secciones, se ofrece una lista de las opciones de configuración para cada uno de los tipos de VPN mencionados.

Configuración del protocolo L2TP con clave precompartida

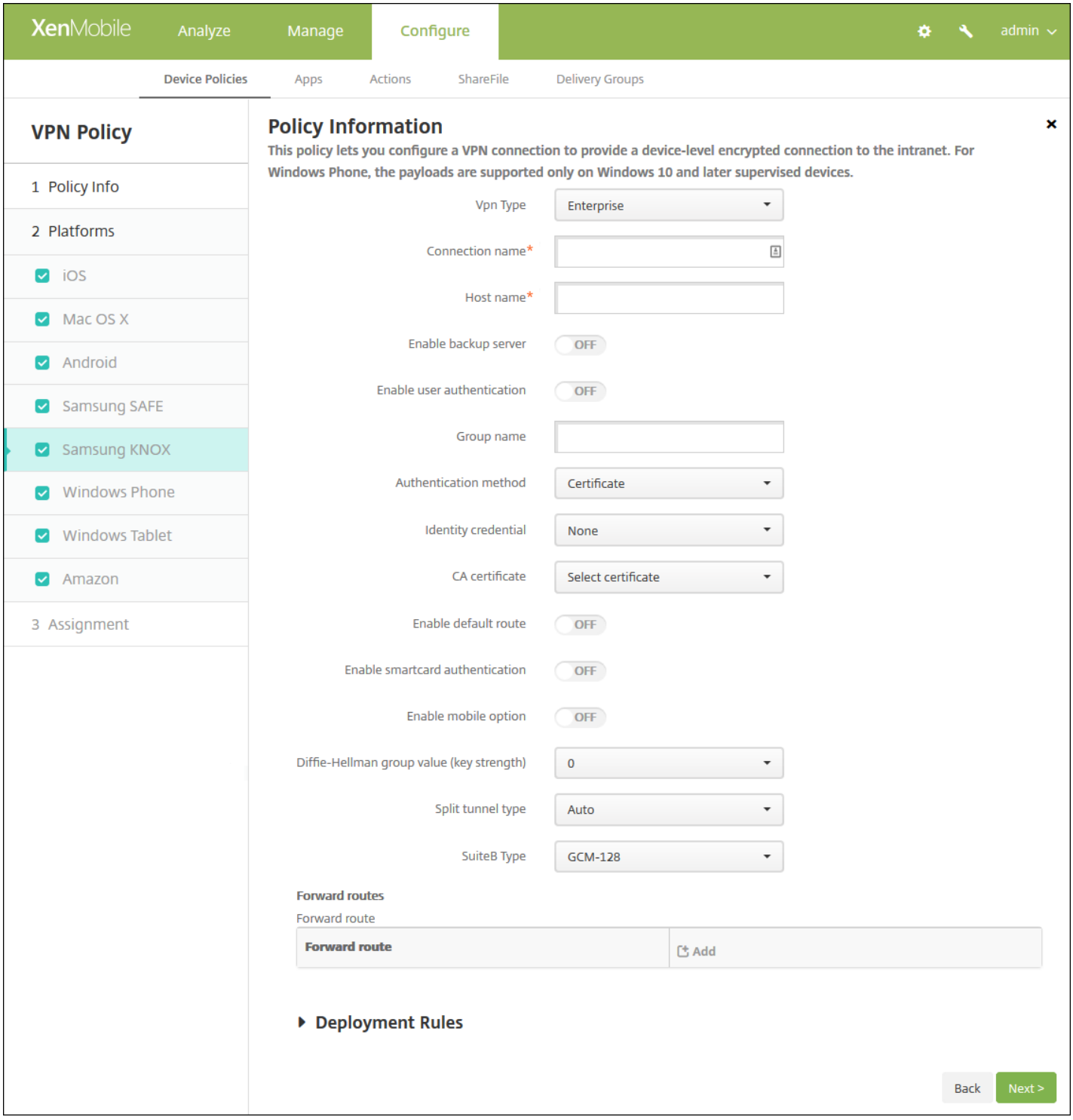
Configuración del protocolo L2TP con certificado

Configuración del protocolo PPTP

Configuración del protocolo de empresa

Configuración del protocolo genérico

Configuración de los parámetros de Samsung KNOX



Nota: Al configurar una directiva para Samsung KNOX, solo se aplicará dentro del contenedor Samsung KNOX.

Configure estos parámetros:

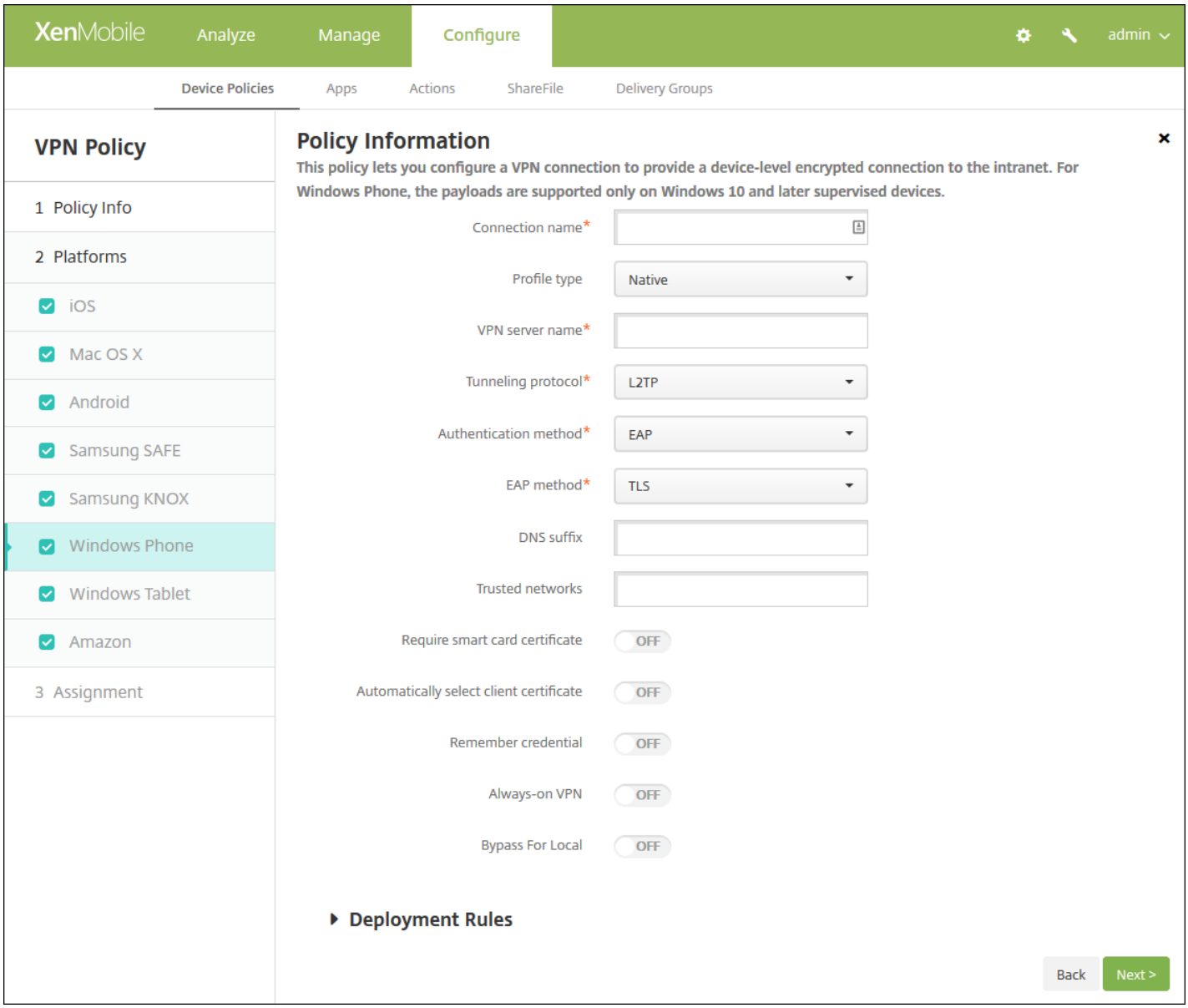
- **Vpn Type**. En la lista, haga clic en el tipo de conexión VPN a configurar, **Enterprise** (se aplica a las versiones KNOX anteriores a 2.0) o **Generic** (se aplica a KNOX 2.0 o versiones posteriores). El valor predeterminado es **Enterprise**.

En las siguientes secciones se enumeran las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configuración del protocolo de empresa

Configuración del protocolo genérico

Configuración de los parámetros de Windows Phone



Nota: Esta configuración solo se admite en teléfonos supervisados con Windows 10 y versiones posteriores.

Configure estos parámetros:

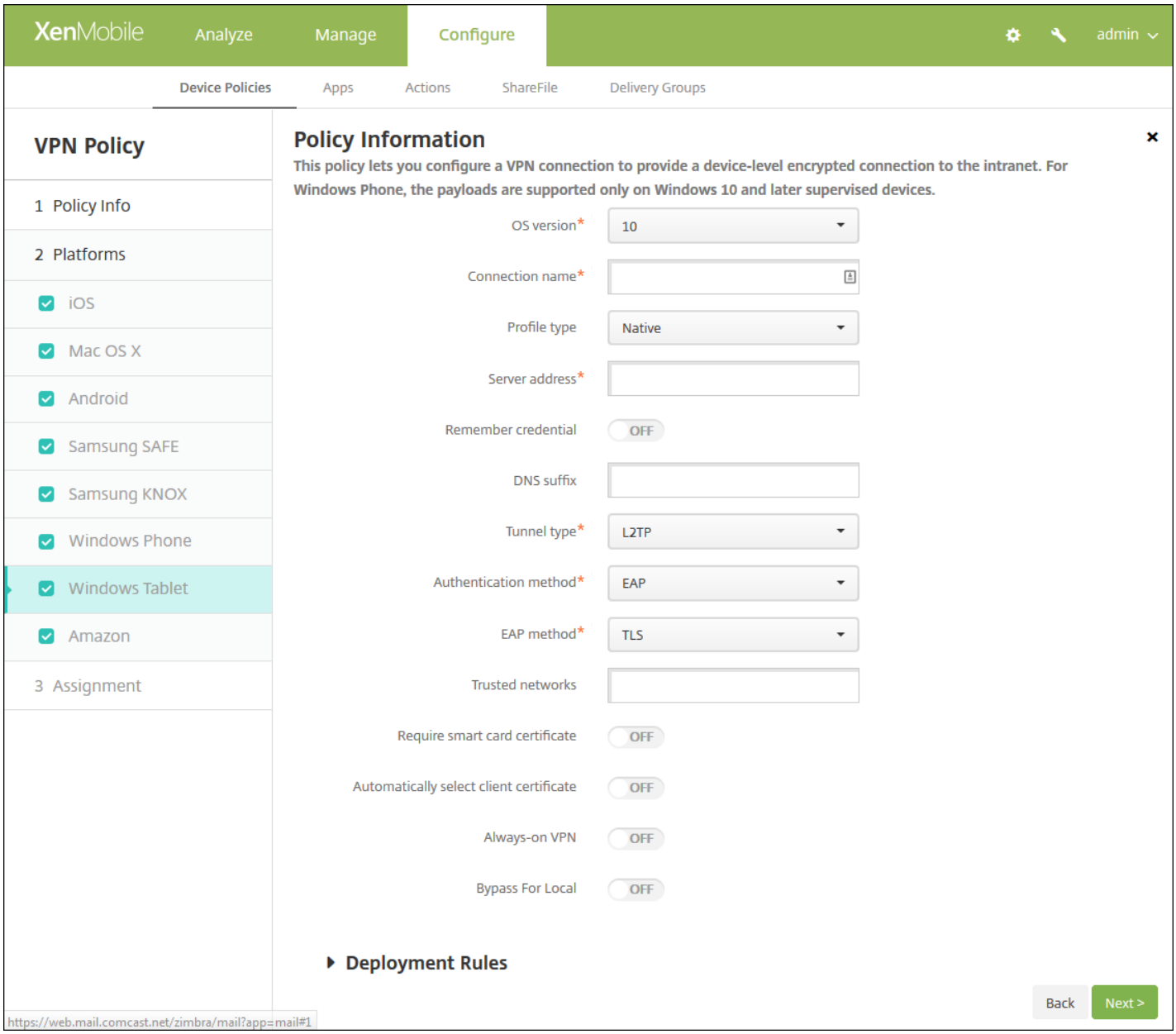
- **Connection name**. Escriba el nombre de la conexión. Este campo es obligatorio.
- **Profile type**. En la lista, haga clic en **Native** o **Plugin**. El valor predeterminado es **Native**. En los siguientes apartados, se describe la configuración de cada una de las opciones.
- **Configure Native profile type settings**. Esta configuración se aplica a la red VPN integrada en los teléfonos Windows de los usuarios.
  - **VPN server name**. Escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor VPN. Este campo es obligatorio.

- **Tunneling protocol**. En la lista, haga clic en el tipo de túnel VPN a usar. El valor predeterminado es **L2TP**. Las opciones posibles son:
  - **L2TP**. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP**. Túnel punto a punto.
  - **IKEv2**. Versión 2 de Intercambio de claves por red.
- **Authentication method**. En la lista, haga clic en el método de autenticación que se va a usar. El valor predeterminado es **EAP**. Las opciones posibles son:
  - **EAP**. Protocolo de autenticación extensible (EAP).
  - **MSCHAPv2**. Usa el protocolo de autenticación por desafío mutuo de Microsoft para la autenticación mutua. Esta opción no está disponible si se selecciona IKEv2 como tipo de túnel. Al elegir MSChapV2, aparece la opción **Automatically use Windows credentials**; el valor predeterminado es **OFF**.
- **EAP method**. En la lista, haga clic en el método EAP que se va a usar. El valor predeterminado es **TLS**. Este campo no está disponible si se habilita la autenticación MSChapV2. Las opciones posibles son:
  - **TLS**. Seguridad de la capa de transporte (Transport Layer Security).
  - **PEAP**. Protocolo de autenticación extensible protegido (Protected Extensible Authentication Protocol).
- **DNS Suffix**. Escriba el sufijo DNS.
- **Trusted networks**. Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.
- **Require smart card certificate**. Seleccione si se debe requerir un certificado de tarjeta inteligente. El valor predeterminado es OFF.
- **Automatically select client certificate**. Seleccione si elegir automáticamente el certificado de cliente para la autenticación. El valor predeterminado es OFF. Esta opción no está disponible si se habilita la opción Require smart card certificate.
- **Remember credential**. Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es OFF. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
- **Always on VPN**: Seleccione si la VPN siempre está activada. El valor predeterminado es OFF. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Bypass For Local**. Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

- **Configure Plugin protocol type**. Estos parámetros se aplican a plug-ins VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
  - **Server address**. Escriba la URL, el nombre de host o la dirección IP del servidor VPN.
  - **Client app ID**. Escriba el nombre de familia del paquete que tenga el plug-in VPN.
  - **Plugin Profile XML**. Seleccione el perfil personalizado de plug-in VPN que se va a usar. Para ello, haga clic en Browse y vaya a la ubicación del archivo. Para obtener información más detallada e indicaciones referentes al formato, póngase en contacto con el proveedor del plug-in.
  - **DNS Suffix**. Escriba el sufijo DNS.
  - **Trusted networks**. Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.
  - **Remember credential**. Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es OFF. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
  - **Always on VPN**: Seleccione si la VPN siempre está activada. El valor predeterminado es OFF. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
  - **Bypass For Local**. Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor

proxy.

Configuración de los parámetros de tabletas Windows



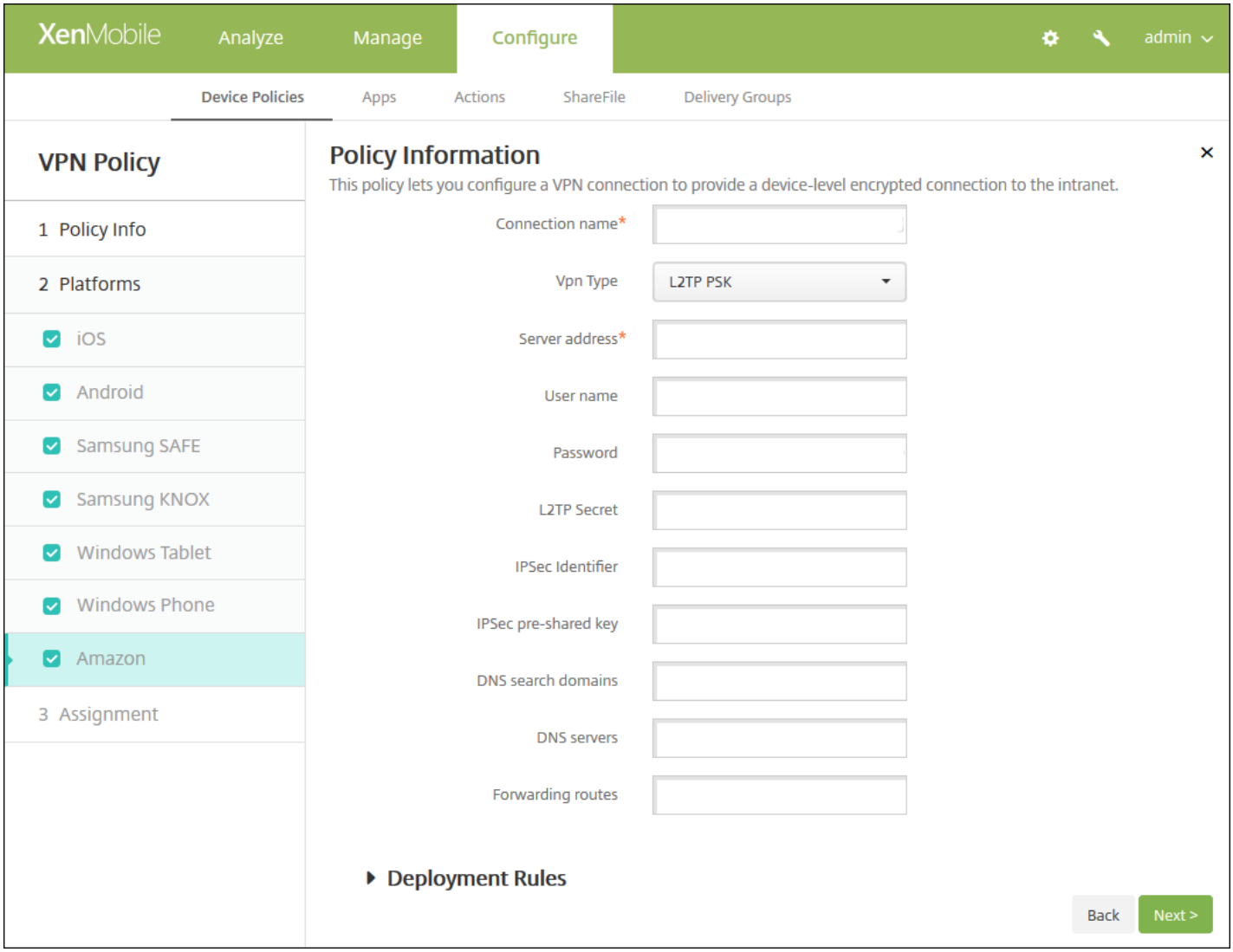
Configure estos parámetros:

- **OS Version**. En la lista, haga clic en **8.1** para Windows 8.1 o en **10** para Windows 10. La opción predeterminada es **10**.

Configuración de los parámetros de Windows 10

Configuración de los parámetros de Windows 8,1

Configuración de los parámetros de Amazon



Configure estos parámetros:

- **Connection name**. Escriba el nombre de la conexión.
- **Vpn type**. Haga clic en el tipo de conexión. Las opciones posibles son:
  - **L2TP PSK**. Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida. Ésta es la opción predeterminada.
  - **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 HYBRID RSA**. Protocolo de seguridad de Internet con autenticación RSA híbrida.
  - **PPTP**. Túnel punto a punto.

En las siguientes secciones se enumeran las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configuración de los parámetros de PSK para protocolos L2TP

Configuración de los parámetros de RSA para protocolos L2TP

Configuración de los parámetros de PSK para XAUTH de IPsec

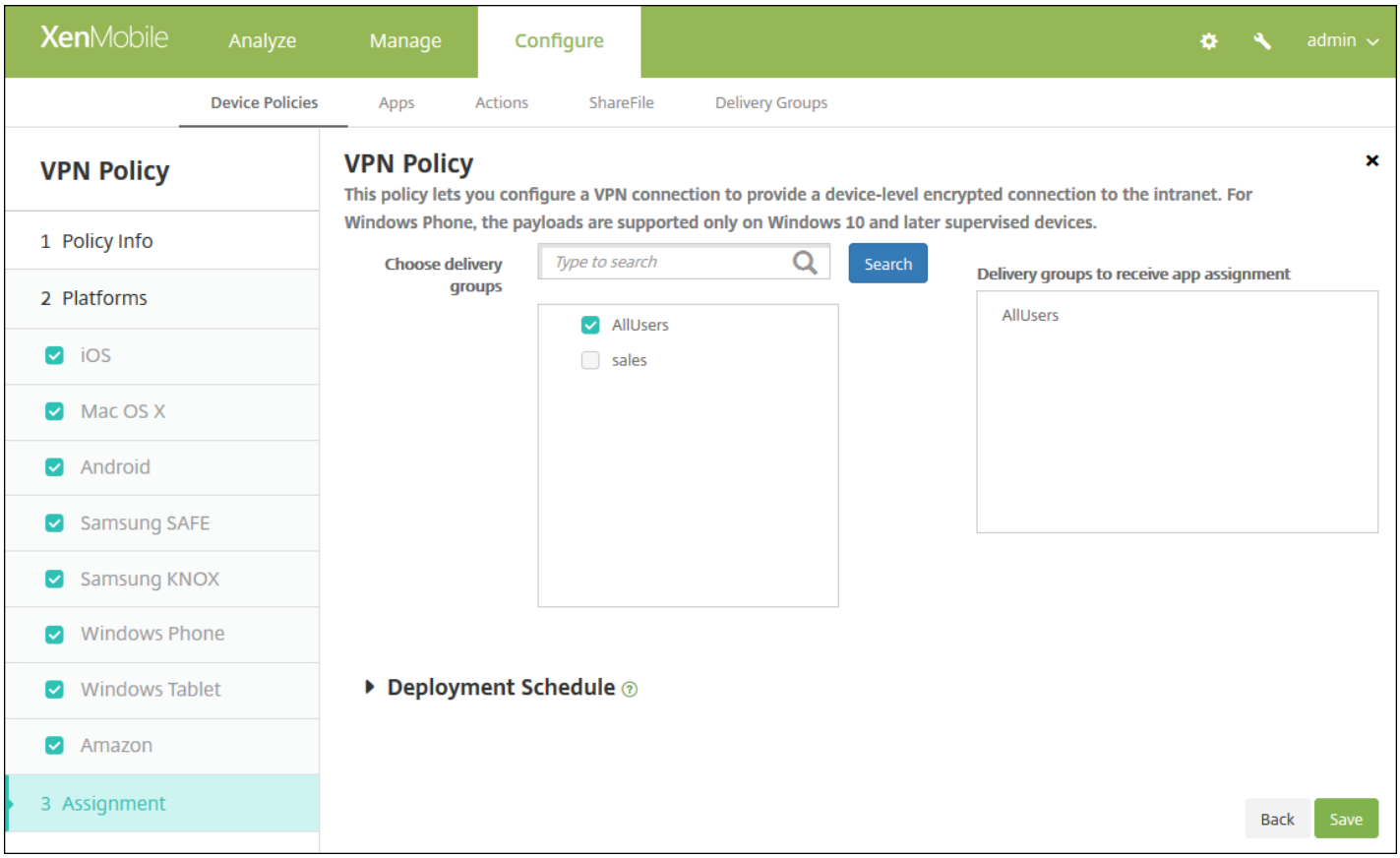
Configuración de los parámetros de RSA para AUTH de IPsec

Configuración de los parámetros de RSA para HYBRID de IPsec

Configuración de los parámetros de PPTP

7. Configure las reglas de implementación.

8. Haga clic en **Next**, aparecerá la página de asignación **VPN 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 los 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**. 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:

- 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.
- 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**.

Directiva de fondos de escritorio

Jul 27, 2016

Puede agregar un archivo JPG o PNG para establecer un fondo de escritorio en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Disponible en iOS 7.1.2 y versiones posteriores. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de pantalla y aplicarlas a los usuarios correspondientes.

En la siguiente tabla, se ofrece una lista de las dimensiones de imagen que recomienda Apple para dispositivos iOS.

Dispositivo		**Dimensiones de imagen en píxeles**
iPhone	**iPad**	
4, 4s		640 x 960
5, 5c, 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

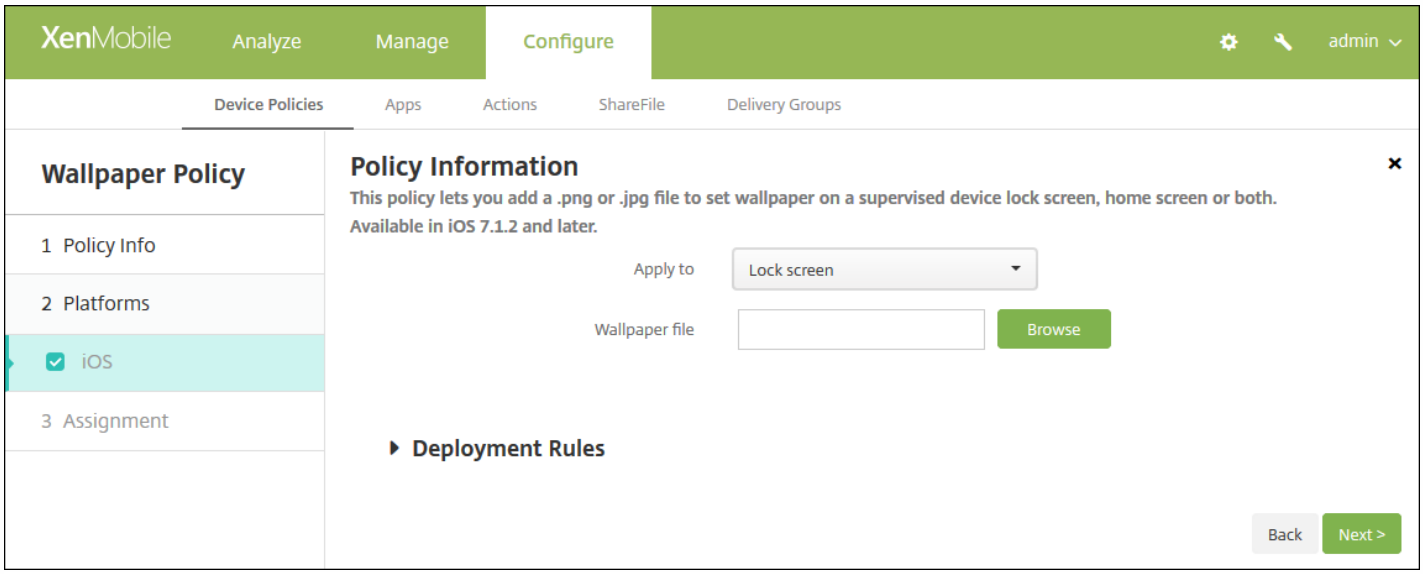
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **More** y, en **End user**, haga clic en **Wallpaper**. Aparecerá la página **Wallpaper Policy**.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

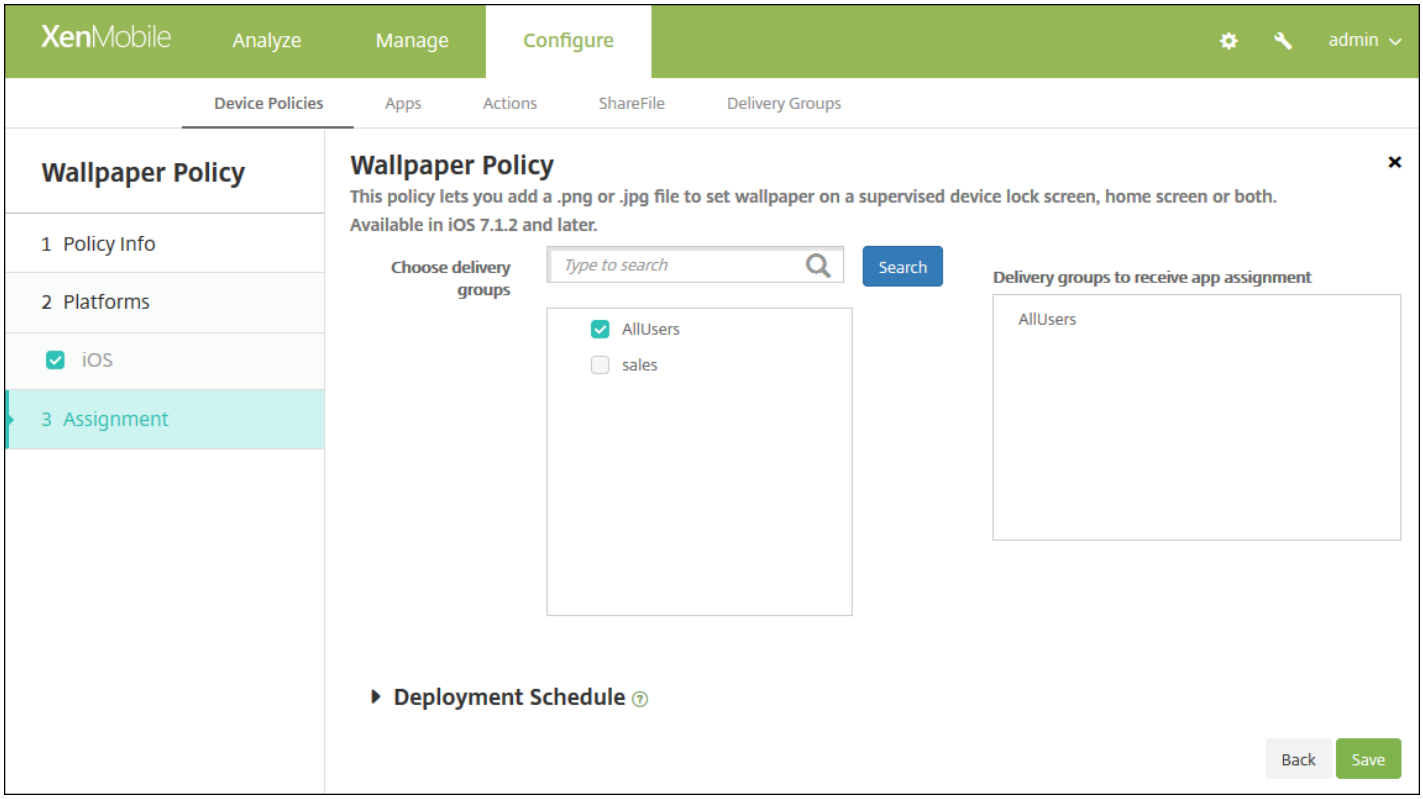


Configure estos parámetros:

- **Apply to**. En la lista, seleccione **Lock screen**, **Home (icon list) screen** o **Lock and home screens** para definir dónde aparecerá el fondo de pantalla.
- **Wallpaper file**. Seleccione el archivo del fondo de pantalla. Para ello, deberá hacer clic en **Browse** y, a continuación, ir a la ubicación del archivo.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Wallpaper 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de contenidos Web

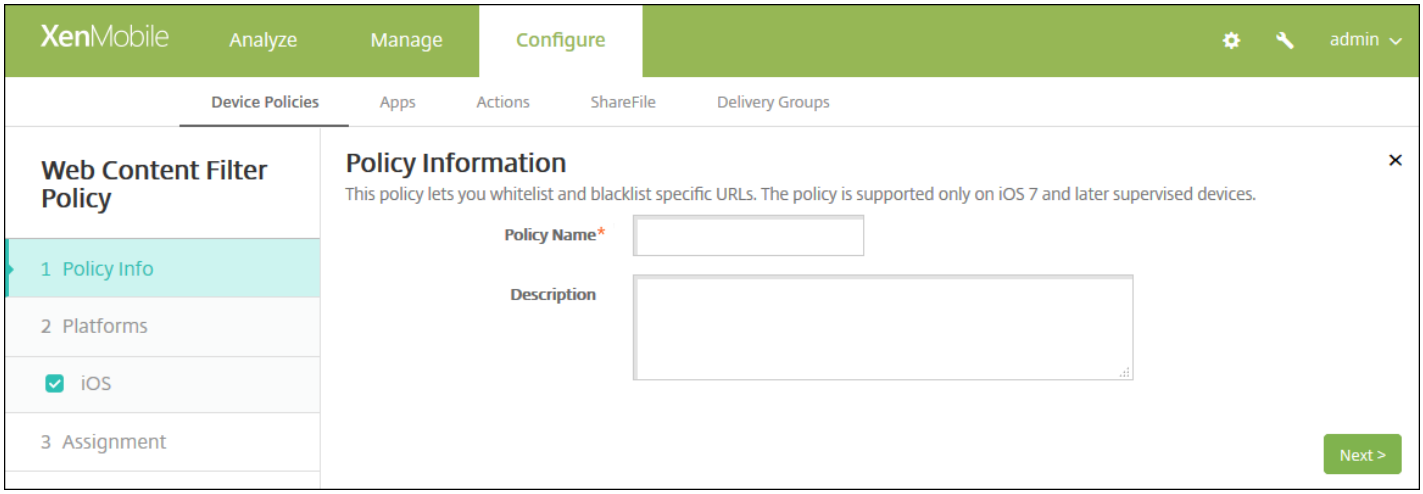
Jul 27, 2016

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**. Aparecerá el cuadro de diálogo **Add a New Policy**.

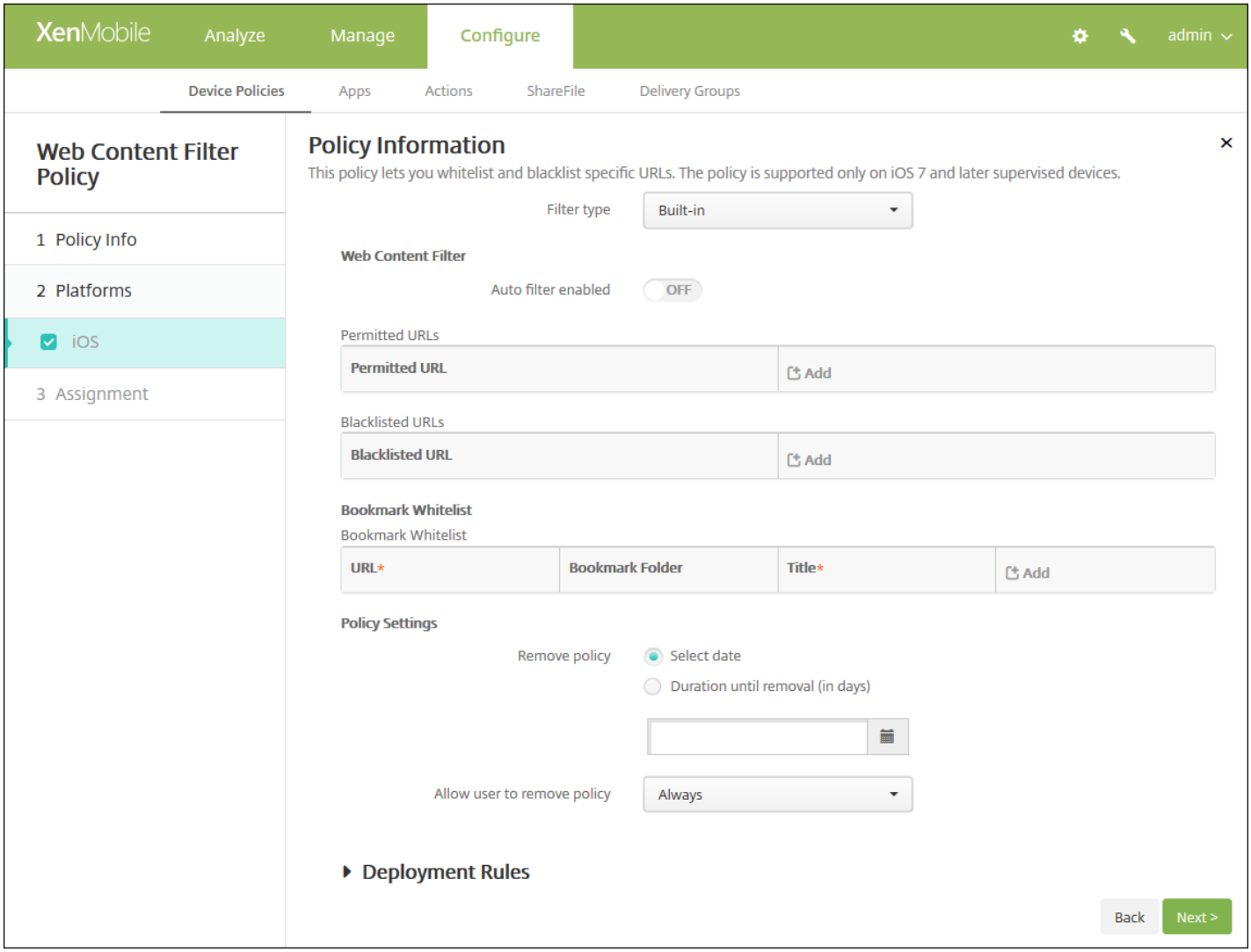
3. Haga clic en **More** y, a continuación, en **Security**, haga clic en **Web Content Filter**. Aparecerá la página **Web Content Filter Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información referente a la plataforma **iOS**.



6. Configure los siguientes parámetros:

- **Filter type**. En la lista, haga clic en **Built-in** o **Plug-in** y, a continuación, siga los procedimientos de la opción que elija. El valor predeterminado es **Built-in**.

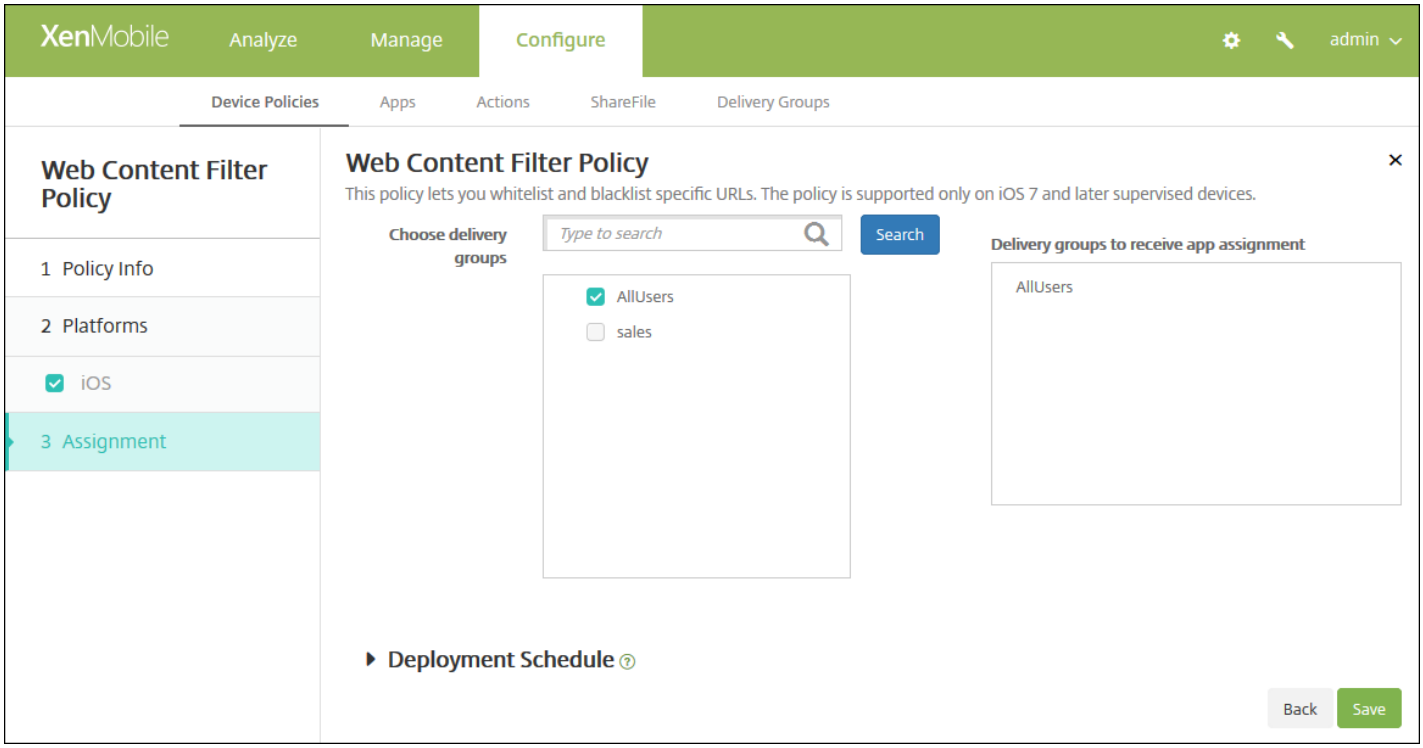
Configuración del tipo de filtro integrado

Configuración del tipo de filtro plug-in

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Web Content Filter 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- **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.
- 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 clips Web

Jul 27, 2016

Puede colocar accesos directos, o clips Web, en los sitios Web para que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips Web en dispositivos iOS, Mac OS X y Android; las tabletas Windows solo requieren una etiqueta y una URL.

Configuración de iOS

Configuración de Mac OS X

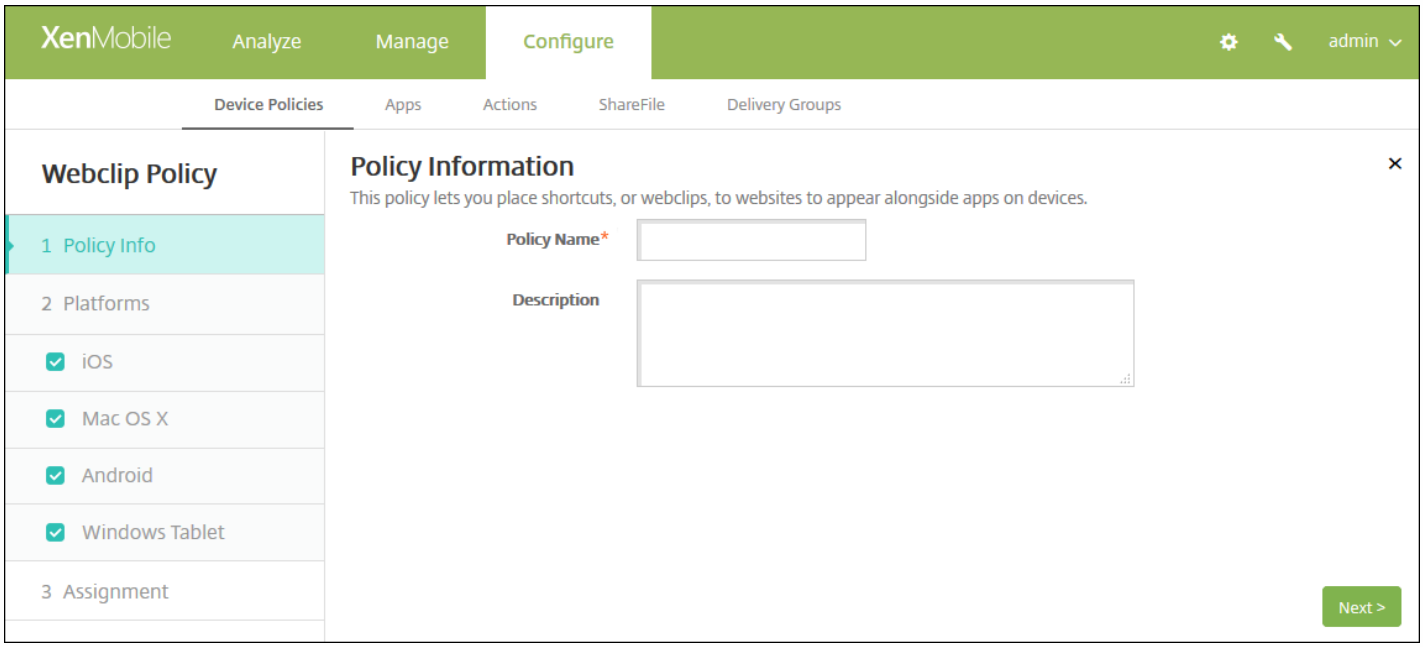
Configuración de Android

Configuración de tabletas Windows

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

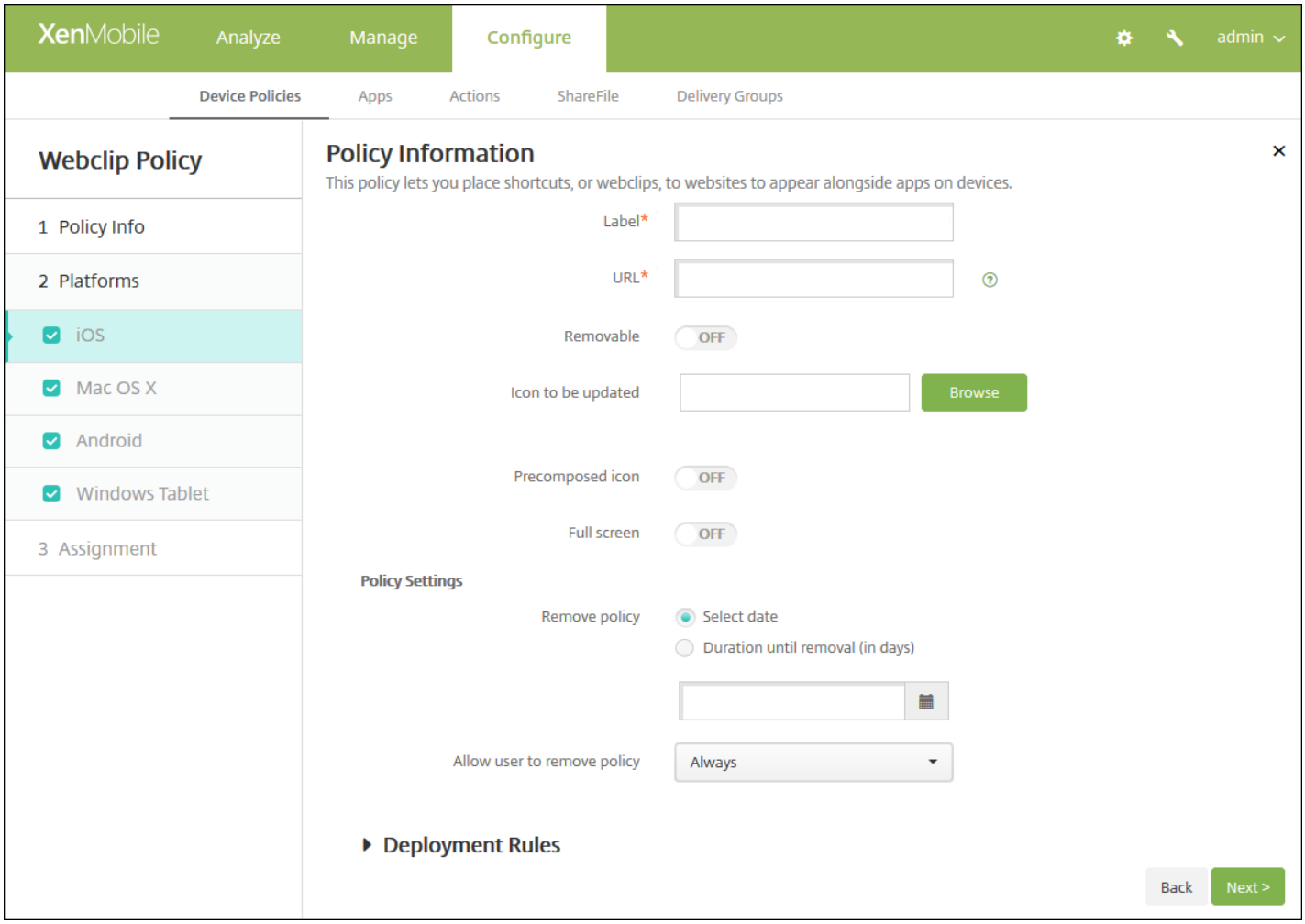
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **clip Web**. Aparece la página **Webclip Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

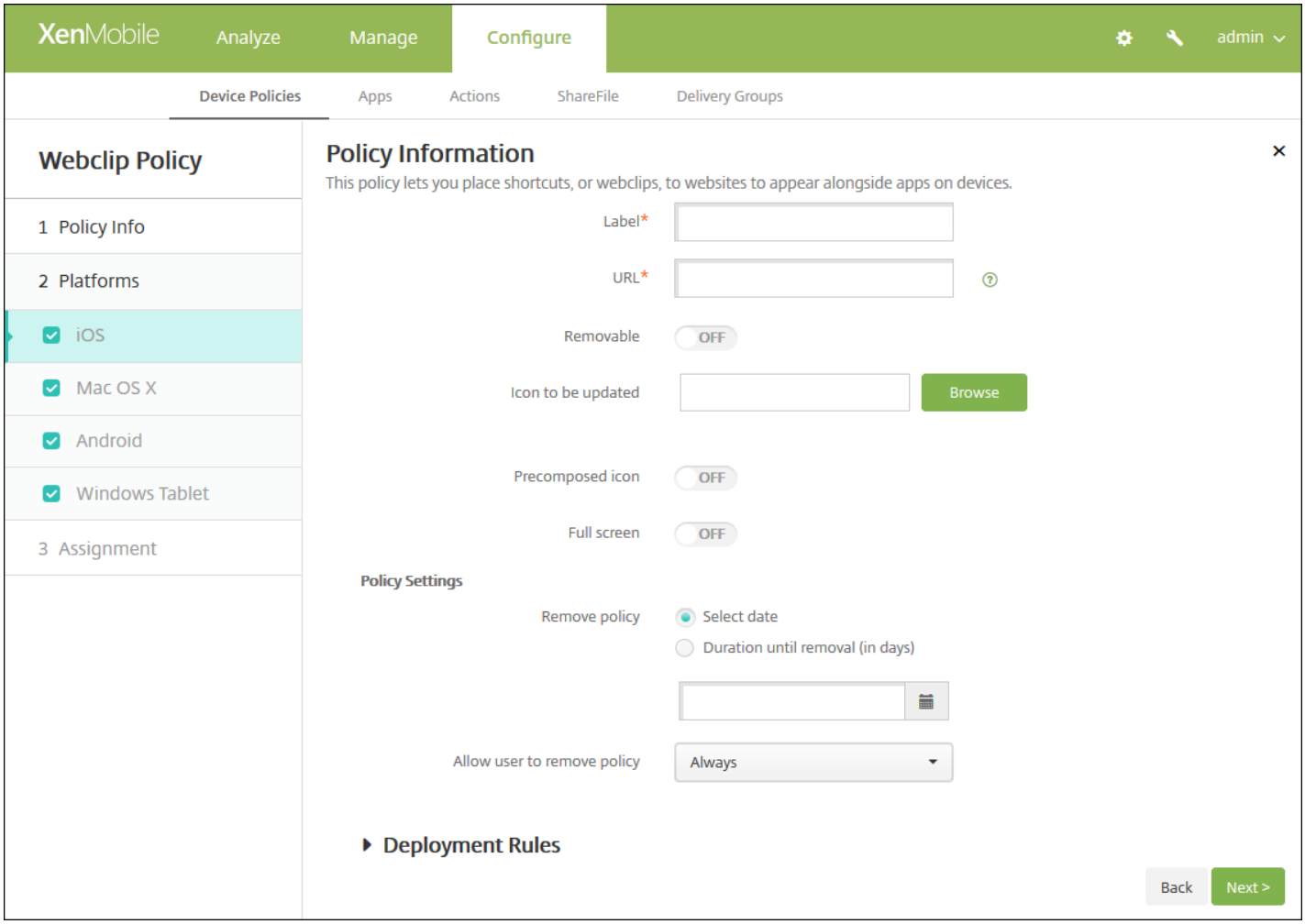
5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

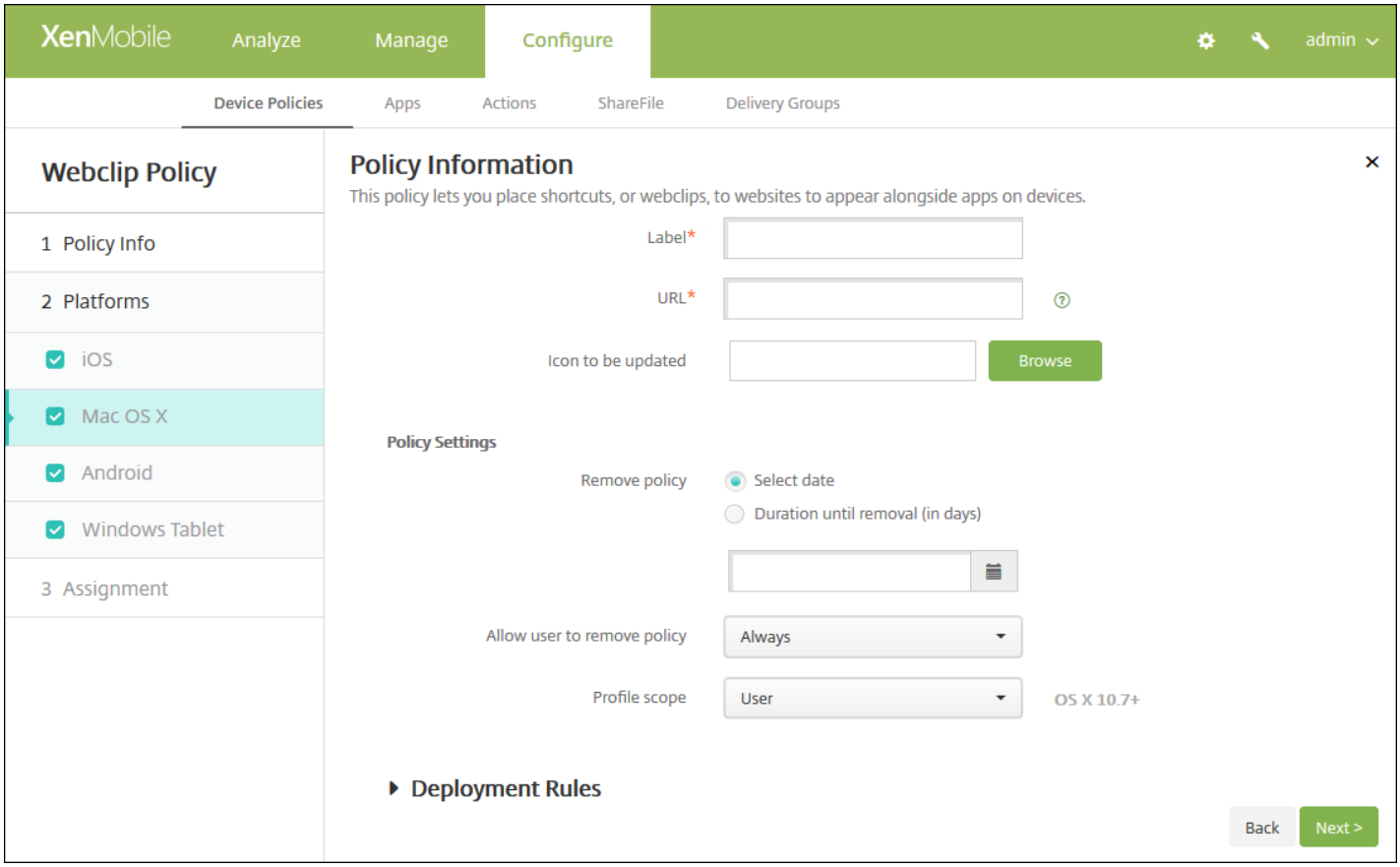
Configuración de los parámetros de iOS



Configure estos parámetros:

- **Label**. Escriba la etiqueta que aparecerá con el clip Web.
- **URL**. Escriba la URL asociada al clip Web. La URL debe comenzar por un protocolo; por ejemplo, http://servidor.
- **Removable**. Seleccione si los usuarios pueden quitar el clip Web. El valor predeterminado es **OFF**.
- **Icon to be updated**. Seleccione el icono para usar con el clip Web haciendo clic en **Browse** para encontrar la ubicación del archivo.
- **Precomposed icon**. Seleccione si habrá efectos que se aplicarán al icono, como esquinas redondeadas, sombra paralela y brillo de reflejos, entre otros. El valor predeterminado es **OFF**, con lo que se agregan efectos.
- **Full screen**. Seleccione si la página Web enlazada se abre en modo de pantalla completa. El valor predeterminado es **OFF**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

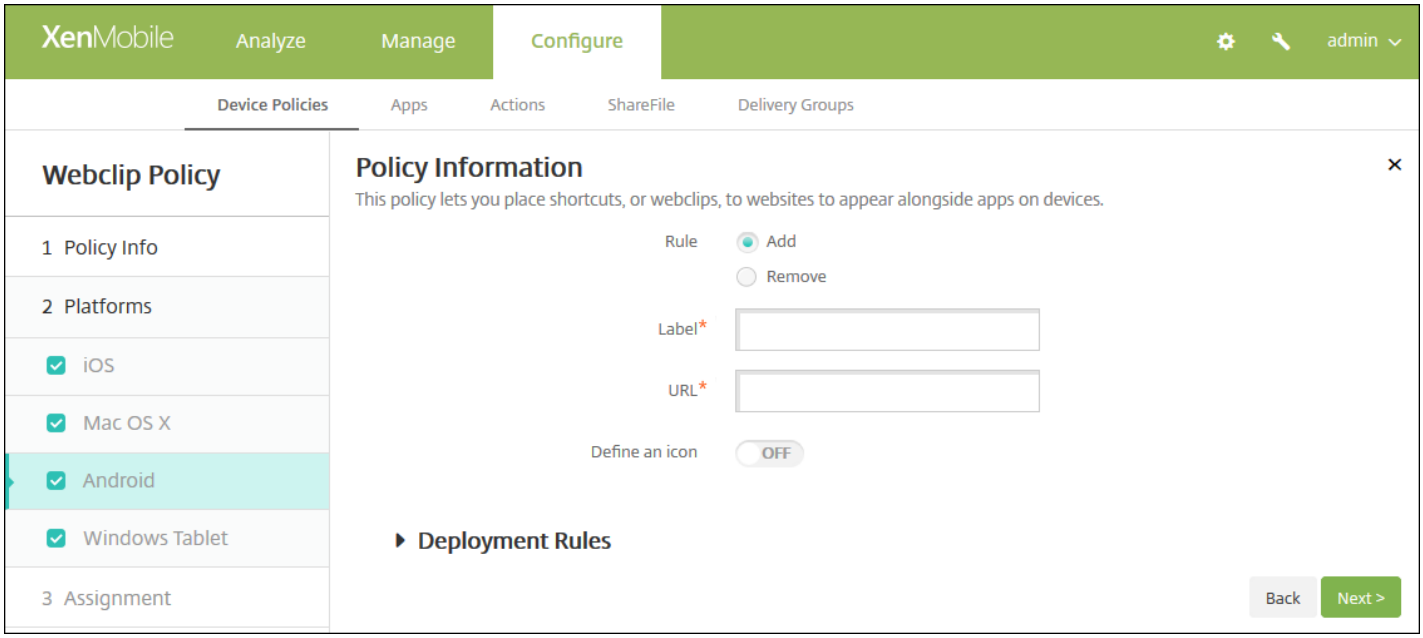
Configuración de los parámetros de Mac OS X



Configure estos parámetros:

- **Label**. Escriba la etiqueta que aparecerá con el clip Web.
- **URL**. Escriba la URL asociada al clip Web. La URL debe comenzar por un protocolo; por ejemplo, http://servidor.
- **Icon to be updated**. Seleccione el icono para usar con el clip Web haciendo clic en Browse para encontrar la ubicación del archivo.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - En la lista **Profile Scope**, haga clic en **User** o **System**. Esta opción está disponible para OS X 10.7 y versiones posteriores.

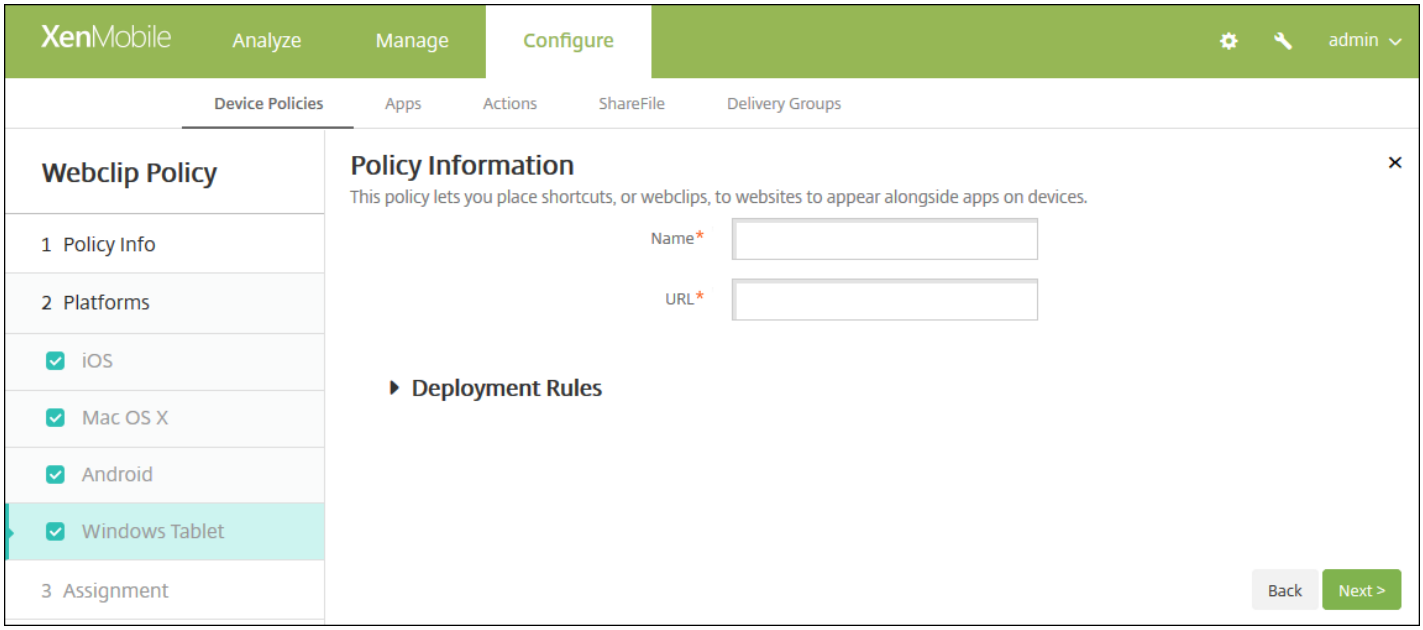
Configuración de los parámetros de Android



Configure estos parámetros:

- **Rule**. Seleccione si esta directiva agrega o quita un clip Web. El valor predeterminado es Add.
- **Label**. Escriba la etiqueta que aparecerá con el clip Web.
- **URL**. Escriba la URL asociada al clip Web.
- **Define an icon**. Seleccione si quiere usar un archivo de icono. El valor predeterminado es **OFF**.
- **Icon file**. Si la opción **Define an icon** está establecida en **ON**, deberá seleccionar el archivo de icono que se va a usar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

Configuración de los parámetros de tabletas Windows

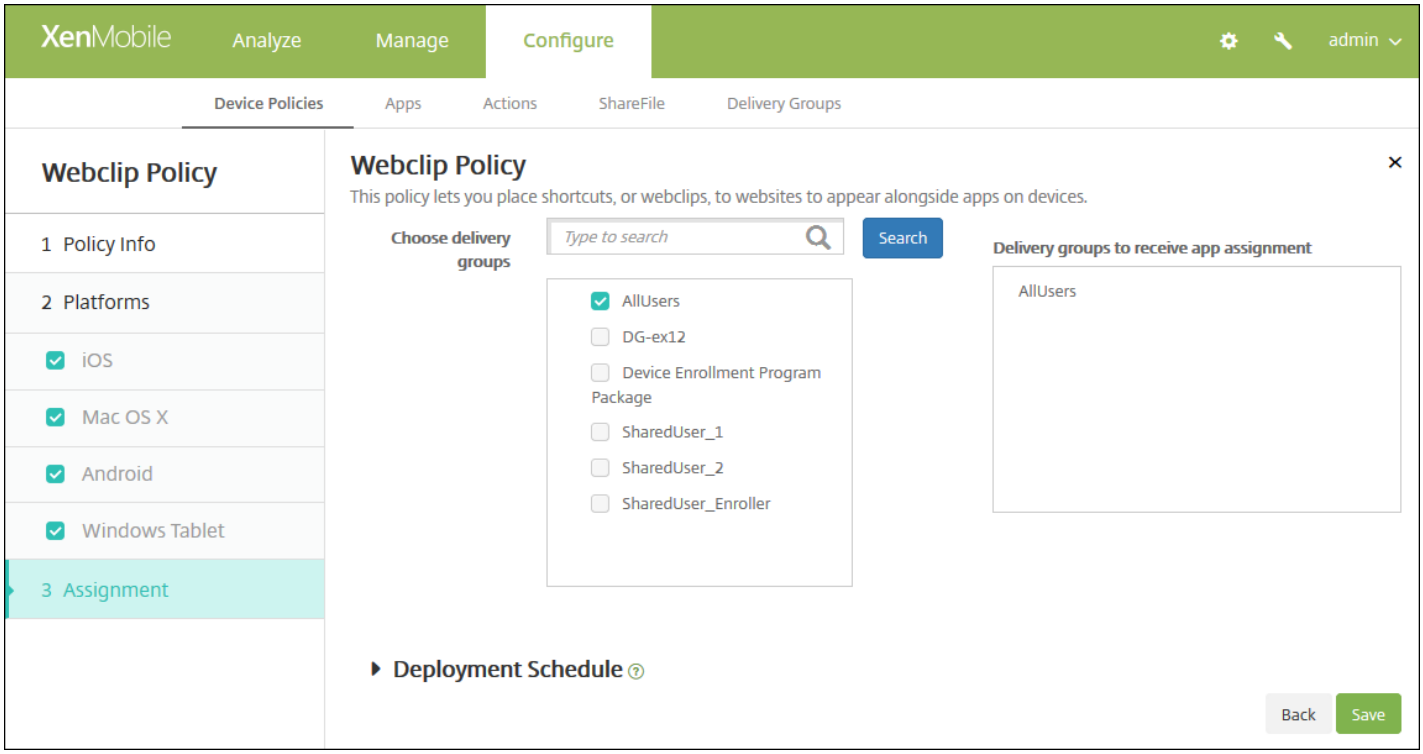


Configure estos parámetros:

- **Nombre**. Escriba la etiqueta que aparecerá con el clip Web.
- **URL**. Escriba la URL asociada al clip Web.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Webclip 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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 a

iOS.

11. Haga clic en **Save** para guardar la directiva.

Directivas WiFi de dispositivos

Jul 27, 2016

En XenMobile, puede crear o modificar las directivas de WiFi 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 las opciones de WiFi para los usuarios de las plataformas siguientes: iOS, Mac OS X, Android (incluidos los dispositivos habilitados para Android for Work), Windows Phone y tabletas Windows. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Configuración de iOS

Configuración de Mac OS X

Configuración de Android

Configuración de Windows Phone

Configuración de tabletas Windows

Important

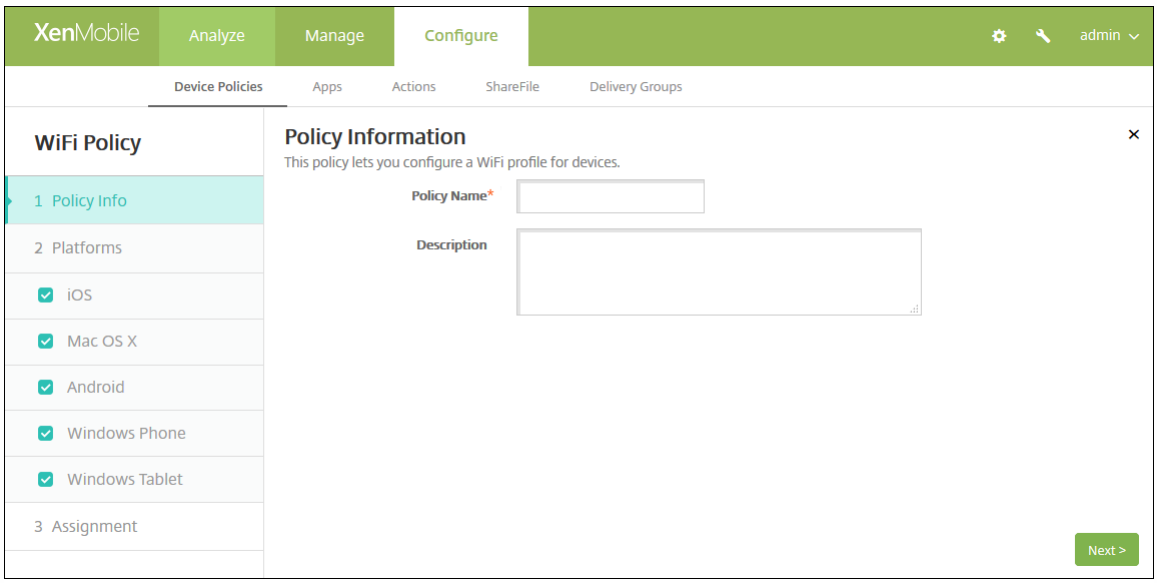
Antes de crear una directiva nueva, lleve a cabo estos pasos:

- 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.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Haga clic en **WiFi**. Aparecerá la página **WiFi Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

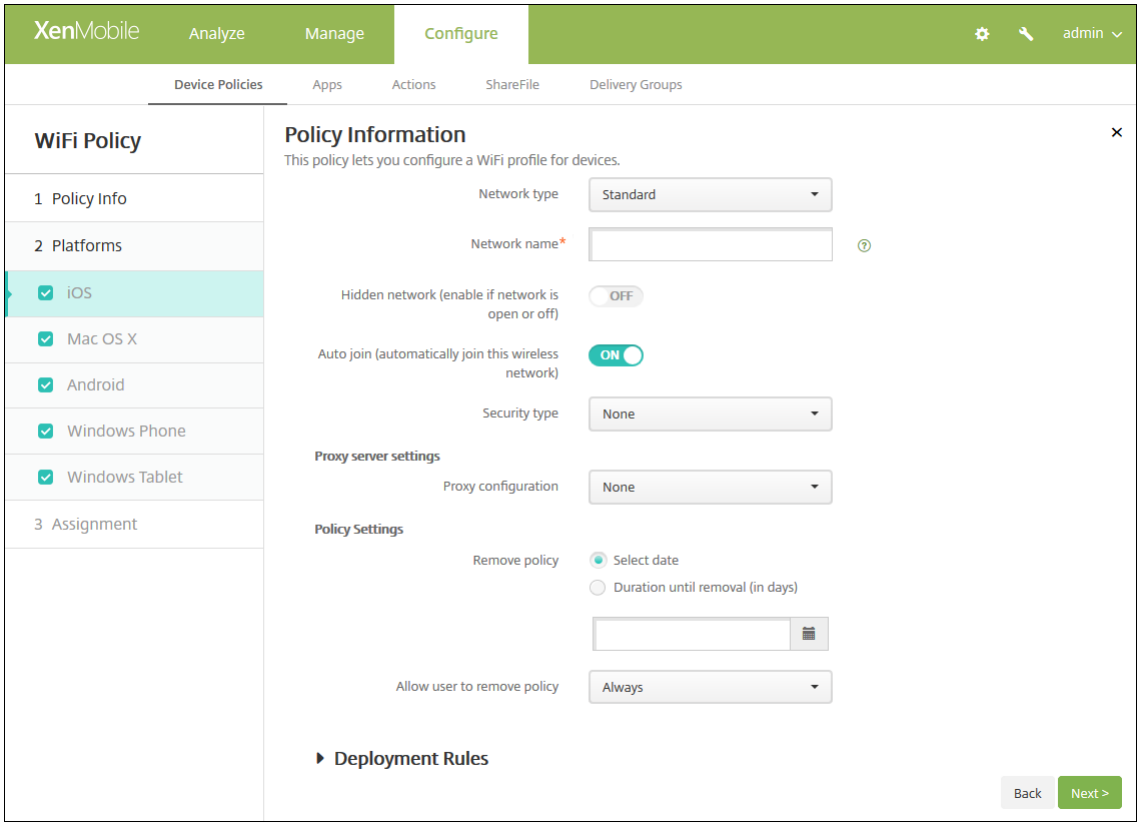
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure estos parámetros:

- **Network type**. En la lista, haga clic en **Standard**, **Legacy Hotspot** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Network Name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Hidden network (enable if network is open or off)**. Seleccione si la red está oculta o no.
- **Auto Join (automatically join this wireless network)**. Seleccione si se conecta a la red automáticamente o no. El valor predeterminado es **ON**.
- **Security type**. En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - None. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Cualquiera (Enterprise)

  En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

WPA, WPA Personal, Any (personal)

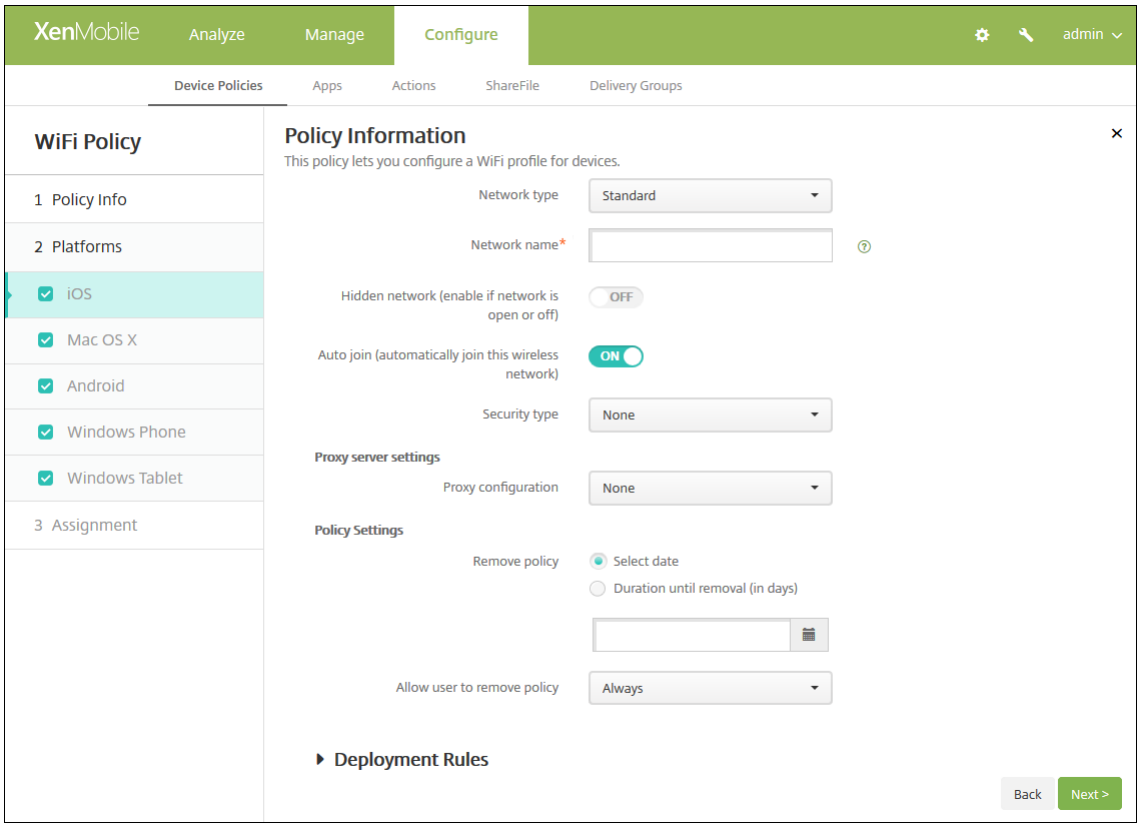
WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

- **Parámetros del servidor proxy**
  - **Proxy configuration**. En la lista, haga clic en None, Manual o Automatic para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es None, que no requiere ninguna configuración adicional.
  - Si hace clic en **Manual**, configure los siguientes parámetros:
    - **Hostname/IP address**. Escriba el nombre o la dirección IP de host del servidor proxy.
    - **Port**. Escriba el número de puerto del servidor proxy.
    - **User name**. Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
    - **Password**. Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
  - Si hace clic en **Automatic**, configure los siguientes parámetros:
    - **Server URL**. Escriba la dirección URL del archivo PAC que define la configuración de proxy.
    - **Allow direct connection if PAC is unreachable**. Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **ON**. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.
- **Hotspot 2.0**
  - **Displayed operator name**. Escriba el nombre de operador que se va a mostrar. Se aplica para iOS 7.0 y versiones posteriores.
  - **Domain name**. Escriba el nombre de dominio usado para la negociación de WiFi Hotspot 2.0. Se aplica para iOS 7.0 y versiones posteriores.
  - **Allow connecting to roaming partner networks**. Seleccione si permitir a los dispositivos conectarse a redes asociadas de roaming. Se aplica para iOS 7.0 y versiones posteriores.
  - **Roaming Consortium Organization Identifiers (OI)**. Si quiere, agregue los identificadores Roaming Consortium Organization Identifiers que se usan para la negociación de WiFi Hotspot 2.0.
  - **Network Access Identifier (NAI) realm names**. Si quiere, agregue los nombres de dominio kerberos NAI que se usan para la negociación de WiFi Hotspot 2.0.
  - **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs)**. Si quiere, agregue los pares de códigos MCC y configuraciones MNC que se usan para la negociación de WiFi Hotspot 2.0. Cada cadena debe contener exactamente seis dígitos.

Consulte las secciones anteriores para obtener información acerca de **protocolos, tipos de EAP aceptados**; **protocolos EAP-FAST** y **autenticación**.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure estos parámetros:

- **Network type**. En la lista, haga clic en **Standard**, **Legacy Hotspot** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Network Name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Hidden network (enable if network is open or off)**. Seleccione si la red está oculta o no.
- **Auto Join (automatically join this wireless network)**. Seleccione si se conecta a la red automáticamente o no. El valor predeterminado es **ON**.
- **Security type**. En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - None. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Cualquiera (Enterprise)

  En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

WPA, WPA Personal, WPA 2 Personal, Any (Personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

- **Use as a Login Window configuration**. Seleccione si utilizar las mismas credenciales especificadas en la ventana de inicio de sesión para autenticar al usuario.
- **Parámetros del servidor proxy**
  - **Proxy configuration**. En la lista, haga clic en None, Manual o Automatic para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es None, que no requiere ninguna configuración adicional.
  - Si hace clic en **Manual**, configure los siguientes parámetros:
    - **Hostname/IP address**. Escriba el nombre o la dirección IP de host del servidor proxy.
    - **Port**. Escriba el número de puerto del servidor proxy.
    - **User name**. Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
    - **Password**. Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
  - Si hace clic en **Automatic**, configure los siguientes parámetros:
    - **Server URL**. Escriba la dirección URL del archivo PAC que define la configuración de proxy.

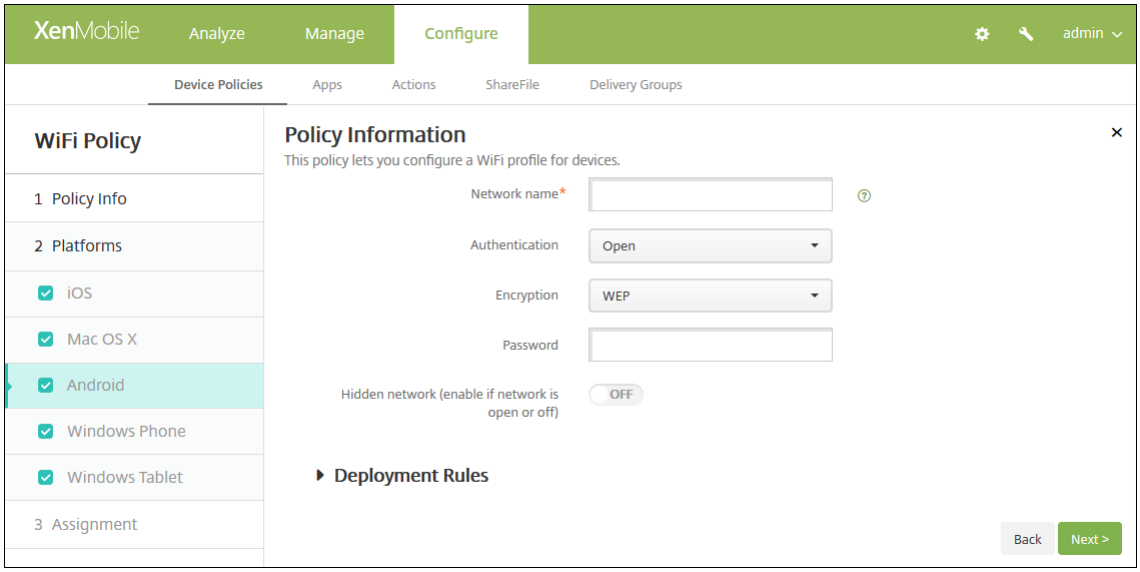
- **Allow direct connection if PAC is unreachable**. Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **ON**. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.

- **Hotspot 2.0**
  - **Displayed operator name**. Escriba el nombre de operador que se va a mostrar. Se aplica para iOS 7.0 y versiones posteriores.
  - **Domain name**. Escriba el nombre de dominio usado para la negociación de WiFi Hotspot 2.0. Se aplica para iOS 7.0 y versiones posteriores.
  - **Allow connecting to roaming partner networks**. Seleccione si permitir a los dispositivos conectarse a redes asociadas de roaming. Se aplica para iOS 7.0 y versiones posteriores.
  - **Roaming Consortium Organization Identifiers (OI)**. Si quiere, agregue los identificadores Roaming Consortium Organization Identifiers que se usan para la negociación de WiFi Hotspot 2.0.
  - **Network Access Identifier (NAI) realm names**. Si quiere, agregue los nombres de dominio kerberos NAI que se usan para la negociación de WiFi Hotspot 2.0.
  - **Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs)**. Si quiere, agregue los pares de códigos MCC y configuraciones MNC que se usan para la negociación de WiFi Hotspot 2.0. Cada cadena debe contener exactamente seis dígitos.

    Consulte las secciones anteriores para obtener información acerca de **protocolos, tipos de EAP aceptados**; **protocolos EAP-FAST** y **autenticación**.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción está disponible para OS X 10.7 y versiones posteriores.

Configuración de los parámetros de Android



Configure estos parámetros:

- **Network name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **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 las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

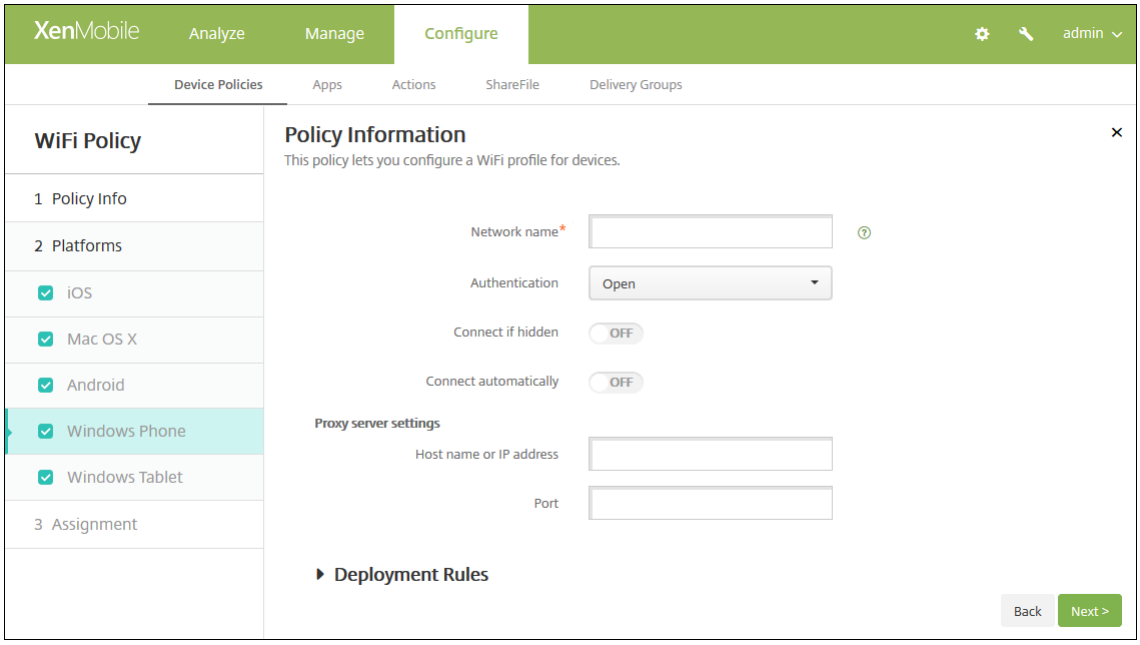
Open, Shared

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

- **Hidden network (Enable if network is open or off)**. Seleccione si la red está oculta o no.

Configuración de los parámetros de Windows Phone



Configure estos parámetros:

- **Network name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **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 las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

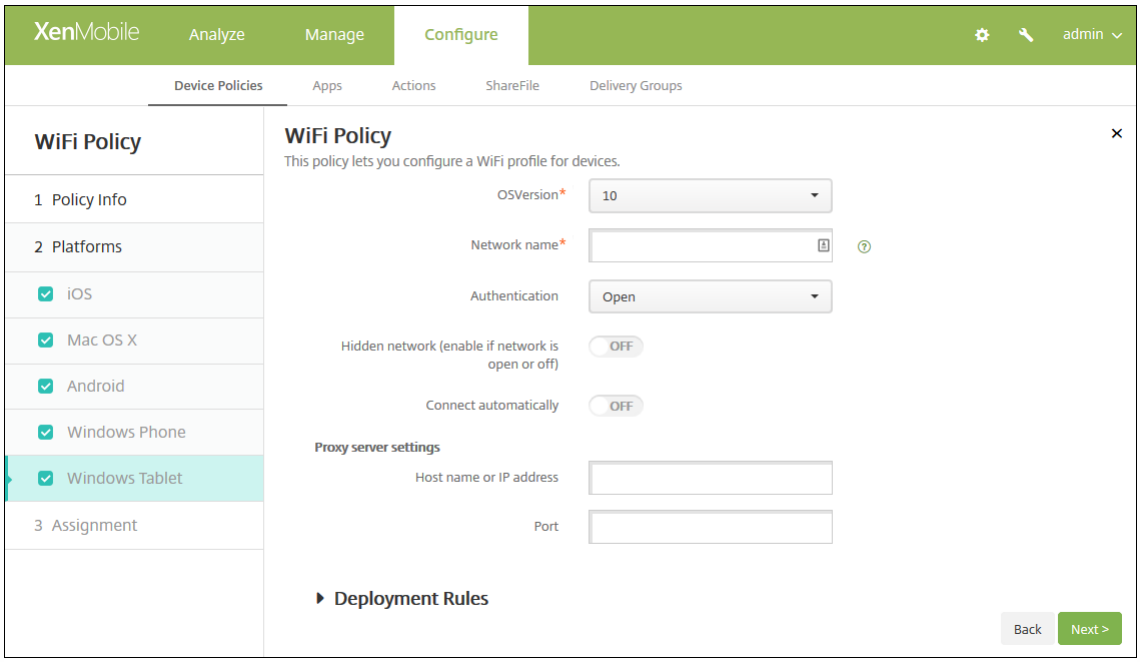
Abierta

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

- **Parámetros del servidor proxy**
  - **Host name or IP address**. Escriba el nombre o la dirección IP del servidor proxy.
  - **Port**. Escriba el número de puerto del servidor proxy.

Configuración de los parámetros de tabletas Windows



Configure los siguientes parámetros:

- **OSVersion**. En la lista, haga clic en **8.1** para Windows 8.1 o **10** para Windows 10. El valor predeterminado es **10**.

Configuración de Windows 10

- **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

  En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Abierta

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

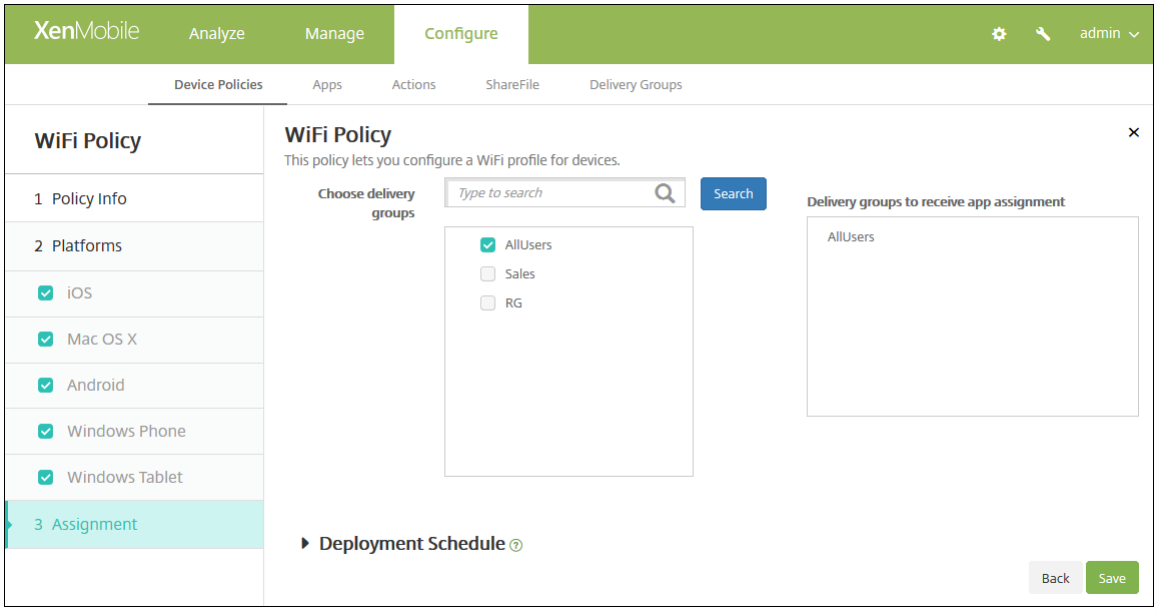
Configuración de Windows 8,1

- **Network name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **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
- **Hidden network (Enable if network is open or off)**. Seleccione si la red está oculta o no.
- **Connect automatically**. Seleccione si establecer conexión con la red de forma automática.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de **WiFi Policy Assignment**.

8. Haga clic en **Next**. Aparecerá la página WiFi Policy **Assignment**.
8. Haga clic en **Next**. Aparecerá la página WiFi Policy **Assignment**.
8. Haga clic en **Next**. Aparecerá la página WiFi 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de certificados de Windows CE

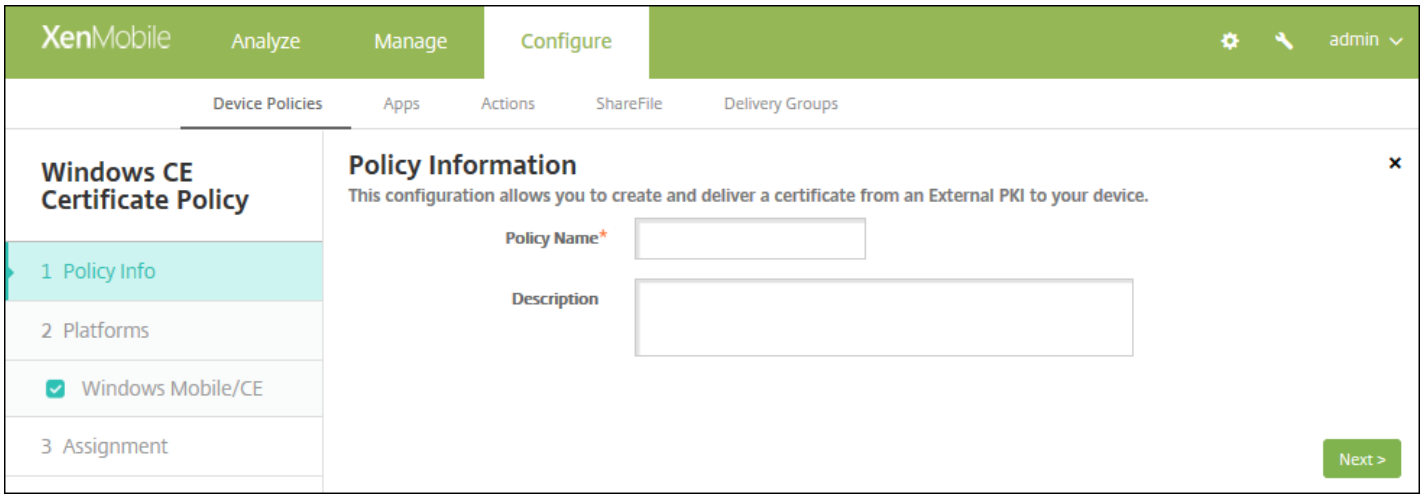
Jul 27, 2016

En XenMobile, puede crear una directiva de dispositivos para crear y entregar certificados de Windows Mobile/CE provenientes de una infraestructura de clave pública externa a los dispositivos de los usuarios. Consulte Certificados para obtener más información acerca de los certificados y las 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 **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.

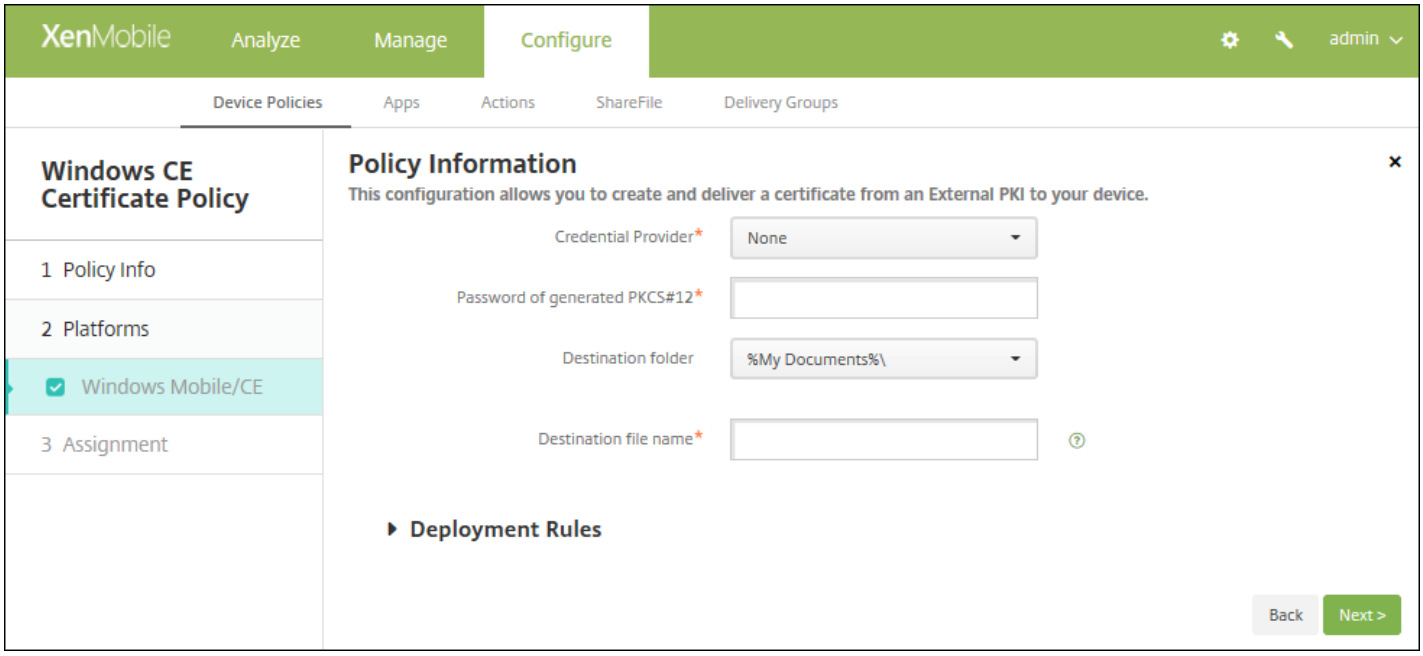
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Windows CE Certificate**. Aparecerá la página de información **Windows CE Certificate Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Windows CE Certificate Policy Platform**.

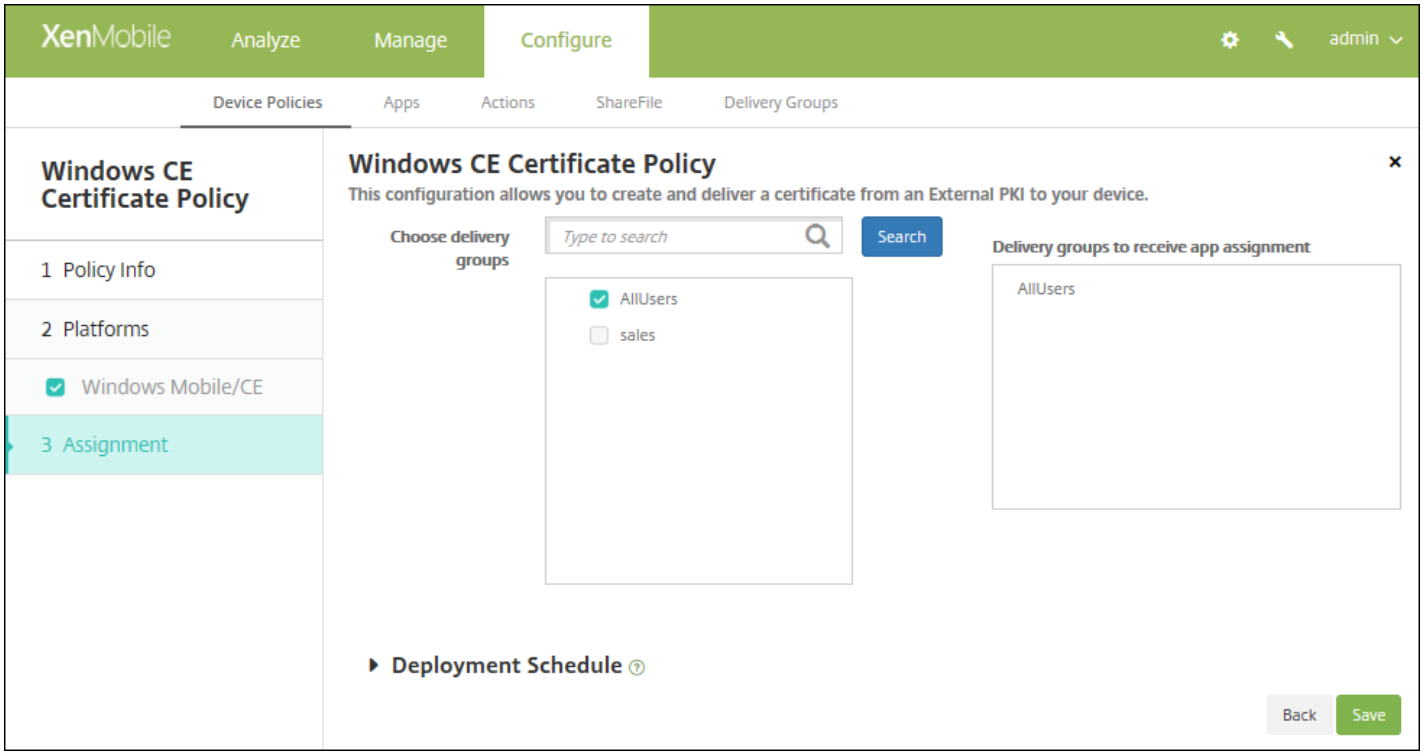


6. Configure los siguientes parámetros:

- **Credential provider**. En la lista, haga clic en el proveedor de credenciales. El valor predeterminado es **None**.
- **Password of generated PKCS#12**. Escriba la contraseña utilizada para cifrar la credencial.
- **Destination folder**. En la lista, haga clic en la carpeta de destino de la credencial, o bien haga clic en **Add new** para agregar una carpeta que no esté ya en la lista. Las opciones predeterminadas son:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**. Escriba el nombre del archivo de credenciales.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Windows CE Certificate 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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.
- 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.
- 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**.

Directiva de Worx Store

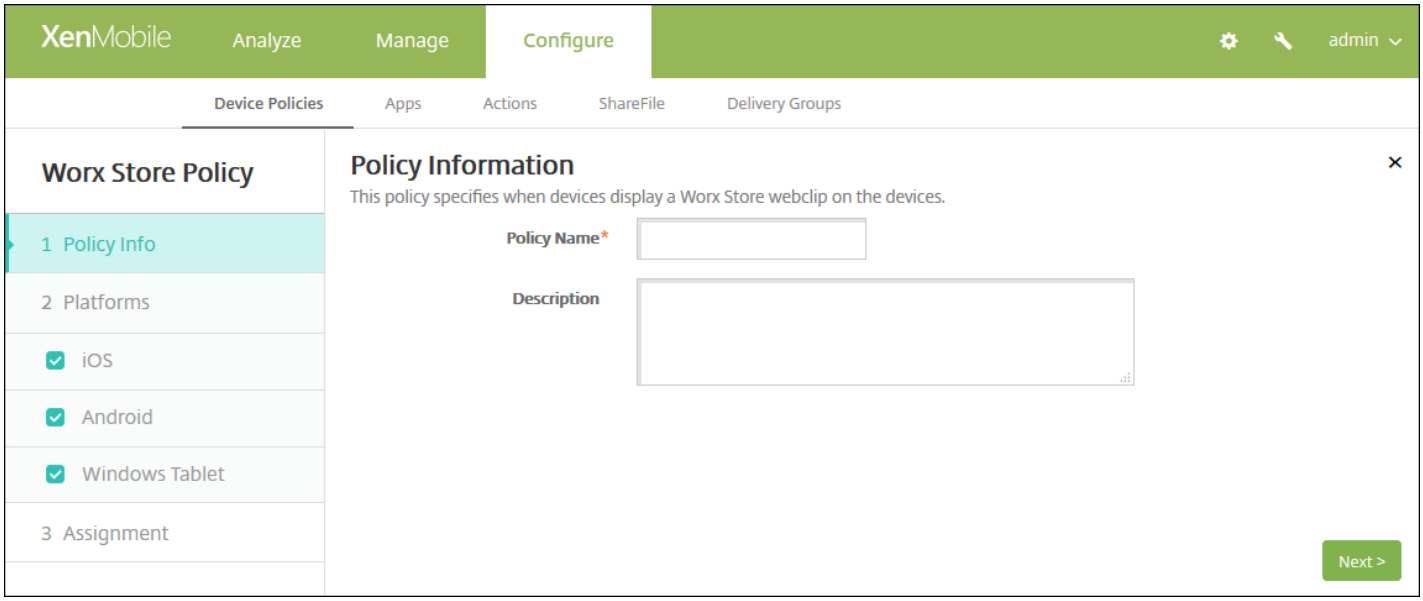
Jul 27, 2016

En XenMobile, puede crear una directiva para especificar si los dispositivos iOS, Android o tabletas Windows mostrarán un clip Web de Worx Store en la pantalla de inicio.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

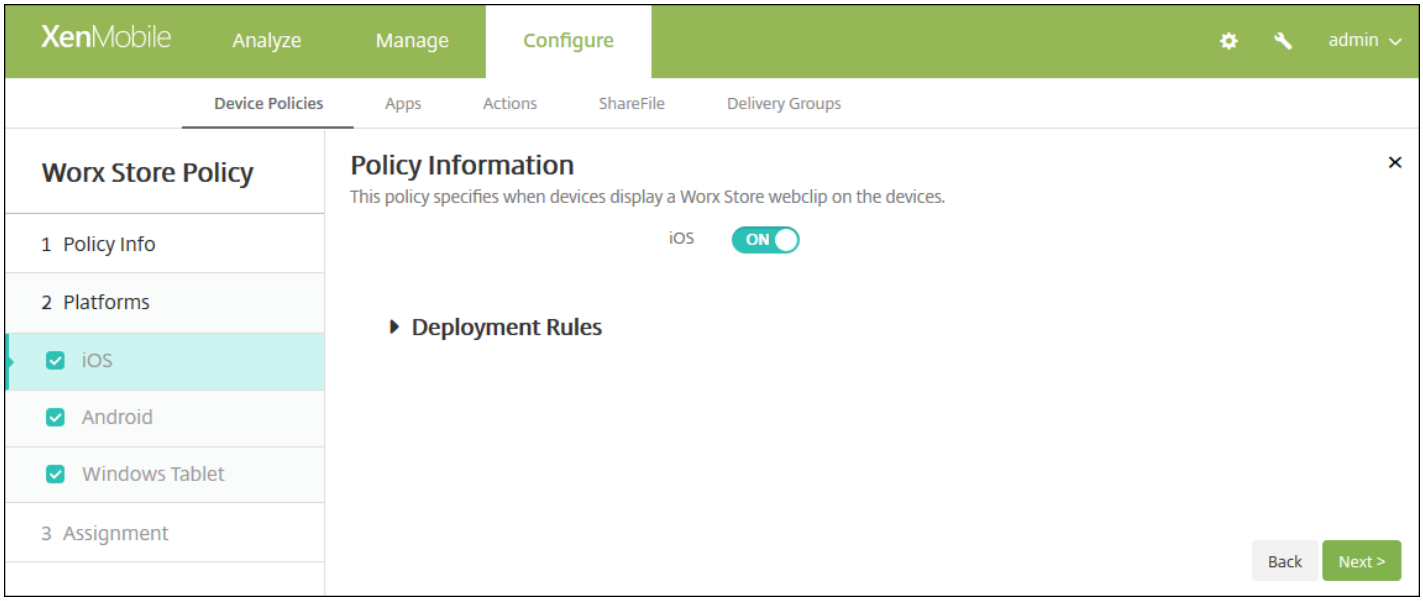
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Worx Store**. Aparecerá la página **Worx Store Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms**.



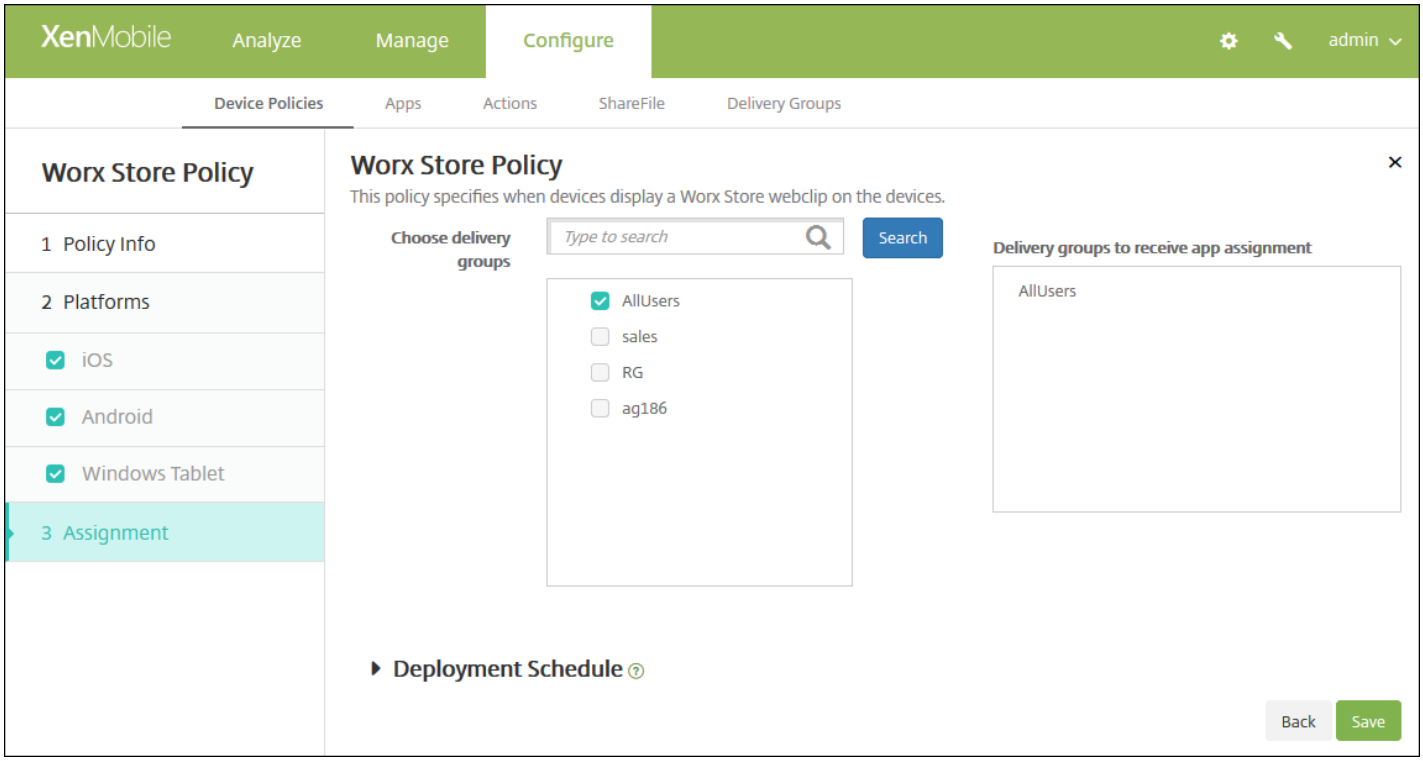
6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

7. Para cada plataforma que quiera configurar, seleccione si aparecerá un clip Web de Worx Store en los dispositivos de los usuarios. El valor predeterminado es **ON**.

Cuando termine de configurar los parámetros de configuración para cada plataforma, consulte el paso 8 para la configuración de las reglas de implementación de cada plataforma.

8. Configure las reglas de implementación.

9. Haga clic en **Next** y aparecerá la página de asignación **Worx Store 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:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directivas de opciones de XenMobile

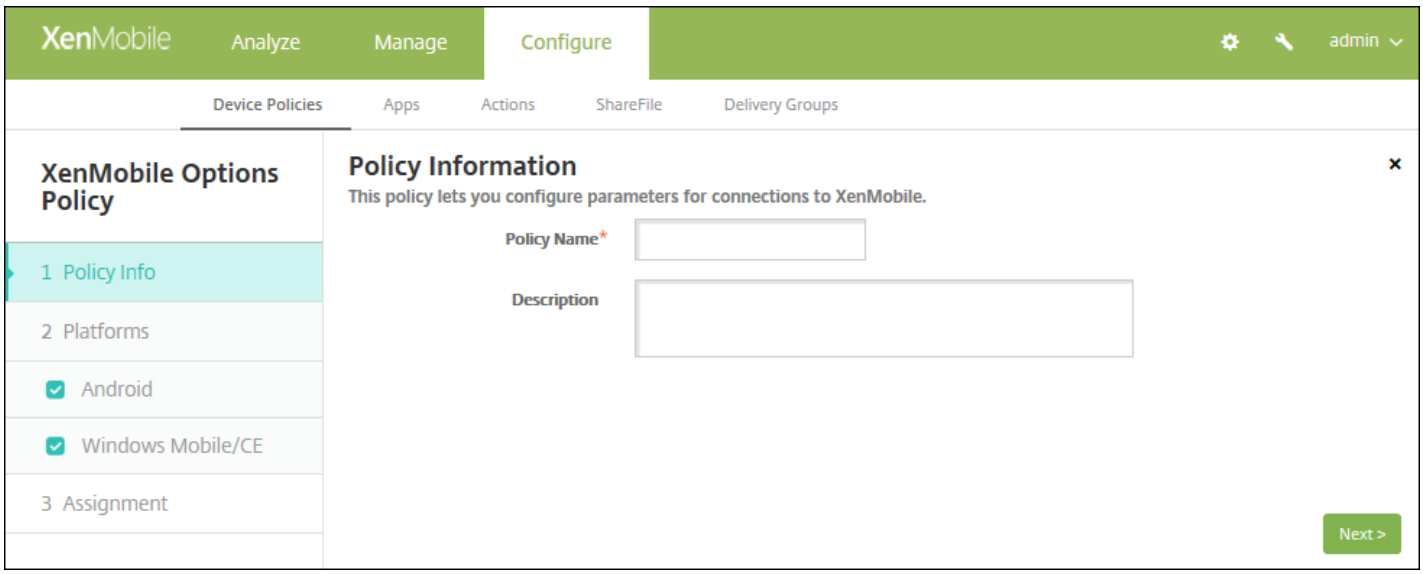
Jul 27, 2016

Puede agregar una directiva de opciones de XenMobile para configurar el comportamiento de Worx Home al conectarse a XenMobile desde dispositivos Android y Windows Mobile/CE.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **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:

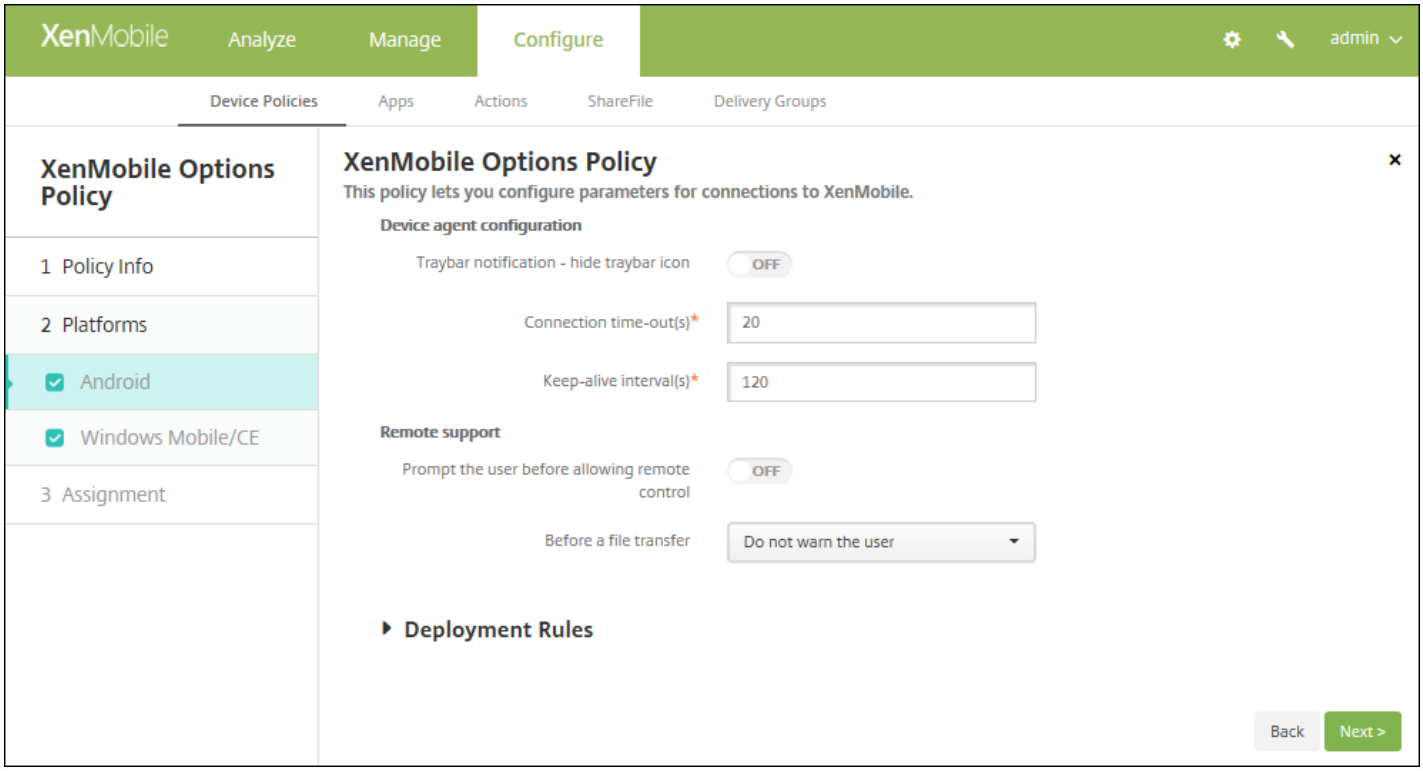
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

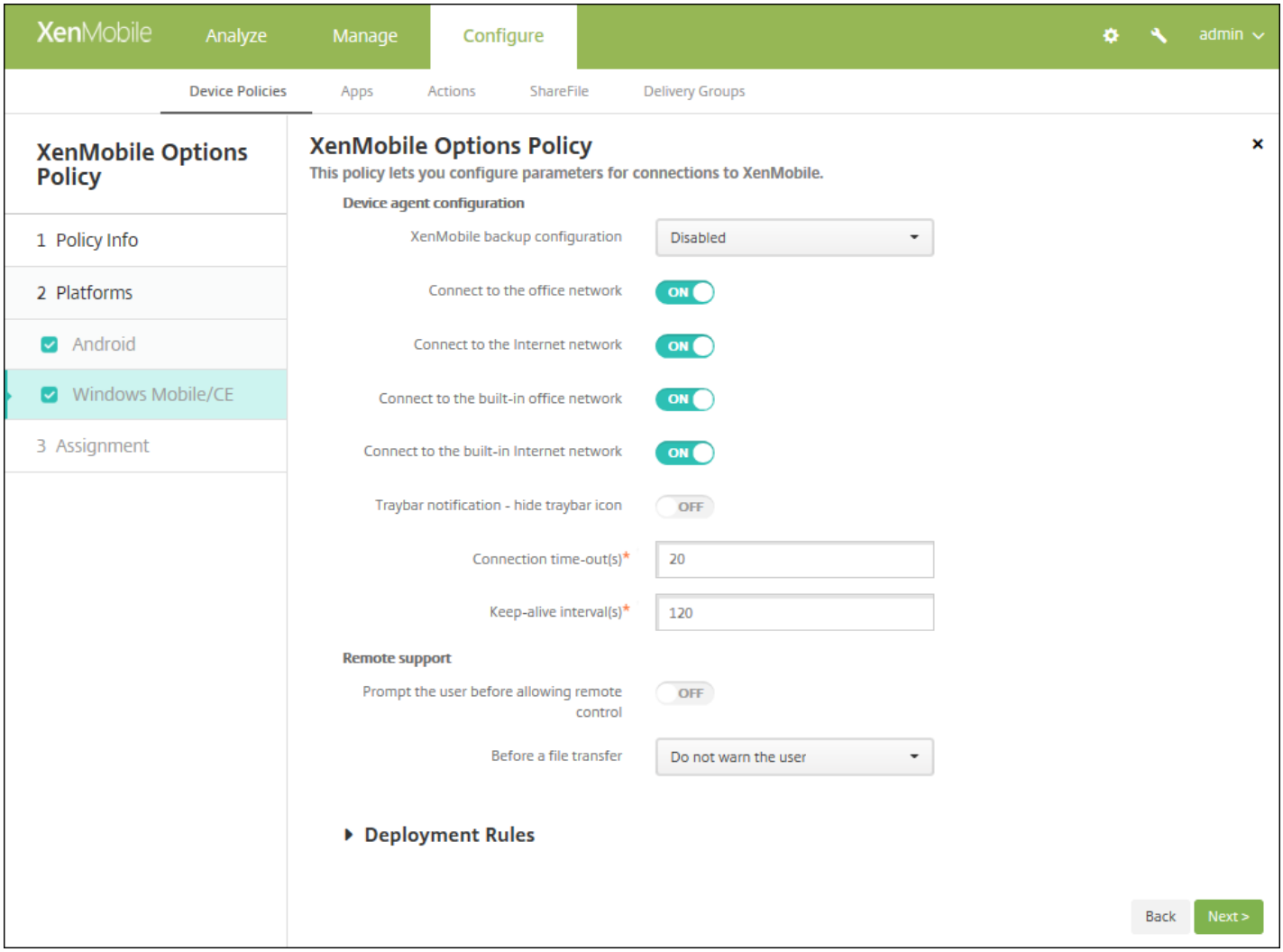
Configuración de los parámetros de Android



Configure estos parámetros:

- **Traybar notification - hide traybar icon**. Seleccione si el icono de la barra de la bandeja será visible o no. El valor predeterminado es **OFF**.
- **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.
- **Keep-alive interval(s)**. Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
- **Prompt the user before allowing remote control**. Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. El valor predeterminado es **OFF**.
- **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. Los valores disponibles son **Do not warn the user**, **Warn the user** y **Ask for user permission**. El valor predeterminado es **Do not warn the user**.

Configuración de los parámetros de Windows Mobile/CE



Configure estos parámetros:

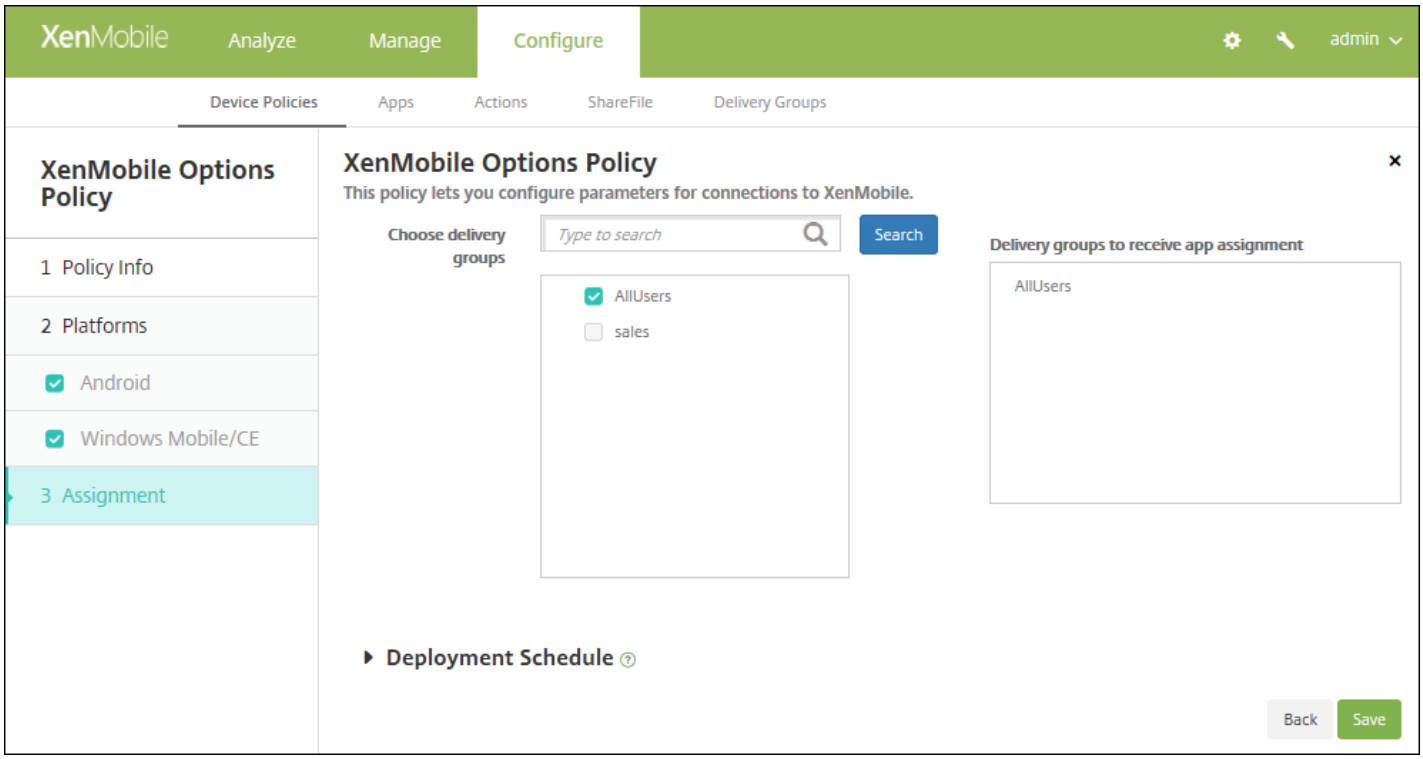
- **Device agent configuration**
  - **XenMobile backup configuration**. En la lista, haga clic en una opción para la copia de seguridad de la configuración de XenMobile en los dispositivos de los usuarios. El valor predeterminado es **Disabled**. Las opciones disponibles son:
    - Inhabilitado
    - At first connection after XenMobile installation
    - At first connection after each device reboot
  - **Connect to the office network**
  - **Connect to the Internet network**
  - **Connect to the built-in office network**: Cuando esta opción tiene el valor **ON**, XenMobile detecta automáticamente la red.
  - **Connect to the built-in Internet network**: Cuando esta opción tiene el valor **ON**, XenMobile detecta automáticamente la red.
  - **Traybar notification - hide traybar icon**. Seleccione si el icono del área de notificaciones será visible o no. El valor predeterminado es **OFF**.
  - **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.
  - **Keep-alive interval(s)**. Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor

predeterminado es de 120 segundos.

- **Remote support**
  - **Prompt the user before allowing remote control**. Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. El valor predeterminado es **OFF**.
  - **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. Los valores disponibles son **Do not warn the user**, **Warn the user** y **Ask for user permission**. El valor predeterminado es **Do not warn the user**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **XenMobile Options 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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Directiva de desinstalaciones de XenMobile

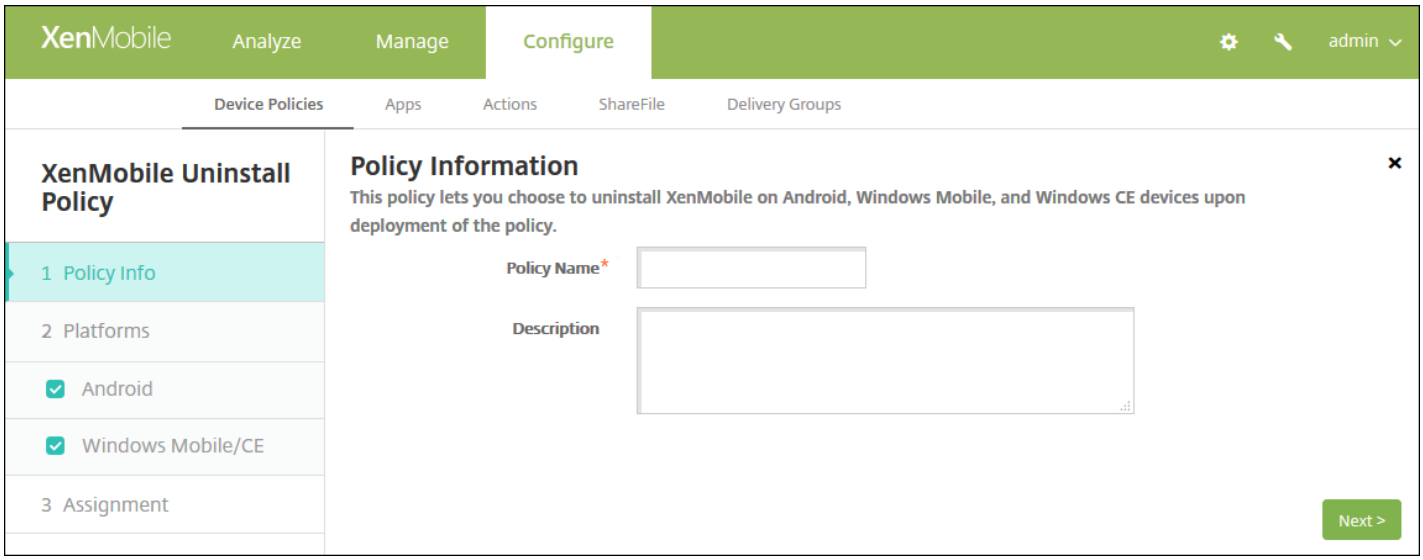
Jul 27, 2016

En XenMobile, puede agregar una directiva de dispositivos para desinstalar XenMobile de dispositivos Android y Windows Mobile/CE. Cuando se implementa, esta directiva elimina XenMobile de todos los dispositivos 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 **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Expanda **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:

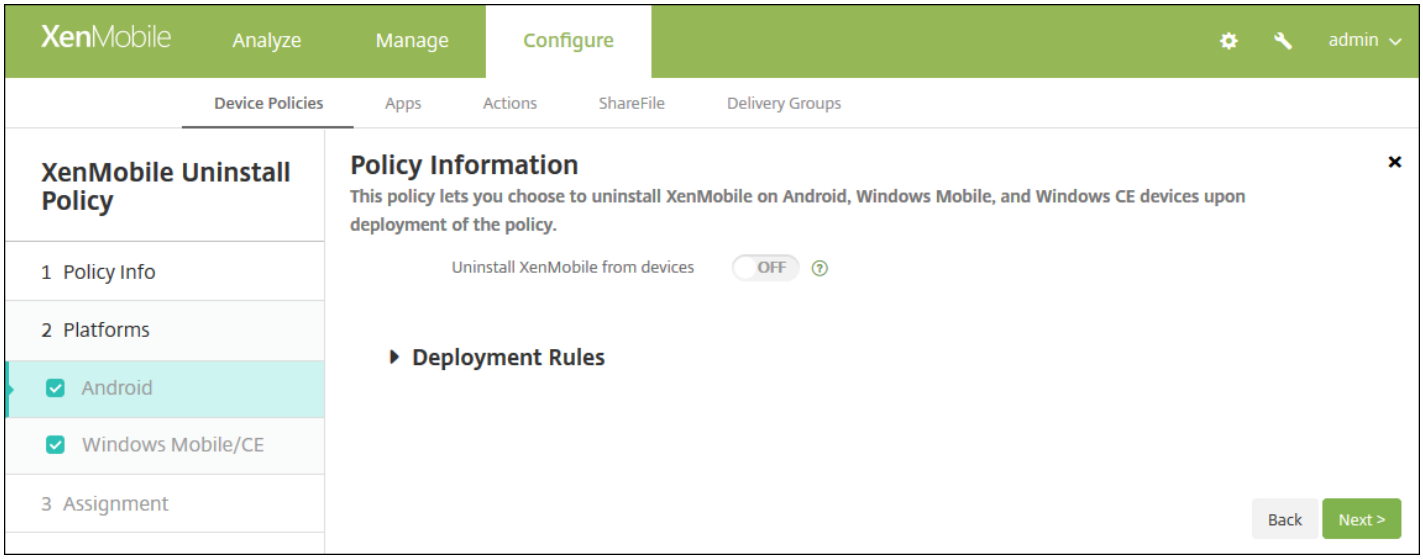
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de Android y Windows Mobile/CE

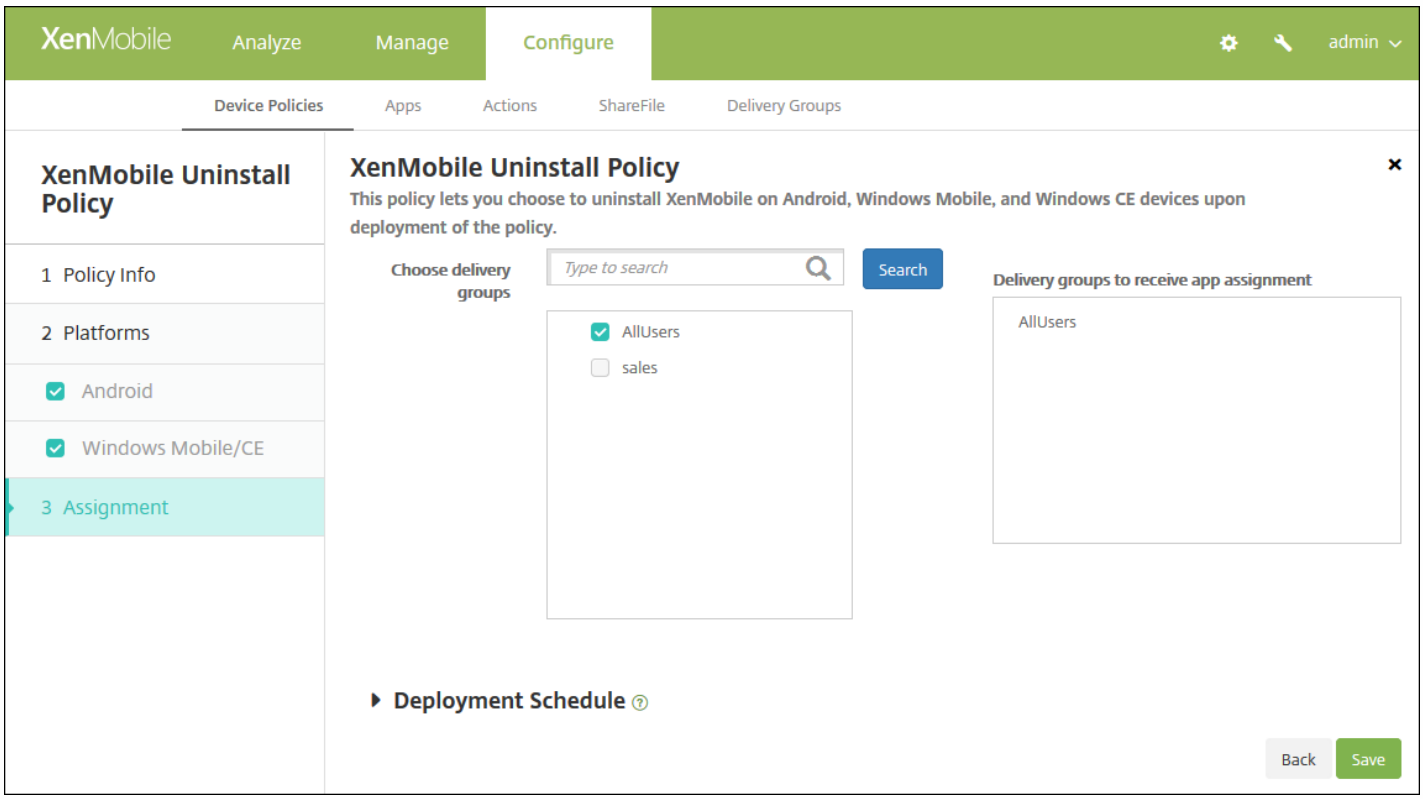


Configure este parámetro para cada plataforma seleccionada:

- **Uninstall XenMobile from devices**. Seleccione si quiere desinstalar XenMobile de todos los dispositivos en los que se implementará esta directiva. El valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

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**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- 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.
- 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**.

Incorporación de aplicaciones a XenMobile

Jul 27, 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.

Puede agregar los siguientes tipos de aplicaciones a XenMobile:

- **MDX**. Se trata de 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 de aplicaciones, como iTunes o Google Play. Por ejemplo, GoToMeeting. Las aplicaciones de Android for Work también se incluyen en esta categoría.
- **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 son aplicaciones nativas que no están empaquetadas con la herramienta MDX Toolkit y no contienen las directivas asociadas a aplicaciones MDX.
- **Web Link**. Se trata de una dirección Web (URL) a un sitio público o privado, o bien a una aplicación Web que no requiere Single Sign-On.

> ## Nota
>
> Citrix admite el modo de instalación silenciosa de aplicaciones de iOS y Samsung Android. La instalación silenciosa significa que no se pide a los usuarios que instalen las aplicaciones que usted implementa en el dispositivo, sino que las aplicaciones se instalan de forma silenciosa en segundo plano. Debe cumplir estos requisitos previos para poder implementar la instalación silenciosa:
>
> - Para las aplicaciones iOS, el dispositivo iOS administrado debe estar en modo supervisado. Para obtener información más detallada, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.
> - Para las aplicaciones Android, las directivas de Samsung for Enterprise (SAFE) o KNOX deben estar habilitadas en el dispositivo. Para ello, configure la directiva de clave de licencia de MDM de Samsung para que genere claves de licencia ELM y KNOX de Samsung. Para obtener más información, consulte **Directivas de claves de licencia para la administración de dispositivos móviles (MDM) Samsung** .

Funcionamiento de las aplicaciones MDX para móviles

XenMobile respalda aplicaciones iOS, Mac OS X, Android y Windows, incluidas las aplicaciones Worx (como Worx Home, WorxMail y WorxWeb) y el uso de directivas MDX. Con la consola de XenMobile, puede cargar aplicaciones y entregarlas a los dispositivos de usuario. Además de las aplicaciones Worx, puede agregar los siguientes tipos de aplicaciones:

- 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 dispositivos iOS, Mac OS X, Android y Windows 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 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

Puede crear su propio conector de aplicaciones y cargar una aplicación de Android for Work en XenMobile. 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 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 lo siguiente:

- 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 artículos según el tipo de aplicación que quiera agregar:

- Incorporación de aplicaciones MDX a XenMobile
- Incorporación de aplicaciones de tienda pública a XenMobile
- Incorporación de aplicaciones Web y SaaS a XenMobile
- Incorporación de aplicaciones de empresa a XenMobile
- Incorporación de aplicaciones de enlaces Web a XenMobile

Después de agregar una aplicación, esta aparecerá en la tabla de la página **Apps**, donde puede modificarla o asignarle categorías en cualquier momento.

Nota

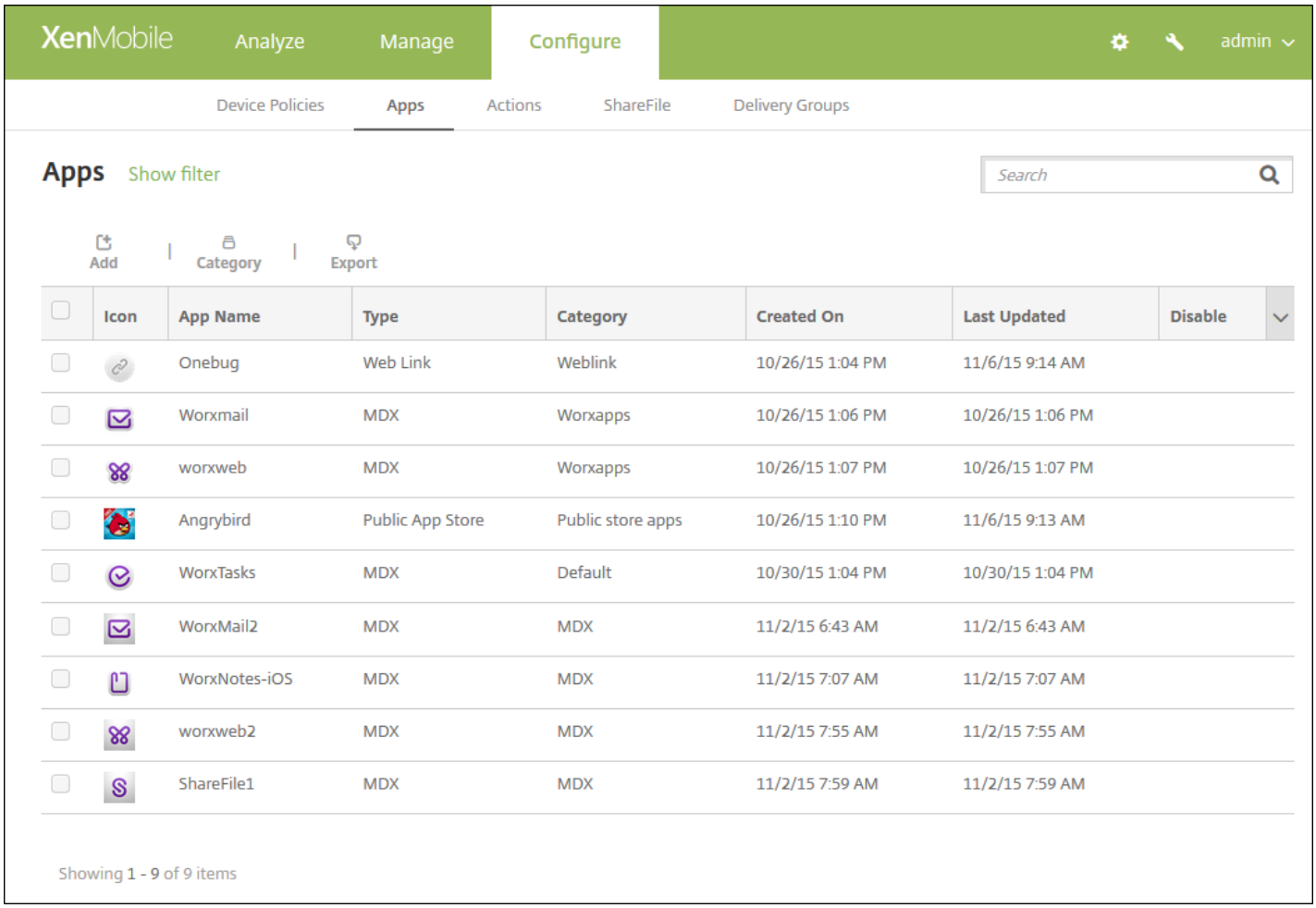
Después de actualizar a XenMobile 10.3, cuando se actualizan las aplicaciones móviles de Worx en XenMobile 10.3 que configuró en una versión anterior, los parámetros de las aplicaciones ya no aparecen en la consola de XenMobile. Es necesario editar y configurar de nuevo los parámetros de estas aplicaciones. No tendrá que volver a instalar las aplicaciones. Solo tiene que hacer esto una vez: los valores permanecerán intactos en futuras versiones del producto si actualiza la aplicación o si actualiza el servidor.

Cómo agregar una aplicación MDX a XenMobile

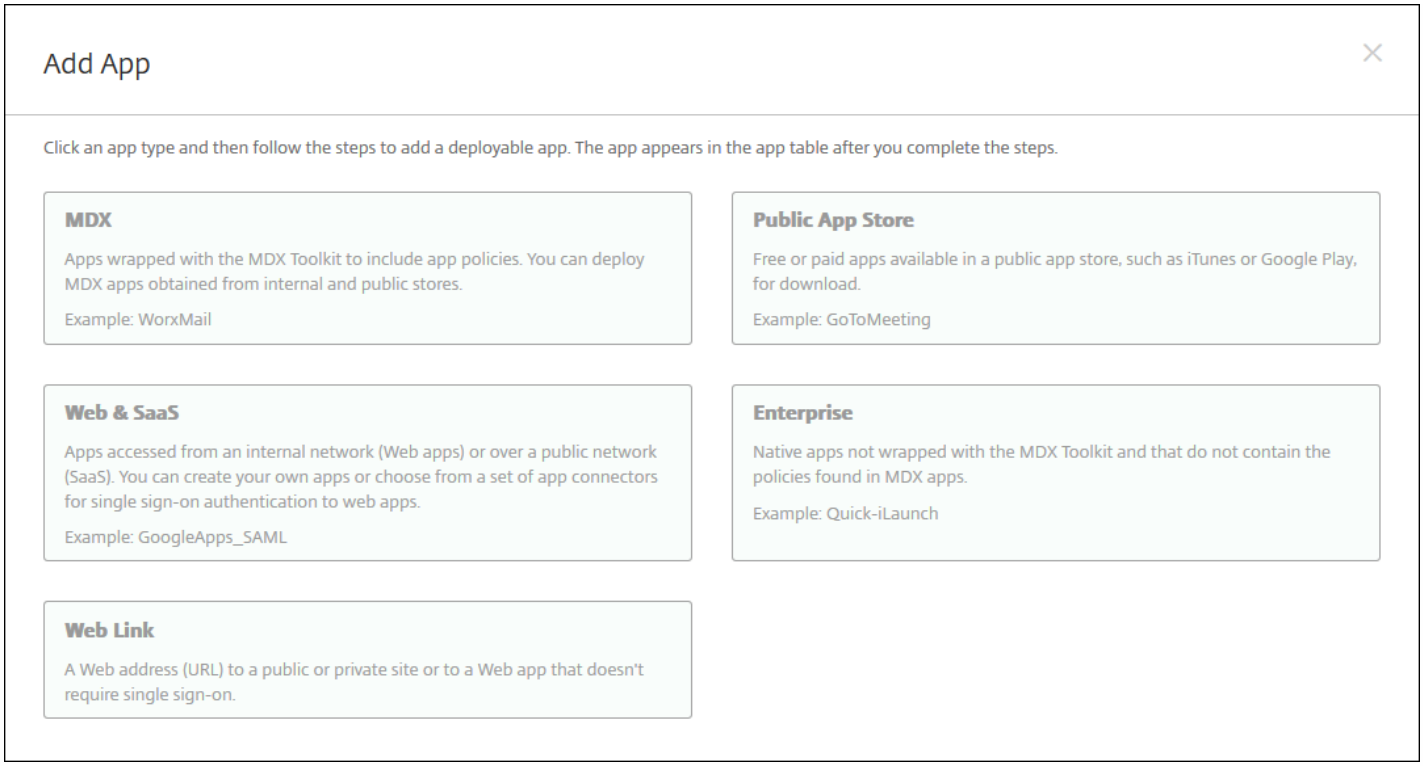
Jul 27, 2016

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. Dicha sección también incluye descripciones detalladas de las directivas.

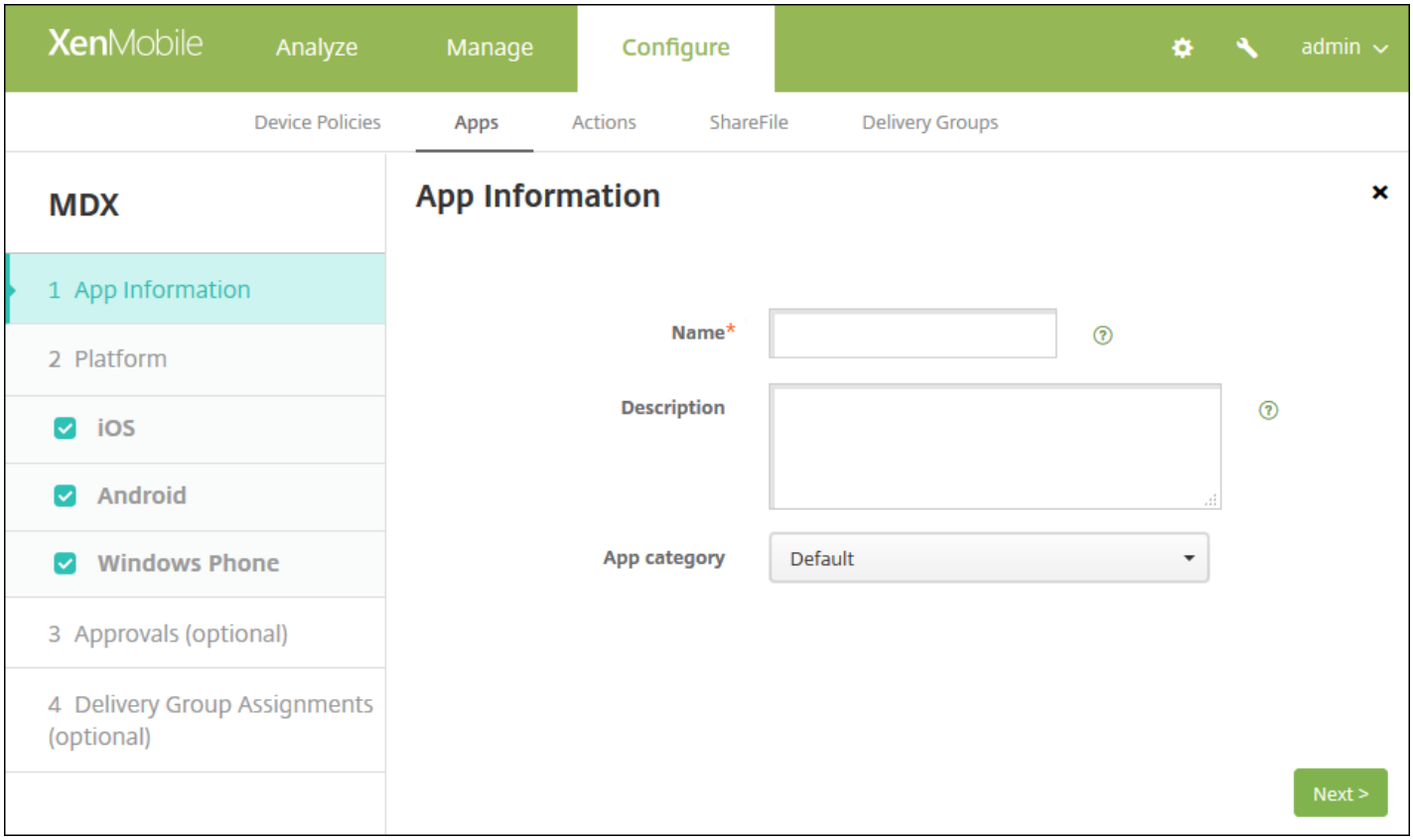
1. En la consola de XenMobile, haga clic en **Configure > Apps**. Aparecerá la página **Apps** .



2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



3. Haga clic en **MDX**. Aparecerá la página **MDX App Information**.



4. En el panel **App Information** , escriba la información siguiente:

- **Name**. Escriba un nombre descriptivo para la aplicación. Este figurará en **App Name**, en la tabla **Apps**.
- **Description**. Escriba, si quiere, una descripción de la aplicación.
- **App category**. Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Creación de categorías de aplicaciones en XenMobile.

5. Haga clic en **Next**. Aparecerá la página **App Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 11 para la configuración de las reglas de implementación de esa plataforma.

7. Debe seleccionar un archivo MDX para cargarlo. Para ello, haga clic en **Upload** y vaya a la ubicación del archivo.

- Si quiere agregar una aplicación VPP B2B de iOS, haga clic en **Your application is a VPP B2B application?** y, en la lista, haga clic en la cuenta B2B del programa VPP que se va a utilizar.

8. Haga clic en **Next**. Aparecerá la página de datos detallados de la aplicación.

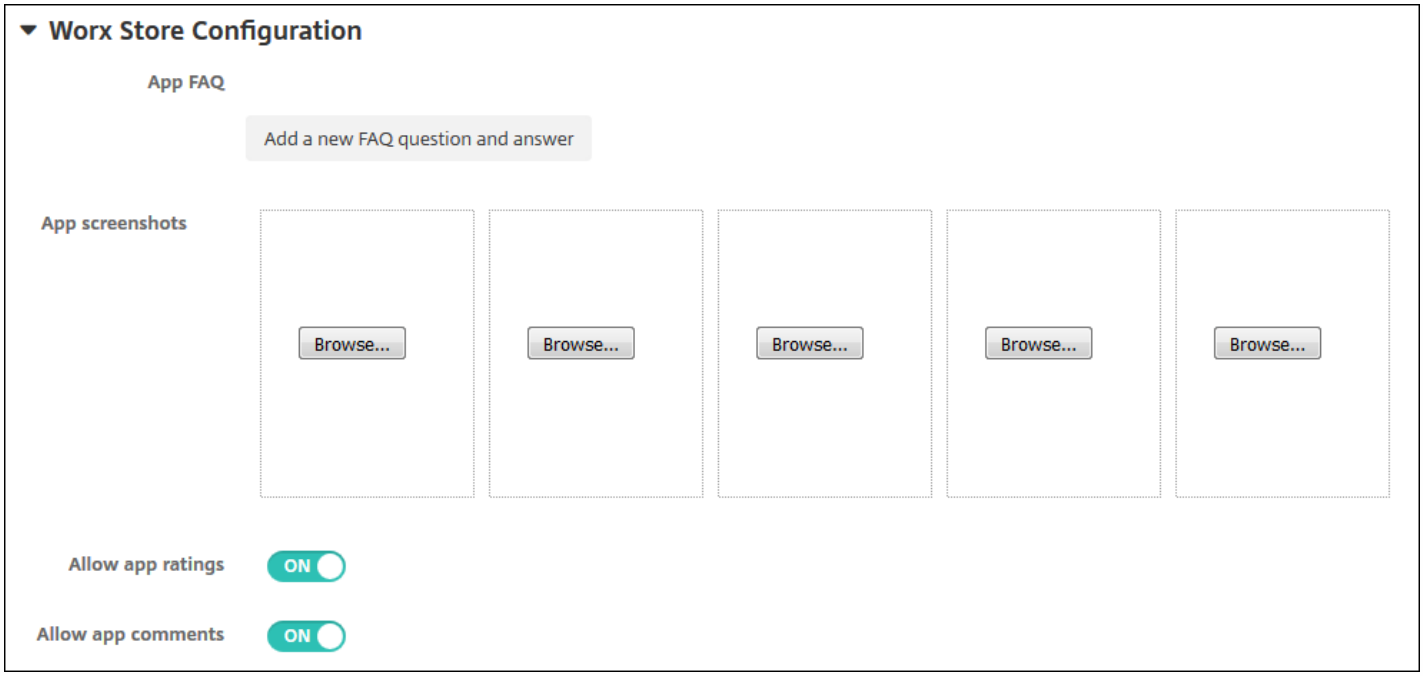
9. Configure los siguientes parámetros:

- **File name**. Escriba el nombre del archivo asociado a la aplicación.
- **App Description**. Escriba una descripción de la aplicación.
- **App version**. Si quiere, escriba el número de versión de la aplicación.
- **Minimum OS version**. Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Maximum OS version**. Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Excluded devices**. Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
- **Remove app if MDM profile is removed**. Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es **ON**.
- **Prevent app data backup**. Seleccione si quiere impedir que los usuarios realicen copias de seguridad de los datos de la aplicación. El valor predeterminado es **ON**.
- **Force app to be managed**. Si se instala una aplicación no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos no supervisados. El valor predeterminado es **ON**. Disponible en iOS 9.0 y versiones posteriores.

10. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos, requisitos de red, otros accesos, cifrado, interacción de las aplicaciones, restricciones de aplicaciones, acceso de las aplicaciones a la red, registros de las aplicaciones y geovallas de las aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener información adicional sobre las directivas de aplicaciones para las aplicaciones MDX, la cual incluye 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.

11. Configure las reglas de implementación.

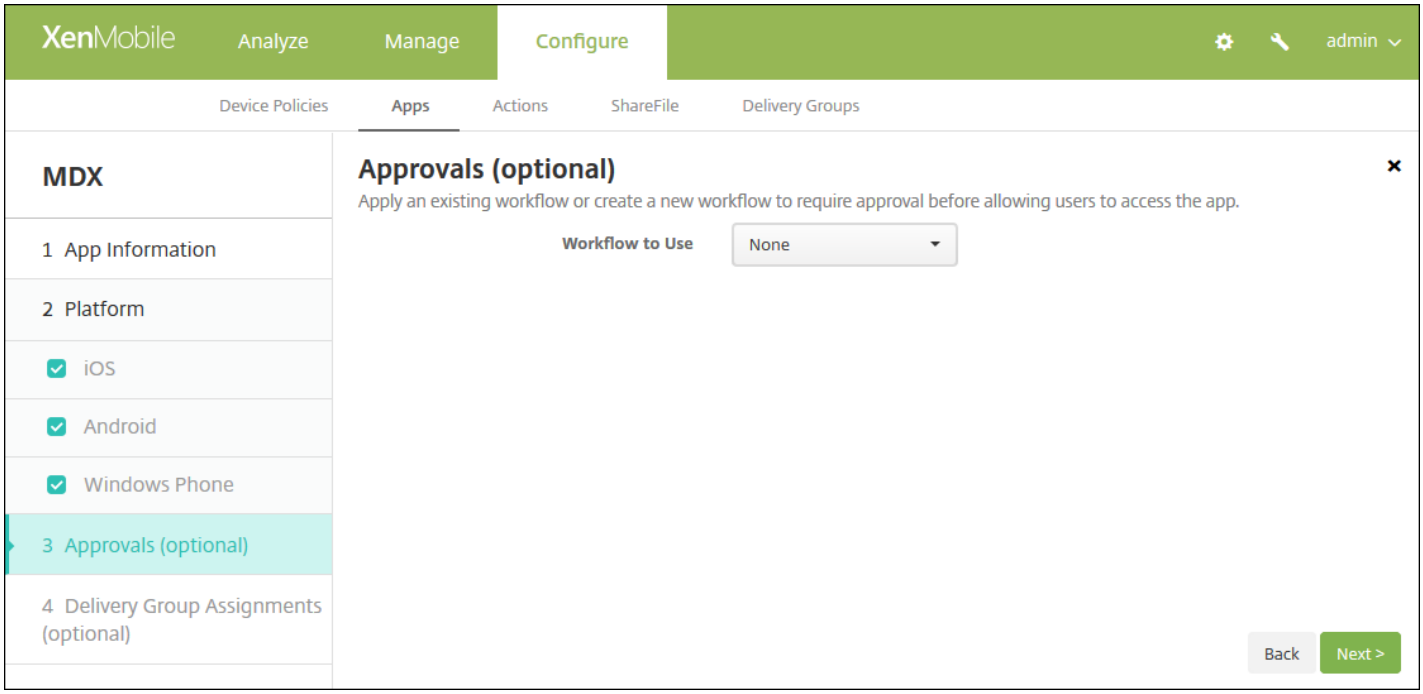
12. Expanda **Worx Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en Worx Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **App FAQ**. Agregue una sección de preguntas frecuentes sobre la aplicación junto con sus respuestas.
  - **App screenshots**. Agregue capturas de pantalla para ayudar a clasificar la aplicación en Worx Store. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Allow app ratings**. Seleccione si permitir a los usuarios puntuar la aplicación. El valor predeterminado es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

13. Haga clic en **Next**. Aparecerá la página **Approvals**.



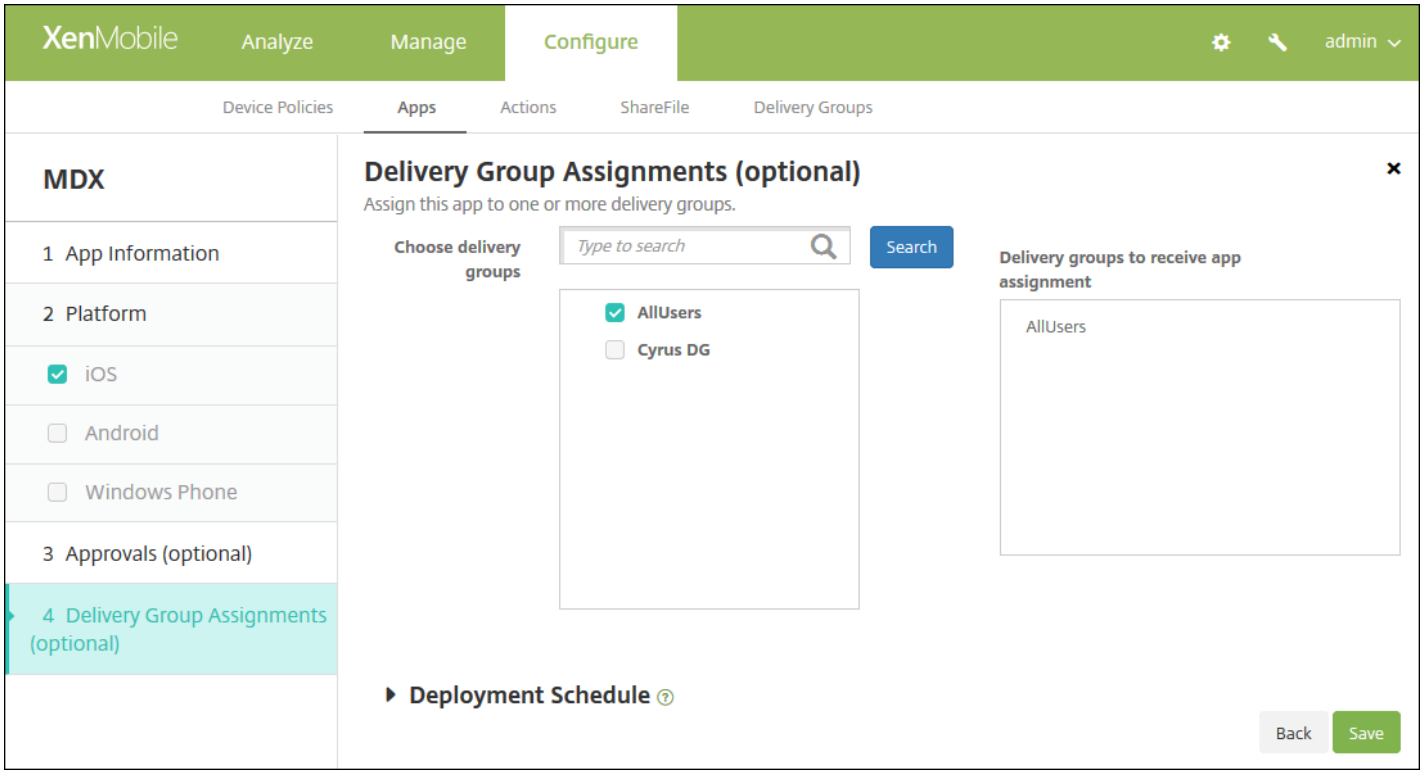
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 15.

Configure esta opción si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use**. En la lista, haga clic en un flujo de trabajo existente o en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name**. Escriba un nombre único para el flujo de trabajo.
  - **Description**. Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates**. En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval**. En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es 1 level. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - 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.

14. Haga clic en **Next**. Aparecerá la página **Delivery Group 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

16. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

- 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 aplica para iOS.

17. Haga clic en **Save**.

Creación de categorías de aplicaciones en XenMobile

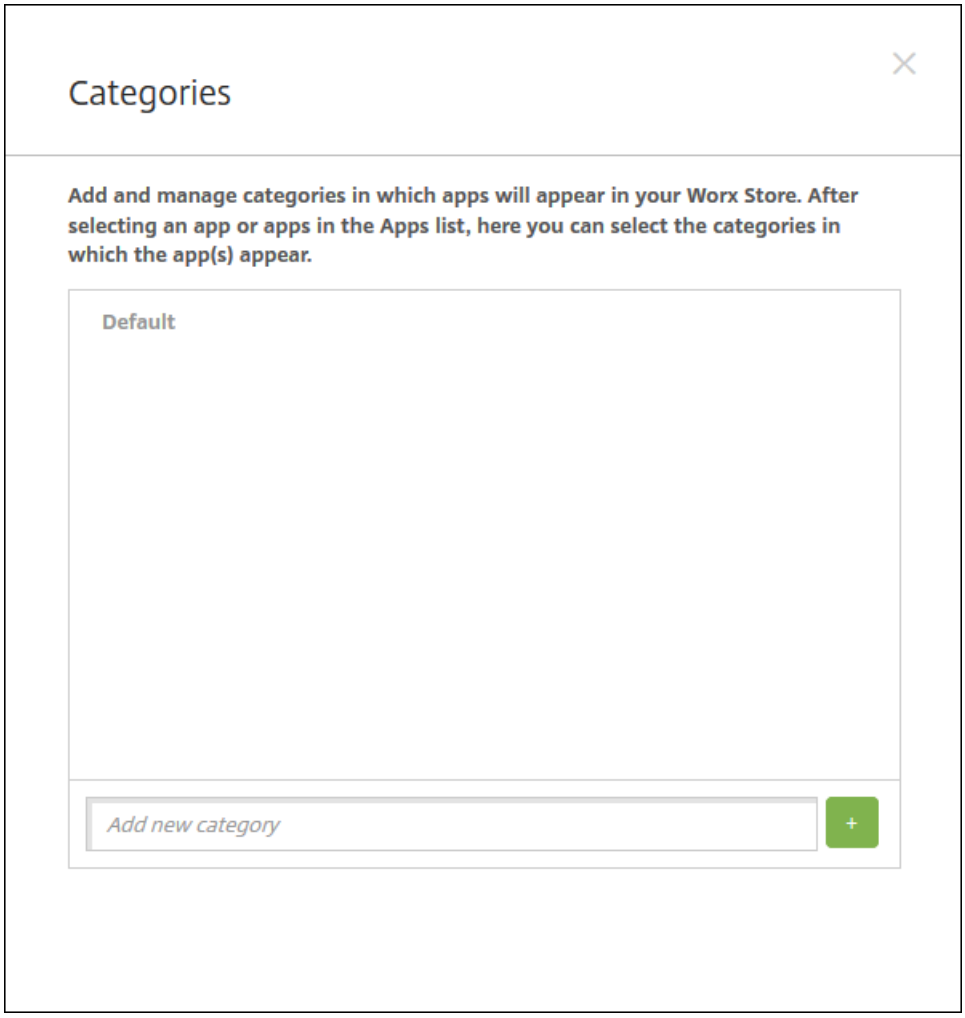
Jul 27, 2016

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 categorías de aplicaciones para 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.

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 agregarlos a una de las categorías que haya configurado.

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Aparecerá la página **Apps**.

2. Haga clic en **Category**. Aparecerá el cuadro de diálogo **Categories**.

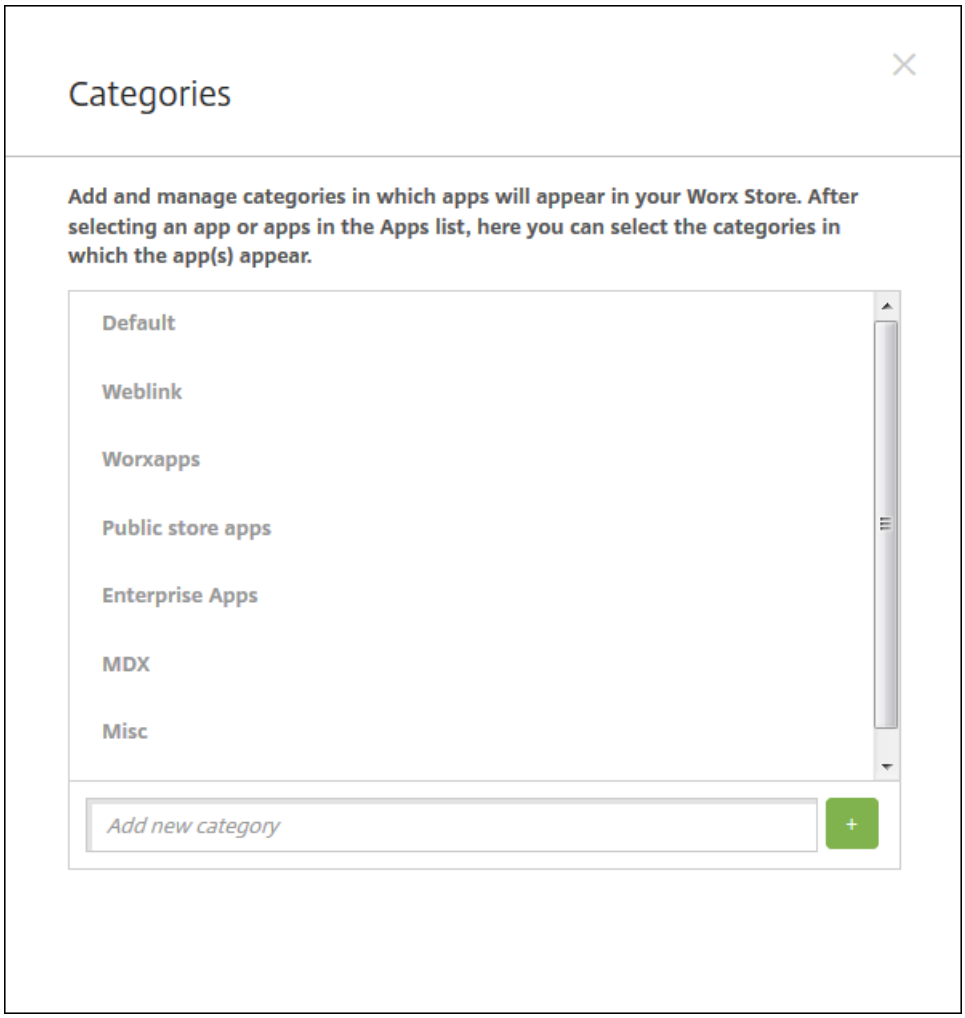


3. Para agregar cada categoría, lleve a cabo lo siguiente:

- Escriba el nombre de la categoría que quiere agregar en el campo **Add a new category**, situado en la parte inferior del cuadro de diálogo. Por ejemplo, puede escribir *Aplicaciones de empresa* para crear una categoría que incluya las

aplicaciones de la empresa.

- Haga clic en el signo más (+) para agregar la categoría. La categoría recién creada se agregará y aparecerá en el mismo cuadro de diálogo **Categories**.



4. Cuando haya terminado de agregar categorías, cierre el cuadro de diálogo **Categories**.

5. En la página **Apps**, puede colocar una aplicación existente en una categoría nueva.

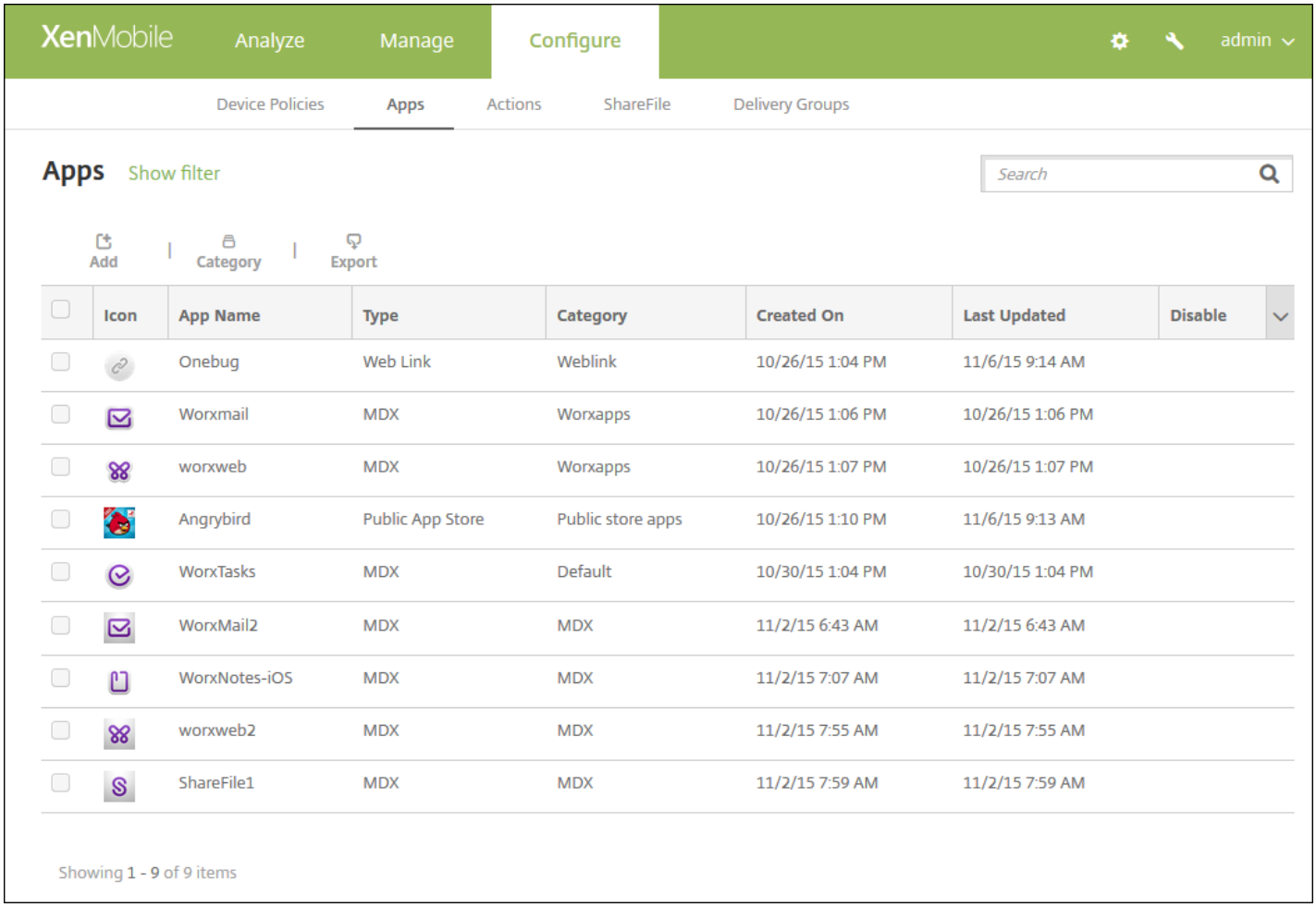
- Seleccione la aplicación que quiera categorizar.
- Haga clic en **Edit**. Aparecerá la página **App Information**.
- En la lista **App category**, aplique la nueva categoría marcando la casilla de verificación de la categoría en cuestión. Desmarque las casillas de aquellas categorías existentes que no quiera aplicar a la aplicación.
- Haga clic en la ficha **Delivery Groups Assignments** o haga clic en **Next** en las páginas restantes de la configuración de la aplicación.
- Haga clic en **Save** en la página **Delivery Groups Assignments** para aplicar la nueva categoría. La nueva categoría se aplicará a la aplicación y aparecerá en la tabla **Apps**.

Incorporación de una aplicación de tienda pública a XenMobile

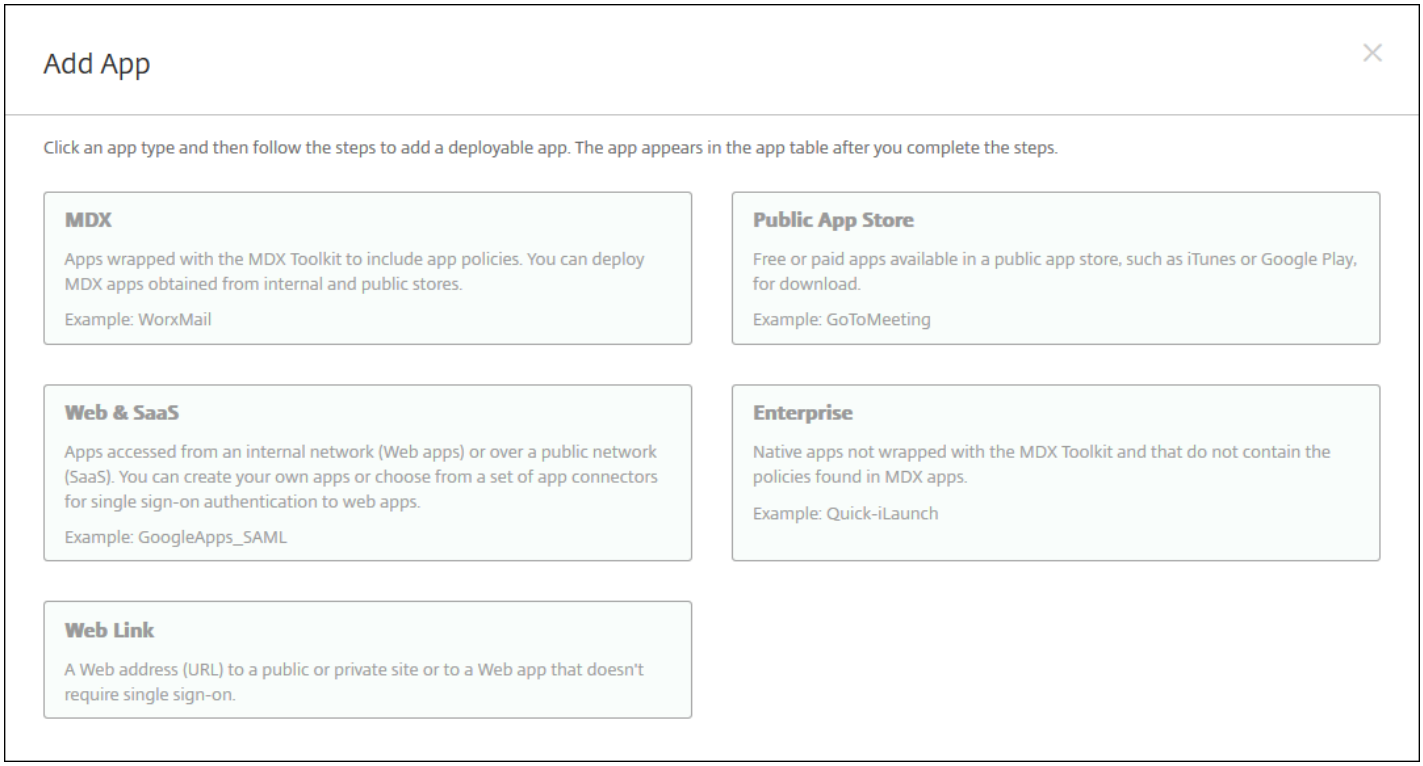
Oct 31, 2016

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. Además, cuando se agrega una aplicación de pago de una tienda pública de aplicaciones para Android for Work, se puede revisar el estado de la licencia de compra en bloque: la cantidad total de licencias disponibles y la cantidad de licencias en uso actualmente, además de la dirección de correo electrónico de cada uno de los usuarios que está consumiendo una licencia. El plan de compra en bloque de Android for Work simplifica el proceso de encontrar, comprar y distribuir aplicaciones y otros datos en masa para una organización.

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Aparecerá la página **Apps**.



2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



3. Haga clic en **Public App Store**. Aparecerá la página **App Information**.

4. En el panel **App Information**, escriba la información siguiente:

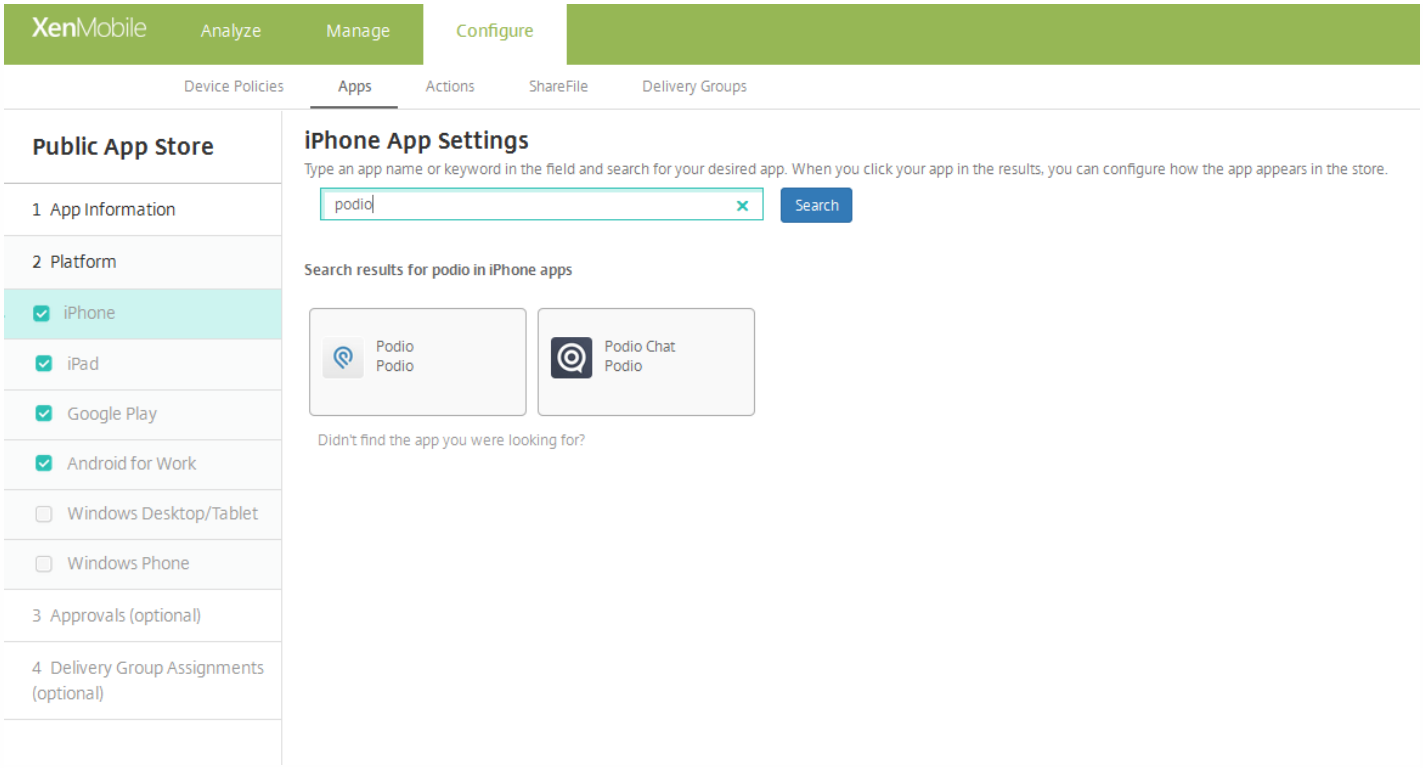
- **Name**. Escriba un nombre descriptivo para la aplicación. Este figurará en App Name, en la tabla Apps.
- **Description**. Escriba, si quiere, una descripción de la aplicación.
- **App category**. Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Creación de categorías de aplicaciones en XenMobile.

5. Haga clic en **Next**. Aparecerá la página **App Platforms**.

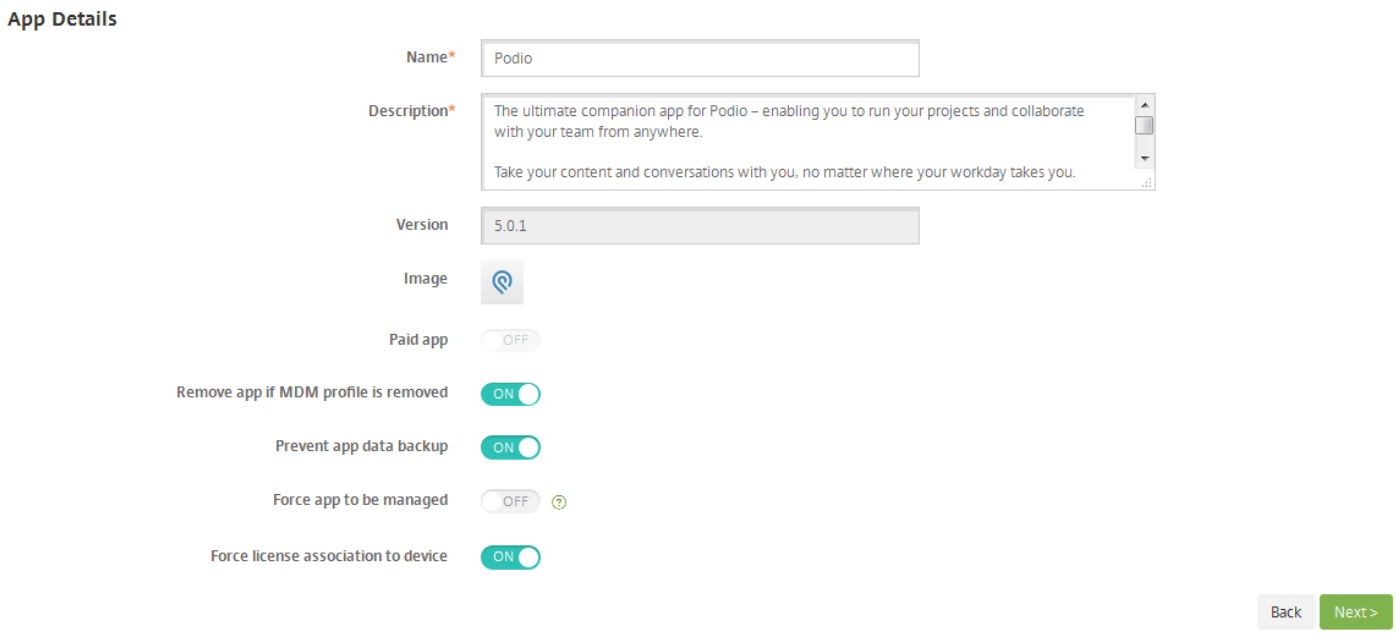
6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 10 para la configuración de las reglas de implementación de esa plataforma.

7. Seleccione la aplicación que quiera agregar. Para ello, escriba el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Search**. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. En la siguiente imagen, se muestran los resultados de la búsqueda *podio*.



8. Haga clic en la aplicación que quiera agregar. Los campos **App Details** aparecerán ya rellenados con información relativa a la aplicación seleccionada (incluido el nombre, la descripción, el número de versión y la imagen asociada).



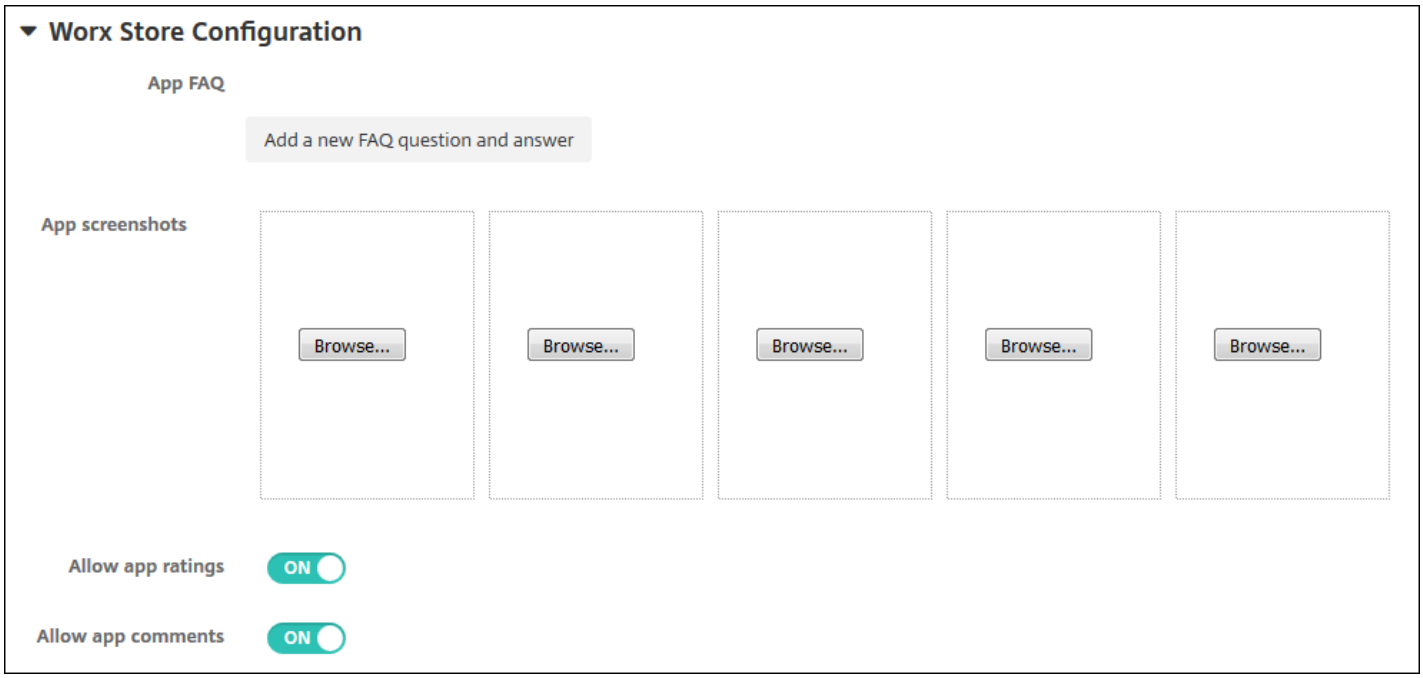
9. Configure los siguientes parámetros:

- Si fuera necesario, cambie el nombre y la descripción de la aplicación.
- **Paid app**. Este campo está preconfigurado y no se puede cambiar.

- **Remove app if MDM profile is removed**. Seleccione si quiere quitar la aplicación cuando se quite el perfil de MDM. El valor predeterminado es **ON**.
- **Prevent app data backup**. Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es **ON**.
- **Force app to be managed**. Si se instala una aplicación no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos no supervisados. El valor predeterminado es **OFF**. Disponible en iOS 9.0 y versiones posteriores.
- **Force license to association to device**. Seleccione si quiere asociar una aplicación (desarrollada con la opción de asociación a un dispositivo habilitada) a un dispositivo en lugar de a un usuario. Disponible en iOS 9 y versiones posteriores. Si la aplicación que ha elegido no admite la asignación a un dispositivo, este campo no se puede cambiar.

10. Configure las reglas de implementación.

11. Expanda **Worx Store Configuration**.

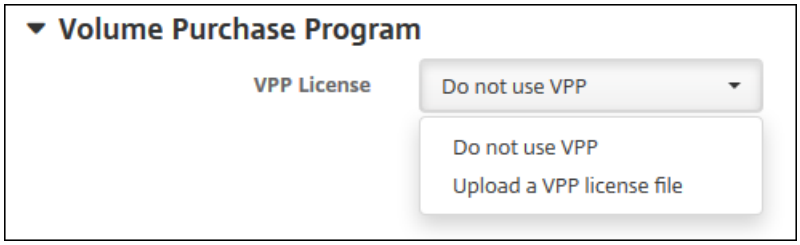


Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en Worx Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **App FAQ**. Agregue una sección de preguntas frecuentes sobre la aplicación junto con sus respuestas.
  - **App screenshots**. Agregue capturas de pantalla para ayudar a clasificar la aplicación en Worx Store. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Allow app ratings**. Seleccione si permitir a los usuarios puntuar la aplicación. El valor predeterminado es ON.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.

12. Expanda **Volume Purchase Program** o, en el caso de Android for Work, expanda **Bulk Purchase**.

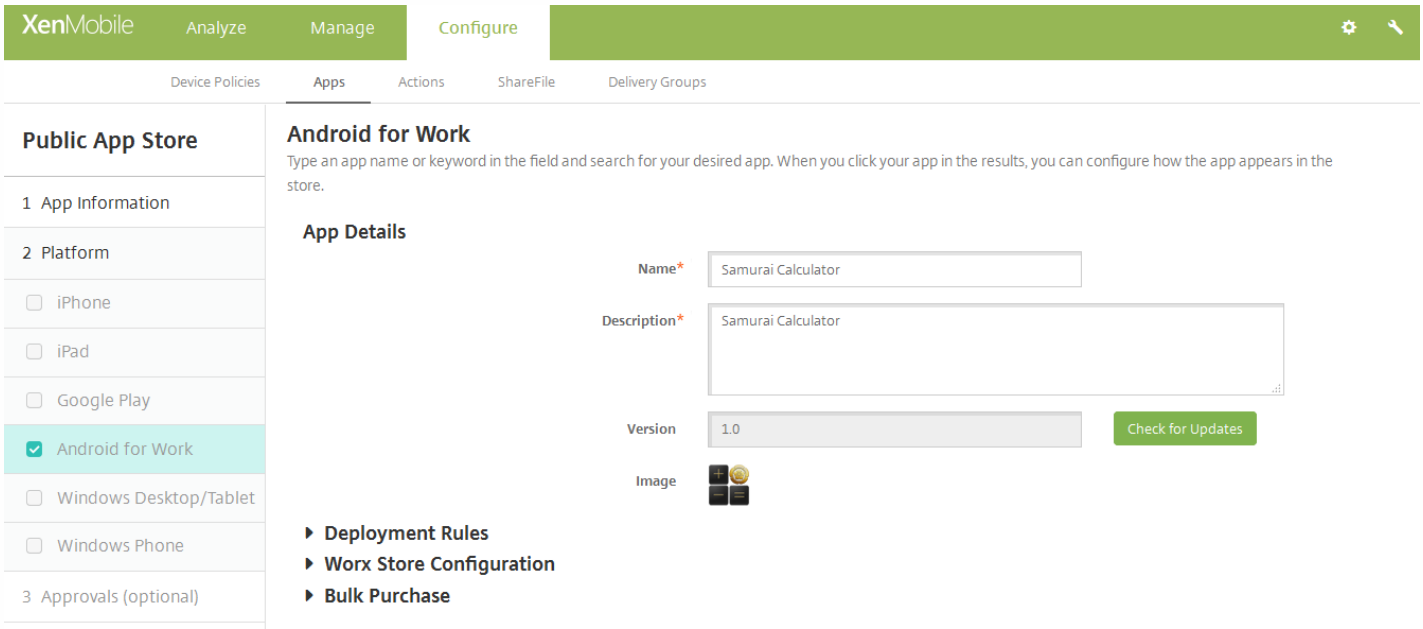
Para el programa Volume Purchase Program de compras por volumen, complete los pasos siguientes.



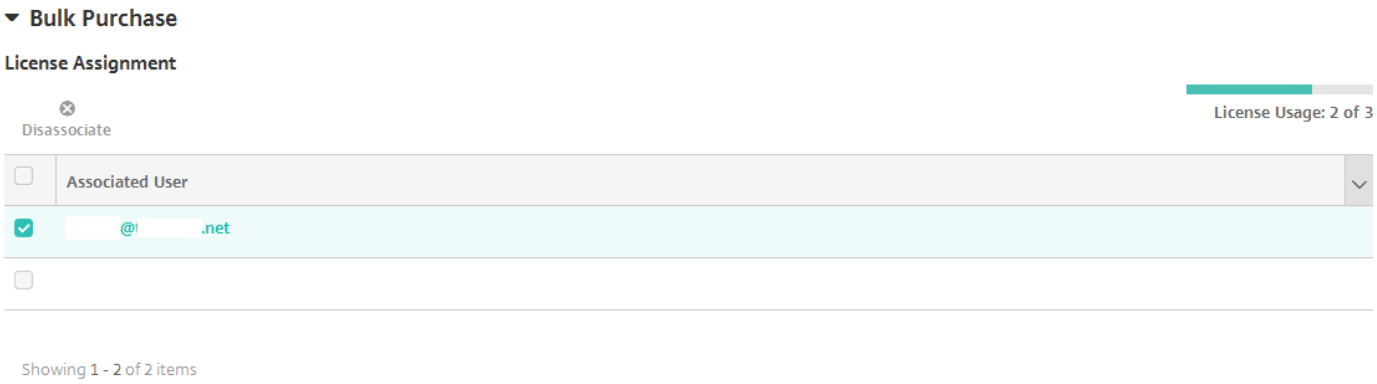
a. En la lista **VPP license**, haga clic en **Upload a VPP license file** si quiere habilitar XenMobile para aplicar una licencia de VPP para la aplicación.

b. En el cuadro de diálogo que aparece, importe la licencia.

Para las compras en bloque de Android for Work, expanda la sección **Bulk Purchase**.



En la tabla License Assignment verá cuántas licencias se están utilizando actualmente para la aplicación del total de licencias disponibles. Puede seleccionar un usuario y hacer clic en **Disassociate** para porner fin a su asignación de licencia y liberar esa licencia para otro usuario. No obstente, solo puede desasociar la licencia si el usuario no forma parte de un grupo de entrega que contiene esa aplicación en concreto.



13. Haga clic en **Next**. Aparece la página Approvals.

Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita configurar flujos de trabajo de aprobación, puede omitir este paso y pasar directamente al paso siguiente.

Configure este parámetro si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use**. En la lista, haga clic en un flujo de trabajo existente o haga clic en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name**. Escriba un nombre único para el flujo de trabajo.
  - **Description**. Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates**. En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval**. En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - 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.

14. Haga clic en **Next**. Aparecerá la página **Delivery Group 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

16. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.

- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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**.

Incorporación de aplicaciones Web y SaaS a XenMobile

Jul 27, 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.

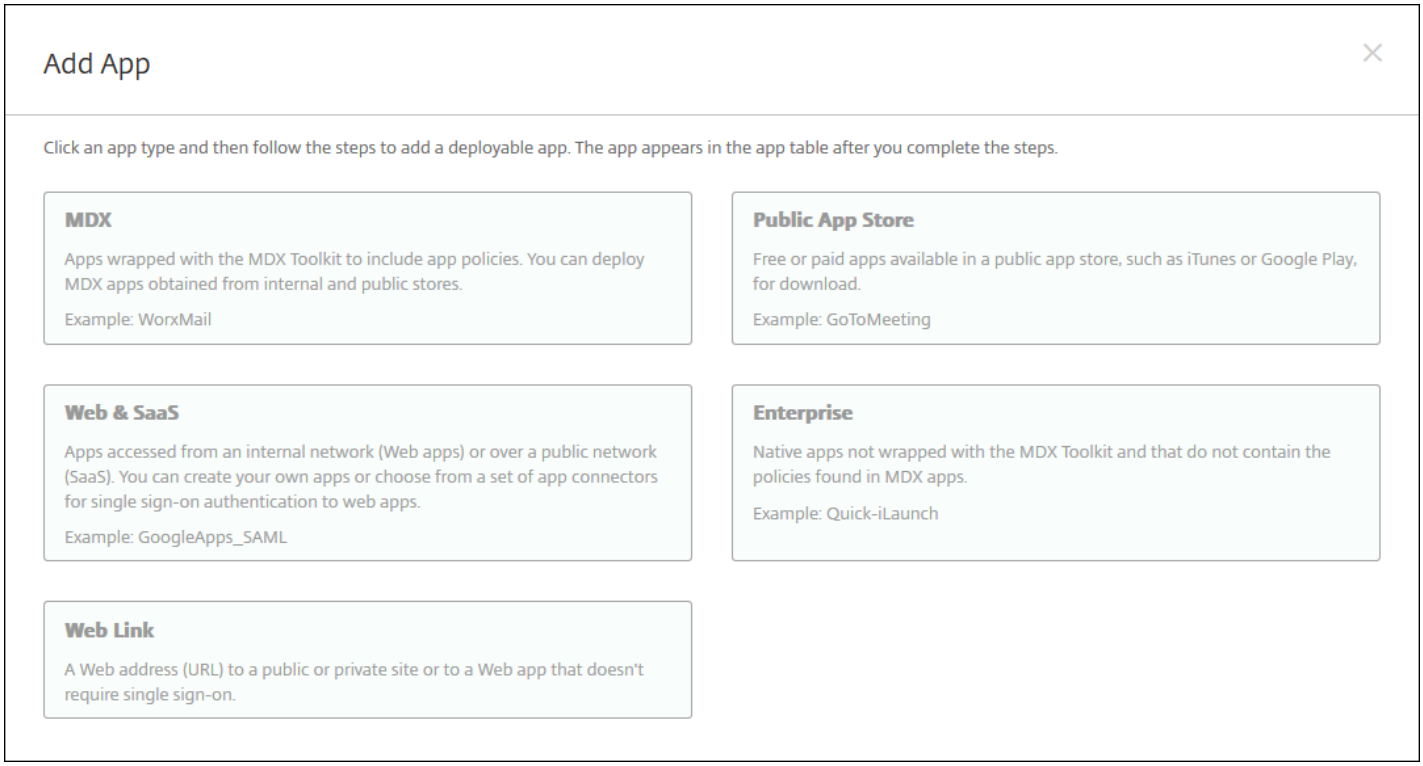
Para configurar un conector, debe proporcionar la siguiente información:

- Nombres diferentes (opcional). Haga uso de cualquier conector de aplicaciones que se muestre en la consola. El conector Box 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 le 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. Especifique las personas que pueden aprobar el grupo de entrega de los usuarios a los que quiere asignar la aplicación.

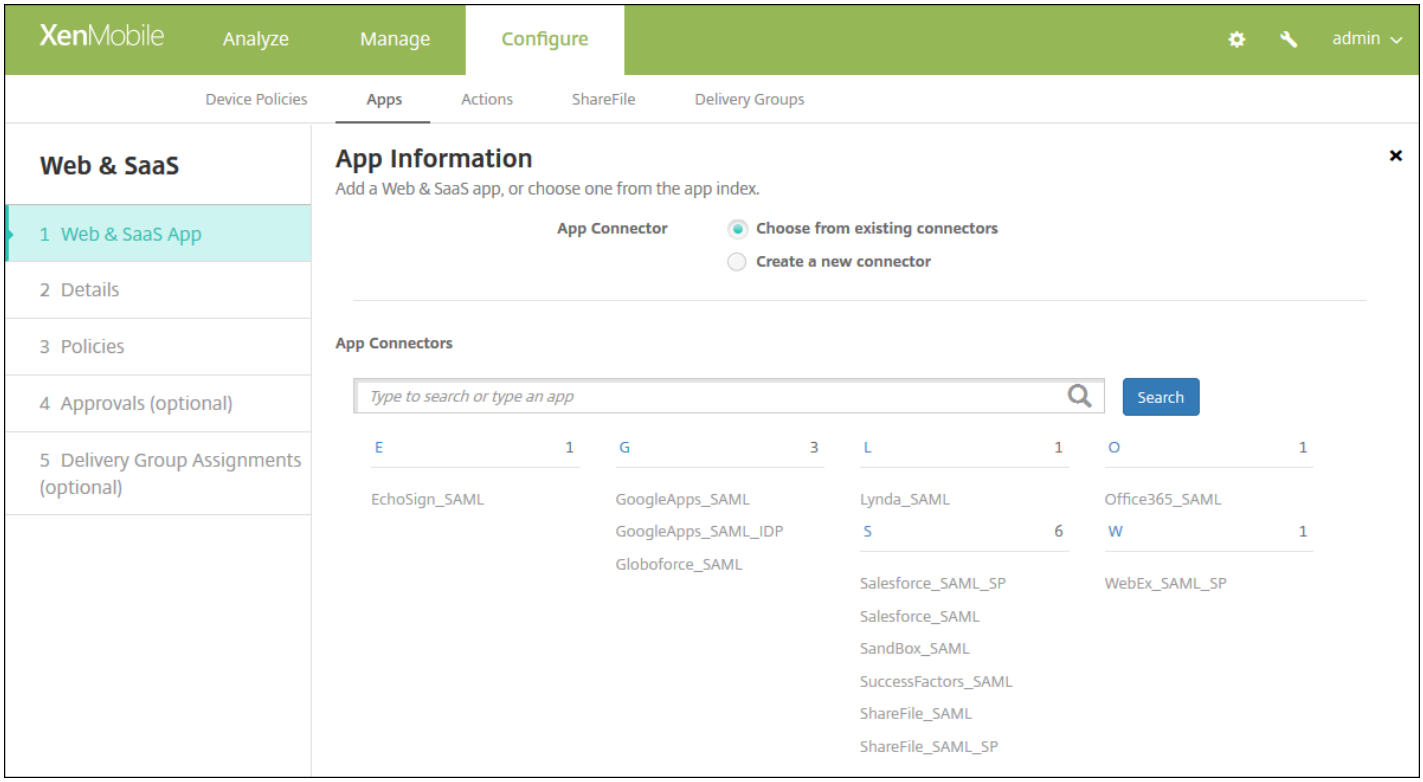
Si una aplicación solo está disponible para SSO, al finalizar la configuración de los parámetros anteriores, guárdelos para que la aplicación aparezca en la ficha **Apps** de la consola de XenMobile.

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Se abrirá la página **Apps**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



3. Haga clic en **Web & SaaS**. Aparecerá la página **App Information**.



4. Configure los siguientes parámetros:

- **App Connector**. Haga clic en **Choose from existing connector** o en **Create a new connector**. El valor

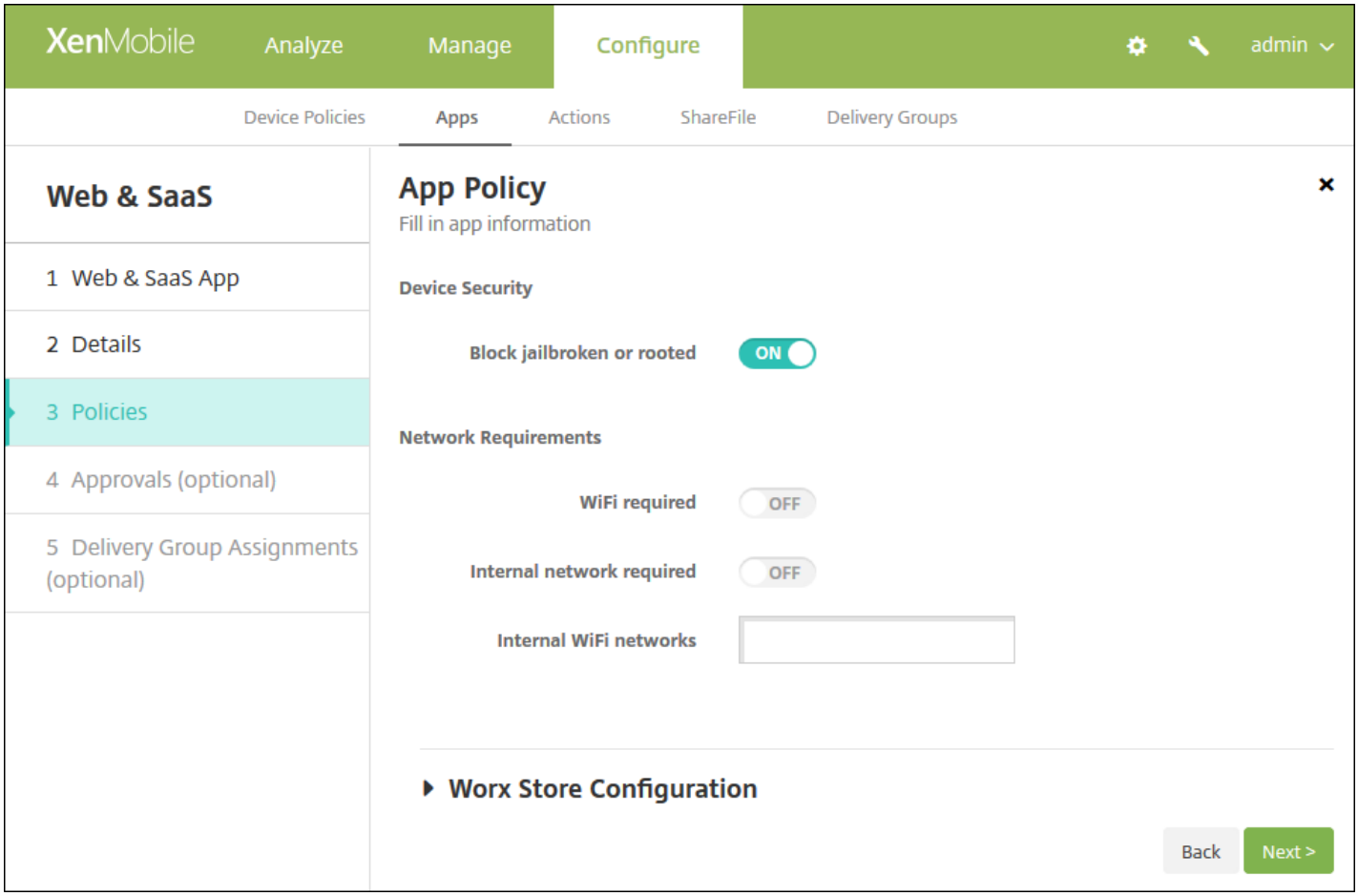
predeterminado es **Choose from existing connector**.

- Si hace clic en **Create a new connector**, aparecen campos que le permiten definir el nuevo conector.
  - Configure estos parámetros:
    - **Name**. Escriba un nombre para el conector. Este campo es obligatorio.
    - **Description**. Escriba una descripción para el conector. Este campo es obligatorio.
    - **Logon URL**. Escriba o copie y pegue la URL donde los usuarios inician sesión en el sitio. Este campo es obligatorio.
    - **SAML version**. Seleccione 1.1 o 2.0. El valor predeterminado es **1.1**.
    - **Entity ID**. Escriba la identidad de la aplicación SAML.
    - **Relay State URL**. Escriba la dirección Web de la aplicación SAML. Esta URL es la URL de respuesta de la aplicación.
    - **Name ID format**. Seleccione "Email Address" o "Unspecified". El valor predeterminado es **Email Address**.
    - **ACS URL**. Escriba la URL del servicio de aserción de consumidor (ACS) del proveedor de identidades o de servicios. La URL del servicio ACS proporciona a los usuarios Single Sign-On (SSO).
    - **Image**. Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es Use default.
      - Si quiere cargar su propia imagen, haga clic en **Browse**, vaya a la ubicación del archivo y selecciónela. El archivo debe ser PNG. No puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.
  - Haga clic en **Agregar**. Aparecerá la página **Details**.
- Si hace clic en **Choose from existing connector** o en **Add** después de configurar un nuevo conector, aparecerá la página **Details**.
- Configure estos parámetros:
  - **App name**. Acepte el nombre que ya aparece o escriba uno nuevo.
  - **App description**. Acepte la descripción que ya aparece o escriba una propia.
  - **URL**. Acepte la URL que ya aparece o escriba la dirección Web de la aplicación. Según el conector que elija, este campo puede contener un marcador de posición que se debe reemplazar antes de pasar a la siguiente página.
  - **Domain name**. Si es necesario, escriba el nombre de dominio de la aplicación. Este campo es obligatorio.
  - **App is hosted in internal network**. Seleccione 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. El valor predeterminado es **OFF**.
  - **App category**. En la lista, si quiere, haga clic en una categoría para aplicarla a la aplicación.
  - **User account provisioning**. Seleccione si quiere crear cuentas de usuario para la aplicación. Si usa el conector Globoforce_SAML, debe habilitar esta opción para garantizar una integración correcta del inicio de sesión SSO.
  - Si habilita **User account provisioning**, configure los siguientes parámetros:
    - **Service Account**
      - **App Name**. Escriba el nombre del administrador de la aplicación. Este campo es obligatorio.
      - **Password**. Escriba la contraseña del administrador. Este campo es obligatorio.
    - **Cuenta de usuario**
      - **When user entitlement ends**. En la lista, haga clic en la acción que se debe realizar cuando los usuarios ya no pueden acceder a la aplicación. El valor predeterminado es **Disable account**. Las opciones posibles son:
        - Disable account
        - Keep account
        - Remove account
    - **User Name Rule**
      - Para cada regla de nombre de usuario que quiera agregar, haga lo siguiente:
        - **User attributes**. En la lista, haga clic en el atributo de usuario que quiere agregar a la regla.

- **Length (characters)**. En la lista, haga clic en la cantidad de caracteres del atributo de usuario que se usarán en la regla de nombre de usuario. El valor predeterminado es **All**.
- **Rule**. Cada atributo de usuario que agregue, se adjunta automáticamente a la regla de nombre de usuario.

- **Password Requirements**
  - **Length**. Escriba la longitud mínima de la contraseña de usuario. El valor predeterminado es **8**.
- **Caducidad de contraseñas**
  - **Validity (days)**. Escriba la cantidad de días durante la cual la contraseña permanecerá válida. Cualquier valor entre 0 y 90 es válido. El valor predeterminado es **90**.
  - **Automatically reset password after it expires**. Seleccione si quiere restablecer la contraseña automáticamente cuando esta caduque. El valor predeterminado es **OFF**. Si no habilita este campo, cuando las contraseñas de los usuarios caduquen, no podrán abrir la aplicación.

5. Haga clic en **Next**. Aparecerá la página **App Policy**.

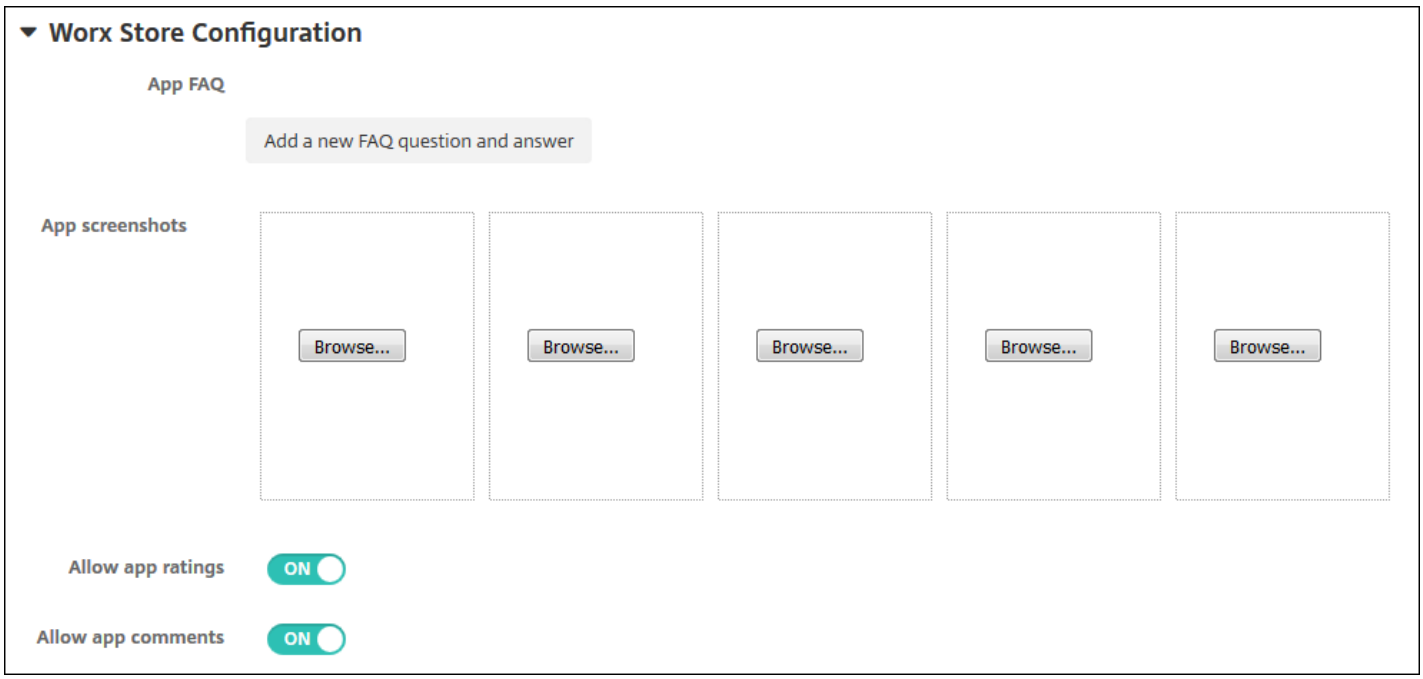


- Configure estos parámetros:
  - **Seguridad del dispositivo**
    - **Block jailbroken or rooted**. Seleccione si impedir que los dispositivos liberados por jailbreak o por root accedan a la aplicación. El valor predeterminado es **ON**.
  - **Requisitos de la red**
    - **WiFi required**. Seleccione si se necesita una conexión WiFi para ejecutar la aplicación. El valor predeterminado es **OFF**.
    - **Internal network required**. Seleccione si se necesita una red interna para ejecutar la aplicación. El valor

predeterminado es **OFF**.

- **Internal WiFi networks**. Si ha habilitado **WiFi required**, escriba las redes WiFi internas que se van a usar.

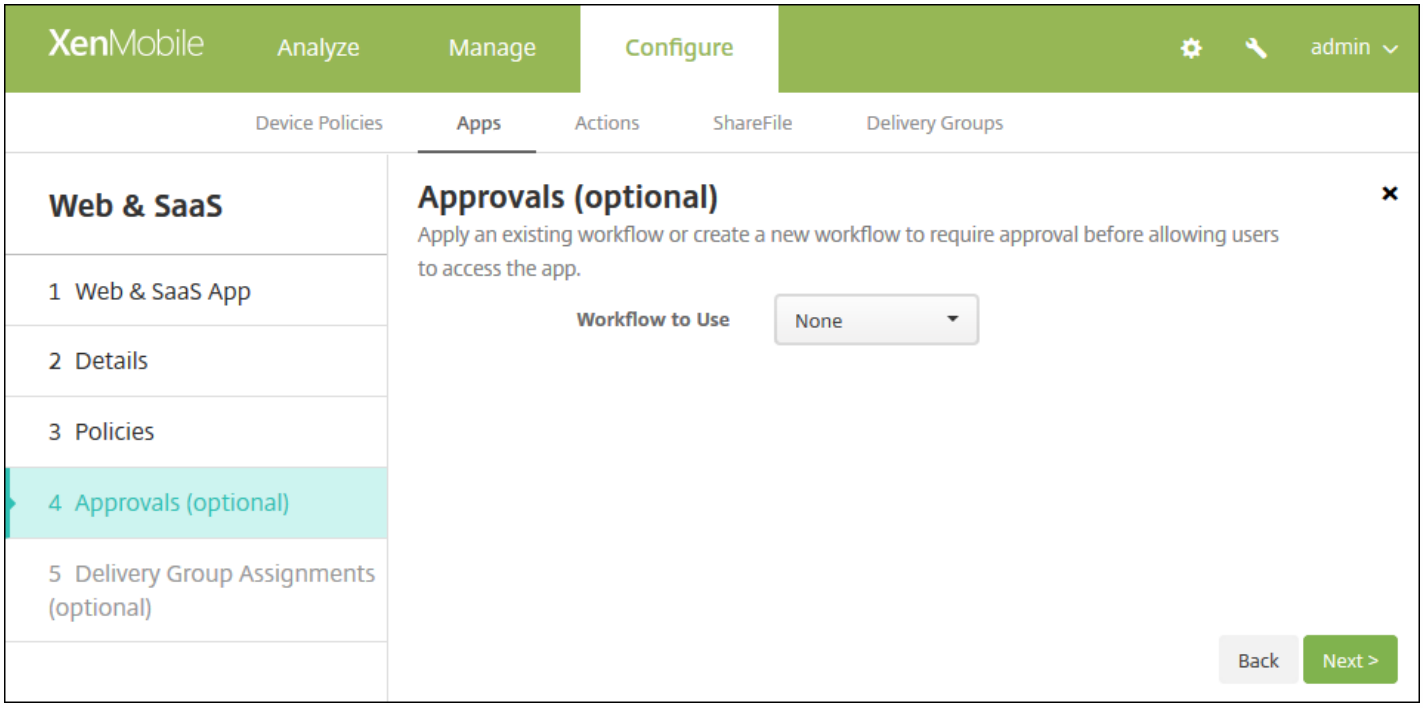
6. Expanda **Worx Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en Worx Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **App FAQ**. Agregue una sección de preguntas frecuentes sobre la aplicación junto con sus respuestas.
  - **App screenshots**. Agregue capturas de pantalla para ayudar a clasificar la aplicación en Worx Store. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Allow app ratings**. Seleccione si permitir a los usuarios puntuar la aplicación. El valor predeterminado es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

7. Haga clic en **Next**. Aparecerá la página **Approvals**.



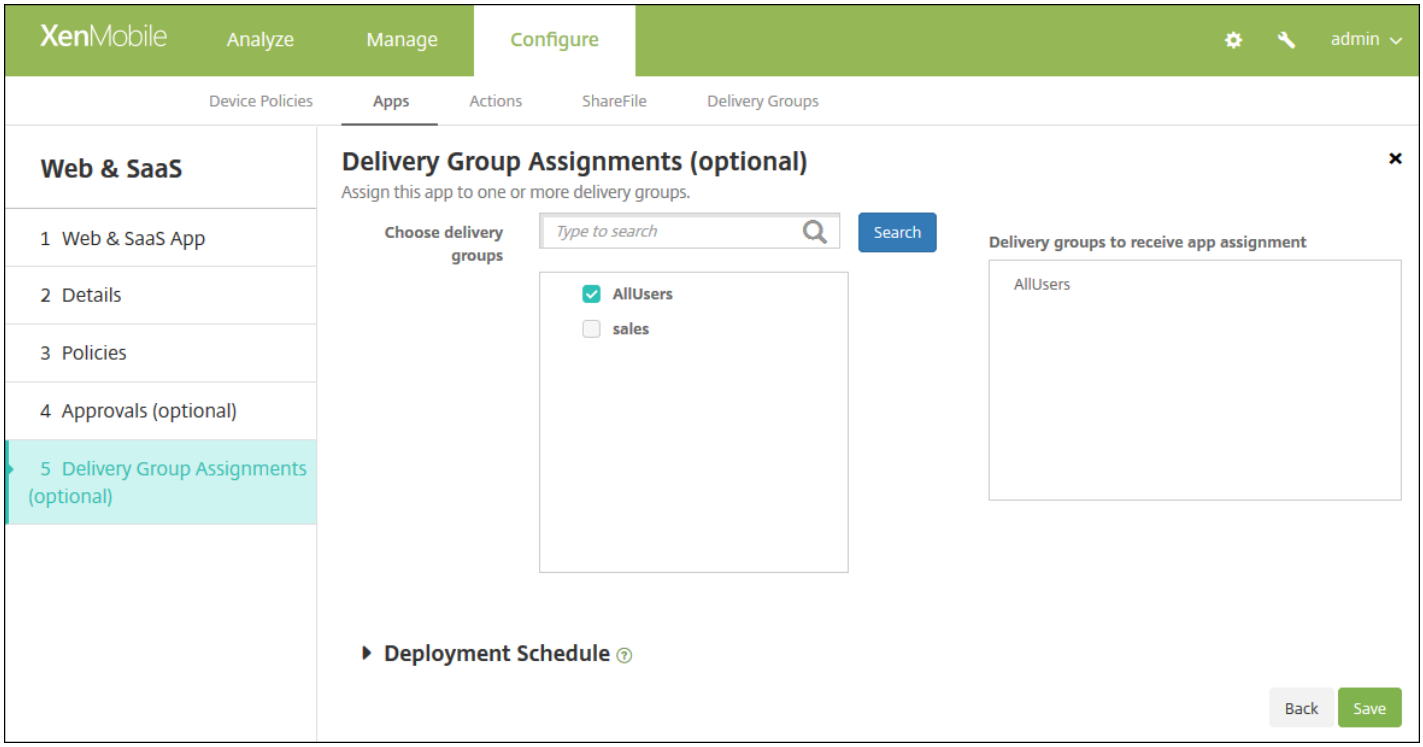
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 8.

Configure este parámetro si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use**. En la lista, haga clic en un flujo de trabajo existente o en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name**. Escriba un nombre único para el flujo de trabajo.
  - **Description**. Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates**. En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval**. En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - 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.

8. Haga clic en **Next**. Aparecerá la página **Delivery Group 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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**.

Lista de tipos de conectores de aplicaciones

Jul 27, 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

Incorporación de aplicaciones de empresa a XenMobile

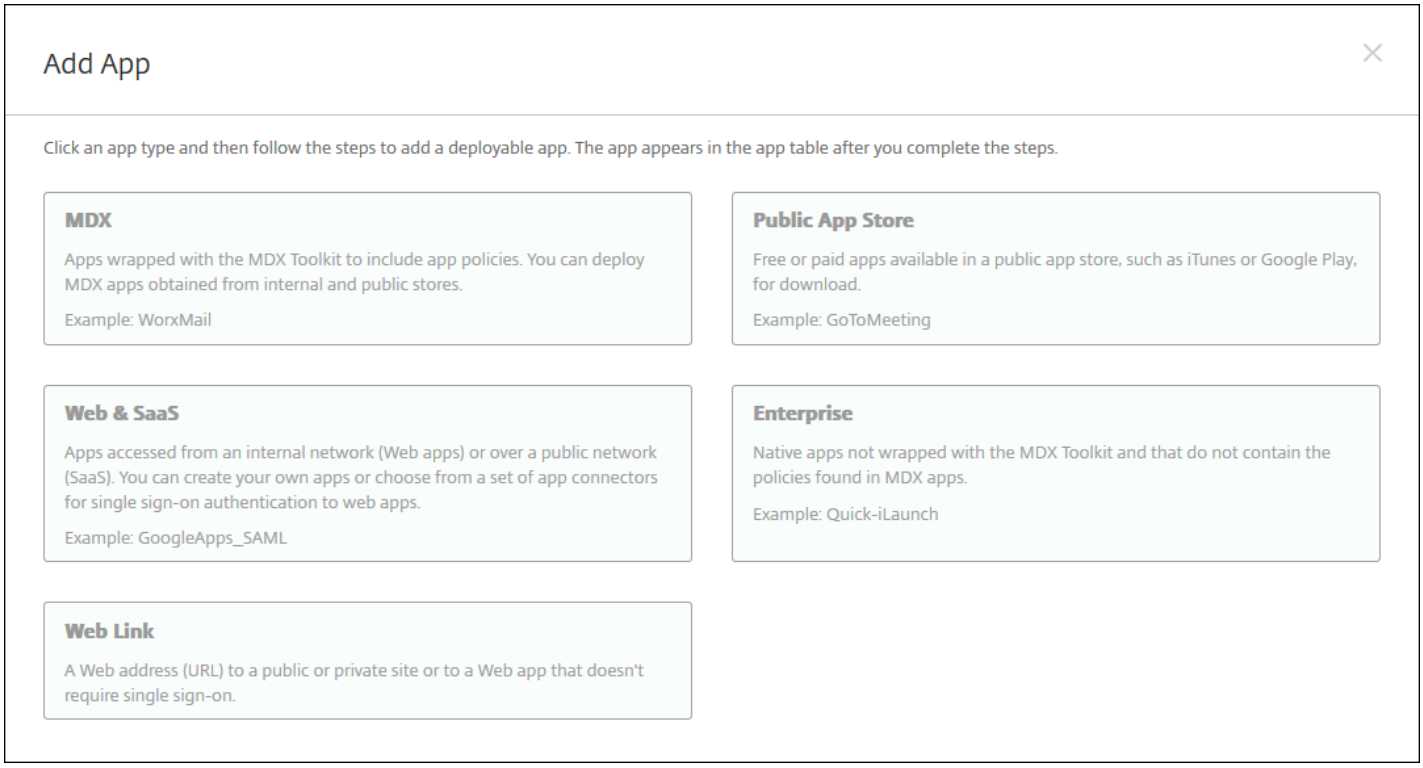
Jul 27, 2016

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):

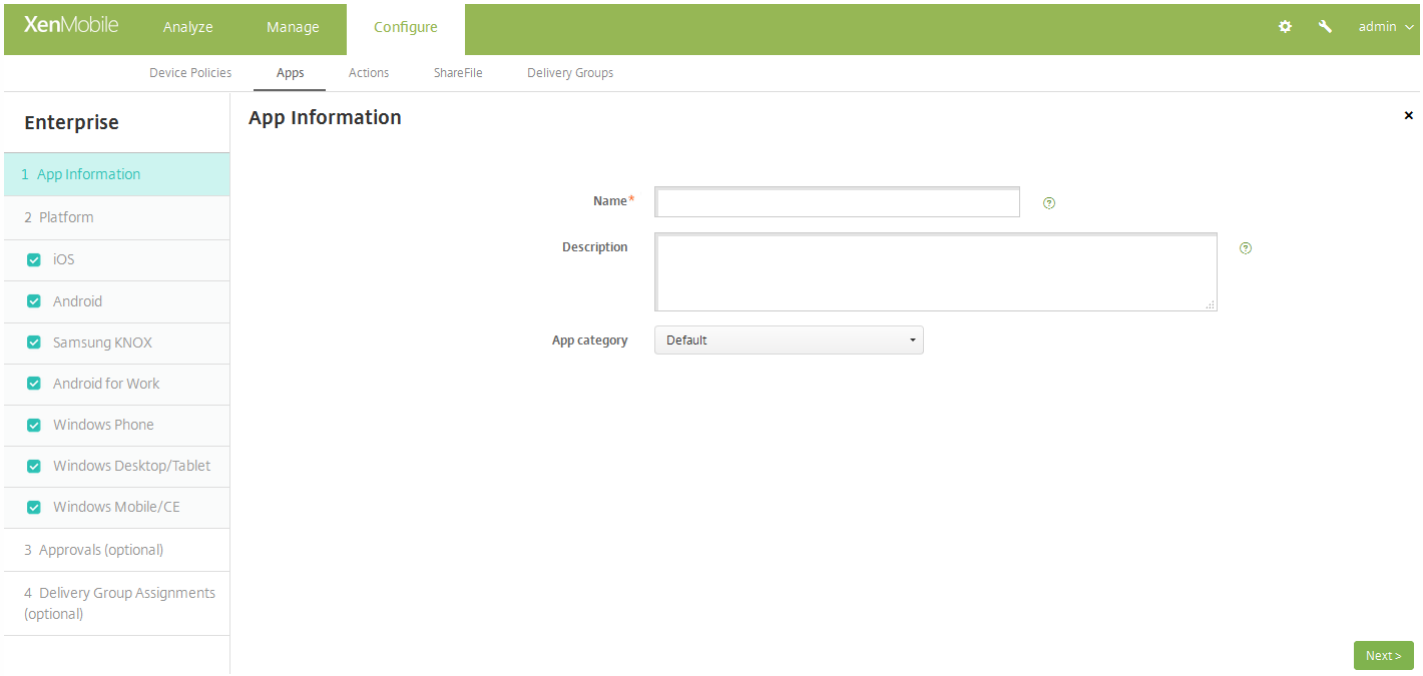
- iOS (archivo .ipa)
- Android (archivo .apk)
- Samsung KNOX (archivo .apk)
- Android for Work (archivo .apk)
- Windows Phone (archivo .xap o .appx)
- Tableta Windows (archivo .appx)
- Windows Mobile/CE (archivo .cab)

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Se abrirá la página **Apps**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



3. Haga clic en **Enterprise**. Aparecerá la página **App Information**.



4. En el panel **App Information**, escriba la información siguiente:

- **Name**. Escriba un nombre descriptivo para la aplicación. Este figurará en App Name, en la tabla Apps.
- **Description**. Escriba, si quiere, una descripción de la aplicación.
- **App category**. Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Creación de categorías de aplicaciones en XenMobile.

5. Haga clic en **Next**. Aparecerá la página **App Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 10 para la configuración de las reglas de implementación de esa plataforma.

7. Elija un archivo que cargar por cada plataforma seleccionada. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

8. Haga clic en **Next**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.

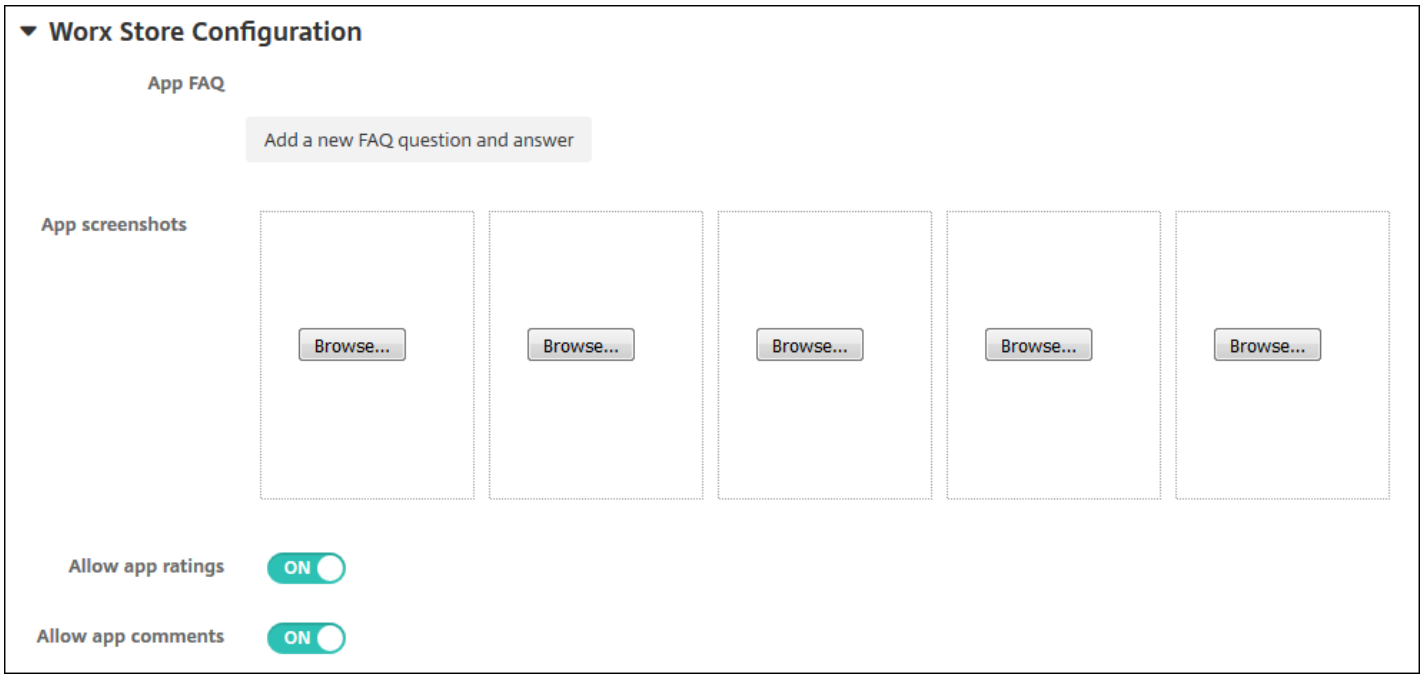
9. Configure los parámetros para el tipo de plataforma, como:

- **File name**. Si quiere, escriba un nuevo nombre para la aplicación.
- **App Description**. Si quiere, indique una nueva descripción de la aplicación.
- **App version**. Este campo no se puede cambiar.
- **Minimum OS version**.
- **Maximum OS version**.
- **Excluded devices**.
- **Remove app if MDM profile is removed**. Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es **ON**.

- **Prevent app data backup**. Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es **ON**.
- **Force app to be managed**. Si instala una aplicación no administrada, seleccione ON para solicitar a los usuarios de dispositivos no supervisados permiso para administrarla. Si el usuario acepta la solicitud, la aplicación se administra. Esta configuración se aplica a dispositivos iOS 9.x.

10. Configure las reglas de implementación.

11. Expanda **Worx Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en Worx Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **App FAQ**. Agregue una sección de preguntas frecuentes sobre la aplicación junto con sus respuestas.
  - **App screenshots**. Agregue capturas de pantalla para ayudar a clasificar la aplicación en Worx Store. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Allow app ratings**. Seleccione si permitir a los usuarios puntuar la aplicación. El valor predeterminado es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

12. Haga clic en **Next**. Aparecerá la página **Approvals**.

Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 13.

Configure este parámetro si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use**. En la lista, haga clic en un flujo de trabajo existente o en **Create a new workflow**. El valor predeterminado es **None**.

- Si selecciona Crear un nuevo flujo de trabajo, configure los siguientes parámetros:
  - **Name**. Escriba un nombre único para el flujo de trabajo.
  - **Description**. Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates**. En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval**. En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - 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.

13. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.

14. 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

15. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta opción se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

- 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.

16. Haga clic en **Save**.

Cómo agregar aplicaciones de enlaces Web a XenMobile

Jul 27, 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 (SSO).

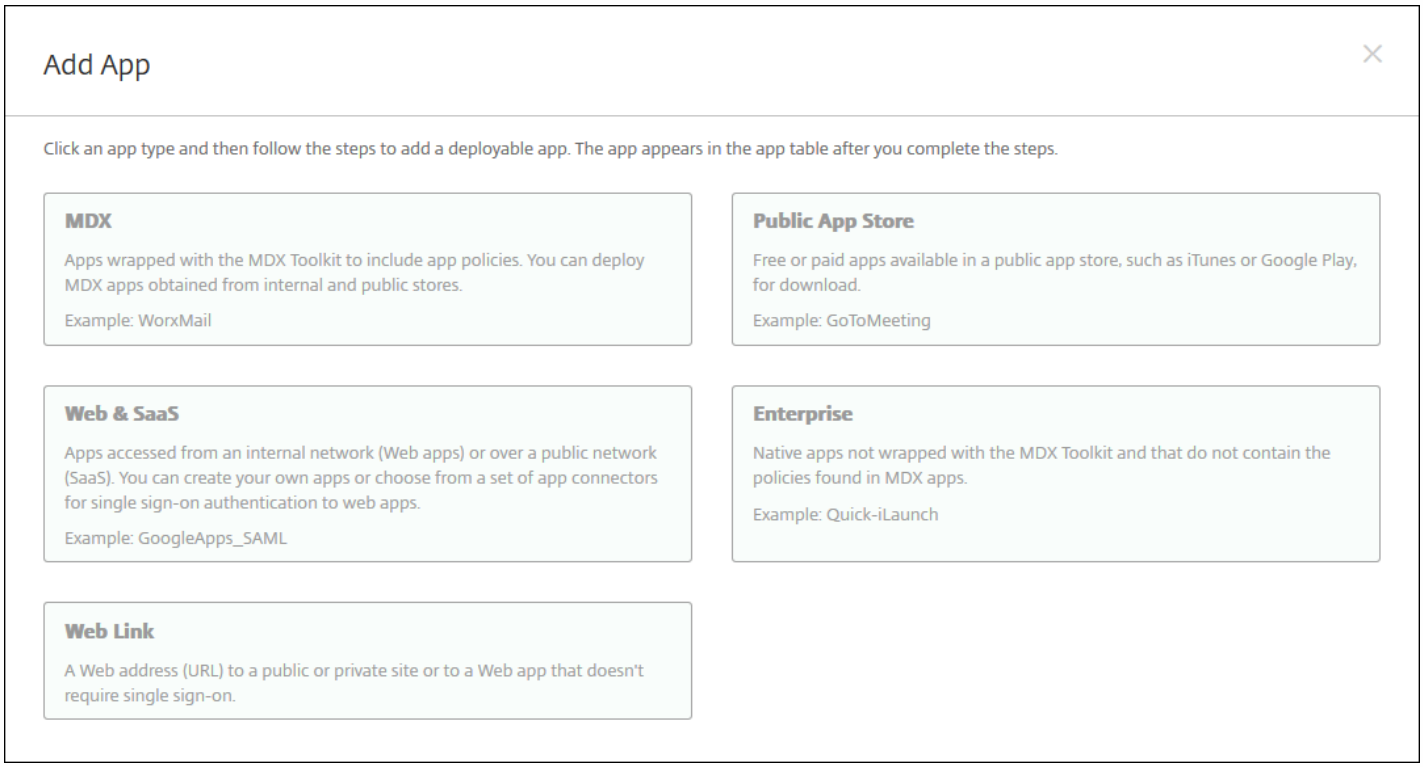
Puede configurar enlaces Web desde la ficha **Apps** de la consola de XenMobile. Una vez configurado el enlace Web, este aparece como un icono de enlace en la lista de la tabla **Apps**. Cuando los usuarios inician sesión en Worx Home, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Para agregar el enlace, debe proporcionar la siguiente información:

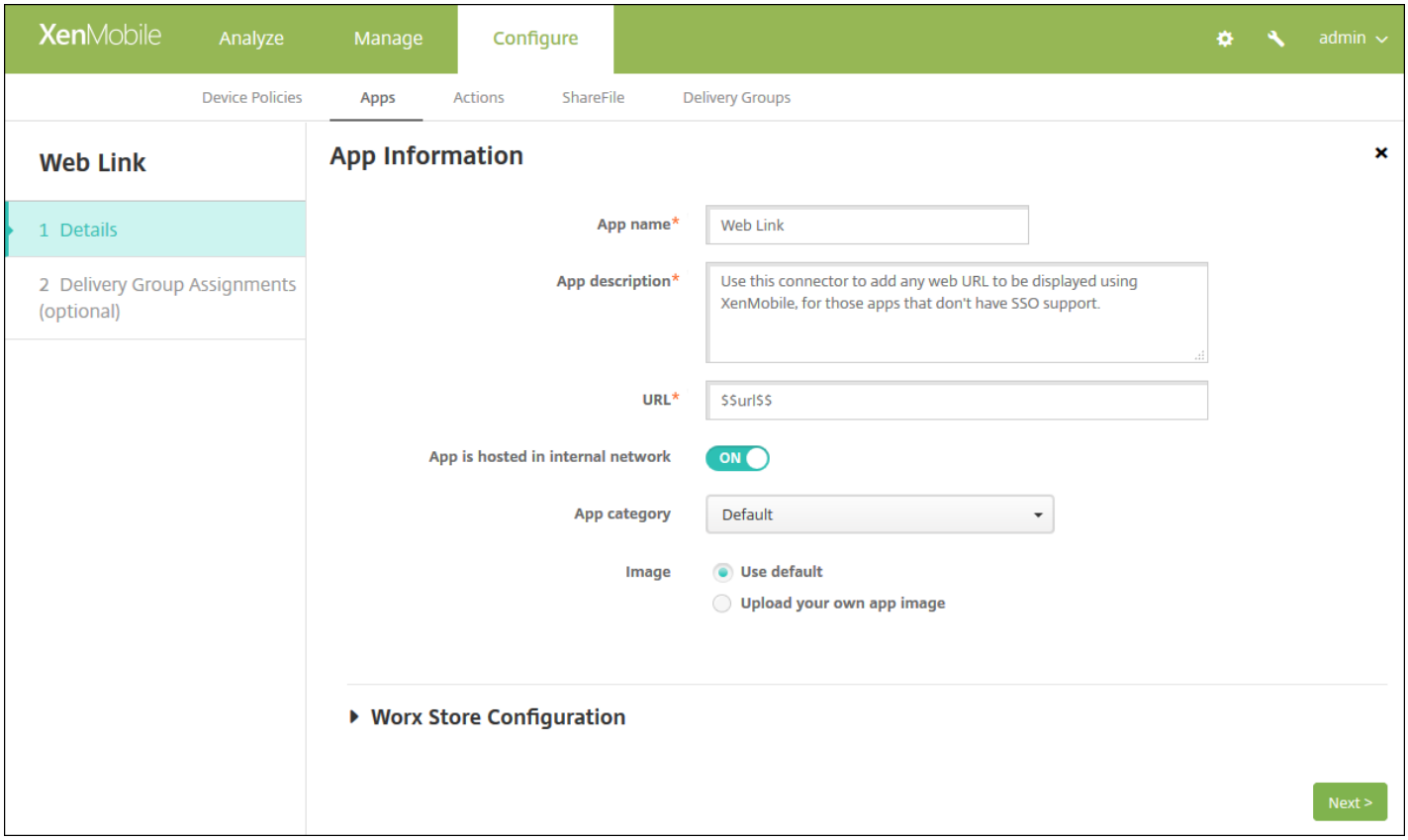
- Nombre para el enlace
- Descripción del enlace
- Dirección Web (URL)
- Categoría
- Rol
- Imagen en formato PNG (optativo)

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Aparecerá la página **Apps**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



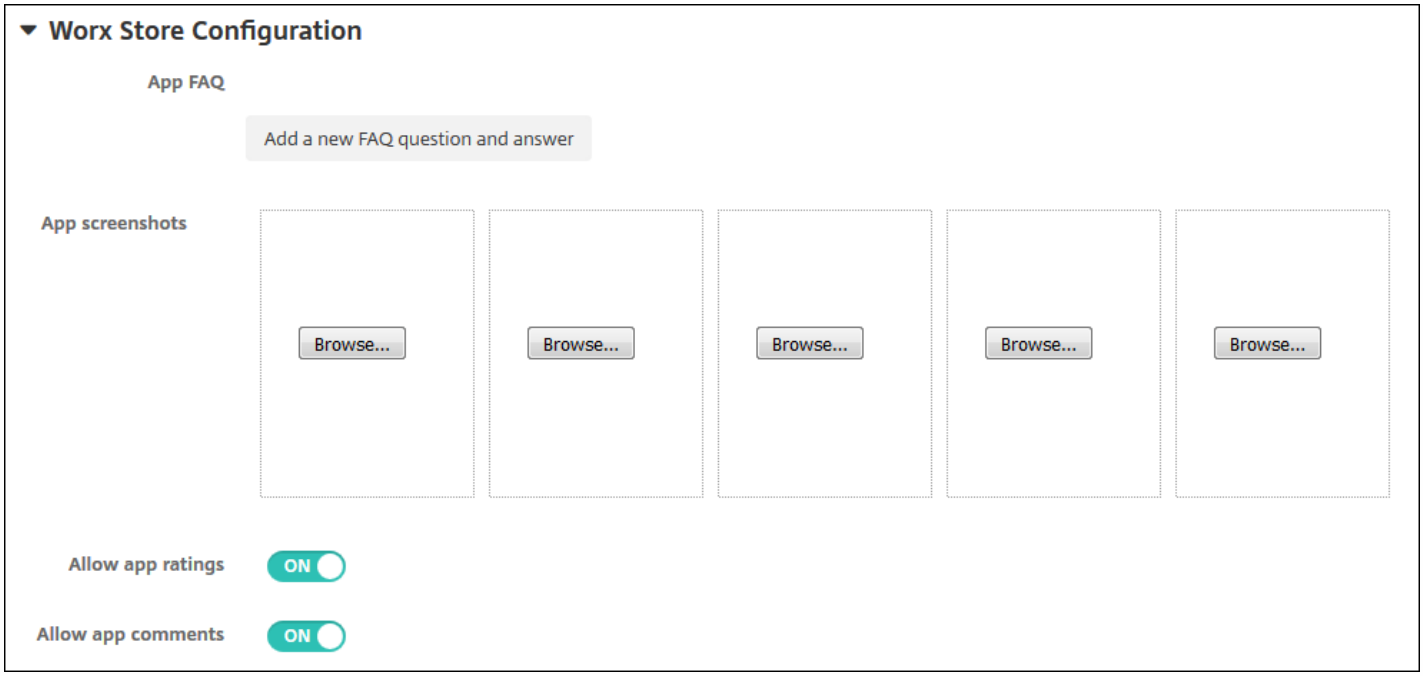
3. Haga clic en **Web Link**. Aparecerá la página **App Information**.



4. Configure los siguientes parámetros:

- **App name**. Acepte el nombre que ya aparece o escriba uno nuevo.
- **App description**. Acepte la descripción que ya aparece o escriba una propia.
- **URL**. Acepte la URL que ya aparece o escriba la dirección Web de la aplicación. Según el conector que elija, este campo puede contener un marcador de posición que se debe reemplazar antes de pasar a la siguiente página.
- **App is hosted in internal network**. Seleccione 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. El valor predeterminado es **OFF**.
- **App category**. En la lista, si quiere, haga clic en una categoría para aplicarla a la aplicación.
- **Image**. Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es Use default.
  - Si quiere cargar su propia imagen, haga clic en **Browse**, vaya a la ubicación del archivo y selecciónela. El archivo debe ser PNG. No puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

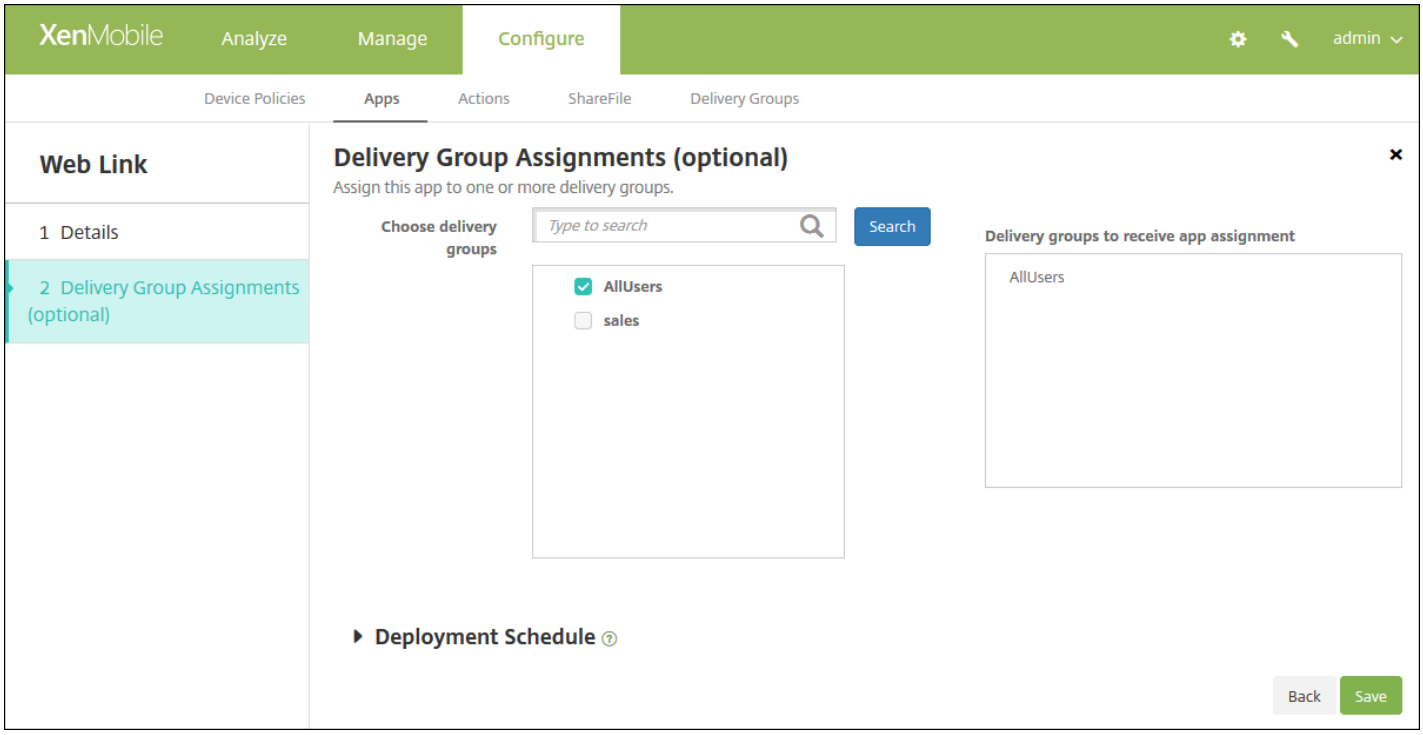
5. Expanda **Worx Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en Worx Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **App FAQ**. Agregue una sección de preguntas frecuentes sobre la aplicación junto con sus respuestas.
  - **App screenshots**. Agregue capturas de pantalla para ayudar a clasificar la aplicación en Worx Store. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Allow app ratings**. Seleccione si permitir a los usuarios puntuar la aplicación. El valor predeterminado es ON.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es ON.

6. Haga clic en **Next**. Aparecerá la página **Delivery Group 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 los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

8. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- 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.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- 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**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- 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**.

Creación y administración de flujos de trabajo en XenMobile

Oct 31, 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.

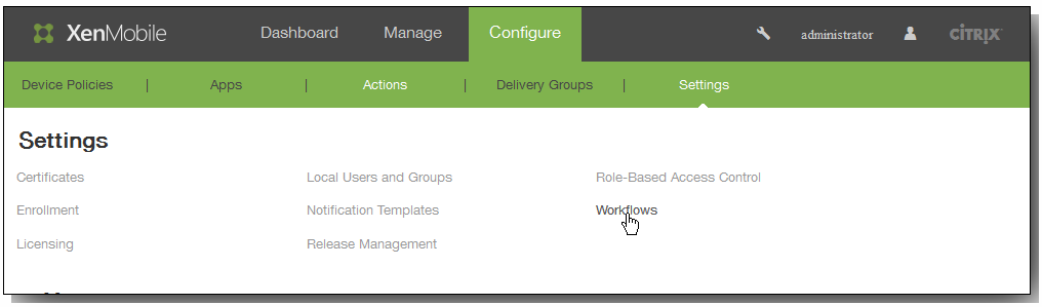
Cuando se configura XenMobile por primera vez, se definen los parámetros de correo electrónico del flujo de trabajo. Debe configurar estos parámetros para poder utilizar flujos de trabajo. Puede cambiar los parámetros de correo electrónico del flujo de trabajo en cualquier momento. Estos parámetros incluyen servidor de correo electrónico, puerto, dirección de correo electrónico, y si la solicitud para crear la cuenta de usuario requiere aprobación o no.

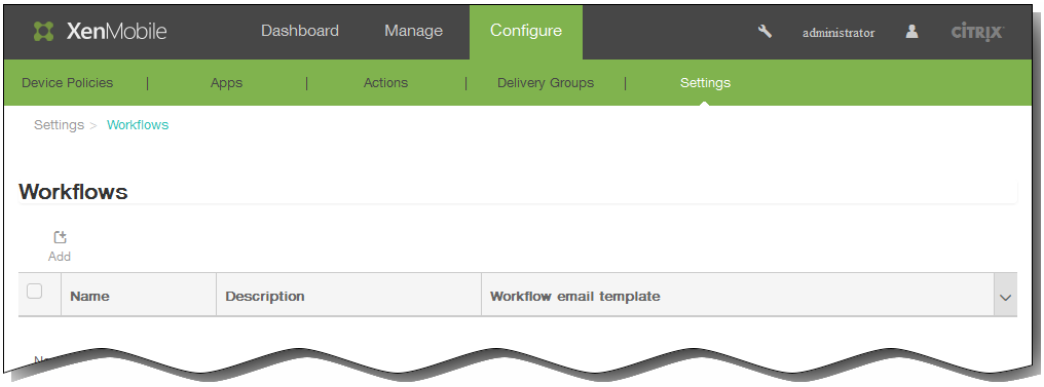
Puede configurar flujos de trabajo en dos lugares de XenMobile:

- 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.

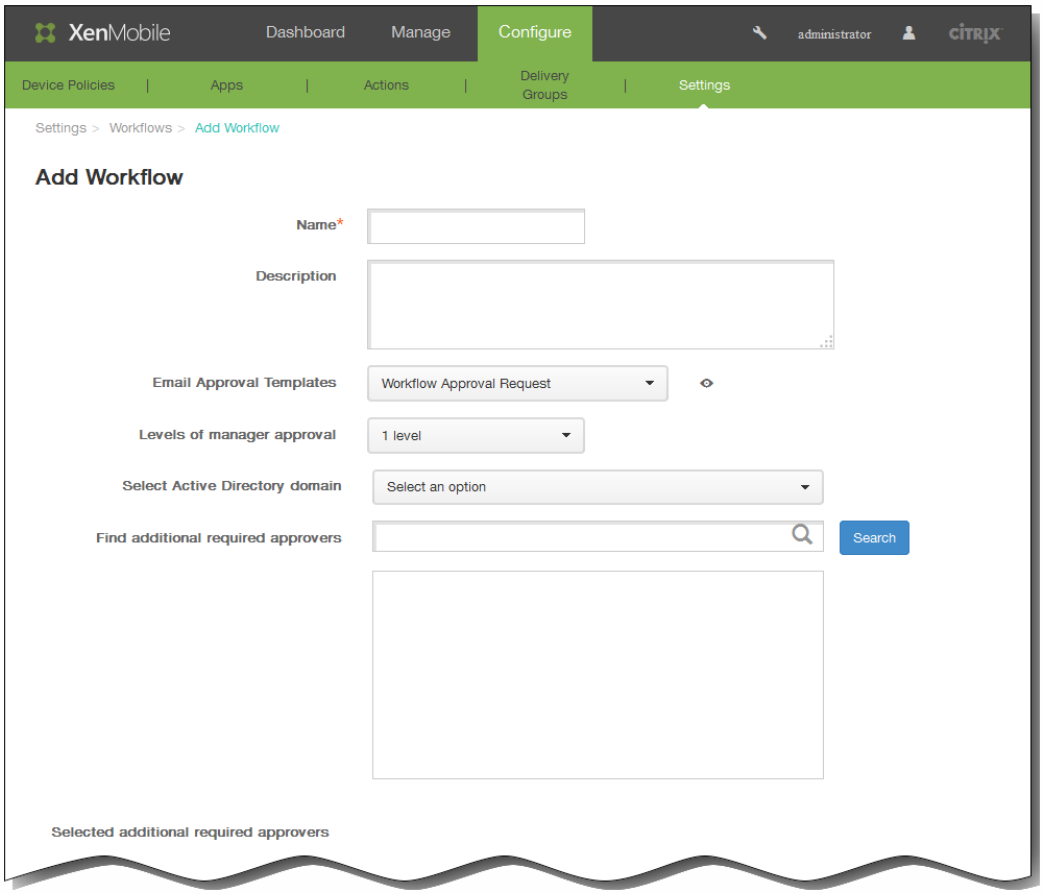
1. En la consola de XenMobile, haga clic en Configure > Settings > Workflows.





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.

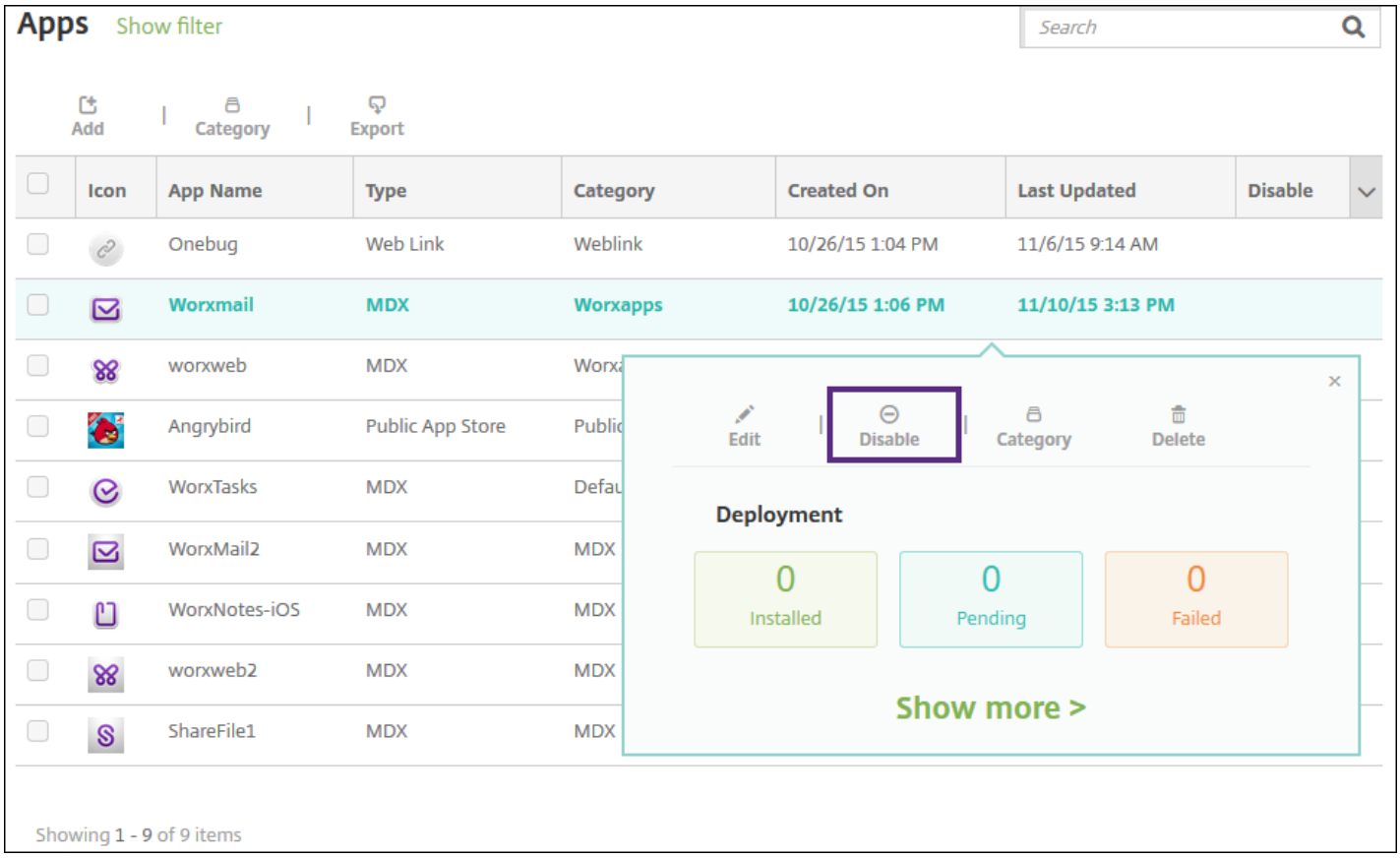
   Las personas de la lista Selected additional required approvers tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.
10. Haga clic en Save.
    El flujo de trabajo 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.

-
-

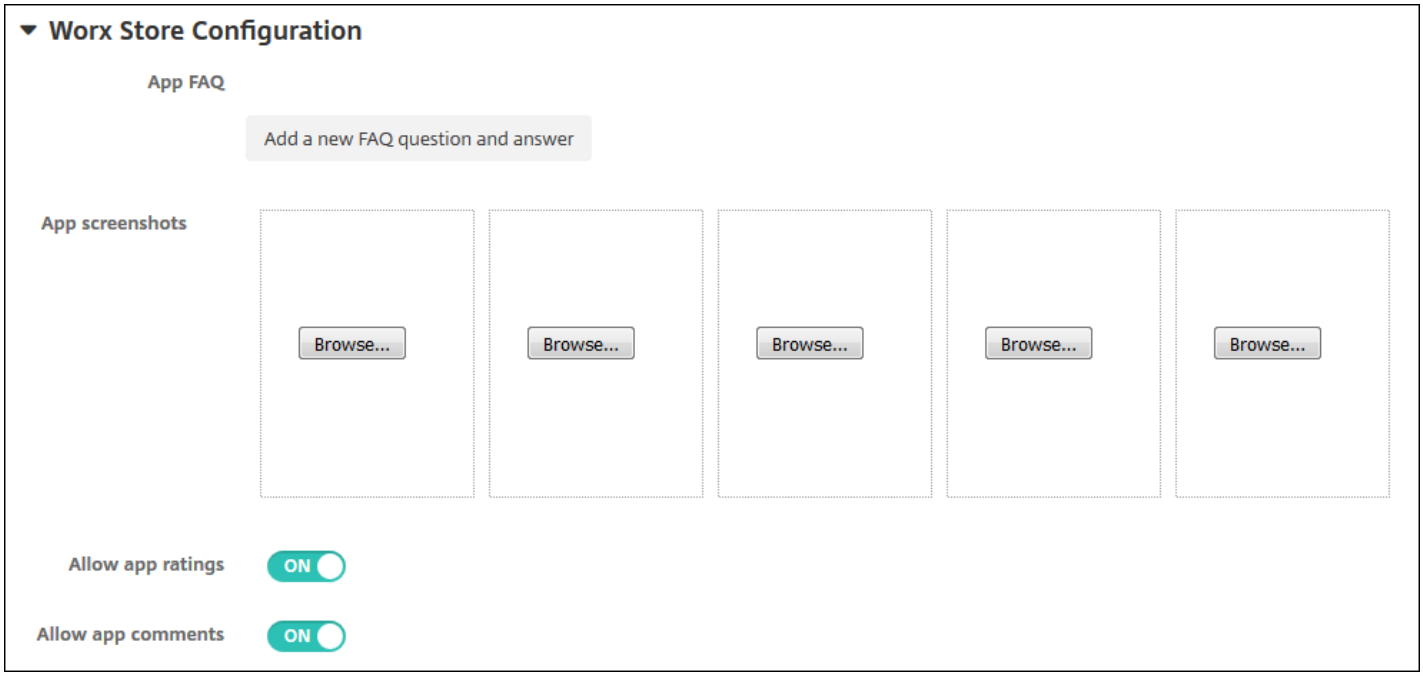


-

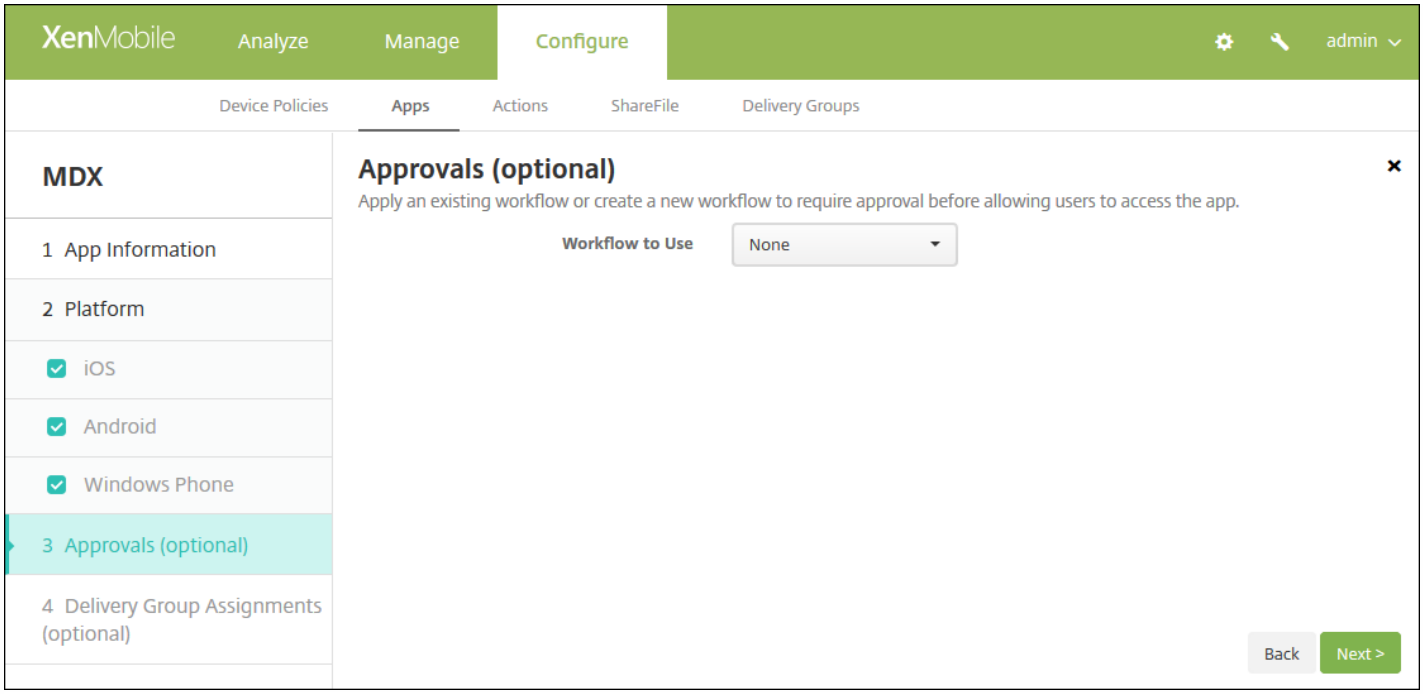
Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
	Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

-
-
-

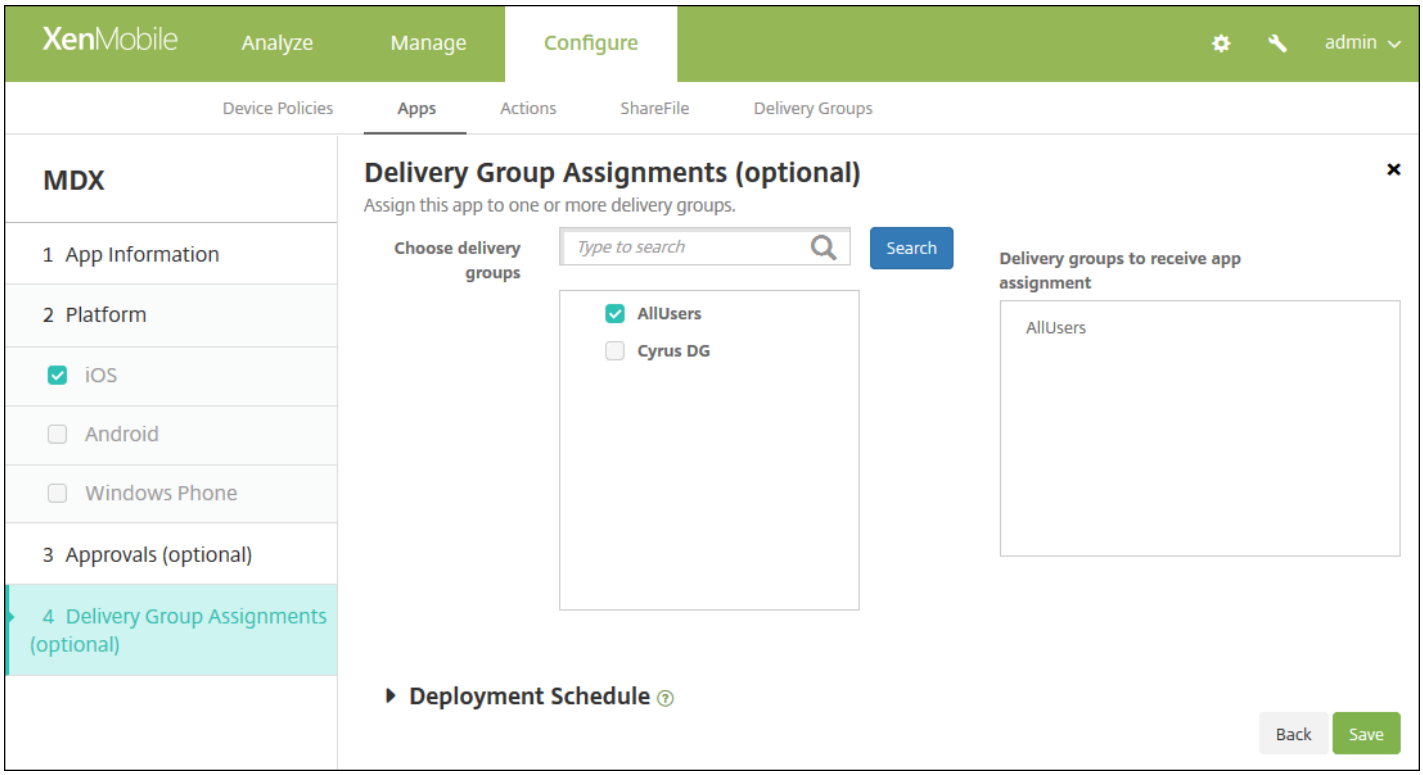
-
-



-
  -
  -
  -
  -

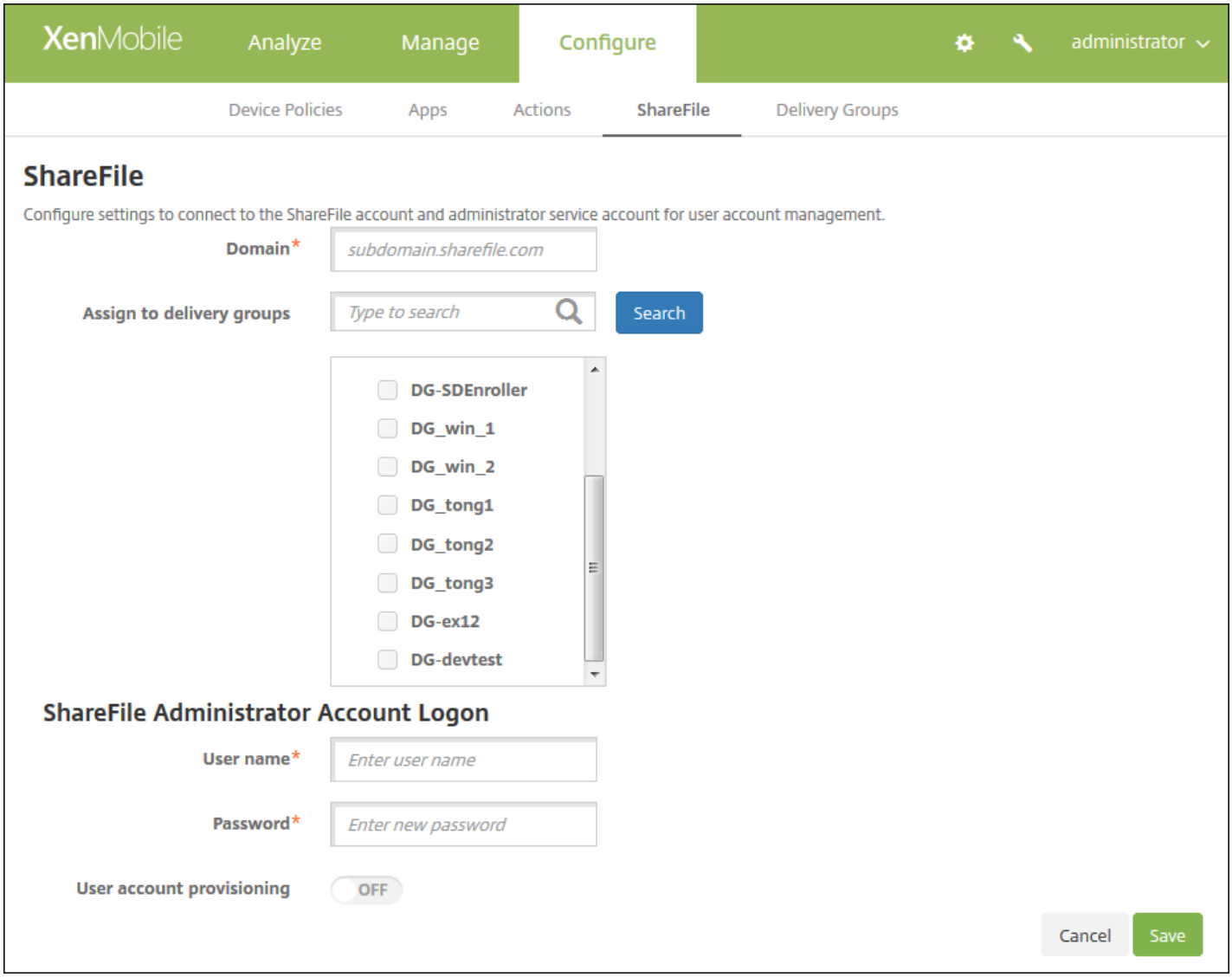


-
-
  -
  -
  -
  -
    -
    -
    -
    -
  -
  -
  -



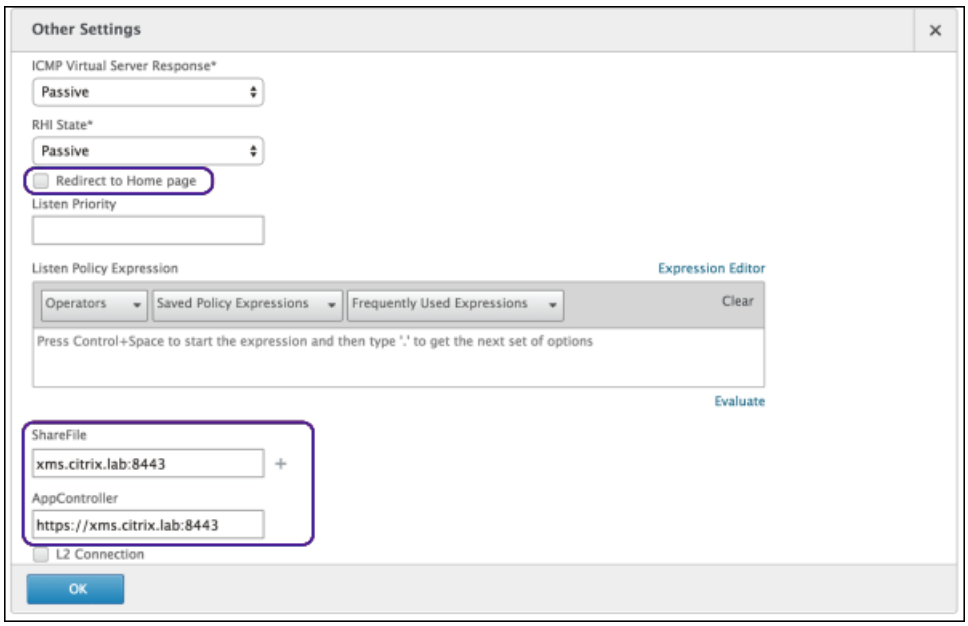
-
-
-
-

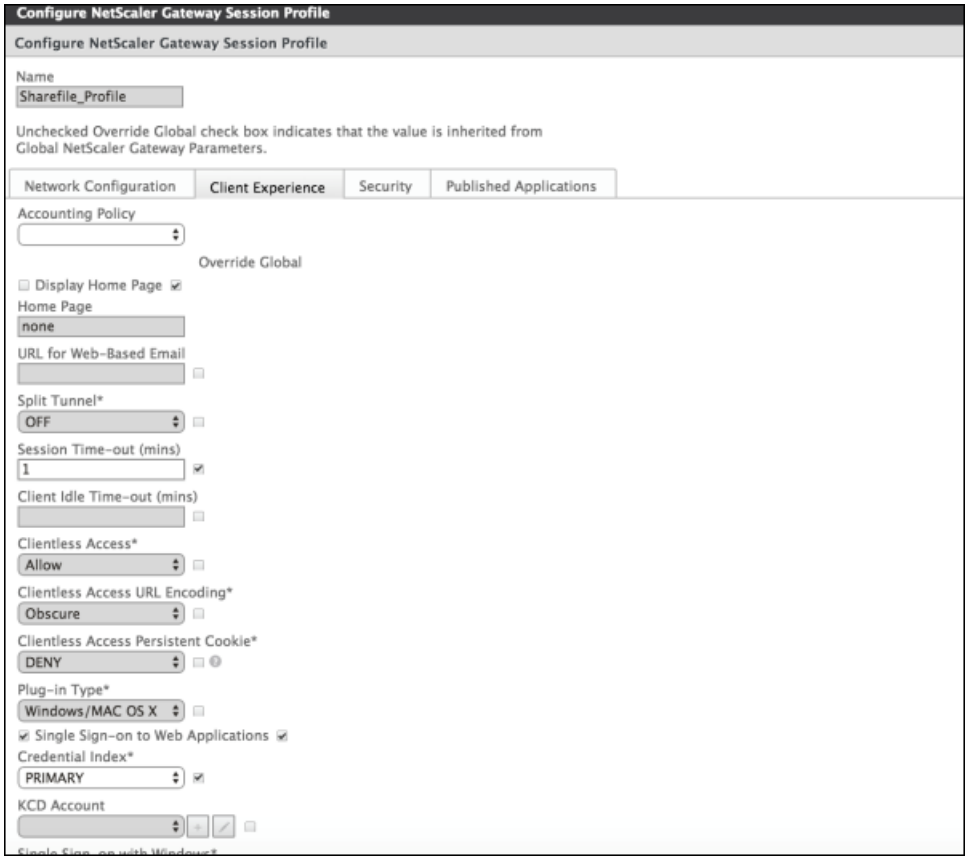
-
-
-
-
  -
  -
  -
-
-



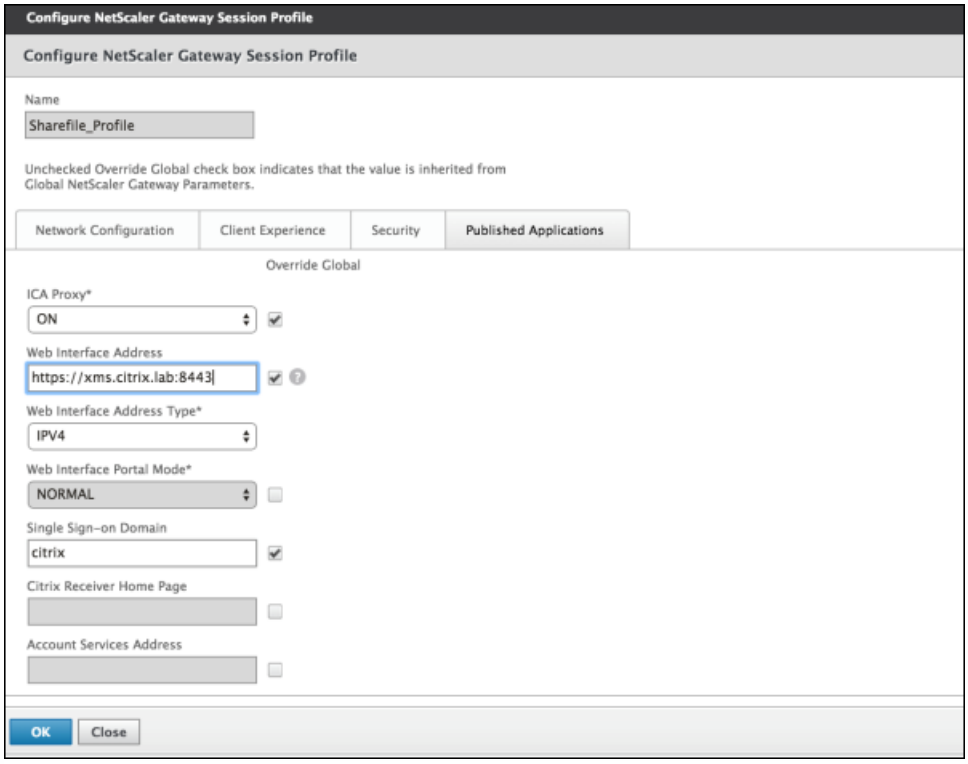
-
-
-
  -
    -
    -

-
-
-

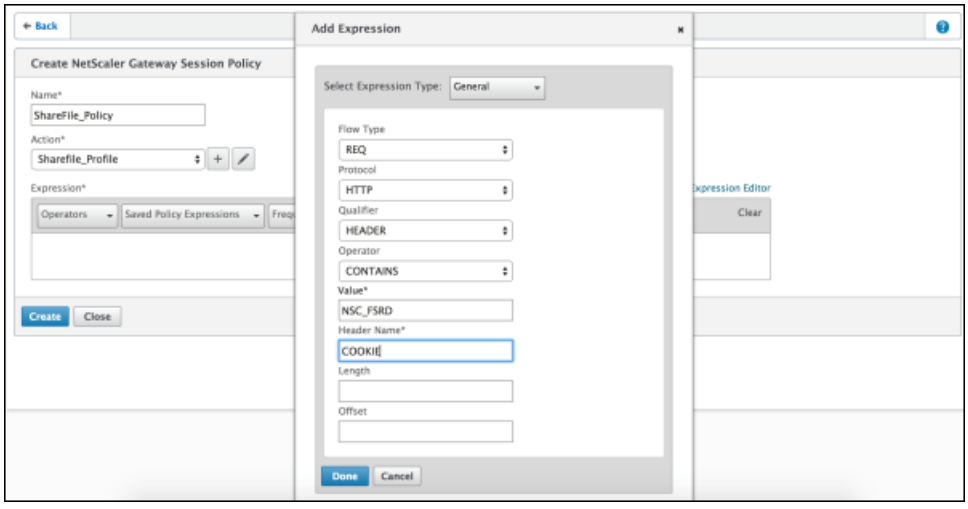




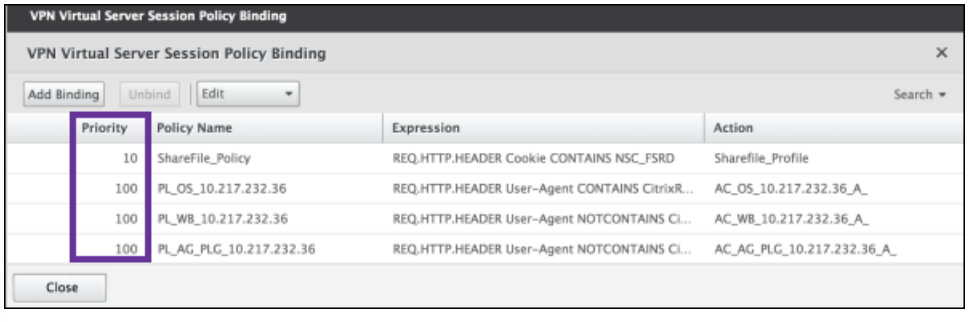
-
-
  -
  -
  -
  -
-

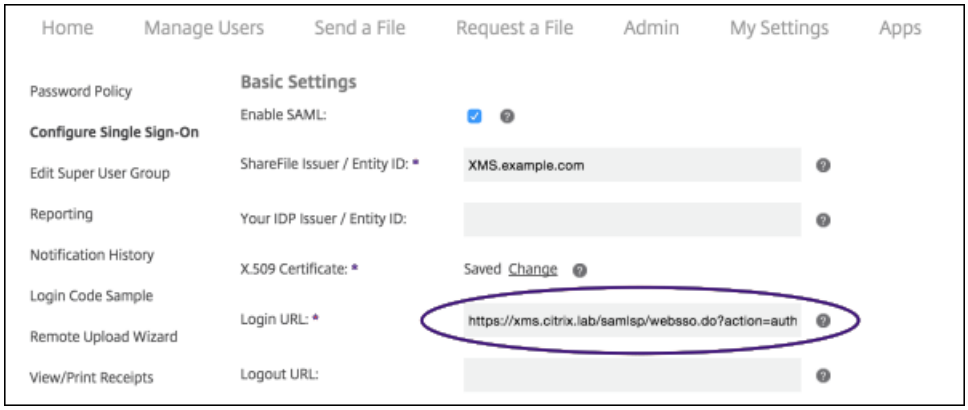


-
-
-

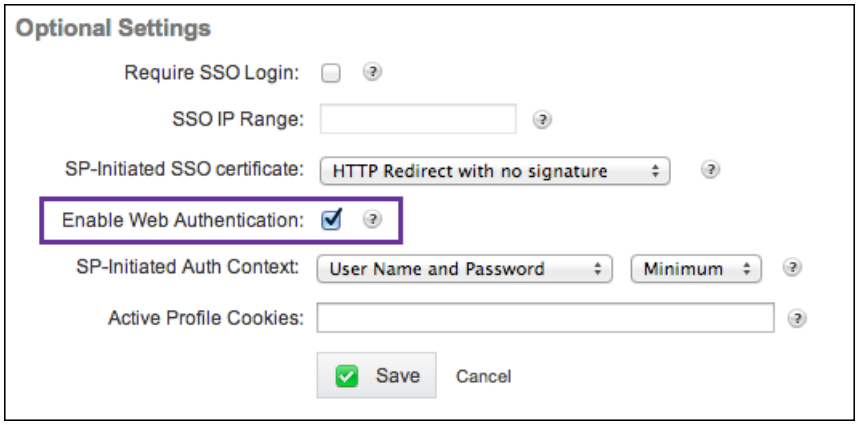


-
-
-





-
-
-



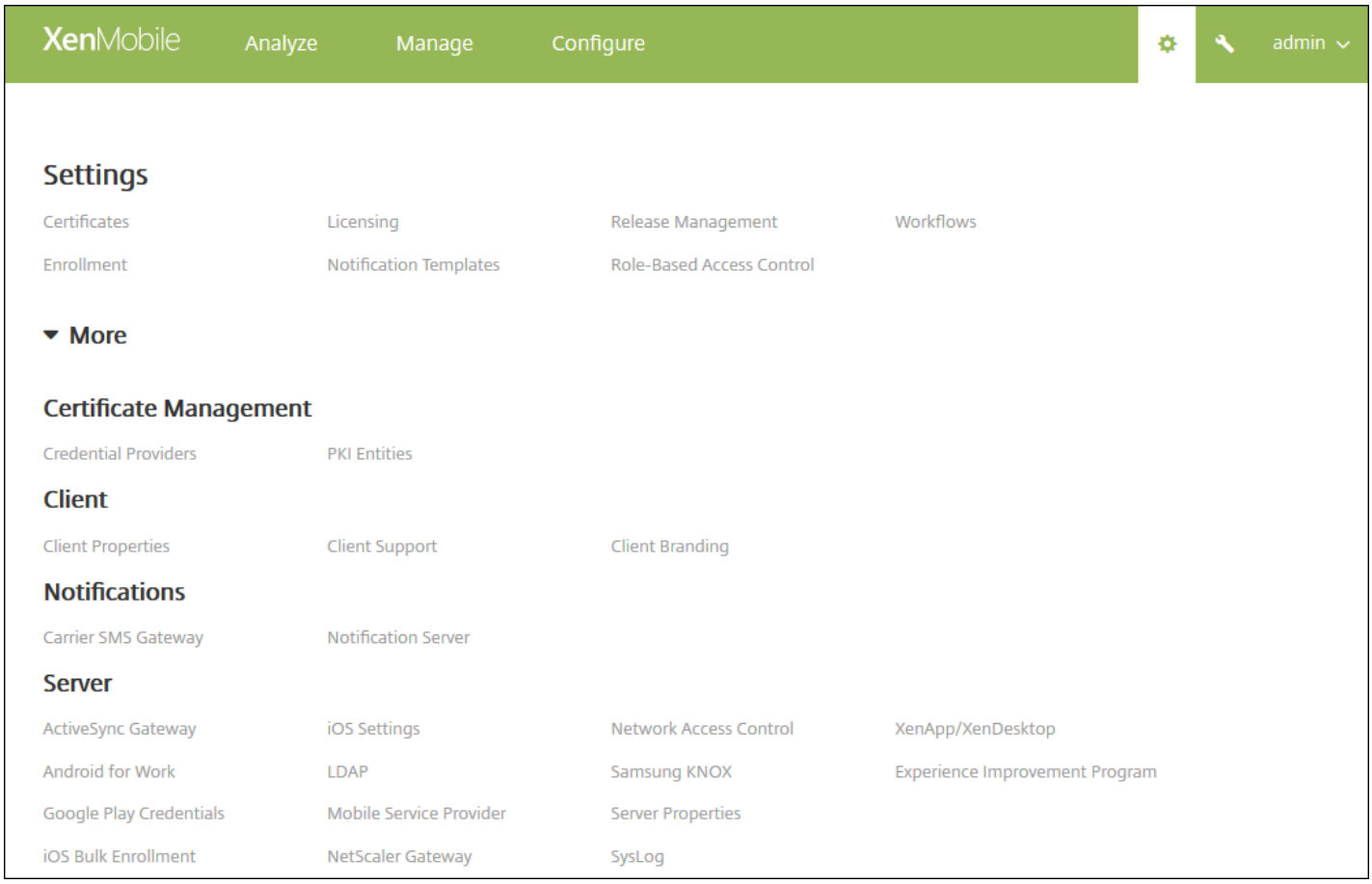
-
-
-
-

-
-

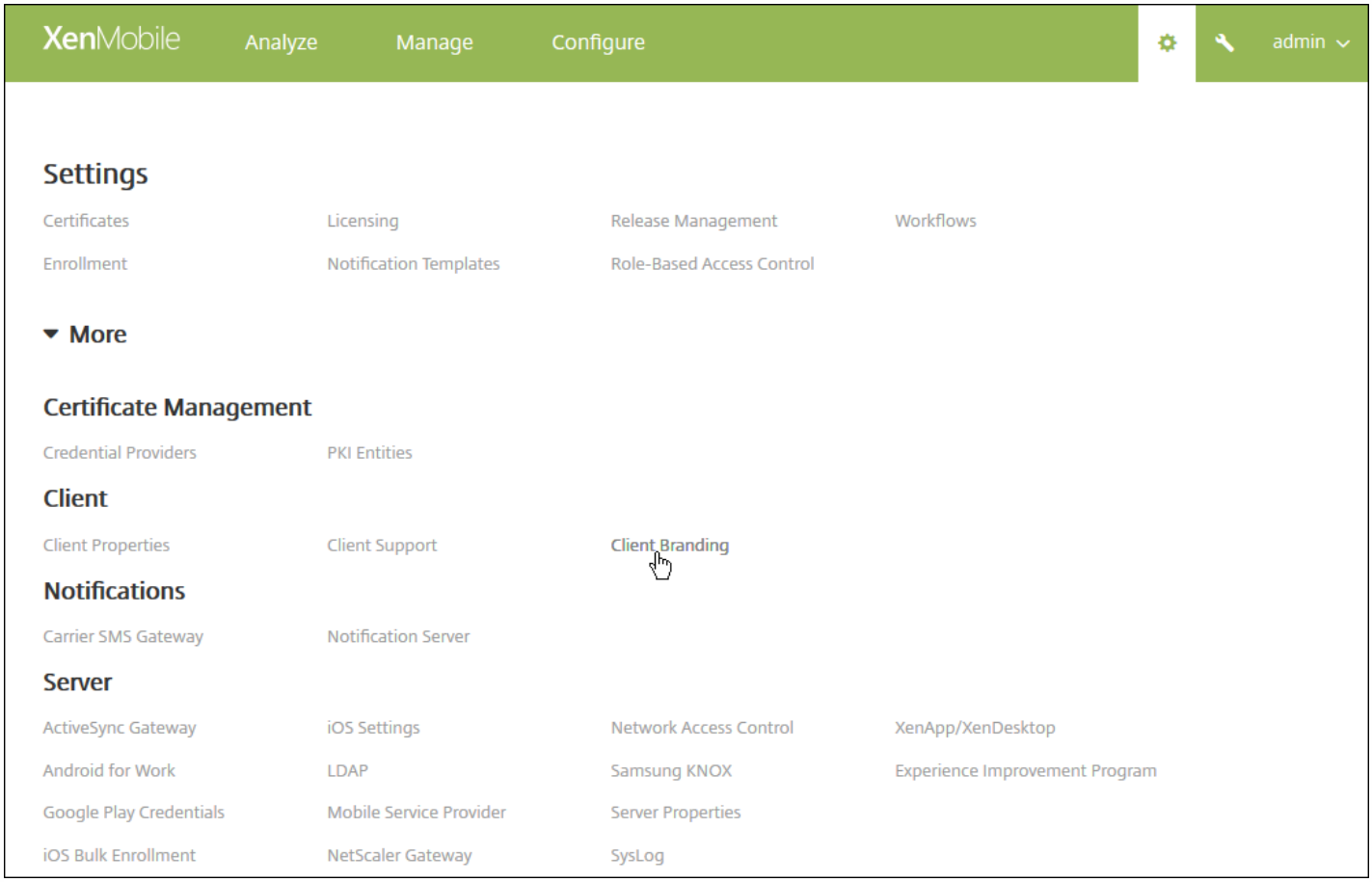
-
-

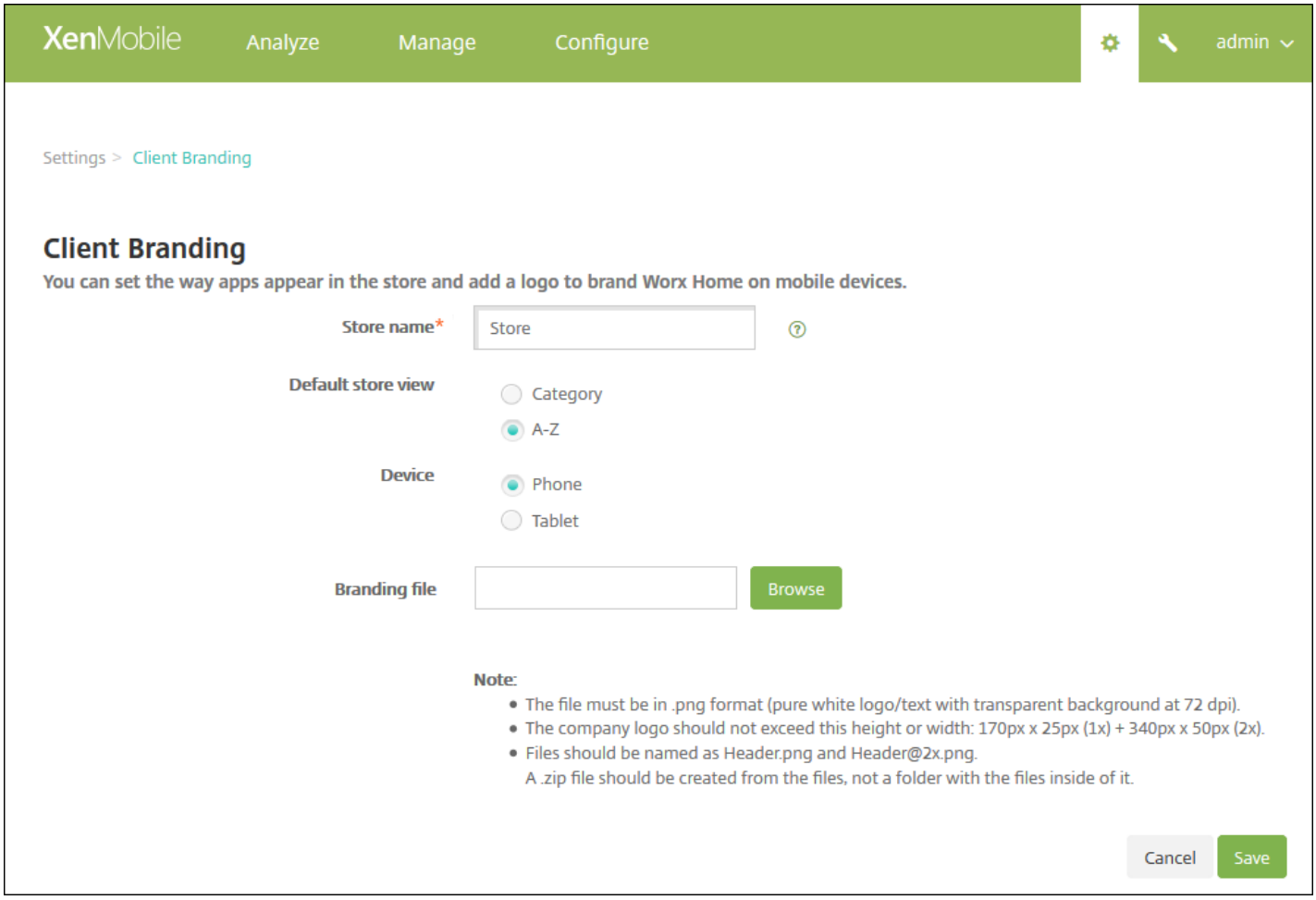
-
-
-
-
-

-
-
-

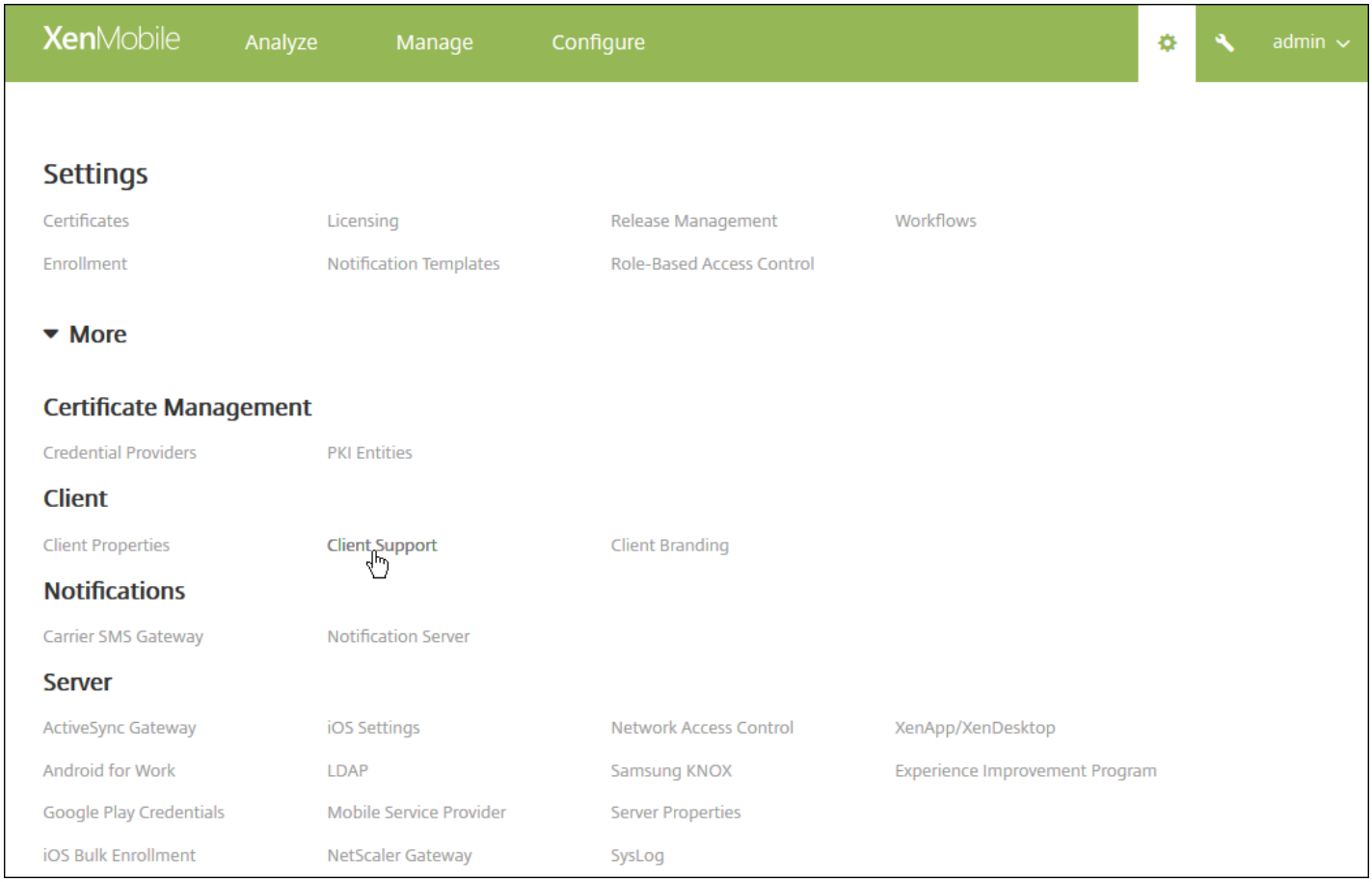


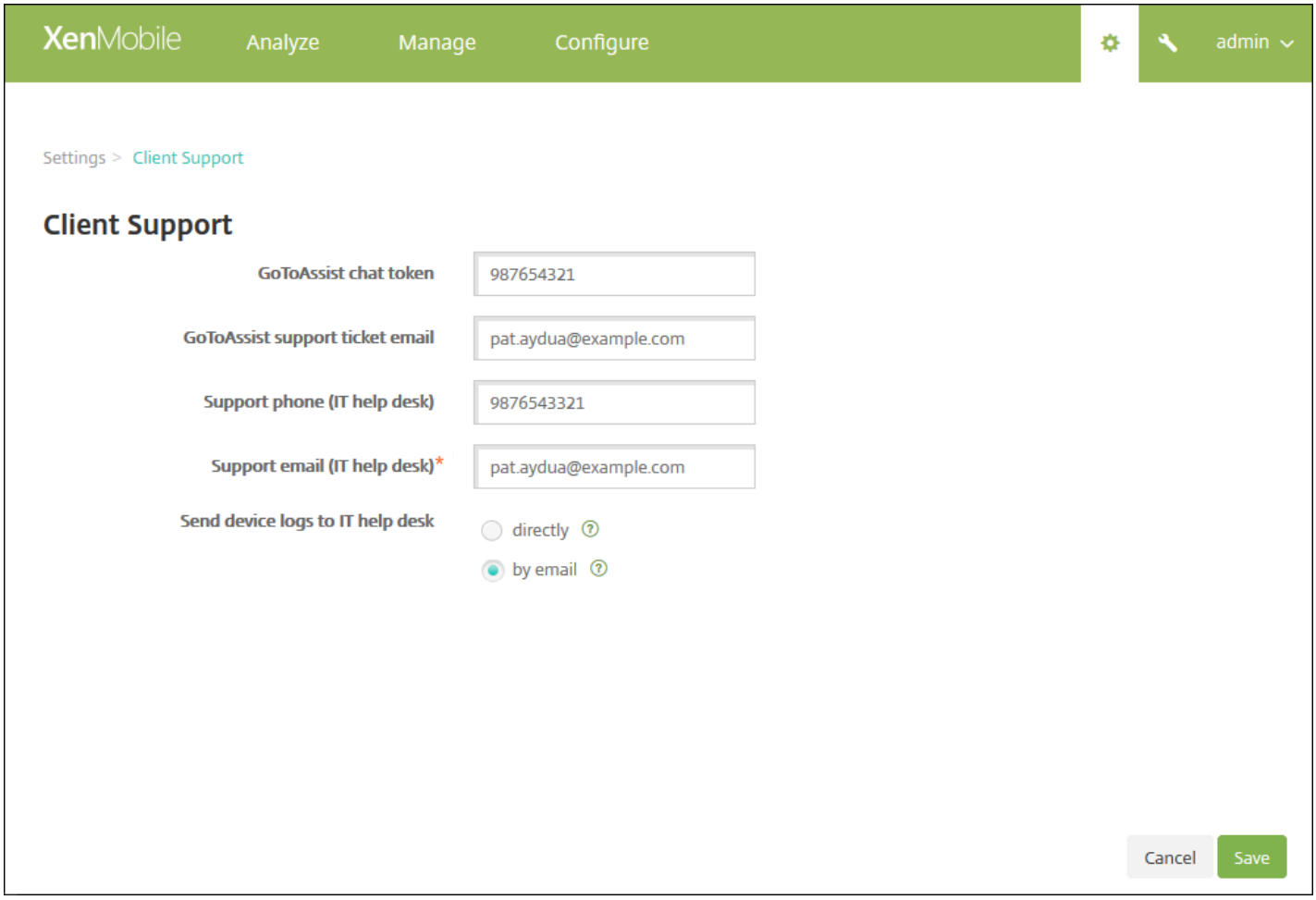
-
-
-
-
-



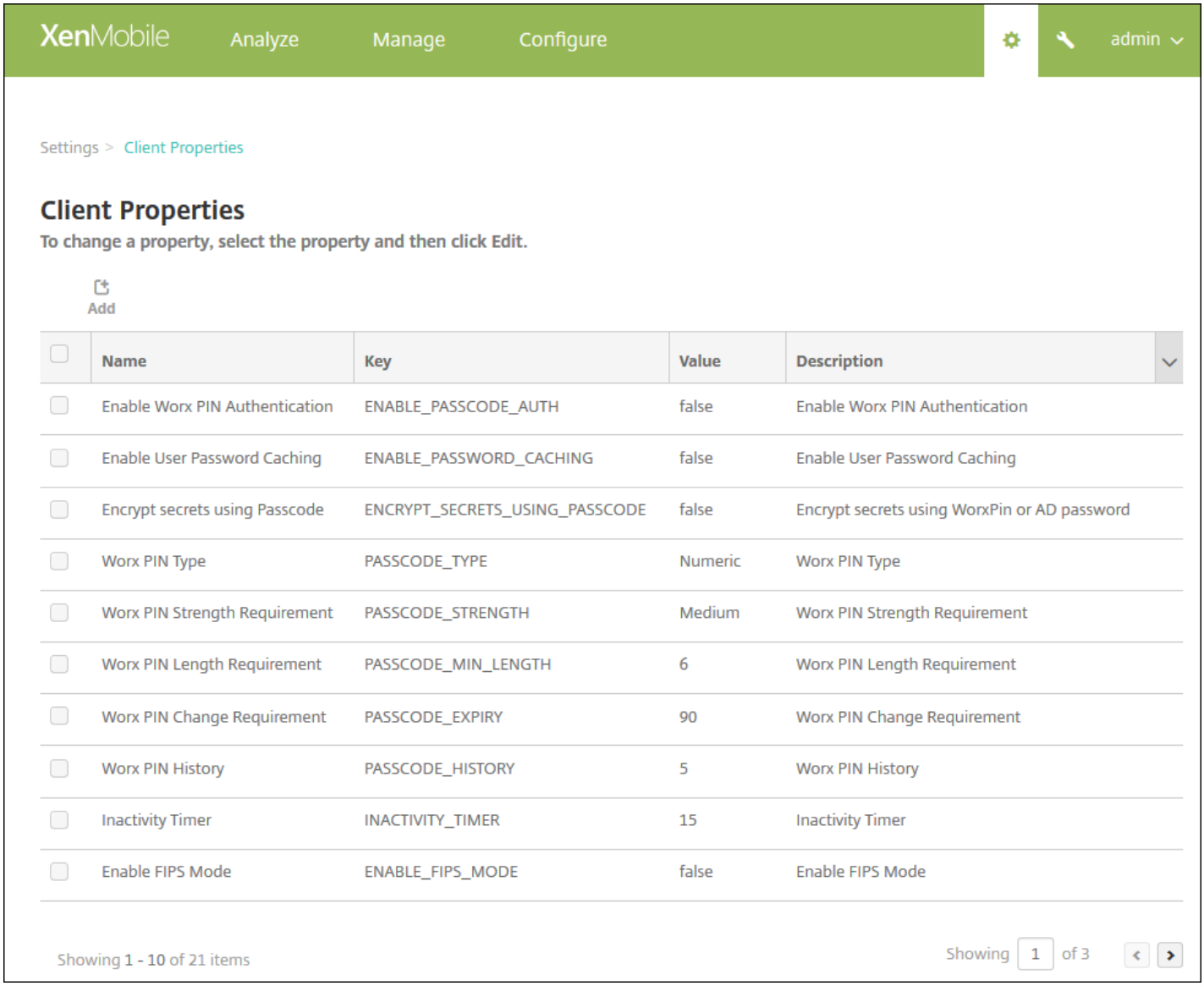


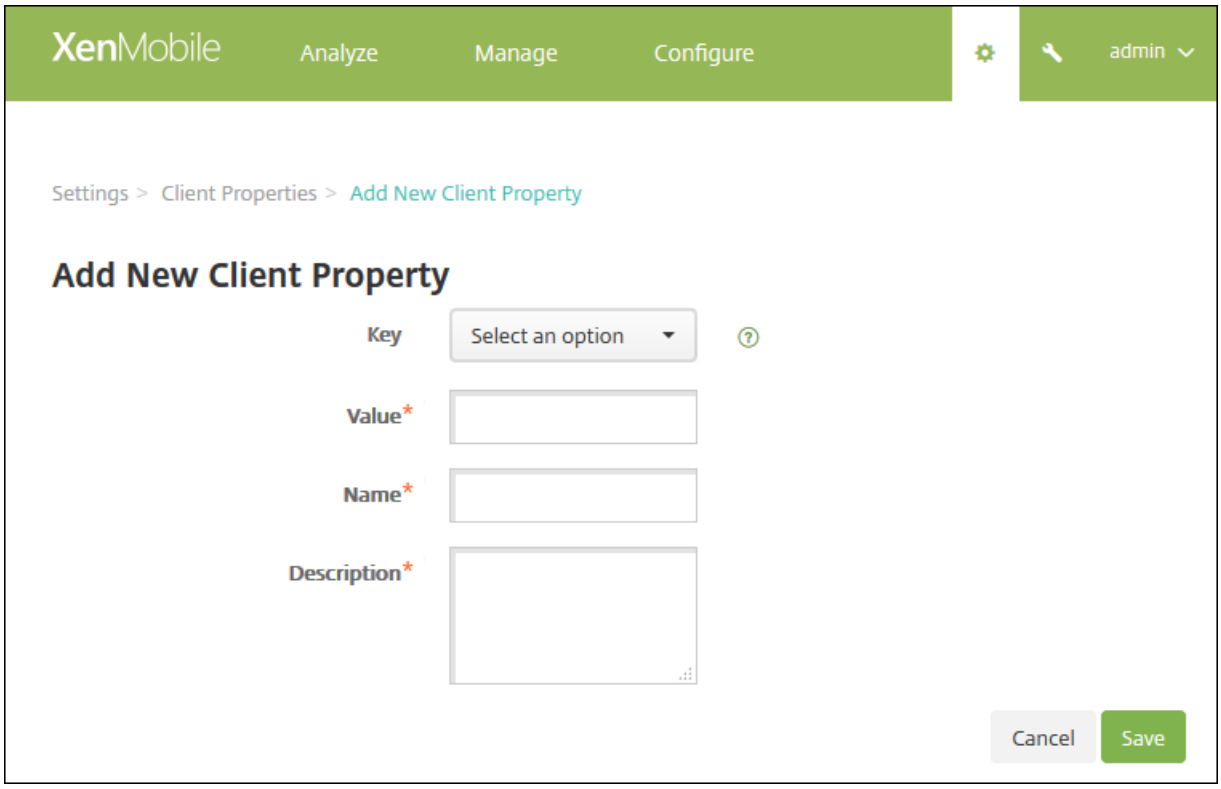
-
-
-
-



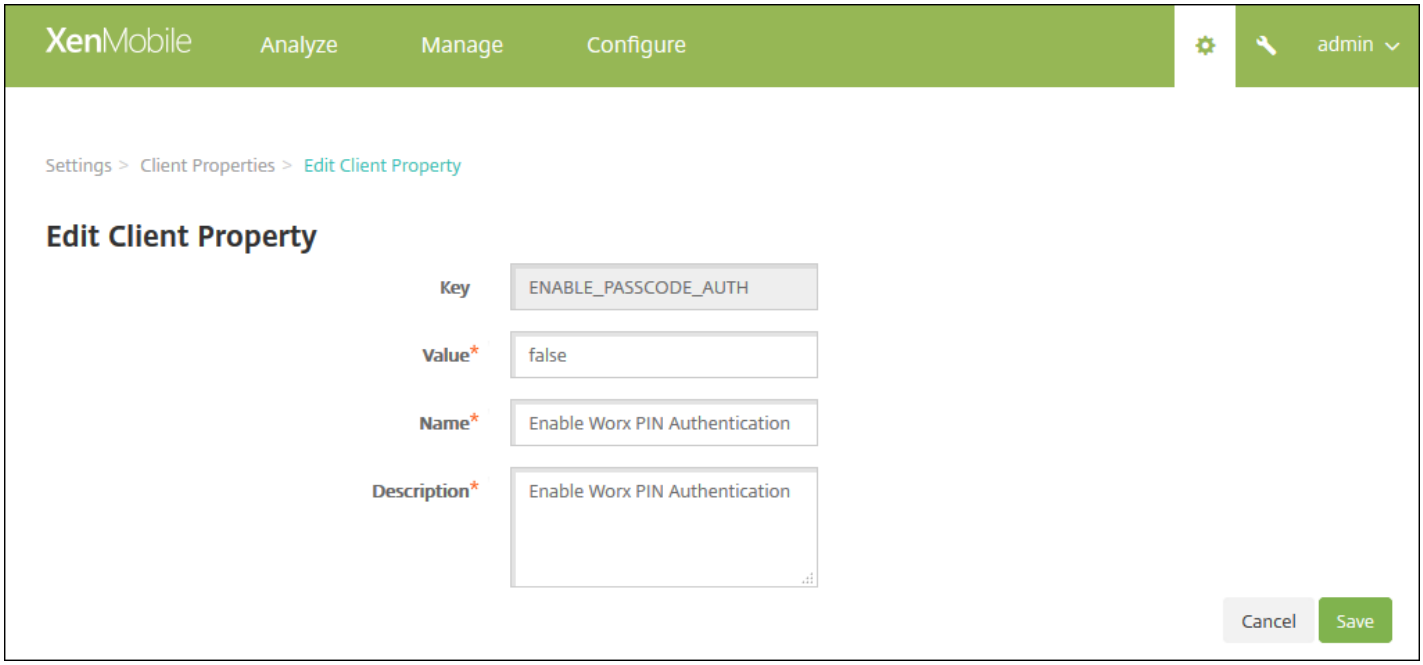


-
-
-
-
-
  -
-
  -



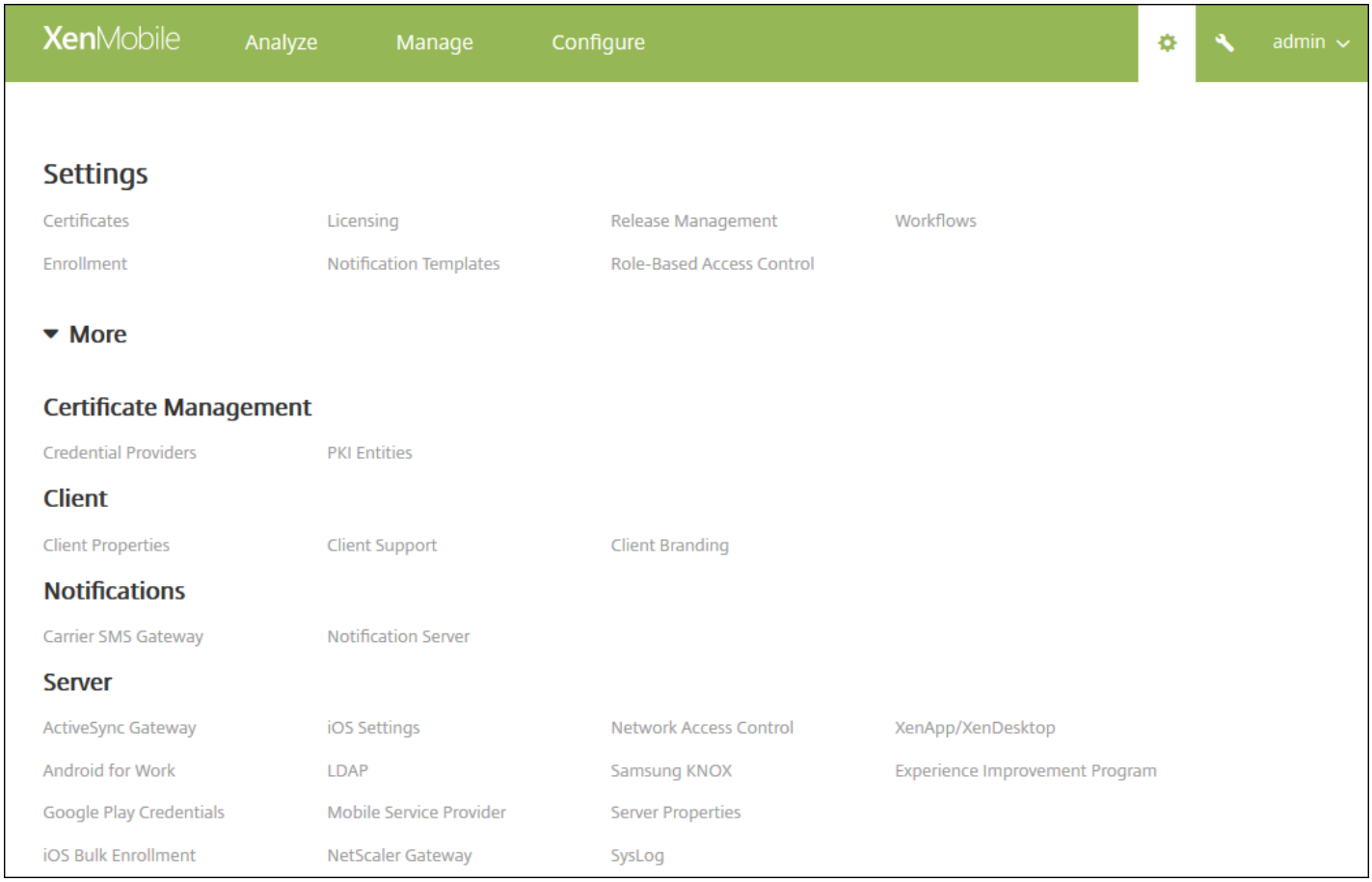


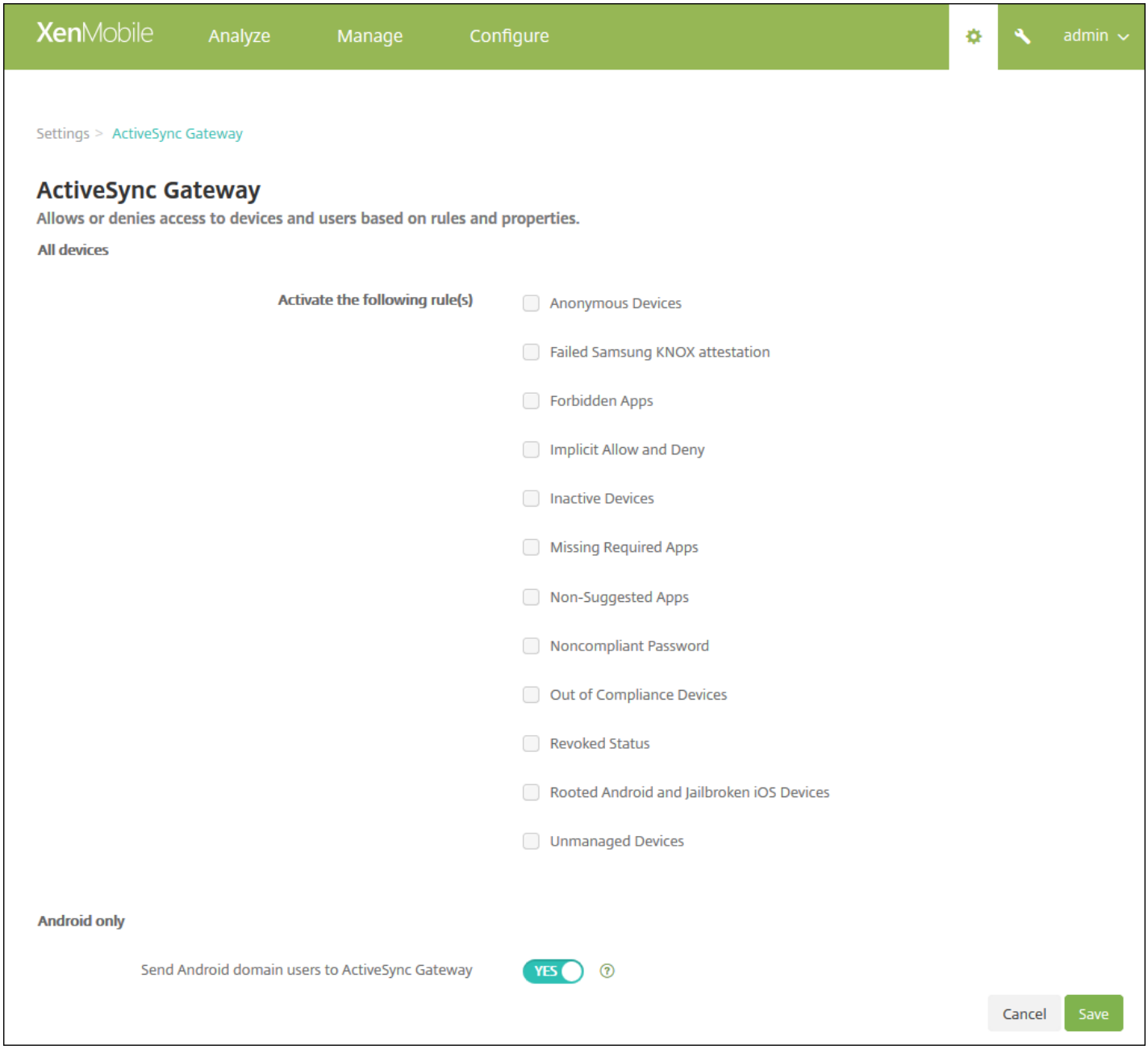
-
-
-
-

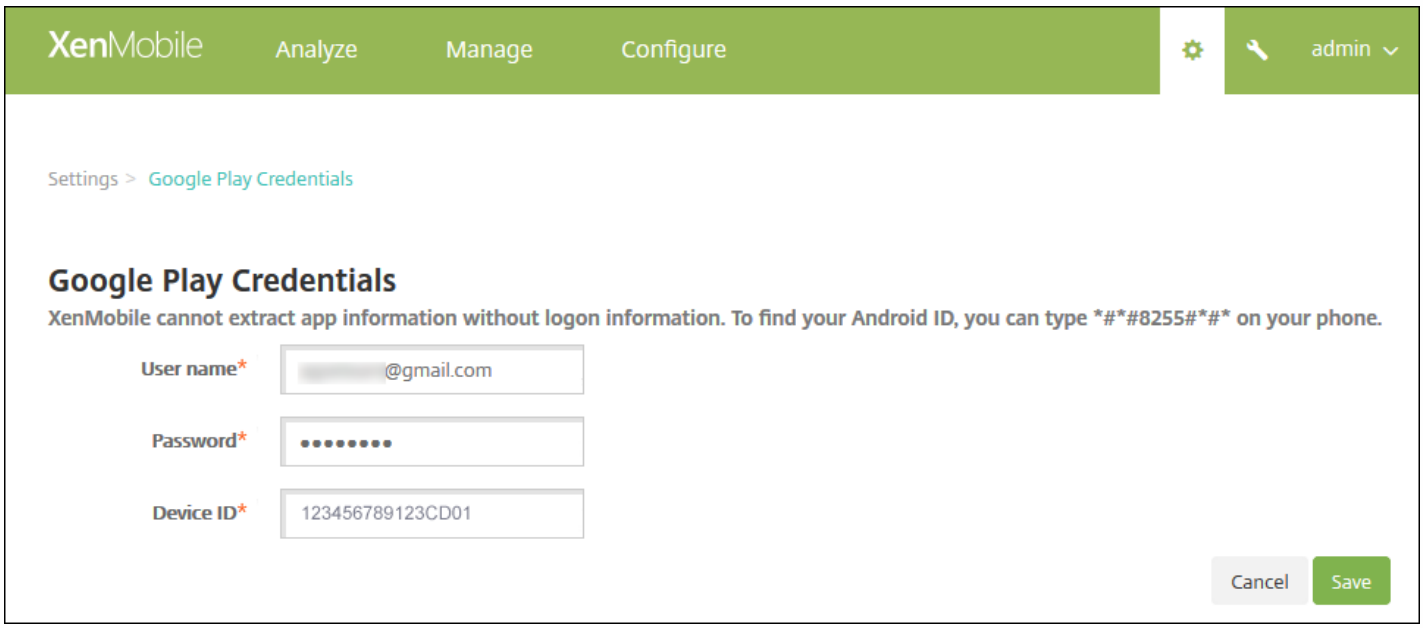


-
-
-
-

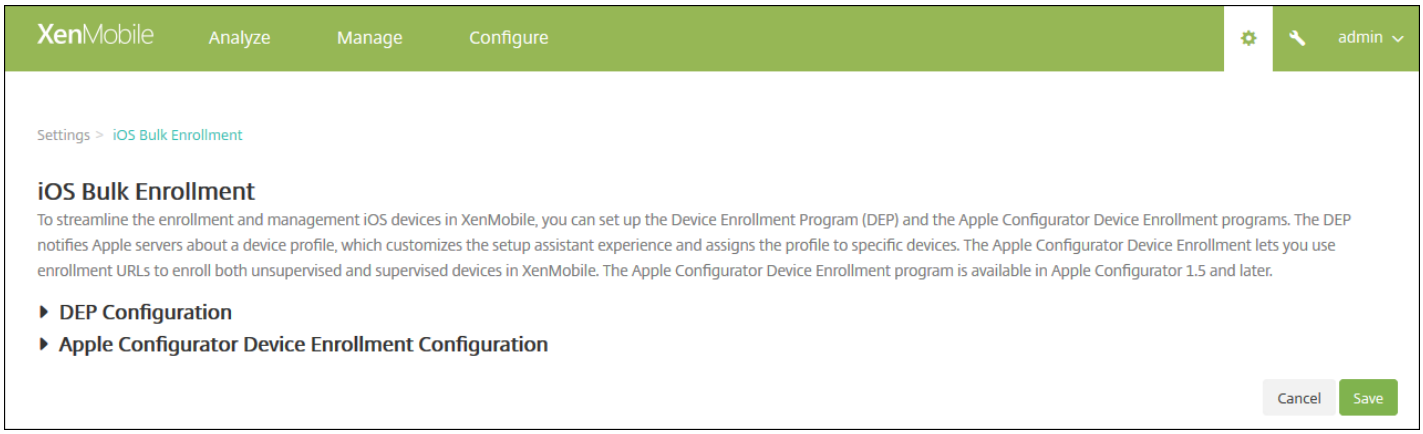
-
-
-
-
-
-
-
-
-
-
-
-
-
-

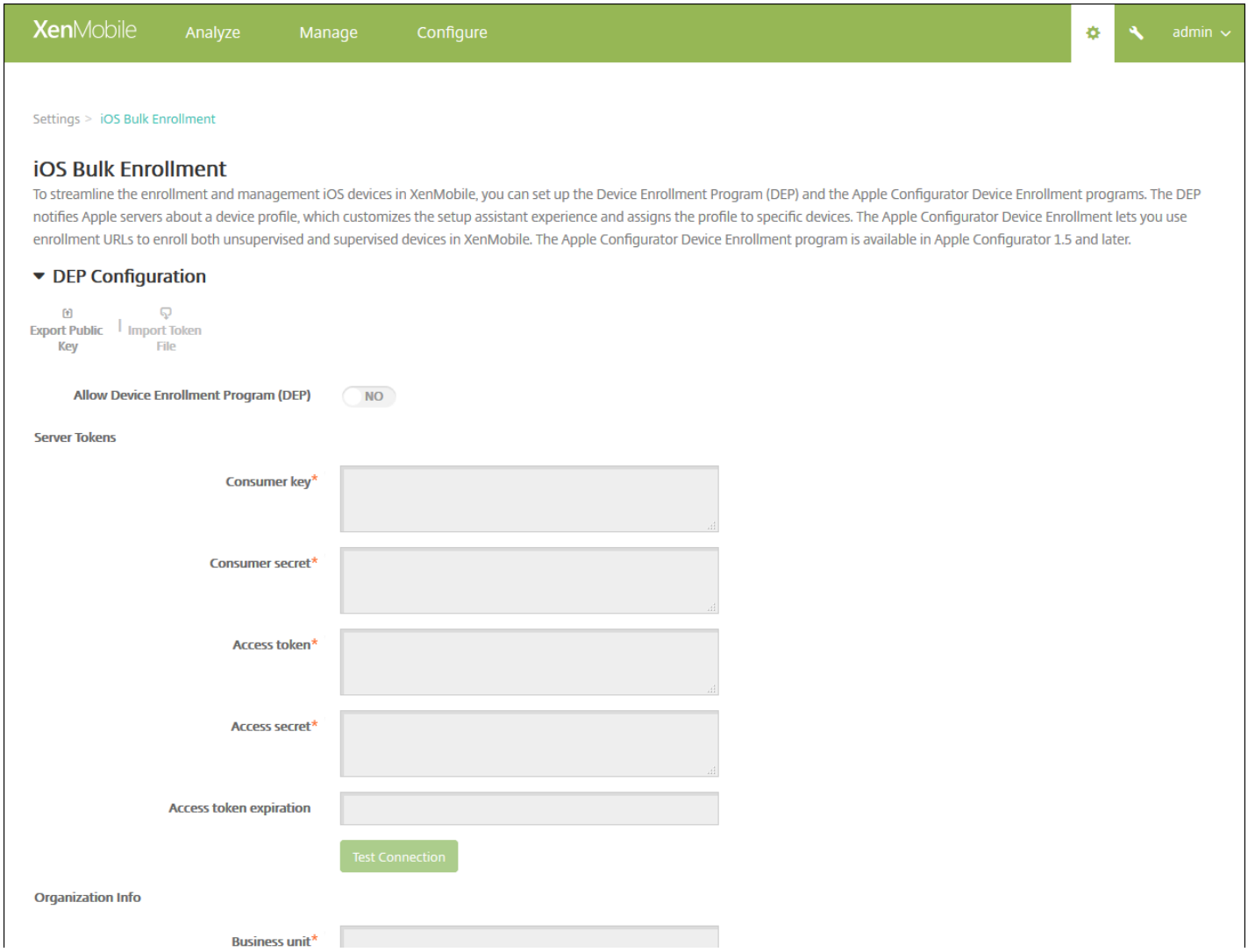


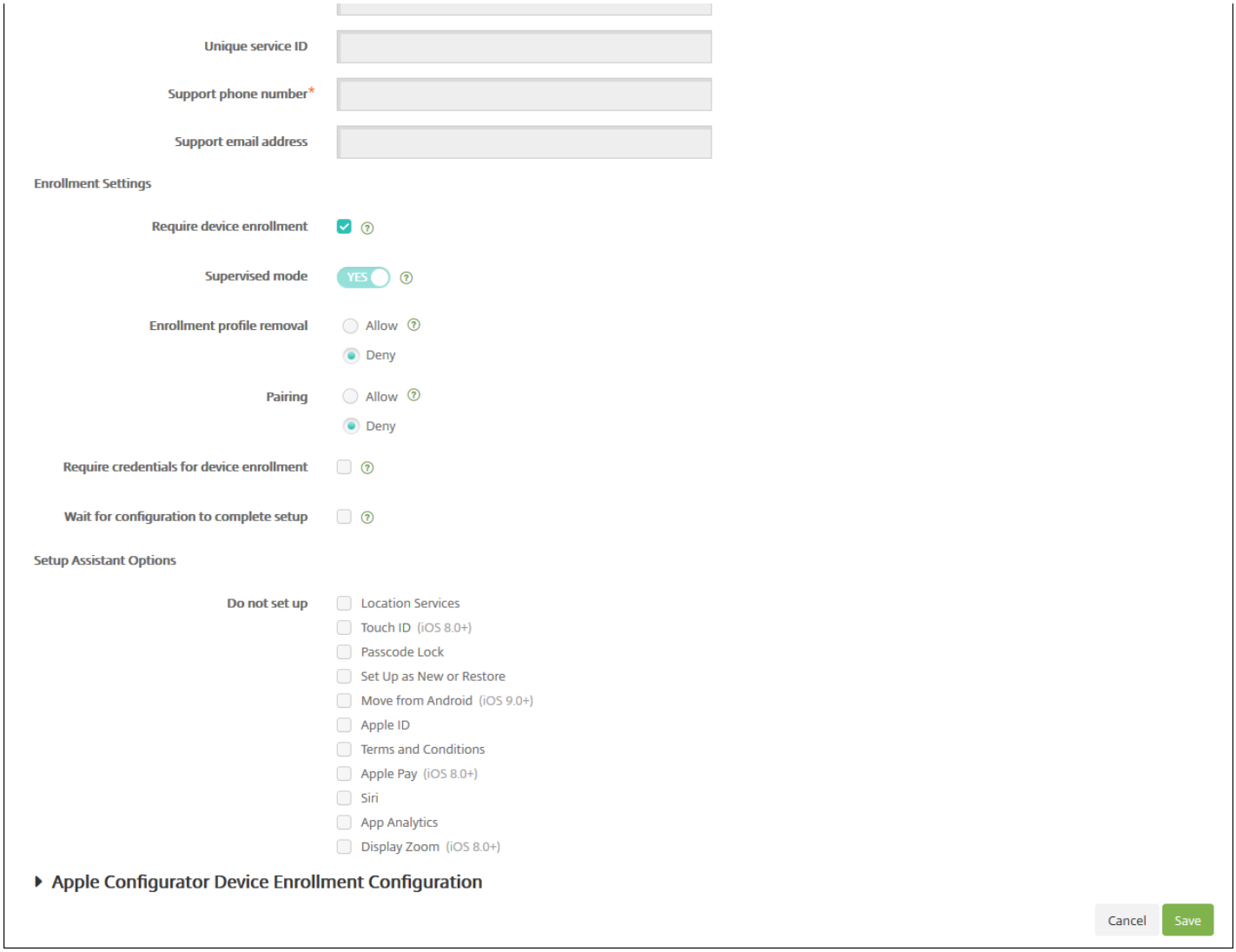




-
-
-

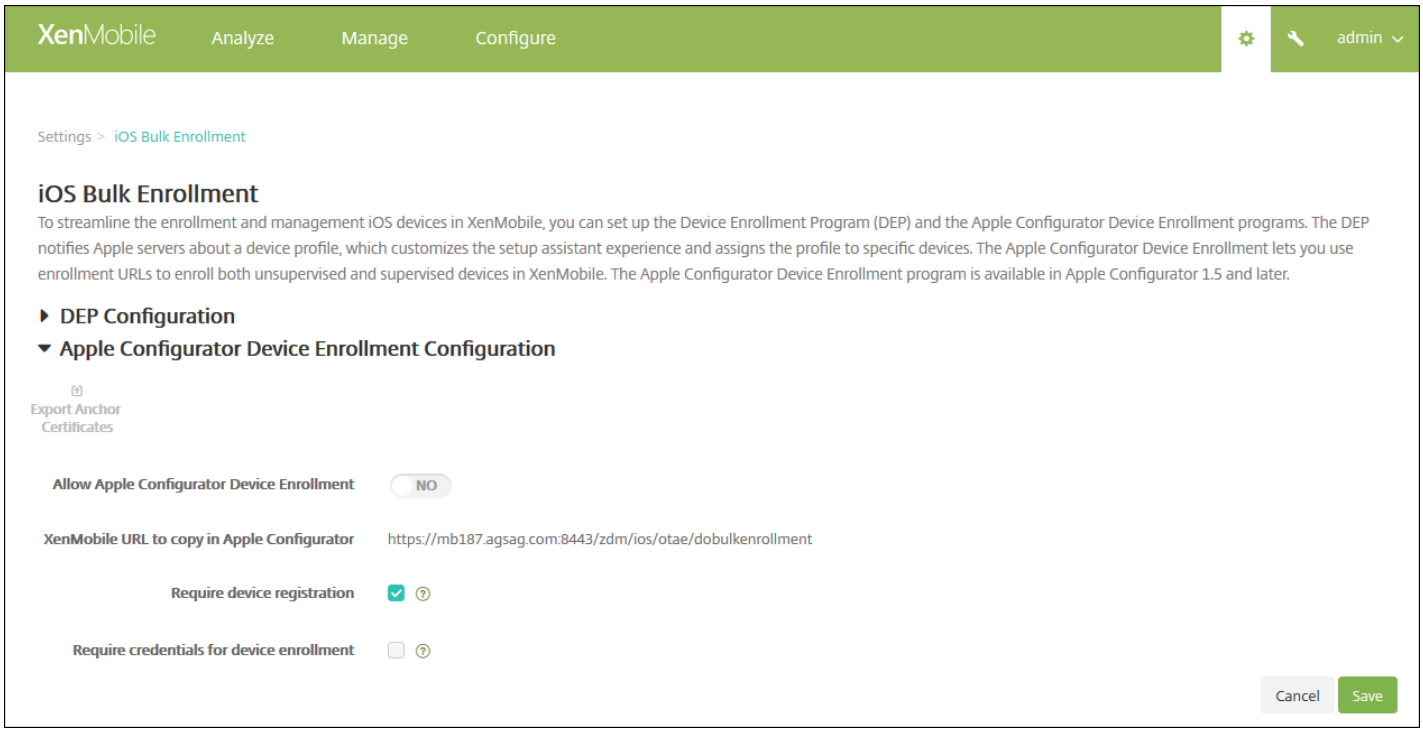






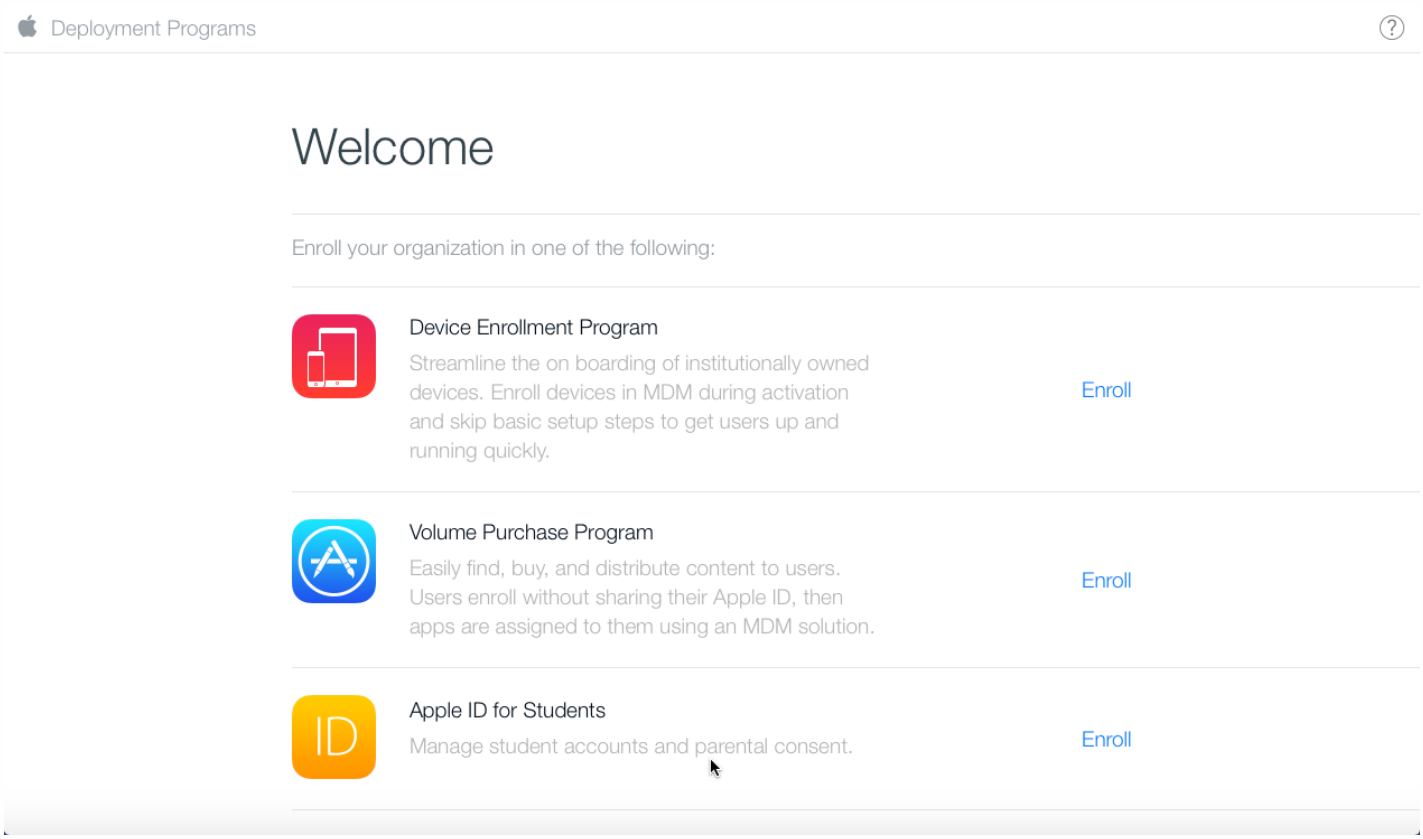
-
-
-
-
-
-

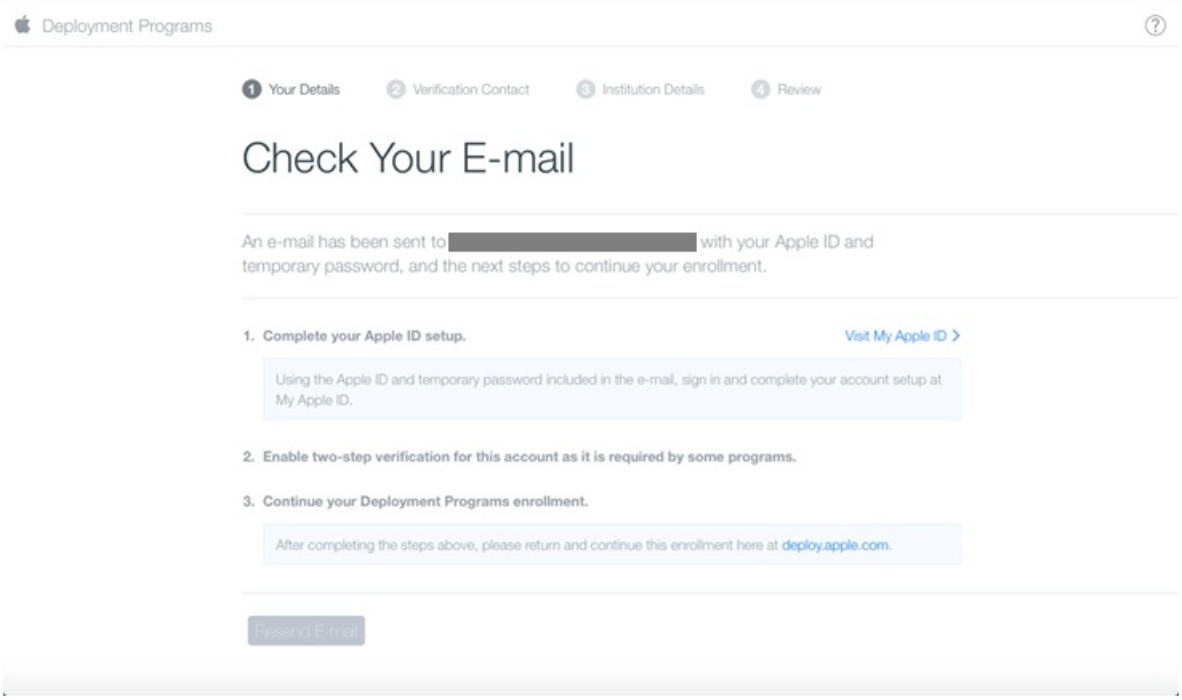
-

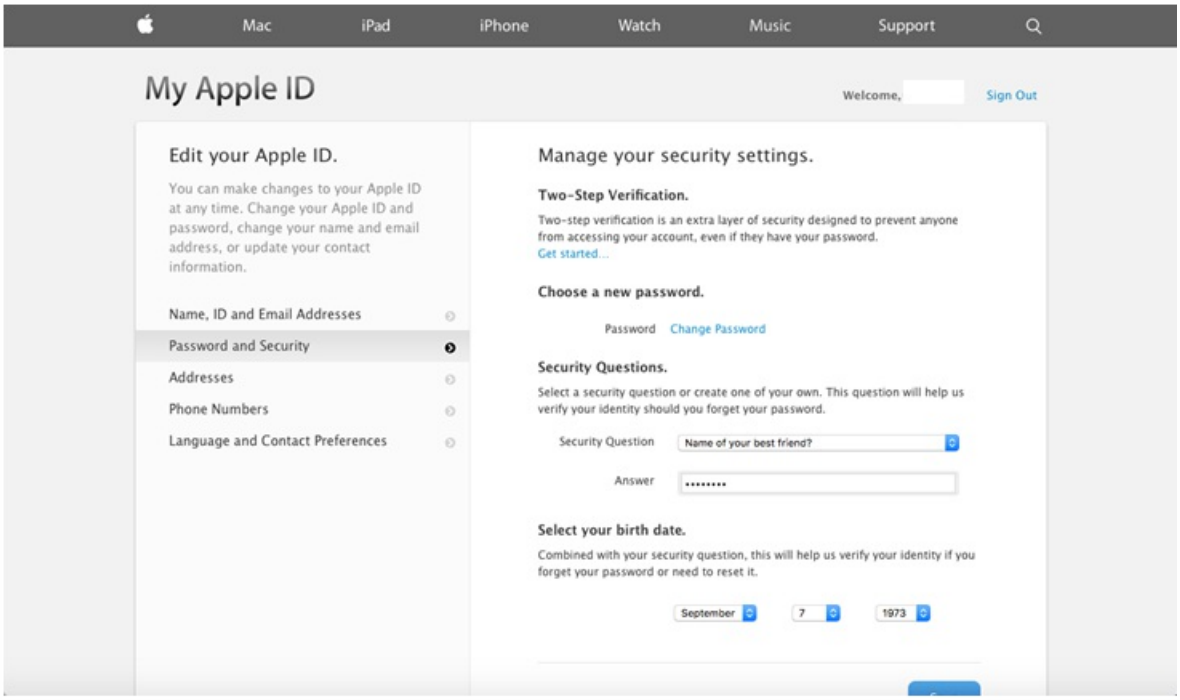


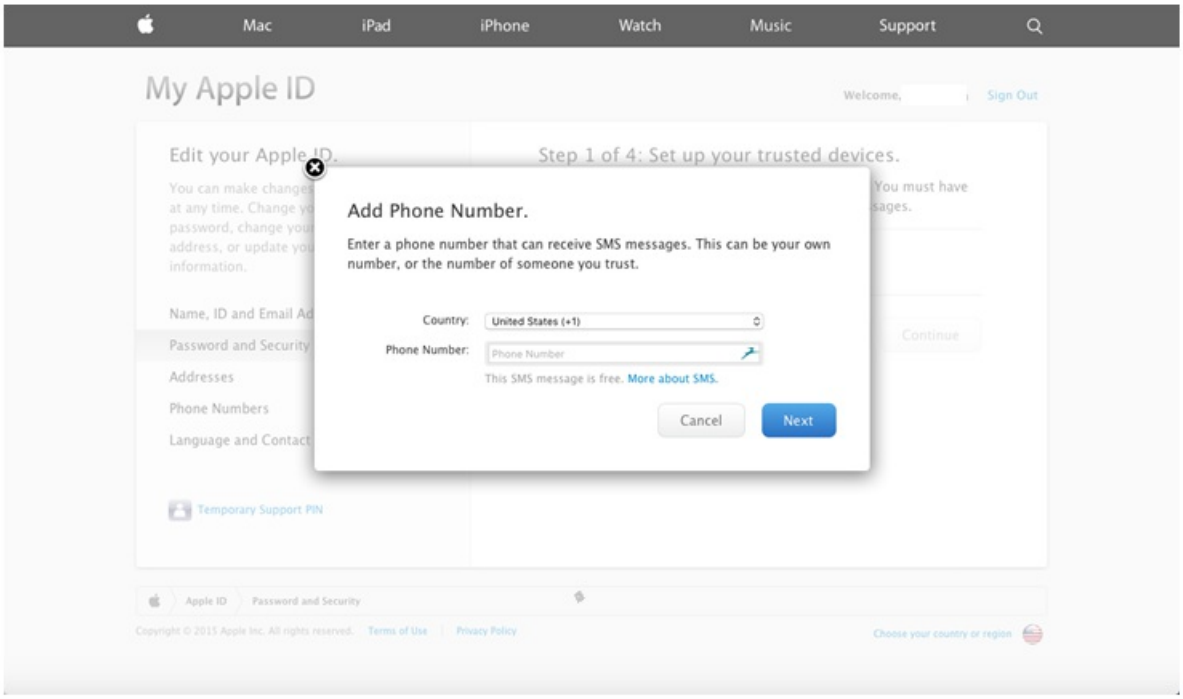
-
-
-

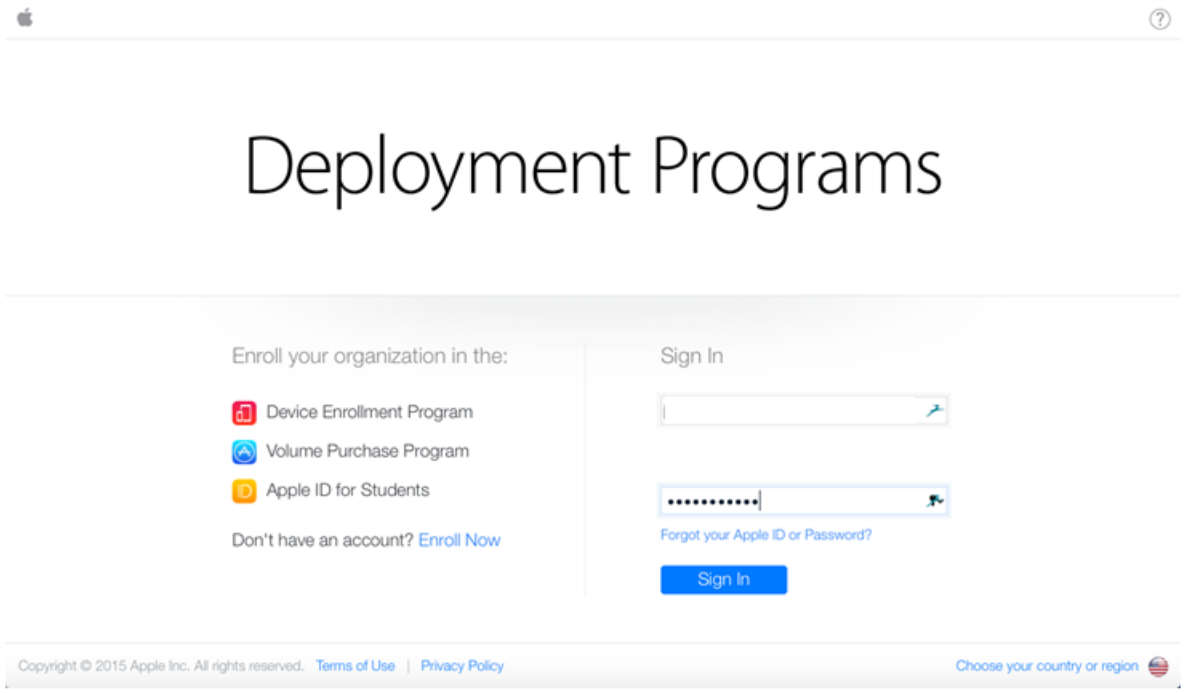
-
-
-
-

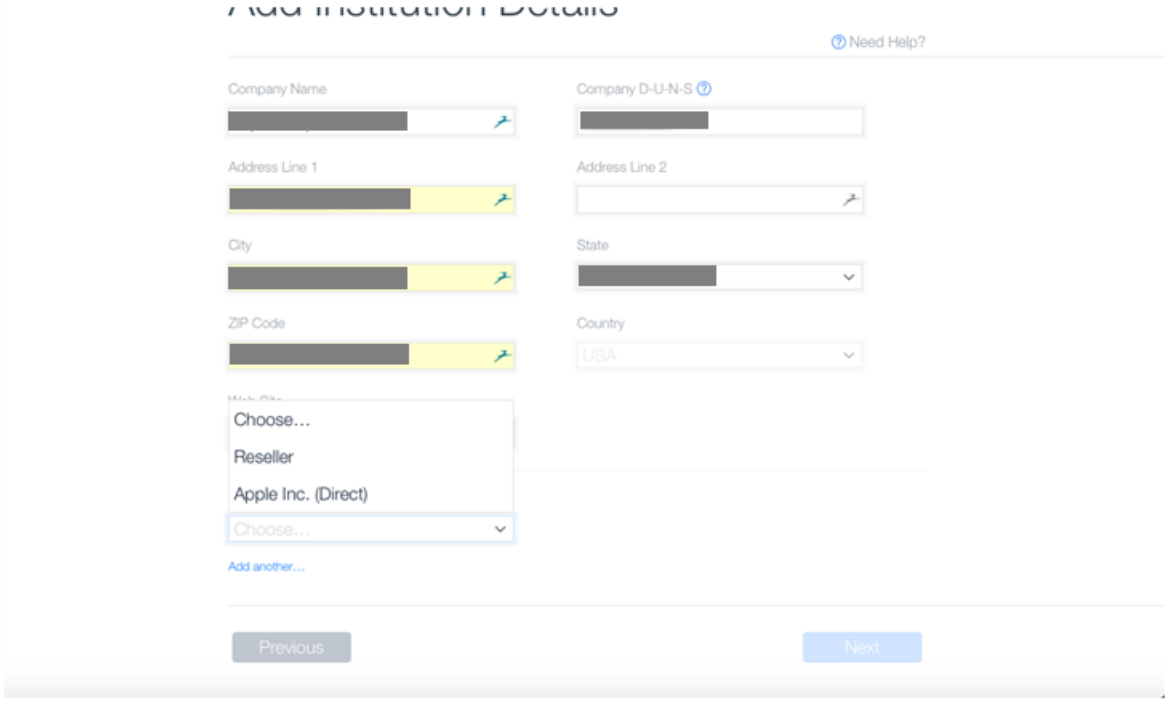


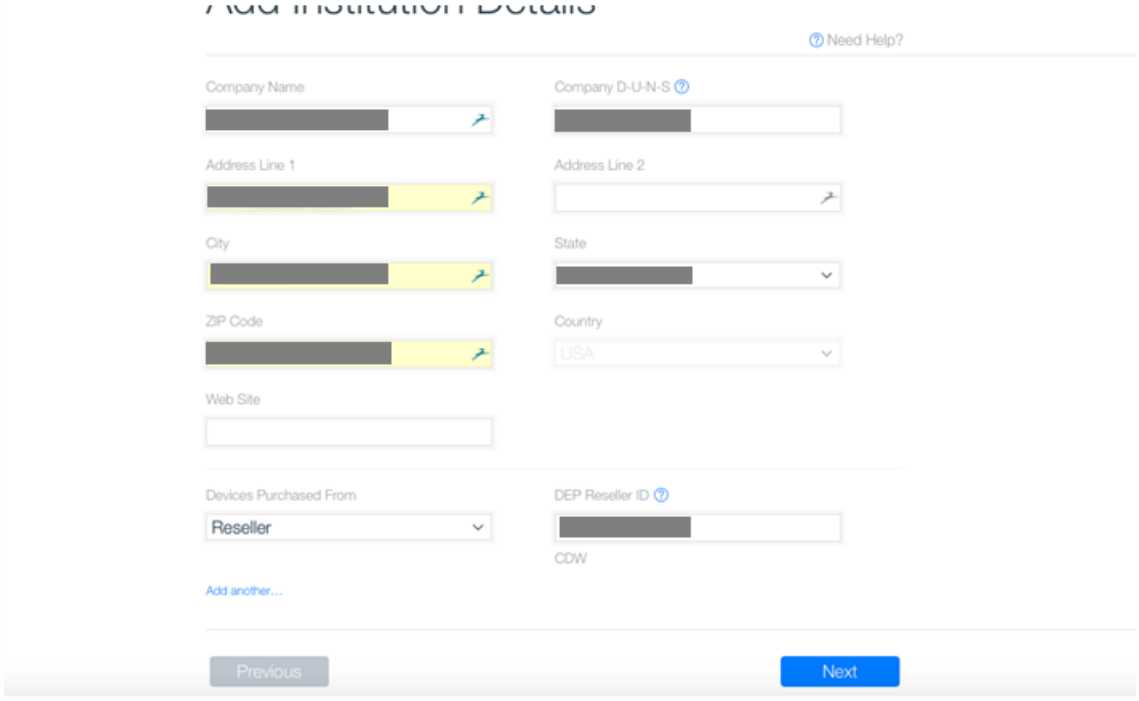


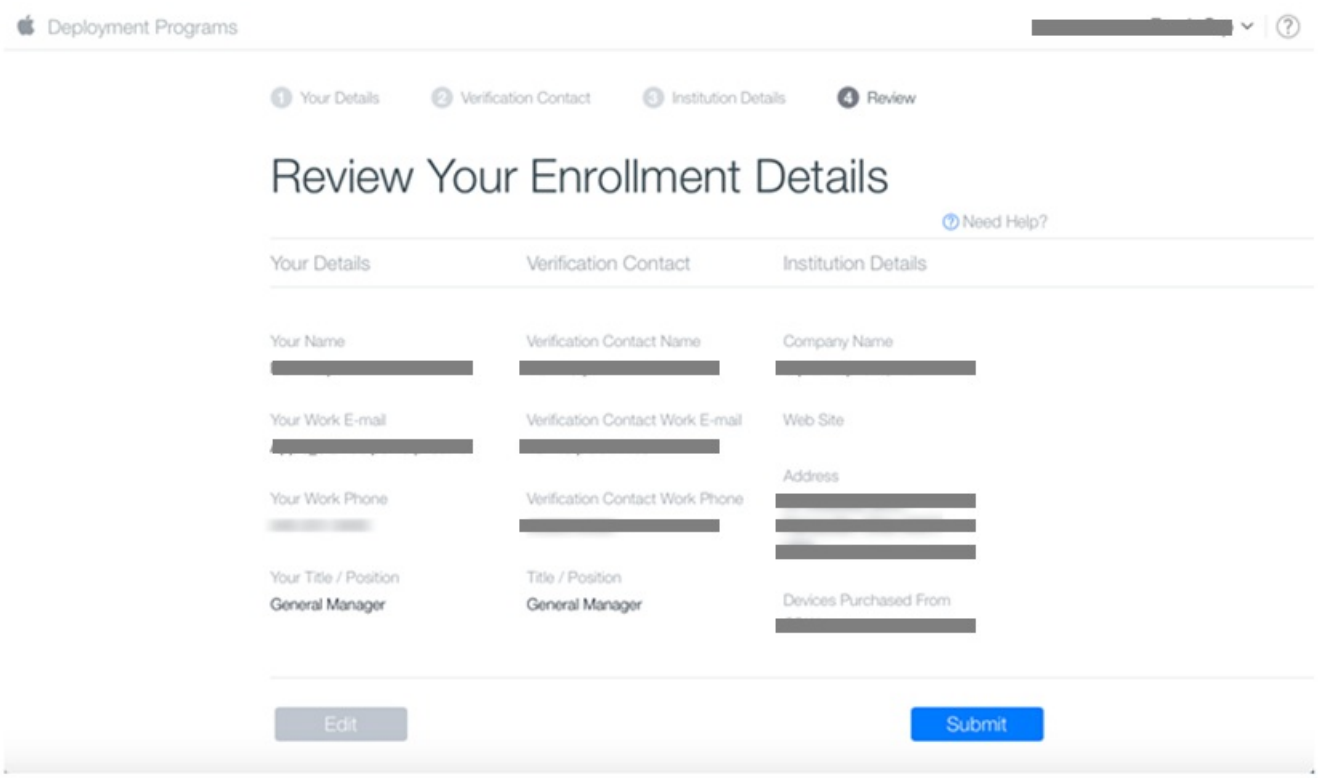


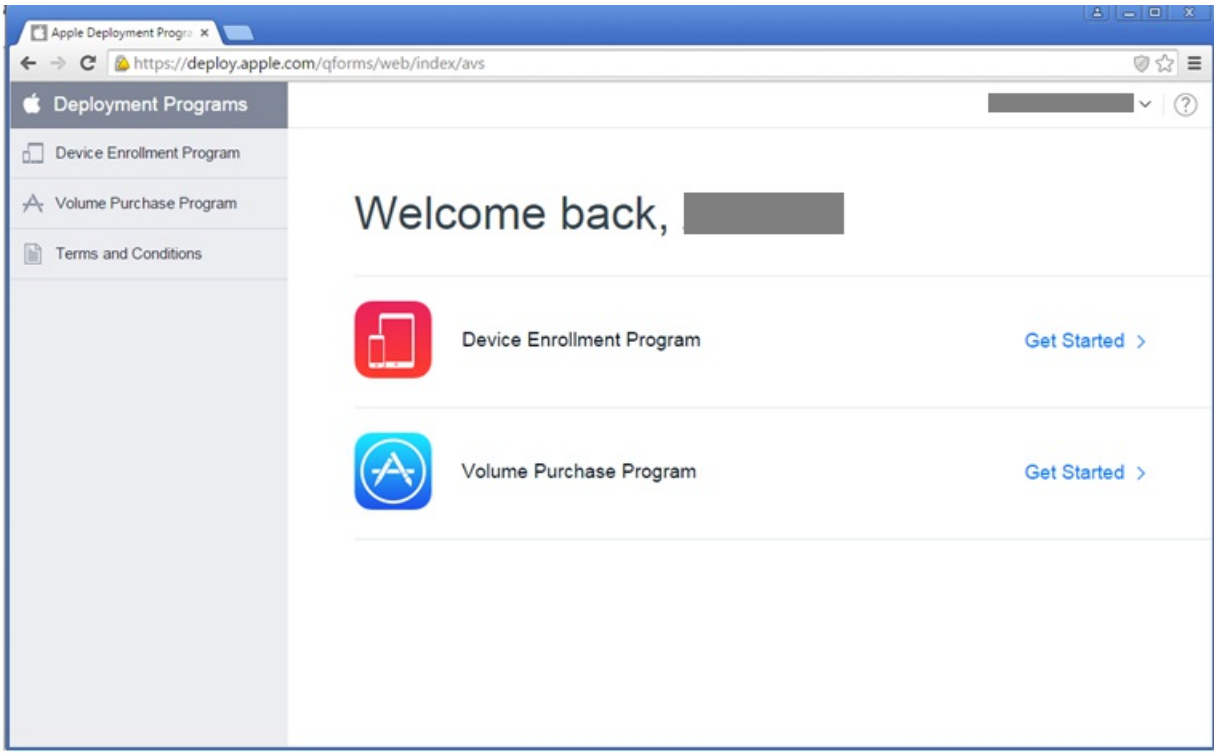


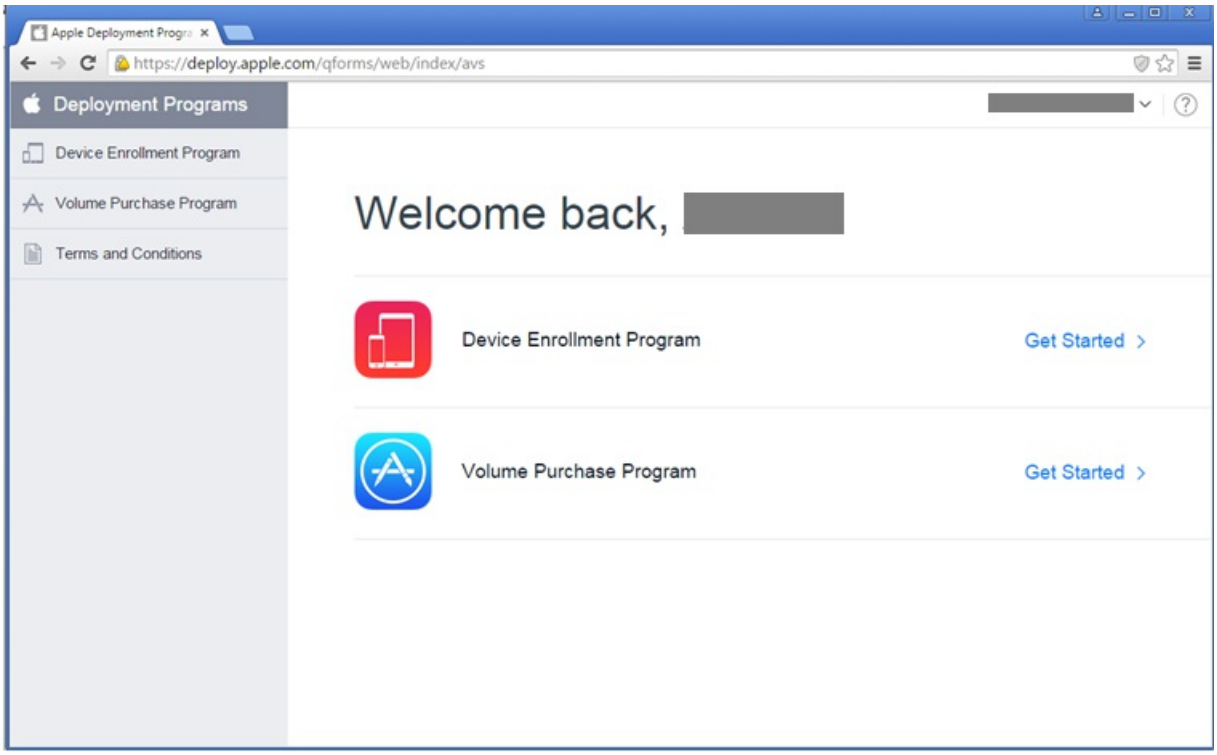


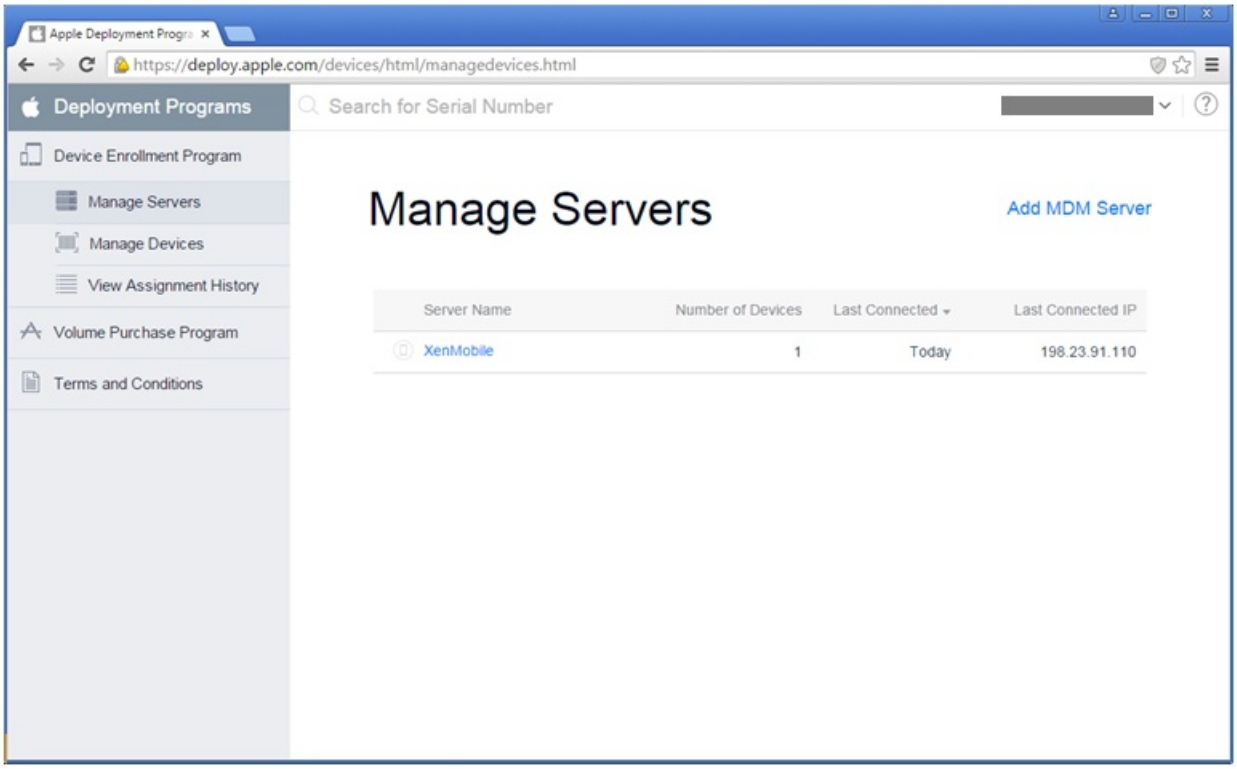


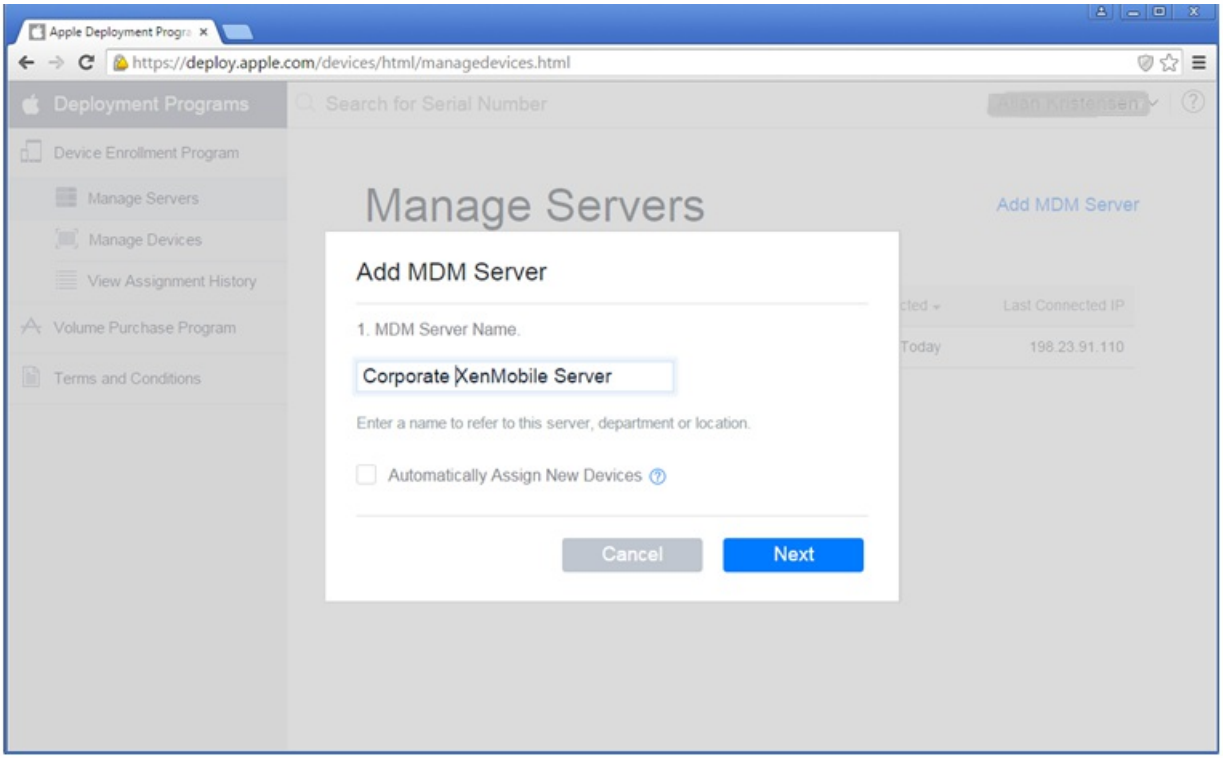


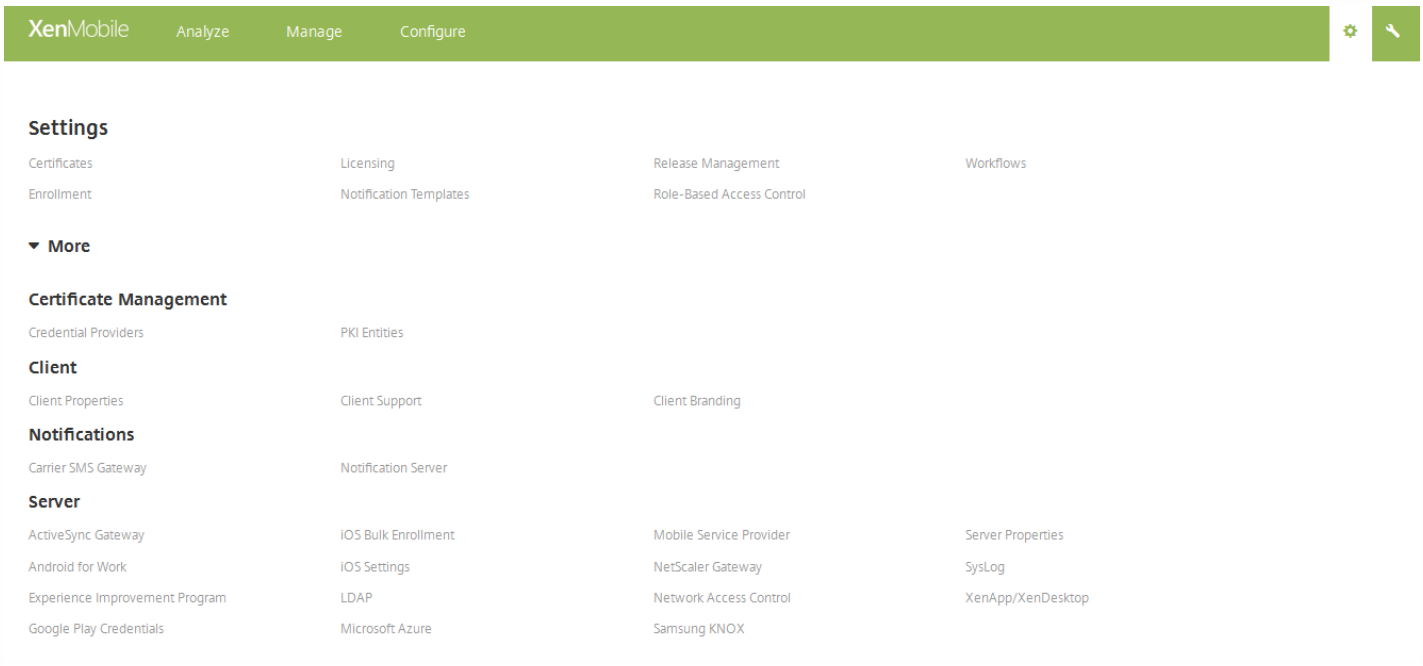


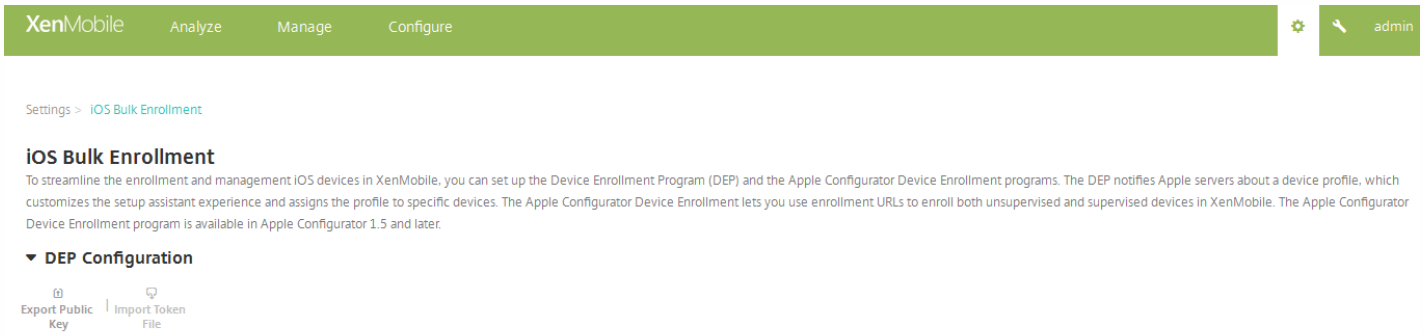


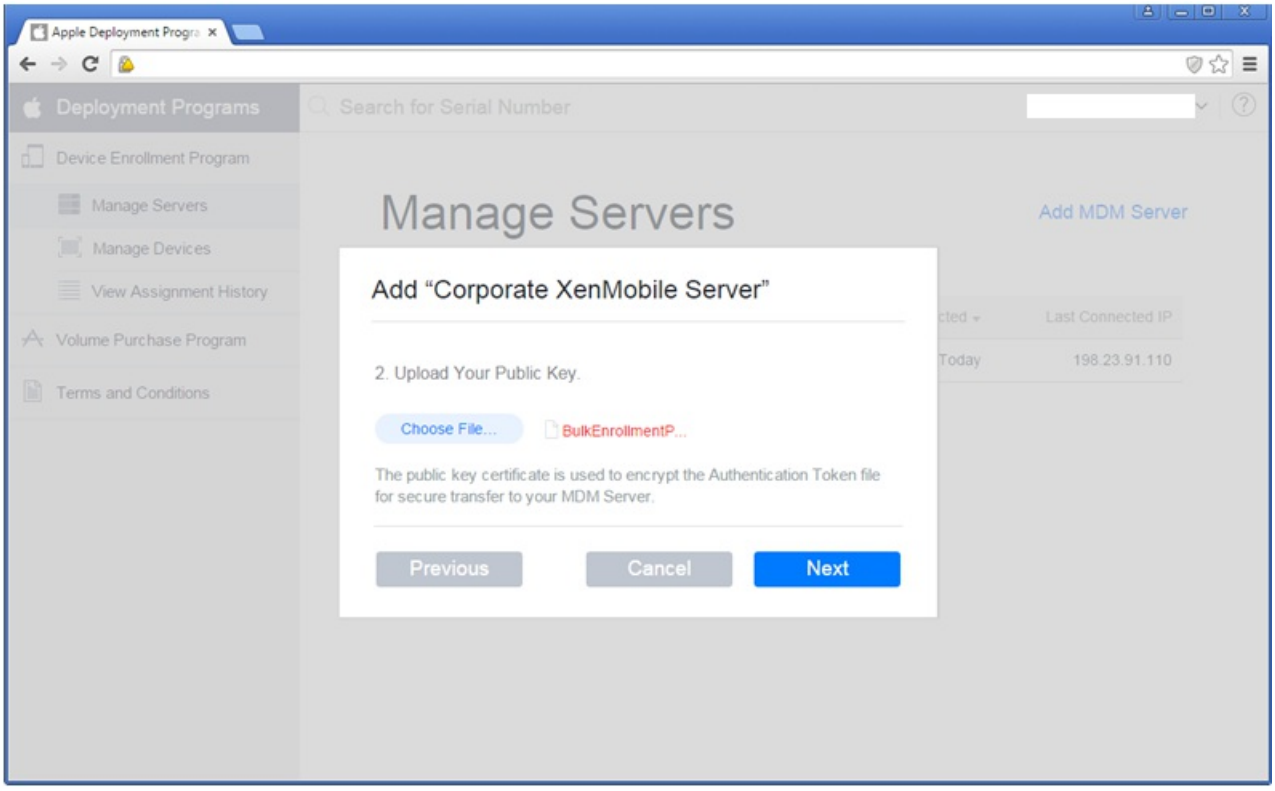


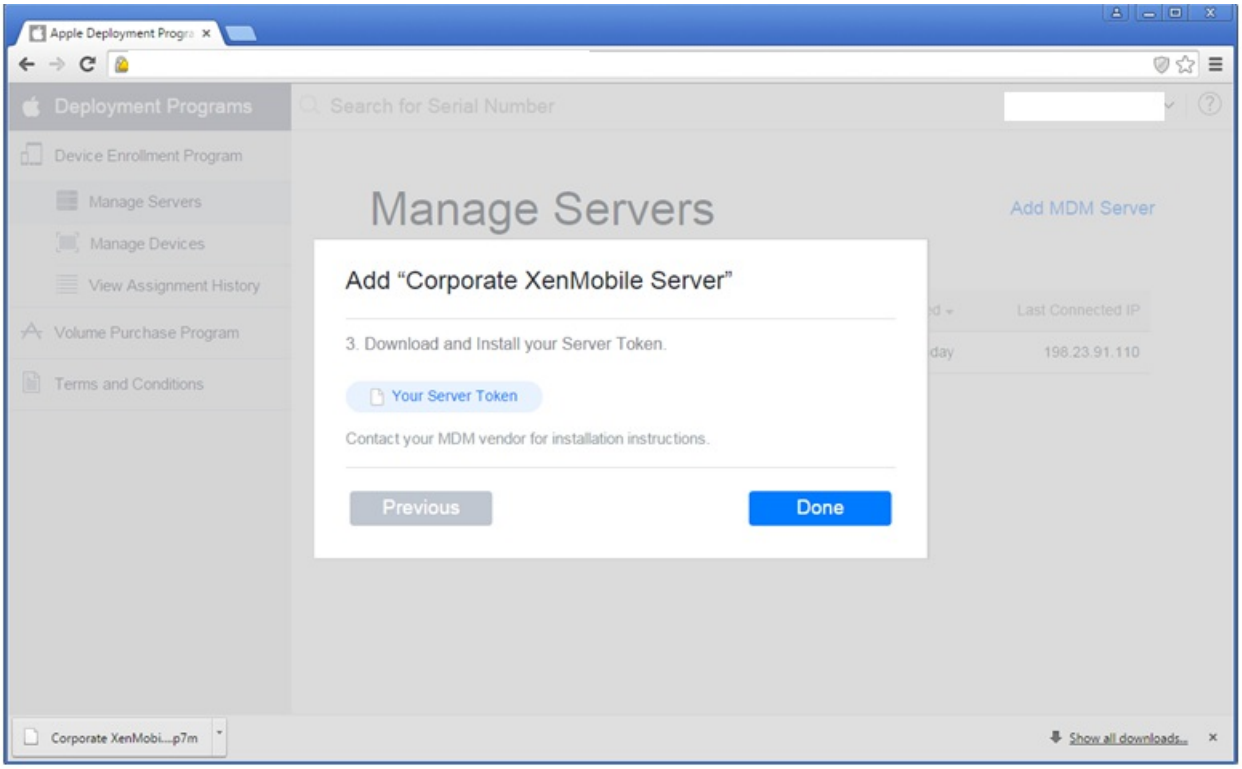


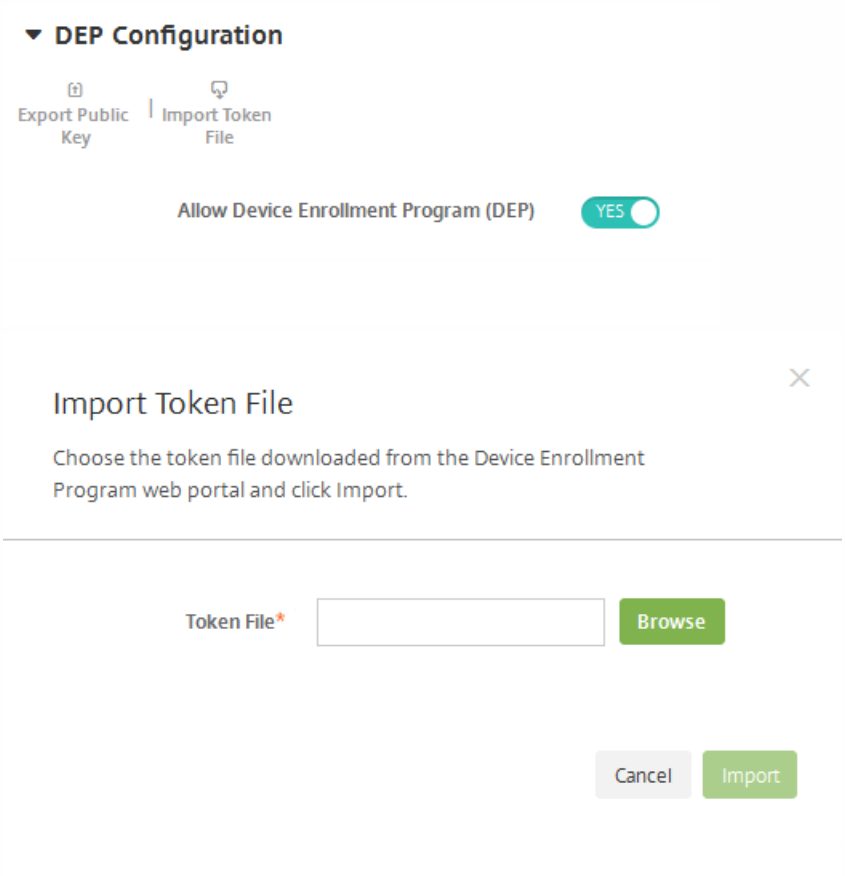


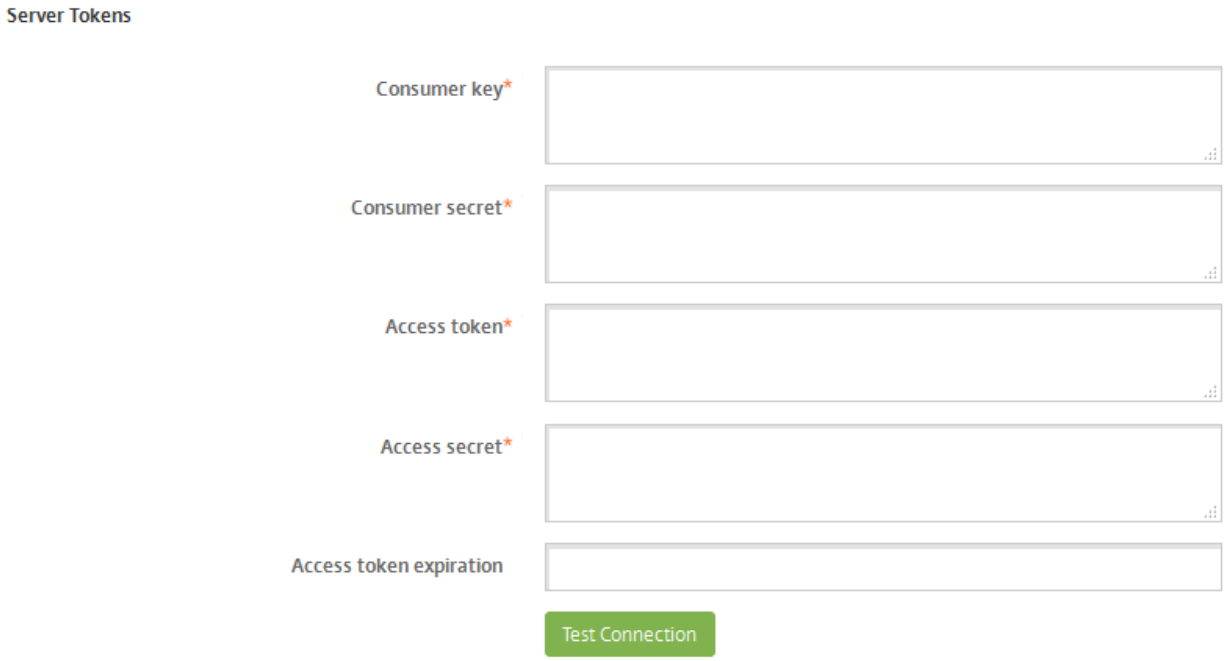


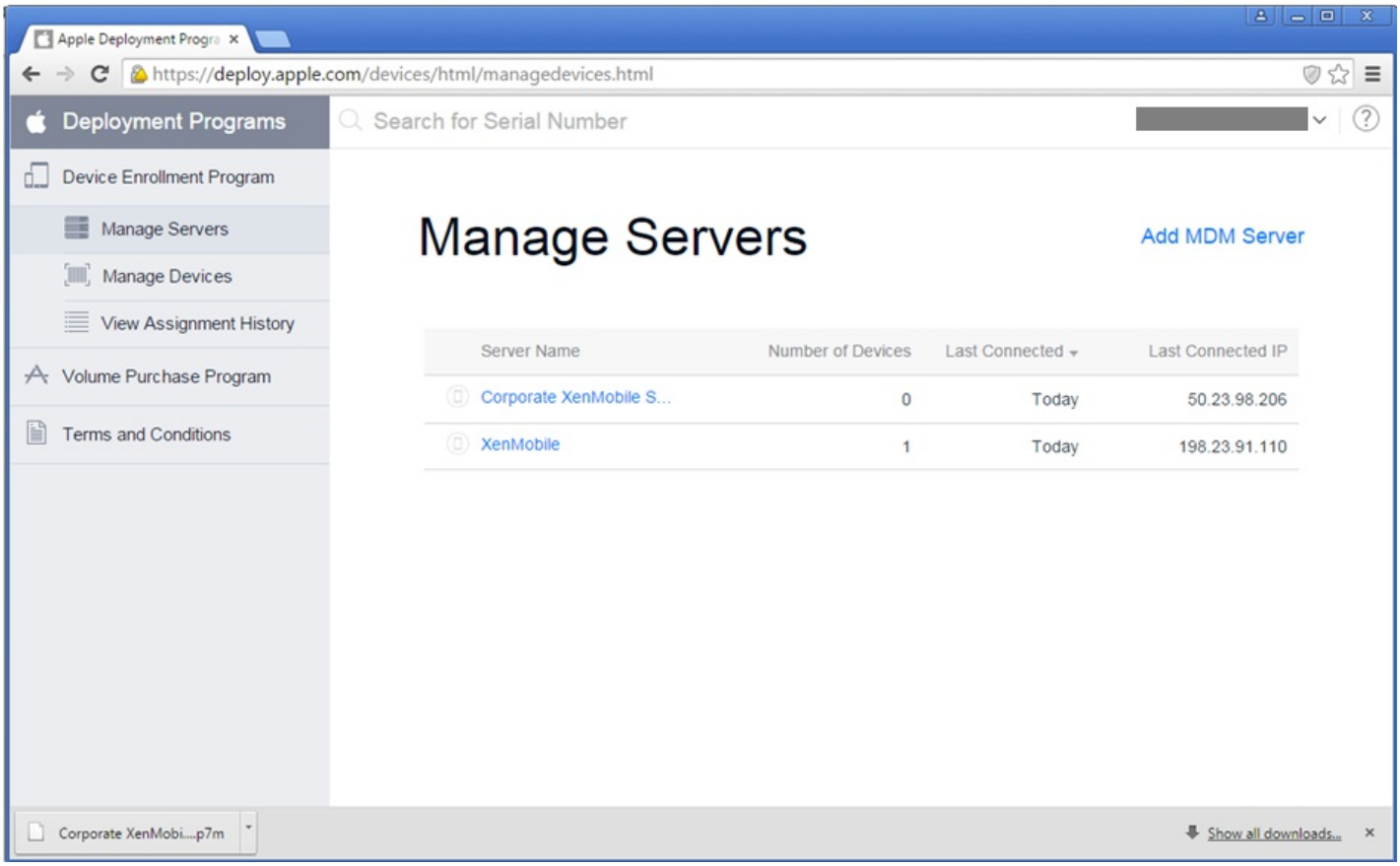


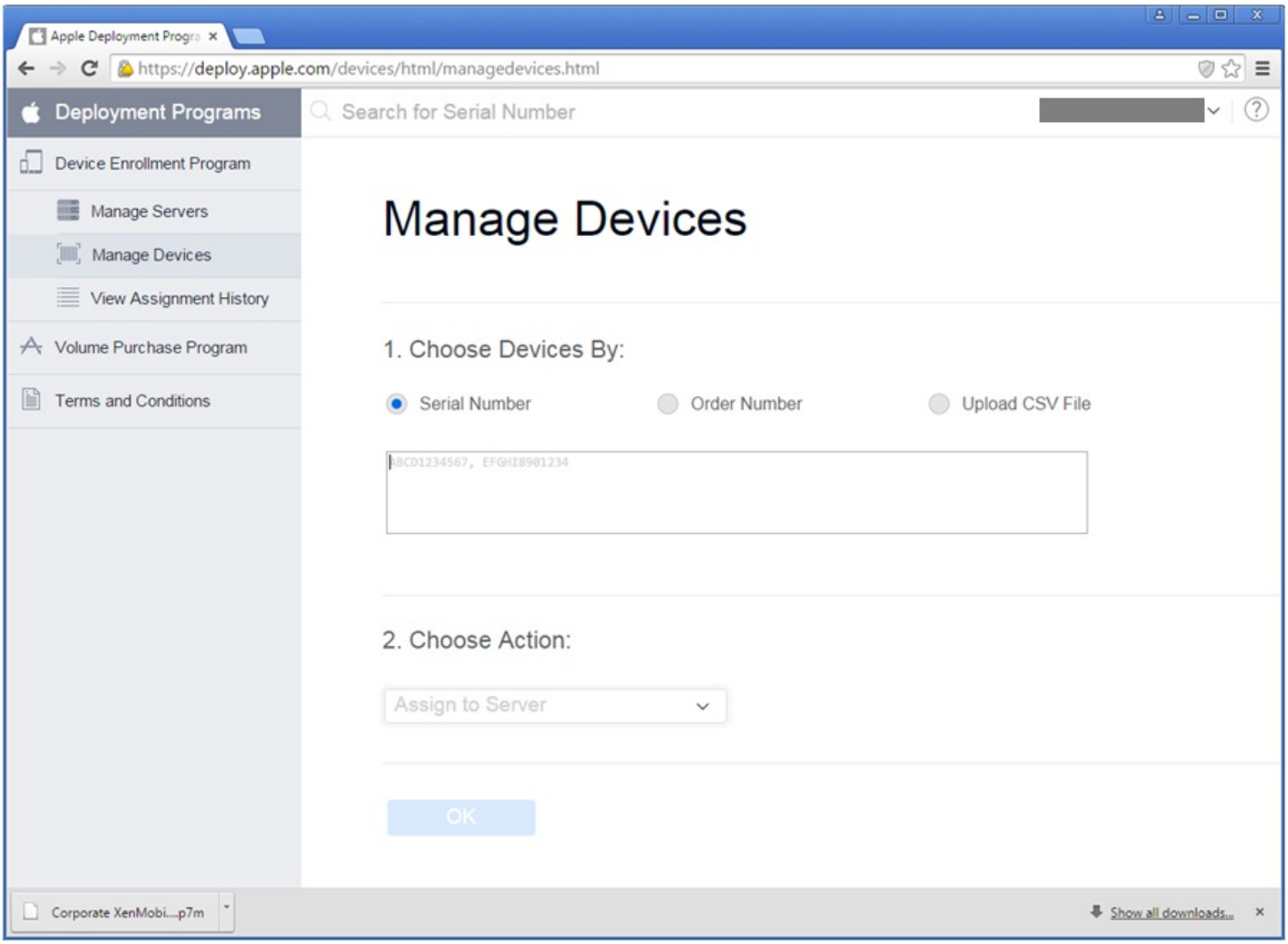


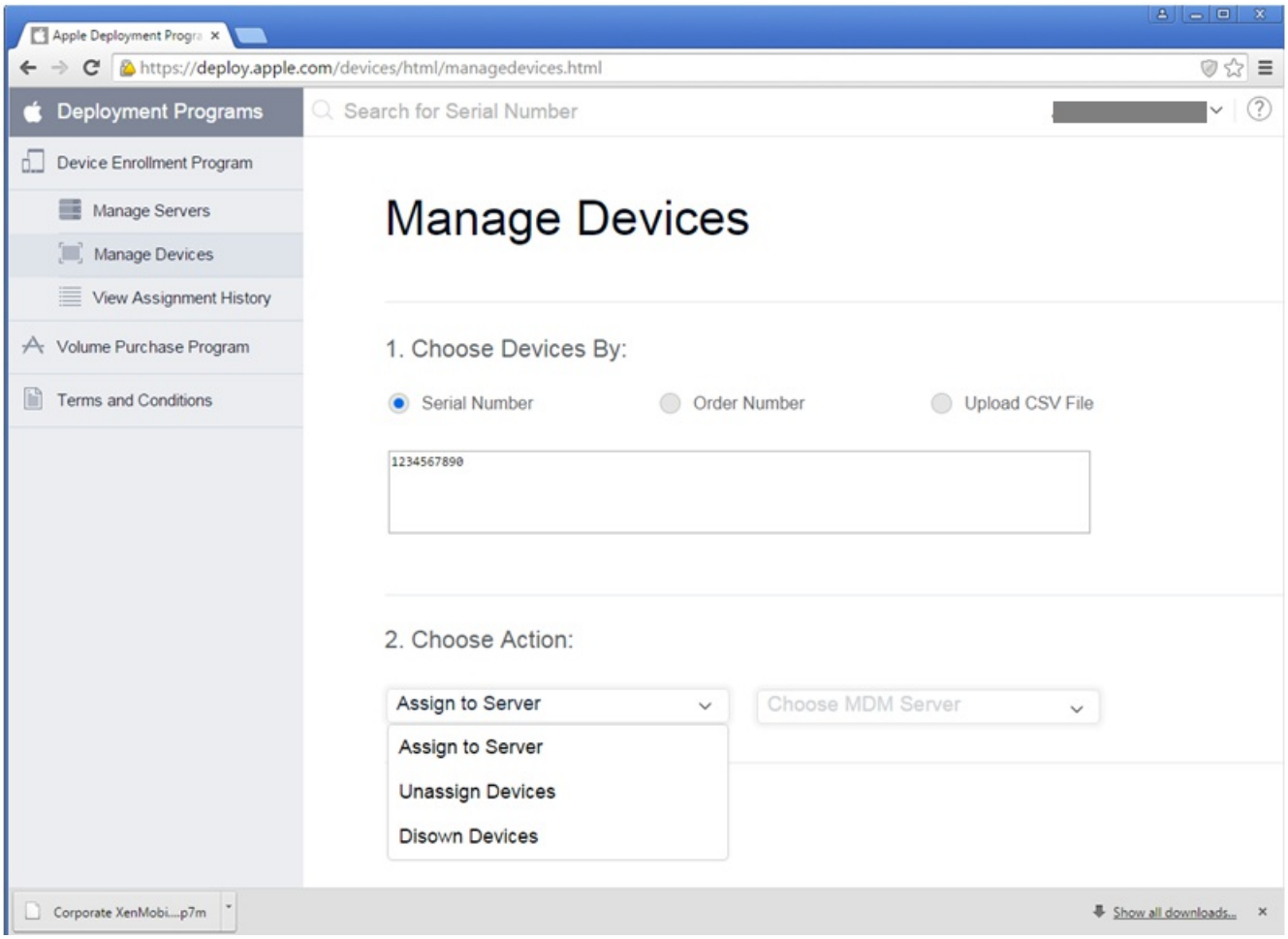


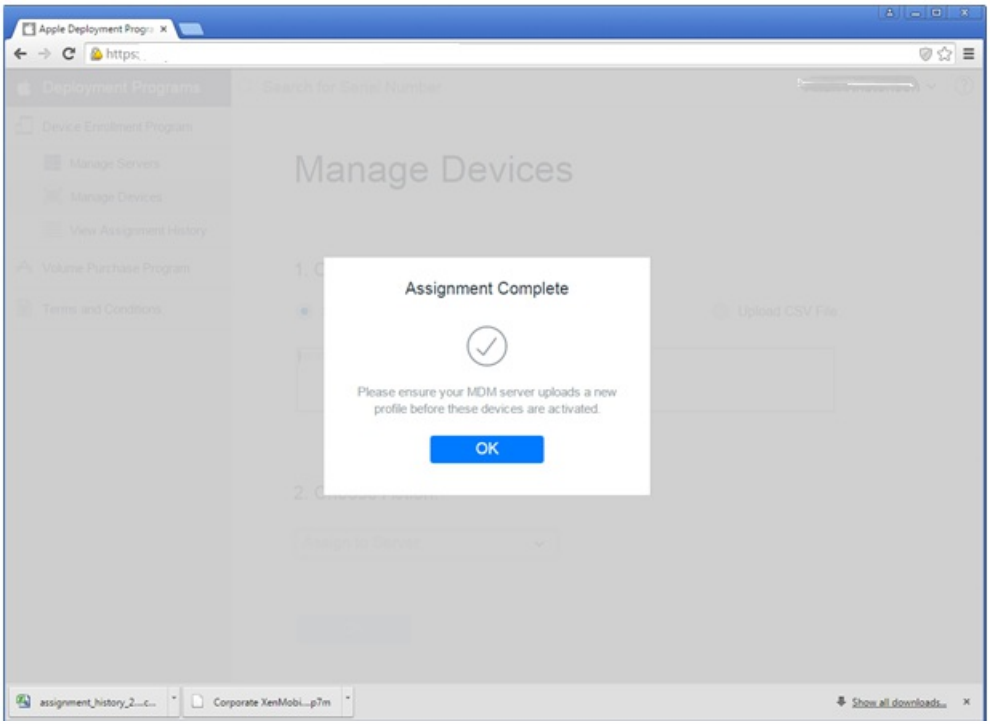


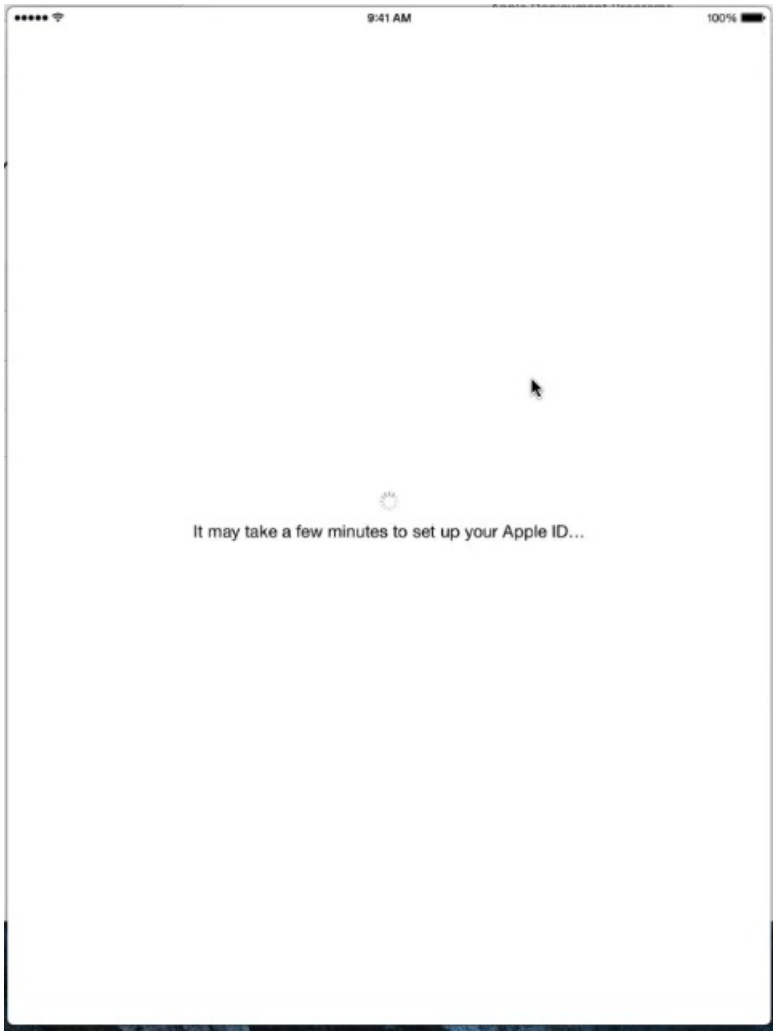


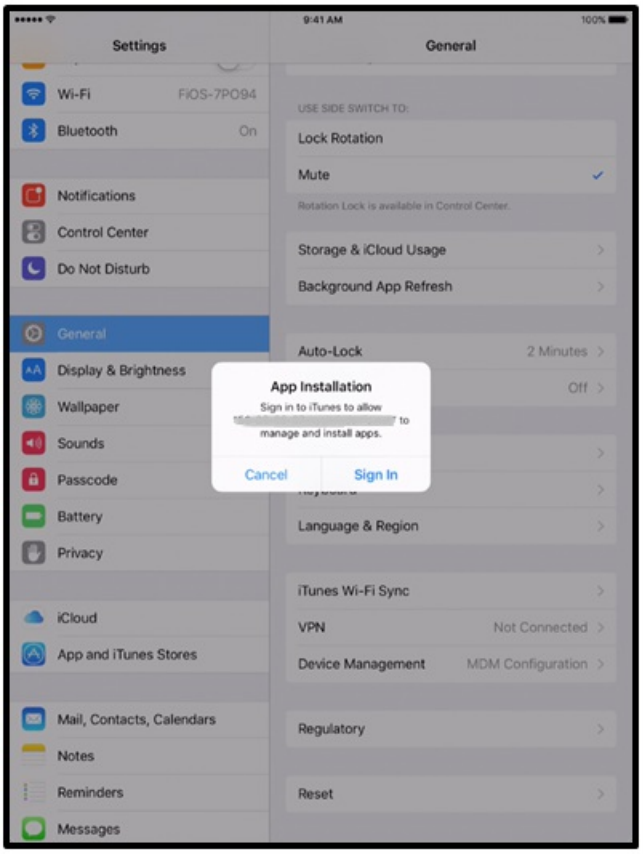


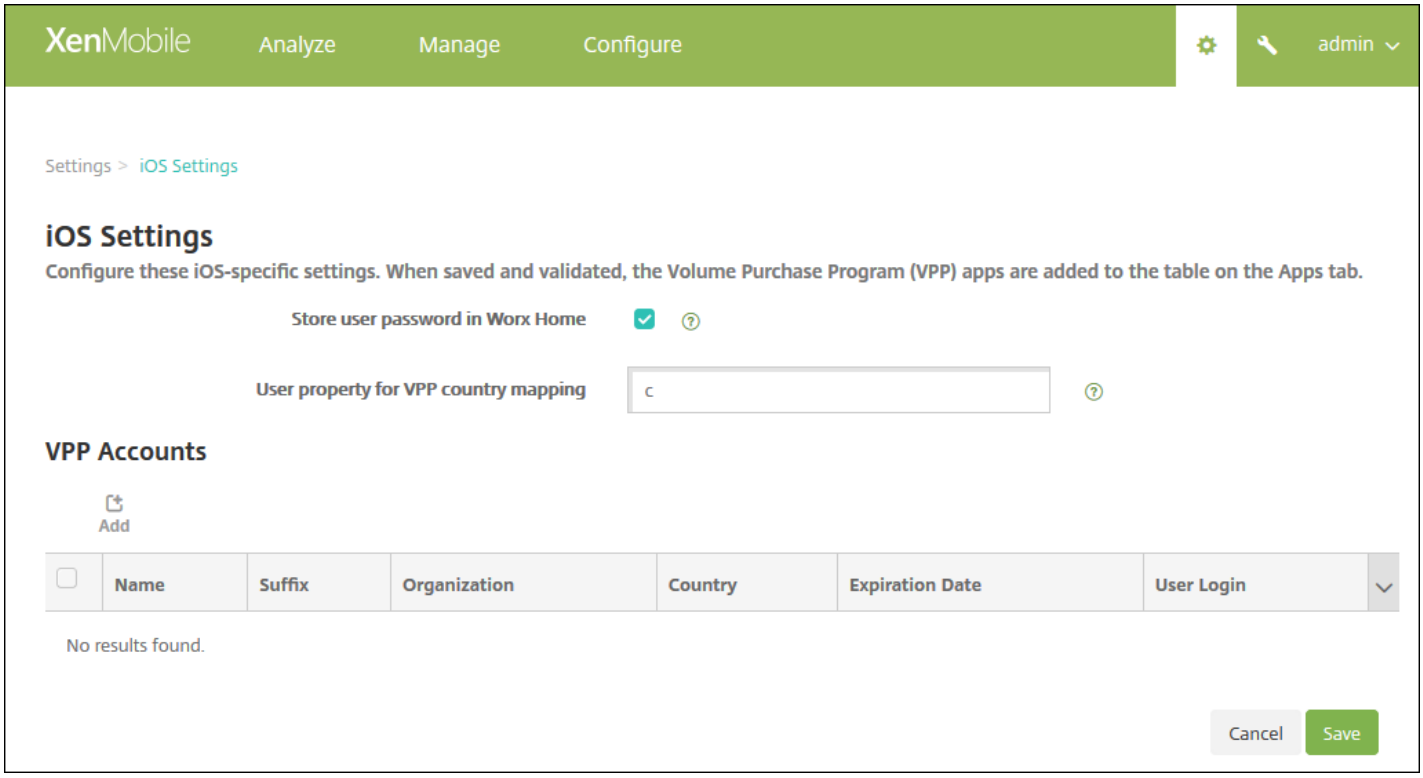






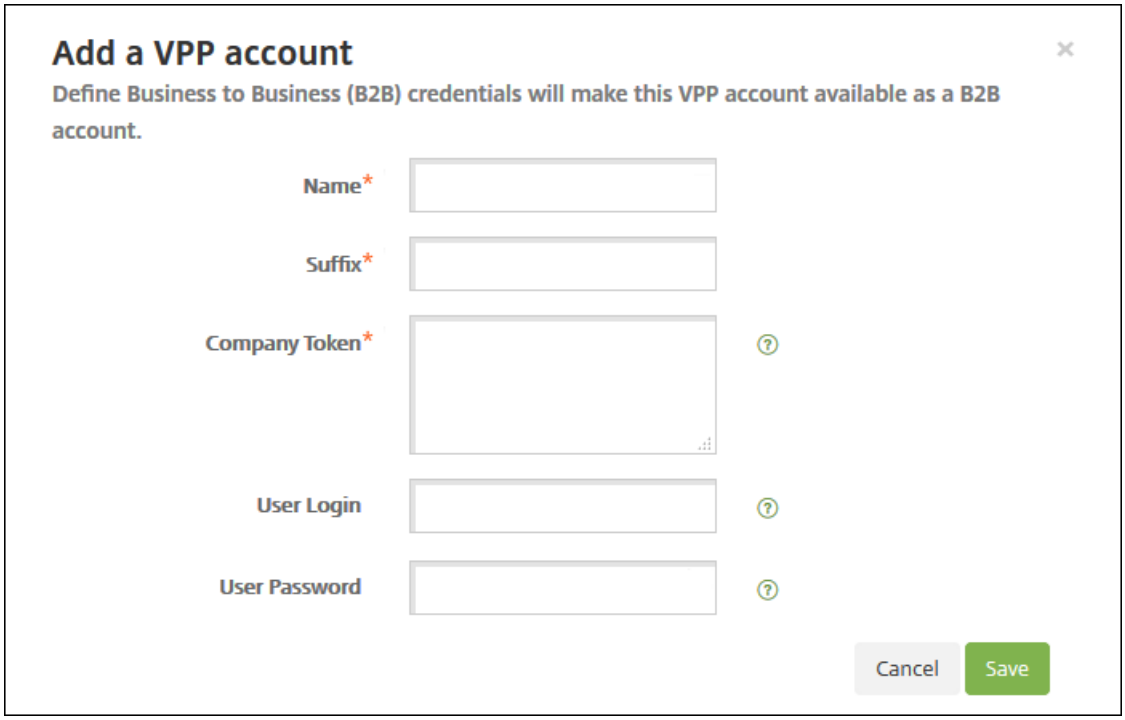




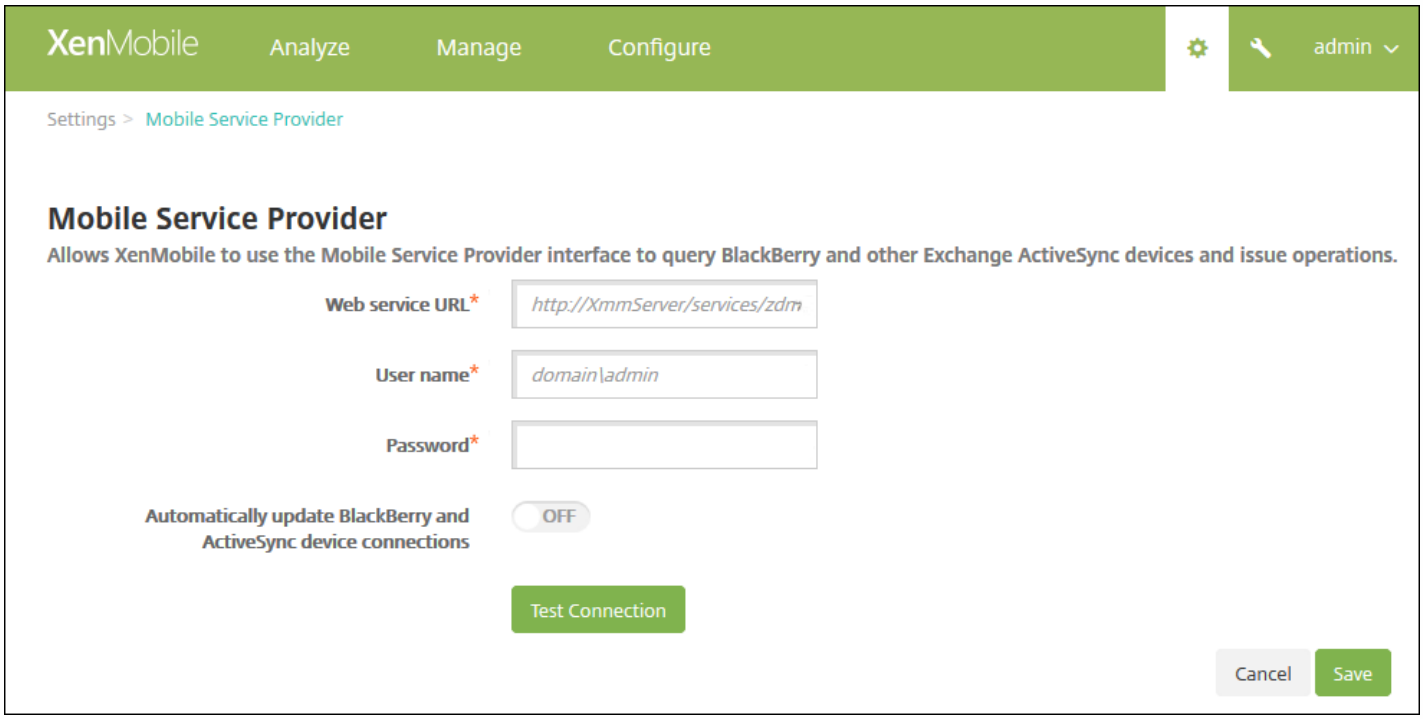


-
-

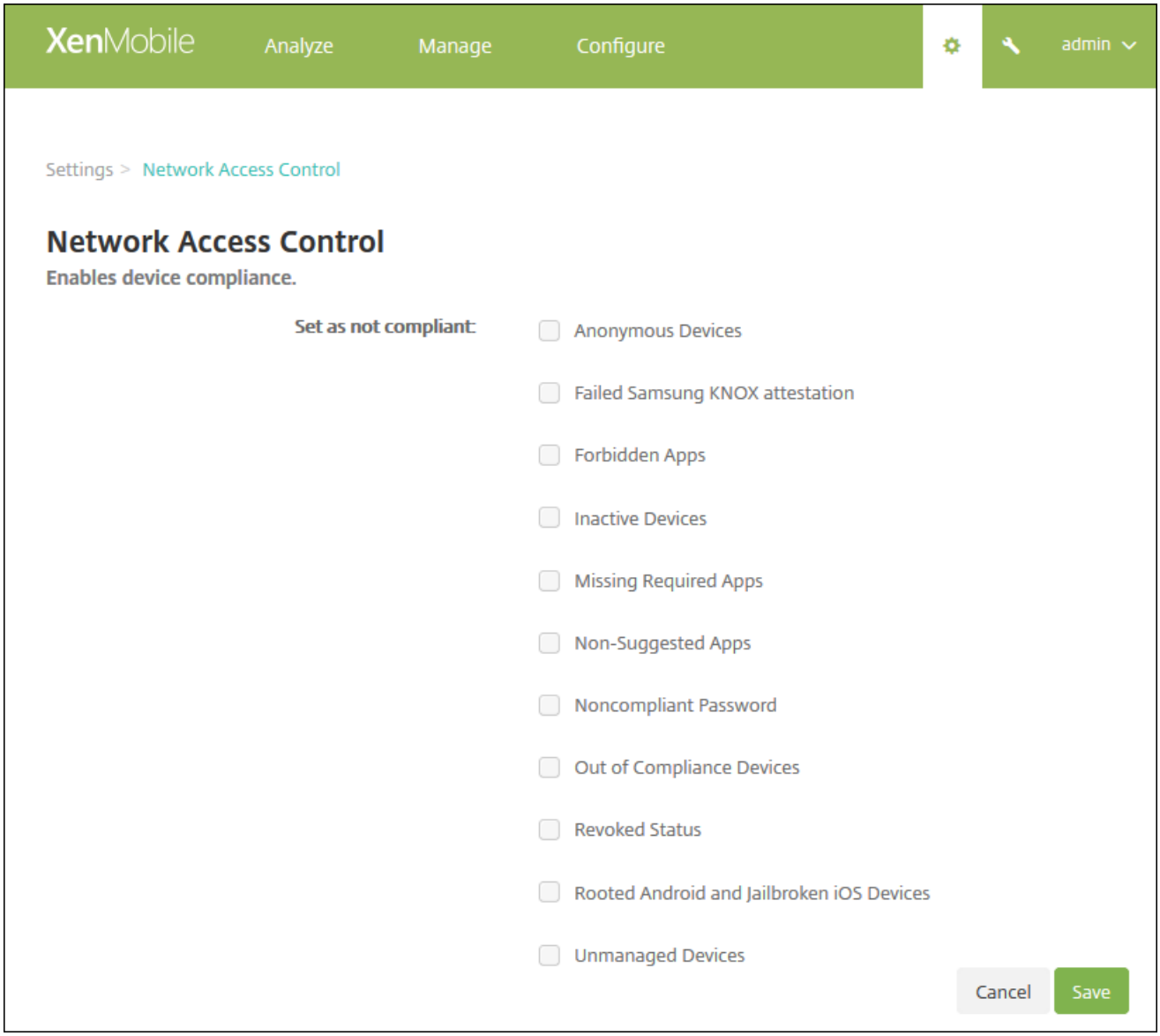
-

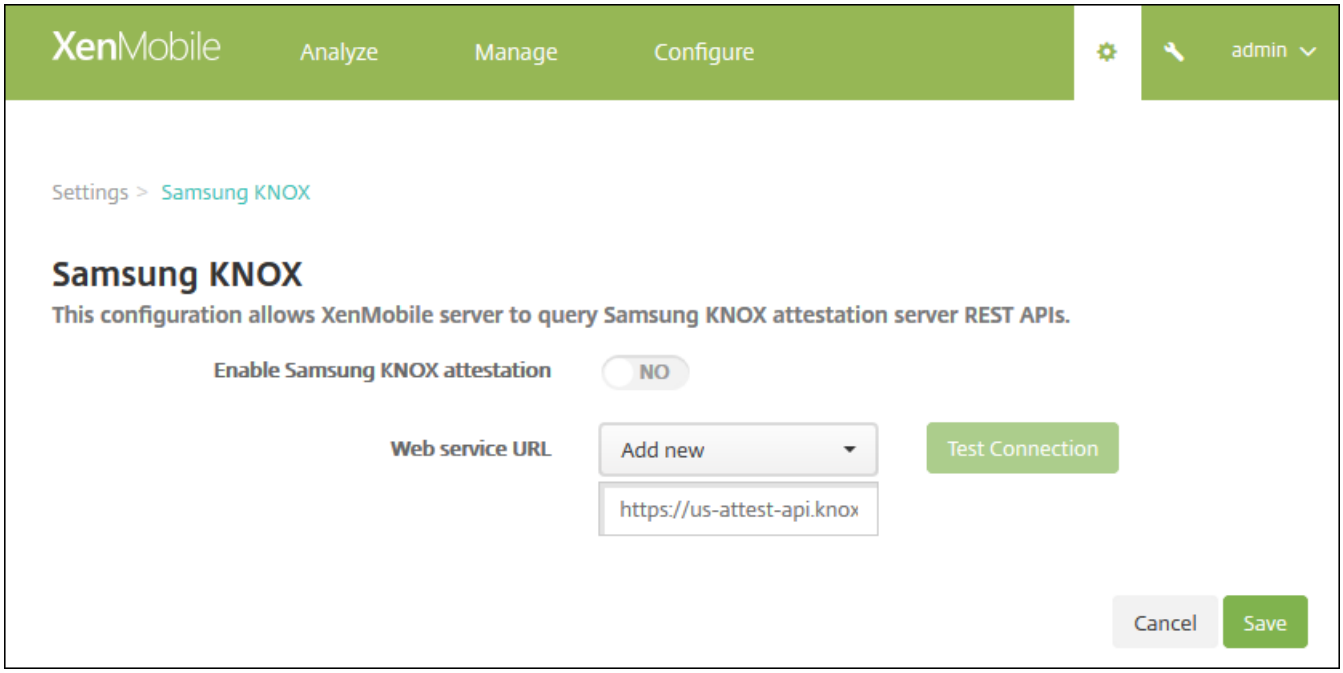


-
-
-
-
-



-
-
-
-
-





-
-

Para agregar, modificar o eliminar propiedades de servidor

Jul 27, 2016

XenMobile tiene más de 100 propiedades que corresponden a operaciones de servidor. En este artículo se describen algunas de las propiedades más importantes del servidor, y también se explica cómo agregar, editar o eliminar propiedades de servidor.

Definiciones de las propiedades del servidor

Audit Log Cleanup Execution Time

Hora de inicio de la limpieza del registro de auditoría, con el formato HH: MM AM/PM. Ejemplo: 04:00 AM. El valor predeterminado es **02:00 AM**.

Audit Log Cleanup Interval (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de auditoría. El valor predeterminado es **1**.

Audit Logger

Si es **False**, no registra eventos de interfaz de usuario (UI). El valor predeterminado es **False**.

Audit Log Retention (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de auditoría. El valor predeterminado es **7**.

Deploy Log Cleanup (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de implementación. El valor predeterminado es **7**.

Disable SSL Server Verification

Si es el valor es **True**, se inhabilita la validación de certificados SSL de servidor cuando se cumplen todas las condiciones siguientes: Se ha habilitado la autenticación basada en certificados en el servidor XenMobile, el servidor de la CA de Microsoft es el emisor del certificado y el certificado ha sido firmado por una CA interna cuya raíz no es de confianza para el servidor XenMobile. El valor predeterminado es **True**.

Inactivity Timeout in Minutes

El tiempo, en minutos, transcurrido el cual se cierra la sesión de un administrador inactivo que usó la API pública de XenMobile para acceder a la consola de XenMobile o cualquier aplicación de terceros. Si se especifica un tiempo de espera de **0**, el usuario inactivo permanece conectado, no se cierra su sesión. El valor predeterminado es **5**.

NetScaler Single Sign-On

Si el valor es **False**, se inhabilita la función de respuesta de XenMobile durante el inicio de sesión Single Sign-on desde NetScaler al servidor XenMobile. La función de respuesta se usa para verificar el ID de sesión de NetScaler Gateway, si

la configuración de NetScaler Gateway incluye una dirección URL de respuesta. El valor predeterminado es **False**.

Session Log Cleanup (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de sesiones. El valor predeterminado es **7**.

Unauthenticated App Download for Android Devices

Si el valor es **True**, se pueden descargar aplicaciones autoalojadas en dispositivos Android que ejecutan Android for Work. Esta propiedad es necesaria si la opción de Android for Work para suministrar una dirección URL en Google Play Store de forma estática está habilitada. En ese caso, las direcciones URL de descarga no pueden incluir un tíquet de uso único (definido por la propiedad de servidor **XAM One-Time Ticket**) que tiene el token de autenticación. El valor predeterminado es **False**.

Unauthenticated App Download for Windows Devices

Sólo se utiliza para versiones anteriores de Worx Home que validan los tiquets de un solo uso. Si el valor es **False**, puede descargar aplicaciones no autenticadas desde XenMobile en dispositivos Windows. El valor predeterminado es **False**.

XAM One-Time Ticket

La validez, en milésimas de segundo, de un token de autenticación de un solo uso (One-Time Token, OTT) para descargar una aplicación. Esta propiedad se utiliza junto con las propiedades **Unauthenticated App download for Android** y **Unauthenticated App download for Windows**, que especifican si se deben permitir descargas de aplicaciones no autenticadas. El valor predeterminado es **3600000**.

XenMobile MDM Self Help Portal console max inactive interval (minutes)

El tiempo, en minutos, transcurrido el cual se cierra la sesión de un usuario inactivo en el Self Help Portal de XenMobile. Si se especifica un tiempo de espera de **0**, el usuario inactivo permanece conectado, no se cierra su sesión. El valor predeterminado es **30**.

Cómo agregar, editar o eliminar propiedades de servidor

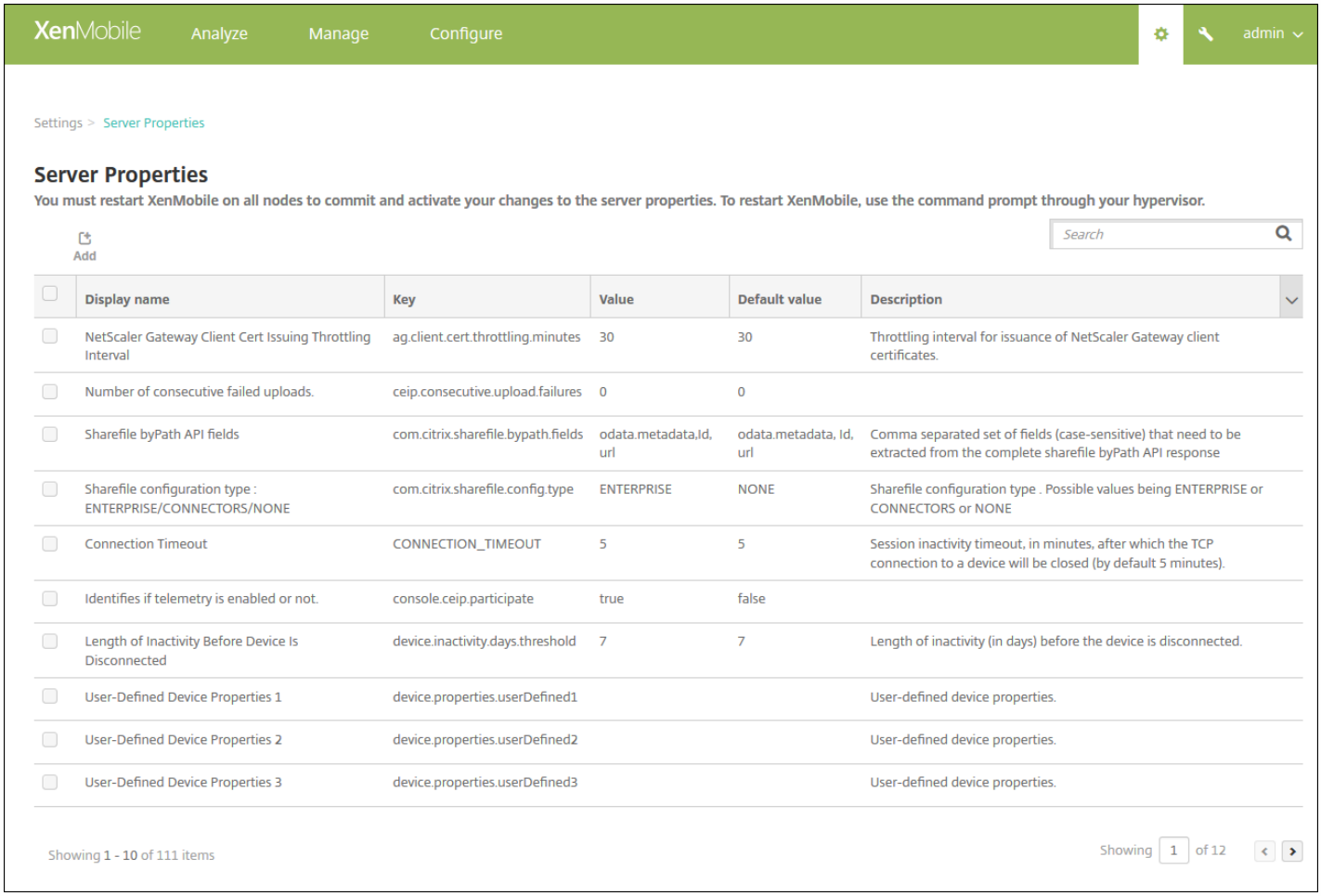
En XenMobile, se pueden aplicar propiedades al servidor. Después de realizar cambios, debe reiniciar XenMobile en todos los nodos para confirmar y activar los cambios.

> **Nota**
>
> Para reiniciar XenMobile, use la línea de comandos a través del hipervisor.

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**.

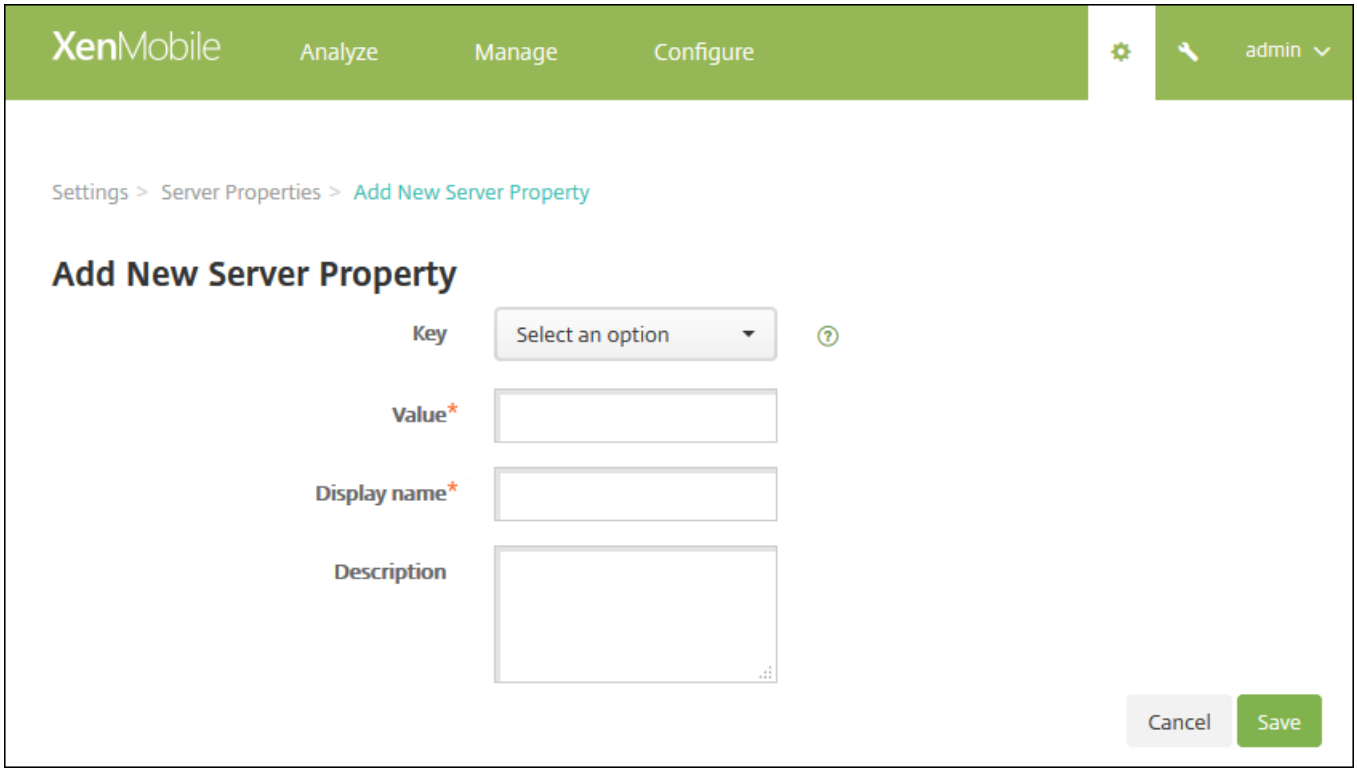
2. En **Server**, haga clic en **Server Properties**. Aparecerá la página **Server Properties**. Puede agregar, modificar o eliminar

propiedades de servidor desde esta página.



Para agregar una propiedad de servidor

1. Haga clic en **Add**. Aparecerá la página **Add New Server Property**.



2. Configure los siguientes parámetros:

- **Key**. En la lista, seleccione la clave apropiada. 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 quiere, escriba una descripción de la nueva directiva de servidor.

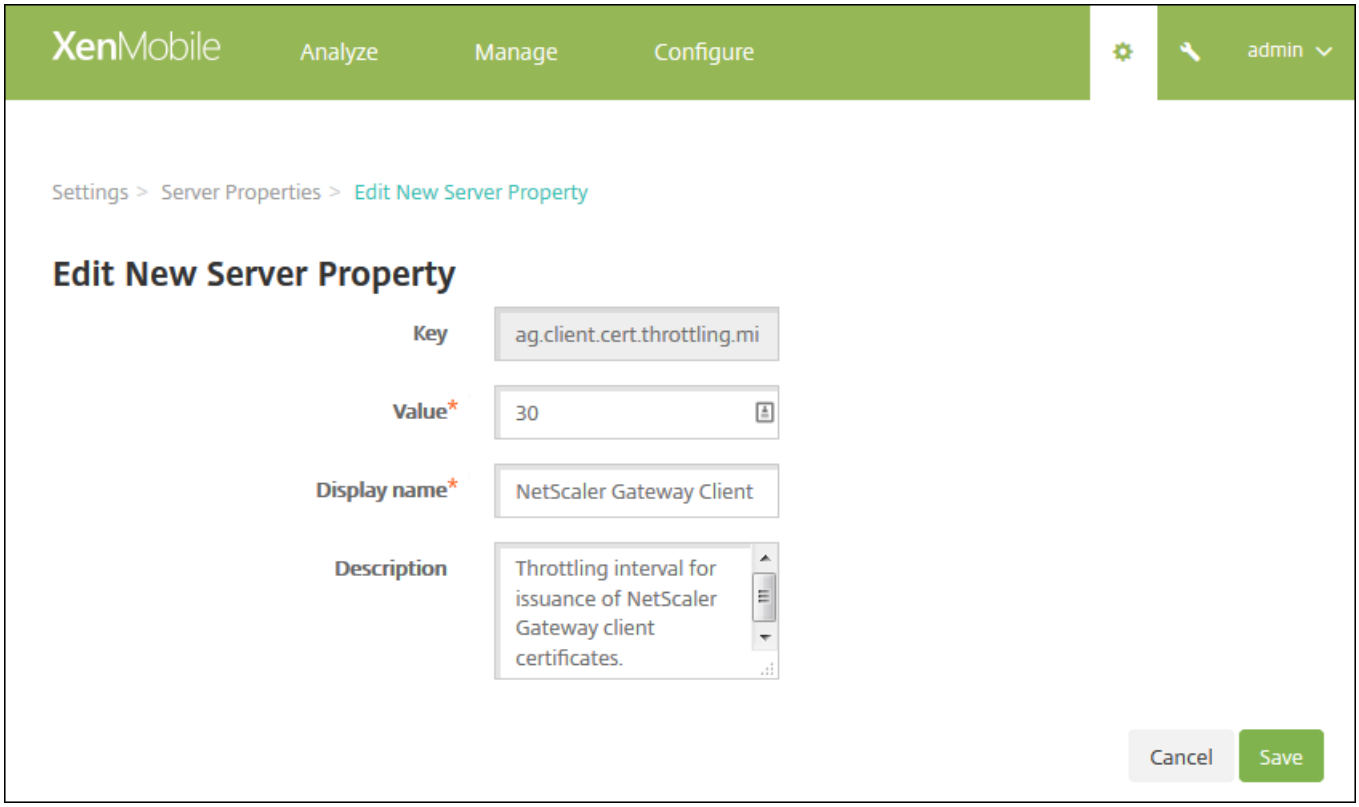
3. Haga clic en **Save**.

Para modificar una propiedad de servidor

1. En la tabla **Server Properties**, seleccione la propiedad de servidor que quiere modificar.

> **Nota**: Si marca la casilla situada junto a una propiedad de servidor, el menú de opciones aparecerá encima de la lista de propiedades de servidor. En cambio, si hace clic en cualquier lugar de la lista, el menú de opciones aparecerá a la derecha de la lista.

2. Haga clic en **Edit**. Aparecerá la página **Edit New Server Property**.



3. Cambie la siguiente información como corresponda:

- **Key**. Este campo no puede cambiarse.
- **Value**. El valor de la propiedad.
- **Display Name**. El nombre de la propiedad.
- **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 servidor

1. En la tabla **Server Properties**, seleccione la propiedad de servidor 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**.

Configuración del modo de servidor efectivo de XenMobile

Jul 27, 2016

En XenMobile, el modo del servidor es un valor establecido en Server Properties. Puede establecer el valor en MAM, MDM o ENT, correspondientes a la administración de aplicaciones, la administración de dispositivos o la administración de aplicaciones y dispositivos respectivamente. Defina la propiedad Server Mode en función de cómo quiere que se registren los dispositivos, según se indica en la tabla más abajo. El modo predeterminado del servidor es ENT, independientemente del tipo de licencia.

Para obtener información sobre cómo establecer el modo de servidor, consulte Para agregar, modificar o eliminar propiedades de servidor.

La siguiente tabla resume la configuración de modo de servidor que debe usarse para el determinado tipo de licencia y modo de dispositivo que se desee:

Tiene licencias para esta edición	Quiere que los dispositivos se registren en este modo	Defina la propiedad Server Mode con el valor
ENT / ADV / MDM	Modo MDM	MDM
ENT / ADV	Modo MAM (también llamado "modo solo MAM")	MAM
ENT / ADV	Modo MDM+MAM	ENT Los usuarios que deciden no participar en la administración de dispositivos funcionarán bajo el modo MAM antiguo.

El *modo efectivo de servidor* es una combinación del tipo de licencia y del modo del servidor. Para una licencia MDM, el modo efectivo del servidor es siempre MDM, independientemente de cómo esté configurado el parámetro de modo del servidor. Si tiene una licencia de MDM Edition, no puede habilitar la administración de aplicaciones definiendo el modo del servidor en MAM o ENT. Para licencias Enterprise y Advanced, el modo efectivo del servidor coincide con el modo del servidor.

El modo de servidor se agrega a los registros del servidor cada vez que se activa o se elimina una licencia, y cuando el modo de servidor se cambia en Server Properties. Para obtener información acerca de la creación y la visualización de archivos de registros, consulte Mantenimiento y asistencia de XenMobile.

SysLog

Jul 27, 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. Se graban los eventos de administrador y los eventos de usuario.

Puede configurar el servidor para recopilar los siguientes tipos de información:

- Registros del sistema que contienen un registro de las acciones que lleva a cabo XenMobile.
- Registros de auditoría que contienen un registro cronológico de las actividades del sistema referentes a XenMobile.

La información de registro que obtiene un servidor syslog desde un dispositivo se almacena en un archivo de registros en forma de mensajes. Por regla general, estos mensajes contienen la siguiente información:

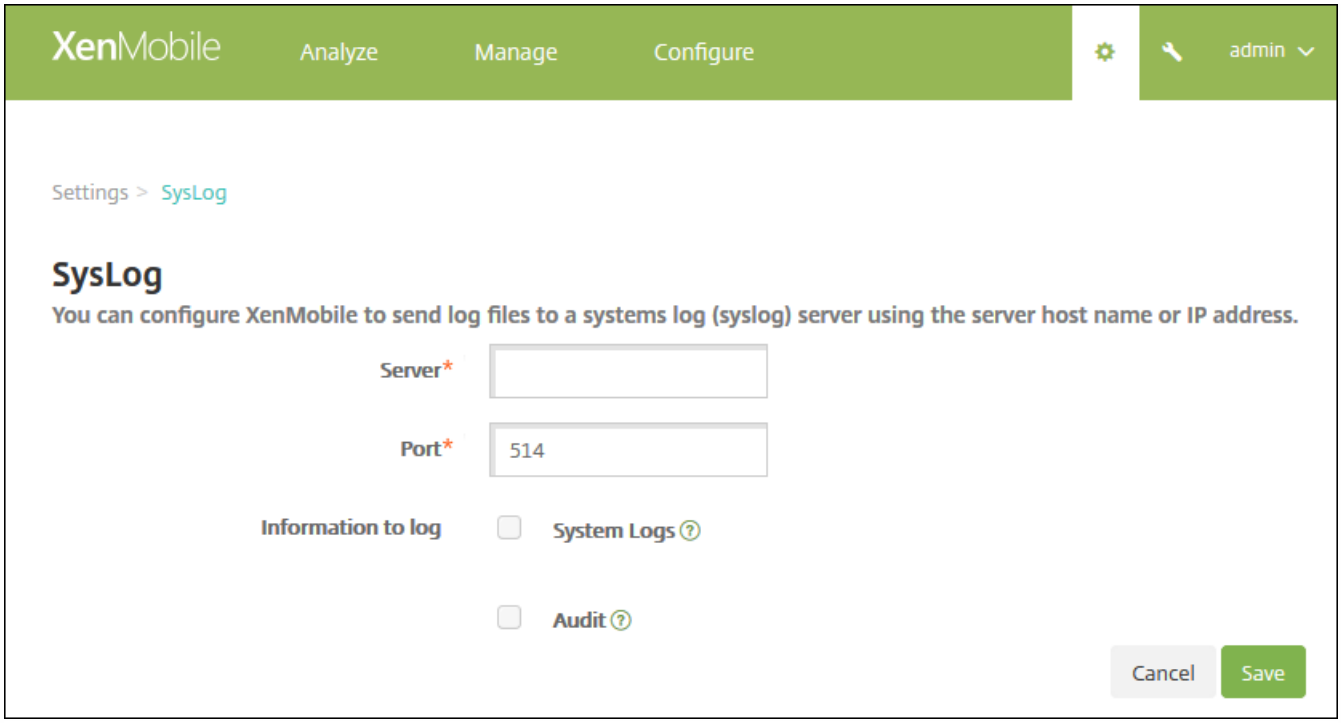
- La dirección IP del dispositivo que generó el mensaje de registro
- Una marca de tiempo
- El tipo de mensaje
- El nivel de registro asociado a un evento (crítico, error, aviso, advertencia, informativo, depuración, alerta o emergencia)
- La información del mensaje

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 más información, consulte Cómo ver y analizar archivos de registros en 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. Haga clic en **Syslog**. Aparecerá la página **Syslog**.



3. Configure los siguientes parámetros:

- **Name**: Escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor syslog.
- **Port**: Escriba el número de puerto. De forma predeterminada, el puerto está configurado en 514.
- **Information to log**. Marque o desmarque **System Logs** y **Audit**.
  - Los registros del sistema contienen las acciones llevadas a cabo por XenMobile.
  - Los registros de auditoría contienen un registro cronológico de las actividades del sistema para XenMobile.

4. Haga clic en **Save**.

Cómo configurar XenApp y XenDesktop

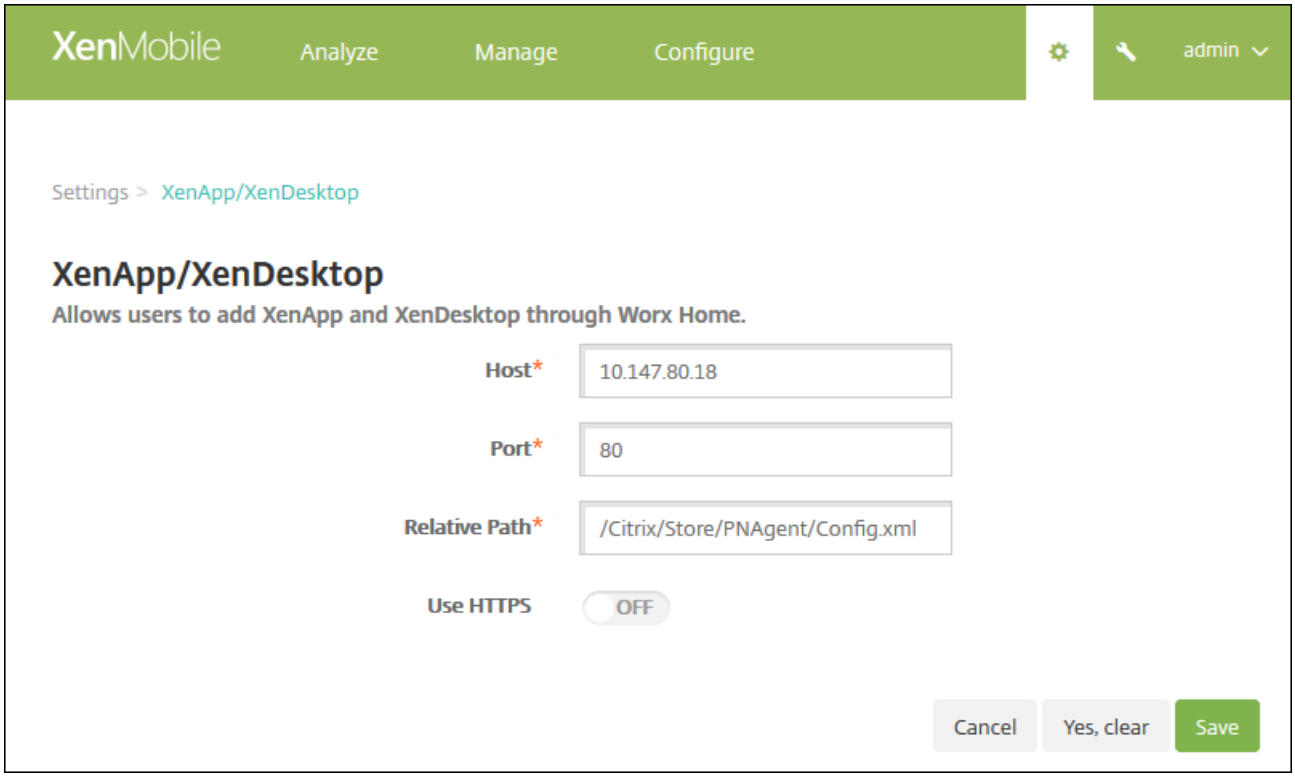
Jul 27, 2016

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. Receiver debe estar instalado en los dispositivos de los usuarios para iniciar las aplicaciones, pero no es necesario configurarlo.

Para configurar este parámetro, se necesita el nombre de dominio completo (FQDN) o la dirección IP y el número de puerto de StoreFront o del sitio de Interfaz Web.

1. En la consola Web de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

2. Haga clic en **XenApp/XenDesktop**. Aparecerá la página **XenApp/XenDesktop**.



3. Configure los siguientes parámetros:

- **Host**. Escriba el nombre de dominio completo (FQDN) o la dirección IP de StoreFront o del sitio de Interfaz Web.
- **Port**. Escriba el número de puerto de StoreFront o del sitio de Interfaz Web. El valor predeterminado es 80.
- **Relative Path**. Escriba la ruta de acceso. Por ejemplo, /Citrix/PNAgent/config.xml.
- **Use HTTPS**. Seleccione si habilitar la autenticación segura entre StoreFront o el sitio de Interfaz Web y el dispositivo cliente. El valor predeterminado es **OFF**.

4. Haga clic en **Save**.

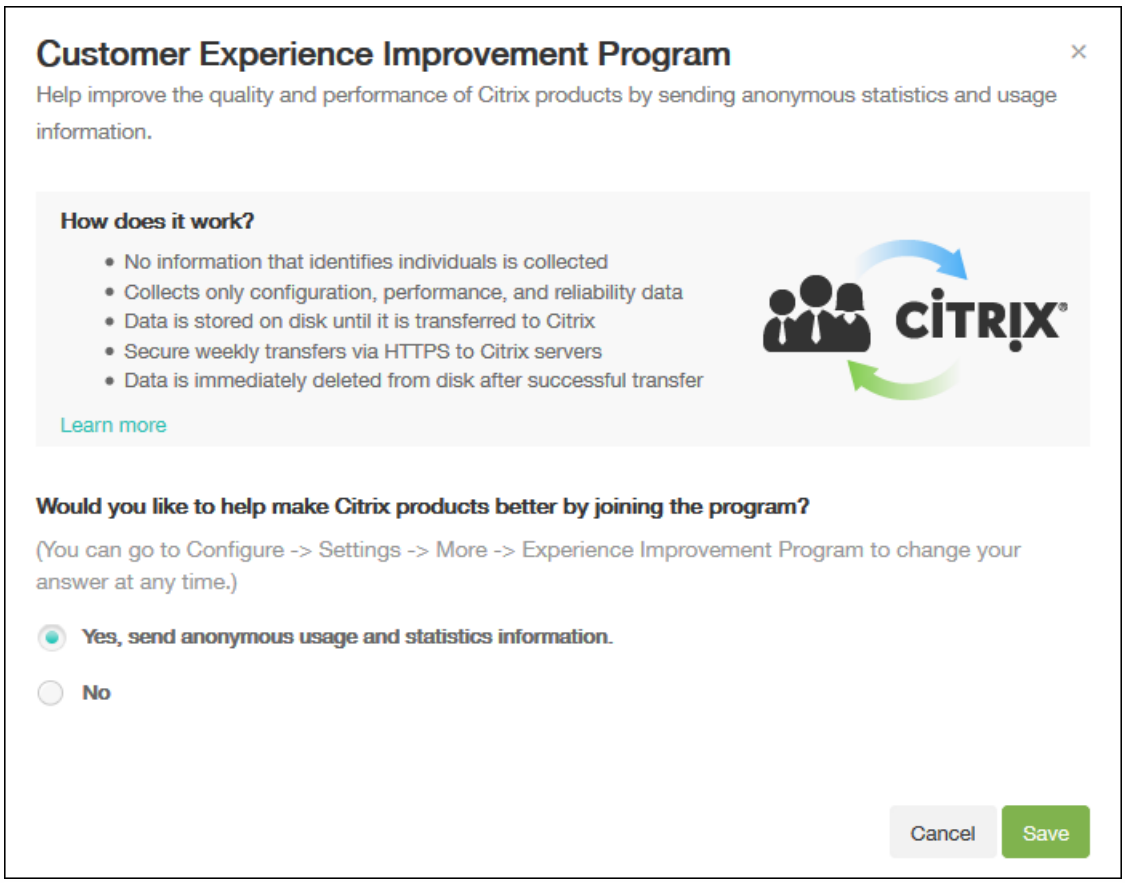
Programa para la mejora de la experiencia del usuario

Jul 27, 2016

El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información anónima de uso y de configuración de XenMobile y envía esos datos automáticamente a Citrix. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de XenMobile. La participación en el programa CEIP es voluntaria. La opción de participar en el programa CEIP se ofrece la primera vez que se instala XenMobile o una actualización. Si participa en el programa, los datos de configuración se recopilan normalmente una vez por semana, mientras que los datos de uso y rendimiento se recopilan cada hora. Los datos se guardan en disco y se transfieren de manera segura vía HTTPS a Citrix una vez por semana. Puede cambiar la participación en el programa CEIP en la consola de XenMobile. Para obtener más información acerca del programa para la mejora de la experiencia del usuario, consulte Acerca del programa Customer Experience Improvement Program de Citrix (CEIP).

Programa CEIP al instalar o actualizar XenMobile

La primera vez que instale XenMobile o cuando realice una actualización, verá el siguiente cuadro de diálogo, donde puede seleccionar si participar o no en el programa; a continuación, haga clic en **Save**.

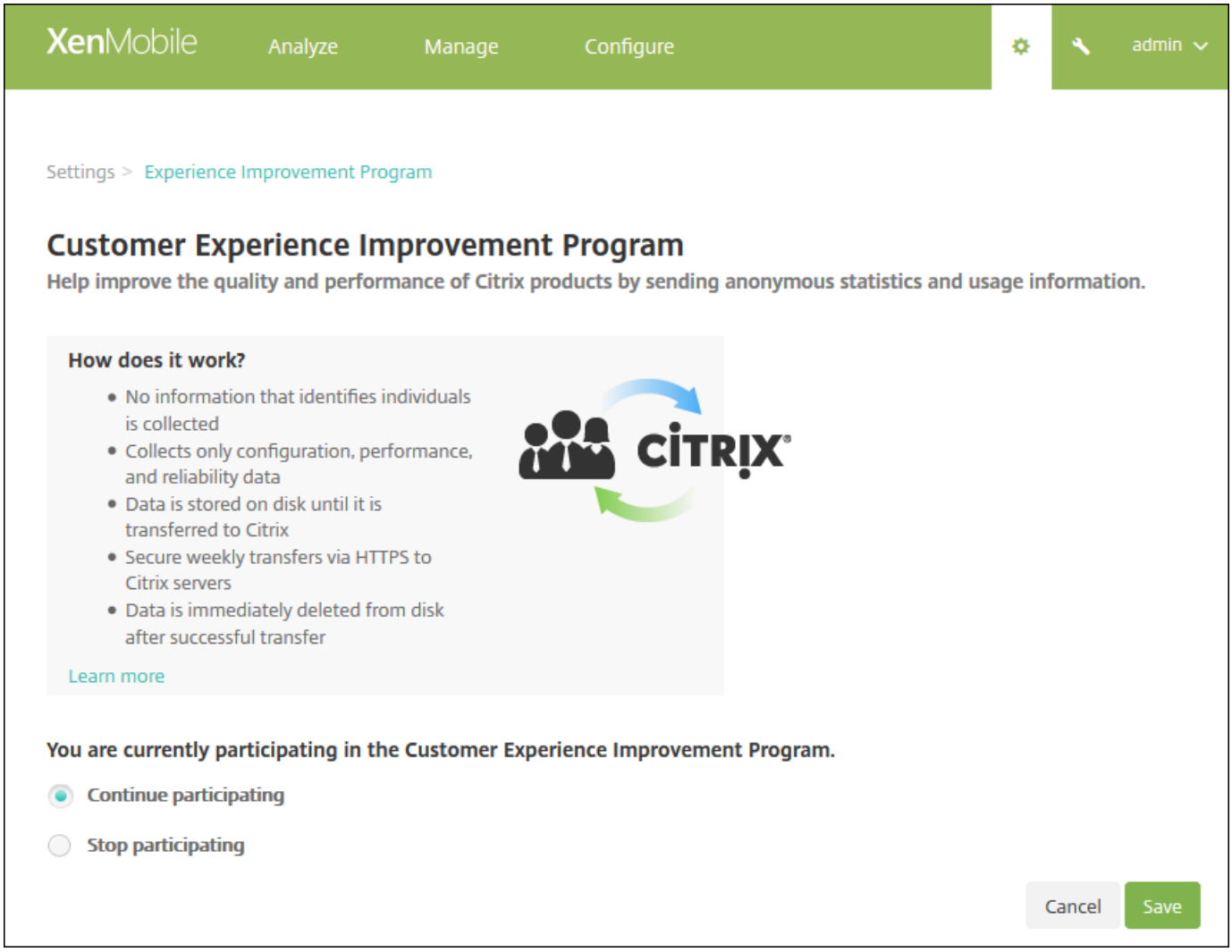


Cómo cambiar el parámetro de participación en el programa CEIP

1. Para cambiar el parámetro de participación en el programa CEIP, en la consola de XenMobile, haga clic en el icono con forma de engranaje ubicado en la esquina superior derecha de la consola para abrir la página **Settings**.

2. En **Server**, haga clic en **Experience Improvement Program**. Aparecerá la página **Customer Experience Improvement**

Program. La página exacta que vea depende de si participa actualmente en el programa CEIP.



3. Si participa actualmente en el programa CEIP y quiere dejar de hacerlo, haga clic en **Stop participating**.

4. Si no participa actualmente en el programa CEIP y quiere hacerlo, haga clic en **Start participating**.

5. Haga clic en **Save**.

Configuración de Microsoft Azure

Jul 27, 2016

Los dispositivos que ejecutan Windows 10 se inscriben con Azure como método federado de autenticación de Active Directory. Puede unir dispositivos Windows 10 con Microsoft Azure Active Directory de cualquiera de las siguientes maneras:

- Inscribirse en MDM como parte de Azure AD Join la primera vez que se encienda el dispositivo.
- Inscribirse en MDM como parte de Azure AD Join desde la página de configuración de Windows una vez que el dispositivo esté configurado.

Necesita una licencia Premium de Microsoft Azure Active Directory para poder integrar XenMobile con Microsoft Azure. La licencia es necesaria para permitir la integración MDM con Azure Active Directory para que los usuarios con dispositivos Windows 10 puedan inscribirse mediante Azure Active Directory. Consulte Microsoft Azure para obtener información sobre la obtención de la licencia Premium. Para obtener información acerca de los precios, consulte Precios de Active Directory de Azure.

Antes de que los usuarios de dispositivos Windows puedan inscribirse con Azure, se deben configurar los parámetros del servidor Microsoft Azure en XenMobile y la directiva de términos y condiciones para dispositivos Windows. En este artículo, se describe cómo configurar los parámetros de Microsoft Azure. Para obtener información acerca de la configuración de una directiva de términos y condiciones para dispositivos Windows, consulte las Directivas de términos y condiciones.

Antes de configurar los parámetros del servidor Microsoft Azure en XenMobile, debe iniciar sesión en el portal de Azure AD y llevar a cabo lo siguiente:

1. Registre el dominio personalizado y verifíquelo. Para obtener más información, consulte Incorporación de su propio nombre de dominio a Azure Active Directory.

2. Extienda el directorio local a Azure Active Directory mediante las herramientas de integración de directorios. Para obtener más información, consulte Integración de directorios.

3. Haga de MDM una parte fiable de Azure Active Directory. Para ello, haga clic en **Azure Active Directory** > **Aplicaciones** y, a continuación, haga clic en **Agregar**. Seleccione **Agregar una aplicación** de la galería. Vaya a **ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES**, seleccione **Aplicación MDM local** y guarde la configuración.

4. En la aplicación, configure los términos de uso de los dispositivos de punto final, URI de ID de aplicación y la detección de servidores XenMobile de la siguiente manera:

- URL de detección MDM: https://:8443/zdm/wpe
- URL de condiciones de uso MDM: https://:8443/zdm/wpe/tou
- URI de ID de aplicación: https://:8443/

5. Seleccione la aplicación MDM local que ha creado en el paso 3 y habilite la opción **Administrar dispositivos para estos usuarios** para permitir la administración de dispositivos móviles de todos los usuarios o de un grupo de usuarios concreto.

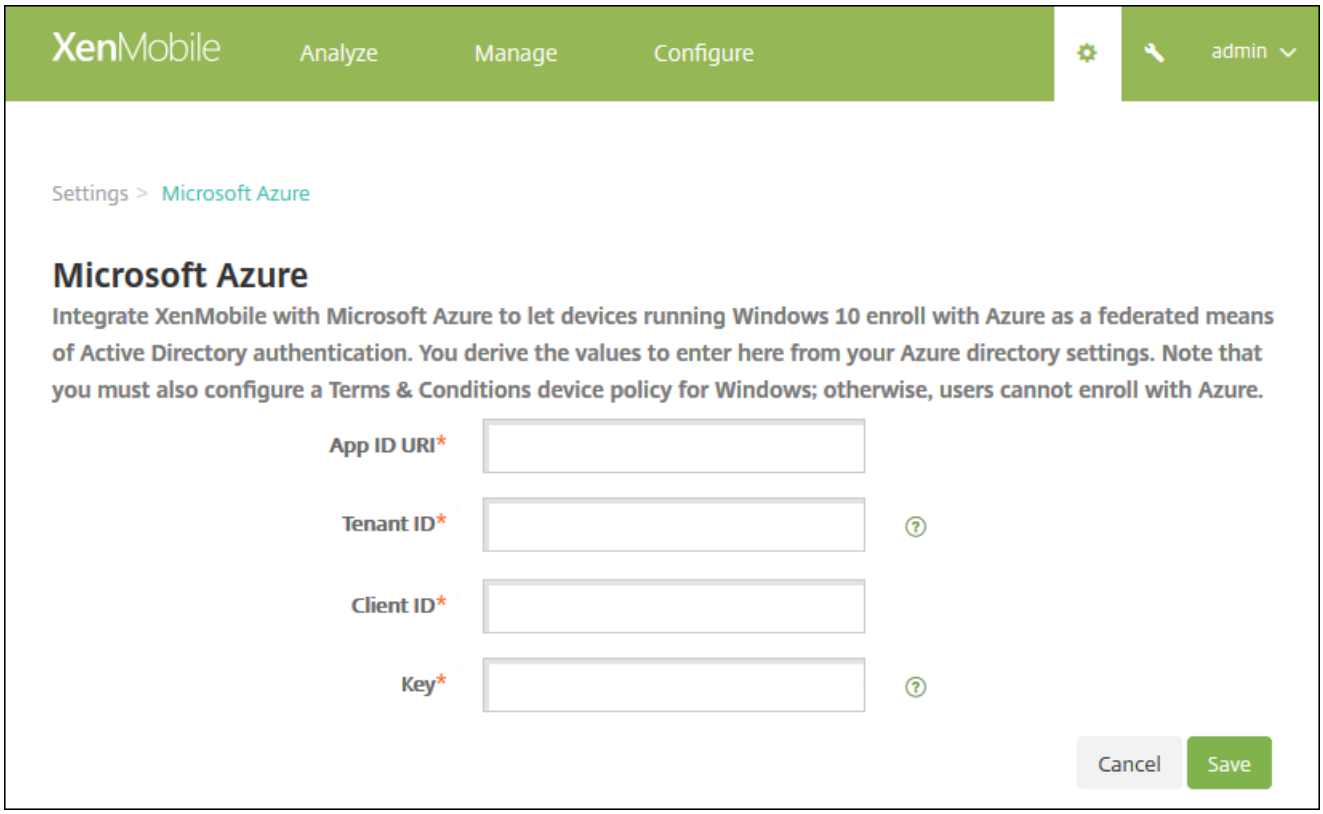
También tendrá que anotar la siguiente información de su cuenta de Microsoft Azure para configurar parámetros en la consola de XenMobile:

- URI de ID de aplicación. La dirección URL del servidor que ejecuta XenMobile.
- ID de inquilino. Obtenida desde la página de parámetros de la aplicación de Azure.
- ID de cliente. Un identificador único para la aplicación.

- Clave. Obtenida desde la página de parámetros de la aplicación de Azure.

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 **Microsoft Azure**. Aparece la página **Microsoft Azure**.



3. Configure los siguientes parámetros:

- **App ID URI**. Escriba la URL del servidor que ejecuta XenMobile que especificó cuando configuró Azure.
- **Tenant ID**. Copie este valor de la página Configuración de la aplicación de Azure. En la barra de direcciones del explorador, copie la sección de números y letras. Por ejemplo, en https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem..., el ID del inquilino es: *abc123-abc123-abc123*.
- **Client ID**. Copie y pegue este valor de la página Configuración de Azure. Este es el identificador único de su aplicación.
- **Key**. Copie este valor de la página Configuración de la aplicación de Azure. En **keys**, seleccione una duración de la lista y, a continuación, guarde la configuración. Ahora, puede copiar la clave y pegarla en este campo. Se necesita una clave para que las aplicaciones lean o escriban datos en Microsoft Azure Active Directory.

4. Haga clic en **Save**.

Important

Cuando los usuarios se unen a Azure AD en sus dispositivos Windows, las directivas de dispositivo para Worx Store y Weblink que se configuraron en XenMobile solo están disponibles para los usuarios de Azure AD y no para los usuarios locales. Para que los usuarios locales puedan usar estas directivas de dispositivo, deben hacer lo siguiente:

1. Unirse a Azure AD de parte de un usuario de Azure en **Settings** > **About** > **Join Azure AD**.
2. Cerrar la sesión en Windows y volver a iniciarla con una cuenta de Azure AD.

Google Cloud Messaging

Jul 27, 2016

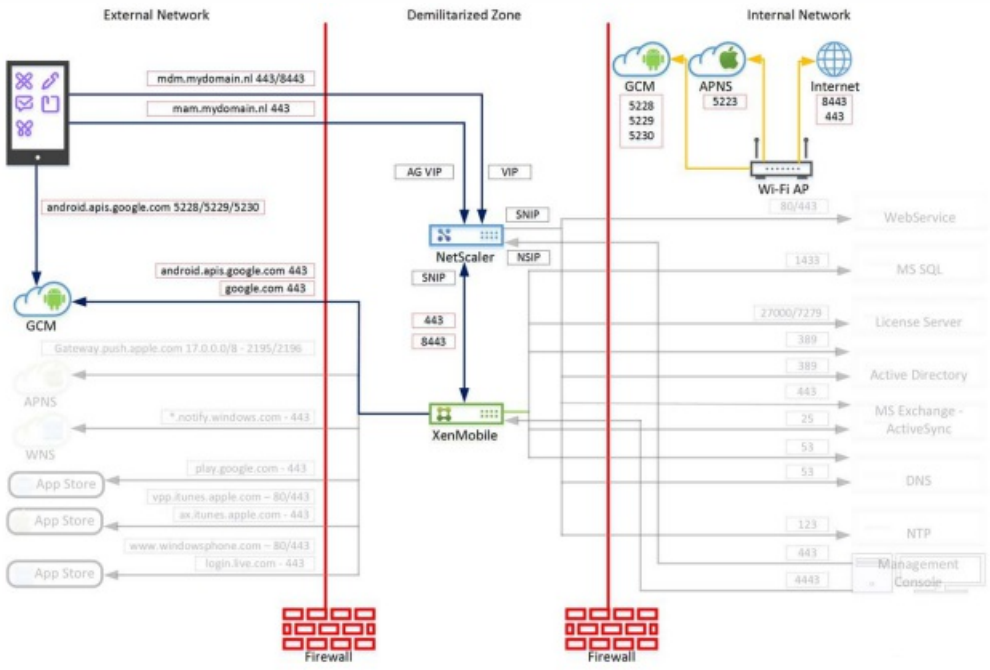
Como alternativa a la directiva MDX, **Active poll period**, puede usar desde Google Cloud Messaging (GCM) para controlar cómo y cuándo los dispositivos Android debe conectarse a XenMobile. Con la configuración que se describe en este artículo, cualquier acción de seguridad o comando de implementación desencadena una notificación push para Worx Home, para pedir al usuario que se reconecte con el servidor XenMobile.

Requisitos previos

- XenMobile 10.3.x
- El cliente más reciente de Worx Home
- Credenciales de cuenta de Google para desarrolladores
- Abra el puerto 443 en XenMobile para Android.apis.google.com y Google.com

Arquitectura

Este diagrama muestra el flujo de comunicación para GCM en la red interna y externa.

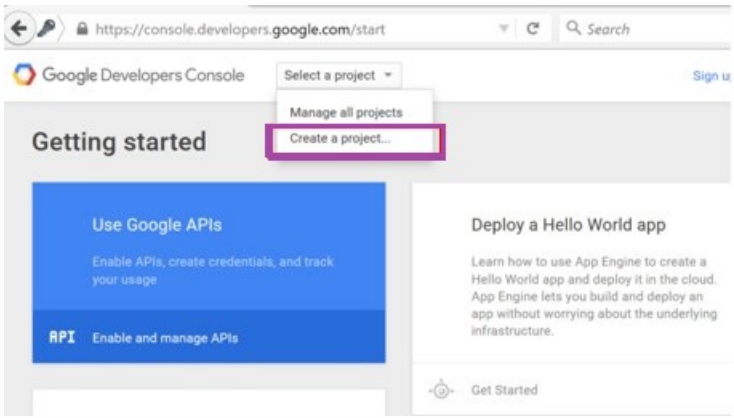


Para configurar su cuenta de Google para GCM

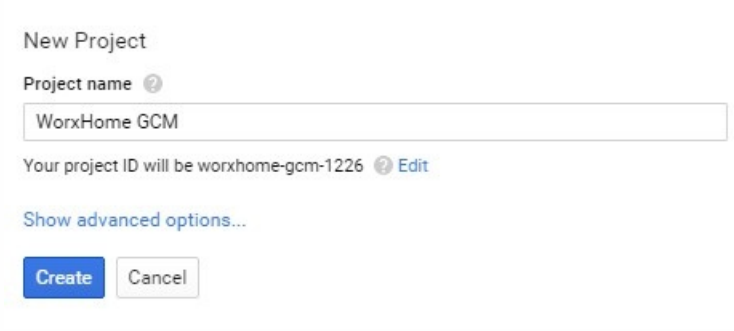
1. Inicie sesión en la siguiente dirección URL con las credenciales de la cuenta de Google para desarrolladores:

   https://console.developers.google.com

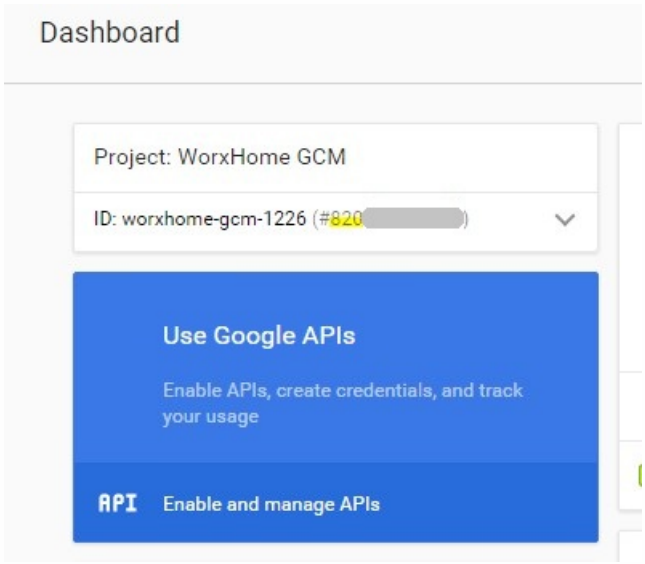
2. En **Selecciona un proyecto**, seleccione **Crear proyecto**.



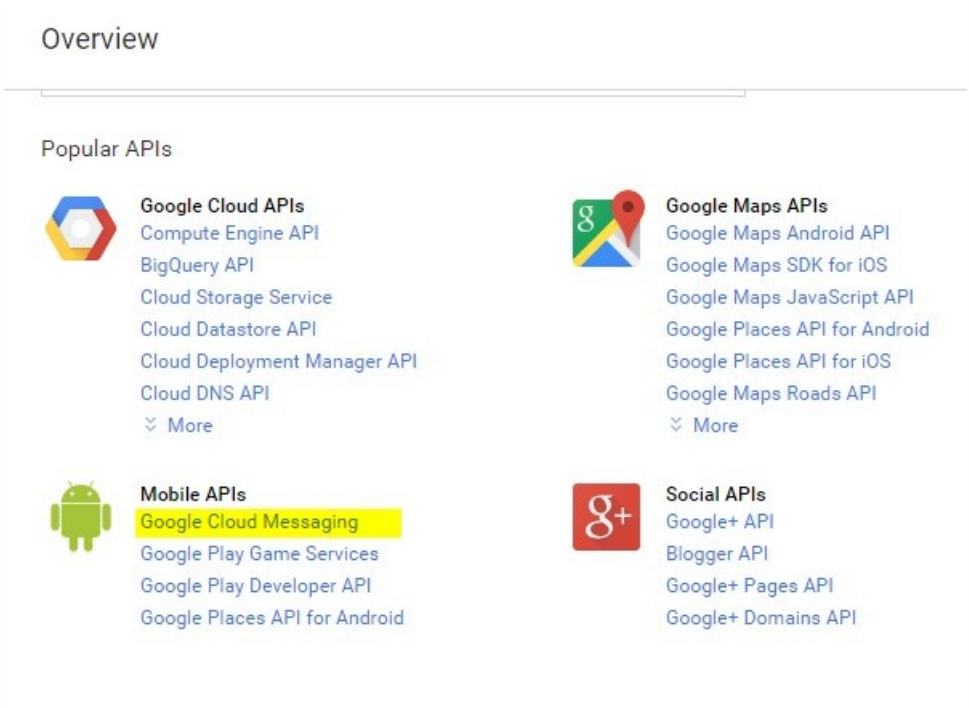
3. Introduzca un **Nombre del proyecto** y haga clic en **Crear**.



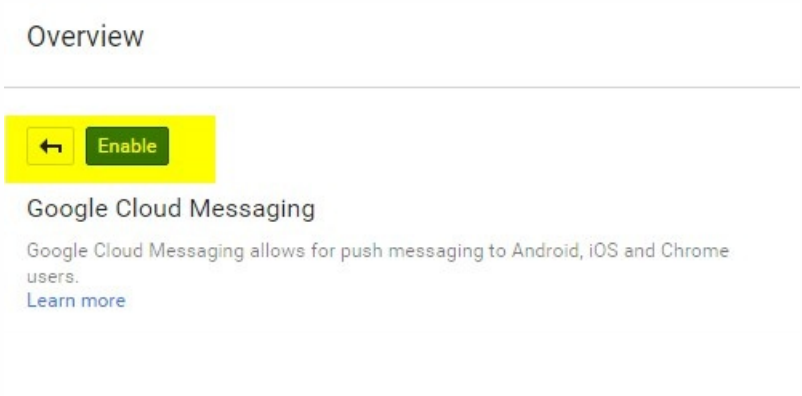
4. En el panel de control, se muestra su ID de envío (resaltado abajo) junto al ID del proyecto. Tome nota de ese ID de envío, porque tendrá que utilizarlo más tarde en los parámetros del servidor XenMobile. Haga clic en **Usar APIs de Google**.



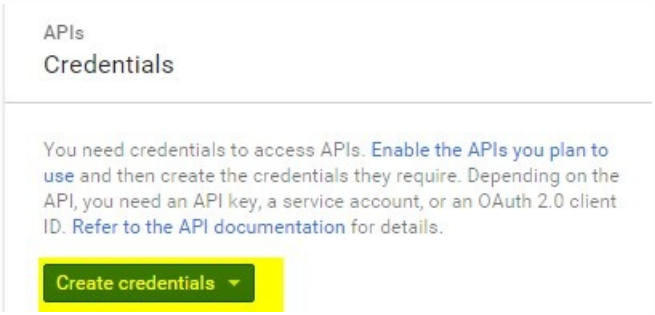
5. En la sección **APIs para móviles**, haga clic en **Google Cloud Messaging**.



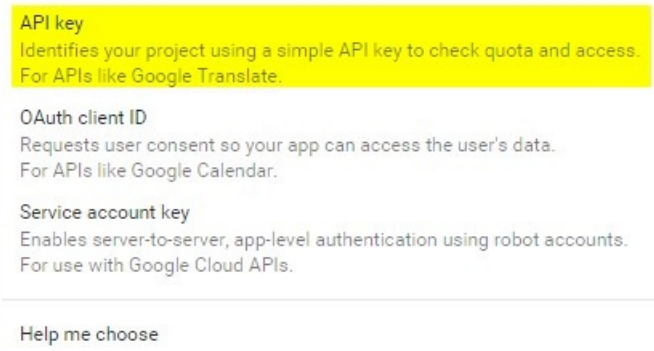
6. Haga clic en **Habilitar**.



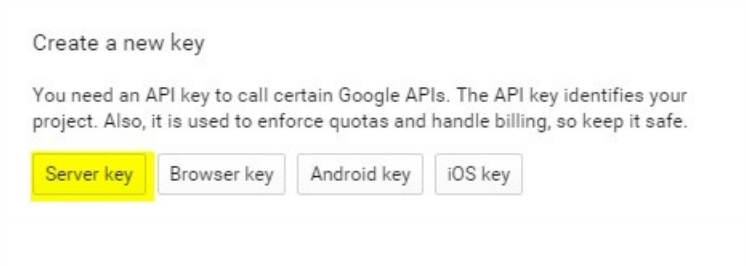
7. En **Credenciales**, haga clic en **Crear credenciales**.



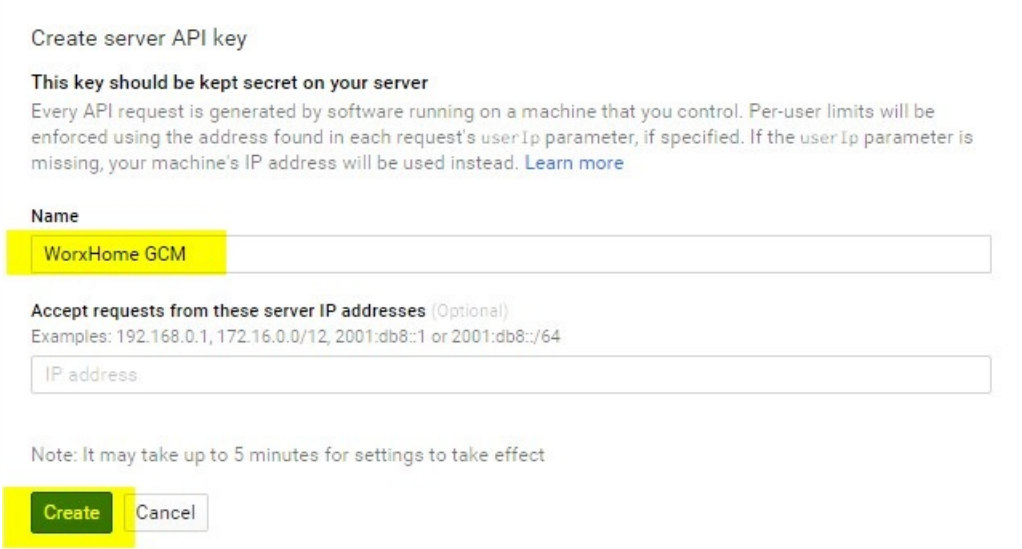
8. Haga clic en **Clave de API**.



9. En **Crear una clave nueva**, haga clic en **Clave de servidor**.



10. En **Crear clave API de servidor**, introduzca un **Nombre** (en este ejemplo, se usa el nombre del proyecto) y, a continuación, haga clic en **Crear**.



11. Tome nota de la clave de API. La necesitará para configurar XenMobile.

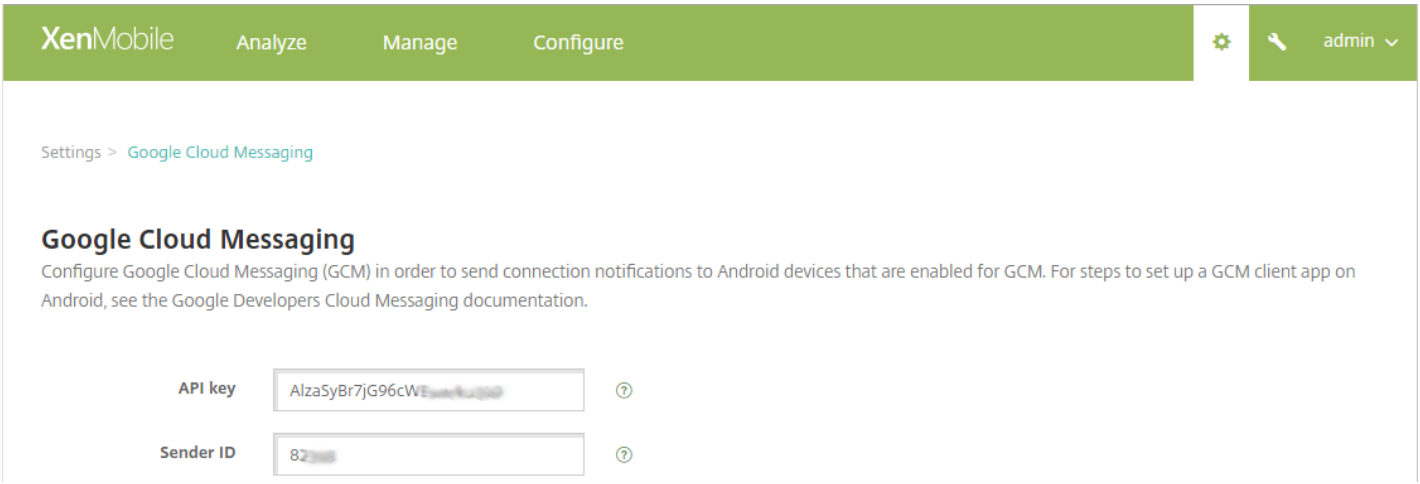
Para configurar XenMobile para GCM

1. Inicie sesión en la consola de administración de XenMobile y haga clic en **Settings > Google Cloud Messaging**.

    a. En **API key**, introduzca la clave API de GCM que copió en el último paso de la configuración de GCM.

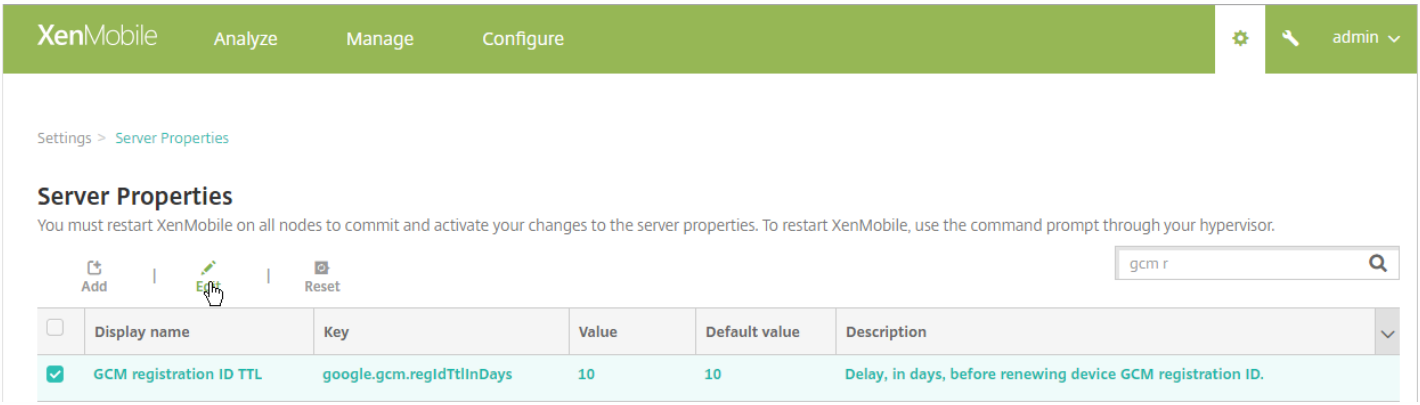
    b. En **Sender ID**, copie el ID de envío que anotó en el procedimiento anterior y haga clic en **Save**.

    Nota: La página **Settings > Google Cloud Messaging** es nueva en la versión 10.3.6 de XenMobile. Si no está usando la versión más reciente de XenMobile, vaya a **Settings > Server** para actualizar el valor de **API key** (google.gcm.apiKey) y de **Sender ID** (google.gcm.senderid).

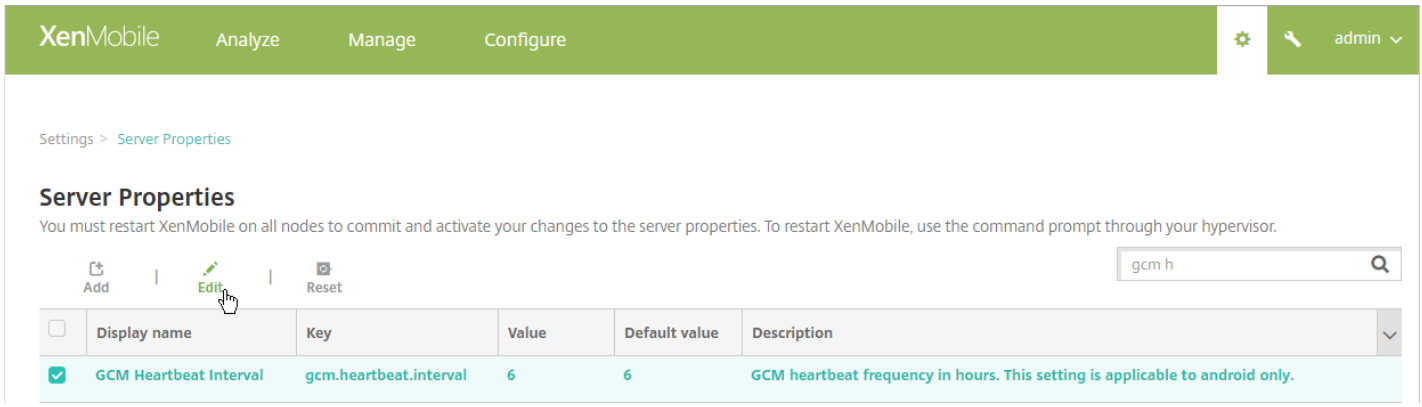


2. Si necesita cambiar los parámetros predeterminados de alguna de las siguientes propiedades, haga clic en **Settings > Server Properties**.

- **GCM Registration ID TTL:** La demora predeterminada antes de renovar el ID de registro de GCM del dispositivo es de **10** días. Para cambiar este valor, escriba **gcm r** en el cuadro de búsqueda, haga clic en **GCM Registration ID TTL**, y luego haga clic en **Edit**.



- **GCM Heartbeat Interval:** La frecuencia predeterminada con la que XenMobile se comunica con el servidor GCM es de **6** horas. Para cambiar este valor, escriba **gcm h** en el cuadro de búsqueda, haga clic en **GCM Heartbeat Interval**, y luego haga clic en **Edit**.

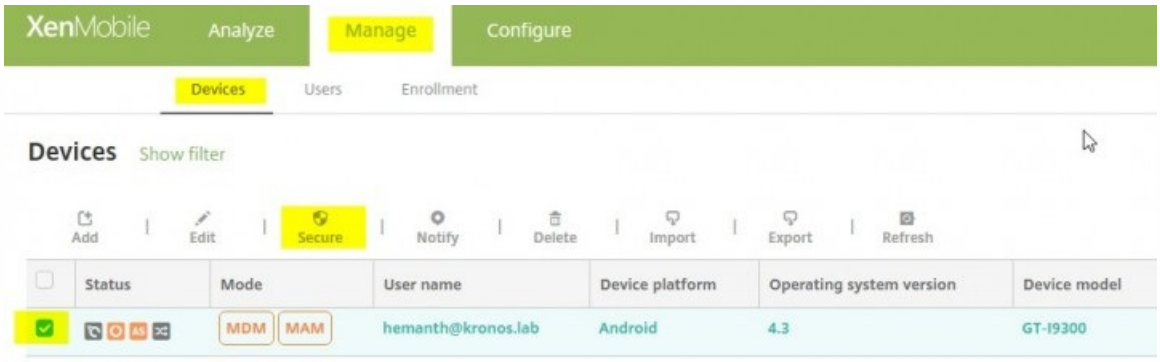


Para probar la configuración

1. Inscriba un dispositivo Android.

2. Deje el dispositivo inactivo durante algún tiempo, de forma que se desconecte del servidor XenMobile.

3. Inicie sesión en la consola de administración de XenMobile, haga clic en **Manage**, seleccione el dispositivo Android, y, a continuación, haga clic en **Secure**.



4. En **Device Actions**, haga clic en **Selective Wipe**.

Si la configuración es correcta, el borrado selectivo tiene lugar en el dispositivo sin necesidad de reconectarse a XenMobile.

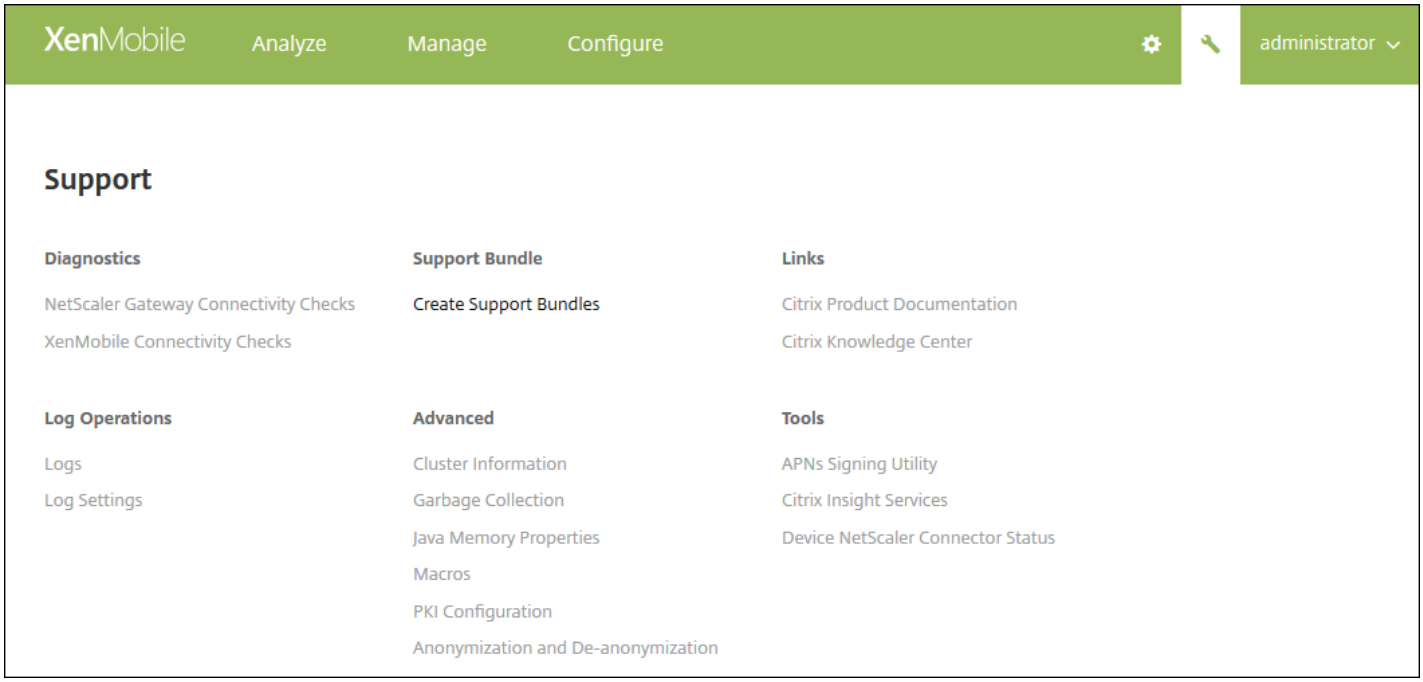
Mantenimiento y asistencia de XenMobile

Jul 27, 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.

En la consola de XenMobile, haga clic en el icono con forma de llave inglesa , situado en la esquina superior derecha de la consola.

Aparecerá la página Support,



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

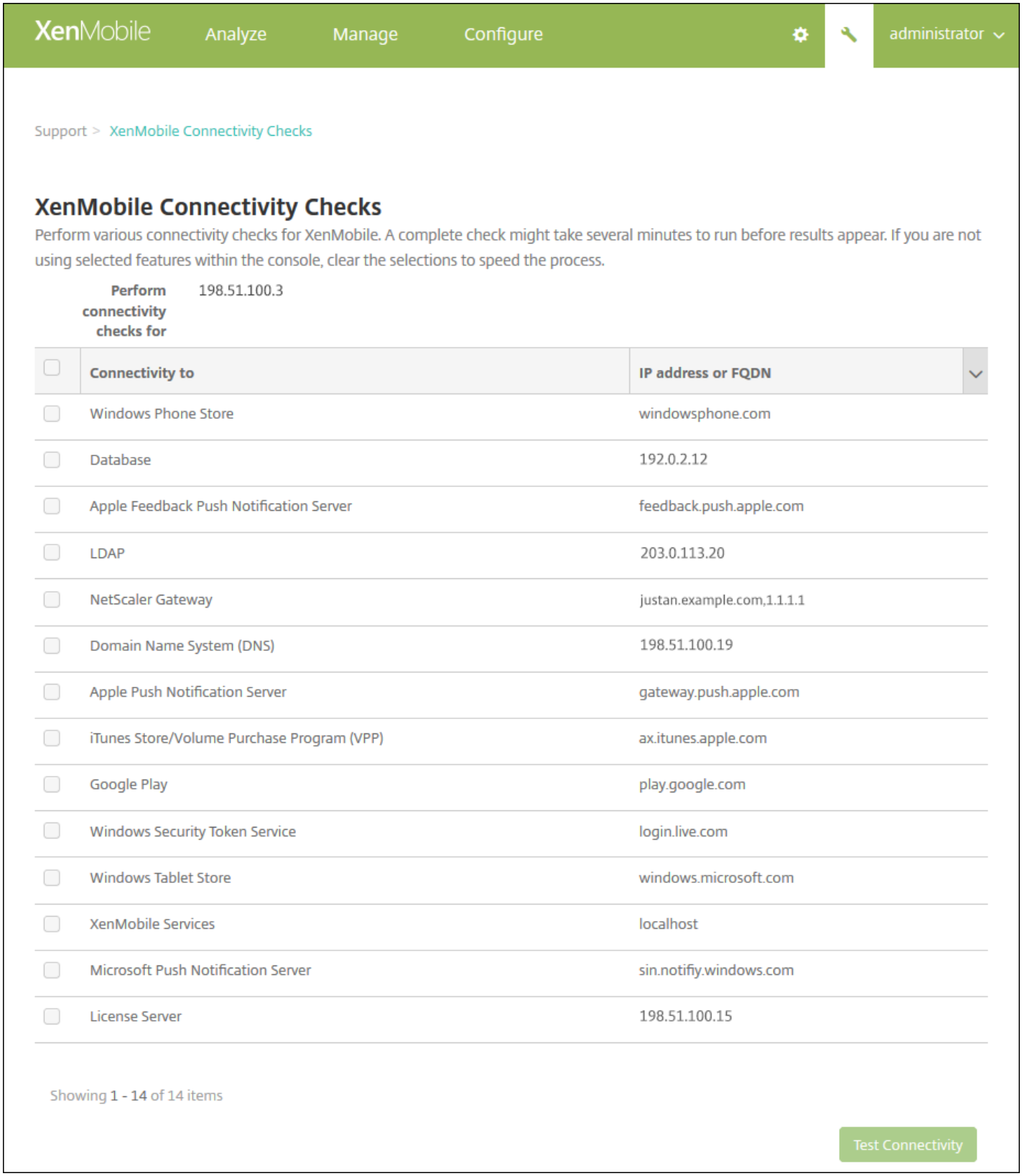
Jul 27, 2016

En la página **Support** de XenMobile, puede comprobar la conexión de XenMobile con NetScaler Gateway y con otros servidores y ubicaciones.

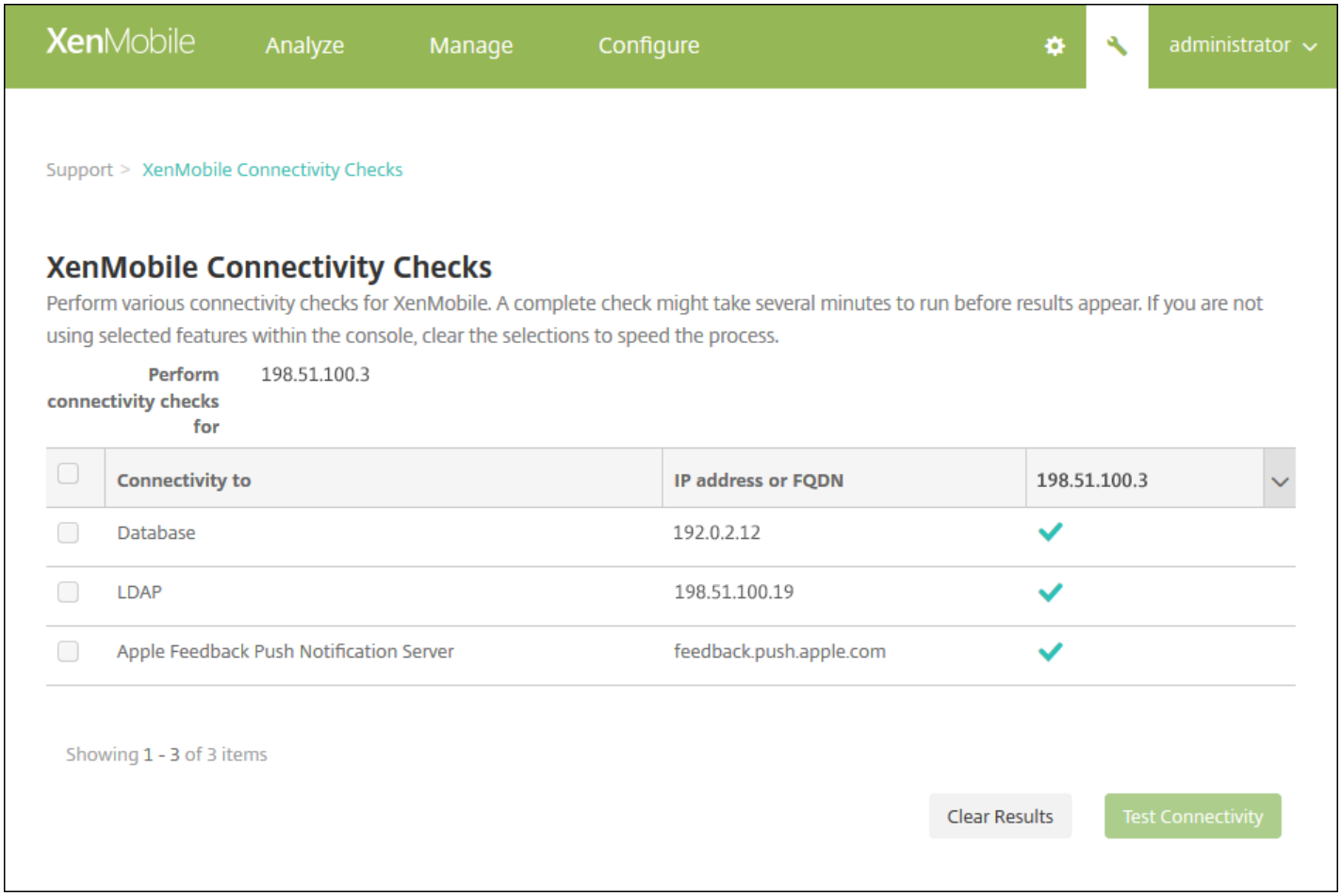
Comprobaciones de conectividad de XenMobile

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. Aparecerá la página **Support**.

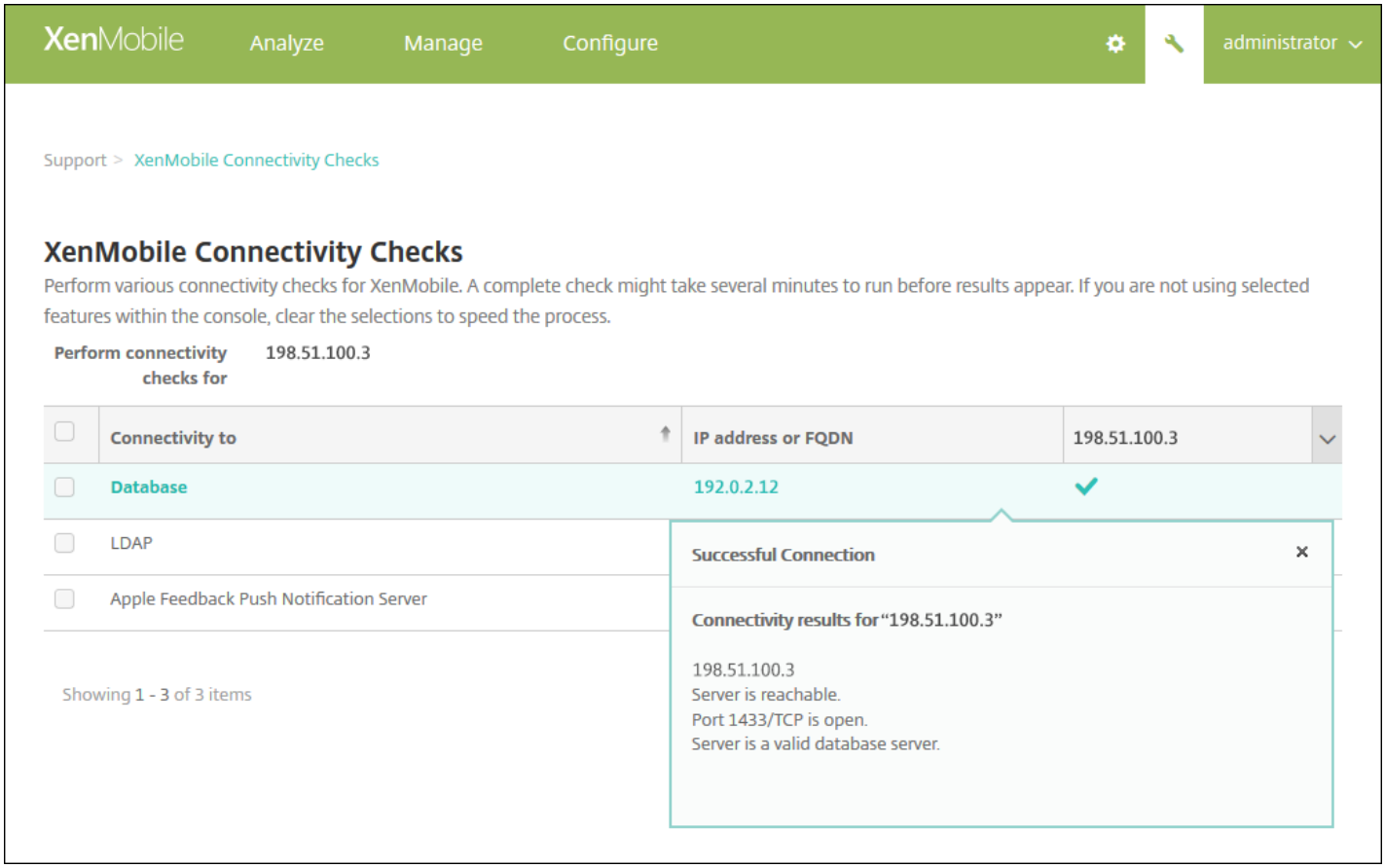
2. En **Diagnostics**, haga clic en **XenMobile Connectivity Checks**. Aparecerá la página **XenMobile Connectivity Checks**. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.



2. Seleccione los servidores a incluir en la prueba de conectividad y, a continuación, haga clic en **Test Connectivity**. Aparecerá la página de resultados de pruebas.

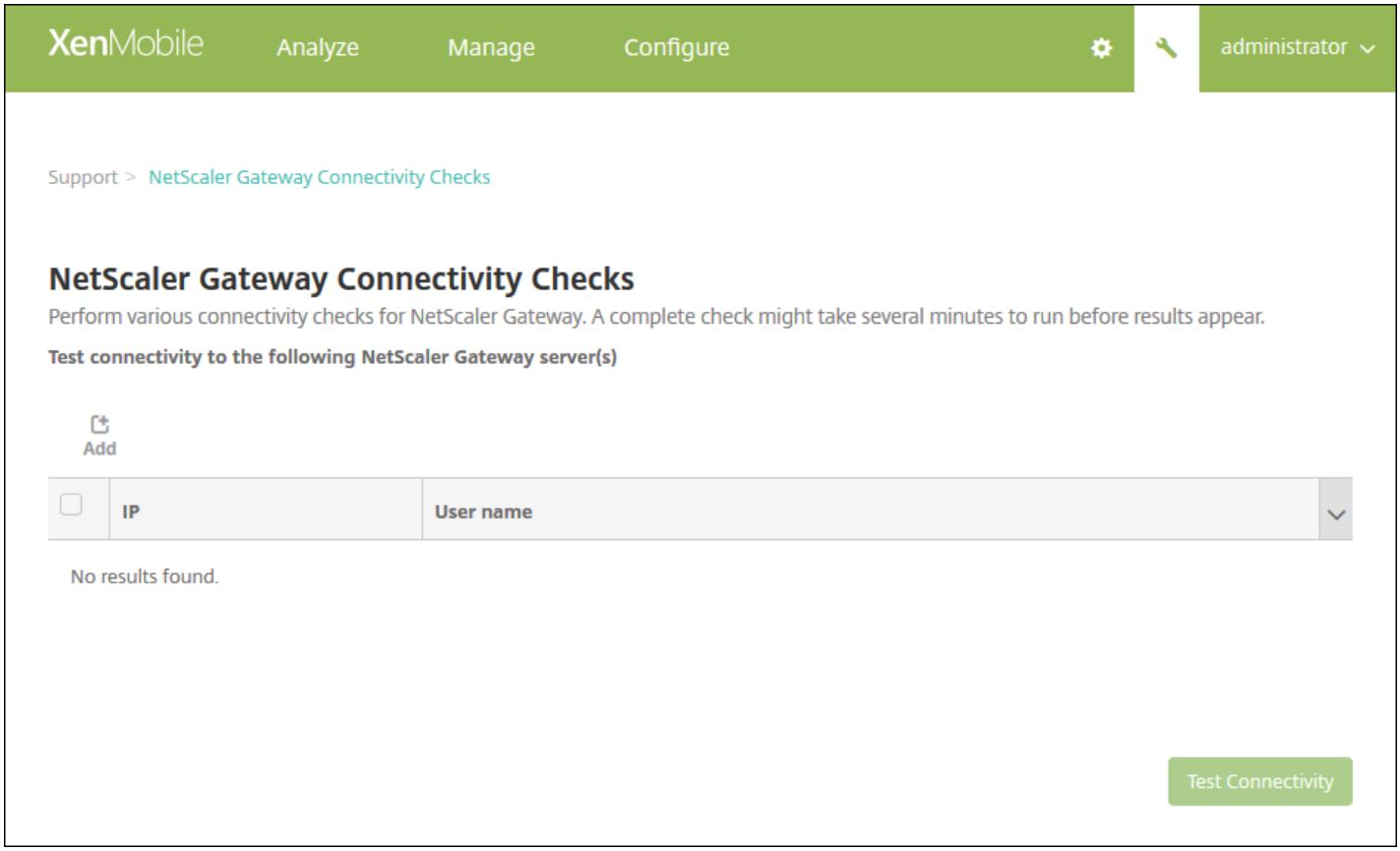


3. Seleccione un servidor de la tabla Test Results para ver los resultados detallados de dicho servidor.

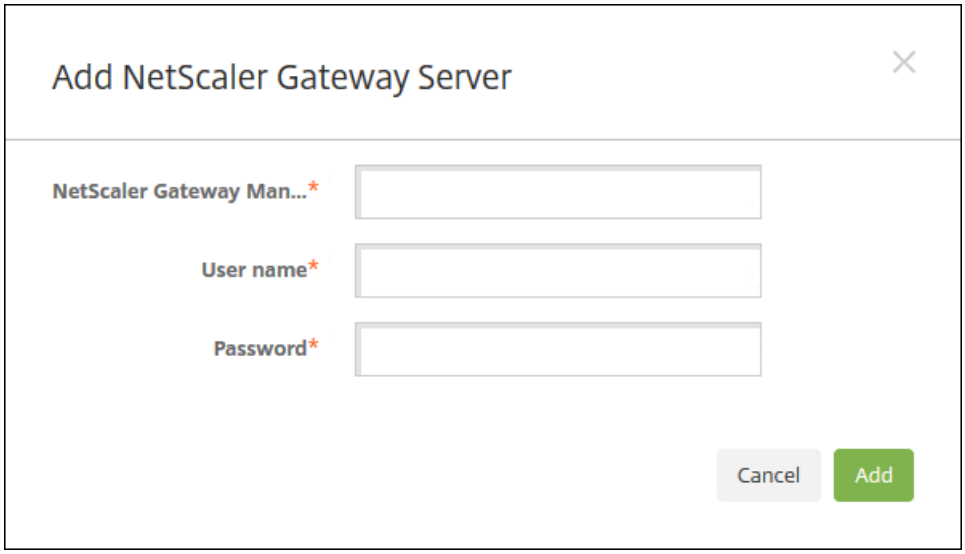


Comprobaciones de conectividad de NetScaler Gateway

1. En la página **Support**, en **Diagnostics**, haga clic en **NetScaler Gateway Connectivity Checks**. Aparecerá la página **NetScaler Gateway Connectivity Checks**. La tabla está vacía si no ha agregado servidores NetScaler Gateway.



2. Haga clic en **Add**. 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 **Add**. 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.

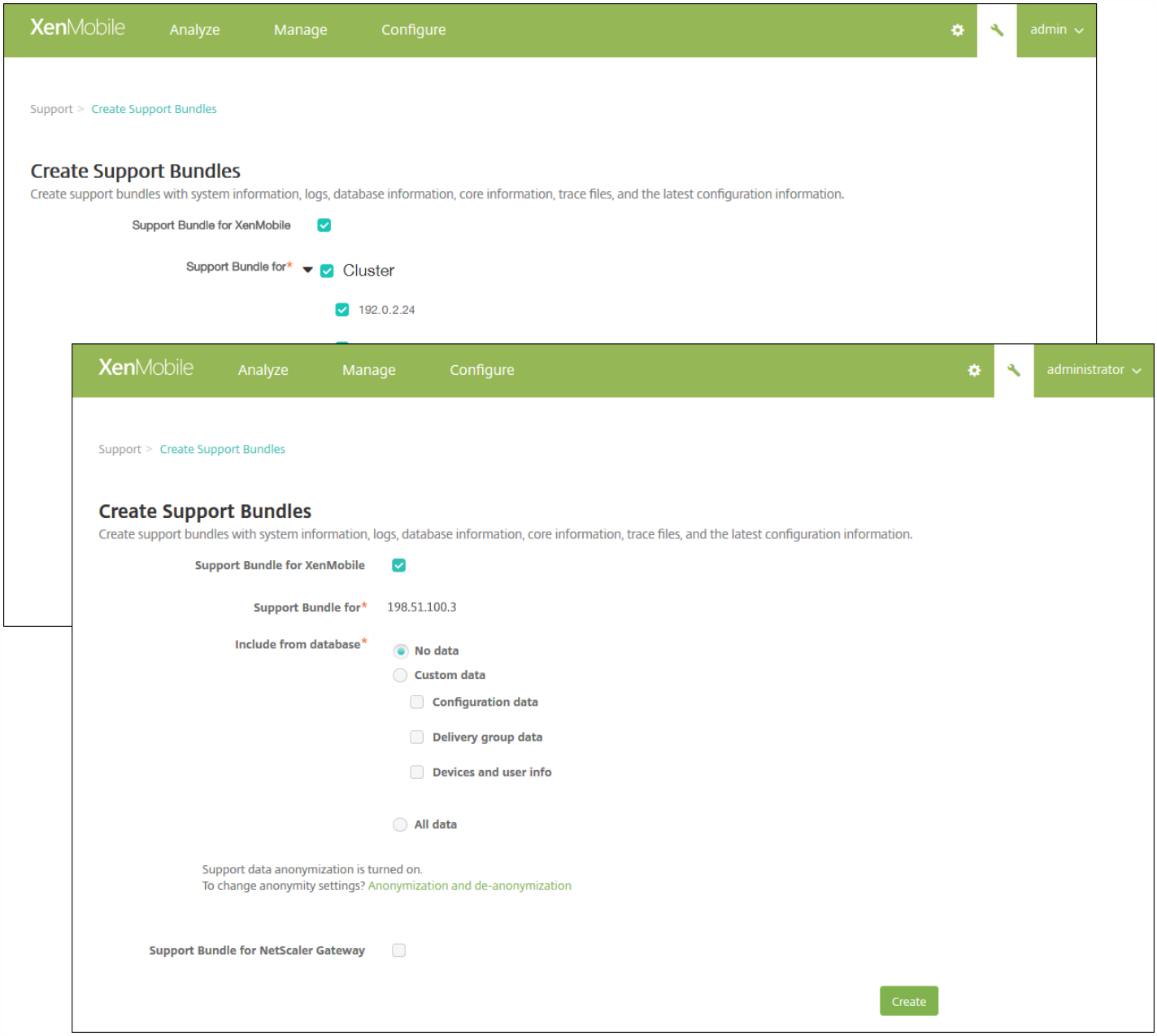
Creación de paquetes de asistencia en XenMobile

Jul 27, 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. Aparecerá la página **Support**.

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.



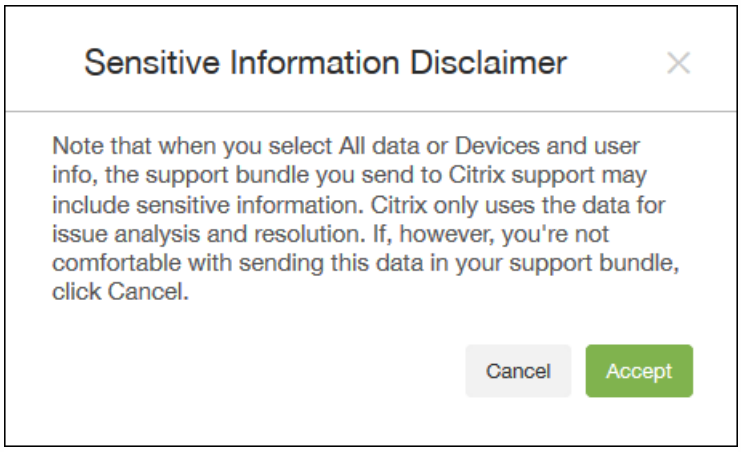
3. Compruebe que está marcada la casilla **Support Bundle for XenMobile**.

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**.

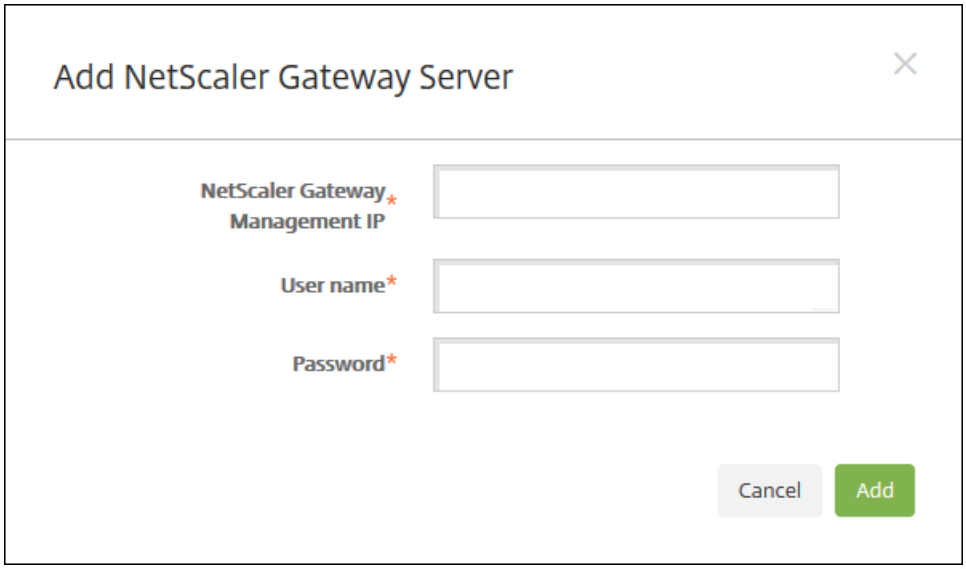
Nota: Si elige **Devices and user info** o **All data** y este es el primer paquete de asistencia que crea, aparecerá el cuadro de diálogo **Sensitive Information Disclaimer**. Lea el aviso de declinación de responsabilidades y, a continuación, haga clic en **Accept** o **Cancel**. Si hace clic en **Cancel**, el paquete de asistencia no se podrá cargar en Citrix. Si hace clic en **Accept**, podrá cargar el paquete de asistencia en Citrix y no verá el aviso de declinación de responsabilidades la próxima vez que se cree un paquete de asistencia que incluya datos de usuario o dispositivo.



6. Debajo de **Include from database**, verá un aviso acerca de si los datos de usuario, servidor y red pasan a ser anónimos en los paquetes de asistencia. El valor predeterminado del parámetro es que los datos sean anónimos. Para cambiar este parámetro, haga clic en el enlace **Anonymization and de-anonymization**. Consulte Anonimato de datos en paquetes de asistencia para obtener más información acerca del anonimato de datos.

6. Marque **Support Bundle for NetScaler Gateway** para incluir paquetes de asistencia de NetScaler Gateway y, a continuación, realice lo siguiente:

- Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add NetScaler Gateway Server**.



- En **NetScaler Gateway Management IP**, escriba la dirección IP de administración de NetScaler referente al dispositivo NetScaler Gateway del que quiere 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.

- En **User name** y **Password**, escriba las credenciales de usuario necesarias para acceder al servidor con 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.

7. Haga clic en **Add**. El nuevo paquete de asistencia de NetScaler Gateway se agrega a la tabla.

8. Repita el paso 7 para agregar más paquetes de asistencia de NetScaler Gateway.

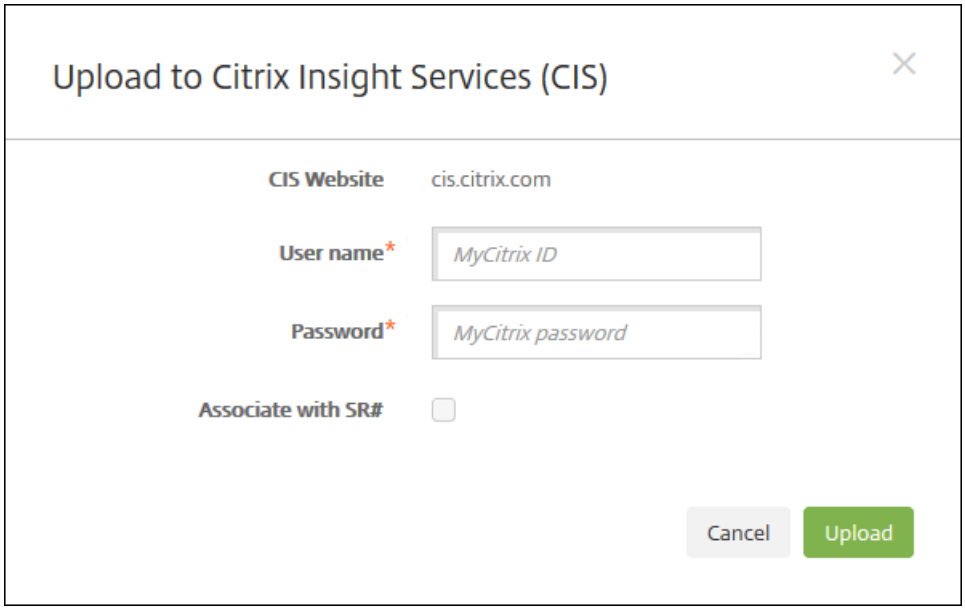
9. Haga clic en **Create**. Se crea el paquete de asistencia y aparecen dos nuevos botones: **Upload to CIS** y **Download to Client**.

Continúe en Carga de paquetes de asistencia en Citrix Insight Services o en Descarga de paquetes de asistencia en el equipo.

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. Necesita un ID y una contraseña de MyCitrix para cargar 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:

- En **SR#**, escriba los 8 dígitos del número de solicitud de servicio a la que se va a asociar este paquete.
- En **SR Description**, escriba una descripción de la solicitud de servicio.

5. Haga clic en **Upload**.

Si es la primera vez que carga un paquete de asistencia en CIS y no ha creado ninguna cuenta en CIS con otro producto ni ha aceptado el acuerdo de recopilación de datos y privacidad, aparecerá el siguiente cuadro de diálogo. Debe aceptar el acuerdo para comenzar la carga. Si dispone de una cuenta en CIS y había aceptado el acuerdo, el paquete de asistencia se carga sin más preámbulos.

6. Lea el acuerdo y haga clic en **Agree and upload**. Se cargará el paquete de asistencia.

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.

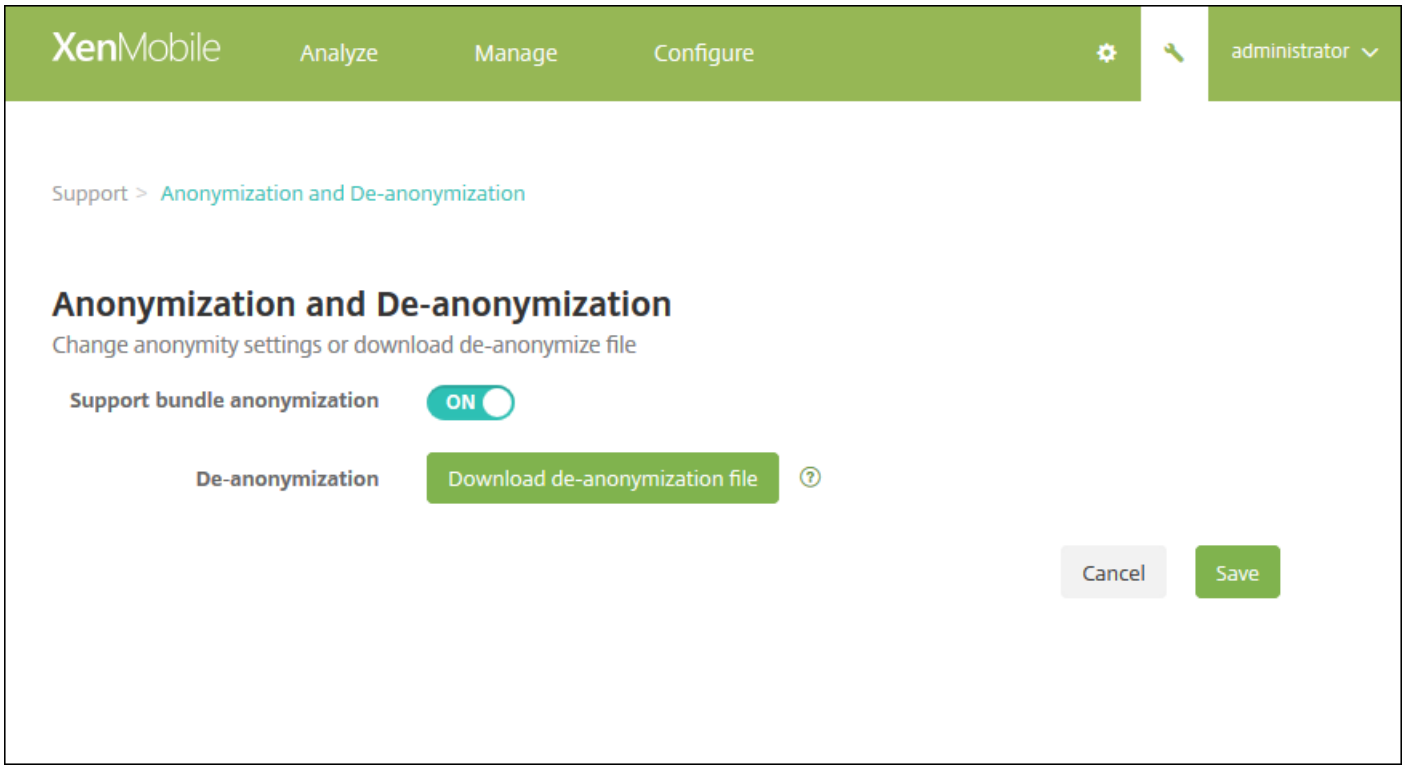
Anonimato de datos en paquetes de asistencia

Jul 27, 2016

En XenMobile, cuando crea paquetes de asistencia, los datos confidenciales de usuario, red y servidor pasan a ser anónimos de forma predeterminada. Puede cambiar este comportamiento en la página Anonymization and De-anonymization. También puede descargar un archivo de asignación que XenMobile guarda cuando los datos pasan a ser anónimos. El servicio de asistencia de Citrix puede solicitar este archivo para convertir datos anónimos en no anónimos y, así, buscar los problemas que haya con un dispositivo o un usuario determinados.

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. Aparecerá la página **Support**.

2. En la página **Support**, en **Advanced**, haga clic en **Anonymization and De-anonymization**. Aparecerá la página **Anonymization and De-anonymization**.



3. En **Support bundle anonymization**, seleccione si los datos pasan a ser anónimos. El valor predeterminado es **ON**.

4. Junto a **De-anonymization**, haga clic en **Download de-anonymization file** para descargar el archivo de asignación que enviará al servicio de asistencia de Citrix cuando necesiten información concreta de dispositivo o usuario para diagnosticar un problema.

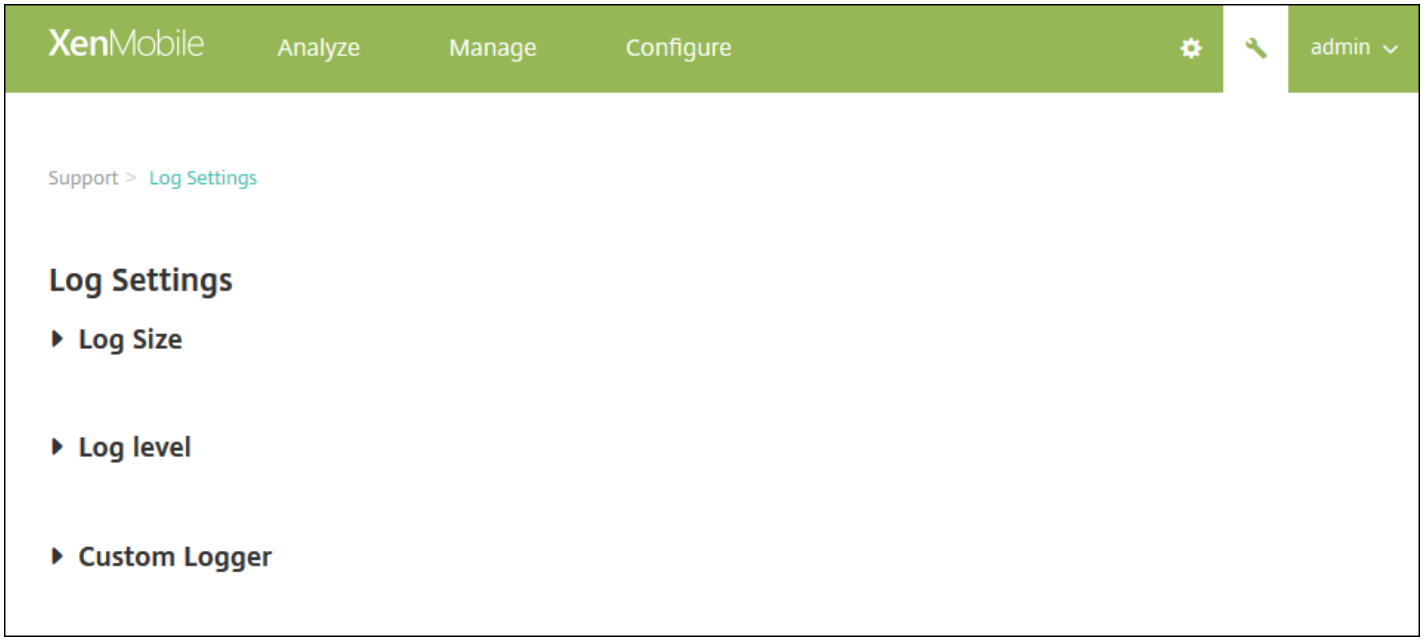
Configuración de los parámetros de registro

Jul 27, 2016

Puede configurar los parámetros de captura de registros para personalizar los registros que genera XenMobile. Si tiene un clúster de servidores XenMobile, cuando se configuran los parámetros de registros en la consola de XenMobile, los parámetros se comparten con todos los servidores del clúster.

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. Aparecerá la página **Support**.

2. En **Log Operations**, haga clic en **Log Settings**. Aparecerá la página **Log Settings**.

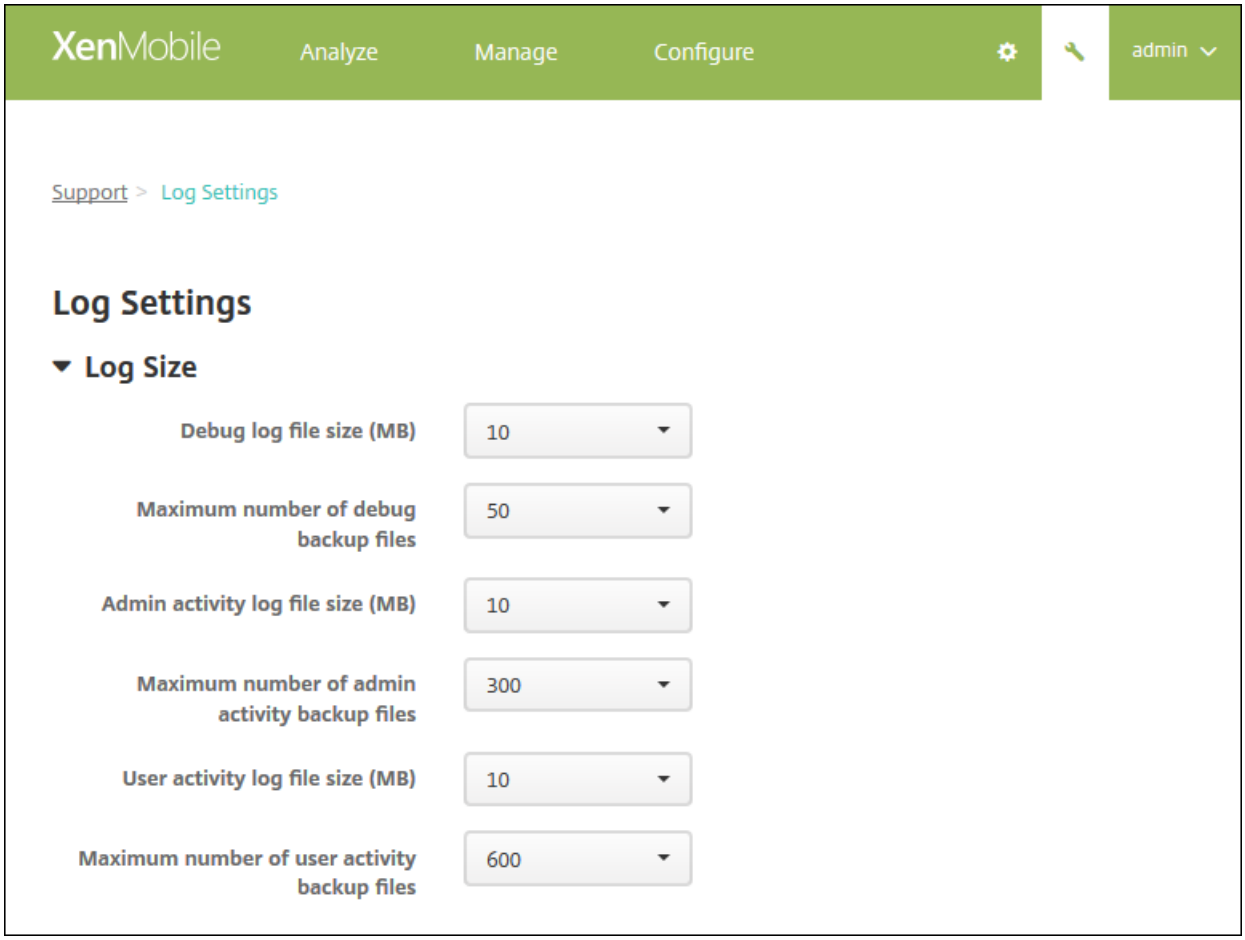


En la página **Log Settings**, puede acceder a las siguientes opciones:

- **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. La opción Log size se aplica a cada archivo de registros admitido por XenMobile (depuración, actividad de administración y actividad de usuarios).
- **Log level**. Use esta opción para cambiar el nivel de captura de registros o 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. En la página **Log Settings**, expanda **Log Size**.



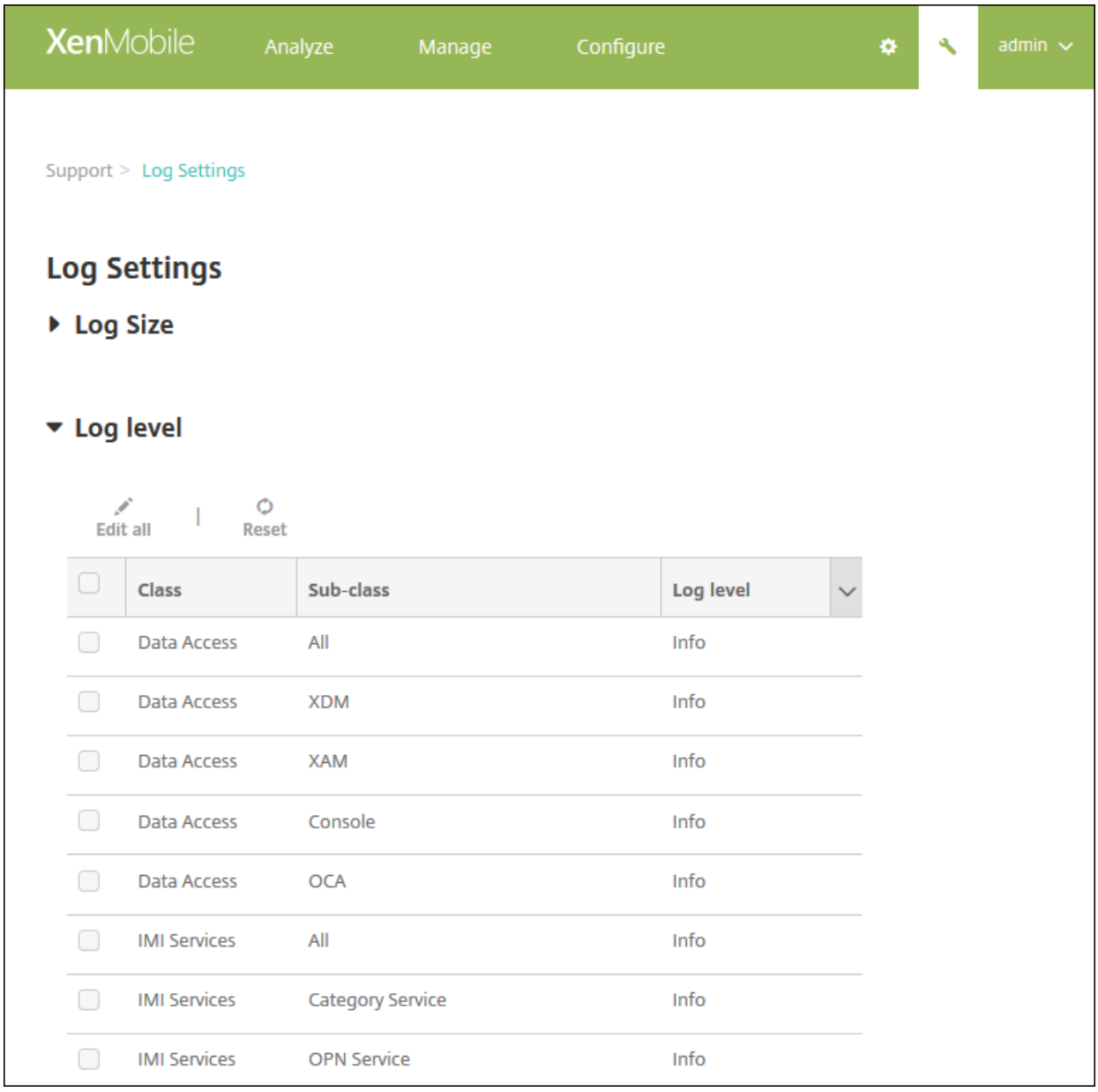
2. Configure los siguientes parámetros:

- **Debug log file size (MB)**: En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de depuración. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of debug backup files**: En la lista, haga clic en el número máximo de archivos de depuración que conservará el servidor. De forma predeterminada, XenMobile conserva 50 archivos de copias de seguridad en el servidor.
- **Admin activity log file size (MB)**: En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de actividad de administración. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of admin activity backup files**: En la lista, haga clic en el número máximo de archivos de actividad de administración que conservará el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.
- **User activity log file size (MB)**: En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de actividad de usuarios. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of user activity backup files**: En la lista, haga clic en el número máximo de archivos de actividad de usuarios que conservará el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.

Para configurar las opciones de nivel de registro

La opción de nivel de registros (Log level) permite especificar qué tipo de información recopila XenMobile en los registros. Puede establecer el mismo nivel para todas las clases o puede definir las clases con niveles de registro específicos.

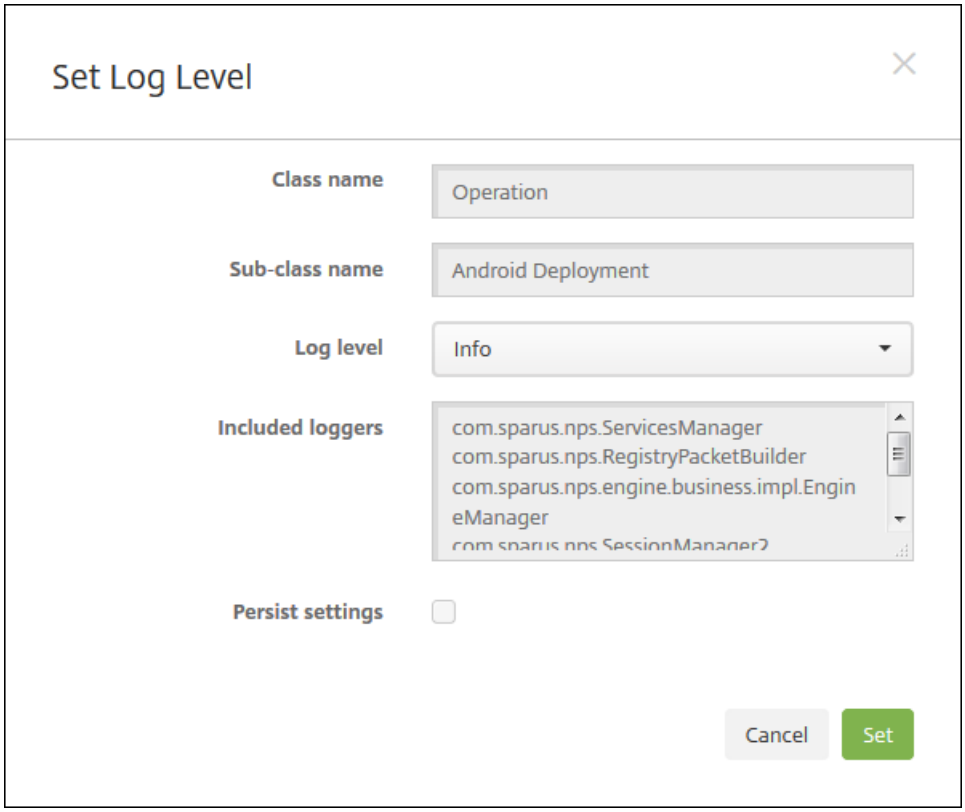
1. En la página **Log Settings**, expanda **Log level**. Aparece la tabla con todas las clases de registros.



2. Lleve a cabo una de las siguientes acciones:

- Marque la casilla junto a una clase y luego haga clic en **Set Level** para cambiar solo el nivel de registro de esa clase.
- Haga clic en **Edit all** para aplicar el cambio de nivel de registro a todas las clases de la tabla.

Aparecerá el cuadro de diálogo **Set Log Level**, donde podrá establecer el nivel de registro y seleccionar si la configuración del nivel de registro se conservará cuando se reinicie el servidor XenMobile.

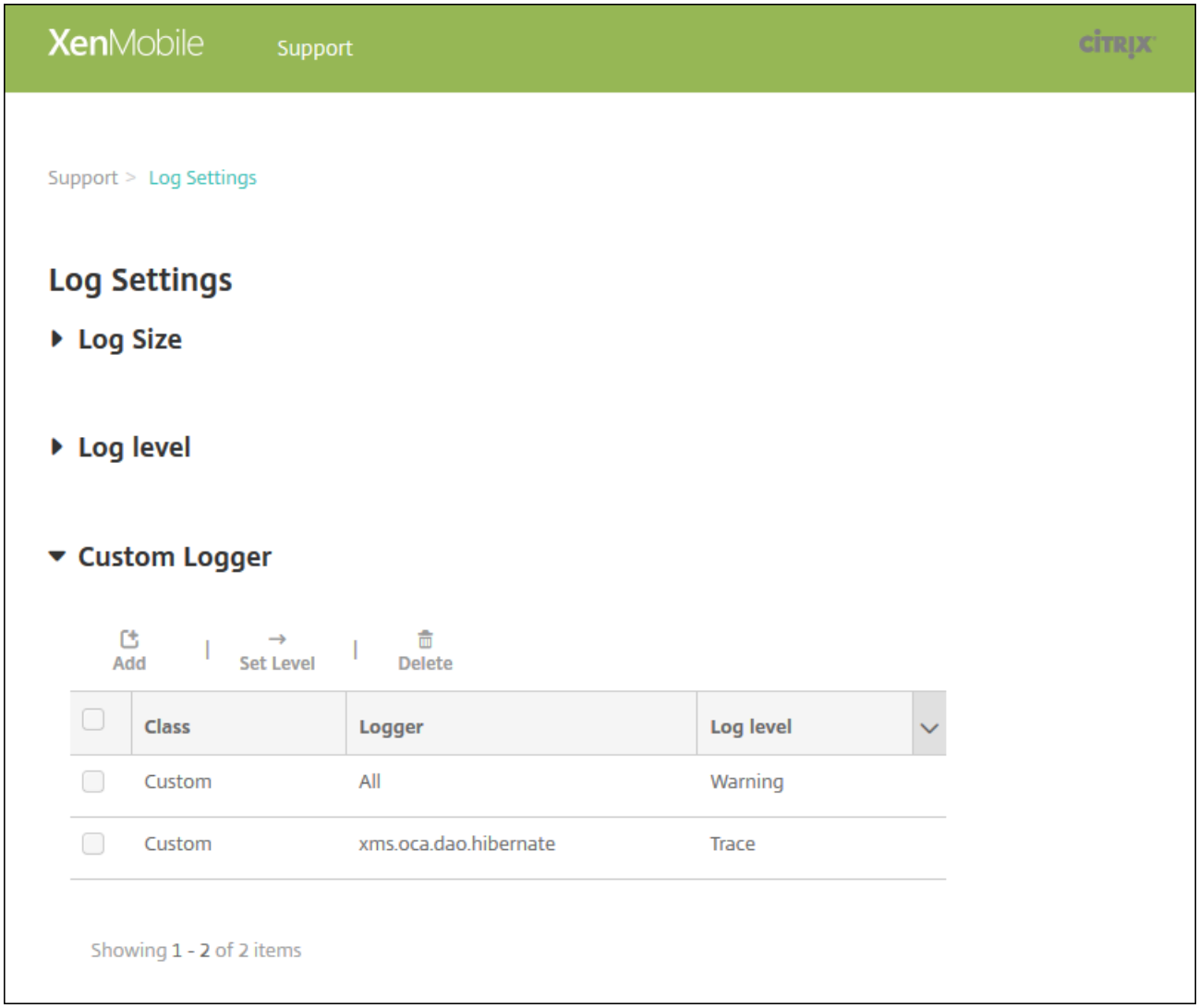


- **Class Name**: Este campo muestra el valor All cuando se está cambiando el nivel de registro para todas las clases, o muestra el nombre de la clase en particular; no es un campo editable.
- **Sub-class name**: Este campo no se puede modificar. Muestra el valor All cuando se está cambiando el nivel de registro de todas las clases, o bien muestra el nombre de la subclase en particular.
- **Log level**: Haga clic en un nivel de registro en la lista. Los niveles de registro respaldados incluyen:
  - Fatal (Grave)
  - Error
  - Advertencia
  - Info (Información)
  - Debug (Depuración)
  - Trace (Seguimiento)
  - Off
- **Included Loggers**: Este campo está en blanco cuando se está cambiando el nivel de registro para todas las clases, o muestra el nombre de los registradores configurados actualmente para una clase en concreto; no es un campo editable.
- **Persist settings**: Si quiere conservar los parámetros de nivel de registro cuando reinicie el servidor, marque esta casilla. Si no se marca esta casilla, los parámetros de nivel de registro vuelven a sus valores predeterminados cuando se reinicia el servidor.

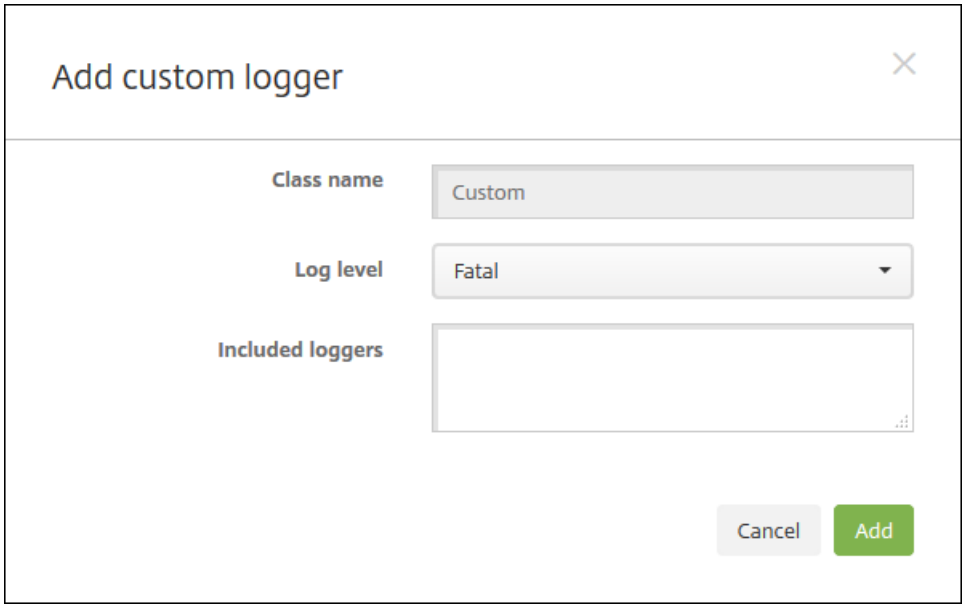
3. Haga clic en **Set** para confirmar los cambios.

Cómo agregar un registrador personalizado

1. En la página **Log Settings**, expanda **Custom Logger**. Aparecerá la tabla **Custom Logger**. Si no ha agregado aún registradores personalizados, la tabla empieza vacía.



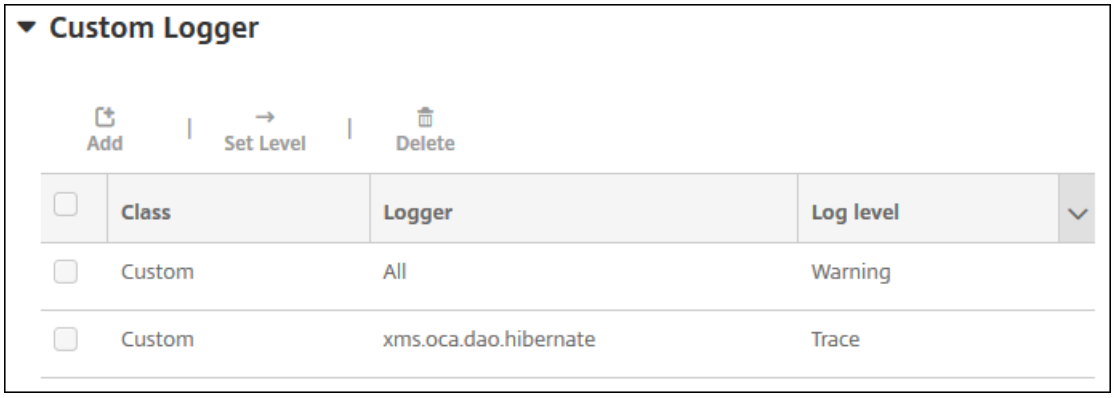
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add custom logger**.



3. Configure los siguientes parámetros:

- **Class Name**: Este campo muestra **Custom**; no es un campo editable.
- **Log level**: Haga clic en un nivel de registro en la lista. Los niveles de registro respaldados incluyen:
  - Fatal (Grave)
  - Error
  - Advertencia
  - Info (Información)
  - Debug (Depuración)
  - Trace (Seguimiento)
  - Off
- **Included Loggers**: Escriba los registradores concretos que quiere incluir como registradores personalizados, o bien deje el campo en blanco para incluir a todos los registradores.

4. Haga clic en **Add**. El registrador personalizado se agrega a la tabla **Custom Logger**.



Para eliminar un registrador personalizado

1. En la página **Log Settings**, expanda **Custom Logger**.

2. Seleccione el registrador personalizado que quiere eliminar.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo para preguntar si quiere eliminar el registrador personalizado. Haga clic en **Aceptar**.

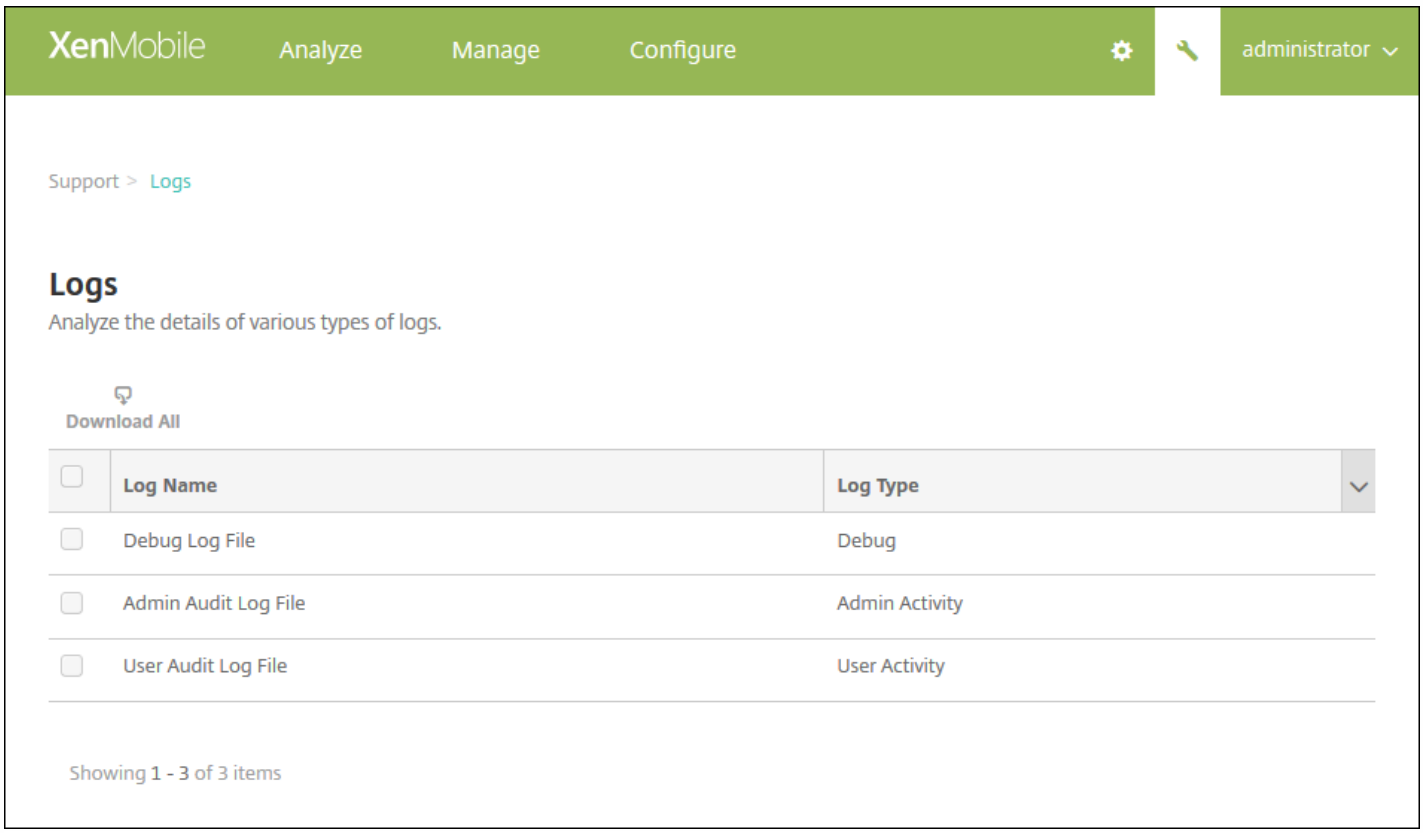
Importante: Esta operación no se puede deshacer.

Cómo ver y analizar archivos de registros en XenMobile

Jul 27, 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**.

2. En **Log Operations**, haga clic en **Logs**. Aparecerá la página **Logs**. Los registros individuales se muestran en una tabla.



3. Seleccione el registro que quiera ver:

- Los archivos de registros de depuración (Debug Log File) contienen información muy útil para el servicio de asistencia Citrix Support, tal como mensajes de error y acciones relacionadas con el servidor.
- Los archivos de registros de auditoría de administración (Admin Audit Log File) contienen información de auditoría sobre actividad en la consola de XenMobile.
- Los archivos de registros de auditoría de usuarios (User Audit Log File) contienen información relacionada con los usuarios configurados.

4. Use las acciones de la parte superior de la tabla para descargar uno o todos los registros, verlos, girarlos o eliminarlos.

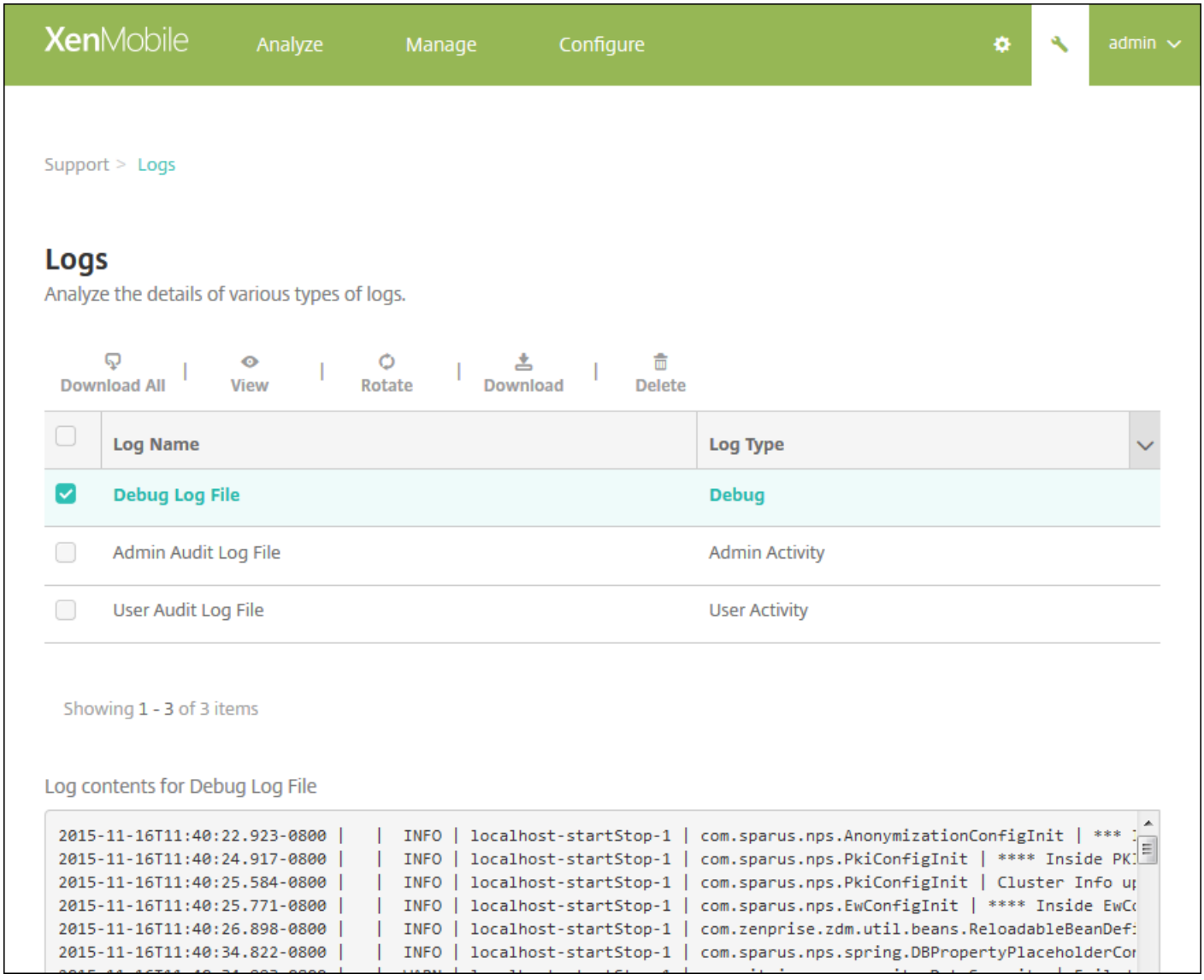
Nota:

- Si selecciona varios archivos de registro, solo estarán disponibles las opciones **Download All** y **Delete**.
- Si tiene servidores XenMobile en clúster, solo puede ver los registros del servidor al que está conectado. Para ver los

registros de otros servidores, use alguna de las opciones de descarga.

5. Lleve a cabo una de las siguientes acciones:

- **Download All**: La consola descarga todos los registros presentes en el sistema (incluidos los registros de depuración, auditoría de administración, auditoría de usuarios, registros del servidor, etcétera).
- **View**: Muestra, a continuación de la tabla, el contenido de los registros.
- **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.
- **Download**: La consola descarga el único tipo de archivo de registros seleccionado y también descarga otros registros ya archivados del mismo tipo.
- **Delete**: Quita permanentemente los archivos de registros seleccionados.



Remote Support

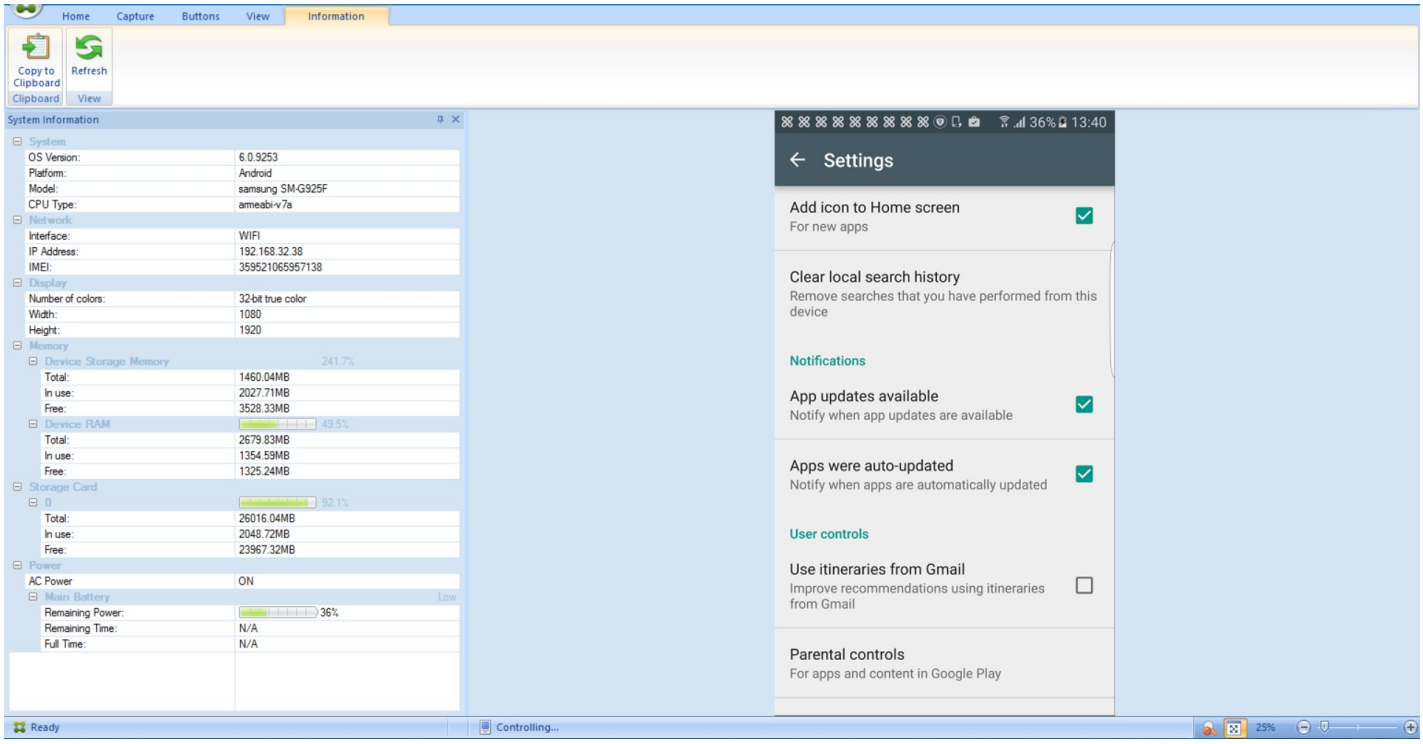
Jul 27, 2016

La asistencia remota (Remote Support) permite que el personal de Help Desk tome el control remoto de los dispositivos móviles Windows y Android administrados. Remote Support está disponible en todos los dispositivos móviles Windows, y en los dispositivos Samsung SAFE de Android. No se respalda el control remoto de dispositivos iOS.

> ## Nota
>
> XenMobile Remote Support no está disponible en las versiones 10.x de XenMobile Cloud.

Durante una sesión de control remoto:

- Los usuarios ven un icono en su dispositivo móvil que indica que hay una sesión de control remoto activa.
- Los usuarios de asistencia remota ven la ventana de la aplicación Remote Support y una ventana de control remoto con una representación del dispositivo controlado.



Con Remote Support, es posible:

- Iniciar sesión de forma remota en el dispositivo móvil de un usuario y controlar la pantalla. Los usuarios pueden verle a usted navegar por la pantalla, lo que puede ser útil con fines de aprendizaje y capacitación.
- Desplazarse y reparar un dispositivo remoto en tiempo real. Puede cambiar las configuraciones, solucionar problemas del sistema operativo e inhabilitar o detener las aplicaciones o los procesos que sean problemáticos.
- Aislar y contener posibles amenazas de seguridad antes de que se propaguen a otros dispositivos móviles inhabilitando el acceso a la red de forma remota, detener procesos no autorizados o sospechosos y quitar aplicaciones o malware.

- Habilitar de forma remota el timbre del dispositivo y llamar al teléfono, para ayudar al usuario a encontrarlo. Si un usuario no puede encontrar el dispositivo, puede borrarlo para salvaguardar la información confidencial que pueda contener.

Remote Support también permite al personal de asistencia técnica:

- Mostrar una lista de todos los dispositivos conectados en uno o más servidores XenMobile.
- Mostrar información del sistema, incluidos el modelo del dispositivo, el nivel del sistema operativo, la identidad de equipo móvil internacional (IMEI) y el número de serie, el estado de la memoria y la batería, y la conectividad.
- Mostrar los usuarios y los grupos del servidor XenMobile.
- Ejecutar el administrador de tareas del dispositivo donde se pueden ver y finalizar procesos activos y reiniciar el dispositivo móvil.
- Ejecutar transferencias remotas de archivos que incluyen la transferencia bidireccional de archivos entre los dispositivos móviles y un servidor de archivos central.
- Descargar e instalar programas de software como un lote para uno o más dispositivos móviles.
- Configurar las opciones de la clave del Registro remota en el dispositivo.
- Optimizar el tiempo de respuesta en las redes celulares de ancho de banda bajo mediante el uso del control remoto en tiempo real en la pantalla del dispositivo.
- Mostrar la máscara del dispositivo para la mayoría de los modelos y marcas de dispositivo móvil. Mostrar un editor de máscaras para agregar nuevos modelos de dispositivo y asignar teclas físicas.
- Habilitar la captura de pantallas del dispositivo, grabar y reproducir con la capacidad de capturar una secuencia de interacciones en el dispositivo y crear un archivo de vídeo AVI.
- Llevar a cabo reuniones con una pizarra compartida, comunicaciones de voz basadas en VoIP y chat entre usuarios móviles y el personal de asistencia técnica.

Requisitos del sistema para Remote Support

El software de Remote Support se puede instalar en equipos Windows que cumplan los siguientes requisitos. Para obtener los requisitos de puerto, consulte Requisitos de puertos.

Plataformas respaldadas

- Intel Xeon o Pentium 4: mínimo 1 GHz de clase de estación de trabajo
- Mínimo 512 MB de RAM
- Mínimo 100 MB de espacio libre en disco

Sistemas operativos respaldados

- Microsoft Windows 2003 Server Standard Edition o Enterprise Edition SP1 o versiones posteriores
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 o versiones posteriores
- Microsoft Windows Vista SP1 o versiones posteriores
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Para instalar el software de Remote Support

1. Para descargar el instalador de Remote Support, vaya a la página de descargas de XenMobile 10 e inicie sesión en su cuenta.
2. Expanda **Tools** y, a continuación, descargue XenMobile Remote Support v9.
   El nombre de archivo de Remote Support es actualmente XenMobileRemoteSupport-9.0.0.35265.exe.
3. Haga doble clic en el instalador de Remote Support y, a continuación, siga las instrucciones del asistente de instalación.

Para instalar Remote Support desde la línea de comandos:

Ejecute el comando siguiente:

RemoteSupport.exe /S

donde *RemoteSupport* es el nombre del programa de instalación. Por ejemplo:

XenMobileRemoteSupport-9.0.0.35265.exe /S

Puede utilizar las siguientes variables al instalar el software de Remote Support:

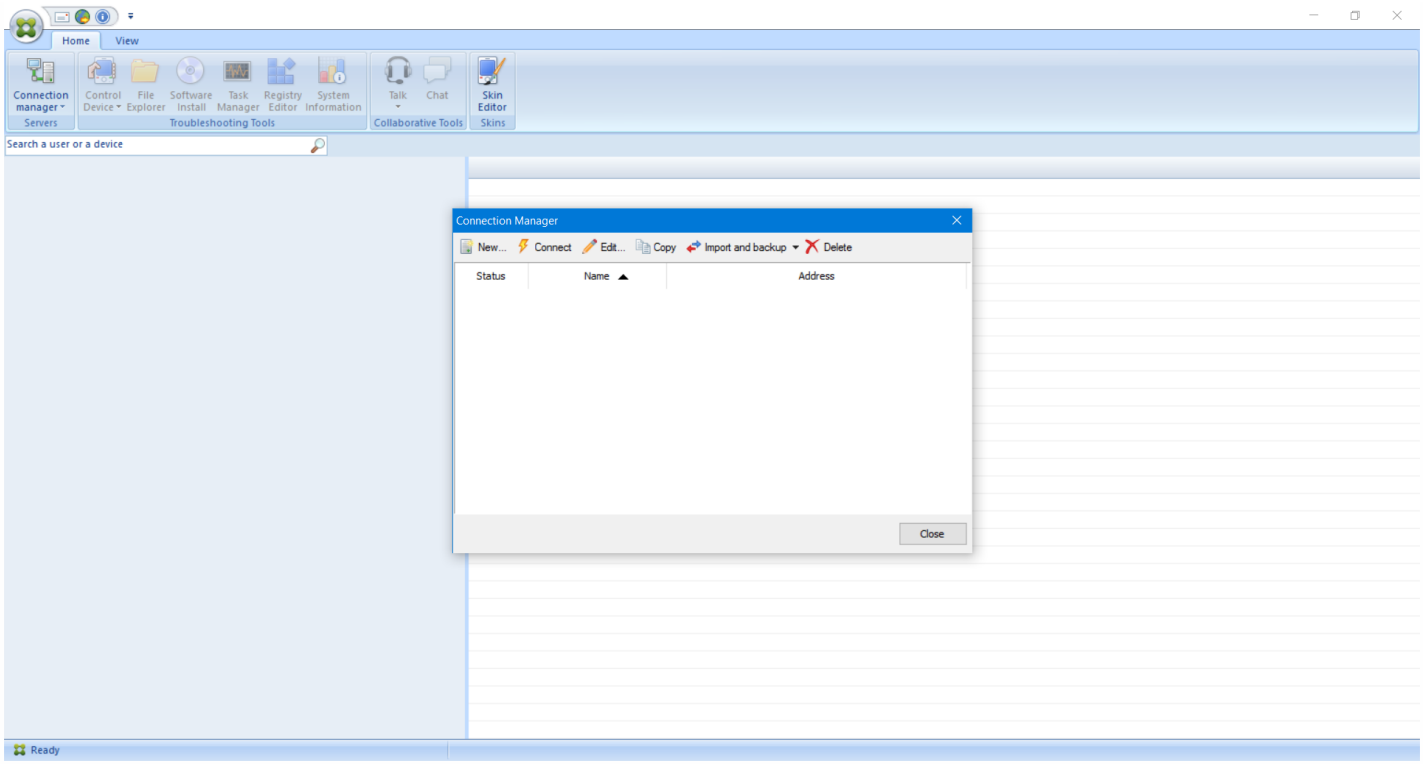
- /S: para instalar de forma silenciosa el software de Remote Support con los parámetros predeterminados.
- /D=dir: para especificar un directorio de instalación personalizado.

Para conectar Remote Support a XenMobile

Para establecer conexiones de asistencia remota con dispositivos administrados, debe agregar una conexión desde Remote Support a los servidores XenMobile que administran los dispositivos. Esta conexión se ejecuta a través de un túnel de aplicaciones definido en la directiva de túneles, una directiva de dispositivo para Android y Windows Mobile/CE. El túnel de aplicaciones debe definirse como se describe en las directivas de dispositivo de túnel de aplicaciones antes de poder conectar Remote Support a XenMobile.

1. Inicie el software de Remote Support y use credenciales de XenMobile para iniciar sesión.

2. En **Connection Manager**, haga clic en **New**.



3. En el cuadro de diálogo **Connection Configuration**, en la ficha **Server**, introduzca los siguientes valores:

   En **Configuration name**, escriba un nombre para la entrada de configuración.

   En **Server IP address or name**, escriba la dirección IP o el nombre DNS del servidor XenMobile.

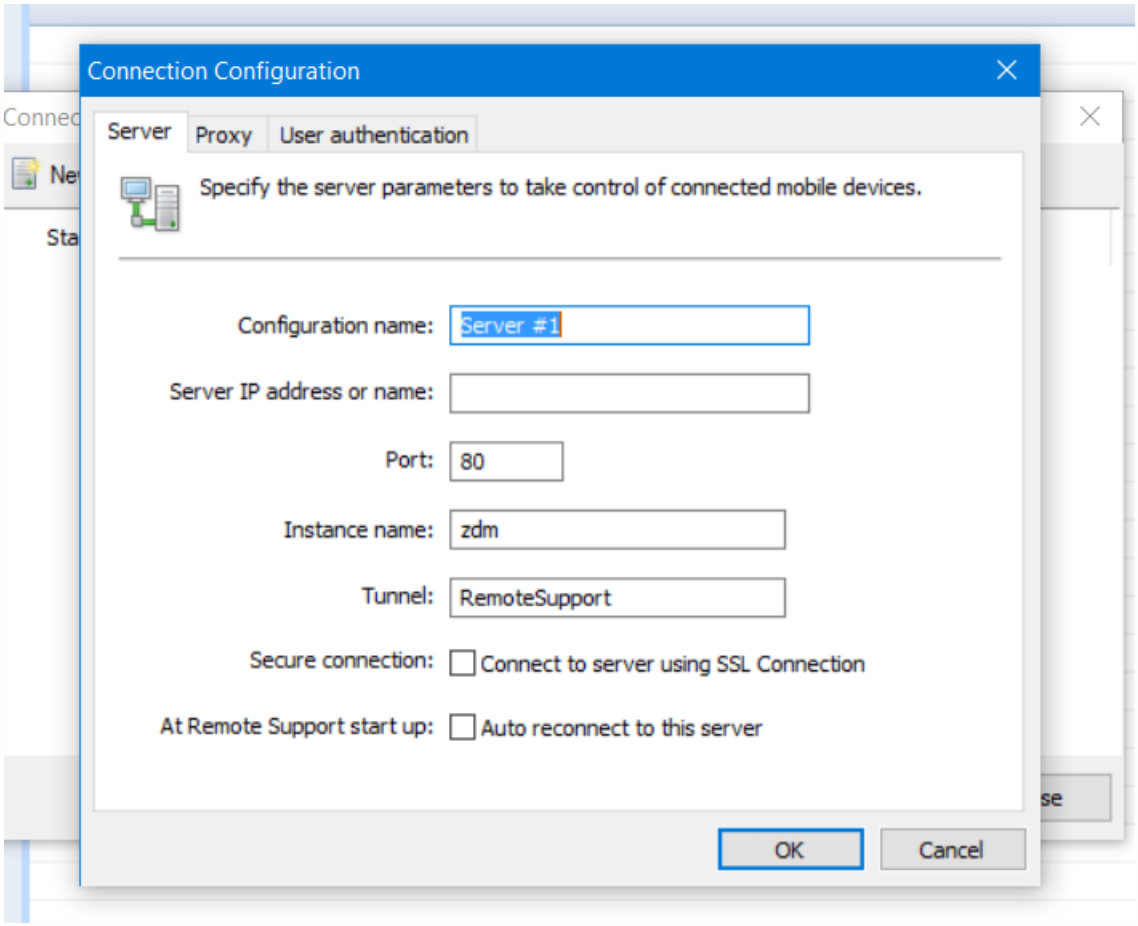
   En **Port**, escriba el número de puerto TCP, como se define en la configuración de servidor de XenMobile.

   En **Instance name**, si XenMobile forma parte de una implementación multiarrendatario, escriba un nombre de instancia.

   En **Tunnel**, escriba el nombre de la directiva de túnel.

   Marque la casilla **Connect to server using SSL Connection**.

   Marque la casilla **Auto reconnect to this server** para conectar con el servidor XenMobile configurado cada vez que se inicie la aplicación Remote Support.



4. En la ficha **Proxy**, seleccione **Use a http proxy server** y, a continuación, introduzca la información siguiente:

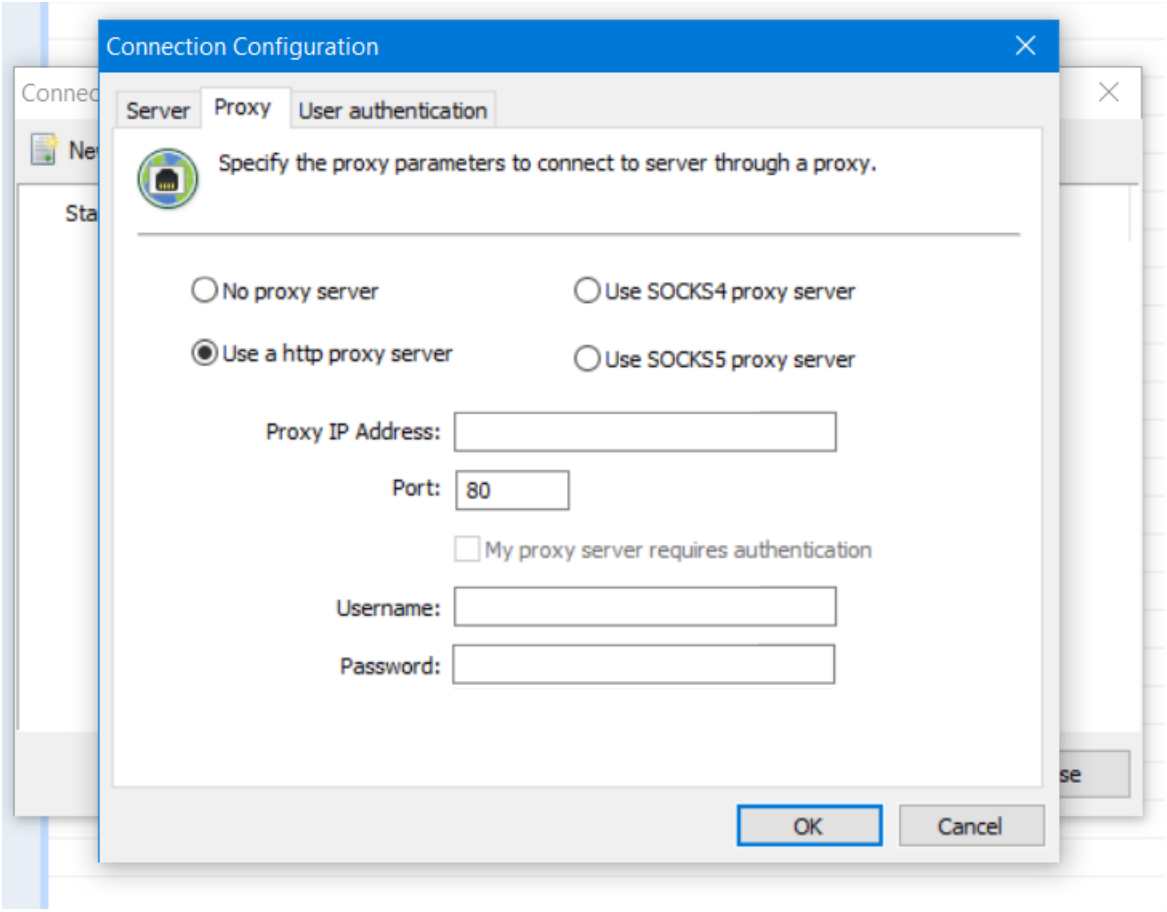
   En **Proxy IP Address**, escriba la dirección IP del servidor proxy.

   En **Port**, escriba el número de puerto TCP utilizado por el proxy.

   Marque la casilla de **My proxy requires authentication** si el servidor proxy requiere autenticación antes de transmitir tráfico.

   En **Username**, escriba el nombre de usuario con el que autenticarse en el servidor proxy.

   En **Password**, escriba la contraseña con la que autenticarse en el servidor proxy.



5. En la ficha **User Authentication**, marque la casilla **Remember my login and password** e introduzca las credenciales.

6. Haga clic en **OK**.

Para conectarse a XenMobile, haga doble clic en la conexión que ha creado y, a continuación, escriba el nombre de usuario y la contraseña que ha configurado para la conexión.

Para habilitar la asistencia remota para dispositivos Samsung KNOX

Puede crear una directiva de asistencia remota Remote Support en XenMobile para darle acceso remoto a dispositivos Samsung

KNOX. 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.

Para obtener información sobre la configuración de la directiva de asistencia remota Remote Support, consulte la directiva de asistencia remota para dispositivos.

Para usar una sesión de Remote Support

Después de iniciar la aplicación Remote Support, en el lado izquierdo de la ventana de la aplicación Remote Support, se presentan los grupos de usuarios de XenMobile, como se han definido en la consola administrativa de Device Manager. De forma predeterminada, solo se muestran los grupos que contienen usuarios conectados actualmente. Puede ver el dispositivo de cada usuario junto a la entrada del usuario.

1. Para ver todos los usuarios, expanda cada grupo de la columna de la izquierda.
   Los usuarios actualmente conectados al servidor XenMobile se indican con un icono verde.
2. Para mostrar todos los usuarios, incluidos los que no están conectados, haga clic en **View** y seleccione **Non-connected devices.**
   Los usuarios no conectados aparecen sin el icono verde.

Los dispositivos conectados al servidor XenMobile pero no asignados a ningún usuario aparecen en modo anónimo. (La cadena **Anonymous** aparece en la lista). Puede controlar estos dispositivos igual que lo hace con los dispositivos donde un usuario ha iniciado una sesión.

Para controlar un dispositivo, seleccione el dispositivo haciendo clic en su fila y luego haga clic en **Control Device**. En la ventana de control remoto aparece una representación del dispositivo. Se puede interactuar con el dispositivo controlado de varias formas, entre ellas:

- Controlar la pantalla del dispositivo, incluidos los colores, en la ventana principal o en la ventana aparte, flotante.
- Establecer una sesión de voz sobre IP (VoIP) entre el servicio de Help Desk y el usuario. Configurar los parámetros de VoIP.
- Establecer una sesión de chat con el usuario.
- Acceder al administrador de tareas del dispositivo para administrar elementos como, por ejemplo, el uso de memoria, el uso de la CPU, y las aplicaciones que se estén ejecutando.
- Explorar los directorios locales del dispositivo móvil. Transferir archivos.
- Editar el Registro del dispositivo en dispositivos Windows Mobile.
- Mostrar información del sistema del dispositivo y todo el software instalado.
- Actualizar el estado de la conexión del dispositivo móvil con el servidor XenMobile.

Opciones de la interfaz de línea de comandos en XenMobile

Jul 27, 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]

Herramienta XenMobile Analyzer

Oct 31, 2016

XenMobile Analyzer es una herramienta basada en la nube que sirve para diagnosticar y solucionar problemas relacionados con la instalación y otras funciones de XenMobile. La herramienta comprueba si hay problemas con la inscripción de dispositivos o usuarios y con la autenticación dentro del entorno de XenMobile.

Para habilitar la comprobación, debe configurar la herramienta para que apunte al servidor XenMobile y debe proporcionar otros datos como el tipo de implementación del servidor, la plataforma móvil, el tipo de autenticación y las credenciales de usuario para las pruebas. La herramienta, a continuación, se conecta al servidor y analiza el entorno para buscar problemas de configuración. Si XenMobile Analyzer detecta problemas, la herramienta muestra recomendaciones para corregirlos.

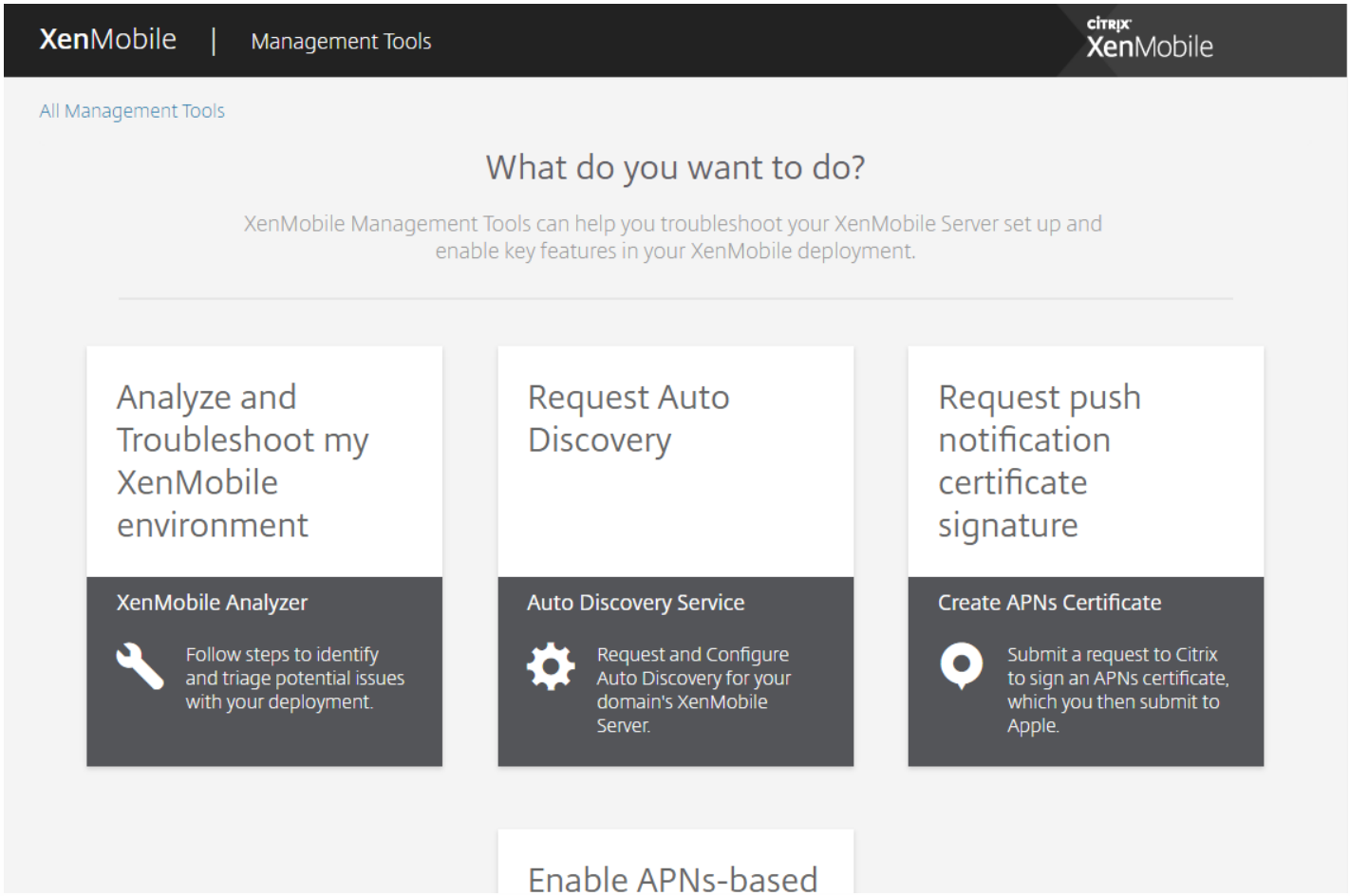
Funciones principales de XenMobile Analyzer

- Ofrece un microservicio seguro basado en la nube para solucionar todo tipo de problemas técnicos relacionados con XenMobile.
- Ofrece recomendaciones precisas cuando hay problemas de configuración de XenMobile.
- Reduce las llamadas de asistencia y acelera la solución de problemas en entornos de XenMobile.
- Ofrece respaldo de día cero para publicaciones del servidor XenMobile.
- Habilita la inscripción personalizada de dispositivos iOS: respaldo de puertos personalizados para XenMobile (en puertos que no sean el 8443).
- Muestra un cuadro de diálogo de aceptación de certificados para certificados de servidor incompletos o que no sean de confianza.
- Detecta automáticamente casos de autenticación de dos factores.
- Pruebas de WorxWeb para la disponibilidad de los sitios de intranet.
- Comprobaciones del servicio de detección automática de WorxMail.
- Comprobaciones de Single Sign-On de ShareFile.
- Habilita el respaldo de puertos personalizados para NetScaler.
- Es compatible con exploradores Web que no estén en inglés.

Requisitos previos

Producto	Versión compatible
XenMobile Server	10.3.0 - 10.3.6
NetScaler Gateway	10.5 - 11.1
Simulación de inscripción de clientes	iOS y Android

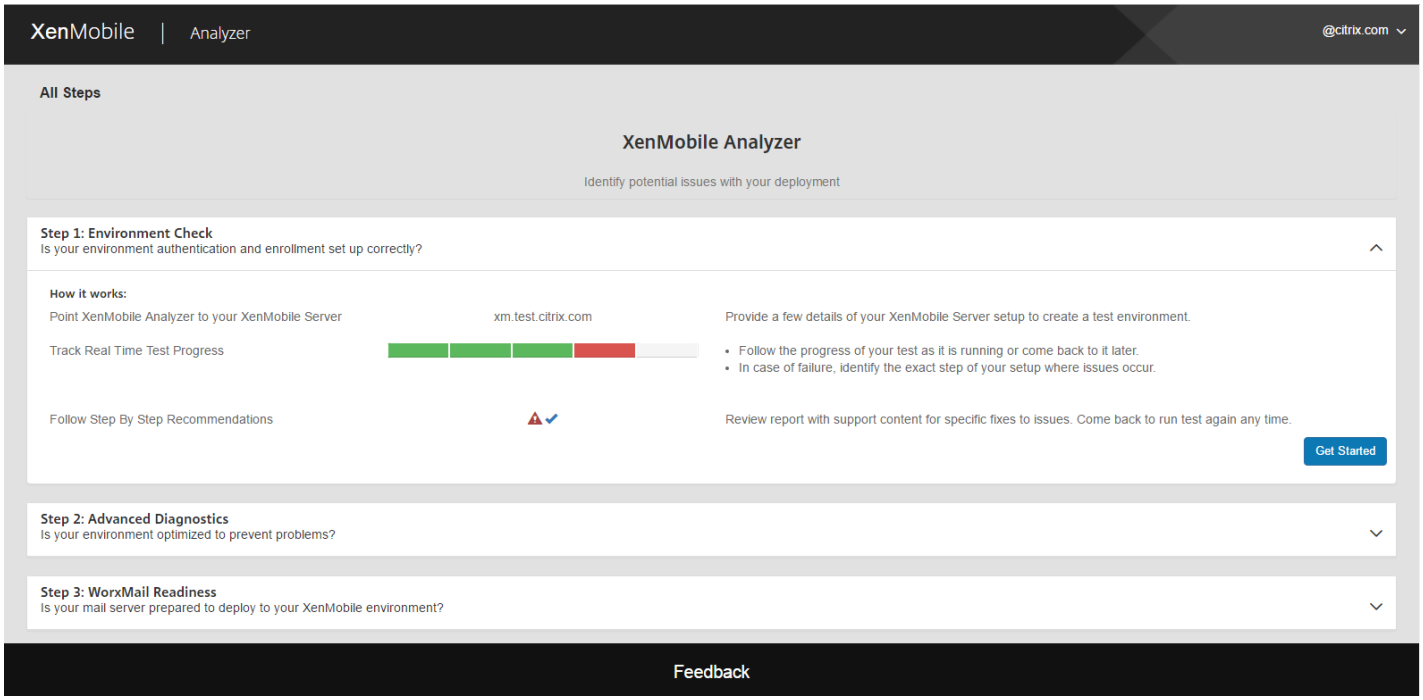
Para obtener acceso a la herramienta desde https://xenmobiletools.citrix.com tiene que usar sus credenciales de MyCitrix. En la página XenMobile Management Tools que se abre, inicie XenMobile Analyzer haciendo clic en **Analyze and Troubleshoot my XenMobile Environment**.



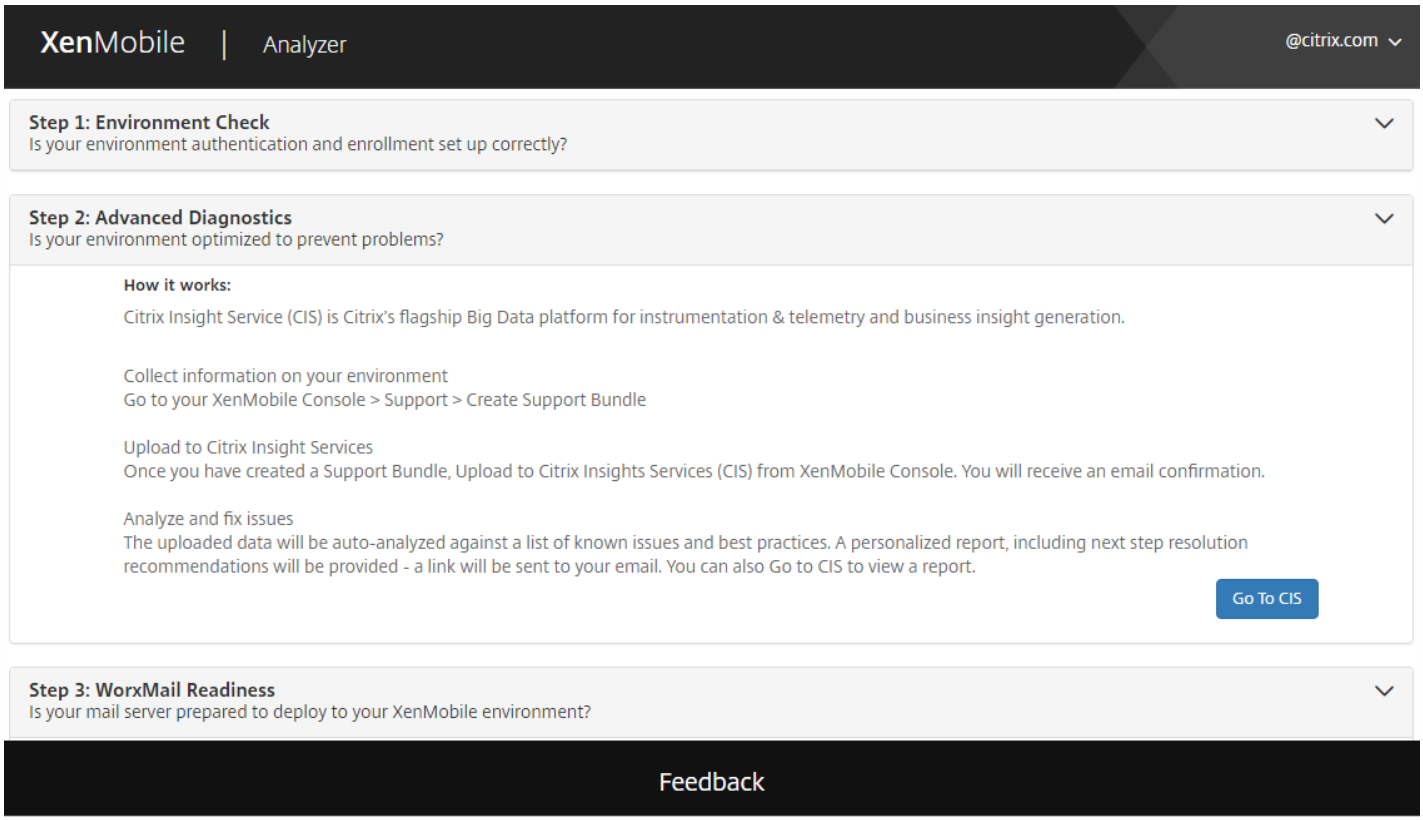
XenMobile Analyzer contiene cinco pasos principales diseñados para guiarle en el proceso de análisis y reducir la cantidad de tiquets de asistencia técnica que tenga que abrir, lo que puede reducir costes para todo el mundo.

Los pasos son:

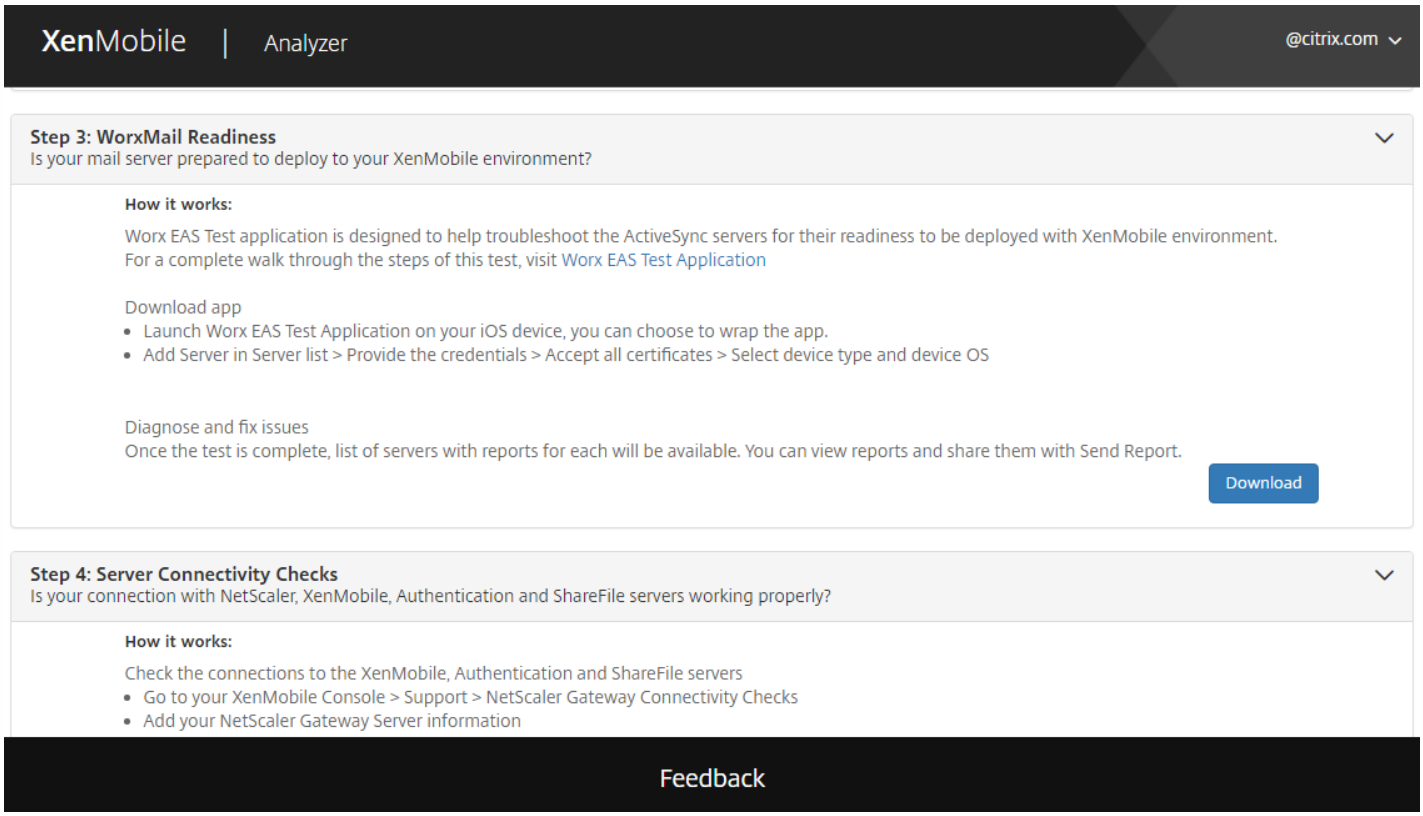
1. **Environment Check**: Este paso le guía a la hora de configurar pruebas para comprobar si hay problemas. También ofrece recomendaciones y soluciones para problemas de dispositivo, inscripción de usuarios y autenticación.



2. **Advanced Diagnostics** : Este paso ofrece información sobre cómo usar Citrix Insight Services para encontrar otros problemas que no se hayan detectado en el paso anterior de comprobación del entorno.

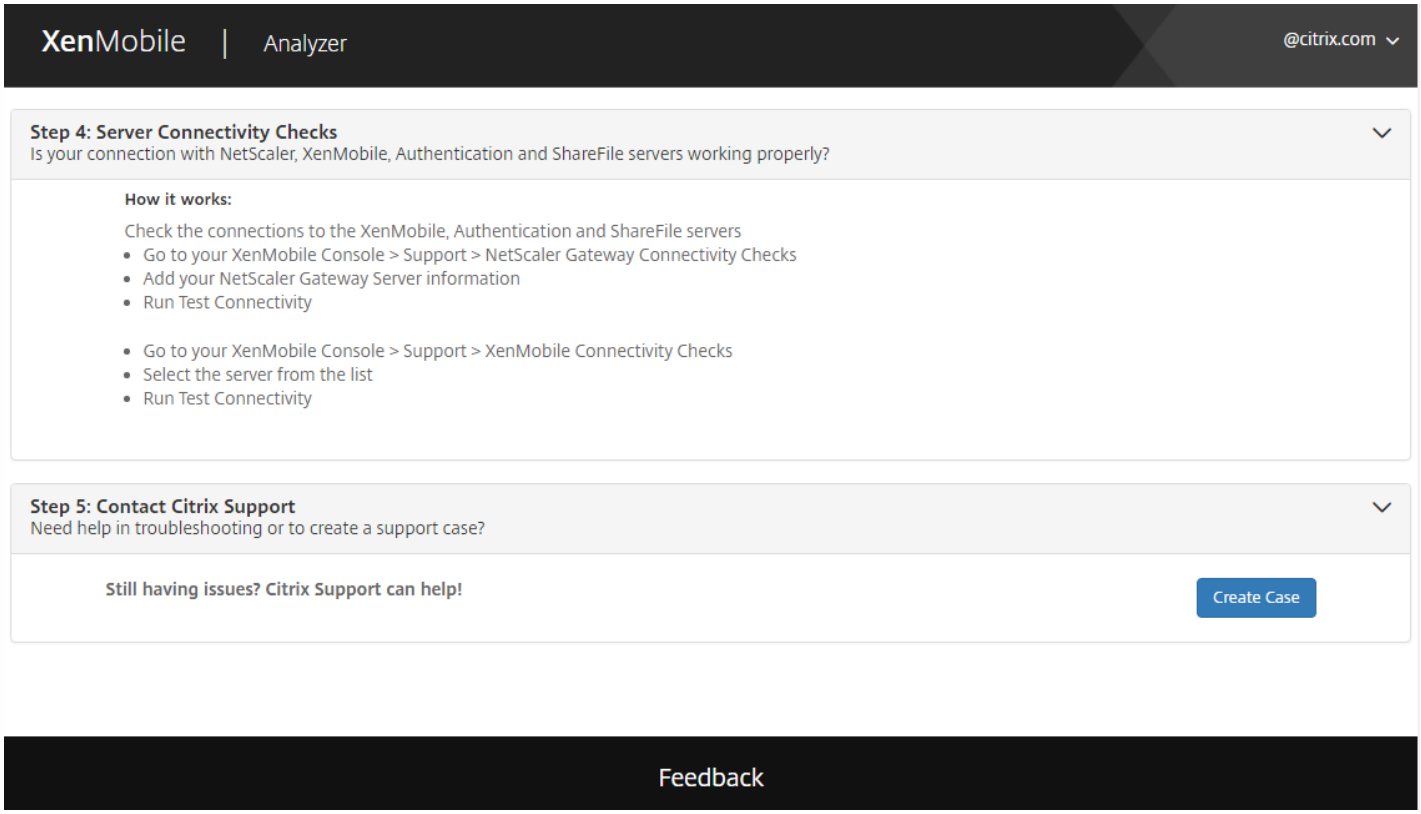


3. **WorxMail Readiness**: Este paso indica cómo descargar la aplicación Worx Exchange ActiveSync Test para ayudarle a solucionar problemas con los servidores de ActiveSync para ver si están preparados para su implementación en un entorno de XenMobile



4. **Server Connectivity Checks**: Este paso indica cómo probar la conectividad de los servidores.

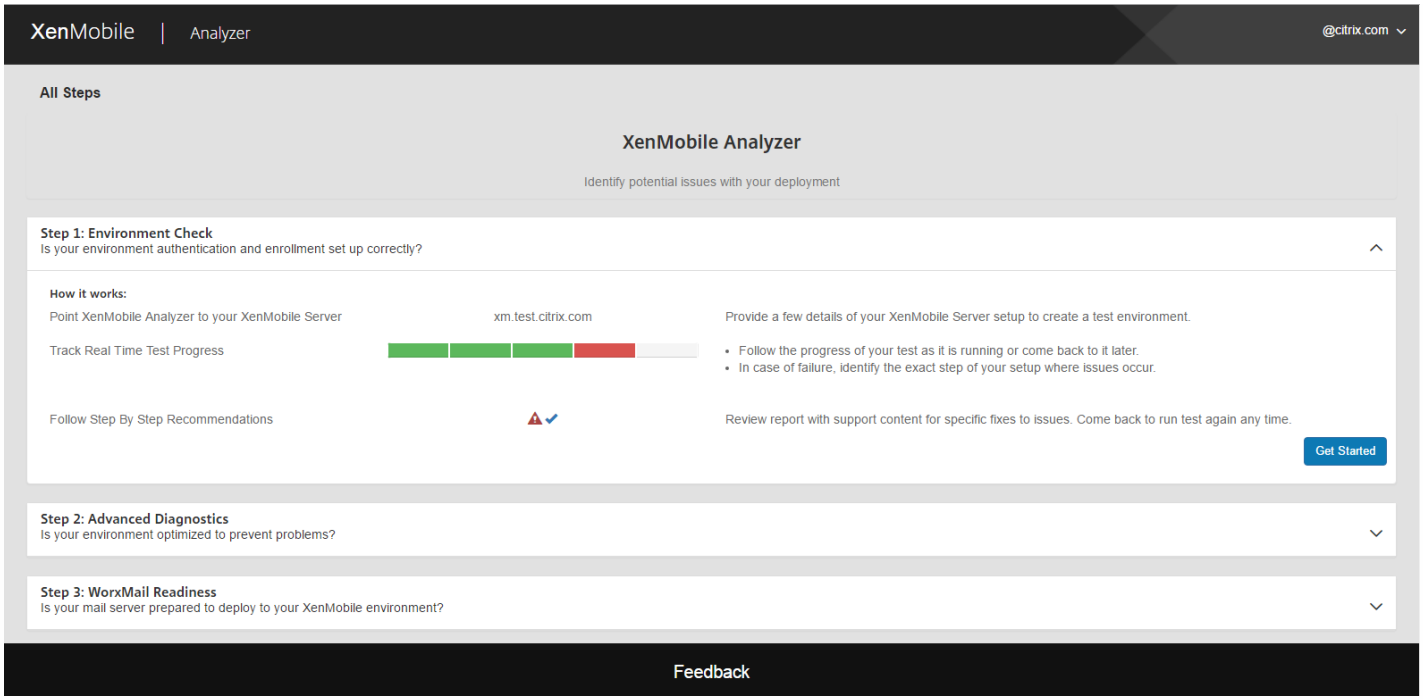
5. **Contact Citrix Support**: Este paso enlaza con el sitio donde puede abrir un caso de asistencia técnica de Citrix Support, si todavía tiene problemas.



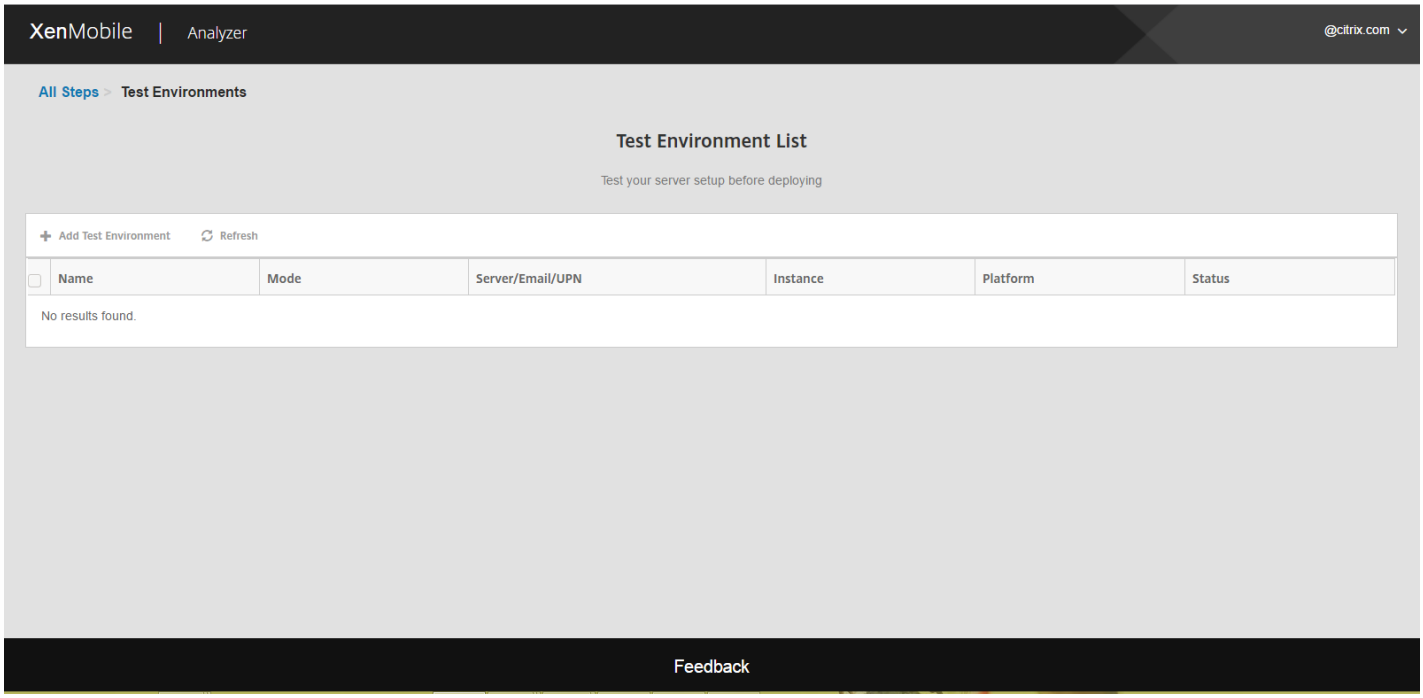
Las secciones siguientes describen cada paso en más detalle.

Comprobación del entorno

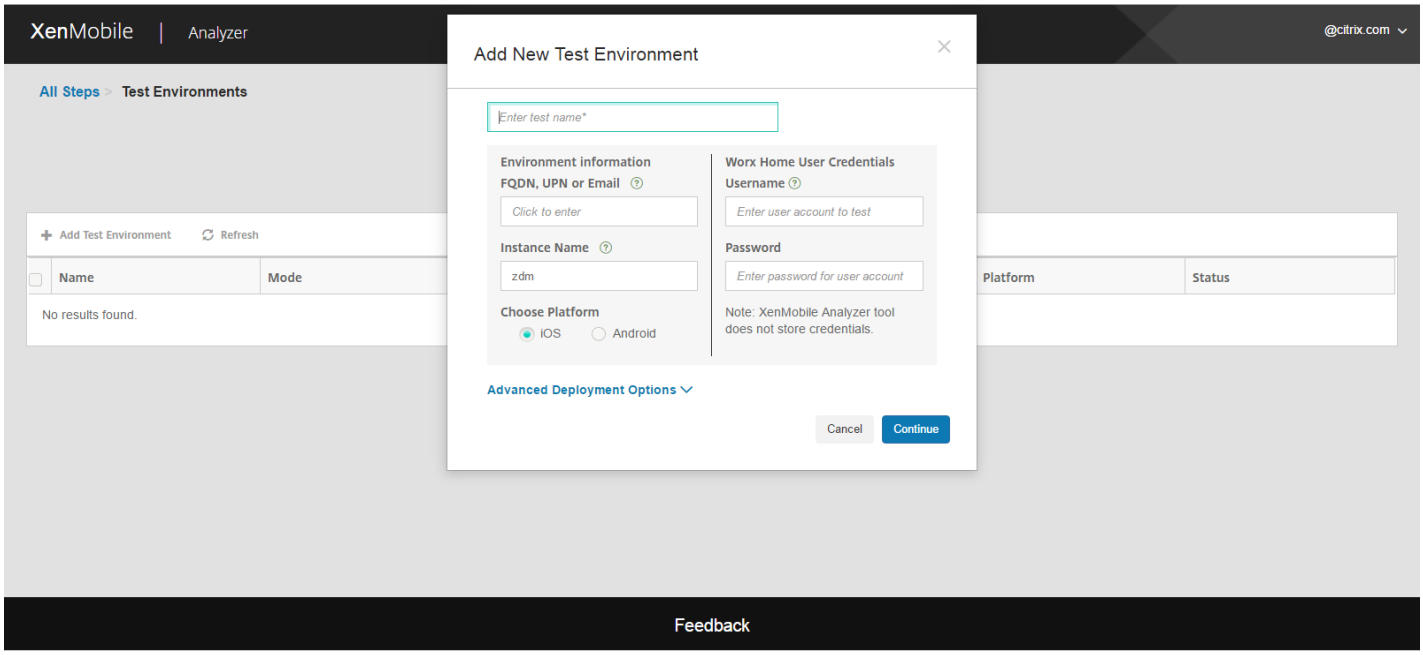
1. Inicie una sesión en XenMobile Analyzer y haga clic en **Step 1: Environment Checks**.
2. Haga clic en **Get Started**.



3. Haga clic en **Add Test Environment**.



4. En el cuadro de diálogo **Add Test Environment** , haga lo siguiente:



a. Proporcione un nombre único para la prueba para poder identificarla en el futuro.

b. Si dispone de una URL de invitación a la inscripción, haga clic en **Advance Deployment Options**. Cuando se expanda, marque la casilla **Do you have invitation URL** y, a continuación, introduzca la URL. Si deja el campo vacío, la herramienta intentará detectar automáticamente el servidor XenMobile, el nombre de usuario y otros detalles.

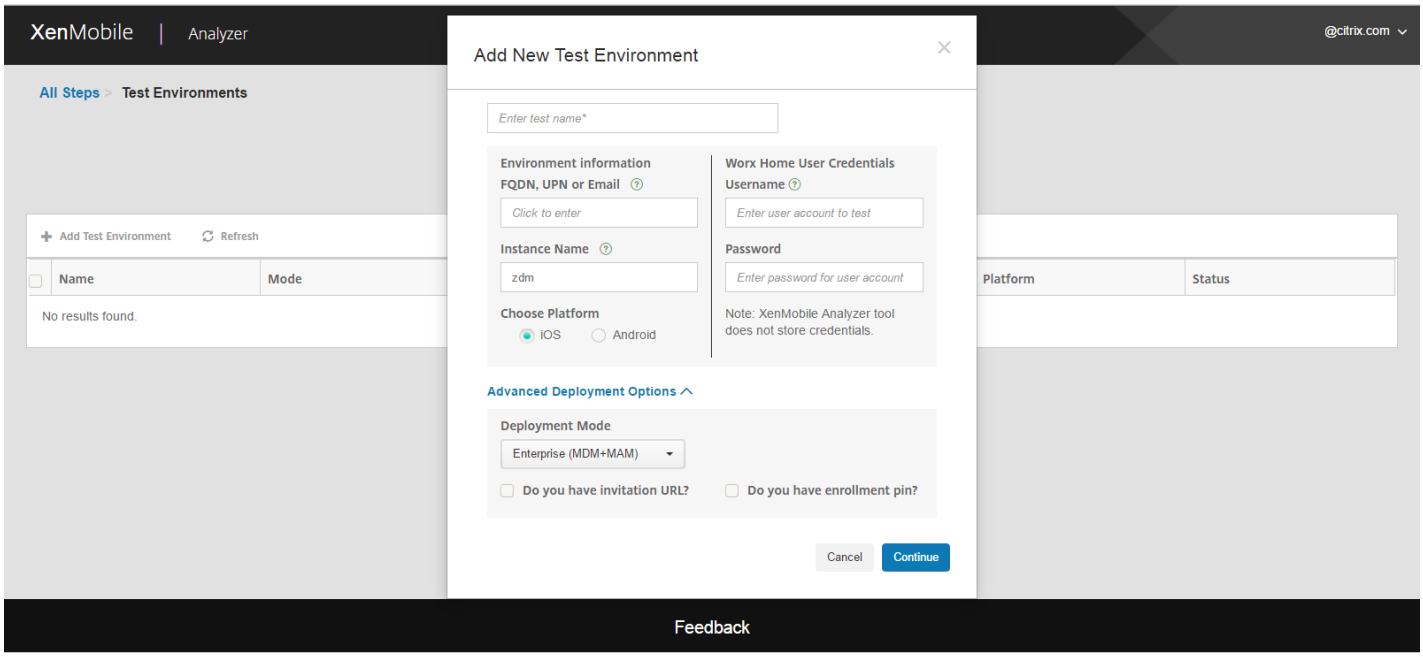
c. Si no dispone de una dirección URL de invitación, puede especificar la información del servidor de forma manual.

d. En la lista **Deployment Mode**, seleccione el modo de implementación de XenMobile.

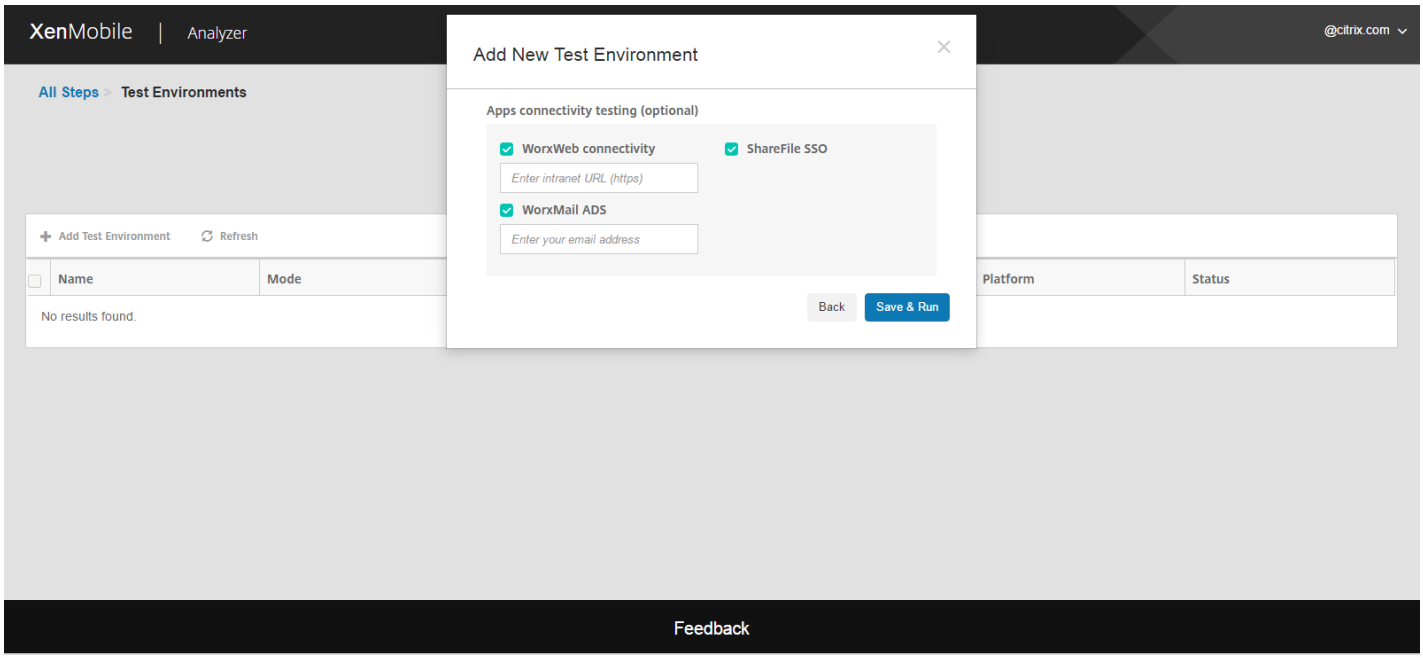
e. En **Instance Name**, introduzca el valor de su instancia personalizada.

f. En **Choose Platform**, seleccione **iOS** o **Android** como plataforma para las pruebas.

g. In **Username** y **Password**, introduzca el nombre de usuario y la contraseña para la autenticación. Si el entorno está configurado para la autenticación de dos factores, marque la casilla **Two Factor Authentication** e introduzca la segunda contraseña.



5. Haga clic en **Continue**.



6. Puede seleccionar pruebas a nivel de aplicaciones a ejecutar. Puede elegir una o varias de las siguientes pruebas.

   a. Conectividad con WorxWeb. Proporcione una URL de intranet. La herramienta comprobará la disponibilidad de la URL. Detectará si hay problemas de conectividad que podrían darse en la aplicación WorxWeb al intentar acceder a las direcciones URL de intranet.

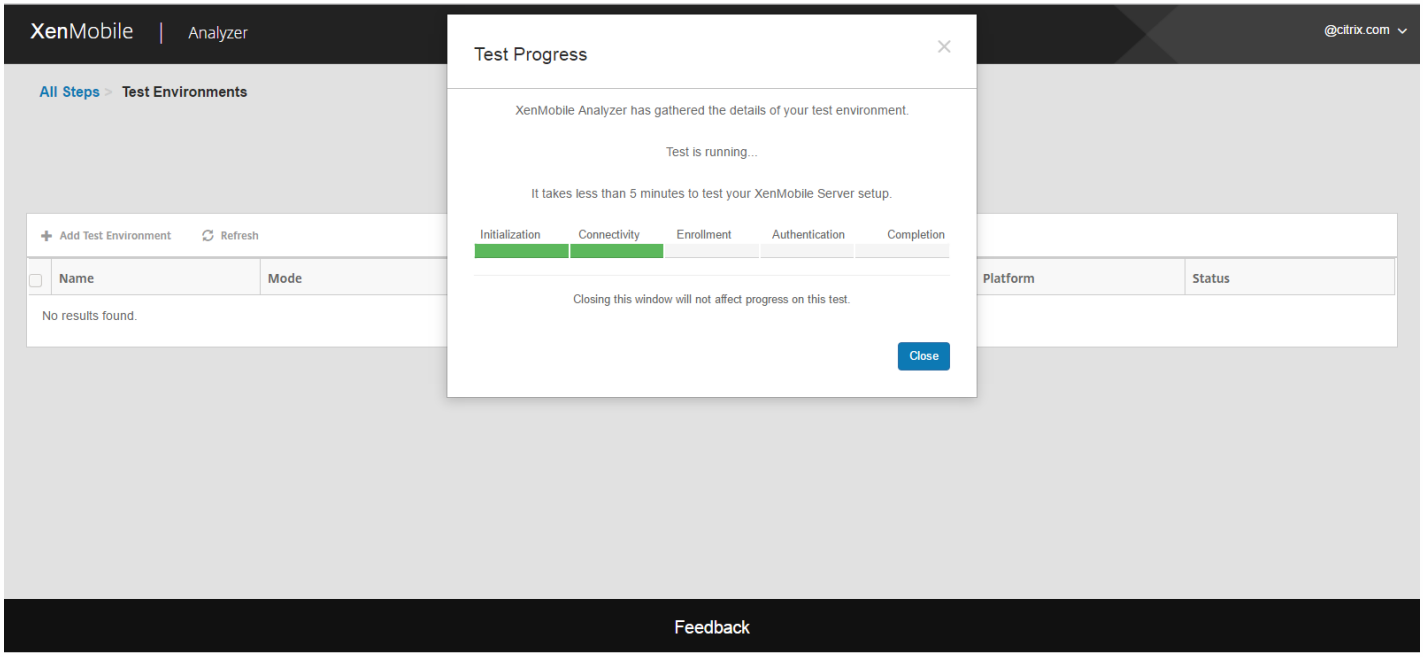
   b. ADS de WorxMail. Introduzca un ID de correo electrónico de usuario. Se utilizará para comprobar la detección automática de Microsoft Exchange Server en el entorno de XenMobile. Detectará si hay problemas relacionados con la detección automática de WorxMail.

c. SSO de ShareFile. Si se selecciona, XenMobile Analyzer comprobará si la resolución DNS de ShareFile se realiza correctamente y si el inicio de sesión único Single Sign-On de ShareFile funciona con las credenciales de usuario proporcionadas.

7. Haga clic en **Save & Run** para iniciar la ejecución de las pruebas.

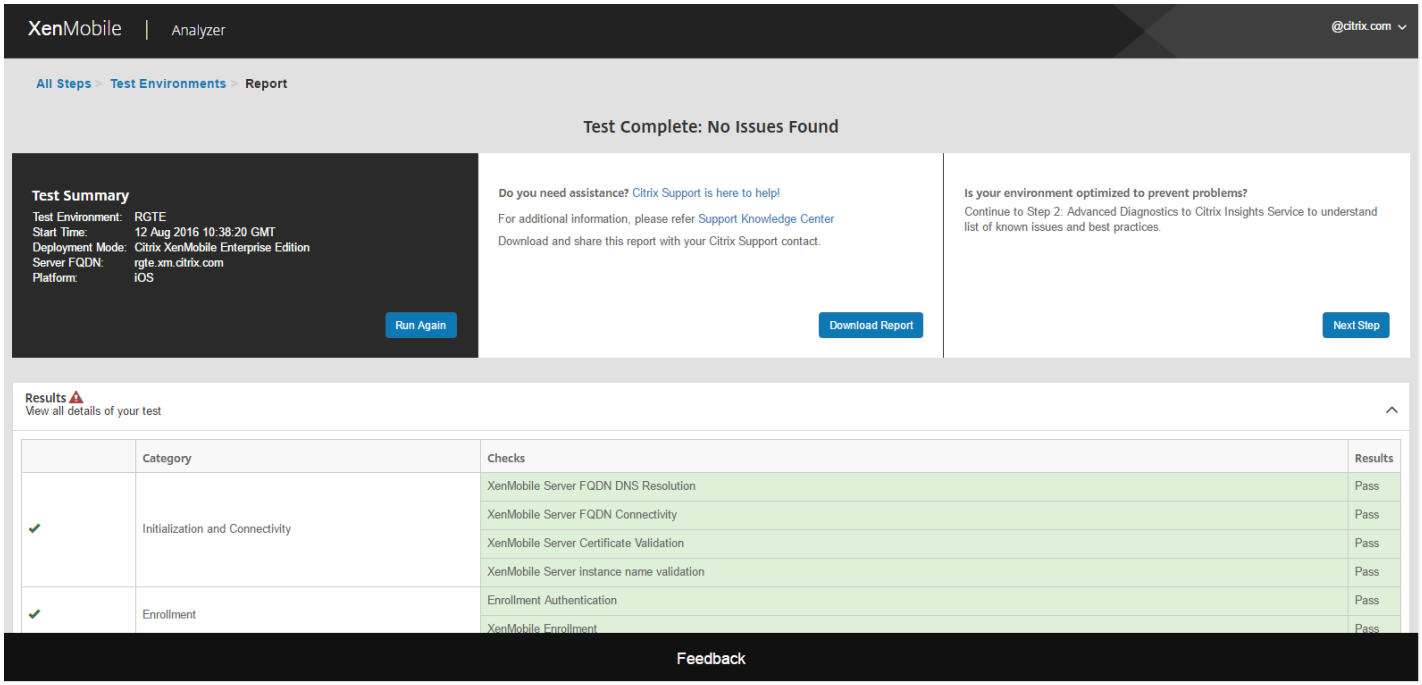
Aparecerá una notificación de progreso. Puede dejar el cuadro de diálogo de progreso abierto o cerrarlo, y las pruebas continuarán ejecutándose.

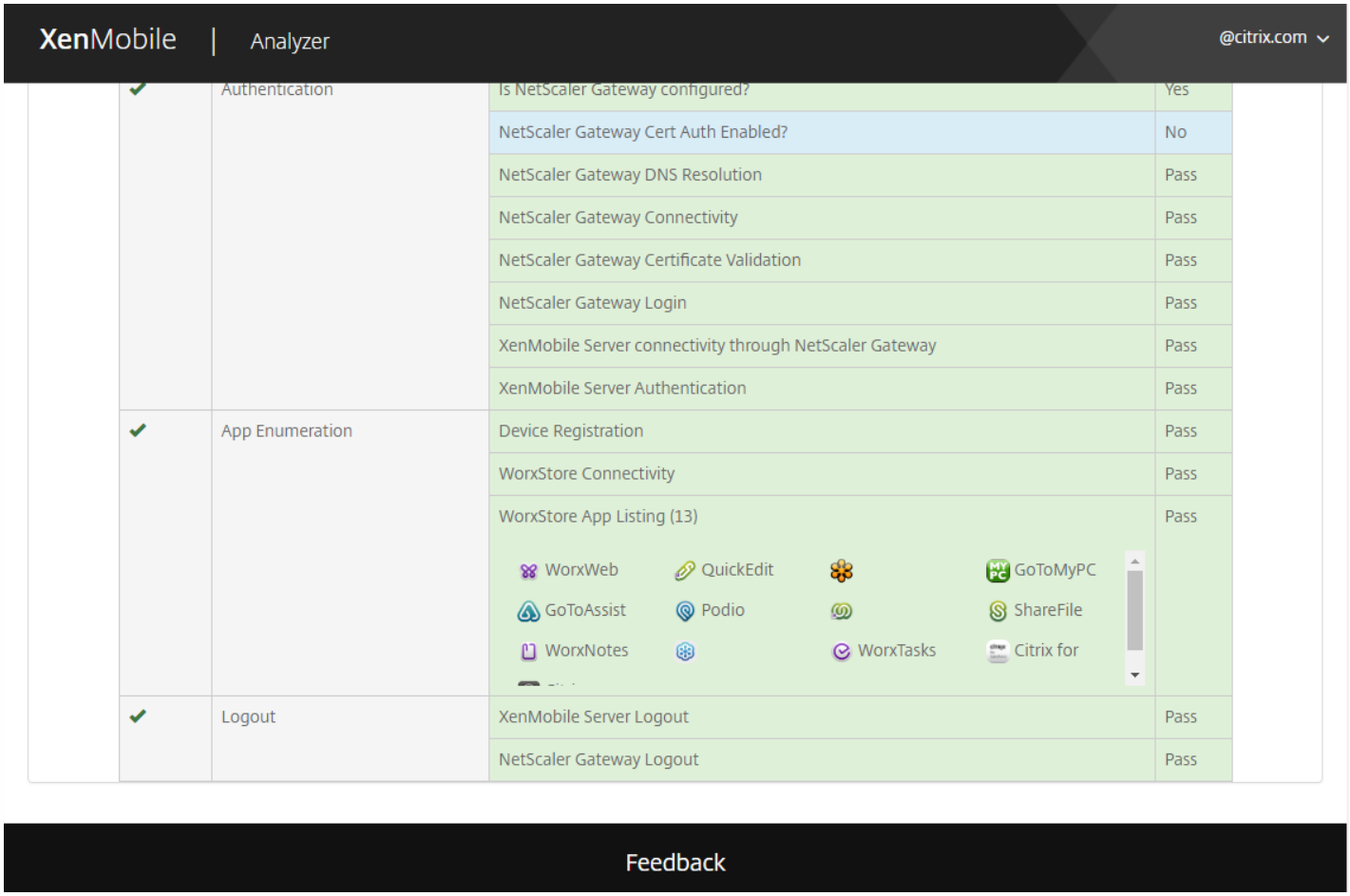
Las pruebas superadas aparecen en verde. Las pruebas que fallan aparecen en rojo.



8. En cualquier momento después de cerrar el cuadro de diálogo de progreso, puede volver a la página **Test Environments List** y hacer clic en el icono **View report** icono para ver los resultados de la prueba.

La página **Results** muestra los detalles de la prueba, recomendaciones y resultados.





Si las recomendaciones tienen artículos de Citrix Knowledge Base asociados a ellas, los artículos se enumeran en la página.

9. Haga clic en la ficha **Results** para mostrar la categoría y las pruebas realizadas por la herramienta, con sus

resultados correspondientes.

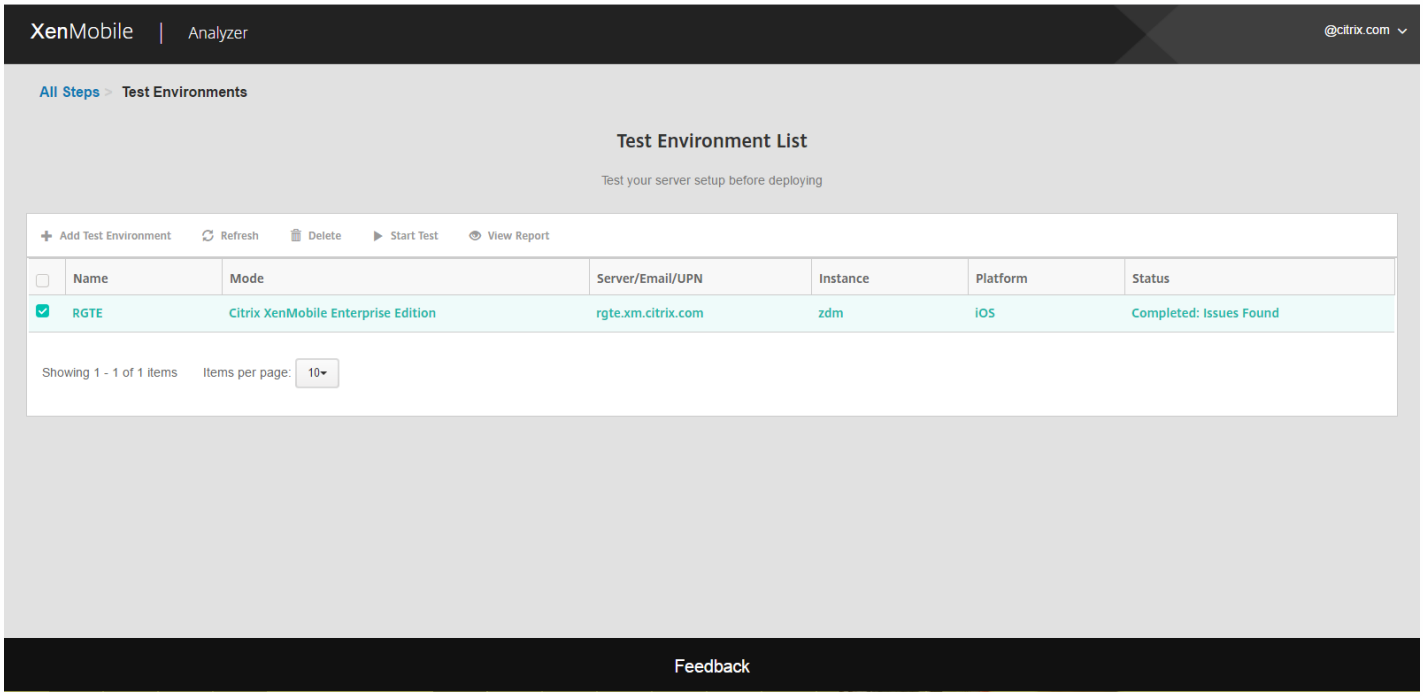
a. Para descargar el informe, haga clic en **Download report**.

b. Para volver a la lista de entornos de prueba, haga clic en **Test Environments**.

c. Para volver a ejecutar la prueba, haga clic en **Run Again**.

d. Si quiere volver a ejecutar otra prueba, vuelva a **Test Environments**, seleccione la prueba y haga clic en **Start Test**.

e. Para ir al siguiente paso de XenMobile Analyzer, haga clic en **Next Step**.



Pasos 2-5 de XenMobile Analyzer

El primer paso de XenMobile Analyzer (comprobación del entorno) es interactivo, mientras que los pasos siguientes del 2 al 5 son informativos. Cada uno de estos pasos proporciona información acerca de otras herramientas de asistencia técnica que se pueden usar para asegurarse de que el entorno de XenMobile esté configurado correctamente.

- **Paso 2** - **Advanced Diagnostics**: Este paso le guía para recopilar información sobre el entorno y luego cargarla en Citrix Insight Services. La herramienta analiza los datos y proporciona un informe personalizado con resoluciones recomendadas.
- **Paso 3** - **WorxMail Readiness**: Este paso le guía para descargar y ejecutar la aplicación Worx Exchange ActiveSync Test. La aplicación detecta problemas en los servidores ActiveSync si no están preparados para implementarse con entornos de XenMobile. Después de ejecutar la aplicación, puede ver informes o compartirlos con otras personas.
- **Paso 4** - **Server Connectivity Checks:** Este paso ofrece instrucciones para comprobar las conexiones con los servidores XenMobile, servidores de autenticación y ShareFile.
- **Paso 5** - **Contact Citrix Support**: Si todo lo anterior falla, puede crear un tiquet de asistencia técnica en Citrix Support.

Problemas conocidos

Estos son los problemas conocidos relacionados con XenMobile Analyzer:

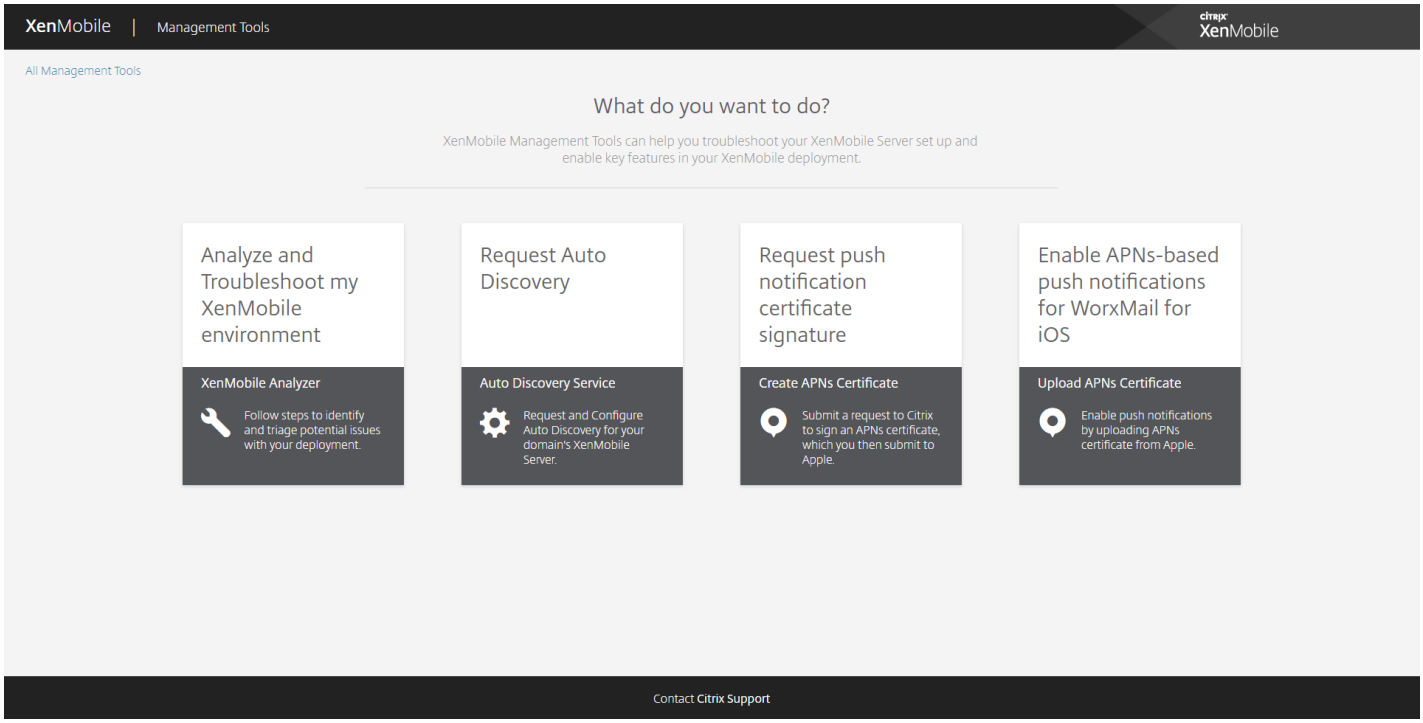
- La cantidad de aplicaciones indicada puede variar en función del cliente, si la directiva Platform Restriction está definida en XenMobile.
- Al comprobar la conectividad de WorxWeb a la intranet, no se respalda introducir varias direcciones URL en el cuadro de texto.
- No se respalda la característica de autenticación de dispositivos compartidos de Worx Home.

XenMobile AutoDiscovery Service

Jul 27, 2016

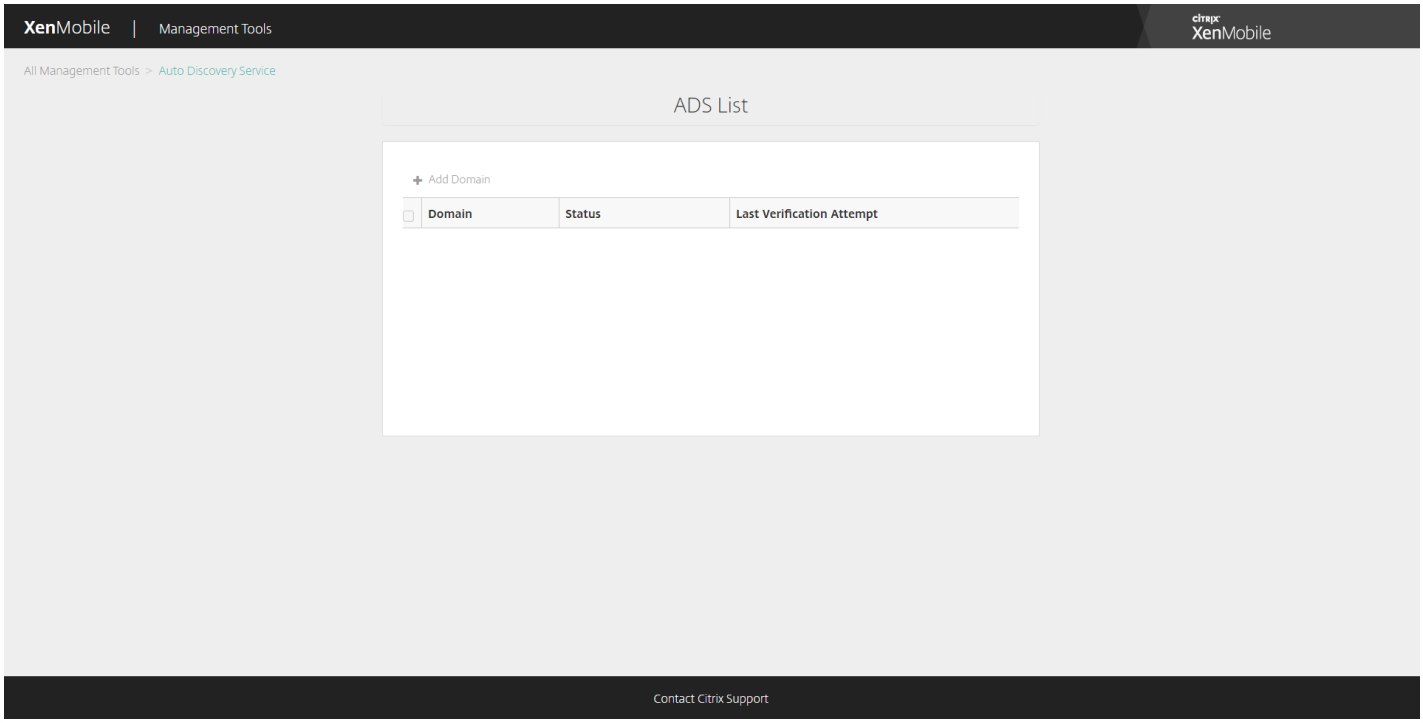
La detección automática es una parte importante de las implementaciones de XenMobile. La detección automática simplifica el proceso de inscripción para los usuarios. Con ella, pueden utilizar sus nombres de usuario y contraseñas de Active Directory para inscribir sus dispositivos, en lugar de tener que 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. XenMobile AutoDiscovery Service permite crear o editar un registro de detección automática sin ayuda del servicio de asistencia de Citrix Support.

Para acceder a XenMobile AutoDiscovery Service, vaya a https://xenmobiletools.citrix.com y haga clic en **Request Auto Discovery**.

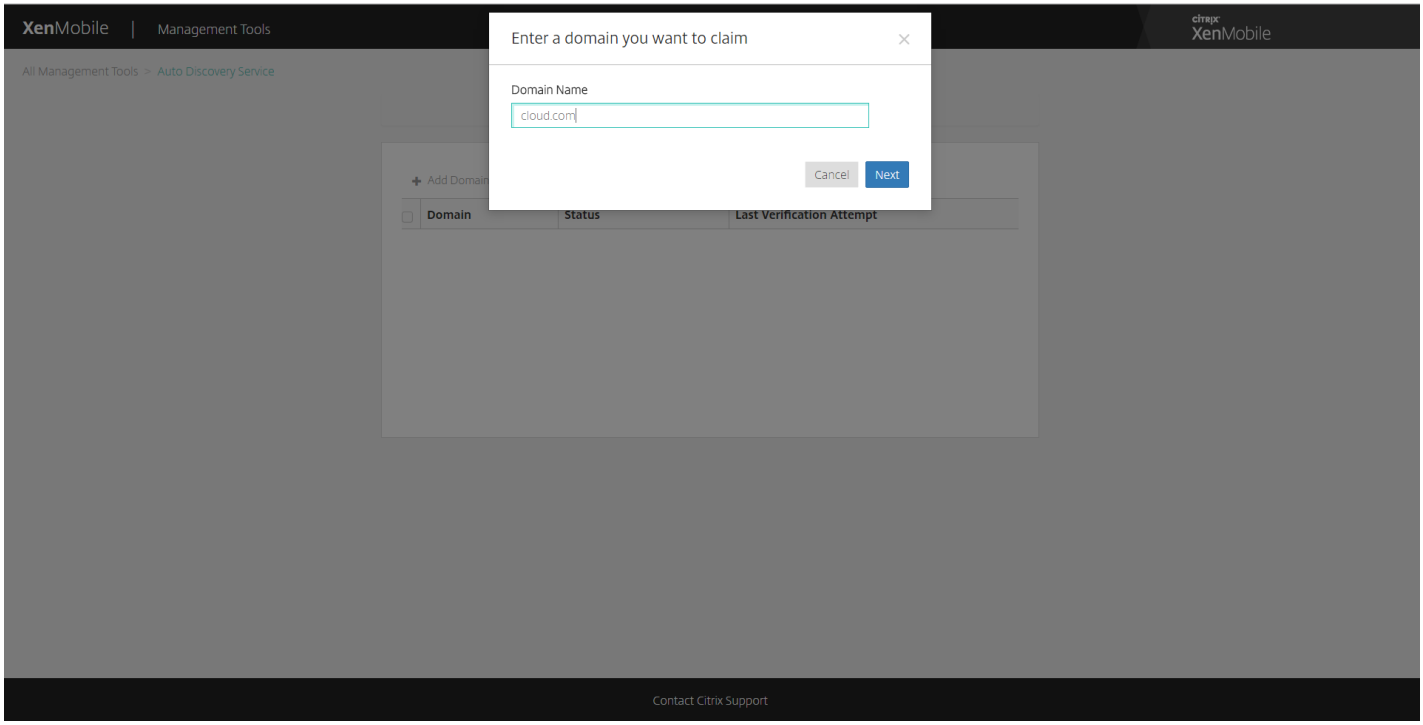


Cómo solicitar el servicio de detección automática

1. En la página AutoDiscovery Service, primero necesita reclamar un dominio. Haga clic en **Add Domain**.



2. En el cuadro de diálogo que se abre, introduzca el nombre de dominio de su entorno de XenMobile y, a continuación, haga clic en **Next**.



3. El paso siguiente proporciona instrucciones para verificar que usted es el propietario del dominio.

a. Copie el token de DNS suministrado en portal de herramientas de XenMobile.

b. Cree un registro TXT de DNS en el archivo de zona de su dominio en el portal de su proveedor de alojamiento de

dominios.

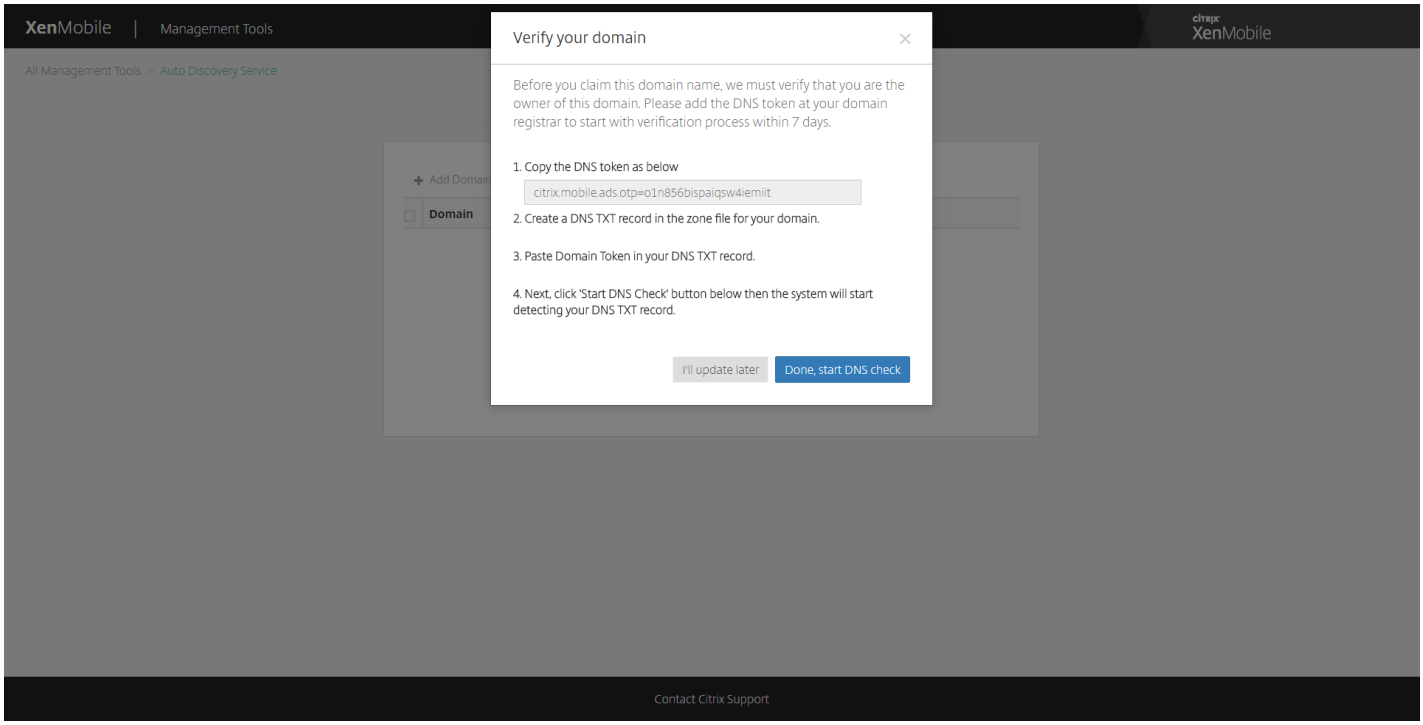
Para crear un registro TXT de DNS es necesario iniciar sesión en el portal del proveedor de alojamiento del dominio que agregó en el paso 2. En el portal de alojamiento de dominios puede editar sus registros de servidor de nombres de dominio (DNS) y agregar un registro TXT personalizado. Abajo hay un ejemplo para agregar una entrada TXT de DNS en el portal de alojamiento del dominio de ejemplo "domain.com".

c. Pegue el token de dominio en el registro TXT de DNS y guarde el registro de servidor de nombres de dominio (DNS).

d. De vuelta en el portal de herramientas de XenMobile, haga clic en Done, start DNS check.

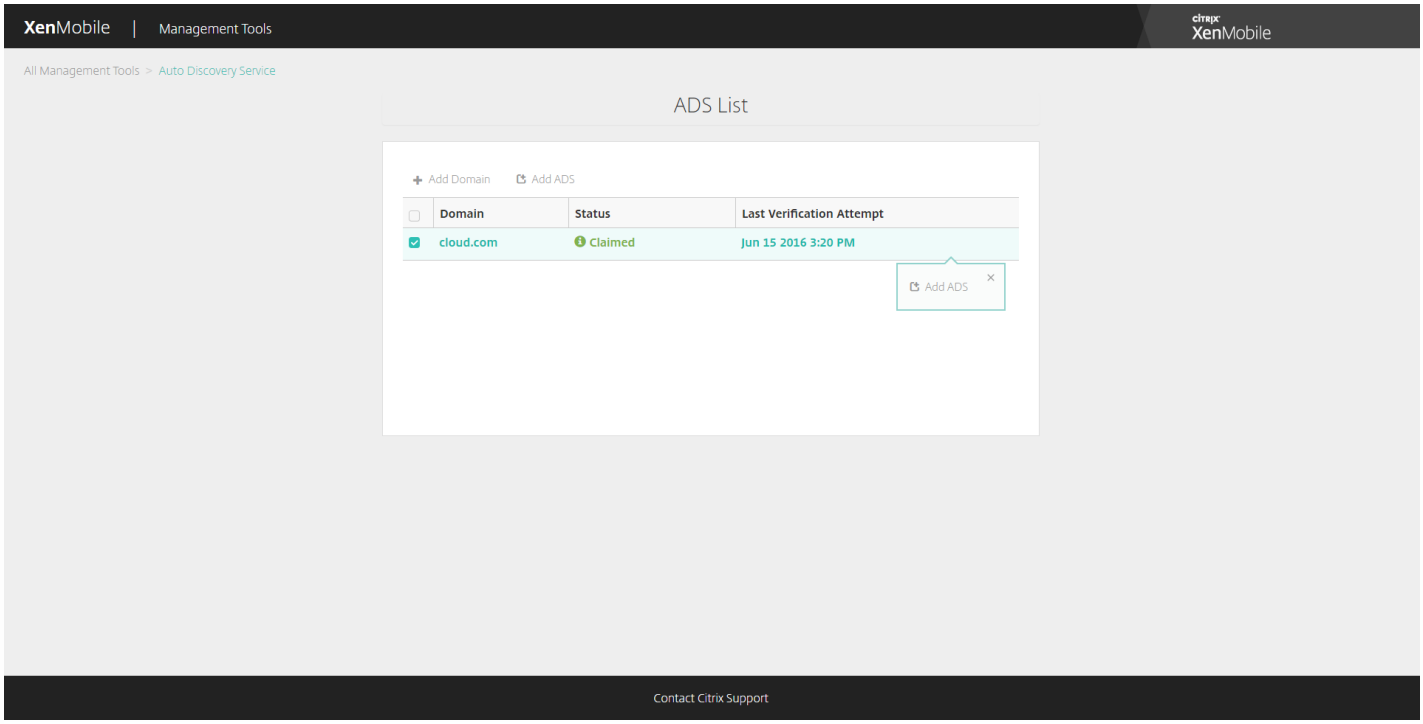
El sistema detecta el registro TXT de DNS. Si lo prefiere, puede hacer clic en I'll update later y el registro se guarda. La comprobación de DNS no se iniciará hasta que seleccione el registro en espera (Waiting) y haga clic en DNS Check.

Esta comprobación normalmente tarda aproximadamente una hora, pero puede tardar hasta dos días en devolver una respuesta. Además, es posible que tenga que abandonar el portal y volver a él para ver el cambio de estado.

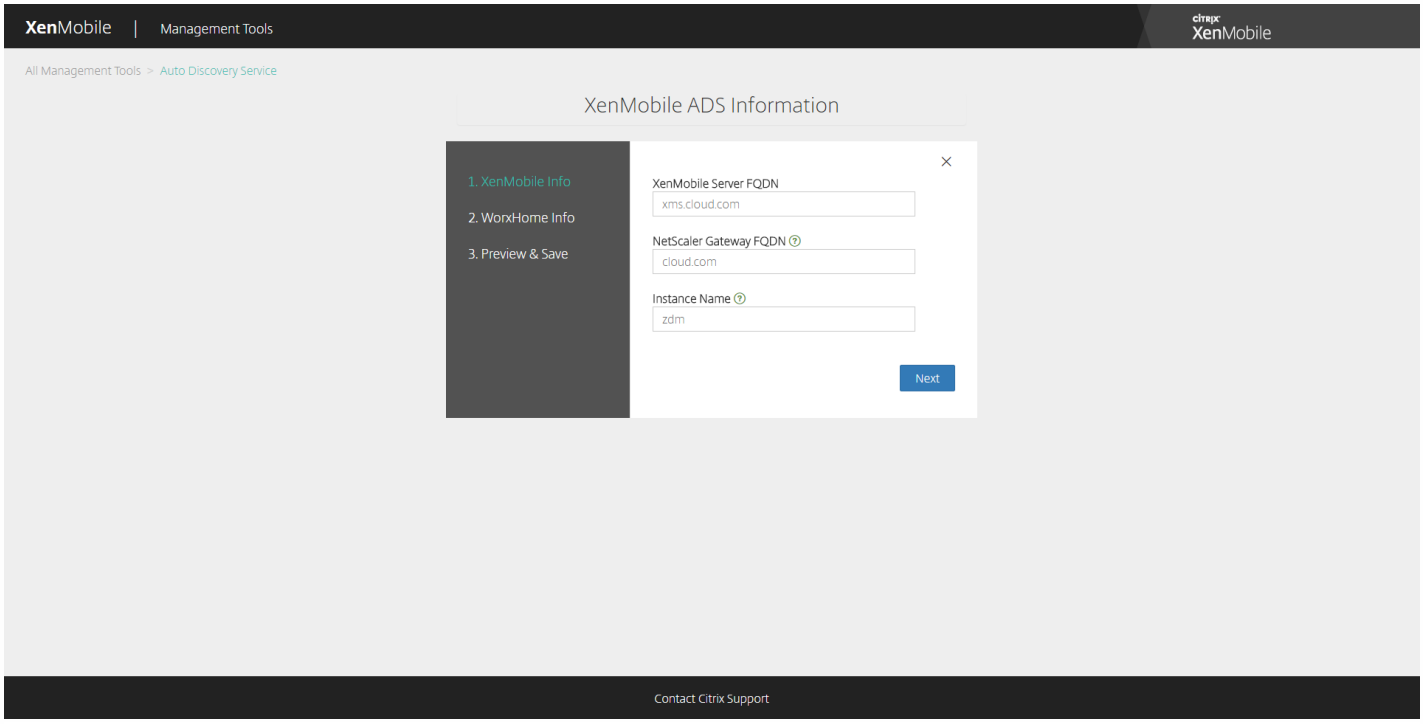


4. Después de reclamar su dominio, puede introducir la información para el servicio de detección automática. Haga clic con el botón secundario en el registro del dominio para el cual quiere solicitar detección automática y luego haga clic en **Agregar ADS**.

Si el dominio ya tiene un registro de AutoDiscovery, inicie un caso con el servicio de asistencia técnica de Citrix para modificar los detalles, según sea necesario.



5. Introduzca los nombres de dominio completos del servidor XenMobile y de NetScaler Gateway en **XenMobile Server FQDN** y **NetScaler Gateway FQDN**, y el nombre de la instancia en **Instance Name** y haga clic en **Next**. Si no está seguro, agregue una instancia predeterminada de "zdm".



6. Introduzca la siguiente información de Worx Home y haga clic en **Next**.

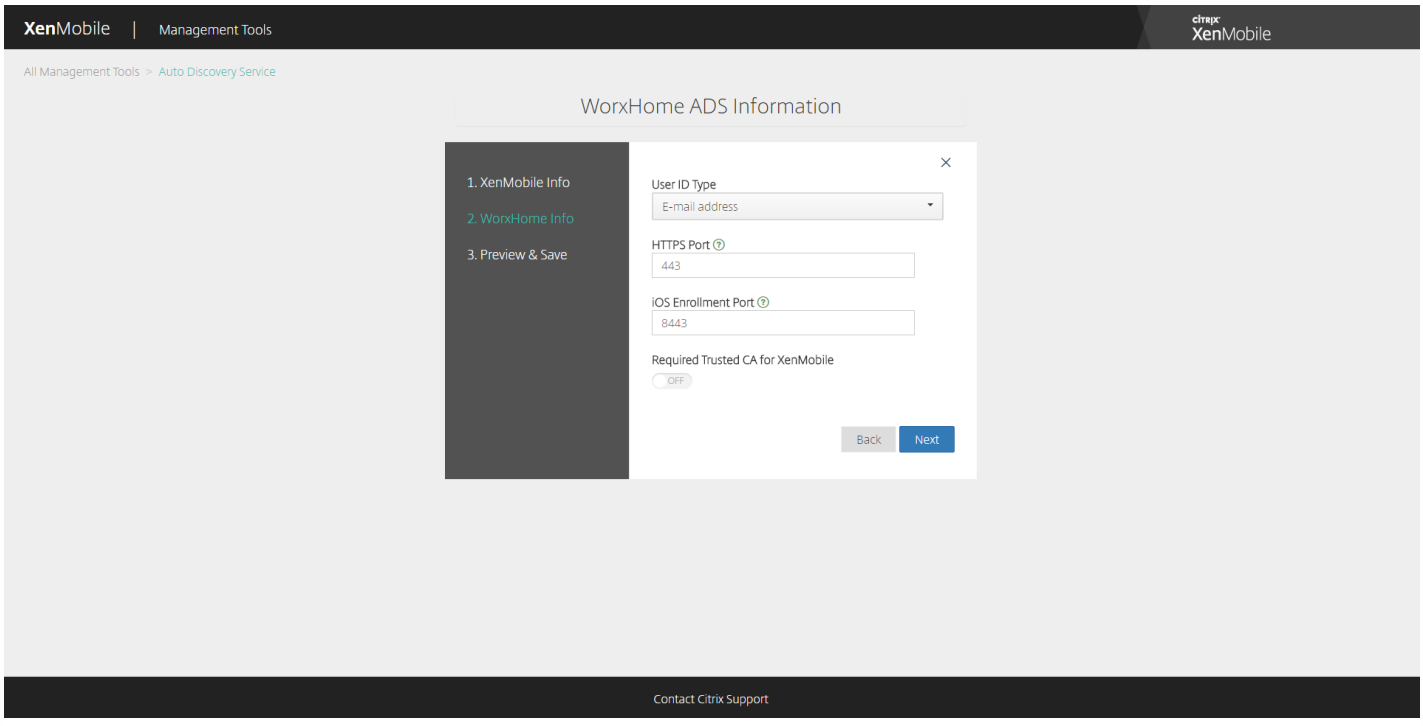
a. **User ID Type**: Seleccione el tipo de ID con el que los usuarios inician sesiones: **E-mail address** o **UPN**.

UPN se utiliza cuando el nombre principal de usuario (UPN) del usuario es el mismo que su dirección de correo electrónico. Ambos métodos usan el dominio especificado para buscar la dirección del servidor. Con **E-mail address** se pide al usuario que introduzca su nombre de usuario y contraseña, y con **UPN**, se le pide que escriba su contraseña.

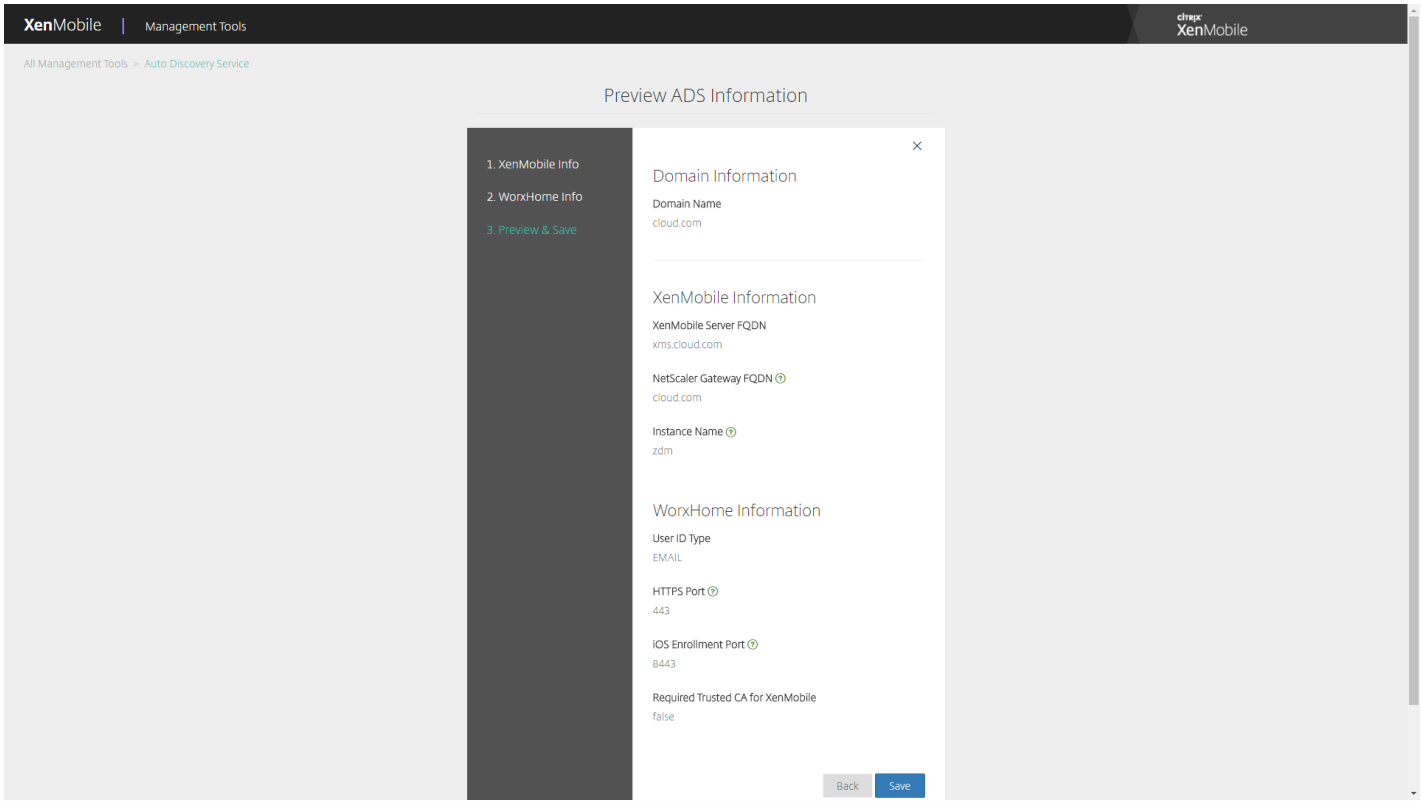
b. **HTTPS Port**: Introduzca el puerto usado para acceder a Worx Home sobre HTTPS. Por lo general, este es el puerto 443.

c. **iOS Enrollment Port**: Escriba el número de puerto que se utiliza para acceder a Worx Home para la inscripción de iOS. Por lo general, este es el puerto 8443.

d. **Required Trusted CA for XenMobile**: Indique si se necesita un certificado de confianza para acceder a XenMobile o no. Esta opción puede ser **OFF** u **ON**. Actualmente, no existe la capacidad para cargar un certificado para esta característica. Si quiere usar esta característica, debe llamar a la asistencia técnica de Citrix Support para que ellos configuren la detección automática. Para obtener más información sobre la fijación de certificados, consulte la sección sobre fijación de certificados en Worx Home. Para obtener más información acerca de los puertos necesarios para que funcione la fijación de certificados, consulte el artículo de asistencia XenMobile Port Requirements for ADS Connectivity.



7. Verá una página de resumen que muestra toda la información que ha introducido en los pasos anteriores. Compruebe que la información es correcta y, a continuación, haga clic en **Save**.



Información acerca de la API de REST en XenMobile

Jul 27, 2016

Con la API de REST de XenMobile puede invocar servicios que están expuestos a través de la consola de XenMobile. Puede invocar servicios REST usando cualquier cliente REST. La API no requiere el inicio de sesión en la consola de XenMobile para llamar a los servicios.

Para consultar toda la documentación sobre el conjunto actual de interfaces API disponibles, descargue el archivo PDF de Información acerca de la API de REST en XenMobile. Este artículo no incluye el conjunto completo de API.

Permisos necesarios para obtener acceso a la API de REST

Necesita uno de los siguientes permisos para acceder a la API de REST:

- Permiso de acceso a la API pública definido como parte de una configuración de acceso basado en roles (para obtener más información sobre cómo establecer el acceso basado en roles, consulte Configuración de roles con RBAC).
- Permiso de superusuario

Cómo invocar servicios de la API de REST

Puede invocar servicios de la API de REST mediante comandos de CURL o el cliente REST. Los ejemplos siguientes usan el cliente Advanced REST para Chrome.

> **Nota**
>
> En los siguientes ejemplos, deberá cambiar el nombre de host y el número de puerto para que coincidan con su entorno.

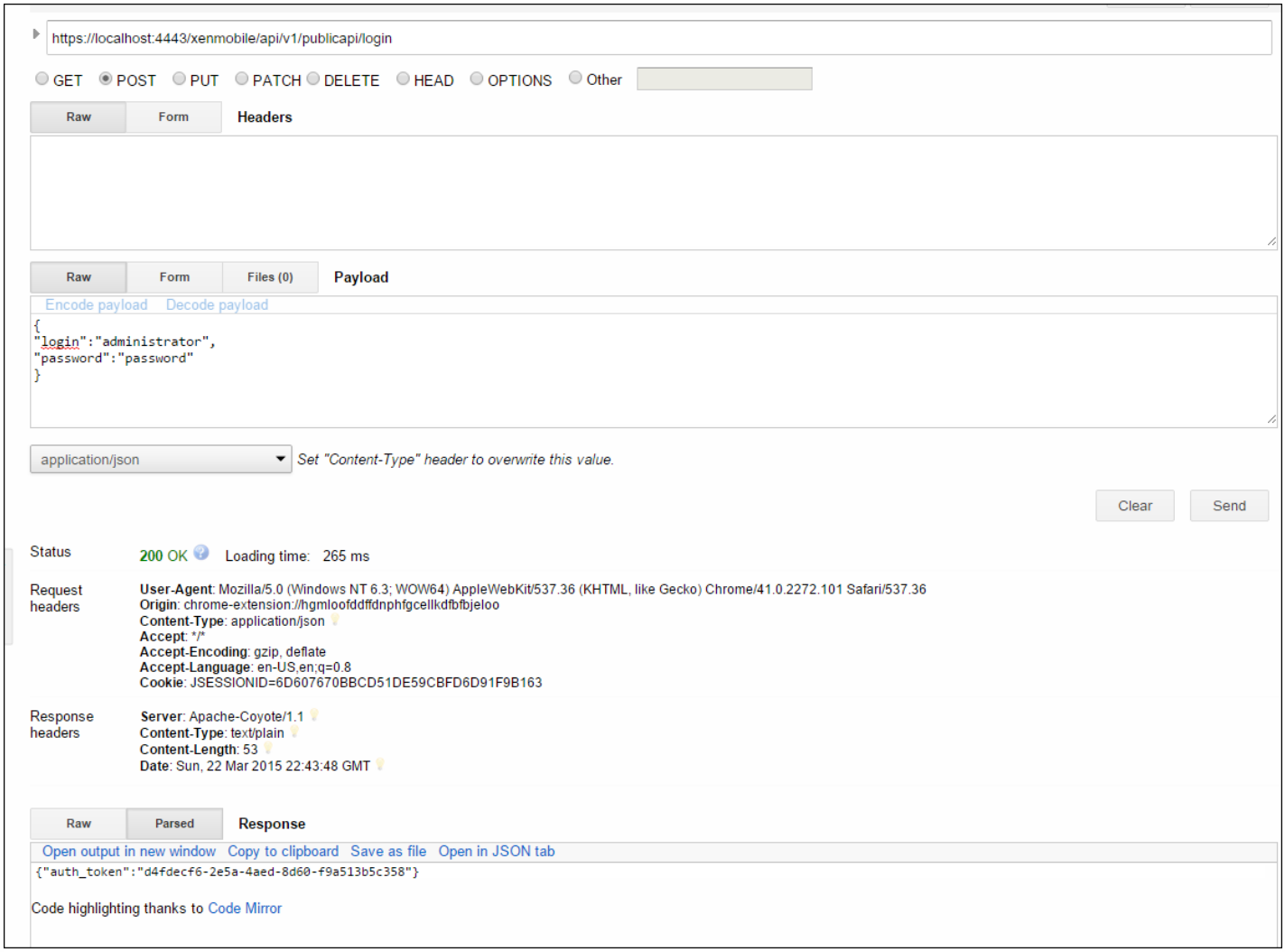
Inicio de sesión

URL: https://:/xenmobile/api/v1/authentication/login

Solicitud: { "login":"administrator", "password":"password" }

Tipo de método: POST

Tipo de contenido: application/json



Obtener grupos de entrega mediante filtro

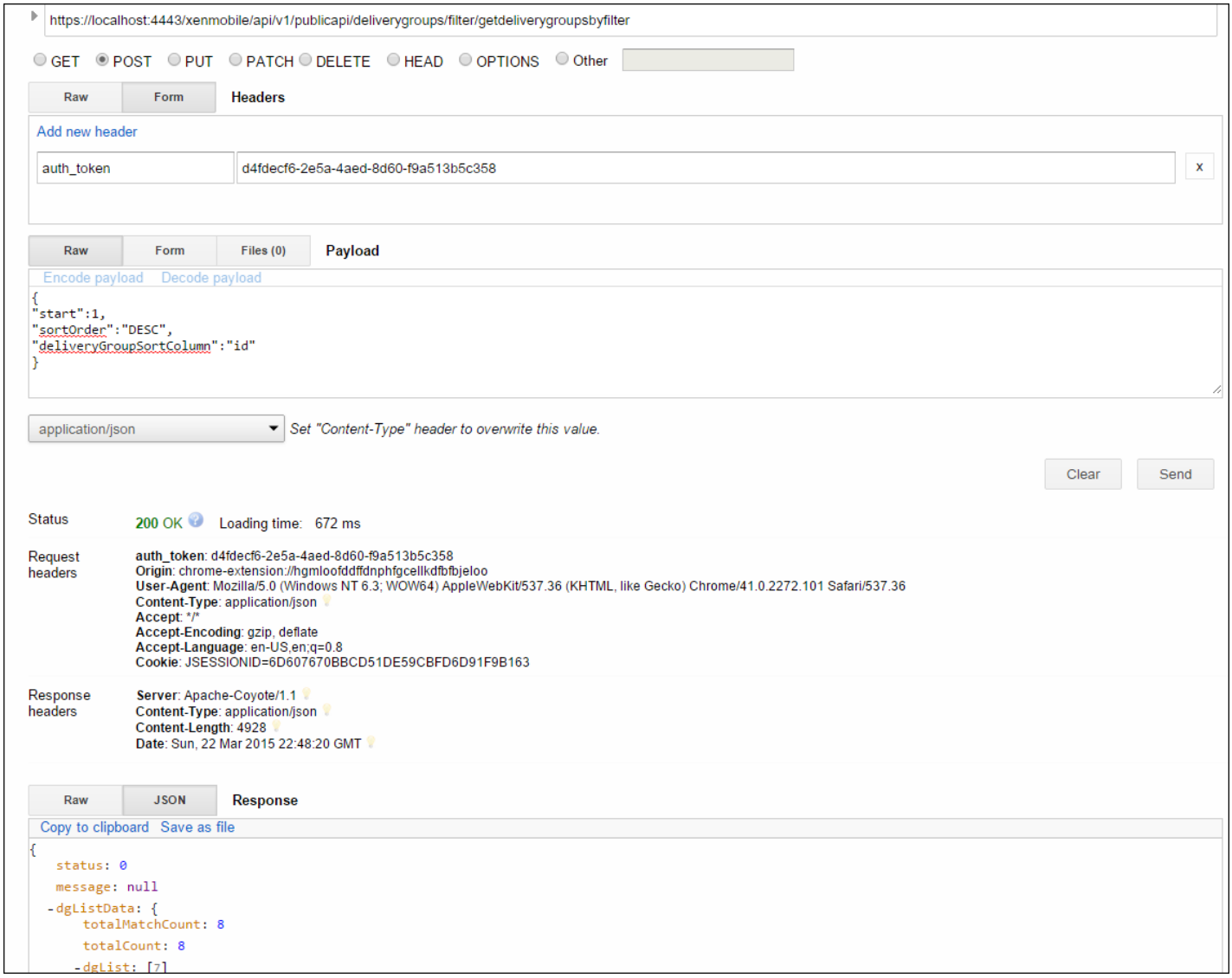
URL: /xenmobile/api/v1/deliverygroups/filter

Solicitud COPIAR

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

Tipo de método: POST

Tipo de contenido: application/json



Definiciones de las API de REST

Las siguientes secciones cubren algunas de las API que se encuentran en el archivo PDF. Consulte el documento PDF para consultar las API completas.

Recuerde: En los siguientes ejemplos, deberá cambiar el nombre de host y el número de puerto por los valores que tengan en su entorno.

Cómo iniciar sesión en la API pública

Con esta opción, se aceptan las credenciales de usuario y se utiliza el AuthenticationManager existente para autenticar al usuario. La primera vez que AuthenticationManager autentica a un usuario, genera un token de autenticación que se incluye en el encabezado de la solicitud.

URL: https://:4443/xenmobile/api/v1/authentication/login

Tipo de solicitud: POST

Parámetros de solicitud COPIAR

```
{ "login":"administrator", "password":"password" }
```

Ejemplo de respuesta COPIAR

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

Para iniciar sesión en la API pública mediante Workspace Cloud

Con esta opción, se aceptan las credenciales de usuario y se utiliza el AuthenticationManager existente para autenticar al usuario. La primera vez que AuthenticationManager autentica a un usuario, genera un token de autenticación que se incluye en el encabezado de la solicitud.

URL: https://:/xenmobile/api/v1/authentication/cwclogin

Tipo de solicitud: POST

Request header: Authorization – CWSAuth service=

Parámetros de solicitud COPIAR

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

Ejemplo de respuesta COPIAR

```
{

    "auth-token":"authentication token"

}
```

Cómo cerrar sesión en la API pública

Con esta opción, se quita el token de autenticación que se emitió cuando el usuario inició sesión y se cierra la sesión del usuario actual. Requiere el nombre de usuario y el token de autenticación.

URL: https://:/xenmobile/api/v1/authentication/logout

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Parámetros de solicitud COPIAR

```
{“login”:”administrator”}
```

Ejemplo de respuesta COPIAR

```
{"Status":"user administrator logged out successfully."}
```

Cómo administrar certificados

Las operaciones de administración de certificados permiten ver, eliminar, importar y agregar certificados a través de la API pública.

Obtener todos los certificados

Con esta opción, se devuelven todos los certificados de la base de datos.

URL: https://:/xenmobile/api/v1/certificates

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Parámetros de solicitud: Ninguno

Ejemplo de respuesta COPIAR


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
```



```
"signatureAlgo": "SHA1WithRSAEncryption",

"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,
```



```
                    "locality": null,

                    "state": null,

                    "country": null,

                    "description": null

                }

            }

        }

    ],

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Eliminar certificados

Con esta opción, se eliminan los certificados especificados. Requiere el ID de cada certificado que se va a eliminar.

URL: https://:/xenmobile/api/v1/publicapi/certificates

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Parámetros de solicitud COPIAR

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Importar certificado como certificado SAML

Con esta opción, se importa el certificado especificado como un certificado SAML.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/saml

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'saml',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```


Importar certificado como certificado de servidor

Con esta opción, se importa el certificado especificado como un certificado de servidor.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/server

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR


```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Importar certificado como certificado de agente de escucha

Con esta opción, se importa el certificado especificado como un certificado de agentes de escucha SSL.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/listener

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'listener',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,
```

```
    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Crear certificado

Con esta opción, se crea un certificado autofirmado o una solicitud de firma de certificado que requiere una firma por parte de la entidad de certificación.

URL: https://:/xenmobile/api/v1/certificates/csr

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/form_url_encoded

Parámetros de solicitud COPIAR

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

Ejemplo de respuesta COPIAR

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Exportar certificado

Con esta opción, se descarga el certificado especificado. En la siguiente tabla, se ofrece una lista de los parámetros necesarios para esta operación.

Parámetro	Requerido	Descripción

id	Sí	El ID numérico del certificado
usuario		La contraseña asociada al certificado que se va a exportar.
exportPrivateKey		Marca que indica si se va a exportar la clave privada.

URL: https://:/xenmobile/api/v1/certificates/export

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

Ejemplo de respuesta: Muestra la cadena de certificado en una solicitud correcta.

Cómo administrar almacenes de claves

Puede importar almacenes de claves a través de la API pública.

Importar un almacén de claves de servidor

Con esta opción, se importa un almacén de claves del servidor.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/server

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importar un almacén de claves de SAML

Con esta opción, se importa un almacén de claves de SAML.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/saml

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
 }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importar un almacén de claves de APNs

Con esta opción, se importa un almacén de claves de APNS.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/apns

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importar un almacén de claves de agente de escucha SSL

Con esta opción, se importa un almacén de claves de agente de escucha SSL.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/listener

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud COPIAR

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Ejemplo de respuesta COPIAR

```
{
```

```
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
"certificate": null,
"apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Cómo administrar licencias

Con esta opción, puede administrar licencias a través de la API pública.

Obtener información de licencia

Con esta opción, se ofrece información acerca de todas las licencias.

URL: https://:/xenmobile/api/v1/licenses

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
{
    sadate: "2015.1210"
    notice: "Example Systems Inc."
    vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
    licensesInUse: 0
    licensesAvailable: 102
    overdraftLicenseCount: 2
    p_E_M: "CXM_ENTU_UD"
    serialNumber: "cxmretailent1000user"
    licenseType: "Retail"
    expirationDate: "01-DEC-2015"
}
licenseNotification:
{
    id: 1
    notificationEnabled: false
    notifyFrequency: 7
    notifyNumberDaysBeforeExpire: 60
    recepientList: ""
```

```
            emailContent: "License expiry notice"

        }

    }

}
```

Guardar información de licencia

Con esta opción, se guarda toda la información de licencia.

URL: https://:/xenmobile/api/v1/licenses

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,
```

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success"
}
```

Cargar archivo de licencia

Con esta opción, se carga el archivo de licencia especificado.

URL: https://:/xenmobile/api/v1/licenses/upload

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: multipart/form-data

Parámetros de solicitud: uploadFile =

Ejemplo de respuesta COPIAR

```
{

   "status": 0,

   "message": "Success"

}
```

Activar licencia

Con esta opción, se activa la licencia especificada.

URL: https://:/xenmobile/api/v1/licenses/activate/{license type}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud: Anexar el tipo de licencia a la URL de activación de licencia.

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success"

    "cpLicenseServer": null

}
```

Quitar todas las licencias

Con esta opción, se quitan todas las licencias.

URL: https://:/xenmobile/api/v1/licenses/remove

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "isConnected": null

}
```

Probar servidor de licencias

Con esta opción, se comprueba la conectividad en el servidor de licencias.

URL: https://:/xenmobile/api/v1/licenses/testserver/

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```

Obtener fecha de caducidad más temprana

Con esta opción, se busca la licencia con la fecha de caducidad más temprana.

URL: https://:/xenmobile/api/v1/licenses/getexpirationdate

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```


Cómo administrar configuraciones de LDAP

En la siguiente tabla, se ofrece una lista de los parámetros utilizados para las operaciones de configuración del protocolo LDAP.

Parámetro	Requerido	Descripción
primaryHost	Sí	Nombre de host o dirección IP del servidor LDAP principal. Entrada como dirección IP o nombre de dominio completo.
secondaryHost	No	Nombre de host o dirección IP del servidor LDAP secundario. Entrada como dirección IP o nombre de dominio completo.
puerto	Sí	Número de puerto del servidor LDAP.
username	Sí	Nombre de usuario válido para el servidor LDAP.
usuario	Sí	Contraseña para el nombre de usuario.
userBaseDN	Sí	
lockoutLimit	No	

lockoutTime	No	
useSecure	No	
userSearchBy	Sí	Busca usuarios por UPN o samaccount.
dominio	Sí	Nombre de dominio único para el servidor LDAP.
domainAlias	Sí	Alias para el dominio de LDAP.
globalCatalogPort	No	
gcRootContext	No	
groupBaseDN	Sí	
isDefault	No	Parte de la respuesta GET que indica si la configuración de LDAP es la predeterminada.
name	No	Parte de la respuesta GET que es un identificador único usado para actualizar o eliminar la configuración de LDAP.

Mostrar configuración de LDAP

Con esta opción, se muestra toda la configuración de LDAP en XenMobile.

URL: https://:/xenmobile/api/v1/ldap

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

Agregar nueva configuración de LDAP

Con esta opción, se agrega una nueva configuración de LDAP. El nombre de dominio debe ser único y no puede coincidir con ninguna otra configuración de LDAP.

URL: https://:/xenmobile/api/v1/ldap/msactivedirectory

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Ejemplo de respuesta COPIAR

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Modificar configuración de LDAP

Con esta opción, se modifica toda la configuración existente de LDAP salvo el dominio, que no se cambia con la operación de modificación.

URL: https://:/xenmobile/api/v1/ldap/msactivedirectory/{name}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Establecer la configuración predeterminada de LDAP

Con esta opción, se establece la configuración de LDAP especificada como el valor predeterminado.

URL: https://:/xenmobile/api/v1/ldap/default/{name}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Eliminar configuración de LDAP

Con esta opción, se elimina la configuración de LDAP especificada.

URL: https://:/xenmobile/api/v1/ldap/{name}

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Cómo administrar configuraciones de NetScaler Gateway

Con ello, puede administrar las configuraciones de NetScaler Gateway. En la siguiente tabla, se ofrece una lista de los parámetros utilizados en operaciones de NetScaler Gateway.

Parámetro	Requerido	Descripción
name	Sí	Nombre único de NetScaler Gateway
alias	No	
url	Sí	Dirección URL de acceso público para NetScaler Gateway.
passwordRequired	Sí	
logonType	Sí	Valores válidos: domain-only, domain-token, domain-certificate, certificate-only, certificate-token y token-only.
callback	No	
predeterminada,	Sí	Se establece en true o false al agregar o modificar una configuración de NetScaler Gateway. Si este parámetro no se aprueba, el valor predeterminado se establece en false.

id	No	Parte de la respuesta GET que es un identificador único usado para actualizar o eliminar la configuración de NetScaler Gateway.

Mostrar todas las configuraciones de NetScaler Gateway

Con esta opción, se muestra toda la configuración de NetScaler Gateway en XenMobile.

URL: https://:/xenmobile/api/v1/netscaler

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
```

```
        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false",

        "id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        }

    ]

}
```

Agregar nueva configuración de NetScaler Gateway

Con esta opción, se agrega una nueva configuración de NetScaler Gateway.

URL: https://:/xenmobile/api/v1/netscaler

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Modificar configuración de NetScaler Gateway

Con esta opción, se modifica la configuración de NetScaler Gateway especificada.

URL: https://:/xenmobile/api/v1/netscaler/{id}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain",

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Eliminar configuración de NetScaler Gateway

Con esta opción, se elimina la configuración de NetScaler Gateway especificada.

URL: https://:/xenmobile/api/v1/netscaler/{id}

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Establecer la configuración predeterminada de NetScaler

Con esta opción, se establece la configuración de NetScaler Gateway especificada como el valor predeterminado.

URL: https://:/xenmobile/api/v1/netscaler/default/{id}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Cómo administrar configuraciones del servidor de notificaciones SMS y SMTP

Las configuraciones del servidor SMS y SMTP se pueden agregar, modificar, activar (establecer como predeterminadas) o eliminar. En la siguiente tabla, se ofrece una lista de los parámetros utilizados para las operaciones de configuración del servidor SMS y SMTP.

Parámetro	Requerido	Descripción
name	Sí	Nombre único de la configuración de SMS o SMTP.
serverType	No	Tipo de servidor de notificaciones (SMS o SMTP) que ha enviado el servidor en la solicitud GET.
active	No	Indica si el servidor se usa para las notificaciones. Solo puede estar activo un servidor por cada tipo.
id	No	Identificador único que se usa para actualizar, eliminar o activar el servidor.
description	No	Descripción del servidor.
Parámetros SMS		
key	Sí	
secret	Sí	
virtualPhoneNumber	Sí	Debe estar en formato de número de teléfono.
https	Sí	El valor predeterminado es false.
country	Sí	
carrierGateway	Sí	El valor predeterminado es false.
Parámetros SMTP		
secureChannelProtocol	Sí	El tipo de protocolo de seguridad que se va a usar. Los valores válidos son:

		None, SSL y TLS. El valor predeterminado es None.
puerto	Sí	
authentication	Sí	Indica si se debe usar la autenticación. Los valores válidos son true y false.
username	Sí, si la autenticación es true.	
usuario	Sí, si la autenticación es true.	
msSecurePasswordAuth	Sí	El valor predeterminado es false.
fromName	Sí	
fromEmail	Sí	
numOfRetries	No	Un número entero. El valor predeterminado es 5.
timeout	No	Un número entero. El valor predeterminado es 30.
maxRecipients	No	Un número entero. El valor predeterminado es 100.

Mostrar todos los servidores SMTP y SMS

Con esta opción, se muestran todos los servidores SMTP y SMS en XenMobile.

URL: https://:/xenmobile/api/v1/notificationserver

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Aceptar: application/json

Ejemplo de respuesta COPIAR

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Obtener datos de servidor

Con esta opción, se obtiene información detallada sobre el servidor mediante el ID de ese servidor.

URL: https://:/xenmobile/api/v1/notificationserver/{id}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Aceptar: application/json

Ejemplo de respuesta SMS COPIAR

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Ejemplo de respuesta SMTP

COPIAR

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Agregar configuración de servidor SMS

Con esta opción, se agrega una configuración de servidor SMS.

URL: https://:/xenmobile/api/v1/notificationserver/sms

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

Modificar configuración de servidor SMS

Con esta opción, se modifica la configuración de servidor SMS especificada.

URL: https://:/xenmobile/api/v1/notificationserver/sms/{id}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Agregar configuración de servidor SMTP

Con esta opción, se agrega una configuración de servidor SMTP.

URL: https://:/xenmobile/api/v1/notificationserver/smtp

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Modificar configuración de SMTP

Con esta opción, se modifica la configuración de servidor SMTP especificada.

URL: https://:/xenmobile/api/v1/notificationserver/smtp/{id}

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Eliminar configuración de servidor

Con esta opción, se elimina la configuración de servidor SMS o SMTP especificada.

URL: https://:/xenmobile/api/v1/notificationserver/{id}

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Establecer la configuración predeterminada de SMS

Con esta opción, se establece la configuración de servidor SMS especificada como el valor predeterminado.

URL: https://:/xenmobile/api/v1/notificationserver/activate/sms/{id}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Establecer la configuración predeterminada de SMTP

Con esta opción, se establece la configuración de servidor SMTP especificada como el valor predeterminado.

URL: https://:/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Cómo administrar grupos y usuarios locales

Puede administrar grupos y usuarios locales con la ayuda de los siguientes servicios.

Obtener todos los usuarios

Con esta opción, se obtienen todos los usuarios locales.

URL: https://:/xenmobile/api/v1/localusersgroups

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```



```
    ]

}
```

Obtener un usuario

Con esta opción, se obtiene el usuario local especificado.

URL: https://:/xenmobile/api/v1/localusersgroups/{name}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```

```
            company": "Example
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

Agregar usuario

Con esta opción, se agrega un usuario con los atributos especificados.

URL: https://:/xenmobile/api/v1/localusersgroups

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Actualizar usuario

Con esta opción, se actualizan los atributos de usuario.

URL: https://:/xenmobile/api/v1/localusersgroups

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "attributes": {

          "badpwdcount": "4",

          "asuseremail": "justa.name@example.com",

          "company": "example",

          "mobile": "4695557854"

          },

    "groups": [

          "MSP"

          ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

Cambiar contraseña de usuario

Con esta opción, puede restablecer la contraseña de un usuario. También puede cambiar la contraseña de un usuario en la llamada a la actualización de usuario local.

URL: https://:/xenmobile/api/v1/localusersgroups/resetpassword

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Ejemplo de respuesta COPIAR

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Eliminar usuarios

Con esta opción, se eliminan los usuarios especificados.

URL: https://:/xenmobile/api/v1/localusersgroups/resetpassword

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{ justaname XX }
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Eliminar un usuario

Con esta opción, se elimina el usuario especificado.

URL: https://:/xenmobile/api/v1/localusersgroups/

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Importar archivo de aprovisionamiento

Con esta opción, se carga un archivo que contiene los datos de usuario local. El archivo a cargar debe estar en formato CSV. Para obtener más información acerca de los archivos de aprovisionamiento, consulte Formatos de archivo de aprovisionamiento.

URL: https://:/xenmobile/api/v1/localusersgroups/importprovisioningfile

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Ejemplo de respuesta COPIAR

```
{

   "status": 0,

   "message": "Success",

   "user": null

}
```

Cómo administrar aplicaciones

Puede administrar aplicaciones con la ayuda de los siguientes servicios.

Obtener todas las aplicaciones mediante filtrado

Con esta opción, se obtienen las aplicaciones basadas en parámetros especificados de filtrado.

URL: https://:/xenmobile/api/v1/application/filter

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.
Tipo de contenido: application/json

Ejemplo de datos de solicitud COPIAR

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.d
}
```

Ejemplo de datos de respuesta COPIAR


```
{
  "status": 0,
  "message": "Success",
  "applicationListData": {
    "totalMatchCount": 2,
    "totalCount": 2,
    "appList": [{
      "id": 2,
      "name": "WorxNotes",
      "description": "Worx Notes Application",
      "createdOn": "6/7/16 3:55 PM",
      "lastUpdated": "6/7/16 5:11 PM",
      "disabled": false,
      "nbSuccess": 0,
      "nbFailure": 0,
      "nbPending": 0,
      "schedule": null,
      "permitAsRequired": true,
      "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",
```



```
    "appType": "MDX",
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
```



```
        "categories": ["Default"],
        "roles": null,
        "workflow": null,
        "vppAccount": null
      }]
  }
}
```

Obtener aplicaciones para móvil mediante contenedor

Con esta opción, se obtienen las aplicaciones para móvil que haya en el contenedor especificado.

URL: https://:/xenmobile/api/v1/application/mobile/{containerId}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
```

```
"description": "",
"createdOn": null,
"lastUpdated": null,
"disabled": false,
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"schedule": {
    "enableDeployment": true,
    "deploySchedule": "NOW",
    "deployScheduleCondition": "EVERYTIME",
    "deployDate": null,
    "deployTime": null,
    "deployInBackground": false
},
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
```



```
"roles": [],

"workflow": null,

"ios": {

    "displayName": "GoToMeeting",

    "description": "G2MW_IOS_5.3.3_075_01",

    "paid": false,

    "removeWithMdm": true,

    "preventBackup": true,

    "appVersion": "5.3.3.075",

    "minOsVersion": "",

    "maxOsVersion": "",

    "excludedDevices": "",

    "avppParams": null,

    "avppTokenParams": null,

    "rules": null,

    "appType": "mobile_ios",

    "uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",

   "id": 0,

    "store": {

        "rating": {
```



```
        "rating": {
            "rating": 0,
            "reviewerCount": 0
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
```



```
            "explanation": null

        },

        {

            "policyName": "BlockJailbrokenDevices",

            "policyValue": "true",

            "policyType": "boolean",

            "policyCategory": "Device Security",

            "title": "Block jailbroken or rooted",

            "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",

            "units": null,

            "explanation": null

        },

        {

            "policyName": "CertificateLabel",

            "policyValue": "",

            "policyType": "string",

            "policyCategory": "Network Access",

            "title": "Certificate label",

            "description": "\nThe label for the certificate.\n                                                    Default value is er

            "units": null,
```



```
                    "explanation": null

                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```


Obtener aplicaciones de almacén público mediante contenedor

Con esta opción, se obtienen las aplicaciones de almacén público que contenga el contenedor especificado.

URL: https://:/xenmobile/api/v1/application/mobile/appstore/{containerId}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Eliminar contenedor de aplicaciones

Con esta opción, se elimina el contenedor de aplicaciones especificado.

URL: https://:/xenmobile/api/v1/application/{containerId}

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Cómo administrar configuraciones de grupos de entrega

Puede administrar configuraciones de grupos de entrega con la ayuda de los siguientes servicios.

Obtener grupos de entrega mediante el filtro

Con esta opción, se utilizan los parámetros especificados de filtrado para obtener grupos de entrega.

URL: https://:/xenmobile/api/v1/deliverygroups/filter

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{

  "start": 1,

  "sortOrder": "DESC",

  "deliveryGroupSortColumn": "id",

  “limit”:10,

  "search": "add"

}
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,
```

```
"message": "Success",

"dgListData": {

    "totalMatchCount": 7,

    "totalCount": 10,

    "dgList": [

        {

            "id": null,

            "name": "add delivery group 6.0",

            "description": "testing add delivery group 6.0",

        "groups": [[{

                {

                    "id": 1null,

            "userListId": 1null,

            "name": "MSPTESTLOCALGROUP",

            "uniqueName": "MSPTESTLOCALGROUP",

            "uniqueId": "MSPTESTLOCALGROUP",

            "domainName": "local",

            "primaryToken": 0null,

                }"objectSid": null

            ],},
```



```
        {

            "id": null,

            "userListId": null,

            "name": "AC08EP61S75",

            "uniqueName": "AC08EP61S75",

            "uniqueId": "AC08EP61S75",

            "domainName": "local",

            "primaryToken": null,

            "objectSid": null

        }],

        "users": [{

            "uniqueName": null,

            "domainName": "local",

            "name": null,

            "objectId": "shankar",

            "customProperties": {

                "name": "value",

                "name1": "value1"

            },
```

```
            "uniqueId": "shankar"

        }],

            "zoneId": null,

            "zoneDomain": null,

            "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

            "disabled": false,

            "lastUpdated": 1427144713353,

            "anonymousUser": true,

            "roledefLangVersionId": 1,

            "applications": [

                {

                    "name": "Web Link",

                    "required": false

                },

                {

                    "name": "GoogleApps_SAML",

                    "required": true

                }

            ],

            "devicePolicies": [
```



```
                "test terms conditions"

            ],

            "smartActions": [

                "shankar ganesh"

            ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0

        },

        {

            "id": null,

            "name": "add delivery group 5.0",

            "description": "testing add delivery group 5.0",

            "groups": [

                {

                    "id": 1,

                    "userListId": 1,

                    "name": "MSP",

                    "uniqueName": "MSP",

                    "uniqueId": "MSP",
```



```
            "domainName": "local",
            "primaryToken": 0
        }
    ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId
    "disabled": false,
    "lastUpdated": 1426891345698,
    "anonymousUser": true,
    "roledefLangVersionId": 1,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "Web Link",
            "required": false
        }
```



```
                    ],

                    "devicePolicies": [

                        "test terms conditions"

                    ],

                    "smartActions": [

                        "shankar ganesh"

                    ],

                    "nbSuccess": 0,

                    "nbFailure": 0,

                    "nbPending": 0

                }

            ]

        }



}
```


Obtener grupos de entrega mediante el nombre

URL: https://:/xenmobile/api/v1/deliverygroups/{name}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
```



```
        },
        {
            "name": "test all",
            "required": false
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
```

```
            "test terms conditions"

        ],

        "smartActions": [

            "justa name"

        ],

        "nbSuccess": 0,

        "nbFailure": 0,

        "nbPending": 0

    }

}
```

Modificar grupo de entrega

URL: https://:/xenmobile/api/v1/deliverygroups

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{

  "name": "temp3",

  "description": "temp3 desc",
```

```
   "applications": [
{
            "name": "TESTAPP",
             "priority": -1,
             "required": false
                    }      ],
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
         }
      ],
    "smartActions": [
        {
           "name":"Smart Action Name 1",
           "priority":-1
         }
      ],
   "groups": [
     {
  "uniqueName": "AC08EP61S75",
       "domainName": "local",
       "name": "AC08EP61S75",
```



```
        "objectSid": "AC08EP61S75",

"uniqueId": "AC08EP61S75",

"customProperties": {

    "gr1": "gr1",

    "gr2": "gr2"

  }

    }

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": " testuser ",

      "objectId": " testuser "

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" te

}
```


Ejemplo de respuesta COPIAR


```
{
        "status": 0,
        "message": "Success",
"role": {
            "id": null,
            "name": "temp4",
            "description": "temp4 desc",
            "zoneId": null,
            "zoneDomain": null,
            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
            "disabled": false,
            "lastUpdated": null,
            "anonymousUser": false,
            "roledefLangVersionId": null,
            "applications": [
                {
                "name": "TESTAPP2",
```



```
                "priority": -1,

                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [
```



```
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                  "uniqueName": "AC08EP61S75",
                 "domainName": "local",
                "name": "AC08EP61S75",
                 "objectSid": "AC08EP61S75",
                "uniqueId": "AC08EP61S75",
                "customProperties": {
                  "gr1": "gr1",
```



```
                "gr2": "gr2"

            }

        }],

        "users": [{

            "uniqueName": " tempuser ",

            "domainName": "local",

            "name": " tempuser ",

            "objectId": " tempuser ",

            "customProperties": null,

            "uniqueId": " tempuser "

        }]


    }
```

Agregar grupo de entrega

Con esta opción, se agrega un grupo de entrega.

URL: https://:/xenmobile/api/v1/deliverygroups

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{

   "name": "temp3",

   "description": "temp3 desc",

   "applications": [

{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

   "groups": [

     {
```

```
{
  "uniqueName": "AC08EP61S75",
        "domainName": "local",
        "name": "AC08EP61S75",
        "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
    "gr1": "gr1",
    "gr2": "gr2"
  }}
  ],
  "users": [
    {
      "uniqueName": "testuser",
      "domainName": "local",
      "name": " testuser ",
      "objectId": " testuser "
    }
  ],
  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" te
```



```
}
```

Ejemplo de respuesta COPIAR


```
{
    "status": 0,
    "message": "Success",
"role": {
        "id": null,
        "name": "temp4",
        "description": "temp4 desc",
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": null,
        "applications": [
            {
                "name": "TESTAPP2"
```



```
                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],
```



```
            "smartActions": [
{
                    "name": "TestAction2",
                    "priority": -1
            },
{
                    "name": "TestAction3",
                    "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                    "uniqueName": "AC08EP61S75",
          "domainName": "local",
          "name": "AC08EP61S75",
          "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
```



```
    "gr1": "gr1",

    "gr2": "gr2"

}       }],

        "users": [{

            "uniqueName": " tempuser ",

            "domainName": "local",

            "name": " tempuser ",

            "objectId": " tempuser ",

            "customProperties": null,

            "uniqueId": " tempuser "

        }]


  }
```

Eliminar grupo de entrega

Con esta opción, se eliminan los grupos de entrega especificados.

URL: https://:/xenmobile/api/v1/deliverygroups

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
[ "add delivery group 11.0" ]
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "roleNames": [

        "add delivery group 11.0"

    ]

}
```

Habilitar o inhabilitar grupo de entrega

Habilite o inhabilite los grupos de entrega especificados.

URL: https://:/xenmobile/api/v1/deliverygroups/{delivery group name}/{enable/disable}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "roleName": "AllUsers"

}
```

Cómo administrar propiedades de servidor

Puede administrar las propiedades del servidor XenMobile con la ayuda de los siguientes servicios.

Obtener todas las propiedades de servidor

Con esta opción, se obtienen todas las propiedades actuales del servidor XenMobile.

URL: https://:/xenmobile/api/v1/serverproperties

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 1,

            "name": "ios.mdm.pki.ca-root.certificatefile",
```

```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",

        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,
```



```
            "markDeleted": false

        },

        {

            "id": 3,

            "name": "ios.mdm.enrolment.checkRemoteAddress",

            "value": "false",

            "displayName": "iOS Device Management Enrollment - Check Remote Address",

            "description": "",

            "defaultValue": "false",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": false,

            "markDeleted": false

        },

    ]

}
```


Obtener propiedades de servidor mediante filtro

Con esta opción, se obtienen las propiedades del servidor mediante parámetros especificados de filtrado.

URL: https://:/xenmobile/api/v1/serverproperties/filter

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
```

```
            "value": "justaserver1",

            "displayName": "justarserver display name",

            "description": "justaserver description",

            "defaultValue": "justaserver1",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": true,

            "markDeleted": false

        }

    ]

}
```

Agregar propiedad de servidor

Con esta opción, se agrega la propiedad de servidor especificada.

URL: https://:/xenmobile/api/v1/serverproperties

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

Modificar propiedades de servidor

Con esta opción, se modifica la propiedad de servidor especificada.

URL: https://:/xenmobile/api/v1/serverproperties

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Restablecer propiedades de servidor

Con esta opción, se restablecen las propiedades de servidor especificadas.

URL: https://:/xenmobile/api/v1/serverproperties/reset

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{

    "names": [,

        "justaname7"

        ]

}
```

Ejemplo de respuesta COPIAR

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Eliminar propiedades de servidor

URL: https://:/xenmobile/api/v1/serverproperties

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Parámetros de solicitud COPIAR

```
{
    "justaname3",
    "justaname4"
}
```

Ejemplo de respuesta COPIAR

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Para administrar dispositivos

En XenMobile, puede administrar dispositivos con la ayuda de los siguientes servicios.

Obtener dispositivos mediante filtro

URL: https://:/xenmobile/api/v1/device/filter

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Todos los parámetros de solicitud, **Request Parameters**, son opcionales.

Los valores válidos de **sortOrder** son: ASC, DSC y DESC.

Los valores válidos de **sortColumn** son: ID, SERIAL, IMEI, ACTIVESYNCID, WIFIMAC, BLUETOOTHMAC, OSFAMILY, SYSTEM_OEM, SYSTEM_PLATFORM, SYSTEM_OS_VERSION, DEVICE_PROPERTY, LASTAUTHDATE, INACTIVITYDAYS, ISACTIVE, LASTUSER, BLCOMPLIANT, WLCOMPLIANT, RLCOMPLIANT, MANAGED, SHAREABLE y BULKPROFILESTATUS.

Parámetros de solicitud COPIAR

```
{
   "start": "0-999",
   "limit": "0-999",
   "sortOrder": "ASC",
   "sortColumn": "ID",
   "search": "Any search term",
   "enableCount": "false",
   "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iO
   "filterIds": "['group#/group/MSP@_fn_@normal']"
}
```

Ejemplo de respuesta COPIAR

```
{
   "id": "1-9999999",
```

```
"jailBroken": "true/false",

"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",
```



```
    "inactivityDays": "Number of days device has been inactive",

    "shareable": "Flag indicating if the device is shareable",

    "sharedStatus": "Get shareable status of the device",

    "depRegistered": "Flag indicating if the device is DEP registered",

    "deviceName": "Name of the device",

    "deviceType": "Phone/Tablet",

    "productName": "Product name",

    "platform": "Platform of the device"

}
```

Obtener dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "device": {

  "htcMdm": true,
```

```
"managedByZMSP": true,

"serialNumber": "string",

"id": 0,

"applications": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",

  "lastUpdate": 0,

  "status": "SUCCESS",

  "name": "string"

 }

],

"smartActions": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",
```



```
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
   }
  ],
  "platform": "string",
  "osFamily": "WINDOWS",
  "nbSuccess": 0,
  "nbFailure": 0,
  "nbPending": 0,
  "deliveryGroups": [
   {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
   }
  ],
  "lastAuthDate": 0,
```



```
"sharedStatus": "INACTIVE",

"managed": true,

"smgStatus": "ACCESS_ALLOWED",

"mdmKnown": true,

"mamKnown": true,

"mamRegistered": true,

"lastUsername": "string",

"imei": "string",

"activesyncid": "string",

"wifimac": "string",

"bluetoothmac": "string",

"inactivityDays": 0,

"shareable": true,

"bulkProfileStatus": "NO_BULK",

"deviceType": "string",

"softwareInventory": [

 {

   "version": "string",

   "blacklistCompliant": true,

   "suggestedListCompliant": true,
```



```
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"deviceActions": [
  {
    "actionType": "WIPE",
    "failedTime": 0,
    "doneTime": 0,
    "askedTime": 0
  }
],
"managedSoftwareInventory": [
  {
    "version": "string"
```



```
    "blacklistCompliant": true,
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"policies": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
```



```
    "name": "string"
   }
  ],
  "active": true,
  "xmlId": "string",
  "deviceUsers": [
   {
    "user": {
     "displayName": "string",
     "id": 0,
     "xmlId": "string",
     "properties": [
      {
       "displayName": "string",
       "id": 0,
       "b64": true,
       "group": "string",
       "name": "string",
       "value": "string"
      }
```



```
      ]

    },

    "lastAuthDate": 0,

    "prevAuthDate": 0,

    "userLogin": "string"

  }

],

"packageStates": [

  {

    "packageName": "string",

    "packageId": 0,

    "statusLabel": "string",

    "date": 0,

    "status": "PENDING"

  }

],

"pushState": "ENQUEUED",

"pushStateLabel": "string",

"lastPushDate": 0,

"lastSentNotification": 0,
```



```
"lastRepliedNotification": 0,

"strongId": "string",

"lastSoftwareInventoryTime": 0,

"firstConnectionDate": 0,

"lastIOSProfileInventoryTime": 0,

"lastUser": {

 "displayName": "string",

 "id": 0,

 "xmlId": "string",

 "properties": [

  {

   "displayName": "string",

   "id": 0,

   "b64": true,

   "group": "string",

   "name": "string",

   "value": "string"

  }

 ]

},
```



```
"blacklistCompliant": true,

"suggestedListCompliant": true,

"requiredListCompliant": true,

"devicePropertiesTimestamp": 0,

"revoked": true,

"mamDeviceId": "string",

"deviceToken": "string",

"typeInst": 0,

"appLock": true,

"appWipe": true,

"mamReady": true,

"validCertificates": [

 {

   "credentialProviderId": "string",

   "type": "string",

   "issuerName": "string",

   "startDate": 0,

   "endDate": 0,

   "revoked": true,

   "certificateNumber": "string"
```



```
    "certificateNumber": "string"
  }
 ],
 "revokedCertificates": [
  {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
    "certificateNumber": "string"
  }
 ],
 "authorizeEnabled": true,
 "revokeEnabled": true,
 "lockEnabled": true,
 "cancelLockEnabled": true,
 "unlockEnabled": true,
 "cancelUnlockEnabled": true,
```



```
"containerLockEnabled": true,

"cancelContainerLockEnabled": true,

"containerUnlockEnabled": true,

"cancelContainerUnlockEnabled": true,

"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,
```



```
"ringEnabled": true,

"cancelRingEnabled": true,

"newPinCode": "string",

"oldPinCode": "string",

"lockMessage": "string",

"resetPinCode": true,

"scanTime": "string",

"screenSharingPwd": "string",

"iosprofileInventory": [

 {

  "iosConfigInventories": [

   {

    "description": "string",

    "type": "string",

    "organization": "string",

    "identifier": "string",

    "name": "string"

   }

  ],

  "description": "string",
```



```
    "organization": "string",
    "managed": true,
    "identifier": "string",
    "receivedDate": 0,
    "encrypted": true,
    "name": "string"
  }
],
"iosprovisioningProfileInventory": [
  {
    "managed": true,
    "uuid": "string",
    "expiryDate": 0,
    "name": "string"
  }
],
"erasedMemoryCard": true,
"gpsCoordinates": [
  {
    "gpsTimestamp": 0
```



```
    }
  ],
  "lastGpsCoordinate": {
    "gpsTimestamp": 0
  },
  "gpsFilterStartDate": 0,
  "gpsFilterEndDate": 0,
  "wipePinCode": "string",
  "lockPhoneNumber": "string",
  "dstDevIdUsed": true,
  "dstValue": "string",
  "smartActionsFailure": true,
  "policiesFailure": true,
  "applicationsFailure": true,
  "touchdownProperties": [
    {
      "category": "string",
      "name": "string",
      "value": "string"
```

```
  }
],
"appUnwipeEnabled": true,
"requestMirroringEnabled": true,
"cancelRequestMirroringEnabled": true,
"stopMirroringEnabled": true,
"cancelStopMirroringEnabled": true,
"knownByZMSP": true,
"wipeDeviceFlag": true,
"lockDeviceFlag": true,
"appWipeEnabled": true,
"appLockEnabled": true,
"appUnlockEnabled": true,
"bulkEnrolled": true,
"nbAvailable": 0,
"hasContainer": true,
"connected": true,
"properties": [
  {
    "displayName": "string",
```

```
      "id": 0,
      "b64": true,
      "group": "string",
      "name": "string",
      "value": "string"
    }
  ]
 }
}
```

Obtener aplicaciones de dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/apps

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "applications": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```

Obtener acciones de dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/actions

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
 "status": 0,
 "message": "string",
 "actions": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


Obtener grupos de entrega de dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/deliverygroups

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
 "status": 0,
 "message": "string",
 "deliveryGroups": [
  {
   "statusLabel": "string",
   "linkey": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


Obtener inventario de software administrado por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/managedswinventory

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Obtener directivas por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/policies

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "policies": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```


Obtener inventario de software por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/{device_id}/softwareinventory

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Obtener coordenadas de GPS por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/locations/{device_id}

Parámetros de consulta:

startDate: la fecha de inicio para el filtro de coordenadas
endDate: la fecha final para el filtro de coordenadas

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceCoordinates": {

  "deviceCoordinateList": {

   "deviceCoordinateList": [

    {

     "gpsTimestamp": 0

    }

   ],

   "startDate": 0,

   "endDate": 0

  }

}
```

Enviar notificación a una lista de dispositivos o usuarios

URL: https://:/xenmobile/api/v1/device/notify

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{
 "smtpFrom": "Test",
 "to": [
  {
   "deviceId": "1",
   "email": "user@test.com",
   "osFamily": "iOS",
   "serialNumber": "F7NLX6WDF196",
   "smsTo": "+123456676",
   "token": {
    "type": "apns",
     "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
   }
  }
 ],
 "smtpSubject": "This is test subject",
 "smtpMessage": "This is test message",
 "smsMessage": "This is test message",
 "agentMessage": "This is test message",
 "sendAsBCC": "true",
```



```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

 "sound": "Casino.wav"

}
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "notificationRequests": {

  "smtpNotifRequestId": 0,

  "smsNotifRequestId": 0,

  "smsGatewayNotifRequestId": 0,

  "apnsAgentNotifRequestId": 0,

  "shtpAgentNotifRequestId": 0

 }

}
```

Autorizar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/authorize

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Aplicar omisión del bloqueo de activación a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/activationLockBypass

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Aplicar bloqueo de aplicaciones a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/appLock

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Aplicar borrado de aplicaciones a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/appWipe

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Aplicar bloqueo de contenedores a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerLock

Parámetros de consulta: newPinCode. Se trata del código PIN del contenedor de Android.

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar bloqueo de contenedores en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerLock/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Aplicar desbloqueo de contenedores a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerUnlock

Parámetros de consulta: newPinCode. Se trata del código PIN del contenedor de Android.

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar desbloqueo de contenedores en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerUnlock/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Restablecer contraseña de contenedor en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerPwdReset

Parámetros de consulta: newPinCode. Se trata del código PIN del contenedor de Android.

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar restablecimiento de contraseña de contenedor en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/containerPwdReset/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Rechazar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/disown

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Localizar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/locate

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar localización de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/locate/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Aplicar seguimiento GPS a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/track

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar seguimiento GPS en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/track/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Bloquear una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/lock

Parámetros de consulta:

newPinCode. El código PIN debe tener entre 4 y 16 caracteres para dispositivos Android y Symbian. Para dispositivos Windows, el código PIN debe tener 4 dígitos

resetPinCode: agregar una solicitud de restablecimiento del PIN a la solicitud de bloqueo. Disponible solo para Windows Phone 8.1
lockMessage: agregar un mensaje a la solicitud de bloqueo. Disponible solo para iOS 7 y versiones posteriores.
phoneNumber: agregar un número de teléfono a la solicitud de bloqueo. Disponible solo para iOS 7 y versiones posteriores.

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar bloqueo de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/lock/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Desbloquear una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/unlock

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar desbloqueo de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/unlock/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Implementar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/refresh

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Solicitar duplicación de AirPlay en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/requestMirroring

Parámetros de consulta:

dstName: nombre de destino, como nombre o como ID de dispositivo
dstDevId: dirección MAC del dispositivo de destino, como nombre o como ID de dispositivo

scanTime: tiempo, en segundos, para el análisis
screenSharingPwd: contraseña para compartir pantalla

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar solicitud de duplicación de AirPlay en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/requestMirroring/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Detener duplicación de AirPlay en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/stopMirroring

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar detención de duplicación de AirPlay en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/stopMirroring/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Borrar todas las restricciones en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/restrictions/clear

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancelar borrado de todas las restricciones en una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/restrictions/clear/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Revocar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/revoke

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Llamar a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/ring

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar la llamada a una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/ring/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Borrar una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/wipe

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar borrado de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/wipe/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Borrar de forma selectiva una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/selwipe

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar borrado selectivo de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/selwipe/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Borrar tarjetas SD de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/sdcardwipe

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancelar borrado de tarjetas SD de una lista de dispositivos

URL: https://:/xenmobile/api/v1/device/sdcardwipe/cancel

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
[1,2]
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Obtener todas las propiedades de dispositivo conocidas

URL: https://:/xenmobile/api/v1/device/knownProperties

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{
 "status": 0,
 "message": "string",
 "knownProperties": {
  "knownProperties": {
   "knownPropertyList": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string",
     "group": "EVERYWAN",
     "groupLabel": "string"
    }
   ]
  }
}
```


Obtener todas las propiedades de dispositivo usadas

URL: https://:/xenmobile/api/v1/device/usedProperties

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{
 "status": 0,
 "message": "string",
 "deviceUsedPropertiesList": {
  "deviceUsedProperties": {
   "deviceUsedPropertiesParameters": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string"
    }
   ]
  }
 }
}
```

Obtener todas las propiedades de dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/properties/{deviceId}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{

 "status": 0,

 "message": "string",

 "devicePropertiesList": {

  "deviceProperties": {

   "startIndex": 0,

   "devicePropertyParameters": [

    {

     "name": "string",

     "value": "string",

     "id": 0,

     "displayName": "string",

     "group": "string",

     "b64": true

    }

   ],
```



```
    "totalCount": 0
  }
 }
}
```

Actualizar todas las propiedades de dispositivos por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/properties/{deviceId}

Tipo de solicitud: PUT

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{
  "properties": [
    {
      "name": "ACTIVE_ITUNES",
      "value": "0"
    }
  ]
}
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string"

}
```

Agregar o actualizar una propiedad de dispositivo por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/properties/{deviceId}

Tipo de solicitud: POST

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de solicitud COPIAR

```
{

 "name": "PROPERTY_NAME",

 "value": "PROPERTY_VALUE"

}
```

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string"

}
```

Eliminar una propiedad de dispositivo por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/properties/{deviceId}

Tipo de solicitud: DELETE

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string"

}
```

Obtener estado de MDM de dispositivos iOS por ID de dispositivo

URL: https://:/xenmobile/api/v1/device/mdmStatus/{deviceId}

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR

```
{

 "status": 0,

 "message": "string",

 "deviceMdmStatus": {

  "deviceMdmStatusParameters": {

     "pushState": "ENQUEUED",

     "lastPushDate": 0,

     "lastRepliedNotification": 0,

     "lastSentNotification": 0,

     "pushStateLabel": "string"

   }

 }

}
```


Generar código PIN

URL: https://:/xenmobile/api/v1/device/pincode/generate

Parámetros de consulta: pinCodeLength. Longitud del código PIN solicitado.

Tipo de solicitud: GET

Encabezado de solicitud: auth_token. Se trata del token de autenticación obtenido cuando el usuario inició sesión.

Tipo de contenido: application/json

Ejemplo de respuesta COPIAR


```
{

 "status": 0,

 "message": "string",

 "pinCode": {

  "answer": "string"

 }

}
```

Interfaces API SOAP de XenMobile

Aug 25, 2016

En XenMobile, se pueden usar las siguientes API de servicios Web SOAP 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

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

revoke

unlockDevice

wipeDevice

	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

XenMobile Mail Manager 10

Oct 31, 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).

Para descargar XenMobile Mail Manager, vaya al apartado Server Components de XenMobile 10 Server en Citrix.com.

Novedades en XenMobile Mail Manager 10.1

Reglas de acceso

La ventana Rule Analysis (análisis de reglas) tiene una casilla de verificación que, al seleccionarla, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.

El acceso predeterminado (Allow, Block y Unchanged) y los modos de comando de ActiveSync (PowerShell o de simulación) se configuran por separado para cada entorno de Microsoft Exchange establecido en la implementación de XenMobile.

Instantáneas

Puede configurar la cantidad máxima de instantáneas visibles en el historial de instantáneas.

Puede configurar qué errores ignorar durante una instantánea principal. Cuando una instantánea principal genera errores no configurados para ignorarse, se descartan los resultados de las instantáneas.

Para establecer que se ignoren dichos errores, modifique el archivo config.xml mediante un editor XML:

- Si el servidor Exchange es Office 365, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares.
- Si el servidor Exchange es local, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares.
- Si hay más de un entorno de Exchange configurado, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID correspondiente al entorno de Exchange deseado']/ExchangeServer/Specialists/PowerShell. Agregue un nodo secundario IgnorableErrors al nodo de PowerShell y uno para cada mensaje de error que deba ignorarse. Agregue un nodo secundario Error al nodo IgnorableErrors con el texto coincidente en una sección CDATA. También puede utilizar expresiones regulares.

Guarde el archivo config.xml y reinicie el servicio XenMobile Mail Manager.

PowerShell y Exchange

Ahora XenMobile Mail Manager determina de forma dinámica qué cmdlets usar en función de la versión de Exchange a la que esté conectado. Por ejemplo, para Exchange 2010, utiliza Get-ActiveSyncDevice, pero, para Exchange 2013 y Exchange 2016, emplea Get-MobileDevice.

Configuración de Exchange

Las configuraciones del servidor Exchange se pueden modificar y actualizar sin tener que reiniciar el servicio XenMobile Mail Manager.

Dos nuevas columnas que se han agregado a la ficha de resumen del entorno de Exchange muestran el modo de comando del entorno (PowerShell o de simulación) y su modo de acceso (Allow, Block o Unchanged).

Solución de problemas y diagnósticos

En la carpeta Support\PowerShell dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Al probar la conectividad con el servicio Exchange mediante el botón Test Connectivity en la ventana Configuration de la consola, se ejecutan todos los cmdlets de solo lectura que emplea el servicio, se ejecutan pruebas de permisos de RBAC en el servidor Exchange para el usuario configurado y se muestran errores y advertencias por colores (azul y amarillo para advertencias, y rojo y naranja para errores).

Una nueva herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y zonas potencialmente problemáticas, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

En casos de asistencia, todas las propiedades de todos los buzones de correo y dispositivos administrados por XenMobile Mail Manager pueden guardarse si se selecciona una casilla de verificación de diagnóstico de la consola.

Ahora, en dichos casos, se respalda el registro por niveles de seguimiento.

Autenticación

XenMobile Mail Manager respalda la autenticación básica en implementaciones locales. Esto permite que XenMobile Mail Manager pueda usarse cuando el servidor de XenMobile Mail Manager no sea miembro del dominio en que reside el servidor Exchange.

Problemas resueltos

Reglas de acceso

XenMobile Mail Manager aplica reglas locales de control de acceso a todos los usuarios de grupos de Active Directory (AD), aunque haya grupos de AD con más de 1000 usuarios. Antes, XenMobile Mail Manager aplicaba reglas locales de control de acceso únicamente a los 1000 primeros usuarios de un grupo de AD. [#548705]

A veces, la consola de XenMobile Mail Manager no ha respondido cuando se consultaban grupos de Active Directory que contuvieran 1000 usuarios o más. [CXM-11729]

La ventana LDAP Configuration ya no muestra modos de autenticación incorrectos. [CXM-5556]

Instantáneas

Los nombres de usuario con apóstrofos ya no provocan errores en las instantáneas secundarias. [#617549]

En los casos de asistencia en que la canalización esté inhabilitada (la opción Disable Pipelining está seleccionada en la ventana Configuration de la consola de XenMobile Mail Manager), las instantáneas principales ya no fallan en implementaciones locales de Exchange. [#586083]

En los casos de asistencia en que la canalización esté inhabilitada (la opción Disable Pipelining está seleccionada en la ventana Configuration de la consola de XenMobile Mail Manager), ya no se reúnen datos de instantáneas completas independientemente de si el entorno se ha configurado para instantáneas completas o superficiales. Ahora los datos de las instantáneas completas se reúnen únicamente cuando el entorno esté configurado para instantáneas completas. [#586092]

En ocasiones, la primera instantánea principal tras la instalación inicial generaba un error que impedía a XenMobile Mail Manager realizar otras instantáneas principales a menos que el servicio XenMobile Mail Manager se reiniciara. Esto ya no se produce. [CXM-5536]

Acerca de XenMobile Mail Manager 10

Acerca de XenMobile Mail Manager 10.1

Oct 31, 2016

Las siguientes características son nuevas en XenMobile Mail Manager 10.1:

Reglas de acceso

La ventana Rule Analysis (análisis de reglas) tiene una casilla de verificación que, al seleccionarla, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.

El acceso predeterminado (Allow, Block y Unchanged) y los modos de comando de ActiveSync (PowerShell o de simulación) se configuran por separado para cada entorno de Microsoft Exchange establecido en la implementación de XenMobile.

Instantáneas

Puede configurar la cantidad máxima de instantáneas visibles en el historial de instantáneas.

Puede configurar qué errores ignorar durante una instantánea principal. Cuando una instantánea principal genera errores no configurados para ignorarse, se descartan los resultados de las instantáneas.

Para establecer que se ignoren dichos errores, modifique el archivo config.xml mediante un editor XML:

- Si el servidor Exchange es Office 365, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares. Vaya al paso 7.
- Si el servidor Exchange es local, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares. Vaya al paso 7.
- Si hay más de un entorno de Exchange configurado, vaya al nodo /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID correspondiente al entorno de Exchange deseado']/ExchangeServer/Specialists/PowerShell. Agregue el nodo secundario IgnorableErrors al nodo PowerShell y, para cada error que quiera ignorar, agregue un nodo secundario Error al nodo IgnorableErrors con el mismo texto que hay en la sección CDATA. También puede utilizar expresiones regulares.

Guarde el archivo config.xml y reinicie el servicio XenMobile Mail Manager.

PowerShell y Exchange

Ahora XenMobile Mail Manager determina de forma dinámica qué cmdlets usar en función de la versión de Exchange a la que esté conectado. Por ejemplo, para Exchange 2010, utiliza **Get-ActiveSyncDevice**, pero, para Exchange 2013 y Exchange 2016, emplea **Get-MobileDevice**.

Configuración de Exchange

Las configuraciones del servidor Exchange se pueden modificar y actualizar sin tener que reiniciar el servicio XenMobile Mail Manager.

Dos nuevas columnas que se han agregado a la ficha de resumen del entorno de Exchange muestran el modo de comando del entorno (PowerShell o de simulación) y su modo de acceso (Allow, Block o Unchanged).

Solución de problemas y diagnósticos

En la carpeta Support\PowerShell dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Al probar la conectividad con el servicio Exchange mediante el botón **Test Connectivity** en la ventana "Configuration" de la consola, se

ejecutan todos los cmdlets **de solo lectura** que emplea el servicio, se ejecutan pruebas de permisos de RBAC en el servidor Exchange para el usuario configurado y se muestran errores y advertencias por colores (azul y amarillo para advertencias, rojo y naranja para errores).

Una nueva herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y zonas potencialmente problemáticas, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

En casos de asistencia, todas las propiedades de todos los buzones de correo y dispositivos administrados por XenMobile Mail Manager pueden guardarse si se selecciona una casilla de verificación de diagnóstico de la consola.

Ahora, en dichos casos, se respalda el registro por niveles de seguimiento.

Autenticación

XenMobile Mail Manager respalda la autenticación básica en implementaciones locales. Esto permite que XenMobile Mail Manager pueda usarse cuando el servidor de XenMobile Mail Manager no sea miembro del dominio en que reside el servidor Exchange.

Problemas resueltos

Reglas de acceso

XenMobile Mail Manager aplica reglas locales de control de acceso a todos los usuarios de grupos de Active Directory, aunque haya grupos de AD con más de 1000 usuarios. Antes, XenMobile Mail Manager aplicaba reglas locales de control de acceso únicamente a los 1000 primeros usuarios de un grupo de AD. [#548705]

A veces, la consola de XenMobile Mail Manager no ha respondido cuando se consultaban grupos de Active Directory que contuvieran 1.000 usuarios o más. [CXM-11729]

La ventana LDAP Configuration ya no muestra modos de autenticación incorrectos. [CXM-5556]

Instantáneas

Los nombres de usuario con apóstrofos ya no provocan errores en las instantáneas secundarias. [#617549]

En los casos de asistencia en que la canalización esté inhabilitada (la opción **Disable Pipelining** está seleccionada en la ventana "Configuration" de la consola de XenMobile Mail Manager), las instantáneas principales ya no fallan en implementaciones locales de Exchange. [#586083]

En los casos de asistencia en que la canalización esté inhabilitada (la opción **Disable Pipelining** está seleccionada en la ventana "Configuration" de la consola de XenMobile Mail Manager), ya no se recopilan datos de instantáneas completas, independientemente de si el entorno se ha configurado para instantáneas completas o superficiales. Ahora, los datos de las instantáneas completas se recopilan únicamente cuando el entorno está configurado para instantáneas completas. [#586092]

En ocasiones, la primera instantánea principal tras la instalación inicial generaba un error que impedía a XenMobile Mail Manager realizar otras instantáneas principales a menos que el servicio XenMobile Mail Manager se reiniciara. Esto ya no se produce. [CXM-5536]

Acerca de XenMobile Mail Manager 10

Oct 31, 2016

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 tras iniciar una instantánea principal.
- Es posible que XenMobile Mail Manager aplique reglas locales de control de acceso únicamente a los primeros 1000 usuarios de un grupo de Active Directory aunque el grupo contenga más de 1000 usuarios.

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 indicador 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.

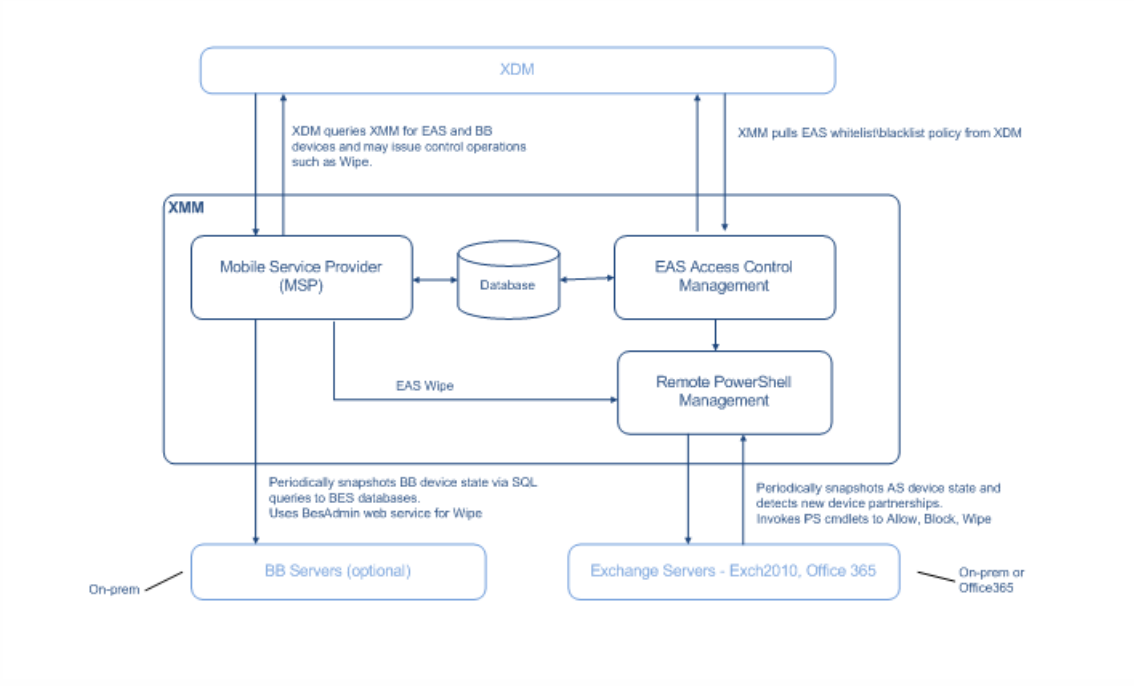
Captura de registros

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 de 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

Oct 31, 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 2016, 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 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

Requisitos previos de XenMobile Mail Manager

- Windows Management Framework debe estar instalado.
  - PowerShell V5, V4 y V3
- 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. 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.

- **Para Exchange Server 2010 SP2:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Para el servidor Exchange Server 2013 y Exchange Server 2016:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- 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 el artículo de Microsoft TechNet about_Remote_Requirements, para establecer una conexión remota y ejecutar comandos remotos, las credenciales deben corresponder a un usuario que sea administrador en la máquina remota. Según esta publicación de blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands (No necesita ser un administrador para ejecutar comandos remotos de PowerShell), 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**. Las credenciales especificadas en la interfaz de usuario de la 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-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 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

Oct 31, 2016

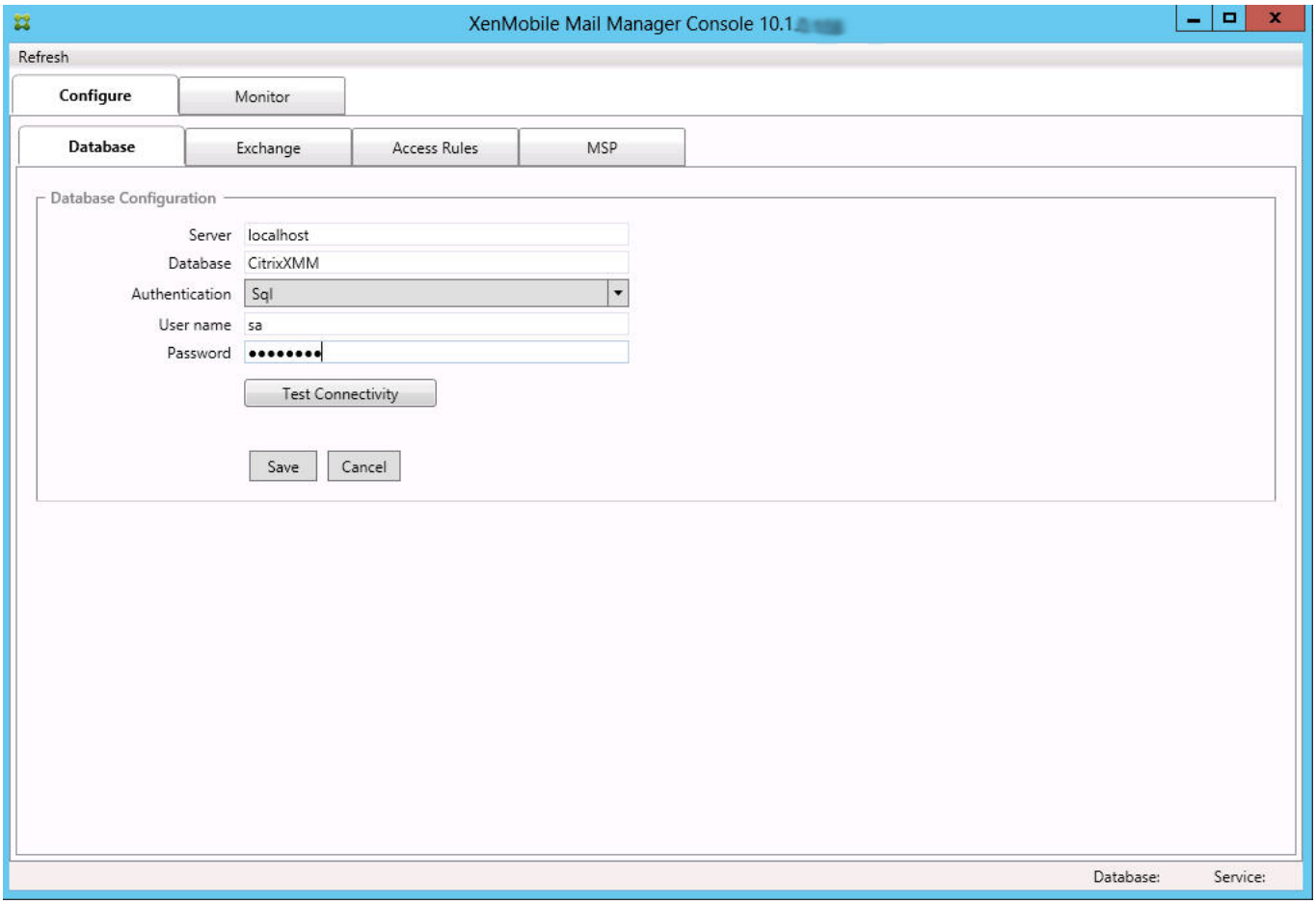
1. Haga clic en el archivo XmmSetup.msi y, a continuación, siga las instrucciones del programa de instalación para instalar XenMobile Mail Manager.

2. Deje **Launch the Configure utility** seleccionado en la última pantalla del asistente de configuración. Si no, en el menú **Inicio**, abra **XenMobile Mail Manager**.

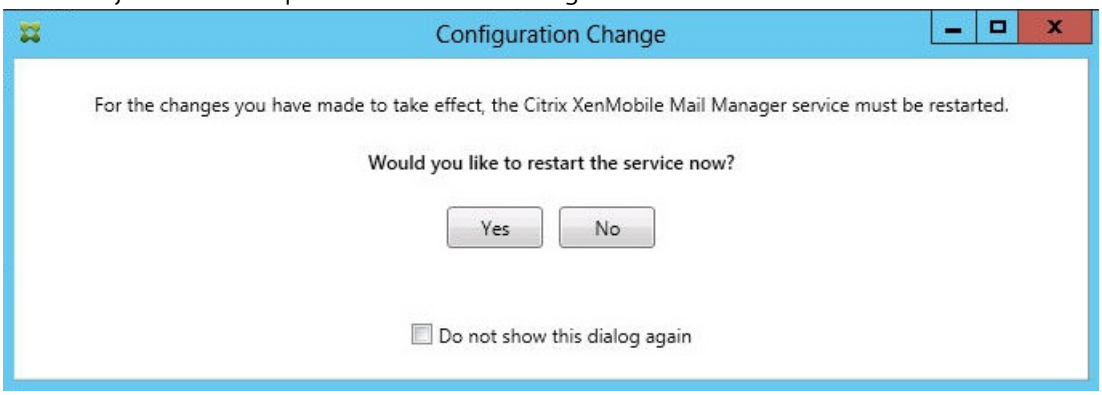
3. Configure las siguientes propiedades de base de datos:
    1. Seleccione la ficha **Configure** > **Database**.
    2. Escriba el nombre del servidor SQL Server (el valor predeterminado es localhost).
    3. Conserve la opción predeterminada de la base de datos, CitrixXmm.
    4. Seleccione uno de 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.

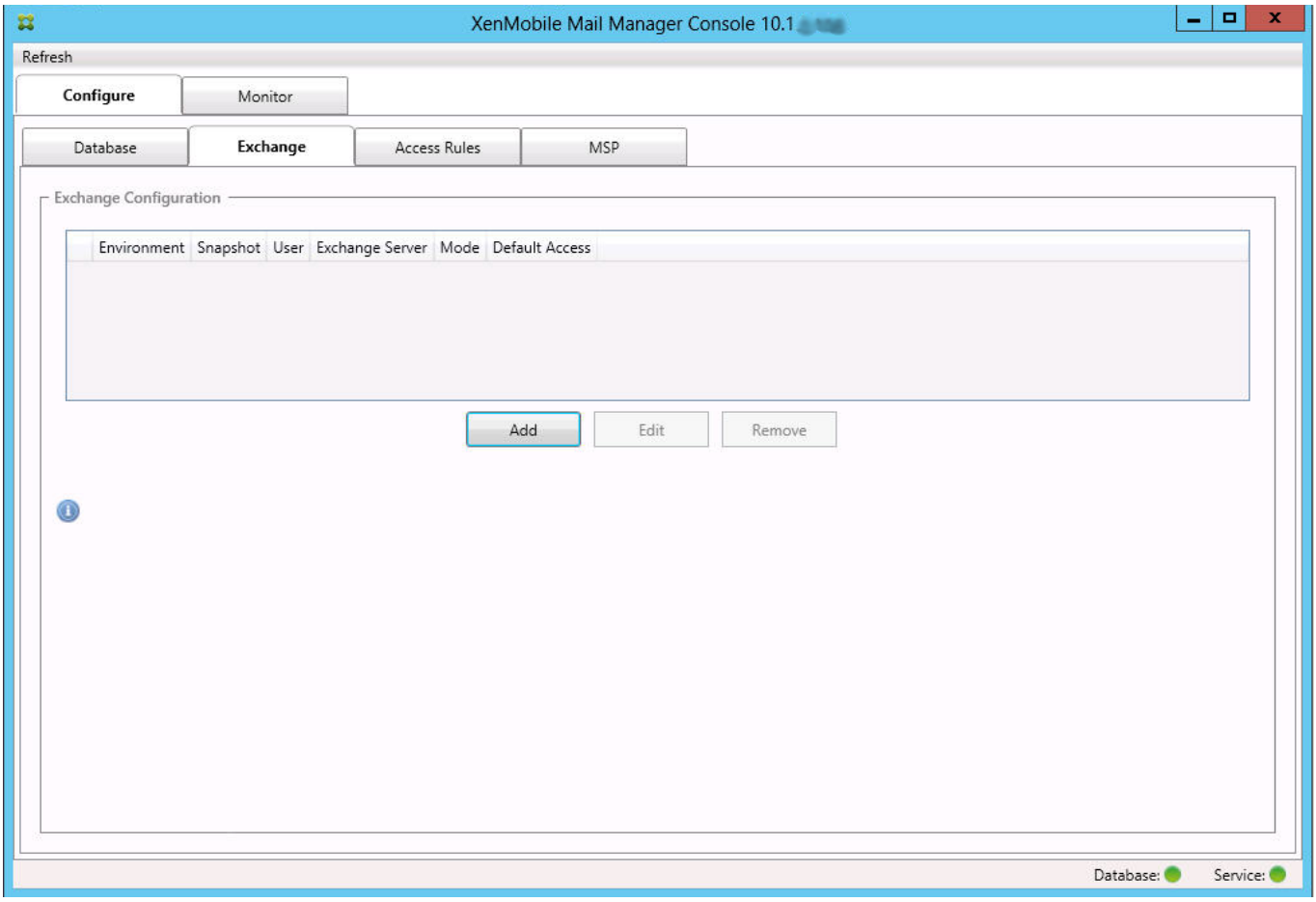
5. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor SQL Server y, a continuación, haga clic en **Save**.



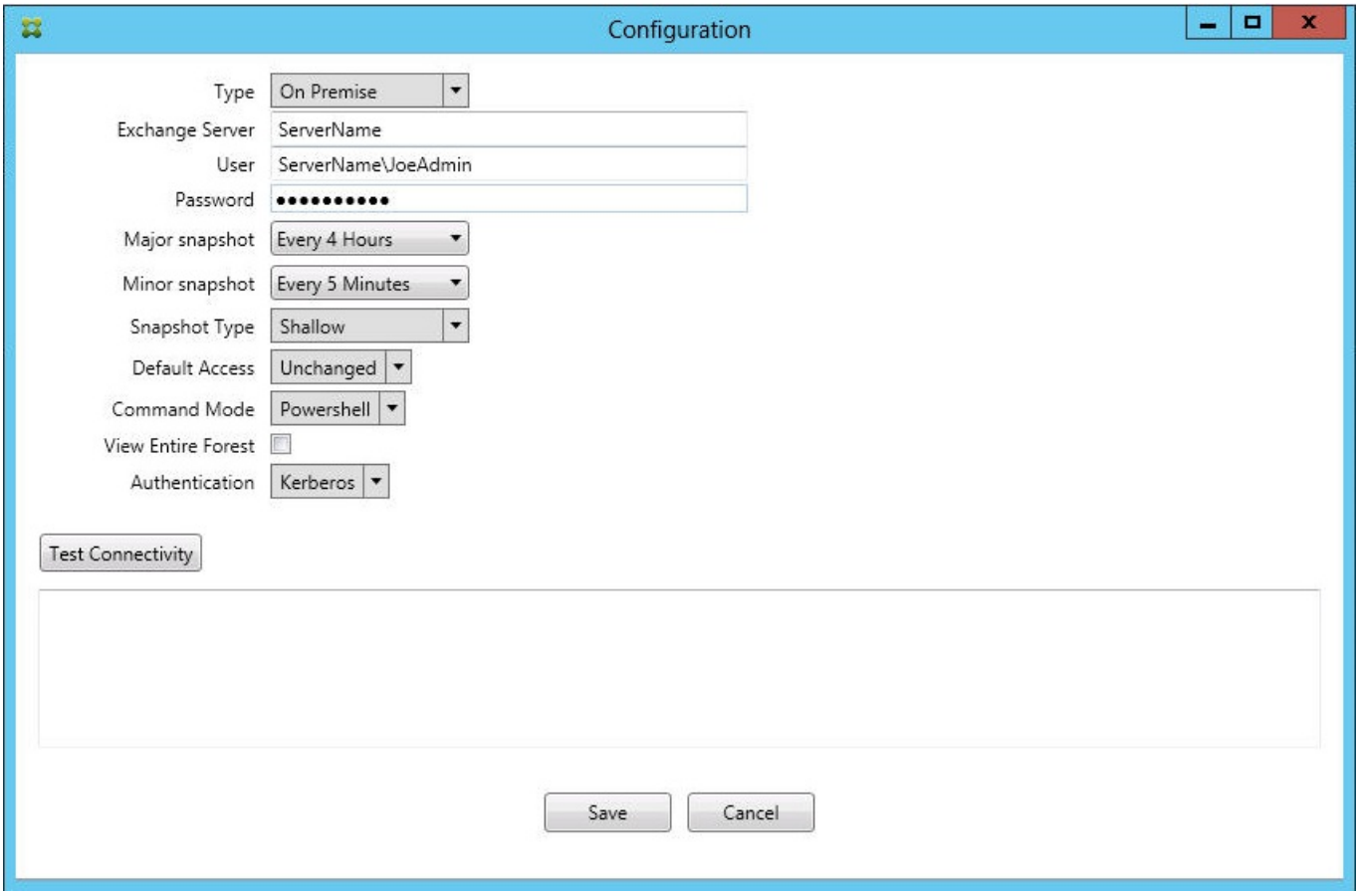
4. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.



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**.



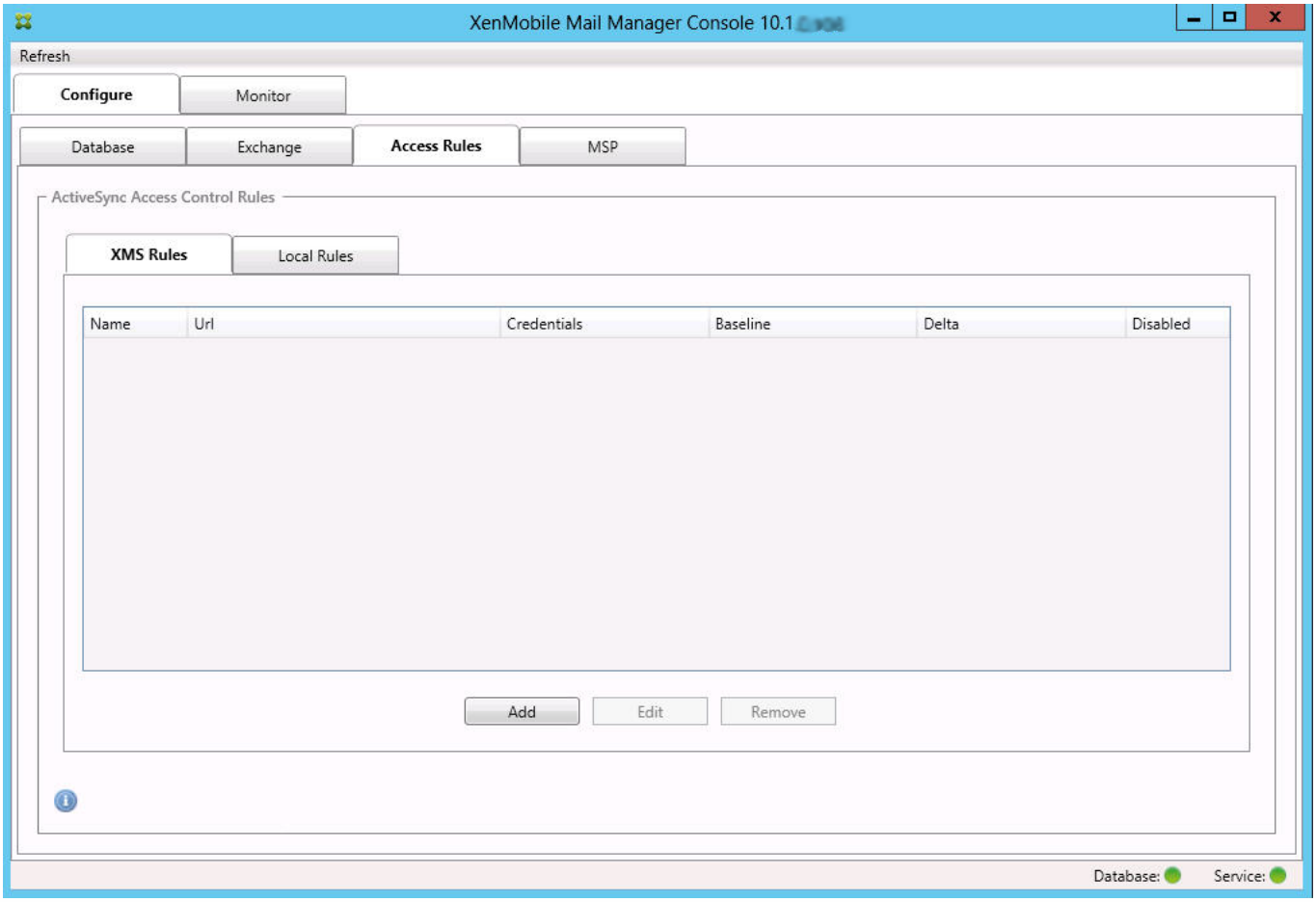
3. Haga clic en **Add**.
4. Seleccione el tipo de entorno del servidor Exchange: **On Premise** u **Office 365**.



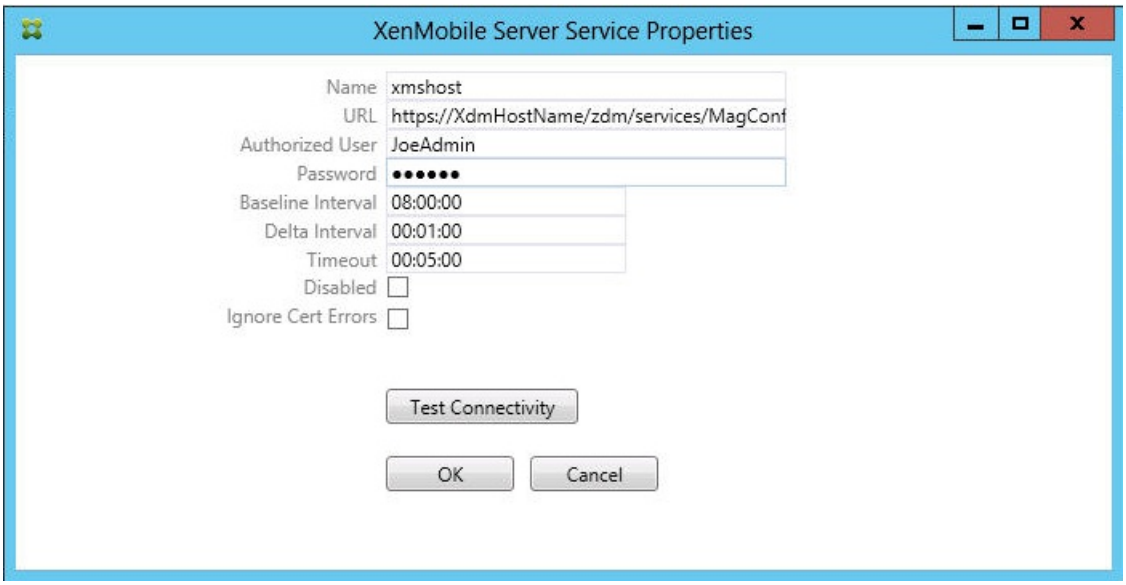
5. Si selecciona **On Premise**, escriba el nombre del servidor Exchange que se usará para los comandos remotos de PowerShell.
6. Escriba el nombre de usuario de una identidad de Windows que tenga los permisos apropiados en el servidor Exchange, como se especifica en el apartado de requisitos.
7. Escriba 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. 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", permitirá el acceso de ActiveSync a dichos dispositivos; si selecciona "Block", denegará el acceso; si selecciona "Unchanged", no se realizará ningún cambio.
12. 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 de simulación, el usuario puede usar la ficha Monitor para ver lo que podría haber ocurrido si se hubiera habilitado el modo de PowerShell.

13. Seleccione **View Entire Forest** para configurar XenMobile Mail Manager y ver todo el bosque de Active Directory en el entorno de Exchange.
14. Seleccione el protocolo de autenticación: **Kerberos** o **Basic**. XenMobile Mail Manager respalda la autenticación básica en implementaciones locales. Esto permite que XenMobile Mail Manager pueda usarse cuando el servidor de XenMobile Mail Manager no sea miembro del dominio en que reside el servidor Exchange.
15. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor Exchange y, a continuación, haga clic en **Save**.
16. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.

6. Configure las reglas de acceso:
    1. Seleccione la ficha **Configure** > **Access Rules**.
    2. Haga clic en la ficha **XDM Rules**.



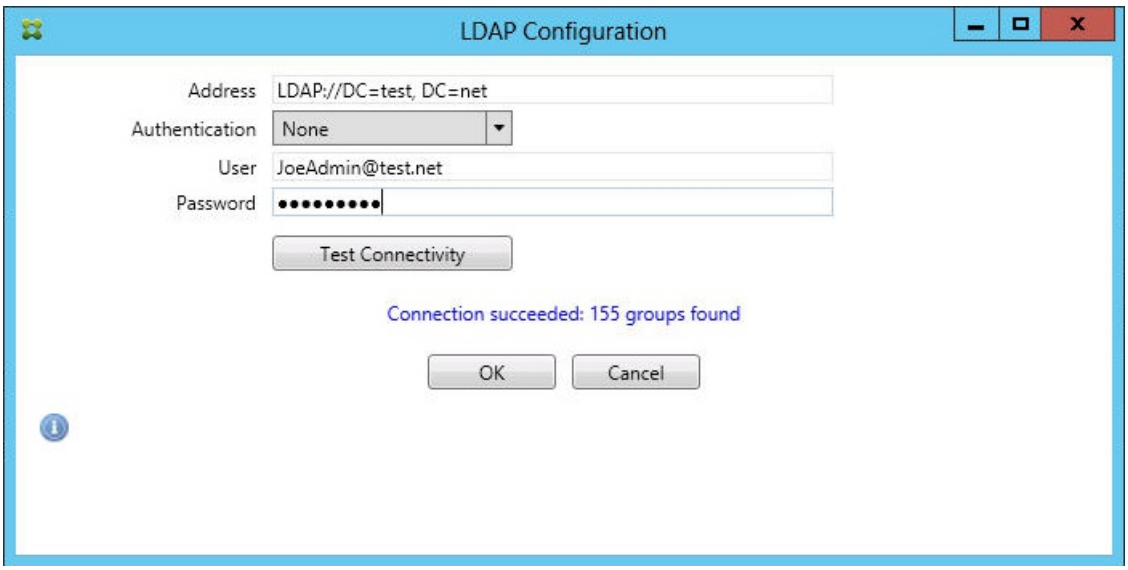
    3. Haga clic en **Add**.



4. Escriba un nombre para las reglas del servidor XenMobile, como XdmHost.
5. 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.

6. Especifique un usuario autorizado en el servidor.
7. Escriba la contraseña del usuario.
8. Conserve los valores predeterminados de **Baseline Interval**, **Delta Interval** y **Timeout values**.
9. 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.
10. Haga clic en **OK**.

7. 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.

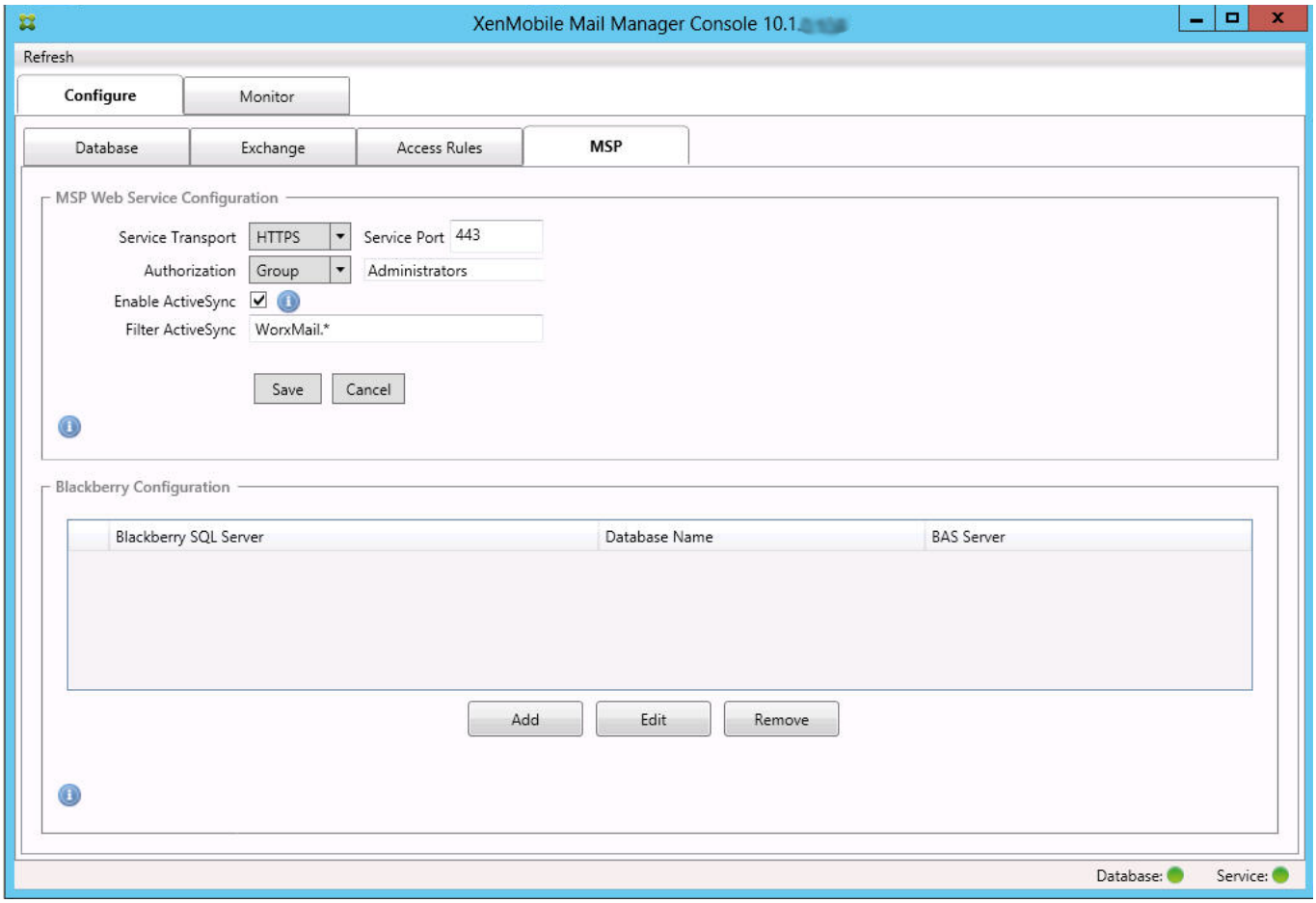


   2. Puede agregar reglas locales en función de: **ActiveSync Device ID** (el ID de dispositivo de ActiveSync), **Device Type** (el tipo de dispositivo), **AD Group** (el grupo de Active Directory), **User** (el usuario) o **UserAgent** (el agente del usuario del dispositivo). En la lista, seleccione el 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**.

8. Configure 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**.

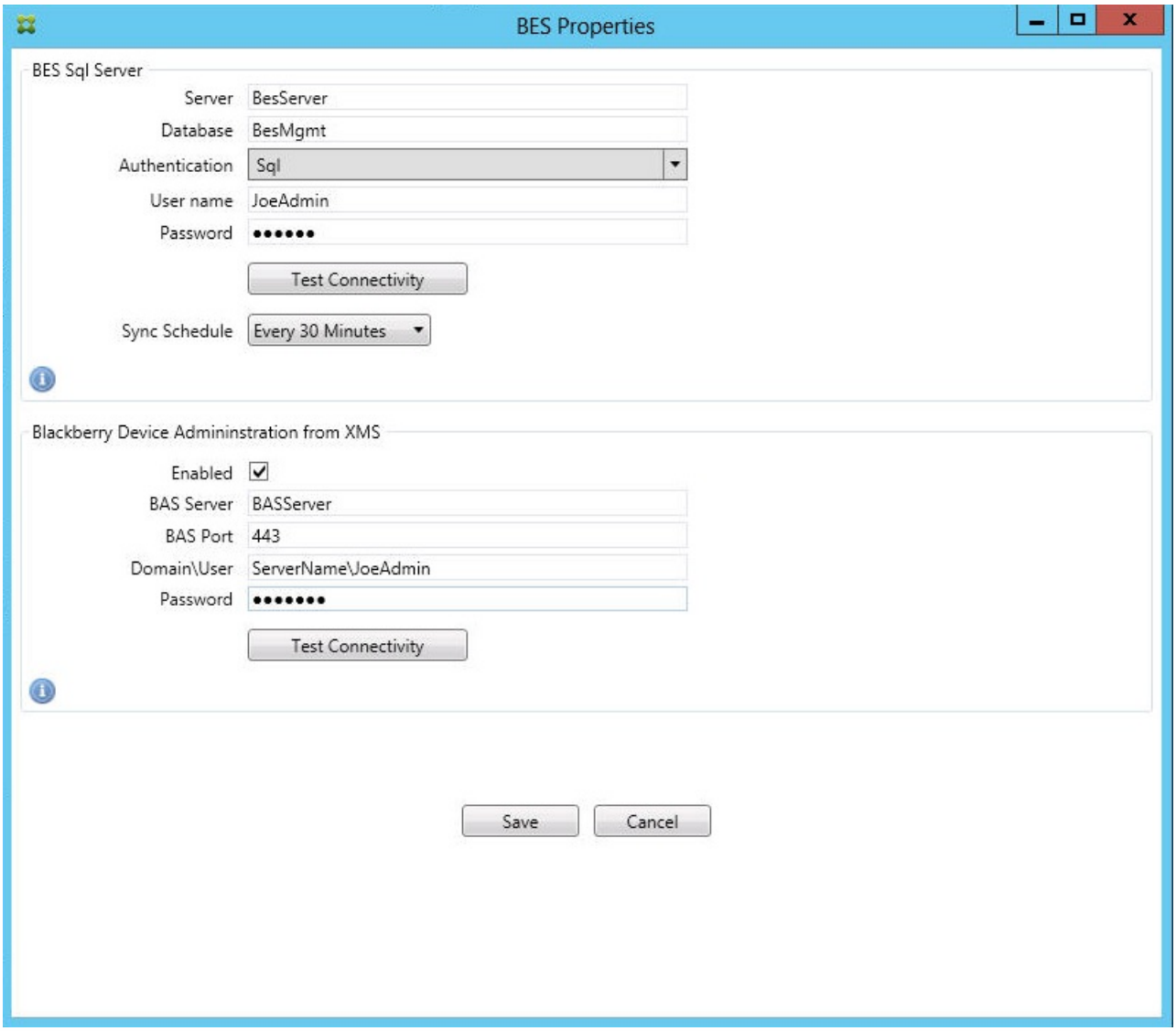


   2. Establezca el tipo de servicio de transporte como **HTTP** o **HTTPS** para el servicio del proveedor de servicios móviles.
   3. Establezca el puerto del servicio (por regla general, 80 y 443) para el servicio del proveedor de servicios móviles.

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**.

9. Si quiere, puede configurar uno o más servidores BlackBerry Enterprise Server (BES):
   1. Haga clic en **Add**.
   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.

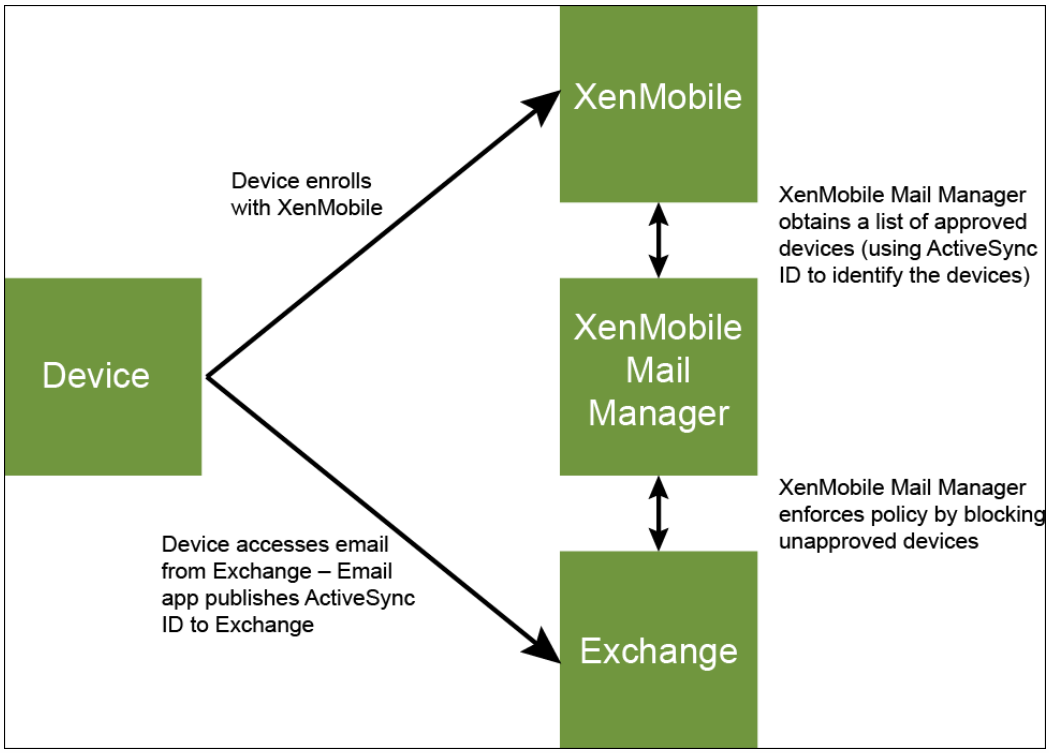
5. Si se selecciona **SQL authentication**, especifique el nombre de usuario y la contraseña.
6. Configure la programación de sincronización en **Sync Schedule**. Esta es la programación usada para conectarse al servidor SQL Server para BES y buscar actualizaciones de dispositivo.
7. Haga clic en **Test 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 **Save**.

Aplicación de directivas de correo electrónico con los ID de ActiveSync

Jul 27, 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

Oct 31, 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 contiene tres tipos de reglas: reglas locales, reglas del servidor XenMobile, (también conocidas como reglas de Device Manager) y la regla del acceso predeterminado.

Reglas locales. 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 del servidor XenMobile ni la regla del acceso predeterminado. Las reglas locales se configuran localmente en XenMobile Mail Manager, desde 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.

Reglas del servidor XenMobile. Las reglas de servidor XenMobile hacen referencia 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.

Regla del acceso predeterminado. 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 local o del servidor XenMobile, el estado del acceso al dispositivo lo determina el estado de la regla del acceso predeterminado.

- Default Access – Allow. Se permitirá el acceso de cualquier dispositivo que no coincida con una regla local o del servidor XenMobile.
- Default Access – Block. Se permitirá el acceso de cualquier dispositivo que no coincida con una regla local o del servidor XenMobile.
- Default Access - Unchanged. XenMobile Mail Manager no modificará el estado de acceso de un dispositivo que no

coincida con una regla local o del servidor XenMobile. 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 del servidor XenMobile

Cuando se encuentra una correspondencia, el cotejo se detiene. Por ejemplo: si una regla local coincide con un dispositivo determinado, este no se cotejará con ninguna regla del servidor XenMobile 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 de un dispositivo concreto, el cotejo se detiene tan pronto como se encuentre la primera correspondencia.

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 el 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

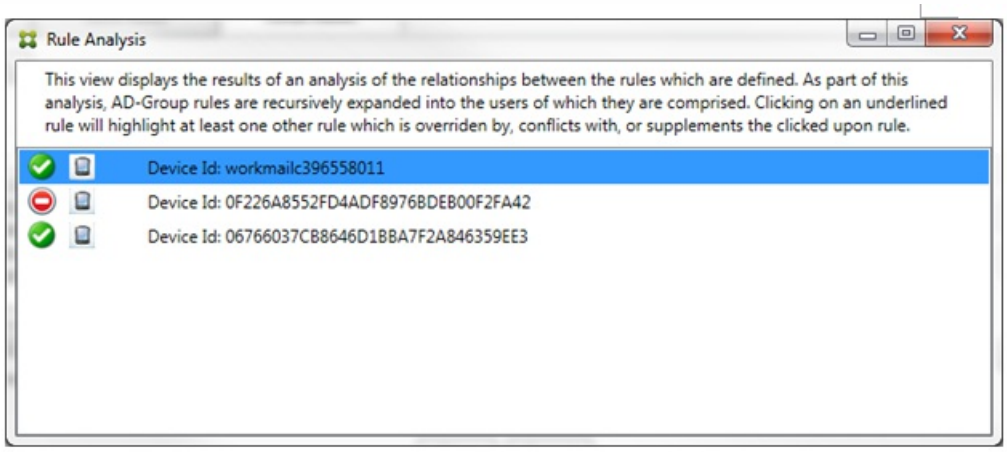
apuntan hacia arriba o hacia abajo. Si una flecha apunta arriba, indica que hay reglas auxiliares que preceden la regla primaria. Si una flecha apunta abajo, indica que hay reglas auxiliares que siguen a la regla primaria. Solo una regla primaria puede estar activa en un momento dado.

- **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.

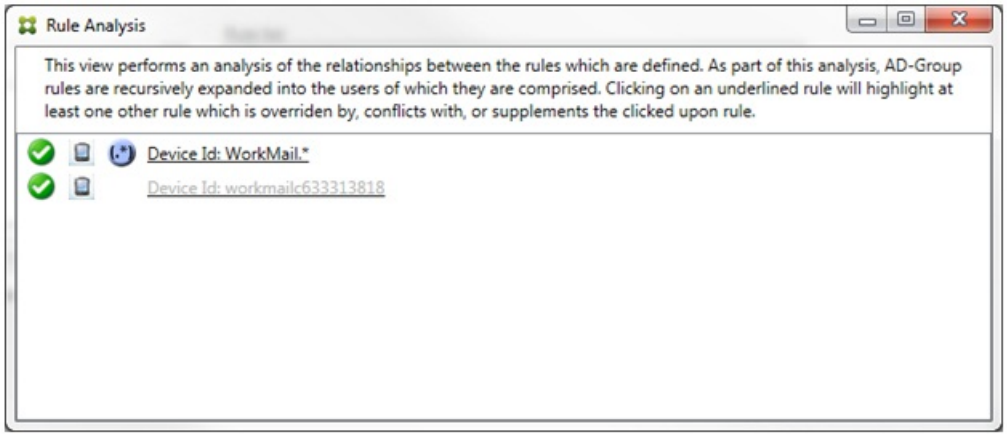
Aspecto de los tipos de reglas en el cuadro del análisis de reglas

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.

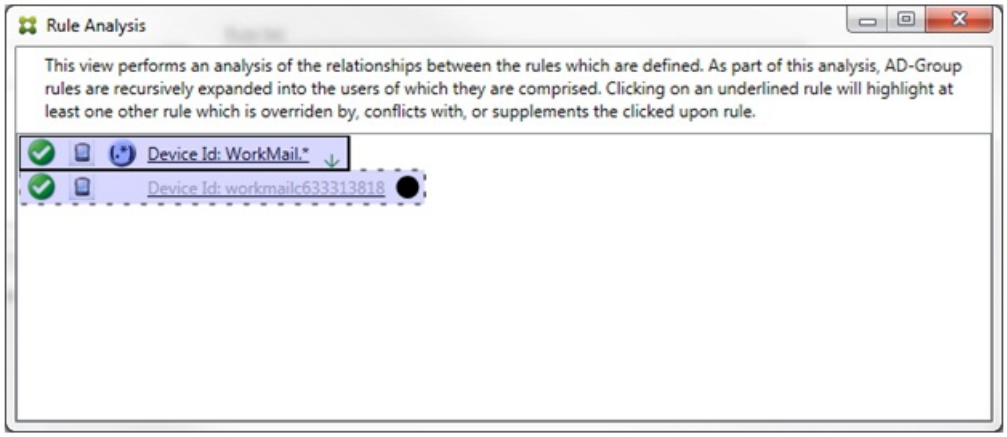
La ventana Rule Analysis (análisis de reglas) tiene una casilla de verificación que, al seleccionarla, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.



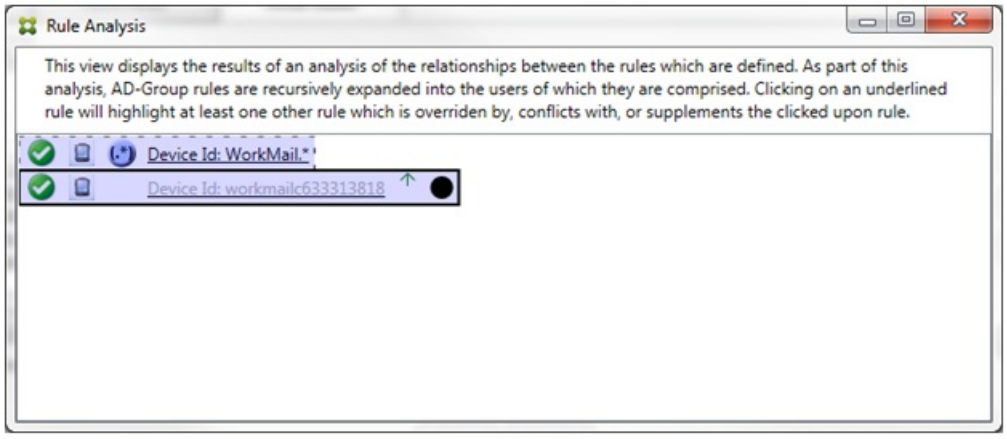
Cuando se produzca una invalidación, se subrayarán al menos dos reglas: la primaria y la(s) auxiliar(es). Al menos una regla auxiliar aparecerá con una fuente más atenuada para indicar que se ha reemplazado por otra regla de mayor prioridad. Puede hacer clic en la regla invalidada para averiguar qué 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:

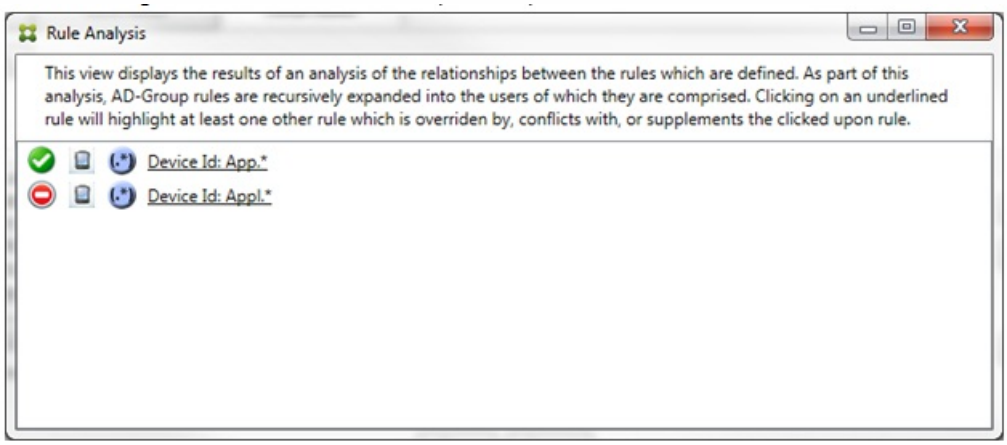


En este ejemplo, la regla de expresión regular WorkMail.* es la regla primaria (indicada con el borde sólido) y la regla normal workmailc633313818 es una regla auxiliar (indicada con el borde discontinuo). El punto negro junto a la regla auxiliar es una indicación visual de que la regla está inactiva (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:

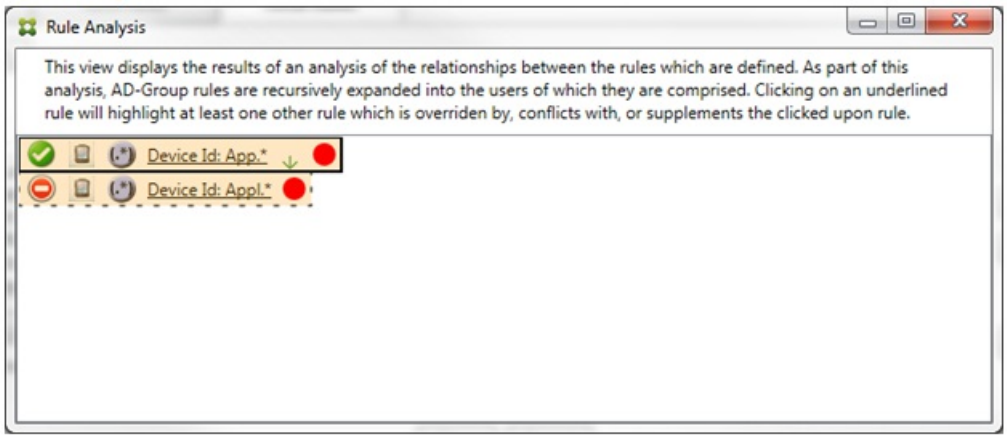


En el ejemplo anterior, la regla de expresión regular WorkMail.* es la regla auxiliar (indicada con el borde discontinuo) y la regla normal workmailc633313818 es la regla primaria (indicada con el borde sólido). En este sencillo ejemplo, no hay mucha diferencia. Para un ejemplo más complejo, consulte 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:

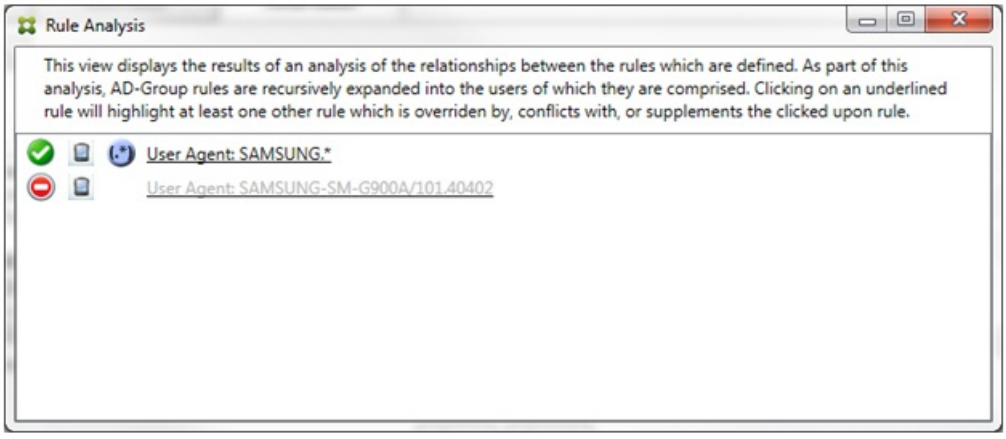


Tras examinar las dos reglas de expresiones regulares, es evidente que la primera regla permite el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "App" y la segunda regla niega el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "Appl". Además, aunque 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:



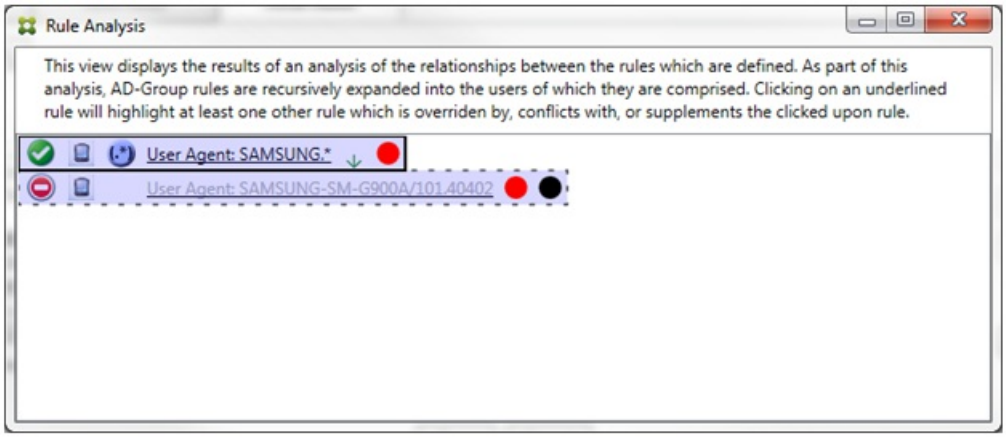
En este caso, tanto la regla primaria (la regla de expresión regular App.*) como la regla auxiliar (la regla de expresión regular Appl.*) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo 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.



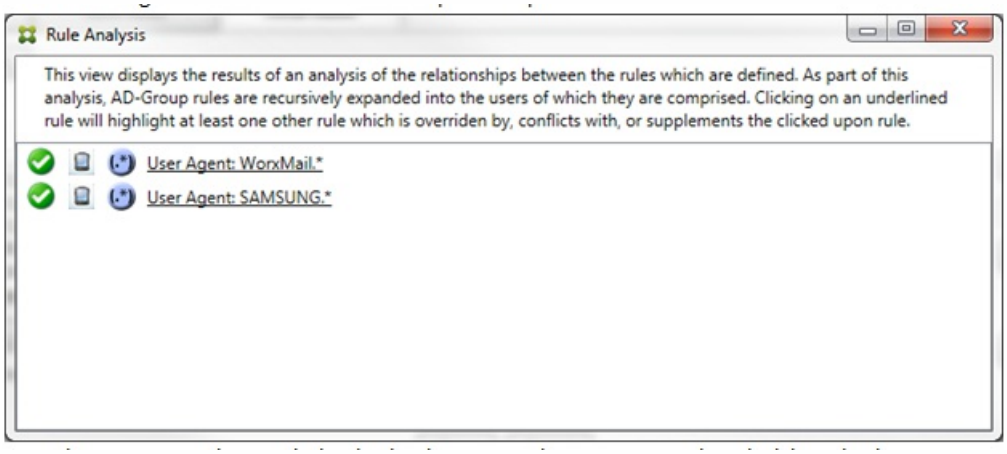
En el ejemplo anterior, es fácil observar que la primera regla (regla de expresión regular SAMSUNG.*) no solo invalida la siguiente regla (regla normal SAMSUNG-SM-G900A/101.40402), sino que las dos reglas se diferencian en su acceso (la primaria especifica Permitir, mientras que la auxiliar especifica 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:

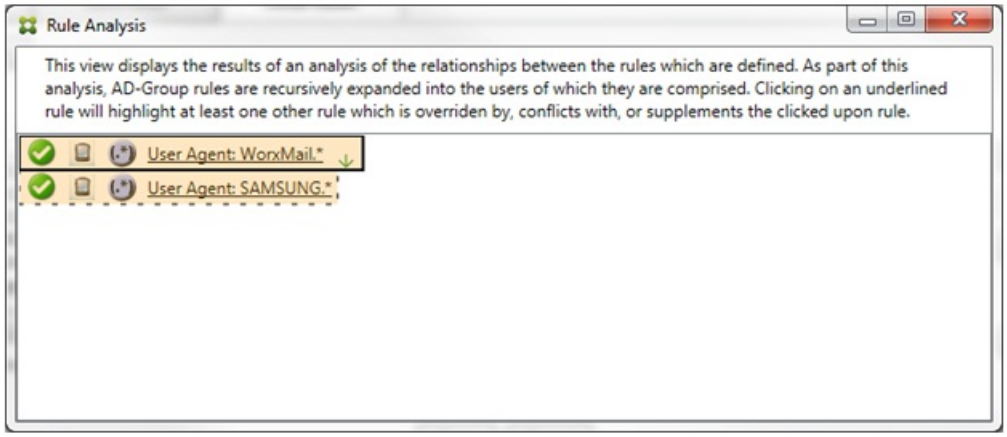


La regla primaria (regla de expresión regular SAMSUNG.*) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal SAMSUNG-SM-G900A/101.40402) va seguida de un punto rojo para indicar que su estado de acceso 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:



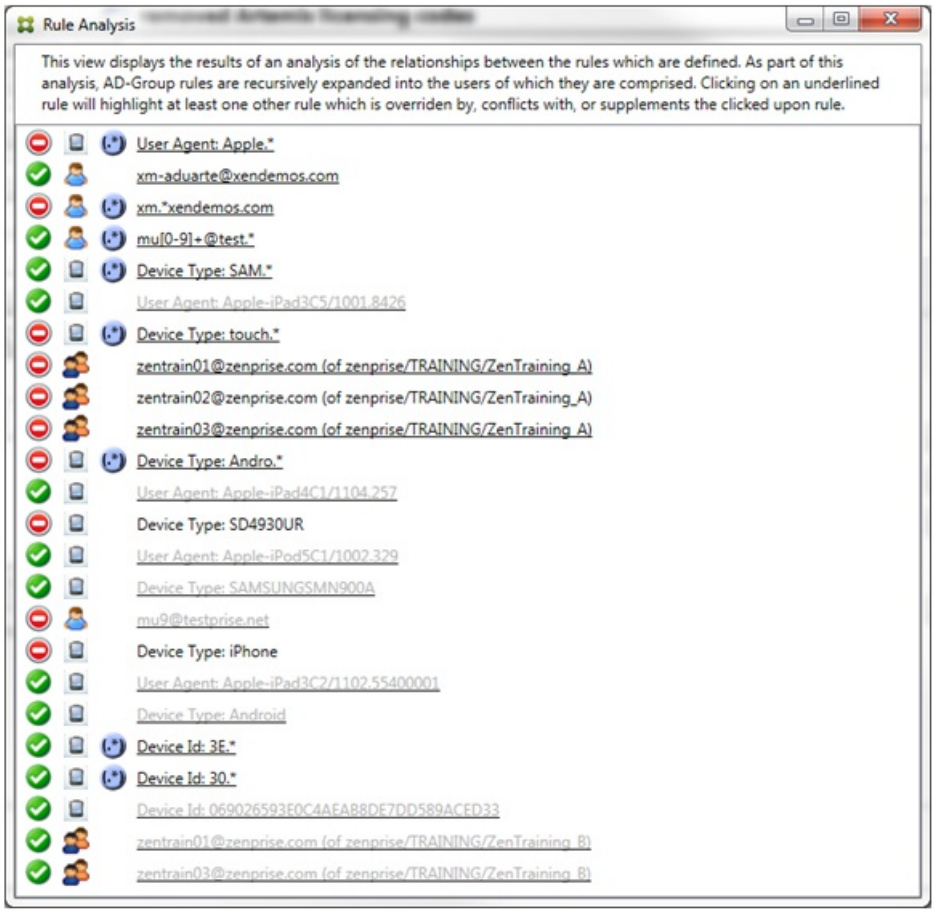
Tras echar un vistazo, es evidente que ambas reglas son de expresión regular y que se han aplicado al campo de ID de dispositivo ActiveSync en XenMobile Mail Manager. Después de hacer clic en la primera regla, el cuadro aparecerá de la siguiente manera:



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

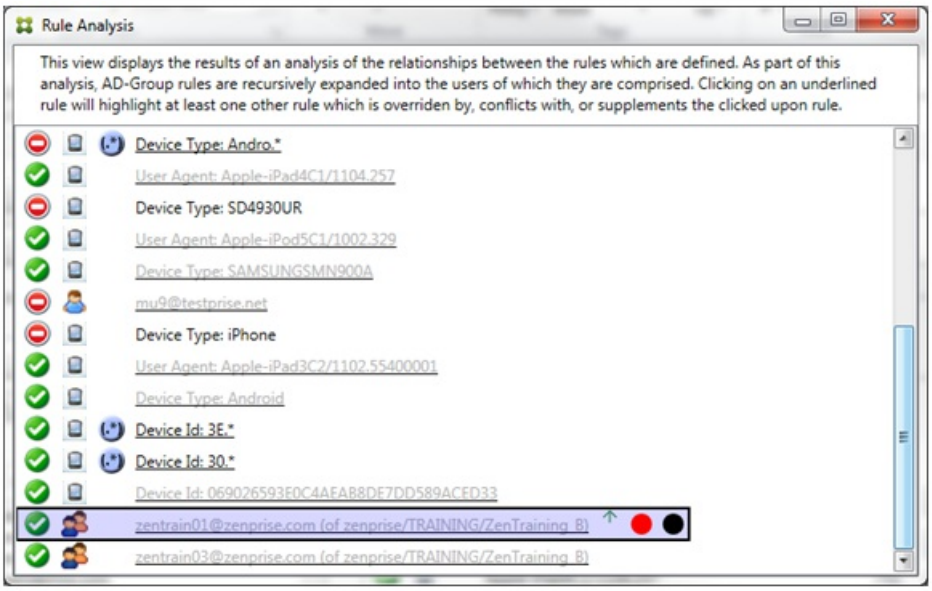
Se pueden producir tantos conflictos, invalidaciones o complementaciones que no se puede ofrecer un ejemplo para todos los casos posibles. En el siguiente ejemplo, se describe lo que no se recomienda hacer y también se ilustra el verdadero potencial de la construcción visual del análisis de reglas. En 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.

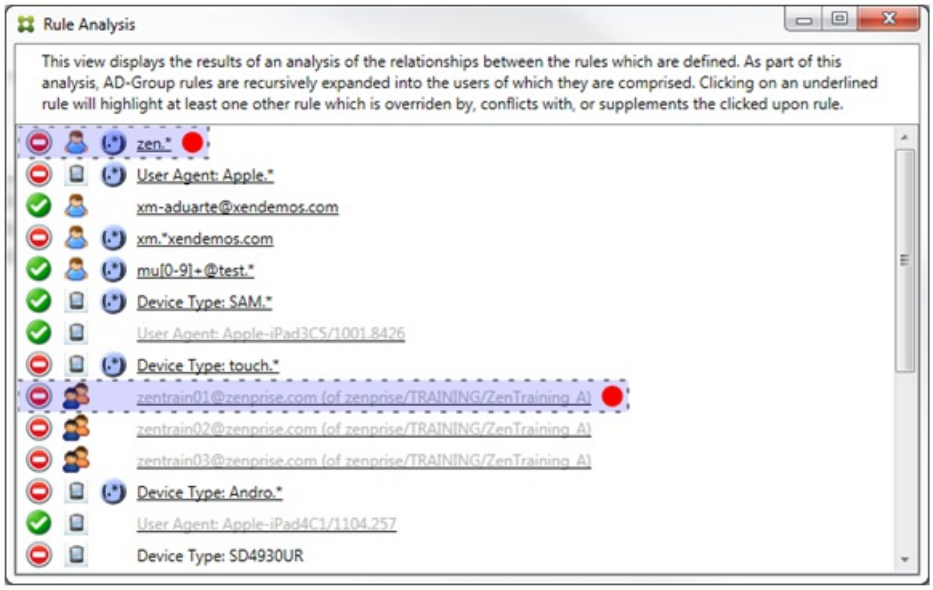
Ejemplo 1. En este ejemplo, se examina por qué zentrain01@zenprise.com se ha invalidado.



La regla primaria (regla del grupo de AD zenprise/TRAINING/ZenTraining B, de la que zentrain01@zenprise.com es miembro) tiene las siguientes características:

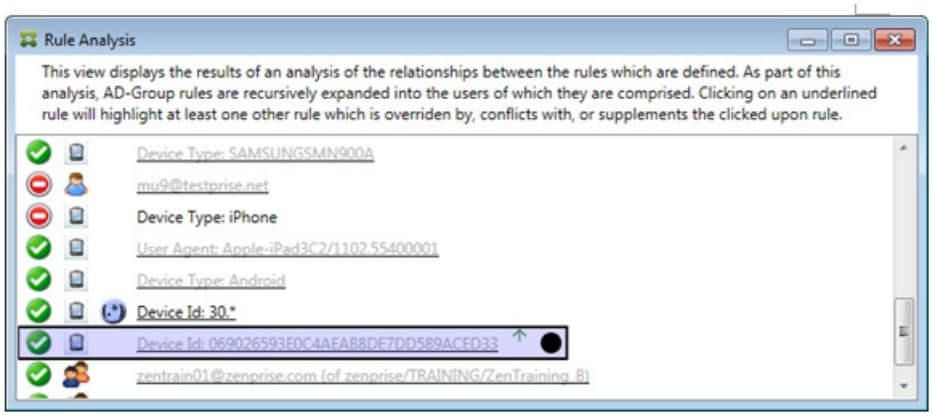
- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que las reglas auxiliares están todas encima de ella).
- Va seguida de un círculo rojo y uno negro para indicar, respectivamente, que una o más reglas están en conflicto con el acceso y que la regla primaria se ha invalidado y, por lo tanto, está inactiva.

Si se desplaza hacia arriba, verá lo siguiente:



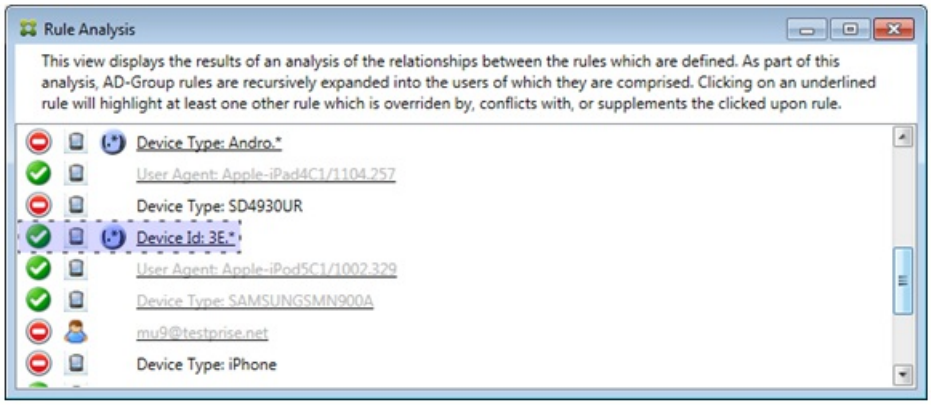
En este caso, hay dos reglas auxiliares que invalidan la regla primaria: la regla de expresión regular zen.* y la regla normal zentrain01@zenprise.com (de zenprise/TRAINING/ZenTraining A). En el caso de la última regla auxiliar, lo que ha ocurrido es que la regla del grupo de Active Directory ZenTraining 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.

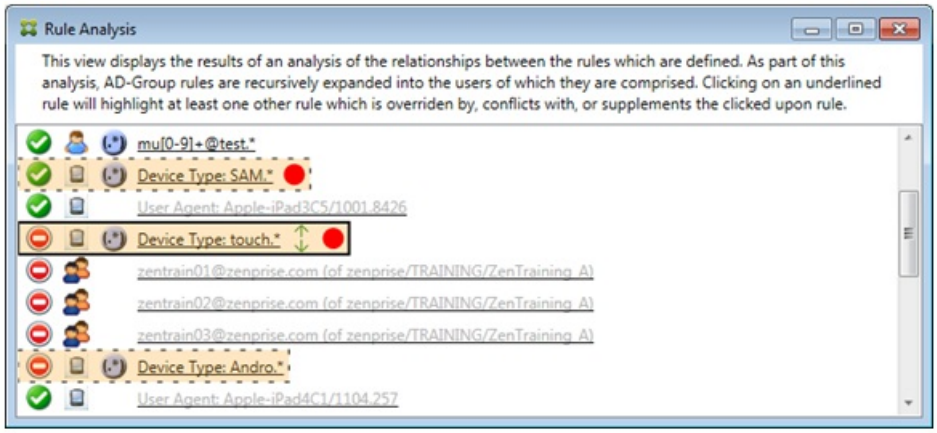
Cómo analizar una complementación y un conflicto

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

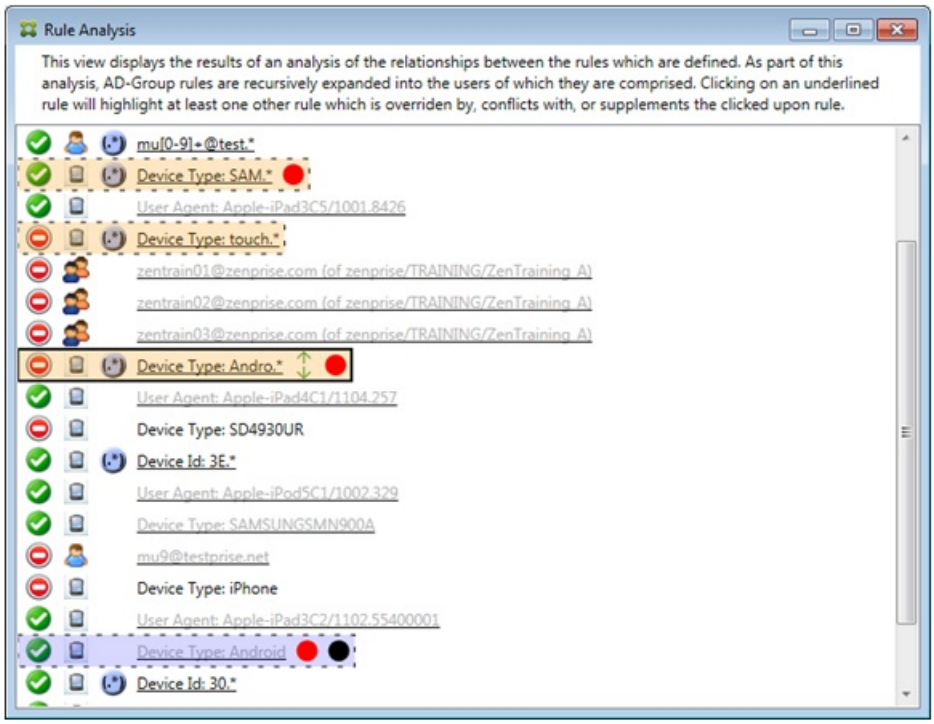
está en conflicto con la regla primaria, cuyo acceso es Bloquear.

- 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

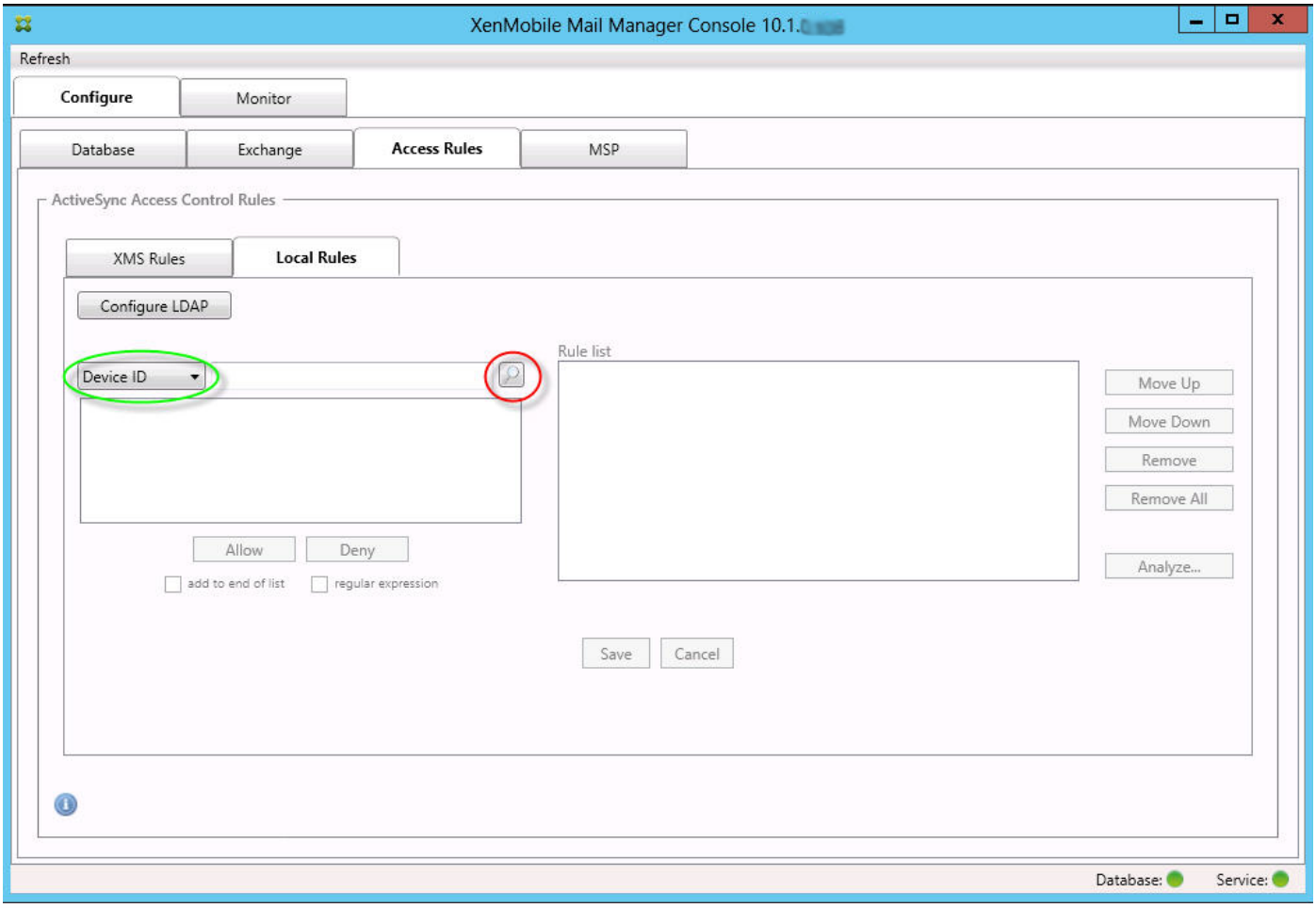
En este ejemplo, se describe cómo las relaciones entre reglas se dan siempre con respecto a la regla primaria. En el ejemplo anterior, se ha mostrado cómo un clic en la regla de expresión regular se aplicaba al campo de regla de tipo de dispositivo con el valor touch.*. Al hacer clic en la regla auxiliar Andro.*, se muestra un conjunto diferente de reglas auxiliares resaltadas.



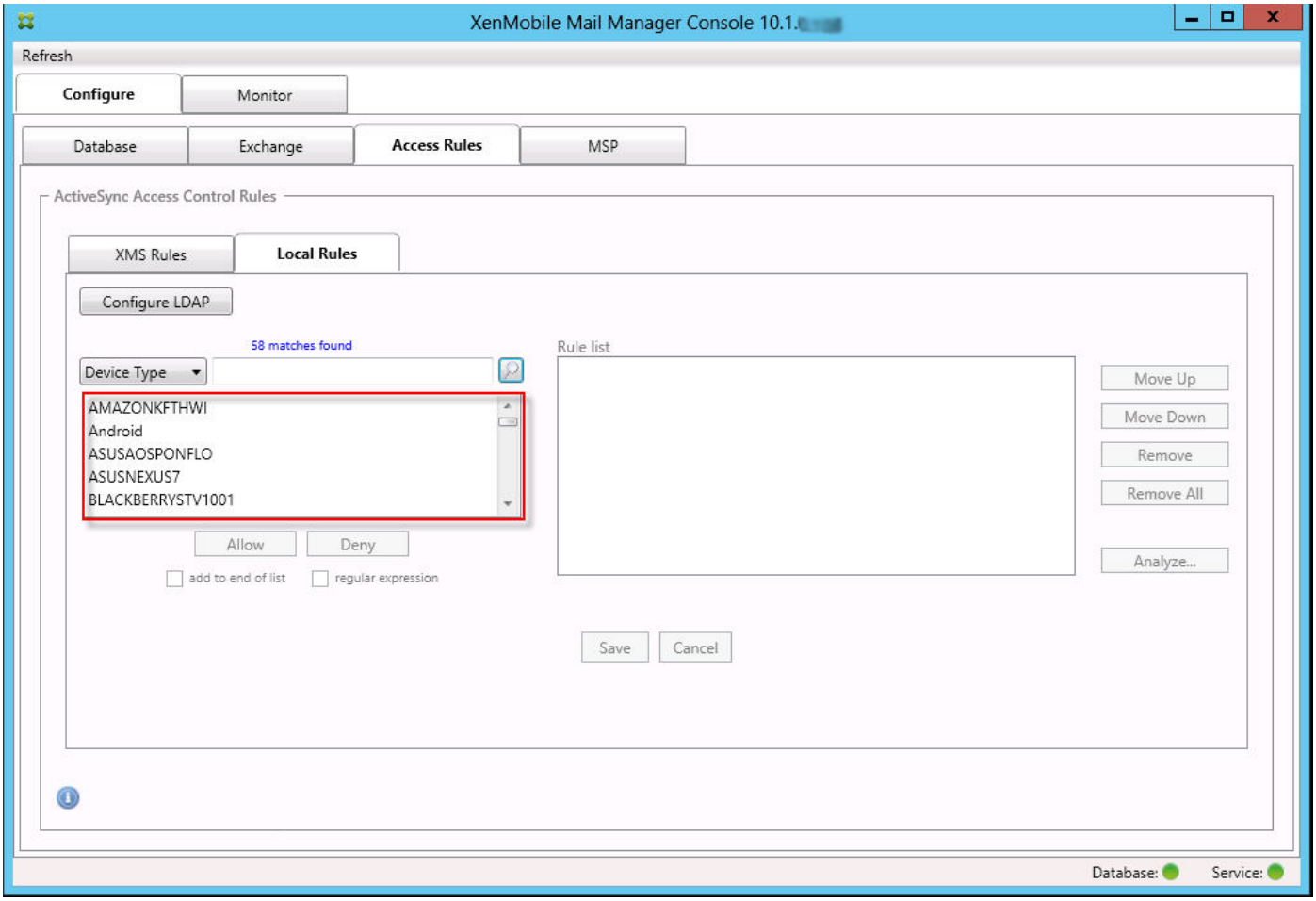
El ejemplo muestra una regla invalidada que se incluye en la relación de las reglas. Esta regla es la regla normal de tipo de dispositivo ActiveSync Android, que se ha invalidado (situación indicada con la fuente más atenuada y el círculo negro junto a ella) y también está en conflicto con el acceso 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.

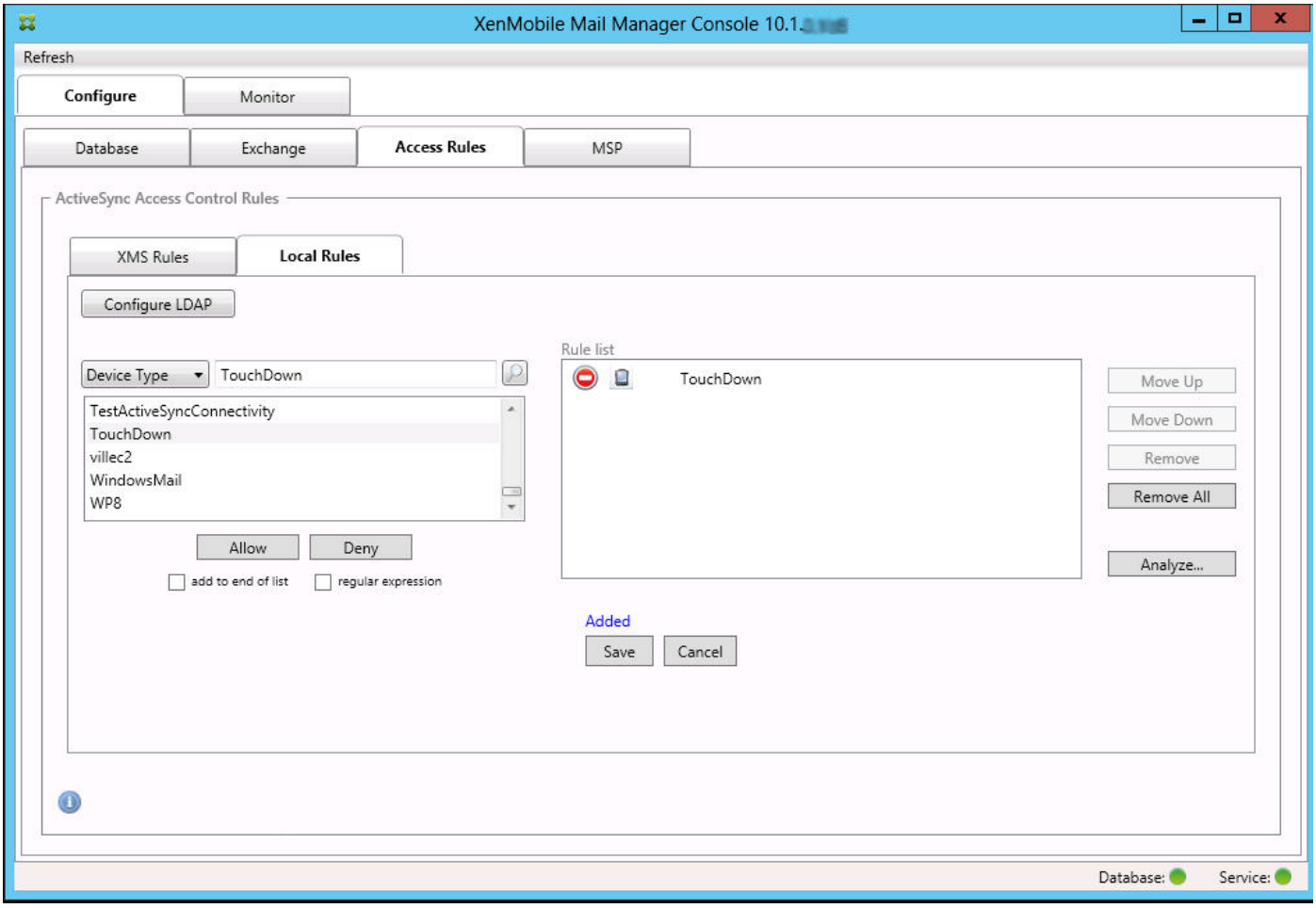


2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, en el cuadro 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.

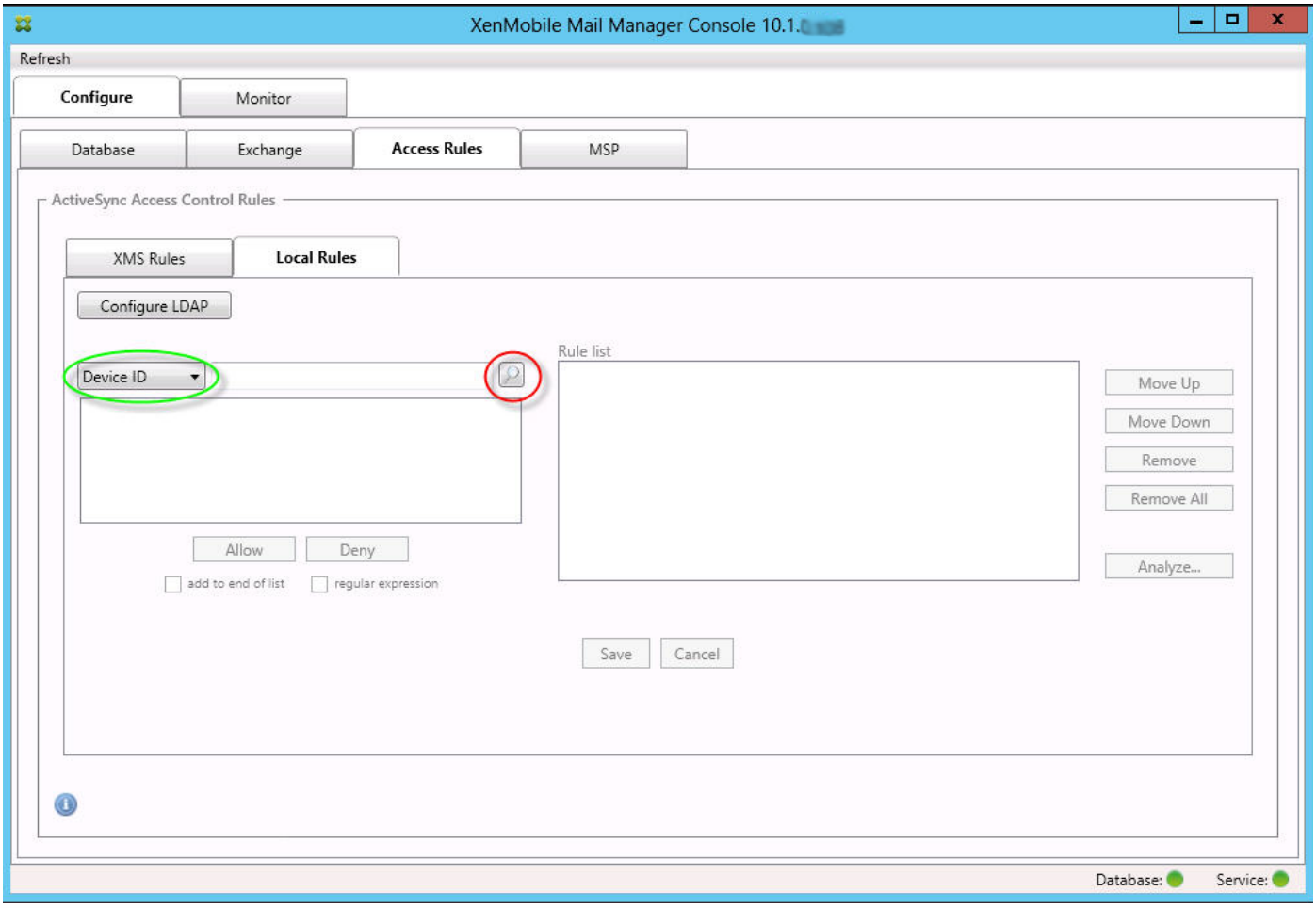


Para agregar una expresión regular

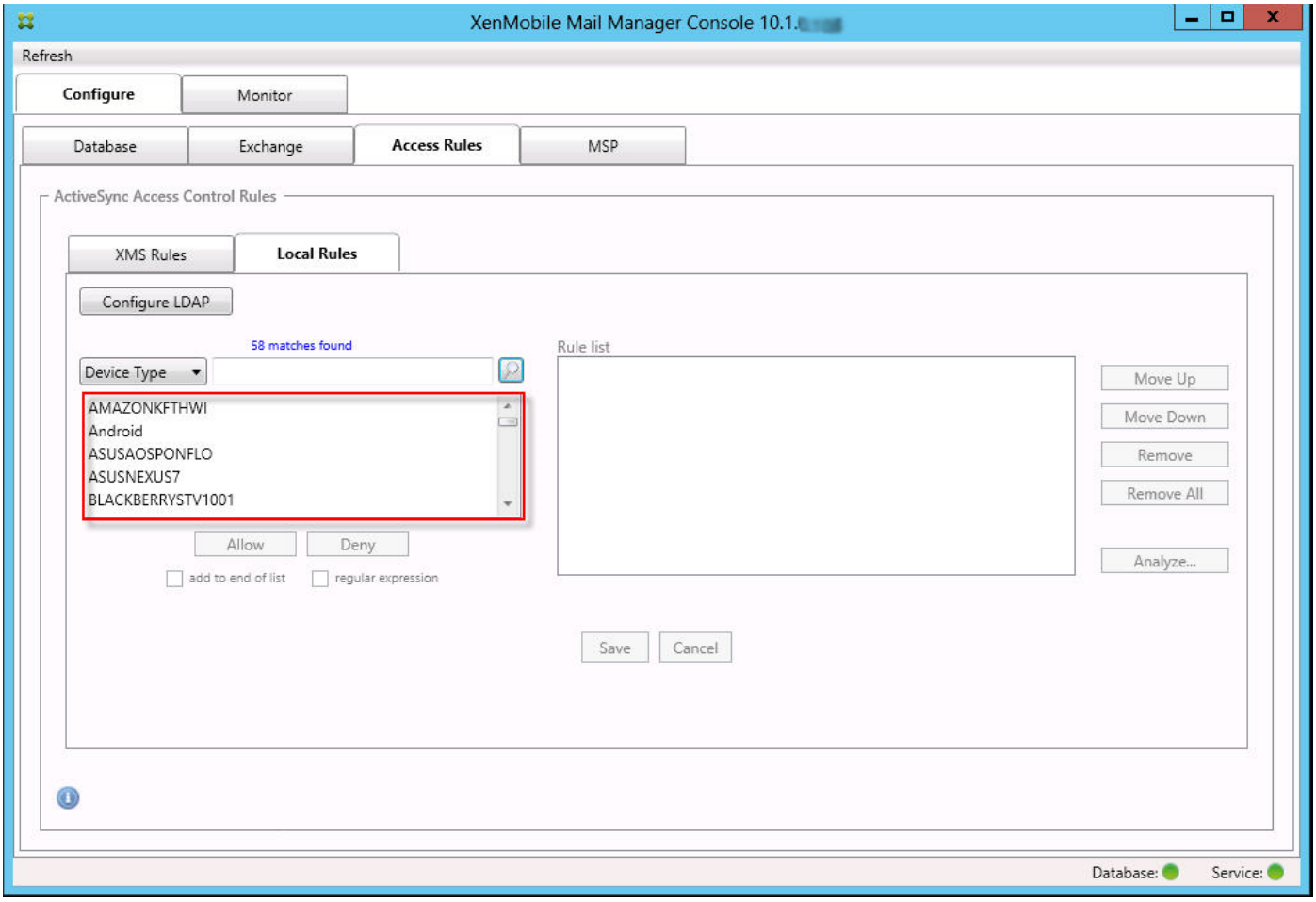
Las reglas locales de expresión regular se distinguen por el icono que aparece junto a ellas - (.*). Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados de un campo determinado (siempre que se haya completado 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

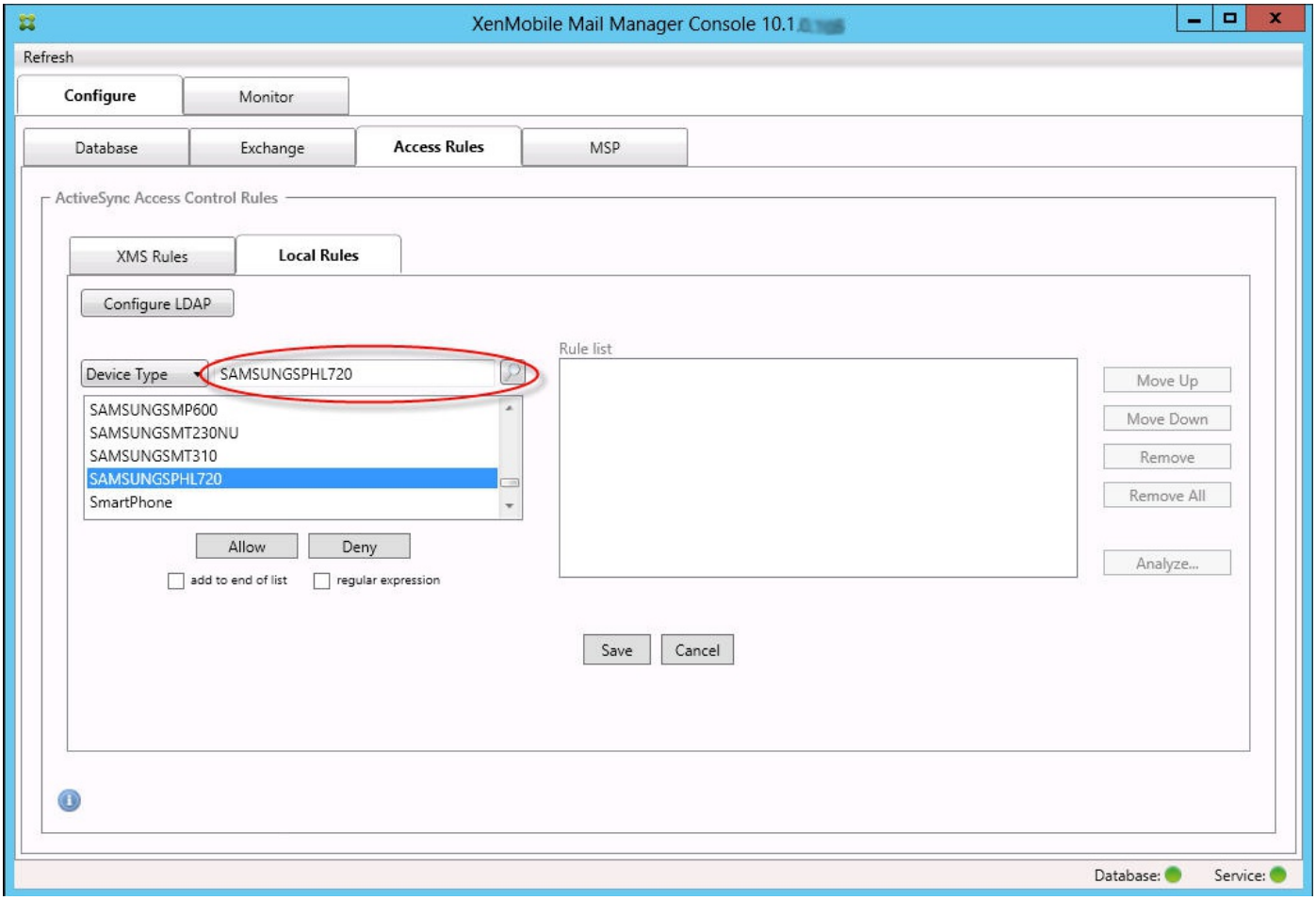
1. Haga clic en la ficha Access Rules.



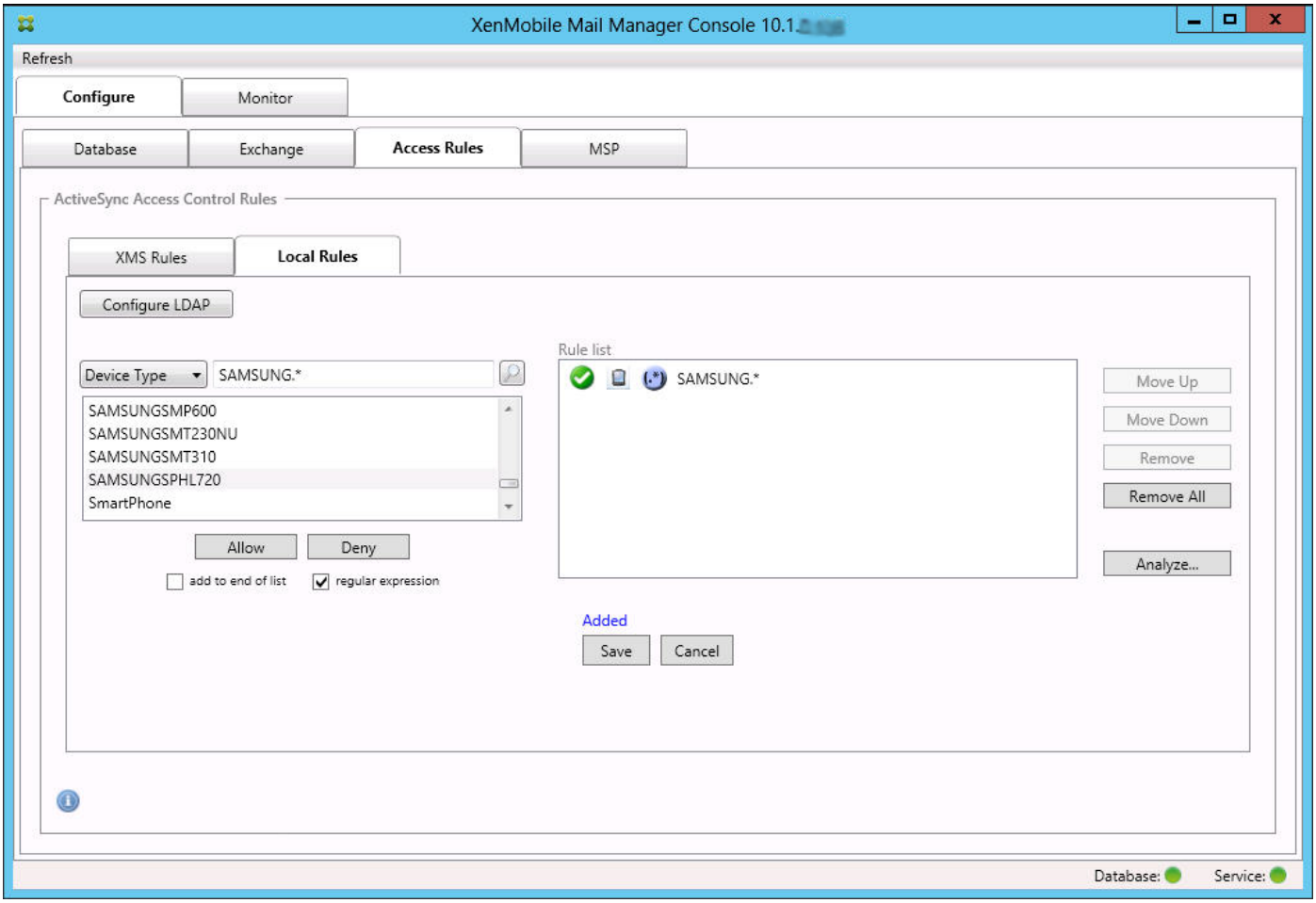
2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local de expresión regular.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, 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.

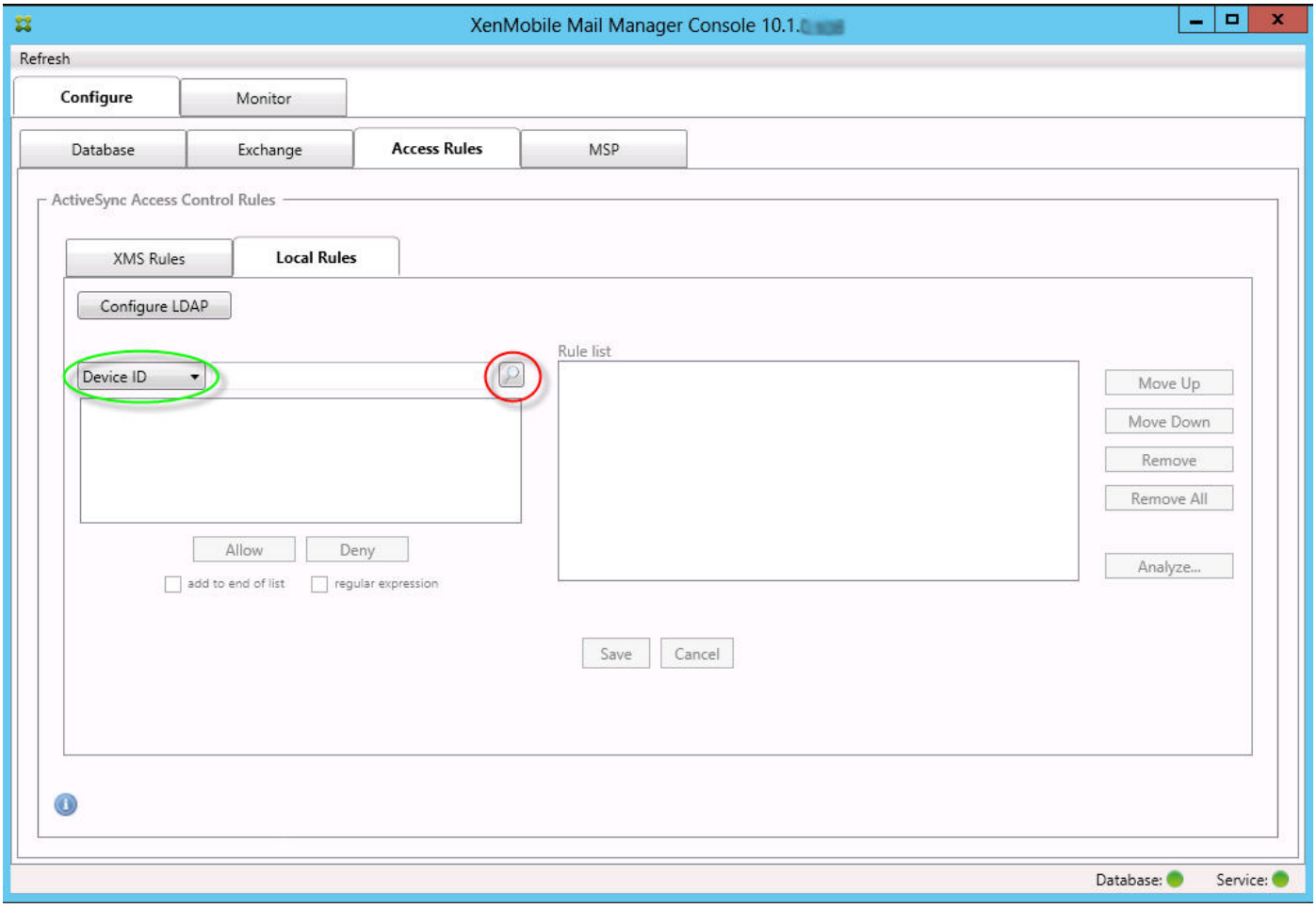


5. Para permitir el acceso a todos los tipos de dispositivos que contengan "Samsung" en su valor de tipo de dispositivo, siga estos pasos para agregar una regla de expresión regular:
   1. Haga clic en el cuadro de texto del elemento seleccionado.
   2. Cambie el texto de SAMSUNGSPHL720 a SAMSUNG.*
   3. Compruebe que la casilla de verificación regular expression está marcada.
   4. Haga clic en Allow.

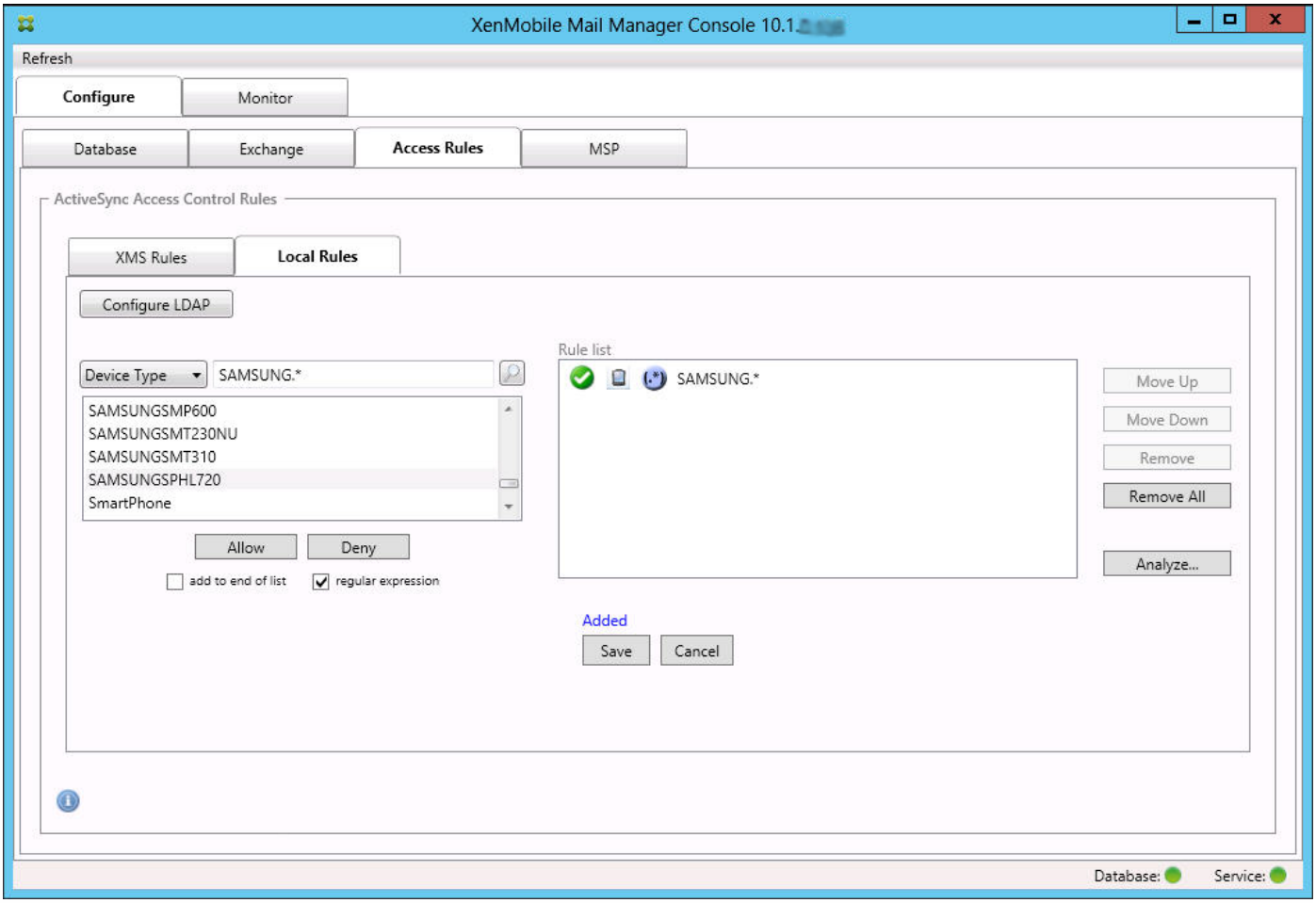


Para crear una regla de acceso

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.



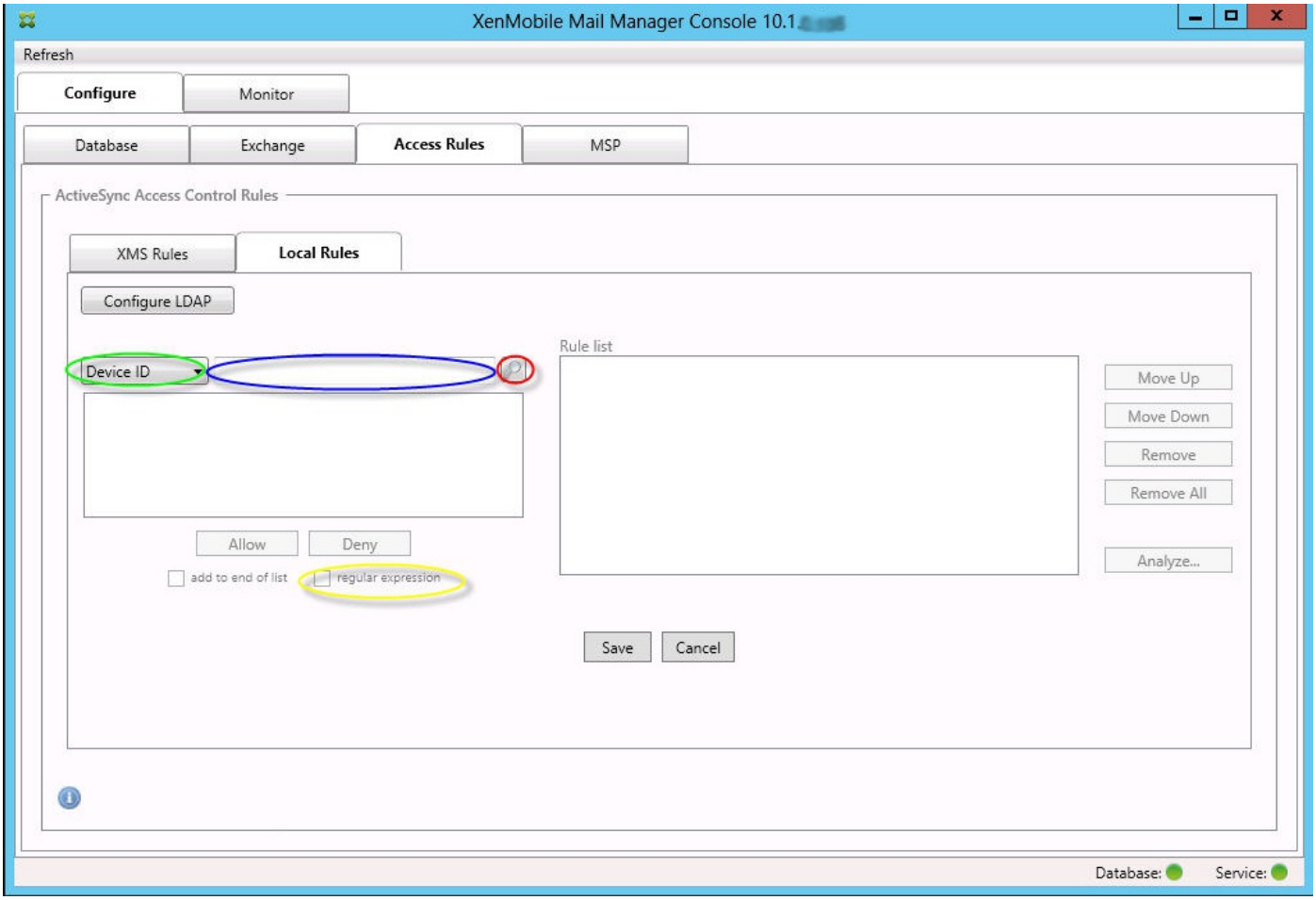
3. Seleccione el campo con el que corresponderse. En este ejemplo, se utiliza Device Type.
4. Escriba la expresión regular. En este ejemplo se usasamsung.*
5. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en Allow o Deny. En este ejemplo, la opción es Allow para que el resultado final sea el siguiente:



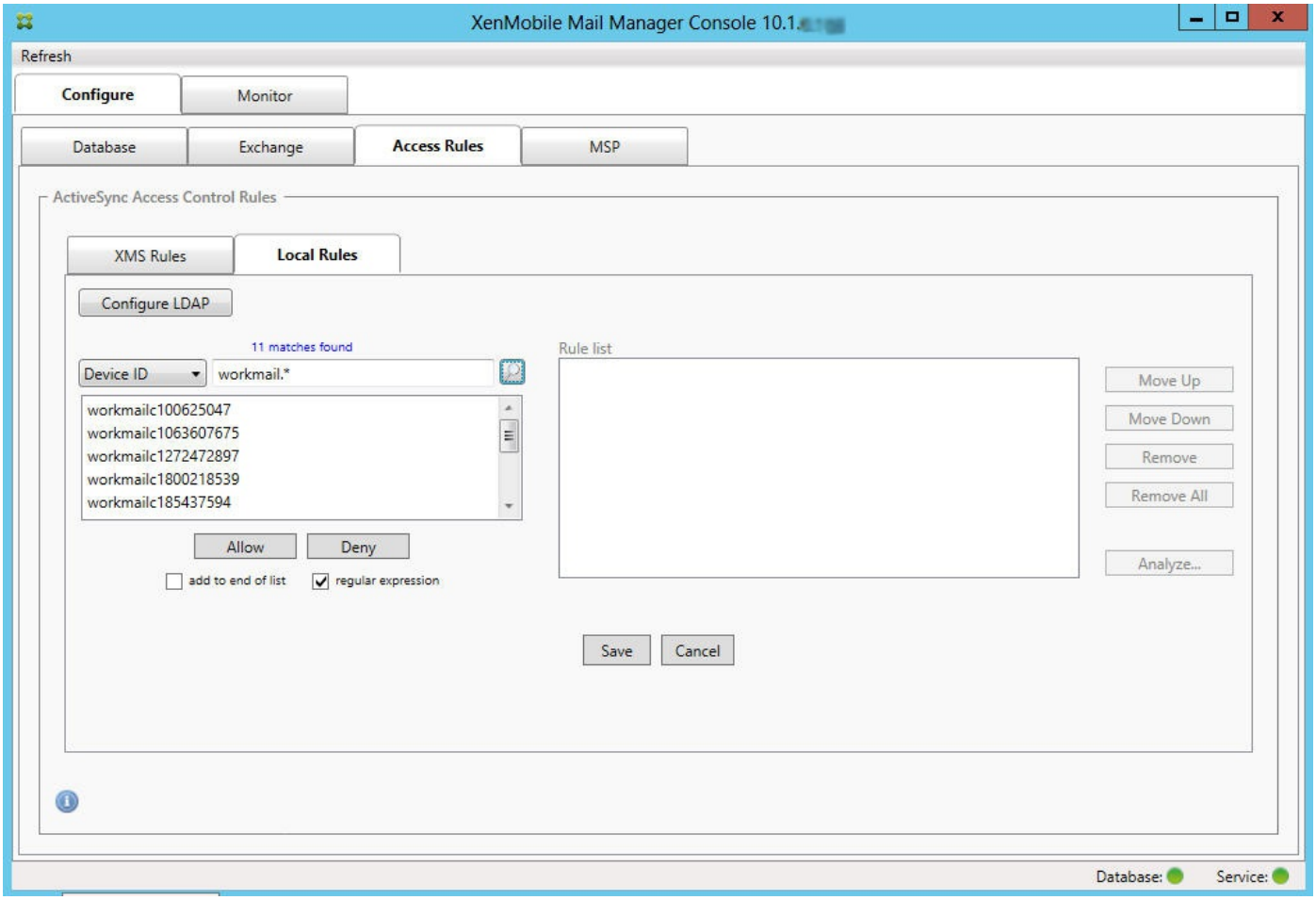
Para buscar dispositivos

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).



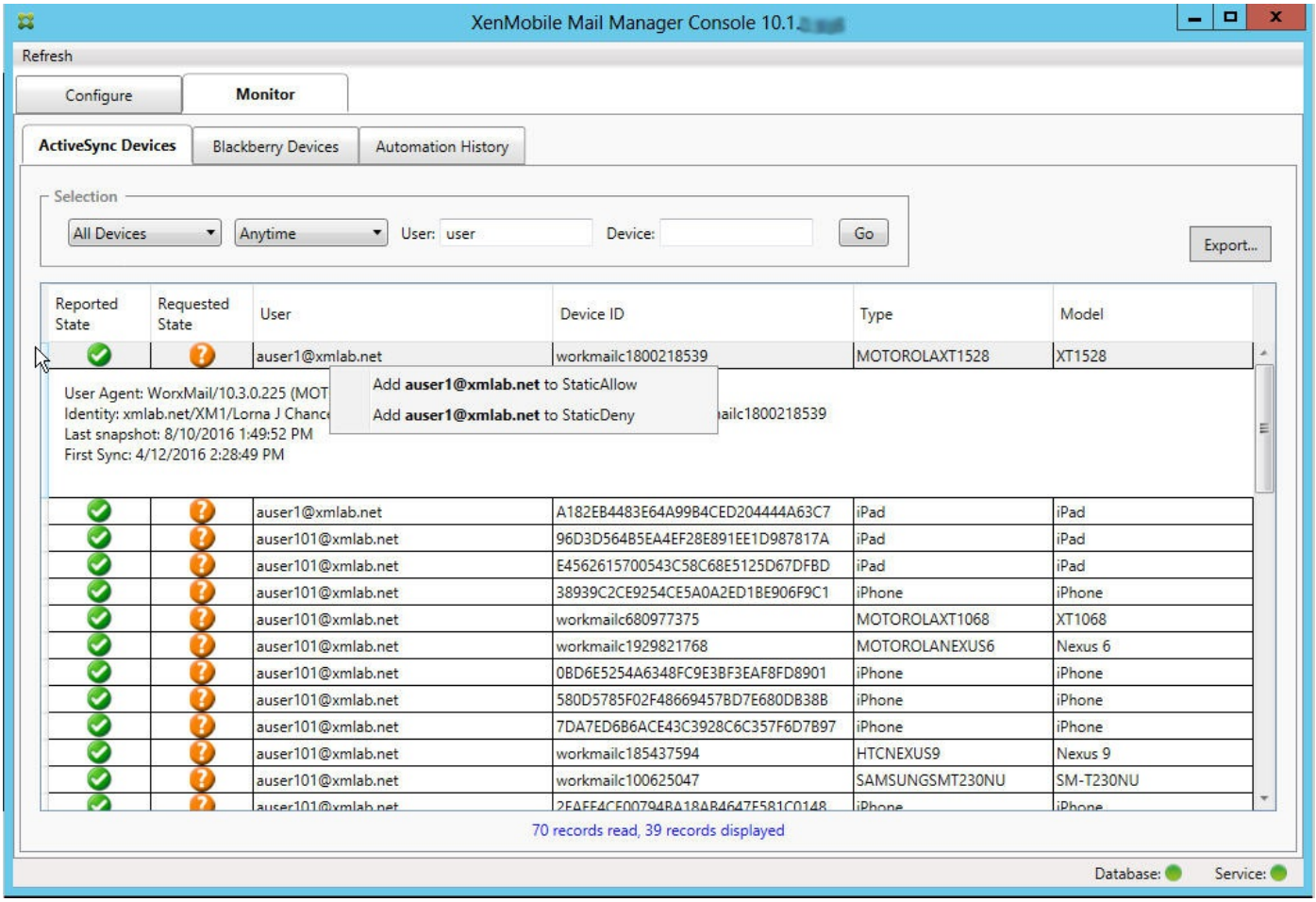
3. Haga clic en el cuadro de texto del elemento seleccionado (como se muestra en azul en la imagen anterior) y escribaworkmail.*.
4. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en el icono de lupa para ver los resultados, tal y como se muestra 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

Jul 27, 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

Oct 31, 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.

Errores comunes

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.

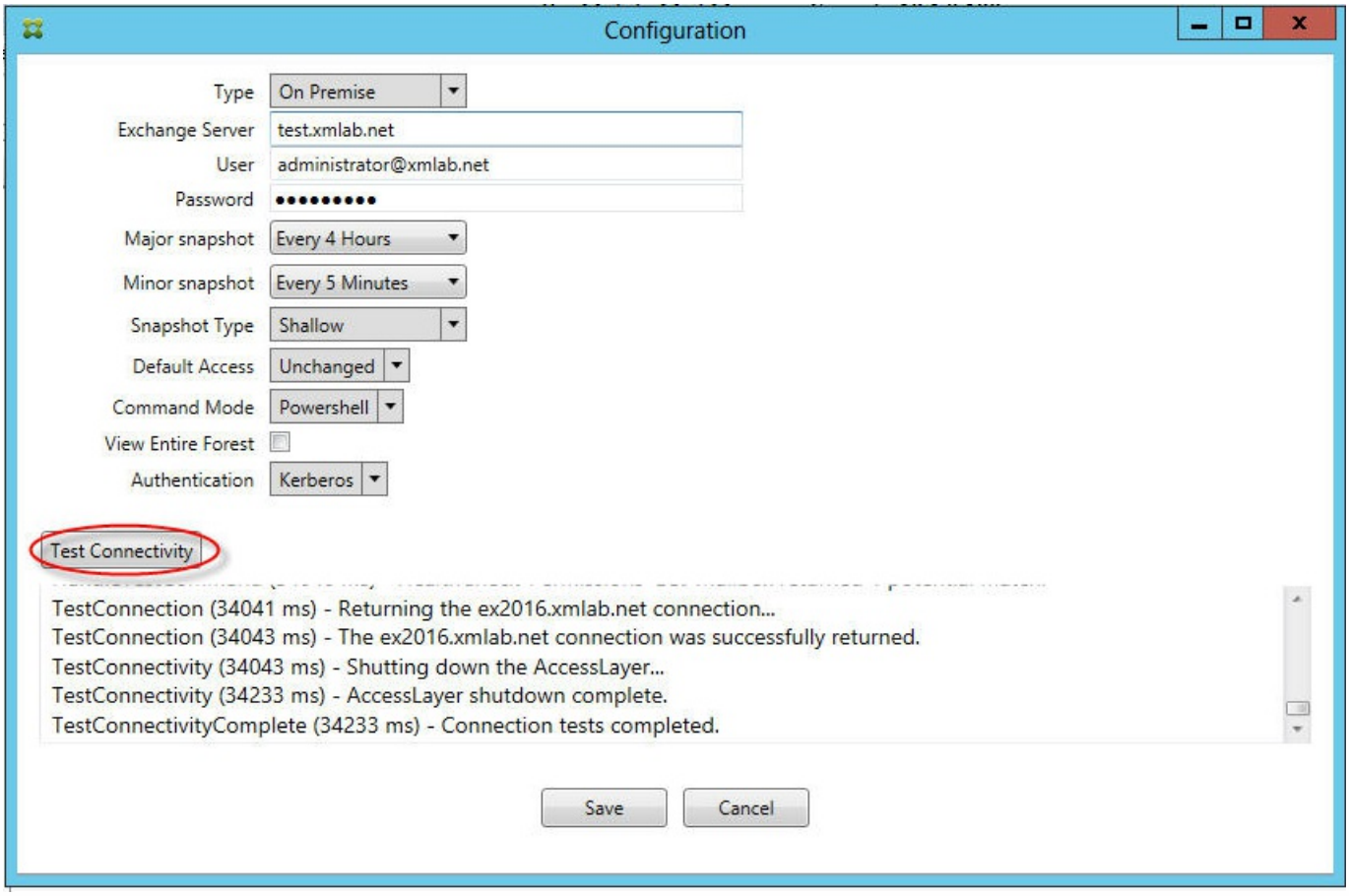
  Si la autenticación integrada de Windows está configurada, la cuenta de usuario del servicio de XenMobile Mail Manager debe tener permitido el inicio de sesión en SQL Server. La cuenta del servicio de XenMobile Mail Manager es, de forma predeterminada, el sistema local, pero se puede cambiar a una cuenta 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 <Carpeta de instalación>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.



Herramientas para solución de problemas

En la carpeta Support\PowerShell dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Una herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y problemas potenciales, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

XenMobile NetScaler Connector

Oct 31, 2016

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.

Para obtener más información, consulte estos artículos:

- XenMobile NetScaler Connector
- ActiveSync Gateway en XenMobile

Para ver diagramas de referencia de arquitectura en detalle, consulte el artículo Reference Architecture for On-Premises Deployments de XenMobile Deployment Handbook.