Novedades en XenMobile Server 10.5

Apr 04, 2017

Este PDF contiene el conjunto completo de documentación de productos de XenMobile Server 10.5.Para obtener la documentación de la versión actual del producto, consulte XenMobile Server.

Para obtener más información sobre la actualización, consulte Actualización. Para acceder a la consola de administración de XenMobile, use solamente el nombre de dominio completo de XenMobile Server o las direcciones IP del nodo.

> **Important**
>
> Para acceder a la consola de administración de XenMobile, use solamente el nombre de dominio completo de XenMobile Server (el FQDN de inscripción) o las direcciones IP del nodo. El acceso a la consola directamente a través de una dirección IP virtual de equilibrio de carga o a través de una dirección IP de NAT ya no está disponible, a menos que instale XenMobile Server 10.5 revisión (rolling patch) 1, publicada el 22 de marzo de 2017. Para obtener más información, consulte https://support.citrix.com/article/CTX221304.

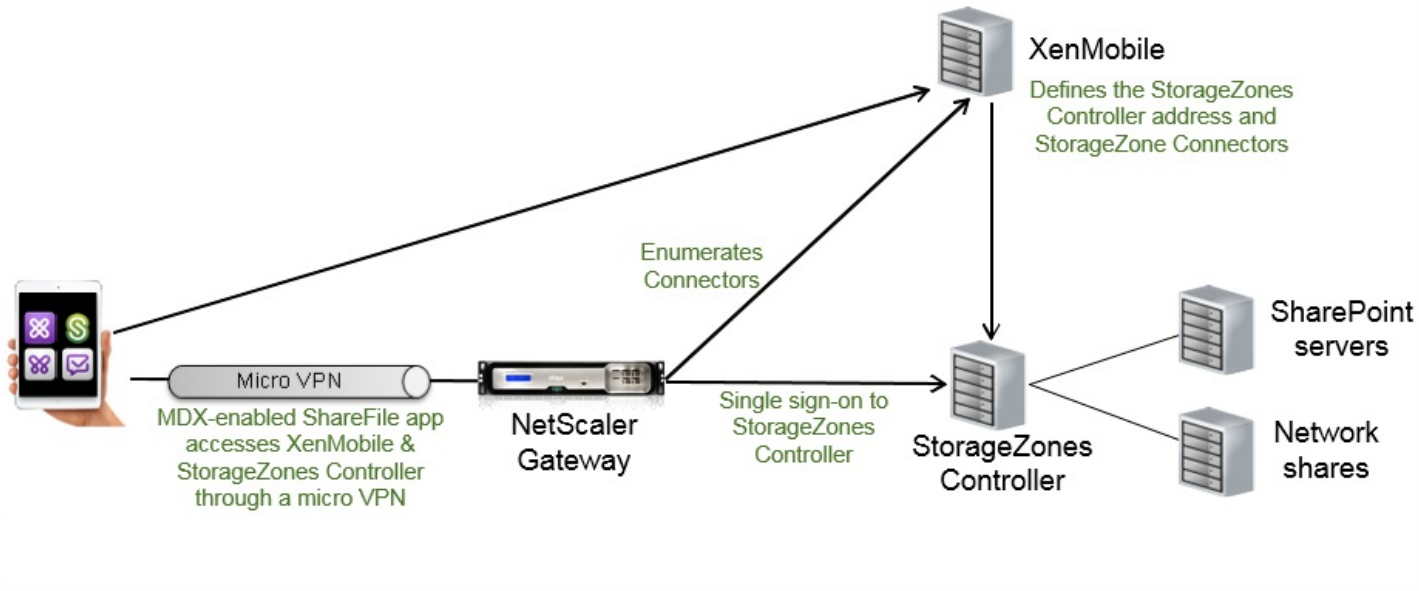
XenMobile Server 10.5 incluye las siguientes características nuevas. Para ver las correcciones de errores, consulte Problemas resueltos.

Administración e implementación más fáciles de conectores de StorageZone en ShareFile

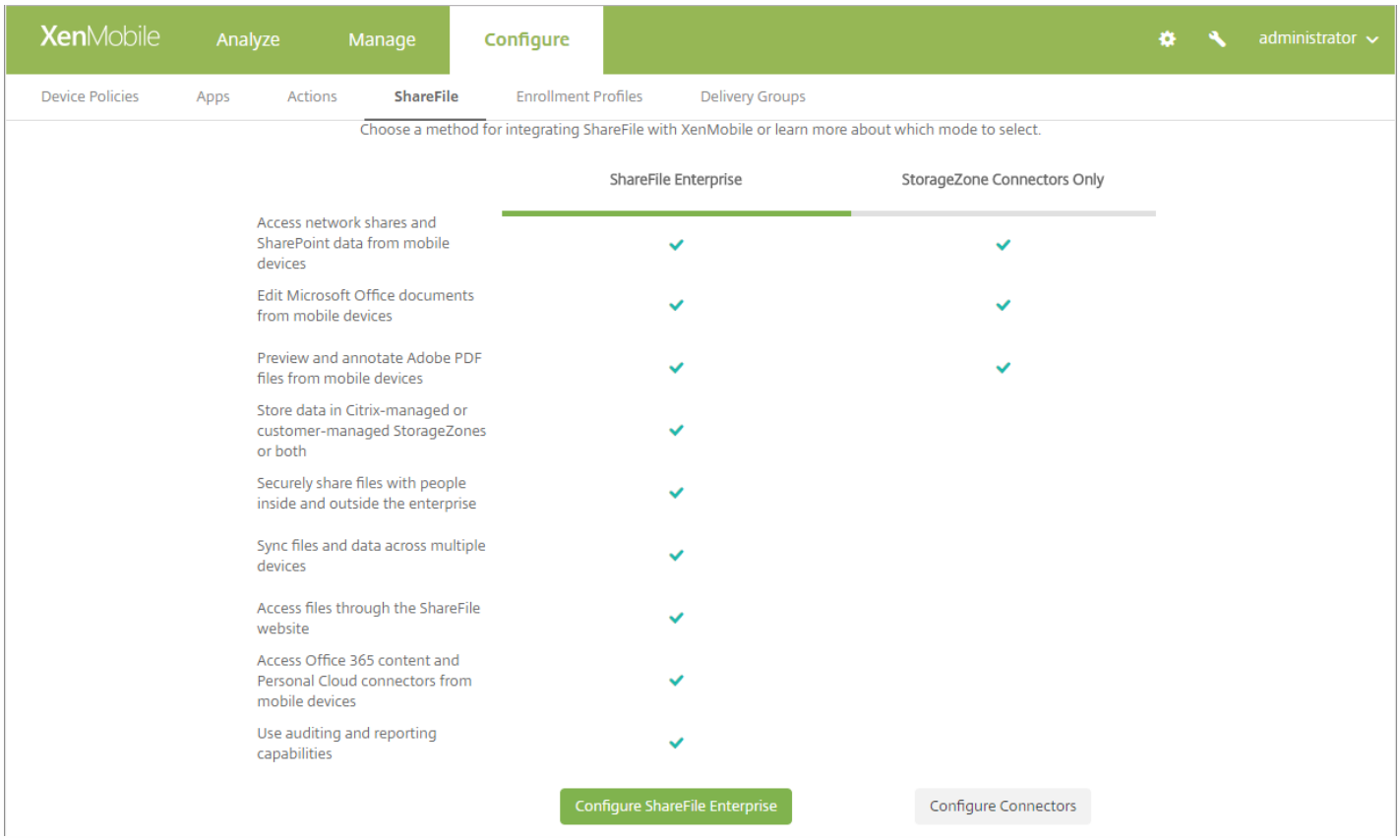
Ahora, puede usar la consola de XenMobile para configurar los conectores StorageZone Connector. Ofrecida como alternativa a XenMobile con ShareFile Enterprise, la opción de utilizar XenMobile con conectores StorageZone Connector:

- Ofrece un acceso móvil seguro a los repositorios del almacenamiento local existente, como sitios de SharePoint y archivos compartidos de red. No se requiere que configure un subdominio de ShareFile ni aprovisione usuarios a ShareFile ni aloje datos de ShareFile.
- Proporciona a los usuarios acceso móvil a los datos a través de las aplicaciones XenMobile de ShareFile para iOS. Los usuarios pueden modificar documentos de Microsoft Office. Los usuarios también pueden obtener vistas previas y escribir notas en archivos PDF de Adobe desde dispositivos móviles.
- El acceso a los archivos se limita en función de los conectores. Los usuarios no tienen acceso a otras funciones de ShareFile (como sincronizar o compartir datos).
- Cumple las restricciones de seguridad contra la filtración de la información de usuarios fuera de la red corporativa.
- Proporciona una configuración simple de conectores StorageZone Connector a través de la consola de XenMobile. Si posteriormente decide usar la funcionalidad completa de ShareFile con XenMobile, puede cambiar la configuración en la consola de XenMobile.
- Requiere la edición XenMobile Enterprise.

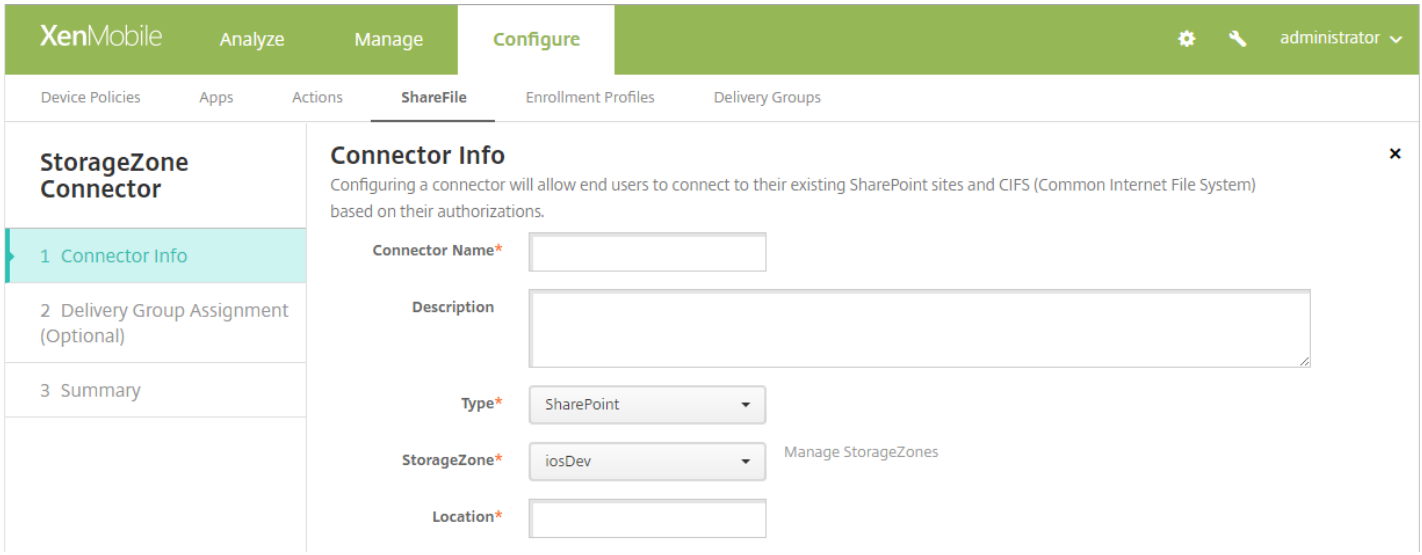
En el siguiente diagrama, se muestra la arquitectura de alto nivel para usar XenMobile con conectores StorageZone Connector.

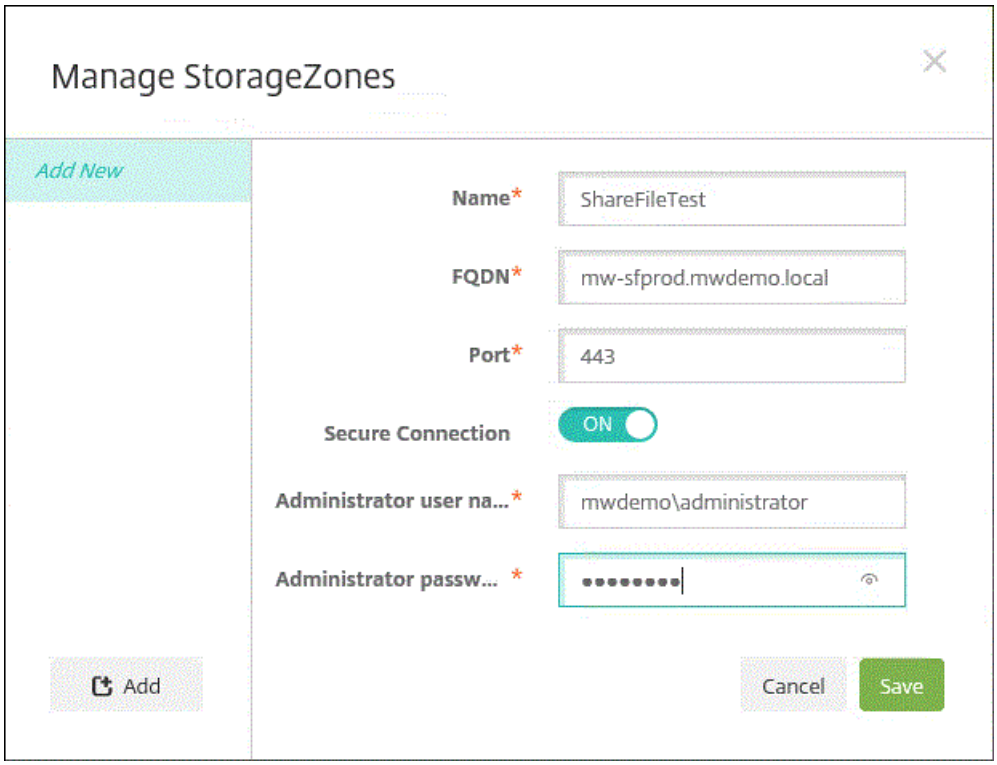


En su primera visita a la página **Configure > ShareFile**, aparecen en la página las diferencias entre usar XenMobile con ShareFile Enterprise y con conectores StorageZone.

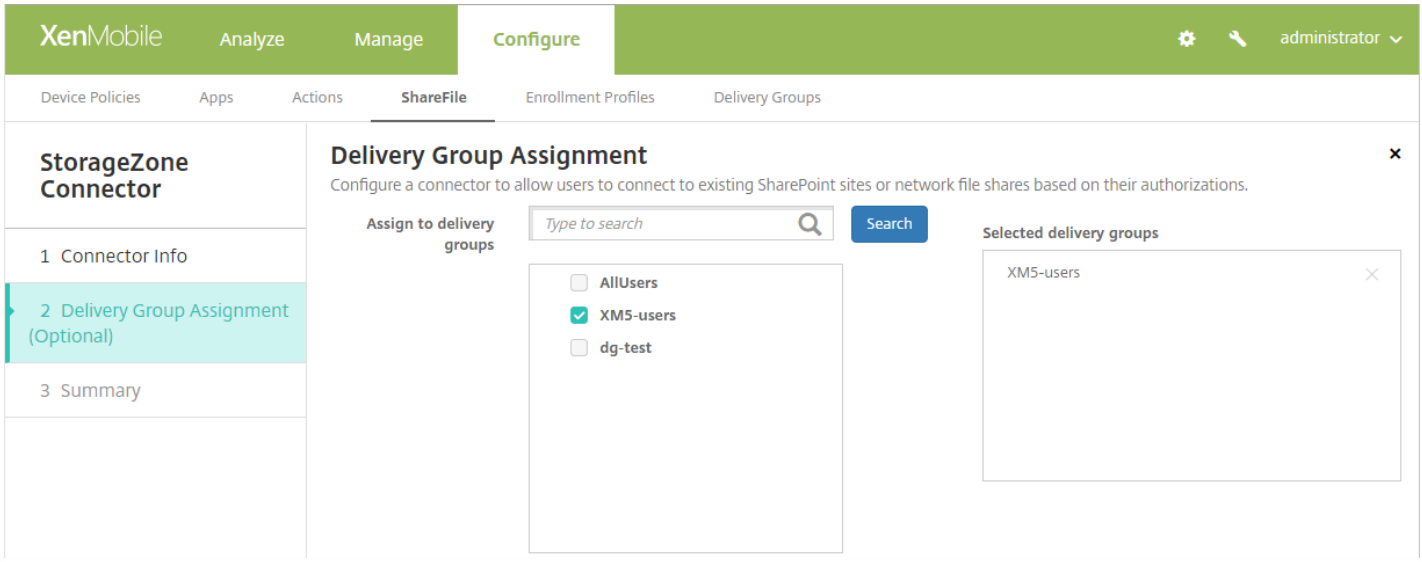


Si hace clic en **Configure Connectors**, debe proporcionar información acerca de los conectores y del Controller de StorageZone.





Cuando cree el conector, puede asociar conectores a grupos de entrega.



También puede asociar conectores a grupos de entrega desde la página **Configure > Delivery Groups**.

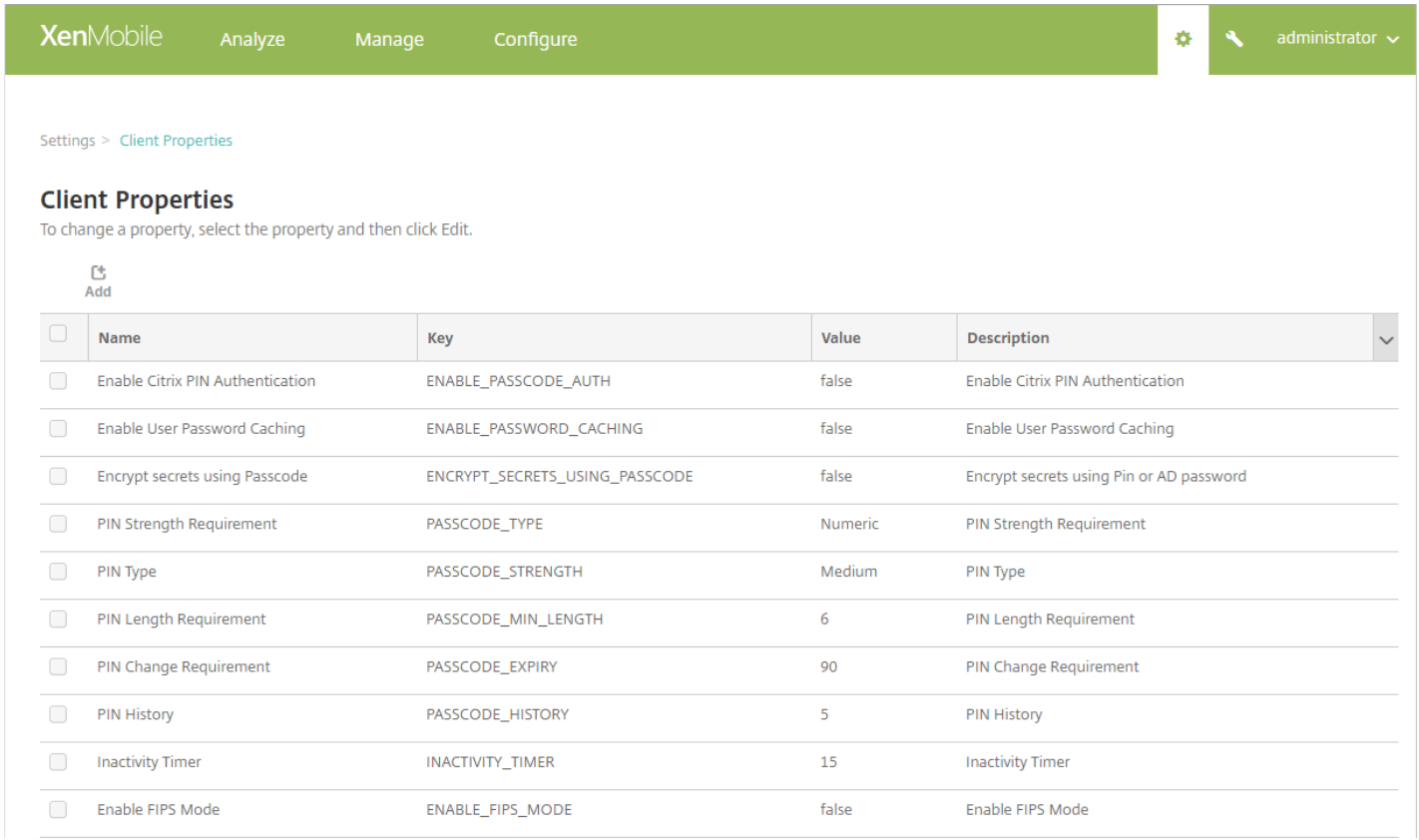
Para obtener más información sobre la integración de conectores de StorageZone en XenMobile, consulte Uso de ShareFile con XenMobile.

Cambio de nombre de propiedades de cliente

Los nombres de propiedades de cliente de XenMobile relacionados con el PIN de Citrix han cambiado:

Antiguo nombre de la propiedad	**Nuevo nombre de la propiedad**
Enable Worx PIN Authentication	Enable Citrix PIN Authentication
Worx PIN Type	Tipo de PIN
PIN Strength Requirement	PIN Strength Requirement
Worx PIN Length Requirement	PIN Length Requirement
Worx PIN Change Requirement	PIN Change Requirement
Worx PIN History	PIN History

Las claves de propiedad siguen siendo las mismas, como se muestra en el ejemplo siguiente:

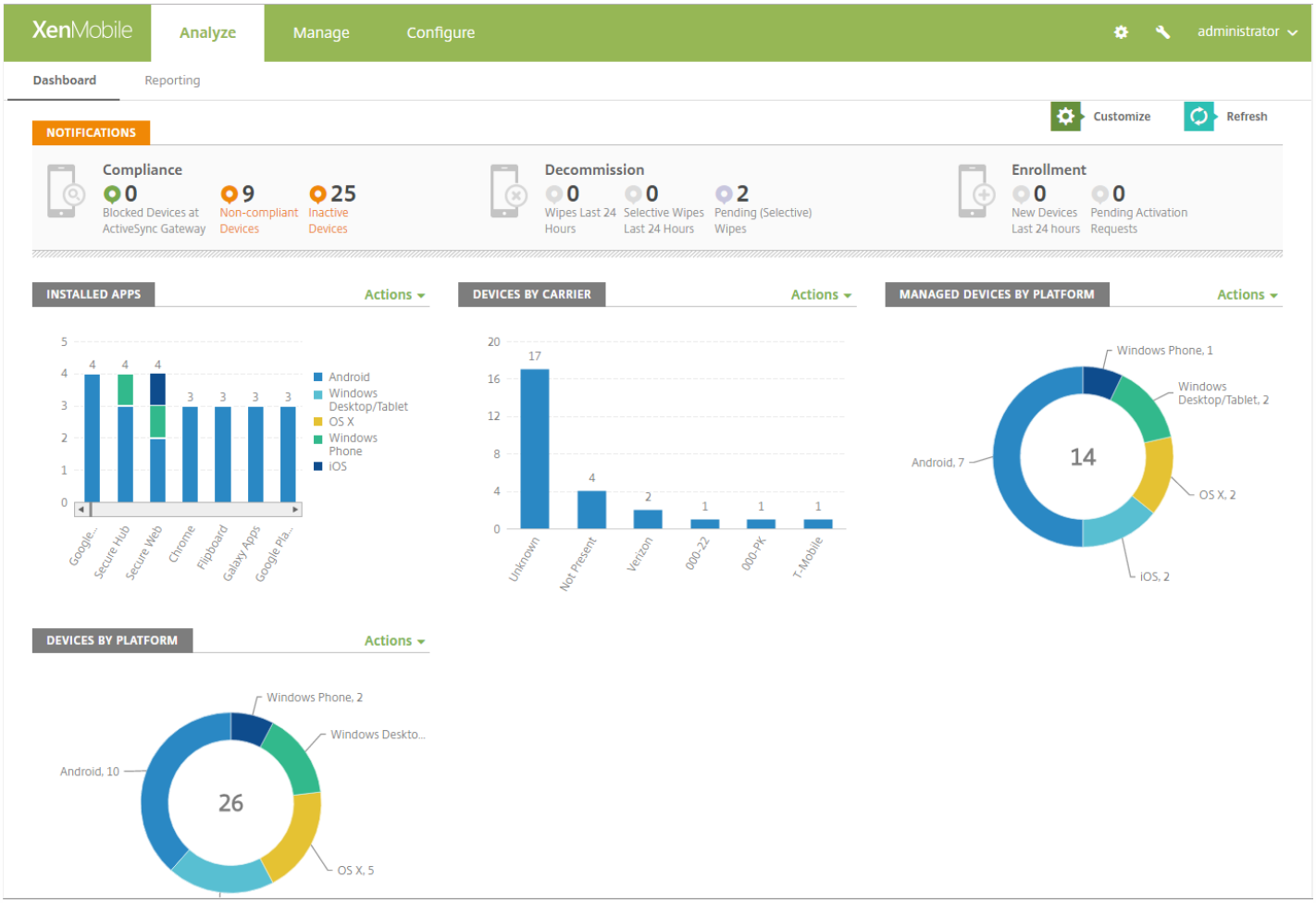


Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

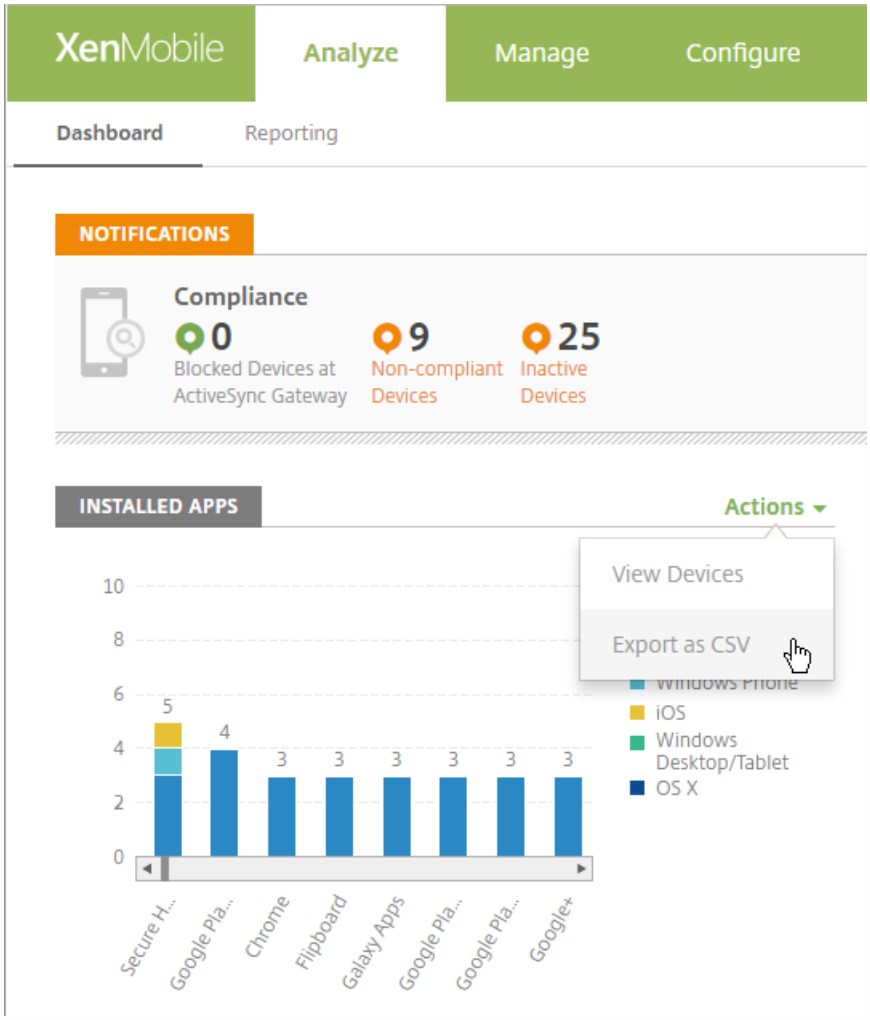
Mejoras en el panel de mandos

En XenMobile, la página **Analyze > Dashboard** tiene un diseño adaptado para mejorar la visualización en dispositivos pequeños. Otras mejoras:

- Ahora, el widget de aplicaciones instaladas muestra las 10 aplicaciones principales. Para ver otras aplicaciones, use la barra de búsqueda.
- Para exportar la información de Installed Apps (el widget de las aplicaciones instaladas) como archivo CSV:
  - Elija una aplicación y, a continuación, expórtela para obtener un informe de esa aplicación únicamente.
  - No elija ninguna aplicación para obtener un informe de todas ellas.
  - Los informes contienen la siguiente información de una aplicación: nombre, propietario, versión, tamaño, ID y hora de instalación.
- Ahora, el widget VPP Apps License Usage (Uso de licencias por parte de aplicaciones provenientes de VPP) muestra todas las aplicaciones del inventario de software. Ya no es necesario buscar aplicaciones.



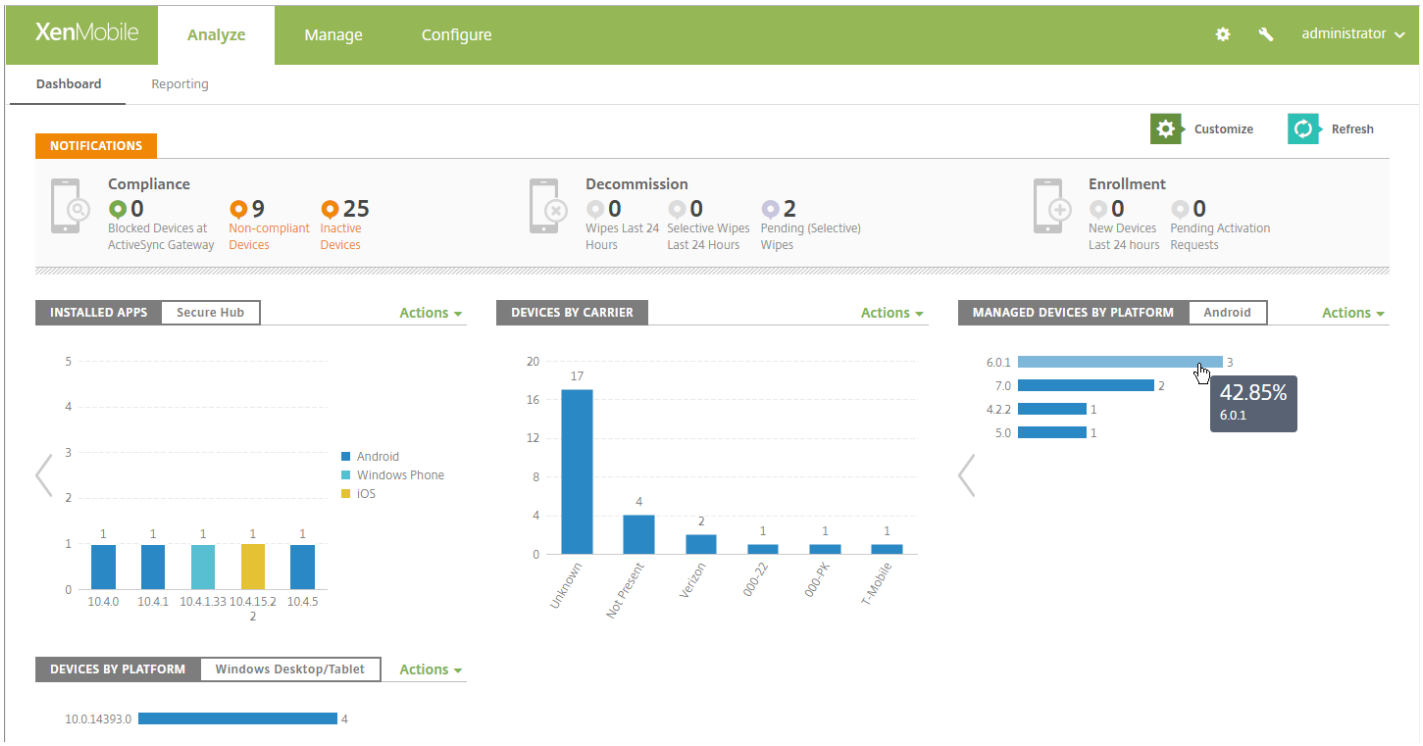
- Los gráficos muestran recuentos en orden descendente.
- Cada widget utiliza el tipo de gráfico más adaptado a la información ofrecida.
- Las acciones disponibles en cada widget aparecen en el menú **Actions**, que ahora incluye solo las acciones que se realizan con mayor frecuencia desde el panel de mandos:
  - **View Devices**. Abre la página **Manage > Devices**.
  - **Export as CSV**. Guarda los datos en un archivo CSV.



- La opción "Export as CSV" exporta la siguiente información de cada aplicación instalada:
  - Nombre
  - Versión
  - Propietario
  - Tamaño
  - ID
  - Hora de instalación
- En los siguientes gráficos, puede desglosar la información en dos niveles de detalle: si hace clic en una plataforma, aparecerá un gráfico de barras con recuentos de versión y, si hace clic en una versión, se abrirá la página **Manage > Devices**.
  Devices By Platform (Dispositivos agrupados por plataforma)
  Managed Devices By Platform (Dispositivos administrados agrupados por plataforma)
  Unmanaged Devices By Platform (Dispositivos no administrados agrupados por plataforma)
  Installed Apps (Aplicaciones instaladas)

- Para abrir la página **Manage > Devices**, puede hacer clic en cualquiera de los siguientes gráficos:
  Devices By Carrier (Dispositivos agrupados por operador)
  Devices By ActiveSync Gateway Status (Dispositivos agrupados por estado de ActiveSync Gateway)
  Devices By Ownership (Dispositivos agrupados por propietario)

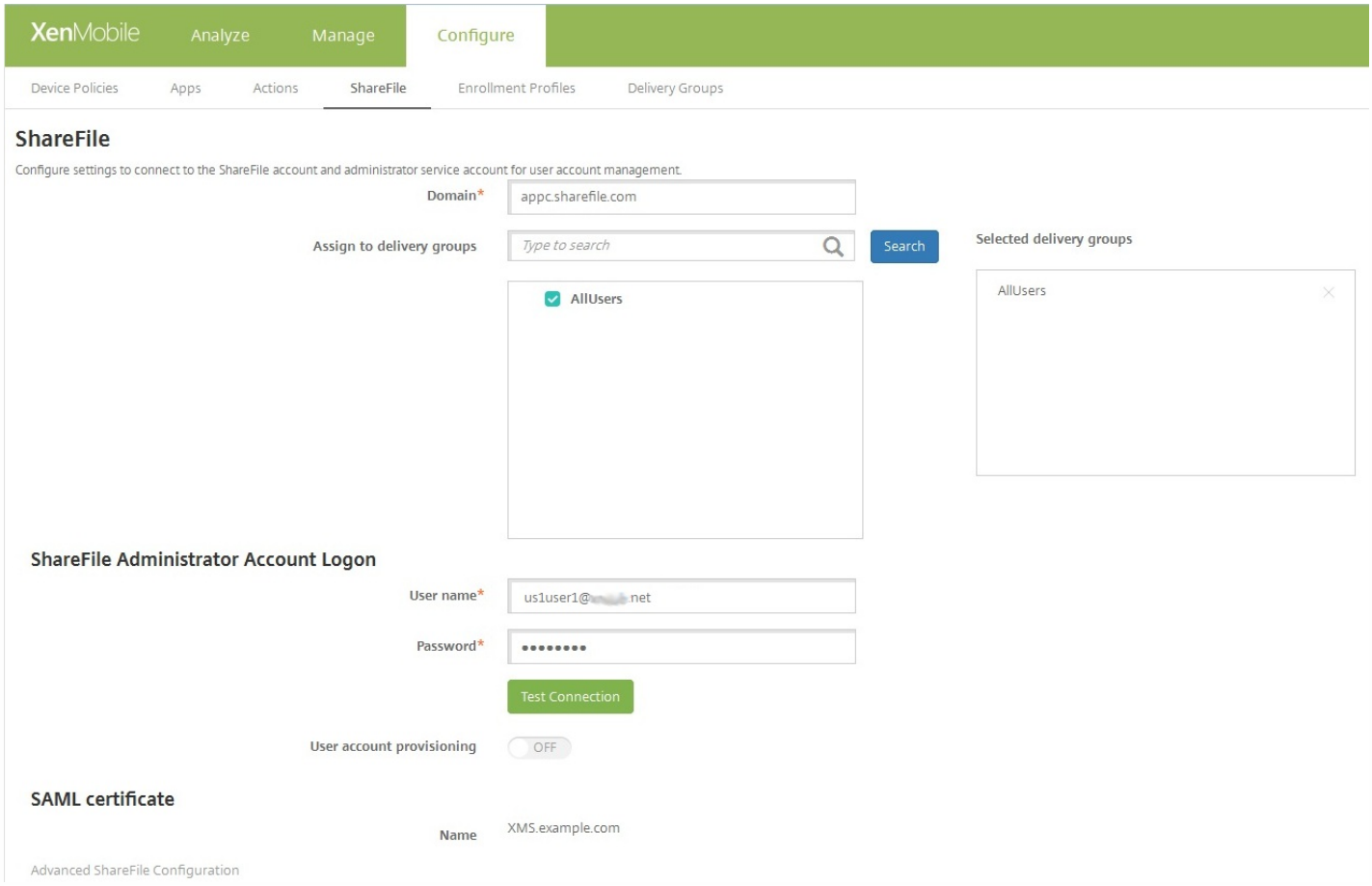
Android TouchDown License Status (Estado de la licencia TouchDown de Android)
Failed Delivery Group Deployments (Implementaciones fallidas de grupos de entrega)
Devices By Blocked Reason (Dispositivos agrupados por motivo de bloqueo)
VPP Apps License Usage (Uso de licencias por parte de aplicaciones provenientes de PCV)



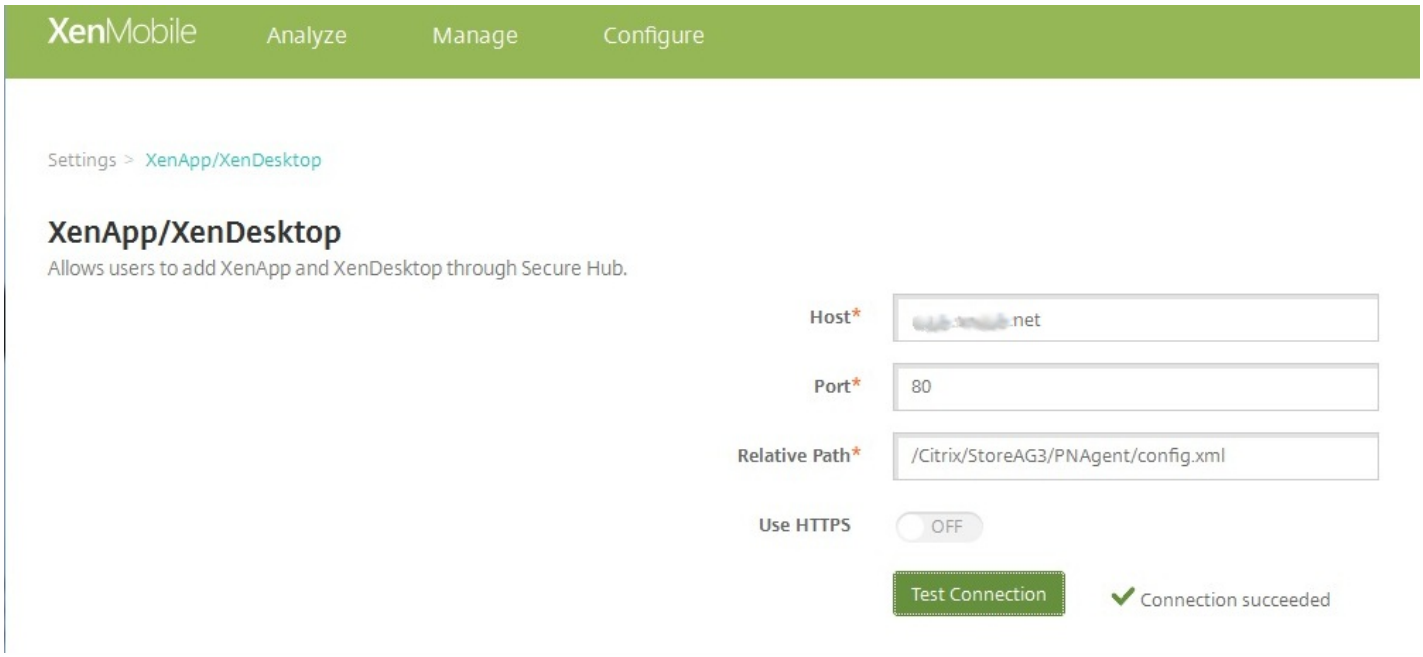
Botones para probar la conexión añadidos a la consola de XenMobile

Ahora, la consola de XenMobile incluye un botón **Test Connection** en estas páginas para probar la conexión:

- **Configure > ShareFile**. Puede usar el botón **Test Connection** para verificar que el nombre de usuario y la contraseña de la cuenta de administrador de ShareFile realizan la autenticación en la cuenta de ShareFile especificada.

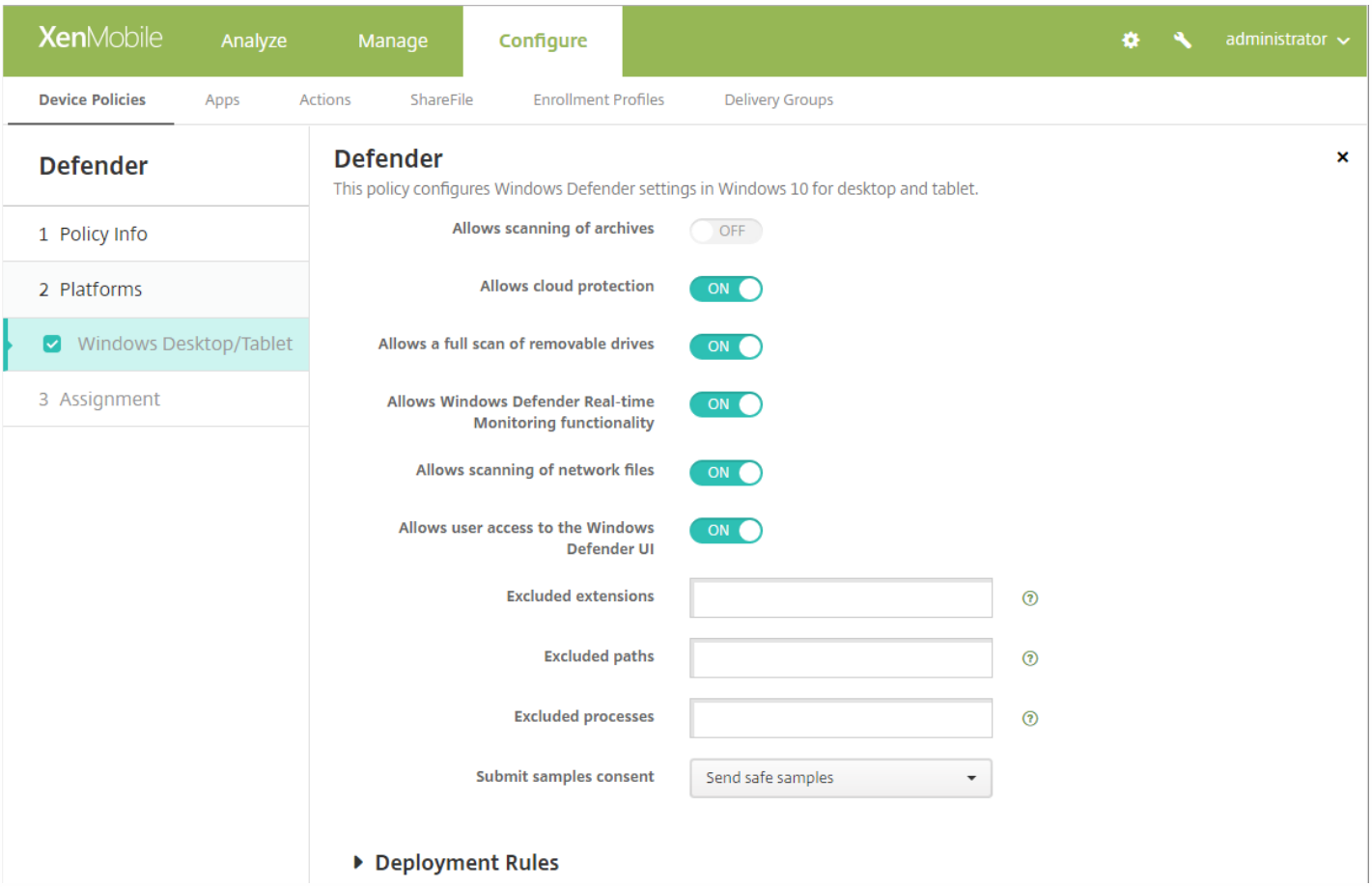


- **Settings > XenApp/XenDesktop**. Puede usar el botón **Test Connection** para verificar que XenMobile puede conectarse al servidor XenApp o XenDesktop especificado.



Directiva de Windows Defender para tabletas y escritorios Windows 10

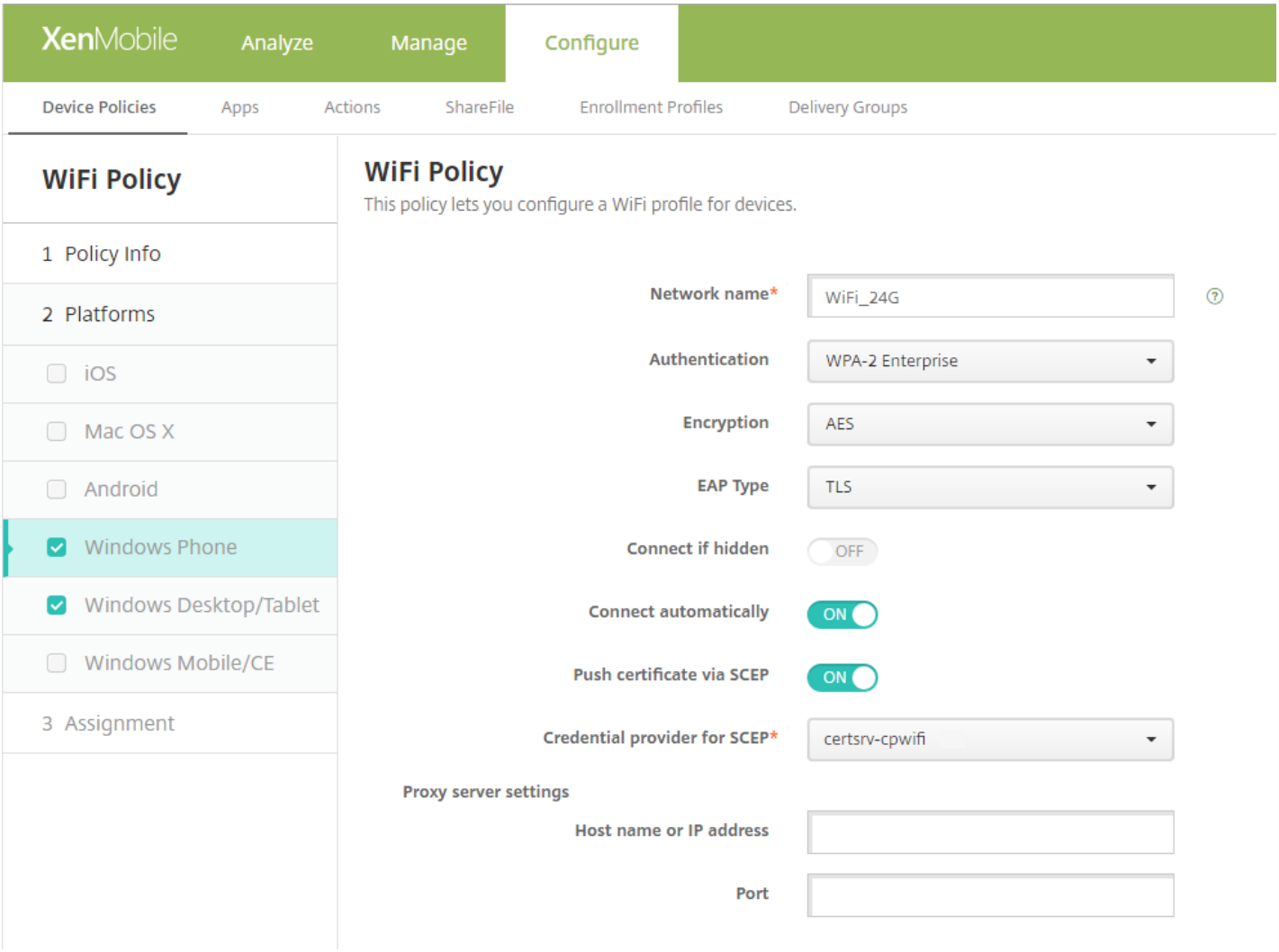
Windows Defender es una protección contra el software malicioso o malware incluida con Windows 10. En XenMobile, puede usar la directiva de dispositivo Defender para configurar la directiva de Microsoft Defender. Para agregar la directiva Defender, vaya a **Configure > Device Policies**, haga clic en **Add**, empiece a teclear **Defender** y, a continuación, haga clic en ese nombre en los resultados de búsqueda.



Para obtener más información, consulte Directiva de dispositivo para Defender.

Respaldo a la directiva Wi-Fi en dispositivos Windows 10

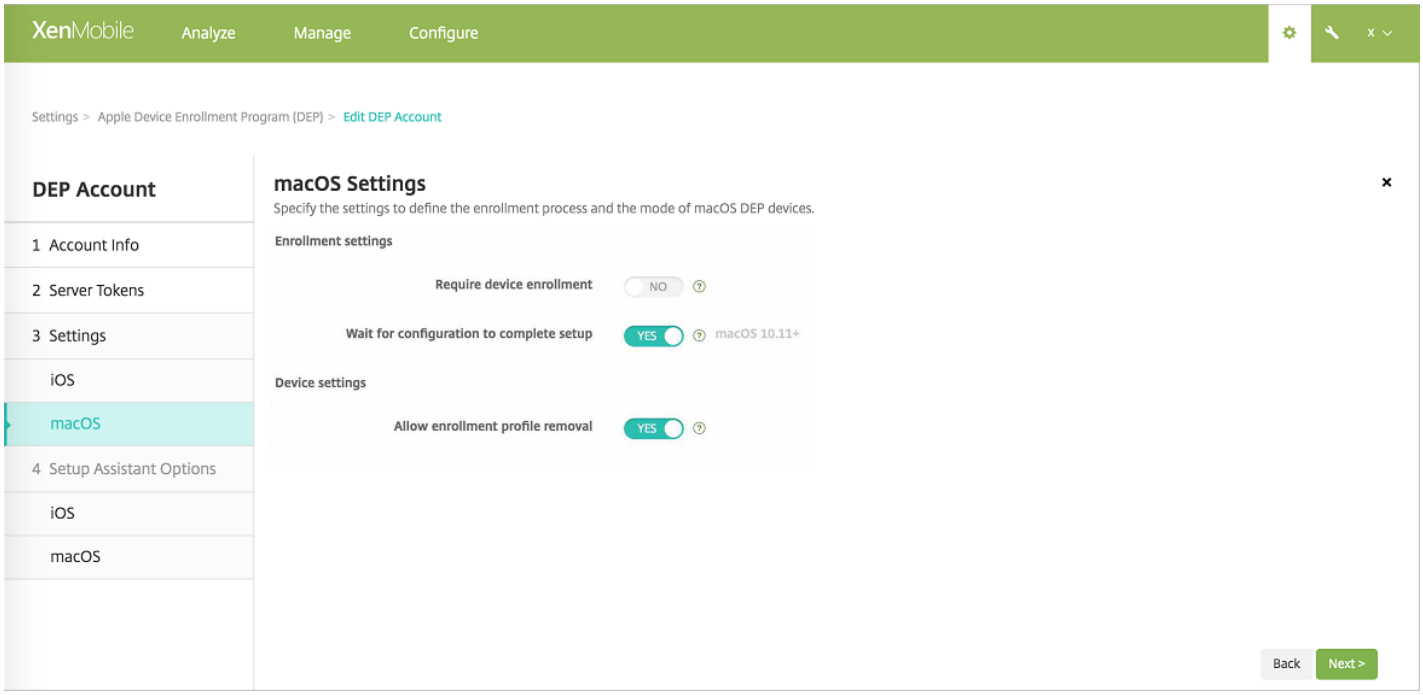
La directiva de redes Wi-Fi incluye ahora respaldo para Windows 10, lo que permite el uso de la autenticación por certificados de cliente para la red Wi-Fi. Para actualizar las directivas Wi-Fi, vaya a **Configure > Device Policies**.



Para obtener más información, consulte Directiva de redes Wi-Fi.

Inscripción en masa de dispositivos macOS

Ahora, la opción Apple Device Enrollment Program (DEP) de XenMobile admite dispositivos macOS que ejecutan OS X 10.10 o una versión posterior. Se sigue el mismo proceso que se describe en Inscripción en masa de dispositivos iOS y macOS. Si agrega una cuenta DEP desde **Settings > Apple Device Enrollment Program (DEP)**, las páginas **Settings** y **Setup Assistant Options** incluyen ahora una página para dispositivos macOS.

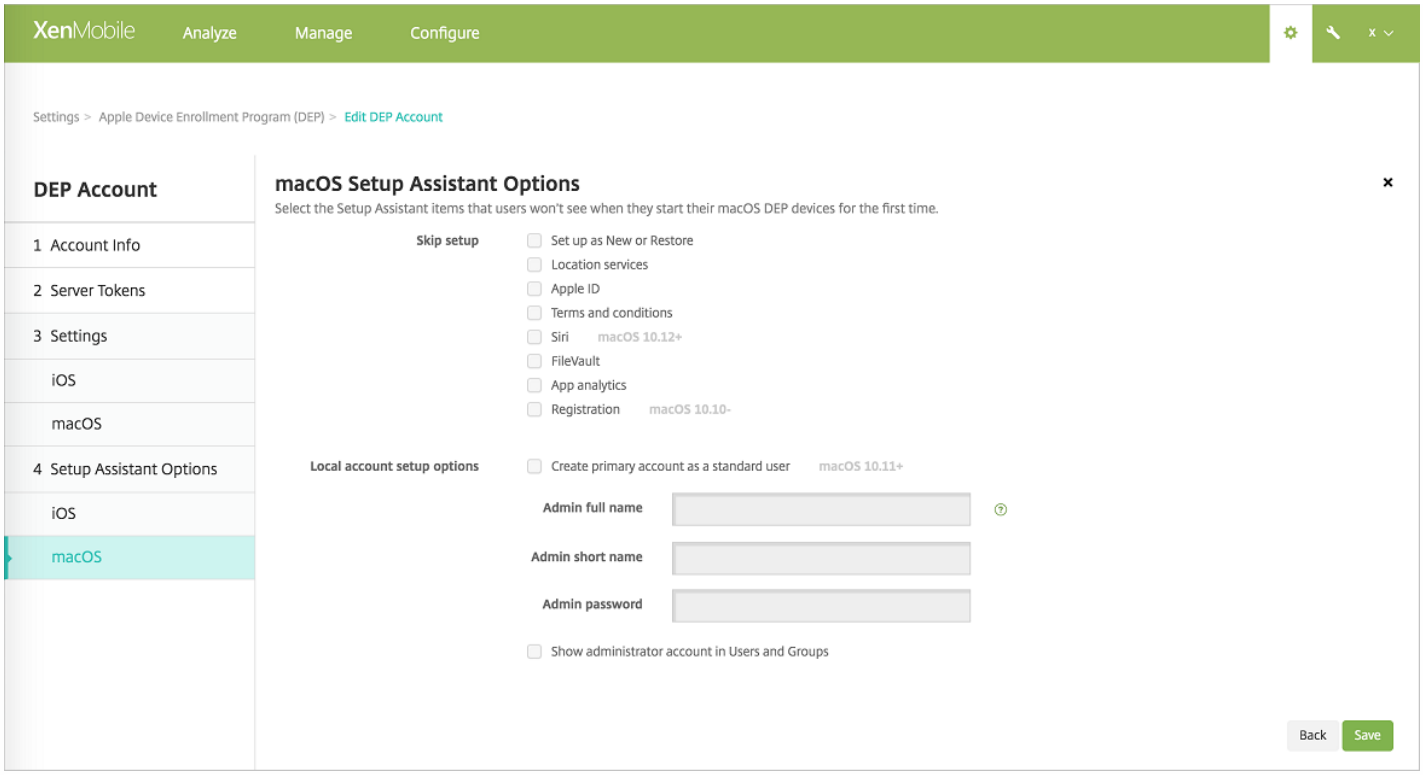


Parámetros de inscripción

- **Require device enrollment**. Puede requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Yes**.
- **Wait for configuration to complete setup**. Si habilita este parámetro, el dispositivo macOS no continúa con el Asistente de instalación hasta que el código de acceso a recursos MDM se implementa en el dispositivo. La implementación del código de acceso a recursos MDM tiene lugar antes de crearse la cuenta local. Esta configuración está disponible para macOS 10.11 y versiones posteriores. El valor predeterminado es **No**.

Parámetros del dispositivo

- **Allow enrollment profile removal**. Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. El valor predeterminado es **No**.



- **Set up as New or Restore**. Puede configurar el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o iTunes.
- **Location Services**. Puede configurar el servicio de localización en el dispositivo.
- **Apple ID**. Configurar una cuenta de ID de Apple para el dispositivo.
- **Terms and Conditions**. Puede requerir que el usuario acepte los términos y condiciones para usar el dispositivo.
- **Siri**. Usar o no usar Siri en el dispositivo.
- **FileVault**. Puede usar FileVault para cifrar el disco de arranque. XenMobile solo aplica el parámetro FileVault si el sistema tiene una cuenta de usuario local única registrada en iCloud.

  Puede usar la funcionalidad de cifrado de disco FileVault en macOS para proteger el volumen del sistema mediante el cifrado de su contenido. Consulte el artículo de asistencia de Apple: https://support.apple.com/en-us/HT204837. Si ejecuta el Asistente de configuración en un modelo reciente de portátil Mac donde FileVault está desactivado, es posible que se le solicite habilitar esta funcionalidad. Si el sistema cumple los siguientes requisitos, la solicitud aparece en los sistemas nuevos y en los sistemas actualizados a OS X 10.10 o 10.11:

  - El sistema tiene una cuenta de administrador local única
  - Esa cuenta está registrada en iCloud
- **App analytics**. Puede configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.
- **Registration**. Puede requerir a los usuarios que registren su dispositivo.

  La información de registro estaba disponible en OS X 10.9. El proceso de registro permitía enviar información de registro del sistema a Apple. Esta información asociaba su información de contacto con el hardware de Mac. Apple utilizaba principalmente la información para facilitar la tarea de la asistencia de Apple. Si había especificado anteriormente un ID de Apple, el Asistente de configuración enviaba opcionalmente la información de registro basada en su ID de cuenta de Apple. Si no había indicado ningún ID de Apple, podía escribir manualmente su información de contacto.

- En **Local account setup options**, puede especificar los parámetros para crear una cuenta de administrador, condición necesaria para macOS. XenMobile crea la cuenta a partir de la información especificada.

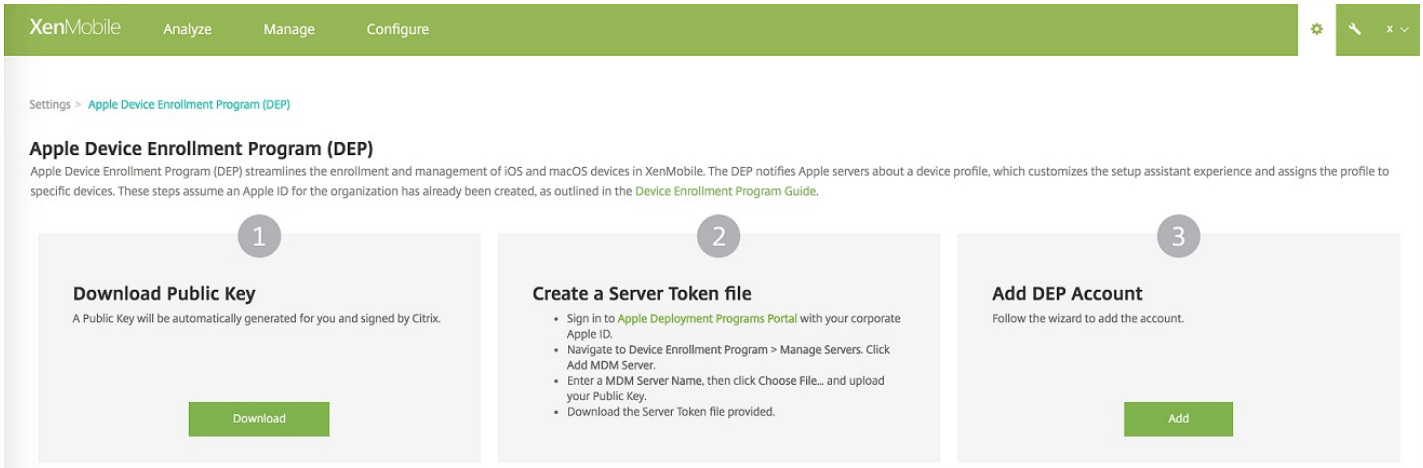
Respaldo para varias cuentas del Programa de inscripción de dispositivos de Apple para dispositivos iOS y macOS

Ahora se pueden definir varias cuentas del programa DEP (Programa de inscripción de dispositivos) de Apple. Esta característica permite utilizar parámetros distintos de inscripción, de dispositivo y opciones diferentes del Asistente de instalación. Puede especificar esos parámetros y opciones por país o departamento, entre otros. A continuación, asocie las cuentas DEP con distintas aplicaciones y directivas de dispositivo mediante reglas de implementación.

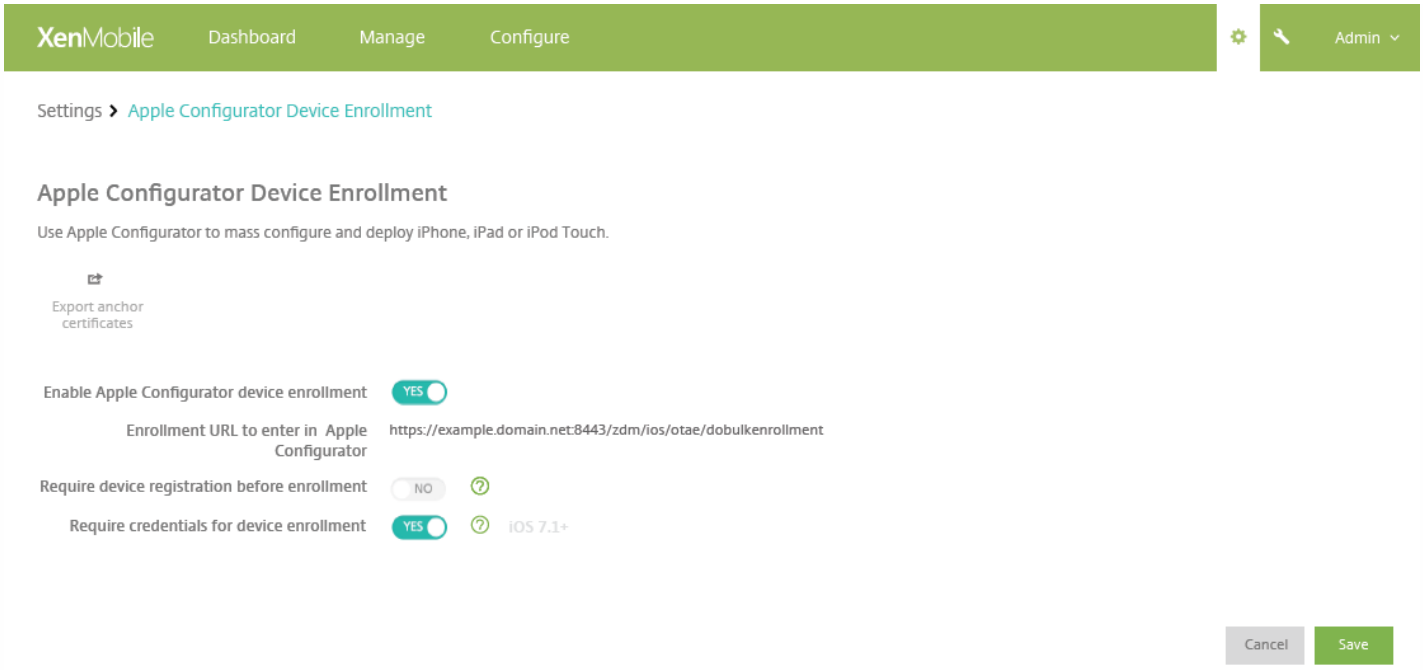
Por ejemplo, puede que le interese centralizar todas las cuentas DEP de diferentes países en el mismo servidor XenMobile. Así, podrá importar y supervisar todos los dispositivos DEP. Al personalizar los parámetros de inscripción por país o cualquier otra estructura, las directivas suministran la funcionalidad adecuada en toda la organización. Al personalizar opciones del Asistente de instalación por país o cualquier otra estructura, los usuarios de las dispositivos reciben la ayuda adecuada para la instalación.

Para admitir varias cuentas DEP, **Settings > iOS Bulk Enrollment** se sustituye por las páginas siguientes:

- **Settings > Apple Device Enrollment Program (DEP)**. Desde esta página, puede:
  - Crear cuentas DEP.
  - Configurar parámetros de inscripción, parámetros de dispositivo para macOS y iOS, así como opciones del Asistente de instalación referentes a cada cuenta.



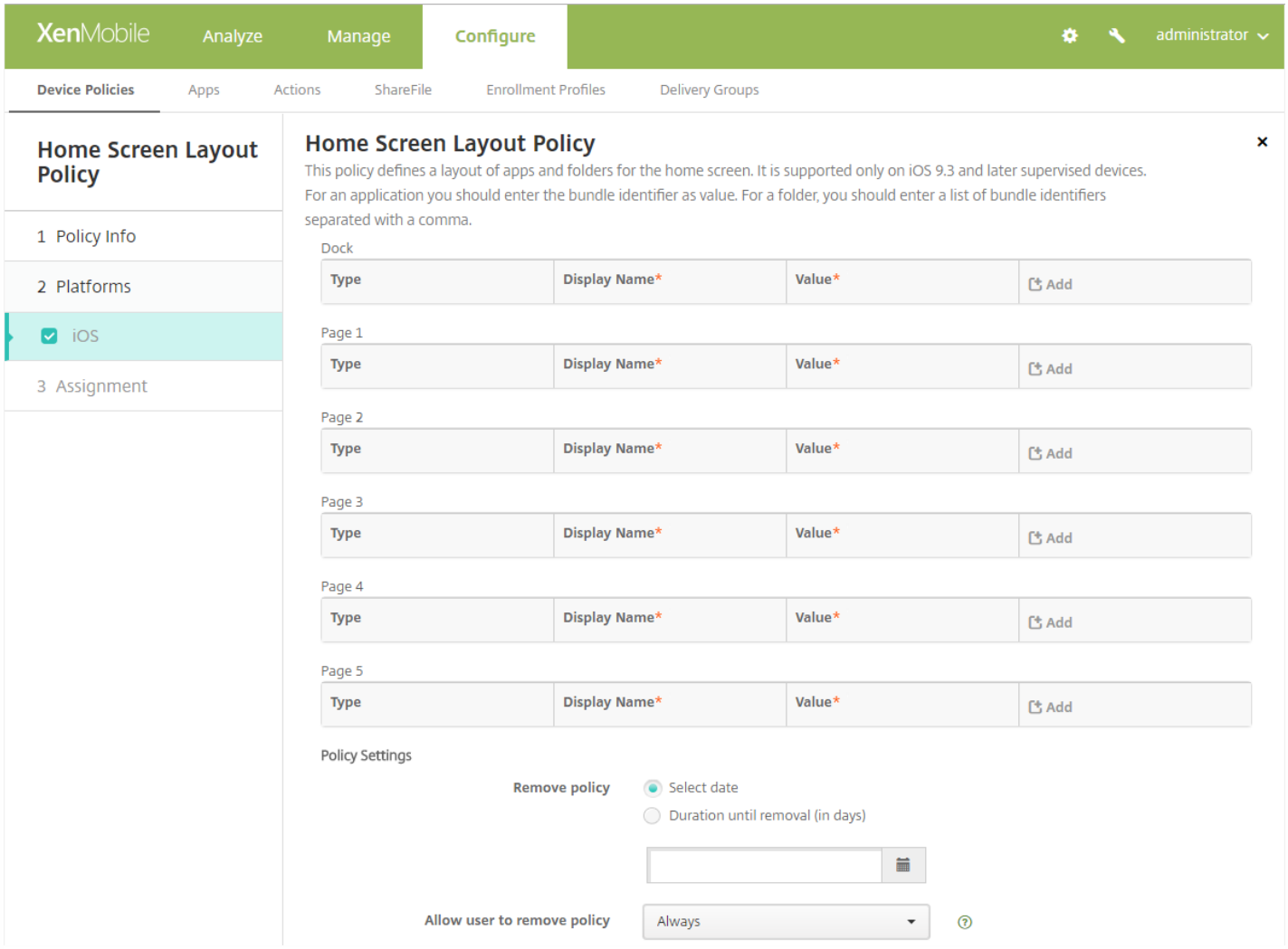
Settings > Apple Configurator Device Enrollment. Esta página se utiliza para configurar directivas y preparar dispositivos iOS y macOS.

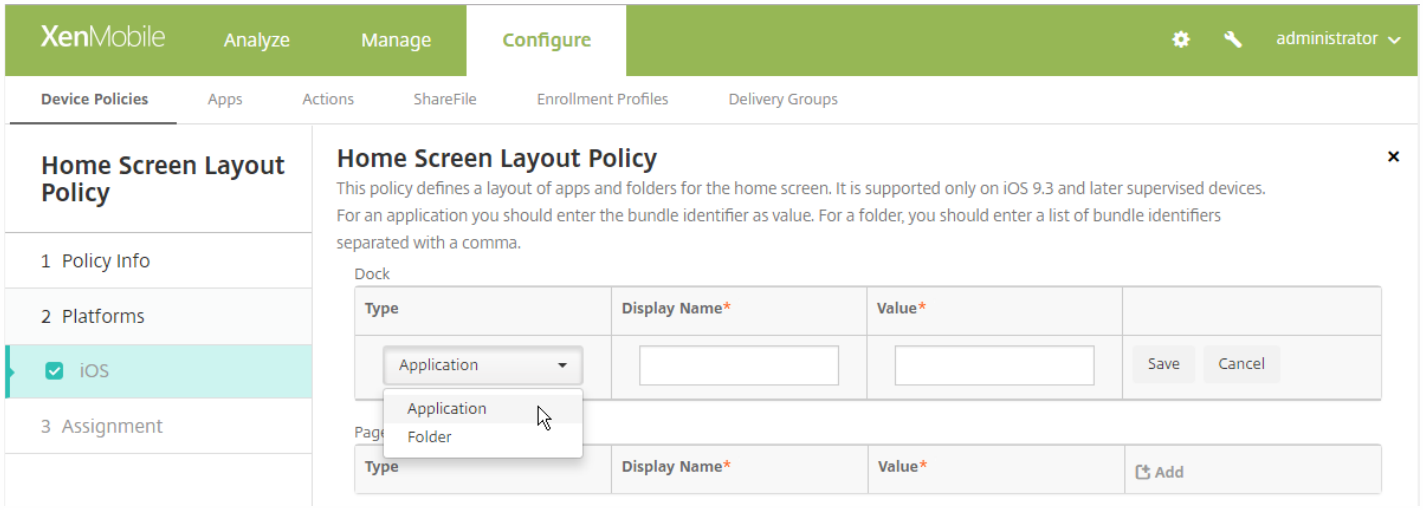


Para obtener más información, consulte Implementación en dispositivos iOS a través de Apple DEP.

Diseño de la pantalla de inicio de iOS

Puede usar la nueva directiva de dispositivo para el diseño de la pantalla de inicio con el objetivo de especificar la distribución de las aplicaciones y las carpetas en la pantalla de inicio de iOS. Esta directiva se admite en dispositivos supervisados con iOS 9.3 y versiones posteriores. Para agregar la directiva, vaya a **Configure > Device Policies**.





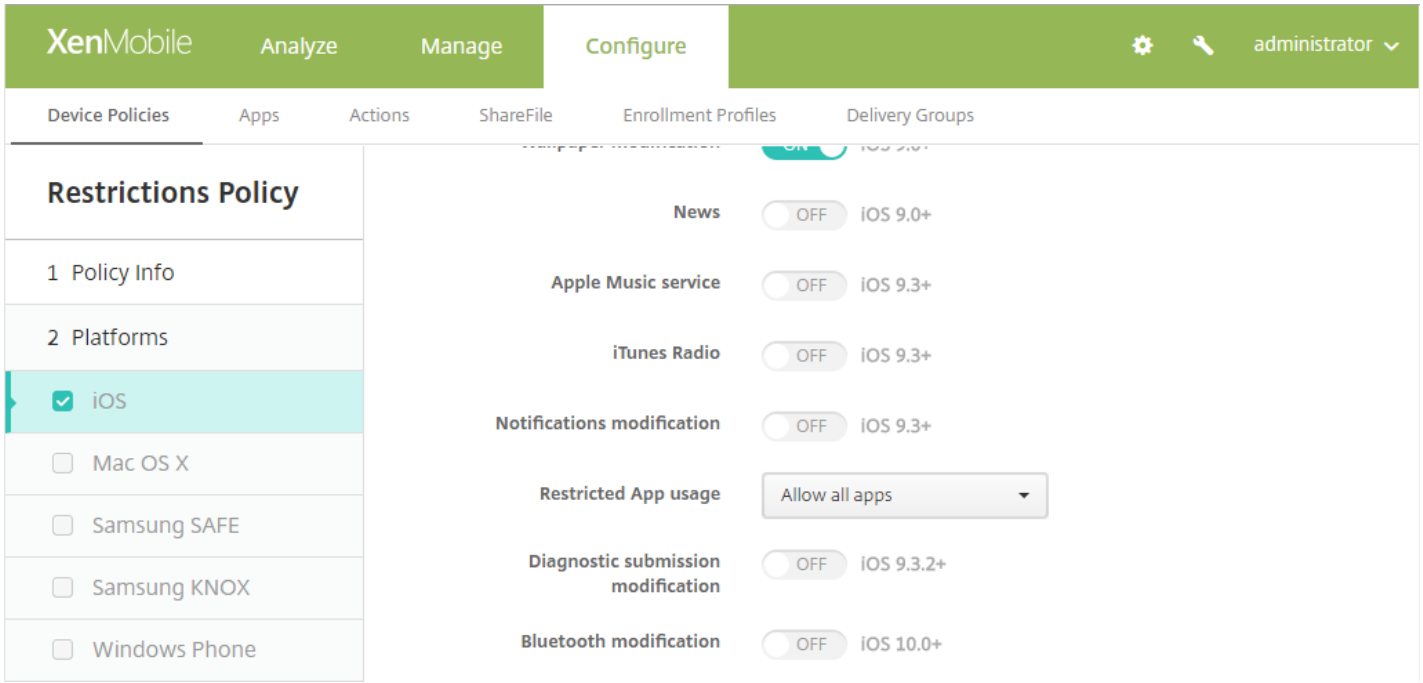
Para obtener más información, consulte Directiva de dispositivo para el diseño de la pantalla de inicio.

Más opciones de restricción de funcionalidades para

dispositivos iOS

Ahora, la directiva de restricciones de iOS incluye las siguientes opciones adicionales de restricción:

- **News**. Puede permitir que los usuarios usen la aplicación News (disponible en iOS 9.0 y versiones posteriores). Se aplica solo a los dispositivos supervisados.
- **Apple Music service**. Puede permitir que los usuarios usen el servicio Apple Music (disponible en iOS 9.3 y versiones posteriores). Si no desea permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico. Se aplica solo a los dispositivos supervisados.
- **iTunes Radio**. Puede permitir que los usuarios usen iTunes Radio (disponible en iOS 9.3 y versiones posteriores). Se aplica solo a los dispositivos supervisados.
- **Notifications modification**. Puede permitir que los usuarios modifiquen los parámetros de notificación (disponible en iOS 9.3 y versiones posteriores). Se aplica solo a los dispositivos supervisados.
- **Restricted App usage**. Puede permitir que los usuarios usen todas las aplicaciones o solo las aplicaciones permitidas o prohibidas por ID de paquete (disponible en iOS 9.3 y versiones posteriores). Se aplica solo a los dispositivos supervisados.
- **Diagnostic submission modification**. Puede permitir que los usuarios modifiquen los parámetros de envío de información de diagnóstico y análisis de aplicaciones desde el panel Diagnóstico y uso en los Ajustes (disponible en iOS 9.3.2 y versiones posteriores). Se aplica solo a los dispositivos supervisados.
- **Bluetooth modification**. Puede permitir que los usuarios modifiquen los parámetros de Bluetooth (disponible en iOS 10.0 y versiones posteriores). Se aplica solo a los dispositivos supervisados.

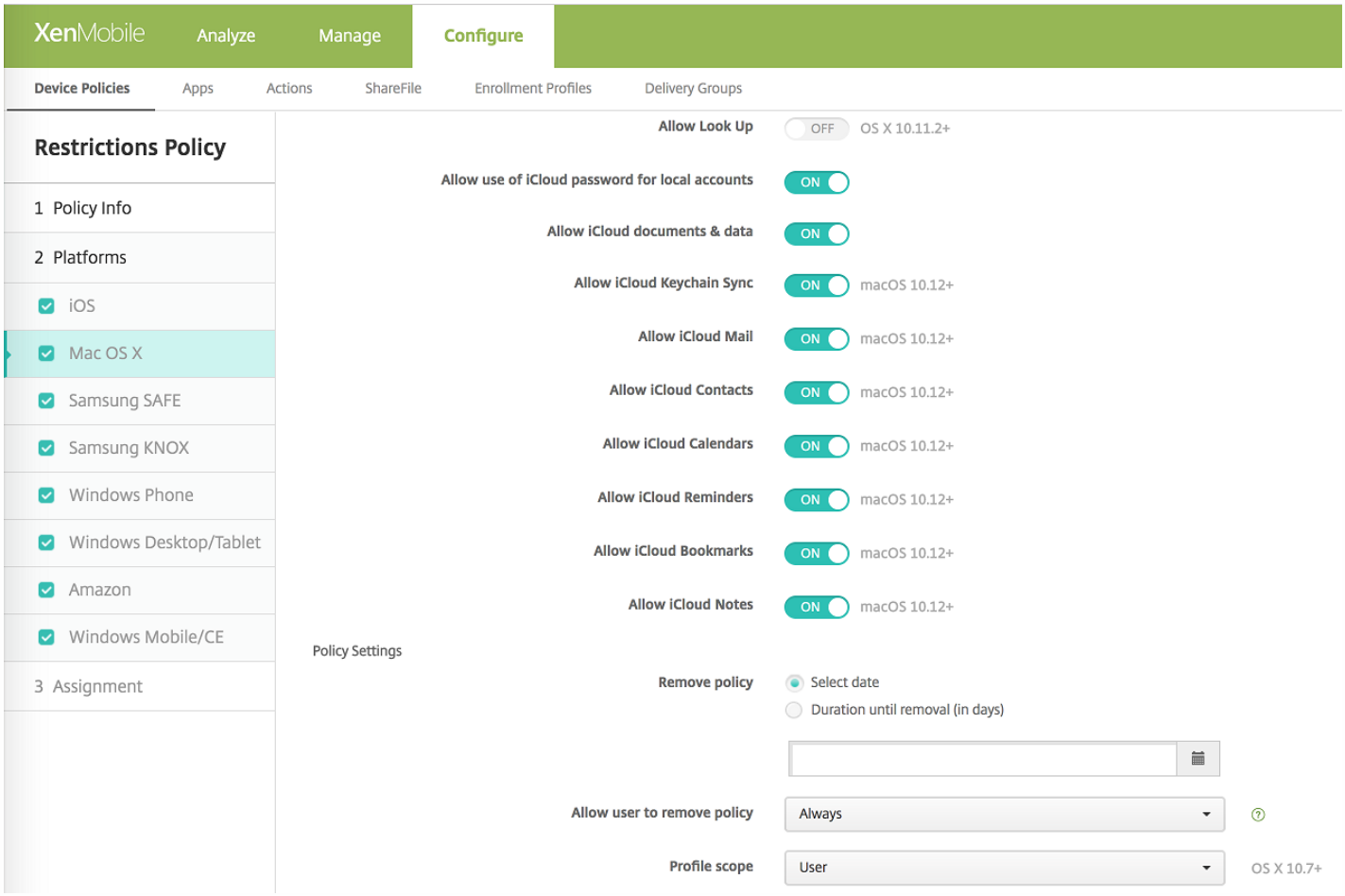


Más opciones de restricción de funcionalidades para dispositivos macOS

Se han añadido las siguientes opciones de restricción a la directiva de restricciones para macOS 10.12 y versiones

posteriores: De forma predeterminada, XenMobile permite estas funcionalidades.

- Allow Apple Music. Si no quiere permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico. Se aplica solo a los dispositivos supervisados.
- Allow iCloud Keychain Sync
- Allow iCloud Mail
- Allow iCloud Contacts
- Allow iCloud Calendars
- Allow iCloud Reminders
- Allow iCloud Bookmarks
- Allow iCloud Notes



Respaldo para el Modo perdido gestionado en dispositivos iOS 9.3

En iOS 9.3 o versiones posteriores, puede usar la administración MDM de Apple para colocar un dispositivo supervisado en el Modo perdido gestionado, un modo dedicado. Puede usar el Modo perdido gestionado para bloquear o localizar dispositivos supervisados perdidos o robados.

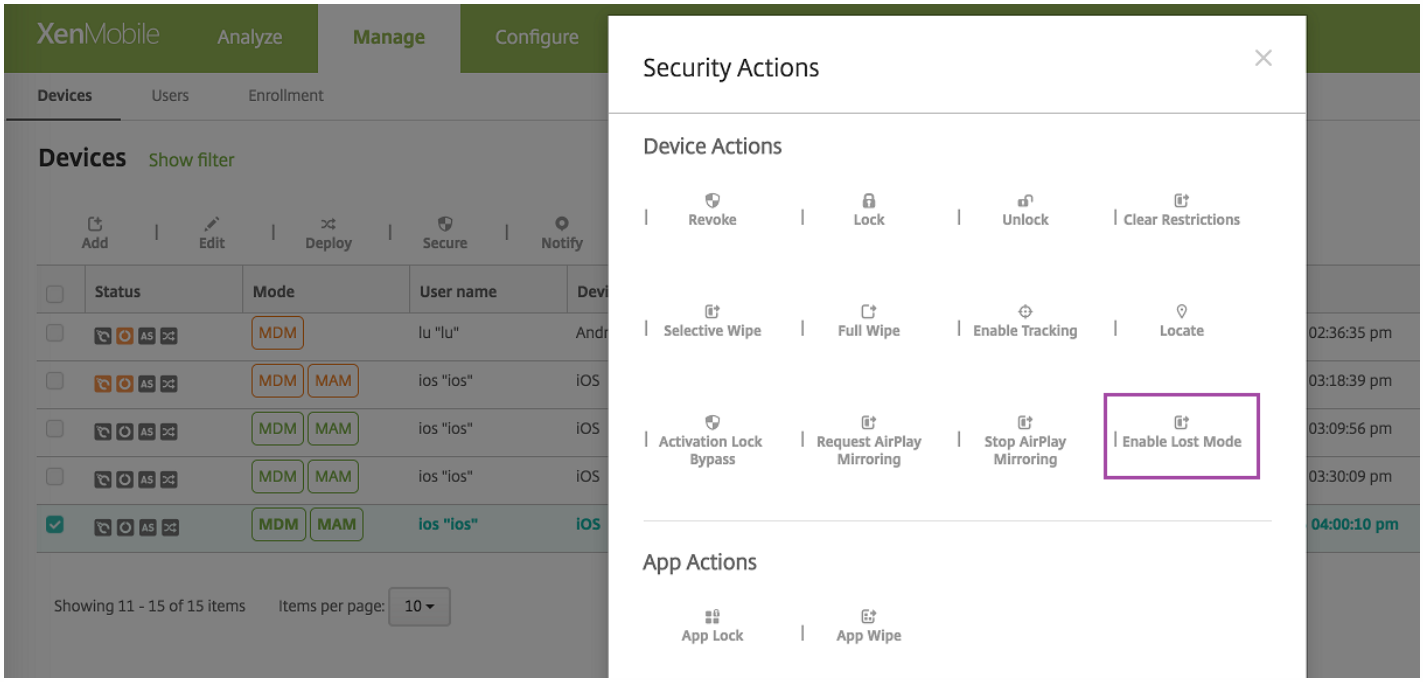
Ahora, XenMobile tiene una propiedad de dispositivo llamada Lost Mode (Modo perdido). A diferencia del Modo perdido

gestionado de Apple, el Modo perdido de XenMobile no requiere que el usuario configure Buscar mi iPhone o iPad ni habilite los servicios de localización geográfica de Citrix Secure Hub para permitir la localización de su dispositivo.

La funcionalidad Modo perdido de XenMobile es similar a la funcionalidad Bloqueo de dispositivo de XenMobile. Sin embargo, en el Modo perdido de XenMobile, solo XenMobile Server puede desbloquear el dispositivo. Al usar el Bloqueo de dispositivo, los usuarios pueden desbloquear el dispositivo directamente mediante un código PIN suministrado por su administrador.

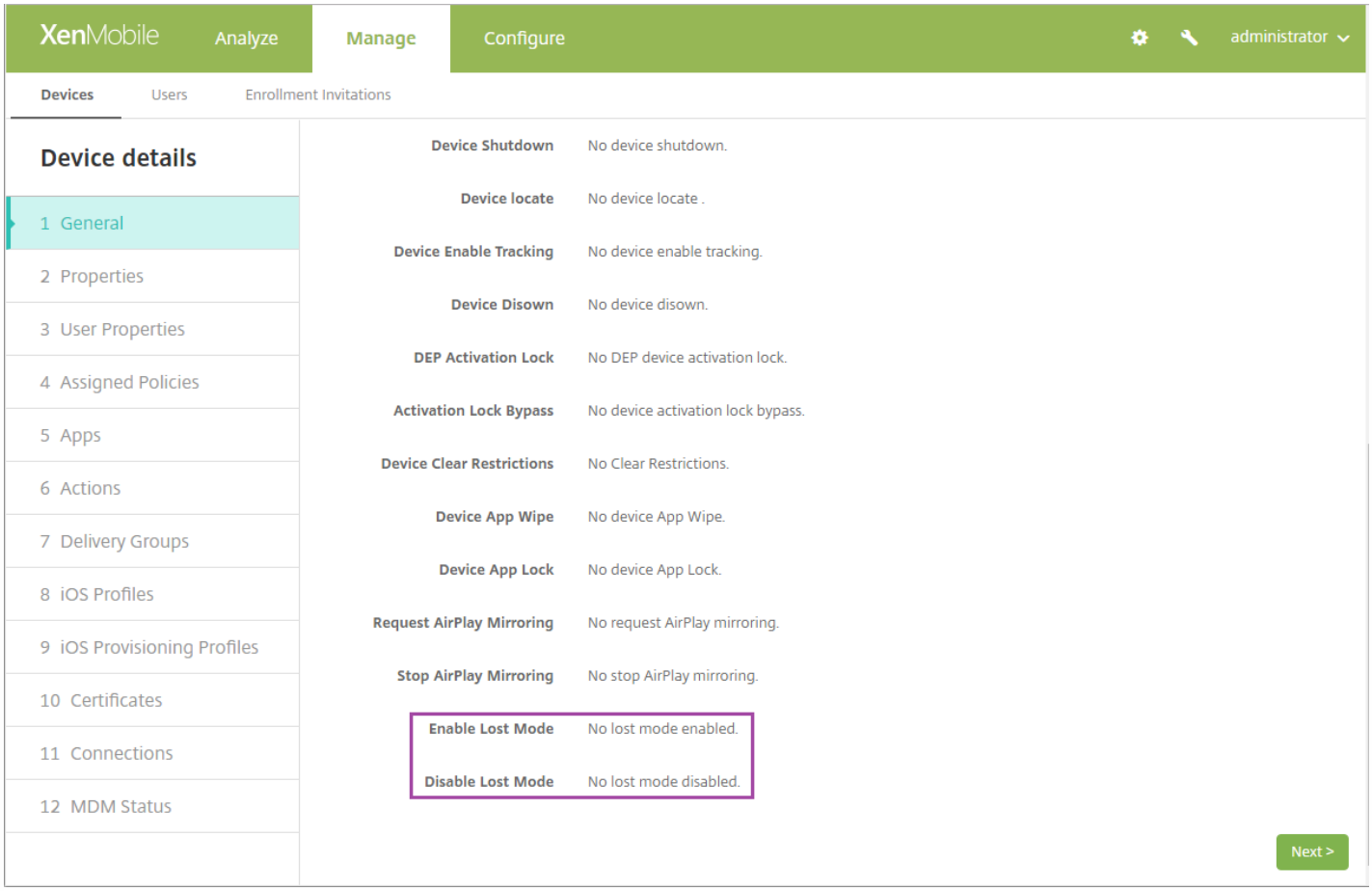
> ## Nota
>
> En iOS 7 y versiones posteriores, también puede usar la funcionalidad de bloqueo de dispositivo propia de iOS para bloquear de forma remota dispositivos supervisados o no supervisados que se hayan perdido o hayan sido robados. Apple recomienda evitar el uso de la funcionalidad de bloqueo de dispositivo de iOS para otros fines.

Para habilitar o inhabilitar el Modo perdido: vaya a **Manage > Devices**, elija un dispositivo iOS supervisado y haga clic en **Secure**. A continuación, haga clic en **Enable Lost Mode** o **Disable Lost Mode**.

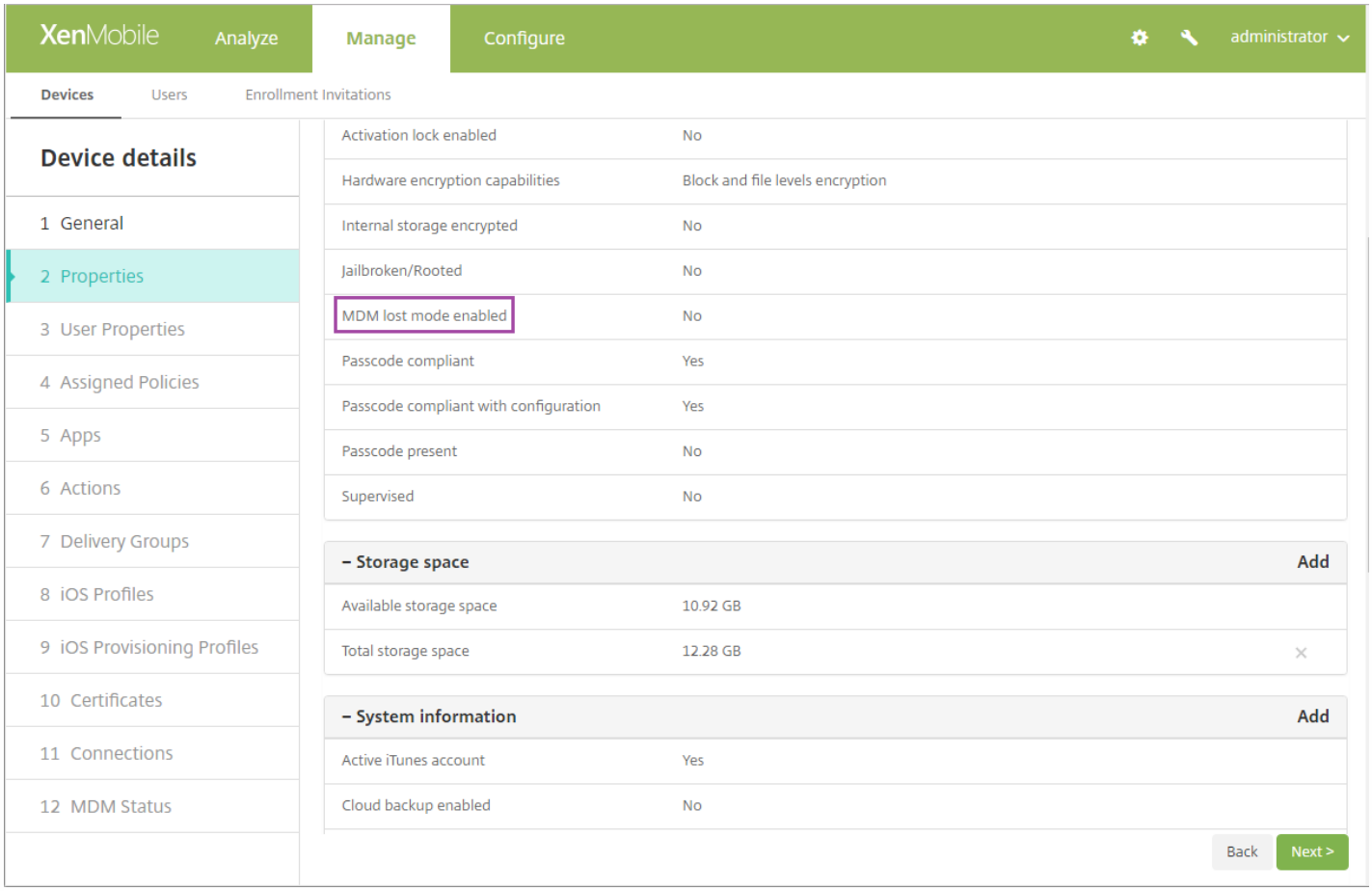


Para comprobar el estado Modo perdido, utilice cualquiera de los siguientes métodos:

- En la ventana **Security Actions**, compruebe si el botón es **Disable Lost Mode**.
- Desde **Manage > Devices**, en la ficha **General**, en **Security**, consulte la información de Enable Lost Mode o Disable Lost Mode action.



- Desde **Manage > Devices**, en la ficha **Properties**, consulte el valor de la opción **MDM lost mode enabled**.



Si habilita el Modo perdido de XenMobile en un dispositivo iOS, la consola de XenMobile cambia de este modo:

- En **Configure > Actions**, la lista **Actions** no incluye las siguientes acciones automatizadas: **Revoke the device**, **Selectively wipe the device** ni **Completely wipe the device**.
- En **Manage > Devices**, la lista **Security Actions** ya no incluye las acciones de dispositivo **Revoke** ni **Selective Wipe**. En cambio, la acción de seguridad para llevar a cabo un borrado completo (la acción **Full Wipe**), seguirá estando disponible, si fuera necesario.

En caso de iPads que ejecutan iOS 7 y versiones posteriores: iOS añade las palabras "iPad perdido" a lo que escriba en el campo **Message** del cuadro de diálogo **Security Actions**. En caso de iPhones que ejecutan iOS 7 y versiones posteriores: Si deja el campo **Message** vacío y proporciona un número de teléfono, Apple mostrará un mensaje del tipo "Llamar al propietario" en la pantalla de bloqueo del dispositivo.

SmartAccess para aplicaciones HDX

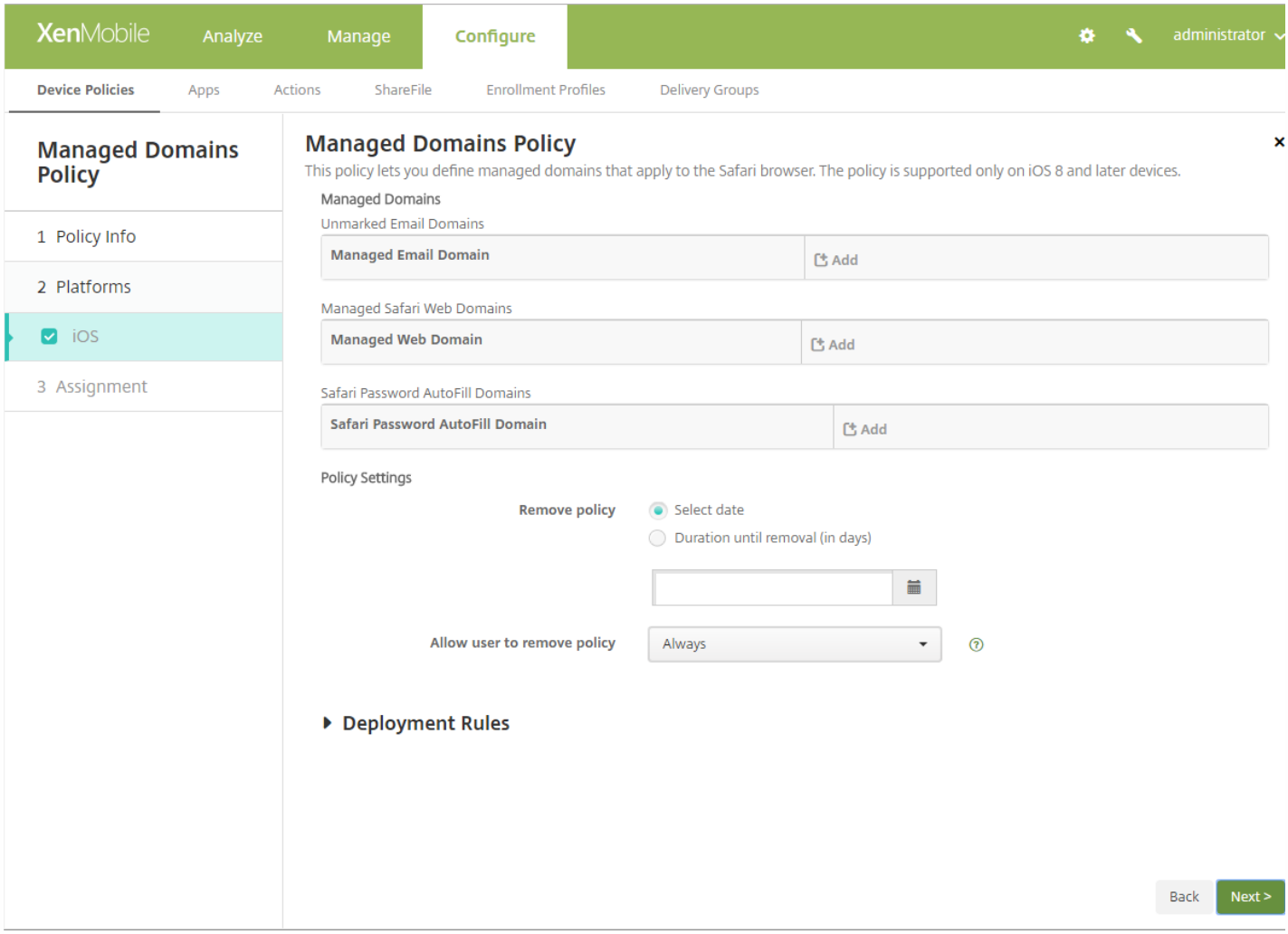
La funcionalidad SmartAccess permite controlar el acceso a las aplicaciones HDX en función de las propiedades del dispositivo, las propiedades del usuario de un dispositivo o las aplicaciones instaladas en él. Puede controlar el acceso mediante acciones automatizadas que marcan el dispositivo como no conforme cuando se dan ciertas condiciones. Para utilizar SmartAccess, configure las aplicaciones HDX de XenApp y XenDesktop con una directiva de SmartAccess que deniega el acceso a los dispositivos no conformes. XenMobile comunica el estado del dispositivo a StoreFront por medio de una etiqueta firmada y cifrada. StoreFront permite o deniega el acceso en función de la directiva de control del acceso de la

aplicación.

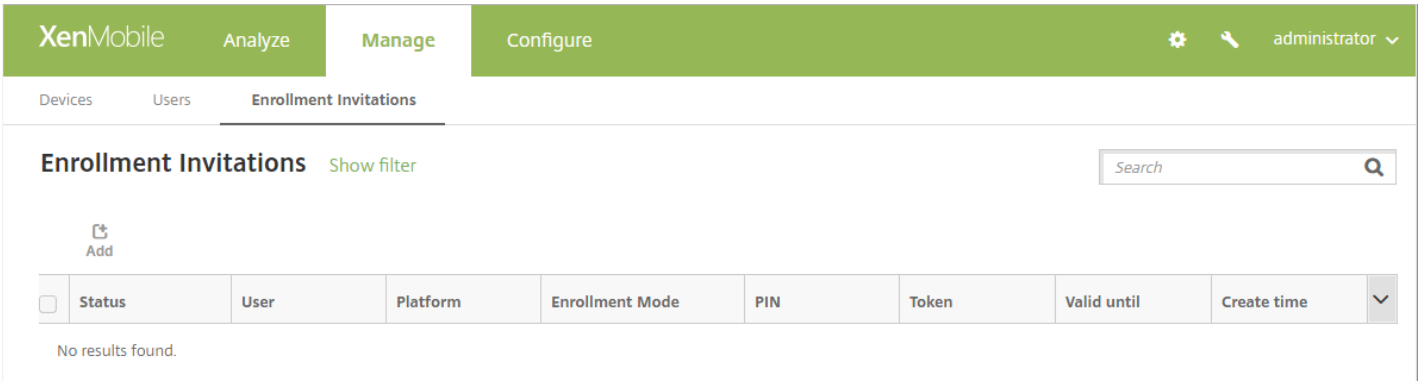
Para obtener más información, consulte Acceso SmartAccess a aplicaciones HDX.

Otras mejoras

- **Más idiomas respaldados**. La consola de XenMobile está ahora disponible en japonés. Secure Hub está ahora disponible en árabe y en ruso.
- **Directiva de redes Wi-Fi**. La directiva de redes Wi-Fi incluye ahora respaldo para Windows 10, lo que permite el uso de la autenticación por certificados de cliente para la red Wi-Fi. Para actualizar las directivas Wi-Fi, vaya a **Configure > Device Policies**.
- **Botón Test Connection para probar la conexión añadido a la página PKI Entities**. Cuando se agrega una entidad de Servicios de certificados de Microsoft, ahora se puede probar la conexión para asegurarse de que es posible contactar con el servidor.
- **Estabilidad mejorada** por optimizaciones de base de datos.
- **Cambios en las horas de últimos accesos para dispositivos de solo MAM**. Antes, las estadísticas de dispositivos registrados en modo MAM utilizaban la hora de registro del dispositivo como la hora del último acceso. Ahora, XenMobile utiliza la hora más reciente de la última autenticación en línea o la última actividad como la hora del último acceso. Ahora, la página **Manage > Devices** incluye la hora del último acceso.
- **Ahora, la directiva de dominios administrados incluye dominios de rellenado automático de contraseñas en Safari**. En caso de dispositivos supervisados con iOS 9.3 y versiones posteriores, ahora puede especificar las direcciones URL desde las que los usuarios pueden guardar contraseñas en Safari. Para ello, vaya a **Configure > Device Policies**. A continuación, agregue o abra **Managed Domains Policy** y complete la configuración de **Safari Password AutoFill Domain**.



- **TLS 1.2 requerido para Secure Hub**. Apple ahora requiere ATS (App Transport Security) para todas las aplicaciones que se envían a la App Store de Apple. ATS usa la versión del protocolo Transport Layer Security (TLS) 1.2, que ahora es el protocolo de servidor necesarios para Secure Hub.
- **Mejoras en la interfaz de la consola para administrar invitaciones de inscripción**. Para aclarar la terminología, la consola de XenMobile presenta las siguientes mejoras:
  - La página **Manage > Enrollments** ha cambiado a **Manage > Enrollment Invitations**.
  - La columna **Enrollment Status** ha cambiado a **Status**. Como antes, esa columna contiene el estado de la invitación a la inscripción, no el estado de la inscripción en sí.
  - Ahora, la terminología utilizada cuando se administra una invitación a la inscripción coincide con la terminología utilizada al crear la invitación. Se han cambiado estas etiquetas:
    La columna **Type** ahora es **Platform**.
    La columna **Mode** ahora es **Enrollment Mode**.
    En el filtro, **Invitations Status** ahora es **Status**.
    En el filtro, **Invitations Mode** ahora es **Enrollment Mode**.
  - Las etiquetas de valor en la columna **Mode** ahora son las mismas que las utilizadas a la hora de crear una invitación. Por ejemplo, la columna **Mode** ahora muestra "User name" en lugar de "classic".

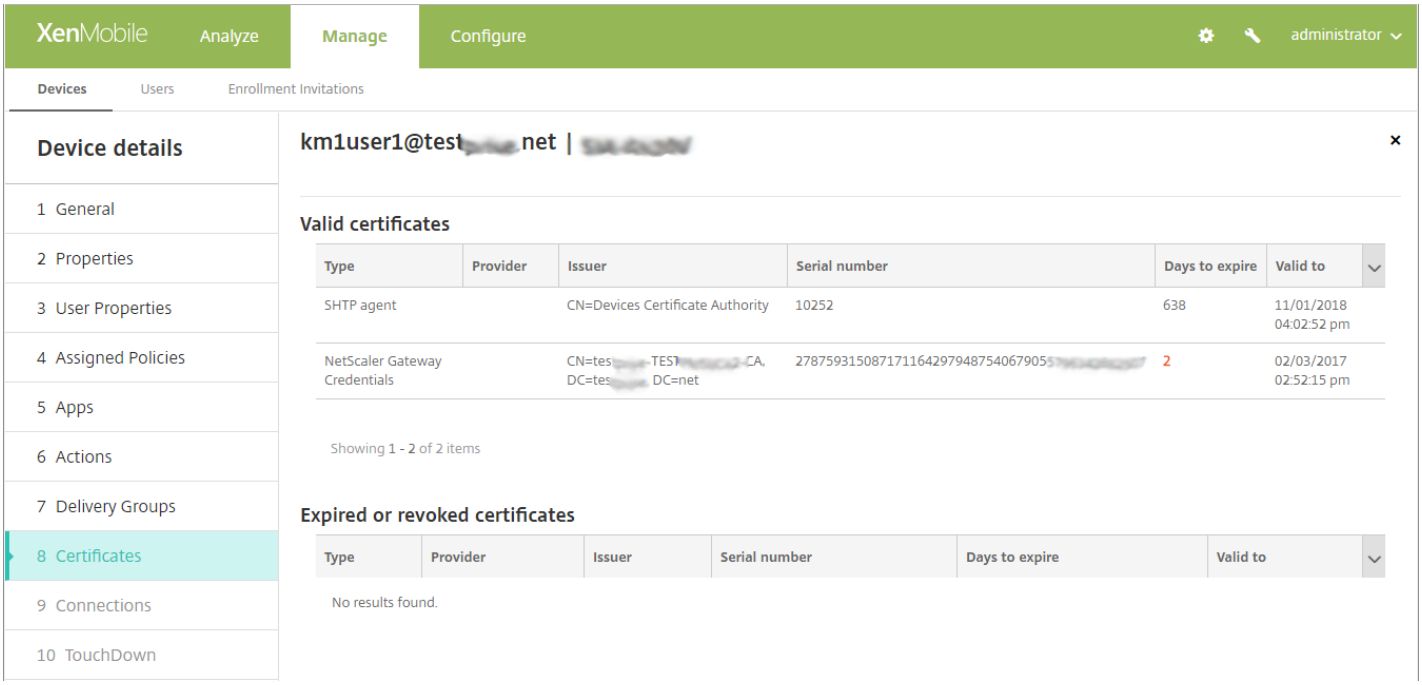


- **Nueva propiedad de servidor para establecer el intervalo mínimo del punto de referencia para licencias PCV**. Periódicamente, XenMobile vuelve a importar licencias del Programa de Compras por Volumen (PCV) desde Apple para que estas reflejen todos los cambios. Se trata de cambios como, por ejemplo, la eliminación manual de una aplicación importada del programa VPP. De forma predeterminada, XenMobile actualiza el punto de referencia para licencias PCV cada 720 minutos como mínimo. Ahora, se puede cambiar el intervalo del punto de referencia desde la nueva propiedad de servidor **VPP baseline interval** (vpp.baseline).

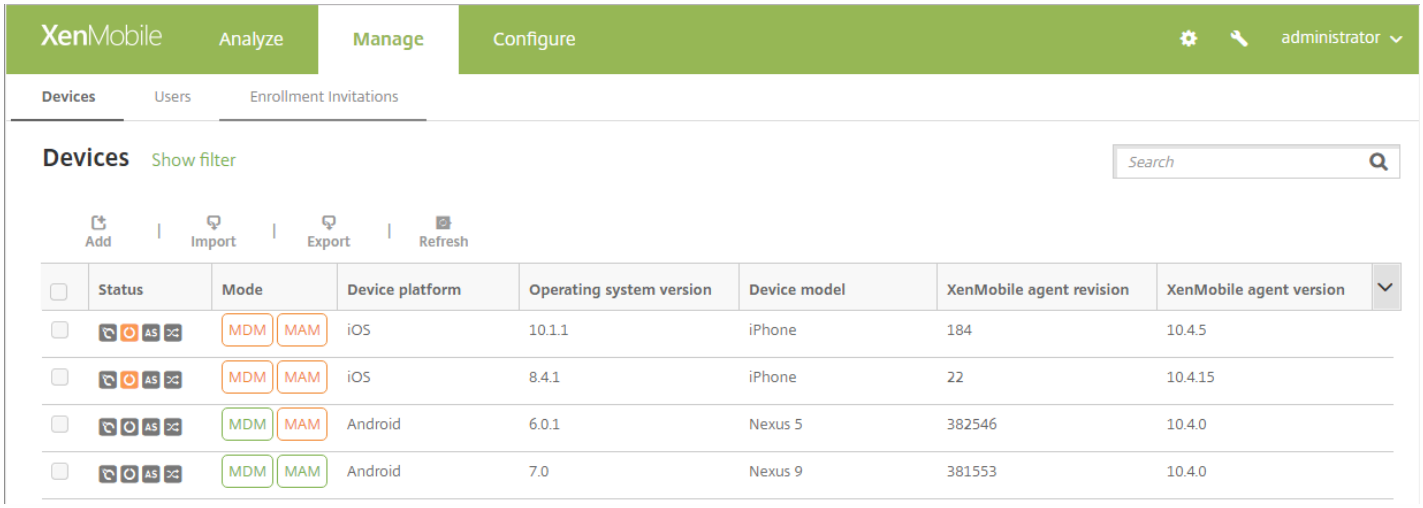
  Si tiene más de 50.000 licencias PCV instaladas, Citrix recomienda aumentar el intervalo del punto de referencia para reducir la frecuencia de la importación de licencias y el consumo de recursos que eso conlleva. Si espera cambios frecuentes en las licencias PCV por parte de Apple, Citrix recomienda reducir el valor para mantener XenMobile actualizado con los cambios. El intervalo mínimo entre dos puntos de referencia es de 60 minutos.

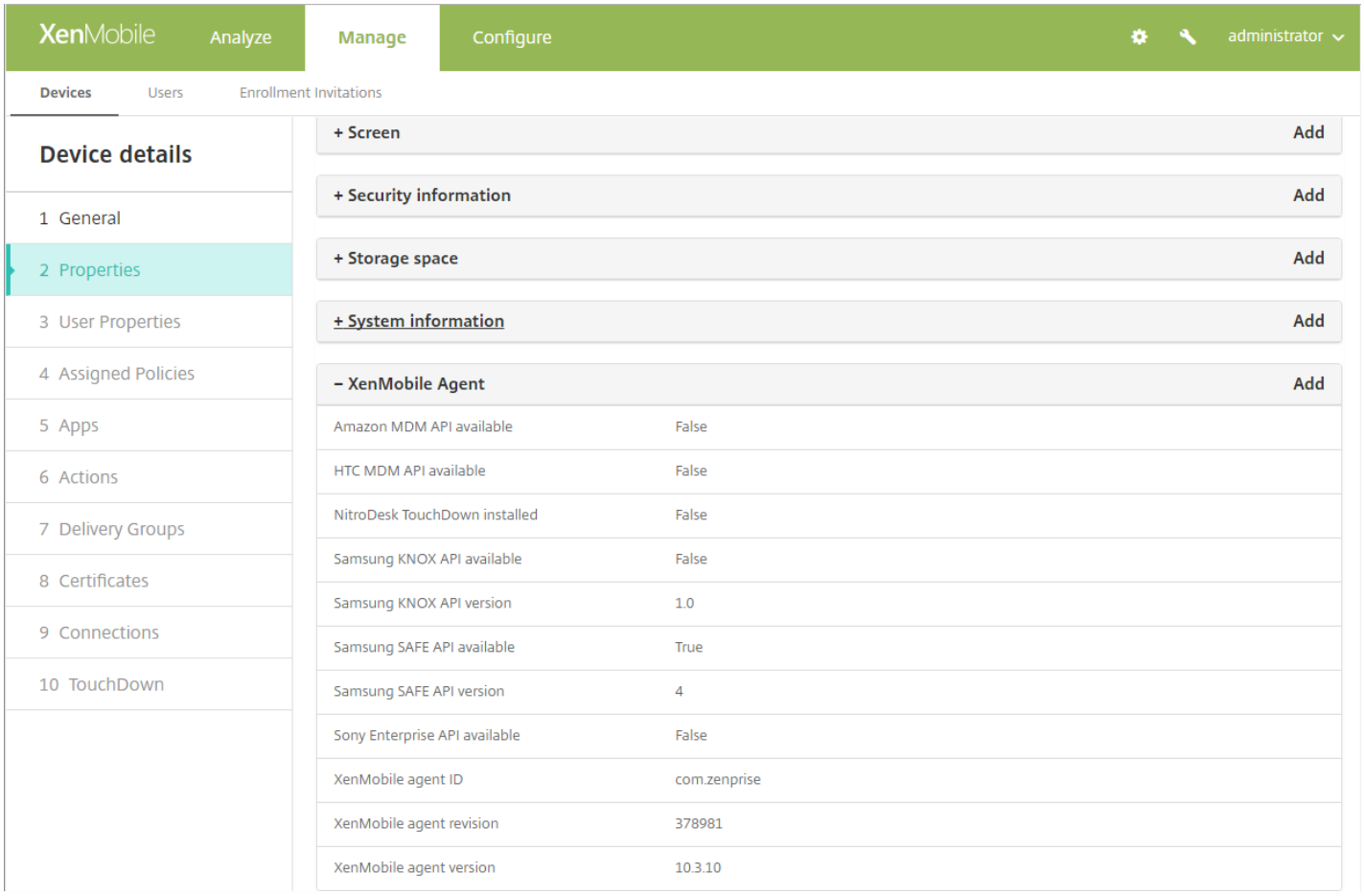
  Además, XenMobile lleva a cabo una importación delta cada 60 minutos, para capturar los cambios realizados desde la última importación. Establecer el intervalo mínimo del punto de referencia de PCV a 60 minutos puede demorar el intervalo entre los puntos de referencia hasta 119 minutos.

- Ahora, la ficha **Certificates** de **Manage > Devices** muestra también la cantidad de días que quedan antes de que el certificado de NetScaler Gateway caduque.

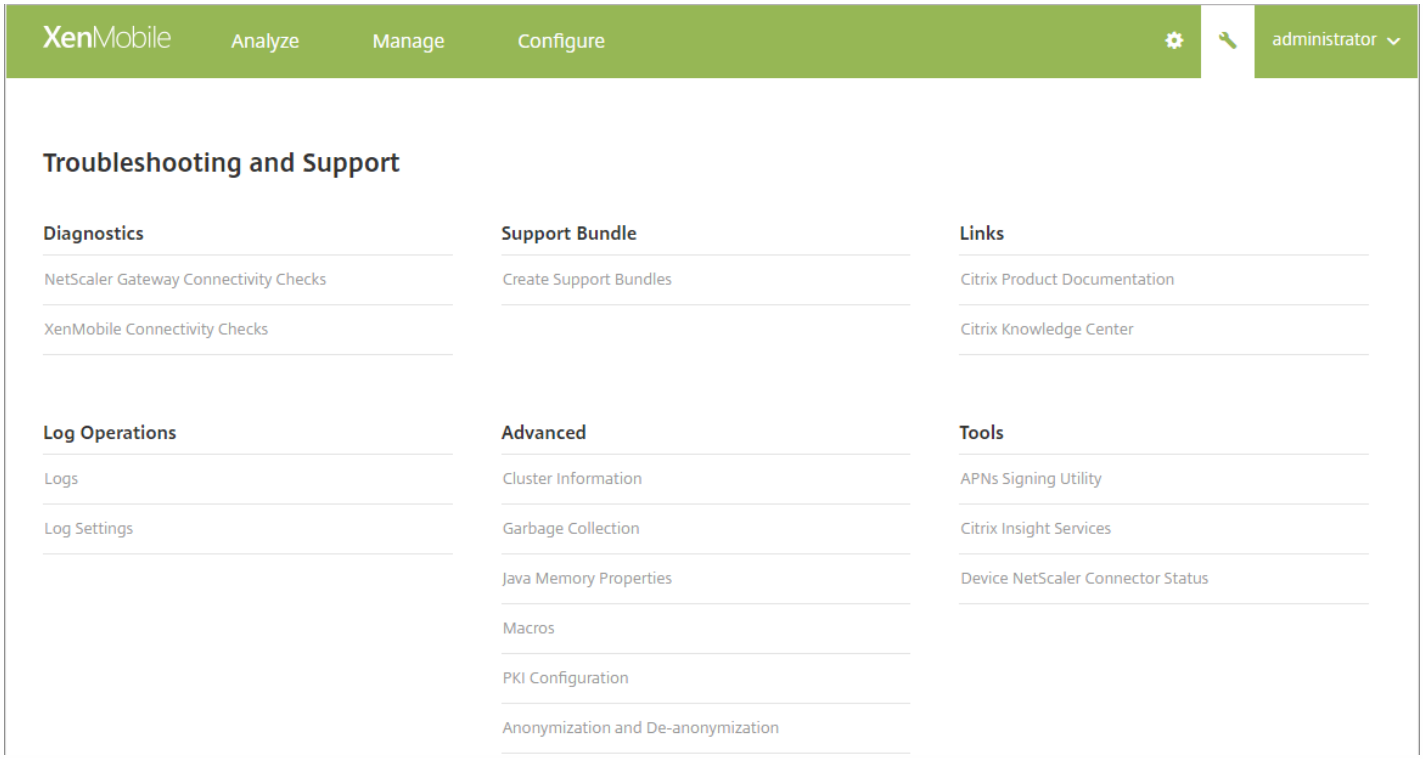


- Ahora, la página **Manage > Devices** y la ficha **Properties** de los dispositivos muestra los números de versión y revisión del agente XenMobile.

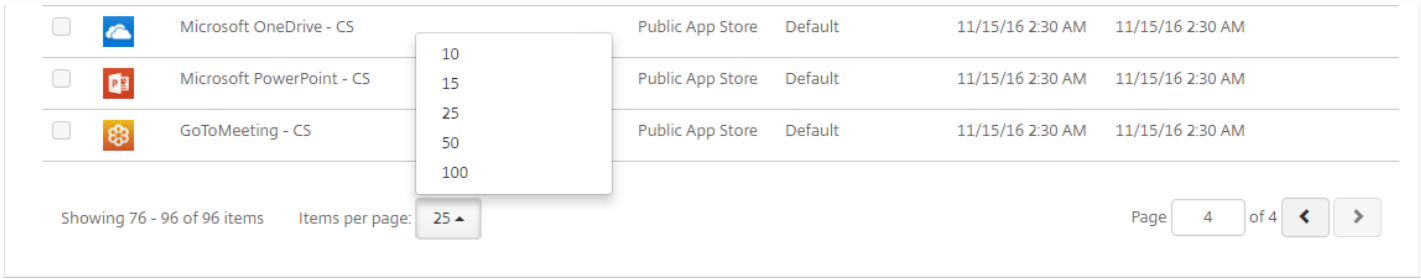




- La página **Troubleshooting and Support** se ha rediseñado para facilitar su uso.



- **Mensajes de registro**. Ahora, los mensajes de registro generados cuando no se puede encontrar un usuario incluyen los motivos posibles. Por ejemplo: credenciales no válidas, configuración de LDAP no válida o el usuario no se encuentra en el dominio LDAP o DN base de usuarios.
- **Paginación de listas**. Las listas de **Manage > Devices**, **Manage > Enrollment Invitations**, **Manage > Users**, **Configure > Device Policies**, **Configure > Apps**, **Configure > Actions**, **Configure > Enrollment Profiles** y **Configure > Delivery Groups** están ahora paginadas. Puede elegir el número de elementos que quiere mostrar en una página.



- **Incorporaciones a la API pública de XenMobile para servicios REST**. Ahora, la API de REST envía todas las propiedades de dispositivo en una llamada de dispositivo que usa un filtro. La API empaqueta las propiedades de dispositivo en un objeto JSON y las incluye como parte de la respuesta.

  La API de REST incluye ahora las llamadas de ShareFile Enterprise, StorageZones de ShareFile y conectores de StorageZone Connector de ShareFile.

  Para obtener más información, consulte el documento PDF de Información acerca de la API pública de servicios REST en XenMobile.

Elementos obsoletos

Ya no se admiten las tabletas Windows 8.1. XenMobile Server ya no admite tabletas Windows 8.1.

Se han eliminado las directivas de dispositivo para tabletas Windows 8.1. Las directivas de dispositivo para la clave de carga lateral y el certificado de firma están obsoletas.

Problemas resueltos

Apr 24, 2017

Se han resuelto los siguientes problemas en XenMobile 10.5. Los problemas resueltos de la herramienta de actualización aparecerán en el apartado XenMobile Upgrade Tool de este artículo.

Para ver los problemas resueltos relacionados con las aplicaciones XenMobile, consulte Problemas resueltos.

En dispositivos iPhone 6, cuando los usuarios intentan inscribir dispositivos con invitaciones de contraseña de un solo uso vinculadas con el IMEI/MEID del dispositivo, el primer perfil se instala correctamente. La segunda instalación de perfil MDM falla con el mensaje de error "Profile Installation Fails. A connection to the server could not be established". En dispositivos iPhone, la contraseña de un solo uso se vincula con el número MEID en lugar del número IMEI. [#606162]

Introducir ***#*#8255#*#*** en el teléfono no da como resultado el ID de Android, al contrario de lo indicado en 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]

Después de actualizar a XenMobile Server 10.4:

- Si abre la ficha **ShareFile**, es posible que la página no se cargue correctamente y la información no aparezca.
- Si intenta agregar o modificar un grupo de entrega, es posible que aparezca el siguiente mensaje de error: "500 Internal Server error" [663344, 663788, CXM-19085]

Después de usar el MDX Toolkit para empaquetar una aplicación que fue desarrollada con Mowbly, los botones de navegación de la aplicación ya no funcionan. [#654962]

El acceso a aplicaciones HDX agregadas en Secure Hub puede fallar y devolver un mensaje de error donde se indica que no se pudieron obtener los detalles de la aplicación y se pide al usuario que vuelva a intentarlo más tarde. [#658058]

Cuando Citrix Launcher se implementa en los dispositivos, las aplicaciones no aparecen en las tareas de segundo plano. [#680978]

Si el archivo JSON del proxy Web de App Controller 9.0 contiene un carácter de barra invertida sin escape en el nombre de usuario del proxy Web, no se puede iniciar XenMobile Server. [CXM-13721]

En implementaciones en clúster de XenMobile administradas por Hazelcast, es posible que un nodo del clúster no aparezca de manera intermitente en la lista de miembros de Hazelcast. [CXM-16537]

Cuando se configura una directiva de dispositivo VPN IPSec, el nombre de grupo y el secreto compartido no se guardan y faltan en el dispositivo. [CXM-17002]

Después de una actualización a la versión 10.3.6, los dispositivos que tienen varias identidades válidas no pueden renovarse. Si hay muchos fallos de renovación, XenMobile puede fallar y dejar de responder repetidamente. [CXM-17358]

Puede producirse un problema con un certificado de CA intermedio utilizado para la autenticación de certificado de cliente. El problema provoca que aparezca un error de acceso a la red en los dispositivos Android. [CXM-17401]

Puede haber problemas con la configuración de la base de datos de SQL al actualizar XenMobile 10.3.5 a XenMobile 10.3.6. [CXM-17565]

La versión local de XenMobile sincroniza periódicamente el servidor de licencias con las licencias que consten en XenMobile.

La sincronización garantiza que el recuento coincida con la cantidad de dispositivos y usuarios. De esta manera, si XenMobile detecta que no coinciden, el problema se resuelve en 24 horas. [CXM-18129]

La consola de XenMobile requiere que se especifique una contraseña para la directiva de redes WiFi, aunque la contraseña sea opcional. [CXM-18249]

XenMobile no implementa perfiles de usuario debido a un formato de fecha incorrecto. [CXM-18250]

Cuando se utiliza la consola de XenMobile con el explorador Internet Explorer 11, no se puede agregar ni editar una configuración de LDAP. [CXM-18324]

Al crear una directiva de Exchange para todos los tipos de dispositivo, si esa directiva contiene la macro **$user.dnsroot** para el campo de dominio, esa directiva no se implementa correctamente. [CXM-18545]

Si un nombre de grupo de entrega contiene un carácter "&", no se puede asignar una directiva a ese grupo de entrega. [CXM-18768]

Después de configurar los parámetros de DEP por primera vez en **Settings > iOS Bulk Enrollment**, puede aparecer este error al hacer clic en **Save**: "Resources bag (container) with name 'Worx Home by Citrix' doesn't exist". Como solución temporal, cree un nuevo grupo de entrega (**Configure > Delivery Groups**) después de configurar los parámetros de DEP y hacer clic en **OK** en la página de error. El grupo de entrega debe incluir lo siguiente:

- El grupo de usuarios llamado **Device Enrollment Program Group**.
- La directiva **DEP Software Inventory**.
- La aplicación requerida **Secure Hub** de Citrix

Este problema no afecta a las inscripciones existentes si el programa DEP se configuró antes de que Citrix Secure Hub saliera al mercado en la tienda de Apple el 6 de octubre de 2016. [CXM-19158]

En caso de las plantillas Enrollment Invitation (Invitación a la inscripción) o Enrollment PIN (PIN de inscripción), si el mensaje de las plantillas contiene ciertas macros, el mensaje enviado a los usuarios contiene la macro en lugar de la información de usuario. Esas macros son "enrollment URL" (${enrollment.url}) y "enrollment PIN" (${enrollment.pin}). [CXM-19210]

A veces, no se puede cargar una aplicación de empresa, porque XenMobile no puede encontrar el icono de la aplicación, aunque el icono se encuentra disponible. [CXM-19213]

En la página **Settings > PKI Entities > Discretionary CA**, solo aparece la primera página de los certificados de CA si hay varias páginas de certificados. [CXM-19736]

En caso de un grupo de entrega que se implementan en varios dispositivos: Si hace clic en un grupo de entrega en **Configure > Delivery Groups** y, a continuación, hace clic en el botón ubicado en **Deployment**, la página **Manage > Devices** mostrará una lista incorrecta de dispositivos. [CXM-19737]

Una vez que un usuario abre una aplicación XenMobile, las solicitudes de actualización de esa aplicación no aparecen en XenMobile Store aunque haya actualizaciones disponibles en el App Store de Apple o en Google Play Store. [CXM-19927]

Una macro de XenMobile que incluya $user.dnsroot no resuelve los dominios donde los dominios principales y los secundarios tienen una relación de confianza con la estructura de raíz-árbol. [CXM-20366]

Si el nombre sAMAccountName es distinto de la parte del nombre del UPN, falla la resolución de macro de la propiedad de cliente SEND_LDAP_ATTRIBUTES. Por ejemplo: El nombre sAMAccountName es **nombredeejemplo** y el nombre UPN es **muestra@ejemplo.com**. [CXM-20414]

En caso de que XenMobile esté en modo MDM y se usa la inscripción de DEP con credenciales de usuario suministradas durante la fase DEP, si un usuario quita Secure Hub del dispositivo poco después de la inscripción, el servidor pasa a un estado inconsistente. Se entiende una hora como "poco después de la inscripción". [CXM-20924]

Un dispositivo no pasa automáticamente al estado de cumplimiento de normativas después de una acción automatizada. [CXM-21006]

Para administradores RBAC en un rol RBAC personalizado que incluye algunas restricciones del grupo de usuarios: si los usuarios de Active Directory que haya en los grupos tienen algunos dispositivos inscritos, la página **Manage > Devices** se abre con lentitud. [CXM-21007, CXM-21009]

Después de actualizar a XenMobile 10.3.6, los administradores con roles RBAC de acceso personalizado verán los dispositivos inscritos de otros dominios incluso aunque la configuración de RBAC restrinja dicho acceso. [CXM-21008]

En XenMobile, los miembros del clúster pueden no responder a algunas solicitudes HTTP, lo que impide que los usuarios se inscriban debido a errores de **Red de empresa no disponible**. [CXM-21010]

Si los parámetros de inscripción en masa de iOS tienen habilitada la opción **Require credentials for device enrollment**, cualquier tipo de invitación a una inscripción DEP provocará errores en XenMobile Server. Los errores pueden ser mensajes de error en Secure Hub, mensajes de error en la consola de XenMobile y la pérdida de la funcionalidad de MDM para todos los dispositivos. Para solucionar este problema, elimine todas las invitaciones de inscripción de los usuarios afectados desde la página **Manage > Enrollment**. Reinicie el servidor XenMobile. [CXM-21500]

Las acciones automatizadas que activa el Modo perdido de XenMobile fallan en dispositivos iOS configurados con un código de acceso. Este problema se aplica a todas las acciones disponibles desencadenadas por el Modo perdido: **App wipe**, **App lock**, **Mark the device as out of compliance** y **Send notification**. [CXM-21579]

El informe Devices & Apps generado a partir de **Analyze > Reporting** muestra un recuento incorrecto de instalaciones de aplicaciones para cada dispositivo. [CXM-21773]

Cuando se agrega la aplicación pública Skype Empresarial a la consola de XenMobile, es posible que no aparezca el icono. No obstante, puede buscar y agregar la aplicación a la consola y la aplicación puede instalarse en el dispositivo. [CXM-21774, #668341]

Algunas aplicaciones de empresa para Android no se cargan en una consola de XenMobile configurada en el modo MDM o XME. [CXM-22377]

No funciona la implementación de recursos basada en las propiedades dinámicas de dispositivo, tales como el código móvil de país actual. XenMobile omite las reglas y permite que los recursos (por ejemplo, las directivas de dispositivo, las aplicaciones y las acciones) se implementen en el dispositivo. [CXM-22565]

No se puede crear un paquete de asistencia desde la CLI de XenMobile. Como solución temporal, use la consola de XenMobile: vaya a **Support > Create Support Bundles** y, a continuación, haga clic en **Create**. [CXM-23091]

Después de actualizar a XenMobile 10.3.6, Secure Hub ya no incluye aplicaciones HDX. Los registros contienen el mensaje "Unable to get the Config xml data Host name" (No se puede obtener el nombre de host de los datos de configuración XML). [CXM-23177]

Si solo modifica los datos de la plataforma de una directiva de dispositivo, los cambios realizados no provocan cambios en **Última actualización** de **Configure > Device Policies**. Después de agregar o quitar plataformas, la hora de la última actualización no cambia. [CXM-23178]

Si el idioma del explorador se establece en francés, no se puede crear ni modificar la directiva de redes WiFi desde la consola de XenMobile. [CXM-23180]

La página **Manage > Devices** muestra los dispositivos iOS como inactivos aunque los dispositivos estén activos y se comuniquen con el servidor XenMobile. Este problema se muestra en los registros de este modo:

java.lang.IllegalStateException: Cannot load backing target entity: has been deleted. [CXM-23181]

Si la propiedad de servidor **StorageZone Connectors supported value** es **NOT SUPPORTED** y configura ShareFile, después de ir a otra página en la consola y, a continuación, volver a la página **Configure > ShareFile**, la página **ShareFile** no muestra la configuración aunque esta se haya guardado. Para solucionar este problema, cambie la propiedad de servidor **ShareFile configuration type** a **ENTERPRISE**. [CXM-23337]

Cuando un dispositivo de DEP se elimina y, a continuación, se vuelve a inscribir, la reinscripción puede fallar con un error de "Perfil no válido". [CXM-24078]

Esta versión contiene una medida de defensa a fondo para CVE-2016-5195, también conocido como Linux Dirty Cow.

Herramienta de actualización Upgrade tool de XenMobile

Si su implementación de XenMobile 9 incluye la aplicación de empresa gpsstats.apk, la actualización a XenMobile 10.4 puede fallar. [CXM-17992]

Después de actualizar desde XenMobile 9 a XenMobile 10.4, los dispositivos Windows y iOS se colocan en el modo MDM en lugar del modo MDM + MAM. Además, XenMobile Store no se abre. Como solución temporal, los usuarios pueden volver a inscribir un dispositivo migrado. [CXM-18532, CXM-23408]

Después de actualizar desde XenMobile 9 a XenMobile 10.4, XenMobile tiene registros duplicados inactivos solo de MAM correspondientes a reinscripciones previas. Este problema ocurre incluso aunque XenMobile 9 requirió la inscripción en Device Manager. [CXM-18544]

Durante una actualización desde XenMobile 9.0 a XenMobile 10.4: La herramienta Upgrade Tool no actualiza el nombre del dispositivo en la tabla de propiedades de dispositivo en caso de dispositivos inscritos en el modo XME (MDM + MAM). [CXM-20821]

Si la base de datos de App Controller contiene usuarios en el formato de datos **nombreDeUsuario**, falla la actualización desde XenMobile 9.0 a XenMobile 10.x. En su lugar, use el formato de datos **dominio\nombreDeUsuario** o **nombreDeUsuario@dominio**. [CXM-21072]

Si la ruta a los certificados de servidor P12 difiere en mayúsculas o minúsculas para HTTP y HTTPS, falla la actualización desde XenMobile 9.0 a XenMobile 10.4. Por ejemplo, si la ruta HTTP es Certificates\MDM.p12 y la ruta HTTPS es certificates\MDM.p12. [CXM-21581]

Después de actualizar desde XenMobile 9 a 10.x, XenMobile Store no contiene aplicaciones. Además, XenMobile no asigna grupos locales a grupos de entrega. Este problema ocurre si un usuario local forma parte de un grupo local y ese usuario local inscribe el dispositivo. [CXM-23375]

Si Device Manager contiene dos registros para un mismo usuario de Active Directory y los registros no coinciden de este modo, se produce un error en la actualización:

- Los registros tienen nombres UPN diferentes. Por ejemplo, el registro de un usuario tiene el nombre UPN de jose.zambrano@es.dominio.com. El registro del otro es jose.zambrano@dominio.com.

- Los registros tienen diferencias de uso de mayúsculas y minúsculas en el nombre samAccountName. Por ejemplo, el registro de un usuario tiene un nombre sAMAccountName "josezambrano". El registro del otro es JOSEZAMBRANO. [CXM-23382]

Después de actualizar desde XenMobile 9 a XenMobile 10.x, en la consola XenMobile actualizada no se puede modificar una directiva de configuración que se personalizó en Device Manager utilizando la herramienta de configuración de iPhone o Apple Configurator. [CXM-23942]

Problemas conocidos

May 11, 2017

A continuación, se describen los problemas conocidos de XenMobile 10.5. Los problemas resueltos de la herramienta de actualización aparecerán en el apartado "XenMobile Upgrade Tool" de este artículo.

Para ver los problemas conocidos relacionados con las aplicaciones XenMobile, consulte Problemas conocidos.

Con NetScaler 12.0.41.16, cuando Secure Mail está configurado con STA, falla la sincronización de correo en dispositivos iOS y Android. El problema está resuelto en NetScaler 12.0 compilación 41.22. Para obtener información más detallada y actualizada, consulte este artículo de asistencia de Knowledge Center. [#685075]

Cuando integra StoreFront con XenMobile e implementa aplicaciones HDX, después de cambiar la contraseña de Active Directory, las aplicaciones HDX desaparecen de XenMobile Store. [CXM-9859]

Después de actualizar a XenMobile 10.4.2, las aplicaciones de Android for Work no aparecen en el dispositivo de un usuario si este usuario está anidado en un grupo de Active Directory. [CXM-19930]

Una actualización XenMobile de 10.3.6 a 10.5 puede cambiar el propietario del dispositivo a "anónimo" en caso de los dispositivos inscritos que ejecutan Android for Work. [CXM-19933]

Los usuarios pueden renovar certificados incluso aunque **Renew certificates when they expire** está establecido en **OFF** en la configuración de XenMobile. [CXM-20923]

En caso de usuarios de Active Directory incluidos en un grupo con permisos para conectores StorageZone: si se mueve a los usuarios fuera del grupo, los usuarios de ShareFile para iOS siguen teniendo acceso a los recursos compartidos de red asociados a esos conectores. Para solucionar este problema, vuelva a instalar la aplicación ShareFile para iOS. [CXM-21859]

Aunque mueva un conector StorageZone de un grupo de entrega A a un grupo de entrega B, los usuarios de ShareFile para iOS del grupo de entrega A pueden seguir usando el conector. [CXM-21860]

Si XenMobile utiliza certificados autofirmados, los usuarios no podrán inscribir dispositivos iOS 10.3 en XenMobile. Esta limitación se produce por un cambio en iOS 10.3. Para inscribir los dispositivos que ejecutan iOS 10.3 o posterior en XenMobile, debe utilizar certificados SSL de confianza en XenMobile. [CXM-24120]

Al implementar aplicaciones, se pide a los usuarios que instalen la aplicación si ya está instalada en el dispositivo, pero nunca se ha abierto. Como parte de una solución para este problema, si se actualiza una aplicación en el servidor, no se actualiza en el dispositivo del usuario hasta que la inicie. [CXM-32193]

Herramienta de actualización Upgrade tool de XenMobile

Después de actualizar XenMobile de 9 a 10.4, algunas directivas para dispositivos Windows aparecen en la consola de XenMobile incluso después de que XenMobile las haya implementado. Concretamente, las directivas permanecen en la ficha **Pending** de la página **Assigned Policies** de **Manage > Devices**. Como solución temporal, modifique y vuelva a implementar las directivas que aparezcan como pendientes. Esa acción borra las directivas para teléfonos Windows de la ficha **Pending**. La directiva de clips Web para tabletas Windows permanece en la ficha **Pending** a pesar de funcionar correctamente en los dispositivos. [CXM-21769]

Arquitectura

Apr 13, 2017

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, para conceder a los usuarios de la organización acceso remoto a las aplicaciones para móvil y realizar un seguimiento de los tipos de dispositivos, debe implementar 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. Esa conexión proporciona acceso 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 sus aplicaciones Web, SaaS y para móvil desde XenMobile mediante Secure Hub.
- 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 estas funciones en un servidor XenMobile local, Citrix recomienda implementar los 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 las aplicaciones para móvil creadas dentro o fuera de la empresa, como las aplicaciones XenMobile. 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 ofrece la administración de dispositivos y la administración de aplicaciones desde 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, utilizar 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 sobre cómo instalar una agrupación en clústeres en XenMobile configurando dos direcciones IP virtuales de equilibrio de carga en NetScaler, consulte Agrupación en clústeres.

Para obtener más información sobre cómo configurar XenMobile para una implementación de recuperación ante desastres, consulte el artículo Disaster Recovery de Deployment Handbook. Ese artículo contiene un diagrama de las arquitecturas.

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 las arquitecturas, consulte los artículos Reference Architecture for On-Premises Deployments y Reference Architecture for Cloud Deployments en "XenMobile Deployment Handbook". Para obtener una lista completa de los puertos, consulte Requisitos de puertos (local) y Requisitos de puertos (en la nube).

Modo de administración de dispositivos móviles (MDM)

XenMobile MDM Edition ofrece la administración de dispositivos móviles. Para conocer las plataformas respaldadas, consulte Sistemas operativos respaldados de dispositivo Puede implementar XenMobile en modo MDM si solo va a utilizar las funcionalidades de MDM de XenMobile. Por ejemplo, si quiere hacer lo siguiente.

- Implementar aplicaciones y directivas de dispositivo.
- Obtener inventarios de activos.
- Llevar a cabo acciones en los dispositivos, como borrados de dispositivos.

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, también denominado modo de solo MAM, ofrece la administración de aplicaciones móviles. Para conocer las plataformas respaldadas, consulte Sistemas operativos respaldados de dispositivo Puede implementar XenMobile en modo MAM si solo va a utilizar las funcionalidades de administración de aplicaciones móviles (MAM) de XenMobile, sin que los dispositivos se inscriban para MDM. Por ejemplo, si quiere hacer lo siguiente.

- Proteger las aplicaciones y los datos en los dispositivos móviles BYOD.
- Entregar aplicaciones móviles de empresa.
- Bloquear aplicaciones y 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

La utilización conjunta de MDM y MAM ofrece la administración de datos y de aplicaciones móviles, así como la administración de dispositivos móviles. Para conocer las plataformas respaldadas, consulte Sistemas operativos respaldados de dispositivo Puede implementar XenMobile en modo ENT (Enterprise) si va a utilizar las funcionalidades de MDM + MAM de XenMobile. Por ejemplo, si quiere:

- Administrar dispositivos de empresa a través de MDM
- Implementar aplicaciones y directivas de dispositivo
- Obtener un inventario de activos
- Borrar dispositivos
- Entregar aplicaciones móviles de empresa
- 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 un servidor XenMobile local 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. En esta implementación, el servidor XenMobile no está en la zona DMZ. Por lo tanto, no es necesario abrir puertos en el firewall interno para permitir el acceso a los servidores SQL Server y PKI desde la zona DMZ.

Requisitos del sistema y compatibilidad

Mar 31, 2017

Para ver información adicional sobre los requisitos y la compatibilidad, consulte los siguientes artículos:

- Compatibilidad de XenMobile
- Sistemas operativos de dispositivo respaldados
- Requisitos de puertos
- Escalabilidad
- Licencia
- Cumplimiento del estándar FIPS 140-2
- Respaldo para idiomas

Para ejecutar XenMobile 10.5, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.5.x o 7.0); para obtener información más detallada, consulte XenServer.
  - VMware (versiones compatibles: ESXi 5.5 o ESXi 6.0). Para obtener información más detallada, consulte VMware.
  - Hyper-V (versiones compatibles: Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2). Para obtener información más detallada, consulte Hyper-V.
- Procesador de doble núcleo
- Cuatro unidades CPU virtuales
- 8 GB de RAM para entornos de producción; 4 GB de RAM para pruebas de concepto y entornos de prueba
- 50 GB de espacio en disco

XenMobile 10.5 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 10.5, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.5 o 7.0)
  - 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 10.5

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 una de las siguientes versiones compatibles. Para obtener más información sobre 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 10.5 respalda los grupos de disponibilidad de SQL AlwaysOn y SQL Clustering para una alta disponibilidad de las bases de datos.

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 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 9.5.2 y 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 3.9
StoreFront 3.8
StoreFront 3.7
StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
Interfaz Web 5.4
XenApp y XenDesktop 7.13
XenApp y XenDesktop 7.12
XenApp y XenDesktop 7.11
XenApp y XenDesktop 7.9
XenApp y XenDesktop 7.8
XenApp y XenDesktop 7.7
XenApp y XenDesktop Long Term Service Release (LTSR)

XenApp y XenDesktop 7.6
XenApp y XenDesktop 7.5
XenApp 6.5

Requisitos de servidor de correo de XenMobile 10.5

XenMobile 10.5 admite los siguientes servidores de correo:

- Exchange 2016
- Exchange 2013
- Exchange 2010

Compatibilidad de XenMobile

Jun 05, 2017

Important

- Citrix ofrece respaldo para la distribución de las aplicaciones de productividad de XenMobile, en su versión de aplicación de empresa y en su versión de tienda pública de aplicaciones hasta el 31 de diciembre de 2017. Consulte la tabla de productos de Citrix para obtener más información. Debe migrar a las aplicaciones de tienda pública antes de esta fecha. A partir de ese momento, solo se dará respaldo a la distribución de tienda pública de aplicaciones. Para obtener más información acerca de las guías de cada aplicación para pasar de las versiones de empresa de XenMobile Apps a las versiones de tienda pública, consulte Guía para migrar a las aplicaciones de tienda pública. El MDX Toolkit seguirá dando respaldo al empaquetado empresarial para los desarrolladores de aplicaciones.
- A partir de la versión 10.4, las aplicaciones móviles Worx pasan a llamarse XenMobile Apps. Todas las aplicaciones XenMobile cambian de nombre. Para obtener más información, consulte Acerca de XenMobile Apps.

En este artículo, se resumen las versiones de los componentes de XenMobile respaldados que se pueden integrar. Esos componentes incluyen NetScaler Gateway y la versión de MDX Toolkit necesaria para empaquetar, configurar y distribuir XenMobile Apps.

Versiones respaldadas y rutas de actualización

Para XenMobile Server y XenMobile Apps, Citrix respalda la versión actual de XenMobile y las dos anteriores. Por ejemplo, si la versión actual es XenMobile Server 10.5, Citrix también respalda las versiones 10.4 10.3.6. Una versión incluye las versiones y los paquetes de servicio Service Packs. XenMobile 10.4 es un Service Pack más que una versión completa.

Ha finalizado el mantenimiento de XenMobile 9. Para obtener más información, consulte la matriz de productos. Citrix admite actualizaciones desde XenMobile 9 a la versión más reciente de XenMobile 10.

	Respaldo a actualizaciones	**Versión más reciente**	**Actualizar desde**
Aplicaciones de empresa empaquetadas (por ejemplo, Secure Mail y Secure Web)	Últimas dos versiones	10.4.5 (iOS), 10.4.6 (Android)	10.3.10 o 10.4
Aplicaciones de tienda pública (por ejemplo, Secure Hub, Secure Mail y Secure Web)	Últimas dos versiones Los usuarios que tienen las actualizaciones automáticas habilitadas reciben la versión más reciente desde la tienda de	10.5.20 (Secure Hub) 10.5.20 (Secure Mail) 10.5.20 (Secure Web)	10.5.10 o 10.5.15 (Secure Hub) 10.5.10 o 10.5.15 (Secure Mail) 10.5 y 10.5.10 (Secure Web)

	aplicaciones. La aplicación más reciente admite los dos archivos MDX anteriores.		Por ejemplo, una versión 10.5.20 de Secure Mail es compatible con un archivo MDX de la versión 10.5.15 o 10.5.10.
MDX	Versión anterior	10.4.10	10.4.5
Servidor (local)	Últimas dos versiones y actualizaciones desde XenMobile 9 RP5	10.5	10.4, 10.3.6, XenMobile 9 RP5

Compatibilidad de XenMobile

Para utilizar las nuevas características, soluciones y actualizaciones de directivas, Citrix recomienda instalar la versión más reciente de MDX Toolkit, Secure Hub y XenMobile Apps.

- Aplicaciones, MDX Toolkit y Secure Hub para la distribución de empresa:
  - La versión más reciente de XenMobile Apps y MDX Toolkit requieren la versión más reciente de Secure Hub.
  - La versión más reciente de MDX Toolkit es necesaria para la versión más reciente XenMobile Apps.
  - Las dos versiones anteriores de las aplicaciones y la versión anterior de MDX Toolkit son compatibles con la versión más reciente de Secure Hub.
- Cliente y servidor: Las versiones más recientes de Secure Hub, MDX Toolkit y XenMobile Apps son compatibles con la última versión más las dos últimas versiones de XenMobile Server.
- Las aplicaciones de tienda pública solo son compatibles con XenMobile 10.4 y versiones posteriores.
- Las aplicaciones de empresa empaquetadas serán compatibles con XenMobile 9 hasta que XenMobile 9 llegue al Fin de vida en junio de 2017.

Versiones de NetScaler Gateway respaldadas:

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

> **Important**
>
> Actualmente, XenMobile no admite NetScaler 12.0.41.16. El problema está resuelto en NetScaler 12.0 compilación 41.22.Para obtener información más detallada y actualizada, consulte este artículo de asistencia de Knowledge Center.

Versiones del MDX Toolkit para iOS y Android	**Versiones compatibles de Secure Hub**	
	Android	**iOS**

10.4.10 10.4.5	10.5.20 10.5.15	10.5.20 10.5.15
MDX Toolkit para Windows Phone	**Versiones compatibles de Secure Hub**	
10.3.9	10.3.5	
10.3.1	10.3	

> ## Nota
>
> XenMobile 10.1 no respalda Windows Phone 10.
>
> Para XenMobile 9, se debe instalar una revisión para que las aplicaciones funcionen correctamente. Para obtener más información, consulte CTX217942.

Aplicaciones disponibles en tiendas públicas de aplicaciones

	Android	**iOS**
Secure Hub	10.5.20	10.5.20
Secure Mail	10.5.20	10.5.20
Secure Web	10.5.20	10.5.20
Secure Notes	10.4.5	10.4.5
Secure Tasks	10.4.5	10.4.5
QuickEdit	6.10	6.10
ShareFile	5.4	5.3
ShareConnect		3.3
ScanDirect		1.2.2

Aplicaciones disponibles para la distribución empresarial

XenMobile 10.x y 9 respalda las versiones de aplicaciones XenMobile o aplicaciones móviles Worx que figuran en la siguiente tabla.

Aplicación	**Android**	**iOS**	**Windows Phone**[1]
Secure Hub	10.5.15 10.5.10	10.4.10 10.4.5	
Worx Home	10.3.10 10.3.9	10.3.10 10.3.9	10.0.3 10.0.0
Secure Forms		10.4.5 10.4.1	
Secure Mail	10.4.6 10.4.5	10.4.5 10.4.0.19	
WorxMail	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.7
Secure Notes	10.4.5 10.4.1	10.4.5 10.4.1	
Worx Notes	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Tasks	10.4.5 10.4.1	10.4.5 10.4.1	
WorxTasks	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Web	10.4.5	10.4.5	

	10.4.1	10.4.1	
WorxWeb	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.3
QuickEdit[2]	6.10	6.10	
ScanDirect		1.2.2	
ShareConnect	3.2.341	3.3	
ShareFile	5.4	5.3	

[1] XenMobile 10.1 no respalda Windows Phone 10.

[2] XenMobile solo respalda las versiones más recientes de QuickEdit, ShareConnect y ShareFile.

Respaldo para exploradores Web

XenMobile 10.x admite los siguientes exploradores Web:

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

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

Sistemas operativos respaldados de dispositivo

Jun 05, 2017

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

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

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

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

Android

XenMobile 10.x

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

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

Worx Home/Secure Hub se admite en dispositivos Android basados en x86 para la administración de dispositivos móviles. En XenMobile 10 y 10.1, la administración de aplicaciones solo está disponible en dispositivos Android con procesadores basados en ARM. Las aplicaciones empaquetadas con MDX no reciben respaldo en dispositivos Android basados en x86.

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

Sistemas operativos y dispositivos Android probados específicamente en XenMobile 10.x en modo MDM + MAM (Enterprise)

- Tableta Google Nexus 7 (sistema operativo 4.4.4)
- Tableta Google Nexus 9 (sistema operativo 7.0)
- Google Nexus 5 (sistema operativo 6.0.1)
- Google Nexus 5X (sistema operativo 7.1.1)
- Google Pixel

- Galaxy S4 modelo GT-I9500 (liberado por root) (sistema operativo 4.2.2)
- Galaxy S7 (sistema operativo 7.0)
- Galaxy S6 (sistema operativo 6.0.1, 5.0)
- Galaxy Tab A (sistema operativo 6.0.)
- Galaxy Note3 modelo SM-N900 (sistema operativo 5.0)
- Galaxy S4, GT-I9500 (sistema operativo 5.0.1)
- Galaxy S3 modelo GT-I9305 (sistema operativo 4.4.4)
- Galaxy S4 GT-I9505 (sistema operativo 4.3)
- Moto Turbo (sistema operativo 6.0.1)
- Nexus 9 Tab (sistema operativo 5.0.1)
- Nexus 9 Tab (sistema operativo 5.1.1)
- Nexus 7 (sistema operativo 4.4)
- Nexus 6P (sistema operativo 7.1.1)
- Nexus 5 (sistema operativo 5.0.1)
- Galaxy S6 Edge, SM-G925F (sistema operativo 6.0.1)
- Huawei Nexus 6 (sistemas operativos 6.0.1 y 7.0)
- Sony Xperia, modelo SGP311 (sistema operativo 5.0.1)
- Galaxy S5 SM-G900F (sistema operativo 6.0.1)
- Galaxy S5 SM-G900H (sistema operativo 6.0.1)
- HTC One M8 (sistema operativo 4.4.2)

Sistemas operativos y dispositivos Android probados específicamente en XenMobile 10.x en modo MDM

- Tableta Google Nexus 7 (sistema operativo 4.4.4)
- Tableta Google Nexus 9 (sistema operativo 7.0)
- Google Nexus 5 (sistema operativo 6.0.1)
- Google Nexus 5X (sistema operativo 7.1.1)
- Google Pixel
- Galaxy S7 (sistema operativo 7.0)
- Galaxy S6 (sistema operativo 6.0.1, 5.0)
- Galaxy Tab A (sistema operativo 6.0.)
- Galaxy S4 modelo GT-I9500 (liberado por root) (sistema operativo 4.2.2)
- Galaxy Note3 modelo SM-N900 (sistema operativo 5.0)
- Galaxy S4, GT-I9500 (sistema operativo 5.0.1)
- Galaxy S3 modelo GT-I9305 (sistema operativo 4.4.4)
- Galaxy S4 GT-I9505 (sistema operativo 4.3)
- Nexus 9 Tab (sistema operativo 5.0.1)
- Nexus 9 Tab (sistema operativo 5.1.1)
- Nexus 7 (sistema operativo 4.4)
- Nexus 5 (sistema operativo 5.0.1)
- Galaxy S6 Edge, SM-G925F (sistema operativo 6.0.1)
- Huawei Nexus 6 (sistemas operativos 6.0.1 y 7.0)
- Sony Xperia, modelo SGP311 (sistema operativo 5.0.1)
- Galaxy S5 SM-G900F (sistema operativo 6.0.1)
- Galaxy S5 SM-G900H (sistema operativo 6.0.1)
- HTC One M8 (sistema operativo 4.4.2)

Además, los siguientes tipos de dispositivo se han probado con Secure Mail.

Tipo de dispositivo	Sistema operativo
Samsung S7	7.0
Samsung S6	6.0.1
Samsung S5	5
Samsung Tab A	6.0.1
Nexus 7	4.4.4

SAFE y KNOX

En dispositivos Samsung compatibles, XenMobile 10.x respalda y extiende directivas de Samsung for Enterprise (SAFE) y Samsung KNOX. XenMobile requiere que se habiliten las API de SAFE antes de implementar directivas de SAFE y directivas de restricciones. Para ello, implemente la clave integrada de Samsung Enterprise License Management (ELM) en un dispositivo. Para habilitar la API de Samsung KNOX:

1. Debe adquirir una licencia de Samsung KNOX mediante el sistema de administración de licencias KNOX (KLMS) de Samsung.

2. Implemente la clave ELM de Samsung.

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

iOS

> ## Nota
>
> Los dispositivos iOS 10.3 no admiten certificados autofirmados. Si XenMobile utiliza certificados autofirmados, los usuarios no podrán inscribir dispositivos iOS 10.3 en XenMobile. Para inscribir los dispositivos que ejecutan iOS 10.3 o posterior en XenMobile, debe utilizar certificados SSL de confianza en XenMobile.

Todas las aplicaciones Worx o XenMobile son compatibles con iOS 10 a partir de la versión 10.3.10. Debe utilizar MDX Toolkit 10.3.10 o una versión posterior para empaquetar aplicaciones móviles o de empresa si quiere garantizar la compatibilidad con iOS 10. Si los usuarios actualizan a iOS 10, también deben actualizar a Worx Home 10.3.10 o una versión posterior (Secure Hub) para poder usar aplicaciones MDX. Para obtener información más detallada, consulte este artículo de asistencia de Knowledge Center.

XenMobile 10.3.x, 10.4 y 10.5

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

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

- iPhone 7+ 10.2.1 (XenMobile 10.5 y versiones posteriores)
- iPhone 6, 6+, 6S, 6S+, 5s, 5, 5c
- iPad 2, 3
- iPad Air, iPad Air-2, iPad Mini-4, Mini-3, Mini-2
- iPad Pro
- Mac OS X
  - MacBook, Air, Mini, Mini Retina 10.9.5, 10.10, 10.11

XenMobile 10 y 10.1

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

Algunos dispositivos iOS respaldados en XenMobile 10 y 10.1:

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

Windows Phone y Tablet

XenMobile 10.5

- Tabletas y teléfonos Windows 10
  - No recibe respaldo cuando XenMobile se encuentra en modo de administración solo de aplicaciones móviles (MAM-only).
- Compatibilidad de Windows Phone 8.1 con Worx Home.
  - Si XenMobile está en modo Enterprise: Worx Home 10.0.
  - Si XenMobile está en modo de solo MDM: Worx Home 9.1.0.
- Windows Mobile/CE
  - No recibe respaldo cuando XenMobile se encuentra en modo de administración solo de aplicaciones móviles (MAM-only).

XenMobile 10.3.x y 10.4

- Windows Tablet 10 RS1, 8.1
  - Windows 10 Tablet no recibe respaldo cuando XenMobile se encuentra en modo de solo MAM.
- Windows Tablet Surface Pro 3, Surface 2, RT
- Windows Phone 10, 8.1
  - Para Windows Phone 10, debe instalar una revisión que se puede obtener en la página de descargas de XenMobile.
  - No reciben respaldo cuando XenMobile se encuentra en modo de administración solo de aplicaciones móviles (MAM-

only).
- Compatibilidad de Windows Phone 8.1 con Worx Home:
  - Worx Home 10.0 cuando XenMobile está en modo Enterprise.
  - Worx Home 9.1.0 cuando XenMobile está en modo de solo MDM.
- Windows 8.1 ediciones Pro y Enterprise (de 32 y 64 bits)
- Windows RT 8.1
- Windows Mobile/CE
  - No recibe respaldo cuando XenMobile se encuentra en modo de administración solo de aplicaciones móviles (MAM-only).

Algunos dispositivos Windows respaldados en XenMobile 10.3:

- Windows Tablet 10, 8.1
- Windows Phone 10, 8.1
- HTC (Windows Phone 8.1)
- Nokia 920, 925, 1020, 1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3
- Windows Tablet Surface 2
- Windows Tablet RT

XenMobile 10 y 10.1

- Windows Tablet 10 RS1
- Windows Phone 8.1 / 10:
  - Windows Phone 8.1 no recibe respaldo cuando XenMobile se encuentra en modo de administración de solo aplicaciones móviles (MAM-only).
  - Windows Phone 10 recibe respaldo en XenMobile 10.3 y versiones posteriores.
  - Windows Phone 10 recibe respaldo en XenMobile 9, pero debe instalar una revisión de Device Manager, como se explica en este artículo de Knowledge Center. Asimismo, tenga en cuenta la revisión de Windows 10 Anniversary Update 1607 si dispone de teléfonos Windows. Para obtener información más detallada, consulte este artículo de Knowledge Center.
- Compatibilidad de Windows Phone 8.1 con Worx Home:
  - Worx Home 10.0 cuando XenMobile está en modo Enterprise
  - WorxHome 9.0.3 cuando XenMobile está en modo de solo MDM
- Windows 8.1 ediciones Pro y Enterprise (de 32 y 64 bits)
- Windows RT 8.1
- Windows Mobile: XenMobile 10.1 no respalda dispositivos Windows Mobile. Los usuarios que tienen dispositivos que ejecutan Windows Mobile o Windows CE deben continuar usando XenMobile 9.

Algunos dispositivos Windows respaldados en XenMobile 10 y 10.1:

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

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

Symbian

XenMobile 10.3.x, 10.4 y 10.5

XenMobile 10.3.x, 10.4 y 10.5 no respaldan Symbian.

XenMobile 10 y 10.1

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

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

BlackBerry

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

Requisitos de puertos

May 22, 2017

Para que dispositivos y aplicaciones puedan comunicarse con XenMobile, debe abrir puertos específicos en los firewalls. En la siguiente tabla se ofrece una lista de los puertos que se deben abrir. Para conocer los requisitos de puertos del servicio XenMobile, consulte Requisitos de puertos.

Apertura de puertos para que NetScaler Gateway y XenMobile administren aplicaciones

Abra los siguientes puertos para permitir las conexiones de usuario desde Citrix Secure Hub, Citrix Receiver y el plug-in de NetScaler Gateway a través de NetScaler Gateway a los siguientes componentes:

- XenMobile
- StoreFront
- XenDesktop
- XenMobile NetScaler Connector
- Otros recursos de red interna, como los sitios Web de intranet

Para permitir el tráfico desde NetScaler al servicio Launch Darkly, puede utilizar las direcciones IP que se indican en este artículo de asistencia de Knowledge Center.

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, consulte Comunicación de dispositivos NetScaler con clientes y servidores en la documentación de NetScaler. Esa sección contiene información sobre las direcciones IP de NetScaler (NSIP), las direcciones IP virtuales (VIP) y las direcciones IP de subred (SNIP).

Puerto TCP	Descripción	Origen	Destino
21 o 22	Se usa para enviar paquetes de asistencia a un servidor FTP o SCP.	XenMobile	Servidor SCP o FTP
53 (TCP y UDP)	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 o 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 (TCP y UDP)	Se usa para los servicios del protocolo de tiempo de red (NTP).	NetScaler Gateway XenMobile	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 móviles (MAM).	XenMobile NetScaler Gateway Dispositivos Internet	XenMobile
4443	Se utiliza para que un administrador acceda a la consola de XenMobile a través del	Punto de acceso (explorador)	XenMobile

	explorador.		
	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 o anular licencias de Citrix.	XenMobile	Demonio de proveedor de Citrix

Apertura de puertos de XenMobile para administrar dispositivos

Abra 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 de la tienda 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 las tiendas de aplicaciones a través de Citrix Mobile Self-Serve en iOS, Secure Hub para Android o Secure Hub 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 o 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	XenMobile	Servidor de autenticación

	seguras.		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.	Cliente Remote Support	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 Secure Hub para Android 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 admitan el servidor proxy. En este caso, permita que la conexión ADS circunvale el servidor proxy.

Si quiere habilitar la fijación de certificados, debe cumplir los siguientes requisitos previos:

- **Obtenga certificados para XenMobile Server 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 de Citrix y solicite la habilitación de la fijación de certificados**. Durante este proceso, se le pedirán los certificados.

La fijación de certificados requiere que los dispositivos se conecten al servicio ADS antes de que el dispositivo se inscriba. Este requisito garantiza que Secure Hub tenga disponible la información de seguridad más actualizada para el entorno en que se va a inscribir el dispositivo. Para que Secure Hub inscriba un dispositivo, éste debe 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 que Secure Hub para Android acceda al servicio ADS, abra el puerto 443 para el nombre de dominio completo (FQDN) y las direcciones IP siguientes:

Nombre de dominio completo (FQDN)	Dirección IP
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

Escalabilidad y rendimiento

Jun 26, 2017

> **Nota**
>
> Para ver las instrucciones de rendimiento y escalabilidad más recientes de XenMobile, consulte Escalabilidad y rendimiento.

Entender la escala que tendrá la infraestructura de XenMobile es vital para decidir cómo implementar y configurar XenMobile. Este artículo contiene datos obtenidos en pruebas de escalabilidad y directrices para determinar los requisitos de infraestructura para el rendimiento y la escalabilidad de implementaciones pequeñas, medianas y grandes locales de XenMobile.

La escalabilidad se define aquí en términos de la capacidad de los dispositivos existentes (es decir, la capacidad de los dispositivos ya inscritos en la implementación) para reconectarse a la implementación al mismo tiempo.

- La *escalabilidad* es la cantidad máxima de dispositivos inscritos en la implementación.
- La *tasa de inicio de sesión* es la velocidad máxima a la que los dispositivos pueden reconectarse a la implementación.

Los datos de este artículo se derivan de pruebas realizadas en implementaciones que van desde 10 000 a 60 000 dispositivos. Las pruebas incluían cargas de trabajo conocidas en los dispositivos móviles.

Todas las pruebas se realizaron en XenMobile Enterprise Edition.

Las pruebas se realizaron con NetScaler Gateway 8200. Un dispositivo NetScaler con igual o mayor capacidad puede producir una escalabilidad y rendimiento similar o superior.

Esta tabla resume los resultados de las pruebas de escalabilidad:

Escalabilidad	**Un máximo de 60 000 dispositivos**	
Tasa de inicio de sesión	Velocidad de reconexión de los usuarios existentes	Un máximo de 7500 dispositivos por hora
Configuración	NetScaler	MPX 8200
	XenMobile Enterprise Edition	Clúster de 5 nodos de XenMobile Server
	Base de datos	Base de datos externa de Microsoft SQL Server

Resultados de las pruebas según cantidad de

dispositivos y configuración de hardware

Esta tabla muestra los resultados de escalabilidad de las cantidades de dispositivos y configuraciones de hardware sometidas a prueba.

Cantidad de dispositivos	10 000	30 000	60 000
Tasa de reconexión de dispositivos existentes por hora	1250	3750	7500
Modo de XenMobile Server	Autónomo	Clúster	Clúster
Clúster de XenMobile Server	N/D	3	5
Dispositivo virtual de XenMobile Server	Memoria = 8 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 8	Memoria = 24 GB de RAM Unidades vCPU = 8
Active Directory	Memoria = 4 GB de RAM Unidades vCPU = 2	Memoria = 8 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 4
Base de datos externa de Microsoft SQL Server	Memoria = 8 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 8	Memoria = 48 GB de RAM Unidades vCPU = 24

Perfil de escalabilidad

En estas tablas, se resume el perfil de prueba utilizado para los datos descritos en este artículo:

Configuración de Active Directory	Perfil utilizado
Usuarios	100 000
Grupos	200 000
Niveles de anidamiento	5

Configuración de XenMobile Server	Total	Por usuario
Directivas	20	20
Aplicaciones	270	60
Aplicación pública	200	0
MDX	60	30
Web y SaaS	20	20
Acciones	60	
Grupos de entrega	20	
Grupos de Active Directory por grupo de entrega	10	

SQL	
Cantidad de bases de datos	1

Actividad de aplicación y conexión de dispositivos

Estas pruebas de escalabilidad recopilaron datos acerca de la capacidad de los dispositivos inscritos en una implementación para reconectarse en un periodo de 8 horas.

Las pruebas simulaban un intervalo de reconexión durante el cual los dispositivos que se reconectan obtienen todas las directivas de seguridad que les corresponden, con lo que los nodos de XenMobile Server están sujetos a condiciones de carga más altas de las normales. Durante las reconexiones siguientes, solo se envían a los dispositivos iOS las directivas nuevas o las que han cambiado, lo que disminuye la carga en los nodos de XenMobile Server.

En las pruebas se usó una combinación de dispositivos: el 50% eran dispositivos iOS y el otro 50% eran dispositivos Android.

En estas pruebas se presupone que los dispositivos Android que se reconectan han recibido previamente notificaciones de GCM.

Durante el intervalo de prueba de 8 horas, tuvieron lugar las siguientes actividades relacionadas con aplicaciones:

- Secure Hub se abrió una vez para enumerar aplicaciones asignadas al usuario
- Se abrieron 2 aplicaciones Web SAML
- Se descargaron 4 aplicaciones MAM
- Se generó 1 STA para su uso en Secure Mail
- Se validaron 240 tíquets de STA, uno para cada evento de reconexión de Secure Mail sobre una micro VPN.

Arquitectura de referencia

Para consultar la arquitectura de referencia para las implementaciones de las pruebas de escalabilidad, consulte "Core MAM+MDM Reference Architecture" en Reference Architecture for On-Premises Deployments.

Advertencias y limitaciones

Al estudiar los resultados de las pruebas de escalabilidad descritos en este artículo tenga en cuenta lo siguiente:

- No se ha probado la plataforma Windows.
- El envío de directivas se ha probado en dispositivos iOS y Android.
- Cada nodo de XenMobile Server admite un máximo de 10 000 dispositivos de forma simultánea.

Licencias

Apr 13, 2017

El servicio XenMobile y el servidor XenMobile no comparten el sistema de licencias:

- Citrix Cloud Operations gestiona las licencias del servicio XenMobile.
- El servidor XenMobile y NetScaler Gateway requieren licencias.

  Para obtener más información sobre el sistema de licencias de NetScaler Gateway, consulte Licencias en la documentación de NetScaler Gateway. XenMobile usa Citrix Licensing para administrar las licencias. Para obtener más información acerca de Citrix Licensing, consulte The Citrix Licensing System.

  Al adquirir XenMobile Server, recibe un correo 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 las licencias de XenMobile.

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

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
>
> La versión más reciente de XenMobile requiere el servidor de licencias de Citrix 11.12.1 o una versión posterior. Las versiones anteriores del servidor de licencias no funcionan con la versión más reciente de XenMobile.

> ## Important
>
> Si va a agrupar nodos en clúster o instancias de XenMobile, debe 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, se incluyen todos los archivos de licencias 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

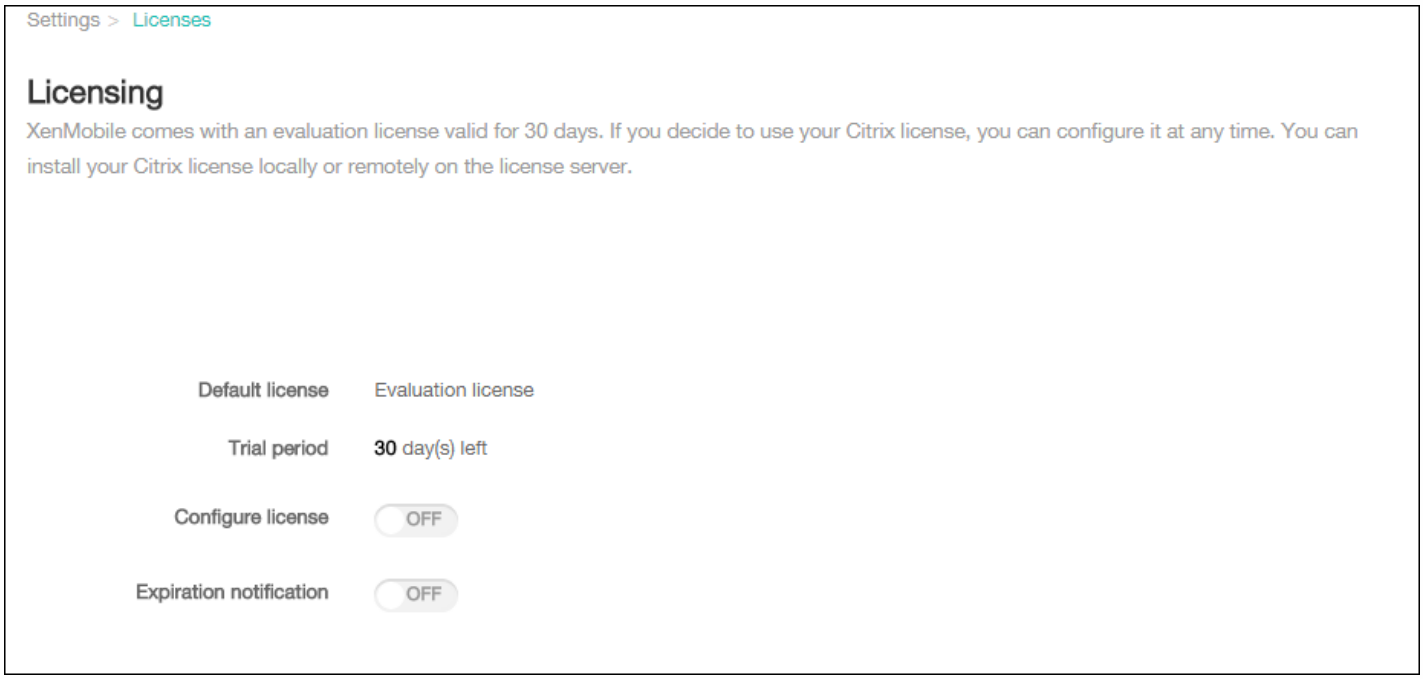
evaluación.

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.

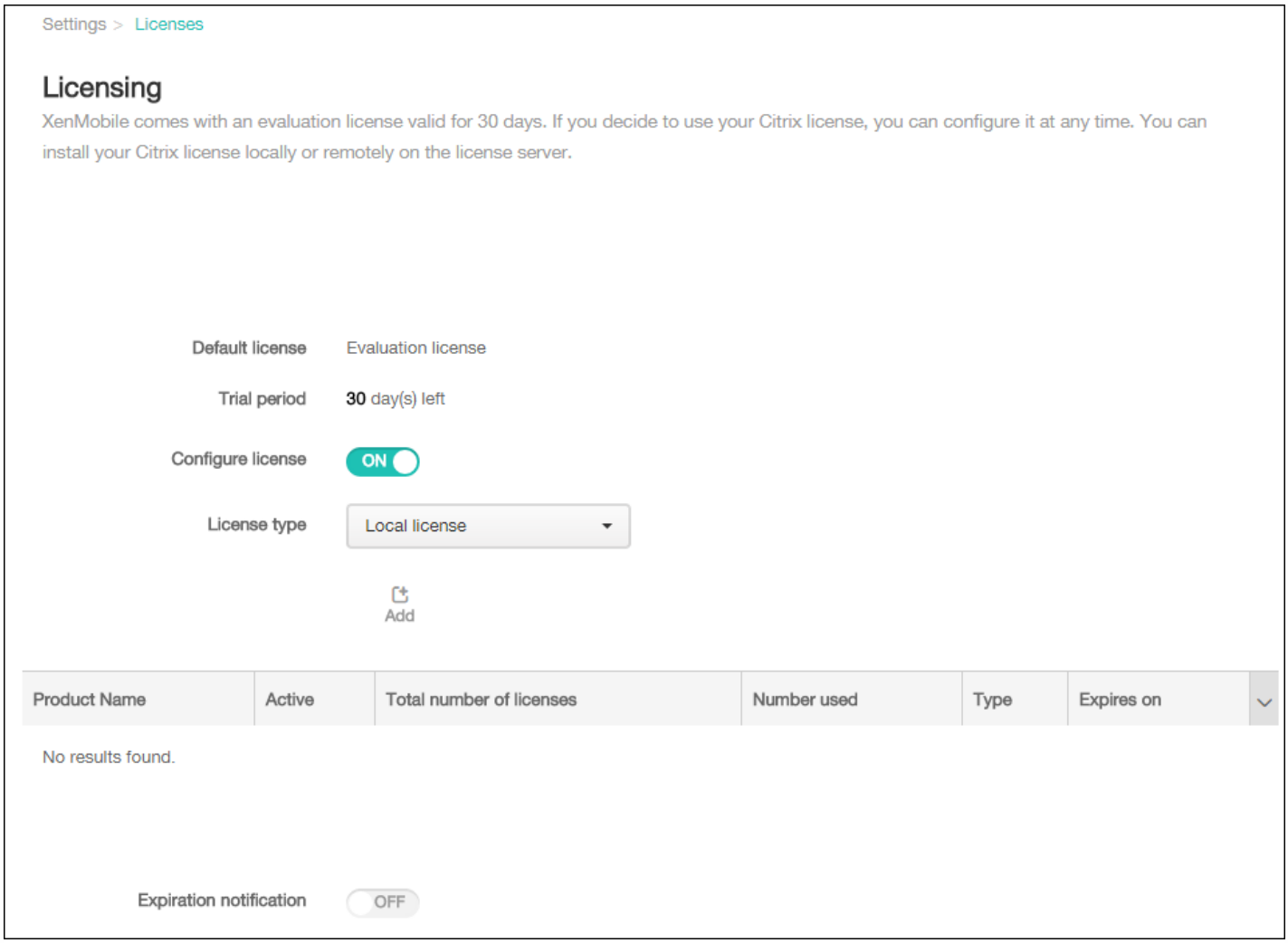
Puede administrar todas las licencias locales a través de la consola de XenMobile.

1. Los archivos de licencias pueden obtenerse del servicio Simple License Service desde la consola License Administration Console o directamente desde su cuenta, en citrix.com. Para obtener información más detallada, consulte Obtención de archivos de licencias.

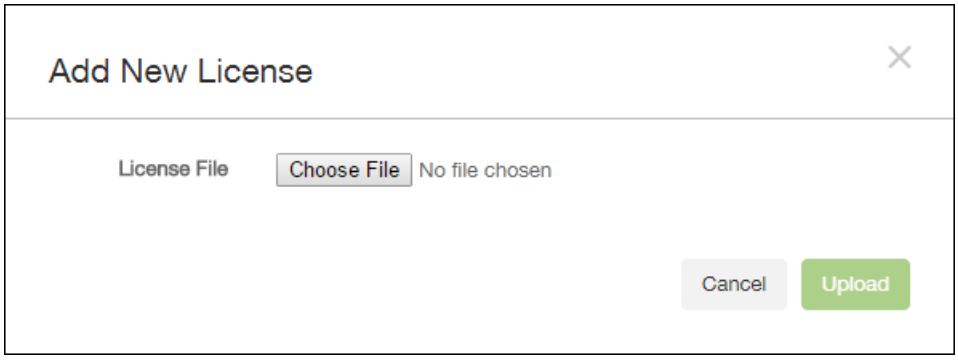
2. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

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 ha usado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.

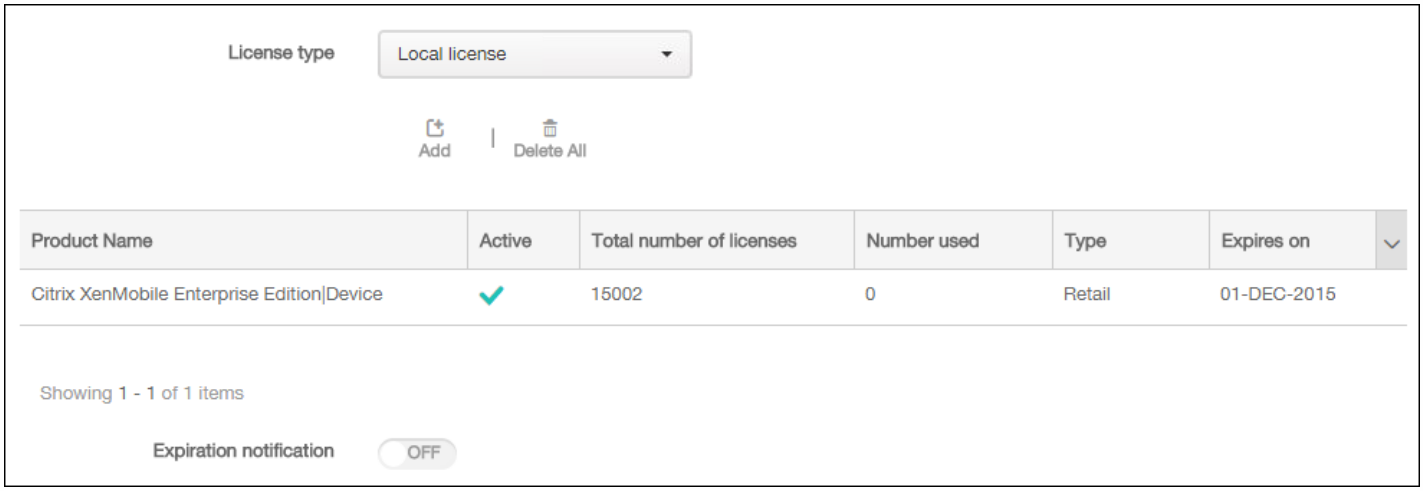


5. Compruebe que **License type** está establecido en **Local license** y, a continuación, haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New License**.



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.



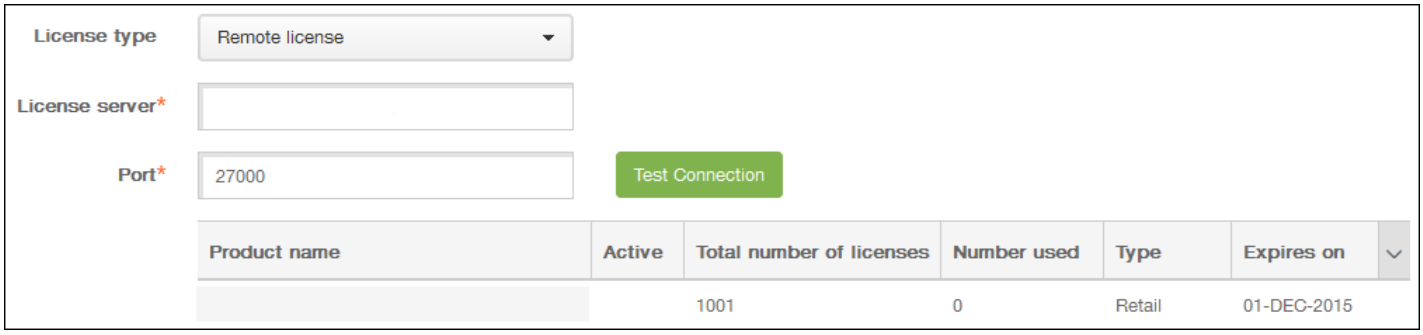
8. Cuando la licencia aparezca en la tabla de la página **Licensing**, actívela. Si se trata de la primera licencia de la tabla, la licencia se activa automáticamente.

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 ha 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** y **Port** y el botón **Test Connection**.



4. Configure estos parámetros:

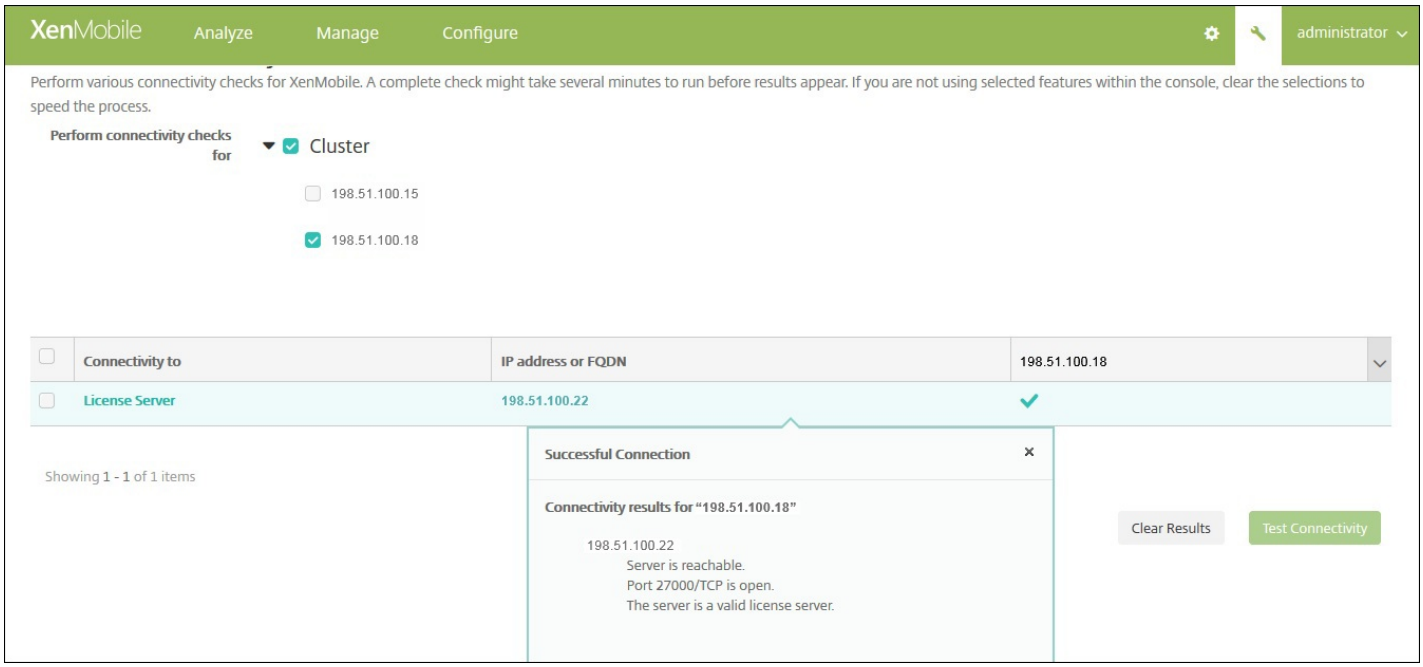
- **License server**. Escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor de licencias remoto.
- **Port**. Acepte el puerto predeterminado o escriba el número de puerto utilizado para comunicarse con el servidor de licencias.

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 lo 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**.

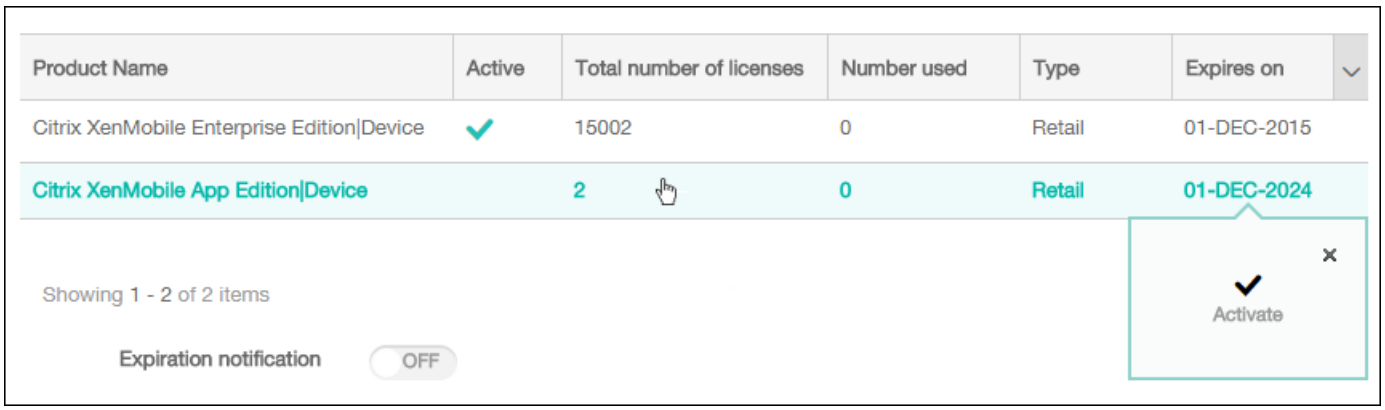


Para activar otra licencia

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**.

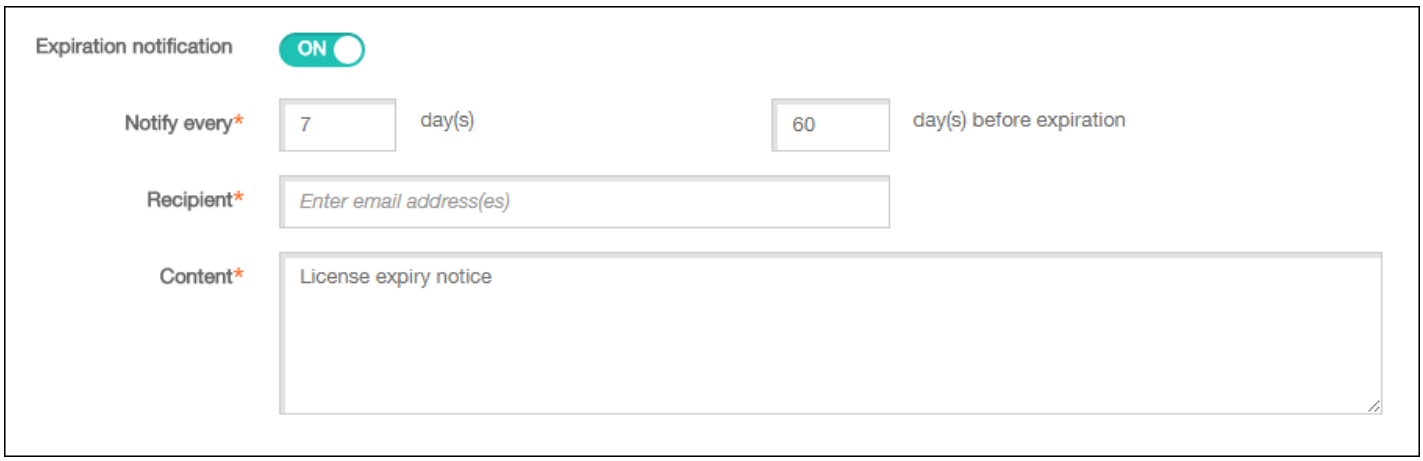
3. Haga clic en **Activate**. Se activa la licencia seleccionada.

> ## 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 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 estos 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**. Según los parámetros 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.

Cumplimiento del estándar FIPS 140-2

Feb 27, 2017

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: FIPS solo se admite en instalaciones locales de XenMobile Server. 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 los dispositivos Windows admitidos, 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 FIPS de NetScaler.

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

Apr 05, 2017

Las aplicaciones XenMobile 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 localizada 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.

Este artículo indica los idiomas respaldados en la versión más reciente de XenMobile.

Consola XenMobile y Self Help Portal

- Francés
- Alemán
- Japonés
- Coreano
- Portugués
- Chino simplificado

Aplicaciones XenMobile

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

Nota: A partir de la versión de la versión 10.4, las aplicaciones móviles Worx pasan a llamarse aplicaciones XenMobile. La mayoría de las aplicaciones individuales de XenMobile también cambian de nombre. Para obtener más información, consulte Acerca de aplicaciones XenMobile.

iOS y Android

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	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	Solo iOS
Árabe	X	X	X	X	X	X
Ruso	X	X	X	X	X	X
Turco	X	X	Solo Android			

Windows

	Secure Hub	**Secure Mail**	**Secure Web**
Francés	X	X	X
Alemán	X	X	X
Español	X	X	X
Italiano	X	X	X
Danés	X	X	X
Sueco	X	X	X

Respaldo para idiomas con escritura de derecha a izquierda

En la tabla siguiente, se resume el respaldo para texto de idiomas de Oriente Medio, para cada aplicación. X indica que la función está disponible para la plataforma. El respaldo para idiomas escritos de derecha a izquierda no está disponible para dispositivos Windows.

	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

Instalación y configuración

Feb 27, 2017

Antes de comenzar:

Puede usar esta lista de verificación para, antes de instalar, 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.

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.

Para conocer los pasos de instalación, consulte la sección Instalación de XenMobile más adelante en este artículo.

Lista de verificación previa a la instalación

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. Si configura un clúster, escriba todas las direcciones IP que necesita.	XenMobile	
	• 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.	NetScaler Gateway	

	Introduzca todas las redes internas y los segmentos de red a los que deben acceder los usuarios cuando se conectan a Secure Hub o NetScaler Gateway Plug-in si la opción de túnel dividido está activada.		
	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 The Citrix Licensing System.

	Requisitos previos	Componente	Escriba la ubicación
	Obtenga licencias universales del sitio Web de Citrix. Para obtener información más detallada, consulte Licencias en la documentación 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 más información, consulte la sección Autenticación en la documentación de 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.

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

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.	XenMobile NetScaler Gateway	

	NetScaler Gateway y XenMobile lo usan para enviar consultas a Active Directory.		

Conexiones entre XenMobile y NetScaler Gateway

	Requisitos previos	Componente	Escriba el parámetro
	Escriba el nombre de host de XenMobile.	XenMobile	
	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 Citrix Secure Hub

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 Secure Hub. Puede crear un segundo servidor virtual para habilitar las conexiones de usuario desde Citrix Receiver y los 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	NetScaler	

	ejecuta Secure Ticket Authority (STA) (solo para conexiones ICA).	Gateway	
	Escriba el nombre FQDN público de XenMobile.	NetScaler Gateway	
	Escriba el nombre FQDN público de Secure Hub.	NetScaler Gateway	

Instalación de XenMobile

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.

> **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 llevar a cabo lo siguiente. 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 llevar a cabo lo siguiente. 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.

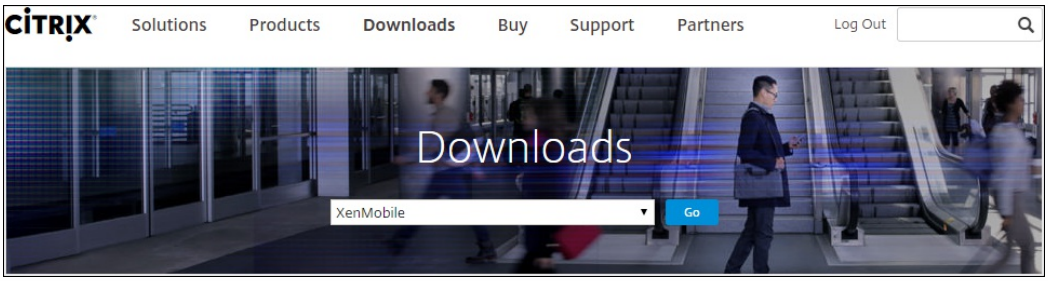
Modo FIPS 140-2. Si quiere instalar el servidor XenMobile en modo FIPS, necesitará completar una serie de requisitos previos como se describe en Configuración de FIPS.

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 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 de la edición de 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 selección 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. En Firmware, haga clic en la versión del software de dispositivo que quiera 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

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.

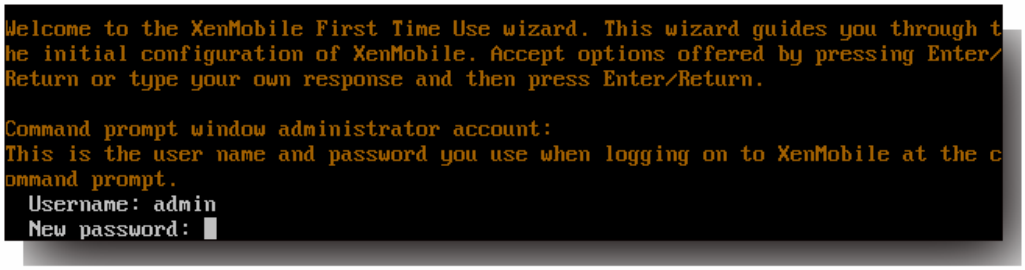
> **Nota**
>
> Cuando se utiliza un cliente Web de vSphere, se recomienda no configurar las propiedades de conexión de red a la hora de implementar la plantilla OVF en la página **Customize template**. Con esto, en una configuración de alta disponibilidad, se evita el problema con la dirección IP que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

2. Acceda a la consola de administración de XenMobile solamente con un nombre de dominio completo de XenMobile Server o las direcciones IP del nodo.

3. Inicie sesión y siga los pasos indicados en las pantallas iniciales de inicio de sesión.

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 (por ejemplo, asteriscos) cuando escriba la nueva contraseña. No aparece nada.

4. Proporcione la siguiente información de red y luego introduzca y para confirmar los parámetros:
   1. Dirección IP del servidor XenMobile

2. Máscara de red (Netmask)
3. Puerta de enlace predeterminada, que es la dirección IP de la puerta de enlace predeterminada en la zona desmilitarizada (DMZ)
4. Servidor DNS principal, que es la dirección IP del servidor DNS
5. Servidor DNS secundario (Secondary DNS server, si quiere)

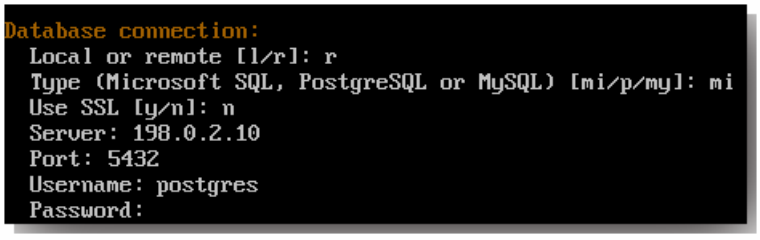
Nota: Las direcciones que se muestran en esta imagen y las imágenes siguientes no son operativas; se proporcionan simplemente como ejemplos.

5. Escriba y para aumentar la seguridad mediante la generación de una frase secreta aleatoria. También puede presionar n para proporcionar su propia frase secreta. Citrix recomienda teclear y 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, debería 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 más información acerca del estándar FIPS, consulte FIPS. Además, debe completar los requisitos previos, como se describe en Configuración de FIPS.

7. Proporcione la siguiente información para configurar la conexión con la base de datos:



1. La base de datos puede ser local o remota. Escriba l para "local" o r para "remota".
2. Seleccione el tipo de base de datos. Escriba mi para Microsoft SQL o p para PostgreSQL.
   Importante:

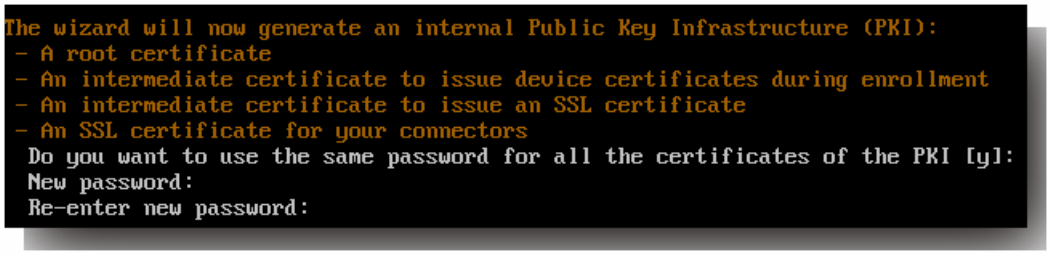
- Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile y se debe utilizar de forma local o remota solo en entornos de prueba.
- No se respalda la migración de la base de datos. Las bases de datos creadas en un entorno de prueba no se pueden mover a un entorno de producción.

3. Si lo prefiere, escriba y 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 su 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 quiere, escriba y para habilitar la organización en clúster de los nodos o las 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.

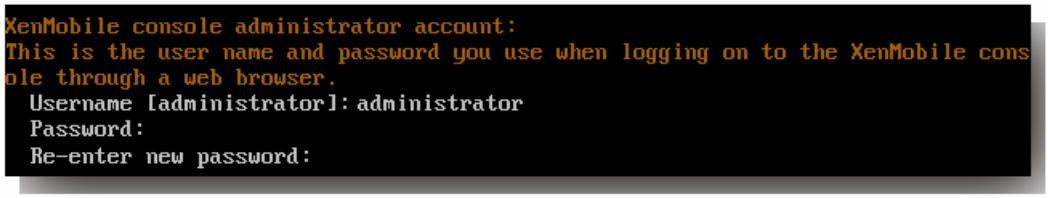
10. Presione **Entrar** para confirmar los parámetros.
11. Identifique los puertos de comunicación. Para obtener información más detallada acerca de los puertos y sus usos, consulte Requisitos de puertos.
    Nota: Para aceptar los puertos predeterminados, presione **Entrar** (Retorno en Mac).

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

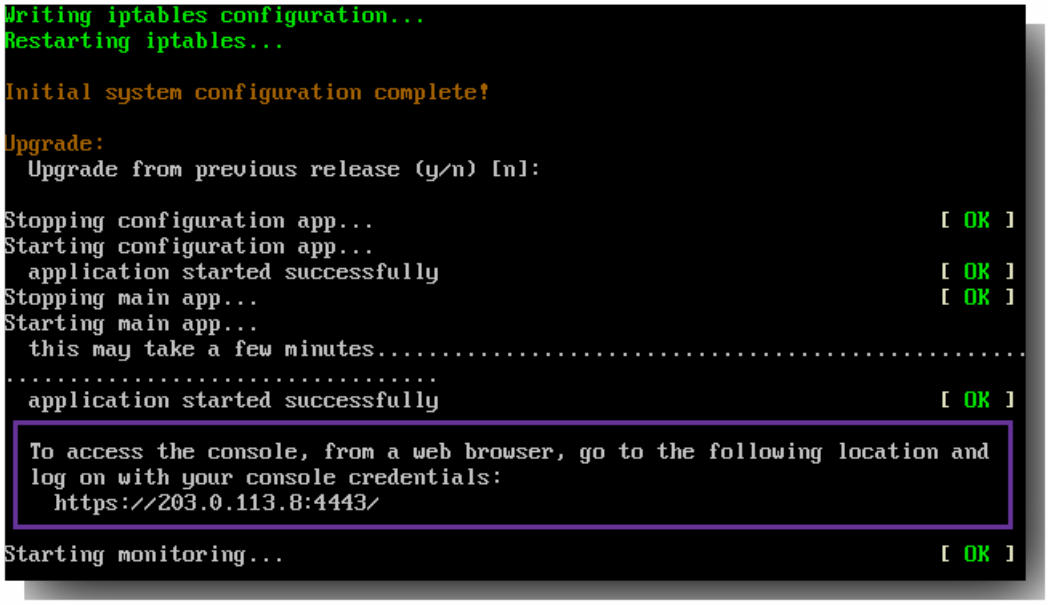


Importante: Si va a agrupar nodos o instancias de XenMobile en clúster, debe proporcionar contraseñas idénticas para los nodos subsiguientes.

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, presione n 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.

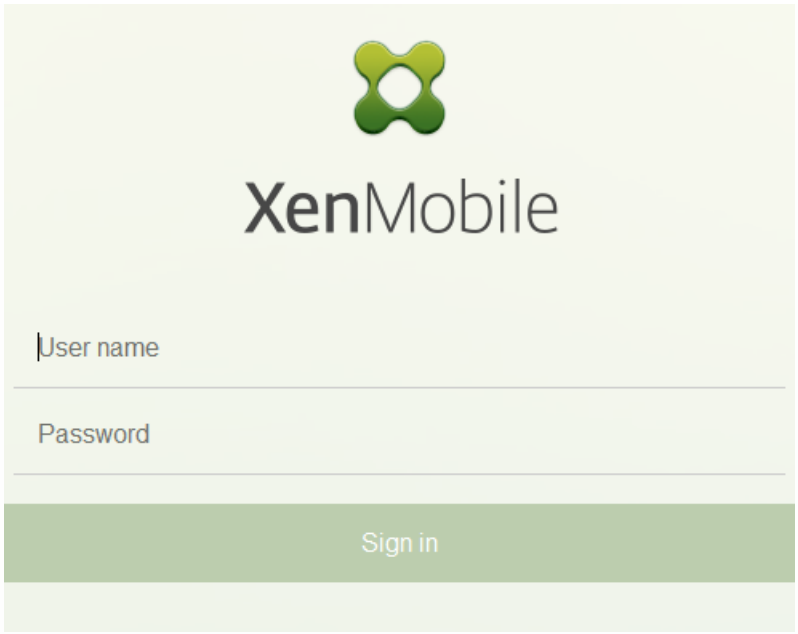


Configuración de XenMobile en un explorador Web

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. Si no se puede cargar una licencia, se utiliza una licencia de evaluación de 30 días. Para obtener más información sobre cómo agregar y configurar licencias y notificaciones de caducidad, consulte Licencias.

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 Certificate, haga clic en Import. Aparecerá el cuadro de diálogo Import.

6. Importe los certificados APNs y el certificado de escucha de SSL. Si desea administrar dispositivos iOS, necesita un certificado APNs. Para obtener más información sobre cómo trabajar con certificados, consulte Certificados.

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 más información sobre la configuración del servidor de notificaciones, consulte Notificaciones.

Requisito posterior: Reinicie el servidor XenMobile para activar los certificados.

Configuración de FIPS con XenMobile

Feb 27, 2017

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, 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 del servidor SQL. Si usó un certificado SSL autofirmado en lugar de un certificado público en el servidor SQL, 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 información más detallada, consulte Cómo cargar el certificado en XenMobile.

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 debe ser segura y la versión debe ser SQL Server 2012 o SQL Server 2014. Para proteger 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. Desmarque la casilla **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. Compruebe 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. Establezca el parámetro **Anónimo** en **habilitado**.

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

6. Compruebe que el archivo CER no esté bloqueado.

7. Vaya a 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, compruebe que ASP está habilitado en el servidor IIS de este modo.

   a. Abra **Administrador del servidor**.

   b. Vaya al asistente en **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 Servidor Web (IIS).

> **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: Sí
- Upload Root Certificate: Sí
- Copy o Import(i): i
- Enter HTTP URL to import: http://*FQDN del servidor IIS*/cert.cer
- Server: *FQDN de 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.

Configuración de la agrupación en clústeres

Feb 27, 2017

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 el equilibrador de carga de MDM y una dirección IP privada para MAM.
- Certificados de servidor.
- Una dirección IP libre para la dirección IP virtual de NetScaler Gateway.

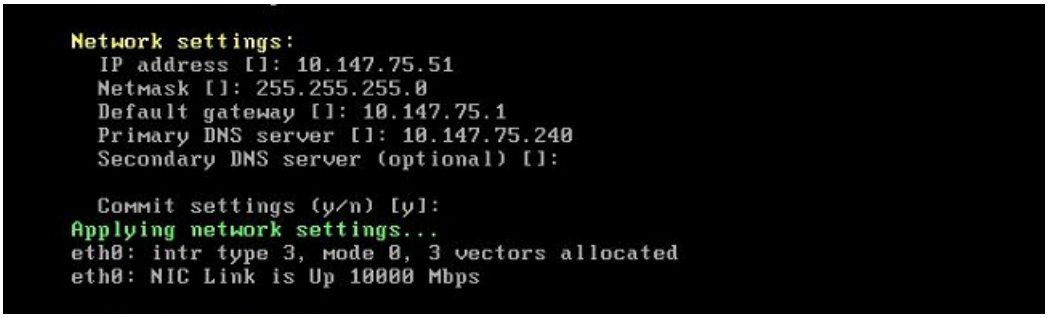
Para ver gráficos de referencia con las arquitecturas de XenMobile 10.x en configuraciones en clúster, consulte Arquitectura.

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.

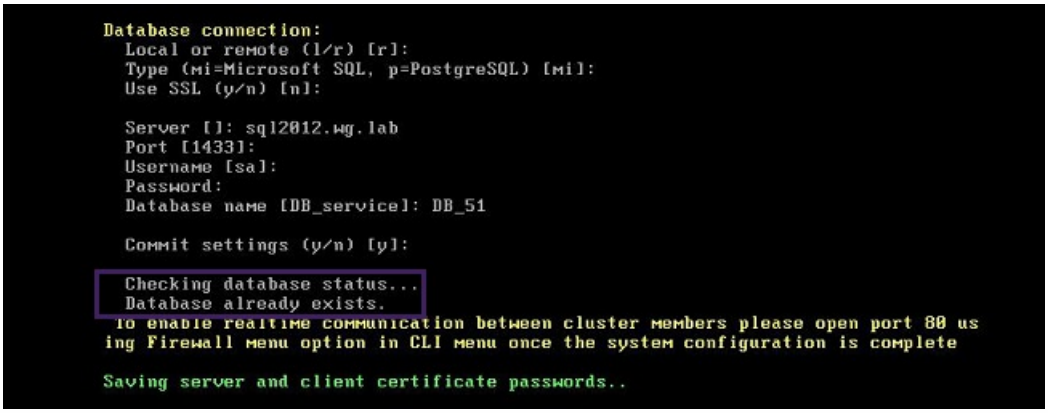
2. Facilite los datos de la configuración de red tal y como se muestra en la imagen siguiente.



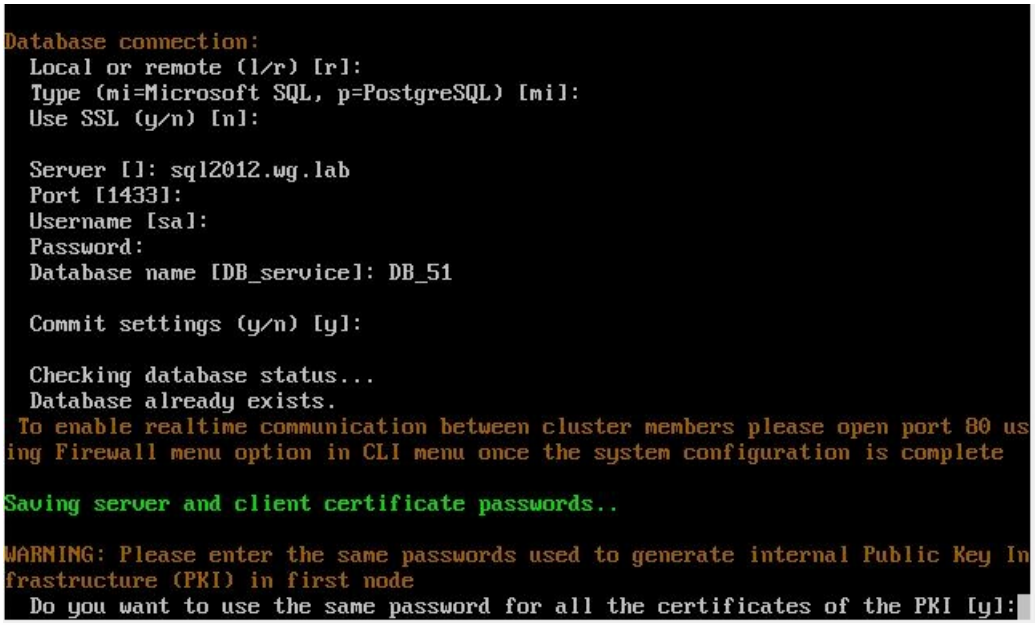
3. Si quiere usar la contraseña predeterminada para la protección de datos, escriba y; o escriba n e introduzca una nueva contraseña.

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

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

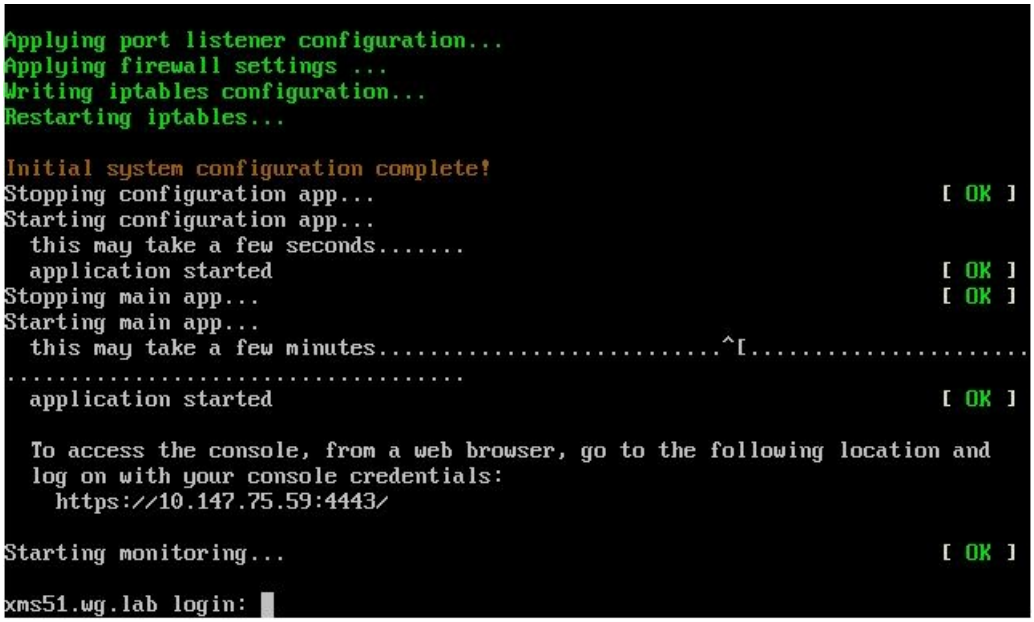


6. Introduzca las mismas contraseñas para los certificados proporcionados a la primera máquina virtual.



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

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



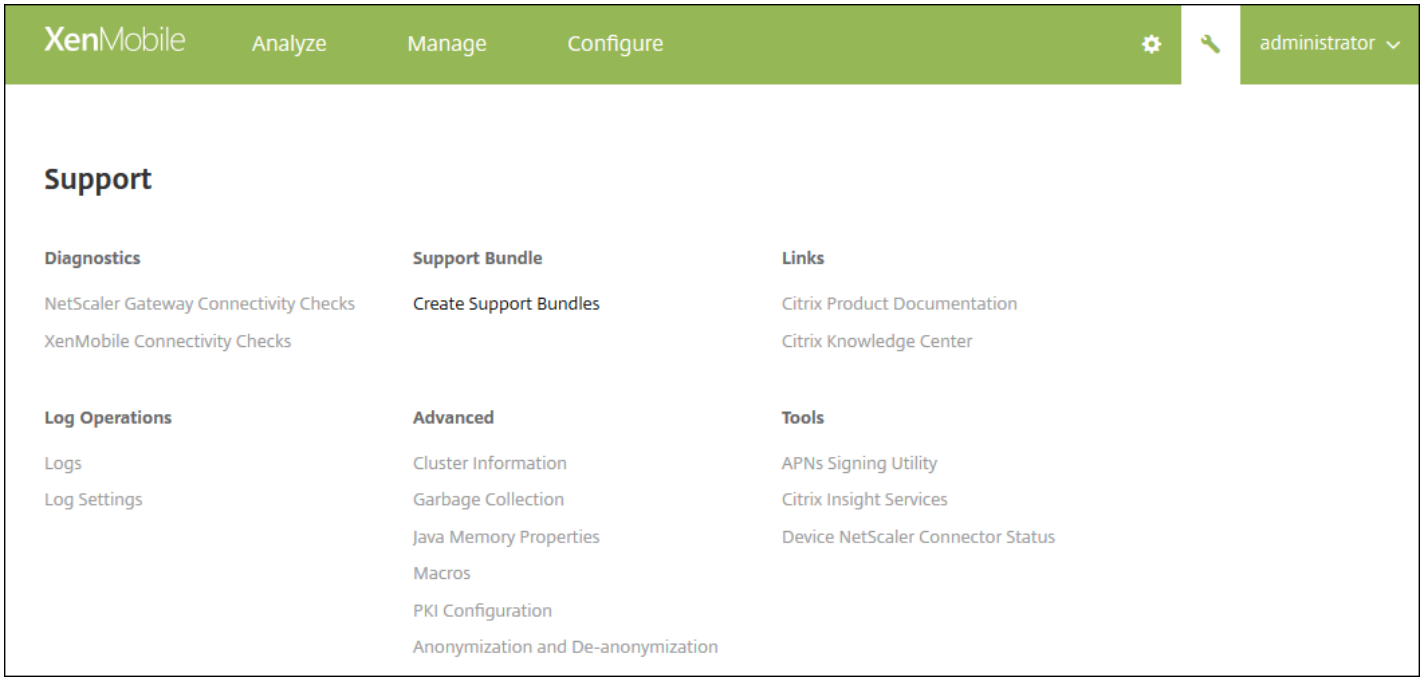
Nota: Este cuadro de diálogo de inicio de sesión es idéntico al cuadro de diálogo del inicio de sesión de la primera máquina virtual. Esta coincidencia sirve para confirmar que ambas máquinas virtuales utilizan el mismo servidor de base de datos.

8. Use el nombre de dominio completo (FQDN) de XenMobile para abrir la consola de XenMobile en un explorador Web.

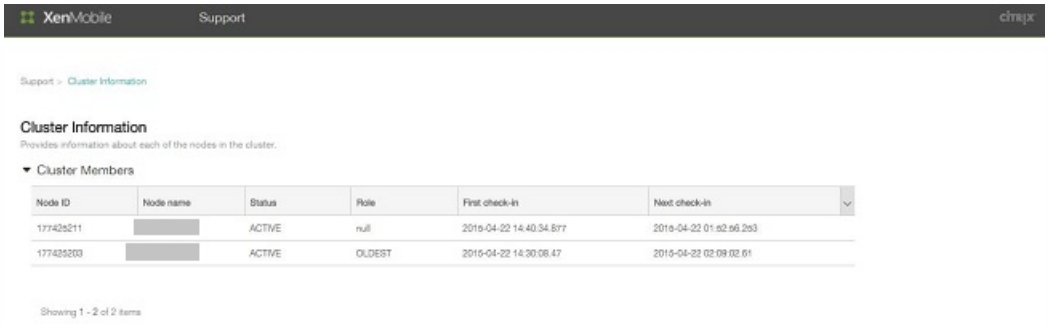
9 En la consola de XenMobile, haga clic en el icono con forma de llave inglesa, situado en la esquina superior derecha de la consola.

Se abrirá la página **Support**.

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.



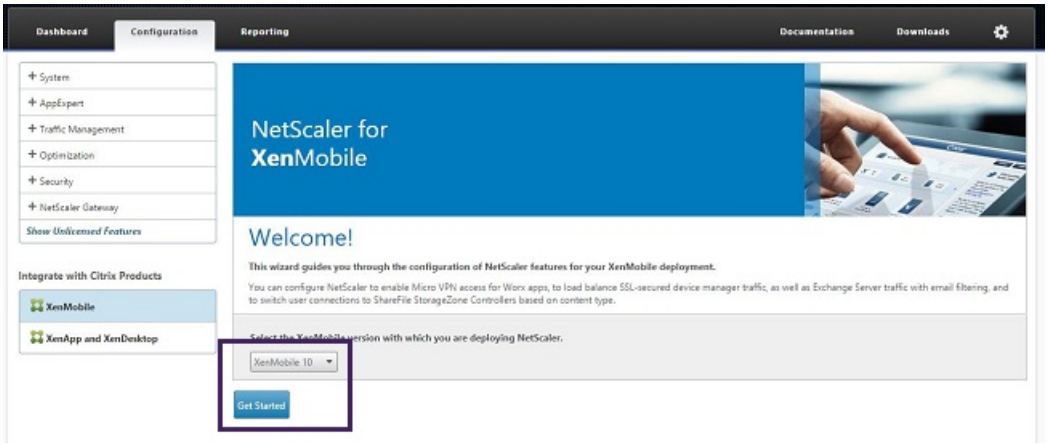
Puede agregar otros nodos siguiendo los mismos pasos. El primer clúster agregado al nodo tiene el rol de **OLDEST**. Los clústeres agregados después, mostrarán el rol **NONE** o **null**.

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

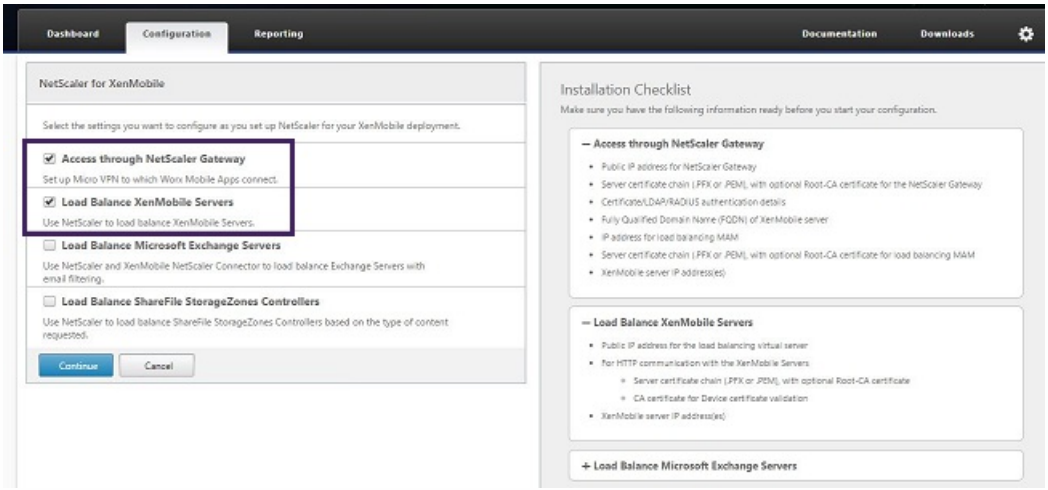
Después de agregar los nodos necesarios como miembros del clúster de XenMobile, deberá equilibrar la carga de esos nodos para poder acceder a los clústeres. La carga se equilibra mediante el asistente de XenMobile disponible en NetScaler 10.5.x. Siga los pasos de este procedimiento para equilibrar la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

1. Inicie sesión en NetScaler.

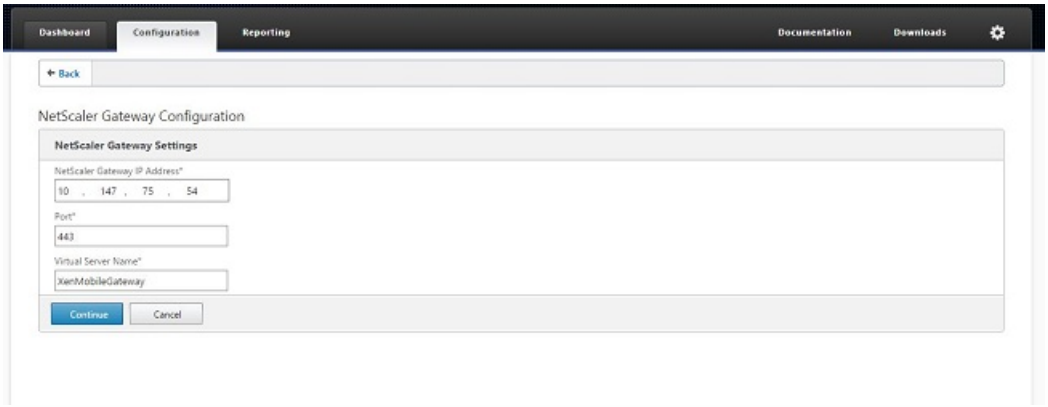
2. En la ficha Configuration, haga clic en XenMobile y en Get Started.



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

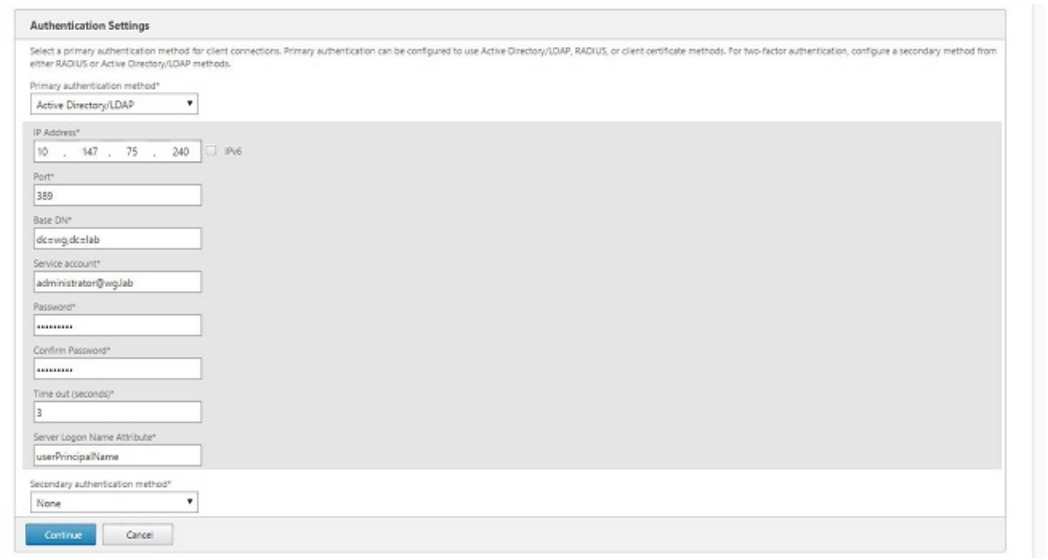


4. Introduzca la dirección IP de NetScaler Gateway y haga clic en Continue.



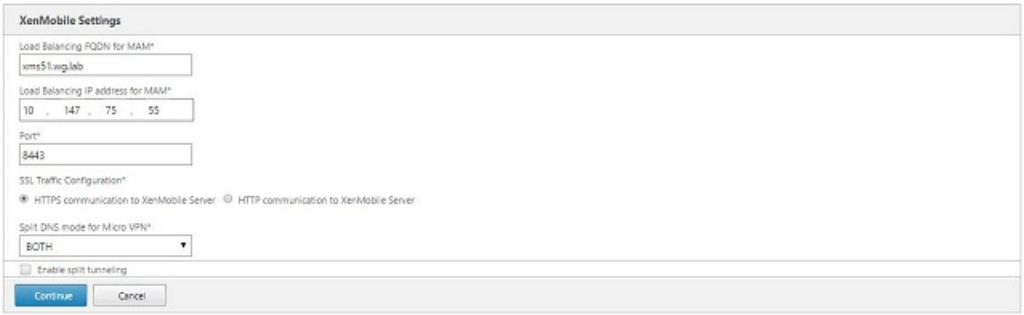
5. Vincule el certificado del servidor a la dirección IP virtual de NetScaler Gateway. Para ello, lleve a cabo una de las siguientes acciones y, a continuación, haga clic en Continue.
   - En Use existing certificate, elija el certificado del servidor de la lista.
   - Haga clic en la ficha Install Certificate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

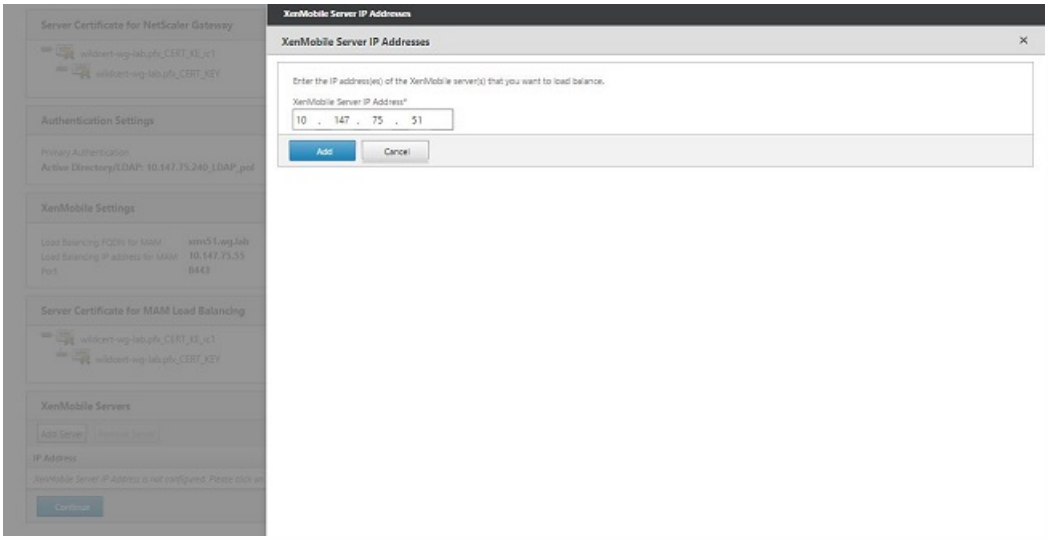


Nota: Compruebe que el nombre de dominio completo perteneciente a la dirección IP virtual de equilibrio de carga para MAM y el nombre de dominio completo de XenMobile coinciden.

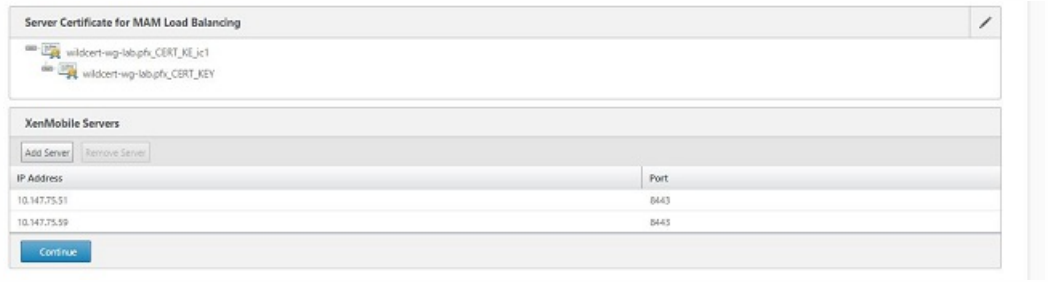
8. Si quiere usar el modo de puente SSL (HTTPS), marque HTTPS communication to XenMobile Server. En cambio, si quiere usar la descarga de SSL, marque HTTP communication to XenMobile Server, como se muestra en la imagen anterior. Dada la finalidad de este artículo, se opta por el modo de puente SSL (HTTPS).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

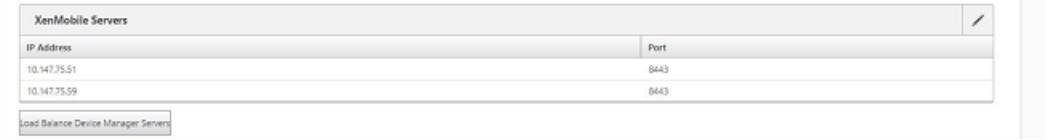
11. Introduzca la dirección IP del nodo de XenMobile y, a continuación, haga clic en Add.



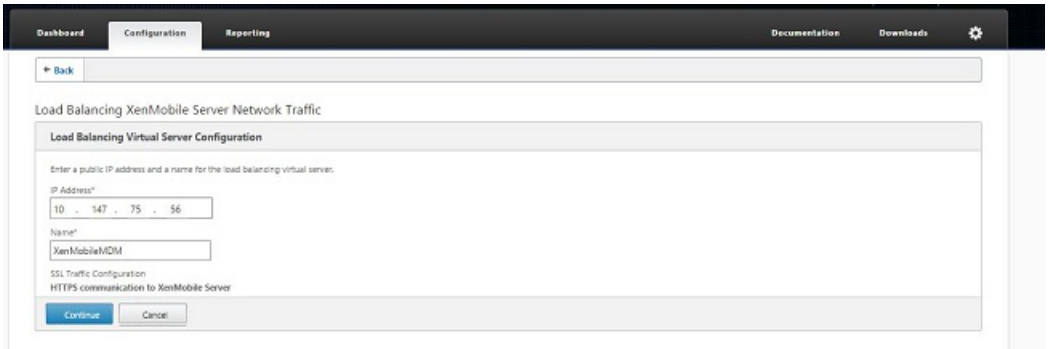
12. Repita los pasos 10 y 11 para agregar nodos de XenMobile adicionales que formen parte del clúster de XenMobile. Verá todos los nodos de XenMobile que haya agregado. Haga clic en Continue.



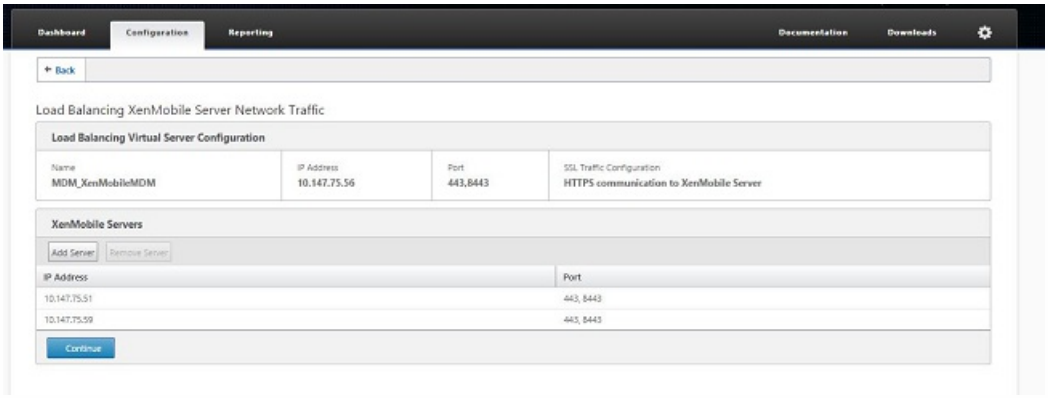
13. Haga clic en Load Balance Device Manager Servers para continuar con la configuración del equilibrio de carga para MDM.



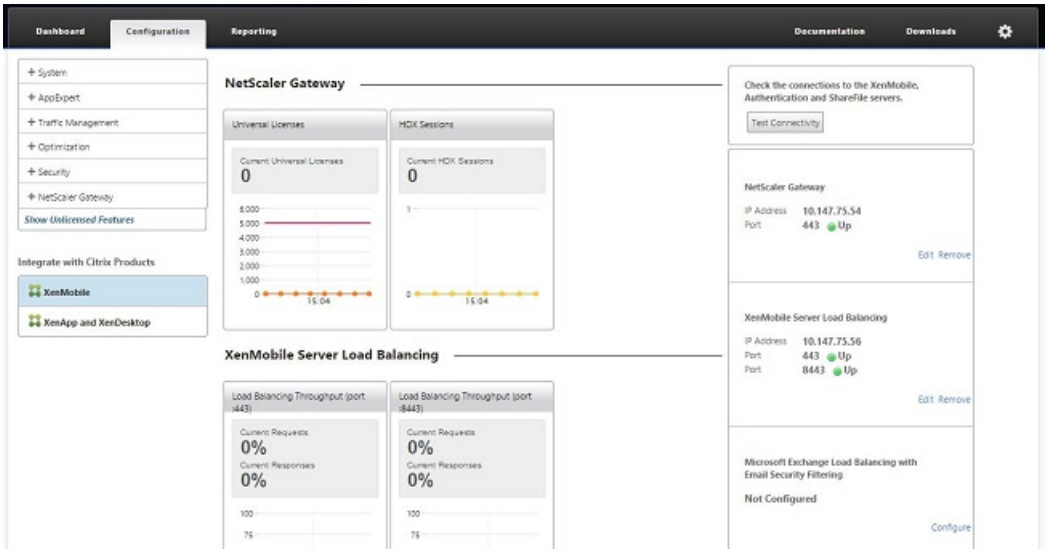
14. Introduzca la dirección IP que se utilizará como la IP de equilibrio de carga para MDM y, a continuación, haga clic en Continue.



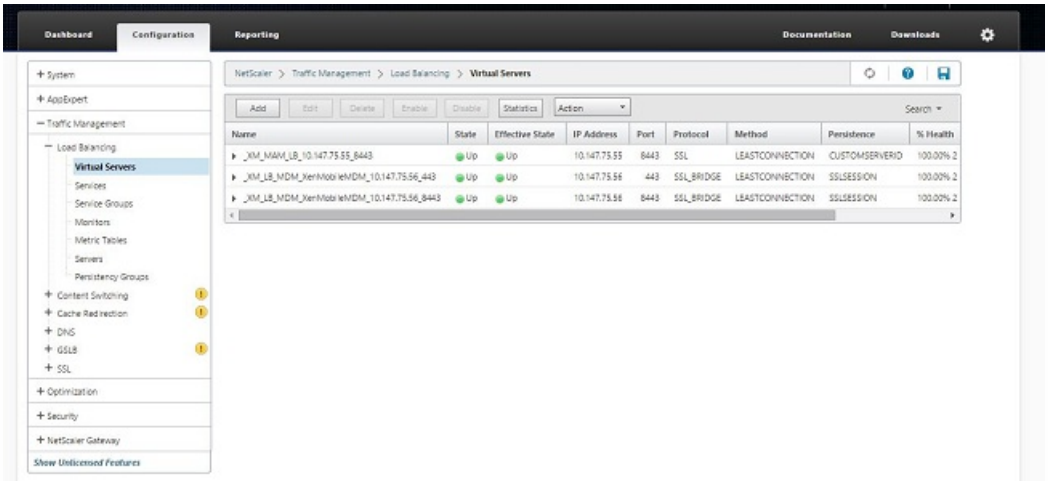
15. Una vez que vea los nodos de XenMobile en la lista, haga clic en Continue y, a continuación, en Done para finalizar el proceso.



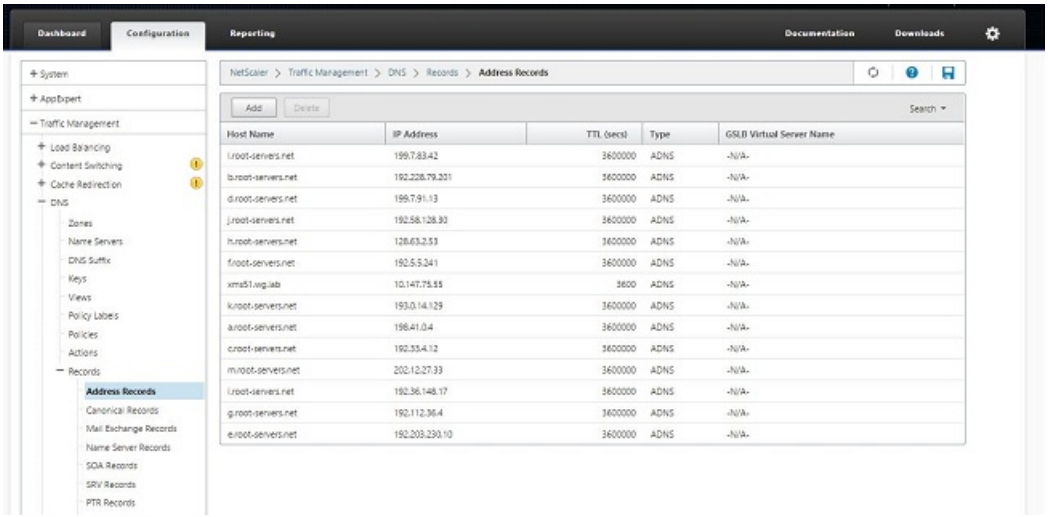
Verá el estado de la dirección IP virtual en la página XenMobile.



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

Feb 27, 2017

Puede planificar y configurar implementaciones de XenMobile que contengan varios sitios para la recuperación ante desastres con la ayuda de una estrategia de conmutación por error activa-pasiva. Para obtener más información, consulte el artículo Disaster Recovery de XenMobile Deployment Handbook.

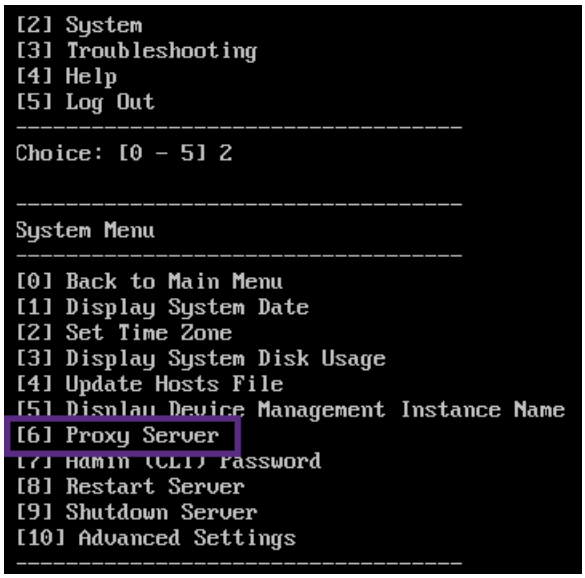
Cómo habilitar servidores proxy

Feb 27, 2017

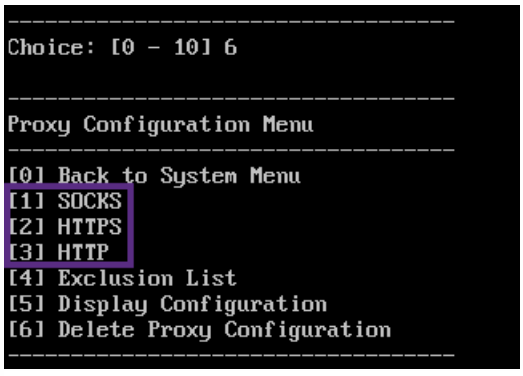
Si desea controlar el tráfico saliente a Internet, puede configurar un servidor proxy en XenMobile para transportar dicho tráfico. Para ello, debe configurar el servidor proxy mediante la interfaz de línea de comandos (CLI). Tenga en cuenta que la configuración del servidor proxy requiere reiniciar el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

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

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



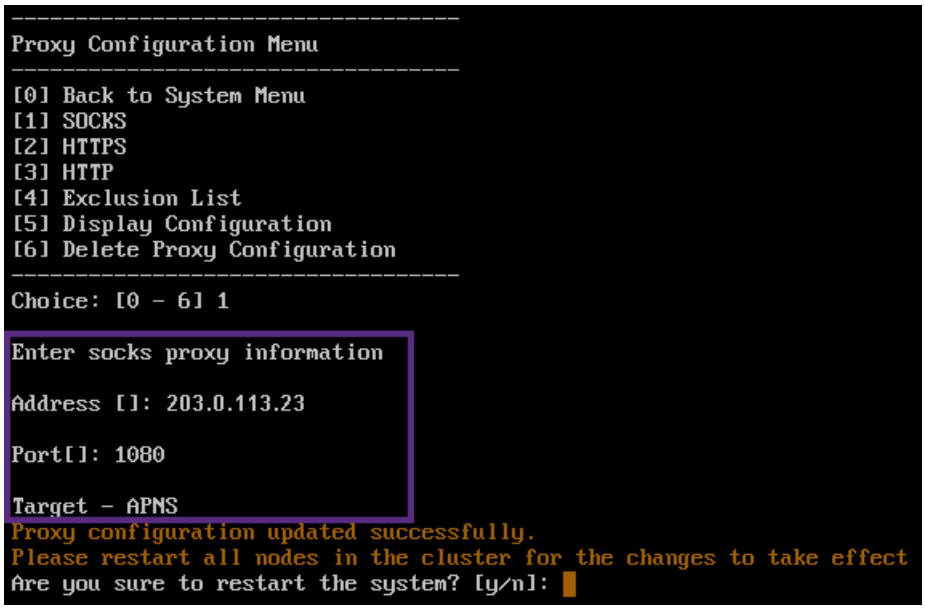
3. En el menú de configuración de proxy, escriba **1** para seleccionar SOCKS, **2** para seleccionar HTTPS o **3** para seleccionar HTTP.



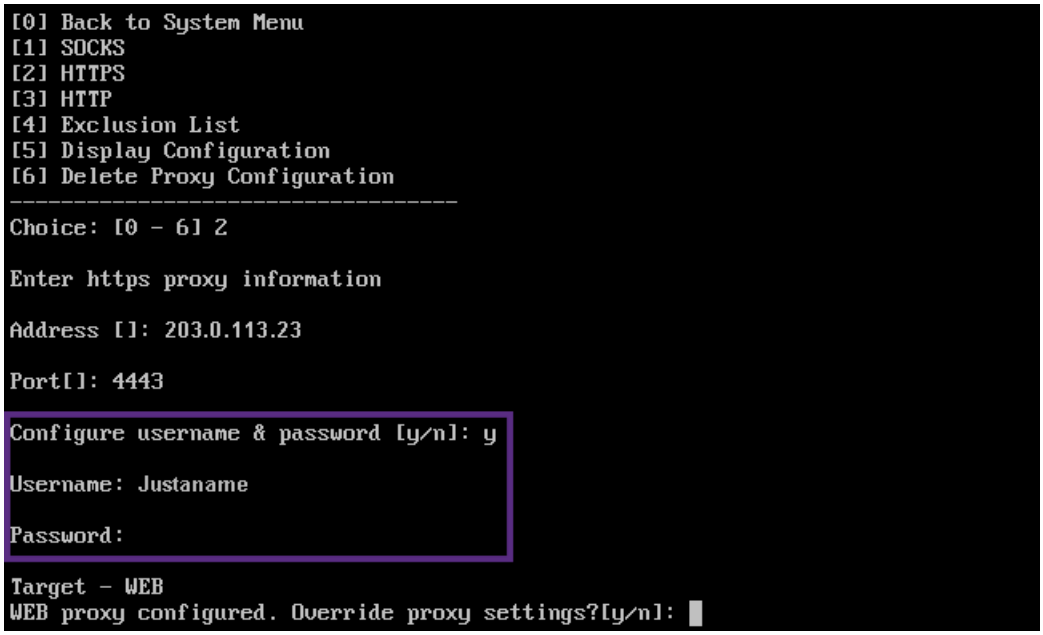
4. Introduzca la dirección IP del servidor proxy, el número de puerto y el destino. Consulte la tabla siguiente para ver los tipos de destino admitidos para cada tipo de servidor proxy.

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, escriba **y** y, a continuación, escriba el nombre de usuario y la contraseña.



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

Propiedades de servidor

Jun 06, 2017

XenMobile tiene muchas propiedades que corresponden a operaciones de servidor. En este artículo, se describen muchas de las propiedades del servidor, y también se explica cómo agregar, modificar o eliminar propiedades de servidor.

Algunas propiedades son claves personalizadas. Para agregar una clave personalizada, haga clic en **Add** y, a continuación, en **Key**, elija **Custom Key**.

Para obtener información sobre las propiedades que se configuran normalmente, consulte Propiedades de servidor en el manual virtual de XenMobile.

Definiciones de las propiedades del servidor

Add Device Always

Si tiene el valor **true**, XenMobile agrega un dispositivo a la consola de XenMobile, incluso aunque falle la inscripción, para poder ver qué dispositivos intentaron inscribirse. El valor predeterminado es **false**.

AG Client Cert Issuing Throttling Interval

El período de gracia entre la generación de certificados. Este intervalo evita que XenMobile genere varios certificados para un dispositivo en un período corto de tiempo. Citrix recomienda no modificar este valor. El valor predeterminado es de **30** minutos.

Audit Log Cleanup Execution Time

La hora a la que debe comenzar la limpieza del registro de auditoria, con el formato HH:MM am o pm. Ejemplo: 04:00 a.m. El valor predeterminado es **02:00 a.m**.

Audit Log Cleanup Interval (in Days)

La cantidad de días que XenMobile conserva 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 XenMobile conserva los registros de auditoría. El valor predeterminado es **7**.

auth.ldap.connect.timeout
auth.ldap.read.timeout

Para compensar las respuestas LDAP lentas, Citrix recomienda que agregue propiedades de servidor a las siguientes claves personalizadas.

Key: **Custom Key**
Key: **auth.ldap.connect.timeout**

Value: **60000**
Display name: **auth.ldap.connect.timeout=60000**
Description: LDAP connection timeout

Key: **Custom Key**
Key: **auth.ldap.read.timeout**
Value: **60000**
Display name: **auth.ldap.read.timeout=60000**
Description: LDAP read timeout

Certificate Renewal in Seconds

Especifica con cuántos segundos de antelación XenMobile empieza a renovar certificados previamente a su caducidad. Por ejemplo, si un certificado caduca el 30 de diciembre y esta propiedad está establecida en 30 días, XenMobile intenta renovar el certificado si el dispositivo se conecta entre el 1 de diciembre y el 30 de diciembre. El valor predeterminado es **2592000** segundos (30 días).

Connection Timeout

El tiempo de espera de la sesión inactiva, en minutos, transcurrido el cual XenMobile cierra la conexión TCP con un dispositivo. La sesión permanece abierta. Se aplica a dispositivos Android y Windows CE y Remote Support. El valor predeterminado es **5** minutos.

Connection Timeout to Microsoft Certification Server

Los segundos durante los que XenMobile espera una respuesta del servidor de certificados. Si el servidor de certificados es lento y tiene una gran cantidad de tráfico, aumente este valor a 60 segundos o más. Un servidor de certificados que no responda al cabo de 120 segundos necesita mantenimiento. El valor predeterminado es **15000** milésimas de segundo (15 segundos).

Default deployment channel

Determina la forma en que XenMobile implementa un recurso en un dispositivo: a nivel de usuario (**DEFAULT_TO_USER**) o a nivel de dispositivo. El valor predeterminado es **DEFAULT_TO_DEVICE**.

Deploy Log Cleanup (in Days)

La cantidad de días que XenMobile conserva los registros de implementación. El valor predeterminado es **7**.

Disable SSL Server Verification

Si **True**, inhabilita la validación de certificados SSL de servidor cuando se cumplen todas las condiciones siguientes:

- Ha habilitado la autenticación basada en certificados en el servidor XenMobile

- El servidor de CA de Microsoft es el emisor del certificado

- Ha firmado el certificado una CA interna en cuya raíz no confía el servidor XenMobile.

El valor predeterminado es **True**.

Enable Console

Si el valor es **true**, permite el acceso de usuarios a la consola de Portal Self Help. El valor predeterminado es **true**.

Habilitar o inhabilitar la captura de estadísticas de hibernación para diagnósticos

Si el valor es **True**, se habilita la captura de estadísticas de hibernación para ayudar a resolver problemas de rendimiento de aplicaciones. La hibernación es un componente que se utiliza para las conexiones de XenMobile a Microsoft SQL Server. 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. El valor predeterminado es **False**.

Enable Notification Trigger

Habilita o inhabilita las notificaciones de cliente de Secure Hub. El valor **true** habilita las notificaciones. El valor predeterminado es **true**.

Full Pull of ActiveSync Allowed and Denied Users

Los segundos durante los que XenMobile espera una respuesta desde el dominio al ejecutar un comando de PowerShell para obtener la información de referencia de los dispositivos de ActiveSync. El valor predeterminado es **28800** segundos.

hibernate.c3p0.max_size

Esta clave personalizada determina la cantidad máxima de conexiones a la base de datos de SQL Server que puede abrir XenMobile. XenMobile utiliza el valor que se especifica para esta clave personalizada como el límite máximo. Las conexiones se abren solo si las necesita. Debe establecer sus parámetros en función de la capacidad del servidor de la base de datos. Para obtener más información, consulte Tuning XenMobile Operations. Configure la clave de este modo. El valor predeterminado es **1000**.

Key: **hibernate.c3p0.max_size**
Value: **500**
Display name: **hibernate.c3p0.max_size=*nnn***
Description: DB connections to SQL

hibernate.c3p0.timeout

Esta clave personalizada determina el tiempo de espera de inactividad. El valor predeterminado es **300**.

Key: **Custom Key**
Key: **hibernate.c3p0.timeout**
Value: **30**
Display name: **hibernate.c3p0.timeout=30**
Description: Database idle timeout

Identifies if telemetry is enabled or not

Identifica si la telemetría (Customer Experience Improvement Program o CEIP) está habilitada. Puede elegir si participar en CEIP al instalar o actualizar XenMobile. Si XenMobile experimenta 15 cargas fallidas consecutivas, se inhabilita la telemetría. El valor predeterminado es **false**.

Inactivity Timeout in Minutes

Si la propiedad de servidor **WebServices timeout type** es **INACTIVITY_TIMEOUT**, esta propiedad define la cantidad de minutos tras los que XenMobile cierra la sesión de un administrador inactivo que haya hecho lo siguiente:

- Ha utilizado la API pública de XenMobile para servicios REST para acceder a la consola de XenMobile

- Ha utilizado la API pública de XenMobile para servicios REST para acceder a una aplicación externa. Un tiempo de espera de **0** significa que no se cierra la sesión de un usuario inactivo.

El valor predeterminado es **5**.

iOS Device Management Enrollment Auto-Install Enabled

Si el valor es True, esta propiedad reduce la cantidad de interacción del usuario necesaria durante la inscripción de dispositivos. Los usuarios deben hacer clic en **Root CA install** (si es necesario) y **MDM Profile install**.

iOS Device Management Enrollment First Step Delayed

Después de que un usuario introduzca sus credenciales durante la inscripción del dispositivo, este valor de propiedad especifica el tiempo de espera antes de pedir la CA raíz. Citrix recomienda no modificar esta propiedad a menos que haya mucha latencia o problemas de velocidad en la red. En ese caso, no configure un valor superior a 5000 milésimas de segundo (5 segundos). El valor predeterminado es **1000** milésimas de segundo (1 segundo).

iOS Device Management Enrollment Last Step Delayed

Durante la inscripción de dispositivos, este valor de propiedad especifica cuánto tiempo se espera entre la instalación del perfil de MDM y el inicio del agente en el dispositivo. Citrix recomienda no modificar esta propiedad a menos que haya mucha latencia o problemas de velocidad en la red. En ese caso, no configure un valor superior a 5000 milésimas de segundo (5 segundos). El valor predeterminado es **1000** milésimas de segundo (1 segundo).

iOS Device Management Identity Delivery Mode

Especifica si XenMobile distribuye el certificado MDM a los dispositivos que usan **SCEP** (recomendado por razones de seguridad) o **PKCS12**. En el modo de PKCS12, el par de claves se genera en el servidor y no se lleva a cabo ninguna negociación. El valor predeterminado es **SCEP**.

iOS Device Management Identity Key Size

Define el tamaño de las claves privadas para las identidades MDM, el servicio de perfiles de iOS y las identidades del agente iOS de XenMobile. El valor predeterminado es **1024**.

iOS Device Management Identity Renewal Days

Especifica con cuántos días de antelación XenMobile empieza a renovar certificados previamente a su fecha de caducidad. Por ejemplo, si un certificado caduca en 10 días y esta propiedad tiene un valor de **10** días, si un dispositivo se conecta 9 días antes de caducar el certificado, XenMobile emite uno nuevo. El valor predeterminado es **30** días.

iOS MDM APNS Private Key Password

Esta propiedad contiene la contraseña de APNs, que XenMobile necesita para enviar notificaciones push a los servidores de Apple.

iOS MDM APNS Private Key Password

Esta propiedad contiene la contraseña de APNs, que XenMobile necesita para enviar notificaciones push a los servidores de Apple.

Length of Inactivity Before Device Is Disconnected

Especifica el tiempo que un dispositivo puede permanecer inactivo, incluida la última autenticación, antes de que XenMobile lo desconecte. El valor predeterminado es **7** días.

MAM Only Device Max

Esta clave personalizada limita la cantidad de dispositivos de solo MAM que puede inscribir un usuario. Configure la clave de este modo. El **valor 0** permite inscripciones ilimitadas de dispositivos.

Key = **number.of.mam.devices.per.user**
Value = **5**
Display name = **MAM Only Device Max**
Description = Limits the number of MAM devices each user can enroll.

NetScaler Single Sign-On

Si el valor es **False**, se inhabilita la función de respuesta de XenMobile durante el inicio de sesión único Single Sign-On desde NetScaler a XenMobile. XenMobile usa la función de respuesta 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**.

Number of consecutive failed uploads

Muestra la cantidad de fallos consecutivos durante cargas de Customer Experience Improvement Program (CEIP). XenMobile aumenta el valor cuando falla una carga. Después de 15 fallos de carga, XenMobile inhabilita el programa CEIP, también conocido como "telemetría". Para obtener más información, consulte la propiedad de servidor **Identifies if telemetry is enabled or not**. XenMobile restablece el valor a **0** si una carga se realiza correctamente.

Number of Users Per Device

La cantidad máxima de usuarios que pueden inscribir el mismo dispositivo en MDM. El valor **0** significa que una cantidad ilimitada de usuarios puede inscribir el mismo dispositivo. El valor predeterminado es **0**.

Pull of Incremental Change of Allowed and Denied Users

Los segundos durante los que XenMobile espera una respuesta desde el dominio al ejecutar un comando de PowerShell para obtener la información nueva de dispositivos de ActiveSync. El valor predeterminado es **180** segundos.

Read Timeout to Microsoft Certification Server

Los segundos durante los que XenMobile espera una respuesta del servidor de certificados al llevar a cabo una lectura. Si el servidor de certificados es lento y tiene una gran cantidad de tráfico, puede aumentar este valor a 60 segundos o más. Un servidor de certificados que no responda al cabo de 120 segundos necesita mantenimiento. El valor predeterminado es **15000** milésimas de segundo (15 segundos).

REST Web Services

Permite el servicio Web REST. El valor predeterminado es **true**.

Retrieves devices information in chunks of specified size

Este valor se usa internamente para subprocesamientos múltiples durante exportaciones de dispositivos. Si el valor es superior, un solo subproceso analiza varios dispositivos. Si el valor es inferior, varios subprocesos se hacen cargo de los dispositivos. Reducir el valor puede aumentar el rendimiento de exportaciones y la lista de dispositivos exportados, aunque puede reducir la memoria disponible. El valor predeterminado es **1000**.

Session Log Cleanup (in Days)

La cantidad de días que XenMobile conserva los registros de sesión. El valor predeterminado es **7**.

Modo de servidor

Determina si XenMobile se ejecuta en modo MAM, MDM o ENT (Enterprise), que corresponden a los modos Administración de aplicaciones, Administración de dispositivos o Administración de dispositivos y aplicaciones 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.

Si dispone de una licencia de XenMobile MDM Edition, el modo de servidor efectivo es siempre MDM, independientemente de cómo se haya establecido el modo de servidor en Server Properties. Si tiene una licencia de MDM Edition, no puede habilitar la administración de aplicaciones definiendo el modo del servidor en MAM o ENT.

Sus licencias son para esta edición	Quiere que los dispositivos se registren en este modo	Defina la propiedad Server Mode con el valor
Enterprise / Advanced	Modo MDM	MDM
Enterprise / Advanced	Modo MDM+MAM	ENT
MDM	Modo MDM	MDM

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. Para licencias Enterprise y Advanced, el modo efectivo del servidor coincide con el modo del servidor, si este es **ENT** o **MDM**. Si el modo del servidor es **MAM**, el modo efectivo del servidor es ENT.

XenMobile agrega el modo de servidor a los registros del servidor cada vez que se activa o se elimina una licencia, y cuando se cambia el modo de servidor en Server Properties. Para obtener más información sobre cómo crear y ver archivos de registro, consulte Registros y Cómo ver y analizar archivos de registros en XenMobile.

ShareFile configuration type

Especifica el tipo de almacenamiento de ShareFile. **ENTERPRISE** habilita el modo ShareFile Enterprise. **CONNECTORS** solo ofrece acceso a los conectores StorageZone que haya creado desde la consola de XenMobile. El valor predeterminado es **NONE**, lo que muestra la vista inicial de la pantalla **Configure > ShareFile**, desde donde elige entre los conectores y ShareFile Enterprise. El valor predeterminado es **NONE**.

Static Timeout in Minutes

Si la propiedad de servidor **WebServices timeout type** es **STATIC_TIMEOUT**, esta propiedad define la cantidad de minutos tras los que XenMobile cierra la sesión de un administrador que haya utilizado:

- La API pública de XenMobile para servicios REST para acceder a la consola de XenMobile

- La API pública de XenMobile para servicios REST para acceder a una aplicación externa

El valor predeterminado es **60**.

Trigger Agent Message Suppression

Habilita o inhabilita la mensajería de cliente de Secure Hub. El valor **false** habilita la mensajería. El valor predeterminado es **true**.

Trigger Agent Sound Suppression

Habilita o inhabilita los sonidos de cliente de Secure Hub. El valor **false** habilita los sonidos. El valor predeterminado es **true**.

Unauthenticated App Download for Android Devices

Si es **True**, puede descargar aplicaciones autoalojadas en dispositivos Android que ejecutan Android for Work. XenMobile necesita esta propiedad si la opción de Android for Work para suministrar una URL de descarga 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

Solo se utiliza para versiones anteriores de Secure Hub que no validan los tíquets de un solo uso. Si es **False**, puede descargar aplicaciones no autenticadas desde XenMobile en dispositivos Windows. El valor predeterminado es **False**.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device

Si es **true**, XenMobile Mail Manager usa el identificador de ActiveSync como argumento para el método asWipeDevice. El valor predeterminado es **false**.

Users only from Exchange

Si es **true**, inhabilita la autenticación de usuario para los usuarios de ActiveSync Exchange. El valor predeterminado es **false**.

VPP baseline interval

El intervalo mínimo tras el que XenMobile vuelve a importar, de Apple, las licencias del programa PCV. Actualizar la información de las licencias garantiza que XenMobile refleja todos los cambios (por ejemplo, si elimina manualmente una aplicación importada del programa PCV). De forma predeterminada, XenMobile actualiza el punto de referencia para las licencias del programa PCV cada **720** minutos como mínimo.

Si tiene una gran cantidad de licencias PCV instaladas (por ejemplo, más de 50.000), Citrix recomienda aumentar el intervalo del punto de referencia para reducir la frecuencia de la importación de licencias y el consumo de recursos que eso conlleva. Si espera cambios frecuentes en las licencias PCV por parte de Apple, Citrix recomienda reducir el valor para mantener XenMobile actualizado con los cambios. El intervalo mínimo entre dos puntos de referencia es de 60

minutos. Además, XenMobile lleva a cabo una importación delta cada 60 minutos, para capturar los cambios realizados desde la última importación. Por eso, si el intervalo del punto de referencia de PCV es de 60 minutos, el intervalo entre los puntos de referencia puede retrasarse hasta 119 minutos.

WebServices Timeout Type

Especifica cómo hacer caducar un token de autenticación obtenido desde la API pública. Si es **STATIC_TIMEOUT**, XenMobile considera caducado un token de autenticación una vez transcurrido el tiempo especificado como valor de la propiedad de servidor **Static Timeout in Minutes**.

Si es **INACTIVITY_TIMEOUT**, XenMobile considera caducado un token de autenticación si el token ha permanecido inactivo durante el tiempo especificado como valor de la propiedad de servidor **Inactivity Timeout in Minutes**. El valor predeterminado es **STATIC_TIMEOUT**.

Windows Phone MDM Certificate Extended Validity (5y)

El periodo de validez del certificado del dispositivo emitido por MDM para Windows Phone y Tablet. Los dispositivos usan un certificado de dispositivo para autenticarse en el servidor MDM durante la administración de dispositivos. Si **true**, el período de validez es de cinco años. Si **false**, el período de validez es de dos años. El valor predeterminado es **true**.

Windows WNS Channel - Number of Days Before Renewal

La frecuencia de renovación de ChannelURI. El valor predeterminado es **10** días.

Windows WNS Heartbeat Interval

El tiempo que espera XenMobile antes de conectarse a un dispositivo tras haberse conectado a él cinco veces cada 3 minutos. El valor predeterminado es de **6** horas.

XAM One-Time Ticket

El período de tiempo, en milisegundos, durante el cual un token de autenticación de un solo uso (OTT) se considera válido para descargar una aplicación. Esta propiedad se utiliza con las propiedades **Unauthenticated App download for Android** y **Unauthenticated App download for Windows**. Esas propiedades especifican si permitir descargas no autenticadas de aplicaciones. El valor predeterminado es **3600000**.

XenMobile MDM Self Help Portal console max inactive interval (minutes)

El tiempo, en minutos, transcurrido el cual XenMobile cierra la sesión de un usuario inactivo en el Self Help Portal de XenMobile. Un tiempo de espera de **0** significa que no se cierra la sesión del usuario inactivo. El valor predeterminado es **30**.

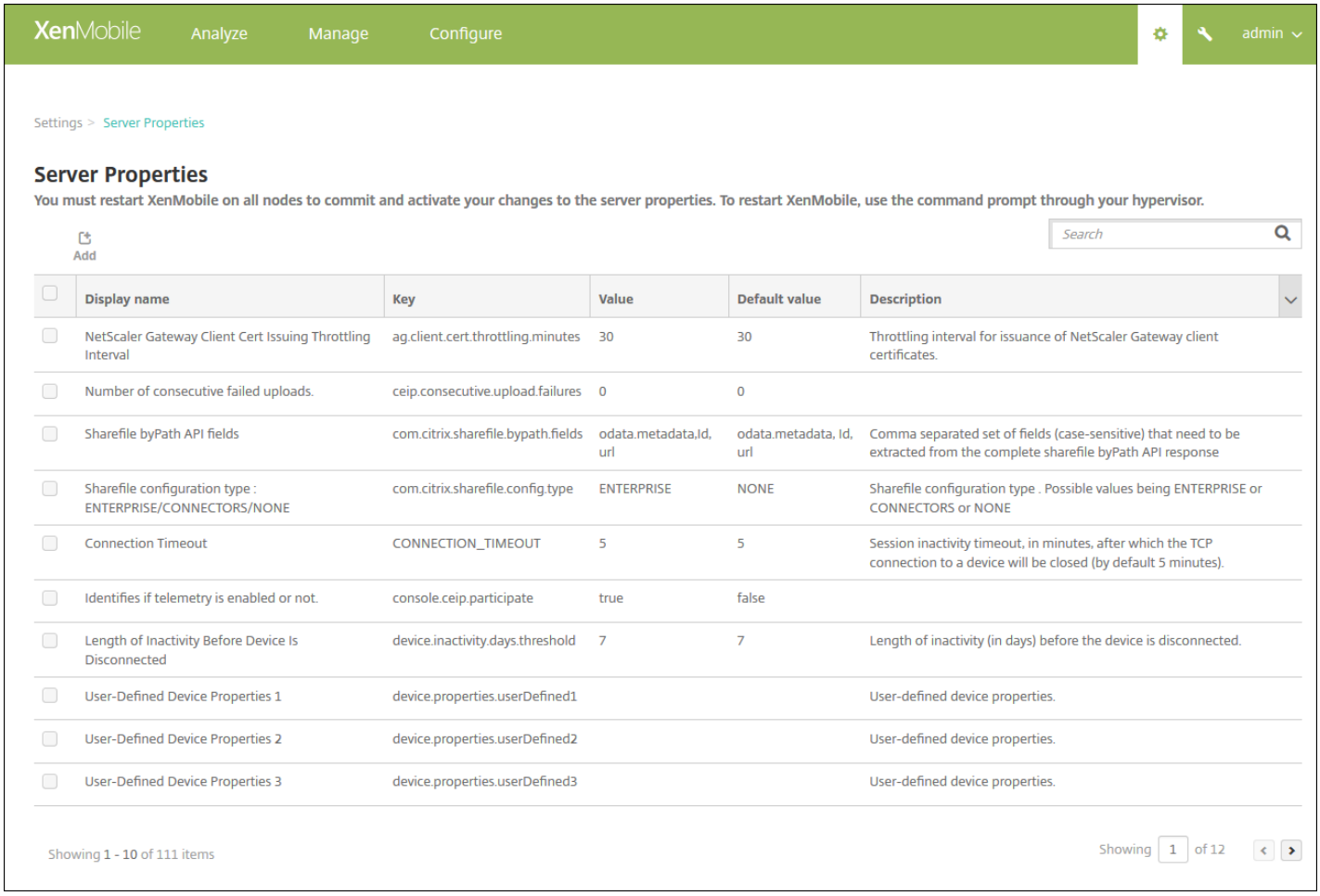
Cómo agregar, modificar o eliminar propiedades de servidor

En XenMobile, se pueden aplicar propiedades al servidor. Después de realizar cambios, debe reiniciar XenMobile en todos los nodos para confirmar y activar esos cambios.

> **Nota**
>
> Para reiniciar XenMobile, use la línea de comandos a través del hipervisor.

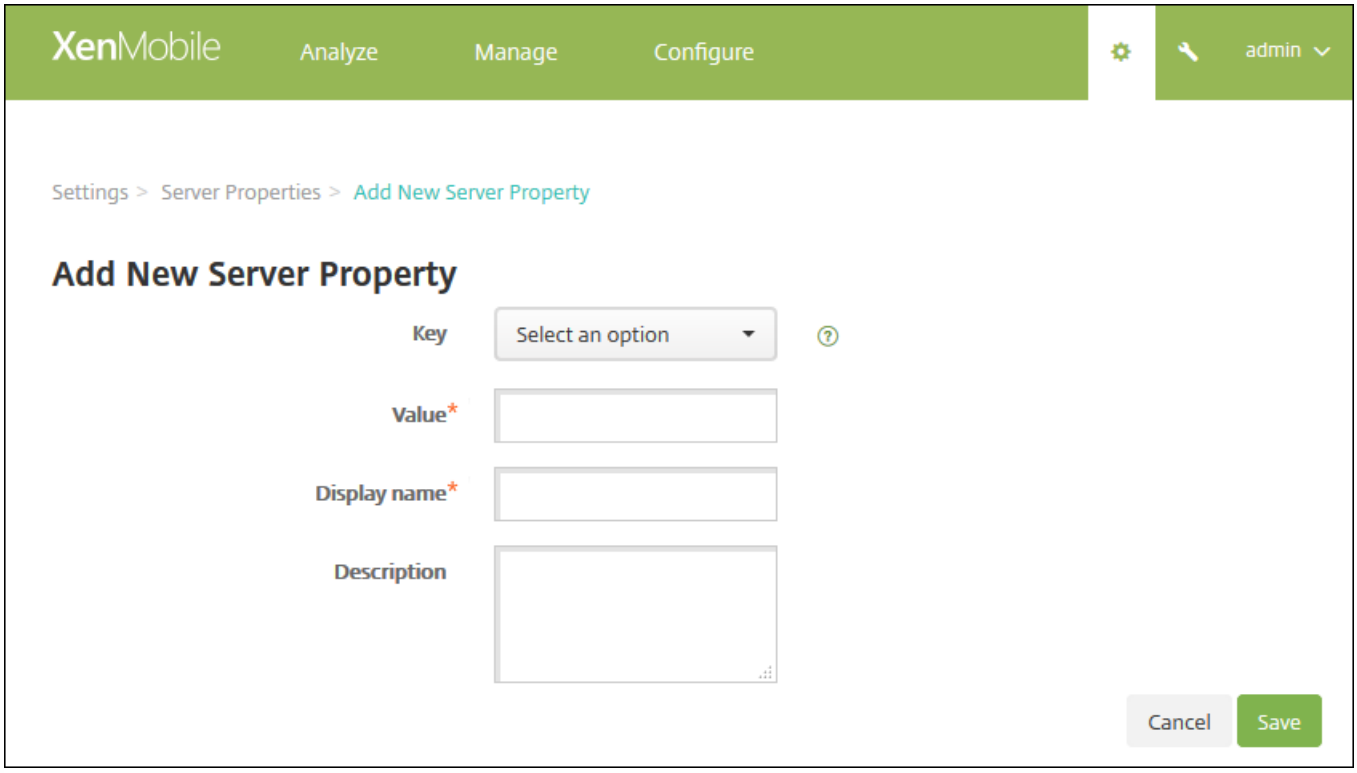
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.

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 estos parámetros:

- **Key**. En la lista, seleccione la clave apropiada. Las claves distinguen mayúsculas y minúsculas. Póngase en contacto con la asistencia de Citrix antes de modificar los valores de propiedad o para 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 propiedad de servidor.

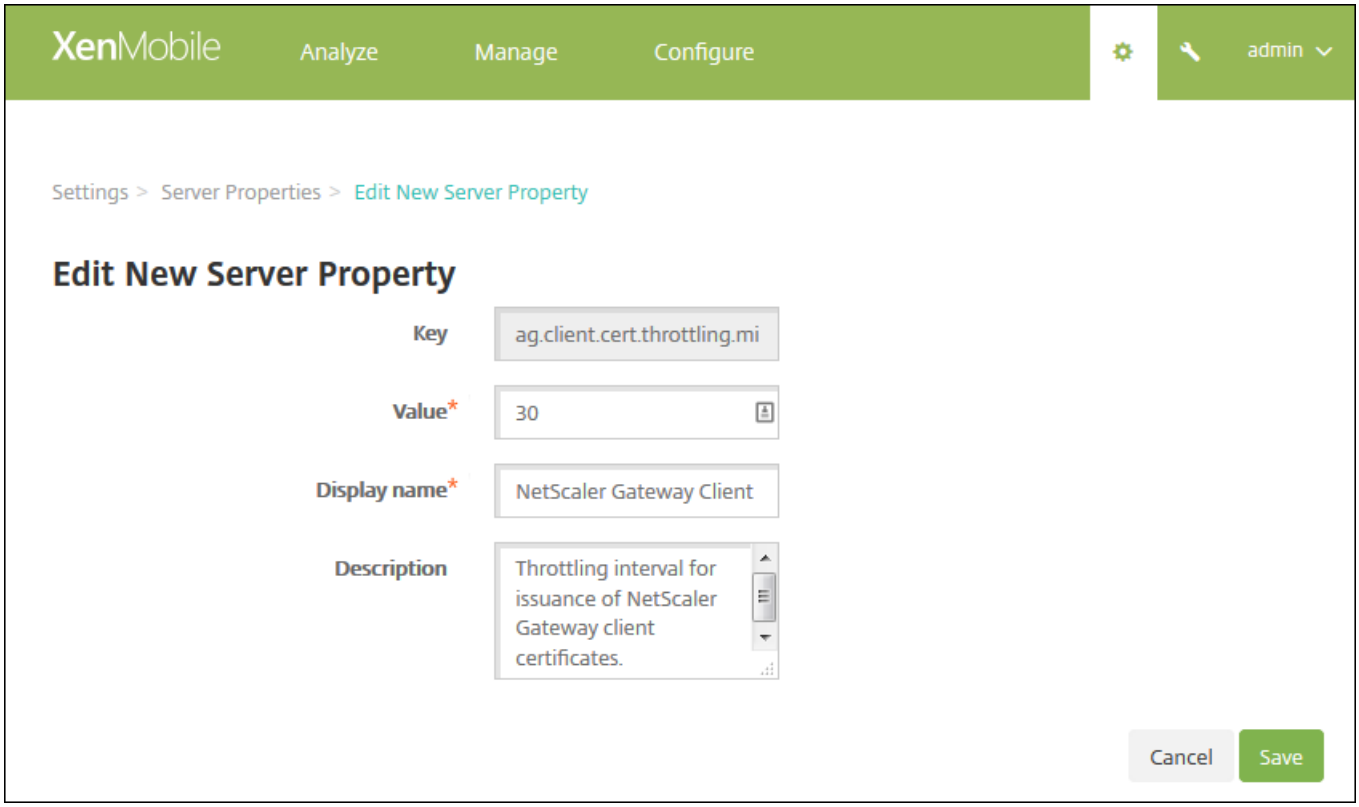
3. Haga clic en **Save**.

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. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece 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**.

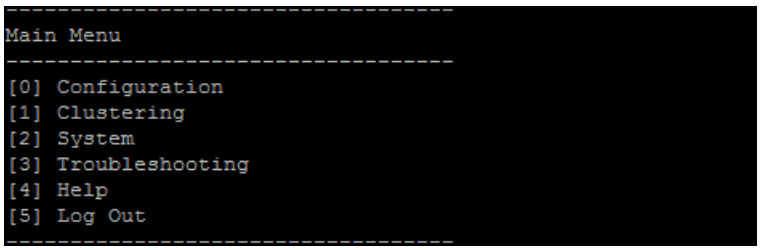
Opciones de la interfaz de línea de comandos

Apr 13, 2017

Para una instalación local del servidor XenMobile, puede acceder a las opciones de línea de comandos en cualquier momento de este modo:

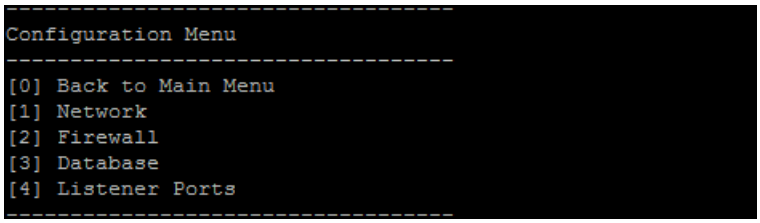
- **Desde el hipervisor donde instaló XenMobile**. En el hipervisor, seleccione la máquina virtual importada de XenMobile, inicie la vista del símbolo del sistema e inicie sesión en su cuenta de administrador de XenMobile. Para obtener información más detallada, consulte la documentación de su hipervisor.
- **A través de SSH, si SSH está habilitado en el firewall**. Inicie sesión en su cuenta de administrador de XenMobile.

Puede realizar varias tareas de configuración y solución de problemas desde la línea de comandos. A continuación, dispone del menú superior de la interfaz de la línea de comandos.

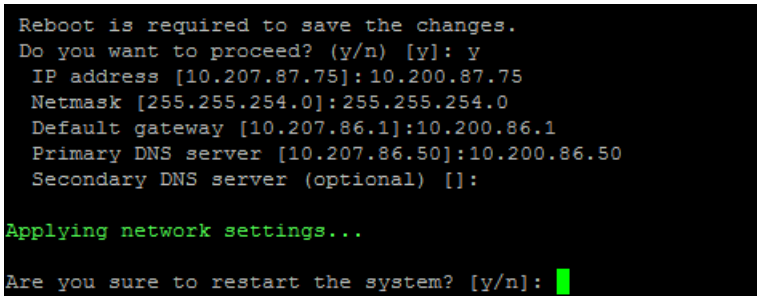


Opciones de Configuration

A continuación, dispone de ejemplos del **menú Configuration** (Configuración) y los parámetros que aparecen en cada opción.



[1] Network (Red)



[2] Firewall

```
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]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  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) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] Database (Base de datos)

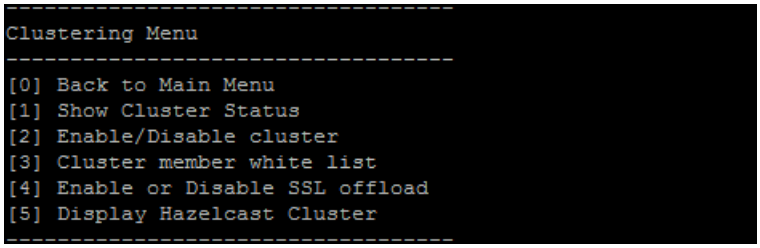
```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

[4] Listener Ports (Puertos de escucha)

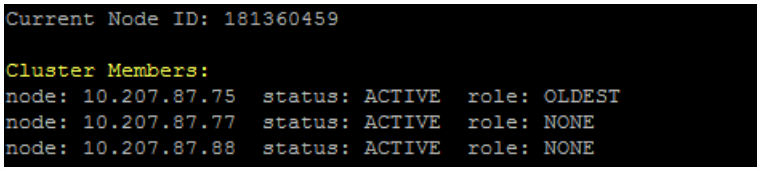
```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Opciones de Clustering

A continuación, dispone de ejemplos del **menú Clustering** (Clústeres) y los parámetros que aparecen en cada opción.



[1] Show Cluster Status (Mostrar estado de clúster)



[2] Enable/Disable cluster (Habilitar o inhabilitar clúster)

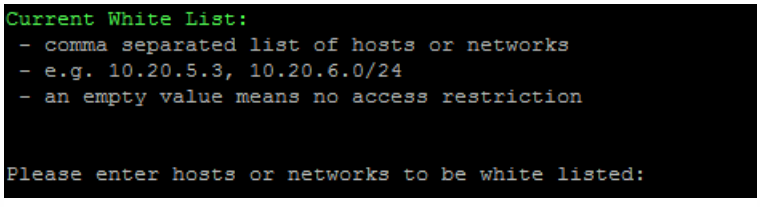
Si opta por habilitar el uso de clústeres, aparecerá el siguiente mensaje:

> To enable realtime communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. (Para habilitar la comunicación en tiempo real entre los miembros de los clústeres, abra el puerto 80 desde la opción del menú Firewall en el menú CLI.) Asimismo, configure la lista blanca de acceso en los parámetros de Firewall para el acceso restringido.

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. (Ha optado por inhabilitar el uso de clústeres. No se necesita el acceso al puerto 80. Puede inhabilitarlo.)

[3] Cluster member white list (Lista blanca de miembros de clúster)



[4] Enable or disable SSL offload (Habilitar o inhabilitar descarga de SSL)

Si opta por habilitar o inhabilitar la descarga de SSL, aparecerá el siguiente mensaje:

> Enabling SSL offload will open port 80 for everyone. (Habilitar la descarga de SSL abrirá el puerto 80 a todos los usuarios.) Please configure Access white list under Firewall settings for restricted access. (Configure la lista blanca de acceso en los parámetros de Firewall para el acceso restringido.)

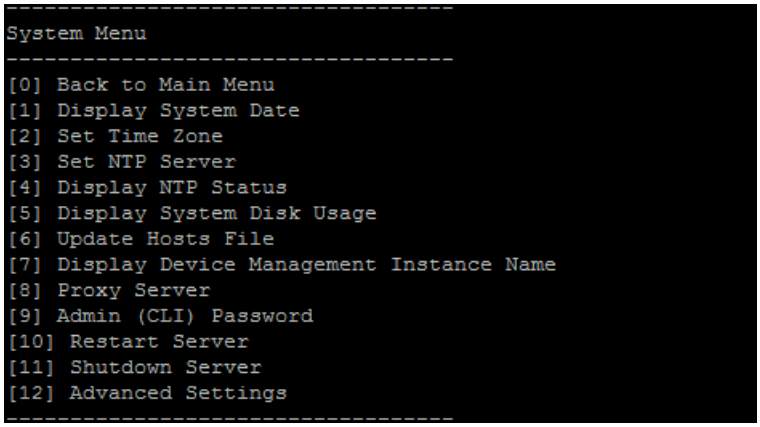
[5] Display Hazelcast Cluster (Mostrar clúster Hazelcast)

Si opta por ver el clúster Hazelcast, aparecerán las siguientes opciones:

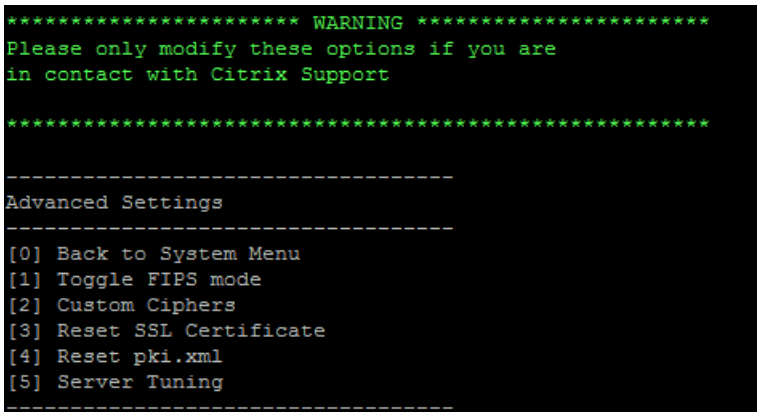
> Hazelcast Cluster Members (Miembros del clúster Hazelcast):
>
> [Lista de direcciones IP]
>
> NOTA: Si uno de los nodos configurados no forma parte del clúster, reinicie ese nodo.

Opciones de System

Desde el **menú System**, puede mostrar o configurar información a nivel del sistema, reiniciar o apagar el servidor, o bien acceder a **Advanced Settings**.



[12] Advanced Settings (Parámetros avanzados)



Las opciones **Server Tuning** contienen los parámetros: tiempo de espera de la conexión al servidor, cantidad máxima de

conexiones (por puerto) y cantidad máxima de subprocesos (por puerto).

Opciones de Troubleshooting

A continuación, dispone de ejemplos del **menú Troubleshooting** (Solución de problemas) y los parámetros que aparecen en cada opción.

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----------------------------------
```

[1] Network Utilities (Utilidades de red)

```
-----------------------------------
Network Menu
-----------------------------------
[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
-----------------------------------
```

[2] Logs (Registros)

```
-----------------------------------
Logs Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display Log File
-----------------------------------
```

[3] Support Bundle (Paquete de asistencia)

```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

Introducción a los flujos de trabajo en la consola de XenMobile

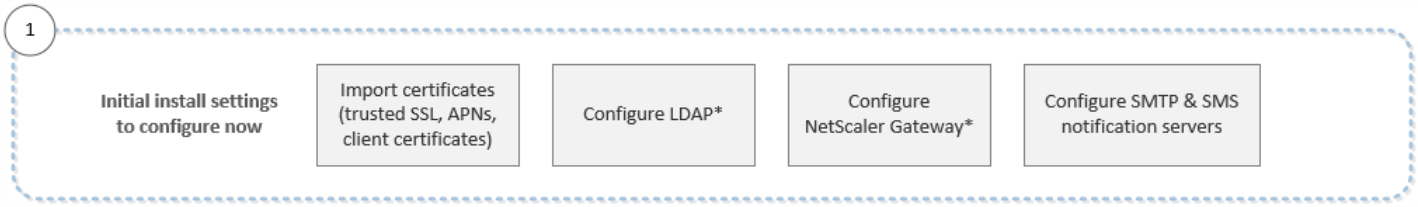
Mar 10, 2017

La consola de XenMobile es la herramienta de administración unificada para XenMobile. En este artículo, se da por hecho que XenMobile ya se ha instalado y está listo para su funcionamiento en la consola. Si aún no ha instalado XenMobile, consulte Instalación de XenMobile. Para obtener más información acerca de los exploradores Web que admite la consola de XenMobile, consulte el artículo Compatibilidad de XenMobile.

Flujo de trabajo de la configuración inicial

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. No se puede volver a las pantallas de configuración inicial. Si omitió algunas configuraciones de la instalación, puede configurar 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.

Nota: Los elementos con asterisco son optativos.



Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- Autenticación
- XenMobile y NetScaler Gateway
- Notificaciones

Para dar respaldo a las plataformas Android, iOS y Windows, debe tener la siguiente configuración relacionada con las cuentas.

Android

- Cree credenciales de Google Play. Para obtener más información, consulte Google Play Launch.
- Cree una cuenta de administrador de Android for Work. Para obtener más información, consulte Android at Work.
- Verifique su nombre de dominio con Google. Para obtener más información, consulte Verify your domain for G Suite.
- Habilite las API y cree una cuenta de servicio para Android for Work. Para obtener más información, consulte la ayuda de Android para empresas.

iOS

- Cree un ID de Apple y una cuenta de desarrollador. Para obtener más información, consulte el sitio Web de Apple Developer Program.

- Cree un certificado APNs (Apple Push Notification Service). Si va a administrar dispositivos iOS con la implementación de servicio XenMobile (en la nube), necesitará un certificado APNs de Apple. Si usa notificaciones push para la implementación de WorxMail, también necesitará un certificado APNs de Apple. Para obtener más información sobre cómo obtener certificados APNs de Apple, vaya a Apple Push Certificates Portal. Para obtener más información acerca de XenMobile y APNs, consulte Certificados APNs y Notificaciones push en WorxMail para iOS.
- Cree un token de empresa del Programa de compras por volumen (VPP). Para obtener más información, consulte Apple Volume Purchasing Program.

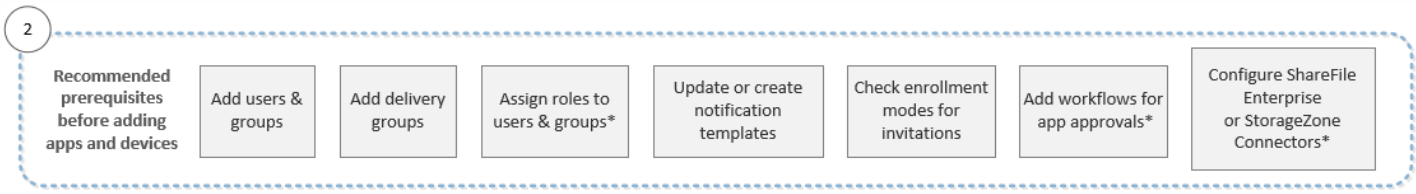
Windows

- Cree una cuenta de desarrollador para la Tienda Windows de Microsoft. Para obtener más información, consulte Microsoft Windows Dev Center.
- Obtenga un ID de publicador para la Tienda Windows de Microsoft. Para obtener más información, consulte Microsoft Windows Dev Center.
- Adquiera un certificado de empresa de Symantec. Para obtener más información, consulte Microsoft Windows Dev Center.
- Si quiere utilizar la detección automática de XenMobile para la inscripción de dispositivos Windows Phone, compruebe que tiene un certificado SSL público disponible. Para obtener más información, consulte Servicio de detección automática de XenMobile.
- Cree un token de inscripción de la aplicación (AET). Para obtener más información, consulte Microsoft Windows Dev Center.

Flujo de trabajo para los requisitos previos de consola

En este flujo de trabajo, se muestran los requisitos previos a configurar antes de agregar aplicaciones y dispositivos.

Nota: Los elementos con asterisco son optativos.



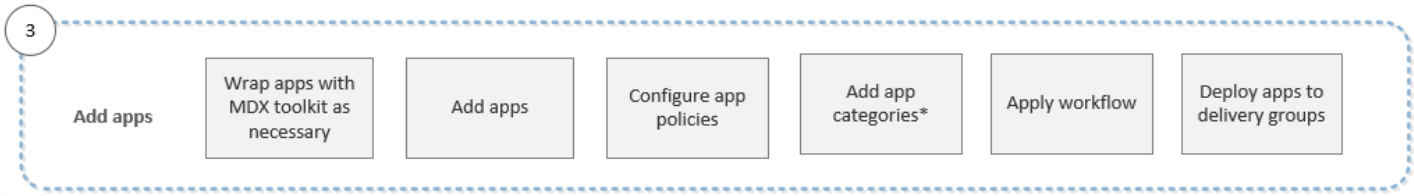
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- Inscripción, roles y cuentas de usuario
- Implementación de recursos
- Configuración de roles con RBAC
- Notificaciones
- Creación y administración de flujos de trabajo
- Uso de ShareFile con XenMobile

Flujo de trabajo para agregar aplicaciones

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

Nota: Los elementos con asterisco son optativos.



Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- Acerca del MDX Toolkit
- Incorporación de aplicaciones
- Vista general de las directivas MDX
- Creación y administración de flujos de trabajo
- Implementación de recursos

Flujo de trabajo para agregar dispositivos

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 asterisco son optativos.

Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- Dispositivos
- Sistemas operativos respaldados de dispositivo
- Implementación de recursos
- Supervisión y asistencia
- Acciones automatizadas

Flujo de trabajo para inscribir dispositivos de usuario

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

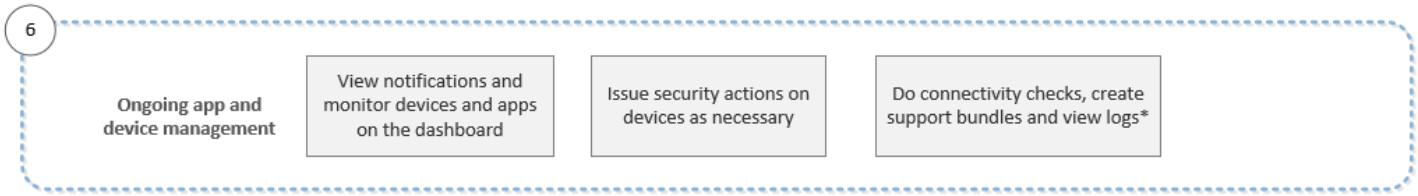
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- Inscripción, roles y cuentas de usuario
- Notificaciones

Flujo de trabajo para la administración continua de dispositivos y aplicaciones

En este flujo de trabajo, se muestran las actividades de administración de dispositivos y aplicaciones que puede realizar en la consola.

Nota: Los elementos con 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 Supervisión y asistencia.

Certificados y autenticación

Feb 27, 2017

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

- **Servidor XenMobile**. La seguridad y la experiencia de la inscripción se definen en el 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 Citrix y configurar la complejidad y el tiempo de caducidad de ese PIN.
- **NetScaler**. Con NetScaler, puede finalizar sesiones SSL de micro VPN. Asimismo, puede 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.
- **Secure Hub**. Secure Hub funciona con el servidor XenMobile en las operaciones de inscripción. Presente en el dispositivo, Secure Hub es la entidad que se comunica con NetScaler. Cuando una sesión caduca, Secure Hub 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 (ataques de tipo "Man in the middle"). Para obtener más información, consulte la sección sobre la fijación de certificados en el artículo Secure Hub.

  Asimismo, Secure Hub 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. Secure Hub también se encarga de detectar la liberación por jailbreak, así como de 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 configuración de la autenticación, incluida una descripción general de los métodos de autenticación de uno y dos factores, consulte el artículo Authentication de Deployment Handbook.

En XenMobile, puede usar certificados para crear conexiones seguras y para autenticar usuarios. En el resto de este artículo, se describen los certificados. Para obtener información adicional acerca de la configuración, consulte los siguientes artículos:

- Autenticación de dominio o dominio + token de seguridad
- Autenticación de certificado de cliente o certificado + dominio
- Entidades de infraestructura PKI
- Proveedores de credenciales
- Certificados APNs
- SAML para Single Sign-On con ShareFile
- Parámetros del servidor Microsoft Azure Active Directory

Certificados

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.

> **Nota**
>
> Los dispositivos iOS 10.3 no admiten certificados autofirmados. Si XenMobile utiliza certificados autofirmados, los usuarios no podrán inscribir dispositivos iOS 10.3 en XenMobile. Para inscribir los dispositivos que ejecutan iOS 10.3 o posterior en XenMobile, debe utilizar certificados SSL de confianza en XenMobile.

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, los usuarios introducen su PIN de Citrix para acceder con inicio de sesión único (Single Sign-On) a las aplicaciones habilitadas para XenMobile. El PIN de Citrix también simplifica la experiencia de autenticación del usuario. El PIN de Citrix se usa para proteger 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 conocer los pasos a seguir, consulte Certificados 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	.p12 (.pfx en equipos basados en Windows)	SSL, SAML, APNs XenMobile también genera una infraestructura de clave pública completa durante el proceso de instalación. **Importante**: XenMobile Server no admite certificados con la extensión 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.

Cada certificado que cargue contiene una entrada en la tabla Certificates, con un resumen de su contenido. Cuando configure los componentes de integración con PKI que requieran un certificado, deberá elegir un certificado que cumpla 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 con un certificado de cliente.

Esta sección ofrece instrucciones generales para cargar certificados. Para obtener más información sobre cómo crear, cargar y configurar los certificados de cliente, consulte Autenticación de certificado de cliente o certificado + dominio.

Requisitos de clave privada

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

Carga de certificados en la consola

Al cargar certificados en la consola, tiene dos opciones:

- Puede hacer clic para importar un almacén de claves. Luego, debe identificar la entrada en el repositorio del almacén de claves que quiere instalar, a menos que quiera cargar un formato PKCS#12.
- Puede hacer clic para importar un certificado.

Puede cargar el certificado de CA (sin la clave privada) que usa la CA para firmar las solicitudes. También puede cargar un certificado de cliente SSL (con la clave privada) para la autenticación de clientes.

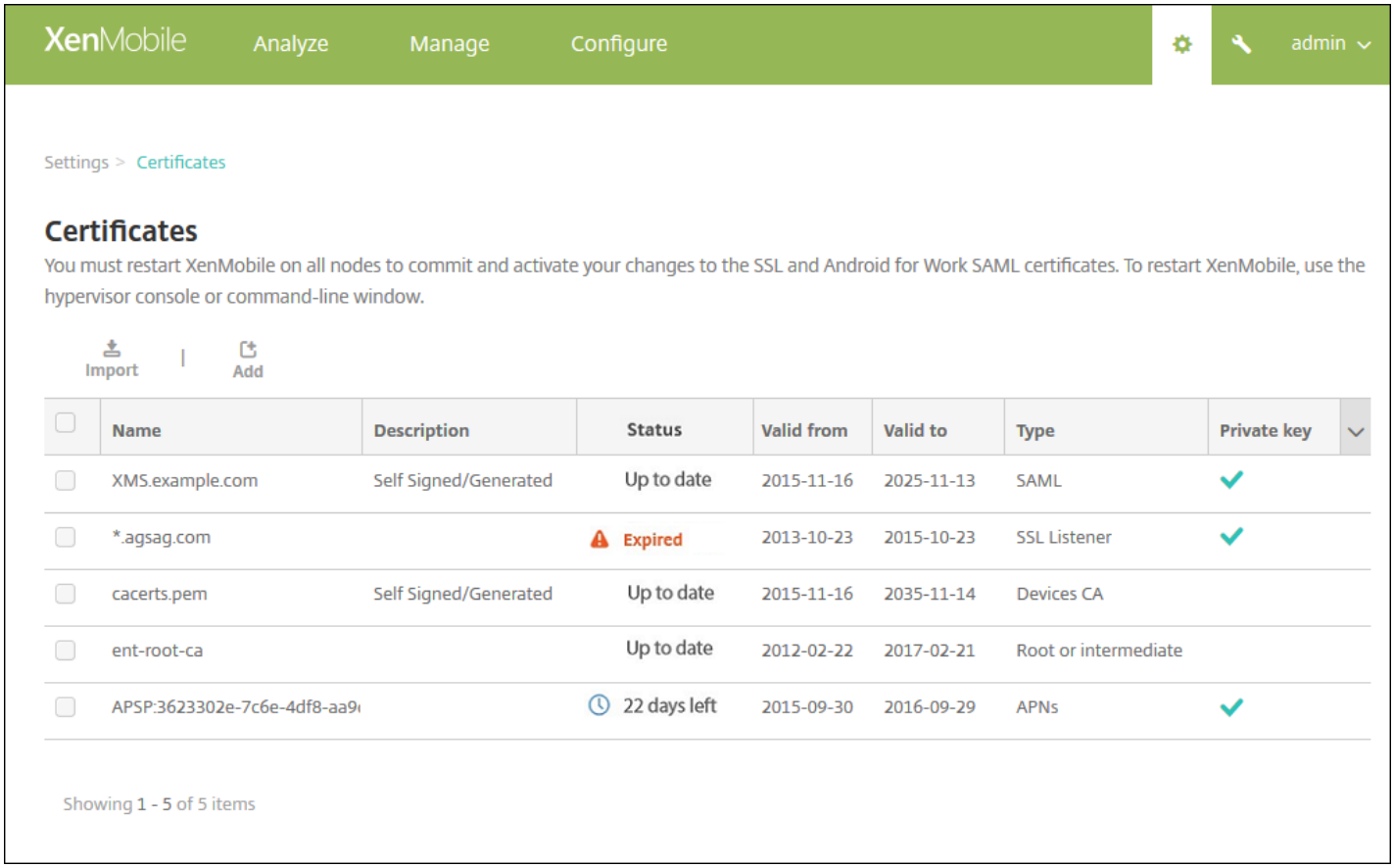
Cuando configure la entidad CA de Microsoft, especifique el certificado de CA. Seleccione el certificado de CA desde una lista de todos los certificados de servidor que sean certificados de CA. Del mismo modo, cuando configure la autenticación de cliente, podrá seleccionar un certificado de servidor de una lista que contiene todos los certificados de servidor para los que XenMobile tiene la clave privada.

Para importar un almacén de claves

Los almacenes de claves, que son repositorios de certificados de seguridad, están diseñados para que puedan contener entradas múltiples. Al cargar entradas desde 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**.

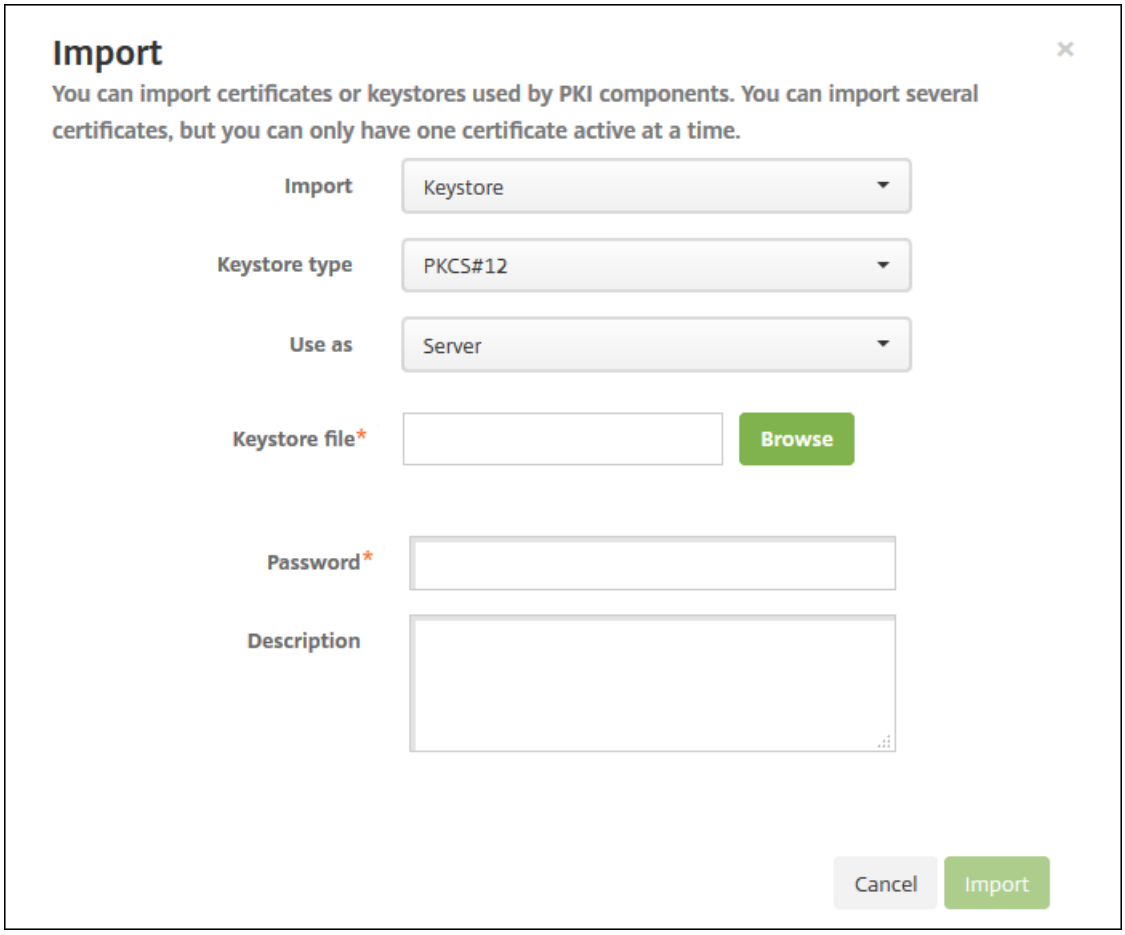
2. Haga clic en **Certificates**. Aparecerá la página **Certificates**.



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

4. Configure estos 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 usará el certificado. Las opciones disponibles son:
  - **Server**. Los certificados de servidor son aquellos que usa el servidor XenMobile, 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 a los servidores, los sitios Web y las aplicaciones.
  - **APNs**. Los certificados APNs de Apple 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**. Busque el almacén de claves que quiere importar del tipo de archivo .p12 (o .pfx en equipos Windows).
- **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.

Para importar un certificado

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 del almacén de claves forman una cadena. Por ejemplo, si cada certificado de la cadena es el emisor del certificado 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, 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 almacén de claves que quiere importar del tipo de archivo .p12 (o .pfx en equipos Windows).

6. Busque el archivo de clave privada optativa del certificado. Junto con el certificado, la clave privada se usa para el cifrado y el descifrado.

7. Si quiere, escriba una descripción del certificado que le ayude a distinguirlo de otros certificados.

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

Actualización de un certificado

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, podrá reemplazar la entrada existente o eliminarla.

En la consola de XenMobile, la forma más eficaz de actualizar los certificados es: 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**. En el cuadro de diálogo **Import**, importe el nuevo certificado.

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.

Administración de certificados en XenMobile

Se recomienda mantener una lista 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:

Servidor XenMobile
Certificado SSL para FQDN de MDM
Certificado SAML (para ShareFile)
Certificados raíz e intermedios de la entidad de certificación 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 Secure Hub del 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 Citrix Secure Mail)
Archivo KeyStore de Android
Windows Phone: certificado Symantec

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

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

> ## Nota
>
> La entidad de certificación (CA) le pide 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 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 en Secure Mail. 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 información más detallada, consulte Certificados APNs.

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

Asimismo, Apple le enviará una notificación por correo electrónico entre 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.

Gracias,

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. La aplicación también debe estar firmada con un certificado de distribución correspondiente.

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 una clave caduca, los usuarios ya no pueden actualizar fácilmente 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. Esos usuarios tampoco podrán 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 la caducidad de los certificados de NetScaler, consulte How to handle certificate expiry on NetScaler en Knowledge Center de la asistencia de Citrix.

Un certificado caducado de NetScaler impide que los usuarios inscriban sus dispositivos y accedan a la tienda. El certificado caducado también impide que los usuarios se conecten al servidor Exchange cuando utilicen Secure Mail. Además, los usuarios no podrán conocer ni abrir las aplicaciones HDX (según el certificado caducado).

Command Center (Centro de comandos) y Expiry Monitor (Centro de supervisión de caducidad) son dos herramientas que pueden ayudarle a hacer un seguimiento de los certificados de NetScaler. Command Center le notifica cuándo caduca el certificado. Esas dos herramientas ayudan a supervisar los siguientes certificados de NetScaler:

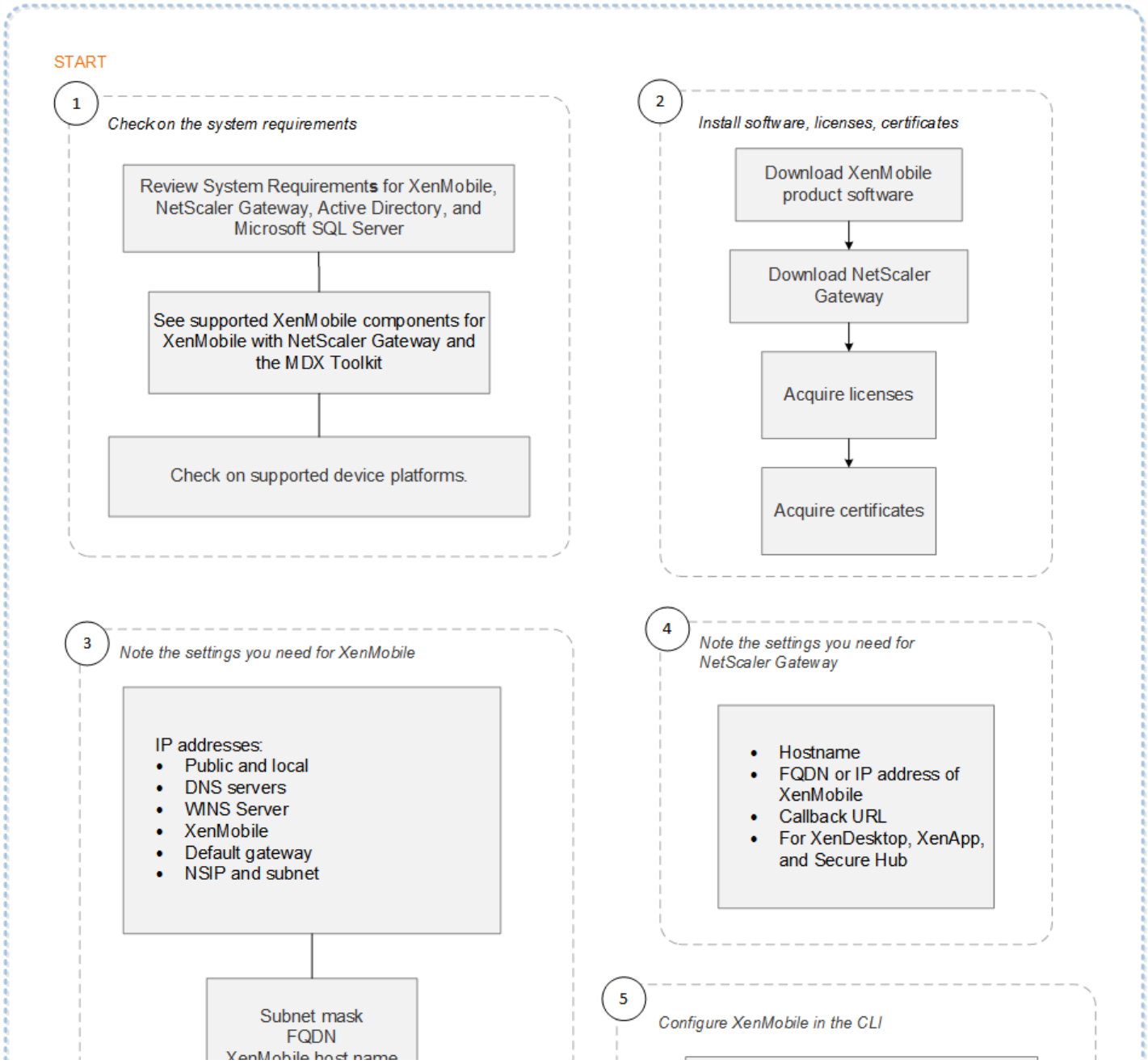
Certificado SSL para FQDN de MDM
Certificado SSL para FQDN de Gateway
Certificado SSL para FQDN de StorageZone C. de ShareFile
Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)
Certificado SSL para el equilibrio de carga de StoreFront
Certificados raíz e intermedios de la entidad de certificación para los certificados anteriores

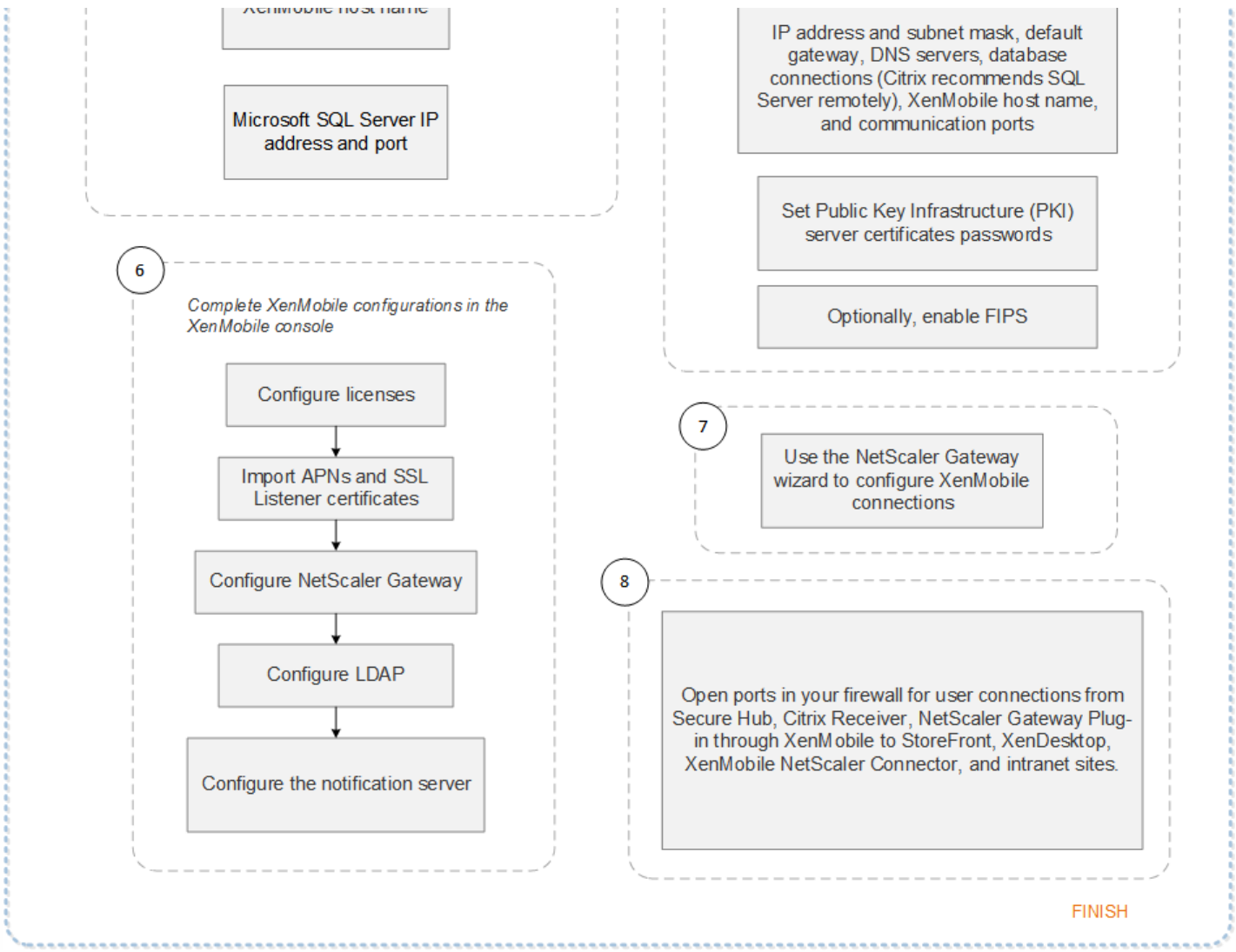
XenMobile y NetScaler Gateway

Feb 27, 2017

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. Puede configurar NetScaler Gateway en la consola de XenMobile, como se describe en este artículo.

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





1

- Requisitos del sistema y compatibilidad

2

- Instalación y configuración

3

- Lista de verificación previa a la instalación

4

- Lista de verificación previa a la instalación

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

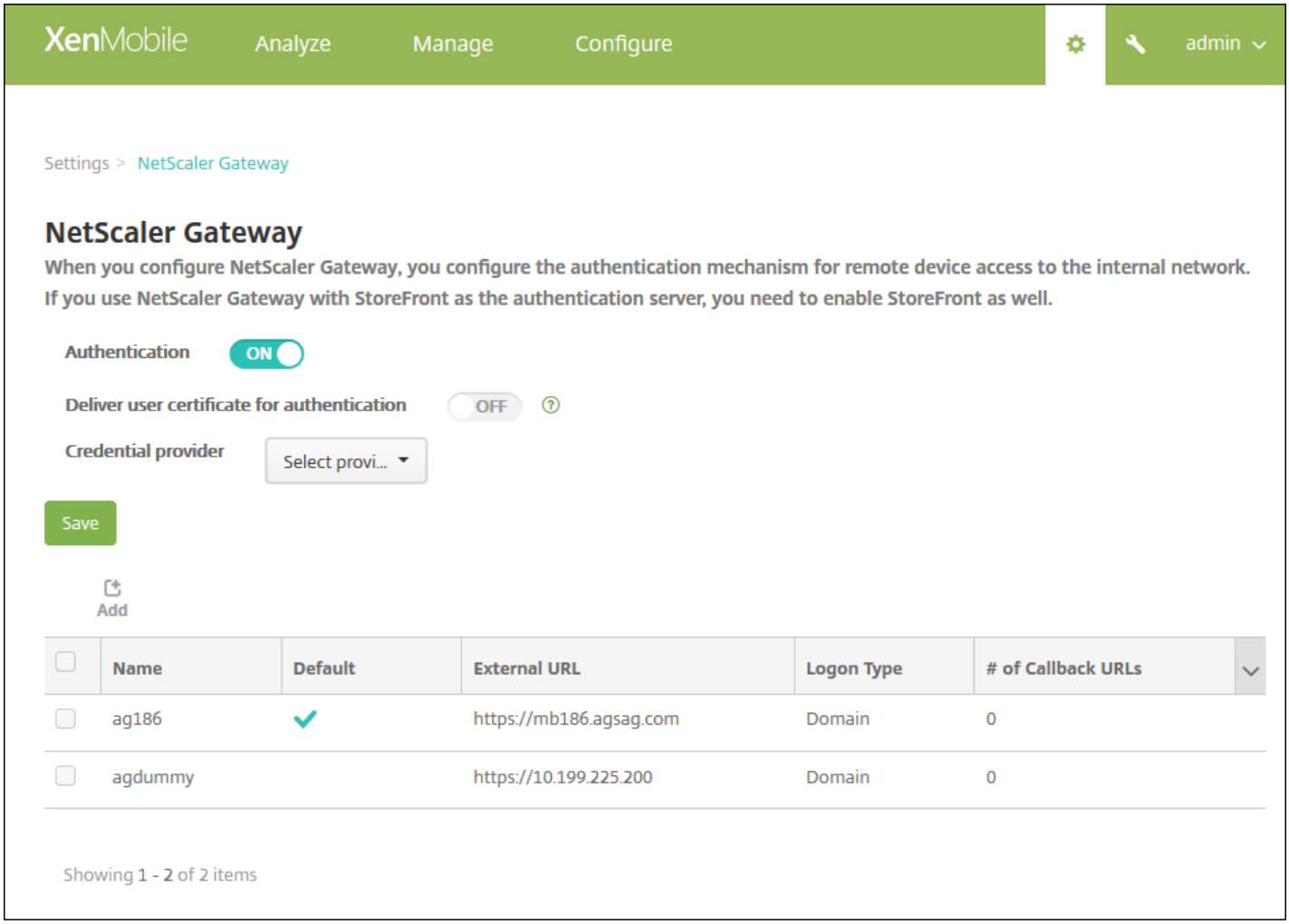
- Puertos

El diagrama de flujo también está disponible en formato PDF.

Diagrama de flujo para la implementación de XenMobile

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:

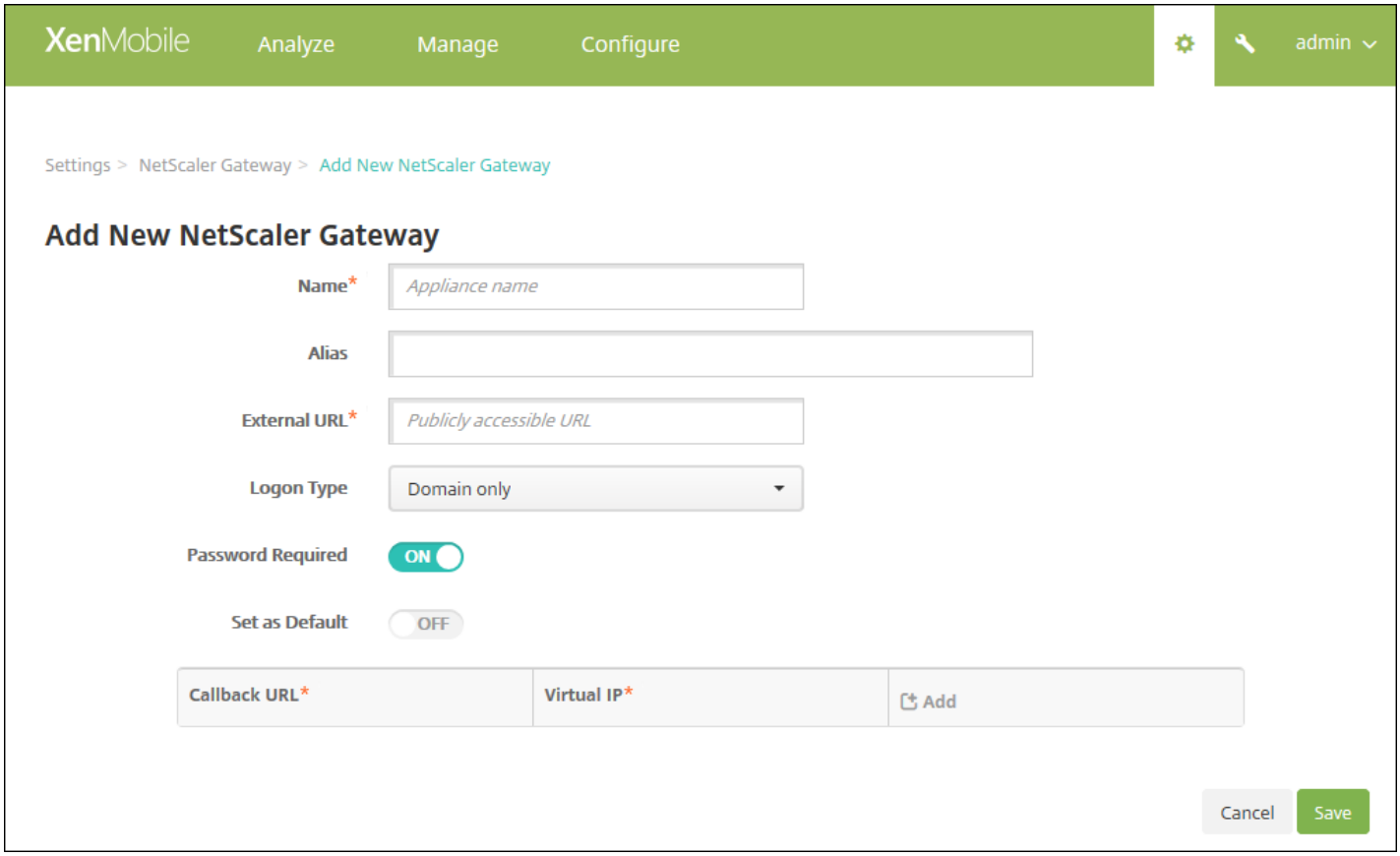
- **Authentication**. Seleccione si quiere habilitar la autenticación. El valor predeterminado es **ON**.
- **Deliver user certificate for authentication**. Seleccione si quiere que XenMobile comparta el certificado de autenticación con Secure Hub para que NetScaler Gateway gestione la autenticación 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.

6. 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. Se abrirá 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 estos parámetros:

- **Name**. Escriba un nombre para la instancia de NetScaler Gateway.
- **Alias**. Si quiere, 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 pueden ser: **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, **Domain only** no funcionará: debe usar **Certificate and domain**. En el caso de algunas opciones, como por ejemplo **Domain only**, no se 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 Secure Hub. Para obtener más información, consulte Configuración de XenMobile para la autenticación con certificado y token de seguridad.
- **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 de 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. La dirección URL de respuesta debe resolverse como una dirección IP que sea accesible desde el servidor XenMobile, pero no tiene que ser una dirección URL externa de NetScaler Gateway.

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

Autenticación de dominio o dominio + token de seguridad

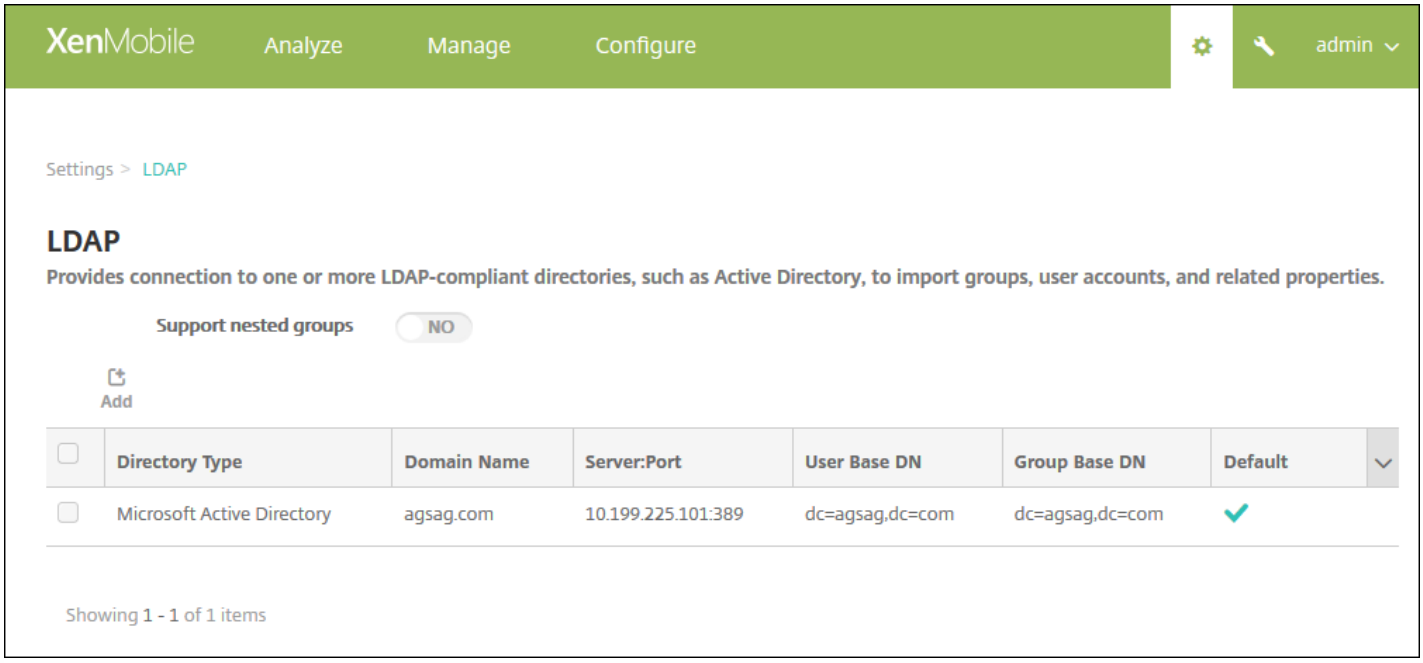
Feb 27, 2017

XenMobile admite la autenticación basada en dominios con uno o varios directorios (como Active Directory), que son compatibles con el protocolo ligero de acceso a directorios (LDAP). En XenMobile, puede configurar una conexión a uno o varios directorios y usar la configuración de LDAP para importar grupos, cuentas de usuario y propiedades relacionadas.

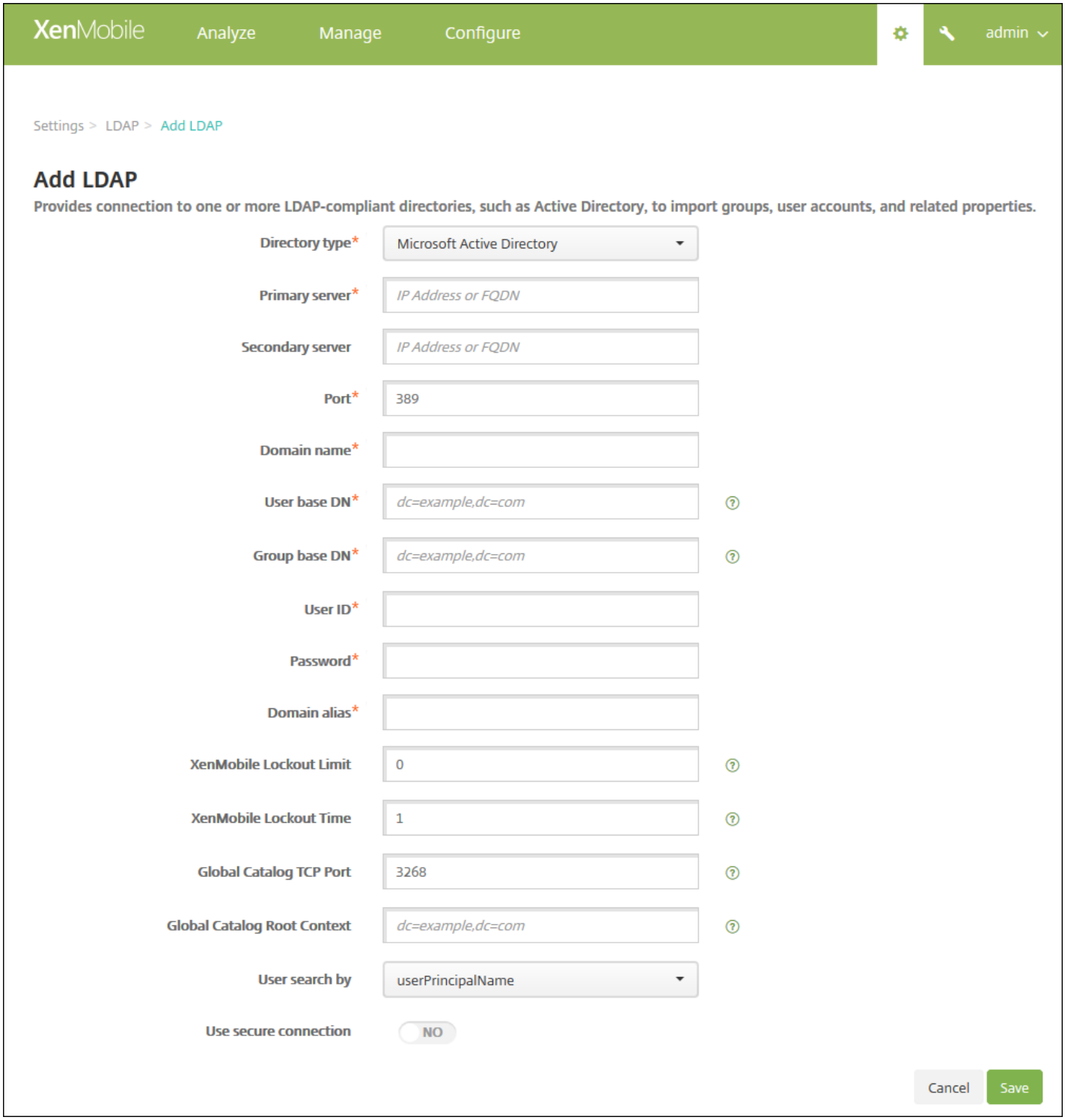
El protocolo LDAP es un protocolo de aplicación de código abierto y no vinculado a ningún proveedor específico. Se utiliza para acceder a servicios de información sobre directorios distribuidos a través de una red de protocolo de Internet (IP) y para su mantenimiento. Los servicios de información de 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.

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.

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 estos 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). Este es un servidor de conmutación por error que se utilizará si no se puede establecer

contacto con el servidor principal.

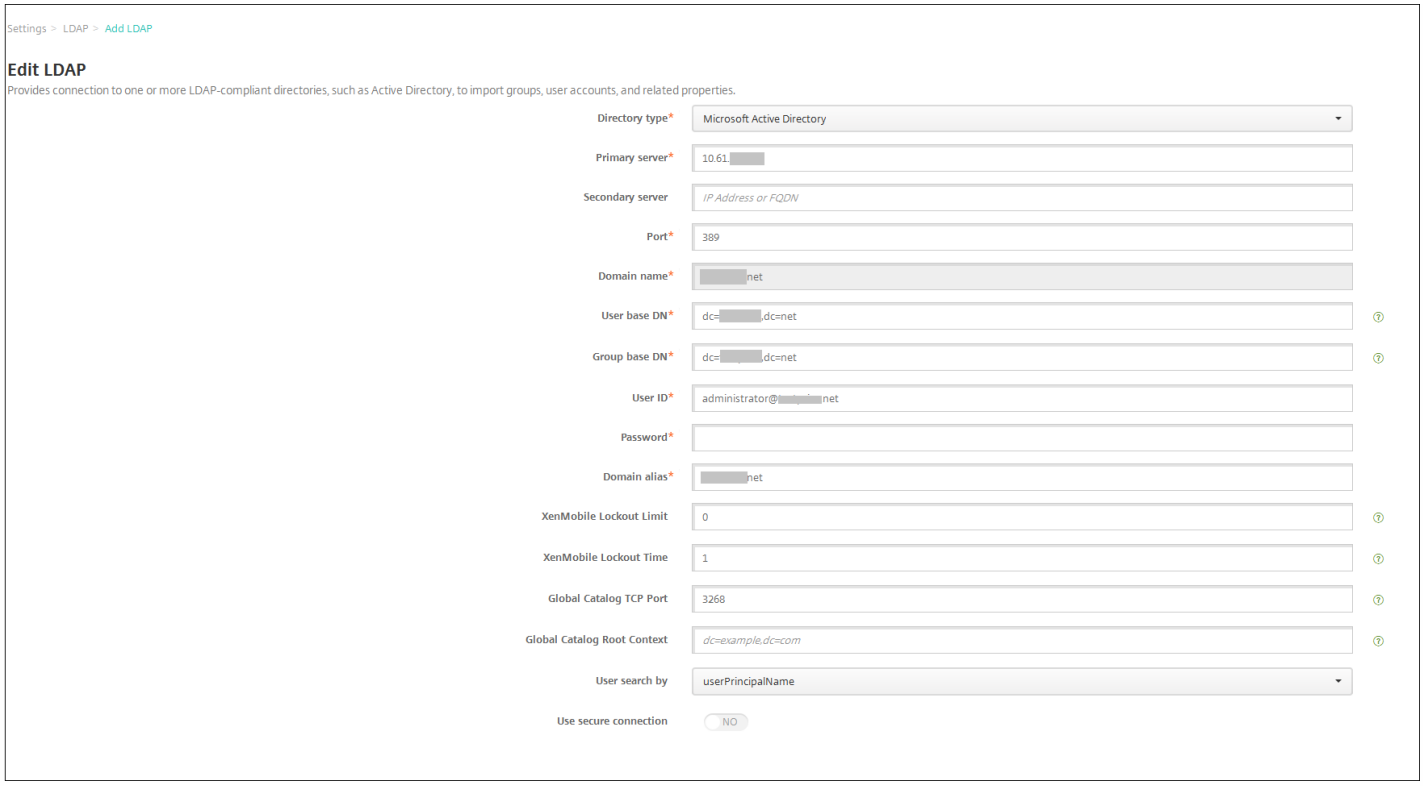
- **Port**. Escriba el número de puerto que utiliza el servidor LDAP. De forma predeterminada, el número de puerto es 389 para conexiones LDAP no protegidas. Use el número de puerto 636 para conexiones LDAP protegidas, el 3268 para conexiones LDAP no protegidas de Microsoft o el 3269 para conexiones 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 la ubicación de los grupos de Active Directory. Por ejemplo, cn = users, dc = dominio, dc = net, donde cn = users representa el nombre del contenedor de los grupos y dc representa el componente de dominio de 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**. 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 **Edit 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 modificar 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=servername, dc=net, donde cn=users es el nombre del grupo; el DN y servername 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 dominio + token de seguridad

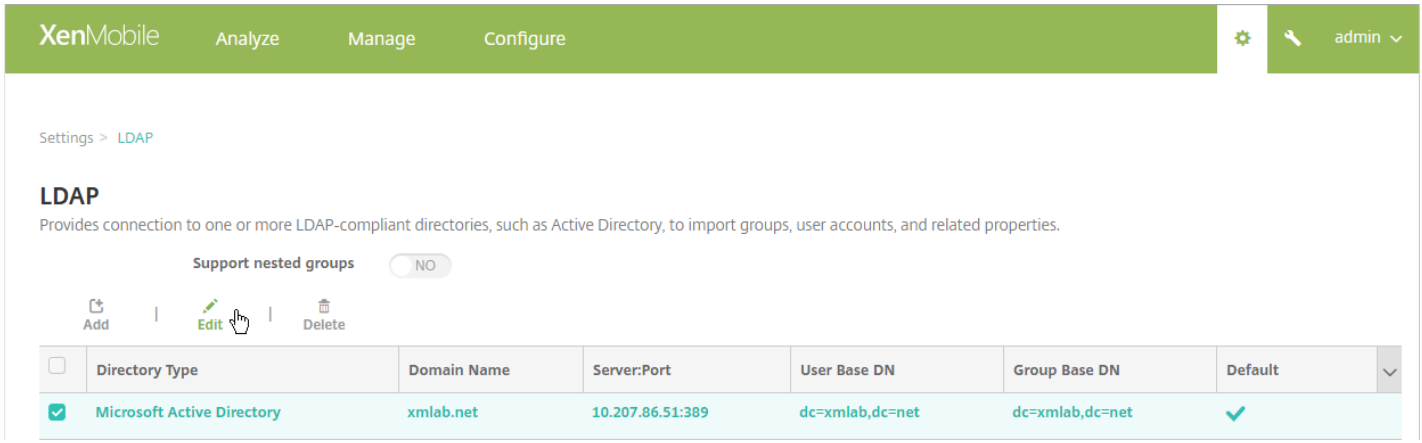
Puede configurar XenMobile para exigir a los usuarios que se autentiquen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso.

Para disfrutar de una usabilidad óptima, puede combinar esta configuración con un PIN de Citrix 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.

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.

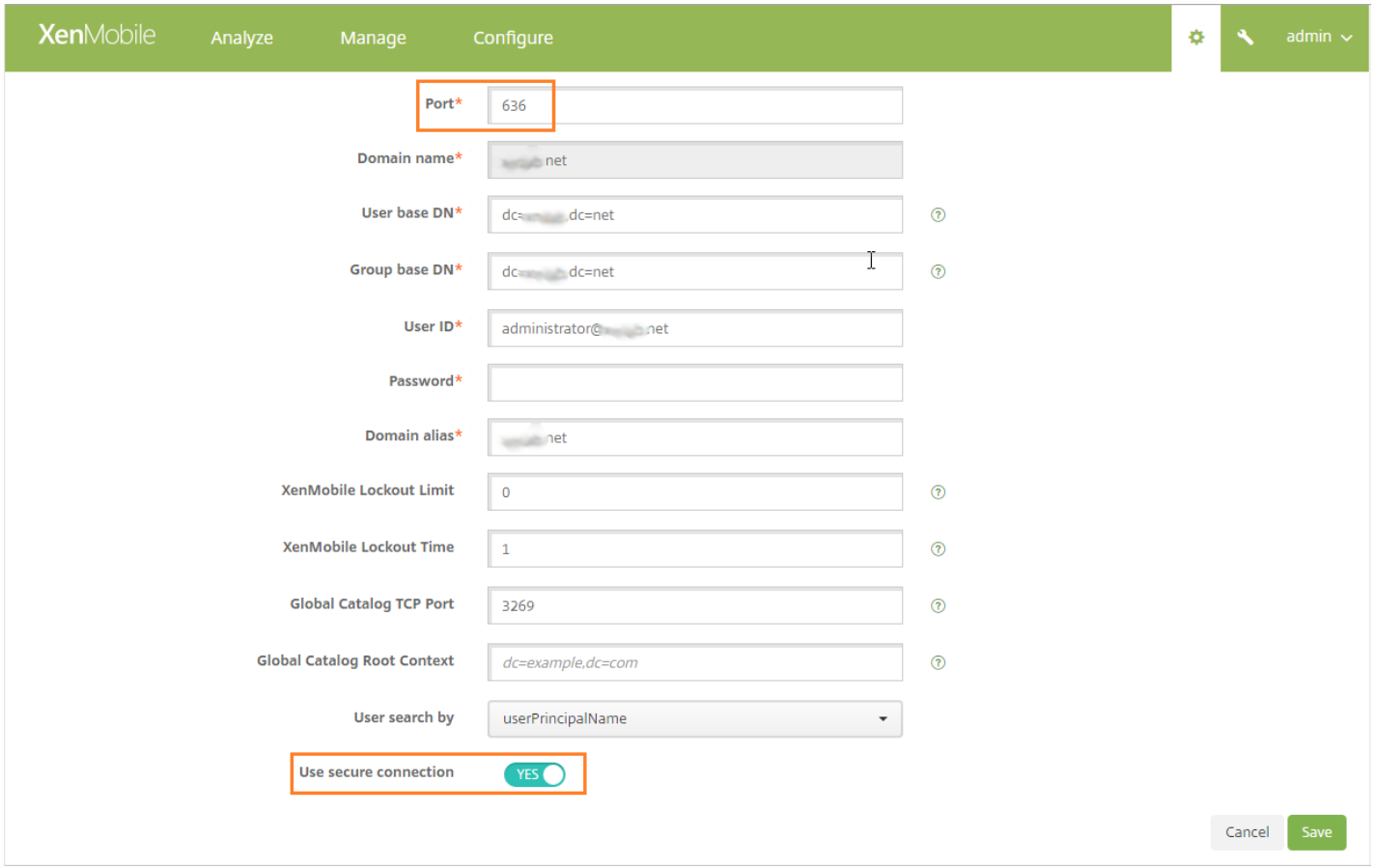
1. En **Settings**, haga clic en **LDAP**.

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**.

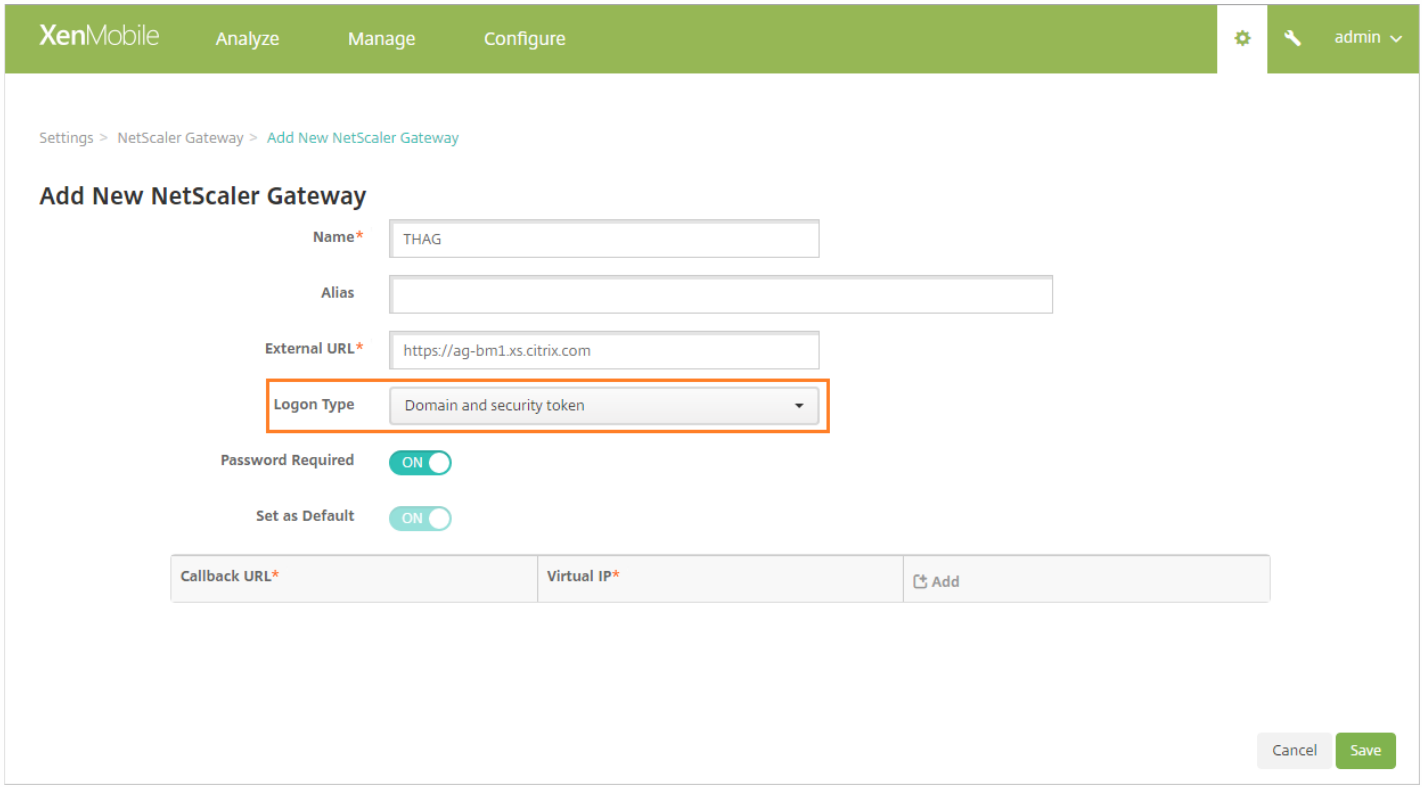


En los siguientes pasos se supone que ya ha agregado una instancia de NetScaler Gateway a XenMobile. Para agregar una instancia de NetScaler Gateway, consulte Para configurar una nueva instancia de NetScaler Gateway.

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

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

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



Para habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas, vaya a **Settings > Client Properties** y marque las casillas **Enable Citrix PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte Propiedades de cliente.

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.

Autenticación de certificado de cliente o certificado + dominio

Feb 27, 2017

En XenMobile, la configuración predeterminada para la autenticación es el nombre de usuario y la contraseña. Para agregar otra capa de seguridad para la inscripción y el acceso al entorno de XenMobile, considere la posibilidad de usar la autenticación basada en certificados. En el entorno de XenMobile, esta configuración es la mejor combinación de seguridad y experiencia de usuario, con las posibilidades óptimas del inicio de sesión SSO ligadas a la seguridad que ofrece la autenticación de dos factores en NetScaler.

Si no permite LDAP y usa tarjetas inteligentes o métodos similares, la configuración de los certificados permite representar una tarjeta inteligente en XenMobile. Los usuarios se inscriben mediante un PIN único que genera XenMobile para ellos. Una vez que el usuario tiene acceso, XenMobile crea e implementa el certificado utilizado a partir de entonces para autenticarse en el entorno de XenMobile.

Puede utilizar el asistente "NetScaler para XenMobile" para llevar a cabo la configuración necesaria para XenMobile cuando se usa la autenticación de solo certificado o la autenticación de certificado y dominio en NetScaler. Puede ejecutar el asistente de NetScaler para XenMobile solamente una vez.

En los entornos de alta seguridad, donde el uso de las credenciales de LDAP fuera de una organización en redes públicas o no seguras se considera una amenaza acuciante a la seguridad de la organización, la autenticación de dos factores mediante un certificado del cliente y un token de seguridad es una posibilidad. Para obtener más información, consulte Configuring XenMobile for Certificate and Security Token Authentication.

La autenticación de certificado del cliente está disponible para el modo XenMobile MAM (solo MAM) y el modo ENT (cuando los usuarios se inscriben en MDM). La autenticación de certificado del cliente no está disponible para el modo XenMobile ENT cuando los usuarios se inscriben en el modo MAM antiguo. 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. Siga estos pasos generales, como se describe en este artículo.

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, configure como se describe en Configuring Client Certificate or Client Certificate and Domain Authentication en la documentación de NetScaler Gateway.

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.

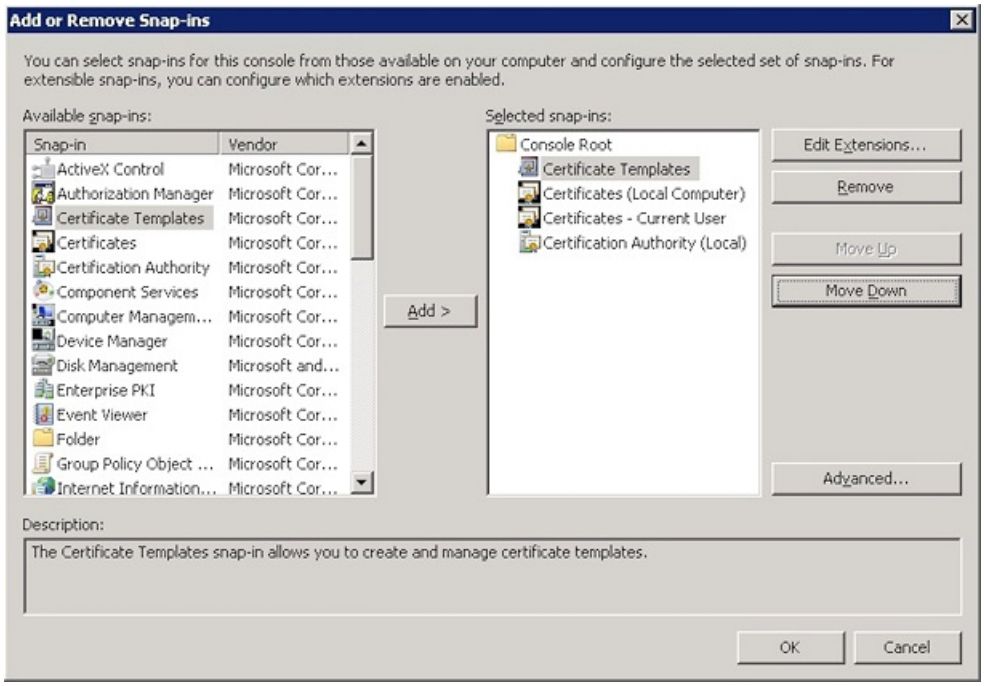
- Para configurar la autenticación basada en certificados para Exchange ActiveSync, consulte este blog de Microsoft.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync hacia el servidor Exchange Server, asegúrese de que los dispositivos móviles tienen todos los certificados raíz e intermedios. De lo contrario, la autenticación basada en certificados fallará durante la configuración de buzones de correo en Secure Mail. 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, en **SSL Settings**, seleccione **Require SSL**.
- Secure Mail debe estar empaquetado con la versión más reciente de MDX Toolkit, si es necesario para su método de implementación.

Cómo agregar el complemento de Certificados a Microsoft Management Console

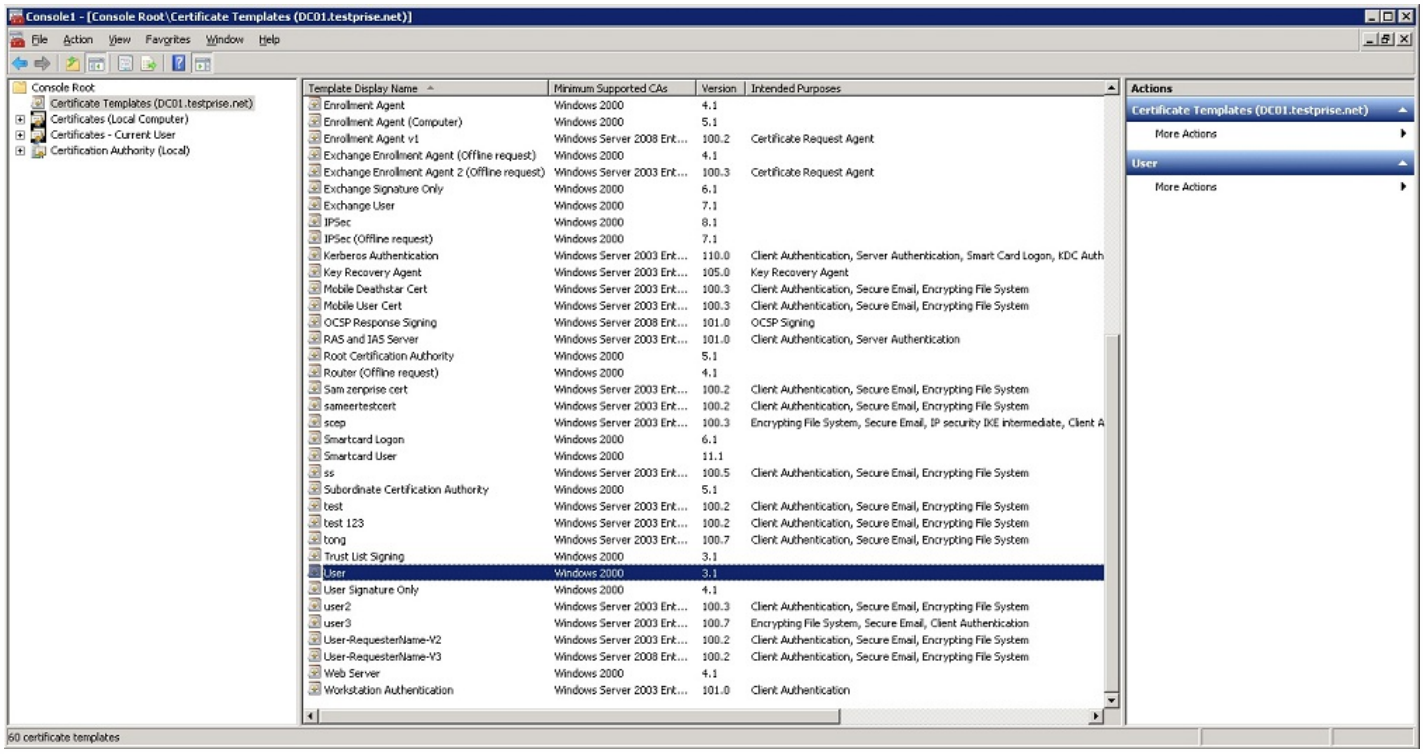
1. Abra la consola Microsoft Management Console (MMC) y haga clic en **Agregar o quitar complemento**.

2. Agregue los complementos siguientes:

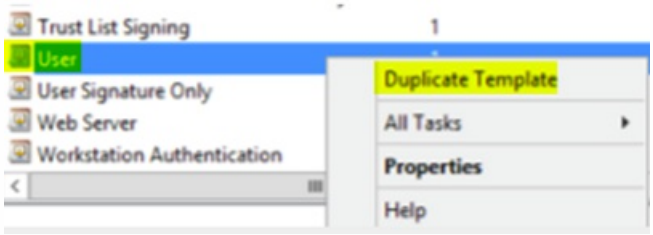
   Plantillas de certificado
   Certificados (equipo local)
   Certificados: usuario actual
   Entidad de certificación (local)



3. Expanda **Plantillas de certificado**.



4. Seleccione la plantilla **Usuario** y **Duplicar plantilla**.

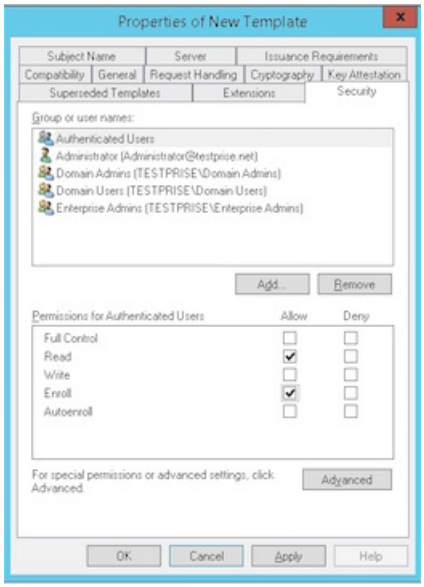


5. Suministre el nombre para mostrar de la plantilla.

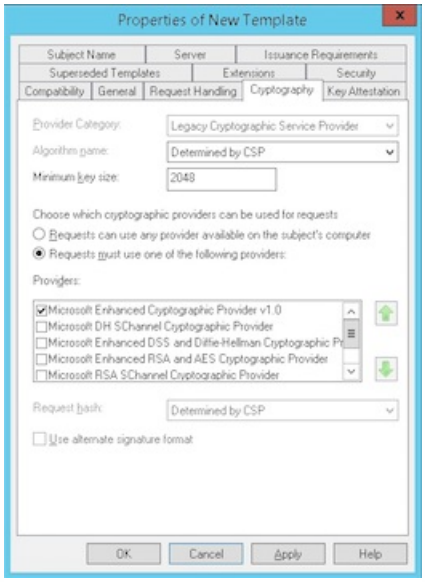
> **Importante**: No marque la casilla **Publicar certificado en Active Directory** a menos que sea necesario. Si se selecciona esta opción, todos los certificado de cliente de los usuarios se insertarán/crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

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

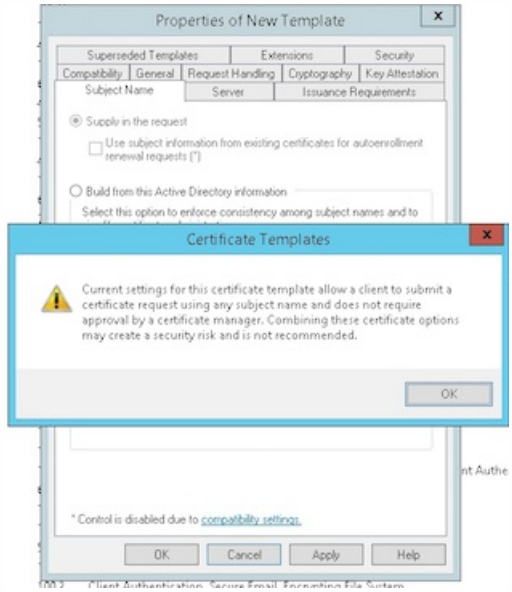
7. En **Seguridad**, seleccione la opción **Inscribir** en la columna **Permitir** para los usuarios autenticados.



8. En **Criptografía**, debe suministrar el tamaño de la clave (necesitará introducirlo también durante la configuración de XenMobile).



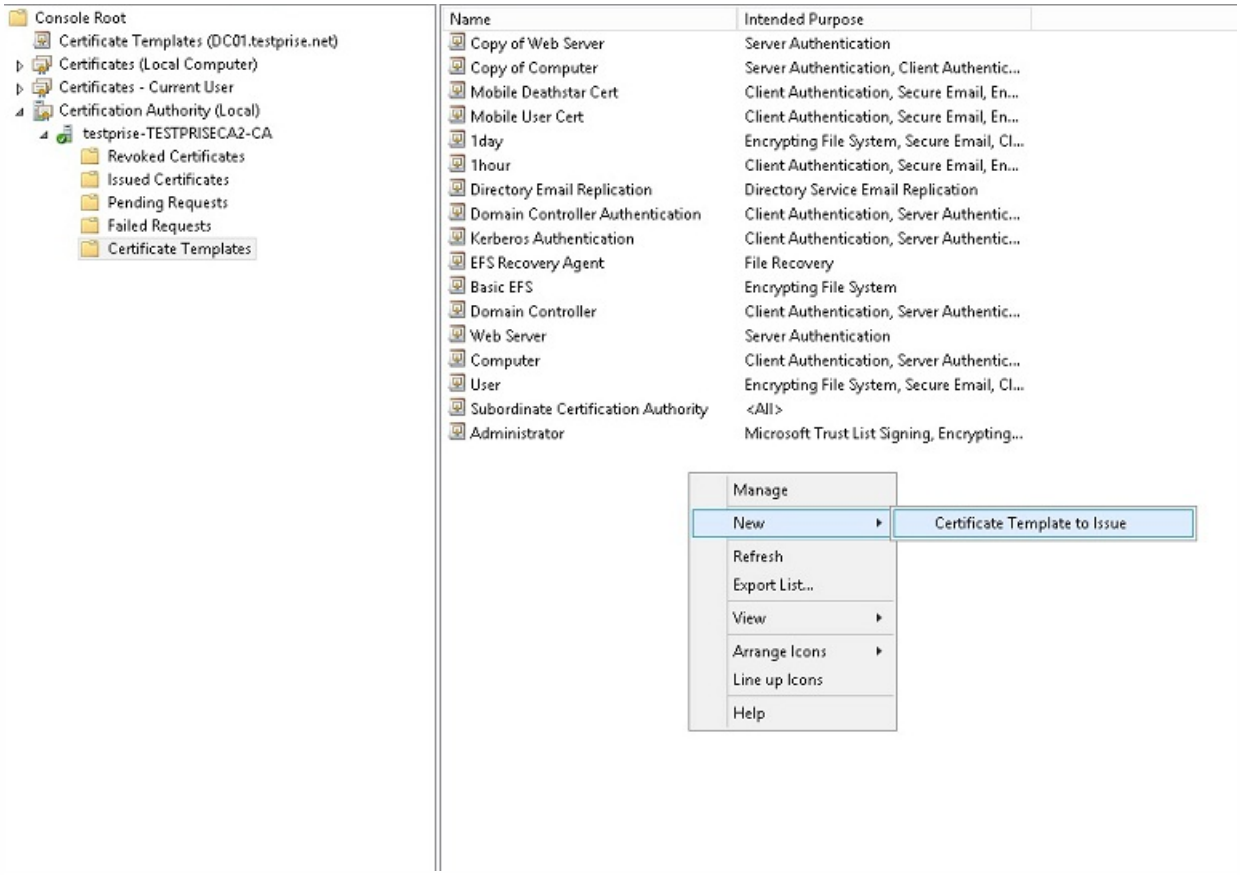
9 En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.



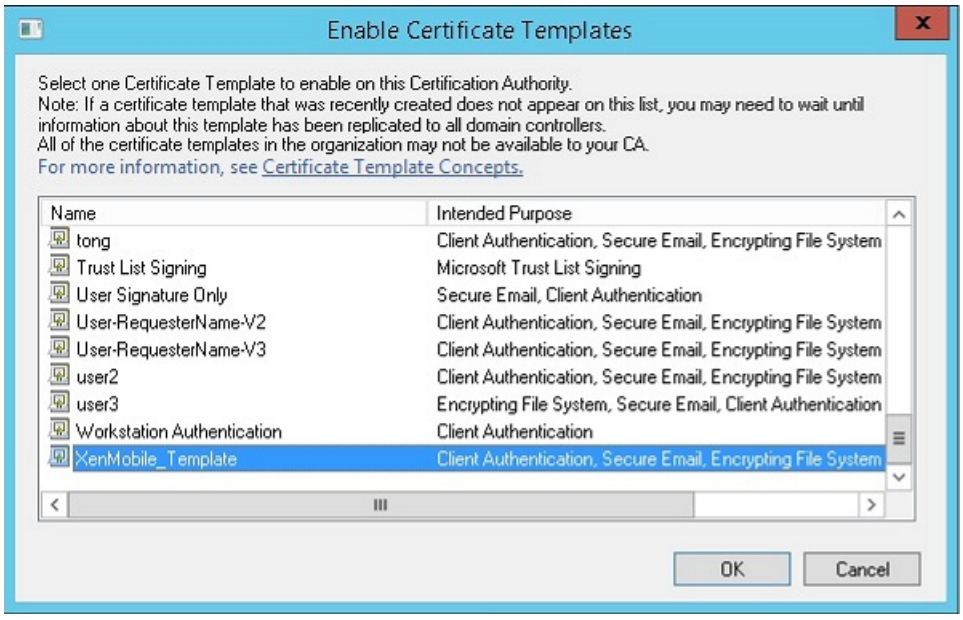
Cómo agregar la plantilla a la entidad de certificación

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 haga clic en **Aceptar** para agregarla a la **Entidad de certificación**.



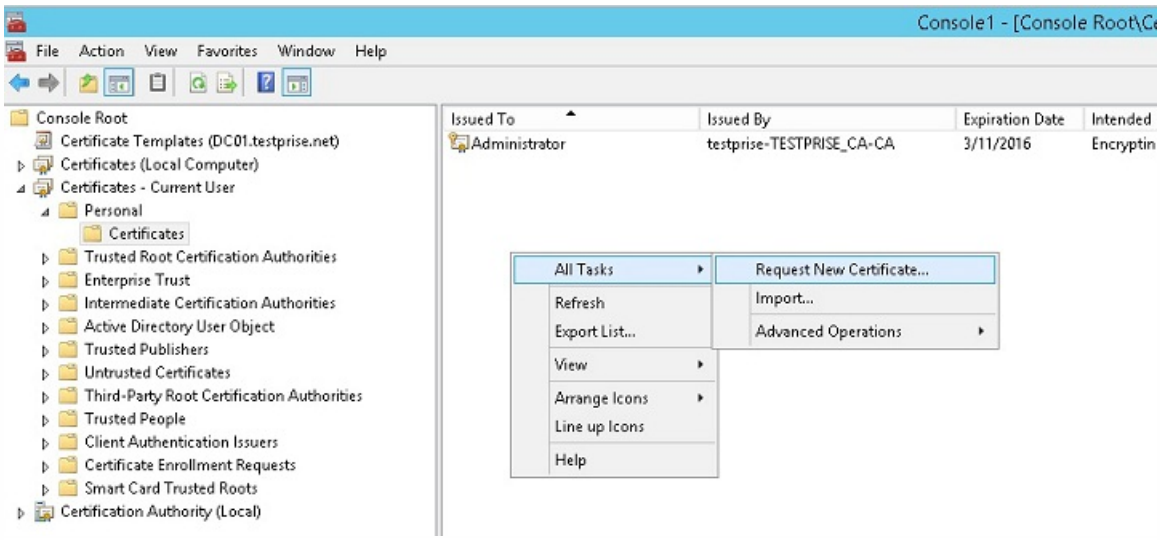
Creación de un certificado PFX desde el servidor de CA

1. Cree un certificado .pfx de usuario con la cuenta de servicio con la que inició sesión. Este .pfx se cargará en XenMobile, lo

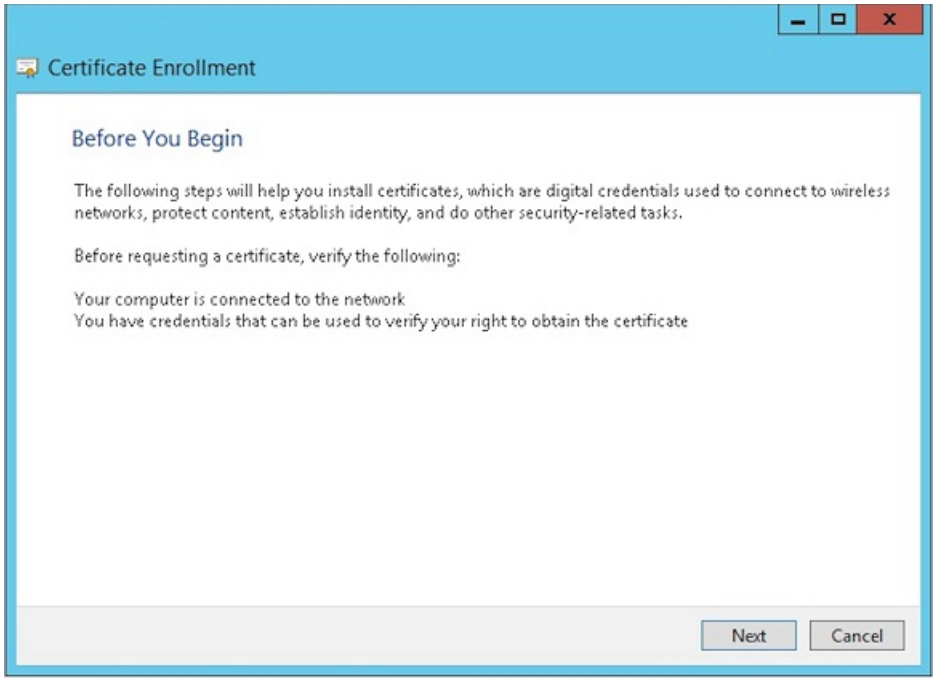
que solicitará un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.

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

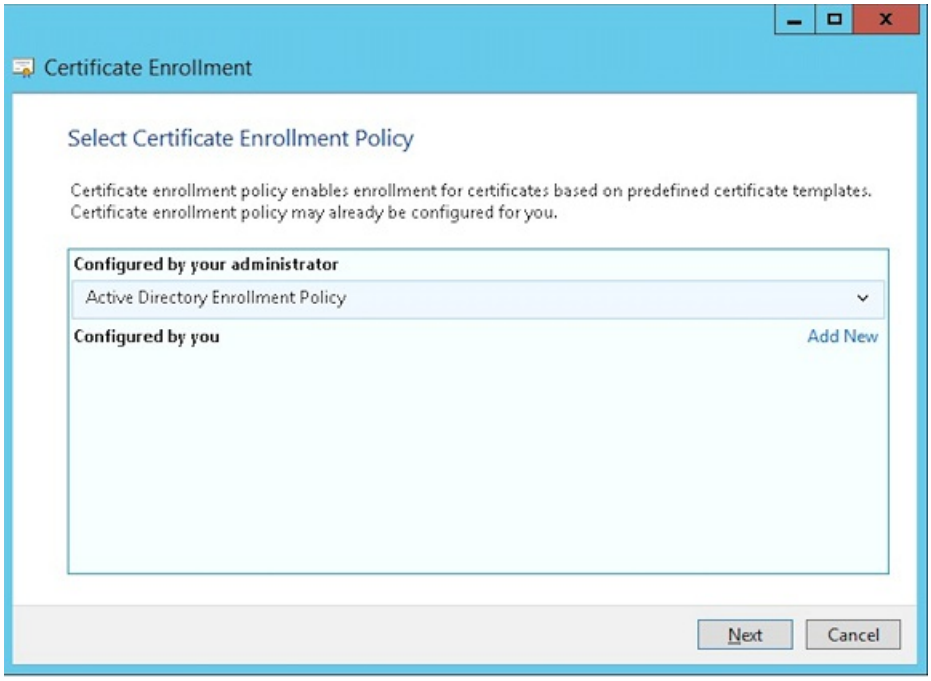
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



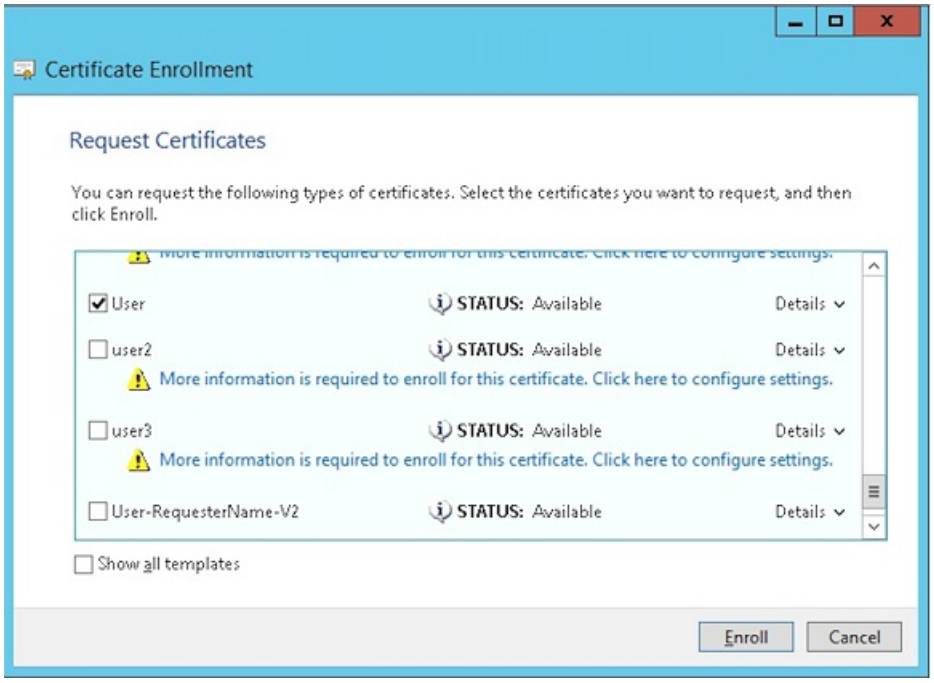
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Next**.



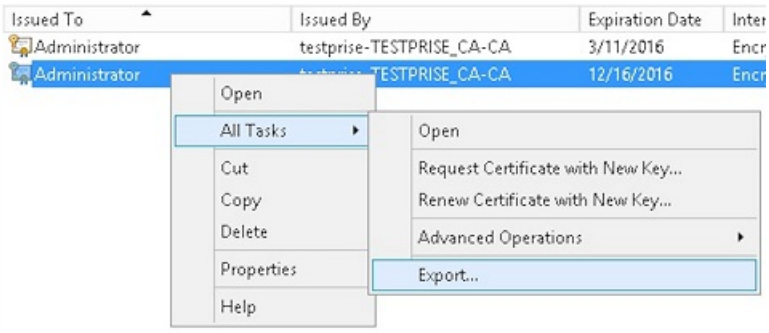
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



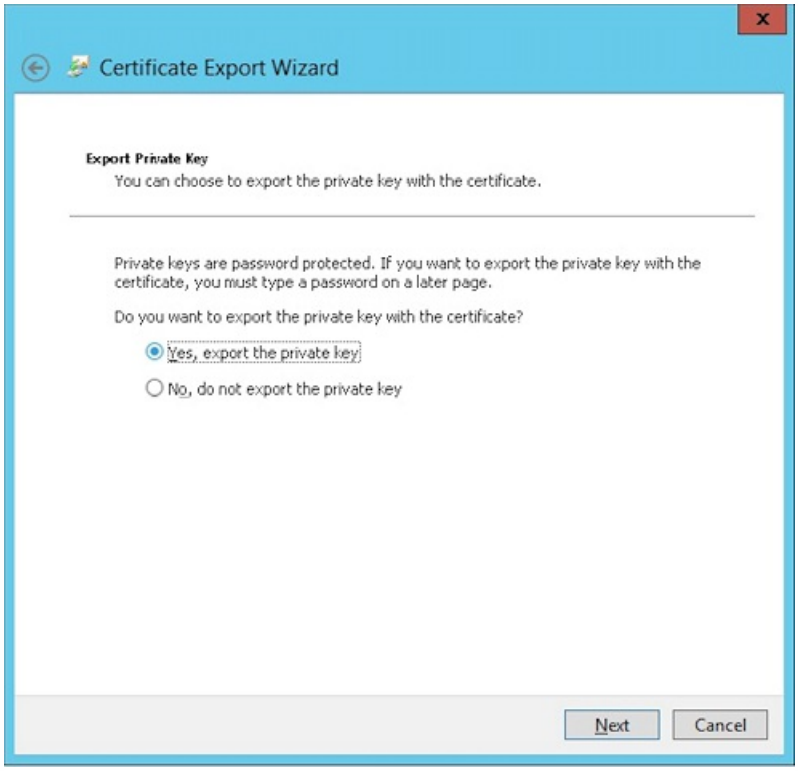
6. Seleccione la plantilla **Usuario** y haga clic en **Inscribir**.



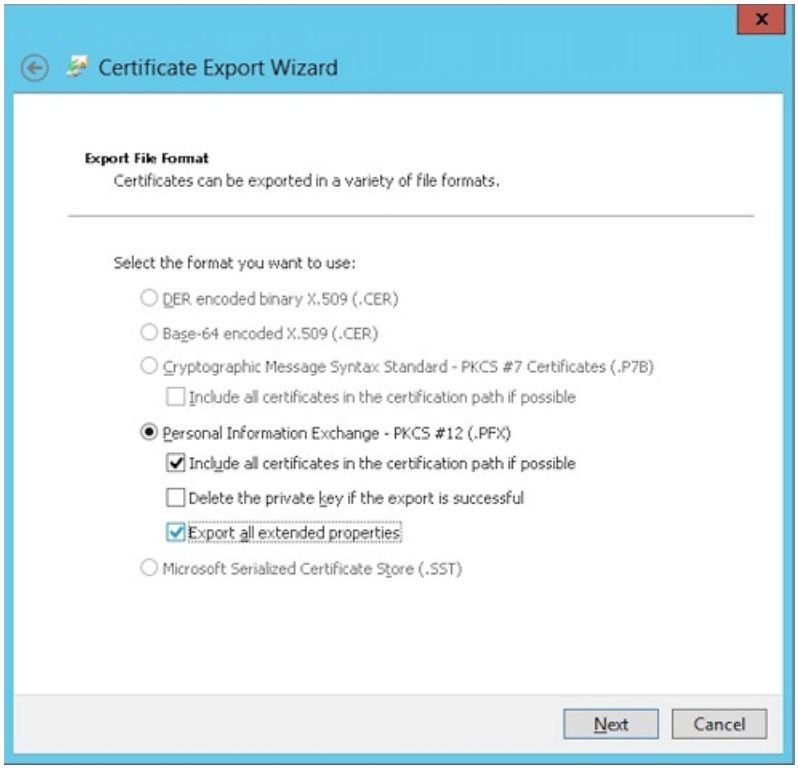
7. Exporte el archivo .pfx que creó en el paso anterior.



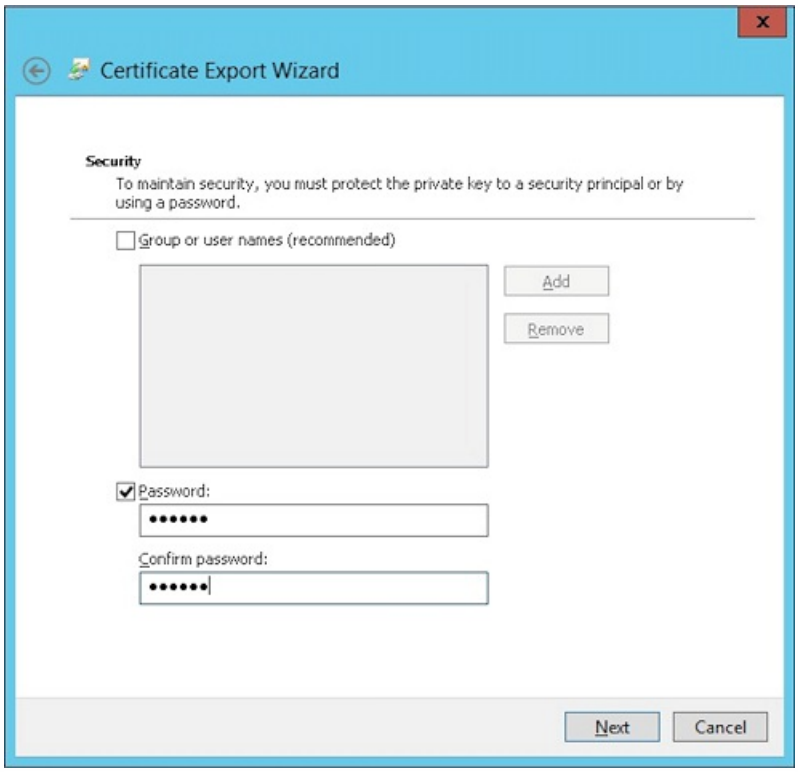
8. Haga clic en **Exportar la clave privada**.



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 la contraseña que va a usar para cargar este certificado en XenMobile.



11. Guarde el certificado en su disco duro.

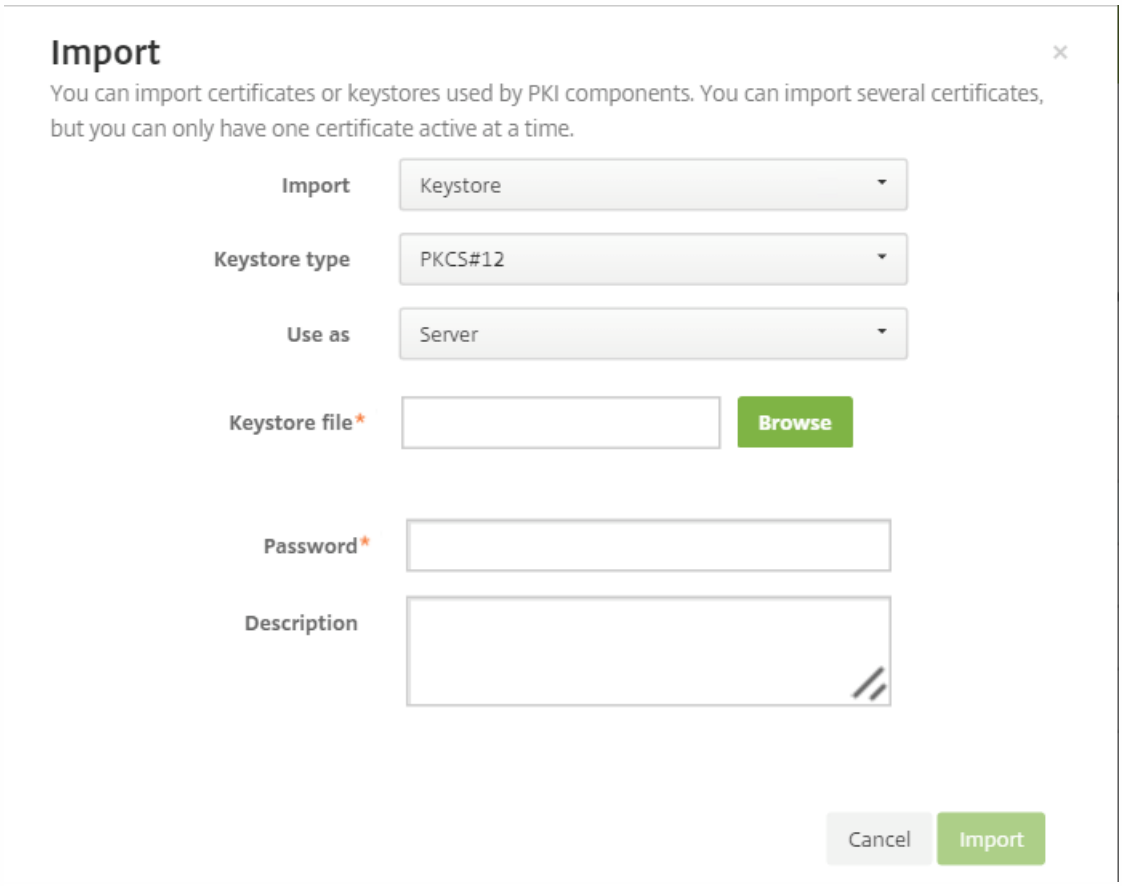
Cómo cargar el certificado en XenMobile

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, a continuación, 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 ha instalado correctamente. Debe aparecer como User certificate.

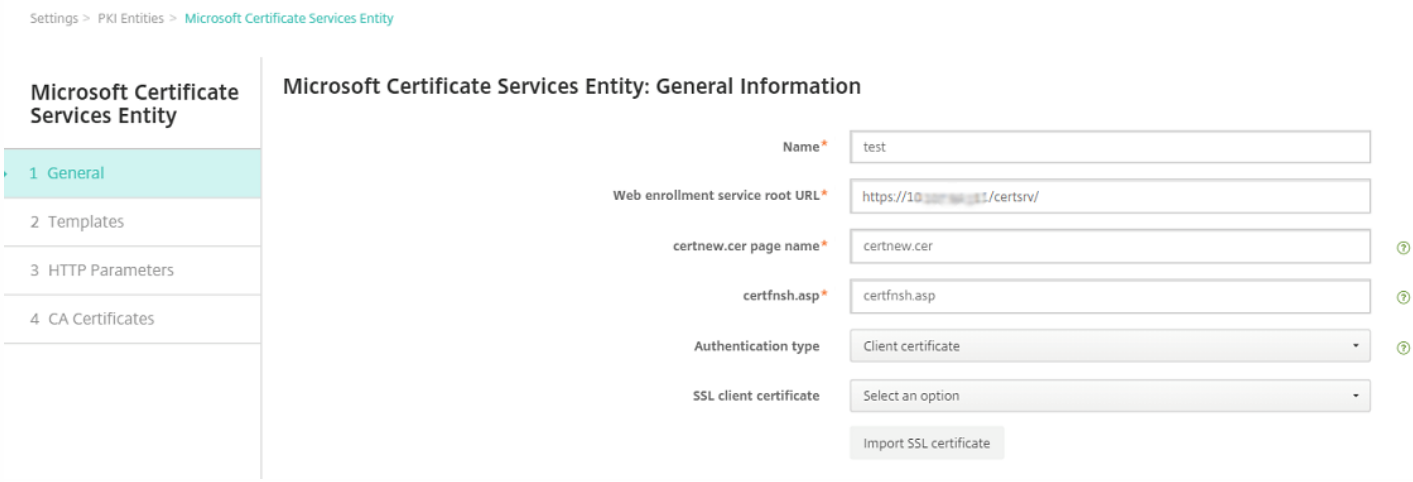
Creación de una entidad PKI para la autenticación basada en certificados

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

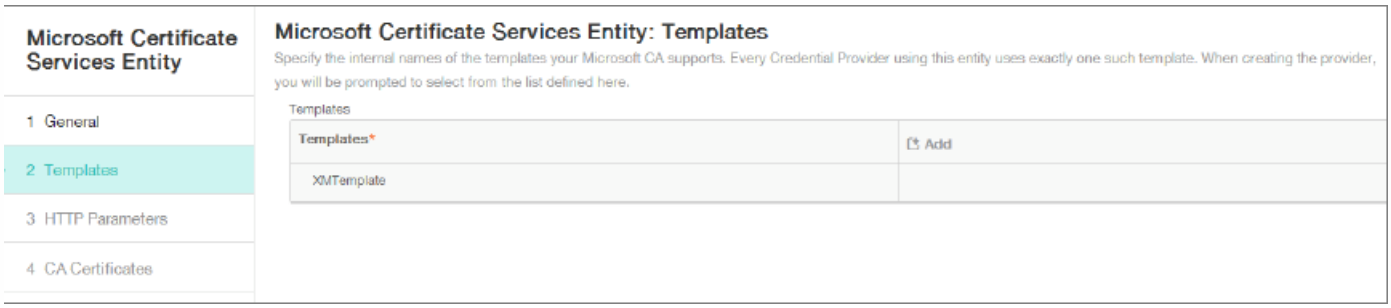
2. Haga clic en **Add** y, a continuación, haga clic en **Microsoft Certificate Services Entity**. Aparecerá la pantalla **Microsoft Certificate Services Entity: General Information**.

3. Introduzca los parámetros siguientes:

- **Name**. Introduzca algún nombre.
- **Web enrollment service root URL**. https://RootCA-URL/certsrv/
  Debe agregar la última barra diagonal (/) a la ruta de 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 XenMobile.

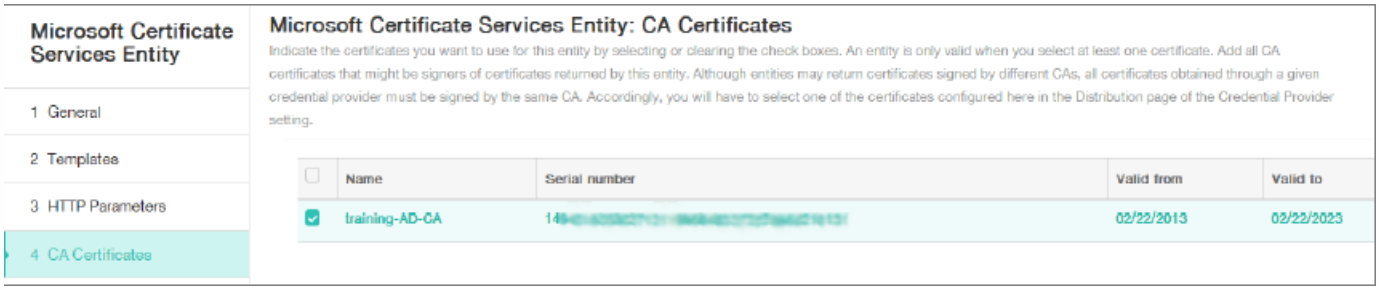


4. En **Templates**, agregue la plantilla que creó cuando configuró el certificado de Microsoft. Asegúrese de no agregar espacios.



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

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



7. Haga clic en **Save**.

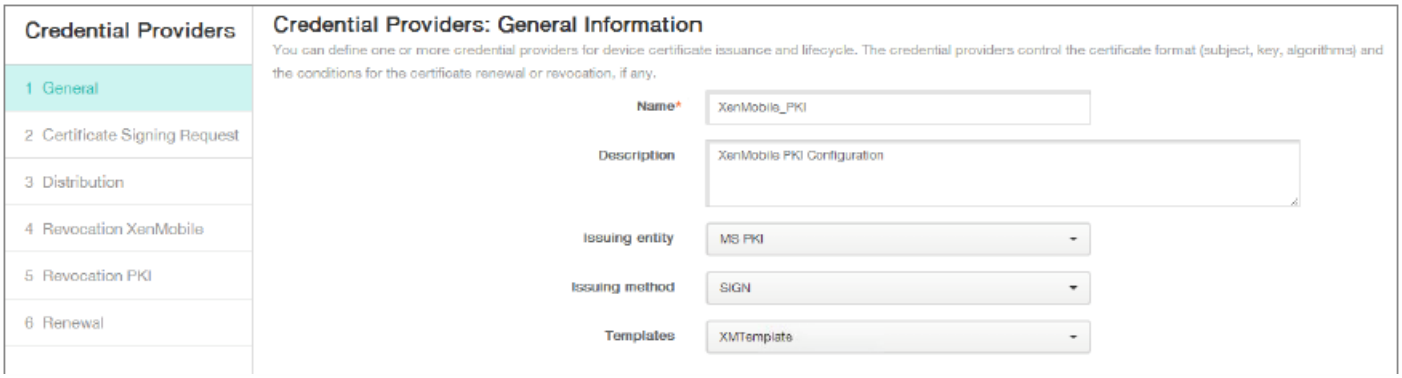
Configuración de proveedores de credenciales

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.

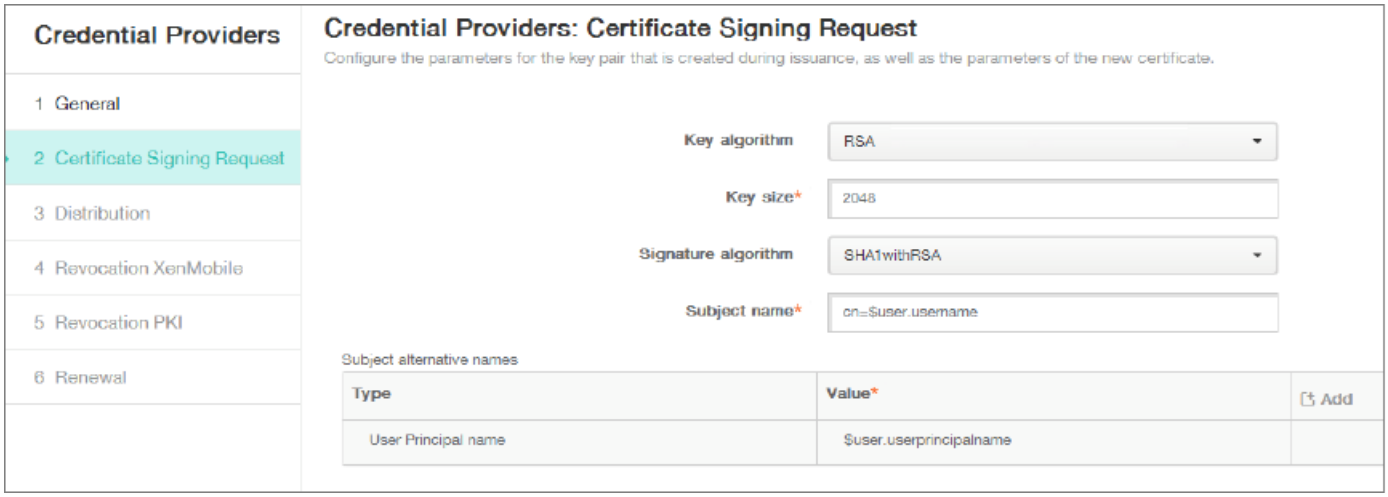


4. Haga clic en **Certificate Signing Request** e introduzca los parámetros siguientes:

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

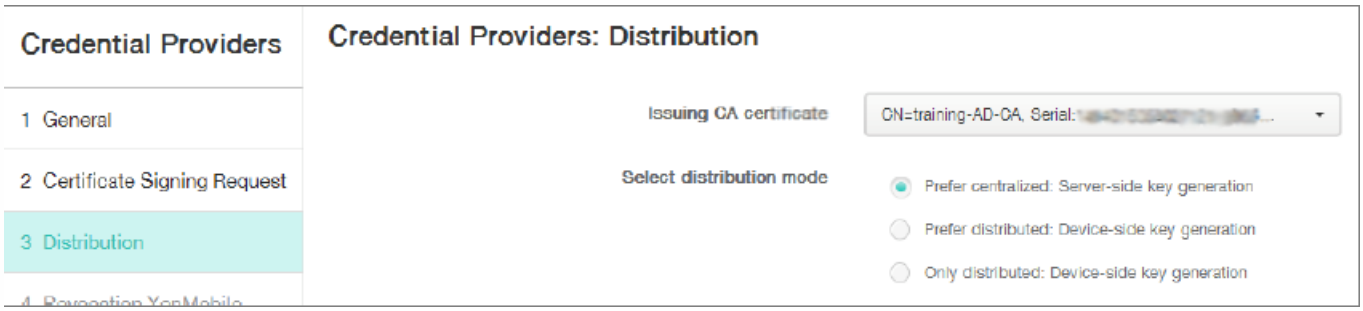
Para **Subject Alternative Names**, haga clic en **Add** e introduzca los parámetros siguientes:

- **Type**. Nombre principal del usuario
- **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 XenMobile.
- **Select distribution mode**. Seleccione **Prefer centralized: Server-side key generation**.

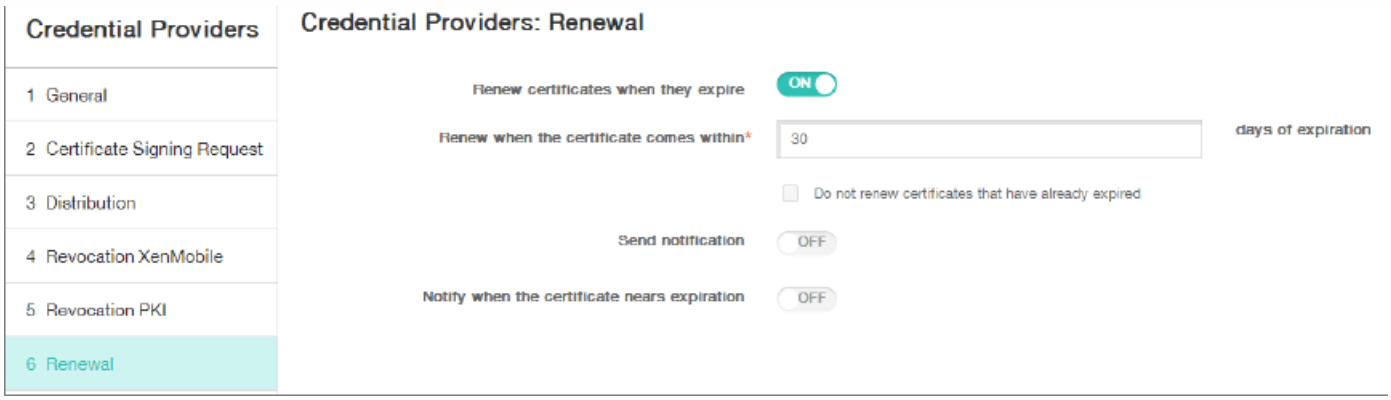


6. Para las dos secciones siguientes (**Revocation XenMobile** y **Revocation PKI**), defina los parámetros como sea necesario. Para el objetivo de este artículo, se omiten ambas opciones.

7. Haga clic en **Renewal**.

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

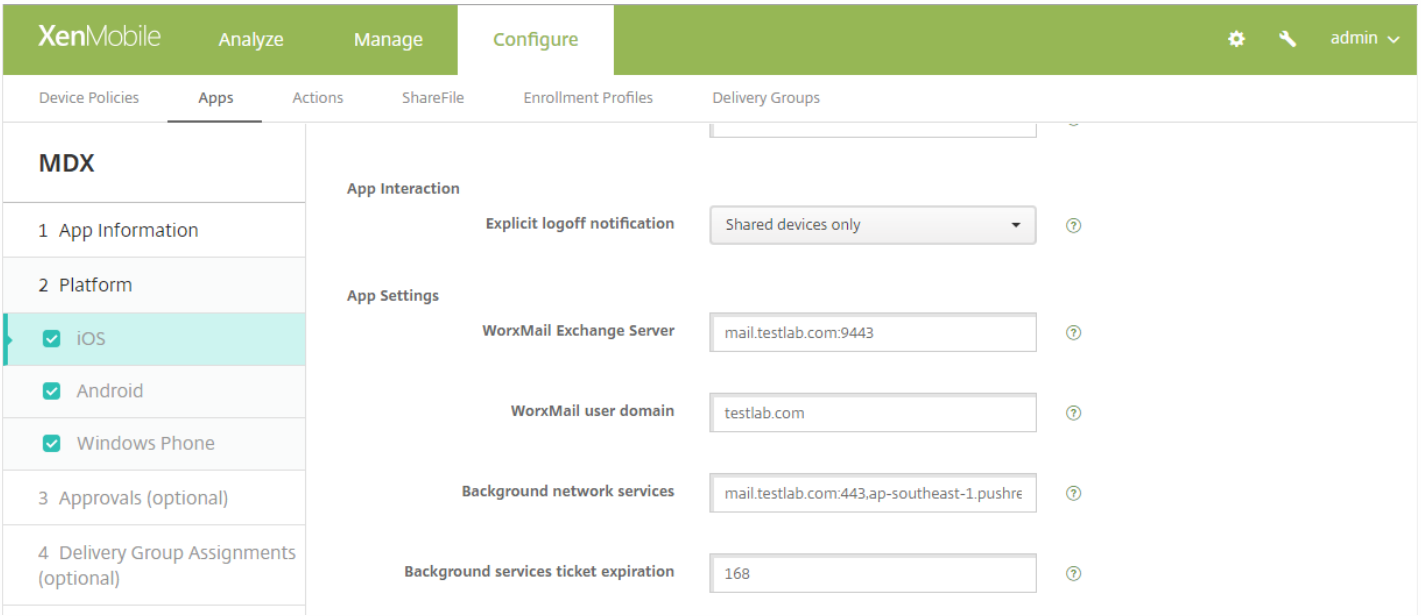
9 Deje todos los demás parámetros con los valores predeterminados o cámbielos si es necesario.



10. Haga clic en **Save**.

Configuración de Secure Mail para la autenticación basada en certificados

Cuando agregue Secure Mail a XenMobile, debe configurar los parámetros de Exchange en **App Settings**.



Configuración de la entrega de certificados de NetScaler en XenMobile

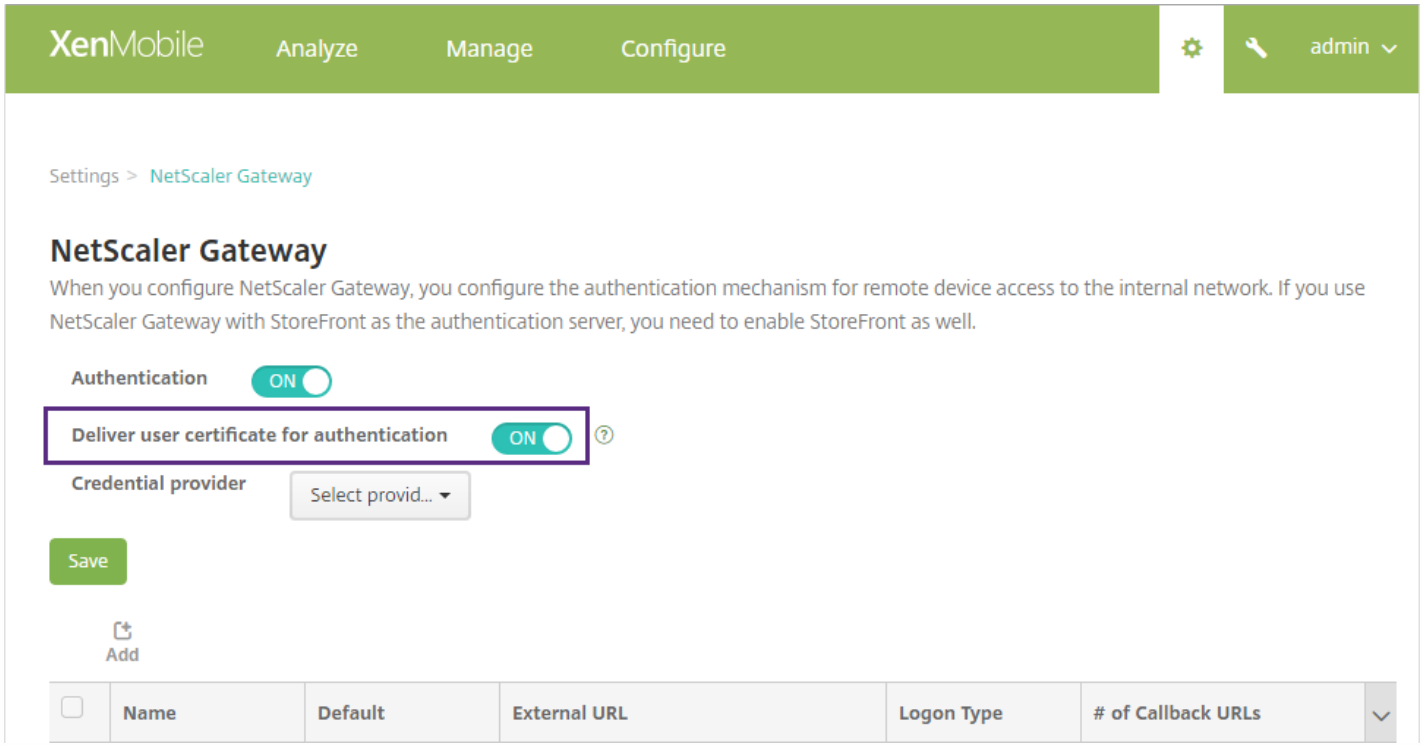
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Settings**.

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

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

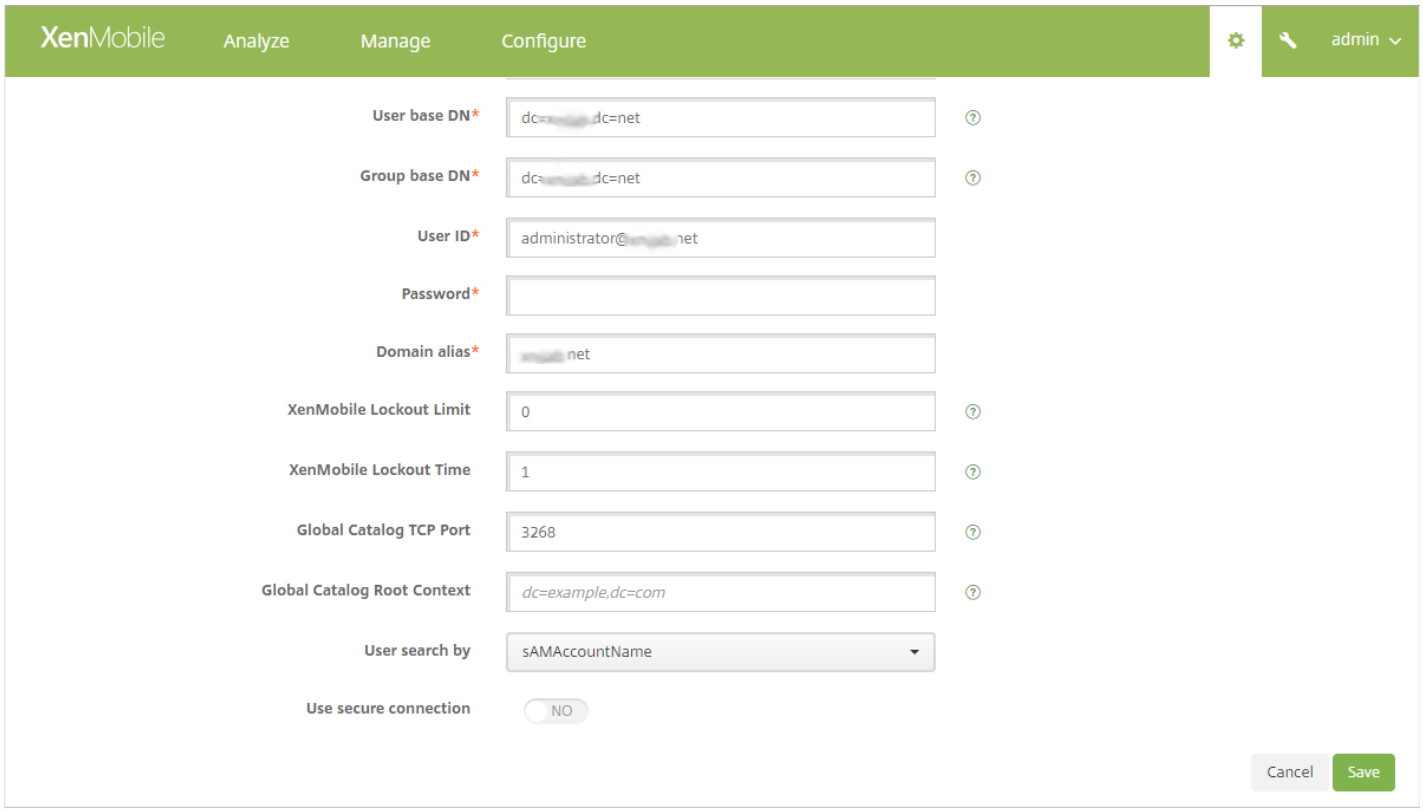
- **External URL**. https://URLdelNetScalerGateway
- **Logon Type**. Certificado.
- **Password Required**. Desactivado (OFF).
- **Set as Default**: Activado (ON).

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



5. En **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 a **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

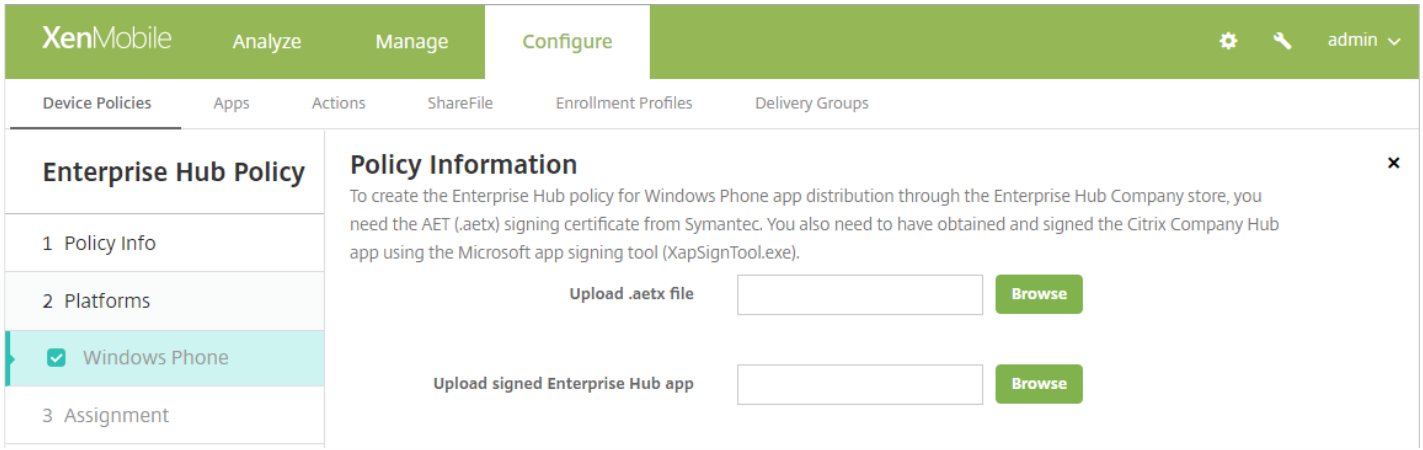
Para dispositivos Windows Phone, es necesario crear una directiva de dispositivos Enterprise Hub para entregar el archivo AETX y el cliente Secure Hub.

> **Nota**
>
> Compruebe que ambos archivos, AETX y Secure Hub, utilicen el mismo certificado de empresa del proveedor de certificados y el mismo ID de publicador de la cuenta de desarrollador para la Tienda Windows.

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

2. Haga clic en **Add** y, a continuación, en **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 Secure Hub firmada para Enterprise Hub.



4. Asigne la directiva a grupos de entrega y guárdela.

Solución de problemas en la configuración de certificados de cliente

Después de definir correctamente la configuración anterior, además de configurar NetScaler Gateway, el flujo de trabajo del usuario es el siguiente:

1. Los usuarios inscriben sus dispositivos móviles.

2. XenMobile solicita a los usuarios que creen un PIN de Citrix.

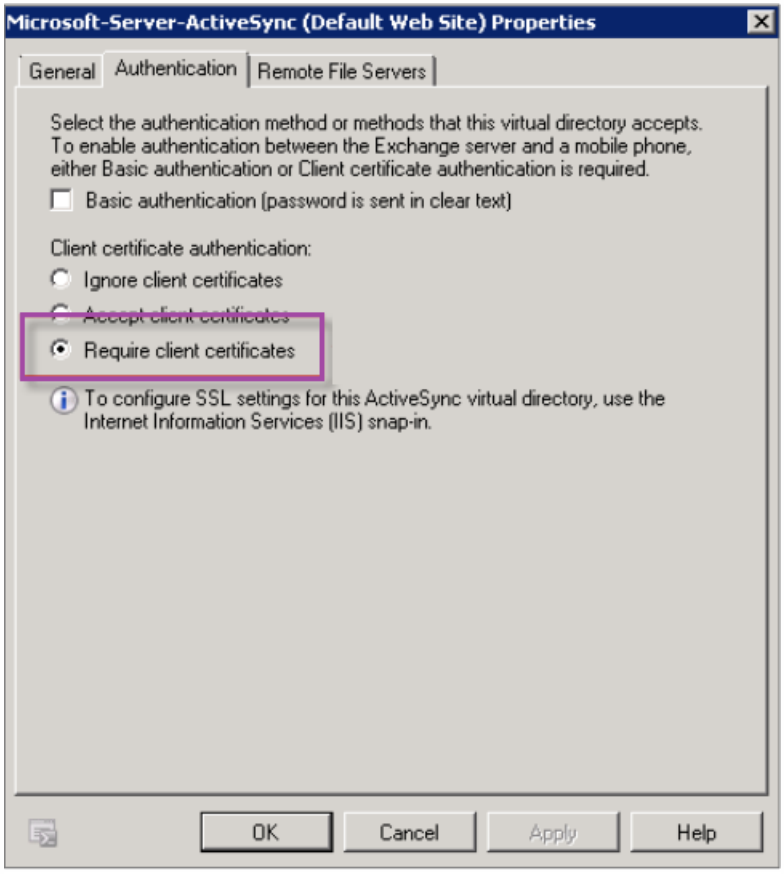
3. Se redirige a los usuarios a XenMobile Store.

4. Cuando los usuarios inician Secure Mail, XenMobile no les pedirá credenciales para configurar su buzón. En su lugar, Secure Mail solicitará el certificado del cliente de Secure Mail y lo enviará a Microsoft Exchange Server para la autenticación. Si XenMobile pide credenciales cuando los usuarios inician Secure Mail, verifique si ha configurado todo correctamente.

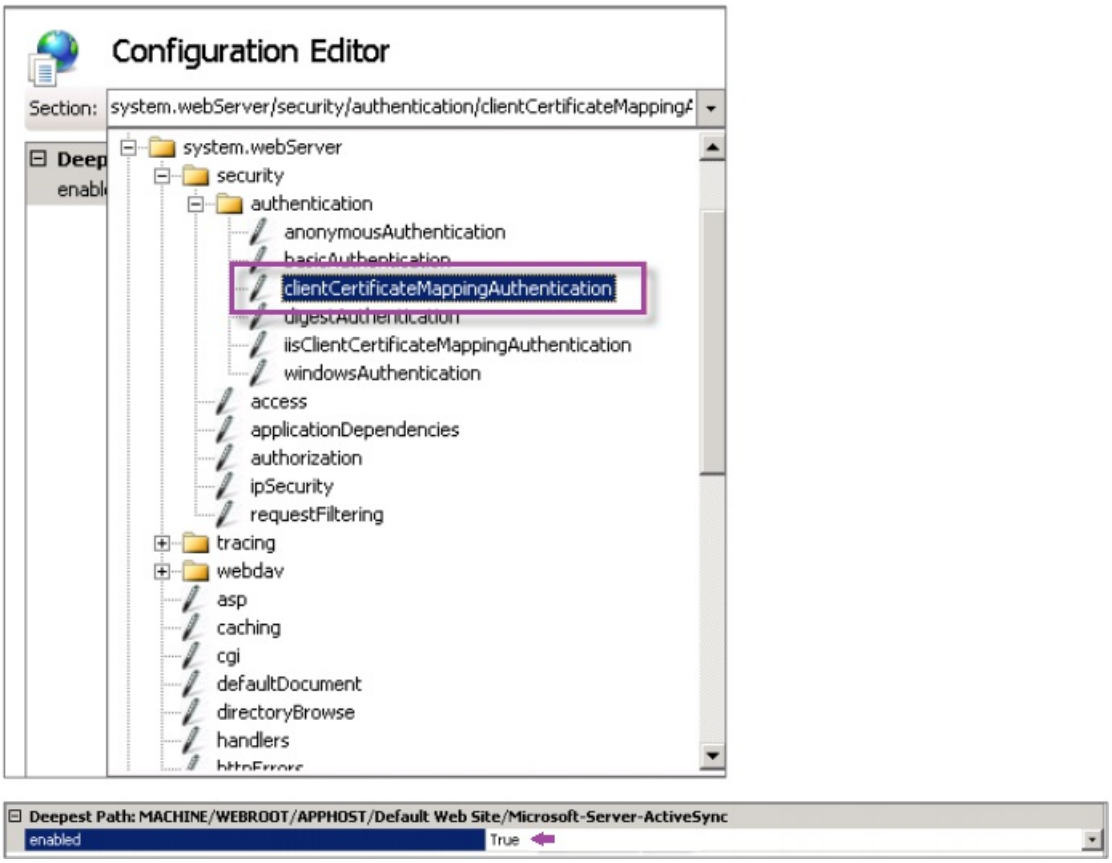
Si los usuarios pueden descargar e instalar Secure Mail, pero durante la configuración de buzones Secure Mail no puede finalizar la configuración:

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, visite el sitio **Microsoft-Server-ActiveSync** para ver si tiene habilitada la autenticación con asignación de certificados del cliente (que está inhabilitada de manera predeterminada). La opción está en **Editor de configuración > Seguridad > Autenticación**.



Nota: Después de seleccionar **Verdadero**, debe hacer clic en **Aplicar** para que los cambios tengan efecto.

4. Revise la configuración de NetScaler Gateway en la consola de XenMobile: **Deliver user certificate for authentication** debe estar establecido en **ON** y **Credential provider** debe tener seleccionado el perfil correcto, como se ha descrito 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 ver 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 Secure Mail 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 con el mismo certificado de empresa del proveedor de certificados utilizado para empaquetar Secure Mail y firmar las aplicaciones de Secure Hub.
- Compruebe que se usa el mismo ID de publicador para firmar y empaquetar Secure Hub, Secure Mail y el token de inscripción de la aplicación.

Entidades de infraestructura PKI

Feb 27, 2017

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)
- Servicios de certificados de Microsoft

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.

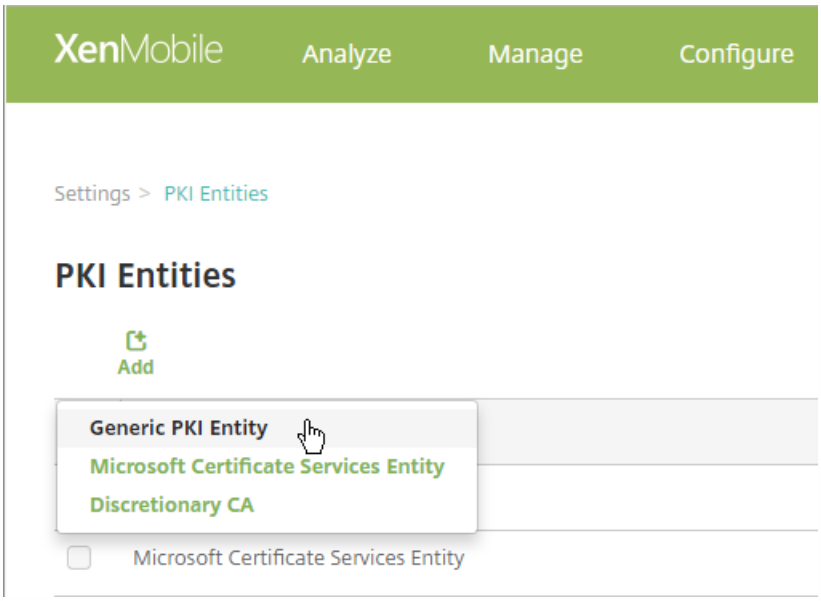
Admitir cada una de las operaciones de PKI en un adaptador es opcional. Si un adaptador admite esa operación, es que tiene la funcionalidad correspondiente (firmar, obtener o revocar). Cada una de estas capacidades se puede asociar a un conjunto de parámetros de usuario.

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 **Settings** > **PKI Entities**.

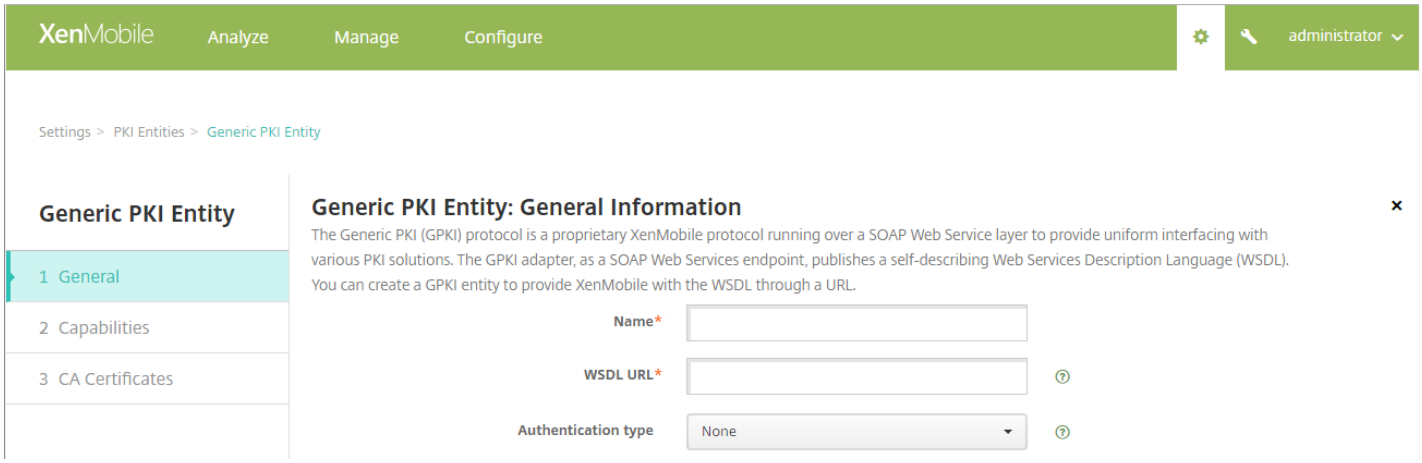
2. En la página **PKI Entities**, haga clic en **Add**.

Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.



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 **PKI Entities**.

2. En la página **PKI Entities**, haga clic en **Add**.

Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.

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**, configure estos parámetros:

- **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 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**. Elija 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 **Test connection** para comprobar que el servidor está accesible. Si no está accesible, aparecerá un mensaje donde se indica que la conexión no ha podido establecerse. Compruebe los parámetros de configuración.

6. 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.

7. 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.

8. 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.

9 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.

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

11. 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, plantéese 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**.

Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.

3. Haga clic en **Discretionary CA**.

Aparece la página **Discretionary CA: General Information**.

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

- **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 las 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**.

Aparece 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**. Identifique el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, deberá establecer las claves apropiadas en **On**. Una vez establecidas, la entidad de certificación está limitada a la emisión de certificados para esos fines.
- **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** (Centralizado: generación de claves en el lado del servidor). 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** (Distribuido: generación de claves en el lado del dispositivo). 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**.

Aparece 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

Feb 27, 2017

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. Si el proveedor de credenciales P se implementa en el dispositivo D como parte de la configuración C, los parámetros de emisión de P determinarán el certificado que se implementará en D, sus parámetros de renovación se aplicarán cuando se actualice C y sus parámetros de revocación se aplicarán cuando se elimine C o se revoque D.

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

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

En XenMobile, hay disponibles dos modos de entrega de certificados: centralizada y distribuida. El modo distribuido usa SCEP (Protocolo de inscripción de certificados simple) y solo está disponible en los casos en que el cliente admite el protocolo (solo para iOS). El modo distribuido es 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. Por eso, XenMobile debe demostrar al cliente que tiene autoridad para actuar como tal. Esta autoridad se establece si se cargan 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

Contexto	Se admite SCEP	Se requiere SCEP
Inscripción de Windows Phone y Tablet	NO	NO
Configuración de Windows Phone y Tablet	No, excepto la directiva de redes Wi-Fi, que está respaldada en Windows Phone 8.1 y la versión más reciente de Windows 10	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 en **Fetch** para designar el método que usará el sistema para obtener certificados de la entidad configurada. Para la autenticación de certificado del cliente, use **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: Nombre principal del usuario
Value: $user.userprincipalname

Nota: Al igual que para el nombre del sujeto (Subject Name), puede usar 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** (Preferir modo centralizado: Generación de clave en el lado del servidor). 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** (Preferir modo distribuido: Generación de clave en el lado del dispositivo). 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** (Solo distribuido: Generación de clave en el lado del dispositivo). 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 elige **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: Establezca **Renew certificates when they expire** en **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 **Send notification** en **On**. Puede elegir entre dos opciones de notificación:

- Si elige **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 elige **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.

Certificados APNs

Feb 27, 2017

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	Crear una solicitud CSR en IIS Crear 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	Enviar una solicitud CSR firmada a Apple	Envíe la solicitud de firma de certificado firmada a Apple por medio del portal Apple Push Certificates 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).

	Crear 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 electrónico**. 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 **Listo** 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: Si quiere usar OpenSSL para 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.
   You are about to be asked to enter information that will be incorporated
   into your certificate request. (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.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank. (Existen varios campos, aunque puede dejar algunos en blanco.
   Algunos campos contendrán 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.
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   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 recuperar 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 **Aceptar**.
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 **Aceptar**. 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 **Aceptar**. 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, visite el portal Apple Push Certificates Portal y cargue 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. Cuando renueve el certificado, debe usar el mismo nombre de organización e ID de Apple.

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 firmada 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**.

SAML para Single Sign-On con ShareFile

Apr 27, 2017

Puede configurar XenMobile y ShareFile para que utilicen el lenguaje Security Assertion Markup Language (SAML) si quiere proporcionar el acceso de inicio de sesión único o Single Sign-On para las aplicaciones móviles de ShareFile. Esta función incluye aquellas aplicaciones de ShareFile que se han empaquetado con MDX Toolkit y los clientes no empaquetados de ShareFile (como el sitio Web, Outlook Plug-in o clientes de sincronización).

- **En caso de aplicaciones de ShareFile empaquetadas**. A los usuarios que inician sesión en ShareFile a través de la aplicación de ShareFile para móvil se les redirige a Secure Hub para la autenticación de usuario y para obtener un token de SAML. Después de una autenticación correcta, la aplicación de ShareFile para móviles envía el token de SAML a ShareFile. Después del primer inicio de sesión, los usuarios pueden acceder a la aplicación de ShareFile para móviles mediante Single Sign-On (SSO) y adjuntar documentos de ShareFile a correos electrónicos de Secure Mail sin iniciar sesión cada vez.
- **En caso de clientes no empaquetados de ShareFile**. A los usuarios que inician sesión en ShareFile a través de un explorador Web u otro cliente de ShareFile se les redirige a XenMobile para la autenticación de usuario y para obtener un token de SAML. Después de una autenticación correcta, el token de SAML se envía a ShareFile. Después del primer inicio de sesión, los usuarios pueden acceder a los clientes de ShareFile mediante Single Sign-On sin iniciar sesión cada vez.

Si quiere usar XenMobile como un proveedor de identidades (IdP) SAML para ShareFile, debe configurar XenMobile para usar ShareFile Enterprise, como se describe en este artículo. De forma alternativa, puede configurar XenMobile para que funcione solamente con conectores de StorageZone. Para obtener más información, consulte Uso de ShareFile con XenMobile.

Para ver diagramas de referencia de arquitectura en detalle, consulte el artículo Reference Architecture for On-Premises Deployments en XenMobile Deployment Handbook.

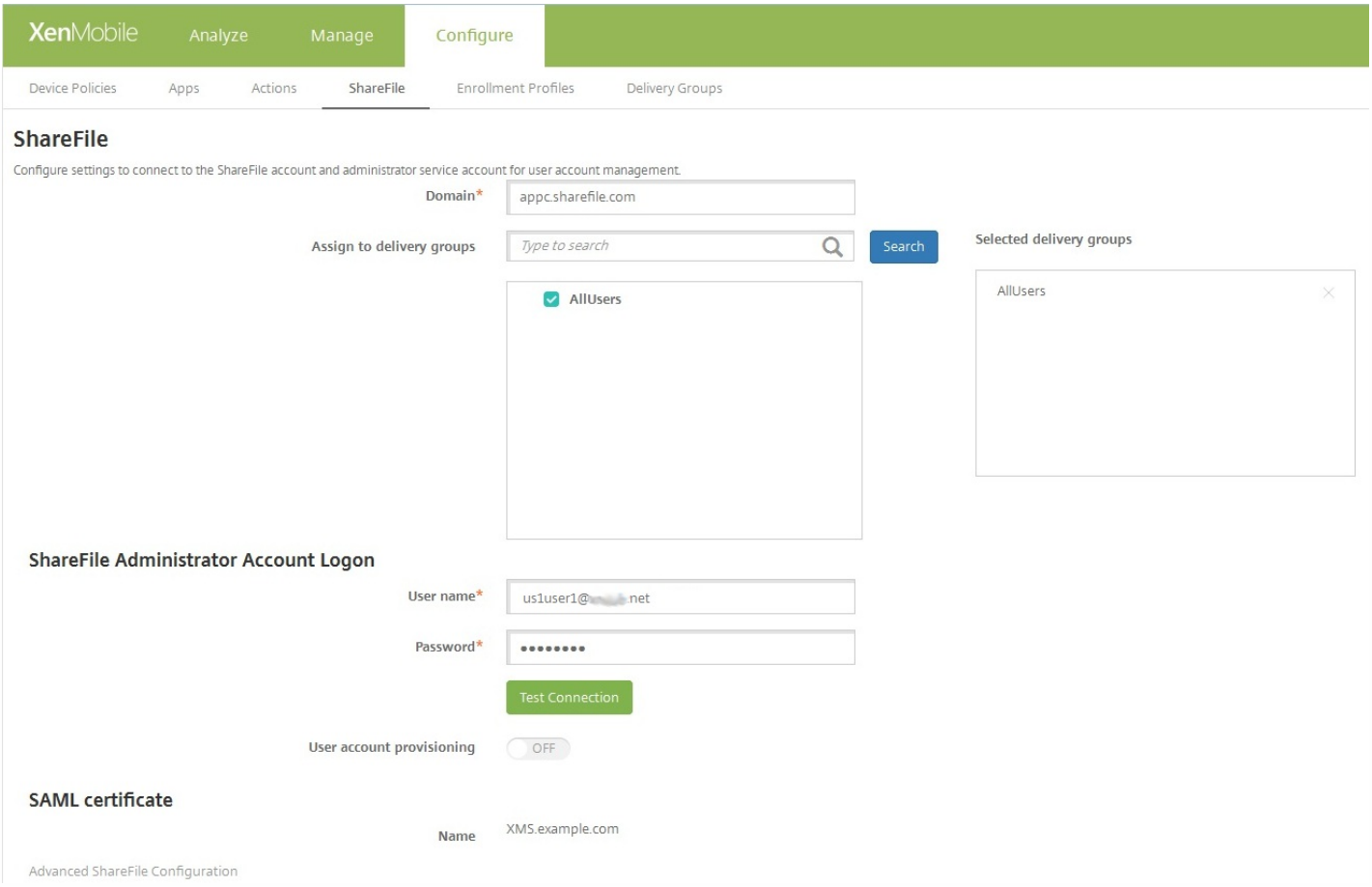
Debe cumplir los siguientes requisitos previos antes de configurar SSO con XenMobile y las aplicaciones de ShareFile:

- Una versión compatible de MDX Toolkit (para aplicaciones móviles de ShareFile)
- Una versión compatible de aplicaciones móviles de ShareFile y Secure Hub
- Cuenta de administrador de ShareFile

Compruebe la conexión entre XenMobile y ShareFile.

Antes de configurar SAML para ShareFile, debe indicar la información de acceso de ShareFile de la siguiente manera:

1. En la consola Web de XenMobile, haga clic en **Configure > ShareFile**. Aparecerá la página de configuración **ShareFile**.



2. Configure estos parámetros:

- **Domain**. Escriba el nombre de subdominio de ShareFile; por ejemplo, ejemplo.sharefile.com.
- **Assign to delivery groups**. Seleccione o busque los grupos de entrega que quiera que puedan usar SSO con ShareFile.
- **Inicio de sesión de cuenta de administrador de ShareFile**
  - **User name**. Escriba el nombre de usuario del administrador de ShareFile. Este usuario debe tener privilegios de administrador.
  - **Password**. Escriba la contraseña del administrador de ShareFile.
  - **User account provisioning**. Active esta opción si quiere habilitar la función de aprovisionamiento de usuarios en XenMobile. Si no, déjela inhabilitada en caso de que vaya a utilizar la herramienta de administración de usuarios (User Management Tool) de ShareFile para el aprovisionamiento.

    Nota: Si se incluye un usuario sin cuenta de ShareFile en los roles seleccionados, XenMobile aprovisionará automáticamente una cuenta de ShareFile a dicho usuario si usted habilita la opción User account provisioning. Citrix recomienda utilizar un rol con una pertenencia limitada para probar la configuración. Esto evita la posibilidad de una gran cantidad de usuarios sin cuentas de ShareFile.

3. Haga clic en **Test Connection** para verificar que el nombre de usuario y la contraseña de la cuenta de administrador de ShareFile realizan la autenticación en la cuenta de ShareFile especificada.

4. Haga clic en **Save**. XenMobile se sincroniza con ShareFile y actualiza la configuración de ShareFile **ShareFile Issuer/Entity ID** y **Login URL**.

Los siguientes pasos se aplican a aplicaciones y dispositivos iOS y Android.

1. Con MDX Toolkit, empaquete la aplicación de ShareFile para móviles. Para obtener más información sobre cómo empaquetar aplicaciones con MDX Toolkit, consulte Empaquetado de aplicaciones con MDX Toolkit.

2. En la consola de XenMobile, cargue la aplicación empaquetada de ShareFile para móviles. Para obtener información sobre cómo cargar aplicaciones MDX, consulte Para agregar una aplicación MDX a XenMobile.

3. Para comprobar los parámetros de SAML, inicie sesión en ShareFile con el nombre de usuario y contraseña de administrador que ha configurado anteriormente.

4. Compruebe que ShareFile y XenMobile están configurados en la misma zona horaria.

Nota: Compruebe que XenMobile muestra la hora correcta con respecto a la zona horaria configurada. Si no es así, puede que se produzca un error de inicio de sesión Single Sign-On.

Cómo validar la aplicación de ShareFile para móviles

1. En el dispositivo de usuario (si no se ha hecho aún), instale y configure Secure Hub.

2. Desde XenMobile Store, descargue e instale la aplicación de ShareFile para móviles.

3. Inicie la aplicación de ShareFile para móviles. ShareFile se inicia sin solicitar el nombre de usuario ni la contraseña.

Validación con Secure Mail

1. En el dispositivo de usuario (si no se ha hecho aún), instale y configure Secure Hub.

2. Desde XenMobile Store, descargue, instale y configure Secure Mail.

3. Abra un nuevo correo electrónico y toque en **Adjuntar desde ShareFile**. Los archivos disponibles para adjuntar al mensaje de correo electrónico se muestran sin solicitar el nombre de usuario ni la contraseña.

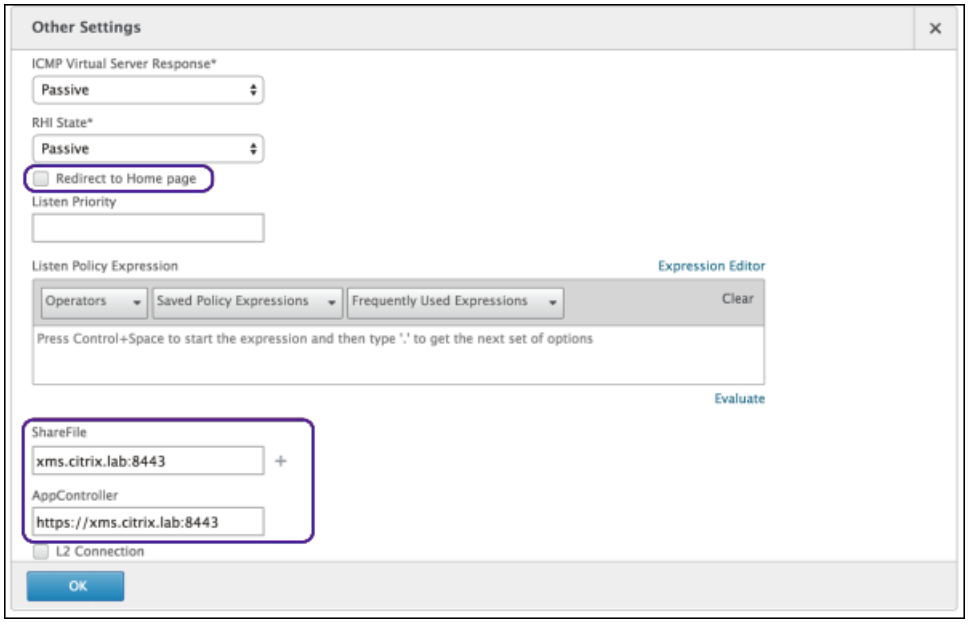
Si quiere configurar el acceso para clientes no empaquetados de ShareFile (como el sitio Web, el plugin para Outlook o los clientes de sincronización), debe configurar NetScaler Gateway para que admita el uso de XenMobile como un proveedor de identidad SAML de la siguiente manera:

- Inhabilite la redirección de la página principal.
- Cree un perfil y una directiva de sesión de ShareFile.
- Configure directivas en el servidor virtual de NetScaler Gateway.

Cómo inhabilitar la redirección de la página principal

Debe inhabilitar el comportamiento predeterminado ante las solicitudes procedentes de la ruta /cginfra, de modo que el usuario vea la URL interna original solicitada en lugar de la página principal configurada.

1. Modifique la configuración del servidor virtual de NetScaler Gateway que se usa para los inicios de sesión de XenMobile. En NetScaler 10.5, vaya a **Other Settings** y, a continuación, desmarque la casilla **Redirect to Home Page**.



2. En **ShareFile**, escriba el número de puerto y el nombre del servidor interno de XenMobile.

3. En **AppController**, escriba la URL de XenMobile.

Esta configuración autoriza solicitudes a la URL que ha especificado mediante la ruta /cginfra.

Creación de un perfil de solicitudes y una directiva de sesión de ShareFile

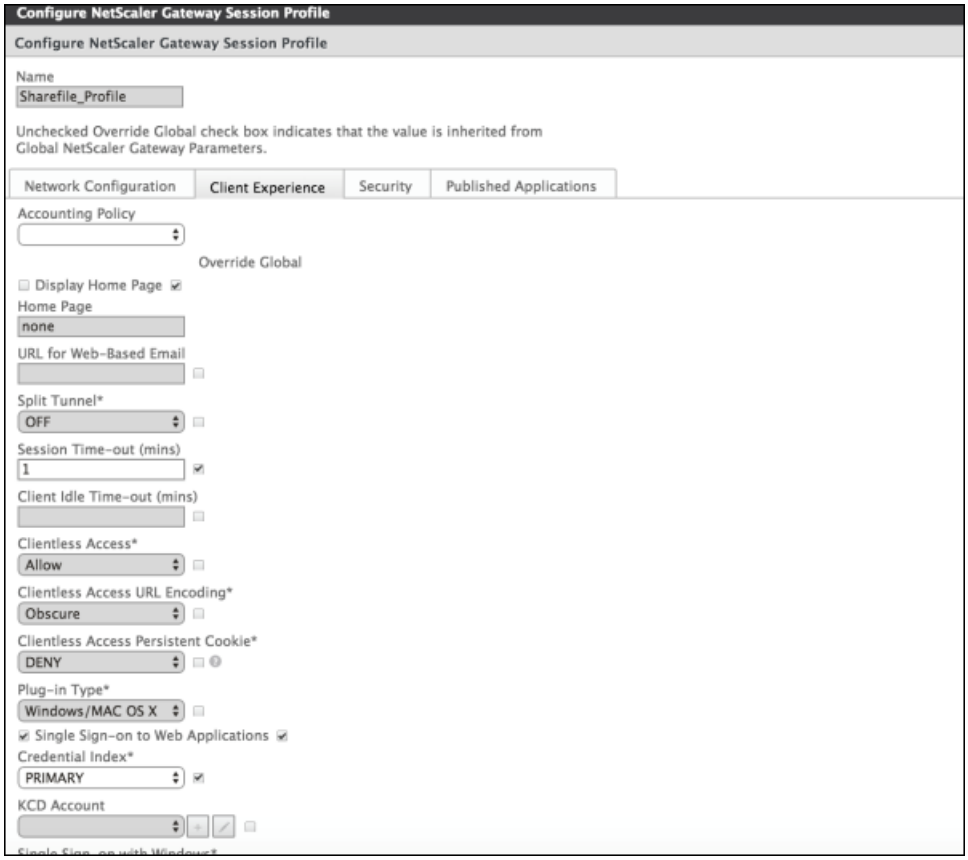
Configure los siguientes parámetros para crear un perfil de solicitudes y una directiva de sesión de ShareFile:

1. En la herramienta de configuración de NetScaler Gateway, en el panel de navegación de la izquierda, haga clic en **NetScaler Gateway > Policies > Session**.

2. Cree una nueva directiva de sesión. En la ficha **Policies**, haga clic en **Add**.

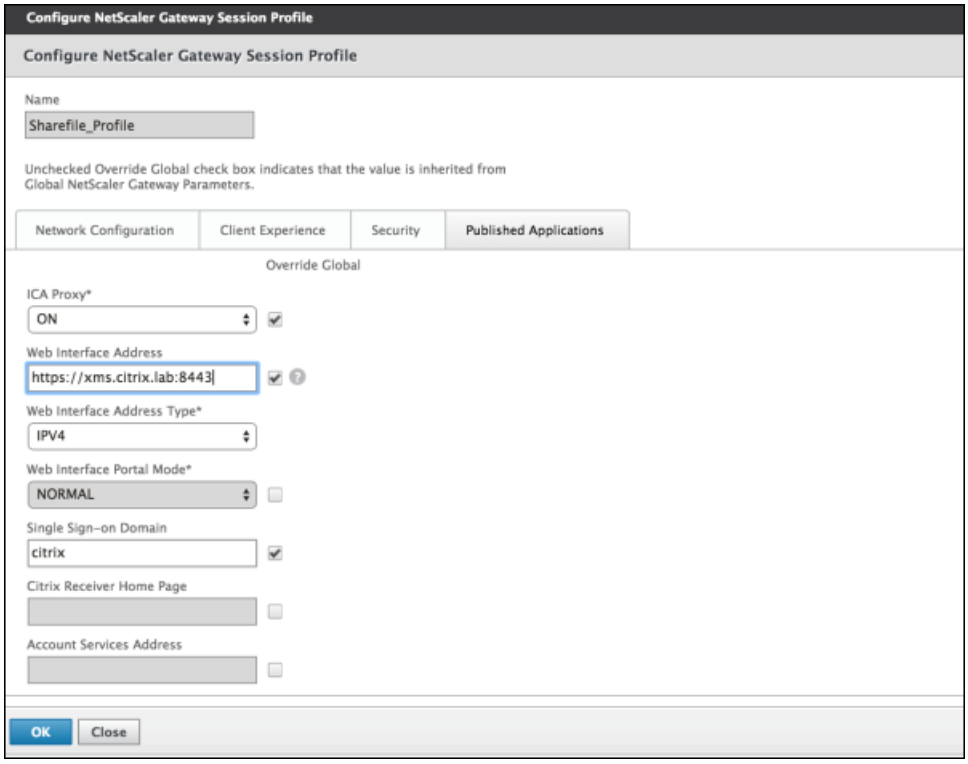
3. En el campo **Name**, escriba **ShareFile_Policy**.

4. Para crear una acción nueva, haga clic en el botón **+**. Aparecerá la página **Create NetScaler Gateway Session Profile**.



Configure estos parámetros:

- **Name**. Escriba ShareFile_Profile.
- Haga clic en la ficha **Client Experience** y, a continuación, configure los siguientes parámetros:
  - **Home Page**. Escriba "none".
  - **Session Time-out (mins)**. Escriba 1.
  - **Single Sign-On to Web Applications**. Marque esta opción de configuración.
  - **Credential Index**. En la lista, haga clic en PRIMARY.
- Haga clic en la ficha **Published Applications**.



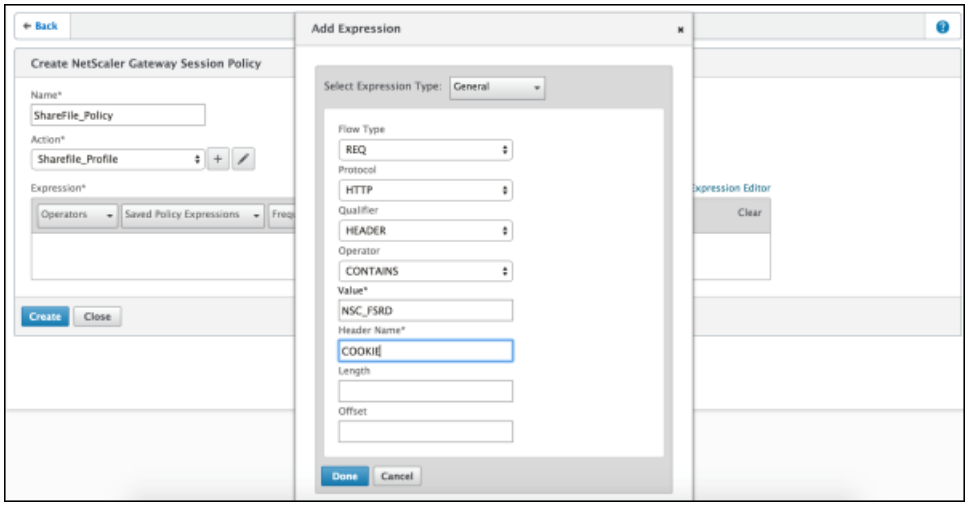
Configure estos parámetros:

- **ICA Proxy**. En la lista, haga clic en **ON**.
- **Web Interface Address**. Escriba la URL del servidor XenMobile.
- **Single Sign-On Domain**. Escriba el nombre del dominio de Active Directory.

  Nota: Al configurar el perfil de sesión de NetScaler Gateway, el sufijo de dominio de **Single Sign-On Domain** debe coincidir con el alias de dominio de XenMobile definido en LDAP.

5. Haga clic en **Create** para definir el perfil de sesión.

6. Haga clic en **Expression Editor**.



Configure estos parámetros:

- **Value**. Escriba NSC_FSRD.
- **Header Name**. Escriba COOKIE.
- Haga clic en **Done**.

7. Haga clic en **Create** y, luego, en **Close**.

Configure directivas en el servidor virtual de NetScaler Gateway.

Configure los siguientes parámetros en el servidor virtual de NetScaler Gateway.

1. En la herramienta de configuración de NetScaler Gateway, en el panel de navegación de la izquierda, haga clic en **NetScaler Gateway > Virtual Servers**.

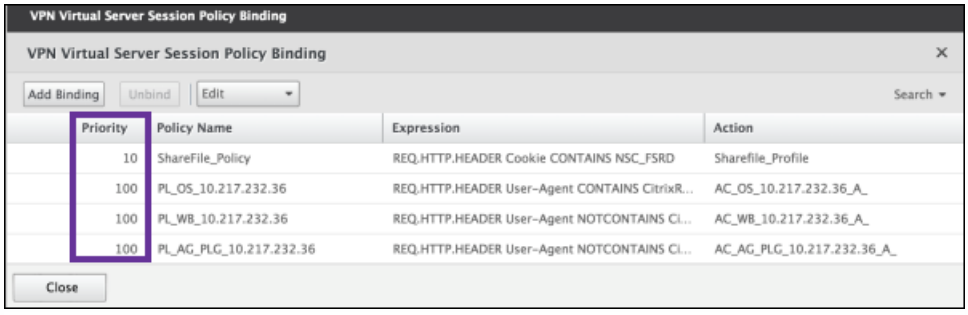
2. En el panel **Details**, haga clic en el servidor virtual de NetScaler Gateway.

3. Haga clic en **Edit**.

4. Haga clic en **Configured policies > Session policies** y, a continuación, haga clic en **Add binding**.

5. Seleccione **ShareFile_Policy**.

6. Modifique el número de **Priority** generado automáticamente de la directiva seleccionada, de modo que esta tenga la prioridad más alta (el número más bajo) en relación con las demás directivas de la lista, tal y como se muestra en la siguiente imagen.



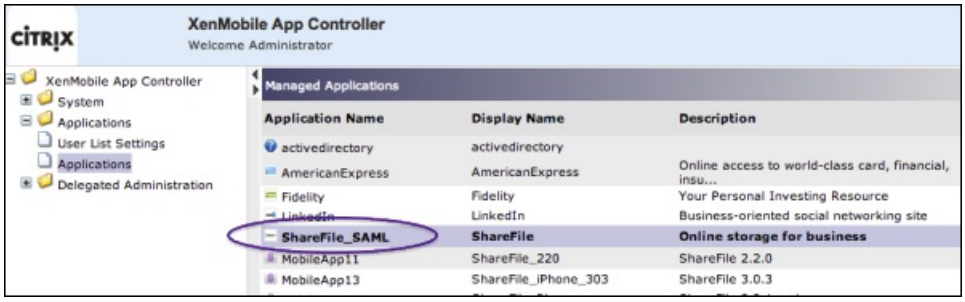
7. Haga clic en **Done** y, a continuación, guarde la configuración activa de NetScaler.

Utilice los siguientes pasos a fin de buscar el nombre interno de la aplicación para la configuración de ShareFile.

1. Inicie sesión en la herramienta de administración de XenMobile a través de la URL **https://:4443/OCA/admin/**. Compruebe que "OCA" está escrito en letras mayúsculas.

2. En la lista **View**, haga clic en **Configuration**.

3. Haga clic en **Applications > Applications** y anote el texto de la columna **Application Name** correspondiente a "ShareFile" en la columna **Display Name**.



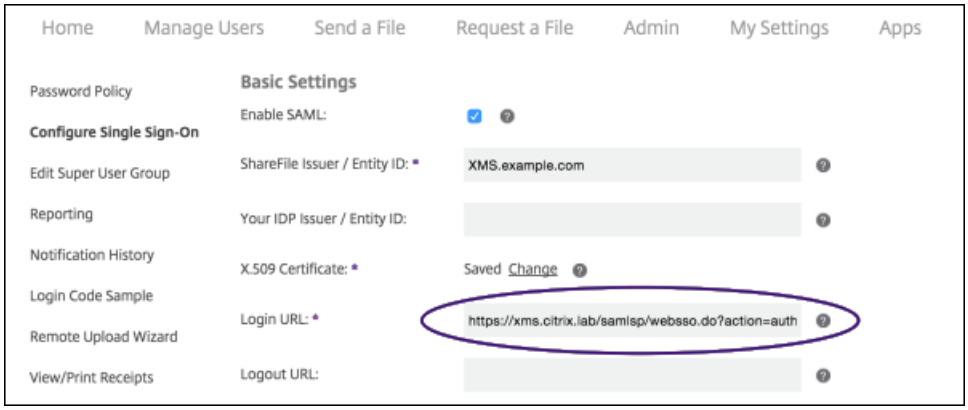
Cómo modificar los parámetros de Single Sign-On de ShareFile.com

1. Inicie sesión en su cuenta de ShareFile (https://.sharefile.com) como administrador de ShareFile.

2. En la interfaz Web de ShareFile, haga clic en **Admin** y, a continuación, seleccione **Configure Single Sign-On**.

3. Modifique el campo **Login URL** de la siguiente manera:

El campo **Login URL** debe ser similar a: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- Inserte el nombre de dominio completo (FQDN) externo del servidor virtual de NetScaler Gateway y "/cginfra/https/" delante del FQDN del servidor XenMobile y, a continuación, agregue "8443" después del FQDN de XenMobile.

  Ahora, la URL debería parecerse a la siguiente:
  https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- Cambie el valor del parámetro **&app=ShareFile_SAML_SP** al nombre interno de la aplicación ShareFile del paso 3 en SAML para Single Sign-On con ShareFile. De forma predeterminada, el nombre interno es **ShareFile_SAML**. Sin embargo, cada vez que cambie la configuración, se agrega un número al nombre interno (ShareFile_SAML_2, ShareFile_SAML_3, y así sucesivamente).

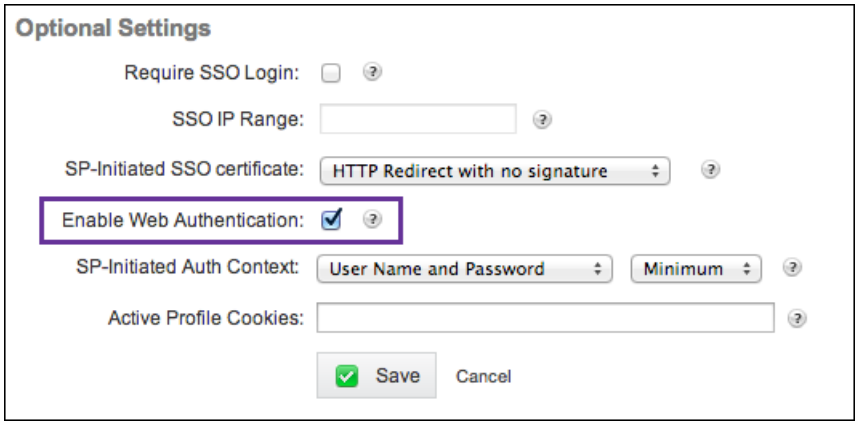
  Ahora, la URL debería parecerse a la siguiente:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUse**r&app=ShareFile_SAML**&reqtype=1

- Agregue "&nssso=true" al final de la URL.

  Ahora, la URL modificada debería parecerse a la siguiente:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**

  Importante: Cada vez que modifique o vuelva a crear la aplicación de ShareFile, o bien cambie los parámetros de ShareFile en la consola de XenMobile, se agrega un número nuevo al nombre interno de la aplicación, lo que significa que también debe actualizar la URL de inicio de sesión en el sitio Web de ShareFile para reflejar el nuevo nombre de la aplicación.

4. En **Optional Settings**, marque la casilla **Enable Web Authentication**.



Lleve a cabo lo siguiente para validar la configuración.

1. Apunte su explorador a https://sharefile.com/saml/login.

Se le redirigirá al formulario de inicio de sesión de NetScaler Gateway. Si no se le redirige, compruebe los parámetros de configuración anteriores.

2. Escriba el nombre de usuario y la contraseña del entorno de XenMobile y NetScaler Gateway que haya configurado.

Aparecerán sus carpetas de ShareFile ubicadas en .sharefile.com. Si no ve las carpetas de ShareFile, compruebe que ha indicado correctamente las credenciales de inicio de sesión.

Parámetros del servidor Microsoft Azure Active Directory

Feb 27, 2017

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 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/

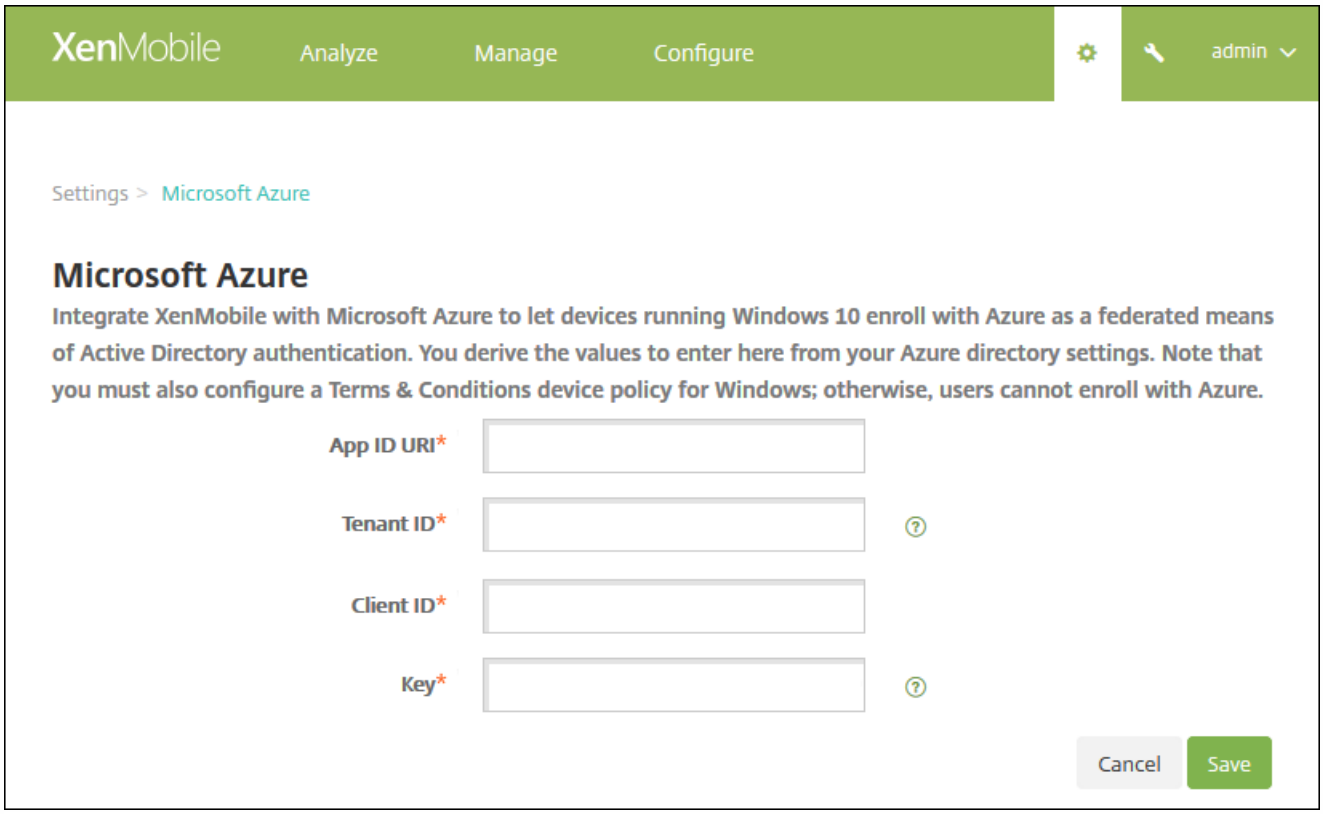
5. Seleccione la aplicación MDM local que ha creado en el paso 3 y habilite la opción **Administrar dispositivos para estos usuarios** para permitir la administración de dispositivos móviles de todos los usuarios o de un grupo de usuarios concreto.

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 **Platforms**, haga clic en **Microsoft Azure**. Aparecerá la página **Microsoft Azure**.



3. Configure estos 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 XenMobile 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 dispositivos, deben hacer lo siguiente:

1. Unirse a Azure AD de parte de un usuario de Azure en **Settings** > **About** > **Join Azure AD**.
2. Cerrar sesión en Windows y volver a iniciarla con una cuenta de Azure AD.

Actualización

Apr 13, 2017

Important

Antes de actualizar a XenMobile 10.5 (local)

1. Si la máquina virtual que ejecuta XenMobile Server que quiere actualizar tiene menos de 4 GB de RAM, debe aumentarla a por lo menos 4 GB. Tenga en cuenta que la memoria RAM mínima recomendada es de 8 GB para entornos de producción.
2. Anote las configuraciones de las directivas de restricciones y código de acceso para tabletas Windows. Esas directivas ya no se basan en WMI. Por eso, la actualización elimina las configuraciones existentes. Después de la actualización, deberá por tanto volver a configurar las directivas de restricciones y código de acceso para tabletas Windows.
3. Para acceder a la consola de administración de XenMobile, use solamente el nombre de dominio completo de XenMobile Server (el FQDN de inscripción) o las direcciones IP del nodo. Para acceder a la consola directamente a través de una dirección IP virtual de equilibrio de carga o a través de una dirección IP de NAT requiere XenMobile Server 10.5 revisión (rolling patch) 1. Dicha revisión se publicó el 22 de marzo de 2017. Para obtener más información, consulte https://support.citrix.com/article/CTX221304.
4. La fecha Subscription Advantage (SA) que consta 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.

Citrix publica las nuevas versiones o las actualizaciones importantes de XenMobile en Citrix.com. Al mismo tiempo, se envía un aviso al contacto registrado de cada cliente.

Dispone de estas opciones para actualizar XenMobile:

- **Para actualizar XenMobile de 9.0 a la versión más reciente.**
  Utilice la herramienta Upgrade Tool de XenMobile que está incorporada en la versión más reciente de XenMobile. Consulte los artículos de esta sección para obtener más información.
  La herramienta de actualización Upgrade Tool de XenMobile 9 admite todas las ediciones de XenMobile: MDM, App y Enterprise.
  Para ver los problemas conocidos y los resueltos, consulte Problemas resueltos y Problemas conocidos.
  Tenga en cuenta que la herramienta de actualización Upgrade Tool de versiones anteriores ya no está disponible en Citrix.com.

- **Para actualizar desde XenMobile 10.3.6 o 10.4 a XenMobile 10.5.**
  Puede hacerlo desde la página **Release Management** de la consola de XenMobile. Consulte las instrucciones descritas en este artículo para obtener más información.
  No use la herramienta Upgrade Tool para versiones de XenMobile que no sean XenMobile 9.0.

- **Para actualizar desde XenMobile 10 o 10.1 a XenMobile 10.5.**
  Primero, actualice de XenMobile 10 o 10.1 a XenMobile 10.3.6 desde la página **Release Management** de la consola de XenMobile. Luego, actualice desde XenMobile 10.3.6 a XenMobile 10.5 desde la página **Release Management** de la consola de XenMobile. Consulte las instrucciones descritas en este artículo para obtener más información. No se usa la herramienta Upgrade Tool para estas instalaciones.

XenMobile Server version	Release number	Upgrade to	Release number	Upgrade path	Update location
XenMobile Server 9 con App Controller Rolling Patch 9 instalado	9.0.0_97106	XenMobile Server 10.5	10.5.0.24	Actualizar XenMobile Server 9 a XenMobile Server 10.5	Descargue el requisito previo de rolling patch de App Controller. • La herramienta de actualización Upgrade Tool para XenMobile 10.5 está incorporada en XenMobile Server. • Para obtener más información, consulte Requisitos previos de la herramienta de actualización.
XenMobile Server 10 o XenMobile 10.1	10.1.0.63030	XenMobile Server 10.3.6	10.3.6	Actualizar XenMobile 10 o XenMobile 10.1 a XenMobile 10.3.6	Descargar
XenMobile Server 10.3.6	10.3.6	XenMobile Server 10.5	10.5.0.24	Actualizar de XenMobile 10.3.x a XenMobile 10.5	Descargar
XenMobile Server 10.4	10.4.x	XenMobile Server 10.5	10.5.0.24	Actualizar de XenMobile 10.4 a XenMobile 10.5	Descargar

Use la página **Release Management** para actualizar desde versiones admitidas de XenMobile 10 (indicadas en la tabla anterior) a la versión más reciente de XenMobile Server.

Requisitos previos:

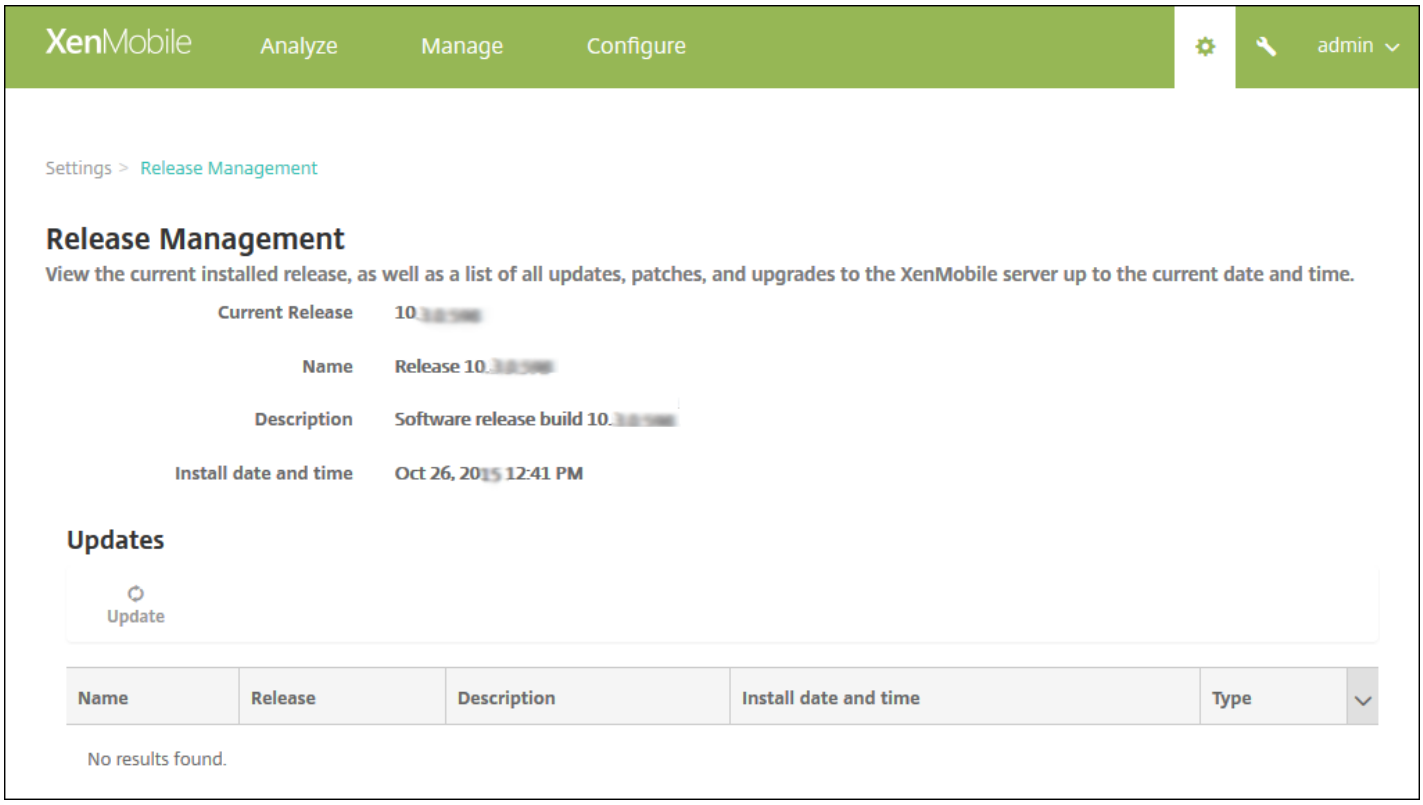
- Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema.
- Realice una copia de seguridad de la base de datos de configuración del sistema.
- Consulte los Requisitos del sistema de la versión a la que está actualizando. Para obtener la versión más reciente de XenMobile, consulte Requisitos del sistema.

Si tiene una implementación en clúster, consulte las instrucciones al final de este artículo.

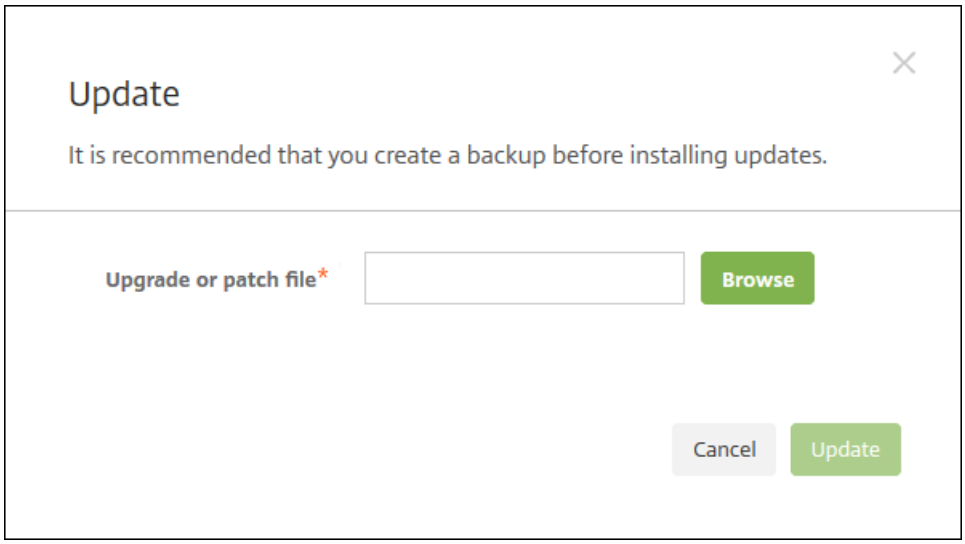
1. Inicie sesión con su cuenta en el sitio Web de Citrix y descargue el archivo de actualización (.bin) de XenMobile a una ubicación apropiada.

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**.



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



5. 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.

6. Haga clic en **Update** y, a continuación, si el sistema se lo solicita, reinicie XenMobile.

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.

Nota: Después de una actualización, XenMobile requiere un reinicio. Utilice la interfaz de línea de comandos de XenMobile para reiniciar el servidor XenMobile. Es importante que borre la caché del explorador Web después de reiniciarse el sistema.

Para actualizar implementaciones de XenMobile en clúster

Si el sistema está configurado en modo de clúster, siga estos pasos para actualizar cada nodo de XenMobile 10:

1. Cargue el archivo BIN en todos los nodos, desde **Settings > Release Management**.

2. Cierre todos los nodos desde el menú **System** en la interfaz de línea de comandos.

3. Desde el menú **System** en la interfaz de línea de comandos, seleccione un nodo y compruebe que el servicio se está ejecutando.

4. Inicie los demás nodos uno tras otro.

Si XenMobile no puede completar la actualización, aparece un mensaje de error que indica el problema. Entonces, XenMobile revierte el sistema al estado anterior al intento de actualización.

Requisitos previos de Upgrade Tool

Feb 27, 2017

Para actualizar desde XenMobile 9.0 a la versión más reciente de XenMobile, utilice la herramienta Upgrade Tool integrada en XenMobile.

La herramienta Upgrade Tool admite:

- Dispositivos iOS y Android inscritos en todos los modos de XenMobile Server (ENT, MAM, MDM)
- Windows Phone y tabletas inscritos en modo MDM
- Windows Phone inscritos en modo Enterprise
- Dispositivos Windows CE en modo MDM

Si la consola Multi-Tenant Console (MTC) está habilitada en XenMobile 9.0, puede migrarla a una implementación independiente de la versión más reciente de XenMobile. XenMobile 10 no respalda la consola MTC, de modo que debe administrar estas instancias individualmente. Después de completar los requisitos previos de este artículo, consulte Actualización del servidor de arrendatario de MTC a XenMobile.

La versión más reciente de XenMobile admite las versiones 11.1.x, 11.0.x y 10.5.x de NetScaler Gateway.

La herramienta Upgrade Tool integrada en XenMobile también admite la versión 10.1.x. de NetScaler Gateway. Citrix no admite NetScaler Gateway 10.1 con la versión más reciente de XenMobile. No obstante, puede actualizar una implementación de NetScaler Gateway 10.1 con la herramienta Upgrade Tool integrada en XenMobile. Después de eso, Citrix recomienda actualizar NetScaler Gateway a la última versión compatible.

> ## Important
>
> El proceso de actualización es complejo. Antes de comenzar una actualización, consulte la sección Problemas conocidos, planifique la actualización y complete todos los requisitos previos, según se describe en este artículo. Además, este blog contiene listas de verificación de requisitos previos que le ayudarán a planificar la actualización.
>
> Después de ejecutar la herramienta de actualización Upgrade Tool, deberá comprobar que cumple todos los requisitos posteriores.
>
> Si no cumple un requisito previo, la actualización puede fallar. Entonces, deberá configurar una nueva instancia de la versión más reciente de XenMobile en la consola de línea de comandos y volver a iniciar la herramienta Upgrade Tool.

Citrix recomienda realizar la actualización siguiendo estas fases.

1. Lleve a cabo una prueba en un entorno de prueba, complete todos los requisitos previos y los pasos de la herramienta Upgrade Tool. Citrix recomienda que lleve a cabo primero una prueba de la actualización para familiarizarse con el proceso y con los resultados que deben obtenerse después de realizar la actualización de producción completa. En la actualización de prueba, se comprueba la actualización de los datos de configuración, no los datos del usuario.

En NetScaler 11.1 (o versión mínima de NetScaler 10.5), Citrix recomienda utilizar el asistente "NetScaler para XenMobile" para configurar una nueva instancia de NetScaler con servidores virtuales de equilibrio de carga de NetScaler Gateway y

NetScaler.

2. Compruebe que los datos de configuración (como LDAP, directivas y aplicaciones) se han actualizado correctamente durante la actualización de prueba. Compruebe los dispositivos de prueba.

3. Lleve a cabo una actualización de producción en el entorno de producción y póngalo en funcionamiento. Incluya un tiempo de inactividad en sus planes durante la ejecución de la actualización.

Acerca de las actualizaciones de prueba y de producción

Con la herramienta de actualización Upgrade Tool de XenMobile, primero se debe probar la actualización y, solo después, realizar la actualización de producción completa.

Cuando opta por una actualización de prueba (Test Drive)
: La herramienta Upgrade Tool realiza una actualización de prueba con los datos de configuración del entorno de producción para comparar XenMobile 9.0 y la versión más reciente de XenMobile, sin que ello afecte a su entorno de producción. La actualización de prueba solo utiliza los datos de configuración, no los datos de dispositivo (en el caso de implementaciones de XenMobile Enterprise Edition) ni los datos de usuario.

Los resultados de una actualización de prueba solo deberían usarse con fines de prueba. No se puede actualizar una implementación de prueba. En vez de ello, debe volver a empezar por la actualización de producción. Una actualización de prueba funciona con cualquier edición de XenMobile 9.0.

Cuando opta por una actualización (Upgrade):
Primero, la herramienta Upgrade Tool copia todos los datos de configuración, dispositivo y usuario desde XenMobile 9.0 a una nueva instancia de la versión más reciente de XenMobile con el mismo nombre de dominio completo (FQDN). Todos los datos en XenMobile 9.0 permanecen intactos hasta que se mueve la nueva instancia del servidor XenMobile al entorno de producción.

Al iniciar sesión en la consola de la nueva instancia de XenMobile después de la actualización, verá todos los datos de usuario y de dispositivo que la actualización haya movido desde XenMobile 9.0.

Acciones que no realiza la herramienta Upgrade Tool

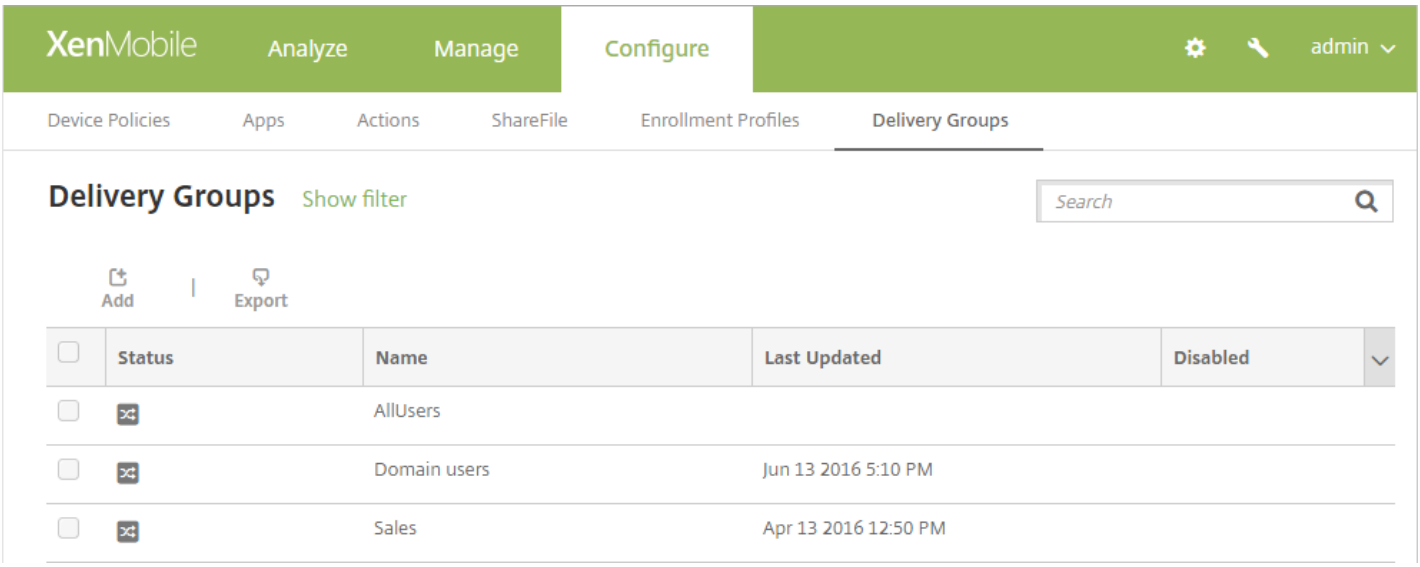
La siguiente información no se actualiza a la versión más reciente de XenMobile cuando se usa la herramienta Upgrade Tool:

- Información acerca de licencias.
- Datos de informes.
- Directivas de grupos de servidores e implementaciones asociadas (no respaldados en la versión más reciente de XenMobile).
- Grupo MSP (proveedor de servicios administrados).
- Directivas y paquetes relacionados con Windows 8.0.
- Paquetes de implementación que no se utilicen; por ejemplo, cuando no hay usuarios ni grupos asignados a un paquete de implementación.
- Cualquier otro dato de configuración o de usuario, según se describe en el archivo de registro de la actualización.
- CXM Web (reemplazado por Citrix Secure Web).
- Directivas DLP (reemplazadas por Citrix ShareFile).
- Atributos personalizados de Active Directory.
- Si ha configurado varias directivas de personalización de marca en XenMobile 9.0, la directiva de personalización de marca

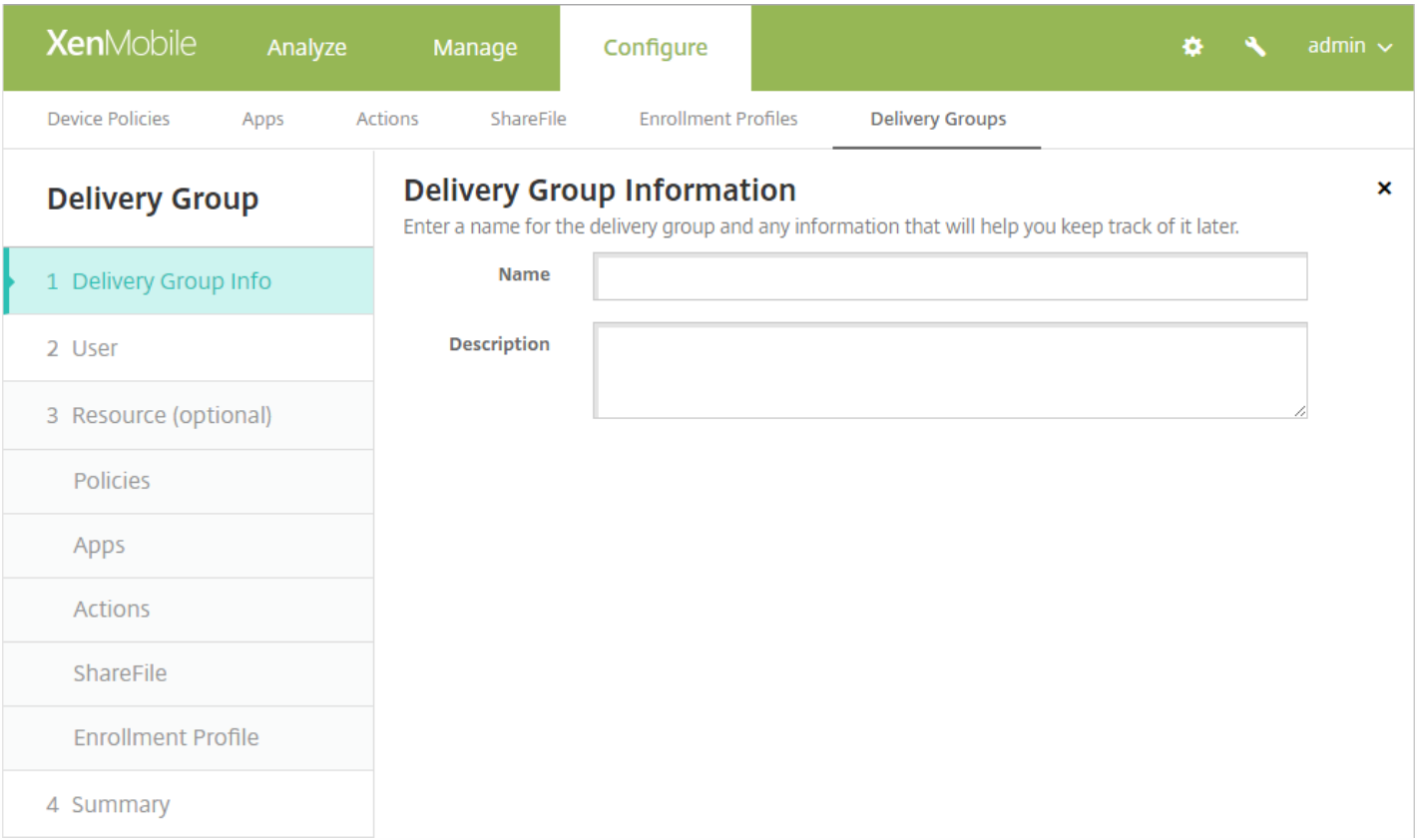
no se actualiza. Las versiones posteriores de XenMobile admiten una directiva de personalización de marca; debe dejar una directiva de personalización de marca en XenMobile 9.0 para actualizar a la versión más reciente de XenMobile.
- Parámetros contenidos en el archivo auth.jsp de XenMobile 9.0 que se usan para restringir el acceso a la consola. En la versión más reciente de XenMobile, las restricciones de acceso a la consola son parámetros del firewall que se pueden configurar desde la interfaz de línea de comandos.
- Configuraciones de servidor de registros del sistema.
- Conectores Form-fill configurados en XenMobile 9.0 (no reciben respaldo en versiones posteriores de XenMobile).

Cambios en XenMobile

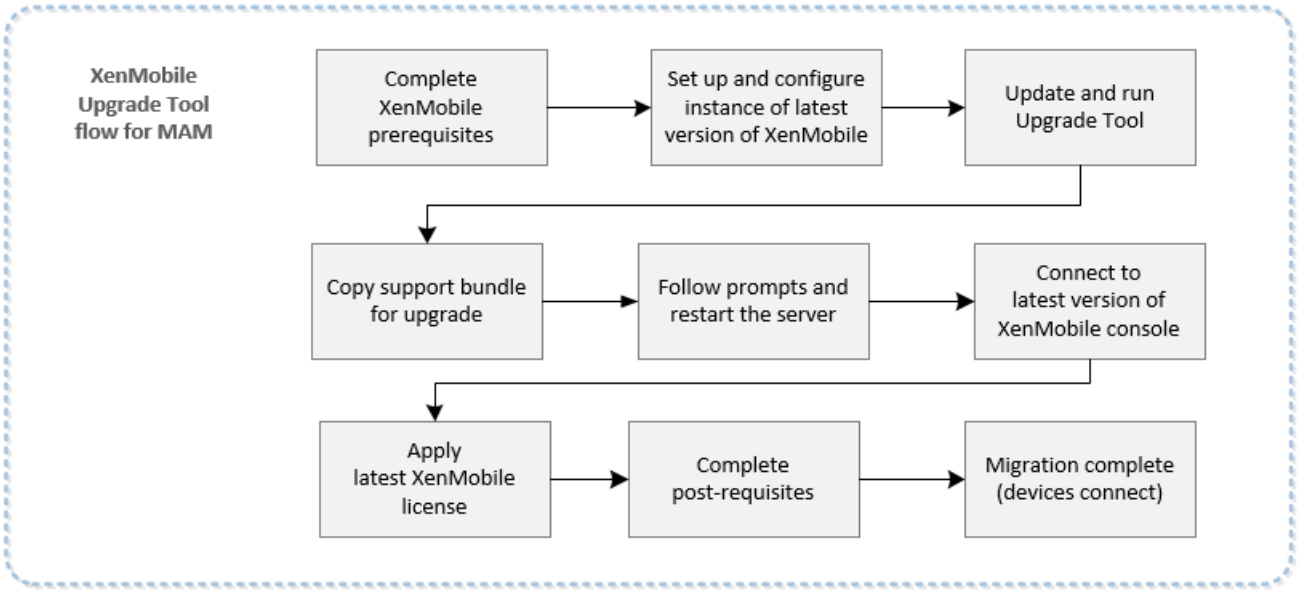
- La herramienta Upgrade Tool no actualiza a los usuarios de Active Directory que están asignados a grupos locales. Los usuarios de Active Directory se pueden asignar posteriormente a grupos locales.
- XenMobile 10 no respalda grupos locales anidados. Una actualización desde XenMobile 9 nivela la jerarquía de grupos locales.
- Los paquetes de implementación de Device Manager se conocen como grupos de entrega en XenMobile, como se muestra en la siguiente imagen. Para obtener más información, consulte Implementación de recursos.

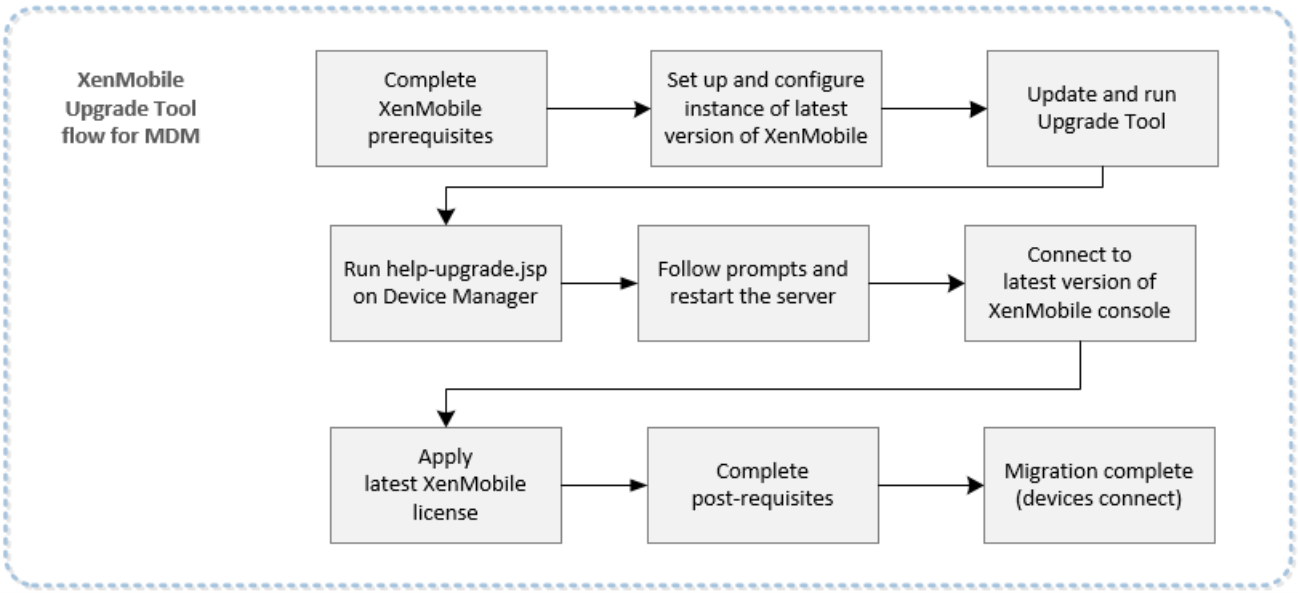


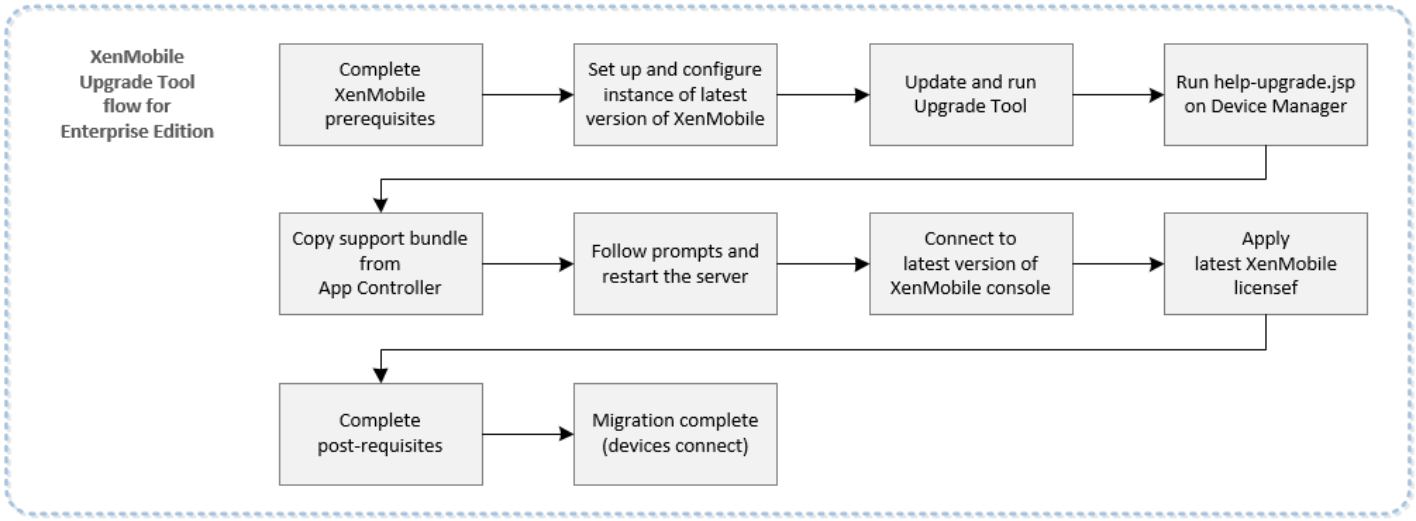
Dentro del grupo de entrega, puede ver las directivas, las acciones y las aplicaciones necesarias para el grupo de usuarios que requieren los recursos.



Los diagramas siguientes ilustran los pasos básicos necesarios para la actualización desde XenMobile 9.0.







Citrix recomienda seguir estos pasos para actualizar a la versión más reciente de XenMobile un entorno de XenMobile 9.0 Enterprise que tiene dispositivos Windows Phone inscritos en modo Enterprise y usa Worx Home 9.x.

1. Actualice Worx Home en Device Manager a la versión 10.2 o posterior y luego implemente Worx Home 10.2.

2. Desinstale manualmente Worx Home 9.x de los dispositivos de los usuarios.

3. Indique a los usuarios que vayan al sitio de descargas en su teléfono para instalar Worx Home 10.2 o posterior, que usted implementó desde Device Manager.

4. Después de completar los requisitos previos que se describen en este artículo, actualice a la versión más reciente de XenMobile como se describe en Cómo habilitar y ejecutar XenMobile Upgrade Tool.

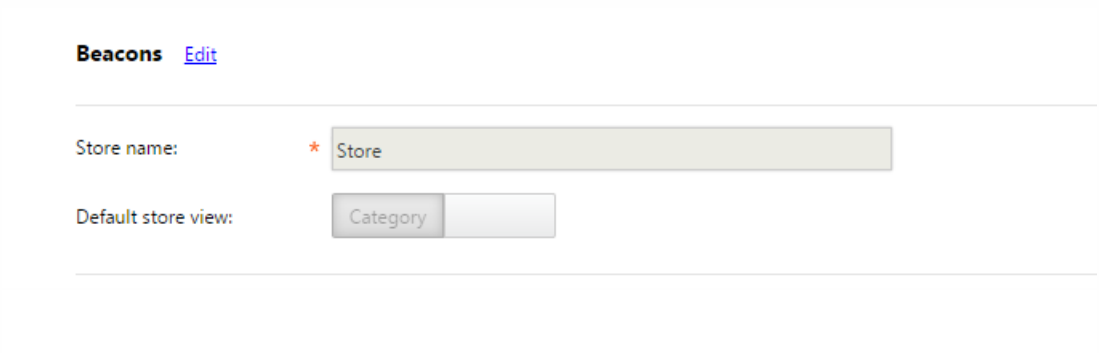
5. Haga cambios en NetScaler para que se vuelvan a conectar los dispositivos, como se describe en Requisitos posteriores de la herramienta Upgrade Tool.

Descargue App Controller Rolling Patch 9 de XenMobile 9.0 desde https://support.citrix.com/article/CTX218552.

En la consola de administración de App Controller, vaya a **Settings > Release Management**. Haga clic en **Update** y, a continuación, seleccione el archivo de revisión que ha descargado. Haga clic en **Upload** y, a continuación, reinicie App Controller.

Antes de actualizar XenMobile 9 a la versión más reciente, debe cambiar el nombre personalizado de su tienda al valor predeterminado, de forma que los dispositivos Windows inscritos puedan seguir funcionando después de la actualización. Para obtener más información, consulte http://support.citrix.com/article/CTX214553.

En una actualización en modo MAM o Enterprise, si el nombre de la tienda se ha cambiado a otro distinto del predeterminado "Store" en App Controller, restaure el nombre predeterminado **Store** antes de generar un paquete de asistencia para la actualización.



Para ver las versiones requeridas de los componentes relacionados (como el servidor de licencias de Citrix), consulte Requisitos del sistema y sus apartados.

- **NetScaler**. Antes de actualizar NetScaler, guarde una copia de seguridad del archivo de configuración (ns.conf) de NetScaler. Las versiones actuales de NetScaler incluyen: una herramienta de implementación rápida y fácil de usar, y el asistente "NetScaler para XenMobile", que le guiará por los pasos necesarios para integrar NetScaler y XenMobile. Para obtener más información, consulte Configuración de parámetros para el entorno de XenMobile y FAQ: XenMobile 10 and NetScaler 10.5 Integration.
- **Firewall Ports**. Abra puertos del firewall para la nueva IP del servidor XenMobile de forma similar a los puertos abiertos para la IP del servidor XenMobile 9.0. Para conocer los requisitos de puertos de XenMobile, consulte Requisitos de puertos.
- **LDAP Server**. Compruebe que el nuevo servidor XenMobile se conecta a uno o varios servidores LDAP. Debe tener una ruta activa hacia los servidores LDAP después de la actualización, cuando reinicie el servidor.

En la siguiente tabla se enumeran las opciones de migración de bases de datos. Para ver los requisitos del sistema, consulte Requisitos de base de datos de XenMobile.

De XenMobile 9.0	A la versión más reciente de XenMobile

Enterprise Edition

App Controller	MDM	
PostgreSQL locales	PostgreSQL locales	PostgreSQL locales
PostgreSQL locales	MS SQL	MS SQL
PostgreSQL locales	PostgreSQL remotas	PostgreSQL remotas

App Edition

PostgreSQL locales	PostgreSQL locales
PostgreSQL locales	PostgreSQL remotas
PostgreSQL locales	MS SQL

MDM Edition

PostgreSQL locales	PostgreSQL locales
MS SQL	MS SQL
PostgreSQL remotas	PostgreSQL remotas

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

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

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

1. Abra el archivo pg_hba.conf y busque la línea siguiente:

    host all all 127.0.0.1/32 md5

2. Para permitir todas las direcciones IP, cambie la línea a:

host all all 0.0.0.0/0 md5

También puede agregar otra entrada de host para permitir las conexiones a la dirección IP del servidor XenMobile:

host all all 10.x.x.x/32 md5

3. Guarde el archivo.

4. Detenga e inicie el servicio.

5. Abra el archivo postgresql.conf y, a continuación, busque la línea siguiente:

#listen_addresses = 'localhost'

6. Cambie la línea a:

listen_addresses = '*'

7. Detenga e inicie el servicio de PostgreSQL para que se apliquen los cambios.

Si la solución de base de datos tiene asignado un puerto personalizado, compruebe que ese puerto está permitido y abierto en el firewall que protege XenMobile 9.0 Device Manager. De esta manera, la nueva instancia de XenMobile puede conectarse a la base de datos y migrar la información pertinente.

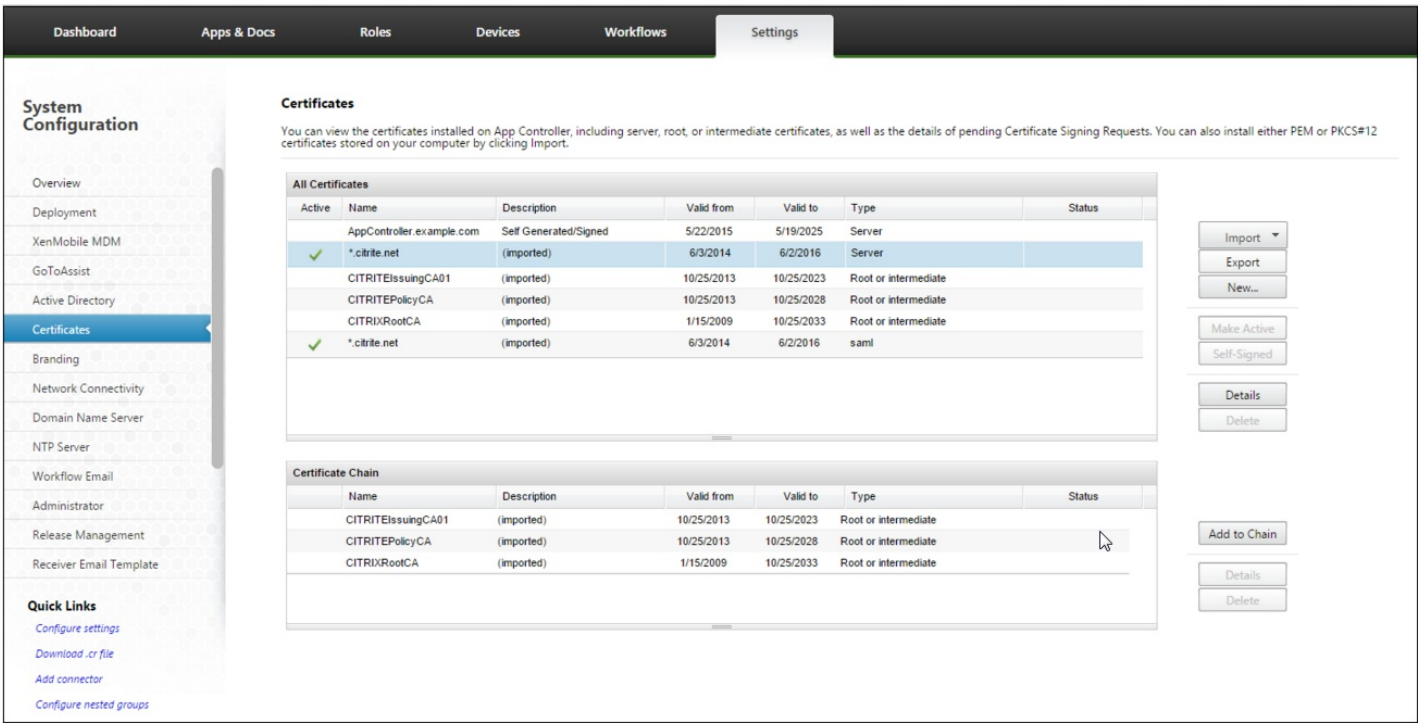
En XenMobile 9.0, se actualizan los nombres de los paquetes de implementación que contengan caracteres especiales (!, $, (), #, % , +, *, ~, ?, |, {} y []), pero no se pueden modificar los grupos de entrega en la nueva instancia de XenMobile después de la actualización. Además, los usuarios locales y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

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

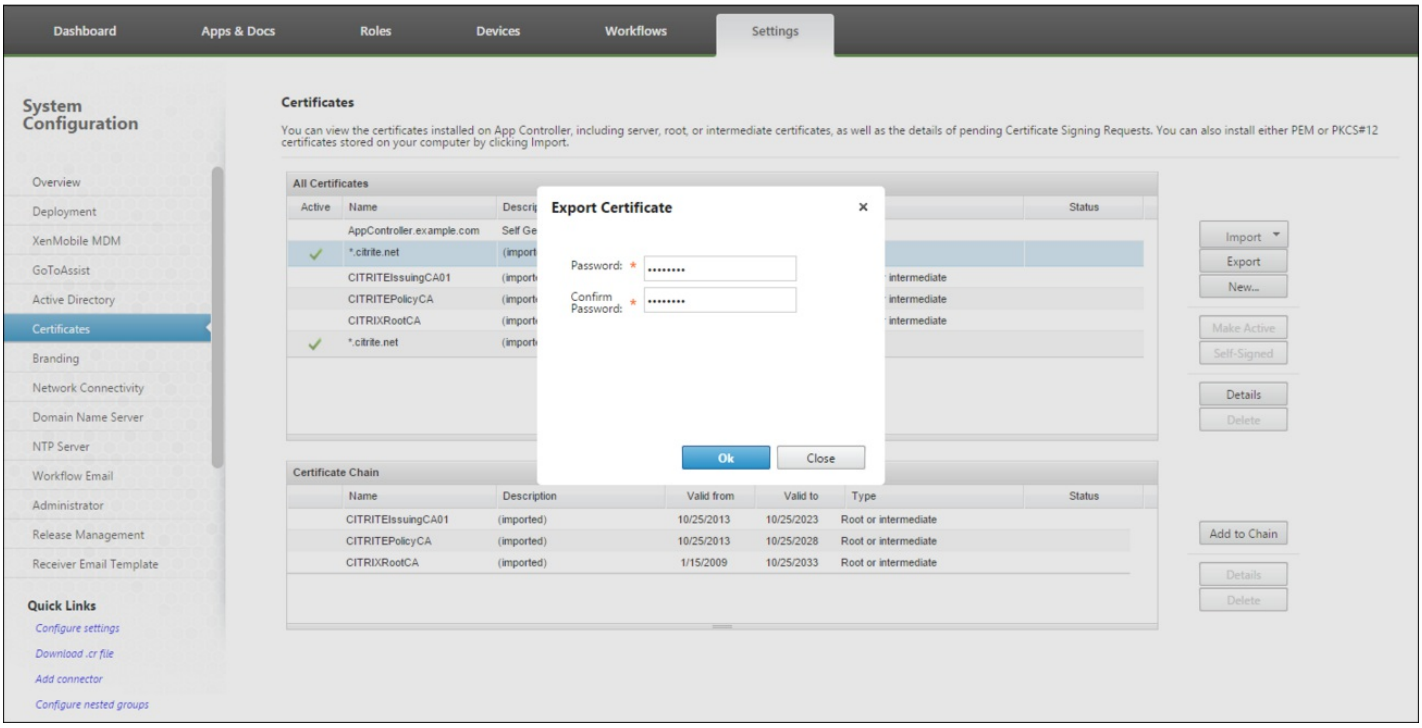
Si actualiza una implementación de XenMobile 9.0 Enterprise Edition, debe exportar el certificado del servidor de App Controller. Posteriormente, cuando complete los requisitos posteriores a la actualización, deberá importar el certificado de servidor en NetScaler Gateway. Siga estos pasos para exportar el certificado de servidor:

1. Inicie sesión en XenMobile 9.0 App Controller y haga clic en **Certificates**.

2. En la lista de certificados, haga clic en el certificado de servidor que quiere exportar y, a continuación, haga clic en **Export**.



3. En el cuadro de diálogo **Export Certificate**, escriba su contraseña de certificado en ambos campos y luego haga clic en **OK**.



Prepare un servidor donde pueda cargar el paquete de asistencia cifrado desde la interfaz de línea de comandos de XenMobile mediante el protocolo de transferencia de archivos (FTP) o el protocolo de copia segura (SCP).

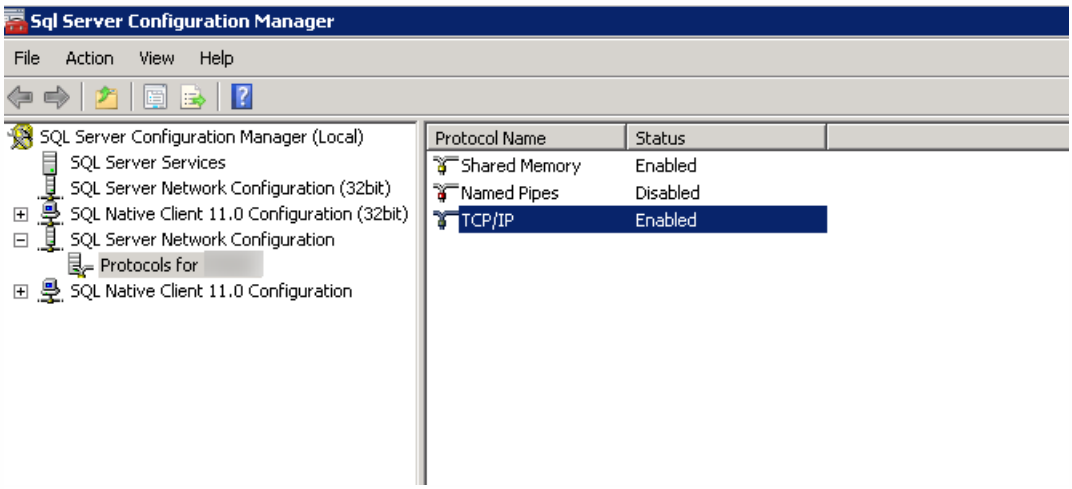
Cómo habilitar y ejecutar XenMobile Upgrade Tool

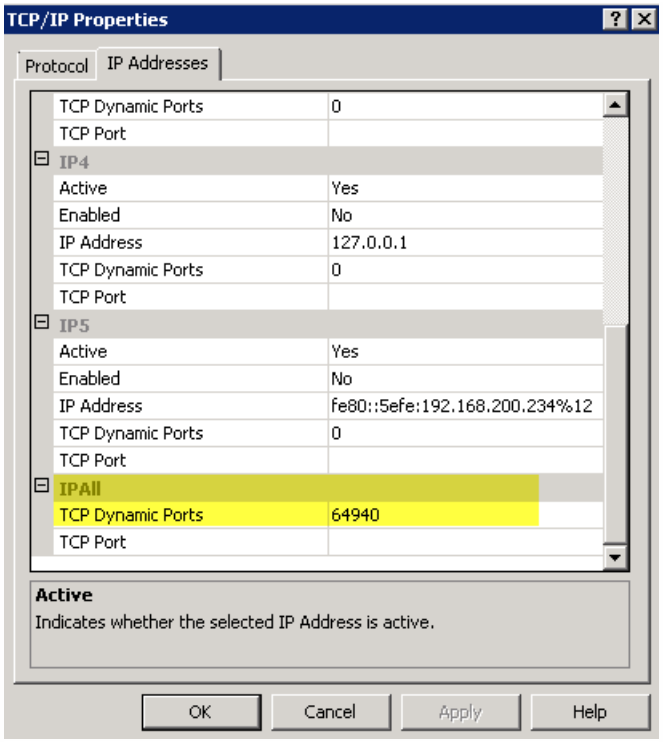
Feb 27, 2017

Si el entorno de XenMobile 9 cumple los requisitos siguientes, siga los pasos indicados en esta sección antes de actualizar.

- La edición XenMobile 9 MDM o Enterprise tiene una base de datos SQL Server externa.
- Una base de datos SQL Server se ejecuta 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.

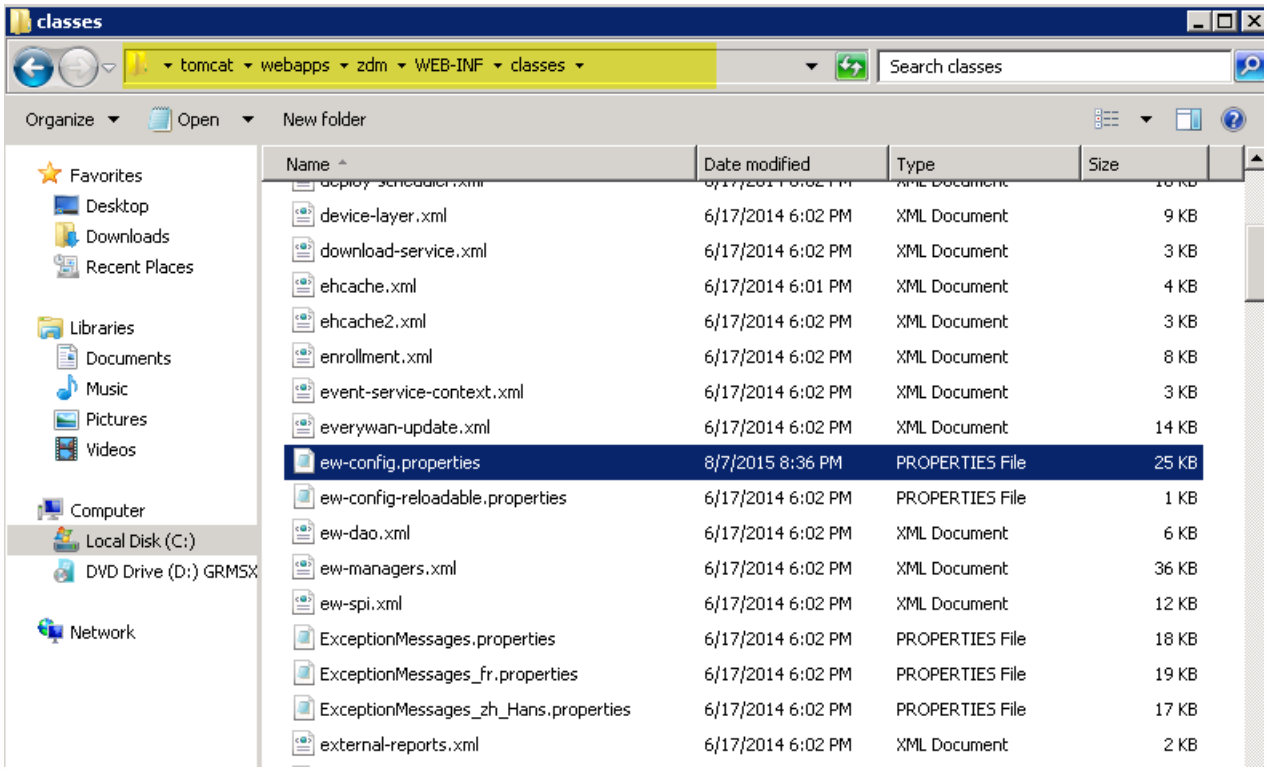
> ## Nota
>
> Citrix recomienda que la instancia de la base de datos de SQL Server se ejecute siempre en un puerto estático, porque el servidor XenMobile necesita acceso continuo a la base de datos. Esta conexión, por lo general, atraviesa un firewall. Como resultado de ello, necesita abrir el puerto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





Pasos previos a la actualización

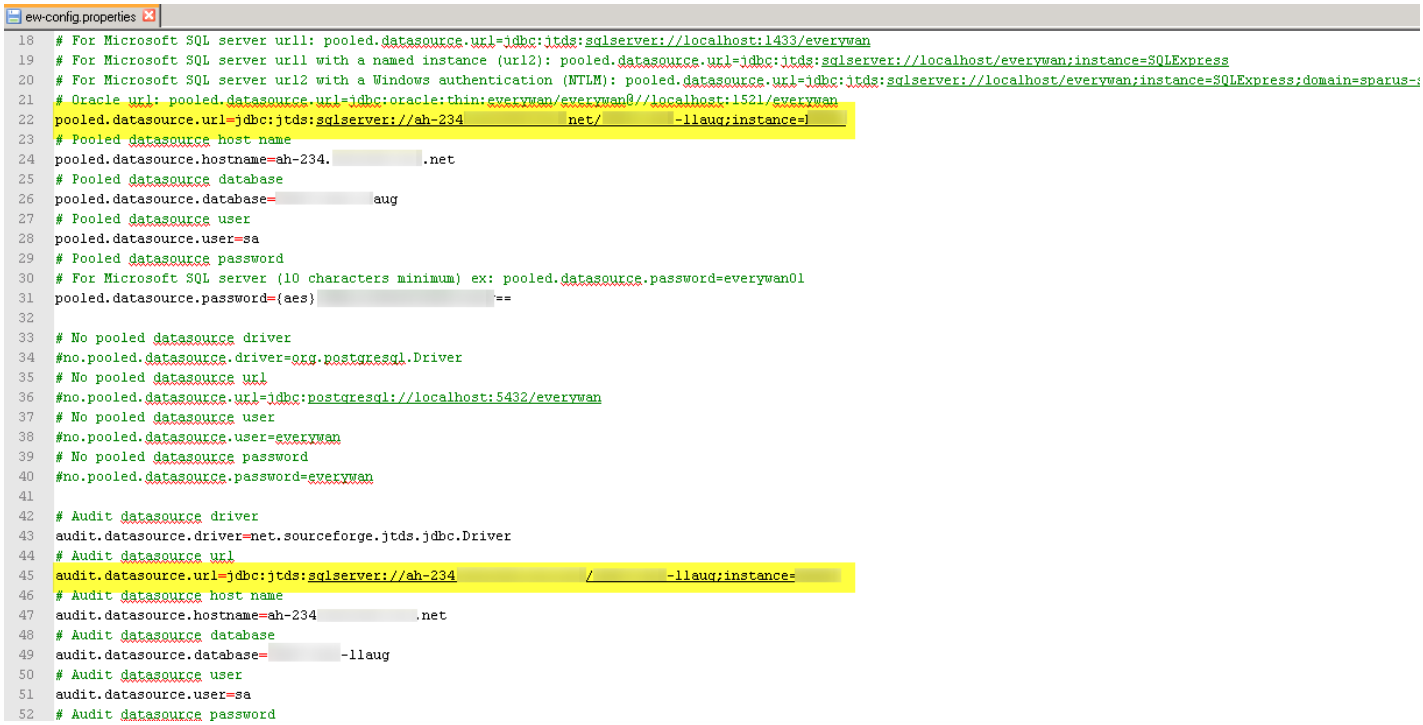
1. Vaya al directorio de instalación de Device Manager y abra el archivo ew-config.properties. Este se encuentra en tomcat\webapps\zdm\WEB-INF\classes.



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=

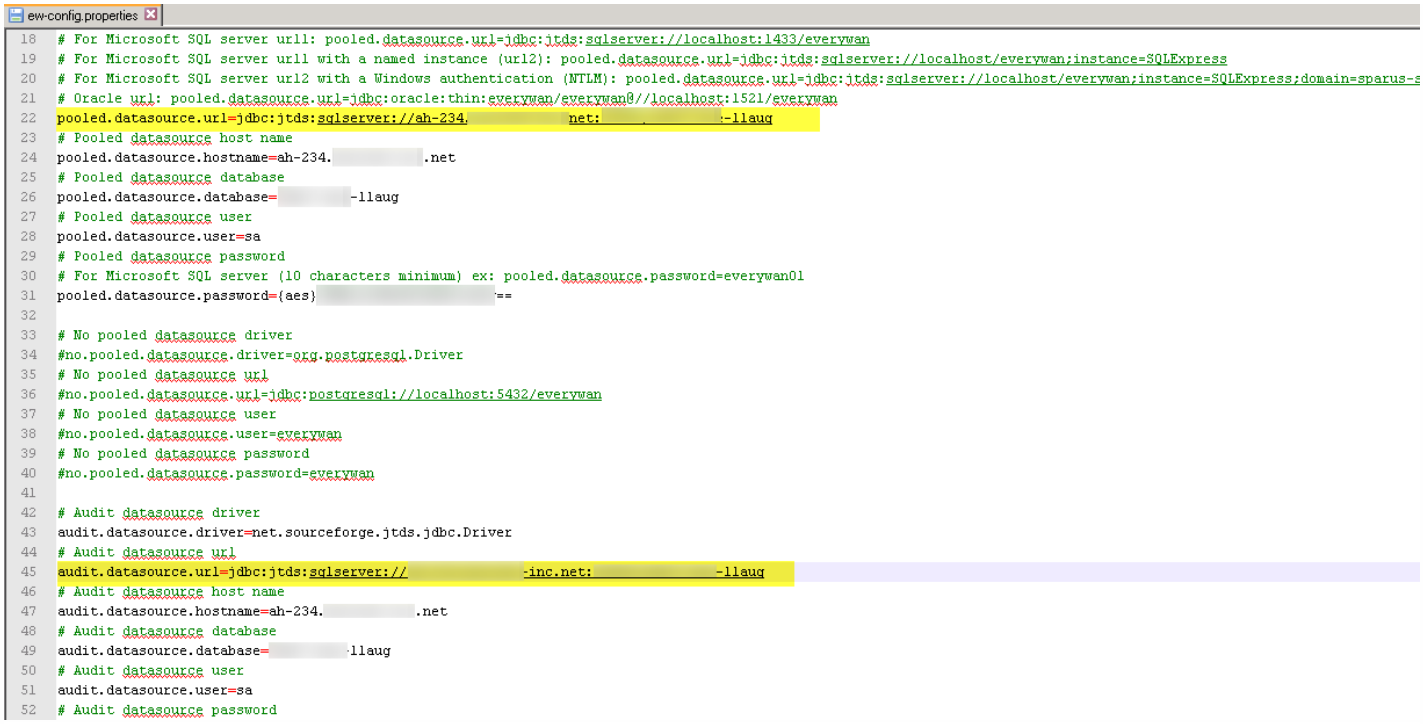


3. Quite el nombre de la instancia en las direcciones URL anteriores, y añada el puerto y el nombre de dominio completo (FQDN) del servidor SQL Server. En este caso, el puerto necesario es el 64940:

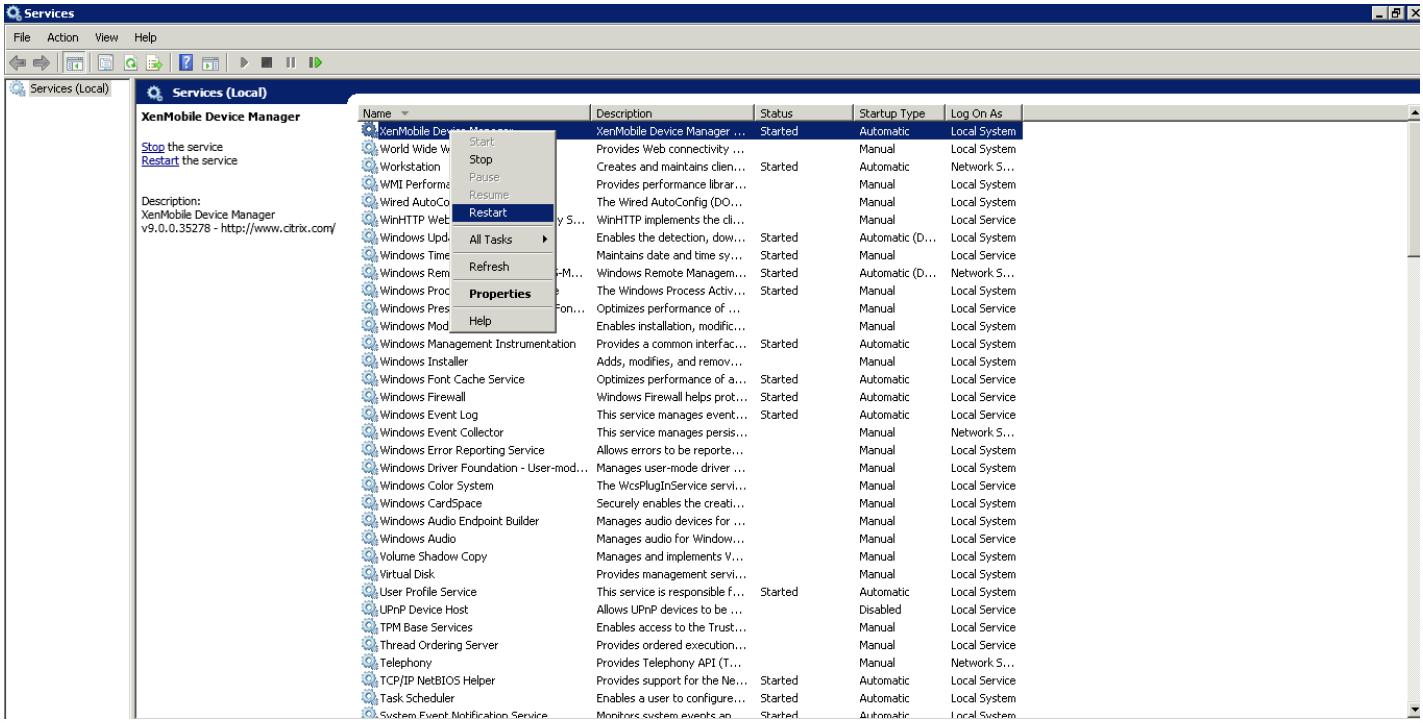
pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

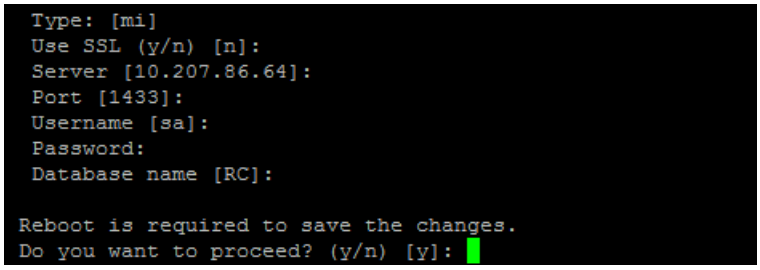
> ## Nota
>
> Citrix recomienda hacer una copia de seguridad, copiar o tomar nota de los cambios realizados en el archivo ew-config.properties. Esta información puede servir de ayuda en caso de que falle la actualización.



4. Reinicie el servicio de Device Manager. Actualice la vista de las conexiones de dispositivos tras el reinicio de la instancia de Device Manager.



5. Determine si el nuevo servidor XenMobile 10.x 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 el puerto es dinámico, Citrix recomienda que convierta que lo convierta en estático. Posteriormente, cuando llegue a la parte siguiente de la instalación de la base de datos durante la actualización, configure el puerto estático en el nuevo servidor XenMobile.



Puede proceder con la actualización.

Si el sistema está configurado en modo de clúster:

1. Apague todos los nodos salvo el que quiera actualizar primero. Para apagar un nodo, use **Settings** en la interfaz de línea de comandos.

2. Actualice el nodo que aún se está ejecutando como se describe en la sección siguiente, "Para habilitar y ejecutar la herramienta de actualización Upgrade Tool".

3. Tras comprobar que la actualización haya ocurrido según lo previsto, vuelva a unir cada uno de los nodos restantes, de uno en uno. Para volver a unir:

    a. Reinicie el nodo.

    b. No actualice el nodo si el sistema se lo solicita.

    c. Una el nodo a la base de datos del clúster.

    XenMobile actualizará automáticamente un nodo después de volver a unirlo al clúster.

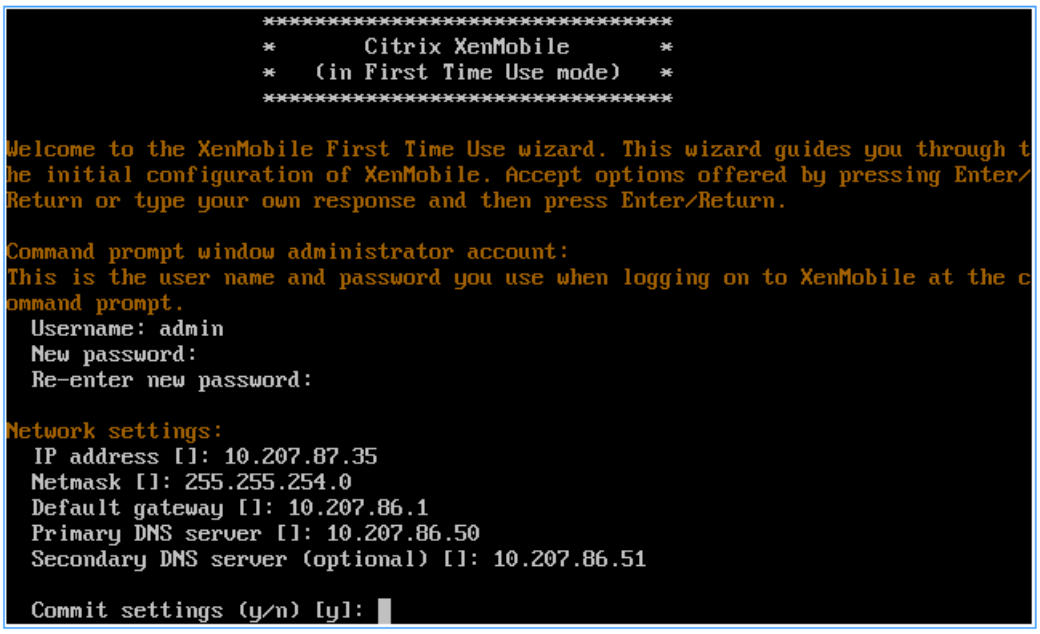
4. Realice todas las tareas de requisitos posteriores en cada nodo después de volverlo a unir al clúster.

Habilite y ejecute la herramienta Upgrade Tool desde la interfaz de línea de comandos (CLI) la primera vez que instale la versión más reciente de XenMobile.

> ### Important
>
> Si quiere tomar una instantánea del sistema, hágalo después de la configuración inicial de la versión más reciente de XenMobile y antes de utilizar a la herramienta de actualización.

1. En la interfaz de línea de comandos, introduzca el nombre de usuario y la contraseña de administrador y especifique los parámetros de red.

2. Introduzca **y** para confirmar los parámetros.

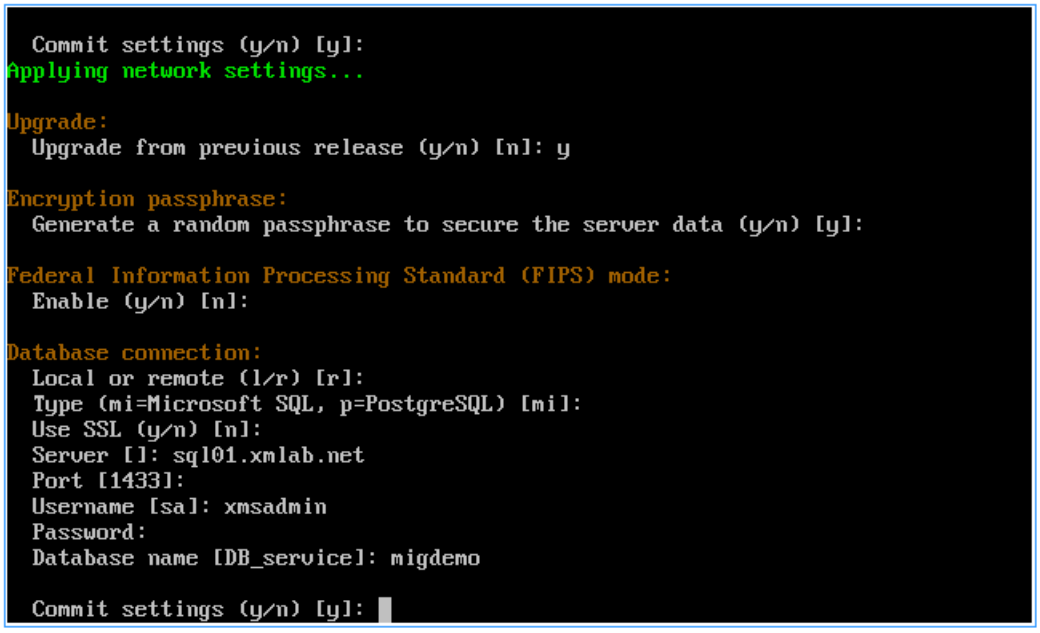


3. Introduzca **y** para actualizar.

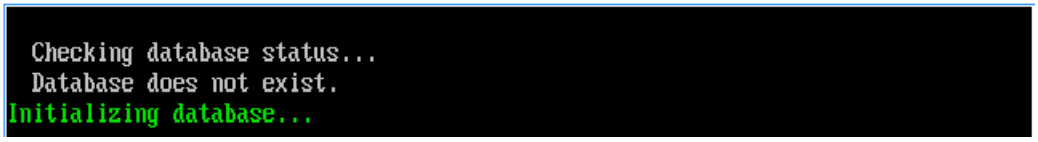
> ## Nota
>
> Si no selecciona "y" aquí, deberá configurar una nueva instancia de la versión más reciente de XenMobile en la consola de línea de comandos e iniciar la herramienta de actualización de nuevo.

4. Seleccione si quiere generar una frase secreta aleatoria y si quiere habilitar FIPS. Introduzca la información de conexión de base de datos.

5. Introduzca **y** para confirmar los parámetros.



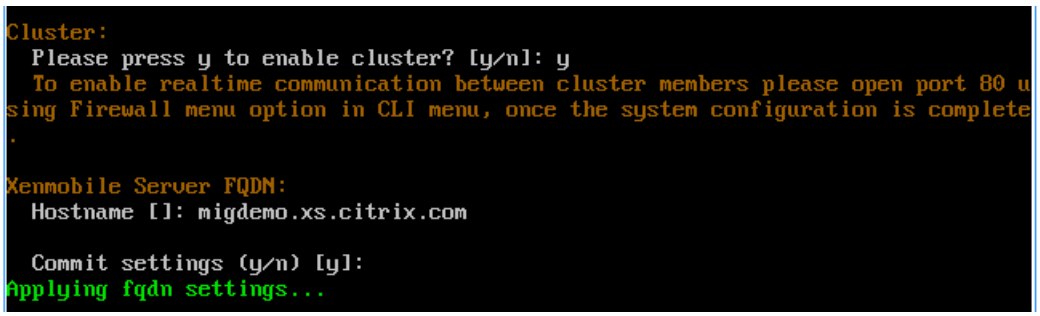
XenMobile inicializa la base de datos.



6. Seleccione si quiere habilitar servidores en clúster. Introduzca el nombre de dominio completo (FQDN) de XenMobile. Tenga en cuenta lo siguiente:

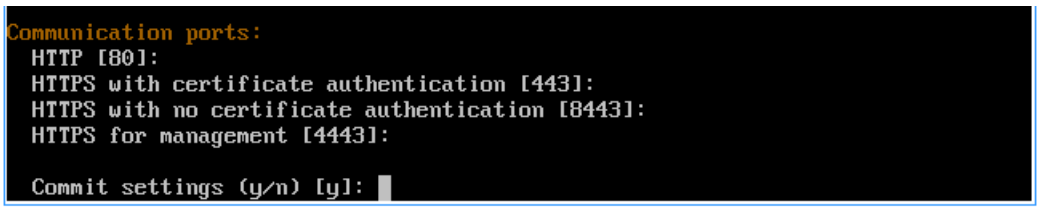
- Para implementaciones de XenMobile Enterprise Edition, el nombre FQDN el mismo que el nombre FQDN de XenMobile 9.0 MDM.
- Para implementaciones de MAM, el nombre FQDN el mismo que el nombre FQDN de XenMobile 9.0 App Controller.
- Para implementaciones de MDM, el nombre FQDN el mismo que el nombre FQDN de XenMobile 9.0 Device Manager.

> **Important**
>
> El nombre de dominio completo (FQDN) de ambos entornos, 9.0 y el nuevo, deben coincidir.



7. Introduzca **y** para confirmar los parámetros.

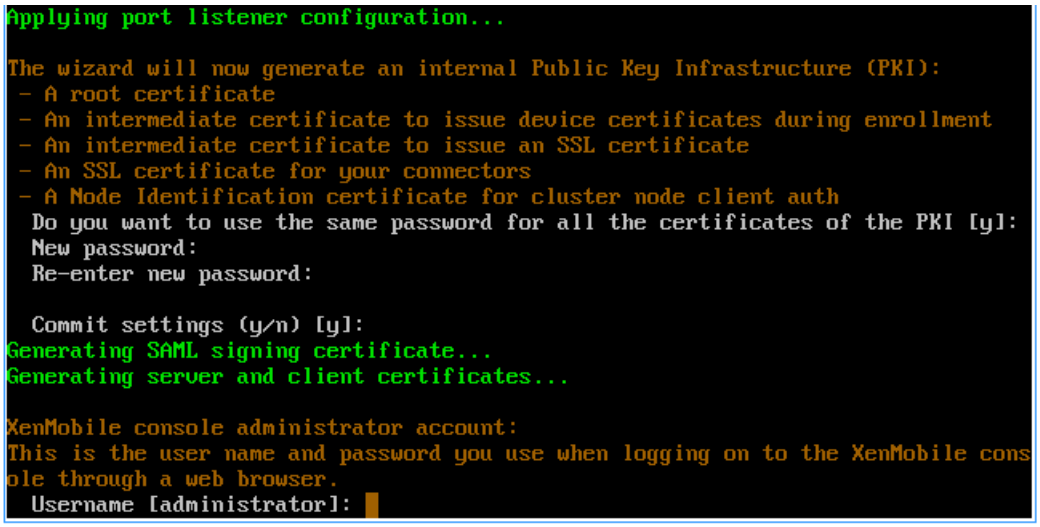
8. Establezca los puertos de comunicación.



9 Introduzca **y** para confirmar los parámetros.

10. Seleccione si utilizar la misma contraseña para todos los certificados y escriba la contraseña que se utilizará para los certificados.

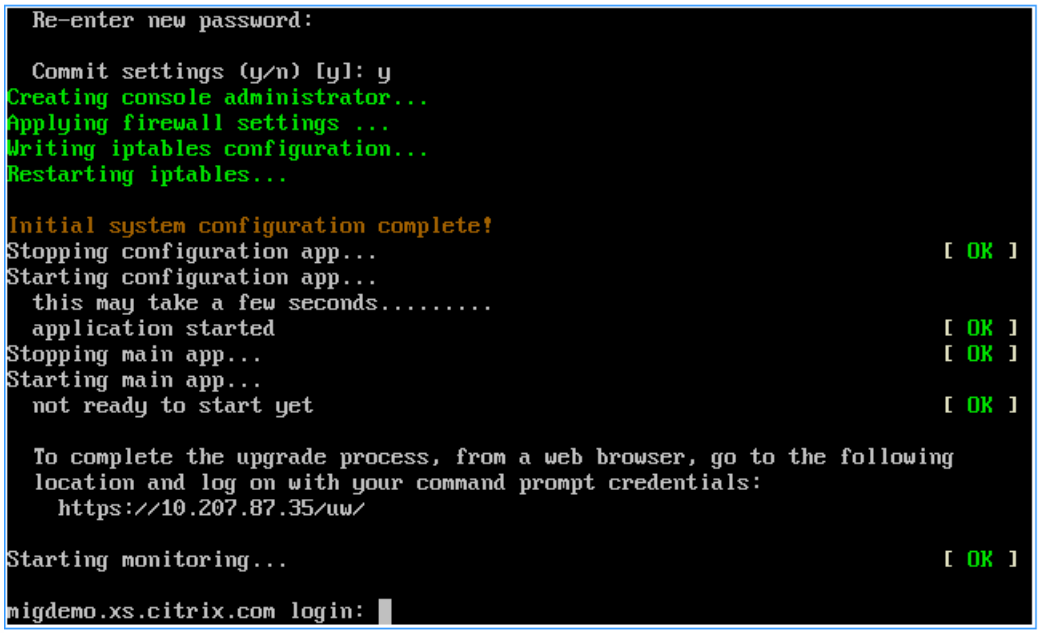
11. Introduzca **y** para confirmar los parámetros.



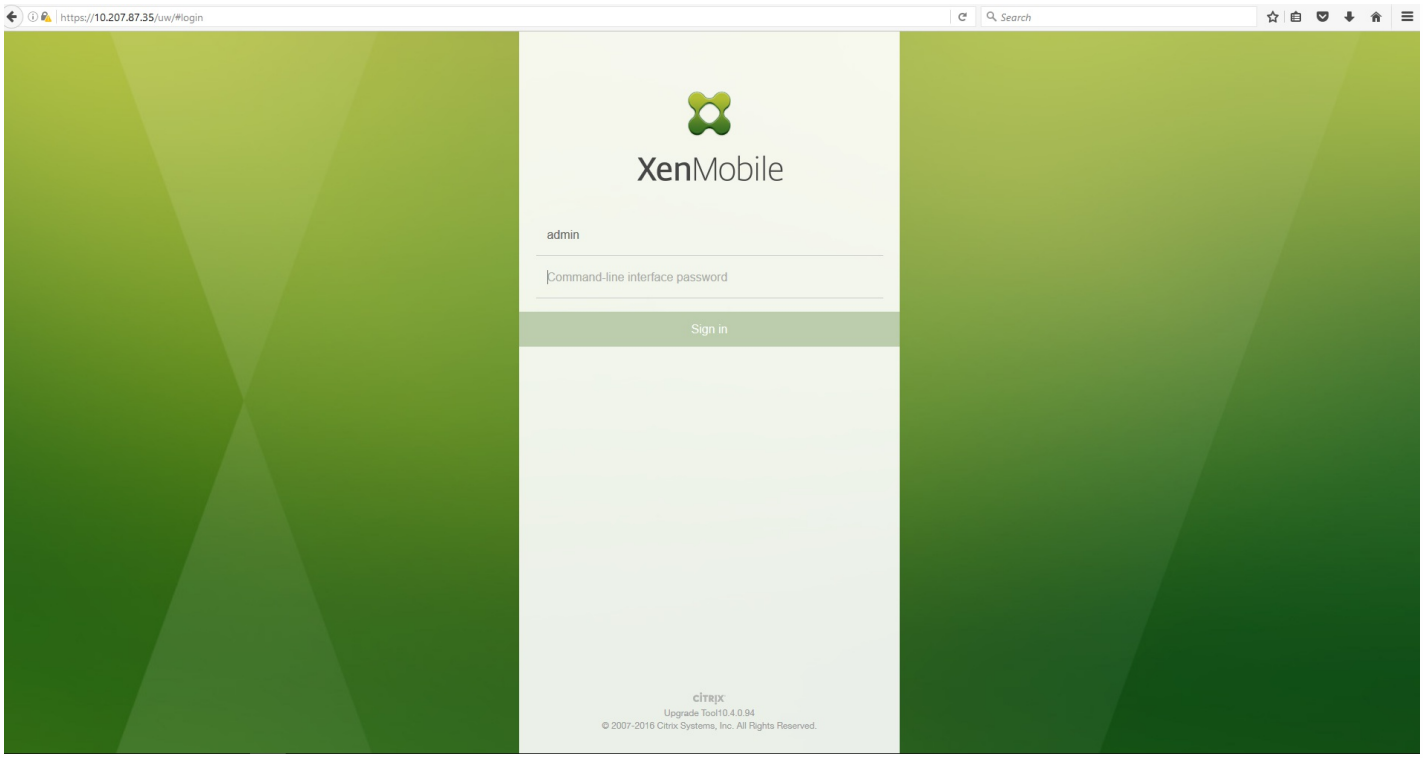
12. Introduzca el nombre de usuario y la contraseña del administrador de la consola de XenMobile.

13. Introduzca **y** para confirmar los parámetros.

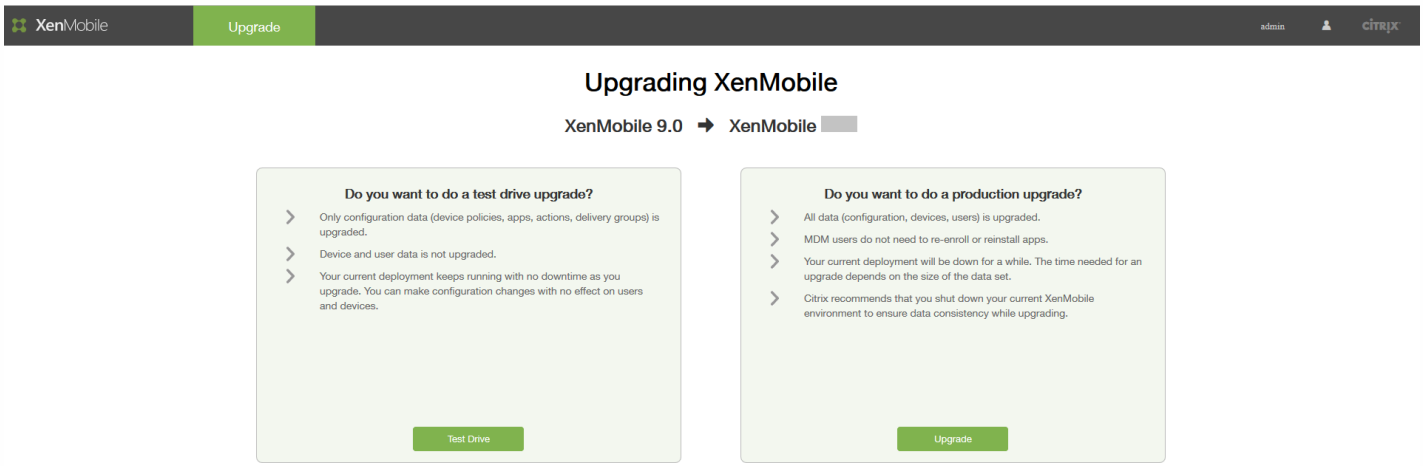
XenMobile habilita la herramienta de actualización Upgrade Tool de un solo uso.



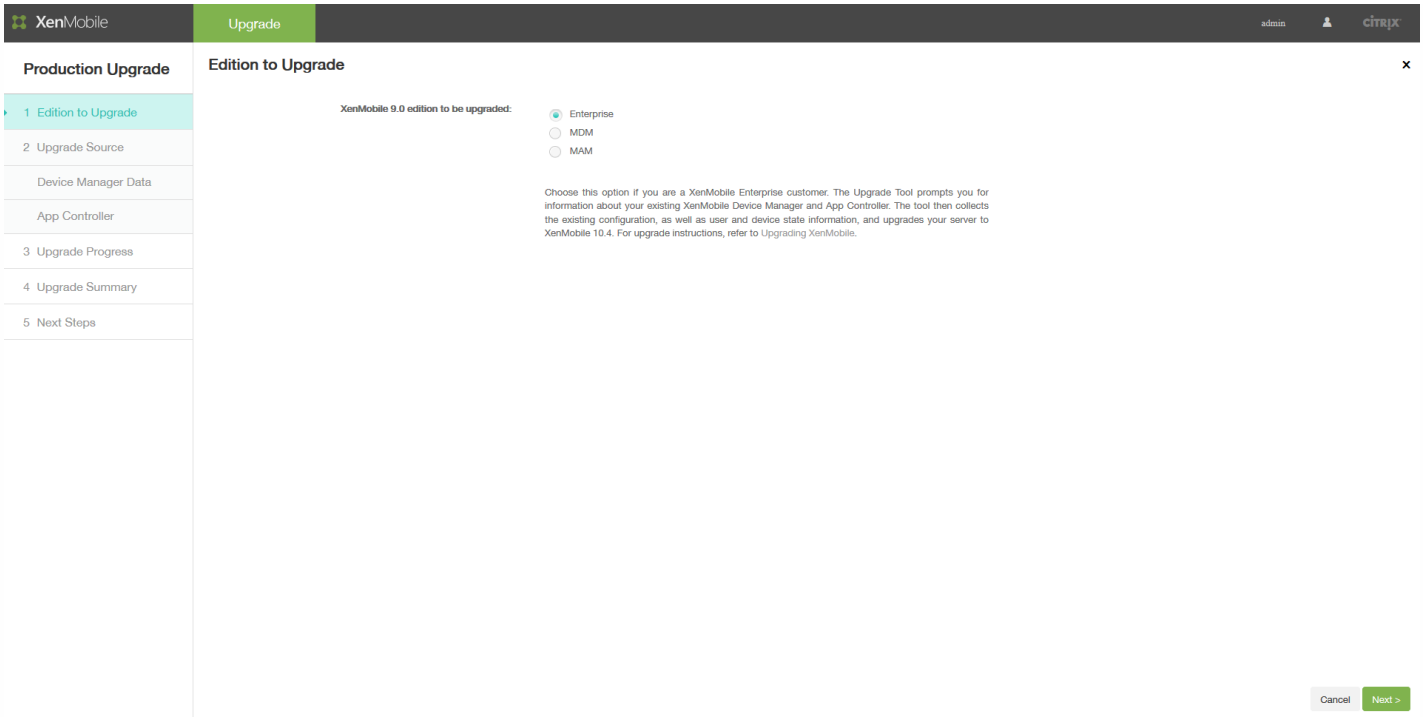
14. Acceda a la herramienta de actualización Upgrade Tool desde un explorador Web con https:///uw/ e inicie sesión con las credenciales que ha especificado en la interfaz de línea de comandos.



15. Ahora, puede elegir entre una actualización de prueba y una actualización de producción. Estas instrucciones son para una actualización de producción. En la página **Upgrading XenMobile**, haga clic en **Upgrade**.



16. En la página **Edition to Upgrade**, seleccione la edición. En el ejemplo siguiente, aparece seleccionada la edición Enterprise.



17. Haga clic en **Next**.

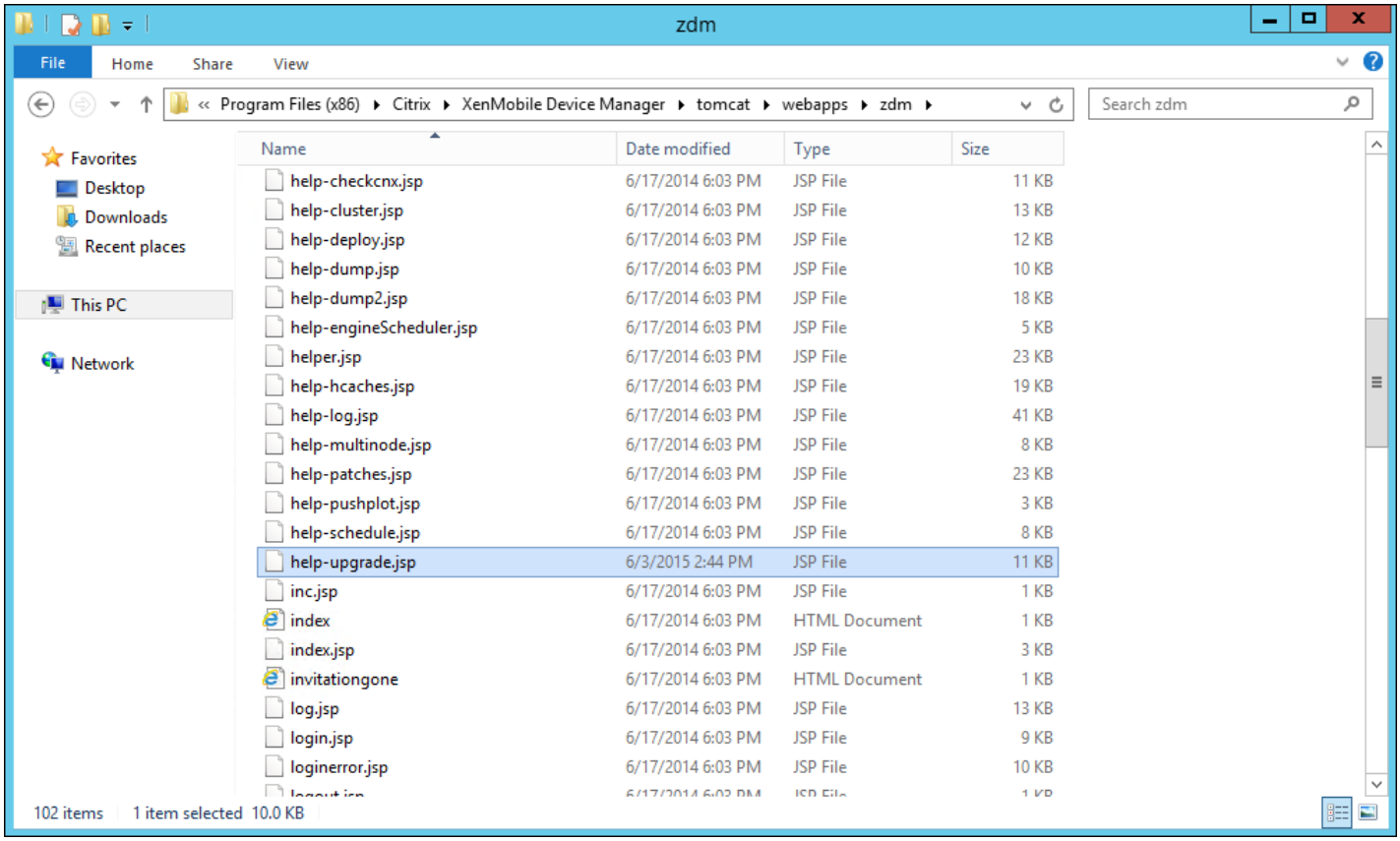
Si actualiza una edición Enterprise o MDM, aparecerá la página **Device Manager**. Siga los pasos del 18 al 22 para completar esta página.

Si actualiza una edición MAM, vaya al paso 23 para completar la página **App Controller**.

18. Recopile los archivos necesarios para migrar los datos existentes de XenMobile 9.0 Device Manager. También obtendrá acceso a la URL y nombre de usuario de la base de datos que copiará en la página **Device Manager**.

    a. Haga clic en el enlace indicado en el paso 1 de la página **Device Manager** y guarde el archivo descargado help-upgrade.zip.

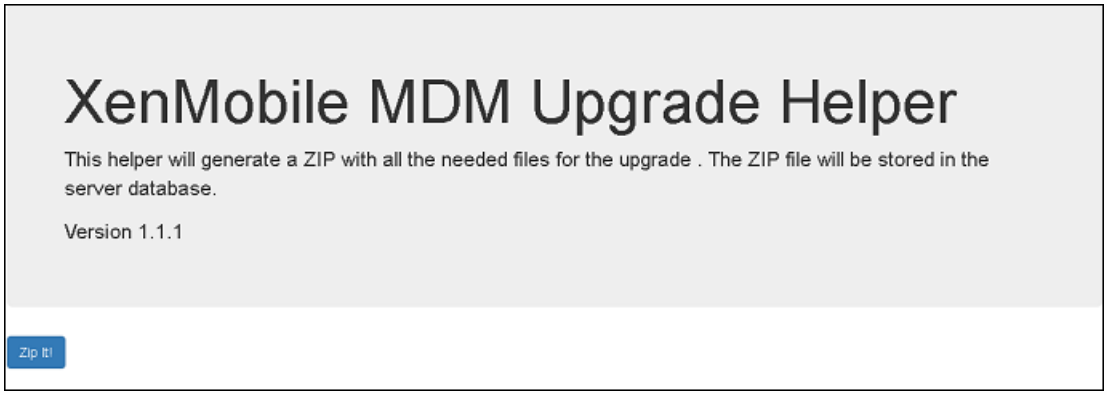
    b. Extraiga el archivo help-upgrade.jsp en \tomcat\webapps\zdm en el XenMobile 9.0 Device Manager existente.



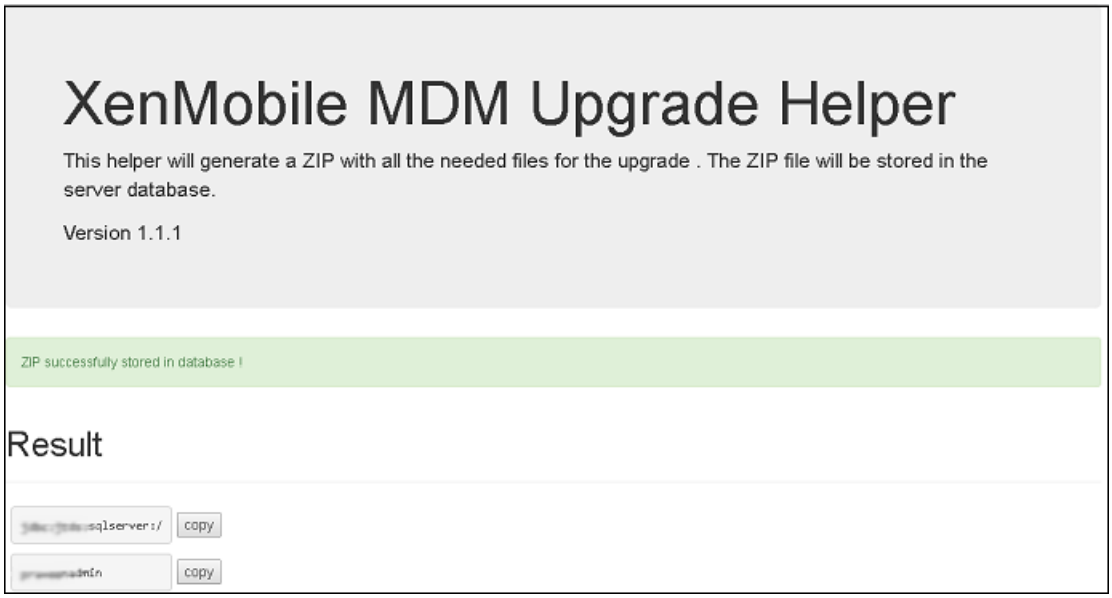
c. En una ventana del explorador, inicie sesión en el servidor XenMobile 9.0.

d. En un explorador Web, escriba la dirección URL: https://localhost/zdm/help-upgrade.jsp. Se abre la página **XenMobile MDM Upgrade Helper**, que recopila y comprime todos los archivos de XenMobile 9.0 necesarios para la actualización a la versión más reciente de XenMobile. A continuación, el archivo zip comprimido se guarda en la base de datos del servidor desde donde se extrae.

e. Haga clic en **Zip it** y luego siga las instrucciones en pantalla para reunir los archivos necesarios para la actualización.



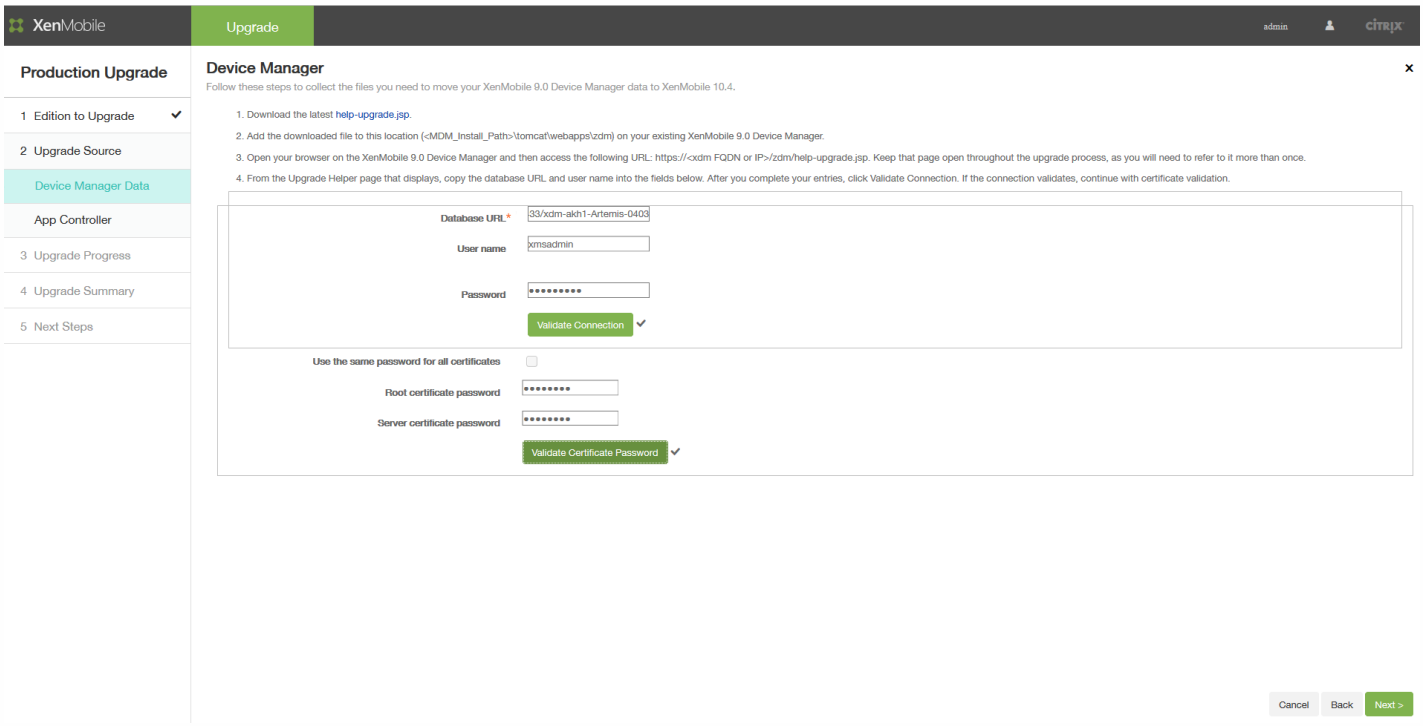
19. En **Result**, copie la URL y péguela en el campo **Database URL** en la página **Device Manager** de la herramienta Upgrade Tool. A continuación, copie el nombre de usuario y péguelo en la página **Device Manager**.



20. En la herramienta Upgrade Tool:

a. Escriba la contraseña y, a continuación, haga clic en **Validate Connection**.

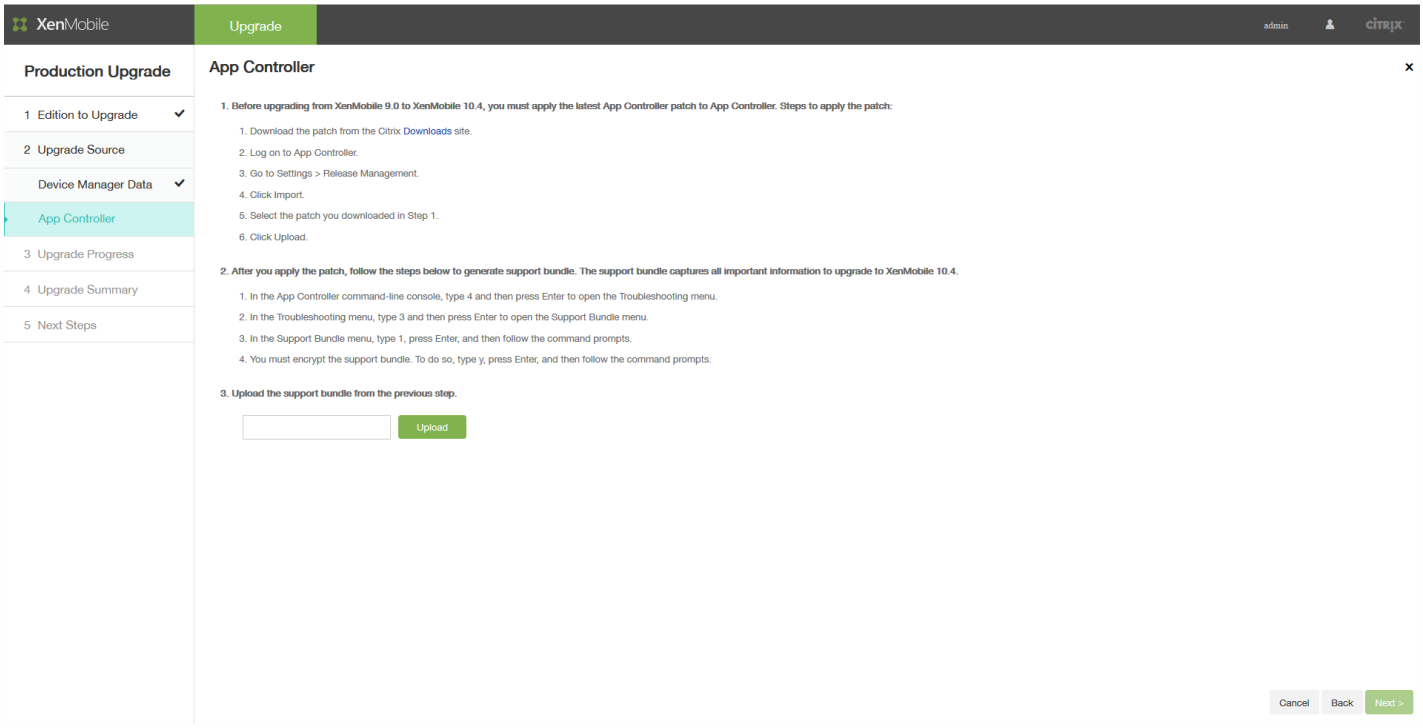
b. Escriba la contraseña de cada certificado y, a continuación, haga clic en **Validate Password**.



21. Haga clic en **Next**.

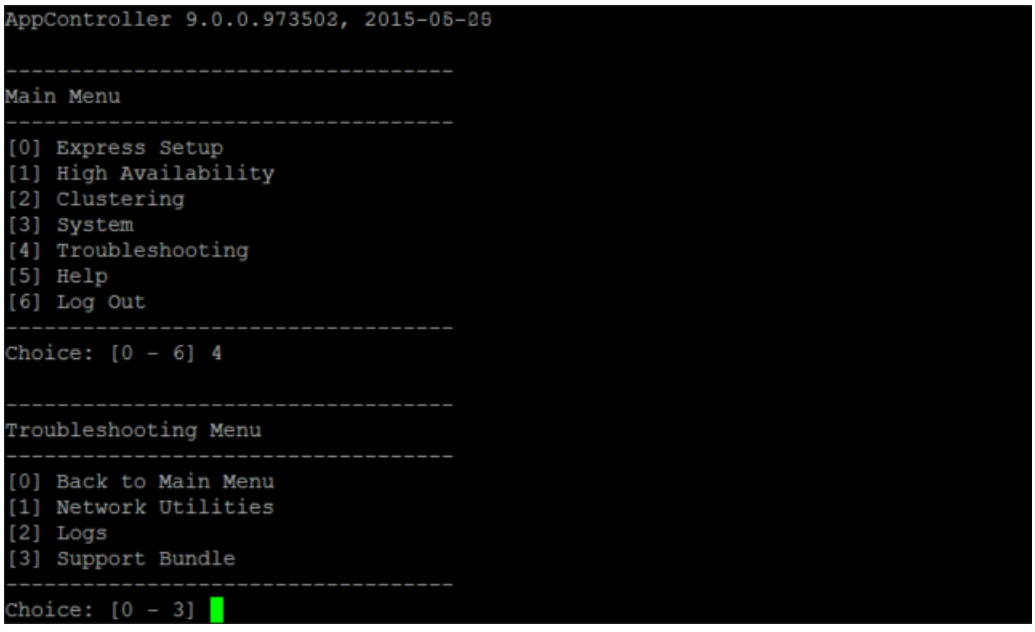
22. Si cambió el archivo ew-config.properties, reinicie el servicio XDM en XenMobile 9 MDM y, a continuación, vaya a https://localhost/zdm/help-upgrade.jsp para volver a ejecutar el archivo comprimido. Con ello, el archivo ew-config.properties vuelva a leerse y se guarda en la base de datos de XenMobile MDM 9 para prepararse a la migración.

23. A continuación, aplicará una revisión de actualización a App Controller. Luego, generará y cargará un paquete de asistencia. Empiece por seguir las instrucciones de la sección 1 de la página **App Controller** para actualizar App Controller.

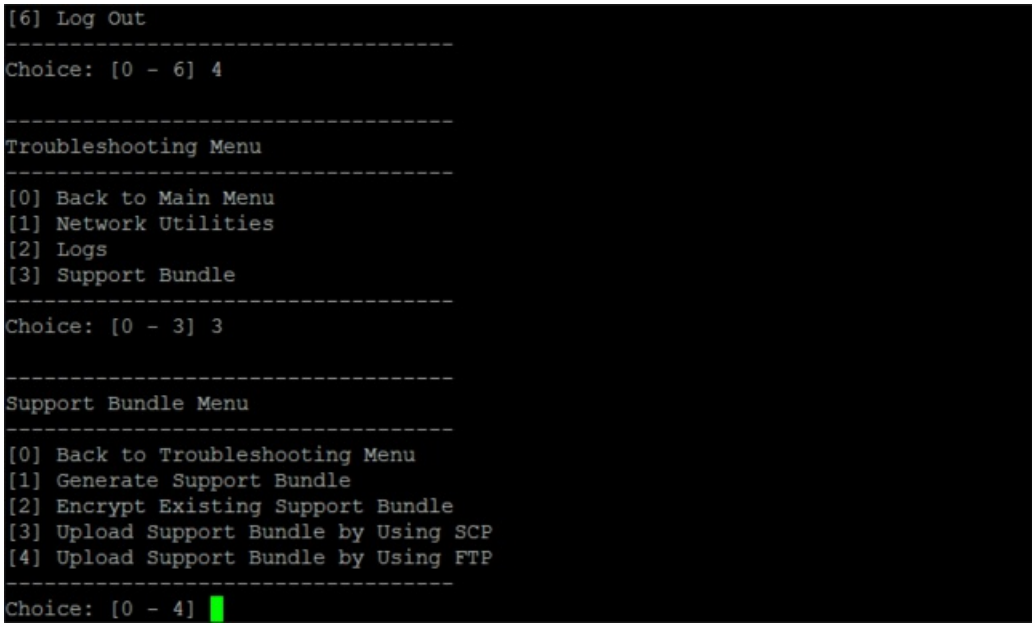


25. Continúe con las instrucciones de la sección 2 de la página **App Controller**:

a. En la consola de línea de comandos de App Controller, escriba **4** y, a continuación, presione ENTRAR para abrir el menú Troubleshooting.

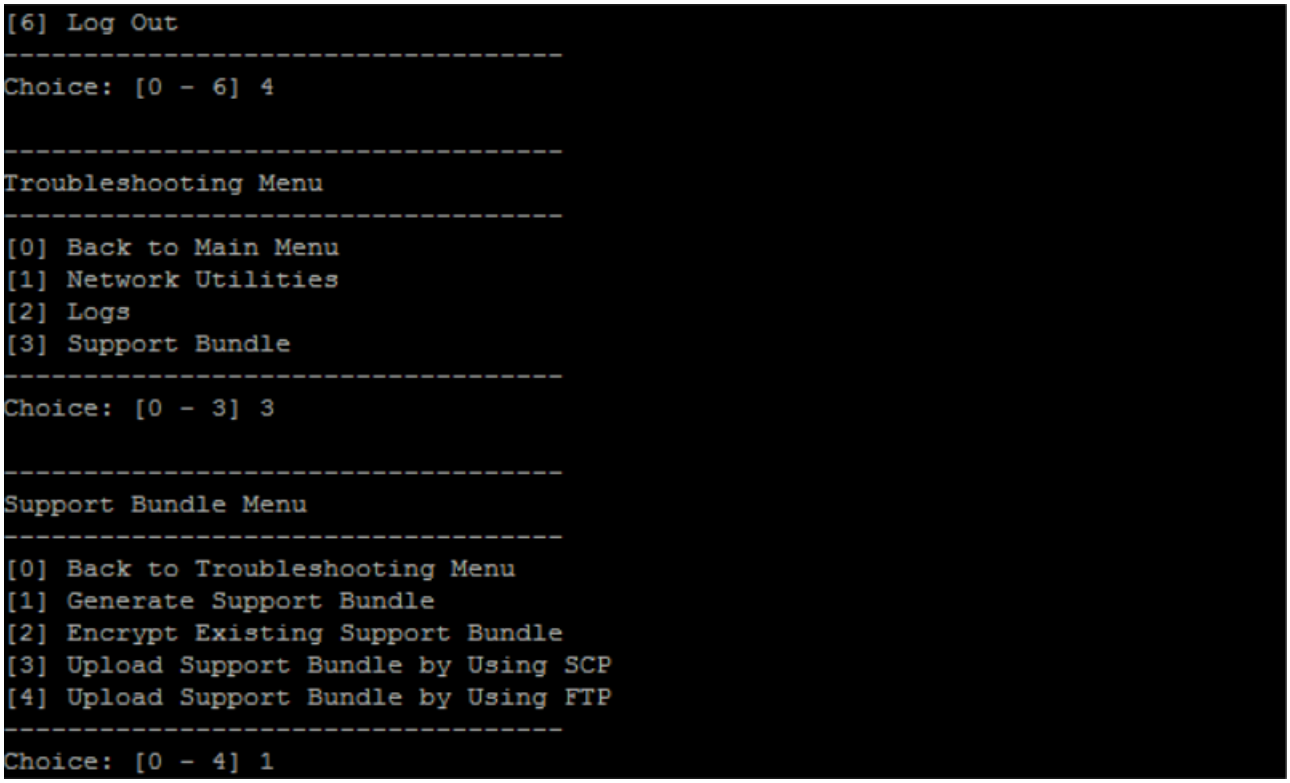


b. En el menú Troubleshooting, escriba **3** y, a continuación, presione ENTRAR para abrir el menú Support Bundle.



c. En el menú Support Bundle, escriba **1** y, a continuación, presione ENTRAR y siga las instrucciones.

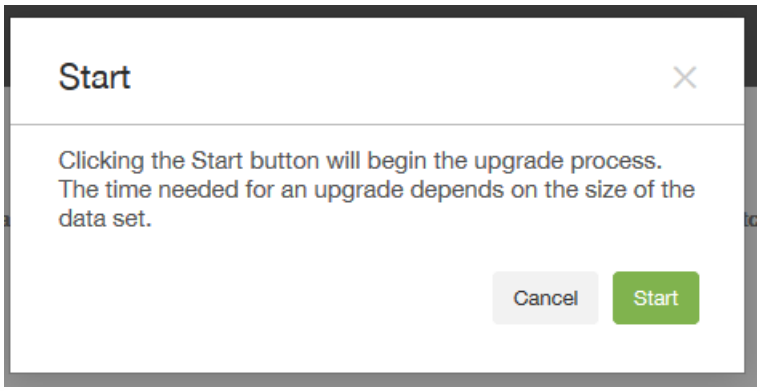
Nota: Debe cifrar el paquete de asistencia.



26. En la sección 3 de la página **App Controller**, especifique el paquete de asistencia y luego haga clic en **Upload**.

La herramienta Upgrade Tool procesará los archivos recopilados (para las ediciones XenMobile Enterprise y MAM) y el paquete de asistencia. Este paso puede tardar más de 15 minutos si está migrando una gran cantidad de usuarios.

27. Haga clic en **Next**. Aparecerá el cuadro de diálogo de confirmación **Start**.



28. Haga clic en **Start**. Aparecerá la página **Upgrade Progress**, con indicadores de progreso para facilitar el seguimiento de la actualización de datos desde XenMobile 9.0. Cuando se complete la actualización, los indicadores de progreso estarán al 100 % y el botón **Next** se habilitará.

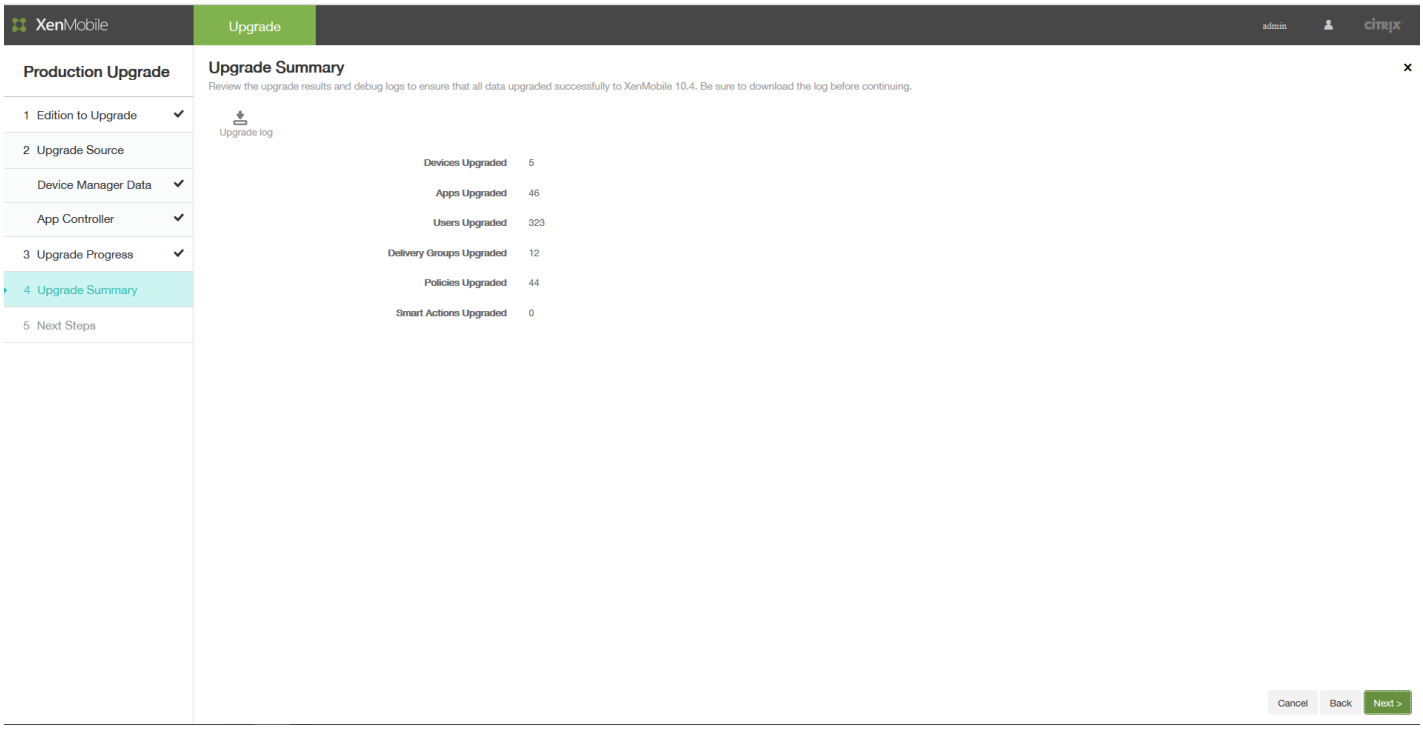
Nota

Si la actualización falla, consulte los registros para averiguar el motivo del error. A continuación, debe importar una nueva instancia de XenMobile y reiniciar el proceso de actualización. No puede usar el botón Atrás del explorador Web para volver a las páginas anteriores y corregir la información.

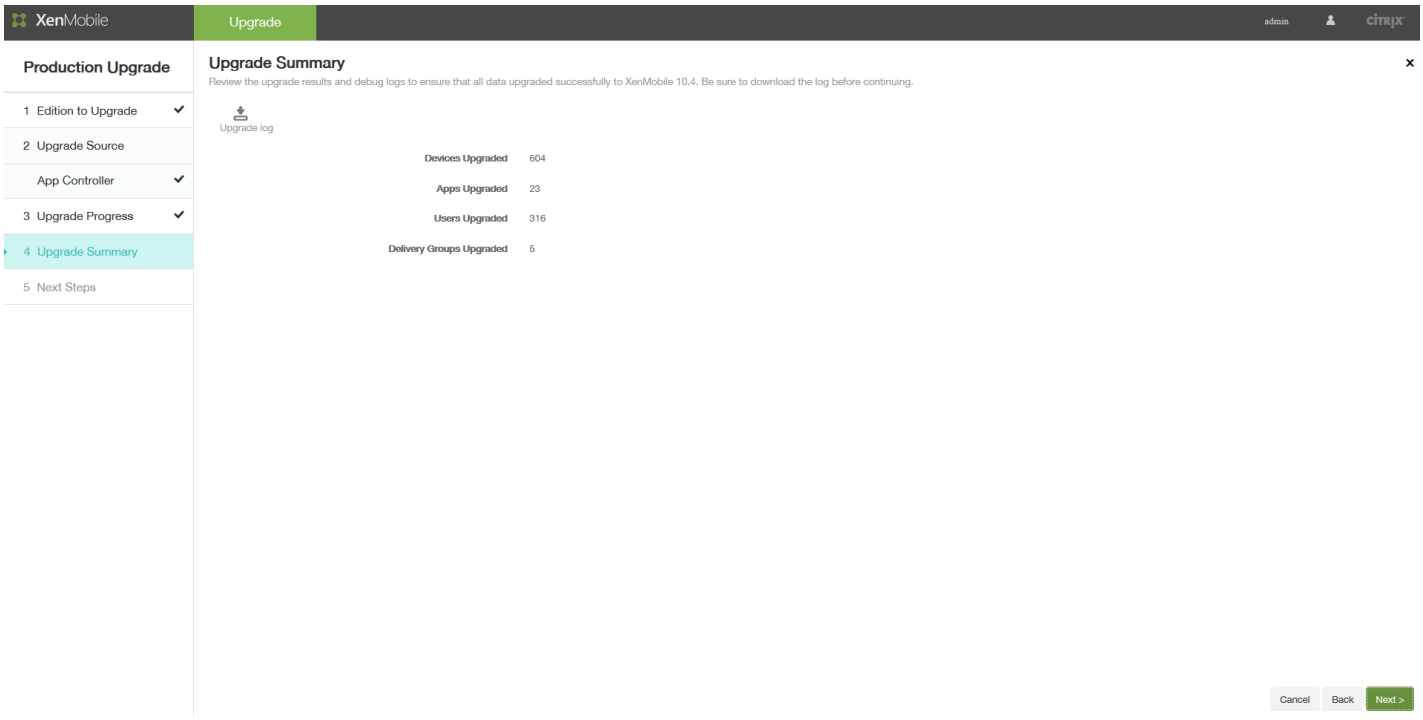
La página Upgrade Progress le notificará cuando la actualización se haya completado correctamente.

29. Haga clic en **Next**. Aparecerá la página **Upgrade Summary**.

Si actualiza una edición Enterprise o MAM, la página **Upgrade Summary** puede tener el siguiente aspecto:



Si actualiza una edición MDM, la página **Upgrade Summary** puede tener el siguiente aspecto:

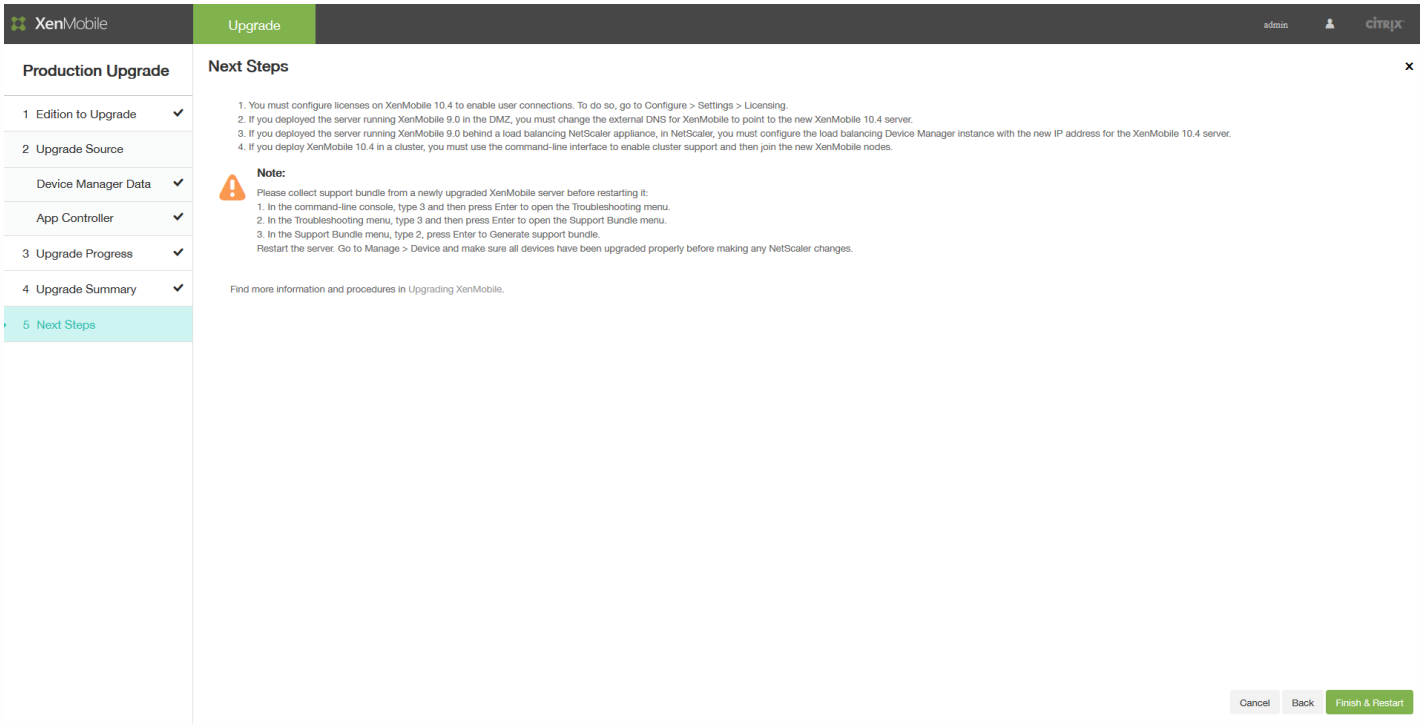


30. Haga clic en el icono **Upgrade log** para descargar los registros. Asegúrese de descargar los registros antes de abandonar esta página.

Citrix recomienda que revise el archivo de registros para determinar las directivas, las configuraciones y los datos de usuario,

etc., que se han actualizado o no a la versión más reciente de XenMobile.

31. Después de descargar los registros de actualización, haga clic en **Next**. Aparecerá la página **Next Steps**.



Para obtener instrucciones relacionadas con estos pasos, consulte Requisitos posteriores de la herramienta de actualización.

Requisitos posteriores de la herramienta Upgrade Tool

Feb 27, 2017

Una vez completada la herramienta de actualización o Upgrade Tool, se ofrece una lista de los próximos pasos generales. Las tareas de requisitos posteriores del entorno pueden variar según la versión instalada de NetScaler, la edición de XenMobile y si se utiliza el asistente "NetScaler para XenMobile" para configurar NetScaler.

Consulte la siguiente lista de tareas y requisitos posteriores, y complete los que se aplican a su entorno.

1. Configuración de licencias en XenMobile para habilitar las conexiones de usuario. Para obtener más información, consulte este procedimiento.

2. Si ha implementado el servidor con XenMobile 9.0 en la zona desmilitarizada (DMZ), debe cambiar el DNS externo para que XenMobile apunte a la nueva instancia de servidor XenMobile.

3. Si ha implementado el servidor con XenMobile 9.0 tras un dispositivo NetScaler de equilibrio de carga, realice los siguientes cambios en NetScaler:

   a. Configure un nuevo servidor virtual de equilibrio de carga para la actualización. Para obtener más información, consulte este procedimiento.

   b. Configure un registro de dirección para apuntar el FQDN del servidor de App Controller al nuevo equilibrador de carga para la actualización. Para obtener más información, consulte este procedimiento.

   c. Cambie el servidor virtual de equilibrio de carga de Device Manager para que apunte a la dirección IP del nuevo servidor XenMobile. Para obtener más información, consulte este procedimiento.

   d. Cambie NetScaler Gateway para que apunte al FQDN del nuevo servidor XenMobile. Para obtener más información, consulte este procedimiento.

   e. Las siguientes tareas solo son necesarias en estos casos:

      - Si ha utilizado el asistente de NetScaler para XenMobile 9 con NetScaler 11.1, 11.0 o 10.5;

      - Si usa NetScaler Gateway 10.1 (no recomendado);

      - Si no usó el asistente de NetScaler para XenMobile cuando configuró NetScaler 10.5 (o posterior) para XenMobile.

   Para conocer los procedimientos que debe seguir en esos casos, consulte los siguientes artículos en la documentación de XenMobile Upgrade Tool 10.1:

      Creación de un nuevo servidor virtual MAM de equilibrio de carga basado en una configuración MDM de modo de puente SSL
      Creación de un nuevo servidor virtual MAM de equilibrio de carga basado en una configuración MDM de descarga de SSL

4. Si implementa la versión más reciente de XenMobile en un clúster, debe usar la interfaz de línea de comandos (CLI) de XenMobile para habilitar el respaldo a clústeres y unir los nuevos nodos de XenMobile. Para obtener ayuda con la interfaz de línea de comandos de XenMobile, consulte Opciones del menú Clustering.

5. Complete el resto de los requisitos posteriores, según sea necesario en su entorno.

Este artículo también contiene requisitos posteriores para los parámetros relacionados con Secure Ticket Authority, el servidor Network Time Protocol, el nombre de host del servidor XenMobile, la actualización de la información que no se ha actualización, nombre de la tienda personalizada e inscripción de dispositivos de XenMobile después de la actualización.

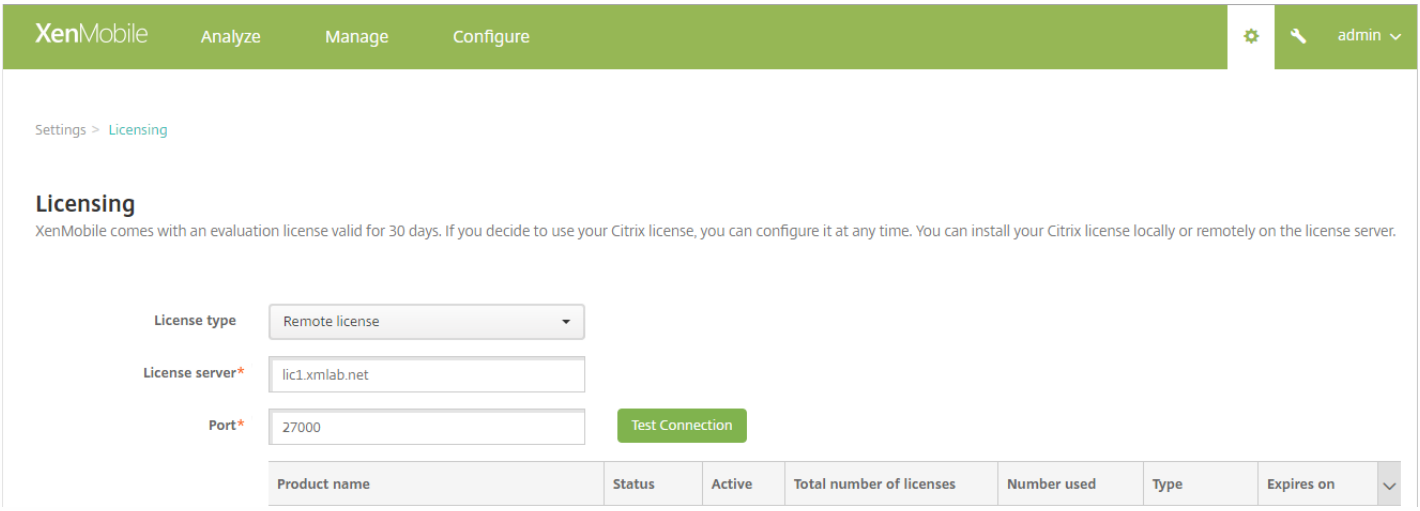
Las versiones más recientes de XenMobile solo admiten el sistema de licencias de Citrix V6. Siga estos pasos para configurar licencias locales o remotas en la nueva consola de XenMobile con el fin de habilitar las conexiones de usuario.

1. Descargue el archivo de licencia. Para ello, consulte Citrix Licensing.

2. Inicie sesión en la nueva consola de XenMobile: Vaya a https://:4443.

- Para actualizaciones MDM o ENT, inicie sesión con las credenciales de administrador de Device Manager para XenMobile 9.0.
- Para actualizaciones MAM, inicie sesión con las credenciales de administrador de App Controller para XenMobile 9.0.

3. Vaya a **Settings > Licensing**.



Para obtener información más detallada sobre cómo agregar licencias locales o remotas, consulte Licencias.

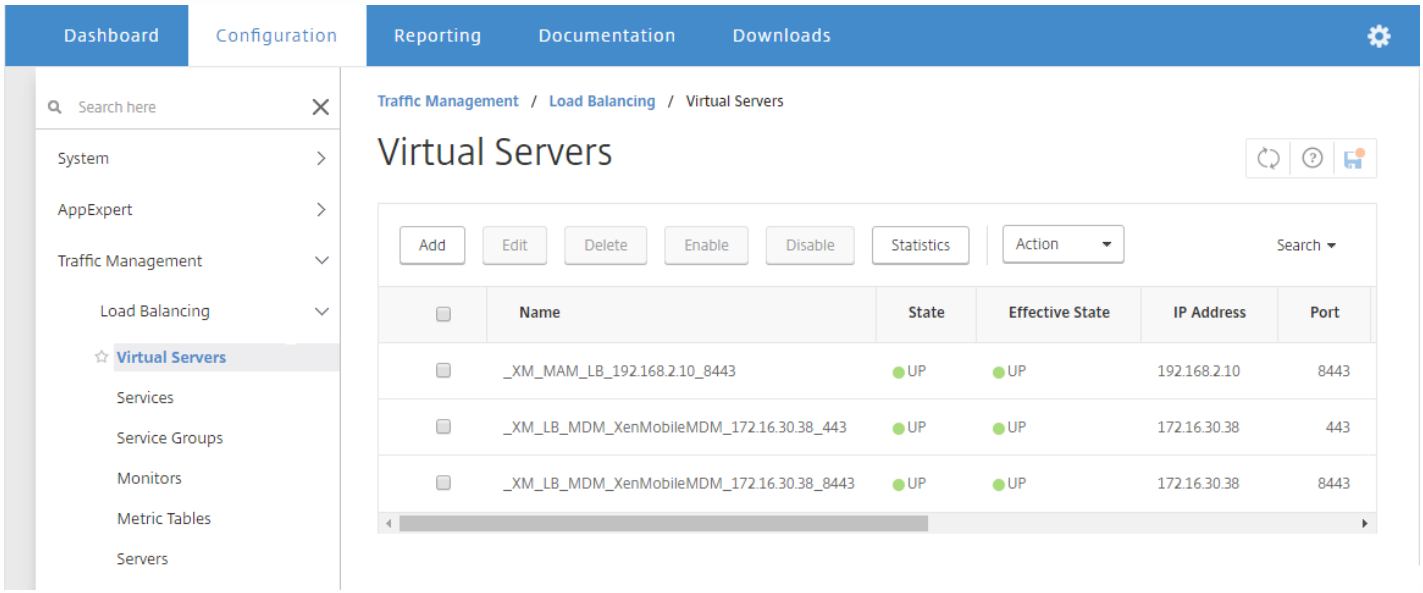
Important

Este requisito posterior *solo* es necesario cuando se realiza una actualización de producción de XenMobile Enterprise Edition. No es necesario para actualizaciones MAM o MDM.

Después de una actualización de producción de XenMobile Enterprise Edition a la versión más reciente de XenMobile, debe configurar un nuevo servidor virtual de equilibrio de carga para el FQDN de App Controller de XenMobile 9.0. Para ello, utilice la herramienta de configuración de NetScaler Gateway.

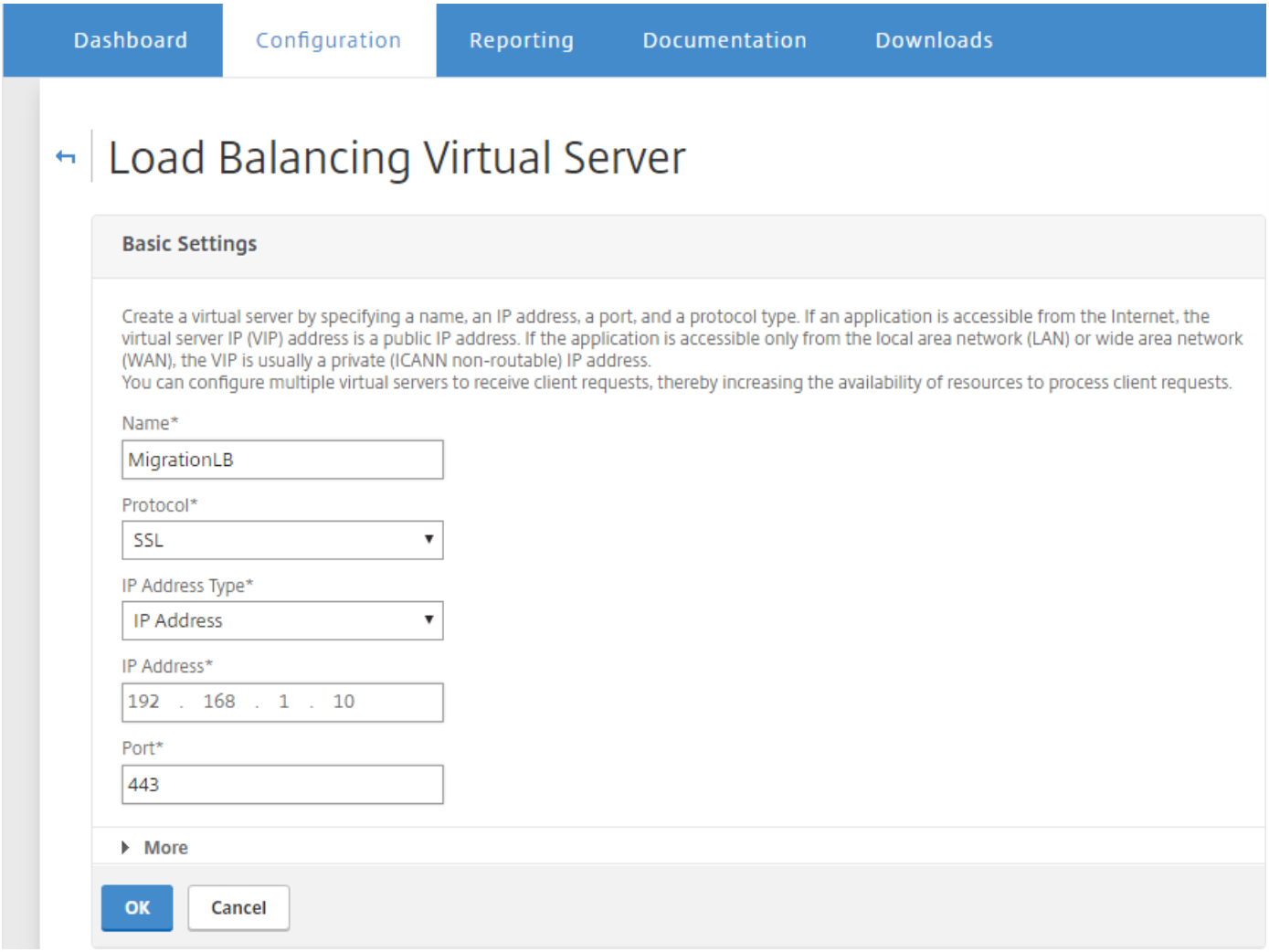
Las pantallas de ejemplo que contiene esta sección, para NetScaler Gateway 11.1, son similares a las de NetScaler Gateway 11.0 y 10.5.

1. Vaya a **Traffic Management > Load Balancing > Virtual Servers**.



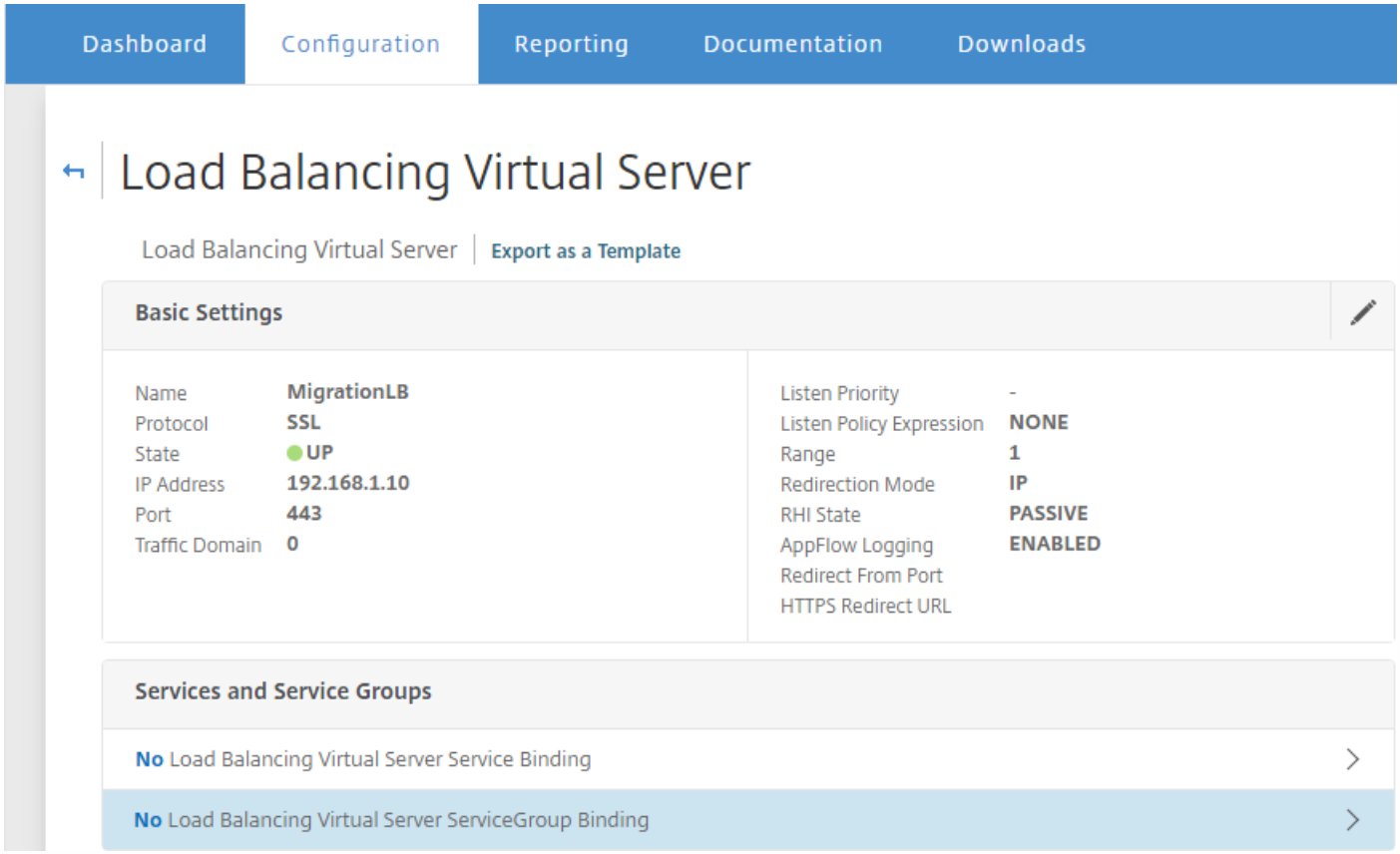
2. Haga clic en **Add**.

3. En la página **Load Balancing Virtual Server**, configure los siguientes parámetros y haga clic en **OK**.

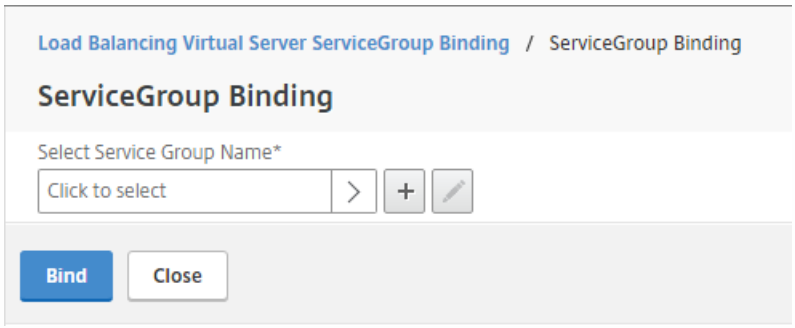


- **Name**. Escriba el nombre del nuevo equilibrador de carga.
- **Protocol**. Establezca el campo en **SSL**. El valor predeterminado es **HTTP**.
- **IP Address**. Escriba una dirección IP para el nuevo equilibrador de carga, el cual sigue el protocolo RFC 1918; por ejemplo: 192.168.1.10.
- **Port**. Establezca el número de puerto en **443**.

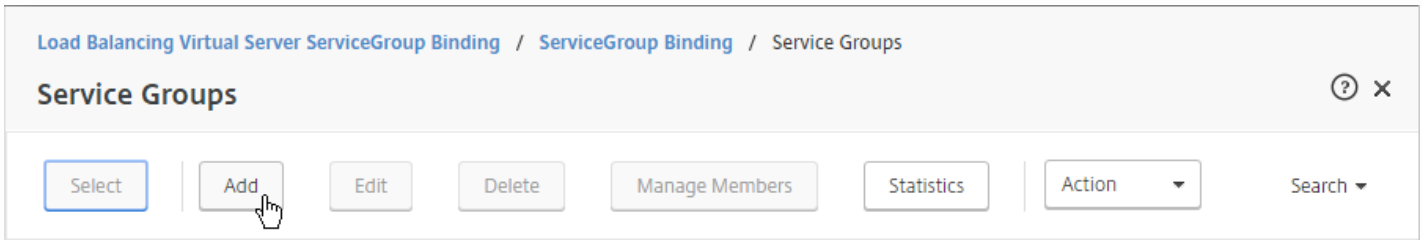
4. En **Services and Service Groups**, haga clic en **No Load Balancing Virtual Server Service Group Binding**.



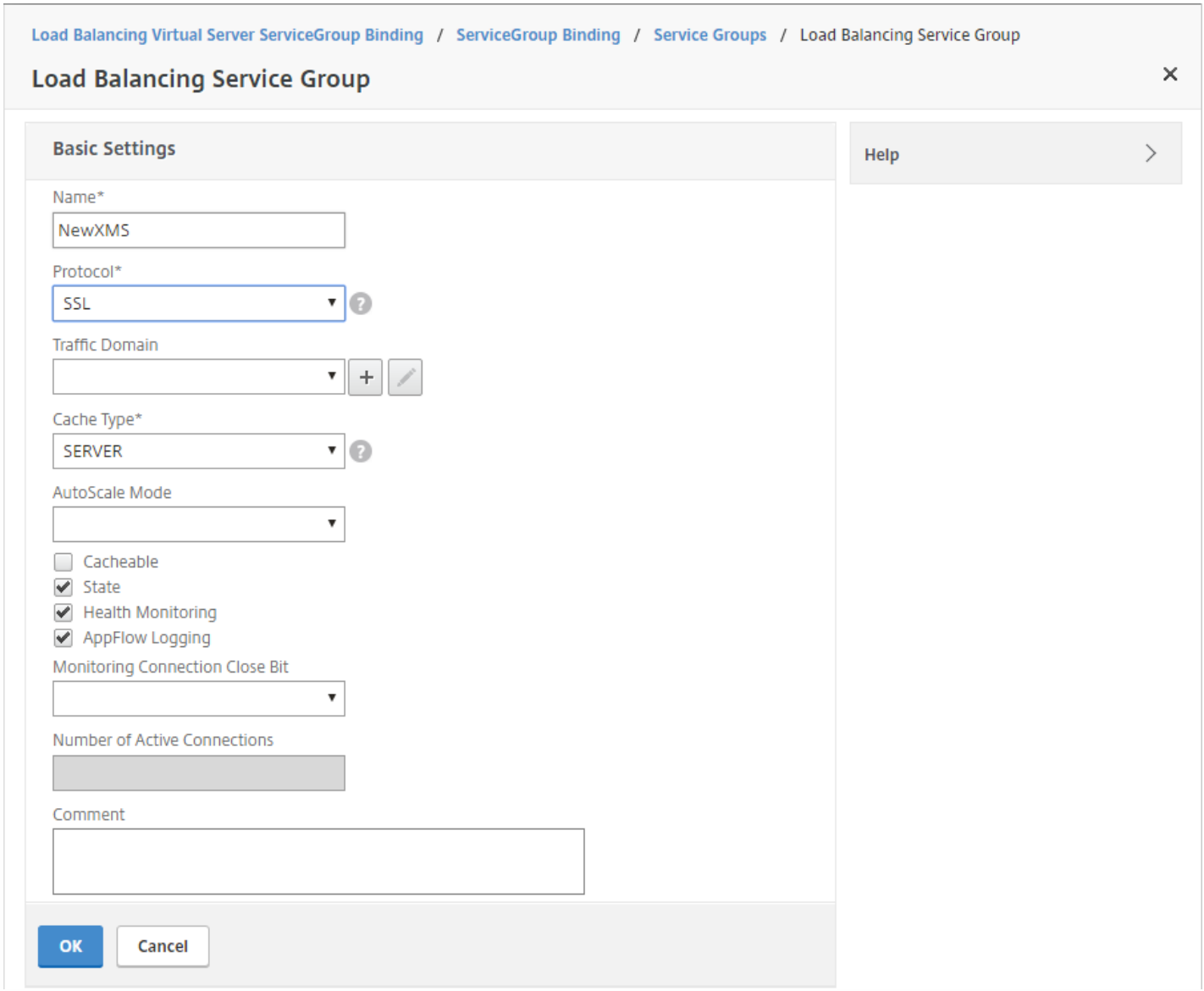
5. En **Select Service Group Name**, haga clic en **Click to Select**.



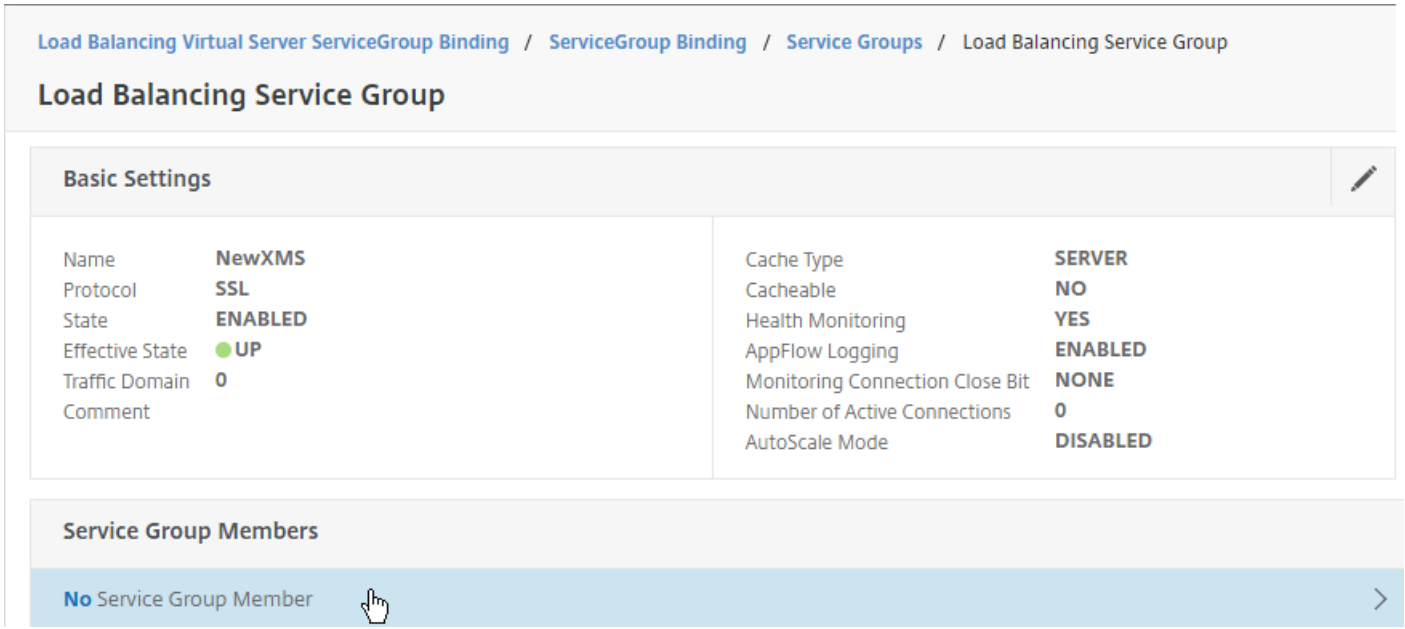
6. Haga clic en **Add** para crear un nuevo grupo de servicio.



7. En la página **Load Balancing Service Group**, escriba un nombre para el nuevo grupo de servicio, compruebe que el protocolo está establecido en **SSL** y, a continuación, haga clic en **OK**.

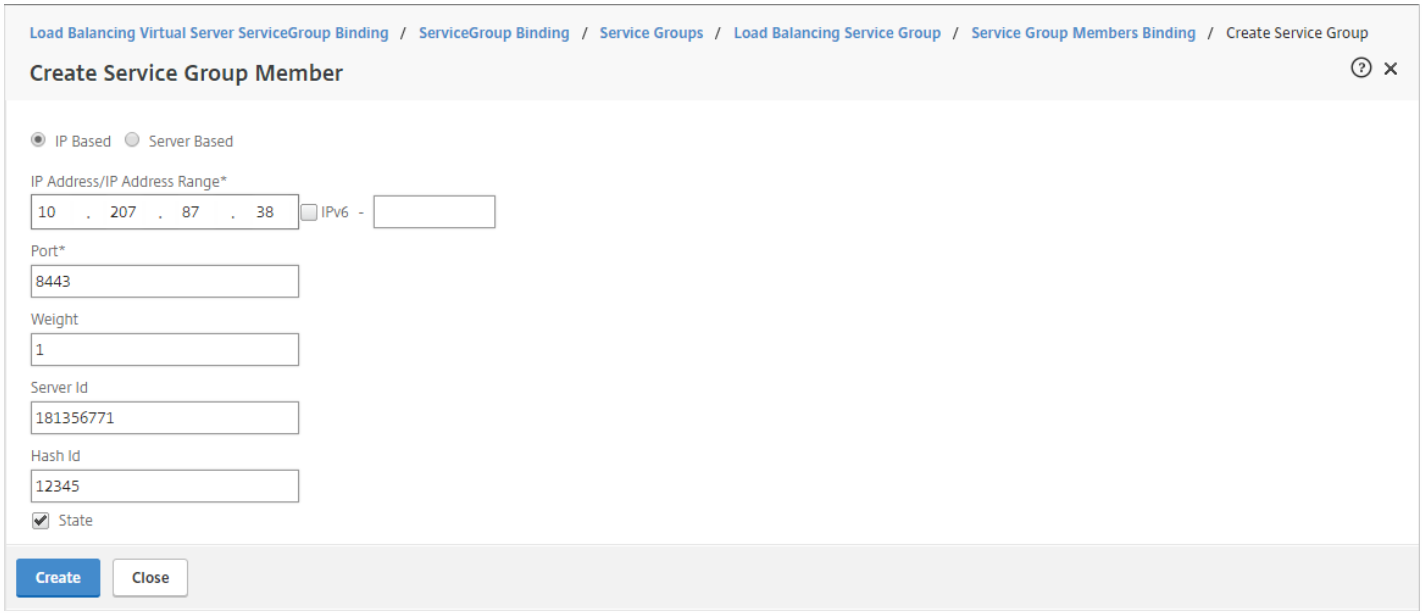


8. Haga clic en **No Service Group Member**.

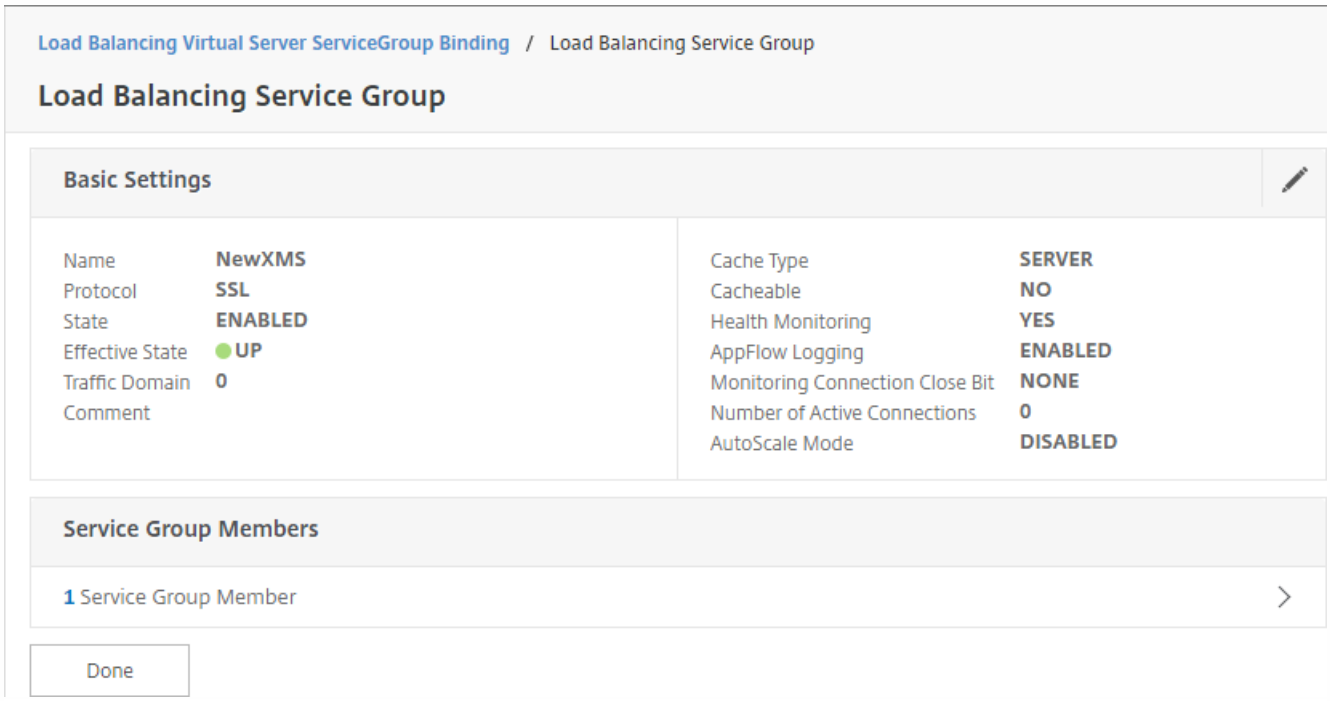


9 En la página **Create Service Group Member**, configure los siguientes parámetros:

- **IP Address/IP Address Range**. Introduzca la dirección IP de la instancia del servidor XenMobile.
- **Port**. Establezca el número de puerto en **8443**.
- **Server ID**. Si realiza la migración desde un entorno de XenMobile 9.0 en clústeres a un nuevo entorno de XenMobile también en clústeres, escriba el ID del nodo del servidor XenMobile actual. Puede obtener el ID del nodo del servidor si inicia sesión en la interfaz de línea de comandos (CLI) del servidor XenMobile y escribe **1** para ir al menú **Clustering**. El ID del nodo de servidor en CLI tiene la etiqueta **Current Node ID**.

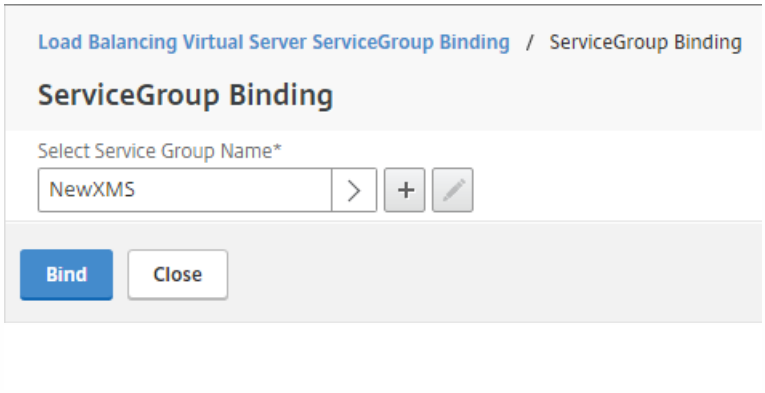


10. Haga clic en **Create** y, luego, en **Done**.

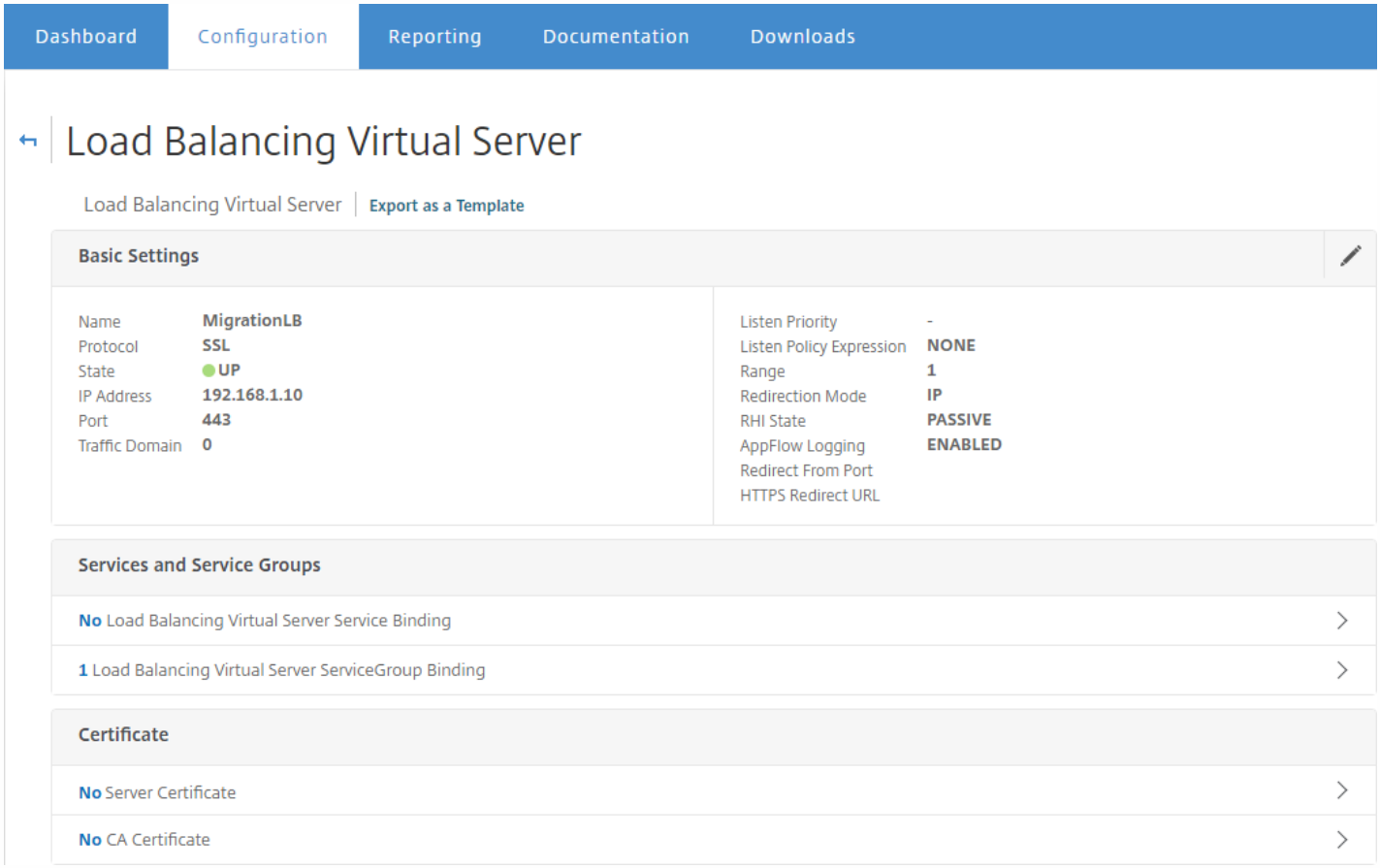


11. Haga clic en **Done** y, a continuación, en **OK**.

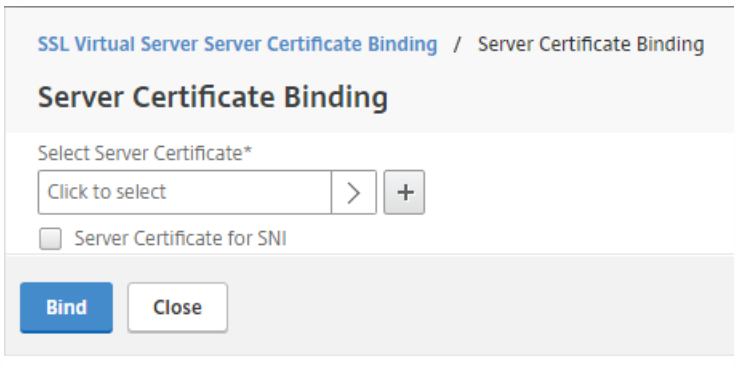
12. Haga clic en **Bind** y, a continuación, en la pantalla siguiente, haga clic en **Done**.



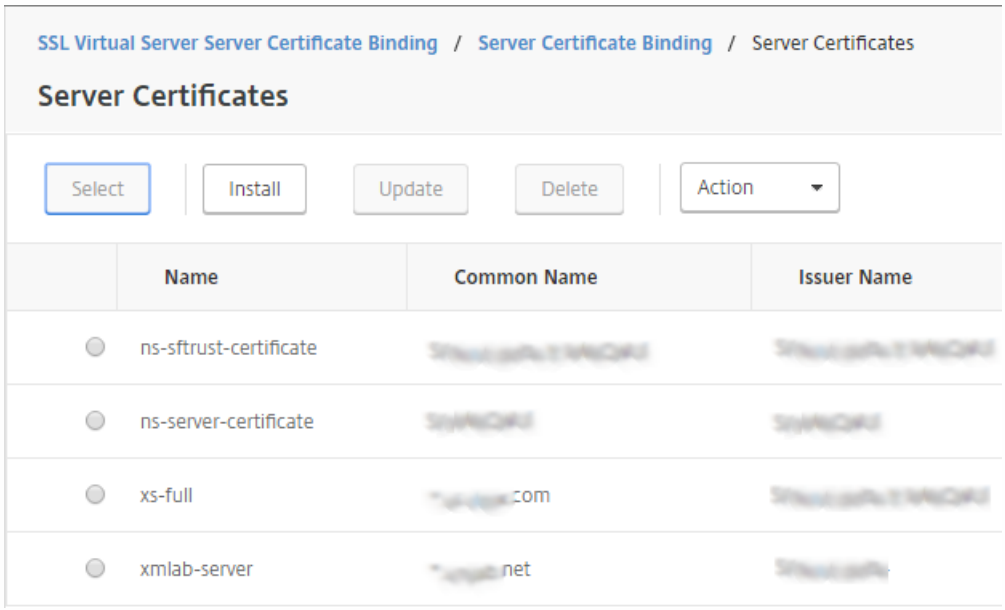
13. En **Certificates**, haga clic en **No Server Certificate**.



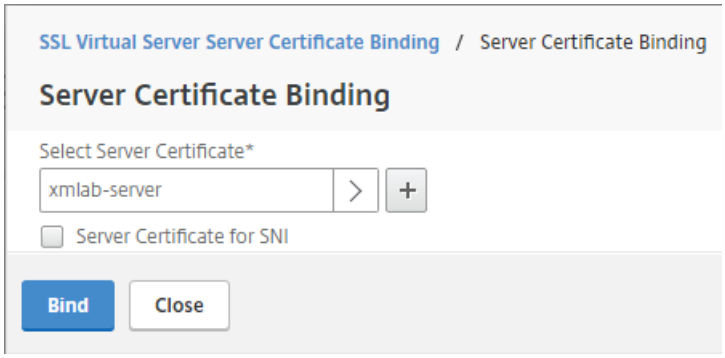
14. En **Server Certificate Binding**, haga clic en **Click to Select**.

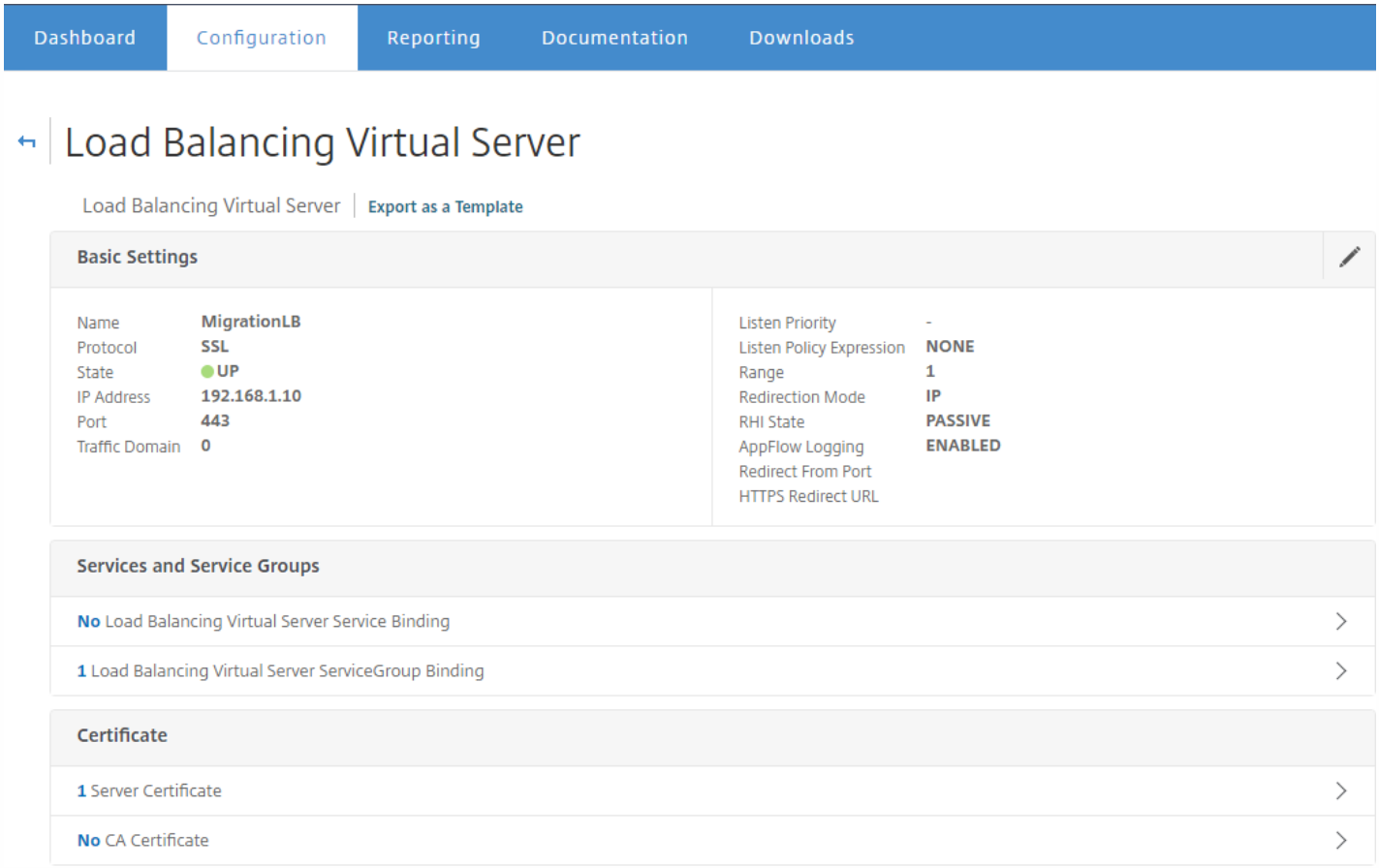


15 En **Certificates**, haga clic en el certificado del servidor XenMobile 9.0 que exportó en Requisitos previos de Upgrade Tool y haga clic en **OK**.

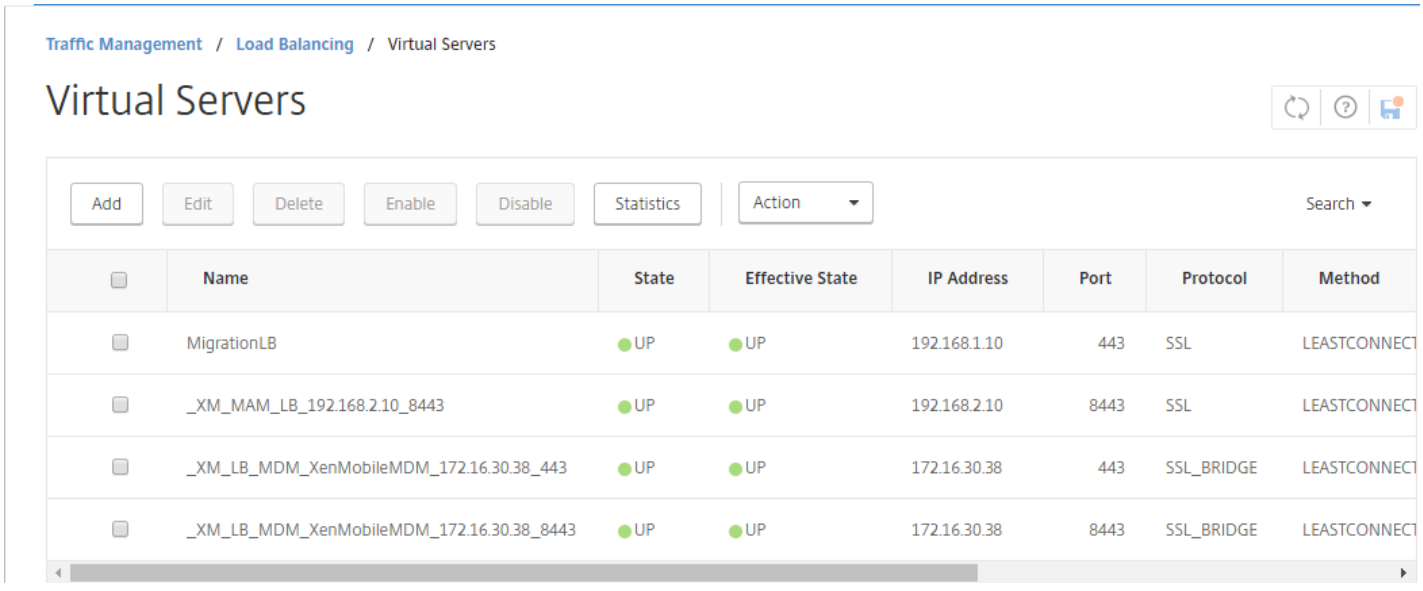


16. Haga clic en **Bind** y, a continuación, en la pantalla siguiente, haga clic en **Done**.



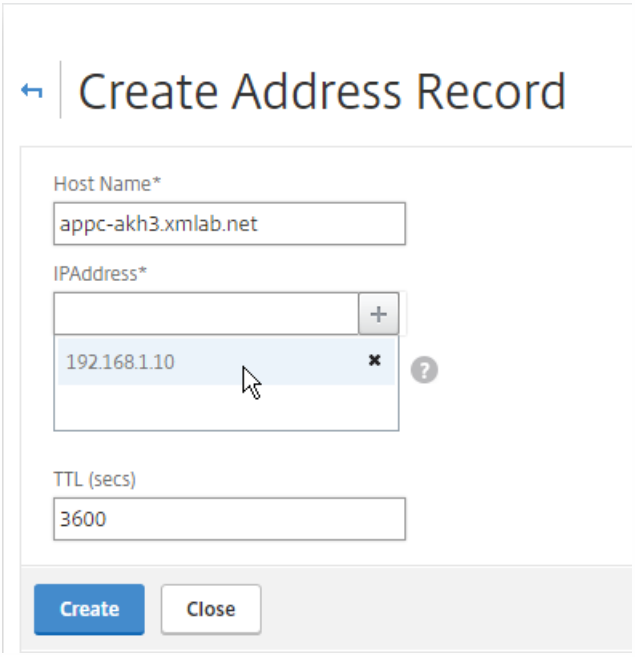


17. Haga clic en el botón de actualización para confirmar que el servidor está activo.



1. Inicie sesión en NetScaler, haga clic en **Traffic Management > DNS > Records > Address Records**. A continuación, haga clic en **Add**.

> **Nota**
>
> Si dispone de una configuración GSLB (equilibrio de carga global de servidores) y agrega un registro de dirección, el sistema GSLB ofrecerá una respuesta de autoridad a aquel servidor que tenga la dirección IP local.

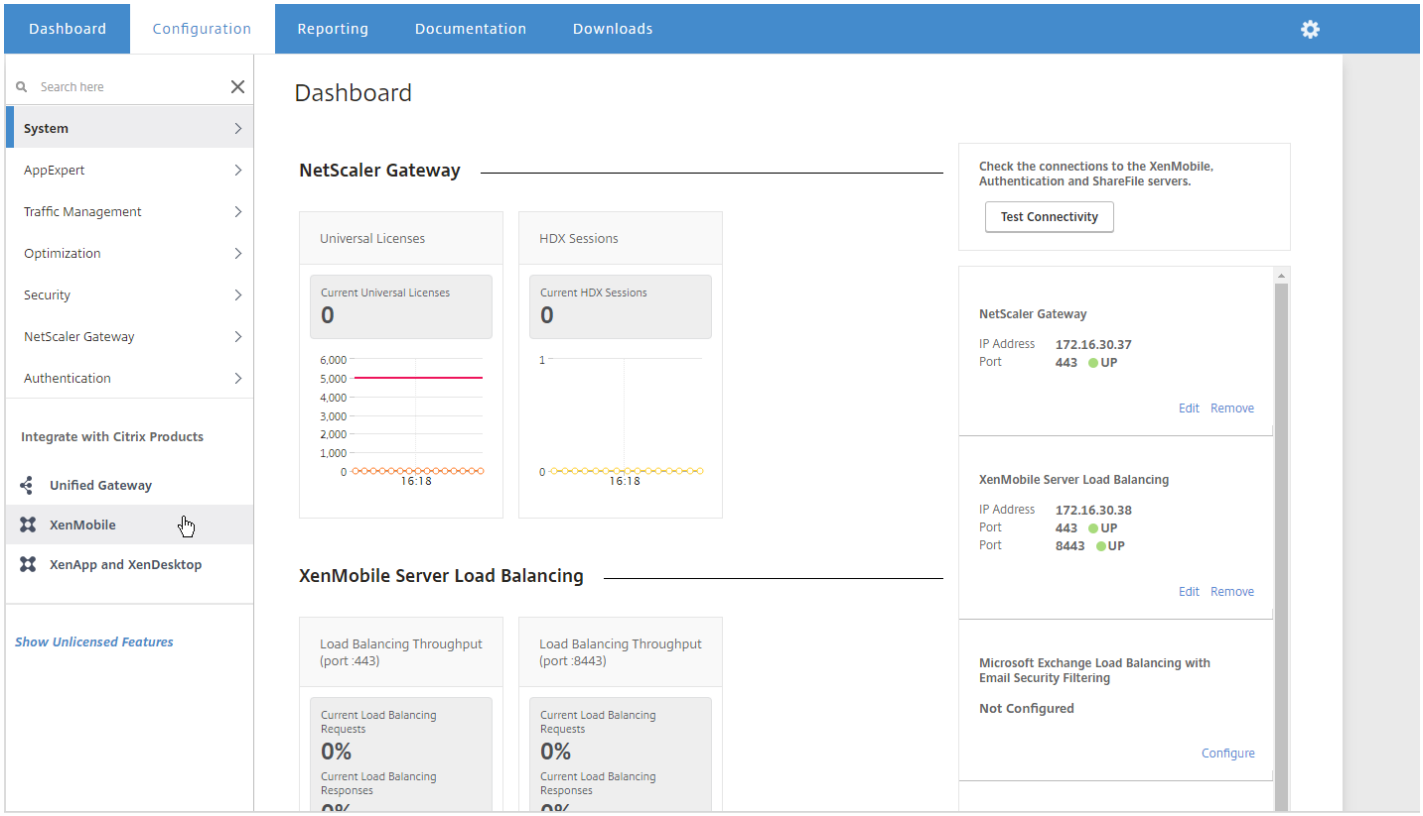


Si ha implementado el servidor con XenMobile 9.0 tras un dispositivo NetScaler de equilibrio de carga, debe configurar la instancia de Device Manager del equilibrio de carga para XenMobile 9.0 en NetScaler con la nueva dirección IP de la nueva instancia del servidor XenMobile.

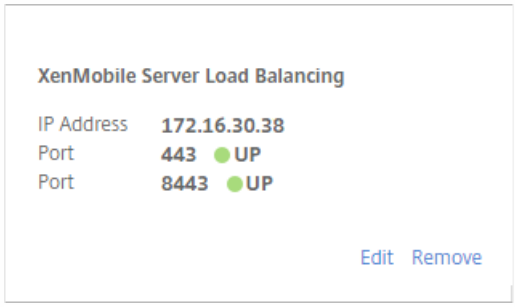
El procedimiento difiere según si se usa NetScaler 11.1 o NetScaler 11.0 o 10.5.

Para NetScaler 11.1

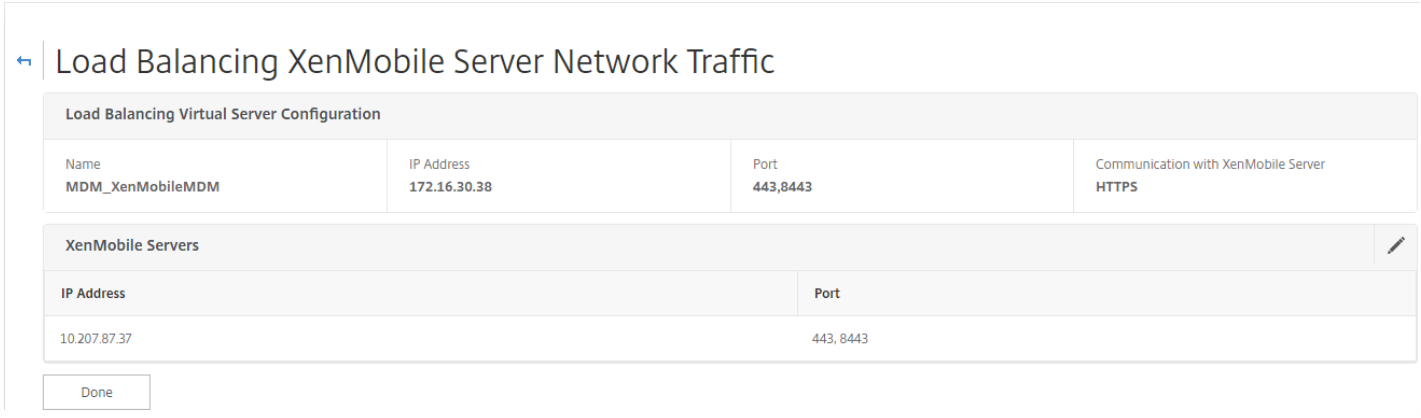
1. En **Integrate with Citrix Products**, haga clic en **XenMobile**.



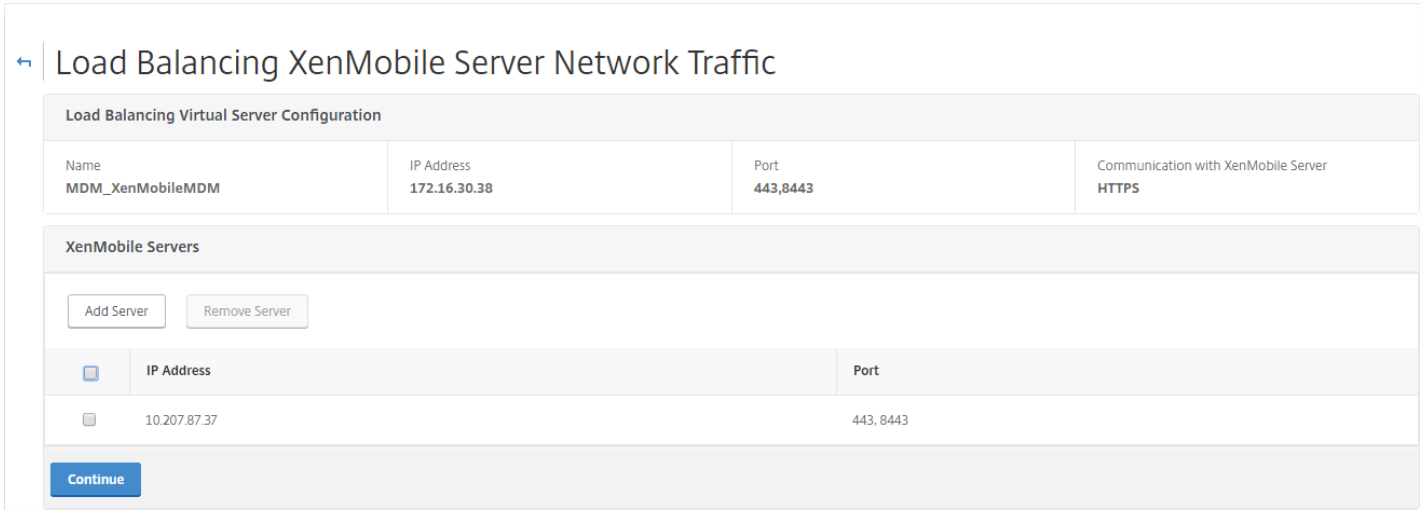
2. En el lado derecho de la pantalla, en **XenMobile Server Load Balancing**, haga clic en **Edit**.



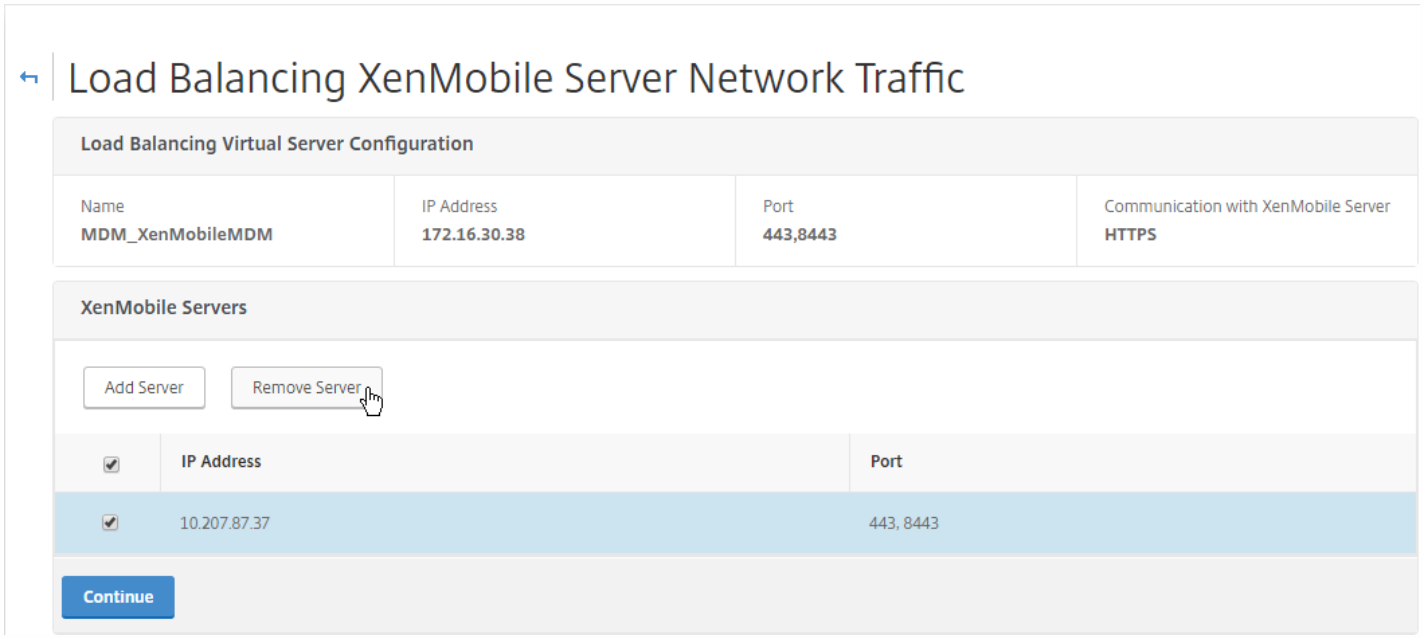
Aparecerá la página **Load Balancing XenMobile Server Network Traffic**.



3. Haga clic en el icono de lápiz para que XenMobile Server abra esos parámetros.



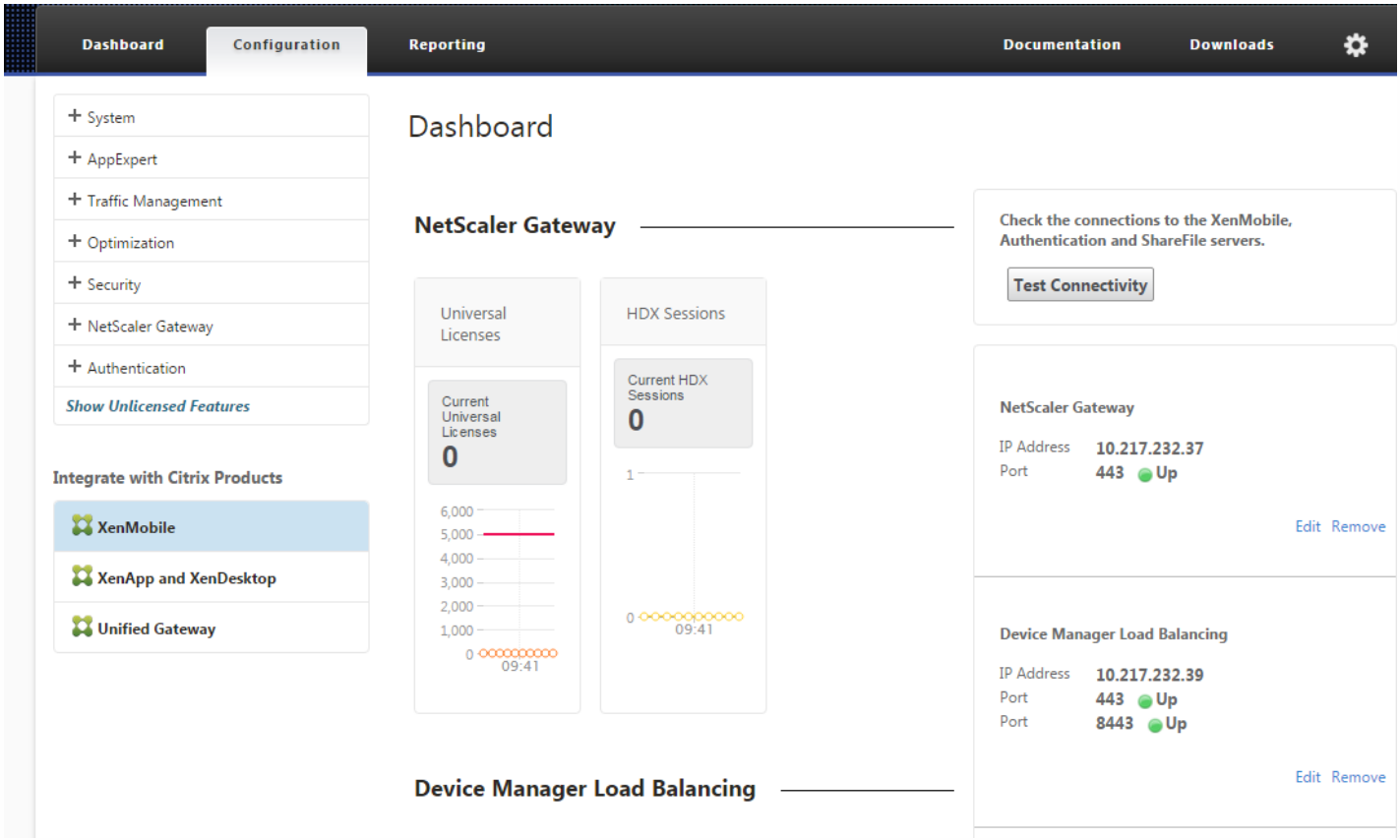
4. Seleccione la IP del servidor de Device Manager de XenMobile 9.0 y haga clic en **Remove Server**.



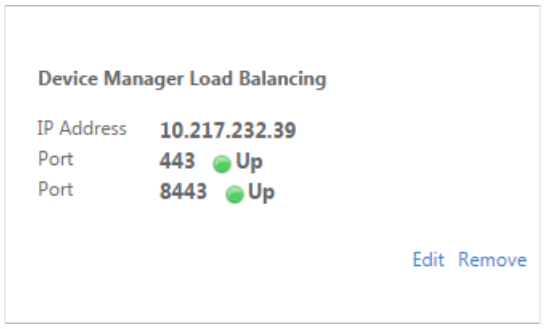
5. Haga clic en **Add Server** y agregue la IP del nuevo servidor XenMobile.

Para las versiones de NetScaler 11.0 o 10.5

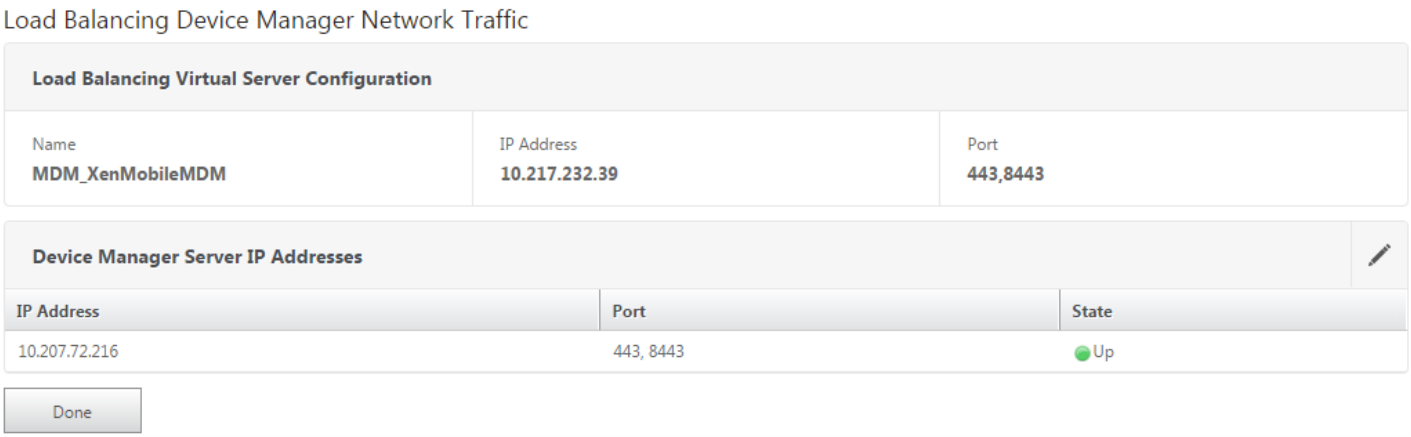
1. En **Integrate with Citrix Products**, haga clic en **XenMobile**.



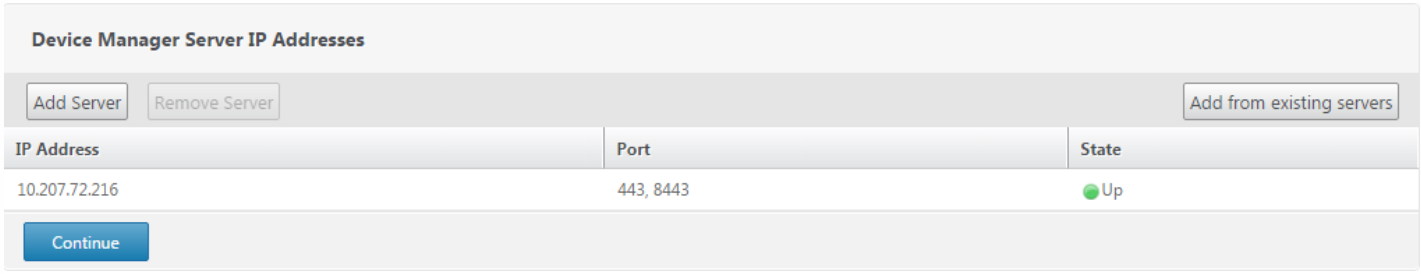
2. En el lado derecho de la pantalla, en **Device Manager Load Balancing**, haga clic en **Edit**.



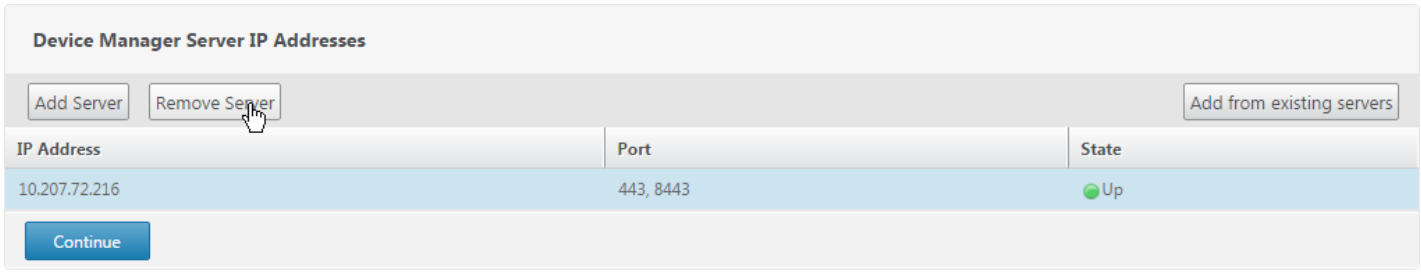
Aparecerá la página **Load Balancing Device Manager Network Traffic**.



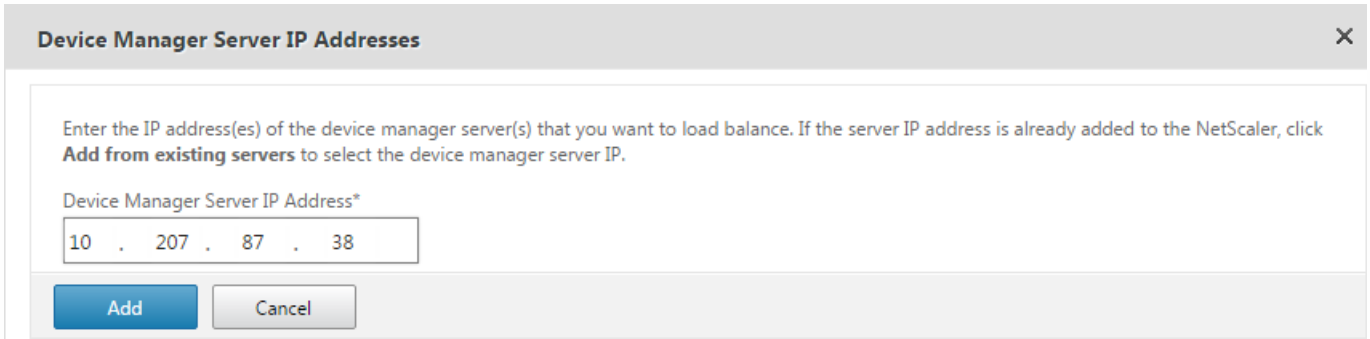
3. Haga clic en el icono de lápiz de **Device Manager Server IP Addresses** para abrir esos parámetros.



4. Seleccione la IP del servidor de Device Manager de XenMobile 9.0 y haga clic en **Remove Server**.



5. Haga clic en **Add Server** y agregue la IP del nuevo servidor XenMobile.



En este punto, NetScaler Gateway apunta al FQDN de App Controller. Debe cambiar NetScaler para que apunte al FQDN del nuevo XenMobile. Las versiones más recientes de XenMobile escuchan en el puerto 8443 en lugar del puerto 443. Si utilizó el asistente de NetScaler para XenMobile 9 para configurar NetScaler, debe incluir el número de puerto con el FQDN, como se muestra en los ejemplos de las siguientes tablas.

XenMobile Enterprise Edition

Cambie el FQDN de App Controller para que apunte al nuevo FQDN de XenMobile, que es el FQDN de Device Manager de XenMobile 9.0 seguido del puerto 8443. En la siguiente tabla, se muestra un ejemplo.

Componente de XenMobile 9.0	FQDN del componente	FQDN de la nueva edición de XenMobile Enterprise
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	N/D
NetScaler Gateway	access.example.com	N/D

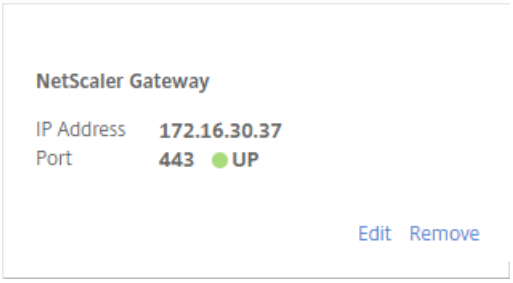
XenMobile App Edition

Cambie el FQDN de App Controller para que apunte al nuevo FQDN de XenMobile, que es el FQDN de App Controller de XenMobile 9.0 seguido del puerto 8443. En la siguiente tabla, se muestra un ejemplo.

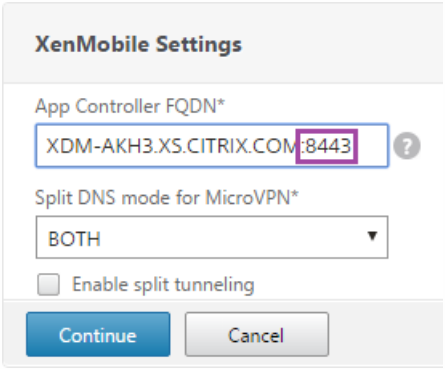
Componente de XenMobile 9.0	FQDN del componente	FQDN de la nueva edición de XenMobile Enterprise
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	N/D

1. En **Integrate with Citrix Products**, haga clic en **XenMobile**.

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



3. Haga clic en el icono de lápiz situado junto a **XenMobile Settings** y cambie el FQDN de App Controller al FQDN del servidor XenMobile y agregue **:8443** al FQDN. Por ejemplo, ***EJEMPLO-XENMOBILE.FQDN*.COM:8443**.

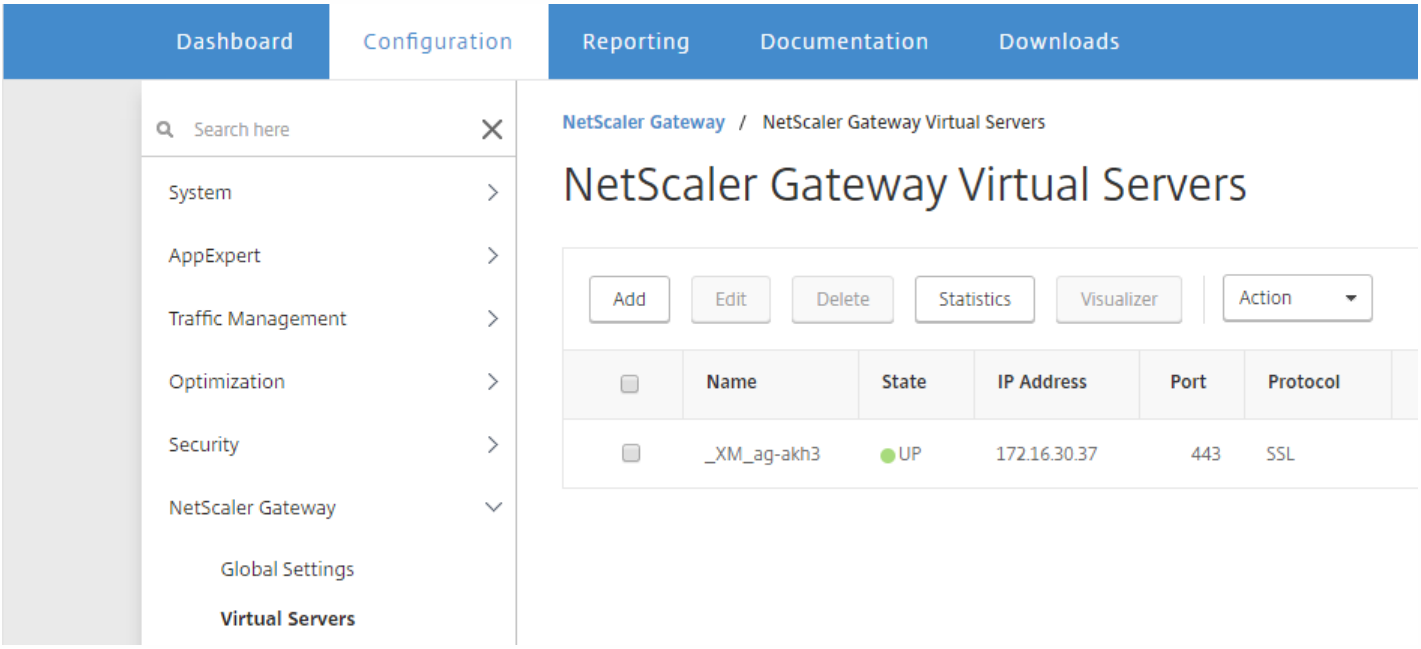


4. Haga clic en **Continue** y en **Finish**.

A continuación, debe actualizar el DNS para resolver el FQDN del servidor que ejecuta Secure Ticket Authority a la dirección IP de la nueva instancia de XenMobile Server. A veces, cuando se cambian los requisitos posteriores, el servidor de STA no está vinculado en NetScaler aunque aparezca en la lista **VPN Virtual Server STA Server Binding**.

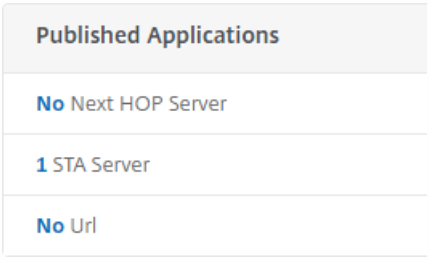
En NetScaler Gateway, agregue la dirección IP o el FQDN del servidor que ejecuta Secure Ticket Authority. Para ello, siga estos pasos:

1. Haga clic en **Netscaler Gateway > Virtual Servers**.

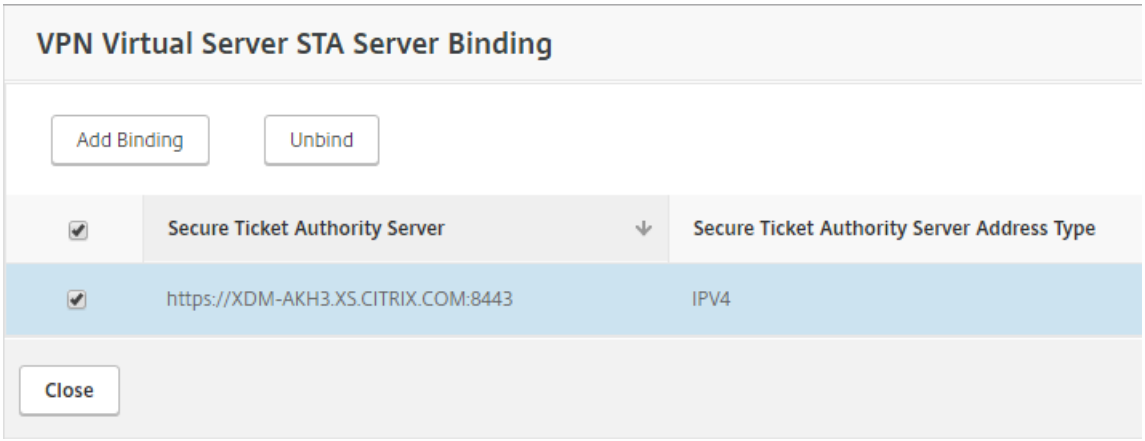


2. Compruebe que el servidor virtual de NetScaler Gateway tiene el estado **Up**. Seleccione el servidor virtual configurado de NetScaler Gateway y, a continuación, haga clic en **Edit**.

3. En **Published Applications**, haga clic en **STA server**.



4. Anote la URL de **Secure Ticket Authority Server**, porque deberá introducirla en el paso 6. A continuación, seleccione el servidor de Secure Ticket Authority en la lista.



5. Haga clic en **Unbind** y, a continuación, en **Add Binding**.

6. En el campo **Secure Ticket Authority Server**, escriba la URL que anotó en el paso 4.

7. Haga clic en **Bind**, en **Close** y, a continuación, en **Done**.

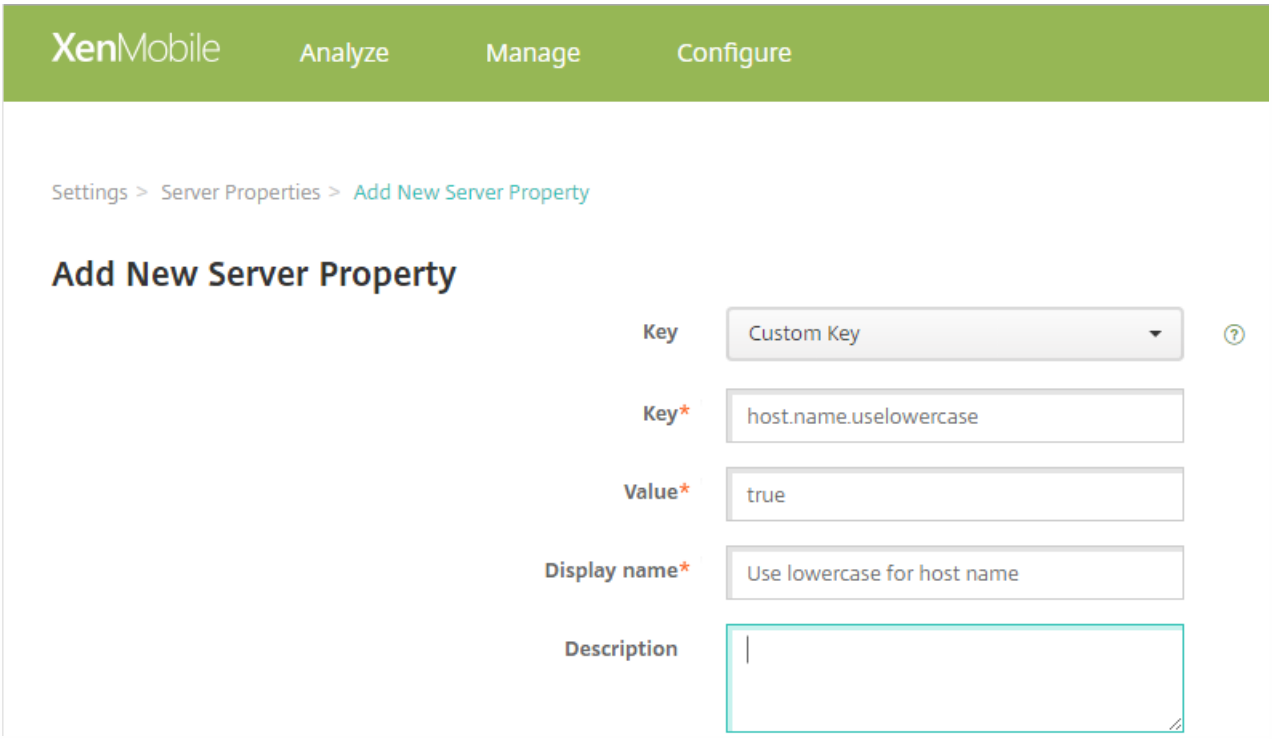
Asegúrese de sincronizar la hora de NetScaler y del servidor XenMobile. Si es posible, haga que NetScaler y el servidor XenMobile apunten a un mismo servidor NTP (Network Time Protocol).

Si el nombre de host de su implementación de XenMobile 9.0 incluye letras mayúsculas, complete los siguientes pasos para que los dispositivos móviles puedan acceder a Citrix Store:

1. En la nueva consola de XenMobile, vaya a **Settings > Server Properties**.

2. Haga clic en **Add** y complete los campos de la siguiente manera:

- **Key**. Seleccione **Custom Key**.
- **Key**. Escriba **nombre.de.host.usarminúscula**.
- **Value**. Escriba **true**.
- **Display name**. Escriba una descripción de la clave.



3. Reinicie el servidor XenMobile.

Actualice lo siguiente según sea necesario:

- Grupo del proveedor de servicios administrado (MSP)
- Atributos personalizados de Active Directory
- Roles de RBAC
  En una actualización local, la configuración de RBAC presenta problemas. Para obtener más información, consulte Problemas conocidos.
- Parámetros de registro
- Datos de configuración o de usuario que contenga el archivo migration.log
- Cualquier configuración del servidor syslog

Antes de actualizar, uno de los pasos de requisitos previos era cambiar un nombre de tienda de Citrix personalizado a su valor predeterminado. Si no ha completado ese requisito previo, debe seguir uno de estos pasos de requisitos posteriores antes de utilizar la versión más reciente de XenMobile Server:

- Si tiene una gran cantidad de dispositivos Windows, cambie el nombre de la tienda al valor predeterminado. Después de ello, los usuarios finales inscritos con dispositivos iOS y Android deberán cerrar sesión en Citrix Secure Hub (anteriormente conocido como Worx Home) y, a continuación, deberán volver a iniciarla.
- Si tiene menos dispositivos Windows que dispositivos iOS y Android, se recomienda los usuarios de Windows vuelvan a inscribir sus dispositivos.

Para obtener más información sobre este problema, consulte http://support.citrix.com/article/CTX214553.

Los usuarios no necesitan volver a inscribir sus dispositivos después de realizar una actualización de producción a la versión más reciente de XenMobile. Los dispositivos deben poder conectarse automáticamente al nuevo servidor XenMobile según el intervalo de latido. No obstante, es posible que los usuarios tengan que volver a autenticarse para que el dispositivo pueda conectar.

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

Actualización del servidor de arrendatario de MTC a XenMobile

Feb 27, 2017

Si XenMobile 9.0 MDM Edition o Enterprise Edition tiene habilitada la consola Multi-Tenant Console (MTC), puede migrar instancias de XenMobile 9 administradas desde esa consola a instancias independientes de la versión más reciente de XenMobile. XenMobile 10.x no admite la consola MTC, de modo que debe administrar individualmente esas instancias actualizadas.

1. Compruebe que ha configurado la traducción de direcciones de red (NAT) al frente de todos los clientes MTC.

2. Instale una instancia de la versión más reciente de XenMobile.

3. Si no hay ninguna asignación de puertos habilitada en el arrendatario MTC, haga lo siguiente:

    a. El puerto del servidor perteneciente a la nueva instancia de XenMobile, que permite la comunicación HTTPS con certificados (normalmente, el puerto 443) y el puerto que permite la comunicación HTTPS sin certificados (8443) deben coincidir con los puertos que se usan para la instancia de XenMobile.

    b. Configure un nuevo puerto para la administración.

    c. Cuando la asignación de puertos esté habilitada, use el puerto asignado y no el puerto en que escucha el servidor XenMobile.

4. Durante el inicio del servidor XenMobile, use el nombre de la instancia, **zdm**.

5. Cuando habilite la herramienta "Upgrade Tool" desde la interfaz de línea de comandos de XenMobile, debe responder **Yes** a la solicitud de actualización.

6. Desde el servidor a actualizar, copie los archivos siguientes desde la unidad C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classes:

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

7. Copie los archivos siguientes desde: C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\"nombre-de-arrendatario":

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

8. Haga una copia del archivo "server.xml" ubicado en la unidad C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml y modifíquelo como se describe en los pasos siguientes.

9 Quite todos los conectores de puertos que use el otro arrendatario en server.xml, excepto la del puerto 80.

10. En el conector de puerto utilizado, quite el nombre de la instancia de todas las rutas de archivo que se encuentren dentro del rango siguiente:

keystoreFile="C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\nombre-de-arrendatario\https.p12"

por:

keystoreFile="C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\https.p1"

11. Repita el paso 10 para las rutas de archivo en:

truststoreFile="C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\cacerts.pem.jks"

por:

truststoreFile="C:\Archivos de programa (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pem.jks"

12. Cree un archivo ZIP con los archivos que copió en los pasos 6 y 8.

13. Abra la dirección IP del nuevo servidor XenMobile con una dirección en el siguiente formato: https://*direcciónIP:puerto*/uw/?cloudMode, donde *puerto* es la conexión HTTPS con un certificado. Se abrirá el asistente de actualización.

14. Con los pasos que se describen en el Asistente de actualización, seleccione **MDM** o **Enterprise**.

Para actualizaciones **MDM**, el asistente le pedirá que cargue el archivo ZIP. También debe comprobar que la base de datos es correcta e introducir la contraseña del certificado de CA.

Para actualizaciones **Enterprise**, el asistente le pedirá que cargue el paquete de asistencia de App Controller.

15 Después de reiniciarse el servidor XenMobile, inicie sesión en la consola de XenMobile con la dirección IP del servidor XenMobile seguida del número del puerto de administración.

16. Cambie la traducción de direcciones de red para que apunte al nuevo servidor.

17. Haga los cambios necesarios en el firewall para permitir los puertos que utilice el servidor XenMobile.

Inscripción, roles y cuentas de usuario

Mar 29, 2017

Puede configurar los elementos siguientes en la consola de XenMobile desde la ficha **Manage** y la página **Settings**:

- Grupos y cuentas de usuario
- Roles para grupos y cuentas de usuario
- Invitaciones y modo de inscripción

Desde la ficha **Manage**, puede llevar a cabo lo siguiente:

- Haga clic en **Users** 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 cuentas de usuarios locales
  - Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV y Formatos de archivo de aprovisionamiento
  - Para agregar o quitar grupos en XenMobile

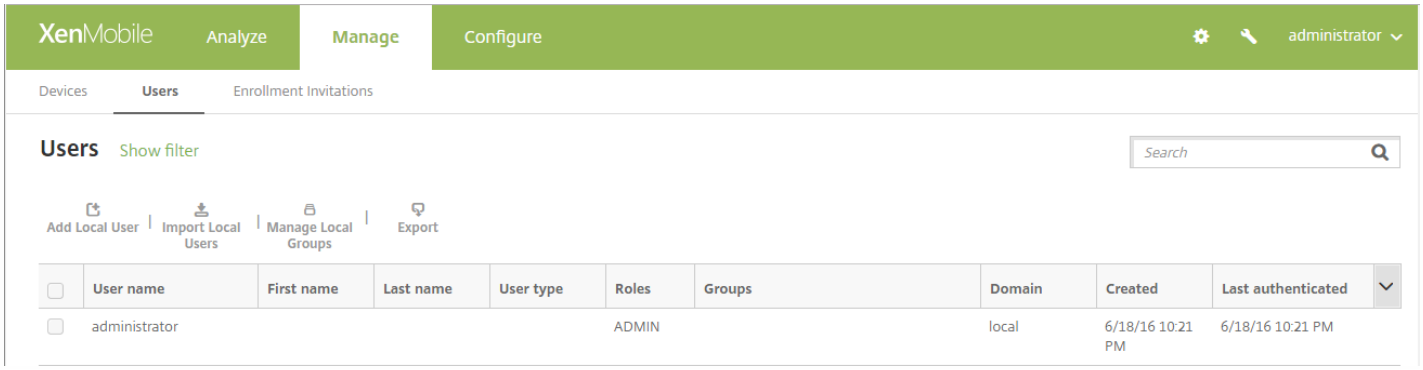
  Asimismo, puede utilizar los flujos de trabajo para administrar la creación y la eliminación de las cuentas de usuario, como se describe más adelante en este artículo, en Creación y administración de flujos de trabajo.
- Haga clic en **Enrollment** para configurar hasta siete modos y enviar invitaciones de inscripción. Cada modo de inscripción ofrece su propio nivel de seguridad y unos pasos propios que los usuarios deberán seguir para inscribir sus dispositivos. 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

En la página **Settings**, puede realizar lo siguiente:

- 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
- 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: Secure Hub, SMTP o SMS. Para obtener más detalles, consulte:
  - Creación y actualización de plantillas de notificaciones

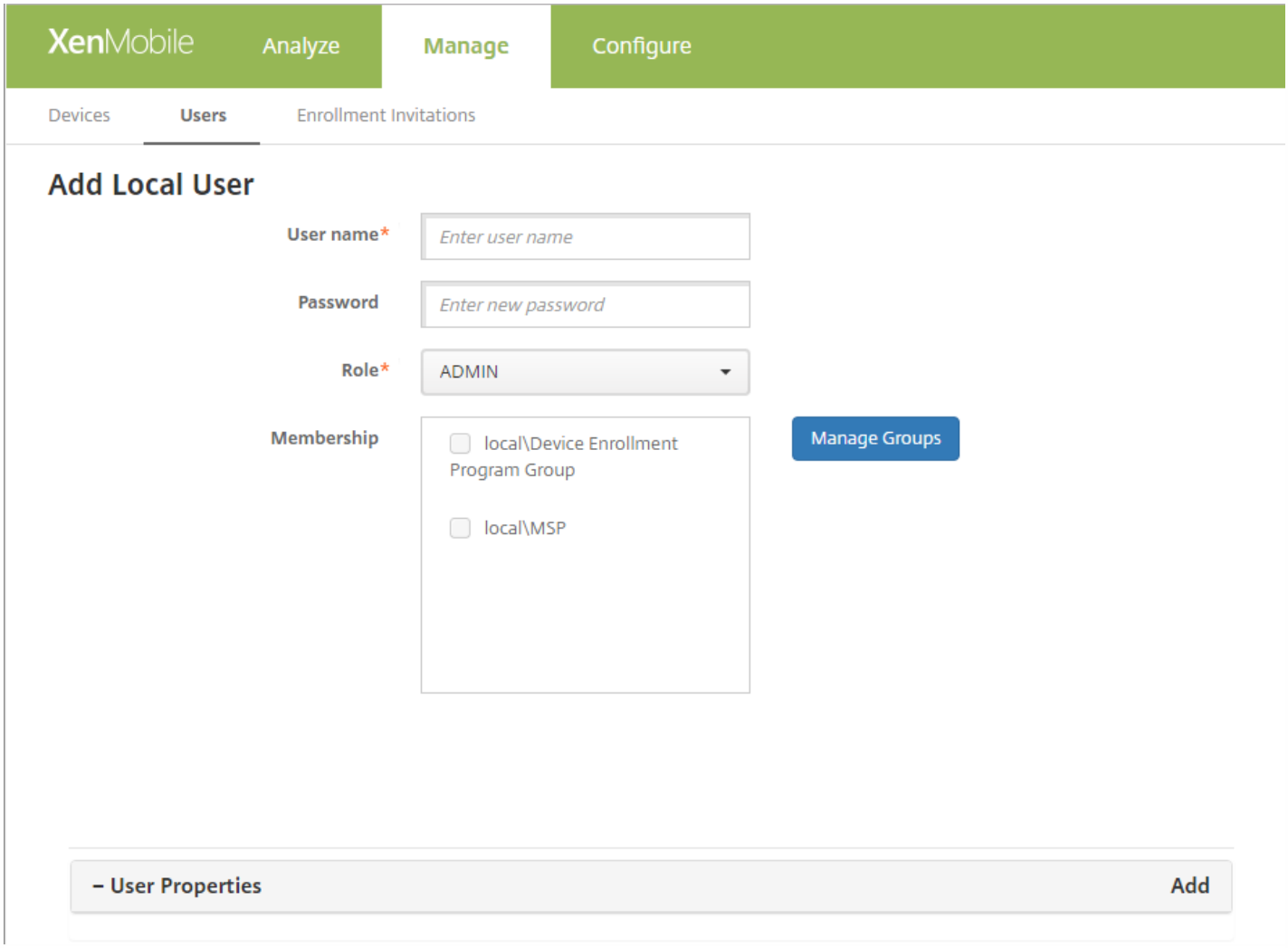
Puede agregar cuentas de usuario local a XenMobile de forma manual, o bien puede usar un archivo de aprovisionamiento para importar las cuentas. Consulte "Para importar cuentas de usuario mediante un archivo de aprovisionamiento CSV" para obtener información acerca de los pasos necesarios para importar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

1. En la consola de XenMobile, haga clic en **Manage** > **Users**. Aparecerá la página **Users**.



Para agregar una cuenta de usuario local

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



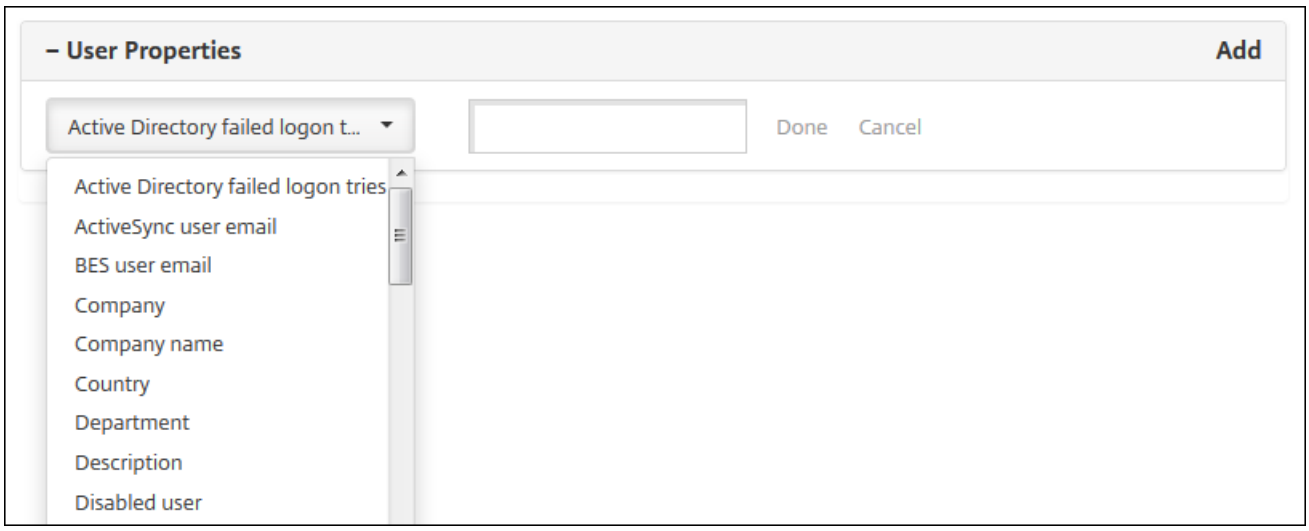
2. Configure estos parámetros:

- **User name**. Este es un campo obligatorio. Escriba el nombre. 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 información más detallada acerca de los roles, consulte Configuración de roles con RBAC. Las opciones posibles son:
  - ADMINISTRACIÓN
  - 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**.

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.

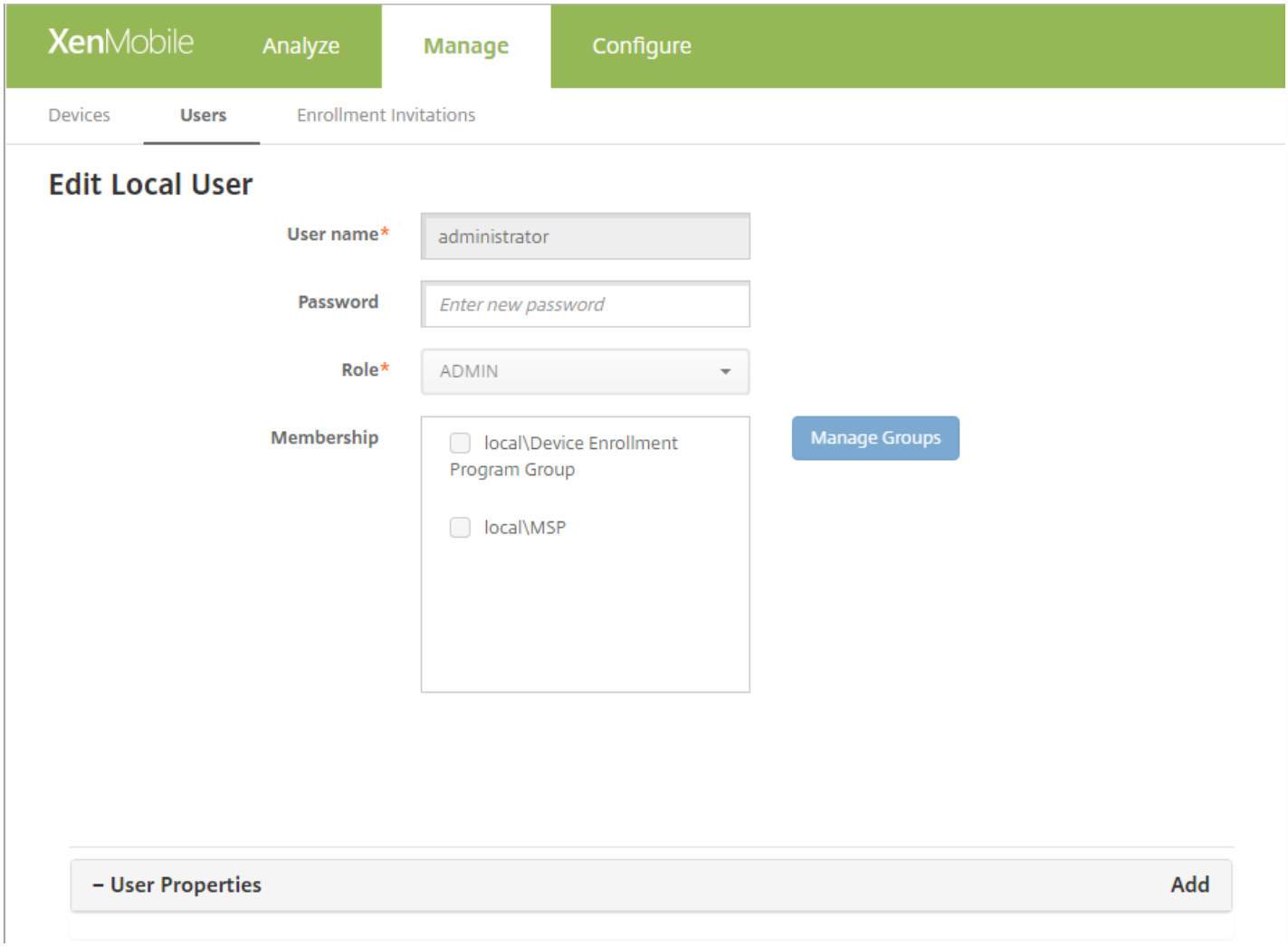
Para modificar una propiedad de usuario, haga clic en la propiedad y realice los cambios. Haga clic en **Done** para guardar los cambios de la lista o haga clic en **Cancel** para no realizar cambios en la lista.



3. Haga clic en **Save**.

Para modificar una cuenta de usuario local

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**.



2. Cambie la siguiente información como corresponda:

- **User name**. No 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 la cuenta de usuario o modificarla. Para quitar la cuenta de 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 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.

Para eliminar una cuenta de usuario local

1. En la página **Users**, en la lista de usuarios, seleccione al usuario.

Nota: Puede eliminar más de una cuenta de usuario. Para ello, deberá marcar la casilla de verificación situada junto a cada cuenta.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.

3. Haga clic en **Delete** para eliminar la cuenta de usuario o en **Cancel**.

Puede importar propiedades y cuentas de usuarios locales 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.

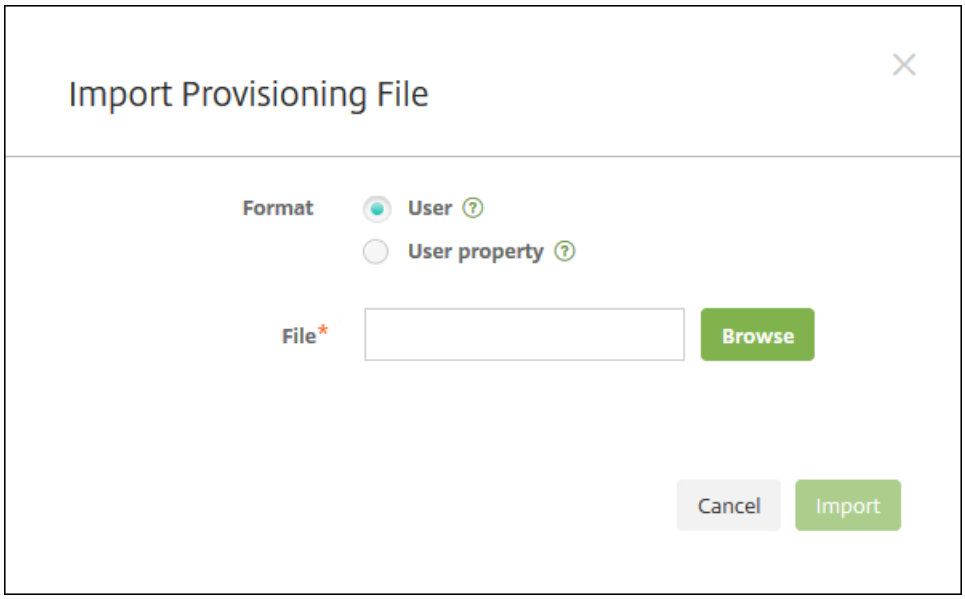
Nota:

- Para los usuarios locales, utilice el nombre de dominio junto con el nombre de usuario en el archivo de importación. Por ejemplo, especifique nombredeusuario@dominio. Si el usuario local que cree o importe es para un dominio administrado en XenMobile, ese usuario no podrá inscribirse mediante las credenciales LDAP correspondientes.
- Si importa cuentas de usuario al directorio interno de usuarios de XenMobile, inhabilite el dominio predeterminado para acelerar el proceso de importación. Tenga en cuenta que inhabilitar el dominio afecta a las inscripciones, por lo que debe volver a habilitar el dominio predeterminado una vez completada la importación de los usuarios internos.
- Los usuarios locales pueden estar en el formato de nombre principal de usuario (UPN). Sin embargo, Citrix recomienda que no utilice el dominio administrado. Por ejemplo, si se administra ejemplo.com, no cree un usuario local en 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**. Aparecerá 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**.

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 del archivo de aprovisionamiento de usuarios**: usuario;contraseña;rol;grupo1;grupo2
- **Campos del archivo de aprovisionamiento de atributos de usuario**: usuario;nombrePropiedad1;valorPropiedad1;nombrePropiedad2;valorPropiedad2

Nota:

- Separe los campos del archivo de aprovisionamiento por un punto y coma (;). Si parte de un campo contiene un punto y coma, debe anteponérsele 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 de **Role** son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE_PROVISIONING, además de cualquier otro rol que haya definido.
- Utilice el carácter de punto (.) como separador para crear la jerarquía de grupos. No use puntos en los nombres de grupo.
- En los archivos de aprovisionamiento de atributos, escriba los atributos de las propiedades en minúsculas. La base de datos distingue entre mayúsculas y minúsculas.

Ejemplo del contenido de un archivo de aprovisionamiento de usuarios

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

Ejemplo del contenido de un archivo de aprovisionamiento de atributos de usuario

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

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 hacer que algunos modos estén disponibles en 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**.

Las invitaciones de inscripción se envían desde la página **Manage** > **Enrollment**. Para obtener información, consulte Envío de una invitación de inscripción.

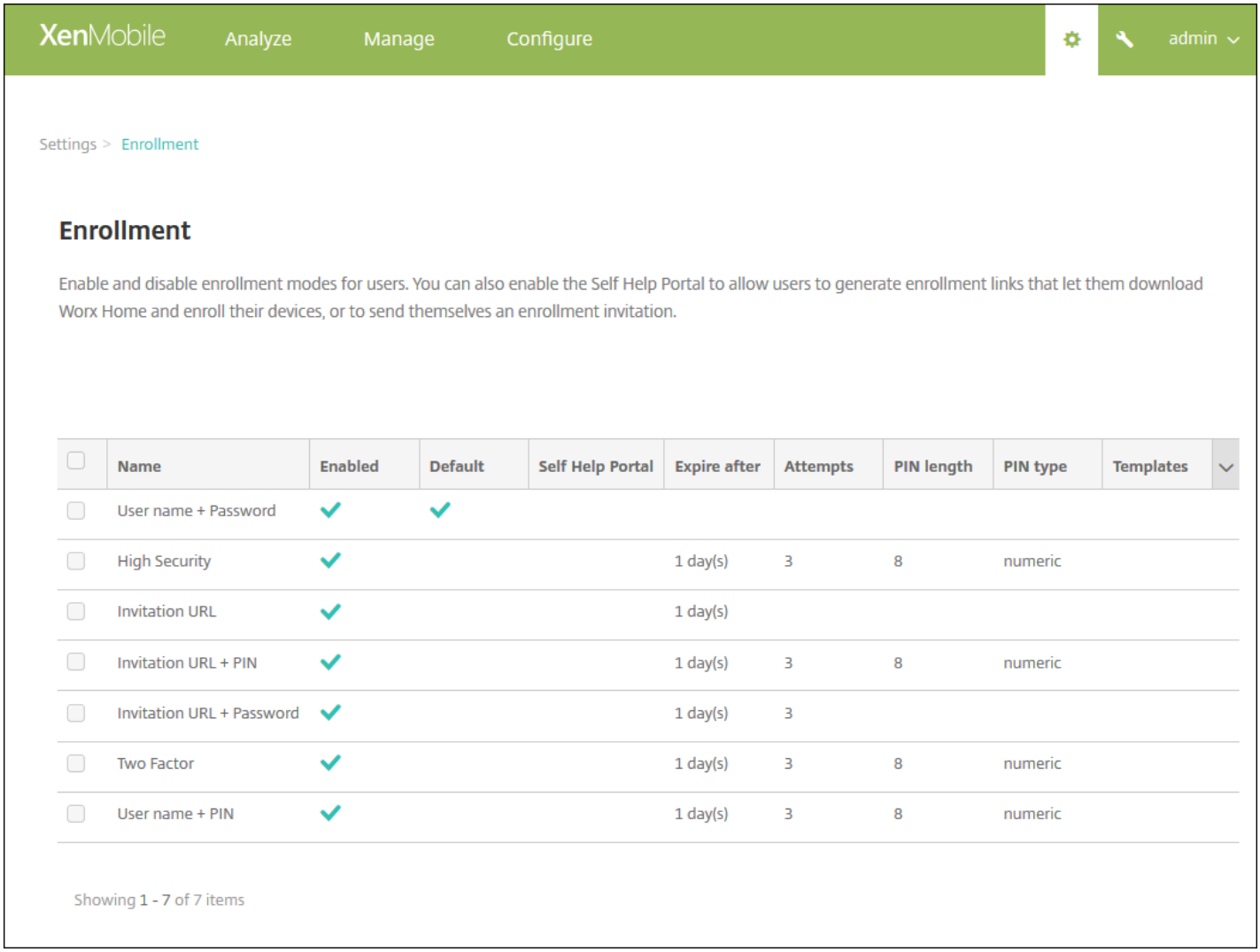
Nota: Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Creación o actualización de plantillas de notificaciones.

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. A continuación, establezca ese modo como predeterminado, inhabilítelo, o bien permita a los usuarios acceder a él a través del portal Self Help Portal.

Nota: Cuando marca la casilla de verificación situada junto a un modo de inscripción, el menú de opciones aparece encima de la lista de los modos de inscripción. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.



Elija entre estos modos de inscripción:

- Nombre de usuario y contraseña
- 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 y PIN

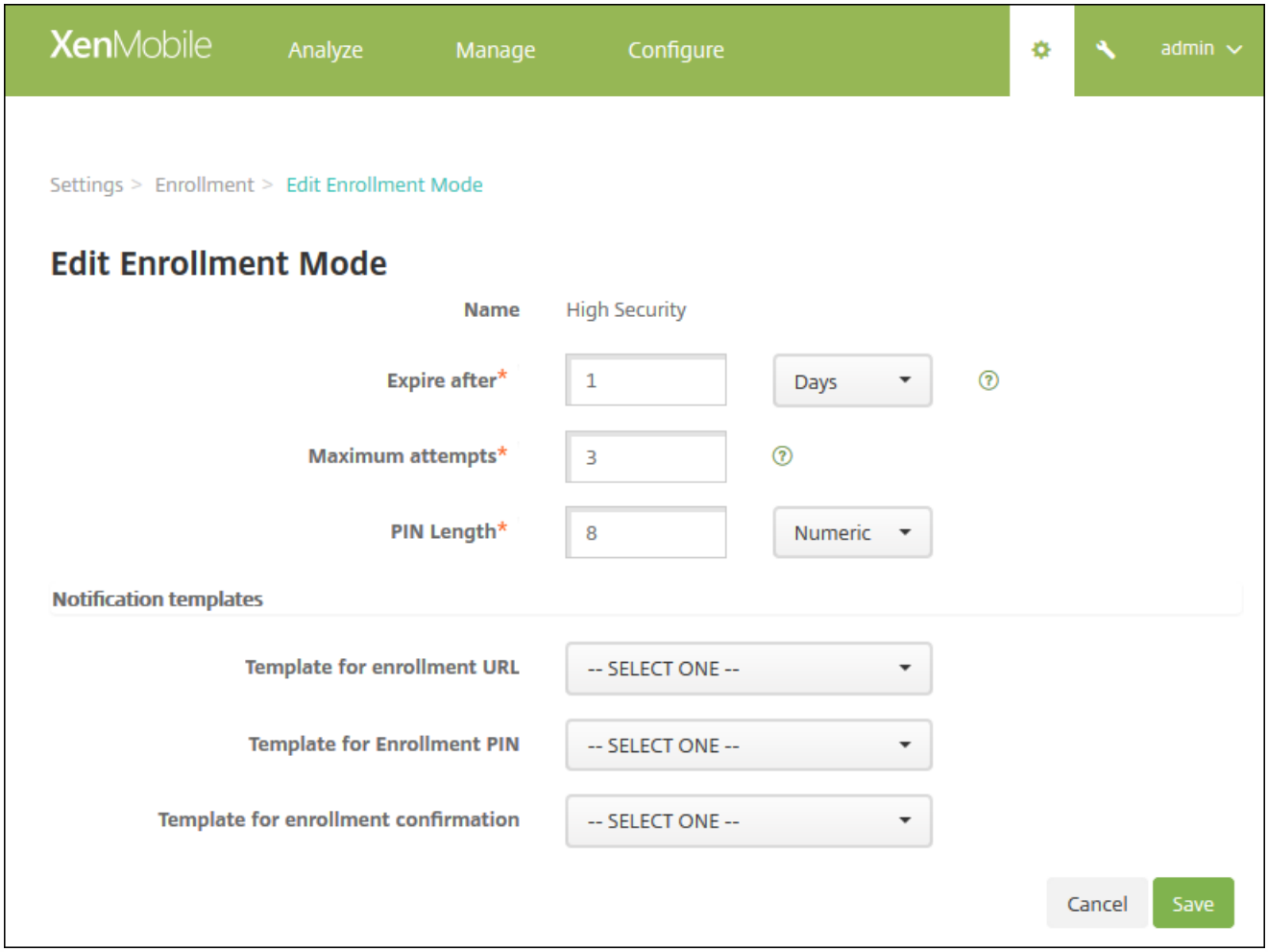
Puede utilizar las invitaciones de inscripción para restringir la inscripción a los usuarios que tengan una invitación.

Puede usar invitaciones de inscripción única (OTP) con PIN como una solución de dos factores. Con las invitaciones de inscripción OTP, puede controlar la cantidad de dispositivos que puede inscribir un usuario.

Para entornos con requerimientos muy altos de seguridad, puede asociar las invitaciones de inscripción a un dispositivo por UDID/SN/EMEI. También hay una opción de dos factores que consiste en solicitar la contraseña de Active Directory y OTP.

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 definir la longitud del PIN generado.
- **Numeric**. En la lista, haga clic en **Numeric** o **Alphanumeric** para el tipo de PIN.
- **Plantillas de notificaciones**:
  - **Template for Enrollment URL**. En la lista, seleccione una plantilla para la URL de inscripción. Por ejemplo, la plantilla de invitación a la inscripción envía a los usuarios un correo electrónico o SMS. El método depende de cómo haya

configurado la plantilla que les permite inscribir sus dispositivos en XenMobile. Para obtener más información acerca de las 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: Los únicos modos de inscripción que puede usar como predeterminados son **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: Para utilizar un modo como predeterminado, primero debe habilitarlo.

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.

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.

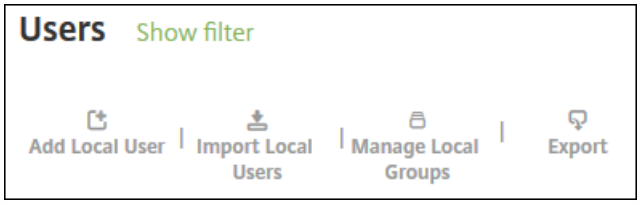
Puede administrar grupos desde el cuadro de diálogo **Manage Groups** de la consola de XenMobile. Puede ver este cuadro en las páginas **Users**, **Add Local User** o **Edit Local User**. No hay ningún comando de modificación de grupos.

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 los usuarios con 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.

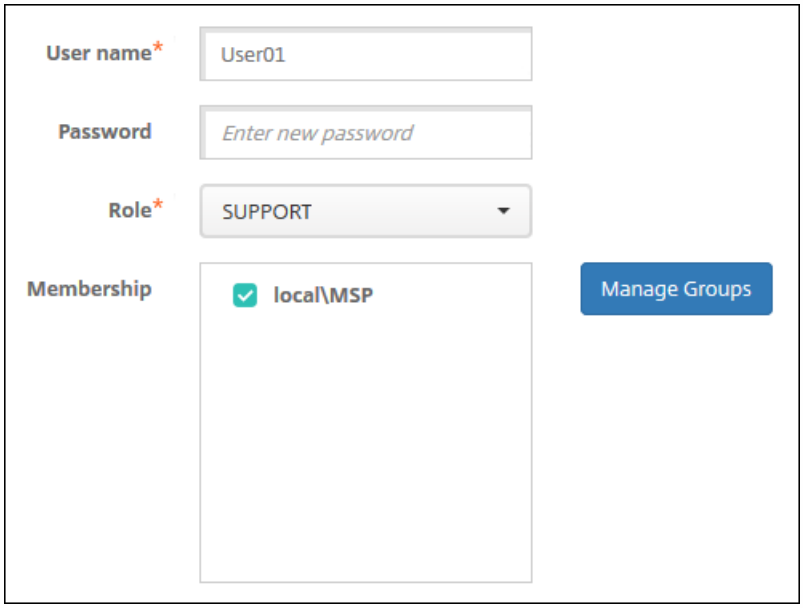
Para agregar un grupo local

1. Lleve a cabo una de las siguientes acciones:

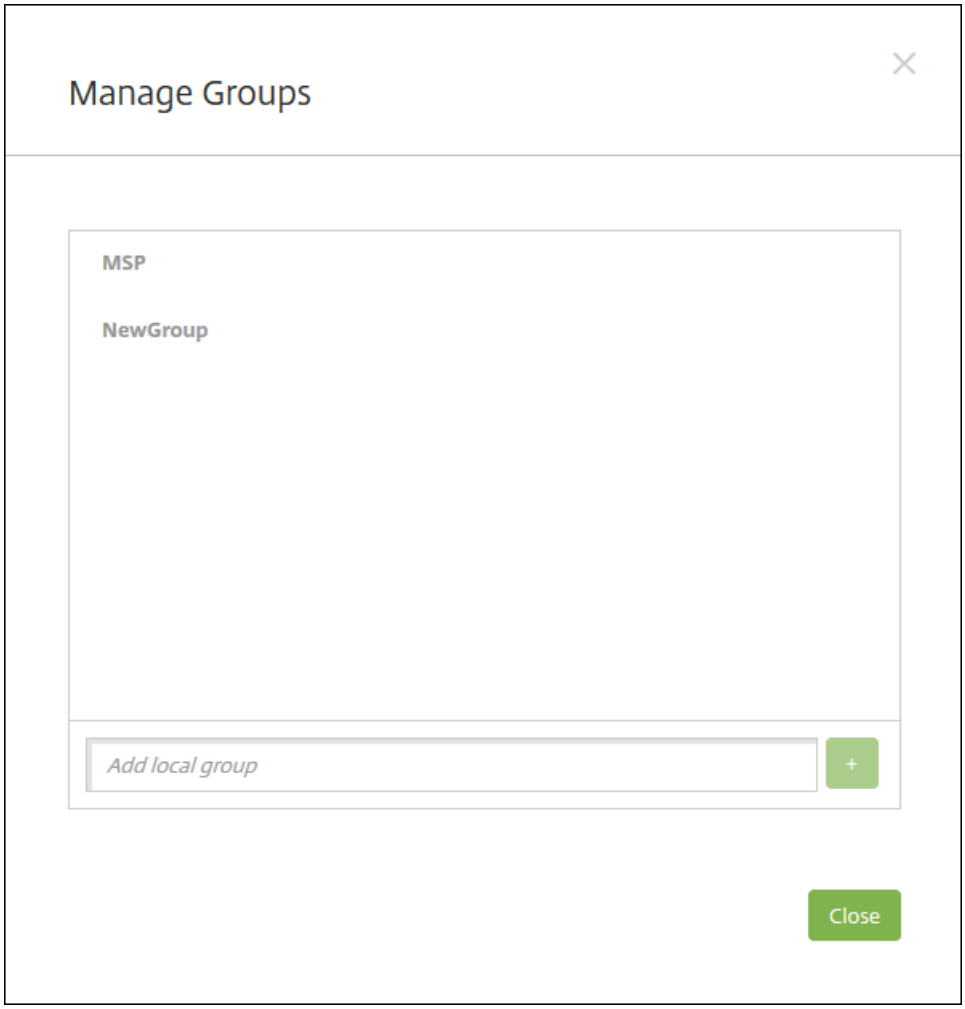
- En la página **Users**, haga clic en **Manage Local Groups**.



- 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. Debajo de 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**.

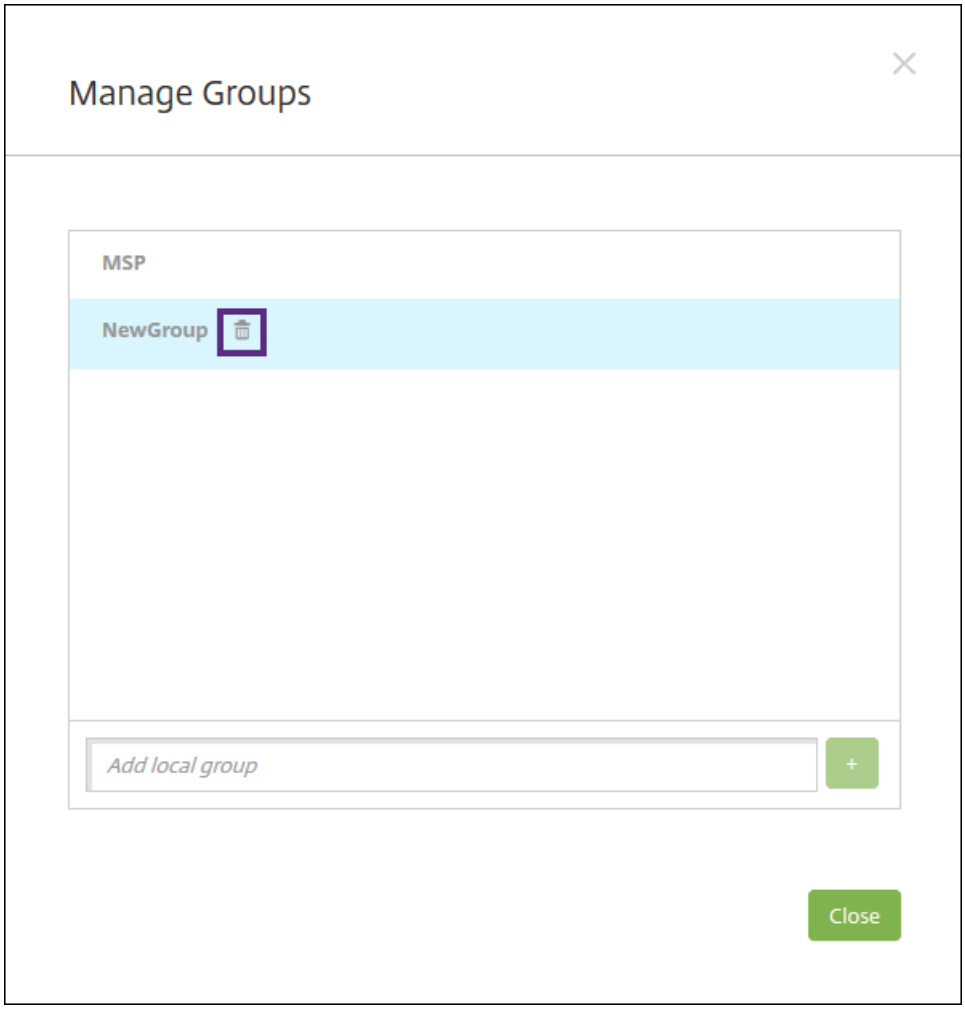
Para quitar un grupo

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**.

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.

Al configurar XenMobile por primera vez, se definen los parámetros de correo electrónico referentes al flujo de trabajo; estos parámetros se deben establecer antes de utilizar los 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.

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 usarlos 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 solicitudes de cuentas 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 otras personas aprueben la cuenta de usuario, puede buscar y seleccionar aprobadores adicionales por nombre o dirección de correo electrónico. Cuando XenMobile los encuentre, podrá agregarlos 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 el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

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

3. Haga clic en **Add**. Aparecerá la página **Add Workflow**.

4. Configure estos 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 al flujo de trabajo. En la consola de XenMobile, puede crear plantillas de correo electrónico desde la sección **Notification Templates**, en **Settings**. Al hacer clic en el icono con forma de ojo situado a la derecha del campo, aparece una vista previa de la plantilla que desea configurar.

- **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:
  - No se necesita
  - 1 nivel
  - 2 niveles
  - 3 niveles
- **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 aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Selected additional required approvers**.
  - Para quitar un nombre de la lista, siga uno de estos procedimientos:
    - 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 situada junto a cada nombre que quiera quitar.

5. 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 otros aprobadores, cree otro 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 concreto. Para ello, haga clic en la fila de la tabla o marque la casilla situada junto al flujo de trabajo.

2. Para eliminar un flujo de trabajo, haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Delete**.

Importante: Esta operación no se puede deshacer.

Configuración de roles con RBAC

Apr 07, 2017

Cada rol predefinido 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 los permisos predeterminados para cada rol integrado, descargue Role-Based Access Control Defaults.

Aplicar permisos equivale a definir los grupos de usuarios que el rol RBAC tiene el permiso de administrar. Tenga en cuenta que el administrador predeterminado no puede cambiar los parámetros de los permisos aplicados; de forma predeterminada, los permisos aplicados se refieren a todos los grupos de usuarios.

Cuando *asigna*, asigna el rol RBAC a un grupo, de modo que el grupo de usuarios posee los derechos de administrador de RBAC.

Rol de administrador

Rol de aprovisionamiento de dispositivos

Rol de asistencia

Rol de usuario

Configuración de roles con RBAC

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:

- **Administrador**. Concede acceso completo al sistema.
- **Aprovisionamiento de dispositivos**. Concede acceso a tareas básicas de administración de dispositivos para dispositivos Windows CE.
- **Asistencia técnica**. Concede acceso para la asistencia remota.
- **Usuario**. 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.

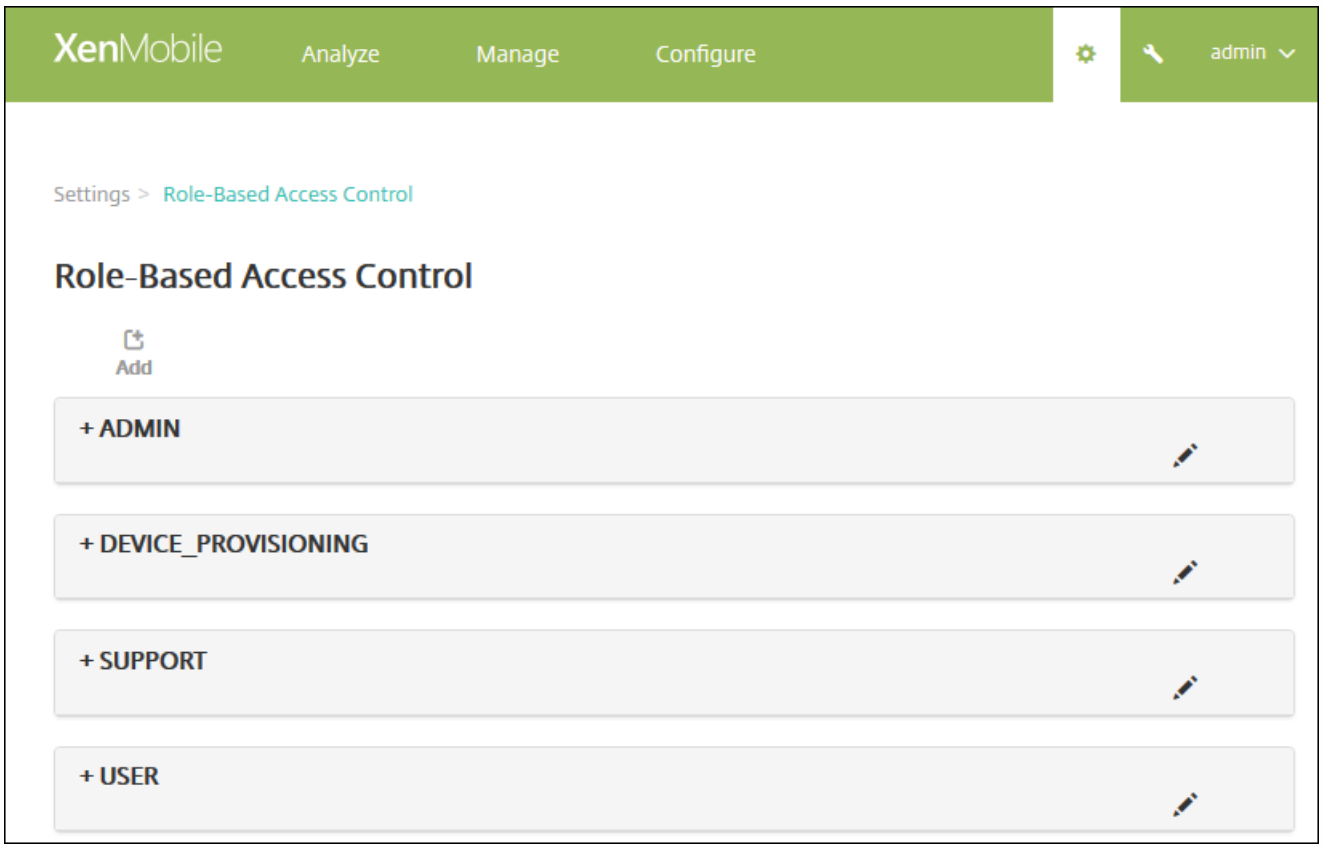
Nota: Los usuarios locales solo pueden tener un rol asignado.

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.

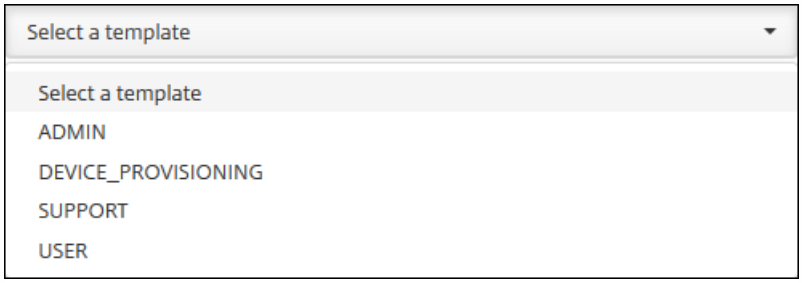
3. Haga clic en **Add** para agregar un nuevo rol de usuario. También puede hacer clic en el icono de lápiz situado a la derecha de un rol existente para modificarlo, y puede hacer clic en el icono de papelera situado a la derecha de un rol previamente definido para eliminarlo. No se pueden eliminar los roles de usuario predeterminados.

- Si hace clic en **Add** o en el icono de lápiz, aparecerá 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.

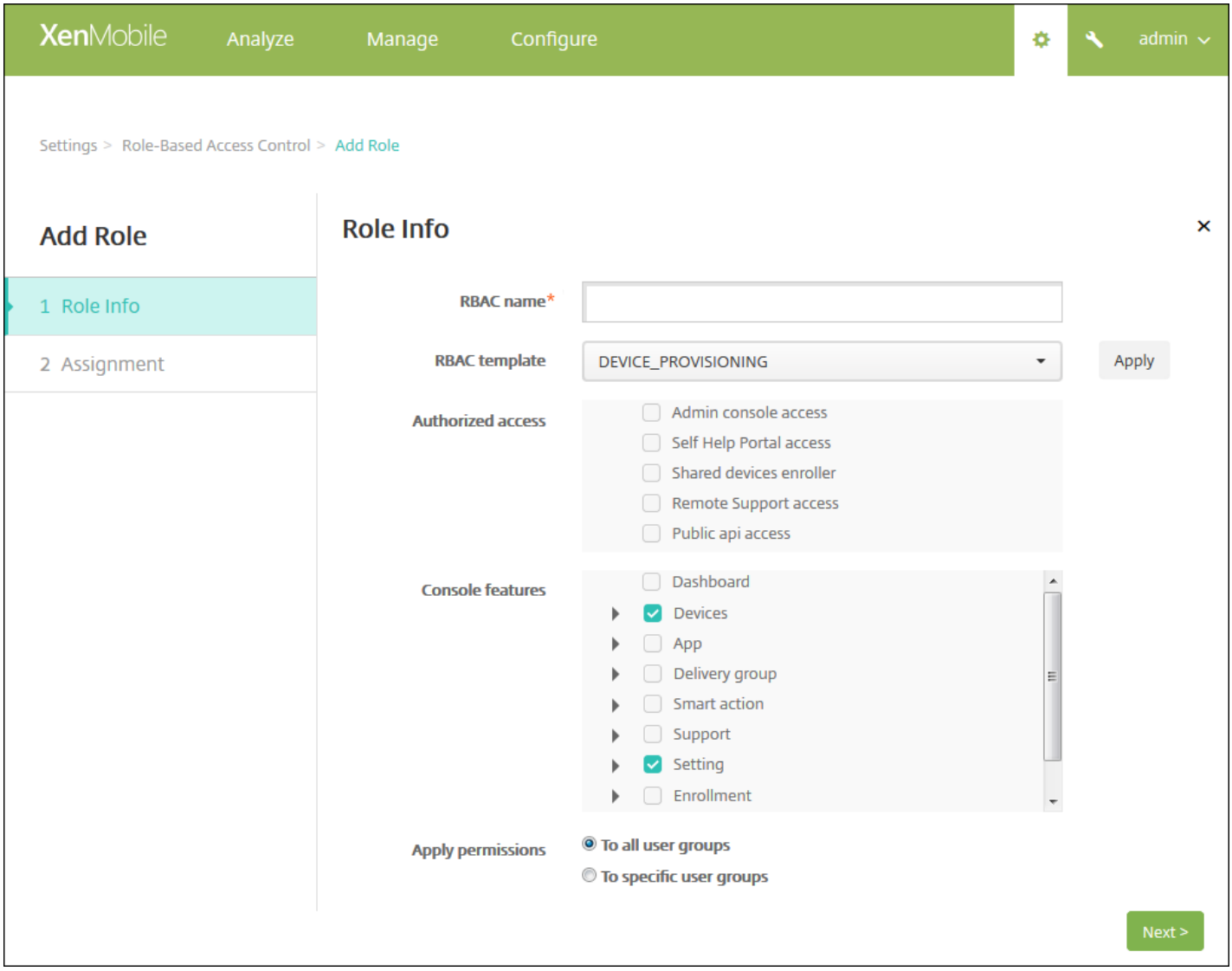
4. Escriba la siguiente información para crear un nuevo rol de usuario o para modificar un rol de usuario existente:

- **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**.

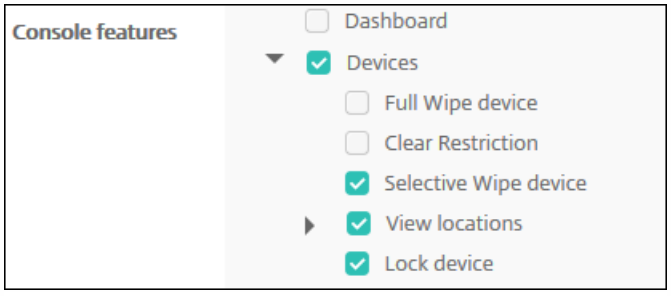


5. Haga clic en **Apply**, situado a la derecha del campo **RBAC template**, para rellenar las casillas **Authorized access** y **Console features** con los permisos concedidos de funciones y acceso predefinidos para la plantilla seleccionada.



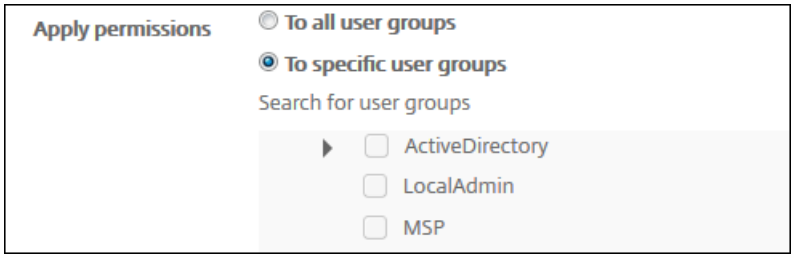
6. Marque y desmarque las casillas de verificación de **Authorized access** y **Console features** para personalizar el rol.

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 imagen 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.

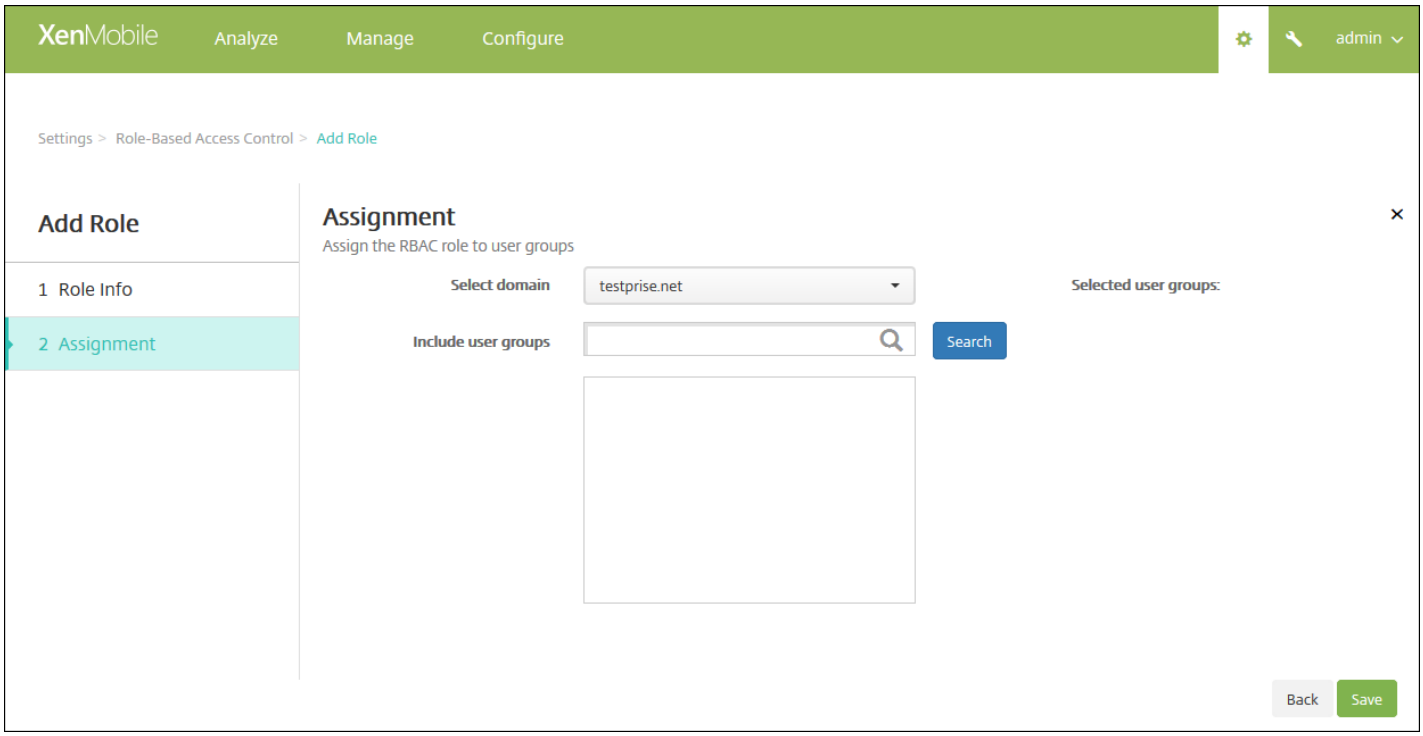


7. **Apply permissions**. Marque los grupos a los que aplicar los permisos seleccionados. Si hace clic en **To specific user**

groups, aparecerá una lista de grupos. De esa lista, puede seleccionar un grupo o varios.

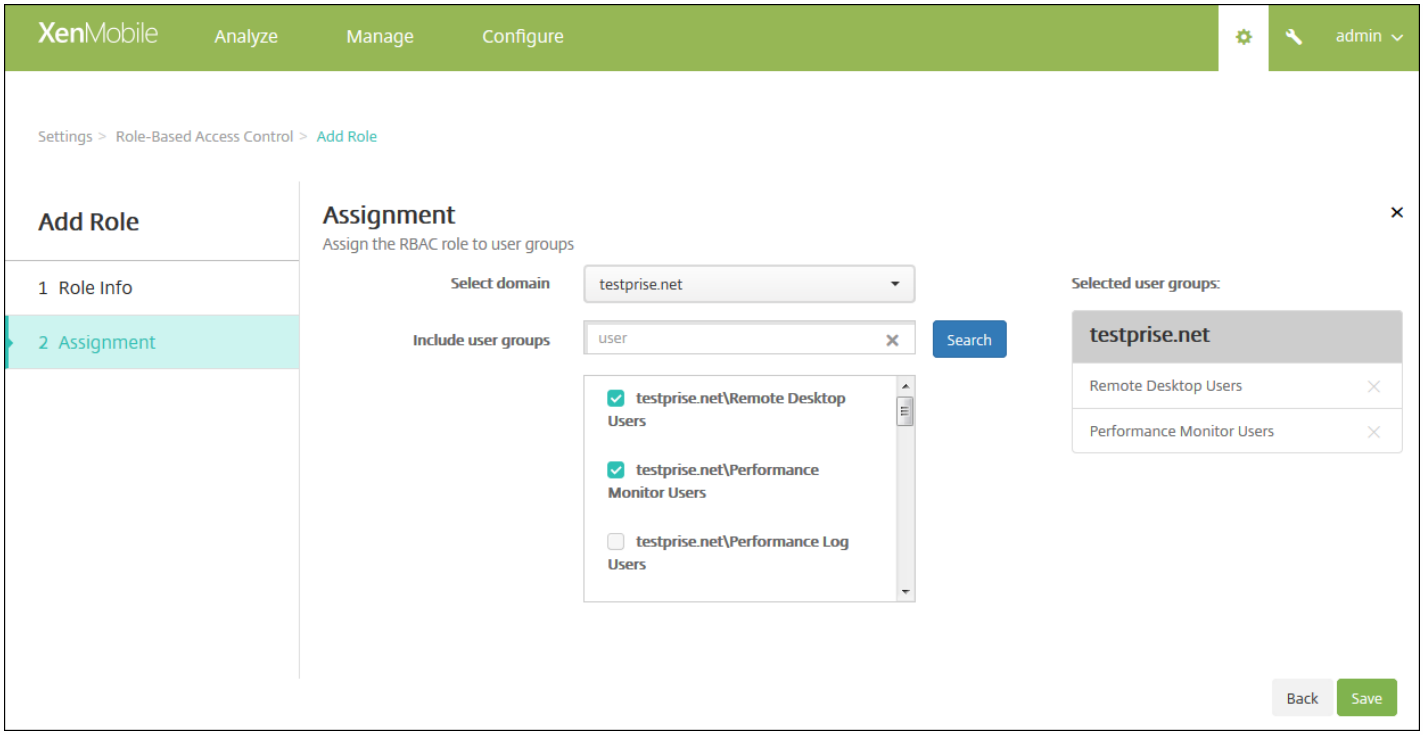


8. Haga clic en **Next**. Aparecerá la página **Assignment**.



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, este 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**.

Notificaciones

Feb 27, 2017

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.
- Para notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se den ciertas condiciones. Por ejemplo:
  - Cuando está a punto de bloquearse el acceso por parte de un dispositivo de usuario al dominio de empresa debido a un problema de cumplimiento de normativas.
  - Cuando el dispositivo se ha liberado por jailbreak o root.

  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. SMS 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.

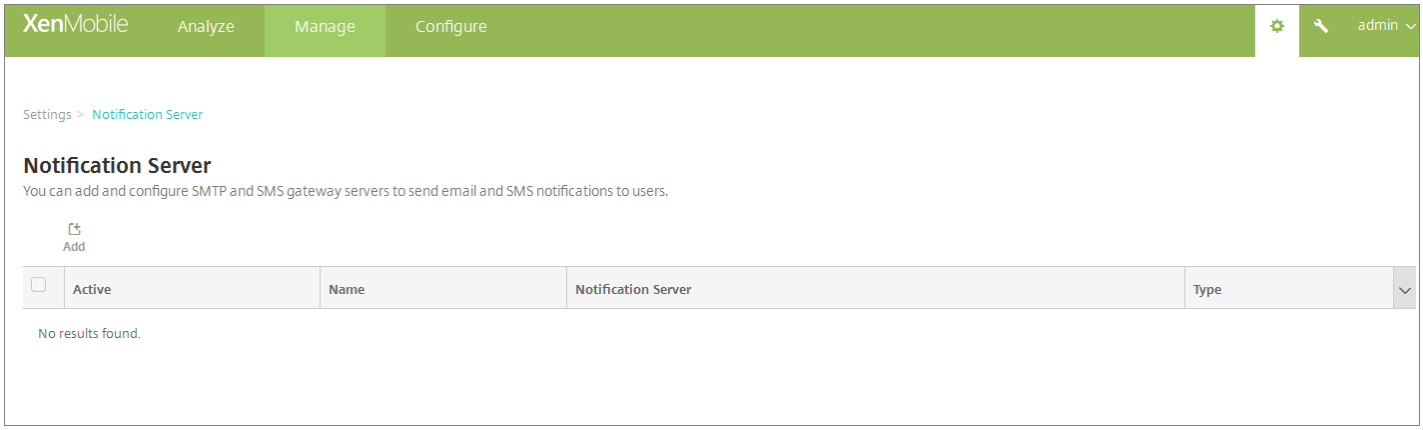
- Antes de configurar la puerta de enlace SMS, acuda al administrador del sistema para obtener la información del servidor. Es importante saber si el servidor SMS está alojado en un servidor interno de la empresa o si el servidor forma parte de un servicio de correo electrónico alojado (en servidores externos). En este último 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 se trata de un servidor del servicio de correo electrónico, busque la información de configuración en el sitio Web del proveedor del servicio.

- Debe haber 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. Esto permite que XenMobile envíe correctamente las notificaciones.

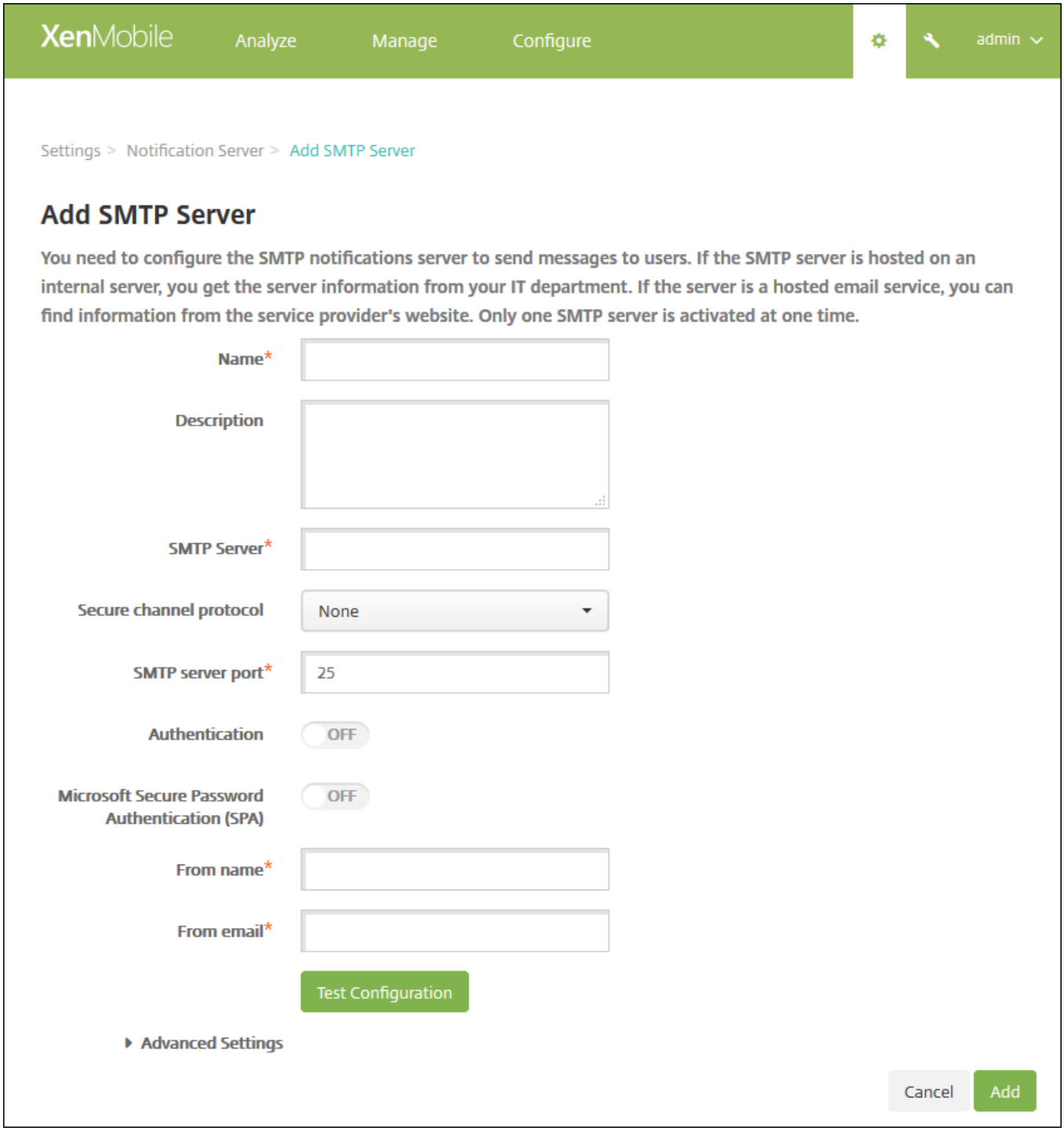
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

2. 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 estos 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.

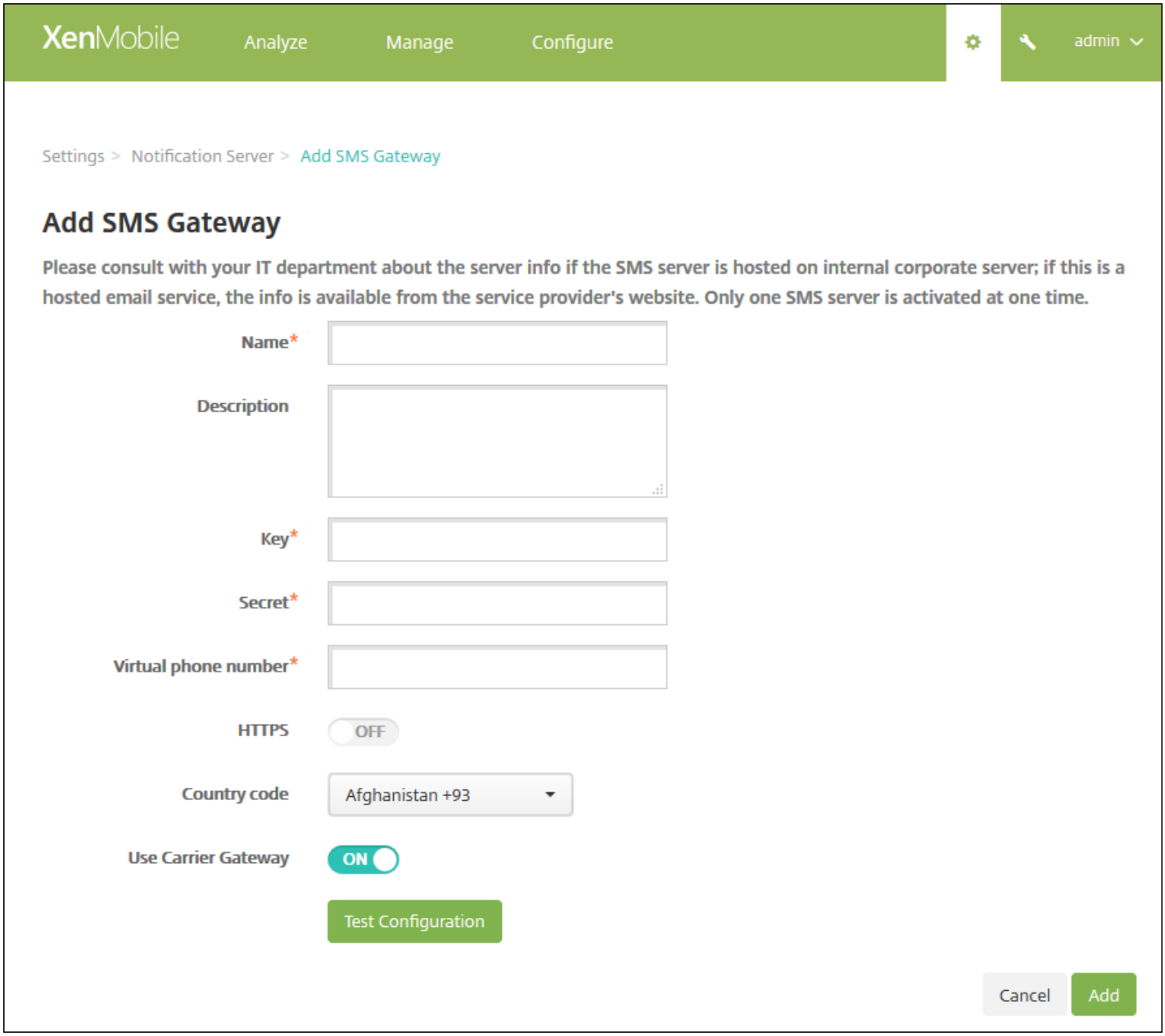
- **Authentication**. Seleccione **ON** u **OFF**. El valor predeterminado es **OFF**.
- Si habilita **Authentication**, configure los siguientes parámetros:
  - **User name**. Escriba el nombre de usuario que se usará para la autenticación.
  - **Password**. Escriba la contraseña de autenticación del 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. De forma predeterminada, se establecen 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 y debe usar solo dígitos en este campo. 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**.

  Importante: Deje "HTTPS" establecido en el valor **ON**, a menos que reciba instrucciones de la Asistencia de Citrix para darle el valor **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**.

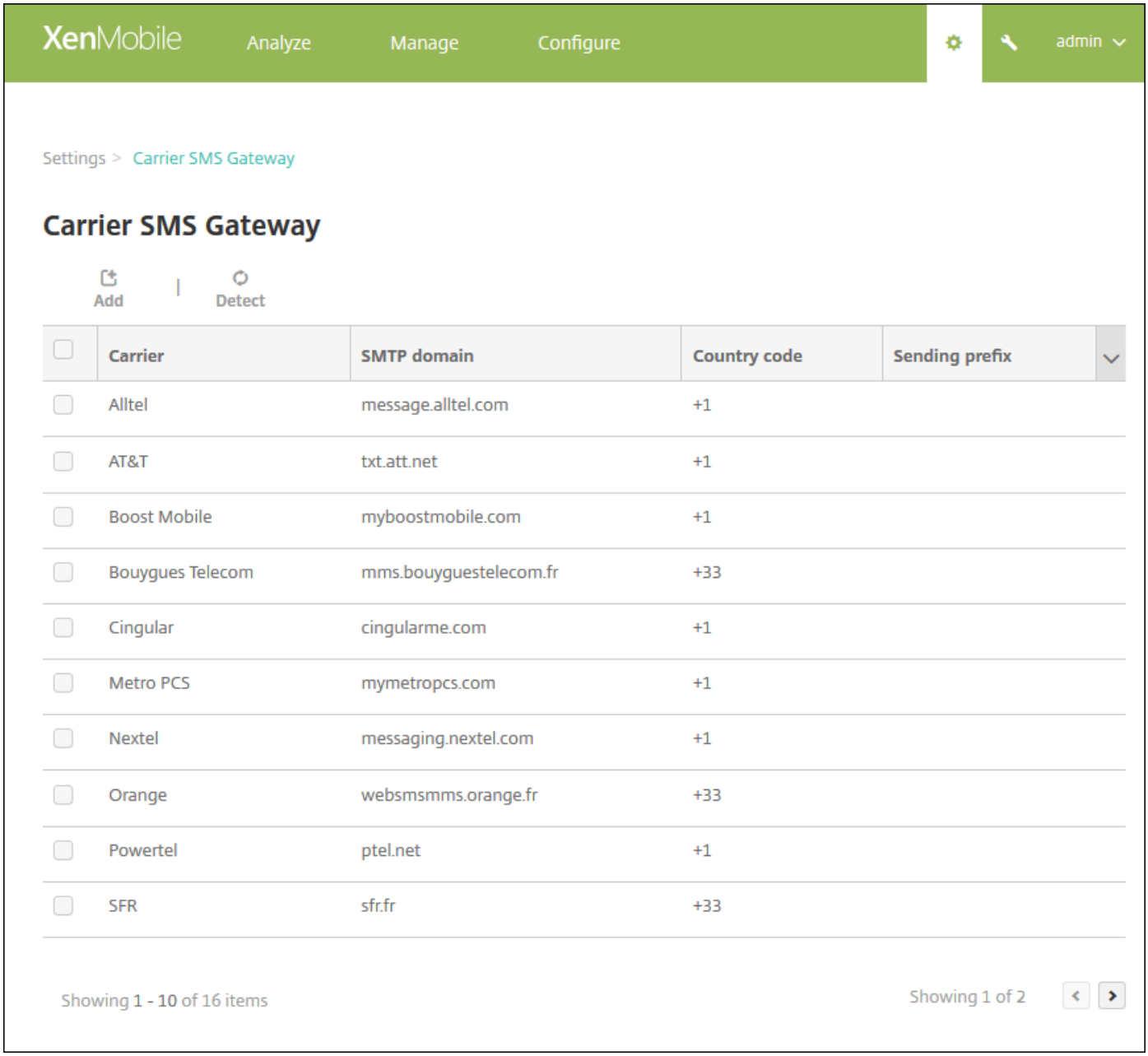
2. Haga clic en **Test Configuration** para enviar un mensaje de prueba con la configuración actual. Los errores de conexión, como aquellos relacionados con errores de autenticación o de números de teléfono virtual, se detectan y aparecen inmediatamente. Los mensajes se reciben en el mismo período de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

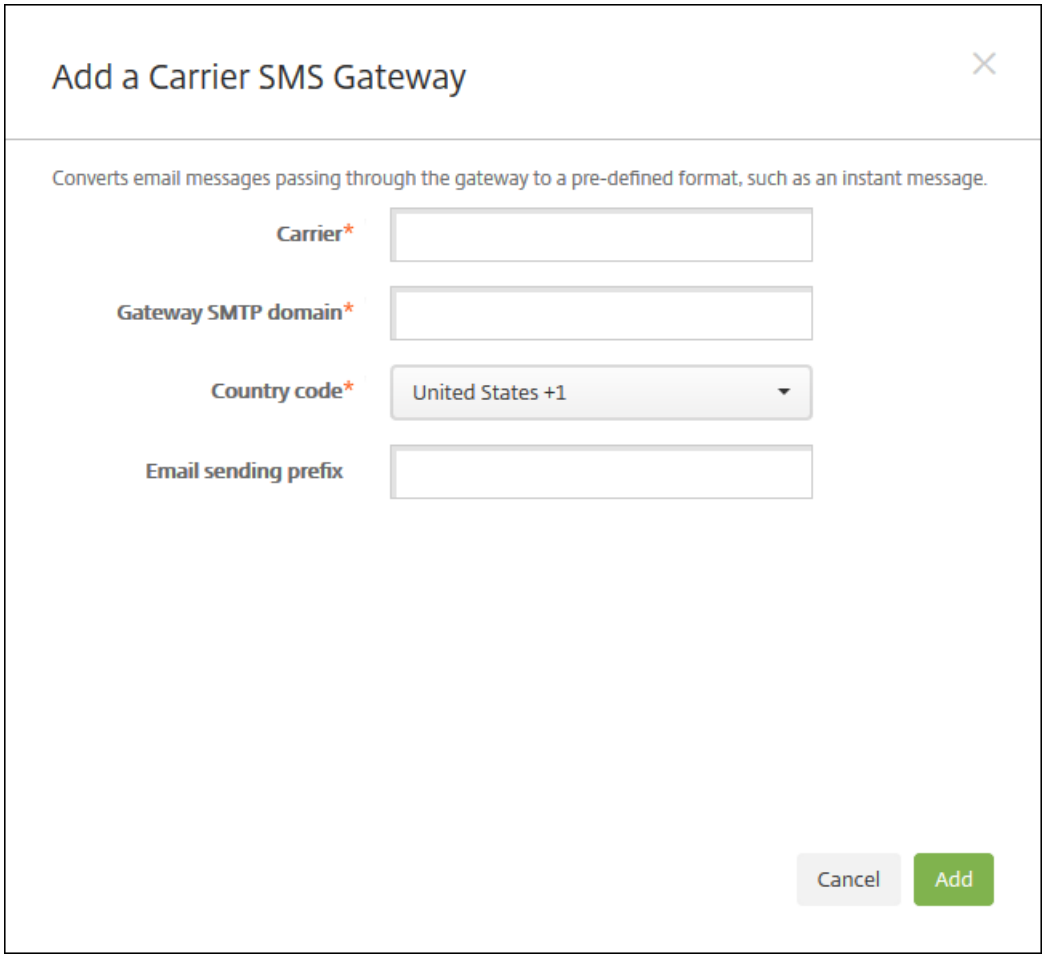
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

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 estos 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.

Creación y actualización de plantillas de notificación

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: Secure Hub, SMTP o SMS.

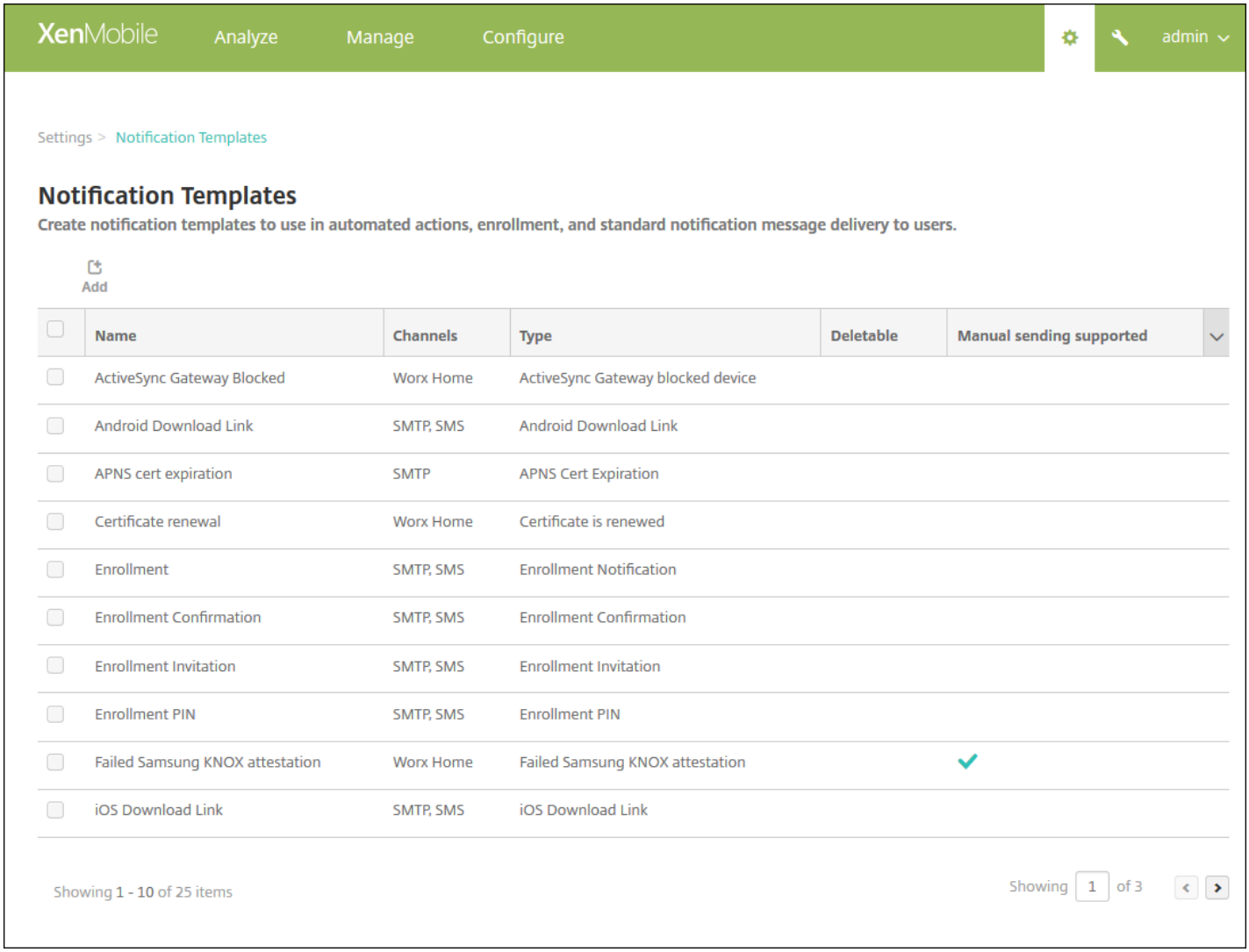
XenMobile incluye varias plantillas de notificaciones predefinidas, las cuales reflejan los distintos tipos de eventos a los que XenMobile responde automáticamente en relación a cada dispositivo del sistema.

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.

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.

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 notificaciones.

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 estos 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" (Se admite el envío manual) debajo del tipo. Lo que 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 para esta notificación. Puede elegir un canal cualquiera o todos. Los canales que seleccione dependen de la forma en que quiera enviar notificaciones:

- Si elige **Secure Hub**, 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 deberían 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.

Secure Hub:

- **Activate**. Haga clic para habilitar el canal de notificación.
- **Message**. Escriba el mensaje que se enviará al usuario. Este campo es necesario si usa Secure Hub.
- **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 concretos en esta página, o bien puede seleccionar los dispositivos desde la página **Manage** > **Devices** y enviar notificaciones desde allí. Para obtener más información, consulte Dispositivos.
- **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 por 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 Secure Hub. Los canales configurados incorrectamente aparecen después de los canales configurados correctamente.

Para modificar una plantilla de notificaciones

1. Seleccione una plantilla de notificaciones. Aparecerá la página de modificación de la plantilla en cuestión. En ella, podrá realizar cambios en todos los campos salvo en **Type**; tampoco podrá activar ni desactivar canales.

2. Haga clic en **Save**.

Para eliminar una plantilla de notificaciones

Nota: Solo puede eliminar las plantillas de notificaciones que haya agregado; no puede eliminar plantillas predeterminadas de notificaciones.

1. Seleccione una plantilla de notificaciones existente.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.

2. Haga clic en **Delete** para eliminar la plantilla de notificaciones o en **Cancel** para cancelar la operación.

Dispositivos

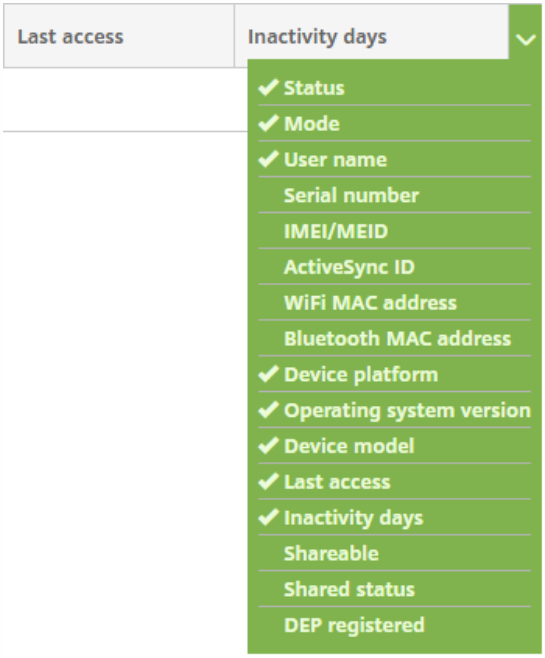
Feb 27, 2017

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, se ofrece una lista de cada dispositivo y la siguiente información:

- **Status** (Los iconos indican el estado de implementación, si está administrado, si ha sido liberado por jailbreak y si ActiveSync Gateway está disponible)
- **Mode** (Si el modo del dispositivo es MDM, MAM o ambos)
- Se ofrece otra información del dispositivo, como **User name**, **Device platform**, **Operating system version**, **Device model**, **Last access** e **Inactivity days**. Estos son los encabezados predeterminados que aparecen.

Puede personalizar lo que aparece en la tabla **Devices**. Para ello, haga clic en la flecha hacia abajo del último encabezado y, a continuación, seleccione los encabezados adicionales que quiera mostrar en la tabla o elimine los que no.



Puede agregar dispositivos manualmente, importar dispositivos desde un archivo de aprovisionamiento de dispositivos, modificar los detalles de los dispositivos, realizar acciones para aumentar la seguridad del dispositivo, enviar notificaciones a dispositivos y eliminar dispositivos. También puede exportar todos los datos de la tabla de dispositivos a un archivo CSV para generar un informe personalizado. El servidor exporta todos los atributos de dispositivo y, si se aplican filtros, XenMobile los tendrá en cuenta al crear el archivo CSV.

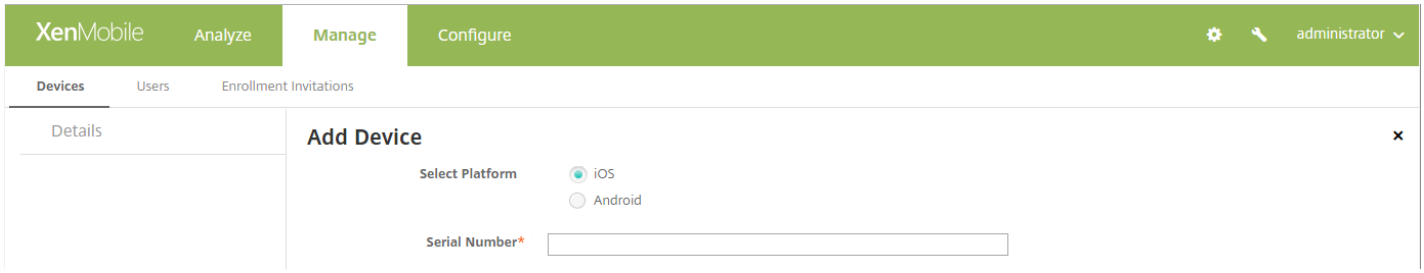
Consulte las secciones siguientes para obtener más información sobre la administración de dispositivos:

- Cómo agregar dispositivos manualmente
- Importación de dispositivos desde un archivo de aprovisionamiento de dispositivos

- Realización de acciones de seguridad
- Envío de una notificación a los dispositivos
- Eliminación de dispositivos
- Exportación de la tabla Devices
- Etiquetado manual los dispositivos del usuario
- Formatos del archivo de aprovisionamiento de dispositivos
- Valores y nombres de propiedades de dispositivo

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**.

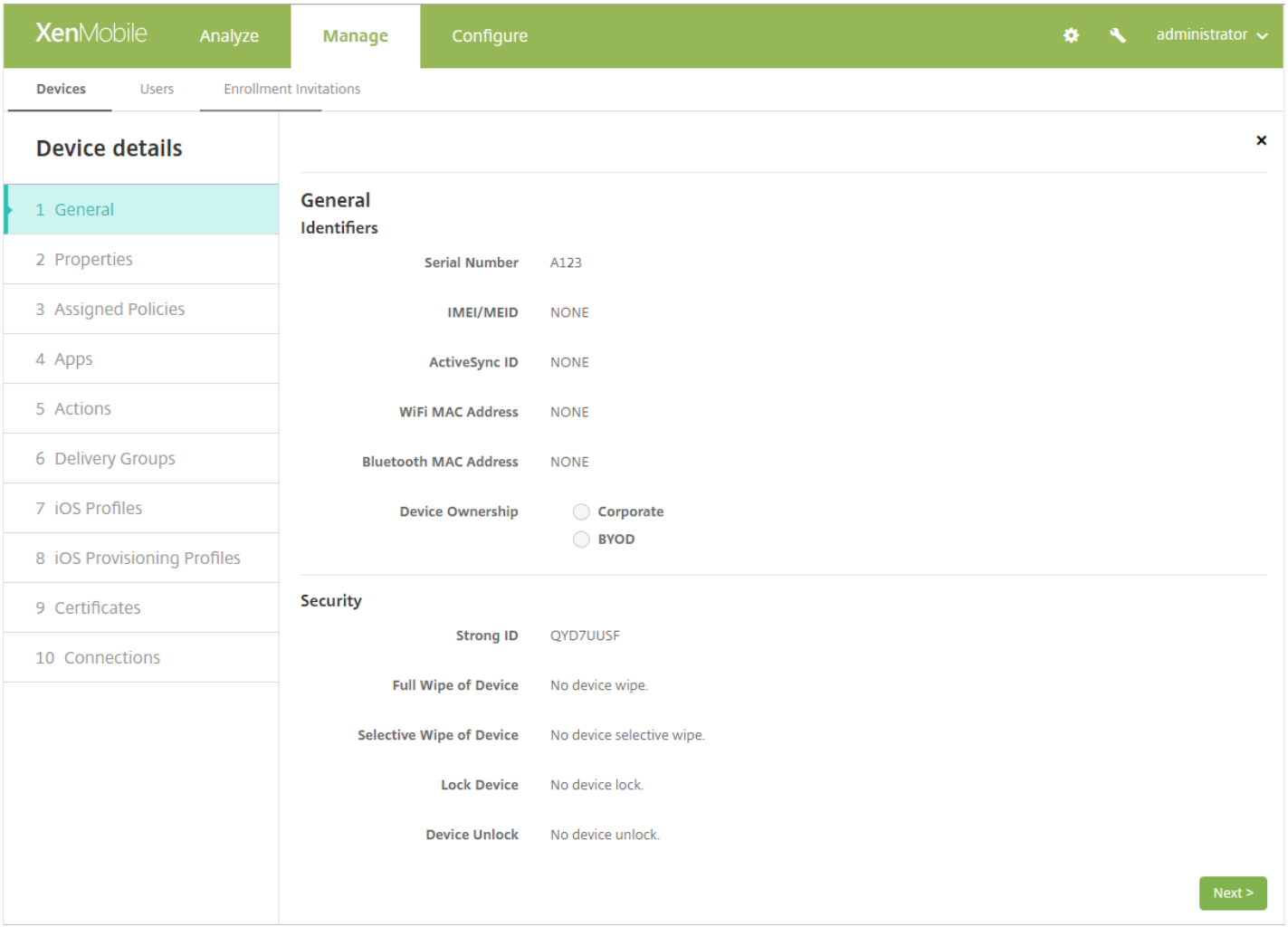


3. Configure estos parámetros:

- **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. La página **General** muestra una lista de los **identificadores** de dispositivo, como el número de serie, el ID de ActiveSync y otra información en función del tipo de plataforma. Para **Device Ownership**, seleccione **Corporate** o **BYOD**.

Asimismo, la página **General** muestra una lista de las propiedades de **seguridad** de que está dotado el dispositivo, como el ID seguro, el bloqueo del dispositivo y la omisión del bloqueo de activación, así como otra información en función del tipo de plataforma.

6. La página **Properties** muestra una lista de las propiedades del dispositivo que aprovisionará XenMobile. La lista contiene todas las propiedades de dispositivo incluidas en el archivo de aprovisionamiento utilizado para agregar el dispositivo. Para agregar una propiedad, haga clic en **Add** y, a continuación, seleccione una propiedad de la lista. Para saber cuáles son los valores válidos para cada propiedad, consulte Valores y nombres de propiedades de dispositivo en este artículo.

Cuando se agrega una propiedad, esta aparece inicialmente en la categoría donde se haya agregado. Después de hacer clic en **Next** y volver a la página **Properties**, la propiedad aparece en la lista apropiada.

Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa (**X**) situada en el lado derecho. XenMobile elimina inmediatamente el elemento.

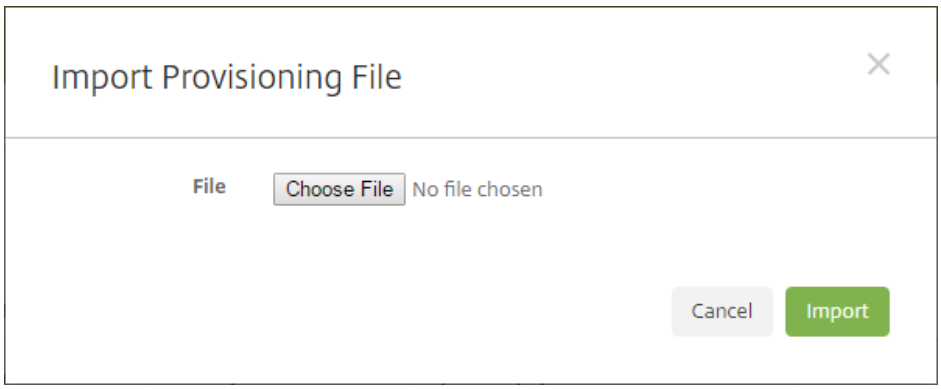
7. Las secciones restantes de **Device Details** contienen información resumida acerca del dispositivo.

- **Assigned Policies**. Muestra la cantidad de directivas asignadas, incluidas las directivas implementadas, pendientes y erróneas. También muestra el nombre, el tipo y la última información implementada de cada directiva.

- **Apps**. Muestra la cantidad de aplicaciones instaladas, pendientes y erróneas según el último inventario. Indica el nombre de la aplicación, el identificador y el tipo, entre otros datos.
- **Actions**. Muestra la cantidad de acciones implementadas, pendientes y erróneas. Indica el nombre de la acción y la hora de la última implementación.
- **Delivery Groups**. Muestra la cantidad de grupos de entrega correctos, pendientes y erróneos. Indica el nombre del grupo de entrega y la hora de cada implementación. Seleccione un grupo de entrega para ver información más detallada (como el estado, la acción, el canal o el usuario).
- **iOS Profiles**. Muestra el último inventario de perfiles iOS, que incluiye el nombre, el tipo, la organización y la descripción.
- **iOS Provisioning Profiles**. Muestra información acerca del perfil de aprovisionamiento utilizado por la empresa para la distribución (como el UUID, la fecha de caducidad y si se administra o no).
- **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 los días que quedan hasta la caducidad.
- **Connections**. Muestra los estados de la primera y la última conexión. Para cada conexión, aparecen el nombre de usuario, así como la hora de las dos últimas autenticaciones (la penúltima y la última).
- **TouchDown** (solo para dispositivos Android). Muestra información acerca de la última autenticación del dispositivo y el último usuario autenticado. Aparecen los nombres y los valores de todas las directivas aplicables.

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. Para obtener más información, consulte Formatos del archivo de aprovisionamiento de dispositivos en este artículo.

1. Vaya a **Manage > Devices** y haga clic en **Import**. Aparecerá el cuadro de diálogo **Import Provisioning File**.



2. Haga clic en **Choose File** y, a continuación, vaya al archivo que quiere importar.

3. Haga clic en **Import**. El archivo importado aparecerá en la tabla **Devices**.

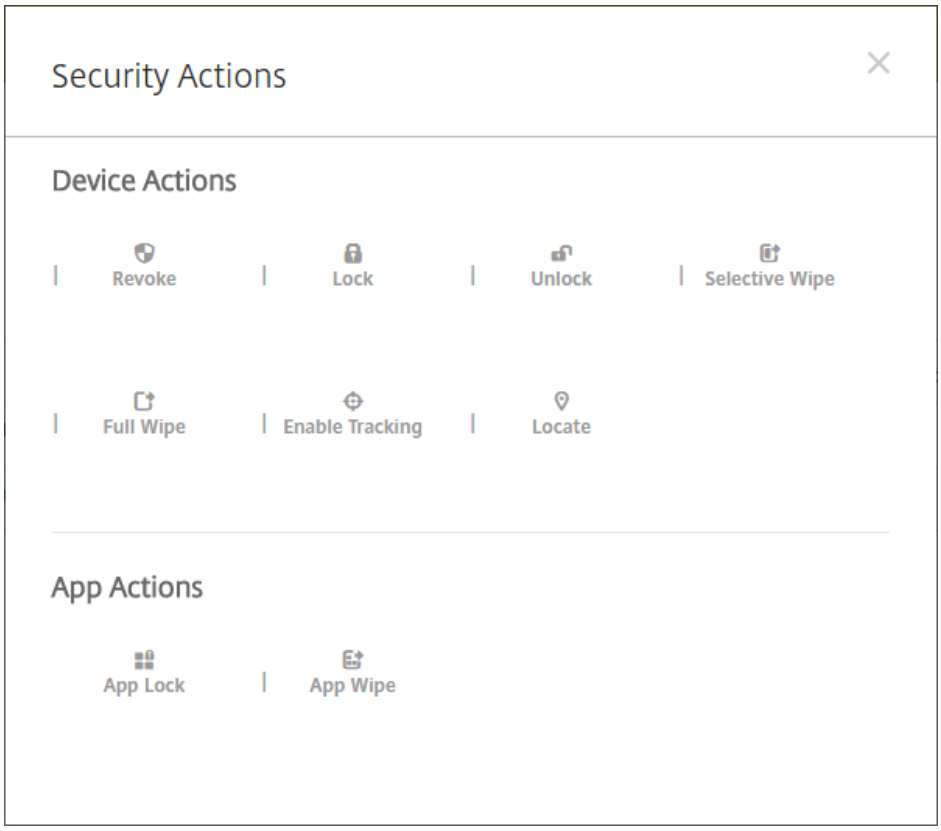
4. Para modificar la información del dispositivo, selecciónelo y, a continuación, haga clic en **Edit**. Para obtener información sobre las páginas **Device details**, consulte Cómo agregar un dispositivo manualmente.

Puede realizar acciones de seguridad en dispositivos y aplicaciones desde la página **Devices**. Las acciones en dispositivos son: revocar, bloquear, desbloquear y borrar. Las acciones de seguridad en las aplicaciones son: bloquear y borrar.

1. En la página **Manage > Devices**, seleccione un dispositivo y haga clic en **Secure**.

2. En **Security Actions**, haga clic en una acción y responda a lo que le solicite el sistema.

Para obtener información detallada acerca de las acciones, consulte Acciones automatizadas.



Para realizar manualmente un bloqueo, desbloqueo, borrado o cancelación de borrado de aplicaciones

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

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

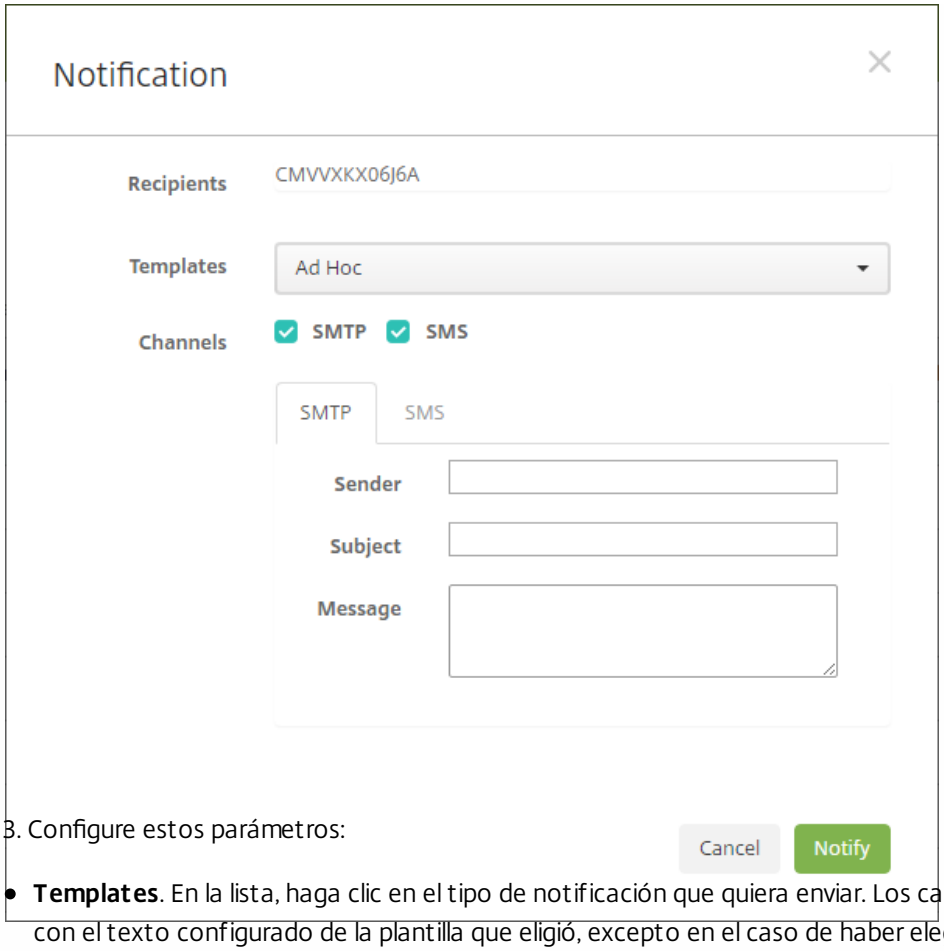
Nota: También puede utilizar este cuadro de diálogo para comprobar el estado del dispositivo de un usuario que usted sepa que está inhabilitado o ha sido eliminado de Active Directory. La presencia de las acciones App Unlock o App Unwipe indican que las aplicaciones de los usuarios están siendo borradas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

3. Confirme la acción.

Puede enviar notificaciones a los dispositivos desde la página Devices. Para obtener más información acerca de las notificaciones, consulte Notificaciones.

1. En la página **Manage > Devices**, 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 estos 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** y **SMS**. Haga clic en las fichas para ver el formato del mensaje para 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**.

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**. Esta operación no se puede deshacer.

1. Filtre la tabla **Devices** según lo que quiera que aparezca en el archivo de exportación.

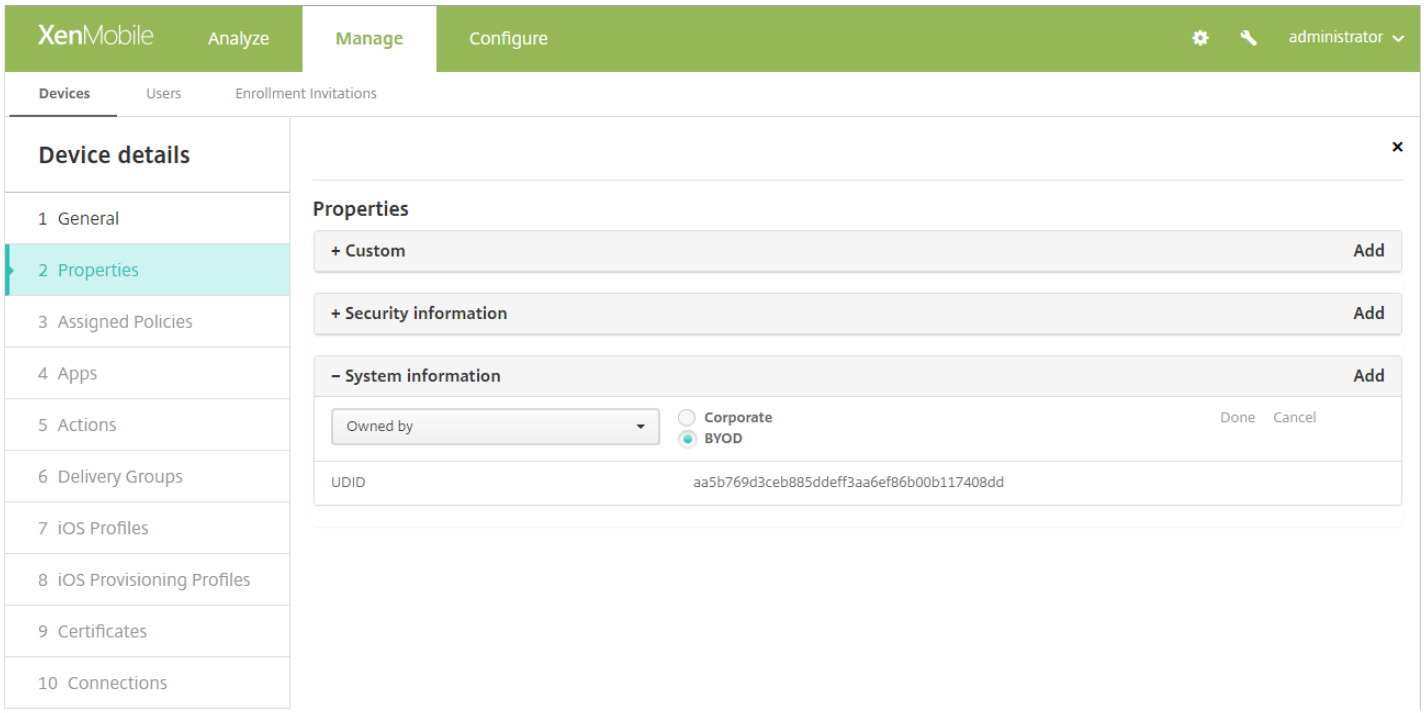
2. Haga clic en el botón **Export** situado sobre la tabla **Devices**. XenMobile extrae la información de la tabla **Devices** y la convierte a un archivo CSV.

3. Cuando se le solicite, abra o guarde el archivo CSV. El modo de hacer esto dependerá del explorador Web que se esté utilizando. También puede cancelar la operación.

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

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

Notas:

- Para conocer los nombres y los valores de las propiedades, consulte "Valores y nombres de propiedades de dispositivo" en la

sección siguiente.

- Use el conjunto de caracteres UTF-8.
- Use un punto y coma (;) para separar los campos que contenga el archivo de aprovisionamiento. Si parte de un campo contiene un punto y coma, debe anteponérsele un carácter de barra diagonal inversa (\).

  Por ejemplo, para esta propiedad:
  propertyV;test;1;2

  Se debe anteponer así:
  propertyV\;test\;1\;2

- El número de serie es obligatorio para dispositivos iOS porque es el identificador del dispositivo iOS.
- Para otras plataformas de dispositivos, se debe incluir el número de serie o el IMEI.
- Los valores válidos para **OperatingSystemFamily** son: **WINDOWS**, **ANDROID** o **iOS**.

```
1050BF3F51730108161006551059039 1;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F51730108161006551059039 2;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F51730108161006551059039 3;35244201625379903;iOS;test;

4050BF3F51730108161006551059039 3;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;
```

Cada línea del archivo describe un dispositivo. La primera entrada del ejemplo significa lo siguiente:

- SerialNumber: 1050BF3F5173010816100655105903 91
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Valores y nombres de propiedades de dispositivo

Nombre de la propiedad en la página Manage > Devices	Nombre y valores del archivo de aprovisionamiento de dispositivos	Tipo de valor
¿Está AIK presente?	WINDOWS_HAS_AIK_PRESENT	Cadena

¿Cuenta suspendida?	GOOGLE_AW_DIRECTORY_SUSPENDED	Cadena
Código de omisión del bloqueo de activación	ACTIVATION_LOCK_BYPASS_CODE	Cadena
Bloqueo de activación habilitado	ACTIVATION_LOCK_ENABLED Significado de los valores: 1 (Sí) 0 (No)	Booleano
Cuenta de iTunes activa	ACTIVE_ITUNES Significado de los valores: 1 (Sí) 0 (No)	Booleano
ID de ActiveSync	EXCHANGE_ACTIVESYNC_ID	Cadena
Dispositivo ActiveSync conocido por MSP	AS_DEVICE_KNOWN_BY_ZMSP Significado de los valores: 1 (True) 0 (False)	Booleano
Administrador inhabilitado	ADMIN_DISABLED Significado de los valores: 1 (Sí) 0 (No)	Booleano
API MDM de Amazon disponible	AMAZON_MDM Significado de los valores: 1 (True) 0 (False)	Booleano
ID del dispositivo Android for Work	GOOGLE_AW_DEVICE_ID	Cadena
¿Dispositivo habilitado para Android for Work?	GOOGLE_AW_ENABLED_DEVICE	Cadena
Tipo de instalación de Android for Work	GOOGLE_AW_INSTALL_TYPE Valores:	Cadena

	DeviceAdministrator (Propietario del dispositivo) AvengerManagedProfile (Dispositivo administrado de trabajo) ManagedProfile (Perfil de trabajo)	
Etiqueta de inventario	ASSET_TAG	Cadena
Estado de la actualización automática	AUTOUPDATE_STATUS	Cadena
RAM disponible	MEMORY_AVAILABLE	Número entero
Espacio de almacenamiento disponible	TOTAL_DISK_SPACE	Número entero
Información de BIOS	BIOS_INFO	Cadena
Batería de reserva	BACKUP_BATTERY_PERCENT	Número entero
Versión de banda base de firmware	MODEM_FIRMWARE_VERSION	Cadena
Estado de la batería	BATTERY_STATUS	Cadena
Carga de batería	BATTERY_CHARGING Significado de los valores: 1 (True) 0 (False)	Booleano
Dispositivo BES conocido por MSP	BES_DEVICE_KNOWN_BY_ZMSP Significado de los valores: 1 (True) 0 (False)	Booleano
PIN de BES	BES_PIN	Cadena
ID del agente del servidor BES	ENROLLMENT_AGENT_ID	Cadena
Nombre del servidor BES	BES_SERVER	Cadena
Versión del servidor BES	BES_VERSION	Cadena

BitLockerStatus	WINDOWS_HAS_BIT_LOCKER_STATUS	Cadena
Dirección MAC de Bluetooth	BLUETOOTH_MAC	Cadena
¿Depuración de arranque habilitada?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	Cadena
BootManagerRevListVersion	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	Cadena
Velocidad de reloj de CPU	CPU_CLOCK_SPEED	Número entero
Tipo de CPU	CPU_TYPE	Cadena
Versión de parámetros de operador	CARRIER_SETTINGS_VERSION	Cadena
Móvil: Latitud	GPS_LATITUDE_FROM_CELLULAR	Cadena
Móvil: Longitud	GPS_LONGITUDE_FROM_CELLULAR	Cadena
Tecnología del móvil	CELLULAR_TECHNOLOGY	Número entero
Móvil: Marca de hora	GPS_TIMESTAMP_FROM_CELLULAR	Fecha
¿Cambiar contraseña en el siguiente inicio de sesión?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	Cadena
ID del dispositivo cliente	CLIENT_DEVICE_ID	Cadena
Copia de seguridad en nube habilitada	CLOUD_BACKUP_ENABLED Significado de los valores: 1 (Sí) 0 (No)	Booleano
¿Integridad de código habilitada?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	Cadena
CodeIntegrityRevListVersion	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	Cadena
Color	COLOR	Cadena

Creado	GOOGLE_AW_DIRECTORY_CREATION_TIME	Cadena
Red del operador actual	CURRENT_CARRIER_NETWORK	Cadena
Código móvil de país actual	CURRENT_MCC	Número entero
Código móvil de red actual	CURRENT_MNC	Cadena
Nombre de la cuenta DEP	BULK_ENROLLMENT_DEP_ACCOUNT_NAME	Cadena
DEPPolicy	WINDOWS_HAS_DEP_POLICY	Cadena
Roaming de datos permitido	DATA_ROAMING_ENABLED Significado de los valores: 1 (Sí) 0 (No)	Booleano
Fecha de la última copia de seguridad en iCloud	LAST_CLOUD_BACKUP_DATE	Fecha
Descripción	DESCRIPCIÓN	Cadena
Perfil asignado de Device Enrollment Program	PROFILE_ASSIGN_TIME	Fecha
Perfil insertado de Device Enrollment Program	PROFILE_PUSH_TIME	Fecha
Perfil eliminado de Device Enrollment Program	PROFILE_REMOVE_TIME	Fecha
Registro de Device Enrollment Program realizado por	DEVICE_ASSIGNED_BY	Cadena
Fecha del registro de Device Enrollment Program	DEVICE_ASSIGNED_DATE	Fecha
Tipo de dispositivo	DEVICE_TYPE	Cadena

Modelo del dispositivo	MODEL_ID	Cadena
Nombre del dispositivo	DEVICE_NAME	Cadena
No Molestar activado	DO_NOT_DISTURB Significado de los valores: 1 (Sí) 0 (No)	Booleano
¿Controlador ELAM cargado?	WINDOWS_HAS_ELAM_DRIVER_LOADED	Cadena
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	Fecha
ID de empresa	ENTERPRISE_ID	Cadena
Almacenamiento externo 1: espacio disponible	EXTERNAL_STORAGE1_FREE_SPACE	Número entero
Almacenamiento externo 1: nombre	EXTERNAL_STORAGE1_NAME	Cadena
Almacenamiento externo 1: espacio total	EXTERNAL_STORAGE1_TOTAL_SPACE	Número entero
Almacenamiento externo 2: espacio disponible	EXTERNAL_STORAGE2_FREE_SPACE	Número entero
Almacenamiento externo 2: nombre	EXTERNAL_STORAGE2_NAME	Cadena
Almacenamiento externo 2: espacio total	EXTERNAL_STORAGE2_TOTAL_SPACE	Número entero
Almacenamiento externo cifrado	EXTERNAL_ENCRYPTION Significado de los valores: 1 (Sí) 0 (No)	Booleano
Estado del firewall	FIREWALL_STATUS	Cadena
Versión del firmware	FIRMWARE_VERSION	Cadena

Primera sincronización	ZMSP_FIRST_SYNC	Fecha
GPS: Altitud	GPS_ALTITUDE_FROM_GPS	Cadena
GPS: Latitud	GPS_LATITUDE_FROM_GPS	Cadena
GPS: Longitud	GPS_LONGITUDE_FROM_GPS	Cadena
GPS: Marca de hora	GPS_TIMESTAMP_FROM_GPS	Fecha
Alias de Directorio Google	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	Cadena
Nombre de familia del Directorio Google	GOOGLE_AW_DIRECTORY_FAMILY_NAME	Cadena
Nombre del Directorio Google	GOOGLE_AW_DIRECTORY_NAME	Cadena
Correo electrónico principal de Directorio Google	GOOGLE_AW_DIRECTORY_PRIMARY	Cadena
ID del usuario de Directorio Google	GOOGLE_AW_DIRECTORY_USER_ID	Cadena
HAS_CONTAINER	HAS_CONTAINER Significado de los valores: 1 (Sí) 0 (No)	Booleano
Versión de API de HTC	HTC_MDM_VERSION	Cadena
API MDM de HTC disponible	HTC_MDM Significado de los valores: 1 (Sí) 0 (No)	Booleano
Capacidades de cifrado del hardware	HARDWARE_ENCRYPTION_CAPS	Número entero
Hash de la cuenta de iTunes Store conectada actualmente	ITUNES_STORE_ACCOUNT_HASH	Cadena

Red del operador local	SIM_CARRIER_NETWORK	Cadena
Código móvil de país local	SIM_MCC	Número entero
Código móvil de red local	SIM_MNC	Cadena
ICCID	ICCID	Cadena
Número IMEI/MEID	IMEI	Cadena
IMSI	IMSI	Cadena
Ubicación IP	IP_LOCATION	Cadena
Identidad	AS_DEVICE_IDENTITY	Cadena
Almacenamiento interno cifrado	LOCAL_ENCRYPTION Significado de los valores: 1 (True) 0 (False)	Booleano
IssuedAt	WINDOWS_HAS_ISSUED_AT	Cadena
Liberado por jailbreak o root	ROOT_ACCESS Significado de los valores: 1 (Sí) 0 (No)	Booleano
¿Depuración de kernel habilitada?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	Cadena
Modo quiosco	IS_KIOSK Significado de los valores: 1 (True) 0 (False)	Booleano
Última dirección IP conocida	LAST_IP_ADDR	Cadena
Última actualización de directivas	LAST_POLICY_UPDATE_TIME	Fecha

Última sincronización	ZMSP_LAST_SYNC	Fecha
Servicio de localización habilitado	DEVICE_LOCATOR Significado de los valores: 1 (Sí) 0 (No)	Booleano
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	Cadena
MEID	MEID	Cadena
Configuración de buzones de correo	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	Cadena
Batería principal	MAIN_BATTERY_PERCENT	Número entero
Número de teléfono móvil	TEL_NUMBER	Cadena
ID del modelo	SYSTEM_OEM	Cadena
Tipo de adaptador de red	NETWORK_ADAPTER_TYPE	Cadena
NitroDesk TouchDown instalado	TOUCHDOWN_FIND Significado de los valores: 1 (True) 0 (False)	Booleano
Licencia de NitroDesk TouchDown activada vía MDM	TOUCHDOWN_LICENSED_VIA_MDM Significado de los valores: 1 (True) 0 (False)	Booleano
Compilación del sistema operativo	SYSTEM_OS_BUILD	Cadena
Idioma del sistema operativo (configuración regional)	SYSTEM_LANGUAGE	Cadena
Versión del sistema operativo	SYSTEM_OS_VERSION	Cadena

Dirección de la organización	ORGANIZATION_ADDRESS	Cadena
Correo electrónico de la organización	ORGANIZATION_EMAIL	Cadena
Ámbito de la organización	ORGANIZATION_MAGIC	Cadena
Nombre de la organización	ORGANIZATION_NAME	Cadena
Número de teléfono de la organización	ORGANIZATION_PHONE	Cadena
Otros	OTROS	Cadena
No conforme	OUT_OF_COMPLIANCE Significado de los valores: 1 (True) 0 (False)	Booleano
Propietario	CORPORATE_OWNED Significado de los valores: 1 (Empresa) 0 (BYOD)	Booleano
PCR0	WINDOWS_HAS_PCR0	Cadena
Código PIN de la geocerca	PIN_CODE_FOR_GEO_FENCE	Cadena
Código de acceso conforme	PASSCODE_IS_COMPLIANT Significado de los valores: 1 (Sí) 0 (No)	Booleano
Código de acceso conforme con configuración	PASSCODE_IS_COMPLIANT_WITH_CFG Significado de los valores: 1 (Sí) 0 (No)	Booleano
Código de acceso presente	PASSCODE_PRESENT Significado de los valores: 1 (Sí)	Booleano

	0 (No)	
Infracción de perímetro	GPS_PERIMETER_BREACH Significado de los valores: 1 (Sí) 0 (No)	Booleano
Personal Hotspot activado	PERSONAL_HOTSPOT_ENABLED Significado de los valores: 1 (Sí) 0 (No)	Booleano
Plataforma	SYSTEM_PLATFORM	Cadena
Nivel de API de la plataforma	API_LEVEL	Número entero
Nombre de directiva	POLICY_NAME	Cadena
Número de teléfono principal	IDENTITY1_PHONENUMBER	Cadena
IMEI de la tarjeta SIM principal	IDENTITY1_IMEI	Cadena
IMSI de la tarjeta SIM principal	IDENTITY1_IMSI	Cadena
Roaming de la tarjeta SIM principal	IDENTITY1_ROAMING Significado de los valores: 1 (True) 0 (False)	Booleano
Nombre del producto	PRODUCT_NAME	Cadena
ID de dispositivo publicador	PUBLISHER_DEVICE_ID	Cadena
ResetCount	WINDOWS_HAS_RESET_COUNT	Cadena
RestartCount	WINDOWS_HAS_RESTART_COUNT	Cadena
SBCPHash	WINDOWS_HAS_SBCP_HASH	Cadena

Capacidad para SMS	IS_SMS_CAPABLE Significado de los valores: 1 (True) 0 (False)	Booleano
¿Modo seguro habilitado?	WINDOWS_HAS_SAFE_MODE	Cadena
API de Samsung KNOX disponible	SAMSUNG_KNOX Significado de los valores: 1 (True) 0 (False)	Booleano
Versión de API de Samsung KNOX	SAMSUNG_KNOX_VERSION	Cadena
Atestación de Samsung KNOX	SAMSUNG_KNOX_ATTESTED Significado de los valores: 1 (Correcto) 0 (Error)	Booleano
Fecha de actualización de atestación de Samsung KNOX	SAMSUNG_KNOX_ATT_UPDATED_TIME	Fecha
API de Samsung SAFE disponible	SAMSUNG_MDM Significado de los valores: 1 (True) 0 (False)	Booleano
Versión de API de Samsung SAFE	SAMSUNG_MDM_VERSION	Cadena
Pantalla: resolución horizontal	SCREEN_XDPI	Número entero (PPI)
Pantalla: resolución vertical	SCREEN_YDPI	Número entero (PPI)
Pantalla: altura	SCREEN_HEIGHT	Número entero

		(píxeles)
Pantalla: cantidad de colores	SCREEN_NB_COLORS	Número entero
Pantalla: tamaño	SCREEN_SIZE	Decimal (pulgadas)
Pantalla: anchura	SCREEN_WIDTH	Número entero (píxeles)
Número de teléfono secundario	IDENTITY2_PHONENUMBER	Cadena
IMEI de la tarjeta SIM secundaria	IDENTITY2_IMEI	Cadena
IMSI de la tarjeta SIM secundaria	IDENTITY2_IMSI	Cadena
Roaming de la tarjeta SIM secundaria	IDENTITY2_ROAMING Significado de los valores: 1 (True) 0 (False)	Booleano
¿Arranque seguro habilitado?	WINDOWS_HAS_SECURE_BOOT_ENABLED	Cadena
Contenedor seguro habilitado	WINDOWS_HAS_BIT_LOCKER_STATUS	Cadena
Número de serie	SERIAL_NUMBER	Cadena
API de Sony Enterprise disponible	SONY_MDM Significado de los valores: 1 (True) 0 (False)	Booleano
Versión de API de Sony Enterprise	SONY_MDM_VERSION	Cadena
Supervisado	Supervisado Significado de los valores: 1 (Sí) 0 (No)	Booleano

Motivo de suspensión	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON	Cadena
Estado manipulado	TAMPERED_STATUS	Cadena
Términos y condiciones	TERMS_AND_CONDITIONS	Cadena
¿Contrato y términos aceptados?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	Cadena
¿Firma de pruebas habilitada?	WINDOWS_HAS_TEST_SIGNING_ENABLED	Cadena
Total de RAM	MEMORY	Número entero
Total de espacio de almacenamiento	FREEDISK	Número entero
UDID	UDID	Cadena
Agente de usuario	USER_AGENT	Cadena
Definido por el usuario #1	USER_DEFINED_1	Cadena
Definido por el usuario #2	USER_DEFINED_2	Cadena
Definido por el usuario #3	USER_DEFINED_3	Cadena
Idioma del usuario (configuración regional)	USER_LANGUAGE	Cadena
¿VSM habilitado?	WINDOWS_HAS_VSM_ENABLED	Cadena
Proveedor	PROVEEDOR	Cadena
Capacidad para voz	IS_VOICE_CAPABLE Significado de los valores: 1 (True) 0 (False)	Booleano
Roaming de voz permitido	VOICE_ROAMING_ENABLED Significado de los valores:	Booleano

	1 (Sí) 0 (No)	
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	Cadena
Estado de notificación WNS	WNS_PUSH_STATUS	Cadena
URL de notificación WNS	PROPERTY_WNS_PUSH_URL	Cadena
Fecha de caducidad de URL de notificación WNS	PROPERTY_WNS_PUSH_URL_EXPIRY	Cadena
Dirección MAC de WiFi	WIFI_MAC	Cadena
¿WinPE habilitado?	WINDOWS_HAS_WINPE	Cadena
ID del agente de XenMobile	AGENT_ID	Cadena
Revisión del agente de XenMobile	EW_REVISION	Cadena
Versión del agente de XenMobile	EW_VERSION	Cadena

Bloqueo de dispositivos iOS

Feb 27, 2017

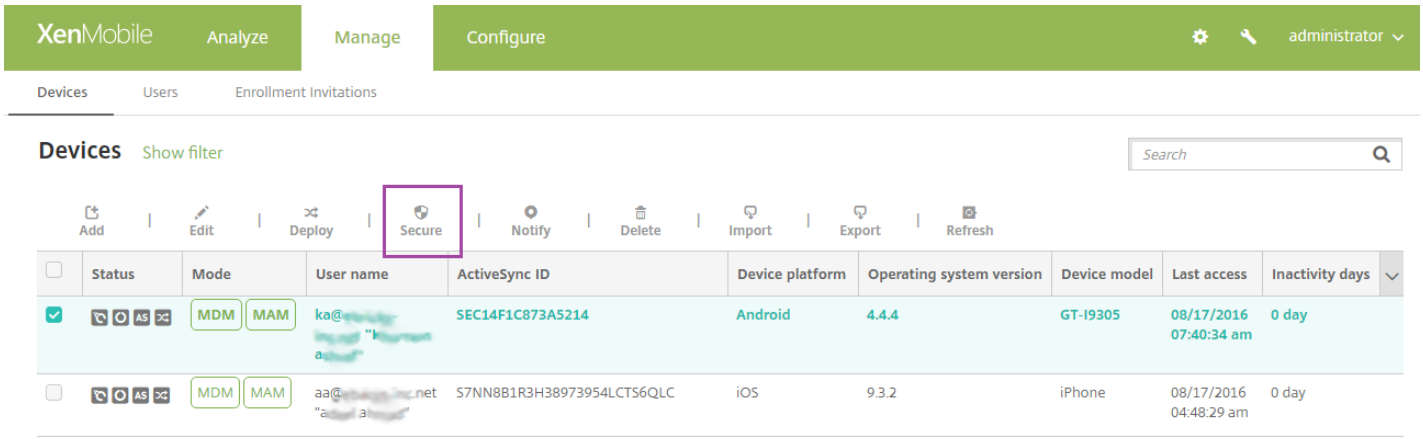
Puede bloquear un dispositivo iOS perdido y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo. Esta función está respaldada en dispositivos iOS 7 y versiones posteriores.

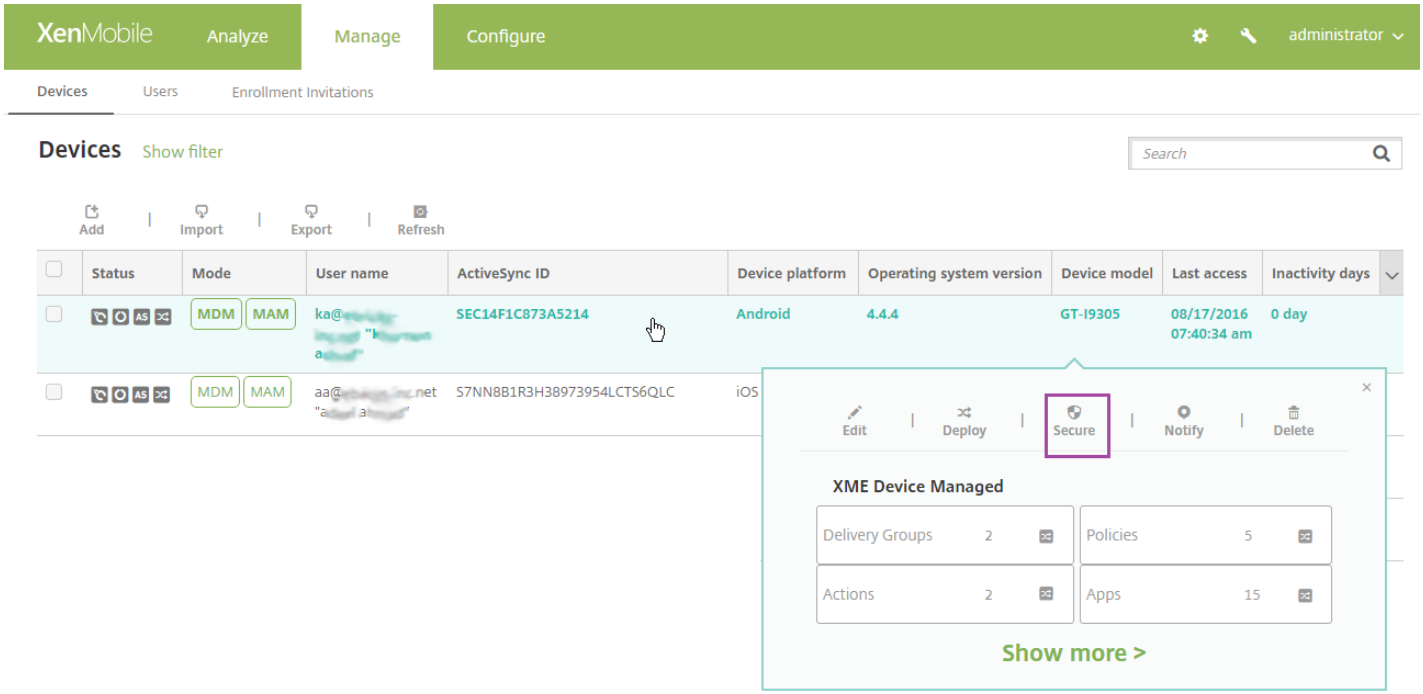
Para que se muestren un mensaje y un teléfono en un dispositivo bloqueado, la directiva de códigos de acceso Passcode debe establecerse en "true" en la consola de XenMobile. De forma alternativa, los usuarios deben habilitar manualmente el código de acceso en el dispositivo.

1. En la consola de XenMobile, haga clic en **Manage > Devices**. Aparecerá la página **Devices**.

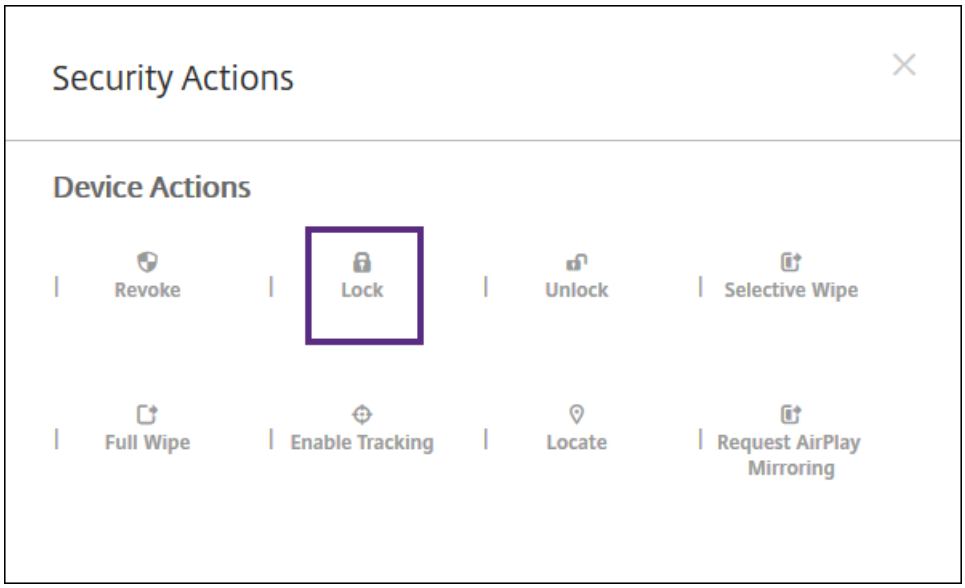
2. Seleccione el dispositivo iOS que quiere bloquear.

Cuando se marca la casilla de verificación situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

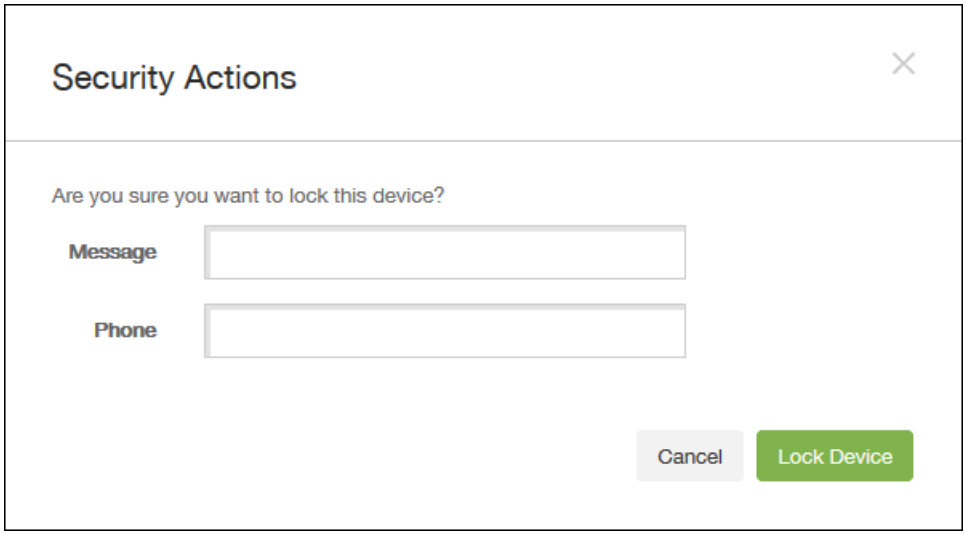




3. En el menú de opciones, seleccione **Secure**. Aparecerá el cuadro de diálogo **Security Actions**.



4. Haga clic en **Lock**. Aparecerá el cuadro de diálogo **Security Actions**.



5. Si lo prefiere, puede introducir el mensaje y el número de teléfono que aparecerán en la pantalla de bloqueo del dispositivo.

Para iPads que ejecutan iOS 7 y versiones posteriores: iOS añade las palabras "iPad perdido" a lo que escriba en el campo **Message**. Para iPhones que ejecutan iOS 7 y versiones posteriores: Si deja el campo **Message** vacío y proporciona un número de teléfono, Apple mostrará un mensaje del tipo "Llamar al propietario" en la pantalla de bloqueo del dispositivo.

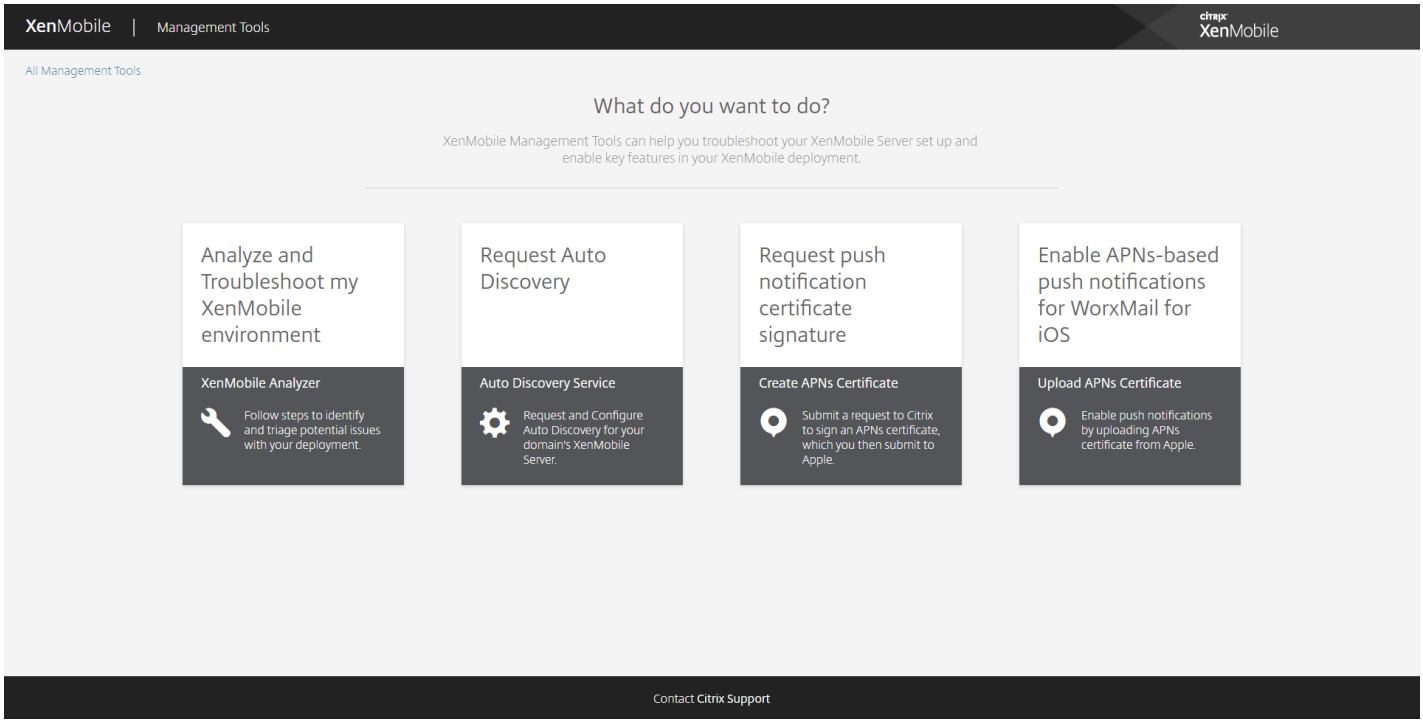
6. Haga clic en **Lock Device**.

Servicio de detección automática en XenMobile

Feb 27, 2017

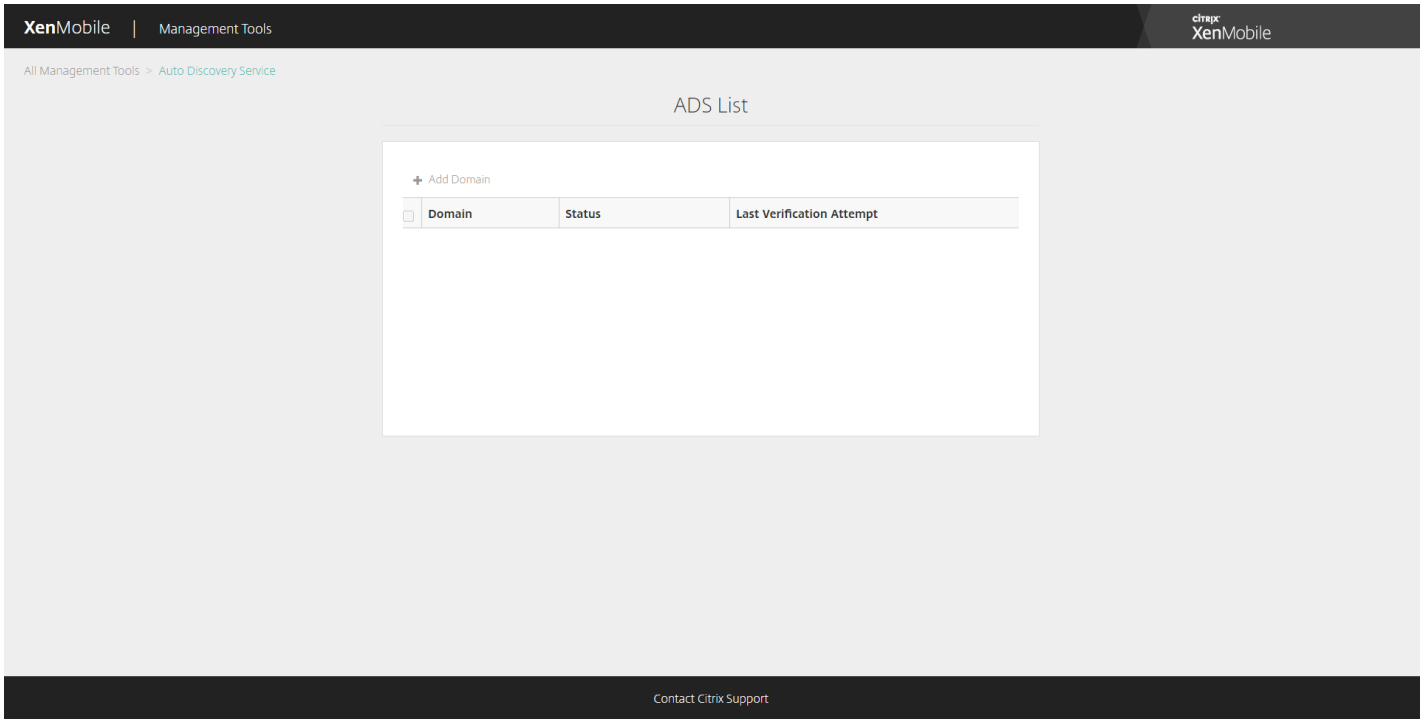
La detección automática es una parte importante de las implementaciones de XenMobile. La detección automática simplifica el proceso de inscripción para los usuarios. Los usuarios pueden utilizar sus nombres de usuario de red y contraseñas de Active Directory para inscribir sus dispositivos, en lugar 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**.

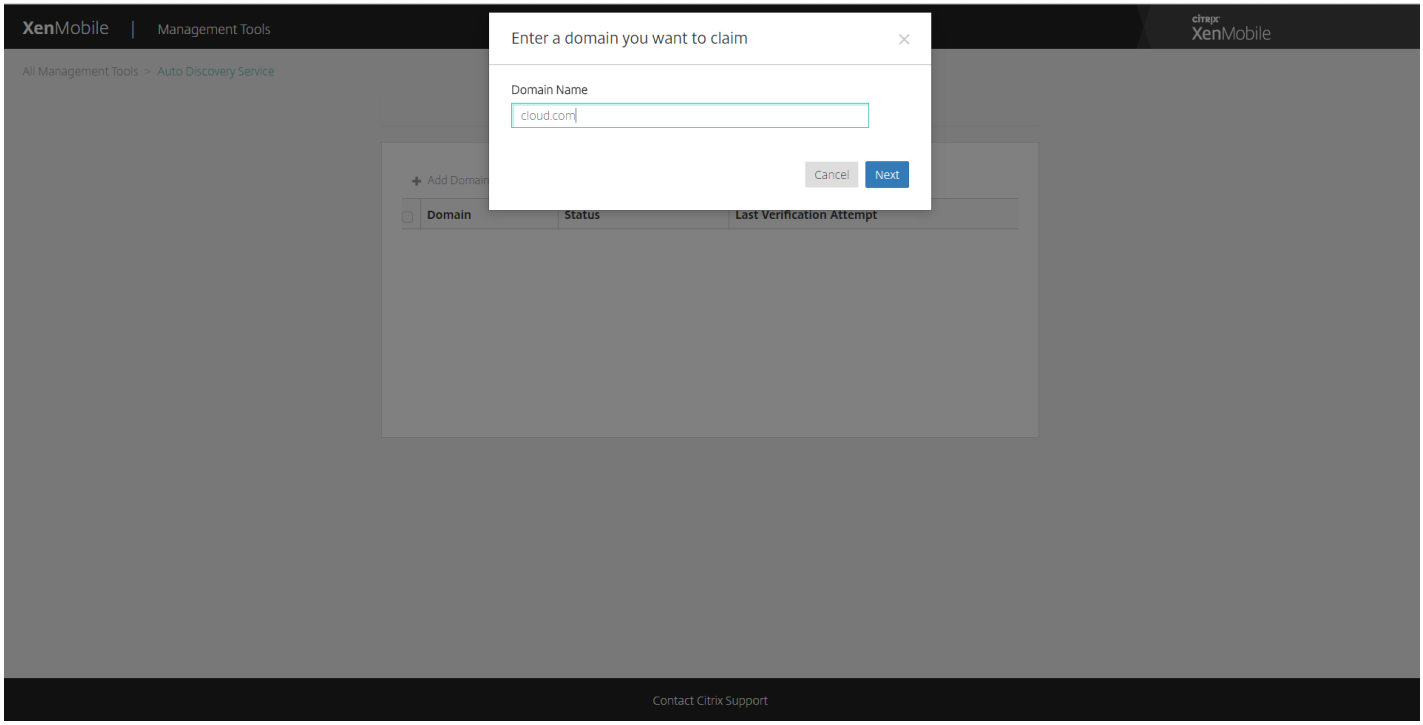


Cómo solicitar el servicio de detección automática

1. En la página AutoDiscovery Service, primero debe 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.

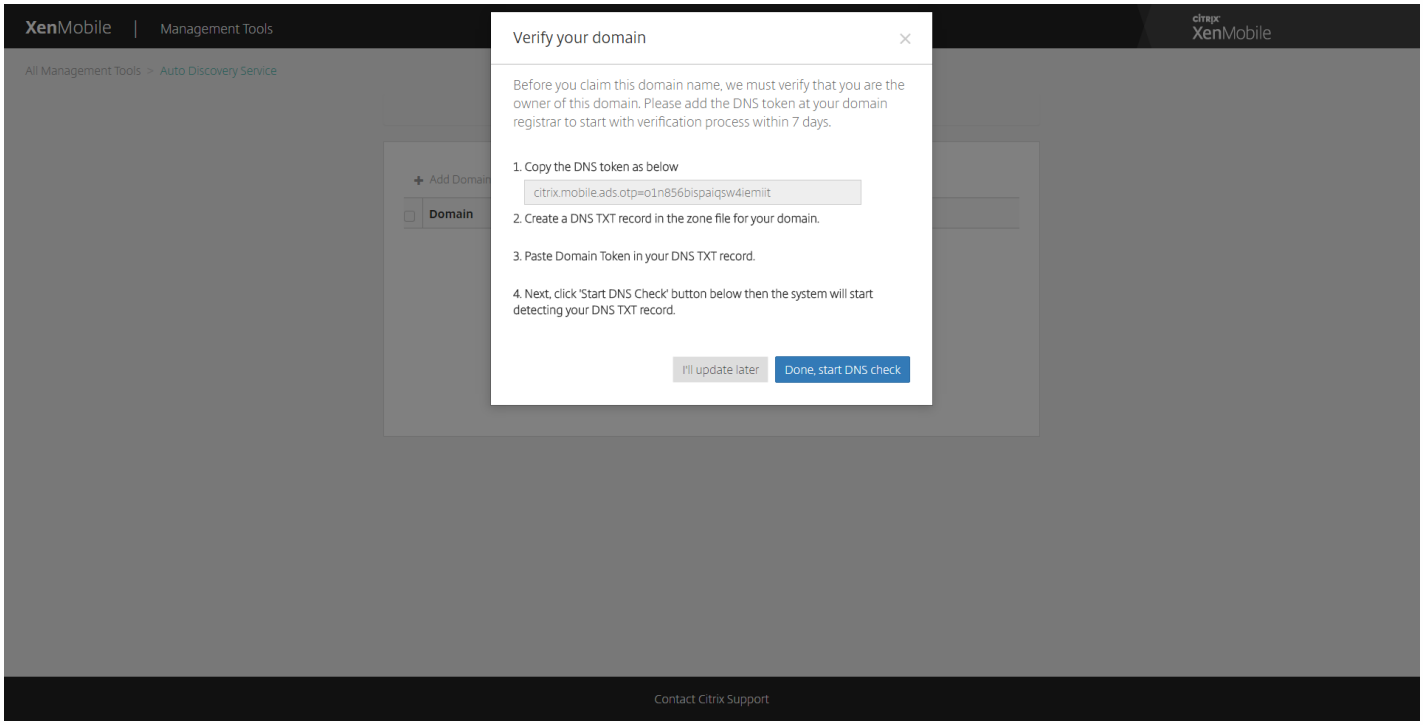
Para crear un registro TXT de DNS es necesario iniciar sesión en el portal del proveedor de alojamiento del dominio que agregó en el paso 2. En el portal de alojamiento de dominios puede editar sus registros de servidor de nombres de dominio (DNS) y agregar un registro TXT personalizado. Abajo hay un 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".

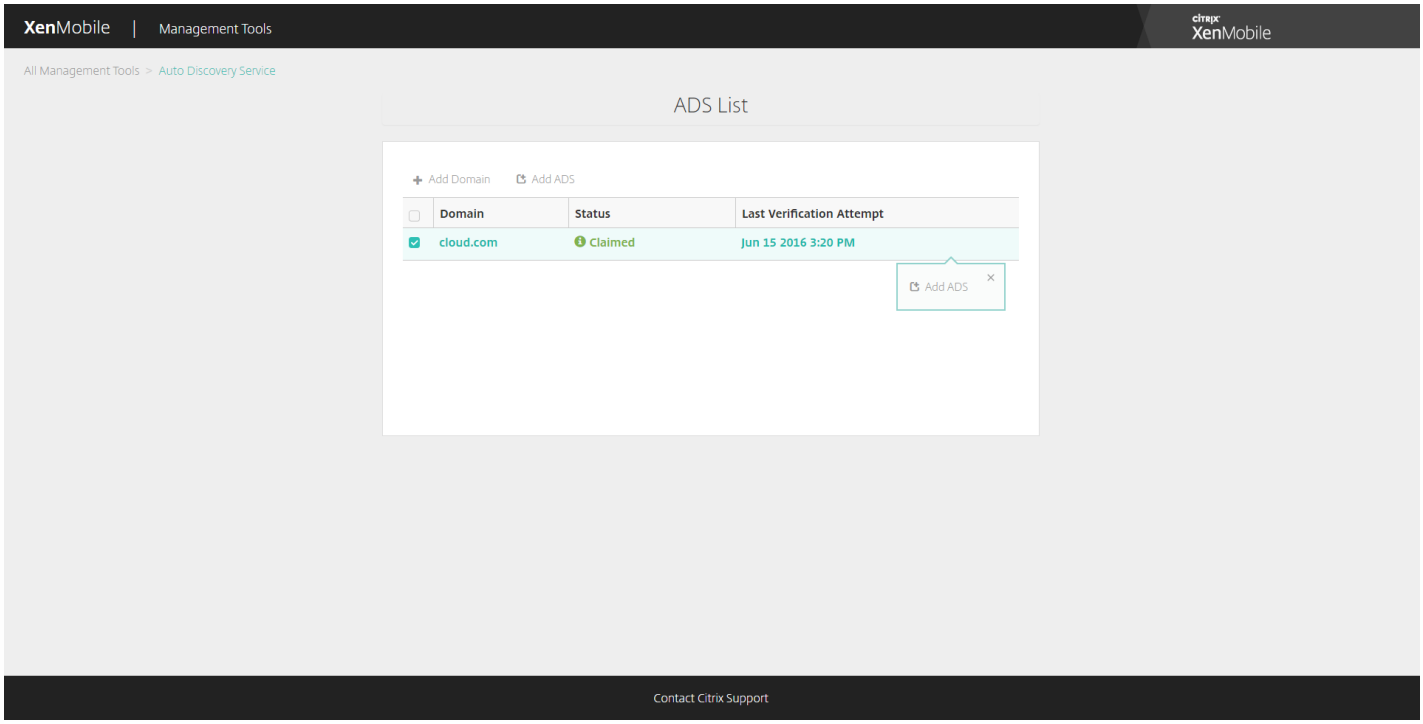
El sistema detecta el registro TXT de DNS. Si lo prefiere, puede hacer clic en I'll update later y el registro se guarda. La comprobación de DNS no se iniciará hasta que seleccione el registro en espera (Waiting) y haga clic en "DNS Check".

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.

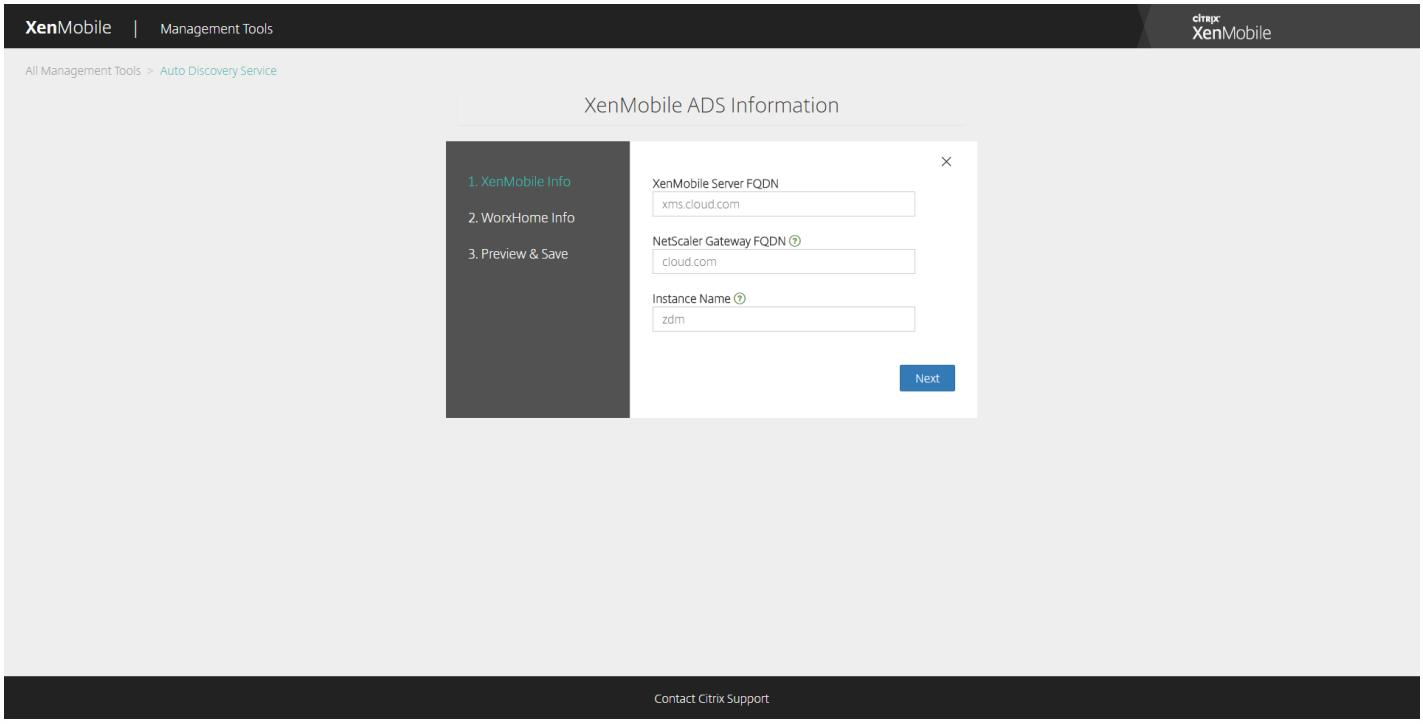


4. Después de reclamar su dominio, puede introducir la información para el servicio de detección automática. Haga clic con el botón secundario en el registro del dominio para el cual quiere solicitar la detección automática y luego haga clic en **Add ADS**.

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".



En la captura de pantalla anterior, tenga en cuenta que ahora Worx Home se llama Secure Hub.

6. Introduzca la siguiente información de Secure Hub y haga clic en **Next**.

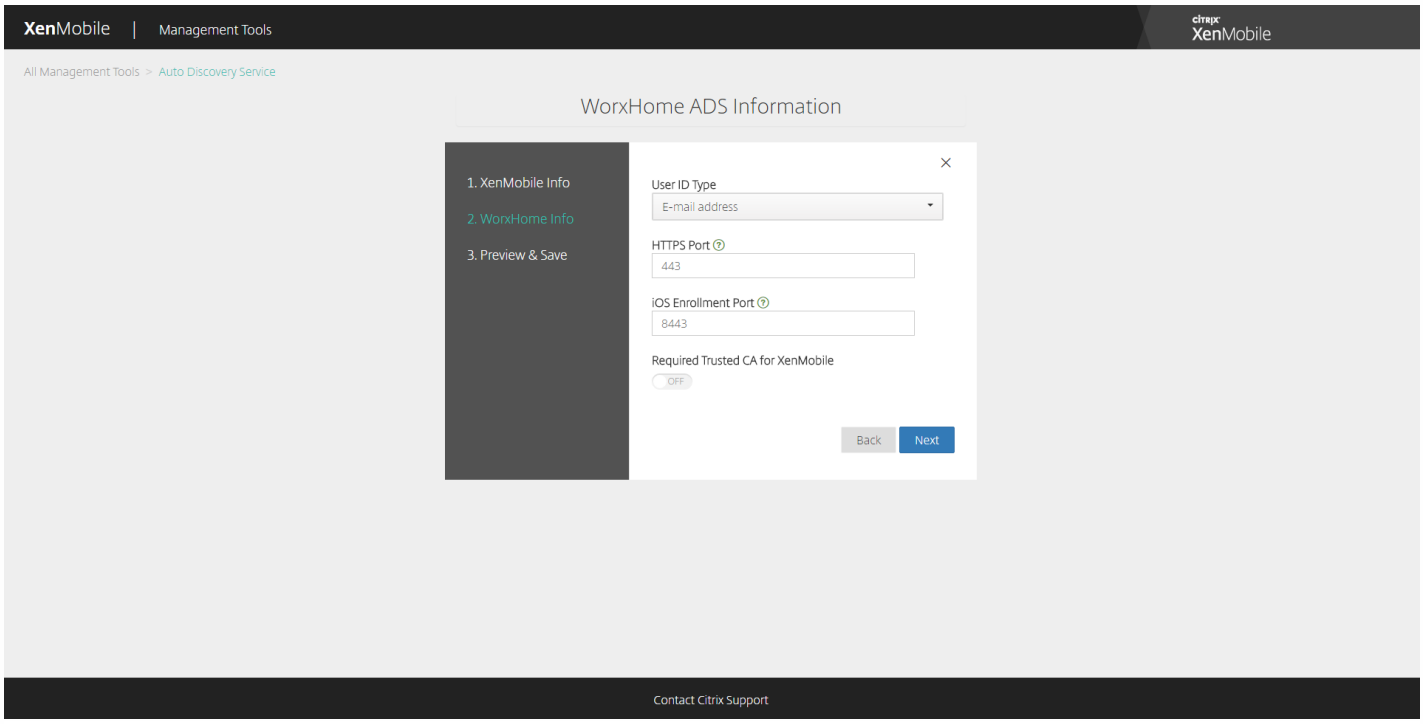
a. **User ID Type**. Seleccione el tipo de ID con que los usuarios inician sesiones: **E-mail address** o **UPN**.

Se utiliza **UPN** 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; con **UPN**, se le pide que escriba su contraseña.

b. **HTTPS Port**. Introduzca el puerto para acceder a Secure Hub sobre HTTPS. Por lo general, este es el puerto 443.

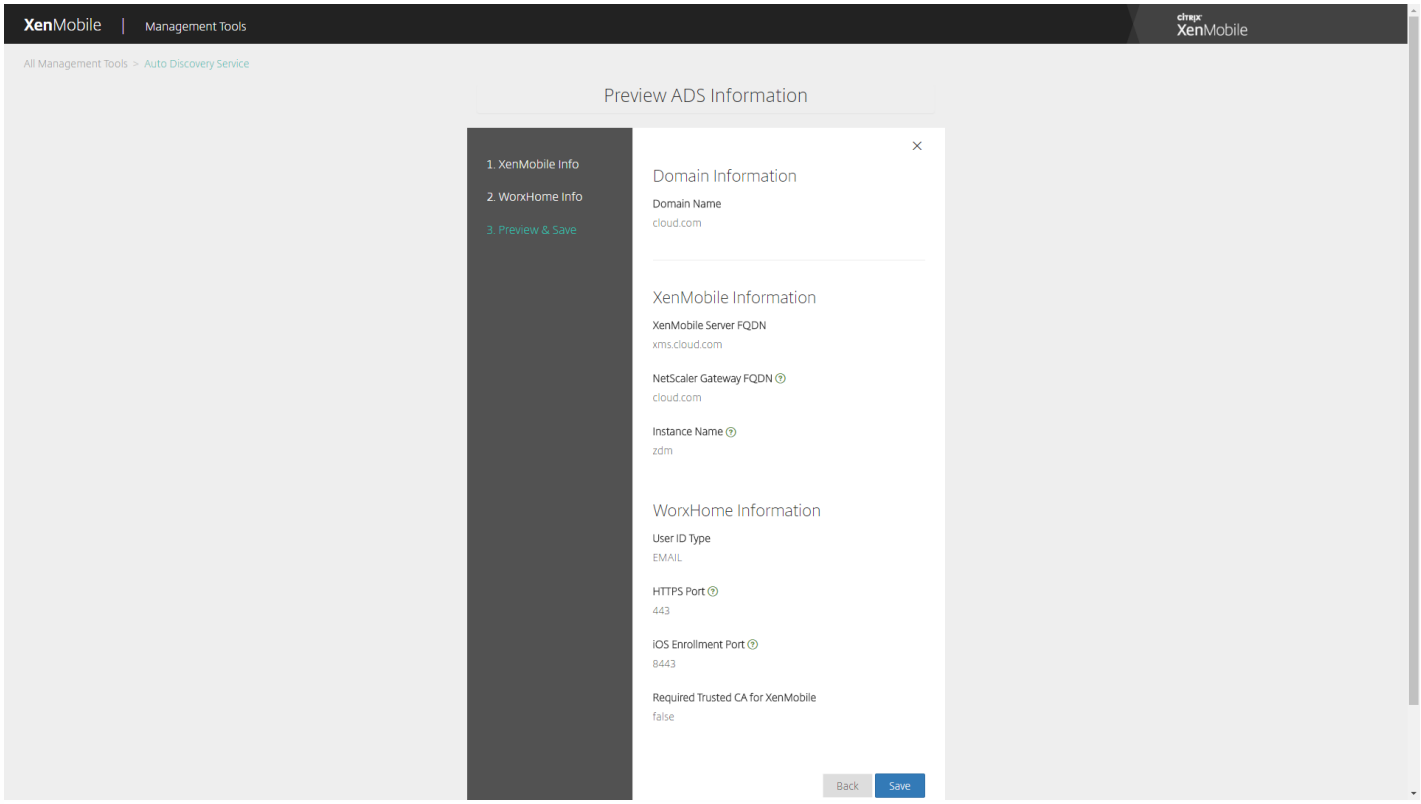
iOS Enrollment Port. Escriba el número de puerto de acceso a Secure Hub para la inscripción de iOS. Por lo general, es el puerto 443.

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 la fijación de certificados en Secure Hub, en la documentación de las aplicaciones XenMobile. 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.



En la captura de pantalla anterior, tenga en cuenta que ahora Worx Home se llama Secure Hub.

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**.



En la captura de pantalla anterior, tenga en cuenta que ahora Worx Home se llama Secure Hub.

Cómo habilitar la detección automática

La detección automática simplifica el proceso de inscripción para los usuarios. Los usuarios pueden utilizar sus nombres de usuario de red y contraseñas de Active Directory para inscribir sus dispositivos, en lugar de tener que especificar también datos del servidor XenMobile. Los usuarios deben especificar su nombre de usuario en el formato del nombre principal de usuario (UPN); por ejemplo, usuario@miempresa.com.

Para habilitar la detección automática, puede acceder al portal Autodiscovery Service en https://xenmobiletools.citrix.com.

En algunos casos, puede que tenga que ponerse en contacto con el servicio de asistencia técnica Citrix Support para habilitar la detección automática. Para hacerlo, siga los procedimientos indicados a continuación para facilitar la información relativa a la implementación. En el caso de dispositivos Windows, también deberá facilitar un certificado SSL al equipo de Asistencia técnica de Citrix. Después de que Citrix reciba esta información, cuando los usuarios inscriban sus dispositivos, se extraerá la información de dominio y esta se asignará a una dirección de servidor. Esta información se conserva en la base de datos de XenMobile para que siempre esté accesible y disponible cuando los usuarios se inscriban.

1. Si no puede habilitar la detección automática desde el portal Autodiscovery Service en https://xenmobiletools.citrix.com, abra un caso de asistencia técnica en el portal de Citrix Support y facilite esta información:

- El dominio que contiene las cuentas con las que se van a inscribir los usuarios.
- El nombre de dominio completo (FQDN) de XenMobile.
- El nombre de la instancia de XenMobile. De forma predeterminada, el nombre de la instancia es zdm y en el campo se distinguen mayúsculas y minúsculas.

- El tipo de ID de usuario, que puede ser UPN o correo electrónico. De forma predeterminada, el tipo es UPN.
- El puerto utilizado para la inscripción de iOS si se ha cambiado el número del puerto predeterminado (8443) a otro número de puerto.
- El puerto a través del cual el servidor XenMobile acepta las conexiones, si se ha cambiado el número del puerto predeterminado (443) a otro número de puerto.
- Si quiere, puede agregar una dirección de correo electrónico para el administrador de XenMobile.

2. Para inscribir dispositivos Windows, lleve a cabo lo siguiente:

- Obtenga un certificado SSL firmado públicamente y sin comodines, para enterpriseenrollment.mycompany.com, donde mycompany.com es el dominio que contiene las cuentas con las que se inscribirán los usuarios. Adjunte el certificado SSL en formato .pfx y su contraseña para la solicitud.
- Cree un registro de nombre canónico (CNAME) en el servidor DNS y asigne la dirección del certificado SSL (enterpriseenrollment.mycompany.com) a autodisc.zc.zenprise.com. Cuando el usuario de un dispositivo Windows se inscribe con un nombre UPN, además de proporcionar la información del servidor XenMobile, el servidor de inscripciones de Citrix ordena al dispositivo que solicite un certificado válido al servidor XenMobile.

Su caso de asistencia técnica se actualizará cuando sus datos y su certificado, si procede, se hayan agregado a los servidores Citrix. A partir de este momento, los usuarios pueden empezar a inscribirse con la detección automática.

Nota: También puede usar un certificado de dominios múltiples, en caso de que quiera inscribirse con más de un dominio. El certificado de dominios múltiples debe tener la siguiente estructura:

- Un nombre SubjectDN con un nombre CN que especifica el dominio principal al que está relacionado (por ejemplo, enterpriseenrollment.mycompany1.com).
- Las redes de área de almacenamiento apropiadas para el resto de los dominios (por ejemplo, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com, entre otros).

Inscripción de dispositivos

May 11, 2017

Para poder administrar dispositivos de usuario de forma remota y segura, dichos dispositivos deben inscribirse 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. A continuación, puede realizar tareas de administración de dispositivos desde la consola de XenMobile. Puede aplicar directivas, implementar aplicaciones, insertar datos en el dispositivo, bloquearlo, borrarle los datos y localizar dispositivos perdidos o robados.

Con XenMobile Service 10.5.1, se respalda la inscripción de Azure Active Directory en dispositivos iOS, Android y Windows 10. Para obtener más información sobre cómo configurar Azure como proveedor de identidades (IdP), consulte el apartado de integración de XenMobile con Active Directory de Azure como IdP en el artículo Novedades de la documentación referente al servicio XenMobile.

Nota: Antes de poder inscribir usuarios de dispositivos iOS, debe solicitar un certificado APNs. Para obtener información más detallada, consulte Certificados.

Puede actualizar las opciones de configuración de usuarios y dispositivos desde la página **Manage > Enrollment Invitations**. Para obtener más información, consulte Envío de una invitación de inscripción en este artículo.

Dispositivos Android

1. Vaya a la tienda Google Play en el dispositivo Android, descargue la aplicación Citrix Secure Hub y, a continuación, toque en ella.
2. Cuando se le solicite instalar la aplicación, haga clic en **Siguiente** y, a continuación, haga clic en **Instalar**.
3. Después de que Secure Hub se instale, toque en **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 en **Activate**.
6. Escriba la contraseña de empresa y, a continuación, toque en **Iniciar sesión**.
7. Según la configuración de XenMobile que tenga, es posible que se le solicite la creación de un PIN de Citrix. Podrá utilizar este PIN para iniciar sesión en Secure Hub o en otras aplicaciones habilitadas para XenMobile, como Secure Mail, Secure Web y ShareFile, entre otros. Deberá introducir su PIN de Citrix dos veces. En la pantalla **Crear PIN de Citrix**, introduzca un PIN.
8. Vuelva a escribir el PIN. Se abrirá Secure Hub. Entonces, podrá acceder a XenMobile 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. Además, las directivas que configure en XenMobile se implementan en el dispositivo. Toque en **Instalar** para instalar las aplicaciones.

Para inscribir y reinscribir un dispositivo Android

Los usuarios pueden desinscribirse una vez dentro de Secure Hub. Cuando los usuarios se desinscriben con el siguiente procedimiento, el dispositivo sigue apareciendo en el inventario de dispositivos en la consola de XenMobile. Sin embargo, no puede realizar acciones en el dispositivo. No puede realizar un seguimiento del dispositivo ni supervisar su estado de cumplimiento.

1. Toque en Secure Hub para abrir la aplicación.

2. Dependiendo de si dispone de un teléfono o una tableta, lleve a cabo lo siguiente:

En un teléfono:

a. Deslice desde la izquierda de la pantalla para abrir un panel de configuración.

b. Toque en **Preferencias** y en **Cuentas**. A continuación, toque en **Eliminar cuenta**.

En una tableta:

a. Pulse la flecha situada junto a su dirección de correo electrónico en la esquina superior derecha.

b. Toque en **Preferencias** y en **Cuentas**. A continuación, toque en **Eliminar cuenta**.

3. Toque en **Reinscribir**. Aparecerá un mensaje para confirmar que quiere volver a inscribir el dispositivo.

4. Toque en **Aceptar**.

El dispositivo está desinscrito.

5. Siga las instrucciones que aparecen en la pantalla para reinscribir el dispositivo.

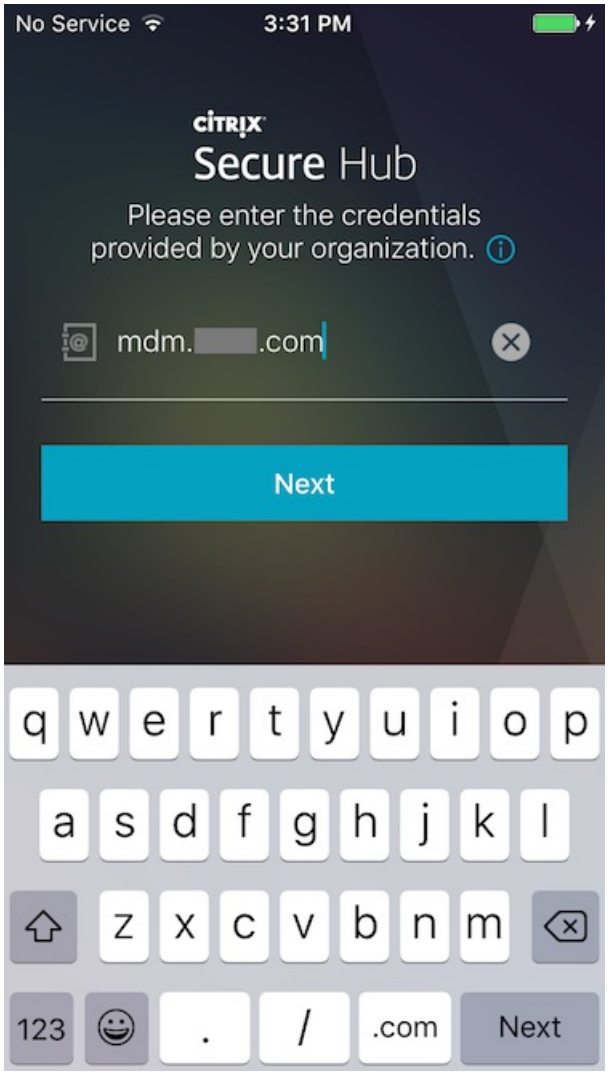
Dispositivos OS

1. Descargue la aplicación Secure Hub desde iTunes, el App Store de Apple, al dispositivo y, a continuación, instale la aplicación en el dispositivo.

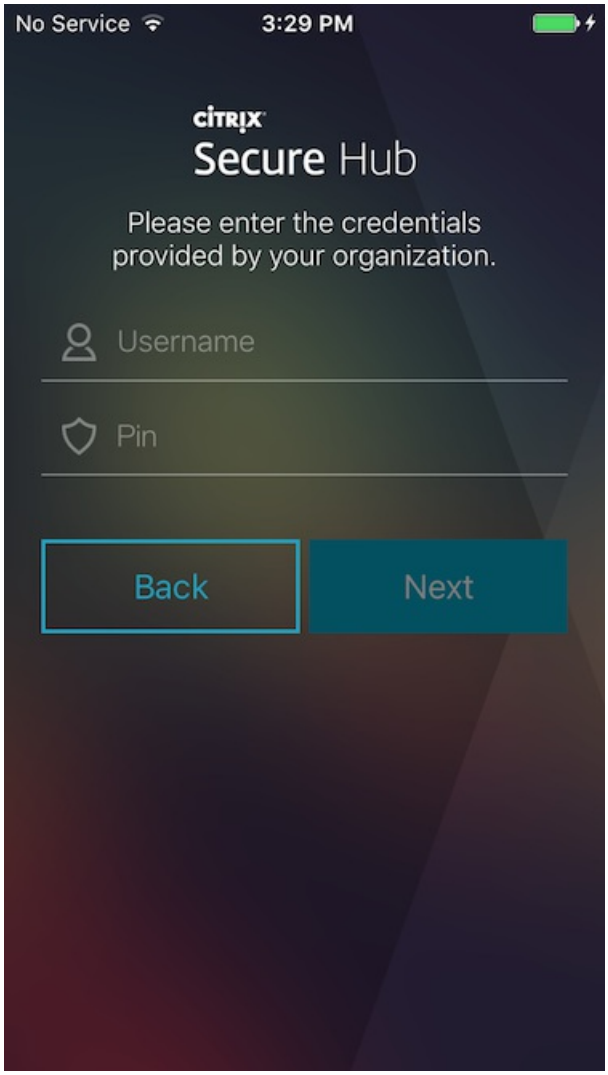
2. En la pantalla de inicio del dispositivo iOS, toque en la aplicación Secure Hub.

3. Cuando se abra Hub Secure, introduzca la dirección del servidor que le haya facilitado el departamento de asistencia técnica.

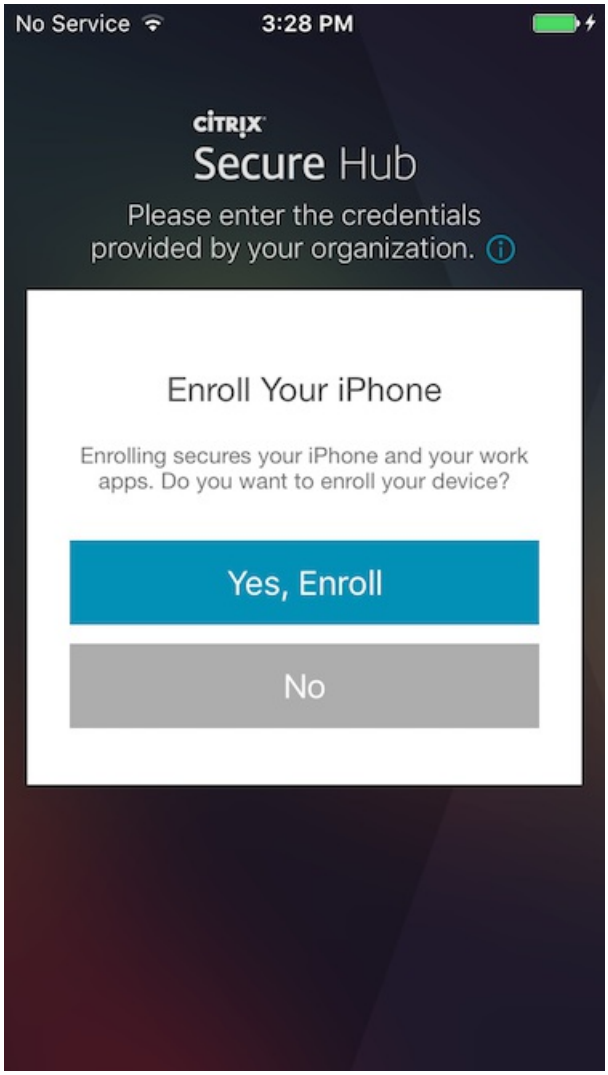
(Las pantallas mostradas pueden ser distintas de estos ejemplos, en función de cómo esté configurado XenMobile.)

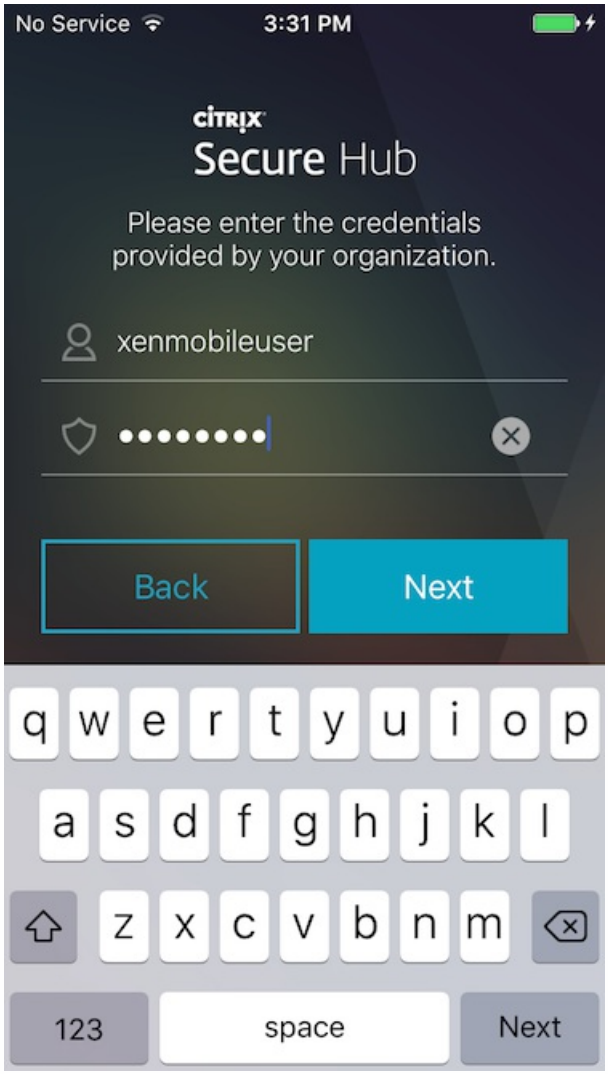


4. Introduzca su nombre de usuario y contraseña o PIN cuando lo pida el sistema. Haga clic en **Next**.



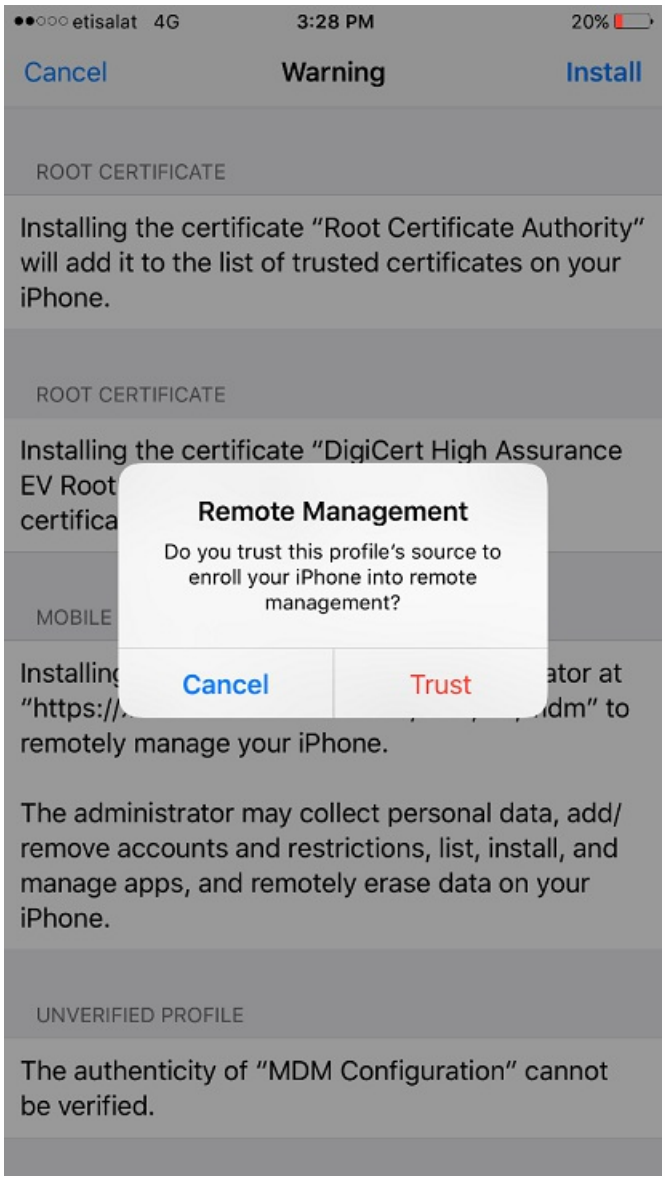
5. Cuando se le solicite la inscripción, haga clic en **Sí, inscribirlo** y, a continuación, introduzca sus credenciales cuando se le pidan.



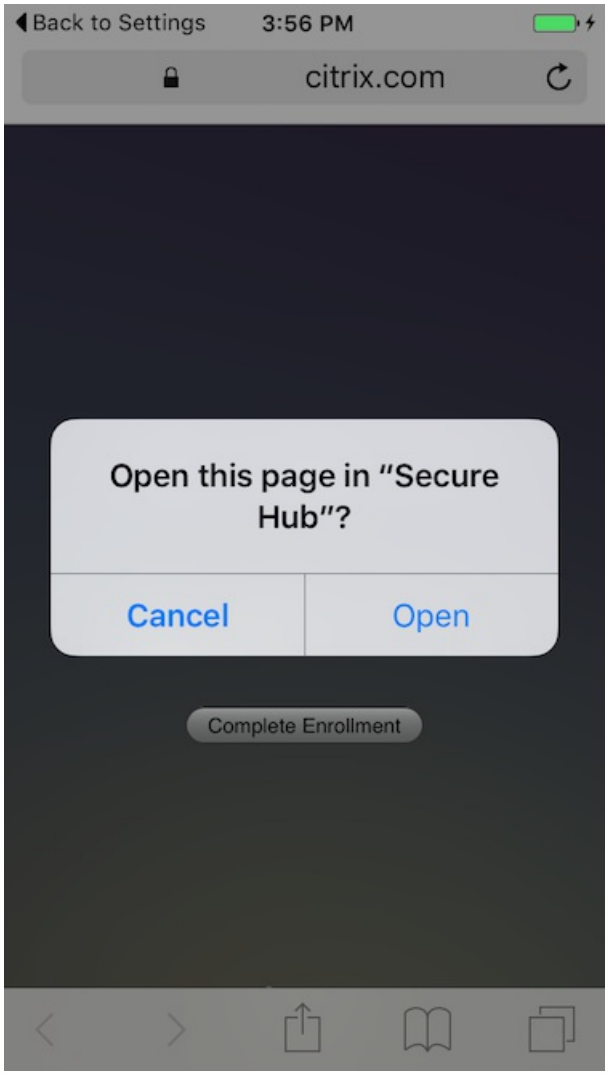


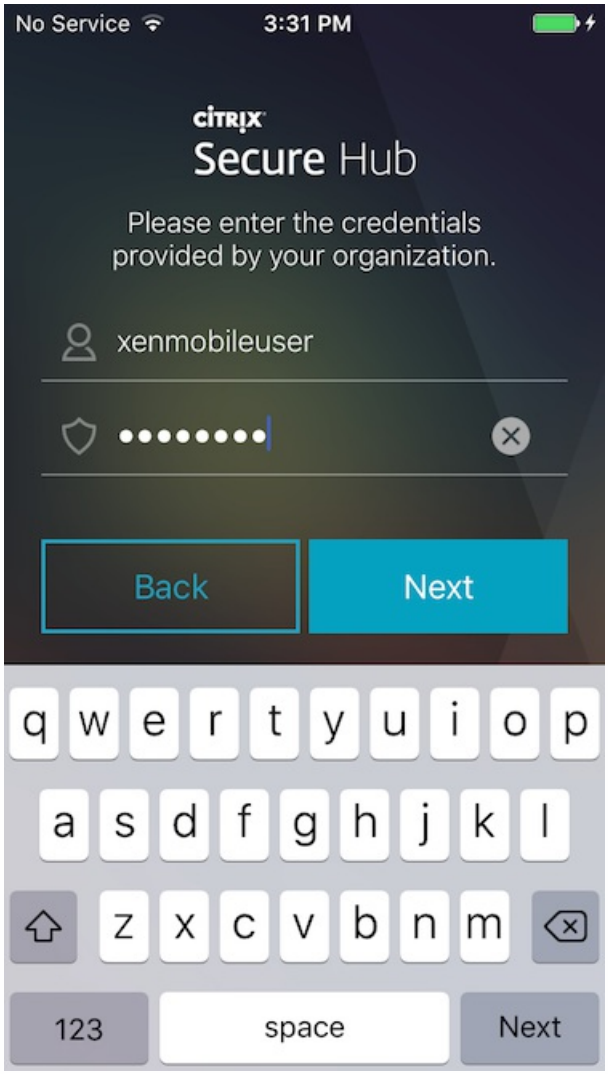
6. Toque en **Instalar** para instalar el servicio de perfiles de Citrix.

7. Toque en **Confiar**.



8. Toque en **Abrir** e introduzca sus credenciales.





Mac OS X

Puede inscribir en XenMobile Macs que ejecuten 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

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.

En XenMobile, puede inscribir dispositivos que ejecuten los siguientes sistemas operativos Windows:

- Windows 10 Phone y Tablet
- Windows Phone 8.1

Los usuarios pueden inscribirse 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 los dispositivos Windows admitidos.

Para que los usuarios de dispositivos Windows puedan inscribir sus dispositivos mediante Azure, debe configurar los parámetros del servidor Microsoft Azure en XenMobile. Para obtener más información, consulte Parámetros del servidor Microsoft Azure Active Directory.

> ## 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

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 activar la detección automática en XenMobile para la inscripción de usuarios.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows.

2. Para Windows 10: En el menú Accesos, toque en **Configuración** > **Cuentas > Obtener acceso a trabajo o escuela >**

Conectarse a la red del trabajo o colegio. Para teléfonos Windows 8.1: Toque en **Configuración de PC > Red > Área de trabajo**.

3. Introduzca su dirección de correo electrónico de la empresa y después toque en **Activar la administración de dispositivos** en Windows 8.1, o bien 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 evitar 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. Para Windows 10: En el cuadro de diálogo **Condiciones de uso**, indique que acepta que el dispositivo sea administrado y, a continuación, toque en **Aceptar**. Para Windows 8.1: En el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique que acepta que el dispositivo sea administrado y, a continuación, toque en **Activar**.
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.

2. Para Windows 10: En el menú Accesos, toque en **Configuración** > **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio**. Para Windows 8.1: Toque en **Configuración de PC > Red > Área de trabajo**.

3. Introduzca la dirección de correo electrónico de empresa.

4. Para 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. Para Windows 8.1: Si la opción de **detectar la dirección del servidor automáticamente** está **activada**, toque en ella para **desactivarla**.

5. Para Windows 10: En el campo **Escribir dirección del servidor**, escriba la 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.

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.

6. Escriba la contraseña.
7. Para Windows 10: En el cuadro de diálogo **Condiciones de uso**, indique que acepta que el dispositivo sea administrado y, a continuación, toque en **Aceptar**. Para Windows 8.1: En el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique que acepta que el dispositivo sea administrado y, a continuación, toque en **Activar**.

Para inscribir dispositivos Windows Phone

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 desde la tienda de Windows Phone de la empresa, antes de que los usuarios se inscriban, compruebe que ha configurado la directiva Enterprise Hub (con una aplicación Secure Hub firmada para Windows Phone para cada plataforma a la que quiera dar respaldo).

1. En la pantalla principal del teléfono Windows, toque el icono **Configuración**.

- Para Windows 10: En función de la versión, toque en **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio** o toque en **Cuentas > Acceso al trabajo > Inscribir en administración de dispositivos (MDM)**.
- Para Windows 8.1: Toque en **Configuración de PC > Red > Área de trabajo**, y después toque en **Agregar cuenta**.

2. 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.

3. En la pantalla siguiente, introduzca la dirección Web del servidor XenMobile, como: https://://wpe. Por ejemplo: https://miempresa.mdm.com:8443/zdm/wpe. **Nota**: Debe adaptar el número de puerto a la implementación, pero debe ser el mismo puerto que se ha usado para la inscripción de iOS.

4. Introduzca el nombre de usuario y el dominio si la autenticación se valida mediante un nombre de usuario y un dominio. A continuación, toque en **Iniciar sesión**.

5. 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 eb **Continuar**. De lo contrario, toque en **Cancelar**.

6. En Windows Phone 8.1, una vez agregada la cuenta, tiene la opción de seleccionar **Instalar aplicación de empresa**. Si el administrador ha configurado una tienda 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.

7. En Windows Phone 8.1, en la pantalla **Cuenta agregada**, toque en **listo**.

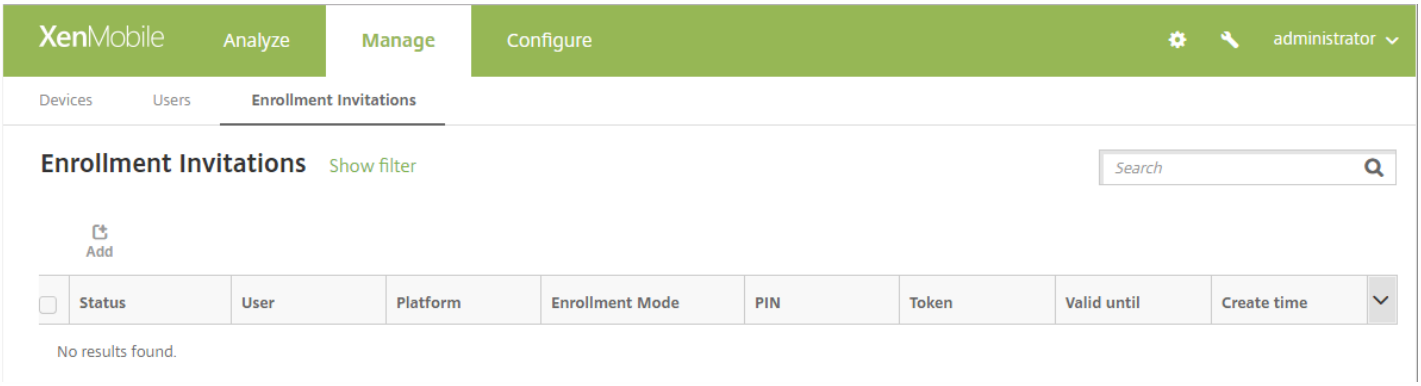
8. Para forzar la conexión con el servidor, toque el icono de actualización. Si el dispositivo no se conecta manualmente al servidor, XenMobile intenta reconectarse. XenMobile se conecta al dispositivo cada 3 minutos 5 veces sucesivas; después, se conecta cada 2 horas. Puede modificar este intervalo de conexión en **Intervalo de latidos del servicio WNS**, ubicado en **Propiedades del servidor**. Una vez finalizada la inscripción, Secure Hub se inscribe en segundo plano. No aparece ningún indicador tras completarse la instalación. Toque en Secure Hub desde la pantalla **All Apps**.

Envío de una invitación de inscripción

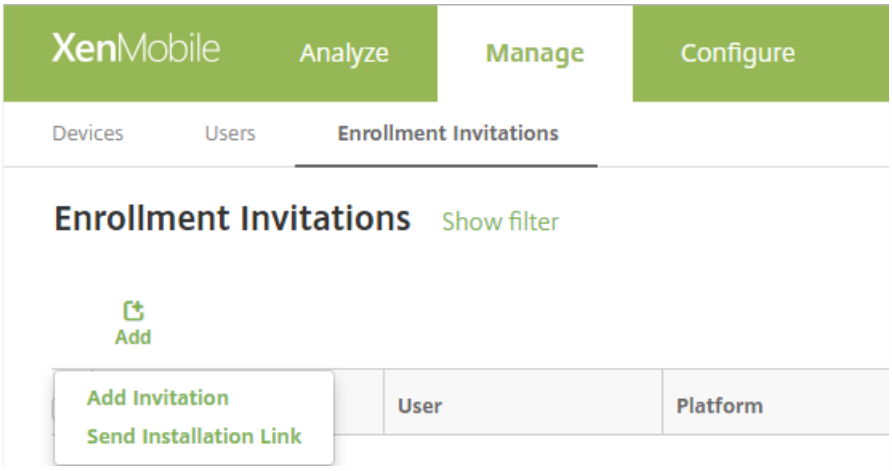
Desde la consola de XenMobile, puede enviar a los usuarios una invitación para la inscripción de dispositivos iOS o Android.

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 Invitations**. Aparecerá la página **Enrollment Invitations**.



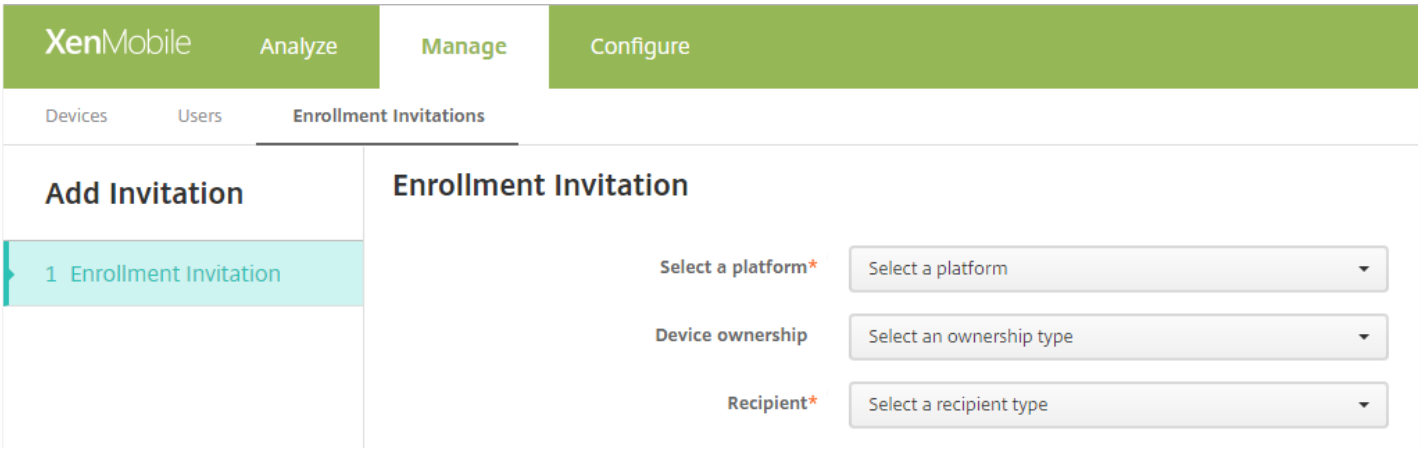
2. Haga clic en **Add**. Aparecerá un menú con opciones de inscripción.



- 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.
- Si quiere 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**.

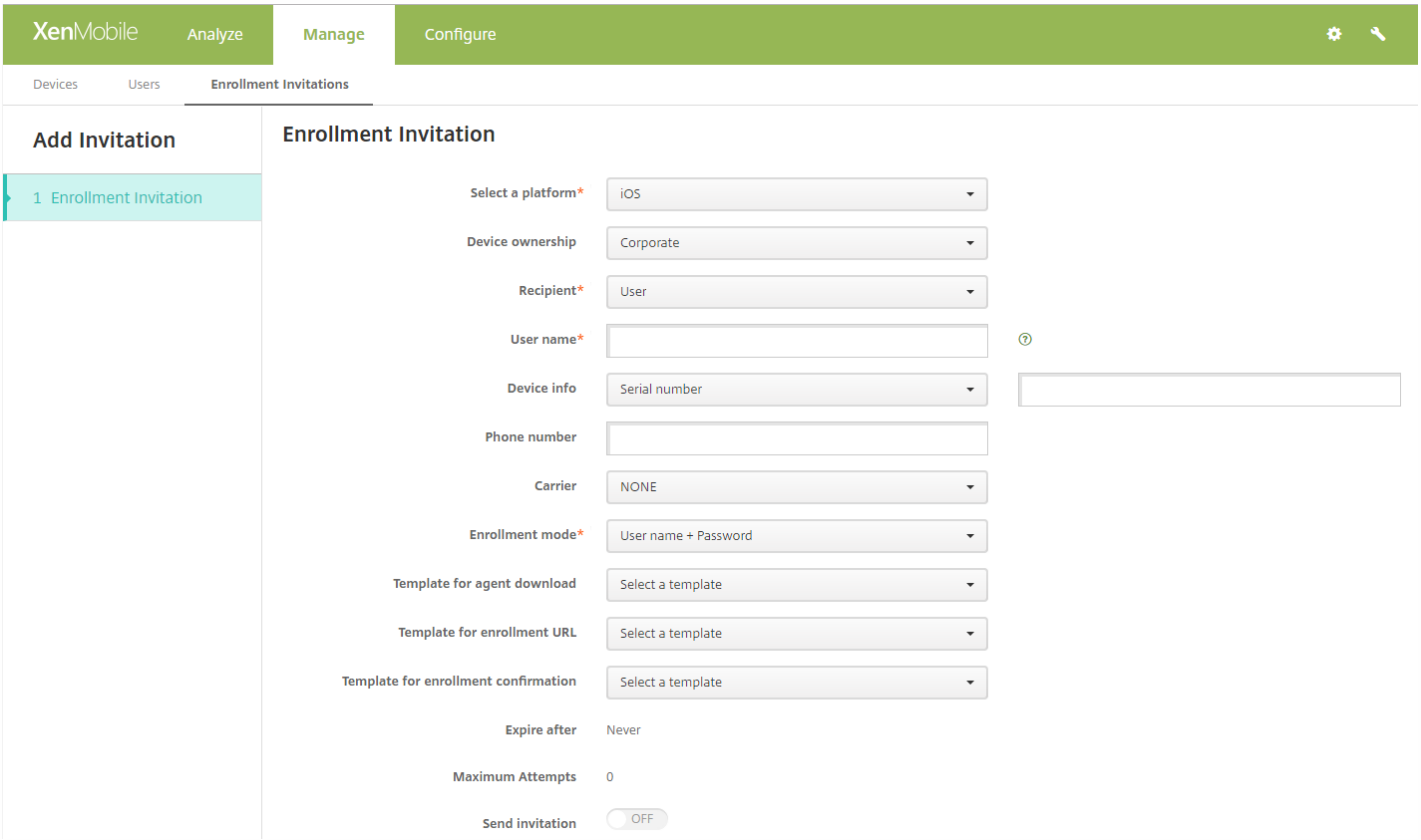


2. Configure estos parámetros:

- **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**.

Verá más o menos opciones a 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



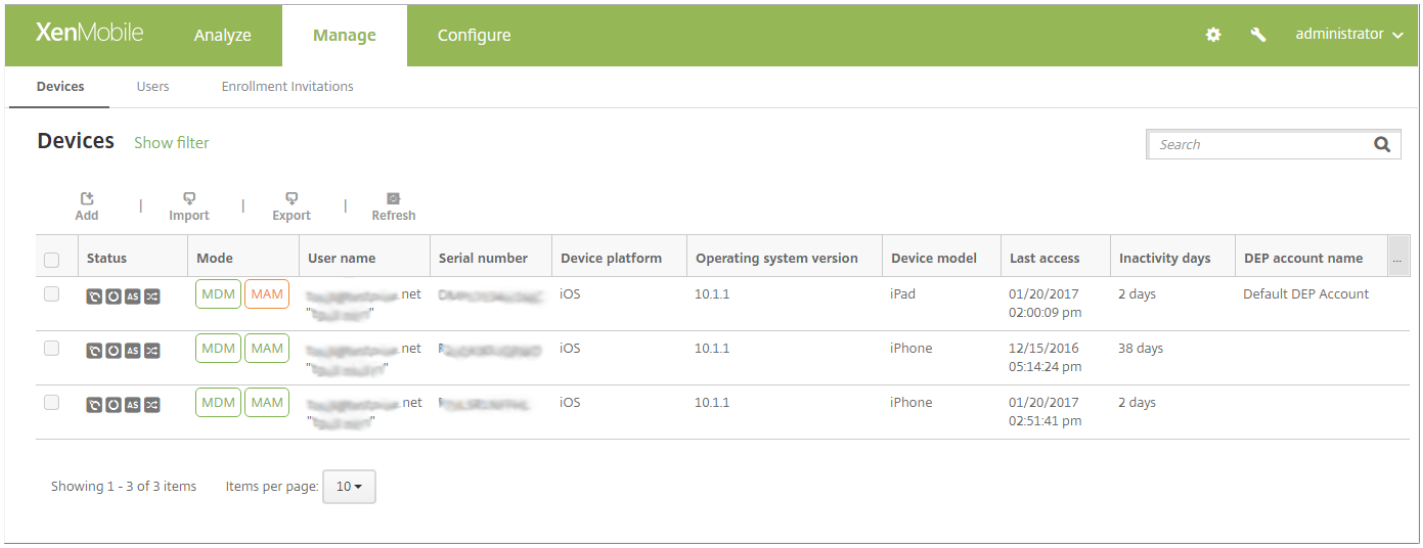
1. Configure estos parámetros de **User**:

- **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 y PIN

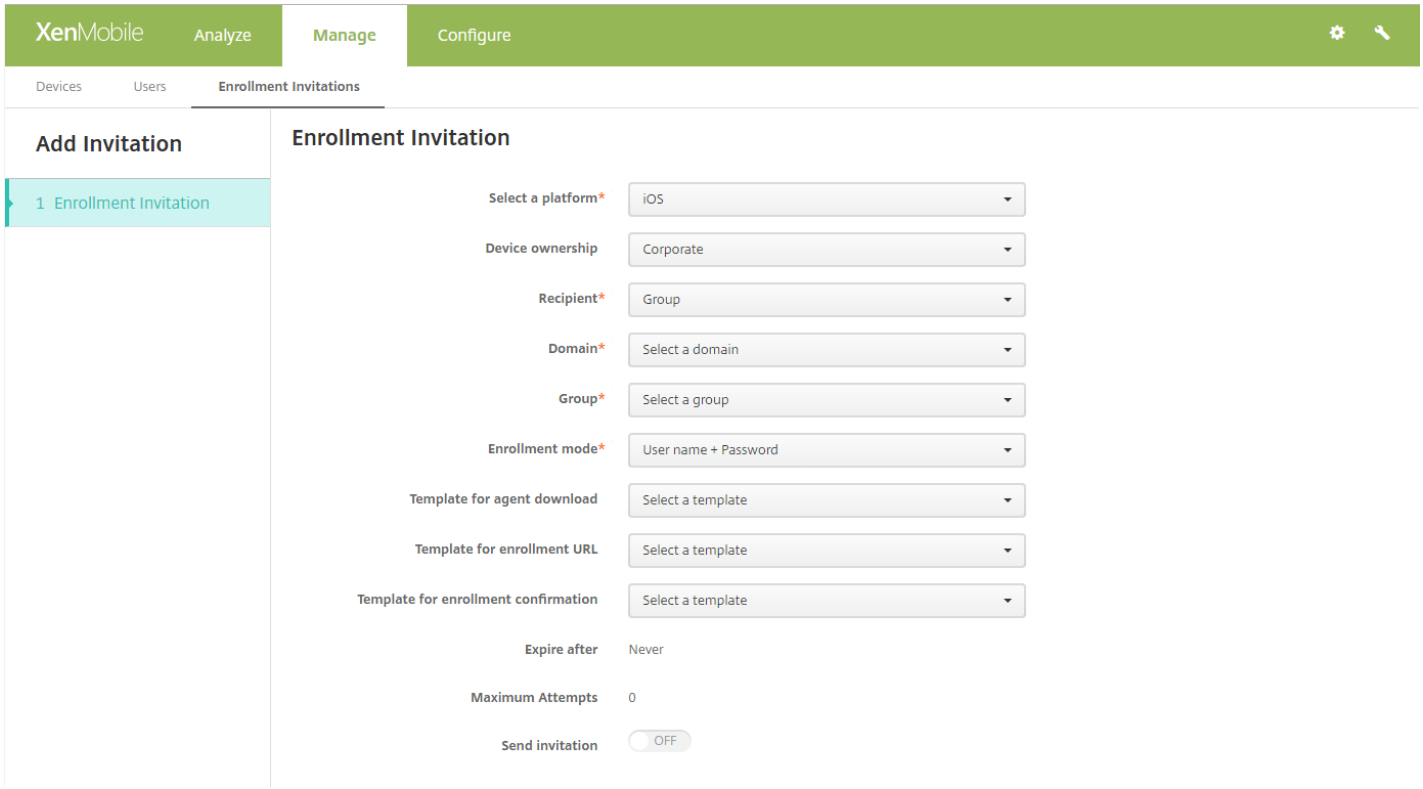
  Nota: Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment PIN**, donde deberá hacer clic en **Enrollment PIN**.

- **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 los modos de inscripción, consulte Para configurar modos de inscripción.
- **Maximum Attempts**. Este campo se establece cuando se configura el modo de inscripción (en **Enrollment Mode**) e indica la cantidad máxima de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar los 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 Invitations**.

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 Invitations**.



Para enviar una invitación de inscripción a un grupo



1. Configure estos parámetros:

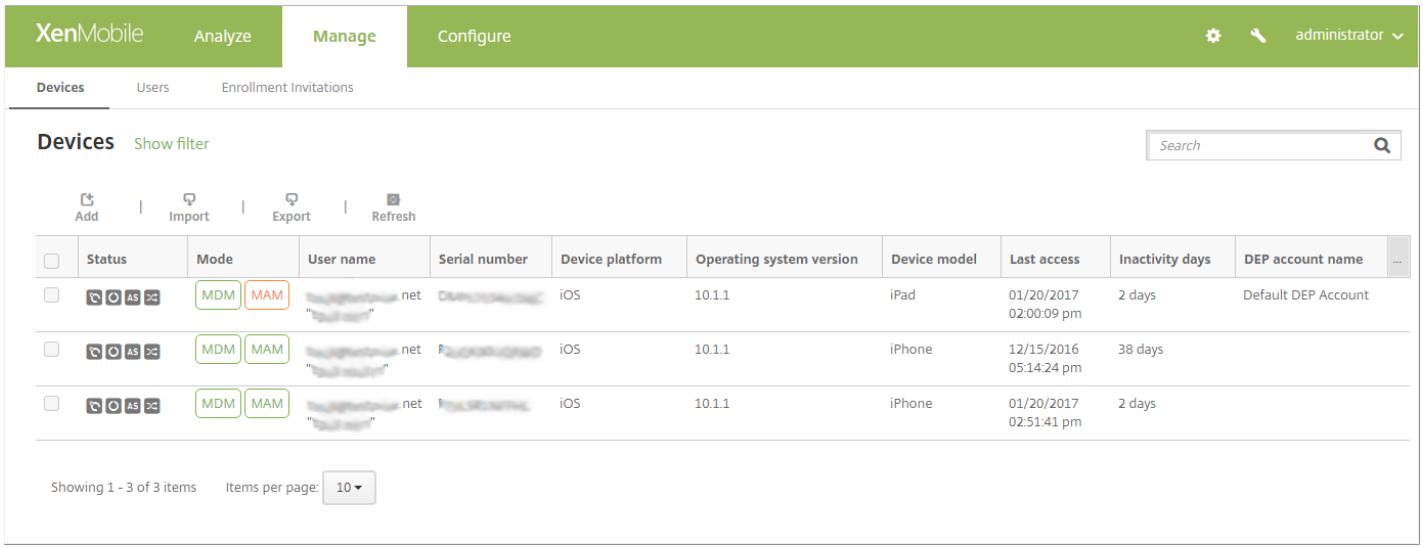
- **Domain**. En la lista, haga clic en el dominio del que se seleccionará el grupo.
- **Group**. En la lista, haga clic en el grupo que recibirá la invitación.
- **Enrollment mode**. En la lista, haga clic en la forma en que quiere que los usuarios del grupo se inscriban. El valor predeterminado es **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 y PIN

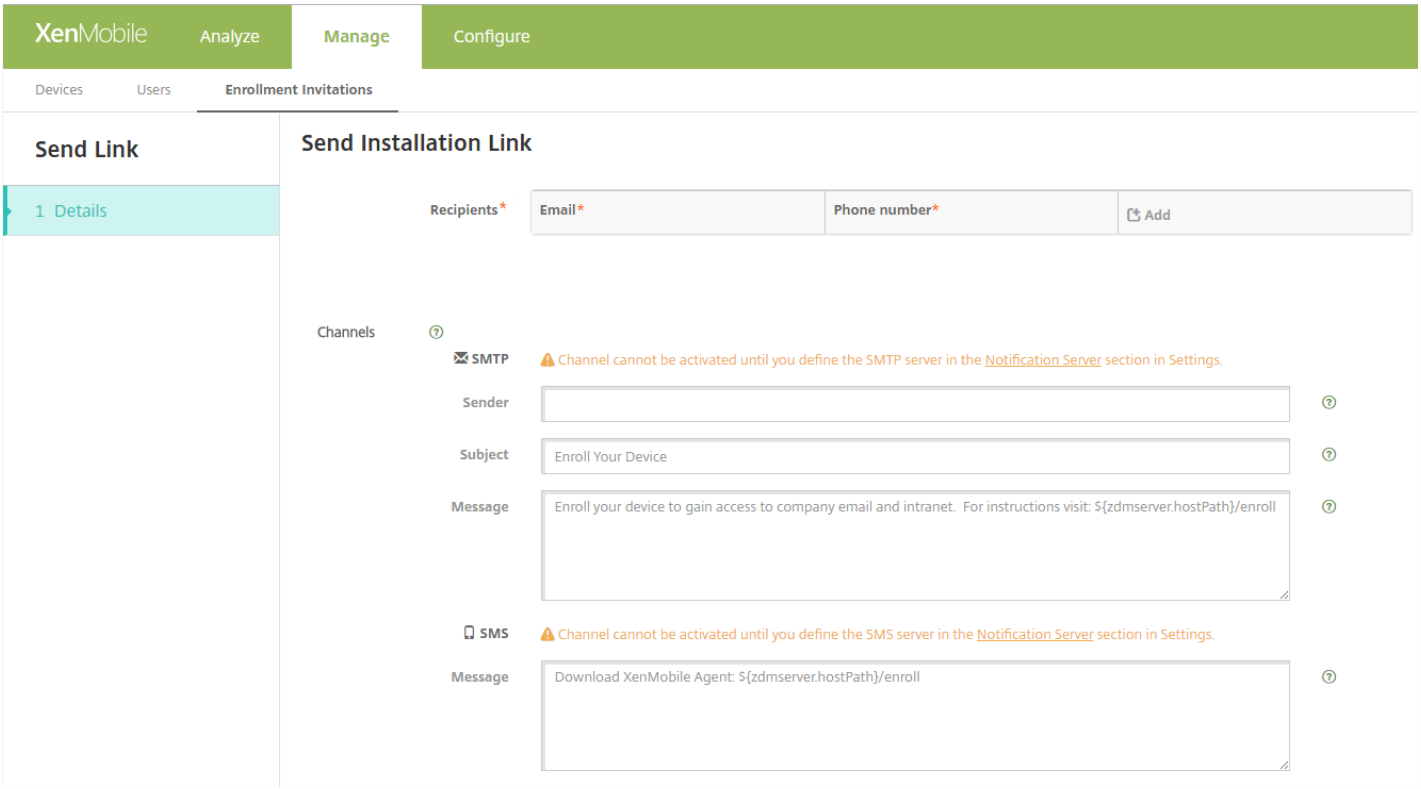
  Nota: Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment PIN**, donde deberá hacer clic en **Enrollment PIN**.

- **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 los modos de inscripción, consulte Para configurar modos de inscripción.
- **Maximum Attempts**. Este campo se establece cuando se configura el modo de inscripción (en Enrollment Mode) e indica la cantidad máxima de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar los 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 Invitations**.

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 Invitations**.



Para enviar un enlace de instalación



Para poder enviar un enlace de instalación para la inscripción, antes debe configurar canales (SMTP o SMS) en el servidor de notificaciones. Puede hacerlo desde la página **Settings**. Para obtener más detalles, consulte Notificaciones.

1. Configure estos parámetros:

- **Recipient**. Para agregar cada destinatario, 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 **Save**.

    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 detalles, consulte Notificaciones.
  - **SMTP**. La configuración de estos parámetros es opcional. 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:
    - **Remitente**. 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 reciban la invitación y hagan clic en el enlace, deberán 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.

Límite de inscripción de dispositivos

Feb 27, 2017

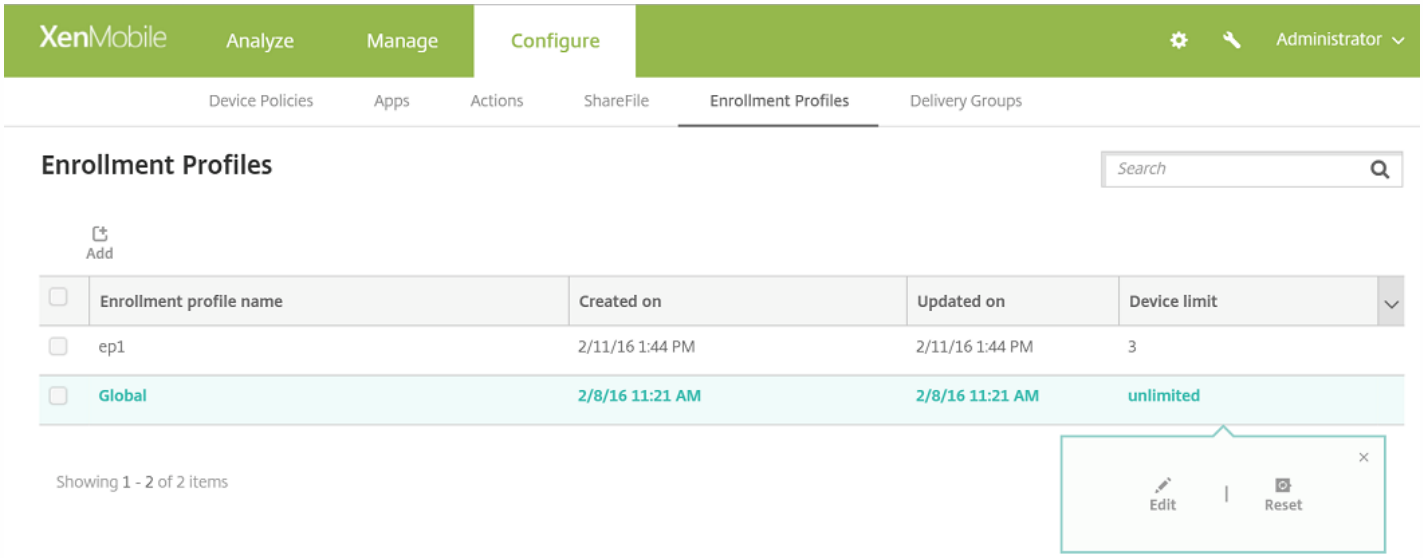
Puede limitar la cantidad de dispositivos que un usuario puede inscribir desde **Configure > Enrollment Profiles** en la consola de XenMobile, en los modos de servidor ENT, MDM y MAM. Las limitaciones se pueden aplicar de forma global o por grupos de entrega. Puede crear varios perfiles de inscripción 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.

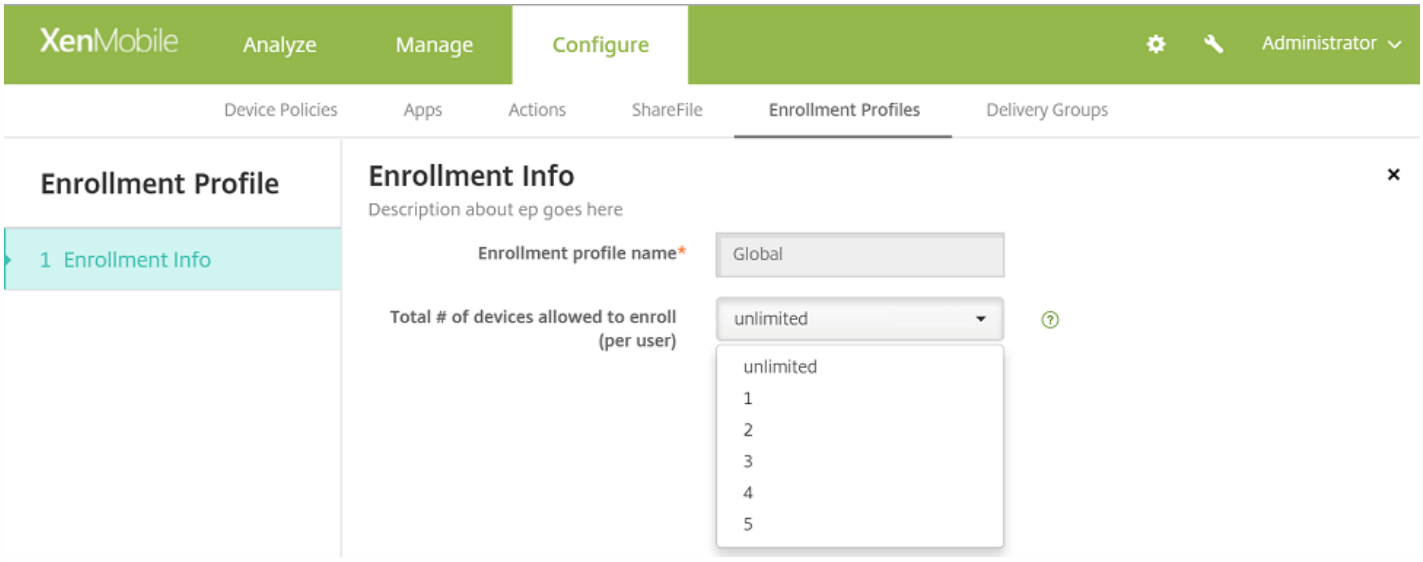
Para configurar un límite global de inscripción de dispositivos

1. Vaya a **Configure > Enrollment Profiles**.

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



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

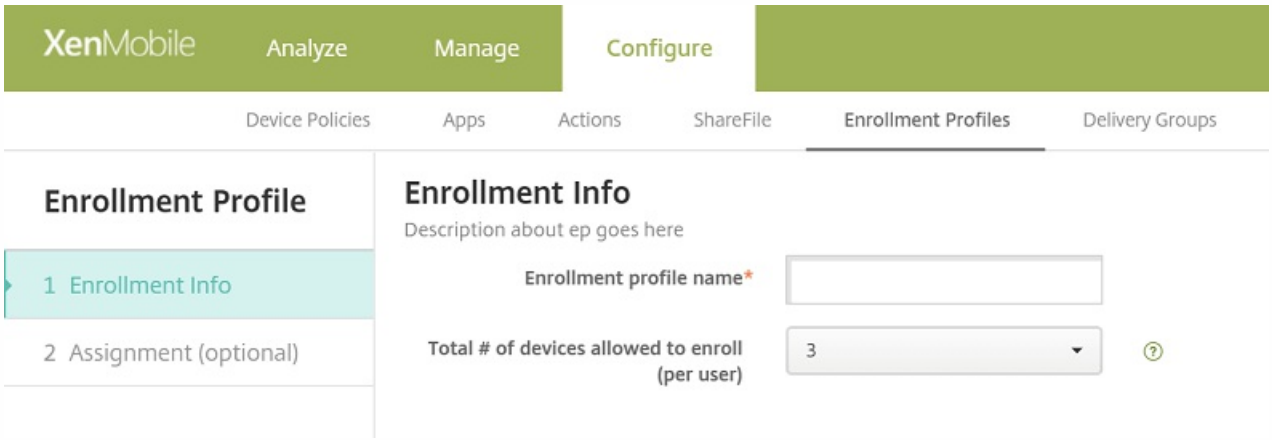


Para configurar un límite de inscripción de dispositivos para un grupo de entrega

1. Vaya a **Configure > Enrollment Profiles > Add**.

   Aparecerá la pantalla **Enrollment Info**.

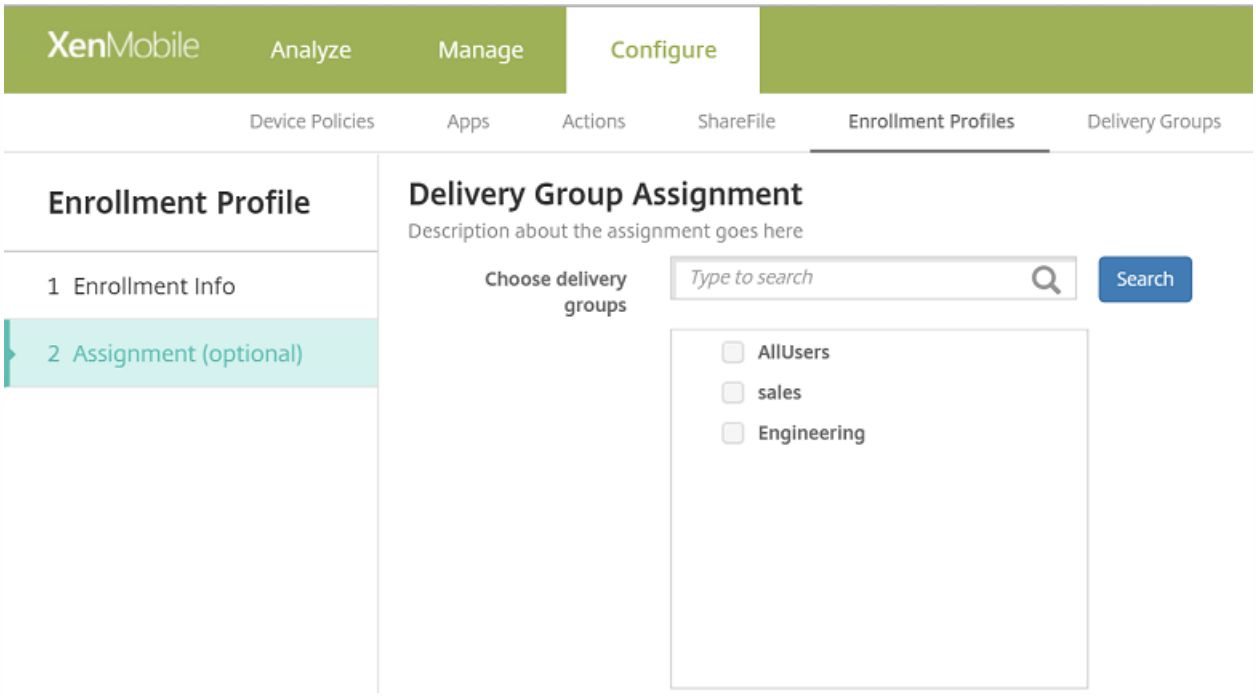
2. Escriba un nombre para el nuevo perfil de inscripción y, a continuación, seleccione la cantidad de dispositivos que podrán inscribir los miembros de este perfil.



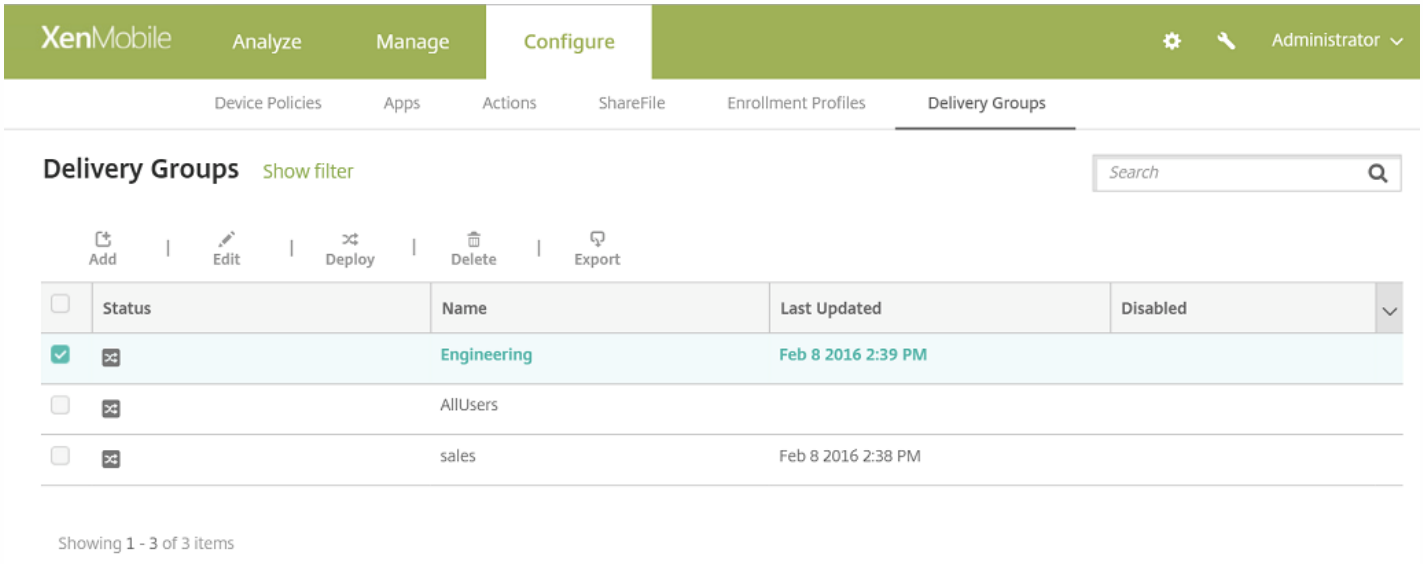
3. Haga clic en **Next**.

   Aparecerá la pantalla **Delivery Group Assignment**.

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

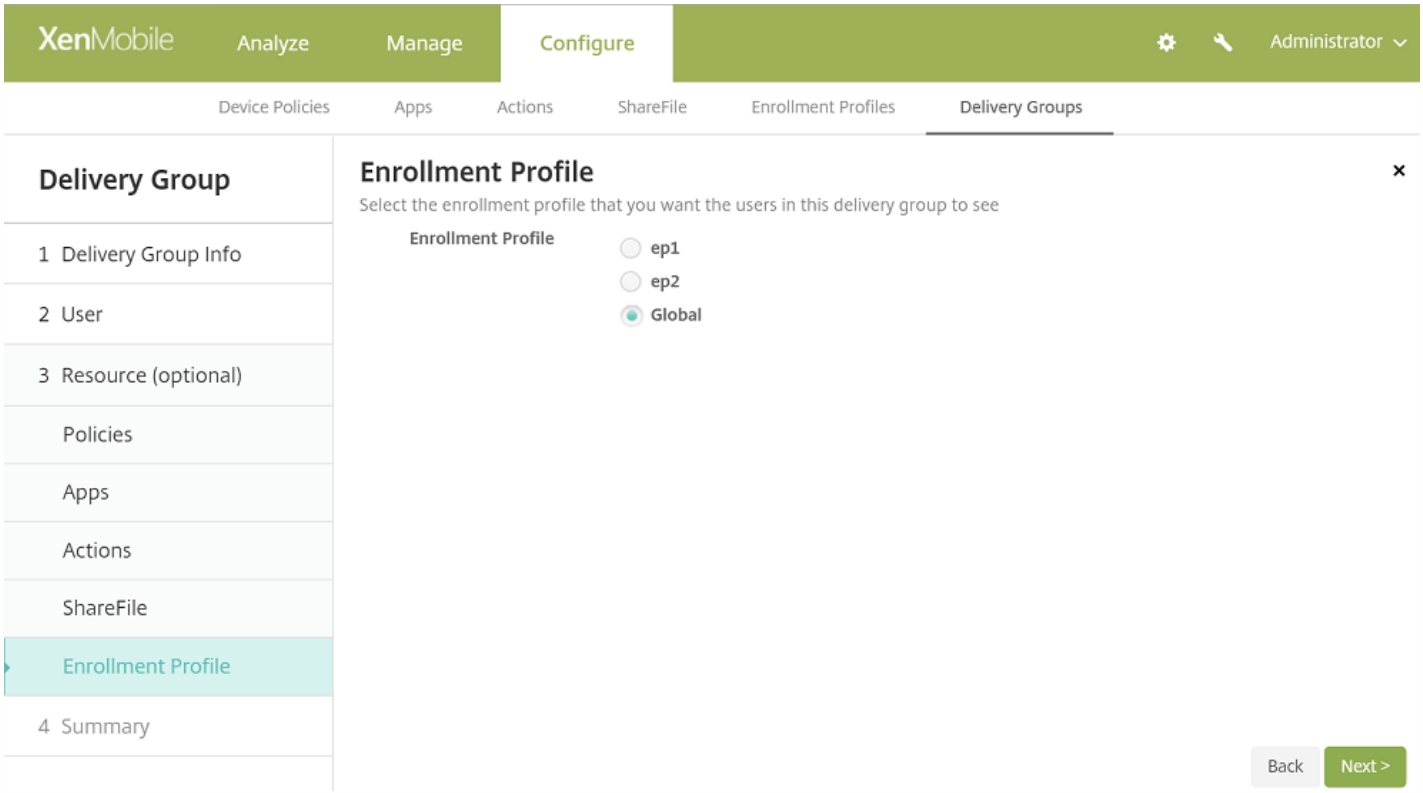


Si más adelante quiere cambiar el perfil de inscripción de un grupo de entrega, vaya a **Configure > Delivery Groups**. Seleccione el grupo en cuestión y haga clic en **Edit**.



Aparecerá la pantalla **Enrollment Profile**.

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



Experiencia del usuario con un límite de inscripción de dispositivos

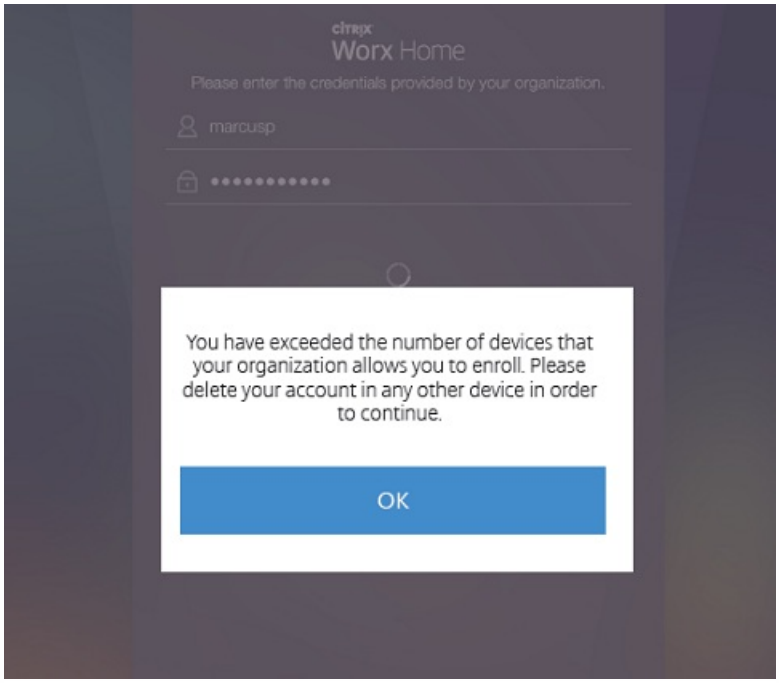
Cuando se establece el límite de inscripción de dispositivos y los usuarios intentan inscribir un dispositivo, siguen estos pasos:

1. Inician sesión en Secure Hub.

2. Escriben la dirección del servidor en que inscribirse.

3. Introducen las credenciales.

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



Aparece de nuevo la pantalla de inscripción de Secure Hub.

Dispositivos compartidos

Feb 27, 2017

XenMobile permite configurar dispositivos que se puedan 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 Citrix, Touch ID, la autenticación de dos factores ni la entropía de usuario.

Modo MDM+MAM

- Disponible solo en tabletas iOS y Android.
- Respaldado en XenMobile 10.3.x y versiones posteriores.
- Solo se respalda la autenticación de nombre de usuario y contraseña de Active Directory.
- No se admiten la autenticación de certificados de cliente, el PIN de Citrix, Touch ID ni la entropía de usuario.
- No se admite el modo solo MAM. Los dispositivos deben inscribirse en MDM.
- Solo se da respaldo a Secure Mail, Secure Web y la aplicación móvil de ShareFile. 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 XenMobile y aplicaciones MDX empaquetadas; no pueden compartir aplicaciones nativas en los dispositivos.
- Una vez se hayan descargado durante la primera inscripción, las aplicaciones XenMobile 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 en **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:

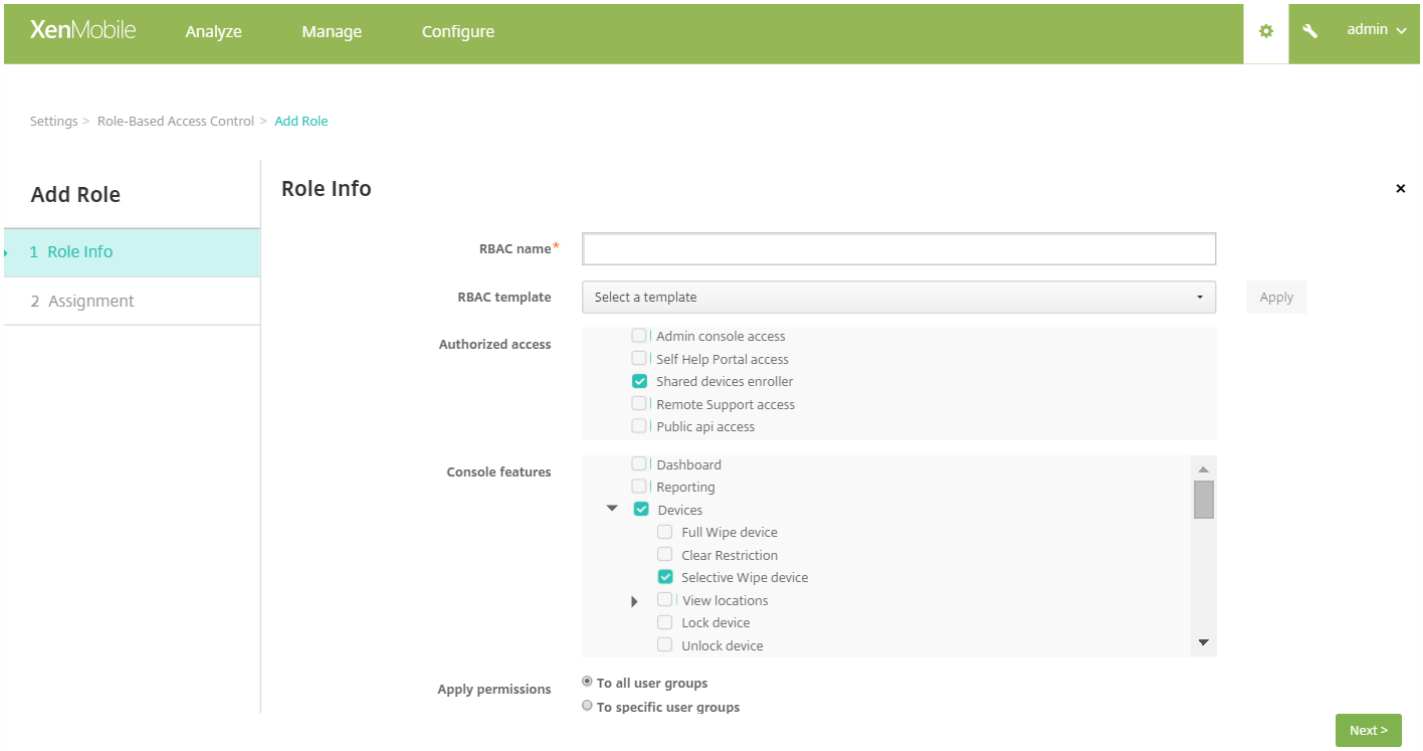
- iOS 9 y 10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (modo solo MDM)

Configuración de un dispositivo compartido

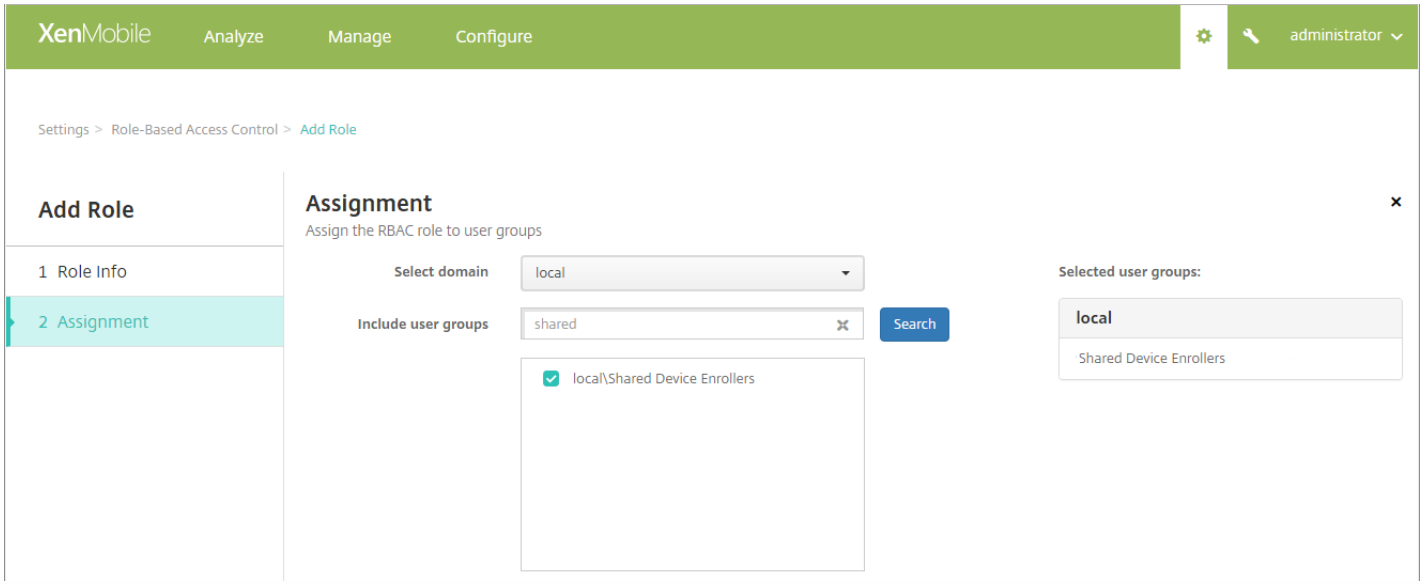
Siga estos pasos para configurar un dispositivo compartido.

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 dispositivos compartidos 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 Secure Hub cuando se anule la inscripción del dispositivo.

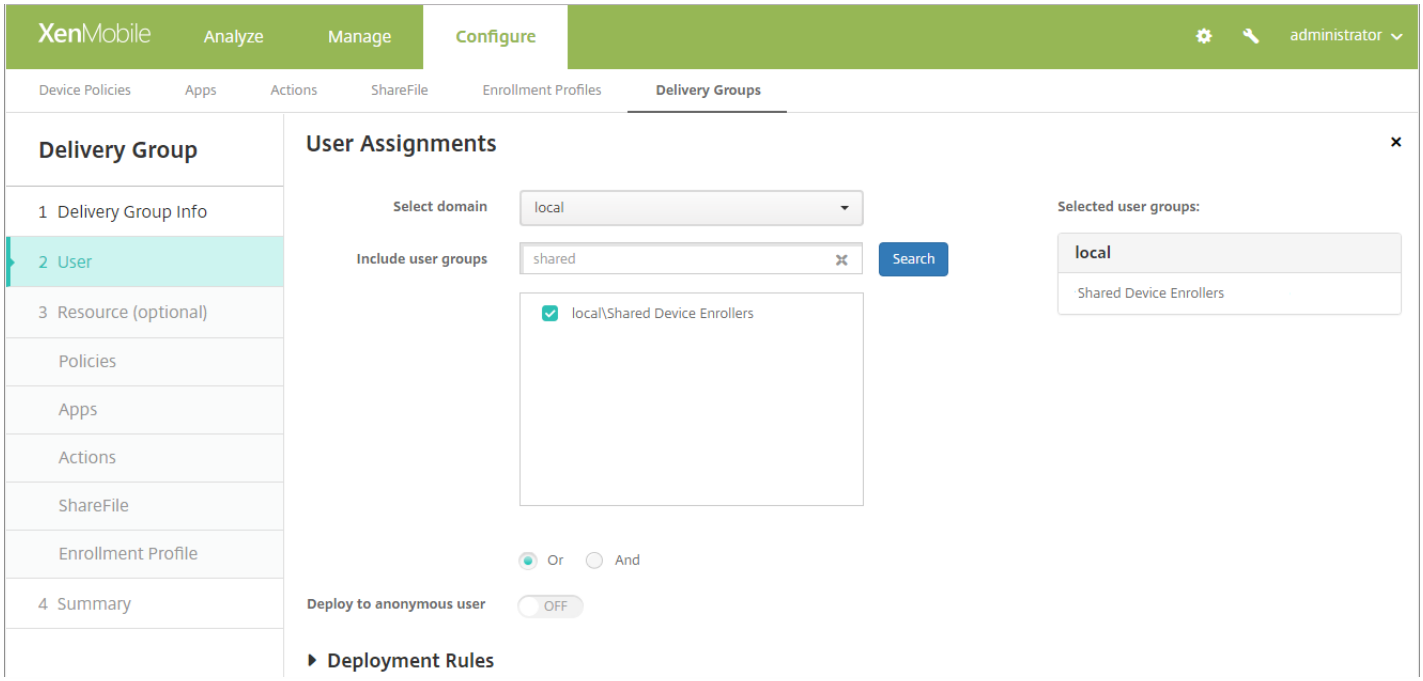
   Para **Apply Permissions**, conserve la configuración predeterminada **To all user groups** o asigne permisos a grupos de usuarios concretos de Active Directory con **To specific user groups**.



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 del usuario de inscripción de dispositivos compartidos.



5. Instale Secure Hub en el dispositivo compartido e inscríbalo en XenMobile con la cuenta del 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 e impleméntelo solo en los 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 Secure Hub, 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

Secure Mail y Secure Web se implementan en el dispositivo cuando el usuario de inscripción de dispositivos compartidos los inscribe. Los datos de usuario se conservan de forma segura en el dispositivo. Los datos no se expondrán a otros usuarios cuando estos usen Secure Mail o Secure Web.

Solo un usuario a la vez puede iniciar sesión en Secure Hub. El usuario anterior debe finalizar la sesión antes de que el siguiente pueda iniciarla. Por motivos de seguridad, Secure Hub 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, Secure Hub 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 recomendadas para Secure Mail

- Para conseguir el mejor funcionamiento de Secure Mail, 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
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 parámetros siguientes para cada usuario. Todos los demás parámetros serán comunes entre los usuarios que compartan el dispositivo:

  Notifications
  Signature
  Out of Office
  Sync Mail Period
  S/MIME
  Check Spelling.

Android at Work

Feb 27, 2017

Android at Work (antes conocido como Android for Work) es un espacio de trabajo seguro disponible en los dispositivos Android que ejecuten Android 5.0 y versiones posteriores. Ese espacio de trabajo aísla las cuentas, las aplicaciones y los datos empresariales de las cuentas por un lado, y las aplicaciones y los datos personales por el otro. En XenMobile, puede administrar tanto dispositivos BYOD (dispositivos personales utilizados en el trabajo) como los dispositivos Android propiedad de la empresa. Para ello, el usuario deberá crear un perfil profesional independiente en sus dispositivos. Mediante la combinación del cifrado de hardware y las directivas que implemente, separará de forma segura los espacios empresarial y personal en un dispositivo. Puede administrar o borrar de forma remota todas las directivas, las aplicaciones y los datos empresariales sin que ello afecte al área personal del usuario. Para obtener más información acerca de los dispositivos Android compatibles, consulte el sitio Web Google Android Enterprise.

Se utiliza Google Play para agregar, comprar y aprobar aplicaciones para su implementación en el espacio de trabajo de Android at Work del dispositivo. Se puede utilizar Google Play para implementar aplicaciones privadas de Android, así como aplicaciones públicas o de terceros. Cuando agrega una aplicación de tienda pública de aplicaciones a Android at Work, puede ver el estado de las licencias de compra en bloque. Ese estado está compuesto por la cantidad total de las licencias disponibles, la cantidad actualmente en uso y la dirección de correo electrónico de cada usuario que consume cada licencia. Para obtener más información sobre cómo agregar una aplicación a XenMobile, consulte Para agregar una aplicación de tienda pública de aplicaciones a XenMobile.

Requisitos de Android at Work:

- Un dominio accesible públicamente
- Una cuenta de administrador de Google
- Dispositivos que ofrezcan respaldo para perfiles administrados y ejecuten Android 5.0 Lollipop o versiones posteriores
- Una cuenta de Google que tenga Google Play instalado
- Un perfil de Work instalado en el dispositivo

Antes de establecer las restricciones de las aplicaciones Android at Work, deberá llevar a cabo lo siguiente:

- Complete, en Google, las tareas de configuración de Android at Work.
- Cree un conjunto de credenciales de Google Play.
- Configure el servidor Android at Work.
- Cree al menos una directiva de dispositivo Android at Work.
- Agregue, compre y apruebe aplicaciones de Android at Work en la tienda de aplicaciones Google Play.

Cuando administre Android at Work, puede utilizar los siguientes enlaces:

- Consola de administración de Google: https://admin.google.com/AdminHome
- Consola de administración de Google Play: https://play.google.com/work/apps
- Publicación en Google Play de aplicaciones alojadas en servidores propios y de canal privado: https://play.google.com/apps/publish
- Google Developer Console para crear cuentas de servicio: https://console.developers.google.com

Requisitos previos de Android at Work

Para poder administrar Android en XenMobile, debe hacer lo siguiente:

- Crear una cuenta de Android at Work.
- Configurar una cuenta de servicio.
- Descargar un certificado de Android at Work.
- Habilitar y autorizar las API de MDM y Admin SDK de Google.
- Autorizar a la cuenta de servicio para que use y Google Play y Google Directorio.
- 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 y administrar aplicaciones Android en XenMobile. Para obtener más información sobre cómo crear un conjunto de credenciales, consulte Credenciales de Google Play.

Crear una cuenta de Android at Work

Antes de configurar una cuenta de Android at Work, debe cumplir los siguientes requisitos previos:

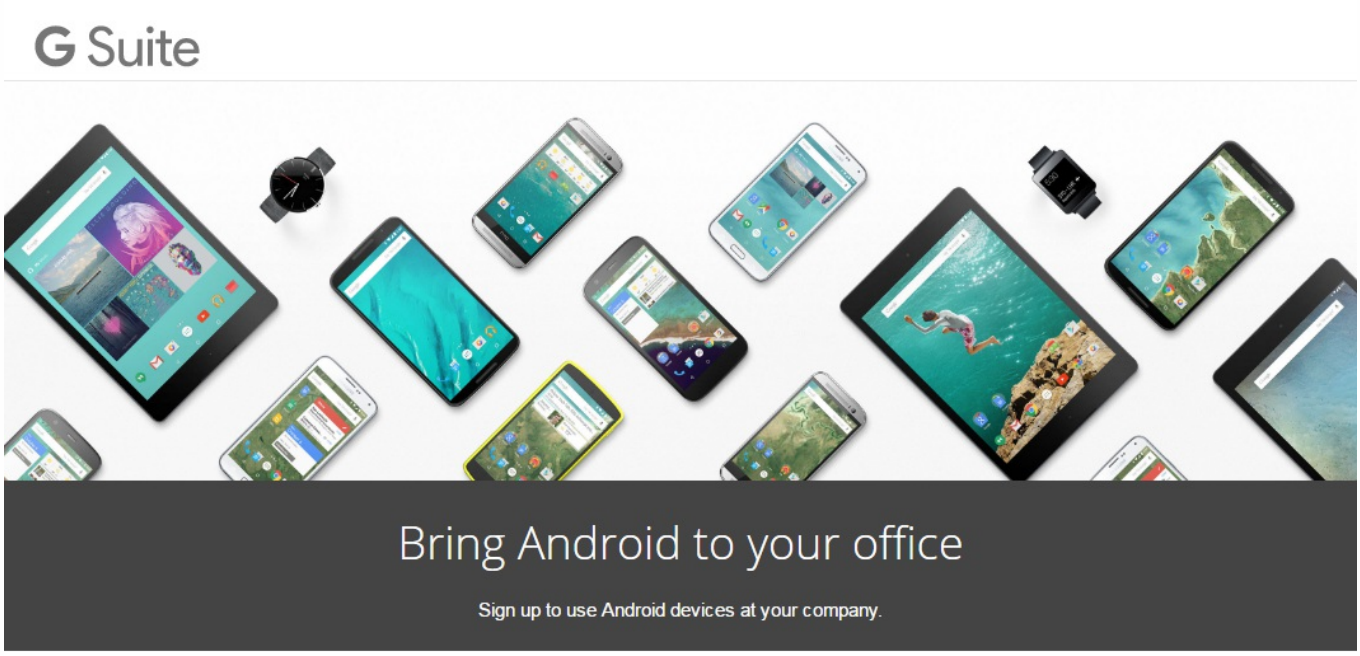
- Disponer de un nombre de dominio; por ejemplo, ejemplo.com.
- Permitir que Google verifique que usted es el propietario del dominio.
- Habilitar y administrar Android at Work a través de un proveedor de administración de movilidad empresarial (EMM), como XenMobile 10.1 o una versión

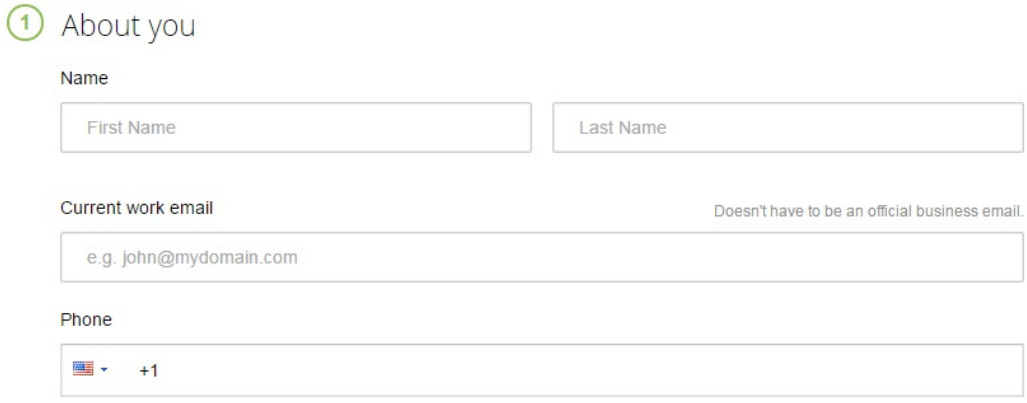
posterior.

Si ya ha verificado el nombre de su dominio con Google, puede pasar a Configuración de una cuenta de servicio de Android at Work y descarga de un certificado de Android at Work.

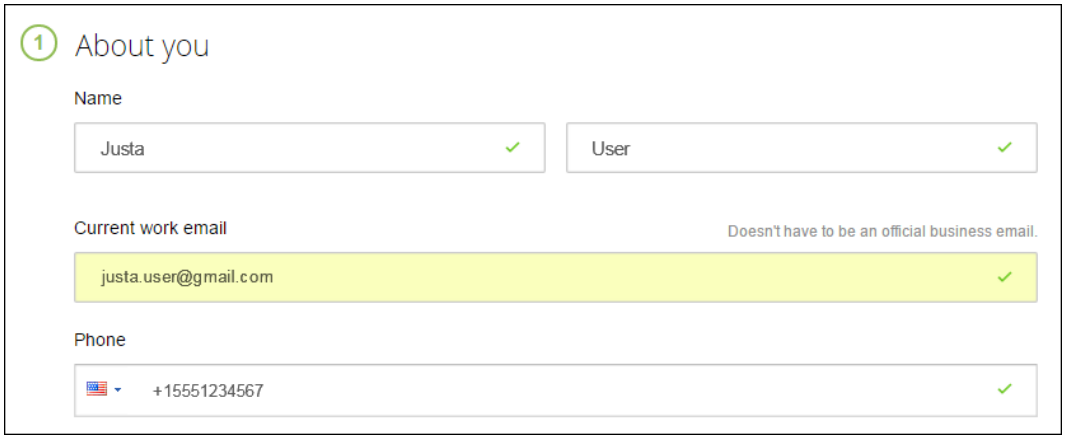
1. Vaya a https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

Aparece la siguiente página, donde puede introducir su información de administrador y la información acerca de la empresa.

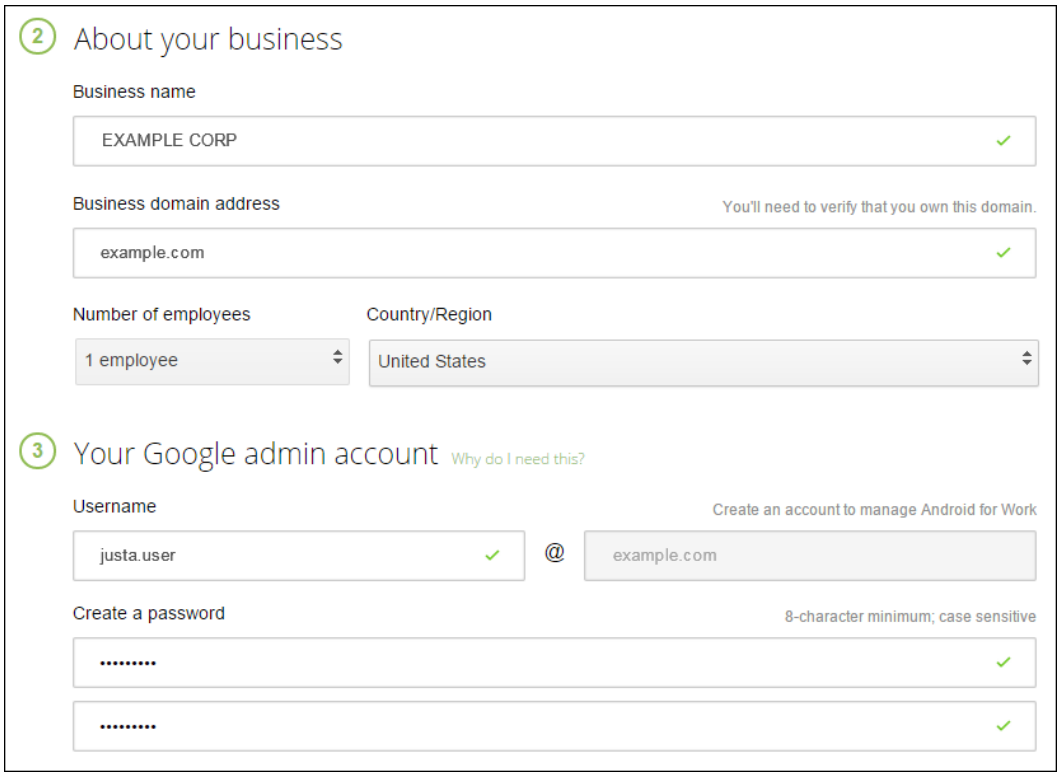




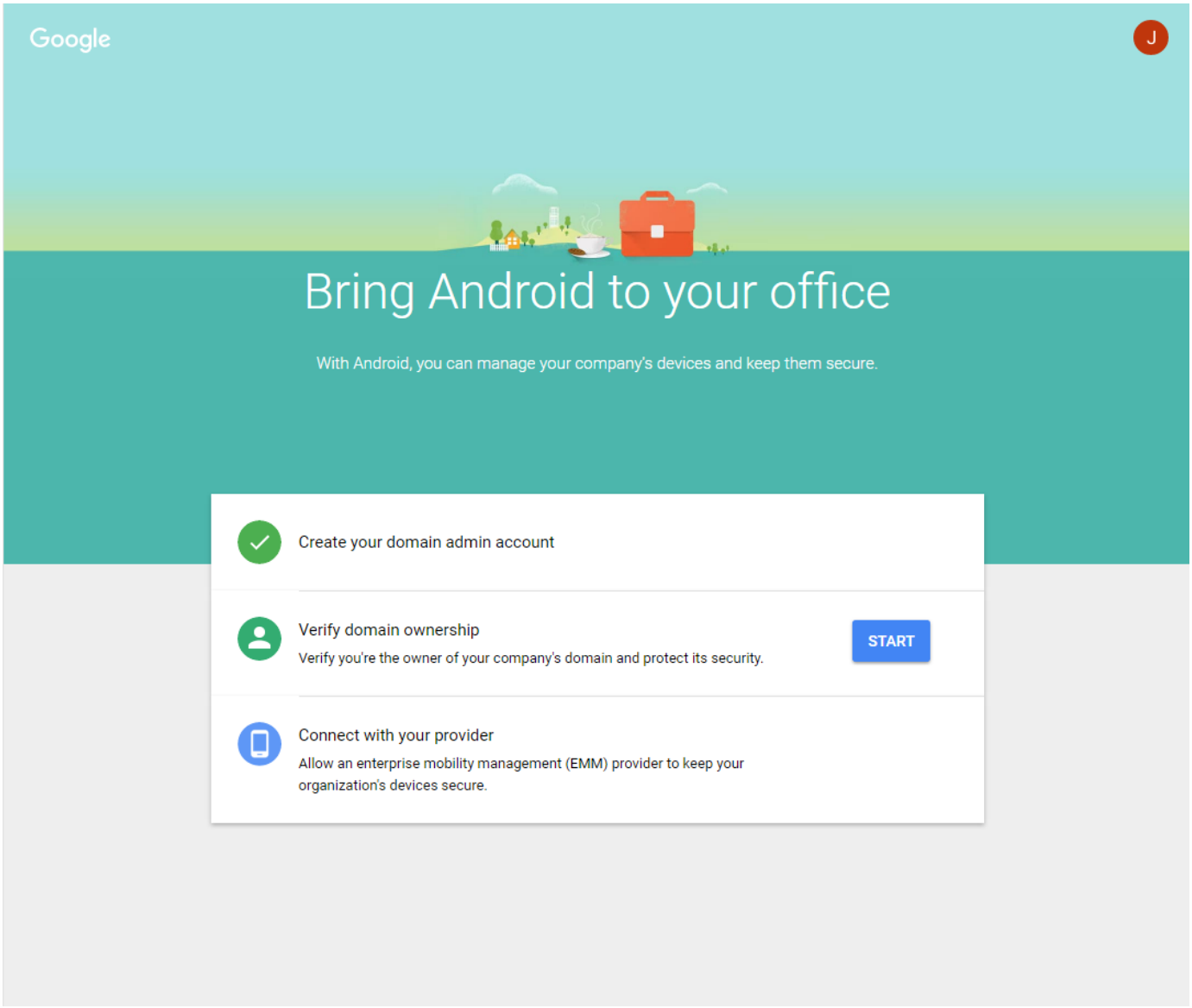
2. Introduzca la información de usuario del administrador.



2. Escriba la información de la empresa, además de la información de su cuenta de administrador.



Una vez completado el primer paso, verá la página siguiente.



Verificación de la propiedad del dominio

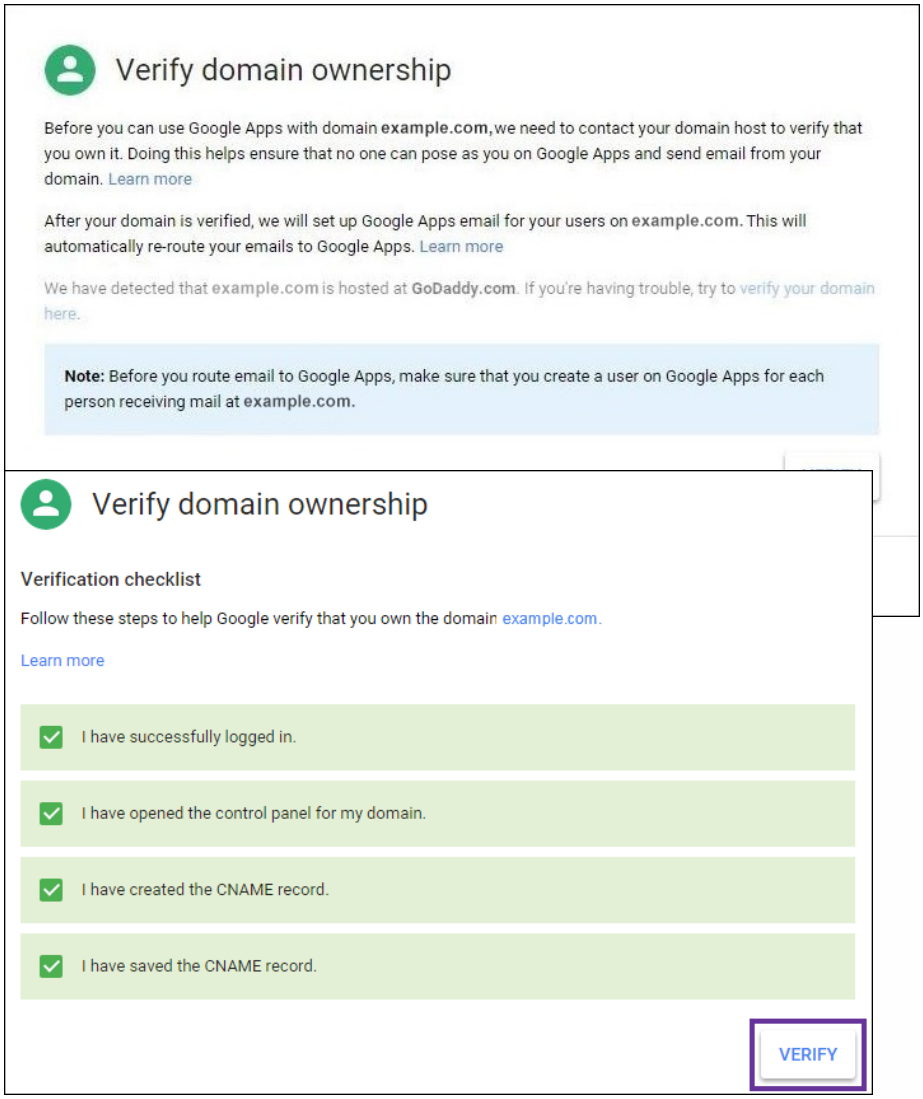
Permita a Google verificar el dominio de alguna de las siguientes maneras:

- Agregue un registro TXT o CNAME al sitio Web de su host de dominio.
- Cargue un archivo HTML en el servidor Web del dominio.
- Agregue una etiqueta META a la página de inicio. 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/.

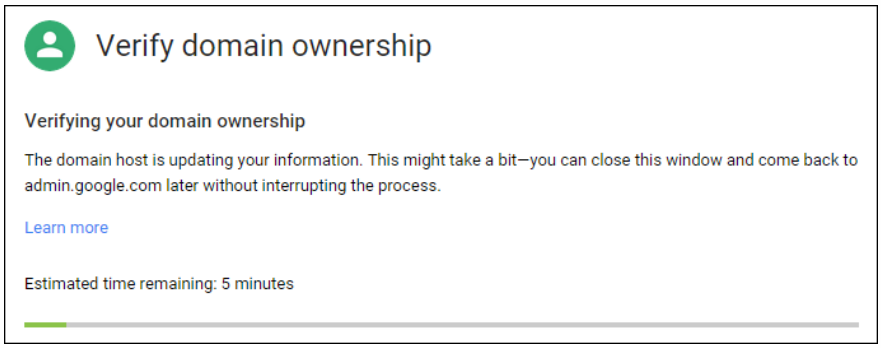
1. Haga clic en **Start** para iniciar la verificación de su dominio.

Verá la página **Verify domain ownership**. Siga las instrucciones de esta página para verificar su dominio.

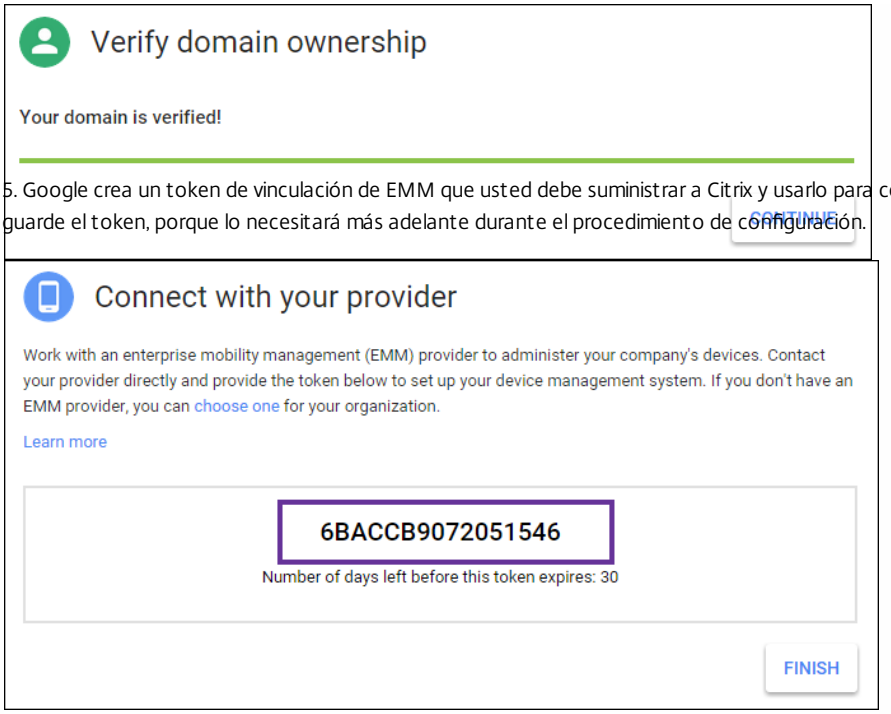
2. Haga clic en **Verify**.



3. Google verifica que usted posee el dominio.



4. Aparecerá la siguiente página tras una verificación correcta. Haga clic en **Continue**.



5. Google crea un token de vinculación de EMM que usted debe suministrar a Citrix y usarlo para configurar los parámetros de Android at 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 at Work. Aparecerá una página que indicará que el dominio se ha verificado correctamente.

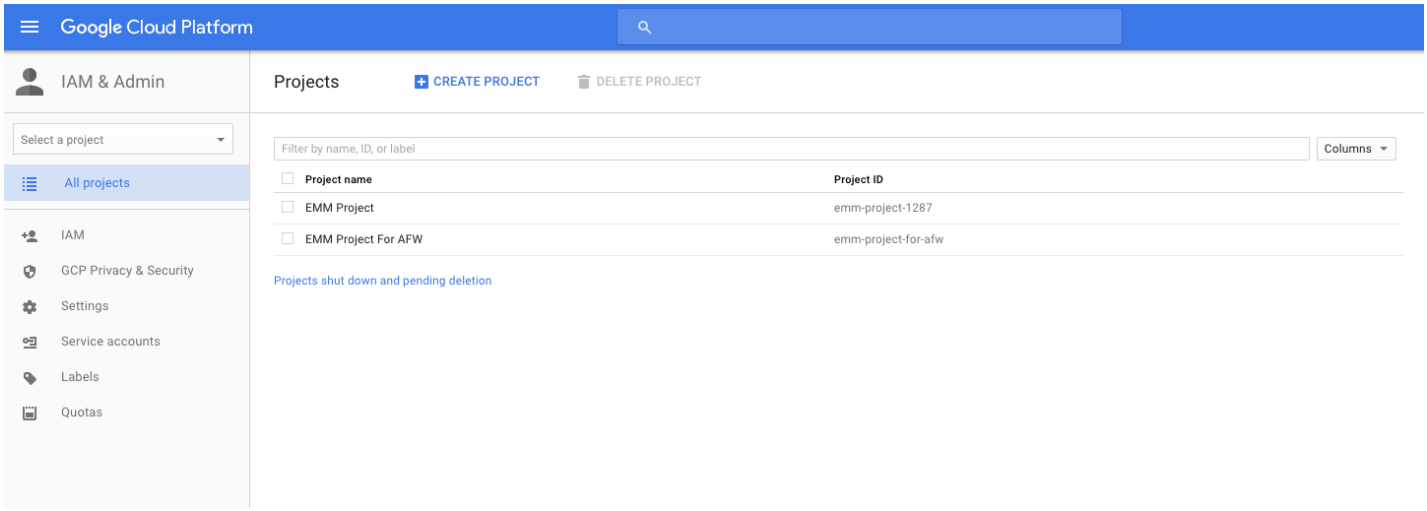
Después de crear una cuenta de servicio de Android at Work, puede iniciar sesión en la consola de administración de Google para administrar sus opciones de movilidad.

Configuración de una cuenta de servicio de Android at Work y descarga de un certificado de Android at Work

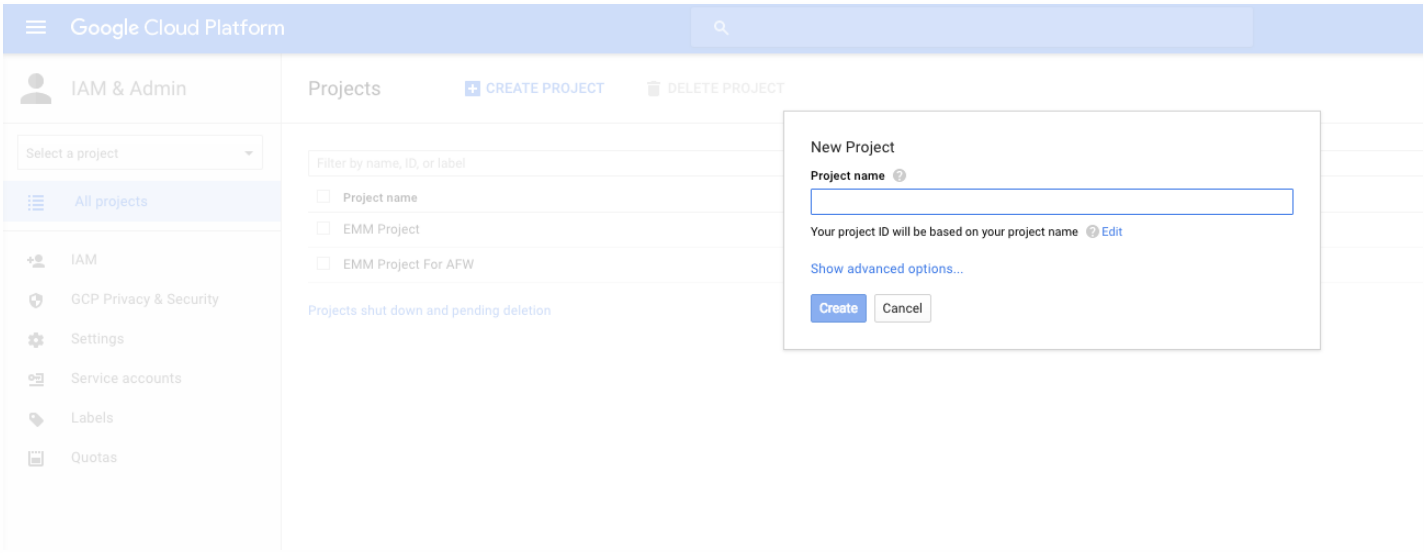
Para permitir que XenMobile establezca contacto con los servicios de Google Play y Google Directorio, debe crear una cuenta de servicio en el portal de proyectos de Google para desarrolladores. Esta cuenta de servicio se utiliza para la comunicación de servidor a servidor entre XenMobile y los servicios de Google para Android. 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.

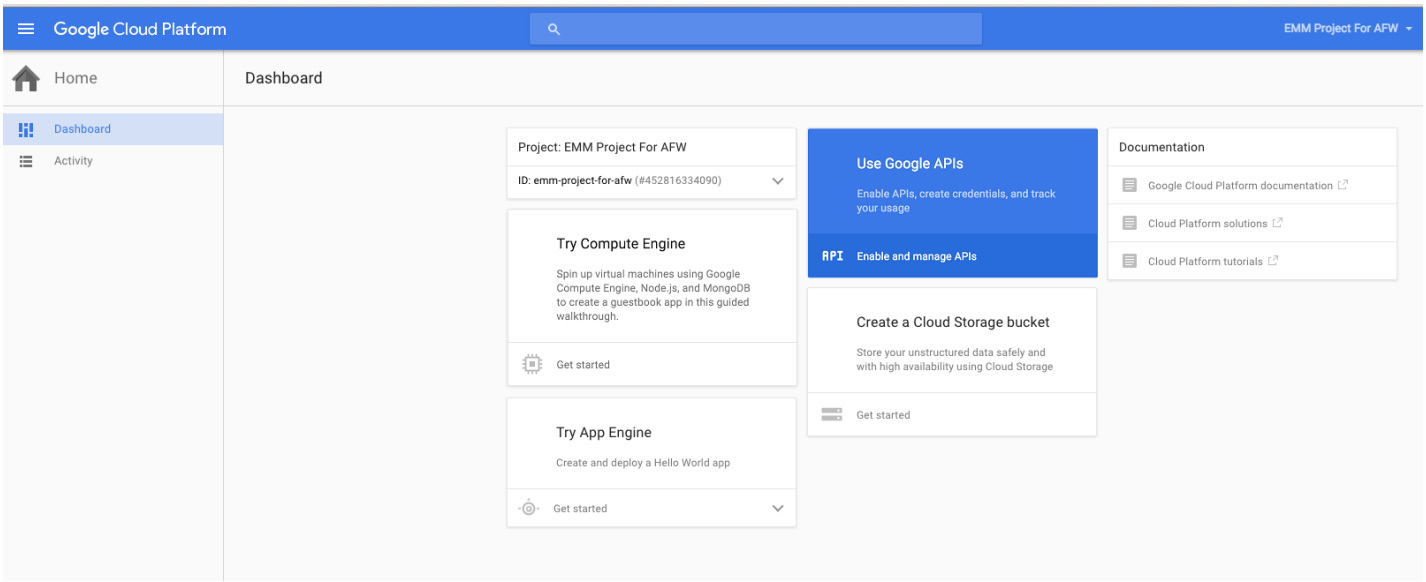
2. En la lista **Projects**, haga clic en **Create Project**.



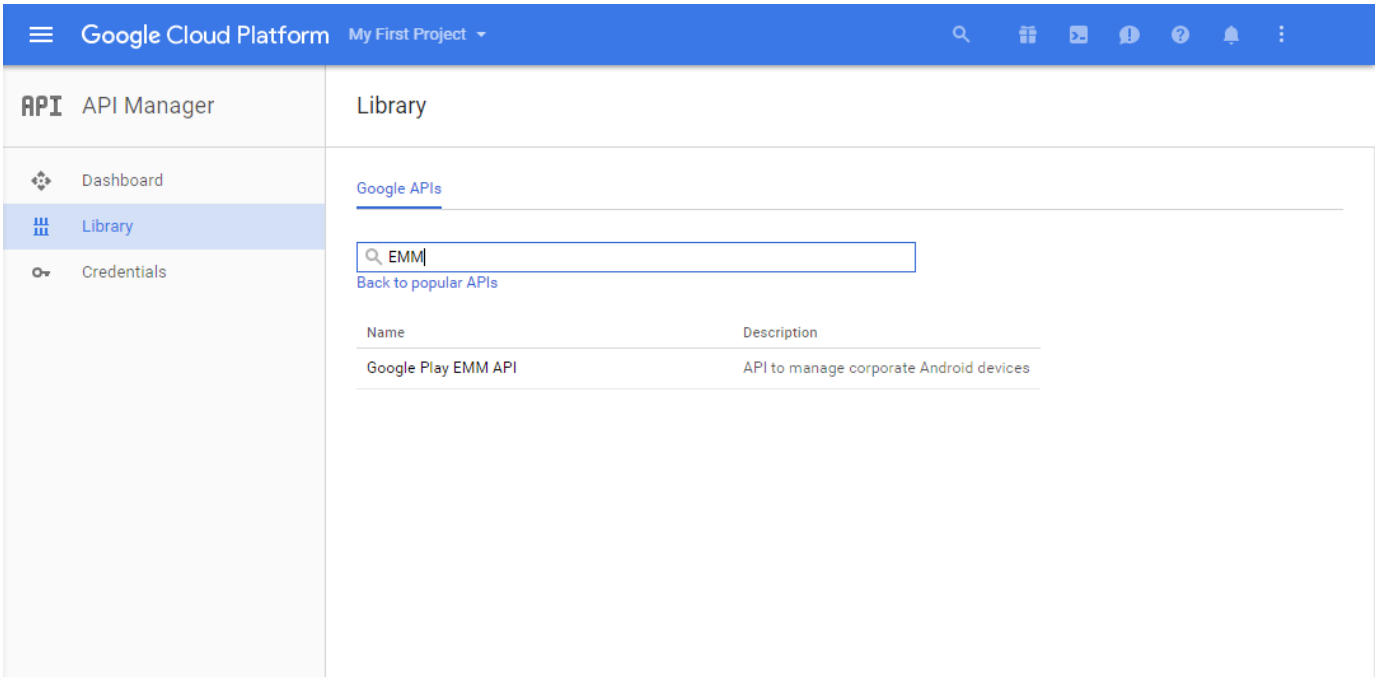
3. En **Project name**, introduzca un nombre para el proyecto.



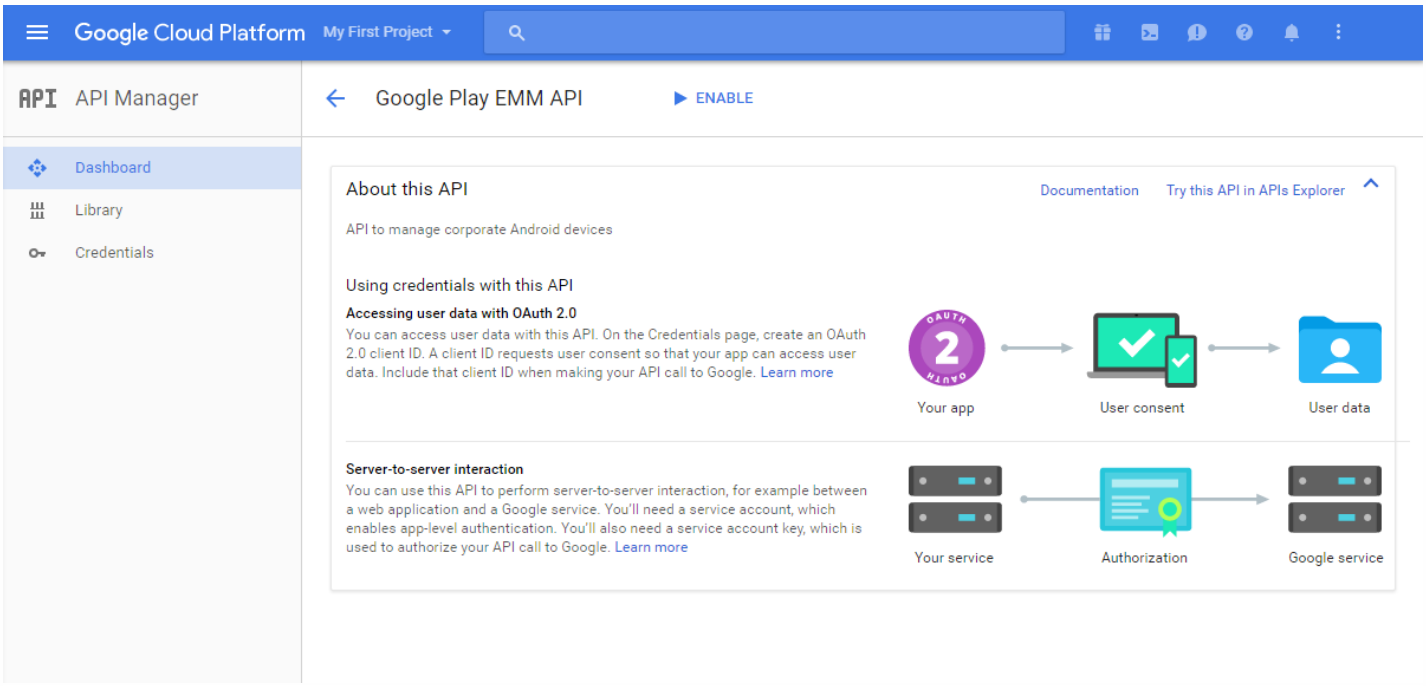
4. En el panel de mandos, haga clic en **Use Google APIs**.



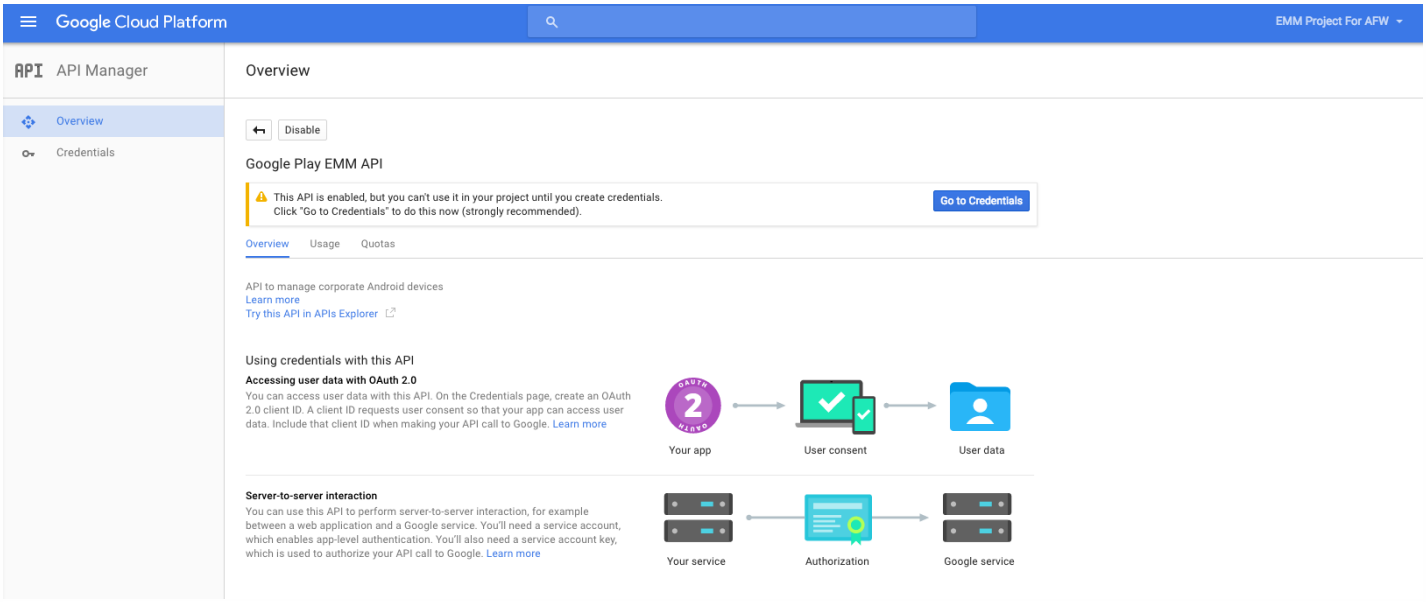
5. Haga clic en **Library** y, en **Search**, escriba **EMM**. A continuación, haga clic en el resultado de la búsqueda.



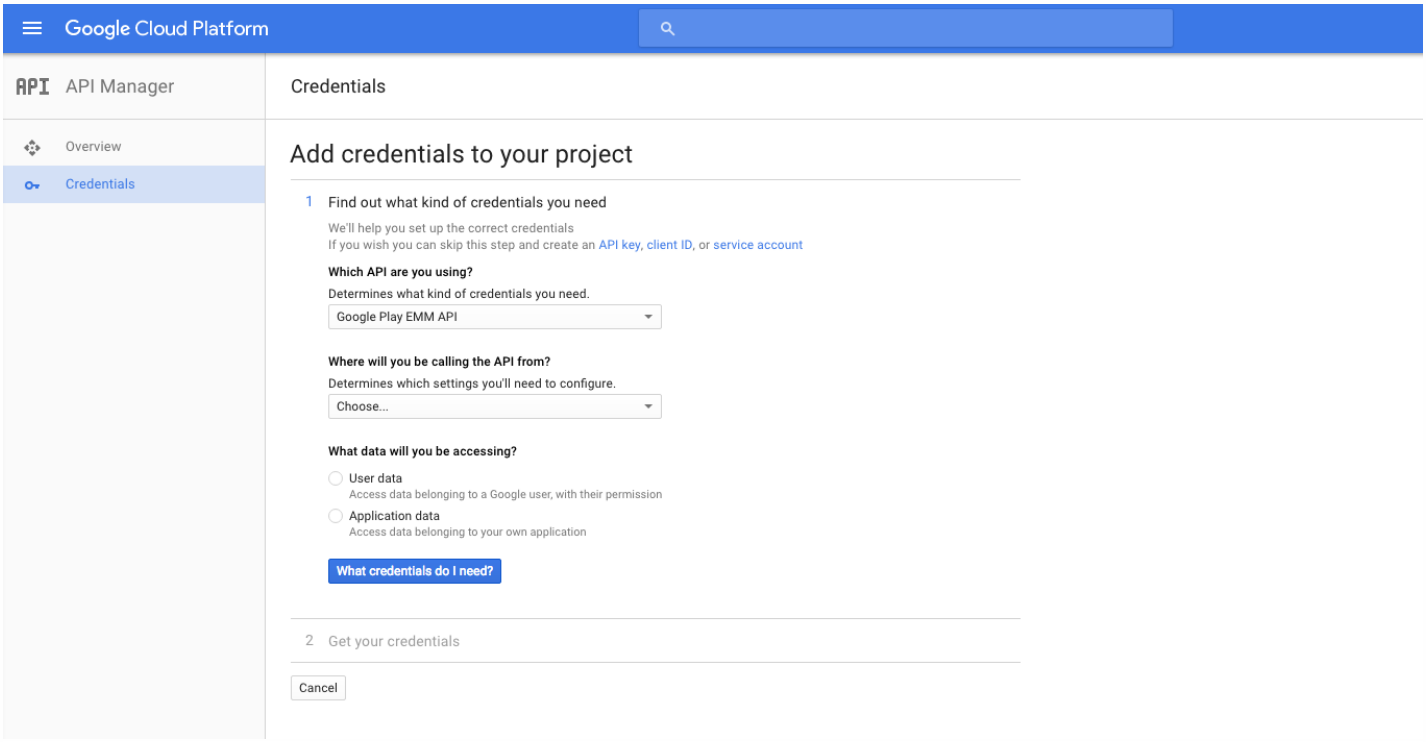
6. En la página **Overview**, haga clic en **Enable**.



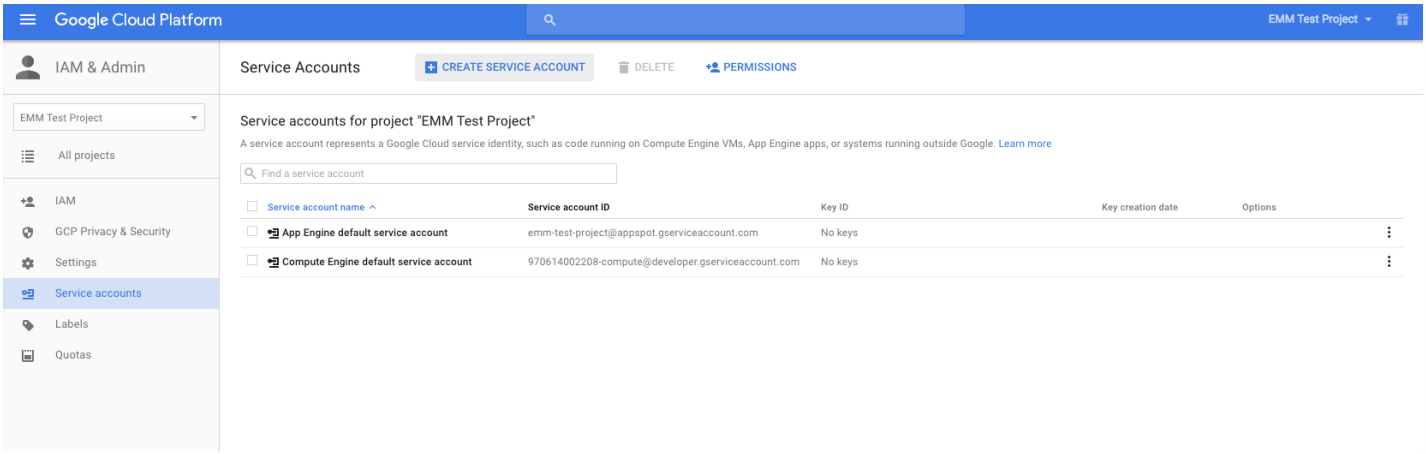
7. Junto a **Google Play EMM API**, haga clic en **Go to Credentials**.



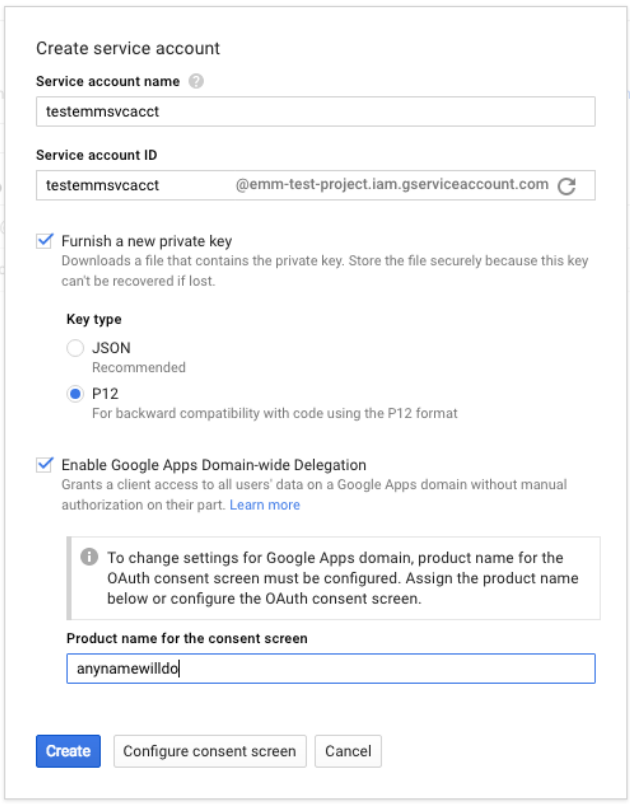
8. En la lista **Add credentials to our project**, en el paso 1, haga clic en **service account**.



9 En la página **Service Accounts**, haga clic en **Create Service Account**.

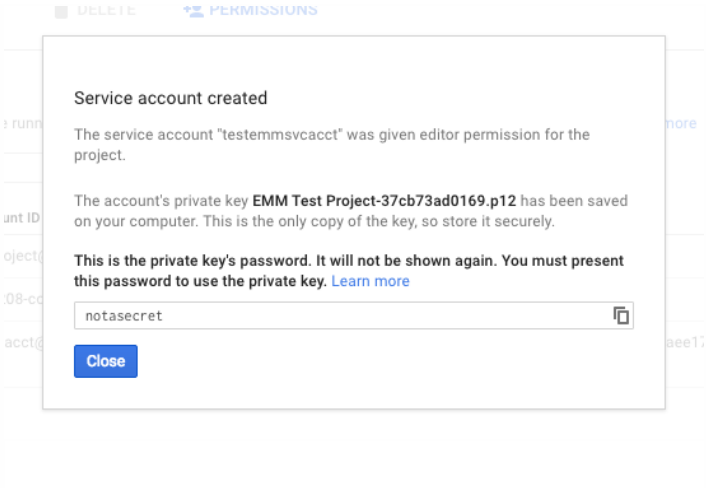


10. En **Create service account**, establezca un nombre para la cuenta y marque la casilla **Furnish a new private key**. Haga clic en **P12**, marque la casilla **Enable Google Apps Domain-wide Delegation** y haga clic en **Create.**

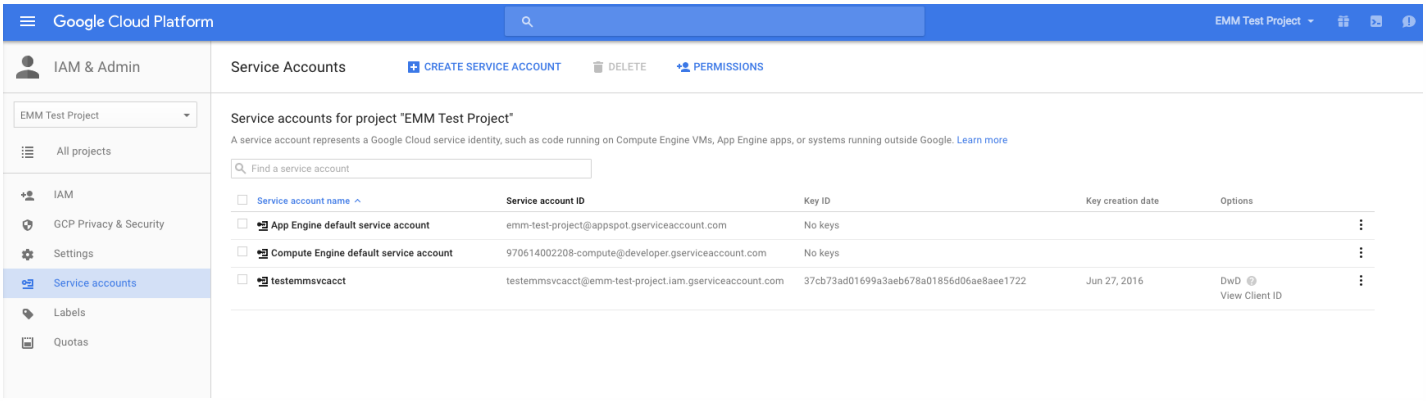


El archivo de certificado (P12) se descargará en su equipo. Guarde el certificado en una ubicación segura.

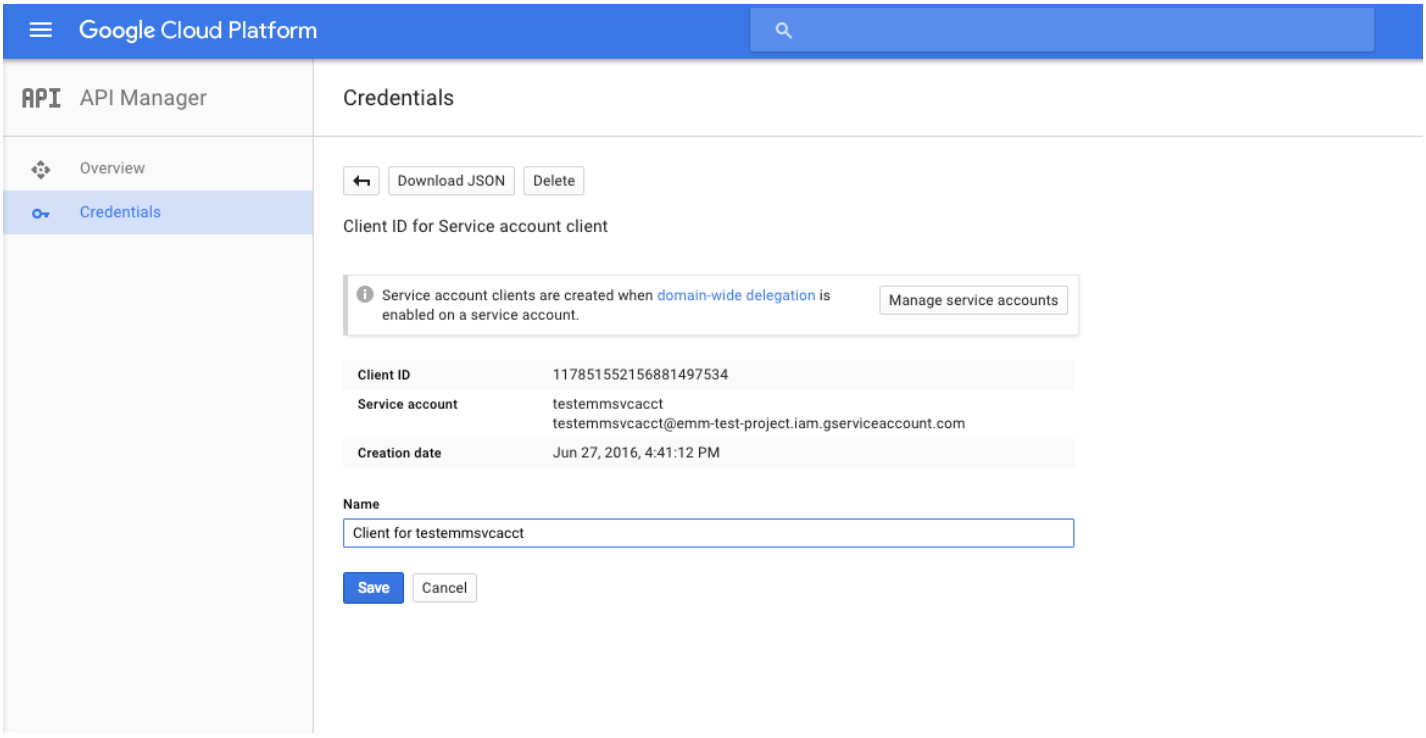
11. En la pantalla de confirmación **Service account created**, haga clic en **Close**.



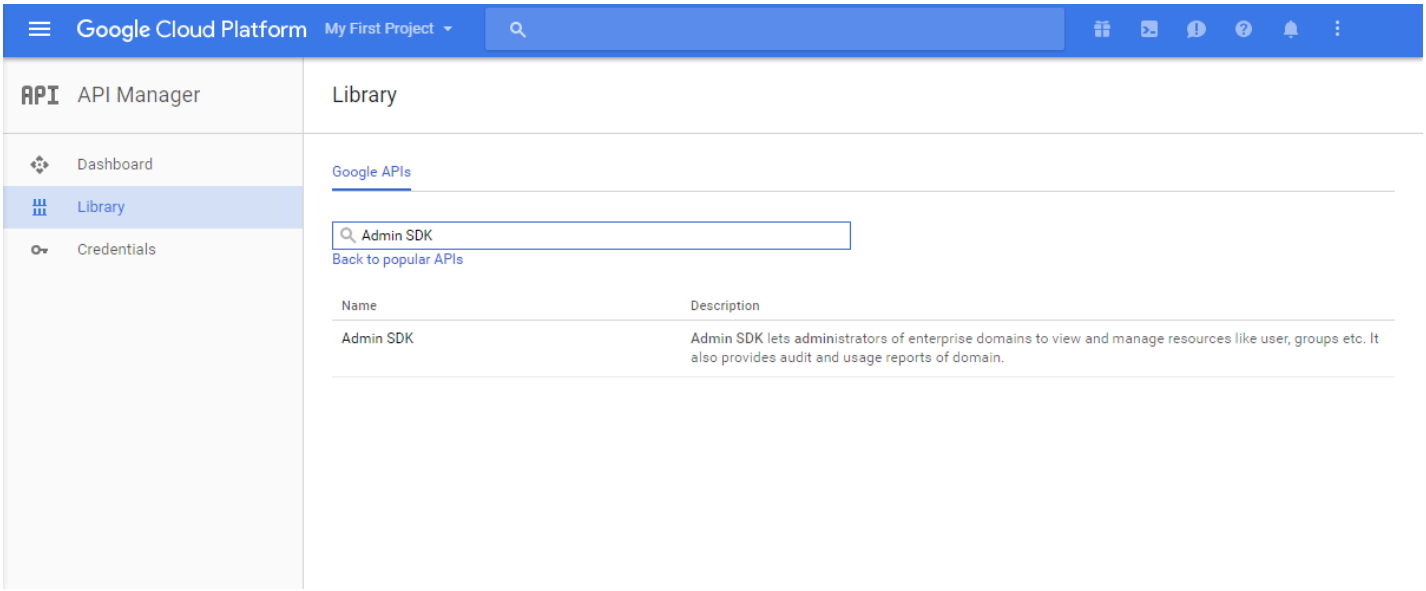
12. En **Permissions**, haga clic en **Service accounts** y, en **Options** para su cuenta de servicio, haga clic en **View Client ID**.



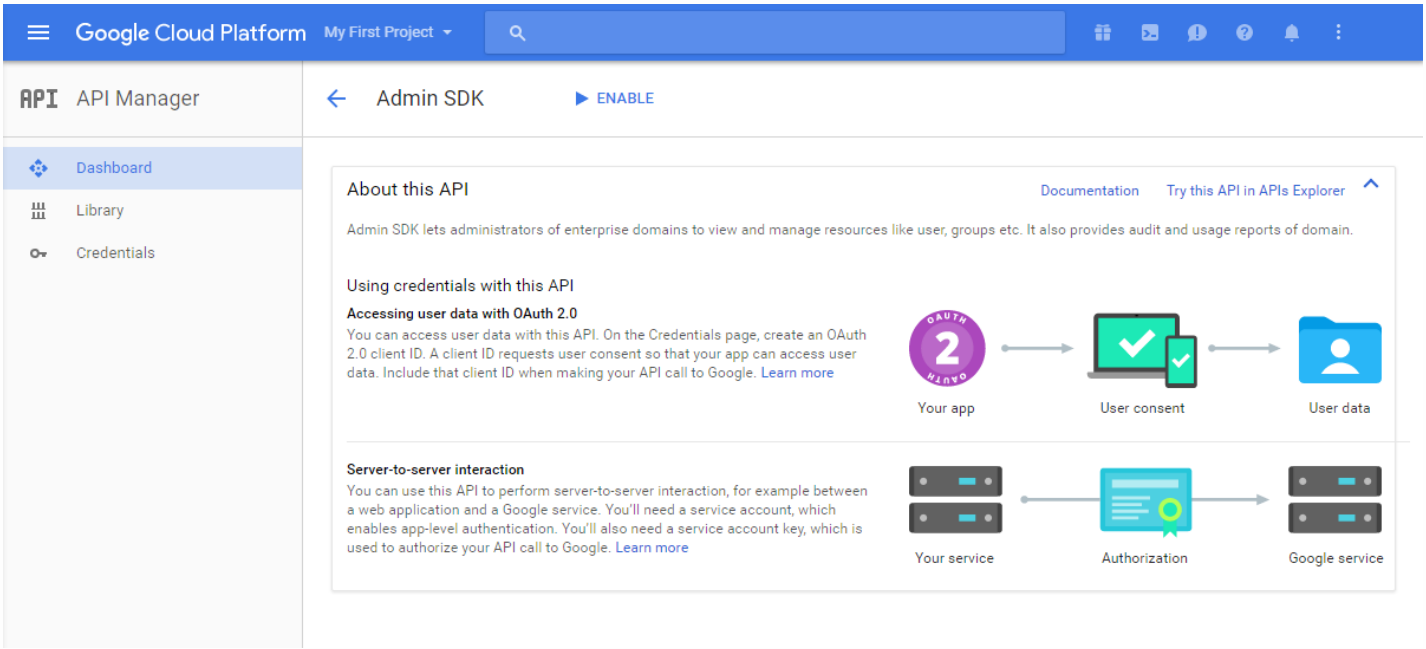
13. Aparecerán los datos requeridos para la autorización de cuentas en la consola de administración de Google. Copie los valores de **Client ID** y **Service account ID** en una ubicación donde pueda encontrarlos más adelante. Necesita esta información, junto con el nombre de dominio, para enviarla a Citrix para su inclusión en una lista blanca.



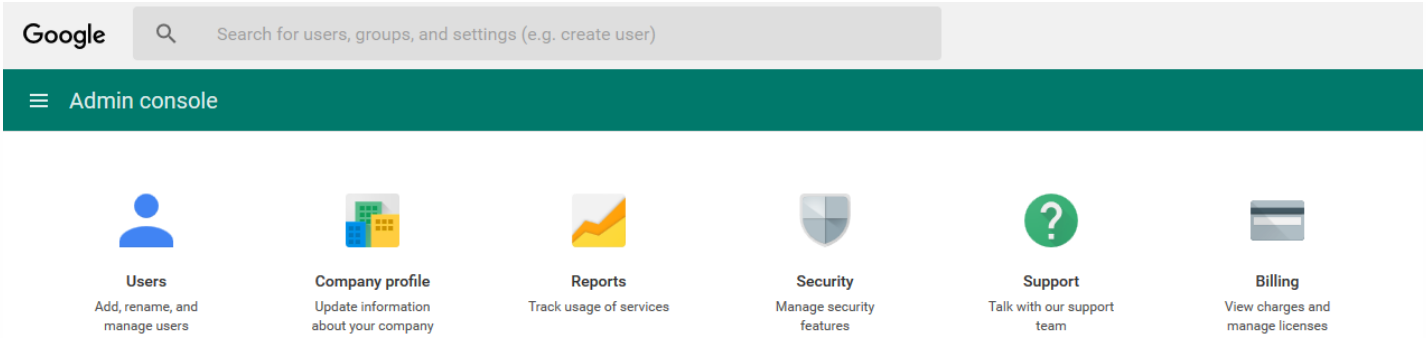
14. En la página **Library**, busque **Admin SDK** y haga clic en el resultado de búsqueda.



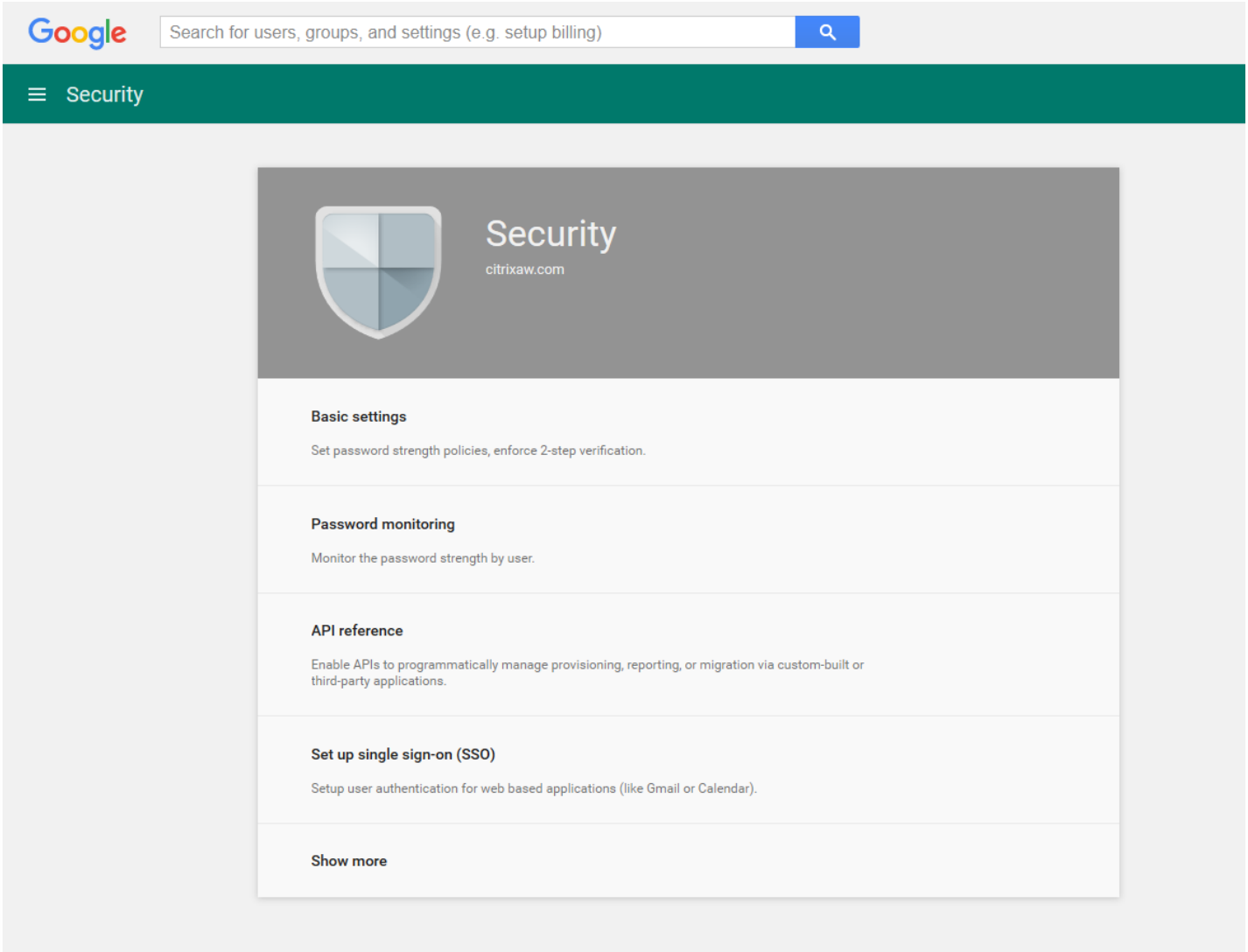
15 En la página **Overview**, haga clic en **Enable**.

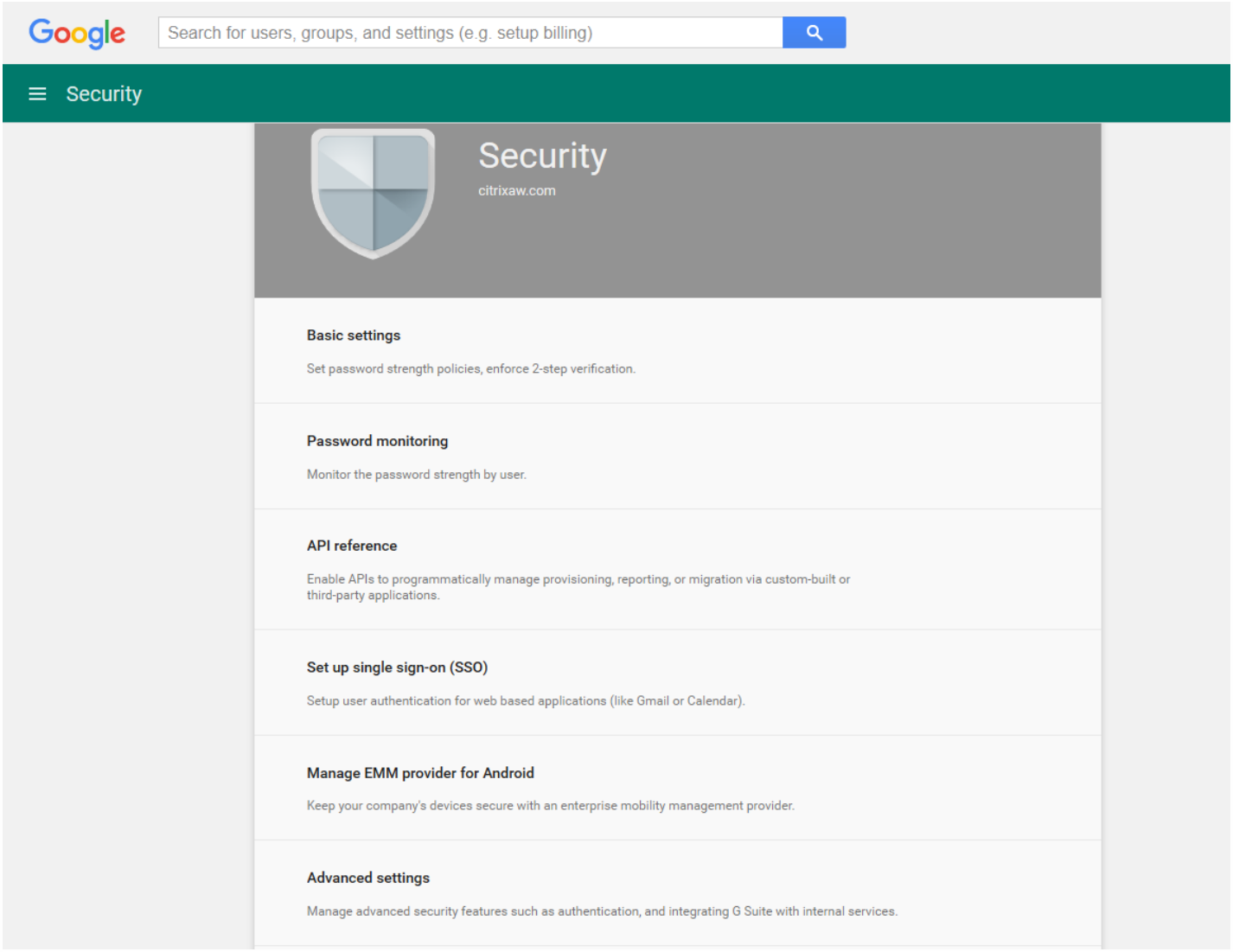


16. Abra la consola de administración de Google para su dominio y haga clic en **Security**.

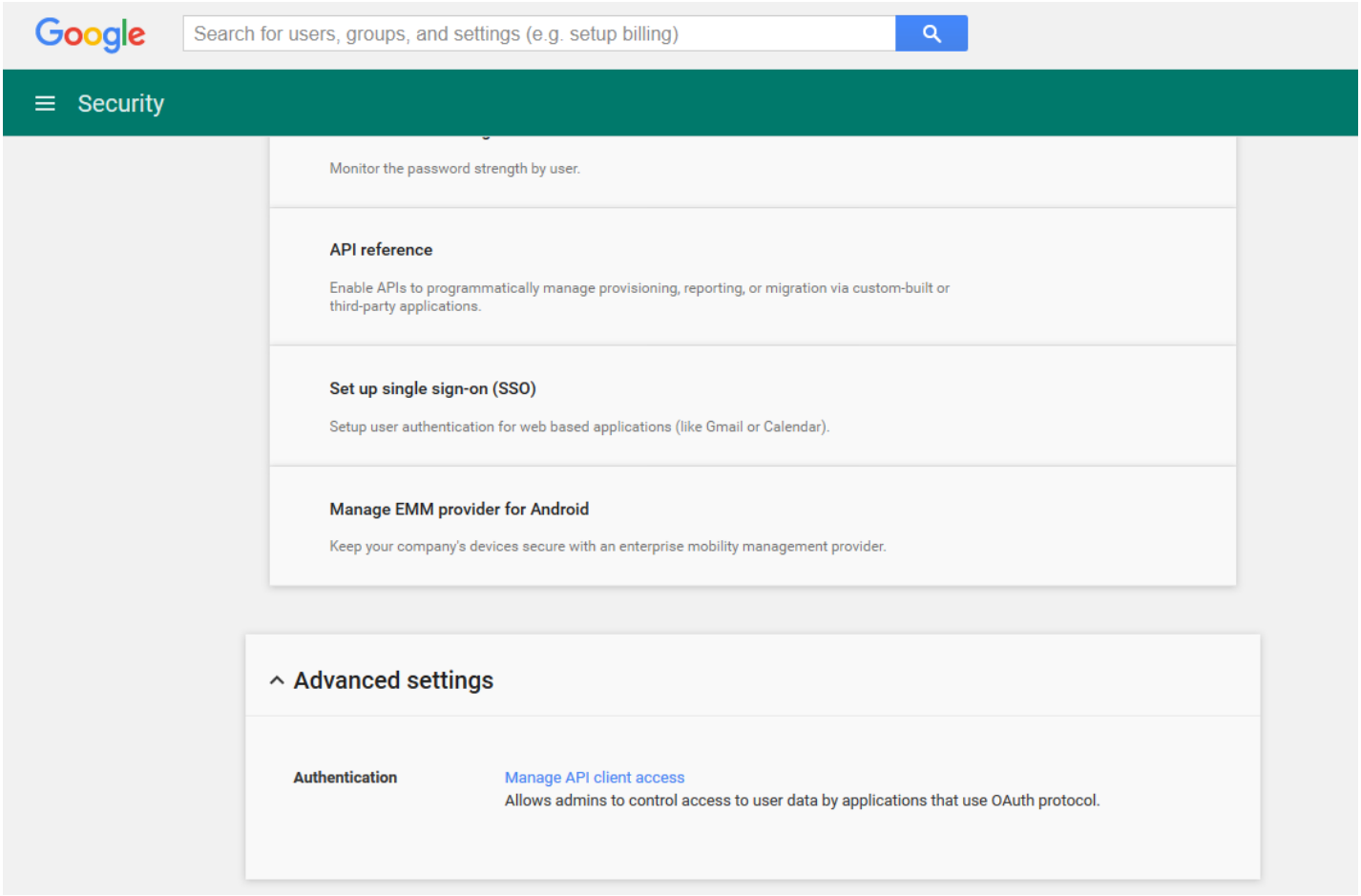


17. En la página **Settings**, haga clic en **Show more** y en **Advanced settings**.

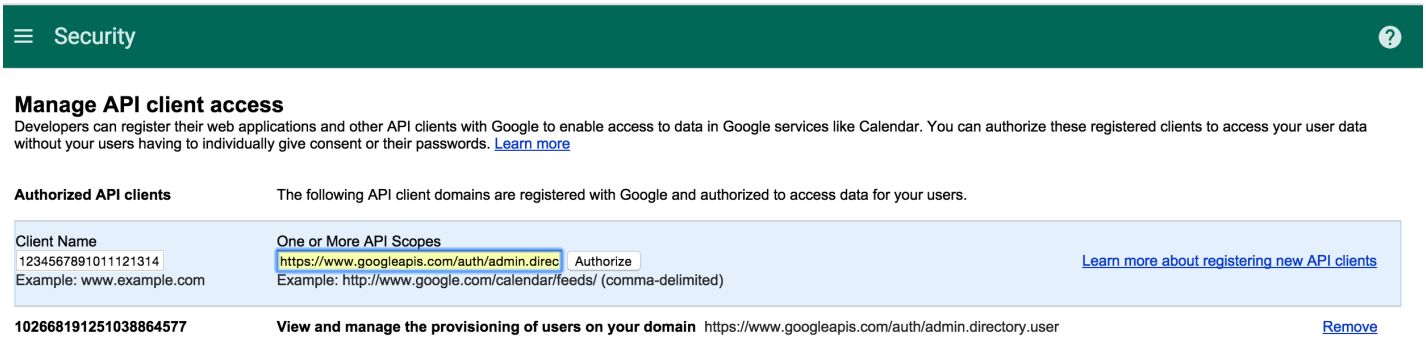




18. Haga clic en **Manage API client access**.



19. 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, debe ponerse en contacto con el servicio de asistencia técnica de Citrix y proporcionarles su nombre de dominio, cuenta de servicio y token de vinculación. Citrix vincula el token con XenMobile como proveedor de administración de movilidad empresarial (EMM). Para obtener la información de contacto de la asistencia técnica de Citrix, consulte Asistencia técnica de Citrix.

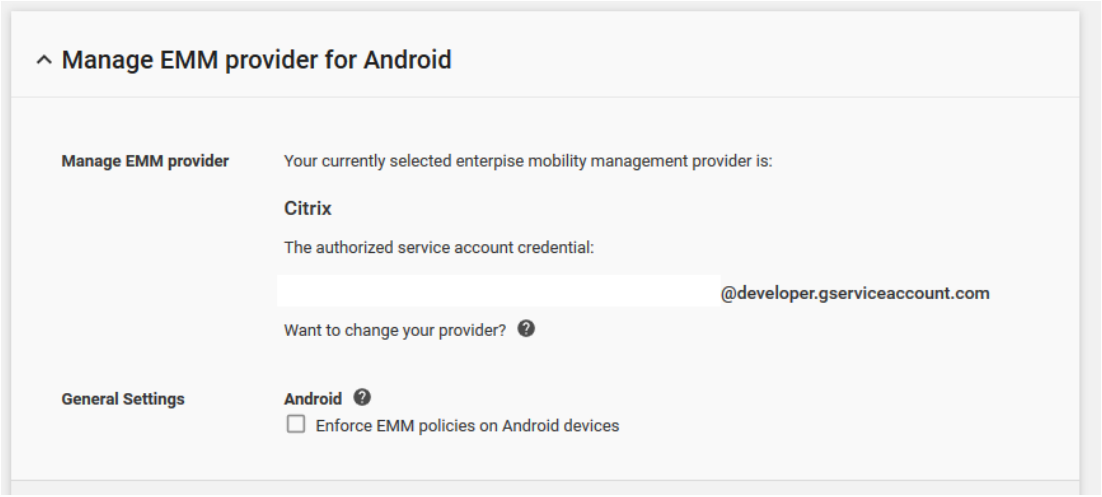
1. Para confirmar la vinculación, inicie sesión en el portal de administración de Google y haga clic en **Security**.

2. Haga clic en **Manage EMM provider for Android**.

Verá que su cuenta de Google Android at Work aparece vinculada a Citrix como su proveedor EMM.

Después de confirmar la vinculación con el token, ya puede empezar a usar la consola de XenMobile para administrar sus dispositivos Android. Importe el certificado P12 generado en el paso 14. Configure los parámetros del servidor de Android at Work, habilite el inicio de sesión Single Sign-On basado en SAML

y defina al menos una directiva de dispositivo para Android at Work.

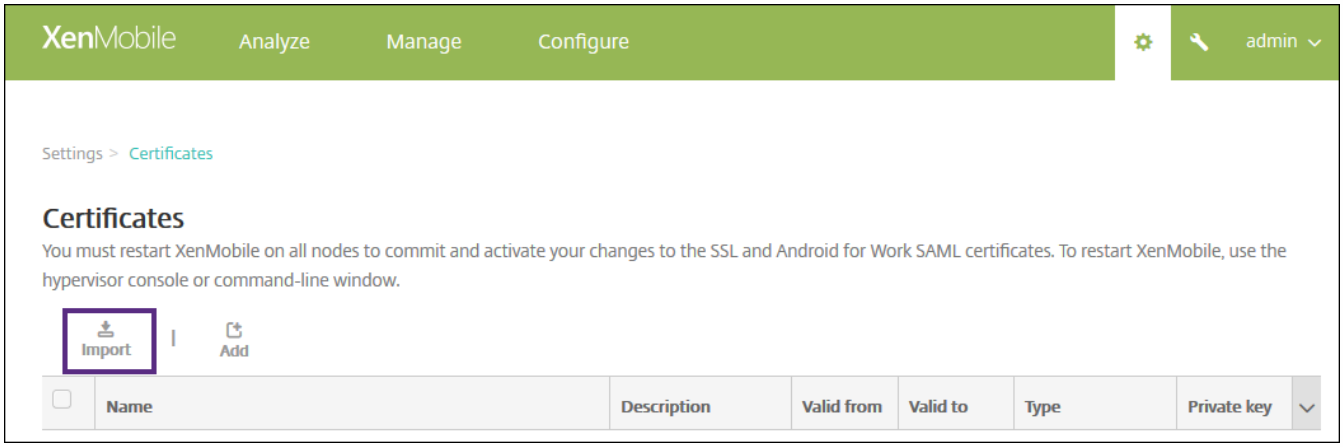


Importación del certificado P12

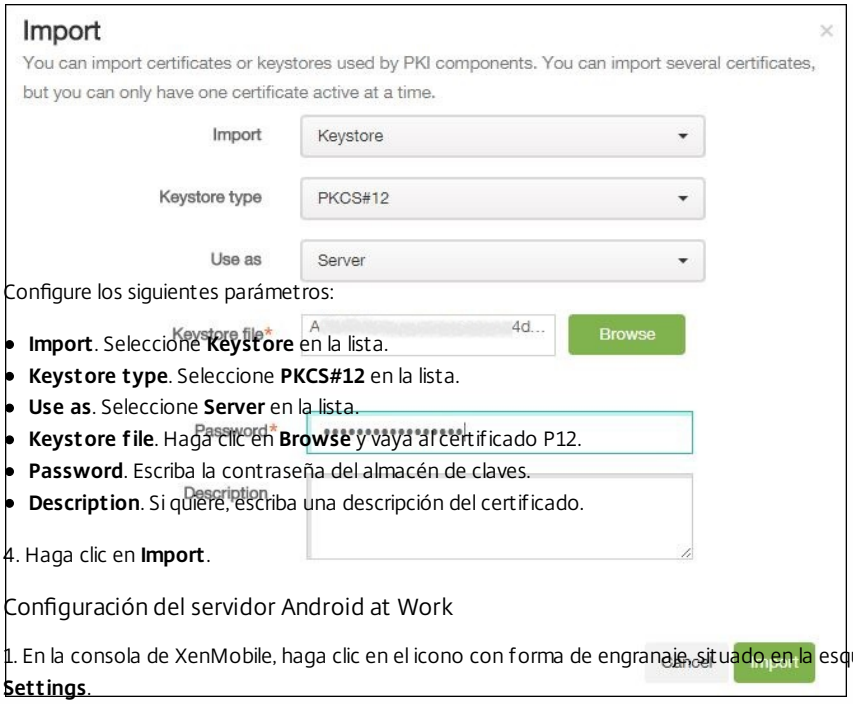
Siga estos pasos para importar el certificado P12 de Android at Work:

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:

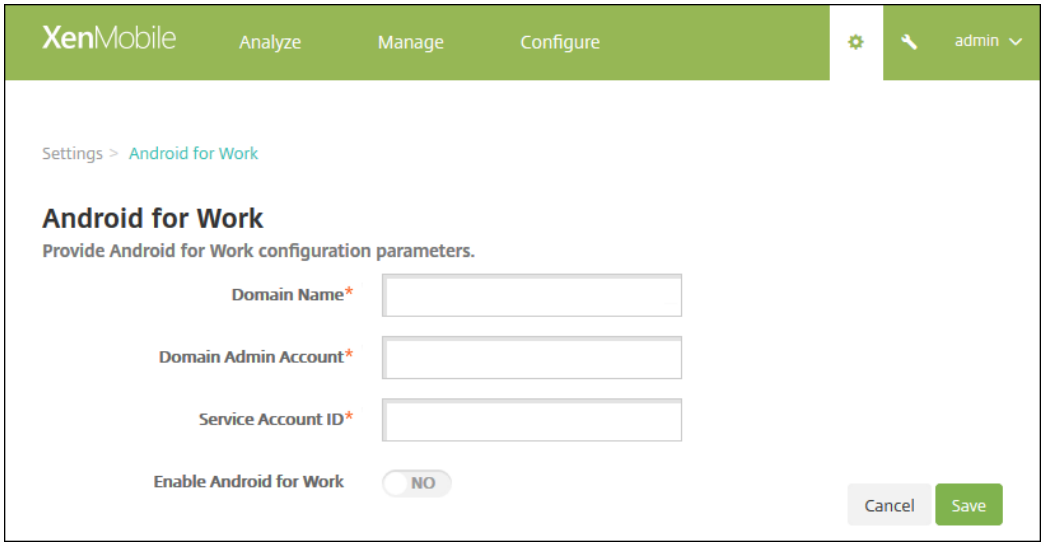
- **Import**. Seleccione **Keystore** en la lista.
- **Keystore type**. Seleccione **PKCS#12** en la lista.
- **Use as**. Seleccione **Server** en la lista.
- **Keystore file**. Haga clic en **Browse** y vaya al certificado P12.
- **Password**. Escriba la contraseña del almacén de claves.
- **Description**. Si quiere, escriba una descripción del certificado.

4. Haga clic en **Import**.

Configuración del servidor Android at 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 at 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 la 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 at Work.

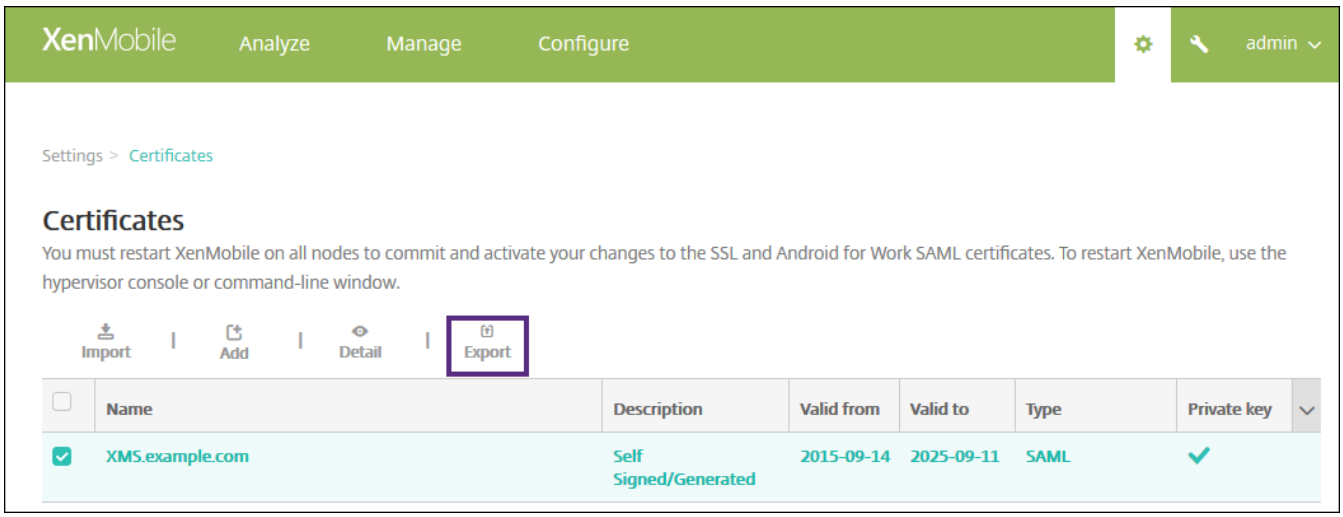
3. Haga clic en **Save**.

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 de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

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

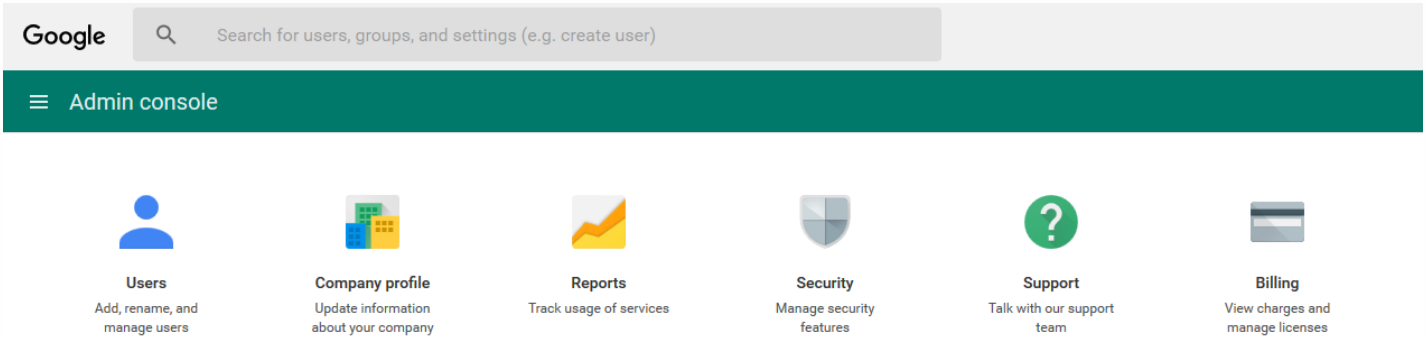


3. En la lista de certificados, haga clic en el certificado SAML.

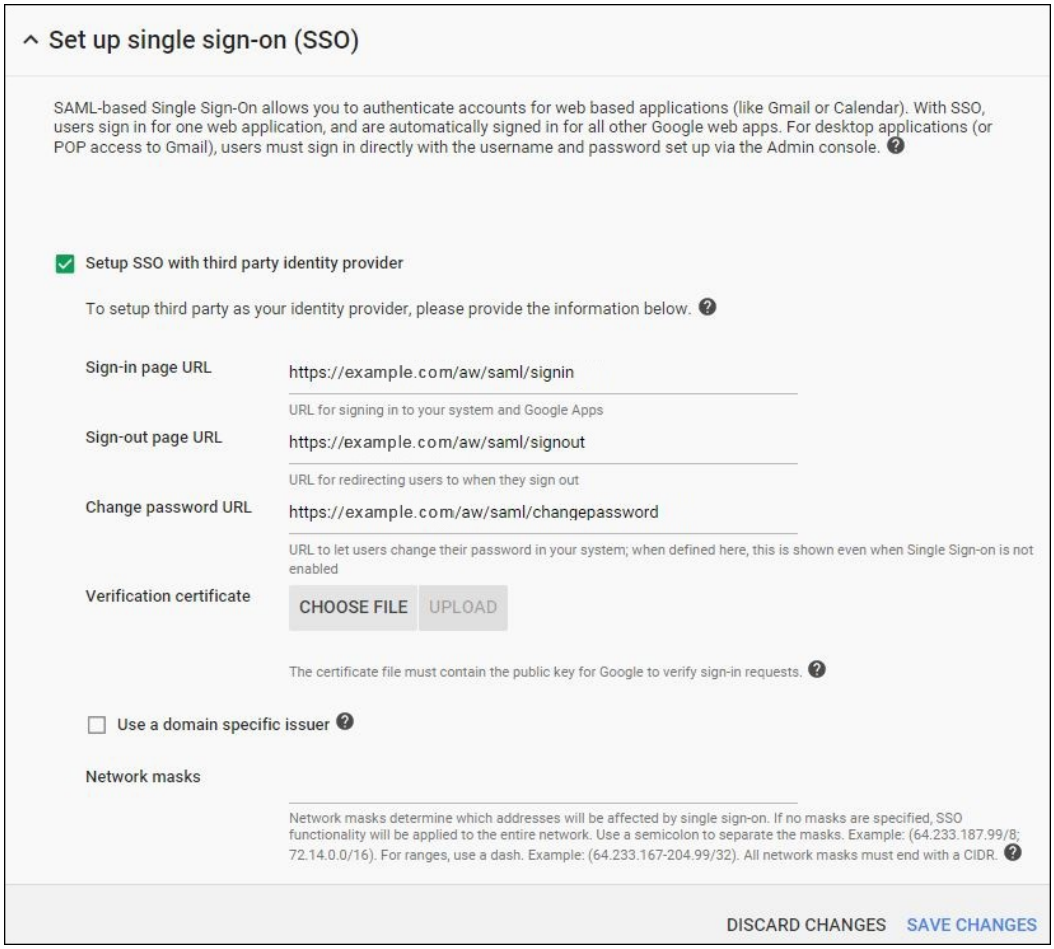
4. Haga clic en **Export** y guarde el certificado en su equipo.

5. Inicie sesión en el portal de Google Admin con las credenciales de administrador de Android at Work. Para acceder al portal, consulte portal Google Admin.

6. Haga clic en **Security**.



7. En **Security**, haga clic en **Set up single sign-on (SSO)** y configure los parámetros siguientes:

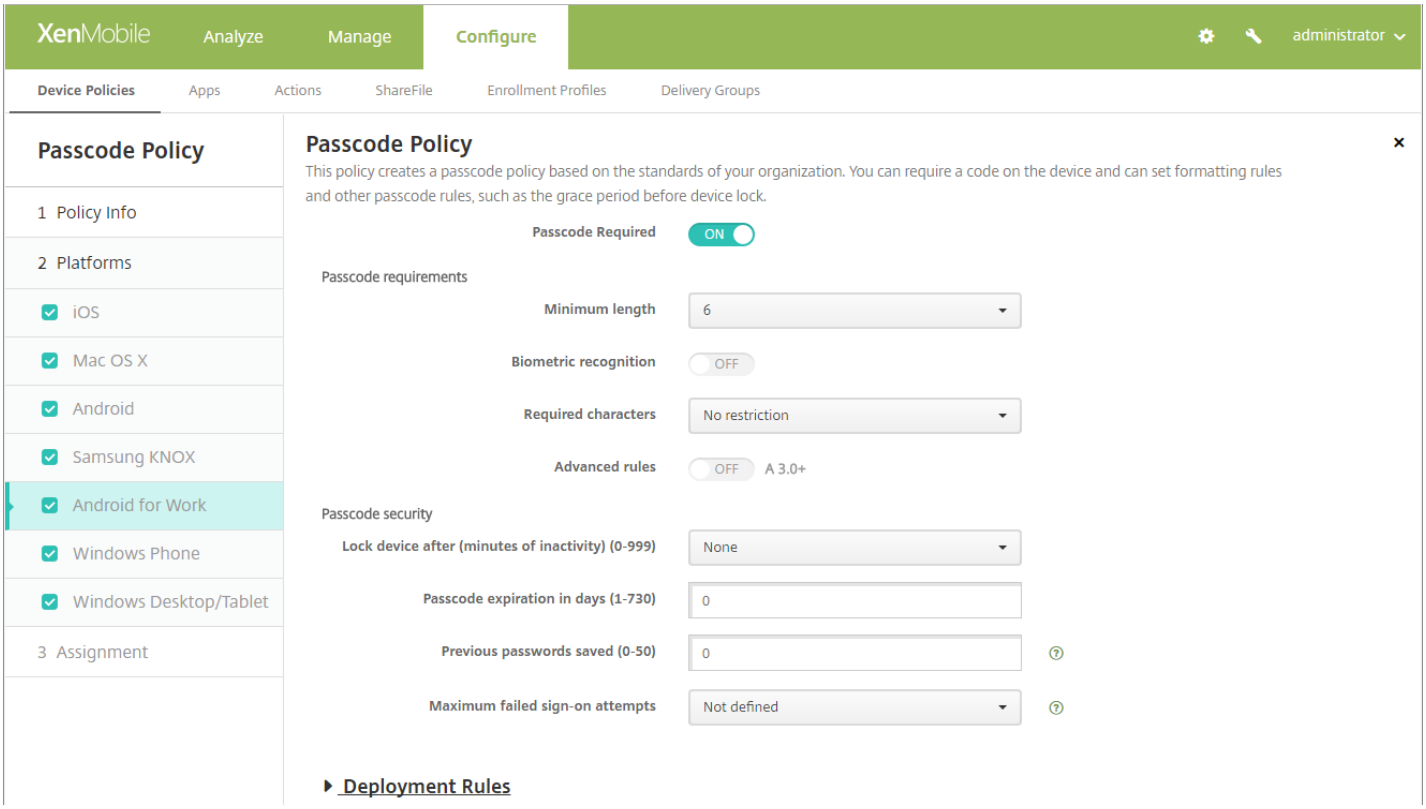


- **Sign-in page URL**: Introduzca la URL para que los usuarios inicien sesiones en el sistema y Google Apps. Por ejemplo: https:///aw/saml/signin.
- **Sign-out page URL**: Introduzca la dirección URL a la que se redirige a los usuarios cuando cierran la sesión. Por ejemplo: https:///aw/saml/signout.
- **Change password URL**: Introduzca la URL para permitir que los usuarios cambien su contraseña en el sistema. Por ejemplo: https:///aw/saml/changepassword. Si se define este campo, los usuarios verán esta solicitud incluso cuando 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 at Work

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 inscriban.



Estos son los pasos básicos para configurar una directiva de dispositivo:

1. Inicie sesión en la consola de XenMobile.

2. Haga clic en **Configure** y, a continuación, en **Device Policies**.

3. Haga clic en **Add** y seleccione la directiva que quiera agregar en el cuadro de diálogo **Add a New Policy** . En este ejemplo, haga clic en **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.

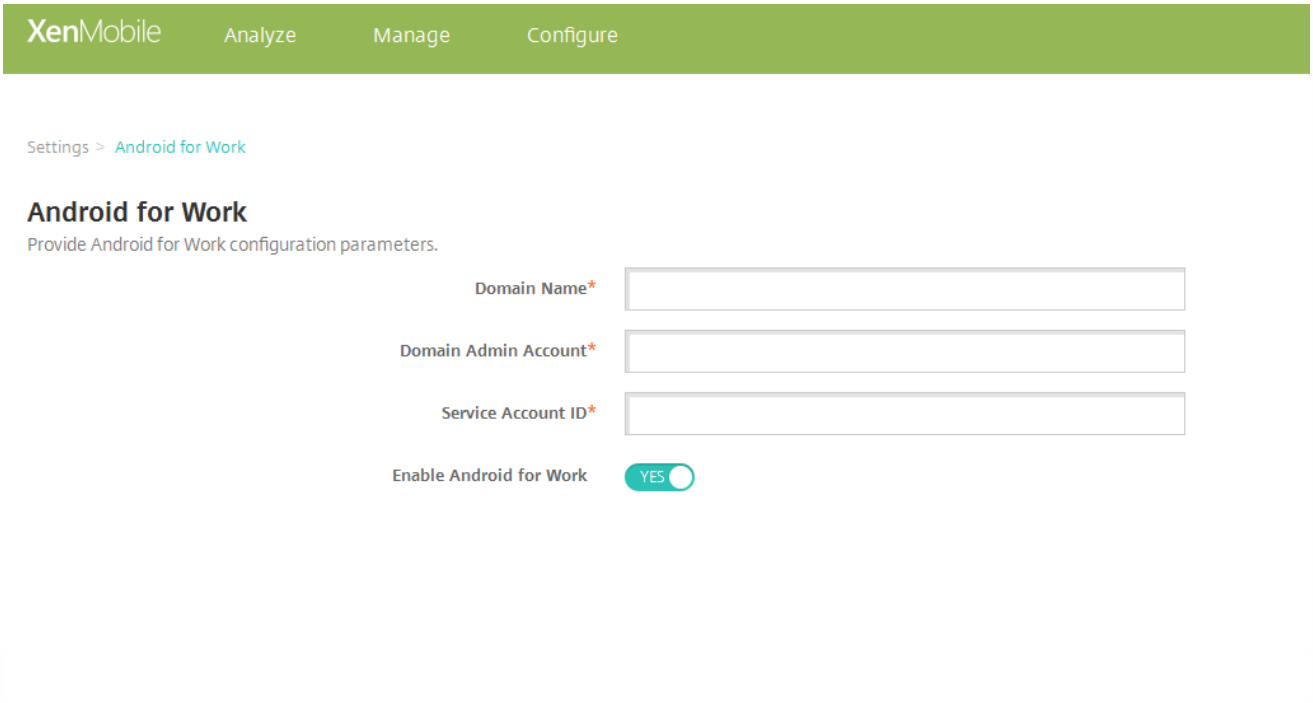
Para obtener más información sobre cómo definir otras directivas de dispositivo que están disponibles para Android for Work, consulte Directivas de dispositivos de XenMobile desglosadas por plataforma.

Configuración de parámetros de cuenta para Android at Work

En XenMobile, antes de empezar a administrar aplicaciones y directivas Android en los dispositivos, debe configurar la información de la cuenta y del dominio de Android at Work. Primero, debe completar las tareas de configuración de Android at Work en Google para definir un administrador de dominio y obtener un ID de cuenta de servicio, así como un token de enlace.

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. 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 del modo Device Owner en Android at Work

Si quiere aprovisionar Android at Work en el modo Device Owner (propietario del dispositivo), debe transferir datos a través de una conexión Near Field Communication (NFC) entre dos dispositivos. Uno debe estar ejecutando la herramienta de aprovisionamiento de XenMobile y el otro debe restaurarse a sus valores predeterminados de fábrica. El modo Device Owner solo está disponible 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 utilizar en ese estado.

Requisitos previos

- Un servidor XenMobile 10.4 habilitado para Android at Work.
- Un dispositivo restablecido a sus valores de fábrica, aprovisionado para Android at Work en modo Device Owner. Dispone de los pasos necesarios para completar este requisito previo más adelante en este artículo.
- Otro dispositivo con capacidades de comunicación NFC, que ejecuta la herramienta Provisioning Tool configurada. La herramienta Provisioning Tool está disponible en Secure Hub 10.4 o en la página de descargas de Citrix.

Cada dispositivo puede tener un solo perfil de Android at Work, administrado por una aplicación para la administración de movilidad empresarial (EMM). En XenMobile, Secure Hub es la aplicación EMM. Solo se permite un perfil por dispositivo. Si intenta agregar una segunda aplicación EMM, se eliminará la primera.

Puede iniciar el modo Device Owner en dispositivos nuevos o en dispositivos que han sido restaurados a sus valores de fábrica. Podrá administrar por completo el dispositivo con XenMobile.

Conexión NFC en modo Device Owner

Para aprovisionar un dispositivo restablecido a sus valores de fábrica, debe enviar los siguientes datos vía una conexión NFC para activar Android at Work:

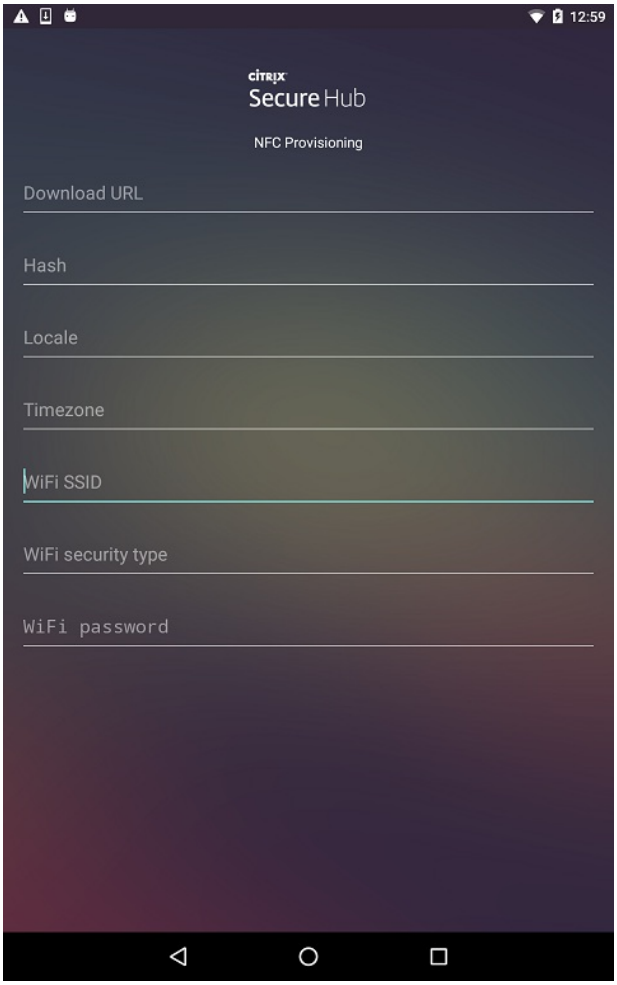
- Nombre del paquete de la aplicación de proveedor EMM que actuará como Device Owner (en este caso, Secure Hub).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación de proveedor EMM.

- Valor hash SHA1 de la aplicación de proveedor EMM para verificar si la descarga fue correcta.
- Datos de la conexión WiFi para que un dispositivo restablecido a sus valores de fábrica pueda conectarse y descargar la aplicación de proveedor EMM. Nota: Android no admite 802.1x WiFi para este paso.
- Zona horaria del dispositivo (opcional).
- Ubicación geográfica del dispositivo (opcional).

Cuando los dos dispositivos se conectan por NFC, los datos de la herramienta Provisioning Tool se envían al dispositivo restablecido a los valores de fábrica. Esos datos se utilizan para descargar Secure Hub 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 XenMobile Provisioning Tool

Antes de una conexión NFC, es necesario configurar la herramienta 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. En los pasos del siguiente procedimiento, se describe cómo configurar un archivo de texto que contenga descripciones para cada campo. 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.

Para configurar Provisioning Tool mediante un archivo de texto

Nombre el archivo **nfcprovisioning.txt** y colóquelo en la tarjeta SD del dispositivo (en la carpeta /sdcard/). 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 línea es la ubicación de intranet o Internet de la aplicación de proveedor EMM. Una vez que el dispositivo restablecido a los valores de fábrica se conecte a WiFi por conexión NFC, el dispositivo debería tener acceso a esta ubicación para la descarga. La URL es una dirección URL normal, sin formato especial.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=
Esta línea es la suma de comprobación de la aplicación de proveedor EMM. Esta suma de comprobación se utiliza para verificar que la descarga se ha realizado correctamente. Los pasos para obtener la suma de comprobación se describen más adelante en este artículo.

android.app.extra.PROVISIONING_WIFI_SSID=
Esta línea es el SSID del dispositivo conectado por WiFi donde se está ejecutando la herramienta 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=
Indique los códigos de idioma y país. Los códigos de idioma son códigos de idioma ISO de dos letras minúsculas (por ejemplo, "es" para español), según se definen en ISO 639-1. Los códigos de país son códigos de país 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 ningún nombre, la zona horaria se rellena automáticamente.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
Estos datos no son necesarios, porque este valor, Secure Hub, está incluido y no se puede modificar en la aplicación. Se menciona aquí a título meramente informativo.

Si existe una red WiFi protegida mediante WPA2, un archivo **nfcprovisioning.txt** completado puede tener el siguiente aspecto:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY _TYPE = WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Si existe una red WiFi no protegida, un archivo nfcprovisioning.txt completado puede tener el siguiente aspecto:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

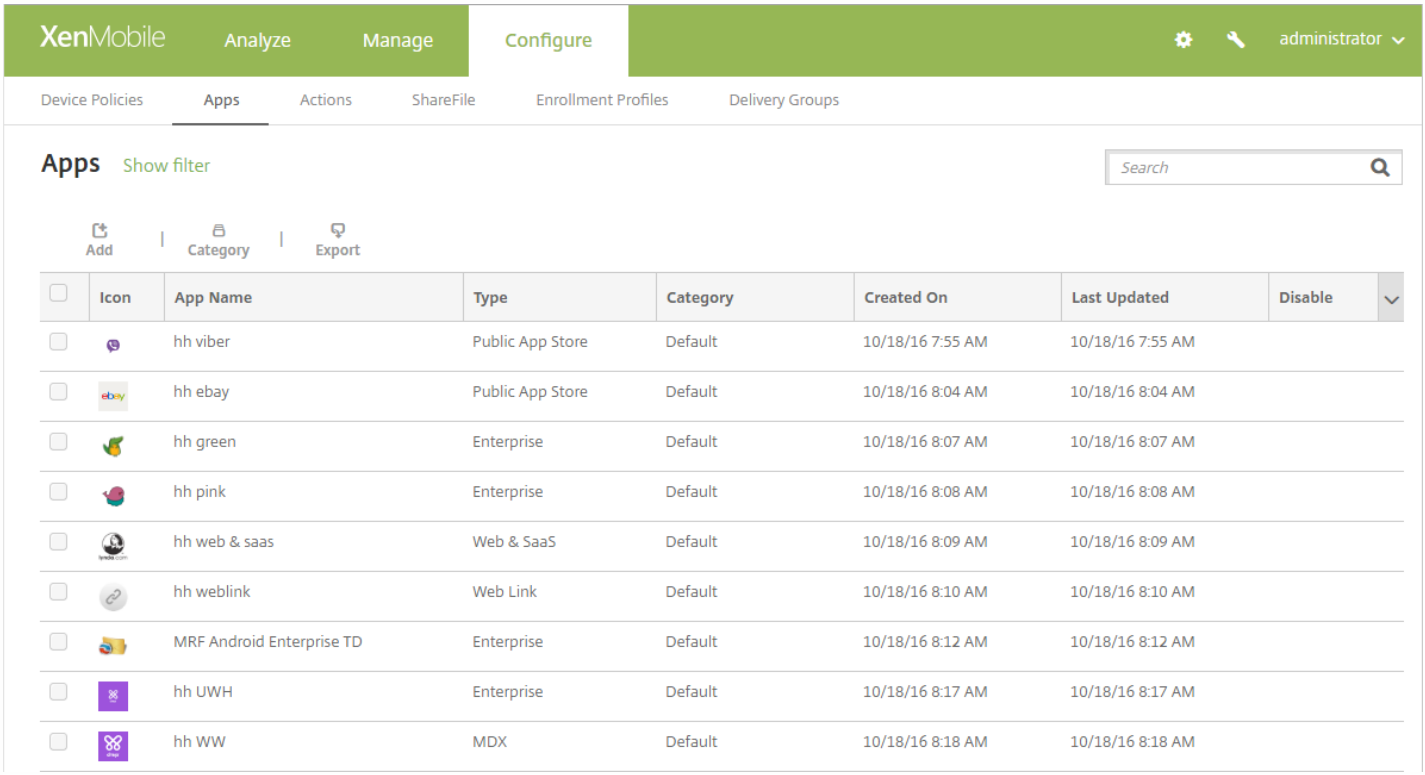
android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Para obtener la suma de comprobación de Secure Hub

Si quiere obtener la suma de comprobación de cualquier aplicación, agregue la aplicación como aplicación de empresa.

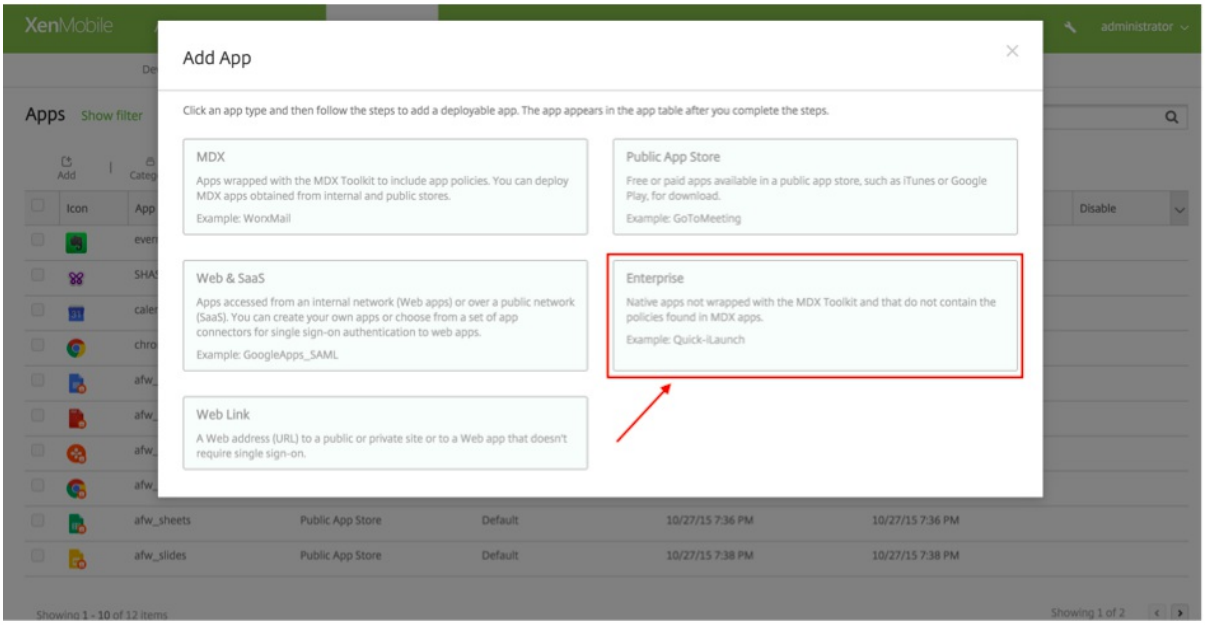
1. En la consola de XenMobile, vaya a **Configure > Apps** y luego haga clic en **Add**.



Aparecerá la ventana **Add App**.

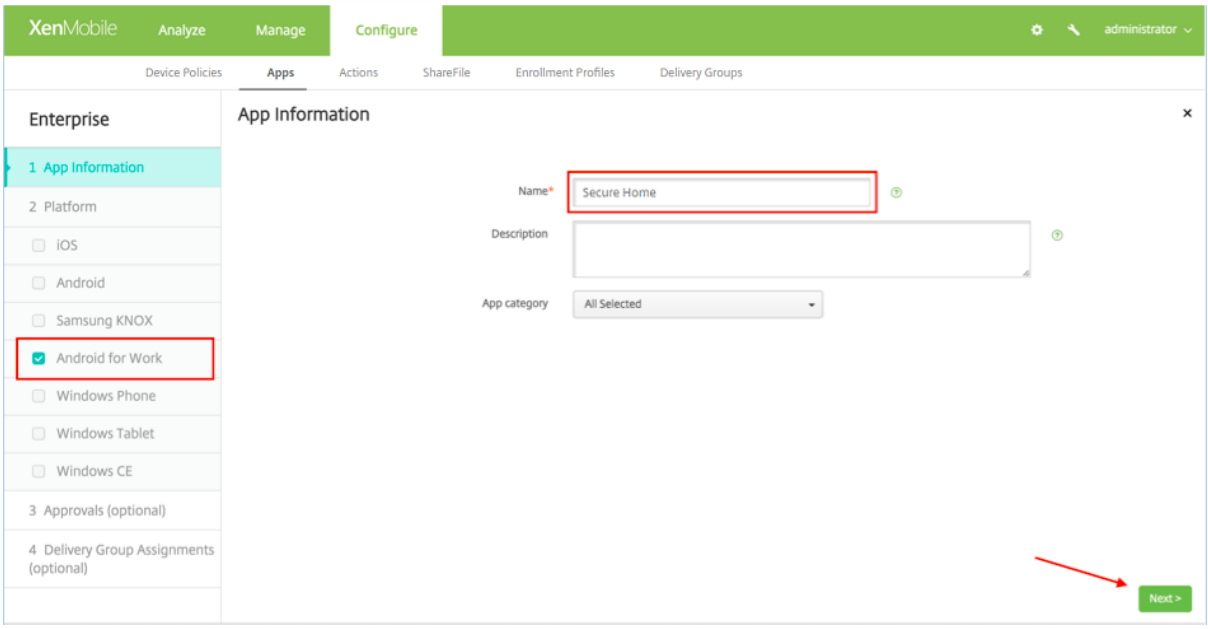
2. Haga clic en **Enterprise**.

Aparecerá la página **App Information**.



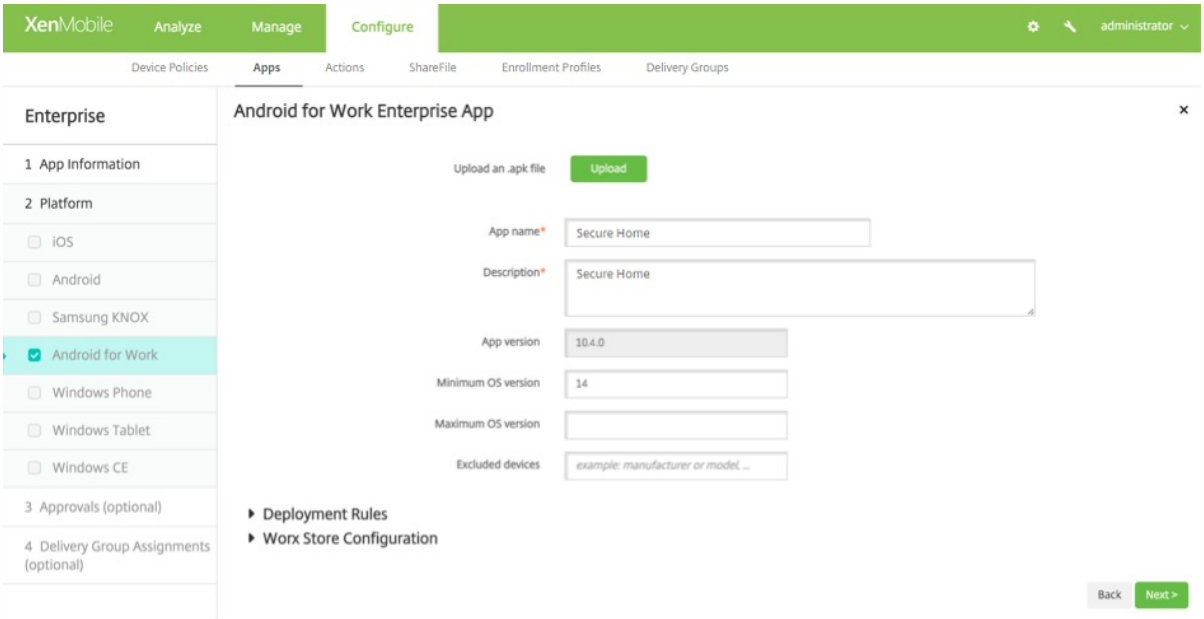
3. Seleccione la configuración siguiente y haga clic en **Next**.

Aparecerá la pantalla **Android for Work Enterprise App**.

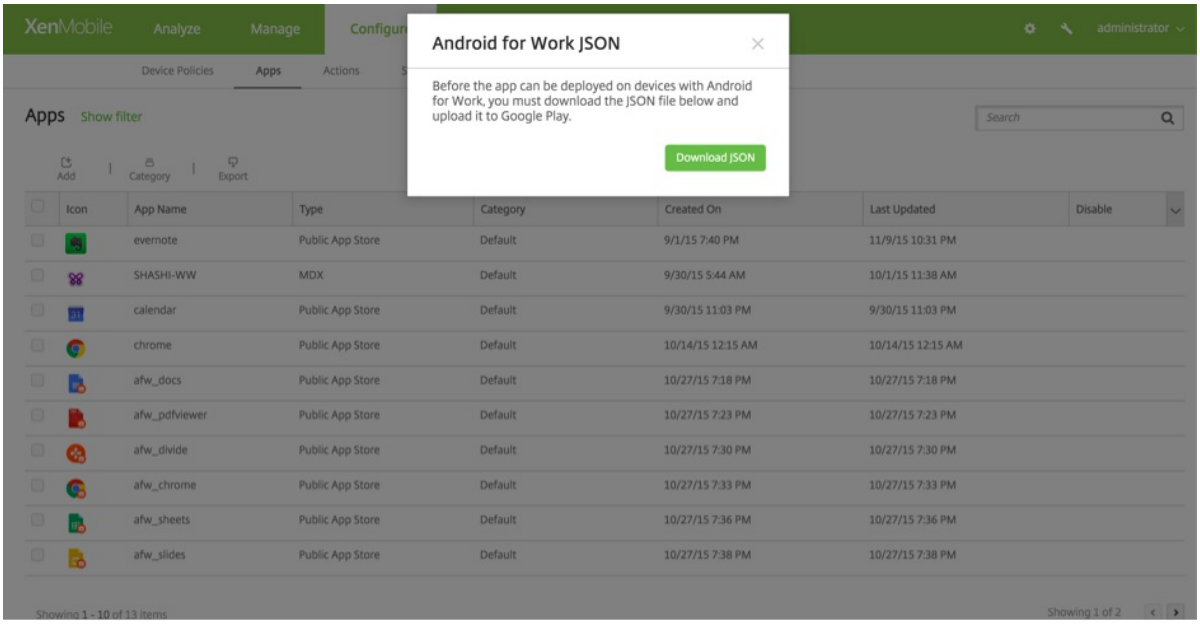


4. Facilite la ruta al archivo APK y haga clic en **Next** para cargar el archivo.

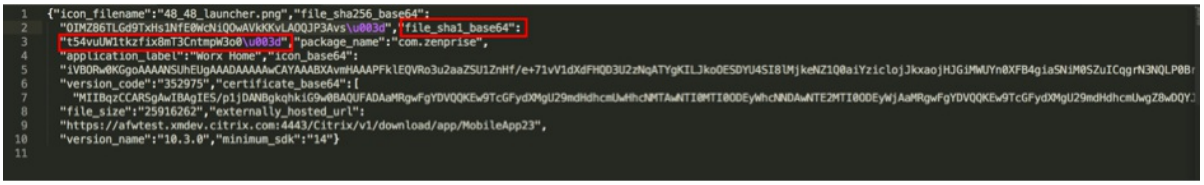
Una vez completada la carga, verá los datos del paquete cargado.



5. Haga clic en **Next** para ver la página desde donde descargar el archivo JSON, que podrá utilizar para hacer cargas en Google Play. Para Secure Hub, 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 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 por **=**

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 comprobar usted mismo que el valor es compatible con direcciones URL.

Bibliotecas utilizadas

La herramienta Provisioning Tool utiliza 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

Inscripción en masa de dispositivos iOS y macOS

Feb 27, 2017

En XenMobile, dispone de dos formas para inscribir una gran cantidad de dispositivos iOS y macOS.

- Puede usar Apple Device Enrollment Program (DEP) para inscribir los dispositivos iOS y macOS adquiridos directamente de Apple, de un distribuidor autorizado de Apple o de un operador.

  Para la inscripción en DEP de dispositivos de macOS, XenMobile requiere que los dispositivos ejecuten OS X 10.10 o una versión posterior.

- O bien, puede usar Apple Configurator para inscribir dispositivos iOS tanto si los adquirió directamente de Apple como si no.

Con DEP, no tiene que preparar ni tocar los dispositivos. Basta con enviar los números de serie o de pedido de compra a través de DEP, y los dispositivos se configuran e inscriben. Una vez que los dispositivos se inscriban en XenMobile, puede entregárselos a los usuarios, y estos pueden comenzar a usarlos inmediatamente. Además, cuando se configuran los dispositivos con DEP, se pueden eliminar algunos de los pasos del asistente de configuración que, de otro modo, los usuarios tendrían que completar al encender por primera vez sus dispositivos. Para obtener más información acerca de la configuración del programa DEP, consulte la página del Programa de inscripción de dispositivos de Apple.

Con Apple Configurator, hay que conectar los dispositivos iOS a un equipo Apple que esté ejecutando OS X 10.7.2 o una versión posterior y la aplicación Apple Configurator 2. Se debe preparar los dispositivos iOS y configurar las directivas mediante Apple Configurator 2. Después de aprovisionar los dispositivos con las directivas necesarias, la primera vez que los dispositivos se conectan a XenMobile, reciben las directivas de XenMobile. A partir de entonces, puede empezar a administrar los dispositivos. Para obtener más información sobre cómo usar el Apple Configurator, consulte la página Apple Configurator.

> **Important**
>
> Debe abrir los puertos necesarios para la conectividad entre XenMobile y Apple. Para obtener más información, consulte Requisitos de puertos.

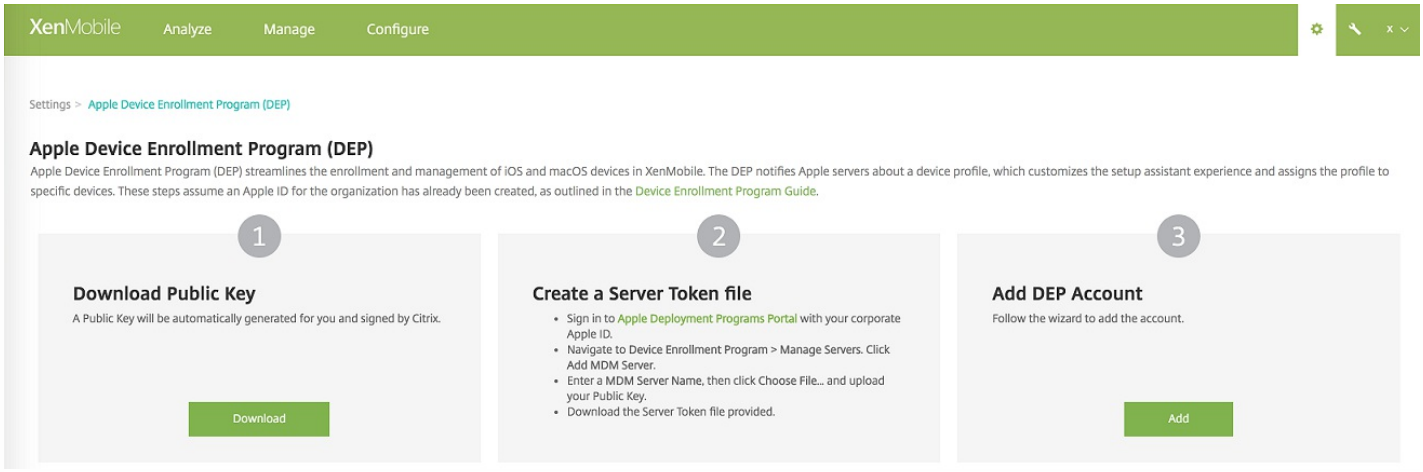
Integración de la cuenta DEP de Apple con XenMobile

Si no dispone de una cuenta DEP de Apple, consulte Implementación de dispositivos iOS y macOS a través del programa DEP de Apple.

Para conectar su cuenta DEP de Apple con el entorno del servidor XenMobile, escriba información en la consola de XenMobile y el portal DEP de Apple, como se describe en los siguientes pasos.

Paso 1. Cargar una clave pública desde el servidor XenMobile

1. Inicie sesión en la consola de XenMobile y vaya a **Settings > Apple Device Enrollment Program (DEP)**.

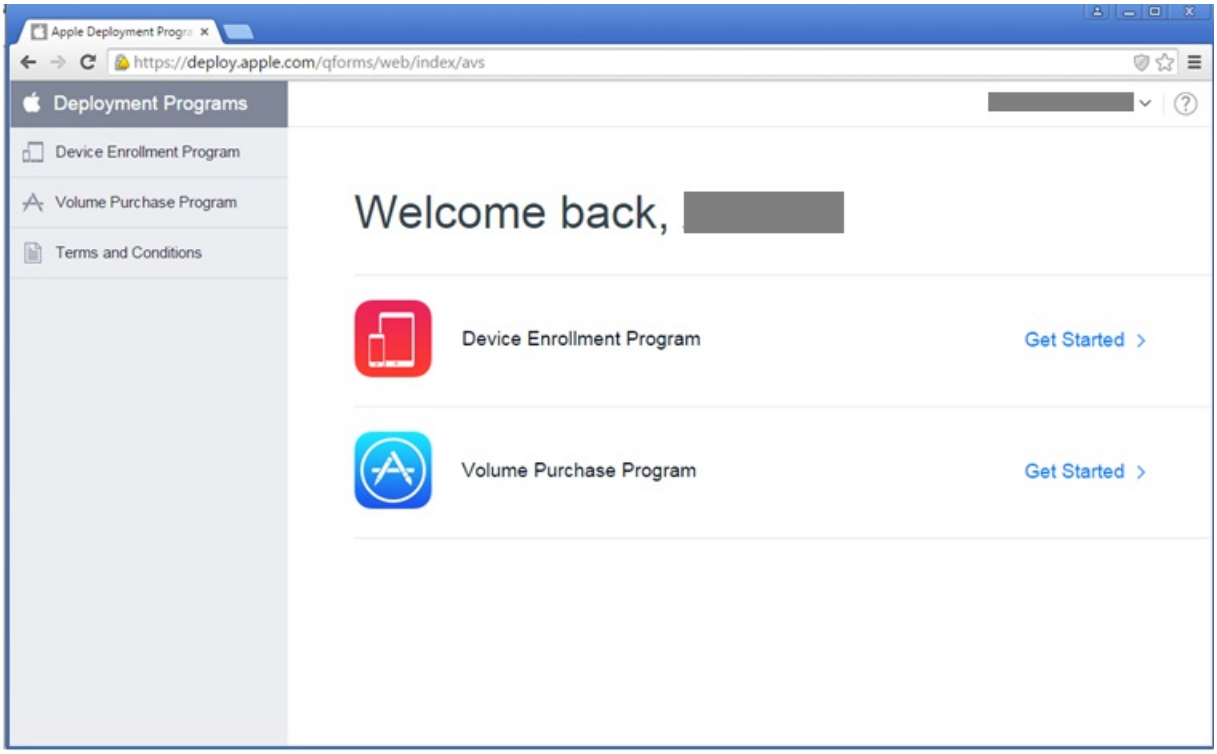


2. En **Download Public Key**, haga clic en **Download**.

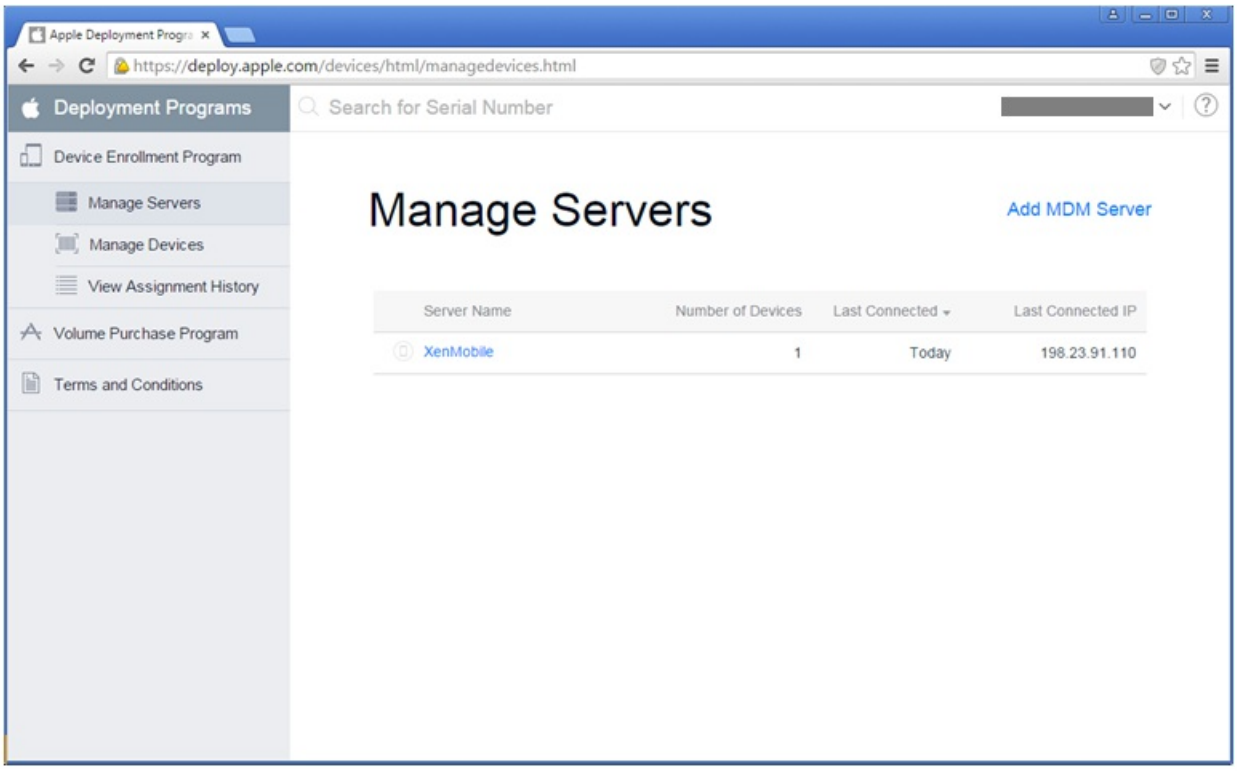
Paso 2: Crear y descargar un archivo de token de servidor desde su cuenta de Apple

1. Con su ID empresarial de Apple, inicie sesión en Apple Deployment Program Portal.

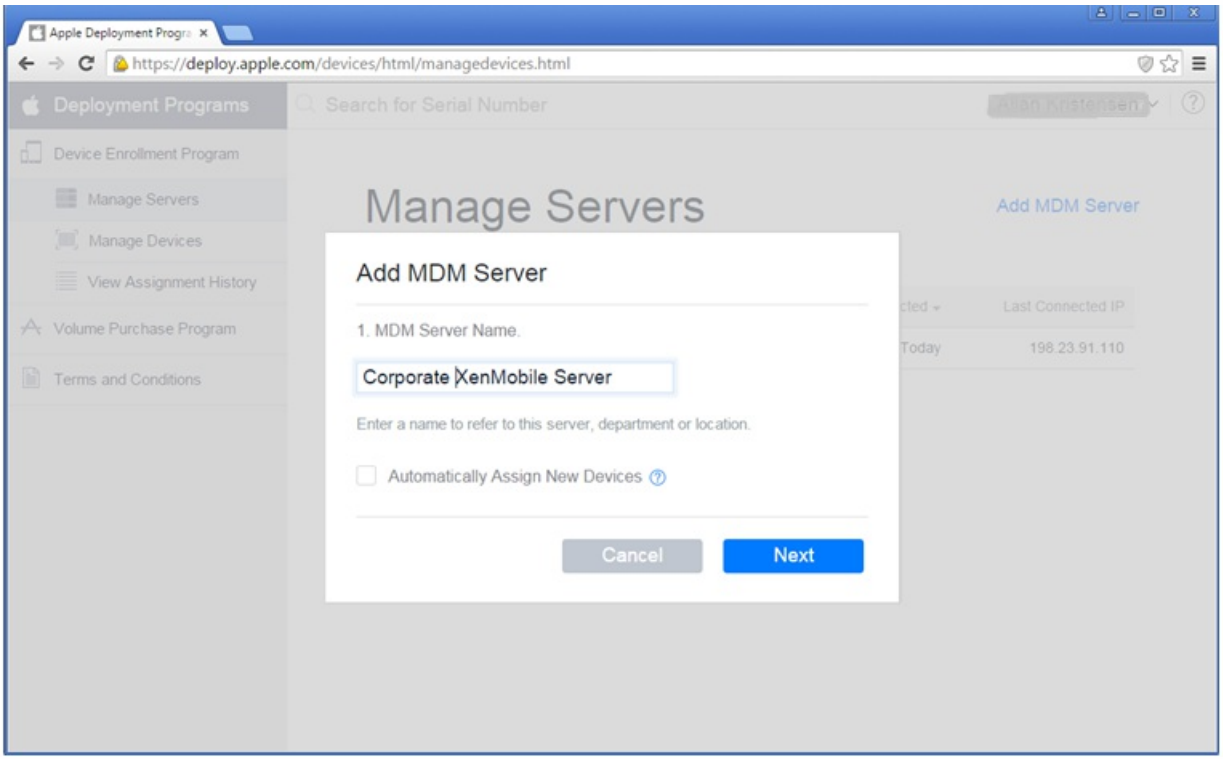
2. En el portal DEP de Apple, haga clic en **Device Enrollment Program**.



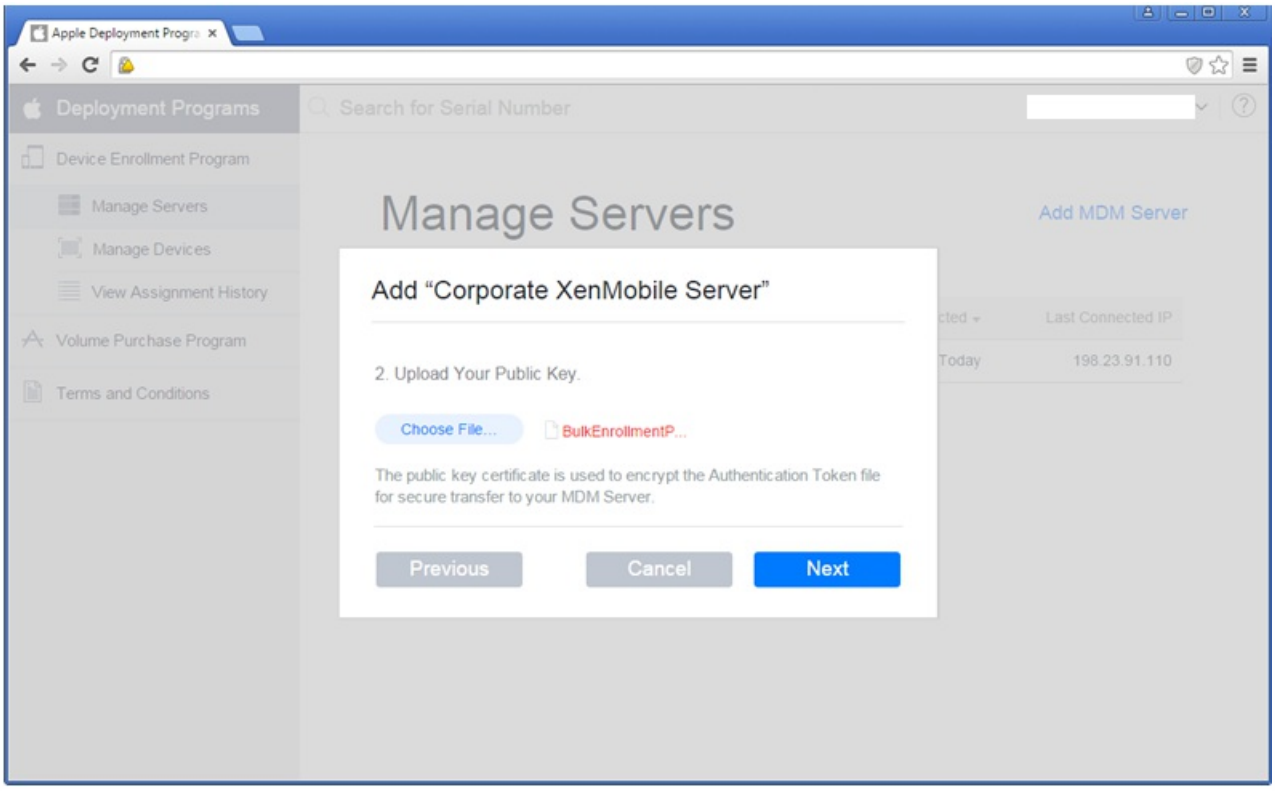
3. Haga clic en **Manage Servers** y, en el lado derecho, haga clic en **Add MDM Server**.



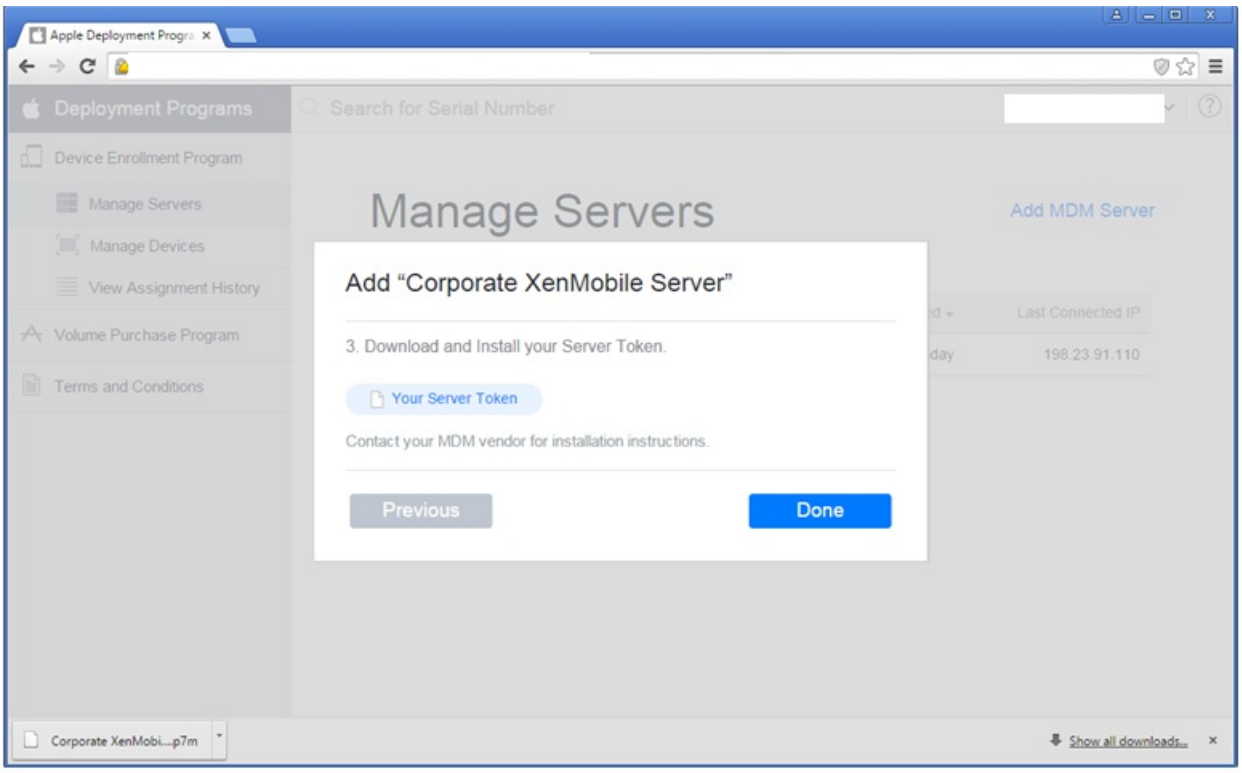
4. En **Add MDM Server**, introduzca el nombre de su servidor XenMobile y haga clic en **Next**.



5. En el portal DEP de Apple, haga clic en **Choose file**, seleccione la clave pública que acaba de descargar y haga clic en **Next**.



6. Haga clic en **Your Server Token** para generar un token de servidor, que se descarga con el explorador Web, y después haga clic en **Done**.



La información del token de Apple DEP aparece en la consola de XenMobile después de importar el archivo de token.

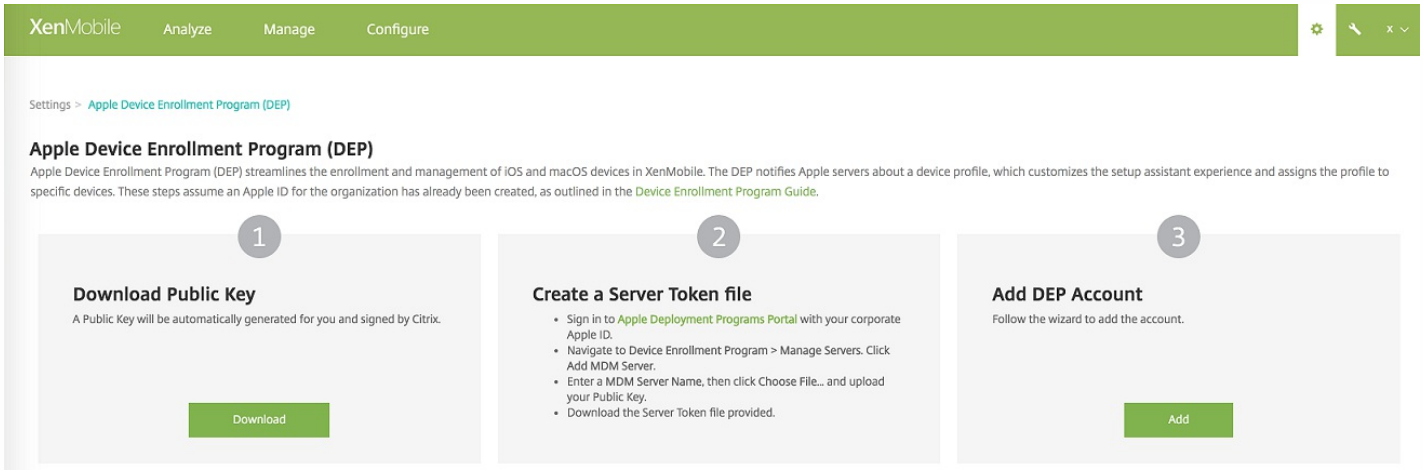
Cargará el archivo de token de servidor cuando agregue la cuenta DEP a XenMobile.

Paso 3: Agregar una cuenta DEP a XenMobile

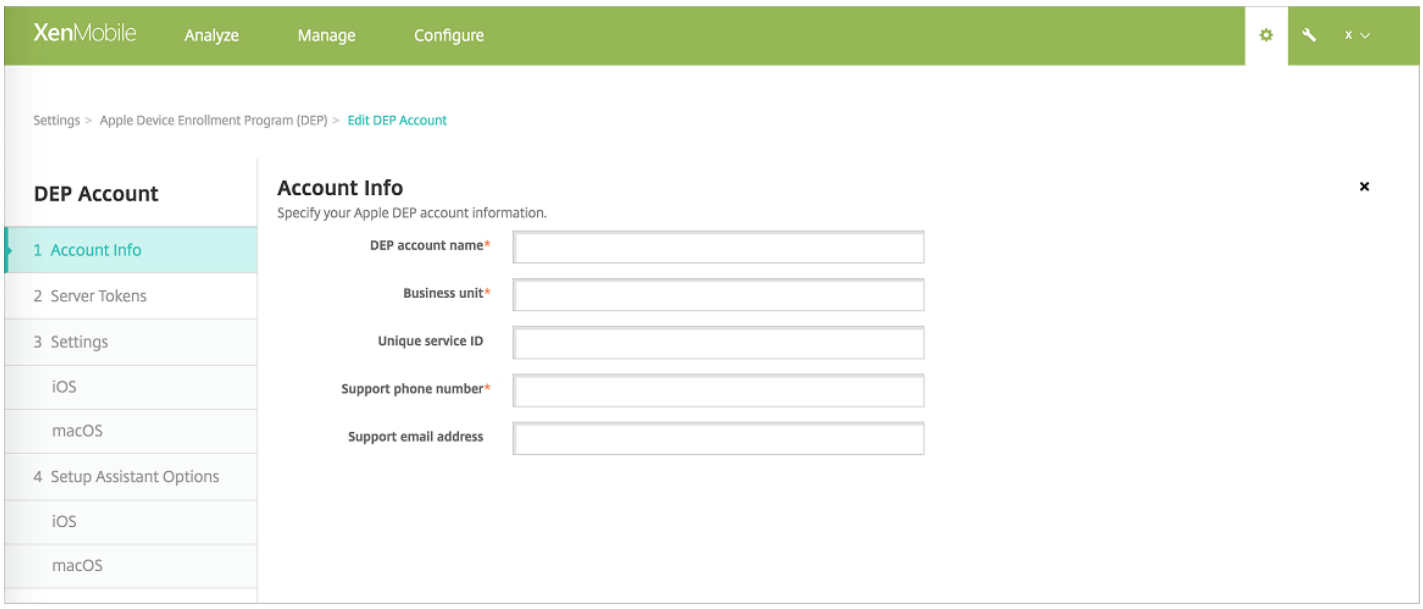
Puede agregar varias cuentas DEP a XenMobile. Esta característica permite utilizar distintos parámetros de inscripción y opciones del asistente de instalación distintas en función del país, del departamento, etcétera. A continuación, puede asociar las cuentas DEP con distintas directivas de dispositivo.

Por ejemplo, puede centralizar todas las cuentas DEP de diferentes países en el mismo servidor XenMobile, para importar y supervisar todos los dispositivos DEP. Al personalizar los parámetros de inscripción y las opciones del asistente de instalación por departamento, jerarquía organizativa, o cualquier otra estructura, se asegura de que las directivas suministran la funcionalidad adecuada en toda la organización y que los usuarios de los dispositivos reciben la ayuda necesaria para la instalación.

1. En la consola de XenMobile, vaya a **Settings > Apple Device Enrollment Program (DEP)** y, en **Add DEP Account**, haga clic en **Add**.

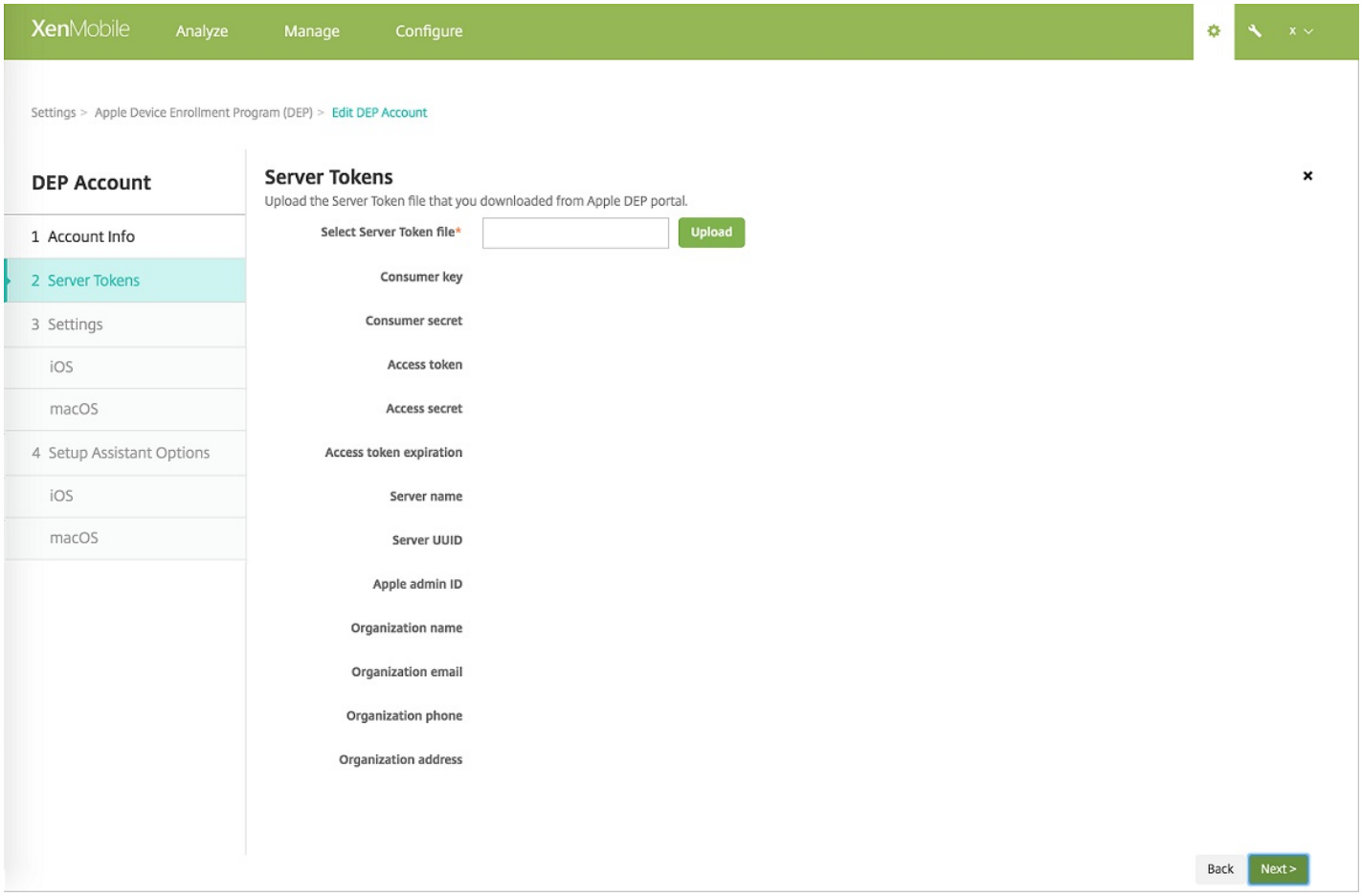


2. En la página **Account Info**, especifique los siguientes parámetros:



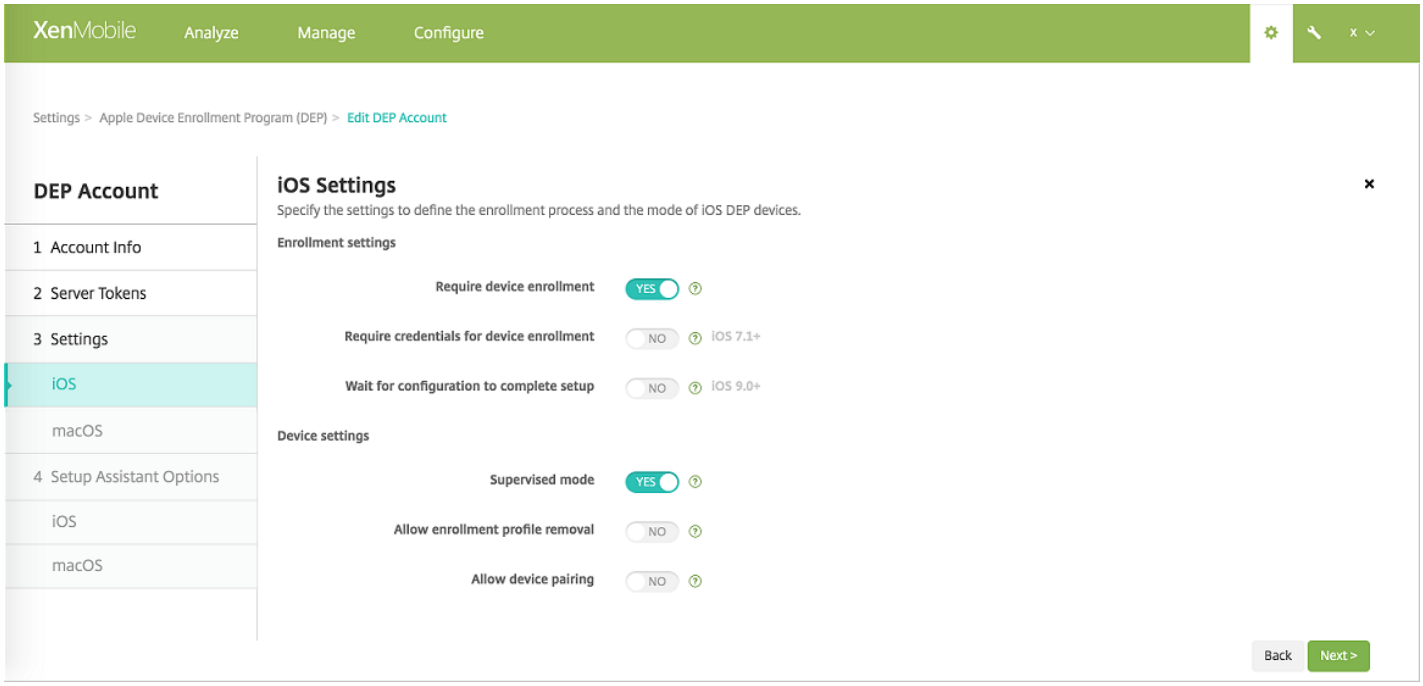
- **DEP account name**. Un nombre único para esta cuenta DEP. Use nombres que reflejen cómo organiza las cuentas DEP (por ejemplo, por país u organización).
- **Business unit**. El departamento o la unidad de negocio a la que se asigna el dispositivo. Este campo es obligatorio.
- **Unique service ID**. Un ID exclusivo optativo para ayudarle a identificar la cuenta.
- **Support phone number**. Un número de teléfono de asistencia al que puedan llamar los usuarios para obtener ayuda durante la instalación. Este campo es obligatorio.
- **Support email address**. Una dirección opcional de correo electrónico de asistencia.

3. En la página **Server Tokens**, especifique su archivo de token de servidor y, a continuación, haga clic en **Upload**.



Aparecerá la información del token de servidor.

4. En **iOS Settings**, especifique los siguientes parámetros:



Parámetros de inscripción

- **Require device enrollment**. Puede requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Yes**.
- **Require credentials for device enrollment**. Puede pedir a los usuarios que indiquen sus credenciales durante la configuración de DEP. Esta función está disponible para iOS 7.1 y versiones posteriores. El valor predeterminado es **No**. Nota: Si DEP está activado en la primera configuración y no se selecciona esta opción, se crean los componentes de DEP (como el usuario DEP, Secure Hub, el inventario de software y el grupo de implementación DEP). Si selecciona esta opción, XenMobile no crea los componentes. Como resultado, si posteriormente desactiva esta opción, los usuarios que no hayan introducido sus credenciales no podrán realizar la inscripción DEP porque los componentes de DEP no existen. Para agregar componentes de DEP, en ese caso, se debe inhabilitar y habilitar la cuenta de DEP.
- **Wait for configuration to complete setup**. Puede requerir que los dispositivos de los usuarios permanezcan en el modo del asistente de instalación hasta implementar todos los recursos de MDM en ellos. Esta función está disponible para dispositivos iOS 9.0 y versiones posteriores en modo supervisado. El valor predeterminado es **No**.
  - En la documentación de Apple consta que los comandos siguientes pueden no funcionar mientras un dispositivo esté en modo de asistente de instalación:
    - InviteToProgram
    - InstallApplication
    - ApplyRedemptionCode
    - InstallMedia
    - RequestMirroring
    - DeviceLock

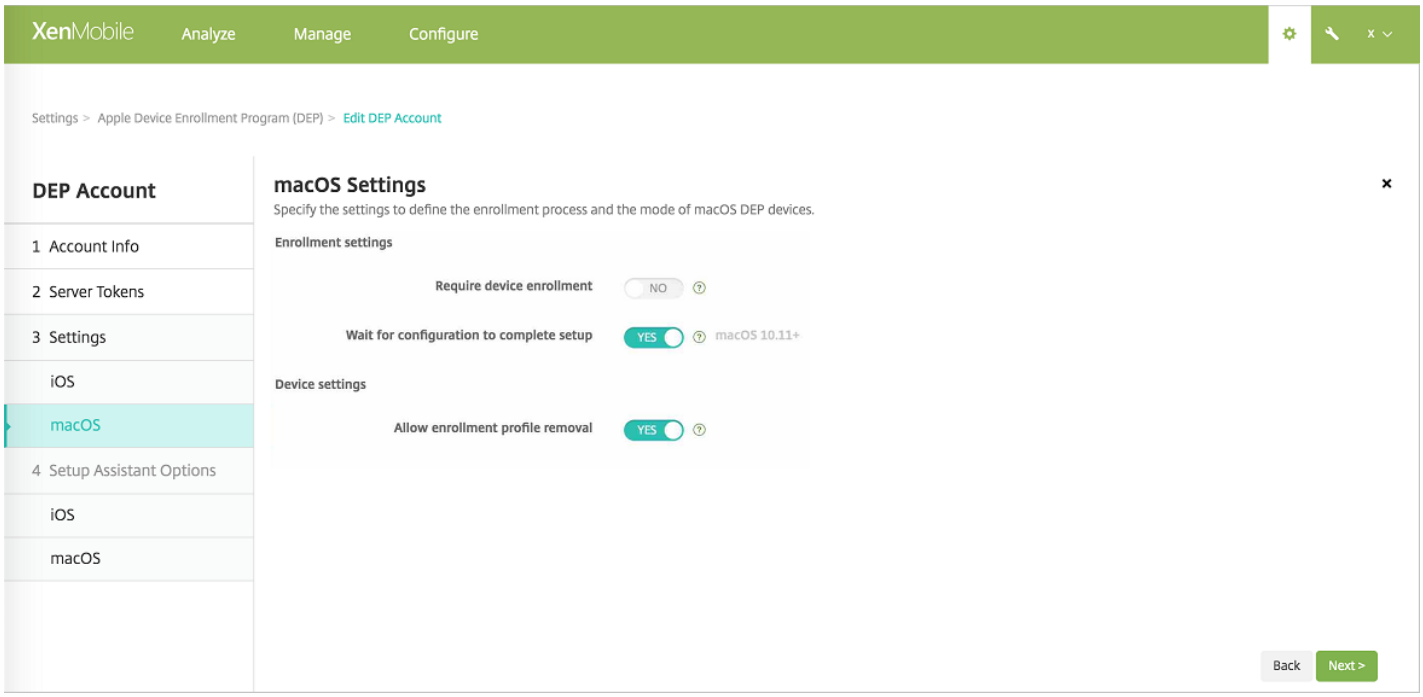
Parámetros del dispositivo

- **Supervised mode**. Se debe establecer en **Yes** si se usa el Apple Configurator para administrar los dispositivos DEP inscritos o si está habilitada la opción **Wait for configuration to complete setup**. El valor predeterminado es **Yes**. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.
- **Allow enrollment profile removal**. Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma

remota. El valor predeterminado es **No**.

- **Allow device pairing**. Seleccione si permitir que los dispositivos inscritos mediante el programa DEP sean administrados a través de iTunes y Apple Configurator. El valor predeterminado es **No**.

5. En **macOS Settings**, especifique los siguientes parámetros:



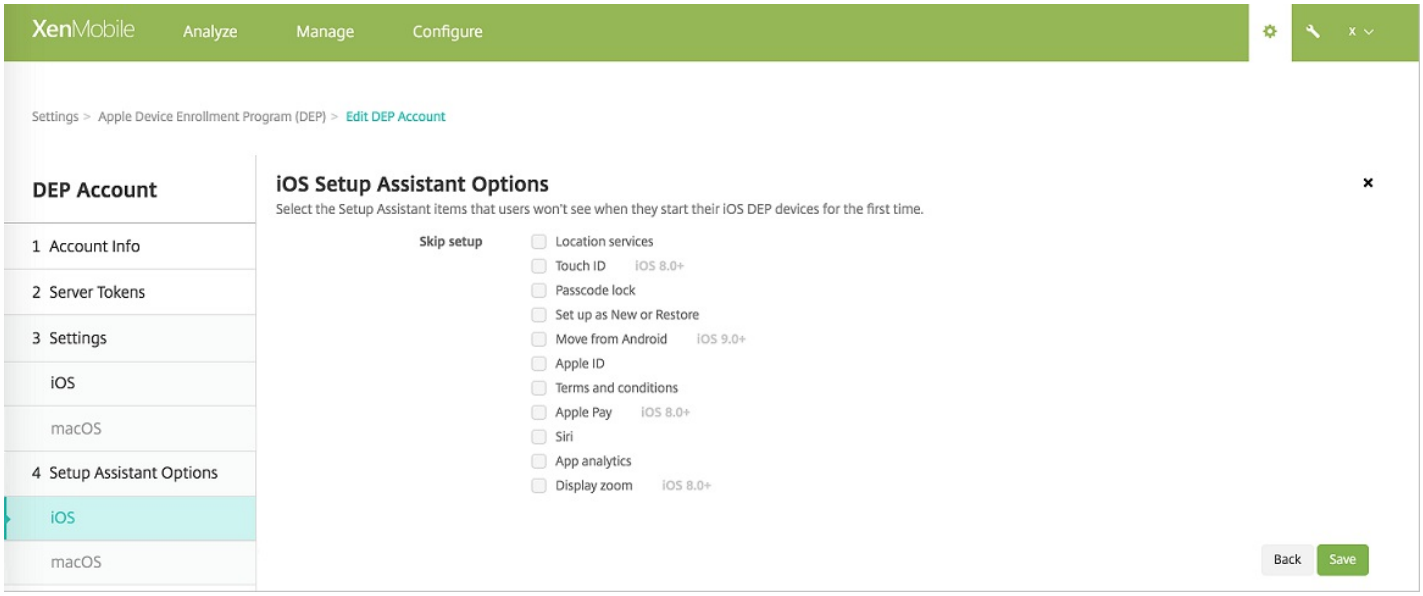
Parámetros de inscripción

- **Require device enrollment**. Puede requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Yes**.
- **Wait for configuration to complete setup**. Si el valor es **Yes**, el dispositivo macOS no continúa con el Asistente de instalación hasta que el código de acceso a recursos MDM se implementa en el dispositivo. La implementación se produce antes de la creación de la cuenta local. Esta configuración está disponible para macOS 10.11 y versiones posteriores. El valor predeterminado es **No**.

Parámetros del dispositivo

- **Allow enrollment profile removal**. Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. El valor predeterminado es **No**.

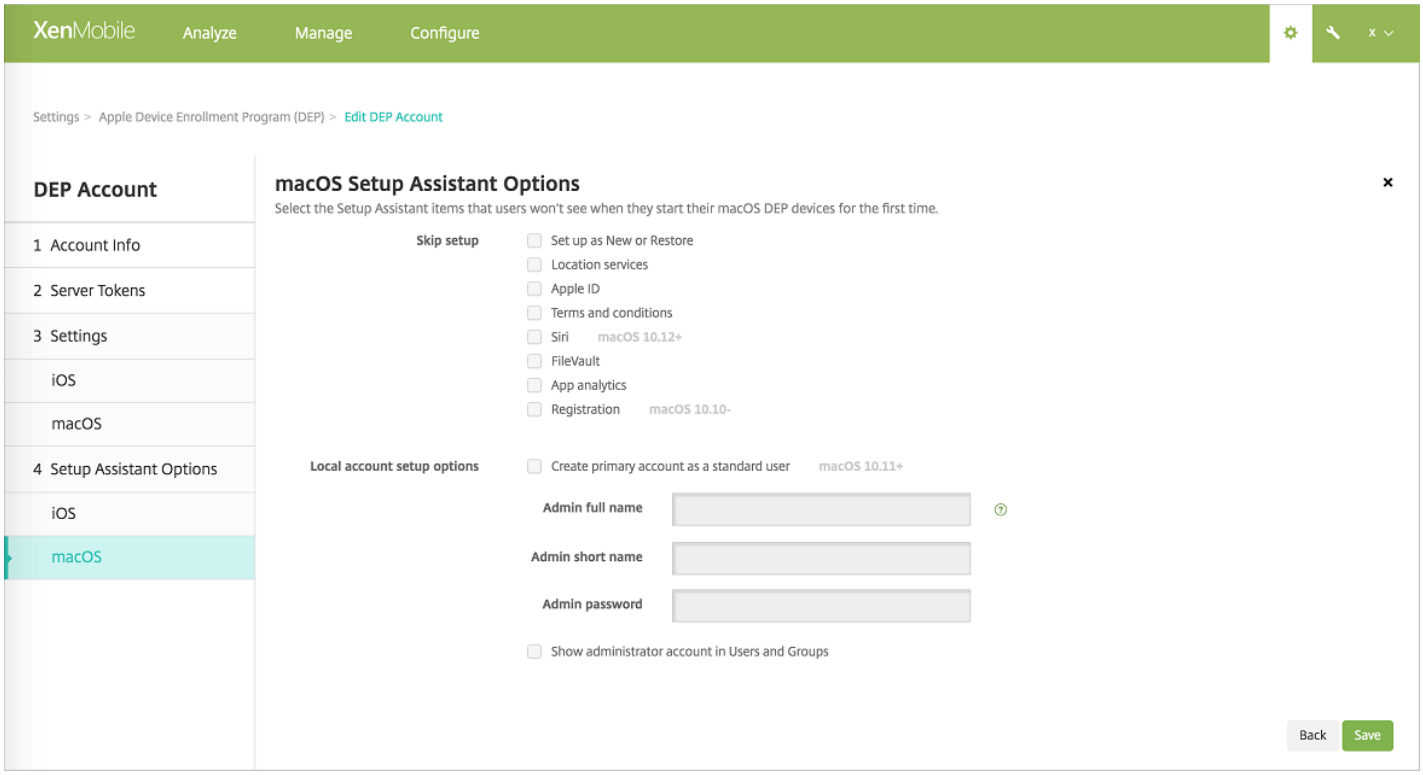
6. En **iOS Setup Assistant Options**, seleccione los pasos a omitir del Asistente de configuración de iOS (es decir, los pasos que los usuarios no tienen que llevar a cabo) cuando inicien sus dispositivos por primera vez. De forma predeterminada, ningún elemento está marcado.



- **Location Services**. Puede configurar el servicio de localización en el dispositivo.
- **Touch ID**. Configurar Touch ID en iOS 8.0 y versiones posteriores.
- **Passcode**. Crear un código de acceso para el dispositivo.
- **Set up as New or Restore**. Configurar el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o iTunes.
- **Move from Android**. Habilitar la transferencia de datos desde un dispositivo Android a un dispositivo iOS 9 o versiones posteriores. Esta opción está disponible solo cuando la opción **Set up as New o Restore** está seleccionada (es decir, se omite el paso).
- **Apple ID**. Configurar una cuenta de ID de Apple para el dispositivo.
- **Terms and Conditions**. Puede requerir que el usuario acepte los términos y condiciones para usar el dispositivo.
- **Apple Pay**. Configurar Apple Pay en iOS 8.0 y versiones posteriores.
- **Siri**. Usar o no usar Siri en el dispositivo.
- **App analytics**. Puede configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.
- **Display Zoom**. Configurar la resolución de la pantalla (estándar o ampliada) en los dispositivos iOS 8.0 o versiones posteriores.

La cuenta DEP aparece en **Settings > Apple Device Enrollment Program (DEP)**.

7. En **macOS Setup Assistant Options**, seleccione los pasos a omitir del Asistente de configuración de macOS (es decir, los pasos que los usuarios no tienen que llevar a cabo) cuando inicien sus dispositivos por primera vez. De forma predeterminada, ningún elemento está marcado.



- **Set up as New or Restore**. Configurar el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o iTunes.
- **Location Services**. Puede configurar el servicio de localización en el dispositivo.
- **Apple ID**. Configurar una cuenta de ID de Apple para el dispositivo.
- **Terms and Conditions**. Puede requerir que el usuario acepte los términos y condiciones para usar el dispositivo.
- **Siri**. Usar o no usar Siri en el dispositivo.
- **FileVault**. Puede usar FileVault para cifrar el disco de arranque. XenMobile solo aplica el parámetro FileVault si el sistema tiene una cuenta de usuario local única registrada en iCloud.

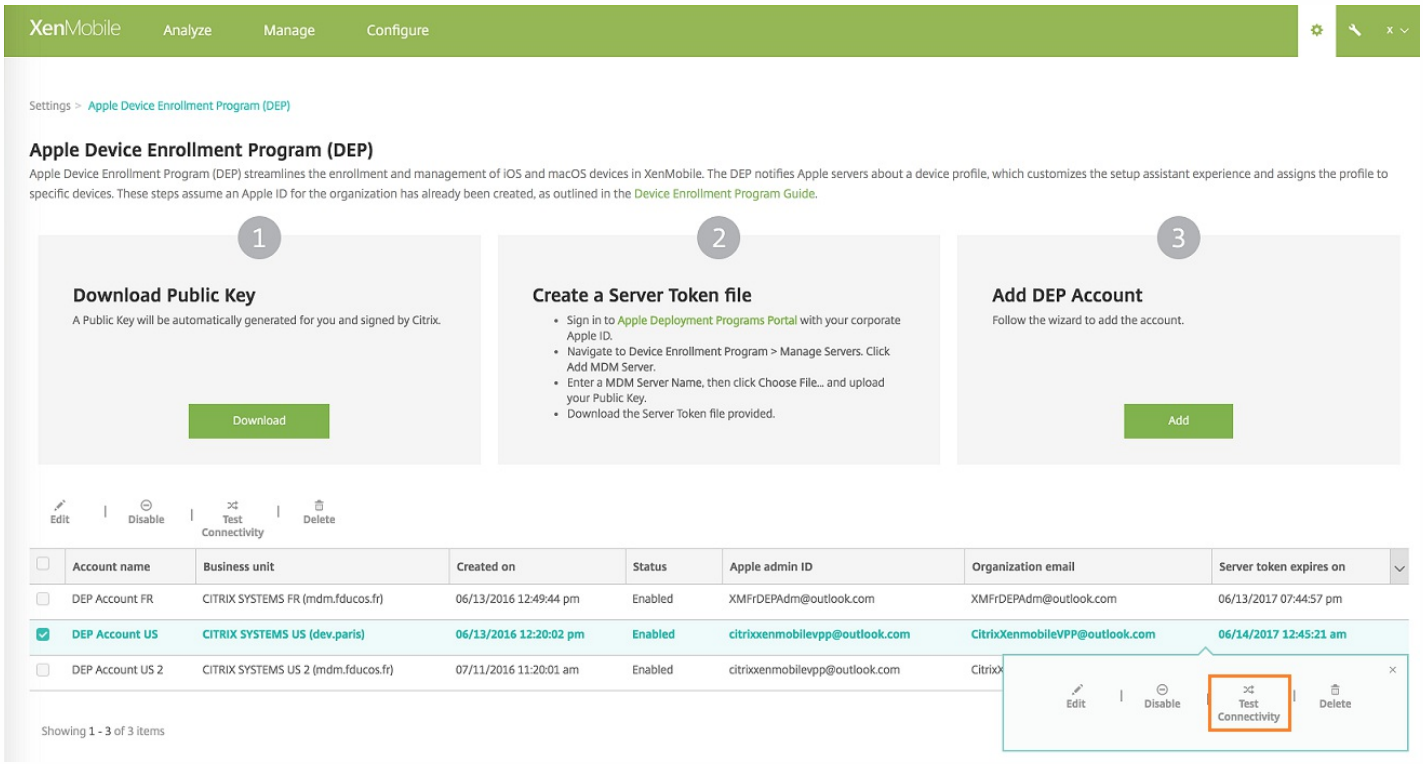
  Puede usar la funcionalidad de cifrado de disco FileVault en macOS para proteger el volumen del sistema mediante el cifrado de su contenido (https://support.apple.com/en-us/HT204837). Si ejecuta el Asistente de configuración en un modelo reciente de portátil Mac donde FileVault está desactivado, es posible que se le solicite habilitar esta funcionalidad. La solicitud aparece en los sistemas nuevos y en los sistemas actualizados a OS X 10.10 o 10.11, pero solo si el sistema tiene una cuenta de administrador local única y esa cuenta está registrada en iCloud.

- **App analytics**. Puede configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.
- **Registration**. Puede requerir a los usuarios que registren su dispositivo.

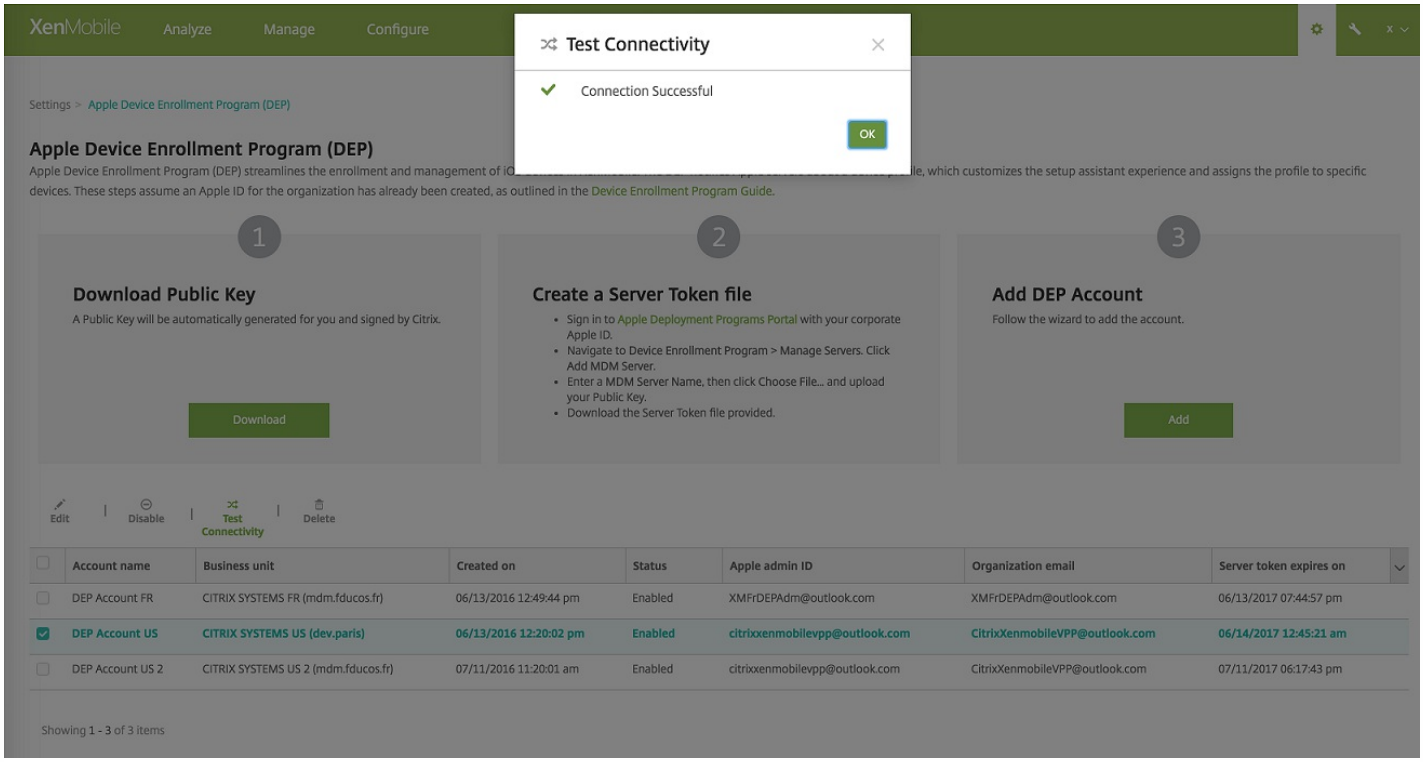
  La información de registro estaba disponible en OS X 10.9. El proceso de registro permitía enviar información de registro del sistema a Apple. Esta información asociaba su información de contacto con el hardware de Mac. Apple utilizaba principalmente la información para facilitar la tarea de la asistencia de AppleCare. Si había especificado anteriormente un ID de Apple, el Asistente de configuración enviaba opcionalmente la información de registro basada en su ID de cuenta de Apple. Si no había indicado ningún ID de Apple, podía escribir manualmente su información de contacto.

En **Local account setup options**, puede especificar los parámetros para crear una cuenta de administrador, condición necesaria para macOS. XenMobile crea la cuenta a partir de la información especificada.

8. Para probar la conectividad entre XenMobile y Apple, seleccione la cuenta y haga clic en **Test Connectivity**.



Aparecerá un mensaje de estado.



Configuración de reglas de implementación de

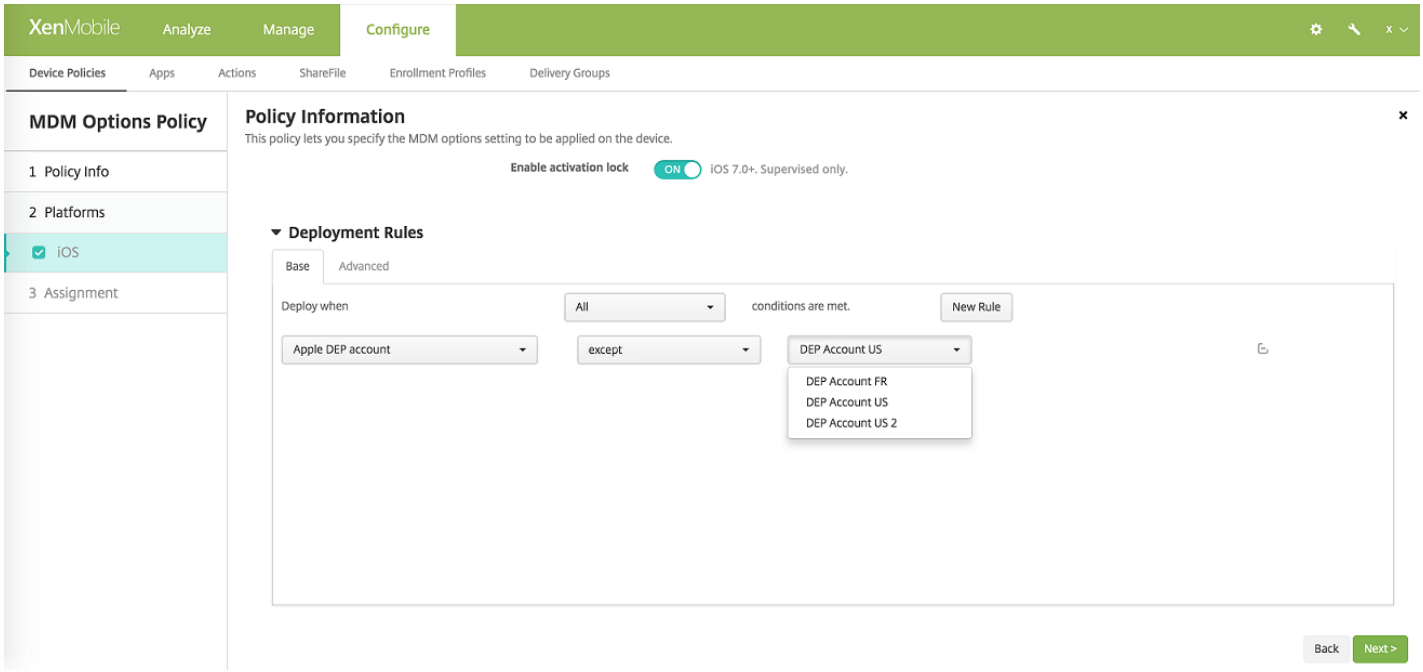
aplicaciones y directivas de dispositivo para cuentas DEP

Puede asociar cuentas DEP con aplicaciones y directivas de dispositivo desde la sesión **Deployment Rules**, en **Configure > Device Policies** y **Configure > Apps**. Puede especificar que una directiva o una aplicación:

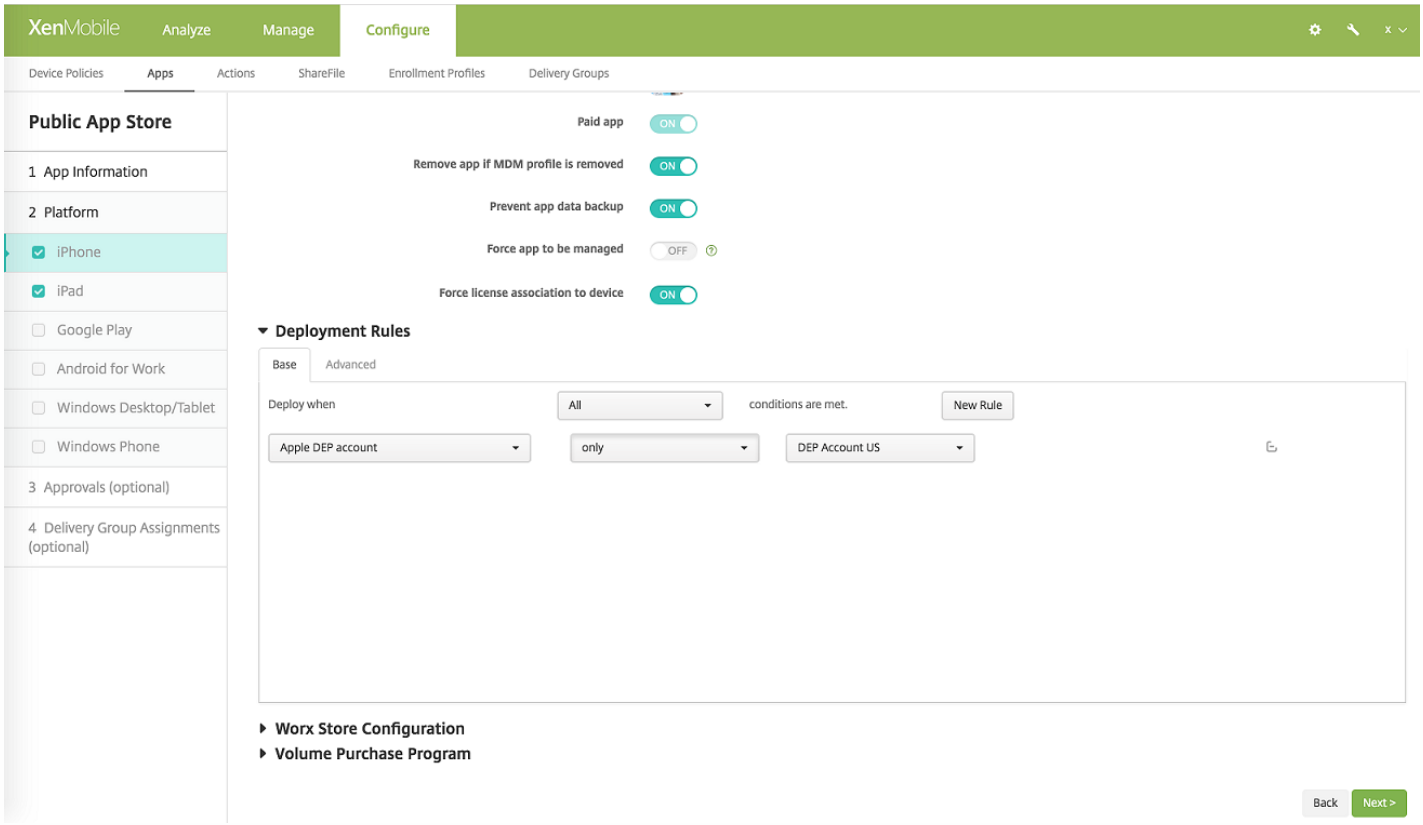
- Se implemente solo para una cuenta concreta DEP de Apple.
- Se implemente para todas las cuentas DEP de Apple, excepto la seleccionada.

La lista de las cuentas DEP solo incluye aquellas cuentas que tengan el estado habilitado o inhabilitado. Si la cuenta DEP está inhabilitada, el dispositivo DEP no pertenece a esta cuenta. Por lo tanto, XenMobile no implementa la aplicación o la directiva en el dispositivo.

En el siguiente ejemplo, la directiva de opciones de MDM para iOS se implementa en todos los dispositivos, salvo en aquellos cuya cuenta DEP de Apple sea "Cuenta DEP para EUA".

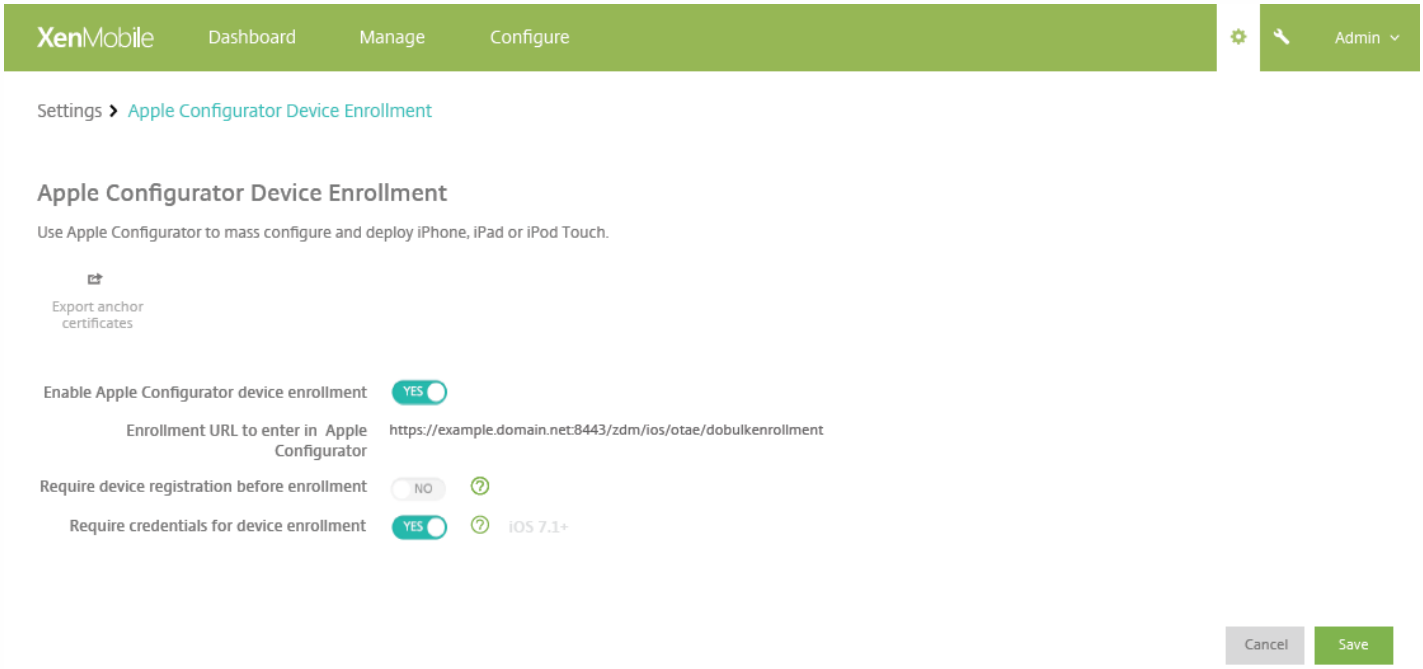


En el siguiente ejemplo, una aplicación de tienda pública de iPhone se implementa solo para dispositivos cuya cuenta DEP de Apple sea "Cuenta DEP para EUA".



Configuración de parámetros de Apple Configurator

1. En la consola de XenMobile, vaya a **Settings > Apple Configurator Device Enrollment**.



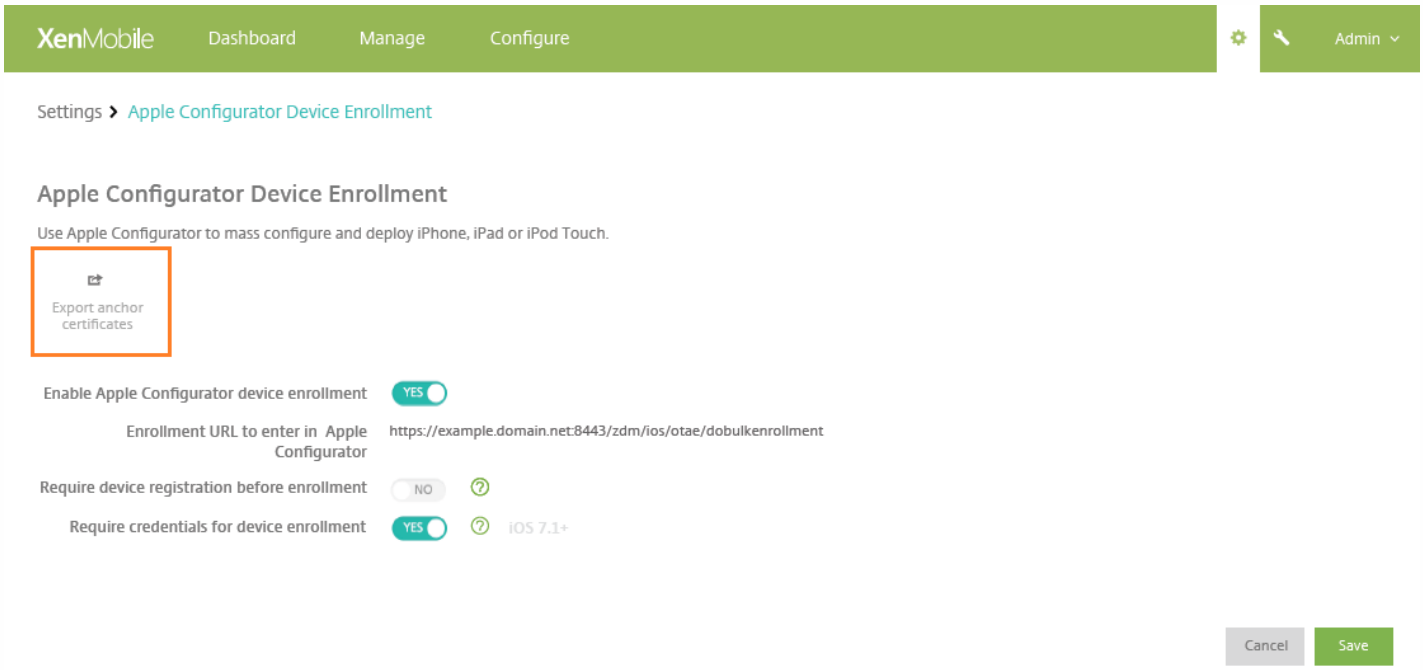
2. Establezca **Enable Apple Configurator Device Enrollment** en **Yes**.

3. **Enrollment URL to enter in Apple Configurator** es un campo de solo lectura. Esta es la URL del servidor XenMobile que se comunica con Apple. Más adelante en estos pasos, copia y pega la dirección URL en Apple Configurator. En Apple Configurator 2, la URL de inscripción es el nombre de dominio completo (FQDN) o la dirección IP del servidor XenMobile (por ejemplo, mdm.servidor.url.com).

4. Para evitar que se inscriban dispositivos desconocidos, establezca **Require device registration before enrollment** en **Yes**. Nota: Si el valor de este parámetro es **Yes**, debe agregar los dispositivos configurados en **Manage > Devices** de XenMobile manualmente o a través de un archivo CSV antes de la inscripción.

5. Para obligar a los usuarios de los dispositivos iOS 7.1 y versiones posteriores que introduzcan sus credenciales cuando se inscriban, establezca **Require credentials for device enrollment** en **Yes**. El valor predeterminado es no requerir credenciales para la inscripción.

6. Nota: Si el servidor XenMobile está usando un certificado SSL de confianza, omita el paso siguiente. Haga clic en **Export anchor certificates** y guarde el archivo certchain.pem en el llavero de OS X (Inicio de sesión o Sistema).



7. Inicie Apple Configurator y vaya a **Prepare > Setup > Configure Settings**.

8. En el parámetro **Device Enrollment**, pegue la URL del servidor MDM del paso 4 en el cuadro **MDM server URL** de Apple Configurator.

9 En el parámetro **Device Enrollment**, copie la entidad de certificación raíz y la entidad de certificación de servidores SSL a los certificados **Anchor**, si XenMobile no está usando un certificado SSL de confianza.

10. Use un cable de conector de Dock con USB para conectar los dispositivos al equipo Mac que ejecuta Apple Configurator para configurar simultáneamente hasta 30 dispositivos conectados. Si no dispone de un conector de Dock, use varios concentradores USB 2.0 de alta velocidad para conectar los dispositivos.

11. Haga clic en **Prepare**. Para obtener más información sobre la preparación de dispositivos con Apple Configurator, consulte la página de ayuda Prepare devices de Apple Configurator.

12. En Apple Configurator, configure las directivas de dispositivo que necesite.

13. A medida que prepare cada dispositivo, enciéndalo para iniciar el asistente de configuración de iOS, que prepara el dispositivo para su primer uso.

Para renovar o actualizar certificados cuando se usa Apple DEP

Cuando se renueva el certificado SSL (Secure Sockets Layer) de XenMobile, hay que cargar un nuevo certificado en la consola de XenMobile, en **Settings** > **Certificates**. En el cuadro de diálogo **Import**, en **Use as**, debe hacer clic en **SSL Listener** de forma que el certificado se utilice para SSL. Después de reiniciar el servidor, XenMobile utiliza el nuevo certificado SSL. Para obtener más información sobre certificados en XenMobile, consulte Carga de certificados en XenMobile.

No es necesario volver a establecer la relación de confianza entre XenMobile y Apple DEP al renovar o actualizar el certificado SSL. No obstante, puede configurar los parámetros de DEP en cualquier momento siguiendo los pasos anteriores en este artículo.

Para obtener más información sobre DEP de Apple, consulte la documentación de Apple.

Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

> ## 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:

a. Cambie **Supervision control** a **On**. Citrix recomienda elegir esta opción si quiere mantener el control del dispositivo de forma continua mediante la aplicación periódica de una configuración.

b. Si lo prefiere, puede proporcionar un nombre para el dispositivo.

c. 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**.

Implementación de dispositivos iOS y macOS a través del programa DEP de Apple

Feb 27, 2017

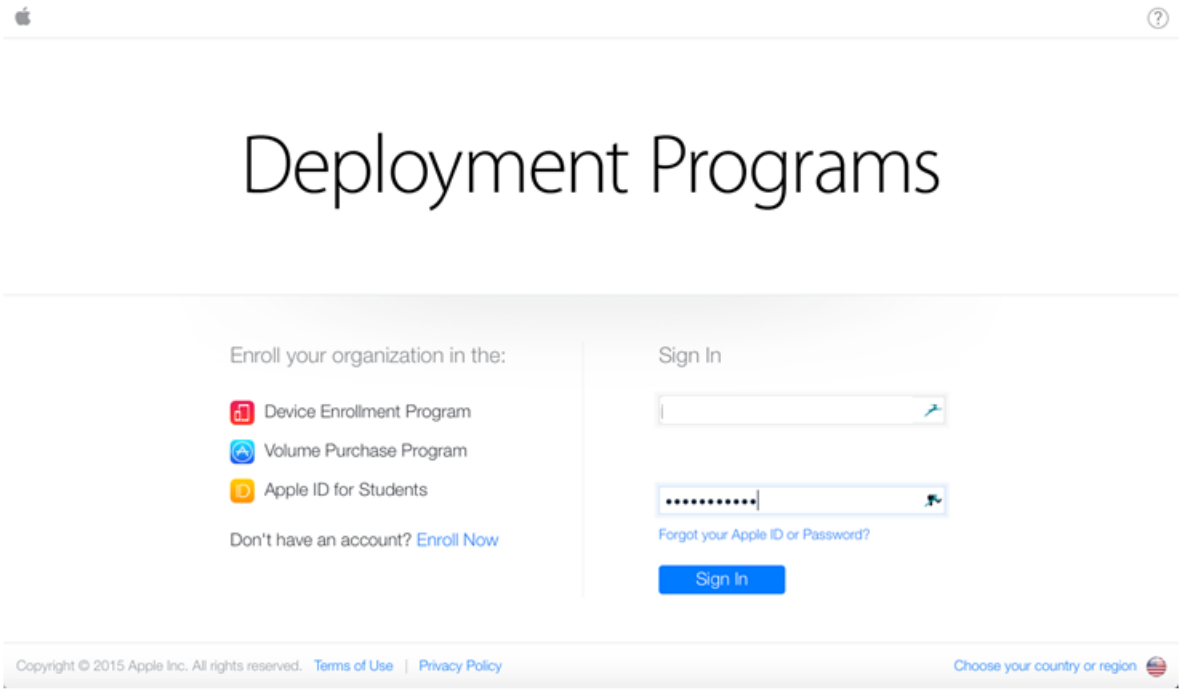
Debe inscribirse en el Programa de implementación de Apple para usar Device Enrollment Program (DEP) para inscribir dispositivos iOS y macOS y administrarlos en XenMobile. Para obtener información sobre cómo obtener una cuenta del Programa de implementación de Apple, consulte este PDF de Apple.

Tenga en cuenta que el Programa de implementación de Apple está disponible para las organizaciones, no para personas individuales. Debe facilitar una cantidad considerable de datos de la empresa para crear una cuenta en el Programa de implementación de Apple. Por lo tanto, puede tardar algún tiempo en solicitar y recibir aprobación para la cuenta.

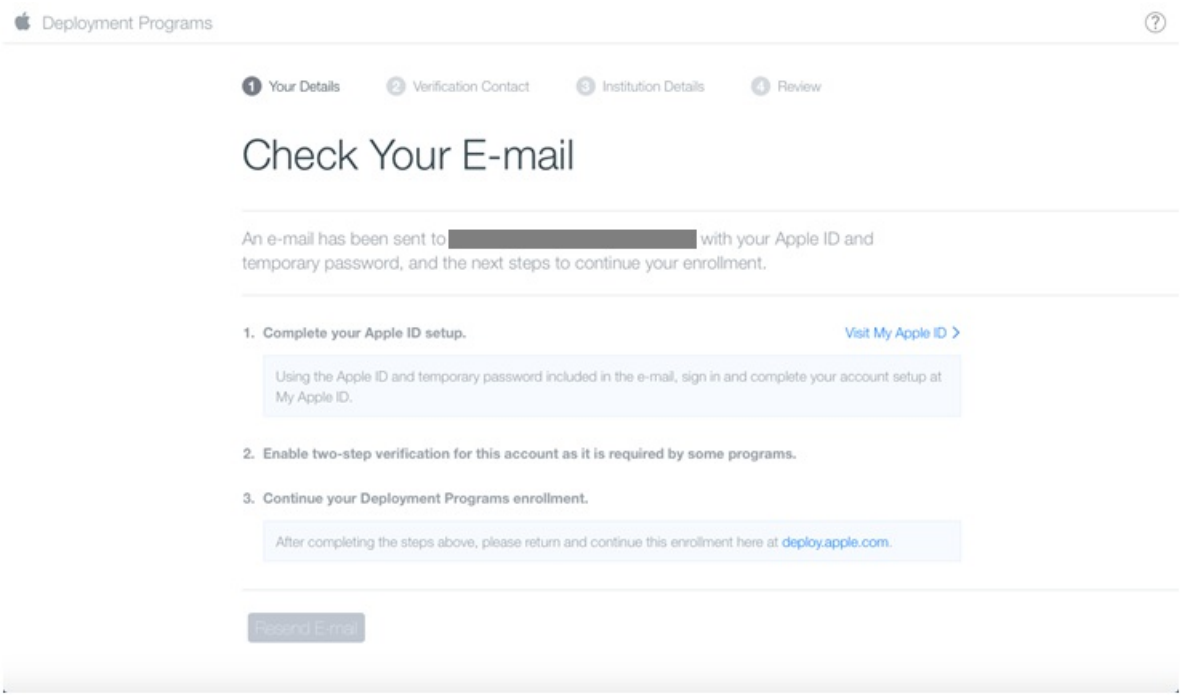
Inscripción en el Programa de implementación de Apple

1. Vaya a deploy.apple.com para solicitar una cuenta del Programa de implementación de Apple. Al solicitar una cuenta DEP, se recomienda usar una dirección de correo electrónico asociada a una organización, como dep@nombre-de-empresa.com.

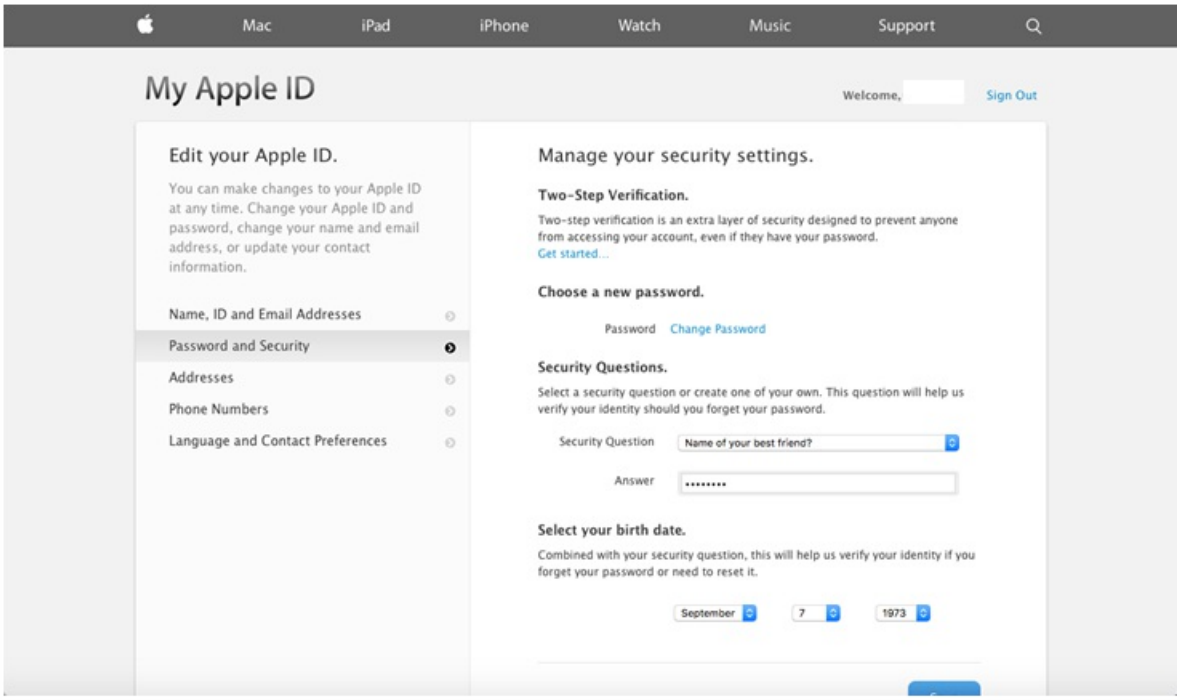
Nota: Para las cuentas del ámbito educativo, vaya a https://school.apple.com/.



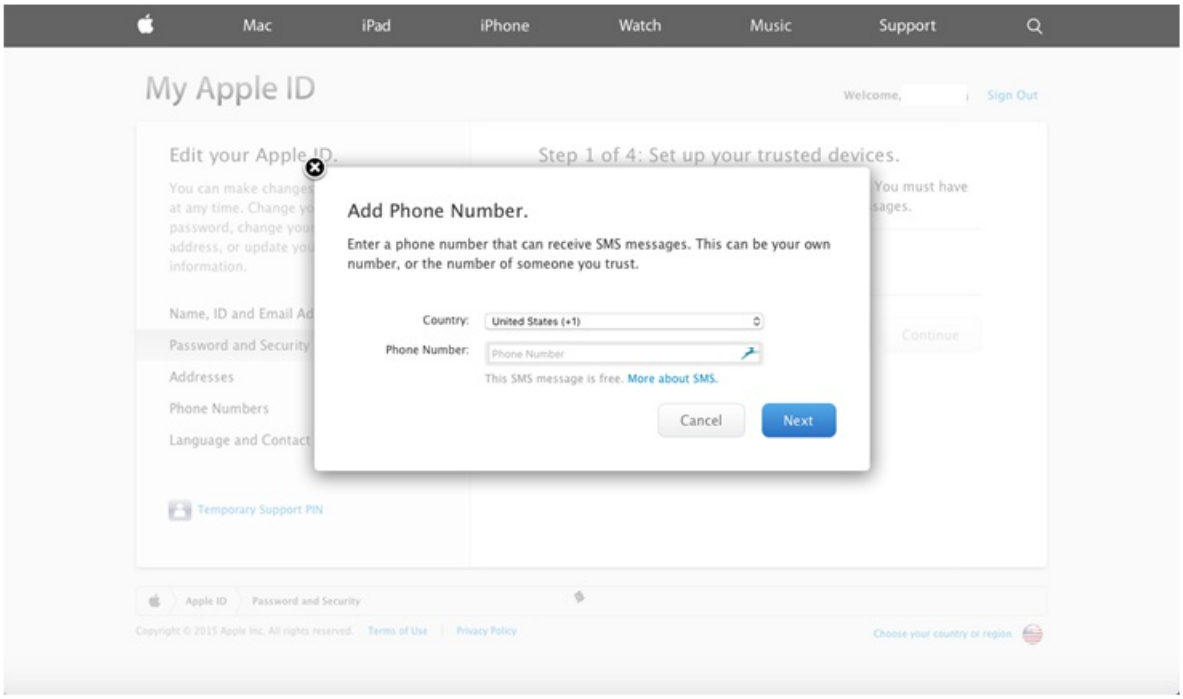
2. Después de introducir los datos de su organización, Apple le enviará una contraseña temporal para el nuevo ID de Apple.



3. A continuación, debe iniciar sesión con el ID de Apple y rellenar los parámetros de seguridad para la cuenta.

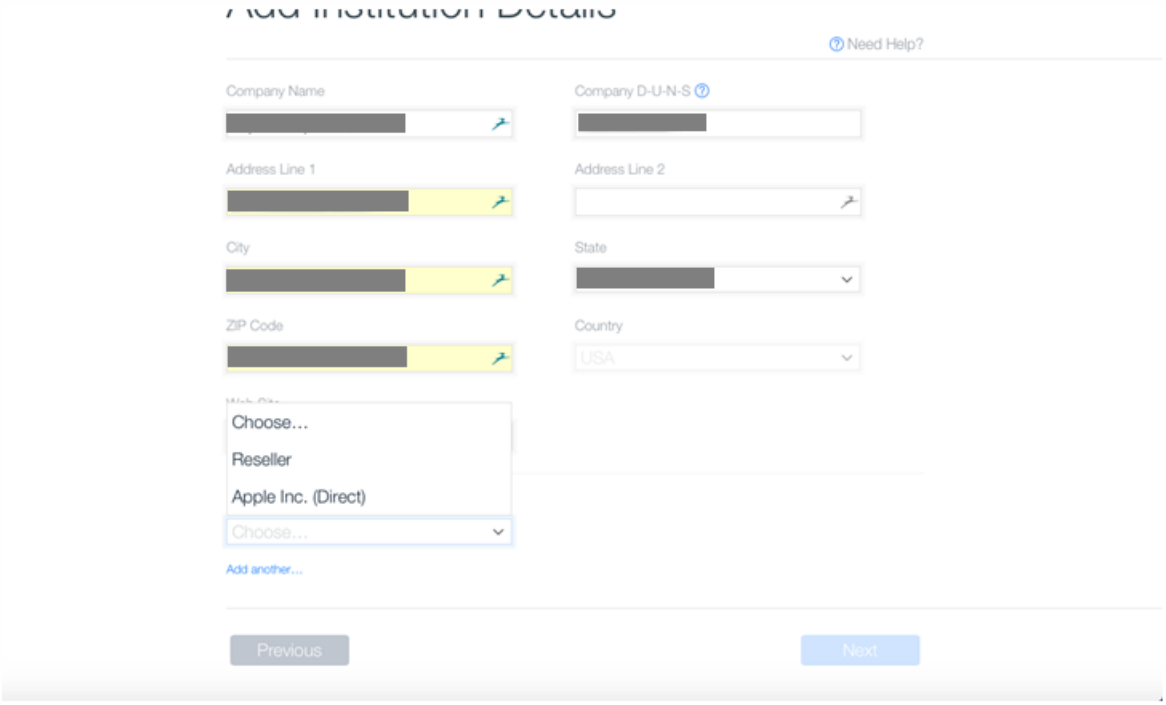


4. Configure y habilite la verificación en dos pasos, necesaria para usar el portal DEP. Durante este procedimiento, después de agregar un número de teléfono, recibirá un PIN de cuatro dígitos para la verificación en dos pasos.

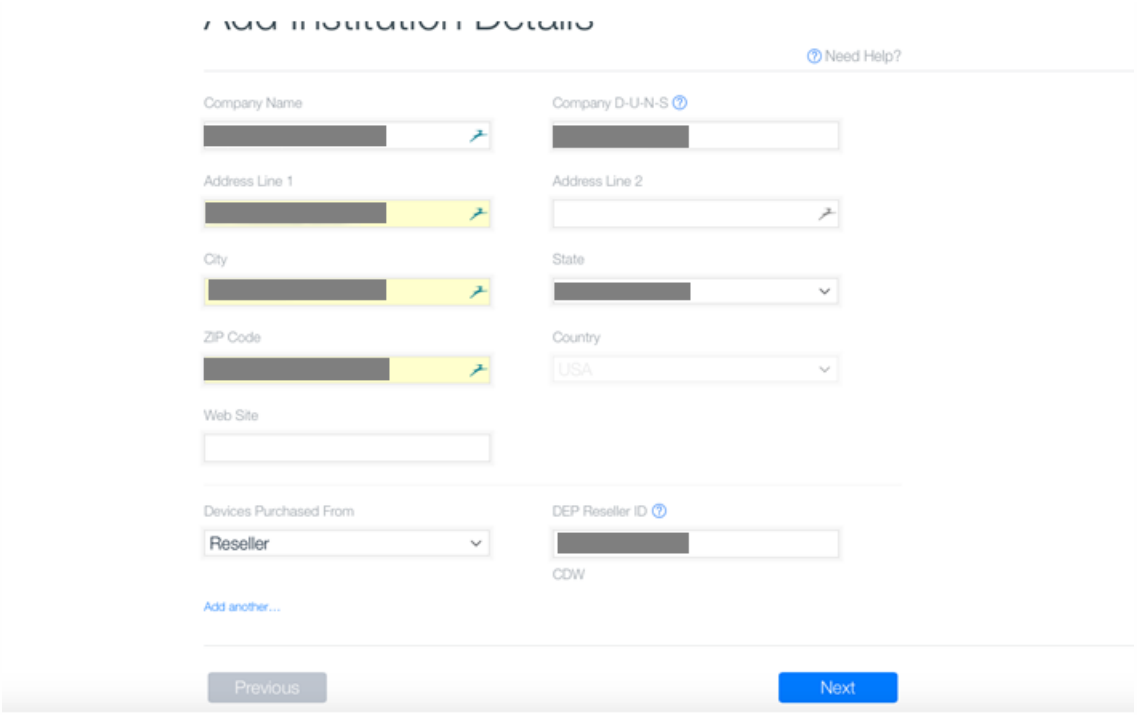


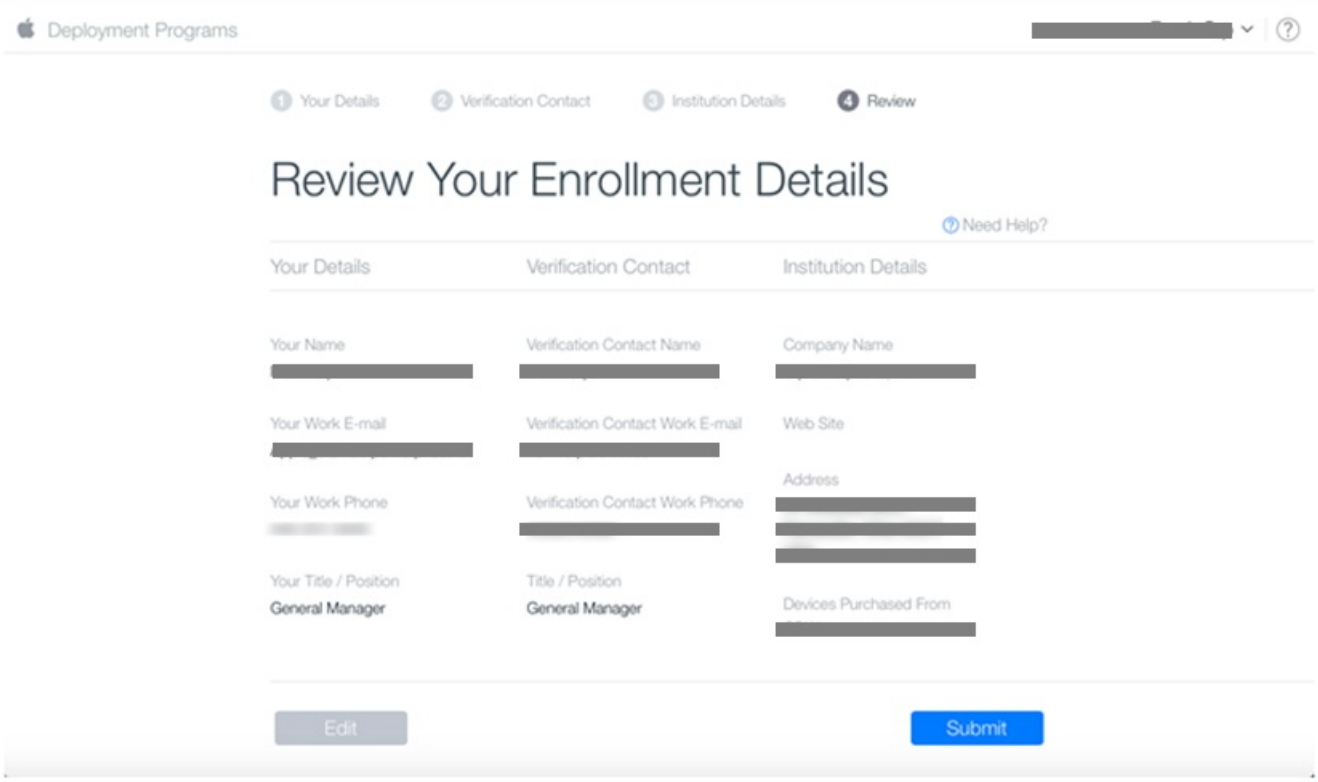
5. Inicie sesión en el portal DEP para completar la configuración de la cuenta mediante la verificación en dos pasos que acaba de configurar.

6. Agregue los datos de su empresa y seleccione dónde adquiere sus dispositivos. Para ver información sobre las opciones de compra, consulte la sección siguiente Cómo adquirir dispositivos habilitados con DEP.

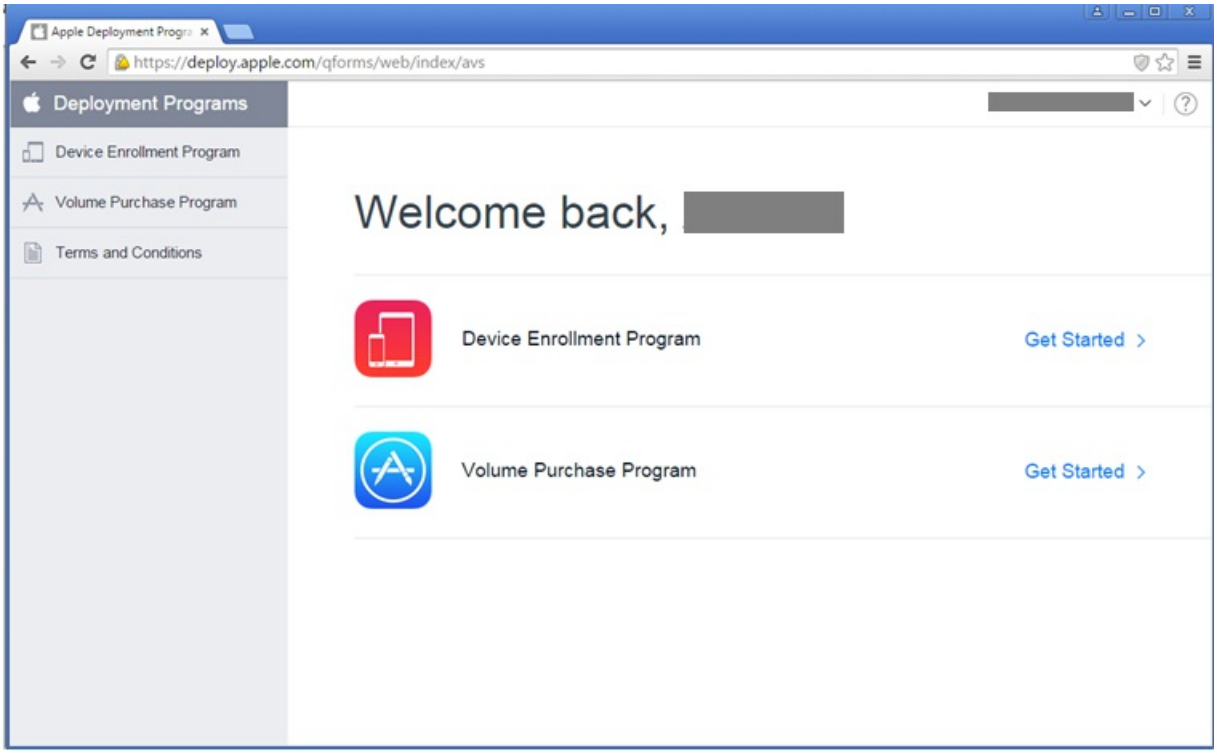


7. Agregue el número de cliente de Apple o el ID del proveedor DEP. Verifique sus datos de inscripción y espere a que Apple apruebe su cuenta.





8. Después de recibir las credenciales de inicio de sesión por parte de Apple, inicie sesión en el portal DEP de Apple.



Para conectar su cuenta a XenMobile, consulte "Integración de la cuenta DEP de Apple con XenMobile" en Inscripción en masa de dispositivos iOS y macOS.

Cómo adquirir dispositivos habilitados con DEP

Puede adquirir dispositivos habilitados con DEP directamente desde Apple o de proveedores y operadores autorizados. Para adquirir productos de Apple, debe proporcionar su ID de cliente de Apple en el portal DEP de Apple. Su ID de cliente permite a Apple asociar los dispositivos adquiridos a la cuenta DEP de Apple.

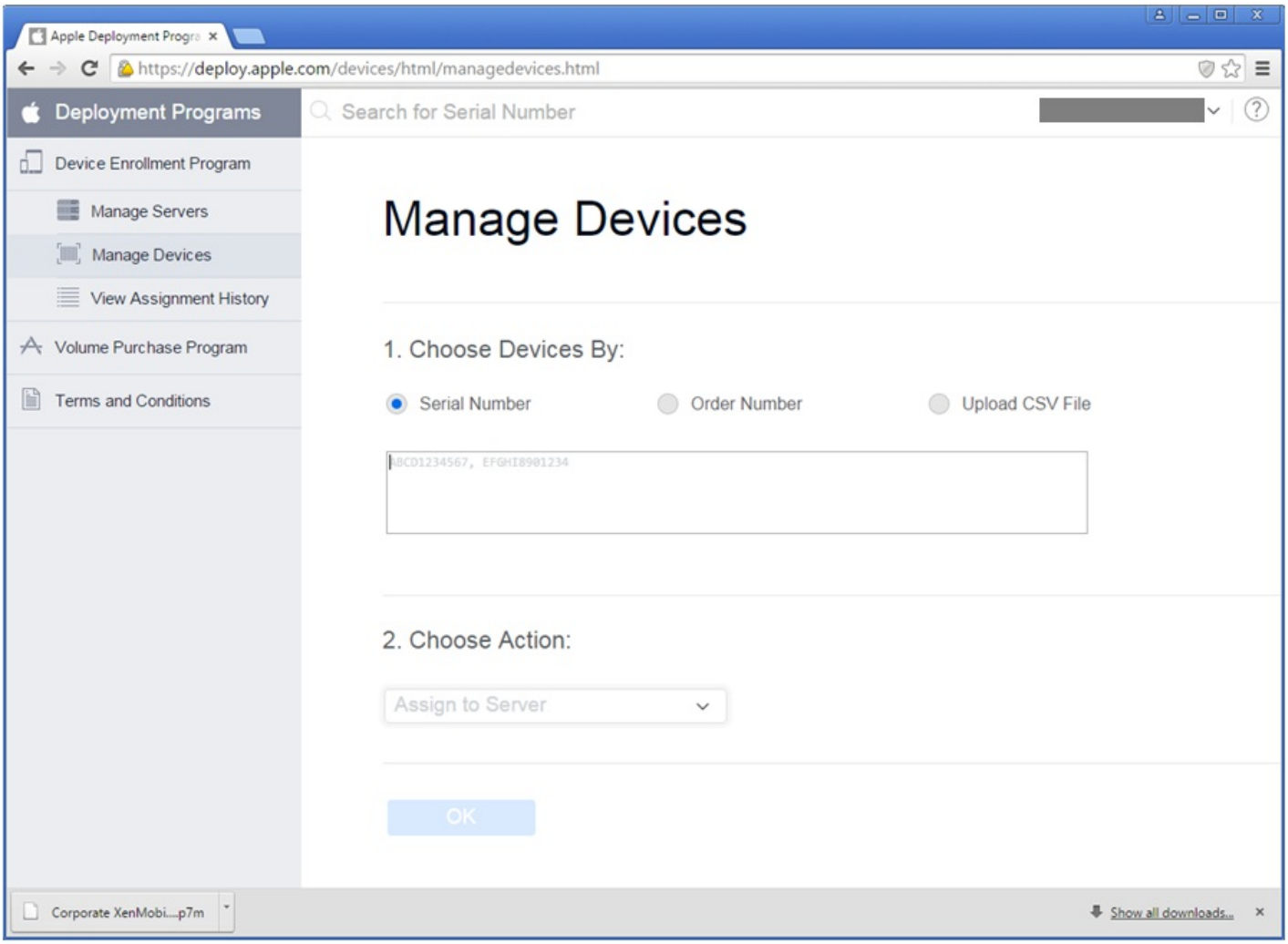
Para adquirirlos de un proveedor o de un operador autorizado de Apple, póngase en contacto con ellos para ver si participan en el programa Apple DEP. Pida el ID de Apple DEP al proveedor cuando compre los dispositivos. Apple necesitará este dato para agregar el proveedor de Apple DEP a su cuenta de Apple DEP. Después de agregar el ID de Apple DEP de su proveedor, recibirá un ID de cliente DEP. Facilite su ID de cliente DEP al proveedor, quien lo usará para enviar información sobre sus compras de dispositivos a Apple. Para obtener más información, consulte este sitio Web de Apple.

Administración de dispositivos habilitados con DEP

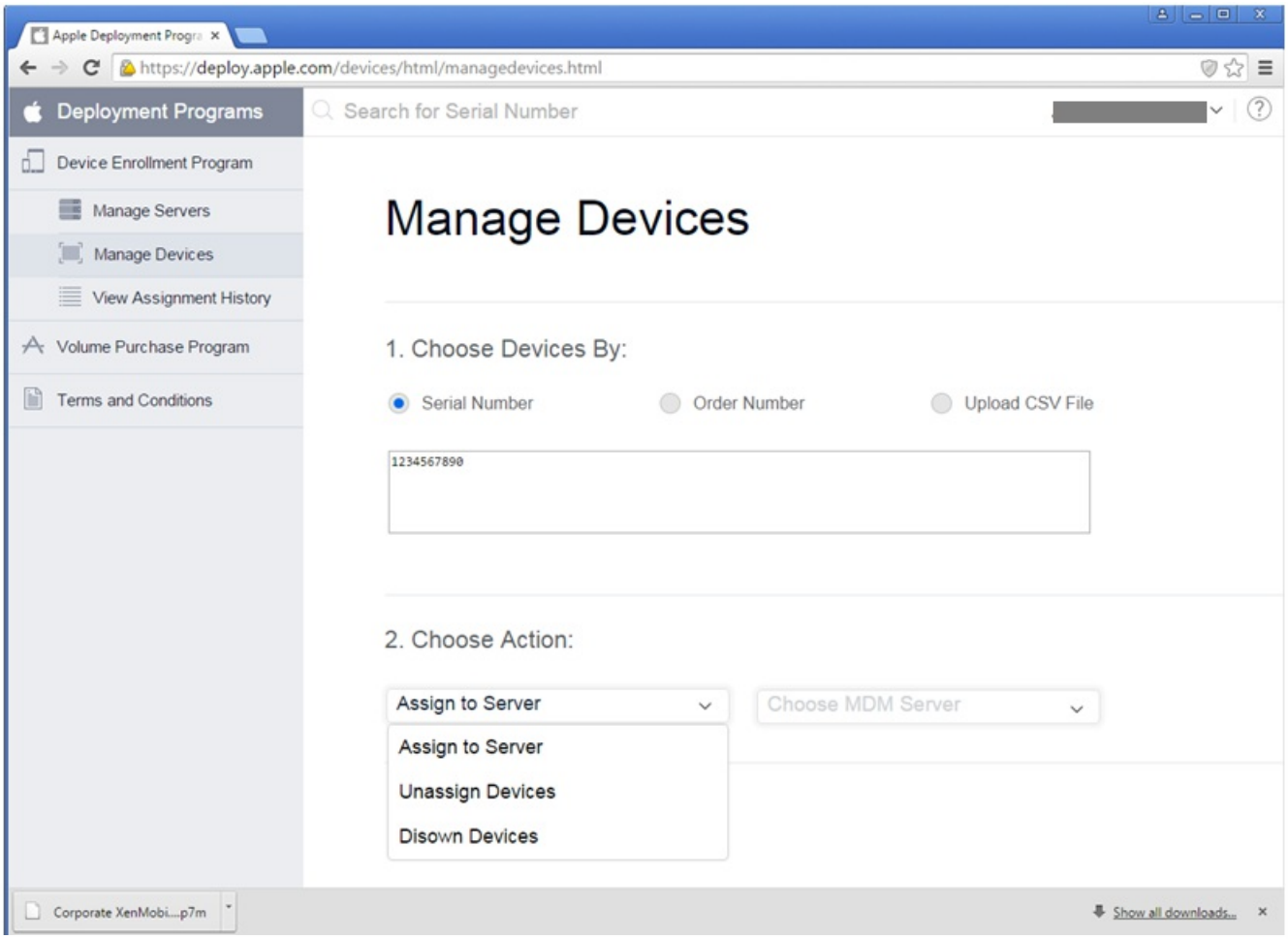
Siga estos pasos para asociar dispositivos a su servidor XenMobile a través del portal DEP y actualizar su cuenta DEP.

1. Inicie sesión en el portal de Apple DEP.

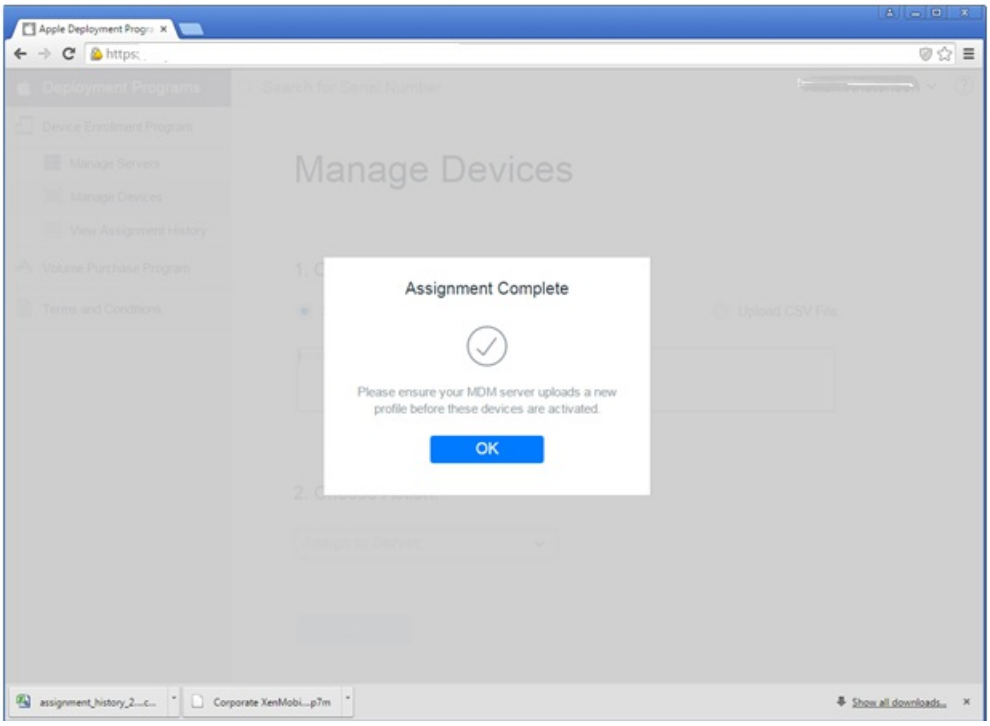
2. Haga clic en **Device Enrollment Program** y, a continuación, haga clic en **Manage Devices**. Haga clic en **Choose Devices By**, elija la opción con la que quiere cargar y definir sus dispositivos habilitados con Apple DEP: **Serial Number**, **Order Number** o **Upload CSV File**.



3. Para asignar los dispositivos a un servidor XenMobile, en **Choose Action**, elija **Assign to server**. A continuación, en la lista, seleccione el nombre del servidor XenMobile. Haga clic en **OK**.



Sus dispositivos Apple DEP están ahora asociados al servidor XenMobile seleccionado.



Experiencia de usuario al inscribir un dispositivo habilitado con Apple DEP

Cuando los usuarios inscriben un dispositivo habilitado con Apple DEP, su experiencia es la siguiente.

1. Los usuarios inician su dispositivo habilitado con Apple DEP.

2. XenMobile entrega la configuración de Apple DEP que ha definido en la consola XenMobile al dispositivo habilitado con Apple DEP.

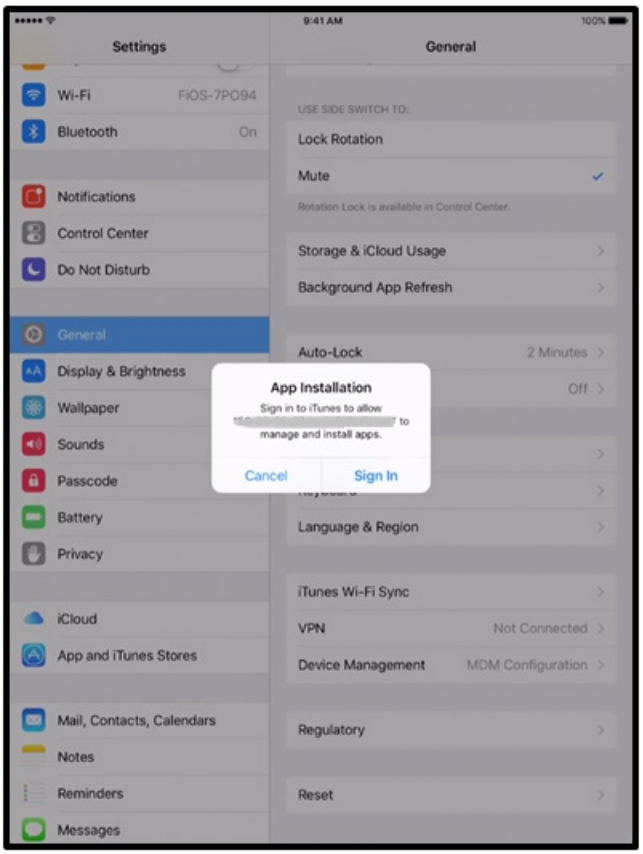
3. Los usuarios configuran los parámetros iniciales en su dispositivo.

4. El dispositivo inicia automáticamente el proceso de inscripción en XenMobile.

5. Los usuarios continúan la configuración de los demás parámetros iniciales en su dispositivo.

6. En la pantalla de inicio, es posible que se solicite a los usuarios iniciar sesión en iTunes para descargar Citrix Secure Hub.

> ### Nota
>
> Este paso es opcional si se configura XenMobile para implementar la aplicación Secure Hub con la asignación de aplicaciones por dispositivos del Programa de Compras por Volumen (PCV). En este caso, no se necesita crear una cuenta de iTunes ni utilizar una cuenta existente.



7. Los usuarios abren Secure Hub e introducen sus credenciales. Si hay una directiva que lo requiera, puede que se pida a los

usuarios que creen y confirmen un PIN.

XenMobile implementa las aplicaciones requeridas restantes en el dispositivo.

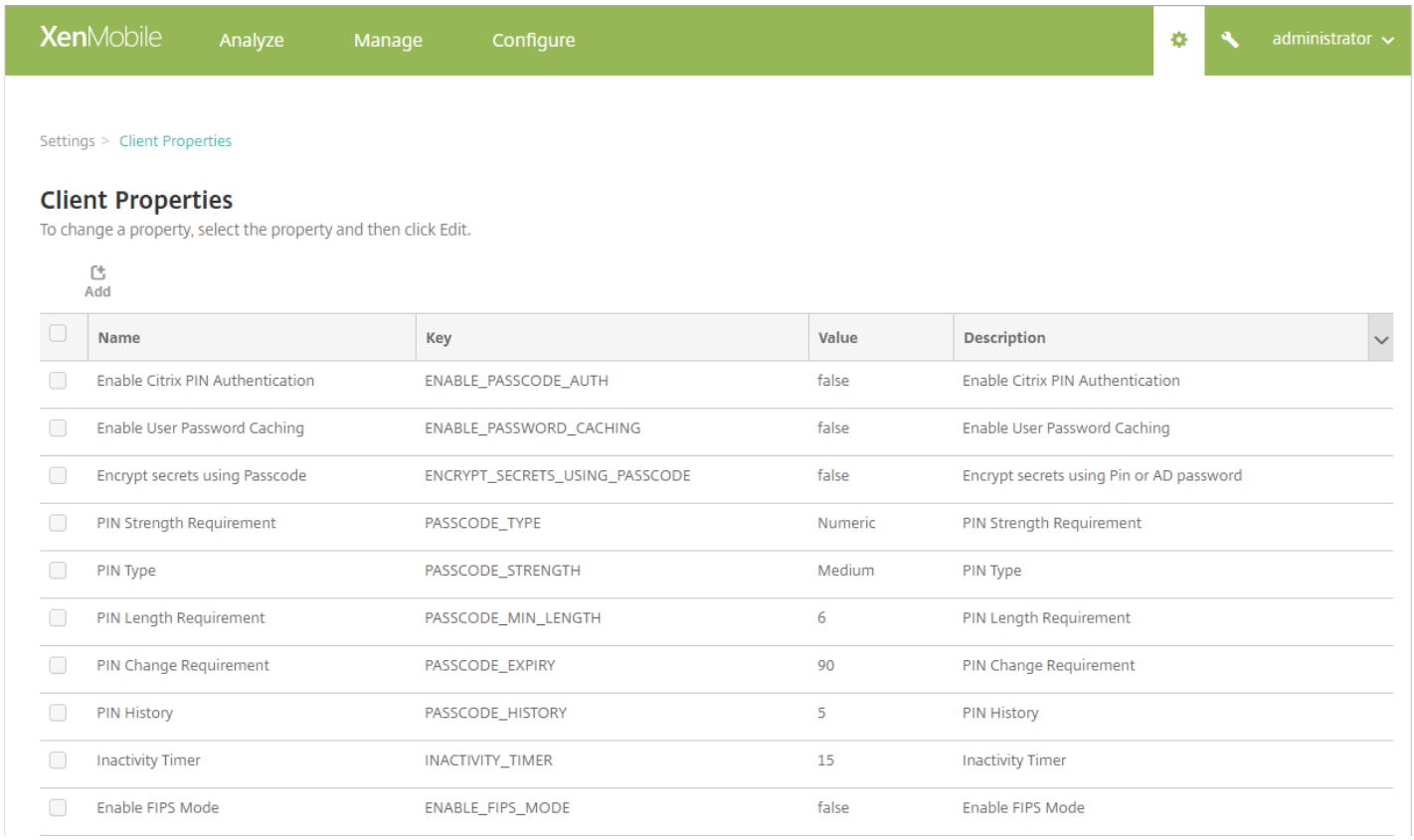
Propiedades de cliente

Apr 26, 2017

En las propiedades de cliente, se ofrece información que se proporciona directamente a Secure Hub en los dispositivos de los usuarios. Puede usar estas propiedades para definir parámetros avanzados de configuración, como el PIN de Citrix. Las propiedades de cliente se obtienen del servicio de asistencia de Citrix.

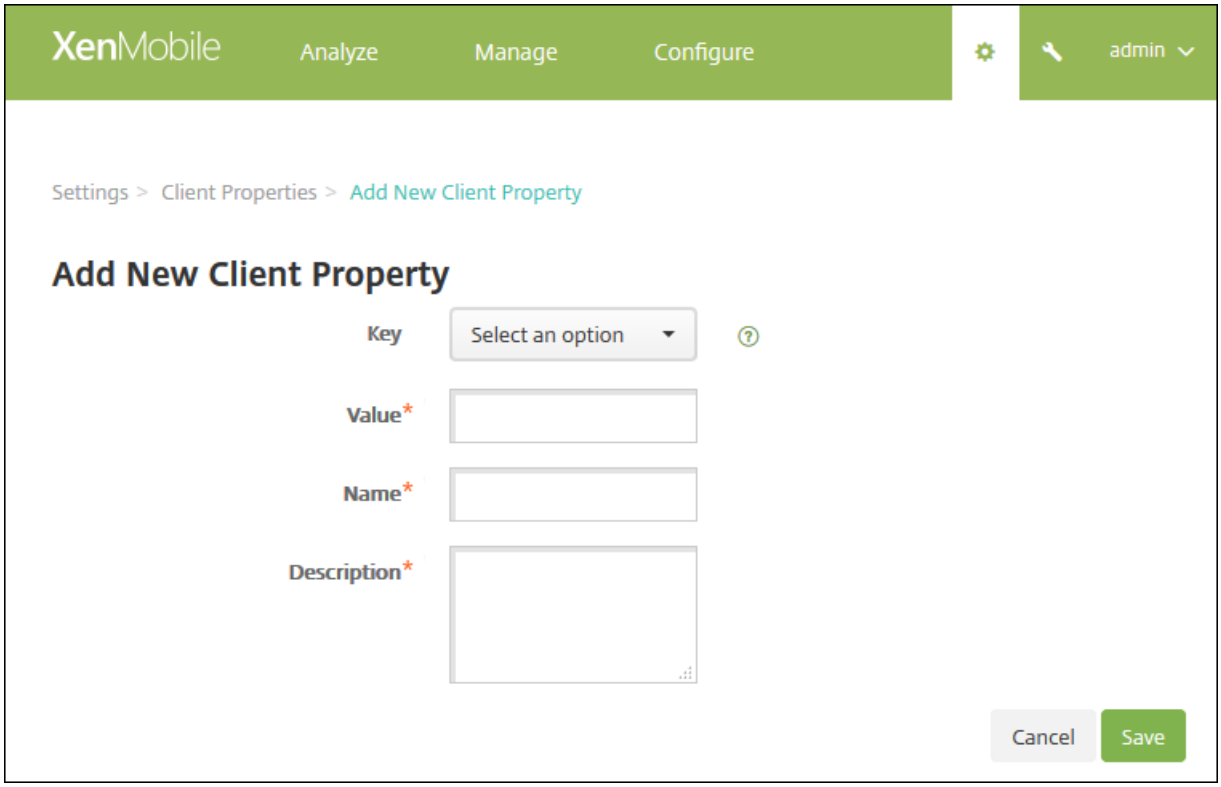
Las propiedades de cliente están sujetas a cambios en cada versión de las aplicaciones cliente, especialmente Secure Hub. Para obtener información más detallada acerca de las propiedades de cliente más comunes a configurar, consulte Referencia de propiedades de cliente más adelante en este artículo.

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 **Client**, haga clic en **Client Properties**. Aparecerá la página **Client Properties**. Puede agregar, modificar y eliminar las propiedades de cliente desde esta página.



Para agregar una propiedad de cliente

1. Haga clic en **Add**. Aparecerá la página **Add New Client Property**.



2. Configure estos parámetros:

- **Key**. En la lista, haga clic en la clave de propiedad que quiere agregar. **Importante**: Póngase en contacto con el servicio de asistencia de Citrix antes de realizar cambios o solicite una clave especial para realizar algún cambio.
- **Value**. Introduzca el valor de la propiedad seleccionada.
- **Name**. Introduzca un nombre para la propiedad.
- **Description**. Introduzca una descripción de la propiedad.

3. Haga clic en **Save**.

Para modificar una propiedad de cliente

1. En la tabla **Client Properties**, seleccione la propiedad de cliente que quiere modificar.

Nota: Si marca la casilla situada junto a una propiedad de cliente, el menú de opciones aparecerá encima de la lista de propiedades de cliente. En cambio, si hace clic en cualquier lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.

2. Haga clic en **Edit**. Aparecerá la página **Edit Client Property**.

3. Cambie la siguiente información como corresponda:

- **Key**. Este campo no puede cambiarse.
- **Value**. El valor de la propiedad.
- **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 cliente

1. En la tabla **Client Properties**, seleccione la propiedad de cliente que quiere eliminar.

> **Nota**: Puede eliminar más de una propiedad. Para ello, deberá marcar la casilla de verificación situada junto a cada propiedad.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Delete** .

Referencia de propiedades de cliente

A continuación, se indican las propiedades de cliente predefinidas en XenMobile, así como sus valores predeterminados.

CONTAINER_SELF_DESTRUCT_PERIOD

> Nombre simplificado: MDX Container Self Destruct Period
>
> La propiedad de autodestrucción "Self-Destruct" impide el acceso a Secure Hub y a aplicaciones administradas después de una cantidad determinada de días de inactividad. Una vez alcanzado el límite de tiempo, las aplicaciones ya no se podrán usar y el dispositivo de usuario quedará desinscrito del servidor XenMobile. El borrado de datos consiste en borrar los datos de todas las aplicaciones instaladas, incluidos los datos de usuario y la memoria caché de la aplicación. El periodo de inactividad se interpreta como el periodo durante el cual el servidor no recibe ninguna solicitud de autenticación para validar a un usuario. Por ejemplo, si indica 30 días en la directiva y el usuario no usa Secure Hub ni otras aplicaciones durante más de 30 días, entonces se aplica la directiva.
>
> Esta directiva de seguridad global se aplica a las plataformas iOS y Android, y es una mejora de las directivas existentes de borrado y bloqueo de aplicaciones.

Para configurar esta directiva global, vaya a **Settings > Client Properties**, y agregue la clave personalizada **CONTAINER_SELF_DESTRUCT_PERIOD**.

Valor: Cantidad de días

DEVICE_LOGS_TO_IT_HELP_DESK

Nombre simplificado: Send device logs to IT help desk

Esta propiedad habilita o inhabilita la capacidad de enviar registros al servicio de asistencia de TI.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

DISABLE_LOGGING

Nombre simplificado: Disable Logging

Esta propiedad permite inhabilitar la capacidad de los usuarios para recopilar y cargar registros desde sus dispositivos. Se inhabilita la captura de registro para Secure Hub y para todas las aplicaciones MDX instaladas. Los usuarios no pueden enviar registros de ninguna aplicación desde la página de asistencia; aunque aparezca el cuadro de diálogo para redactar correos, los registros no se adjuntan y se muestra un mensaje que indica que el registro está inhabilitado. Además de las consecuencias en los dispositivos de los usuarios, en la consola de XenMobile no puede modificar los parámetros de registro para Secure Hub ni las aplicaciones MDX.

Cuando esta propiedad se establece en **true**, Secure Hub establece en **true** la opción **Block application logs**, con lo que las aplicaciones MDX dejan de registrar eventos cuando se aplica la nueva directiva.

Valores posibles: **true** o **false**

Valor predeterminado: **false** (la captura de registros no está inhabilitada)

ENABLE_CRASH_REPORTING

Nombre simplificado: Enable Crash Reporting

Esta propiedad habilita o inhabilita los informes de errores que utilizan Crashlytics para aplicaciones XenMobile.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

ENABLE_CREDENTIAL_STORE

Nombre simplificado: Enable Credential Store

Habilitar el almacén de credenciales significa que los usuarios de iOS o Android introducen su contraseña una vez al acceder a las aplicaciones XenMobile. Puede utilizar el almacén de credenciales independientemente de si habilita el PIN de Citrix. Si no habilita el PIN de Citrix, los usuarios deberán introducir su contraseña de Active Directory. XenMobile admite contraseñas de Active Directory con el almacén de credenciales solo para Secure Hub y las aplicaciones de tienda pública. XenMobile no admite la autenticación de la infraestructura de clave pública si se utilizan contraseñas de Active Directory con el almacén de credenciales.

La inscripción automática en Secure Mail requiere que esta propiedad se establezca en **true**.

Para configurar esta directiva de cliente global, vaya a **Settings > Client Properties** y agregue la clave personalizada **ENABLE_CREDENTIAL_STORE** y defina el valor **True** en **Value**.

ENABLE_FIPS_MODE

Nombre simplificado: Enable FIPS Mode

Esta propiedad habilita o inhabilita el modo FIPS en los dispositivos móviles. Después de cambiar el valor, Secure Hub transferirá el nuevo valor al dispositivo la próxima vez que se autentique en línea.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

Display name: ENABLE_NETWORK_EXTENSION

Display name: ENABLE_NETWORK_EXTENSION

De forma predeterminada, XenMobile habilita el marco de extensiones de red de Apple cuando se instala Secure Hub. Para inhabilitar la extensión de red, vaya a **Settings > Client Properties**, agregue la clave personalizada **ENABLE_NETWORK_EXTENSION** y establezca **Value** en **false**.

Valor predeterminado: **true**

ENABLE_PASSCODE_AUTH

Nombre simplificado: Enable Citrix PIN Authentication

Esta propiedad permite activar la función de PIN de Citrix. Si se activa la función de PIN o código de acceso de Citrix, se solicita a los usuarios que definan un número PIN que se usará en lugar de su contraseña de Active Directory. Este parámetro se habilita automáticamente si la propiedad ENABLE_PASSWORD_CACHING está habilitada o si XenMobile usa la autenticación de certificados.

Si los usuarios se autentican sin conexión, el PIN de Citrix se valida localmente y se permite a los usuarios acceder a la aplicación o al contenido solicitado. Si los usuarios se autentican con conexión, se utiliza el PIN o el código de acceso de Citrix para desbloquear el certificado o la contraseña de Active Directory, enviados a continuación para realizar la autenticación en XenMobile.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

ENABLE_PASSWORD_CACHING

Nombre simplificado: Enable User Password Caching

Esta propiedad permite que la contraseña de Active Directory de los usuarios se almacene en la memoria caché local del dispositivo móvil. Cuando establezca esta propiedad en **true**, también deberá establecer la propiedad ENABLE_PASSCODE_AUTH en **true**. Si se habilita el almacenamiento en caché de las contraseñas de usuario, XenMobile pide a los usuarios que definan un código de acceso o un PIN de Citrix.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

ENABLE_TOUCH_ID_AUTH

Nombre simplificado: Enable Touch ID Authentication

Para los dispositivos que admiten la autenticación Touch ID, esta propiedad habilita o inhabilita la autenticación Touch ID en el dispositivo. Requisitos:

Los dispositivos de usuario deben tener el PIN de Citrix o LDAP habilitado. Si la autenticación de LDAP está desactivada (por ejemplo, debido a que solo se usa la autenticación basada en certificados), los usuarios deben establecer un PIN de Citrix. En este caso, XenMobile pide el PIN de Citrix aunque la propiedad de cliente **ENABLE_PASSCODE_AUTH** sea **false**.

Establezca **ENABLE_PASSCODE_AUTH** en **false** de modo que, cuando los usuarios inicien una aplicación, deban responder a una solicitud de usar Touch ID.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

ENABLE_WORXHOME_CEIP

Nombre simplificado: Enable Worx Home CEIP

Esta propiedad activa el programa CEIP de mejora de la experiencia del cliente. Enviará datos anónimos de uso y configuración a Citrix periódicamente. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de XenMobile.

Valor: **true** o **false**

Valor predeterminado: **false**

ENABLE_WORXHOME_GA

Nombre simplificado: Enable Google Analytics in Worx Home

Esta propiedad habilita o inhabilita la capacidad de recopilar datos mediante Google Analytics en Worx Home. Si cambia este parámetro, el nuevo valor se establece solamente cuando el usuario inicia sesión en Secure Hub (Worx Home).

Valores posibles: **true** o **false**

Valor predeterminado: **true**

ENCRYPT_SECRETS_USING_PASSCODE

Nombre simplificado: Encrypt secrets using Passcode

Esta propiedad permite que los datos confidenciales se almacenen en el dispositivo móvil, en un almacén secreto, en lugar de guardarse en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta propiedad permite un cifrado seguro de los objetos clave, pero también agrega entropía de usuario (un código PIN aleatorio generado por el

usuario y que solo el usuario conoce).

Citrix recomienda habilitar esta propiedad para facilitar una mayor seguridad en los dispositivos de usuario. En consecuencia, los usuarios verán más solicitudes de autenticación para el PIN de Citrix.

Valores posibles: **true** o **false**

Valor predeterminado: **false**

INACTIVITY_TIMER

Nombre simplificado: Inactivity Timer

Esta propiedad define el tiempo en minutos que los usuarios pueden dejar su dispositivo inactivo y luego acceder a una aplicación sin que se solicite un PIN o un código de acceso de Citrix. Si quiere habilitar este parámetro para una aplicación MDX, debe establecer el parámetro App Passcode en On. Si el parámetro App Passcode está desactivado, se redirige a los usuarios a Secure Hub para una autenticación completa. Al cambiar este parámetro, el valor se aplicará la próxima vez que los usuarios deban autenticarse.

Nota: En iOS, el temporizador de inactividad también controla el acceso a Secure Hub, para aplicaciones MDX y aplicaciones que no son MDX.

Valores posibles: Cualquier número entero positivo

Valor predeterminado: **15**

ON_FAILURE_USE_EMAIL

Nombre simplificado: On failure Use Email to Send device logs to IT help desk

Esta propiedad habilita o inhabilita la capacidad de utilizar el correo electrónico para enviar registros del dispositivo al departamento de TI.

Valores posibles: **true** o **false**

Valor predeterminado: **true**

PASSCODE_EXPIRY

Nombre simplificado: PIN Change Requirement

Esta clave define el tiempo en días durante los que el PIN o código de acceso de Citrix es válido. Una vez transcurrido ese período, se obliga al usuario a cambiar su PIN o código de acceso de Citrix. Si cambia este parámetro, el nuevo valor se establece solamente cuando el PIN o el código de acceso de Citrix actuales caducan.

Valores posibles: Se recomienda un valor entre **1** y **99** Si quiere que los usuarios no tengan que restablecer nunca su PIN, defina un valor muy alto (por ejemplo 100.000.000.000). Si al principio se define un periodo de caducidad de entre 1 y 99 días y luego se cambia por uno mayor durante ese periodo, los PIN caducarán al final del periodo definido originalmente, pero ya no caducarán nunca más después de eso.

Valor predeterminado: **90**

PASSCODE_HISTORY

Nombre simplificado: PIN History

Esta propiedad define la cantidad de números PIN o códigos de acceso de Citrix usados anteriormente que los usuarios no pueden volver a utilizar cuando cambien sus números PIN o códigos de acceso de Citrix. Si cambia esta opción de configuración, el nuevo valor se establece la próxima vez que el usuario restablezca su PIN o código de acceso a Citrix.

Valores posibles: **1** - **99**

Valor predeterminado: **5**

PASSCODE_MAX_ATTEMPTS

Nombre simplificado: PIN Attempts

Esta propiedad define cuántos números PIN o códigos de acceso de Citrix incorrectos pueden introducir los usuarios antes de que se les solicite una autenticación completa. Después de que los usuarios realicen correctamente una autenticación completa, se les solicita crear un nuevo PIN o código de acceso de Citrix.

Valores posibles: Cualquier número entero positivo

Valor predeterminado: **15**

PASSCODE_MIN_LENGTH

Nombre simplificado: PIN Length Requirement

Esta propiedad define la seguridad del PIN o código de acceso de Citrix.

Valores posibles: **1** - **99**

Valor predeterminado: **6**

PASSCODE_STRENGTH

Nombre simplificado: PIN Strength Requirement

Esta propiedad define la seguridad del PIN o código de acceso de Citrix. Si cambia este parámetro, se solicitará a los usuarios que establezcan un nuevo PIN o código de acceso de Citrix la próxima vez que deban autenticarse.

Valores posibles: **Low**, **Medium** o **Strong**

Valor predeterminado: **Medium**

En la siguiente tabla se describen las reglas de contraseña para cada parámetro de nivel de seguridad, basado en el parámetro PASSCODE_TYPE:

Seguridad del código de acceso	**Reglas para un código de acceso de tipo numérico**	**Reglas para un código de acceso de tipo alfanumérico**
Baja	Se permiten todos los números y todas las secuencias	Debe contener al menos una letra y un número. No permitido: AAAaaa, aaaaaa, abcdef

		Permitido: aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Nivel medio de seguridad (valor predeterminado)	1. Los números no pueden ser todos iguales. Por ejemplo, no se permite 444444. 2. Los números no pueden ser todos consecutivos. Por ejemplo, no se permite 123456 o 654321. Permitido: 444333, 124567, 136790, 555556, 788888	Además de las reglas para el nivel bajo de seguridad del código de acceso: 1. Las letras y los números no pueden ser iguales. Por ejemplo, no se permiten aaaa11, aa11aa o aaa111. 2. Ni letras ni números pueden ser consecutivos. Por ejemplo, no se permiten abcd12, bcd123, 123abc, xy1234, xyz345, o cba123. Permitido: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Alta	Lo mismo que para el nivel medio del PIN o código de acceso de Citrix.	El código de acceso debe incluir al menos una letra mayúscula y una letra minúscula. No permitido: abcd12, DFGH2 Permitido: Abcd12, jkrtA2, 23Bc#, AbCd
Nivel de seguridad alto	Lo mismo que para el nivel medio del PIN o código de acceso de Citrix.	El código de acceso debe incluir al menos un número, un símbolo especial, una letra mayúscula y una letra minúscula. No permitido: abcd12, Abcd12, dfgh12, jkrtA2 Permitido: Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

PASSCODE_TYPE

Nombre simplificado: PIN Type

Esta propiedad indica si el usuario puede definir un PIN numérico o un código de acceso alfanumérico de Citrix. Si selecciona **Numeric**, el usuario solo podrá definir un valor numérico para el PIN de Citrix. Si selecciona **Alphanumeric**, el usuario podrá utilizar una combinación de letras y números para el código de acceso.

Nota: Si cambia este parámetro, se solicitará a los usuarios que establezcan un nuevo PIN o código de acceso de Citrix la próxima vez que deban autenticarse.

Valores posibles: **Numeric** o **Alphanumeric**

Valor predeterminado: **Numeric**

REFRESHINTERVAL

Nombre simplificado: REFRESHINTERVAL

De forma predeterminada, XenMobile hace ping al servidor de detección automática (ADS) para buscar certificados anclados cada 3 días. Para cambiar el intervalo de actualización, vaya a **Settings > Client Properties**, agregue la clave personalizada **REFRESHINTERVAL** y establezca **Value** en la cantidad de horas.

Valor predeterminado: **72** horas (3 días)

SEND_LDAP_ATTRIBUTES

Para implementaciones de solo MAM, puede configurar XenMobile para que los usuarios con dispositivos iOS o Android que se inscriban en Secure Hub con las credenciales de correo electrónico queden automáticamente inscritos en Secure Mail. Lo que significa que los usuarios no tienen que introducir información adicional ni realizar pasos adicionales para inscribirse en Secure Mail.

Para configurar esta directiva de cliente global, vaya a **Settings > Client Properties** y agregue la clave personalizada **SEND_LDAP_ATTRIBUTES** y defina el valor en **Value** de este modo:

Value: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}

Los valores de atributo se especifican como macros, de forma similar a las directivas MDM.

Este es un ejemplo de respuesta de la cuenta de servicio para esta propiedad:

Nota: En esta propiedad, XenMobile interpreta las comas como terminadores de cadenas. Si un valor de atributo contiene una coma, esta debe estar precedida de una barra diagonal invertida para que el cliente no interprete la coma incluida como el final de un valor de atributo. Los caracteres de barra diagonal invertida se representan así: "\\".

ActiveSync Gateway

Feb 27, 2017

ActiveSync es un protocolo de sincronización de datos móviles desarrollado por Microsoft. ActiveSync sincroniza datos entre dispositivos móviles y equipos de escritorio (o portátiles).

Puede configurar reglas de ActiveSync Gateway en XenMobile. En función de estas reglas, se puede permitir o denegar el acceso de los dispositivos a datos ActiveSync. Por ejemplo, si activa la regla Missing Required Apps, XenMobile comprueba la directiva App Access para ver cuáles son las aplicaciones requeridas y deniega acceso a los datos de ActiveSync si faltan esas aplicaciones. Puede elegir si permitir (**Allow**) o denegar (**Deny**) cada regla. El valor predeterminado es **Allow**.

Para obtener más información acerca de la directiva de dispositivo App Access, consulte Directivas de dispositivo para el acceso a aplicaciones.

XenMobile admite las siguientes reglas:

Anonymous Devices. Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Failed Samsung KNOX attestation. Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung KNOX.

Forbidden Apps. Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva App Access.

Implicit Allow and Deny. Esta acción es la predeterminada de ActiveSync Gateway. La puerta de enlace crea una lista de todos los dispositivos que no cumplen ninguno de los demás criterios de regla o filtro, y permite o deniega conexiones en función de esa lista. Si no coincide ninguna regla, el valor predeterminado es permitir implícitamente (Implicit Allow).

Inactive Devices. Comprueba si un dispositivo está inactivo según se define en el parámetro Device Inactivity Days Threshold en Server Properties.

Missing Required Apps. Comprueba si en un dispositivo faltan aplicaciones requeridas, según se definen en la directiva App Access.

Non-suggested Apps. Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva App Access.

Noncompliant Password. Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, XenMobile puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva de códigos de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva de códigos de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Out of Compliance Devices. Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo Out of Compliance. Esa propiedad es modificada normalmente por las acciones automatizadas o por las API de XenMobile de terceros.

Revoked Status. Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Rooted Android and Jailbroken iOS Devices. Comprueba si un dispositivo iOS o Android está liberado por jailbreak.

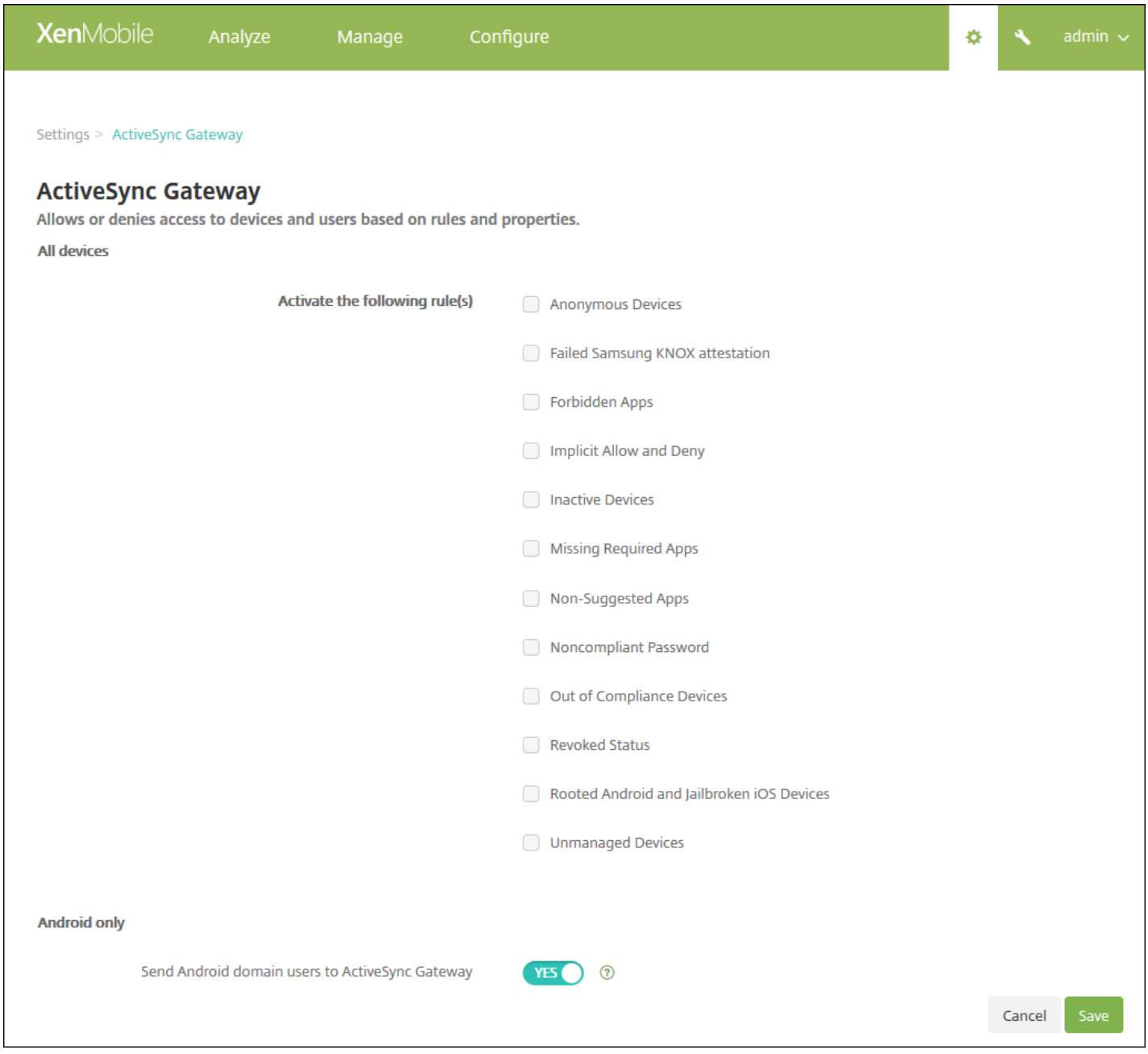
Unmanaged Devices. Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por ejemplo, un dispositivo que se ejecute en modo MAM o que se haya desinscrito no es un dispositivo administrado.

Send Android domain users to ActiveSync Gateway. Haga clic en **YES** para que XenMobile envíe la información de los dispositivos Android a ActiveSync Gateway.

Para configurar los parámetros de ActiveSync Gateway

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

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



3. En **Activate the following rules**, seleccione las reglas que quiera activar.

4. En **Android-only**, en **Send Android domain users to ActiveSync Gateway**, haga clic en **YES** para que XenMobile envíe la información de los dispositivos Android a ActiveSync Gateway.

5. Haga clic en **Save**.

Control de acceso de red

Feb 27, 2017

Si tiene un dispositivo de control de acceso a la red (Network Access Control, NAC) configurado en la red, como Cisco ISE, en XenMobile puede habilitar filtros para configurar dispositivos como conformes o no conformes a NAC, en función de reglas o propiedades. En XenMobile, si un dispositivo administrado no cumple los criterios especificados y se marca como No conforme por eso, el dispositivo de NAC bloqueará ese dispositivo en la red.

En la consola de XenMobile, seleccione los criterios de la lista para establecer un dispositivo como no conforme.

XenMobile da respaldo a los siguientes filtros de conformidad para NAC:

Anonymous Devices. Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Failed Samsung KNOX attestation. Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung KNOX.

Forbidden Apps. Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva App Access. Para obtener más información acerca de la directiva de acceso a aplicaciones (App Access), consulte Directiva de dispositivo para el acceso a aplicaciones.

Inactive Devices. Comprueba si un dispositivo está inactivo según se define en el parámetro Device Inactivity Days Threshold en Server Properties. Para obtener más información, consulte las propiedades del servidor.

Missing Required Apps. Comprueba si en un dispositivo faltan aplicaciones requeridas, según se definen en la directiva de acceso a aplicaciones App Access.

Non-suggested Apps. Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva App Access.

Noncompliant Password. Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, XenMobile puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva de códigos de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva de códigos de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Out of Compliance Devices. Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo Out of Compliance. Esa propiedad se ve modificada normalmente por acciones automatizadas o por el uso que un tercero hace de las API de XenMobile.

Revoked Status. Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Rooted Android and Jailbroken iOS Devices. Comprueba si un dispositivo iOS o Android está liberado por jailbreak.

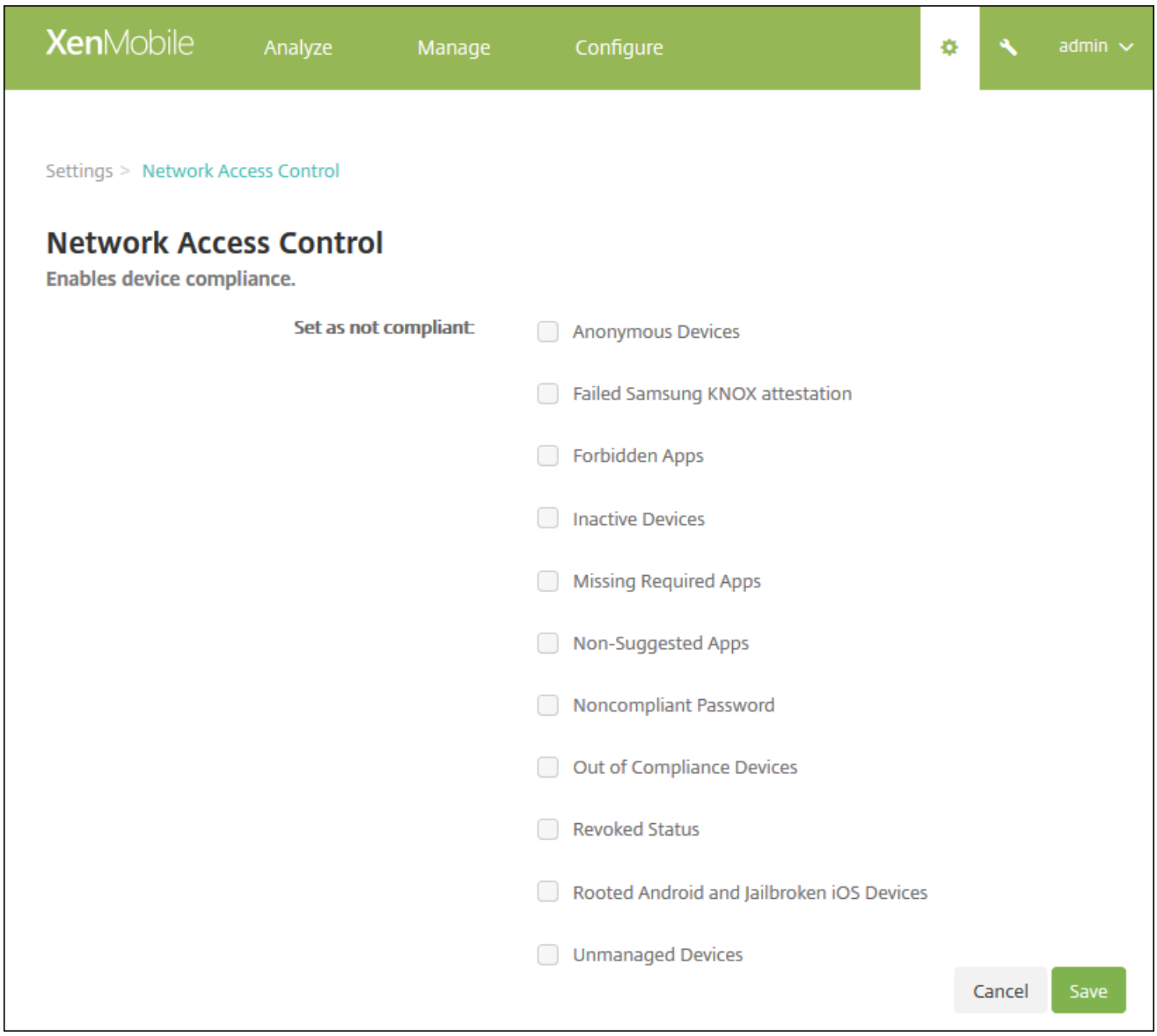
Unmanaged Devices. Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por ejemplo, un dispositivo que se ejecute en modo MAM o que se haya desinscrito no es un dispositivo administrado.

> **Nota**
>
> El filtro de dispositivos que cumplen los requisitos de forma implícita o que no los cumplen establece el valor predeterminado solo en los dispositivos que administra XenMobile. Por ejemplo, los dispositivos que tienen instalada una aplicación prohibida o que no están inscritos se marcan como no conformes y el dispositivo de NAC bloqueará su acceso a la red.

Configuración del control de acceso a la red

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 **Network Access Control**. Aparecerá la página **Network Access Control**.



3. Marque las casillas de verificación de los filtros de **Set as not compliant** que quiera habilitar.

4. Haga clic en **Save**.

Samsung KNOX

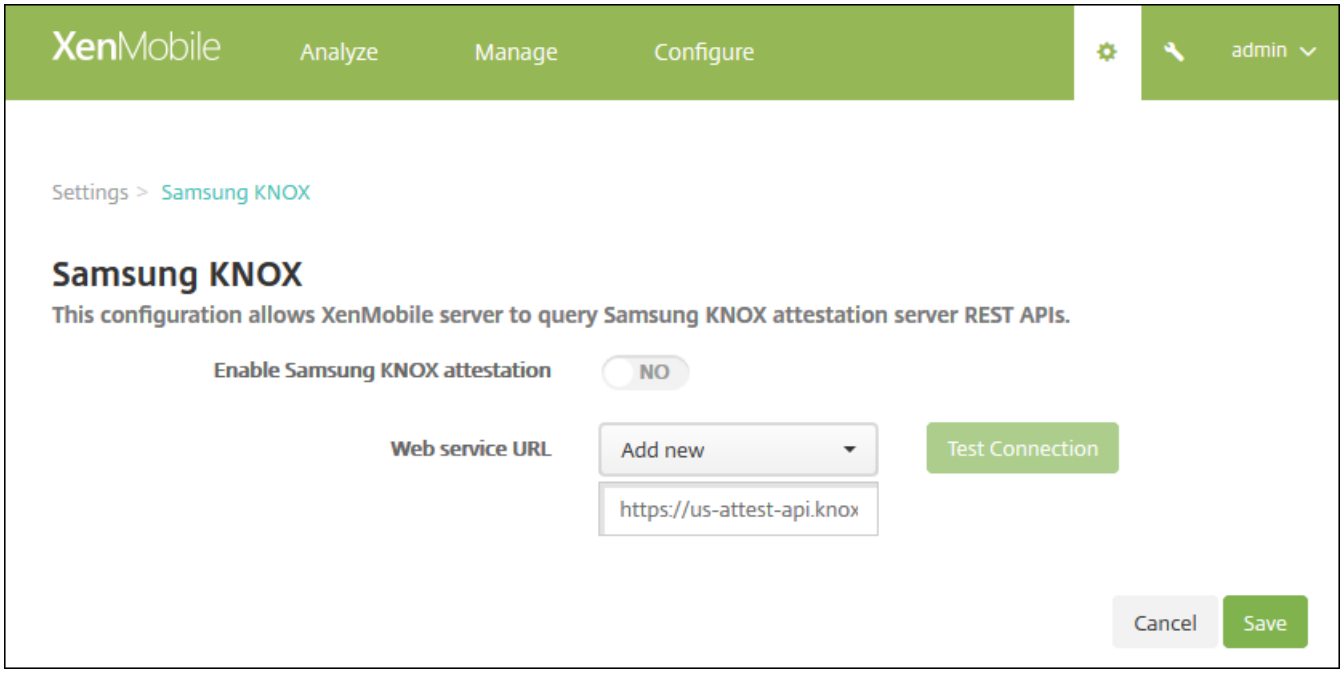
Feb 27, 2017

Puede configurar XenMobile para consultar las API de REST del servidor de atestación de Samsung KNOX.

Samsung KNOX aprovecha las funcionalidades de seguridad de hardware y ofrece varios niveles de protección para el sistema operativo y las aplicaciones. Un nivel de esta seguridad se encuentra en la plataforma mediante la atestación. Un servidor de atestación ofrece la comprobación del software del sistema principal del dispositivo móvil (por ejemplo, los cargadores de arranque y el kernel). La verificación se produce en el tiempo de ejecución en función de los datos recopilados durante el arranque seguro.

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. En **Platforms**, haga clic en **Samsung KNOX**. Aparecerá la página **Samsung KNOX**.



3. En **Enable Samsung KNOX attestation**, seleccione si habilitar la atestación de Samsung KNOX. El valor predeterminado es **NO**.

4. Cuando se configura **Enable Samsung KNOX attestation** con el valor **YES**, se habilita la opción **Web service URL**. A continuación, en la lista, realice una de las siguientes acciones:

   a. Haga clic en el servidor de atestación adecuado.

   b. Haga clic en **Add new** e introduzca la dirección URL del servicio Web.

5. Haga clic en **Test Connection** para comprobar la conexión. Aparecerá un mensaje indicando si la conexión tuvo lugar, o si, por el contrario, hubo algún error.

6. Haga clic en **Save**.

Nota

Puede usar Samsung KNOX Mobile Enrollment para inscribir múltiples dispositivos Samsung KNOX en XenMobile (o en cualquier administrador de dispositivos móviles) sin necesidad de configurar manualmente cada uno de los dispositivos. Para obtener más información, consulte Inscripción en masa de Samsung KNOX.

Firebase Cloud Messaging

Feb 28, 2017

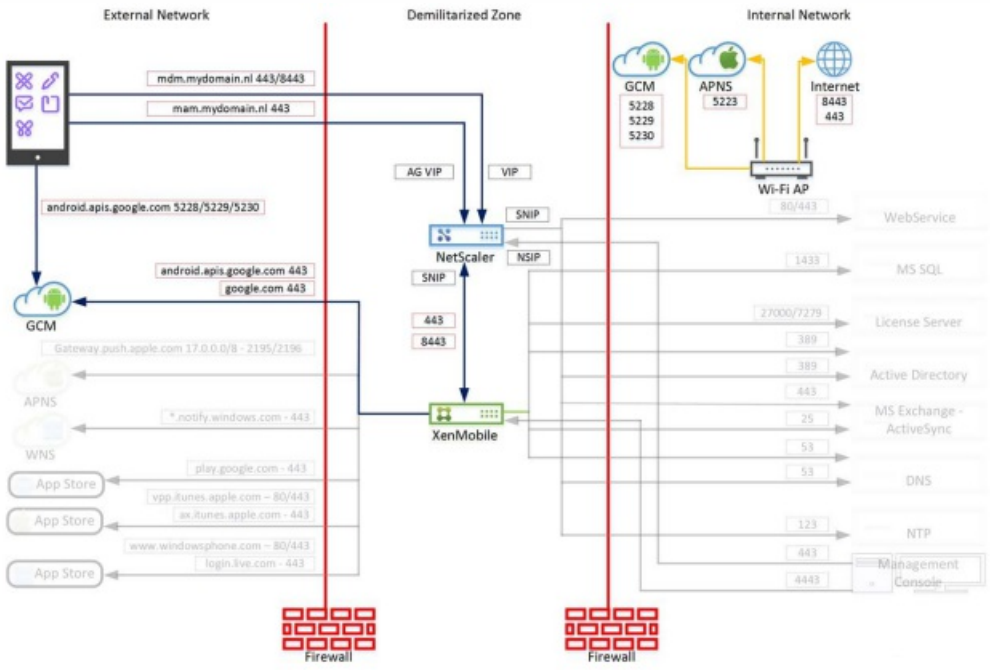
Como alternativa a la directiva **Active poll period**, puede usar Firebase Cloud Messaging (GCM) para controlar cómo y cuándo se conectan los dispositivos Android a XenMobile. Con la siguiente configuración, toda acción de seguridad o comando de implementación desencadena una notificación push que pedirá al usuario que se reconecte al servidor XenMobile.

Requisitos previos

- XenMobile 10.3.x
- Cliente más reciente de Secure Hub
- 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 FCM (o GCM) en la red interna y externa.

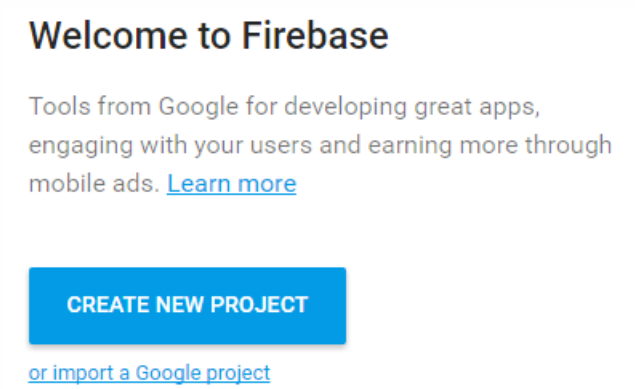


Para configurar su cuenta de Google para GCM

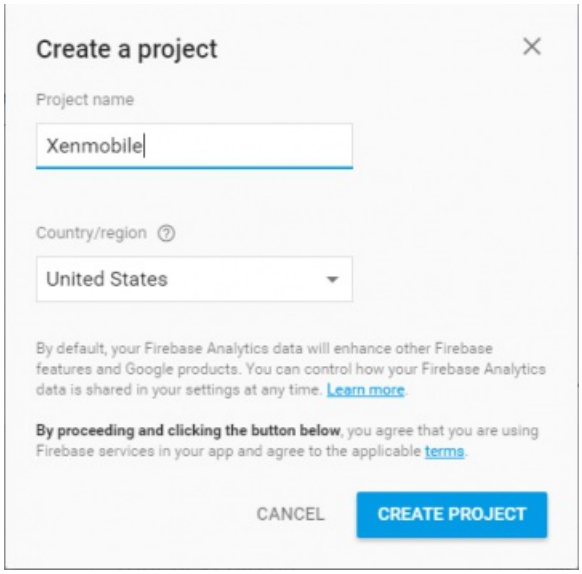
1. Inicie sesión en la siguiente URL con las credenciales de la cuenta de Google para desarrolladores:

   https://console.firebase.google.com/?pli=1

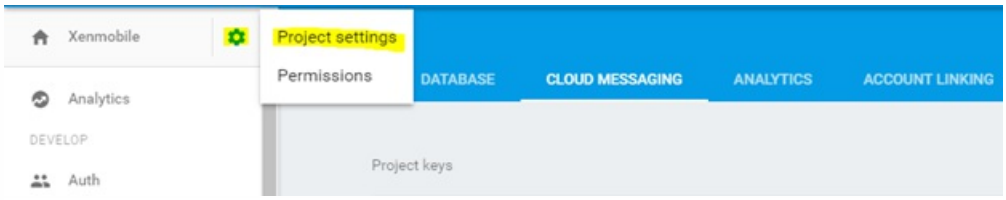
2. Haga clic en **Create a project**.



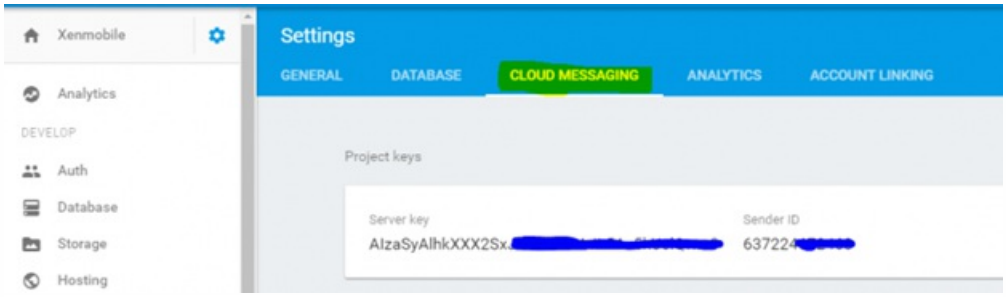
3. Escriba un nombre de proyecto en **Project name** y haga clic en **Create**.



4. Haga clic en el icono de engranaje situado junto al nombre del proyecto, en la esquina superior izquierda, y haga clic en **Project Settings**.



5. Seleccione la ficha **Cloud Messaging**. Puede buscar el ID del remitente y la clave del servidor en esta página. Copie estos valores porque deberá proporcionarlos en el servidor XenMobile. Es importante tener en cuenta que las claves de servidor creadas después de septiembre de 2016 deben crearse en la consola de Firebase.

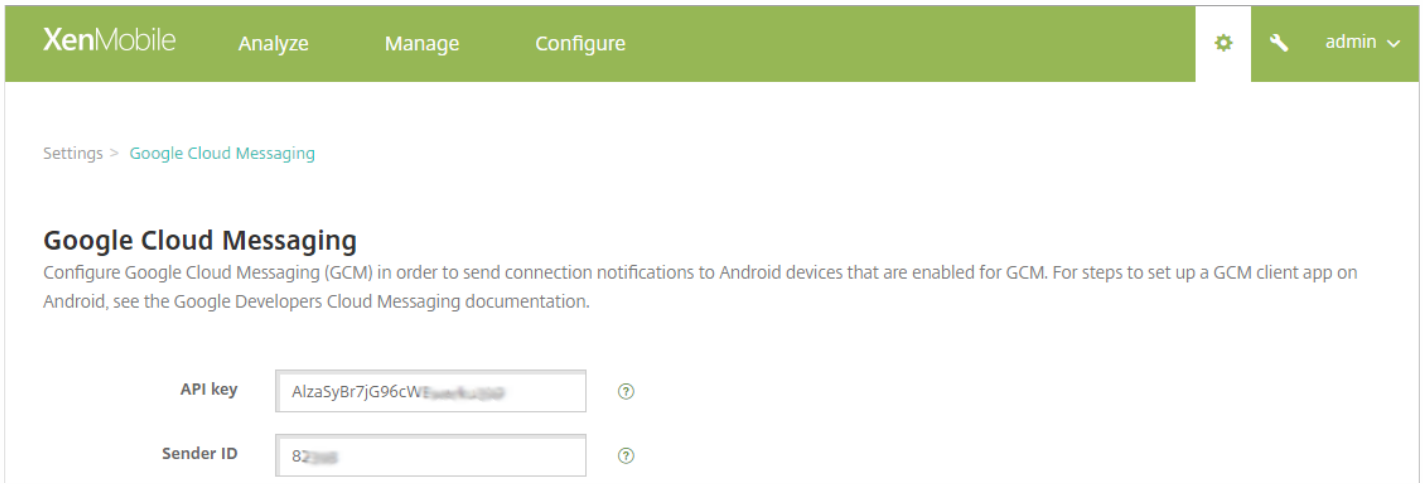


Para configurar XenMobile para GCM

1. Inicie sesión en la consola de XenMobile y vaya a **Settings > Server Properties**. En la barra de búsqueda, escriba **GCM** y haga clic en Buscar.

    a. Modifique la **clave API de GCM** y escriba la clave de API de Firebase Cloud Messaging que copió en el último paso de la configuración de Firebase Cloud Messaging.

    b. Modifique **Sender ID** de **GCM** copiando el ID de envío que anotó en el procedimiento anterior.



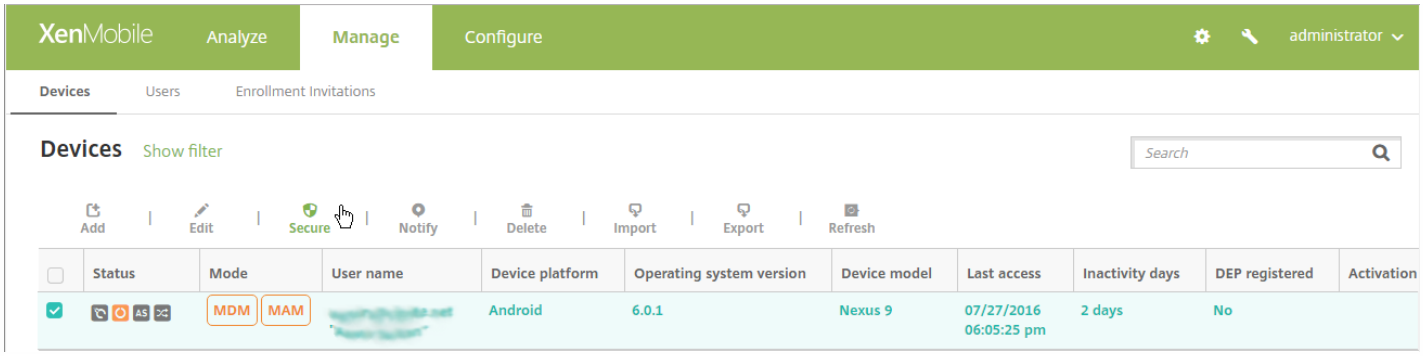
Para probar la configuración

Como requisito previo para probar la configuración de FCM, no debe tener configurada la directiva **Scheduling** (Programación). De forma alternativa, no establezca esa directiva en **Always Connect**. Para obtener más información sobre cómo configurar la directiva **Scheduling**, consulte Directiva de dispositivo para la programación.

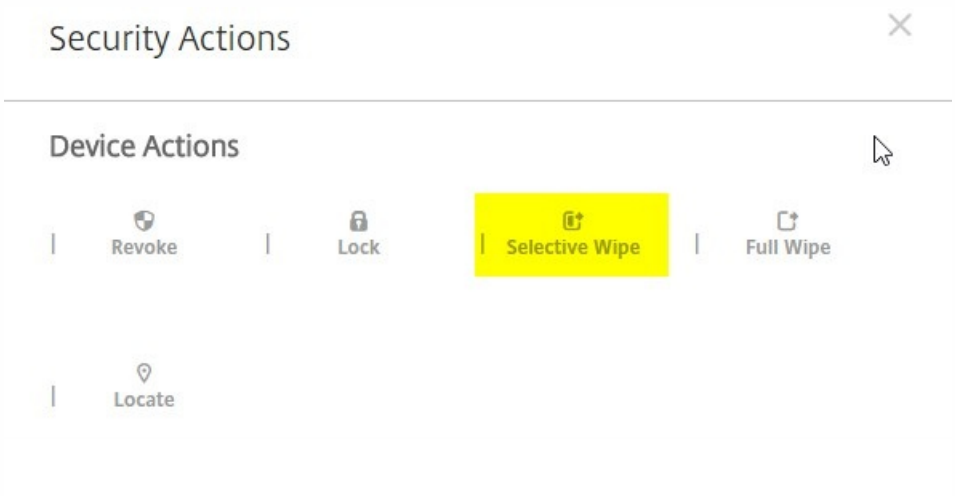
1. Inscriba un dispositivo Android.

2. Deje el dispositivo inactivo durante algún tiempo, de forma que se desconecte del servidor XenMobile.

3. Inicie sesión en la consola de 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.

Credenciales de Google Play

Feb 27, 2017

XenMobile utiliza las credenciales de Google Play para extraer información de las aplicaciones de un dispositivo.

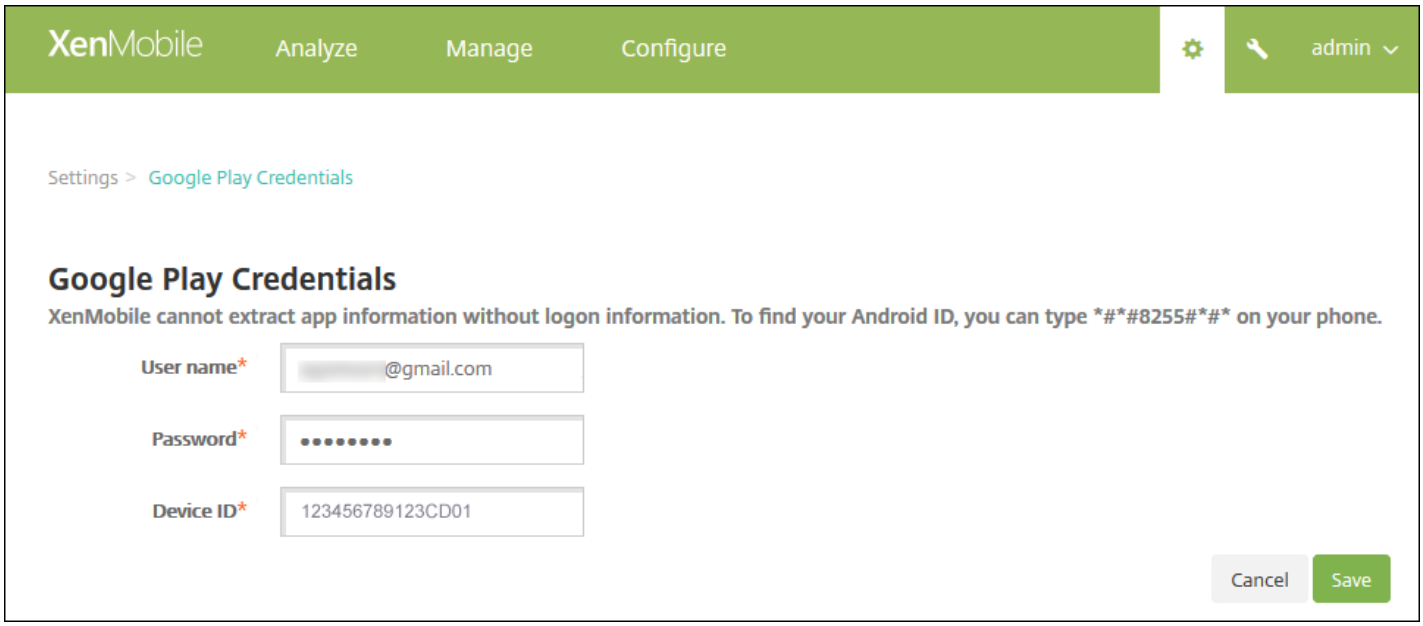
Para buscar el ID de Android, escriba *#*#8255#*#* en el teléfono. Si el código no revela el ID de dispositivo en su tipo de dispositivo, es posible usar una aplicación de terceros para conseguir el ID. El ID necesario es el ID de Google Services Framework con la etiqueta GSF ID.

> ## Nota
>
> Al buscar aplicaciones de Google Play Store desde la consola de XenMobile, la búsqueda mostrará aplicaciones basadas en el sistema operativo Android del dispositivo. Por ejemplo, Samsung S6 Edge está ejecutando la versión 6.0.1 de sistema operativo. Cuando busque aplicaciones, las únicas que aparecerán en el resultado de la búsqueda serán aplicaciones que son compatibles con la versión 6.0.1 de Android.

> ## Important
>
> Si quiere que XenMobile pueda extraer información de las aplicaciones, deberá configurar su cuenta de Gmail para permitir conexiones no seguras. Para saber los pasos a seguir, consulte el sitio Web de asistencia 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. En **Platforms**, haga clic en **Google Play Credentials**. Aparecerá la página Google Play Credentials.



3. Configure estos parámetros:

- **User name**. Escriba el nombre asociado a la cuenta de Google Play.
- **Password**. Escriba la contraseña de usuario.
- **Device ID**. Escriba su ID de Android.
  Consulte la nota anterior en este artículo para ver los pasos para obtener el ID de Android.

3. Haga clic en **Save**.

Directivas de dispositivos

Jul 13, 2017

Puede configurar la interacción entre XenMobile y los dispositivos mediante 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 plataformas e incluso entre dispositivos Android de diferentes fabricantes.

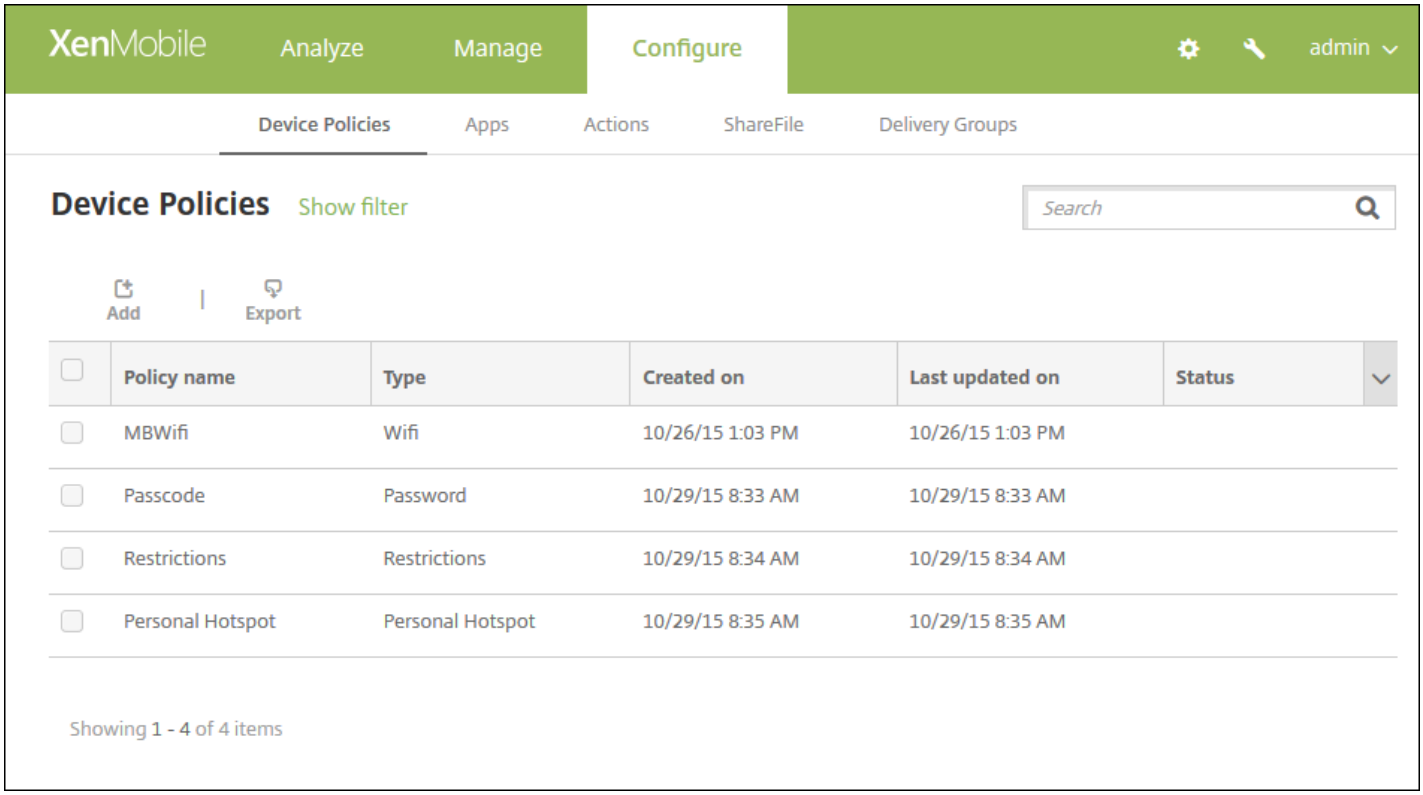
Para ver una tabla de directivas clasificadas por plataforma, descargue Device Policies by Platform Matrix en formato PDF. Para una descripción resumida de cada directiva de dispositivos, consulte Directivas de dispositivos en este artículo.

> ## Important
>
> Antes de crear una directiva, debe completar estos requisitos:
>
> - 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 la directiva para 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).

Para crear y administrar directivas de dispositivos, vaya a **Configure > Device Policies**.



Cómo agregar una directiva de dispositivo

1. En la página **Device Policies**, haga clic en **Add**.

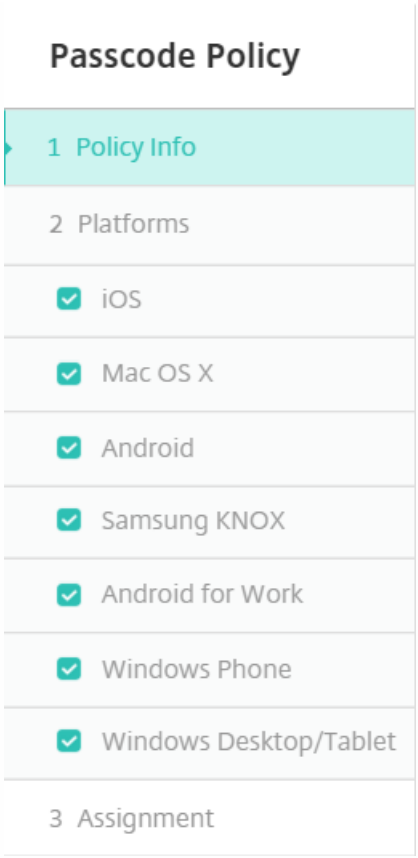
Aparecerá el cuadro de diálogo **Add a New Policy**. Expanda **More** para ver más directivas.

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 cuadro de búsqueda. Cuando escriba, aparecerán posibles coincidencias. Si la directiva está en la lista, haga clic en ella. Solo permanecerá en los resultados la directiva que seleccione. Haga clic en la directiva para abrir la página **Policy Information** referente a ella.
  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 cada plataforma que haya seleccionado en el paso 3. Estas páginas son distintas para cada directiva. Una directiva puede ser diferente en función de las plataformas. No todas las directivas se aplican a todas las plataformas.

Para configurar las reglas de implementación:

Nota: Para obtener más información sobre cómo configurar reglas de implementación, consulte Implementación de recursos.

a. Expanda **Deployment Rules** y, a continuación, configure los siguientes parámetros. La ficha **Base** aparece de forma predeterminada.

- En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es **All**.
- Haga clic en **New Rule** para definir las condiciones.
- En las listas, haga clic en las condiciones (por ejemplo, **Device ownership** y **BYOD**).
- Si quiere agregar más condiciones, haga clic en **New Rule** de nuevo. Puede agregar cuantas condiciones quiera.

b. Haga clic en la ficha **Advanced** para combinar las reglas con opciones booleanas. Las condiciones que haya elegido aparecerán en la ficha **Base**.

c. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.

- Haga clic en **AND**, **OR** o **NOT**.
- En la lista, seleccione las condiciones que quiere agregar a la regla. A continuación, haga clic en el signo más (**+**) situado en el lado derecho para agregar la condición a la regla.

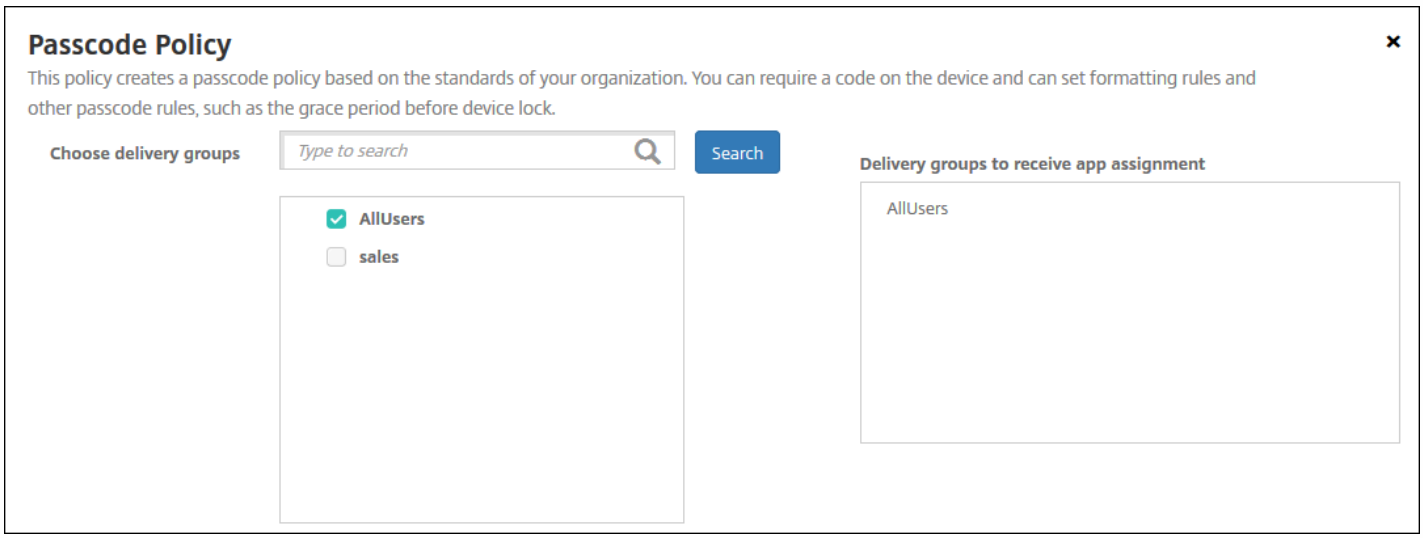
En cualquier momento, puede seleccionar una condición para modificarla o eliminarla si hace clic en **EDIT** o en **Delete** respectivamente.

- Haga clic en **New Rule** para agregar otra condición.

6. 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 **Assignments**.

7. En la página **Assignments**, 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.



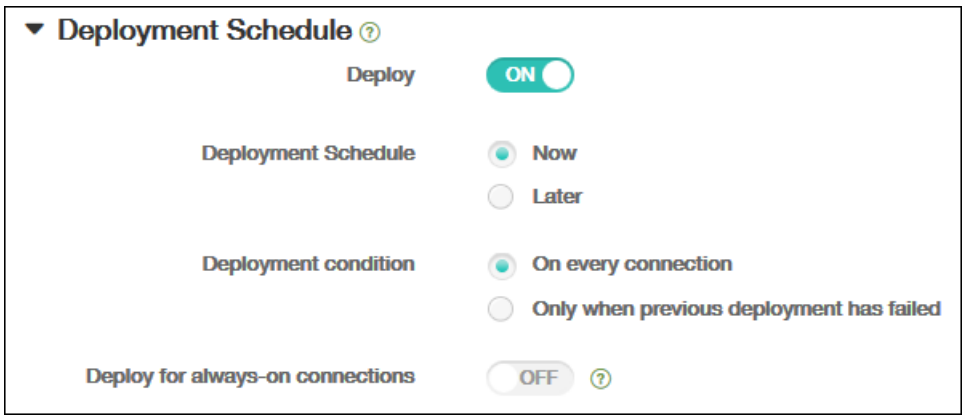
8. En la página **Assignments**, expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**.
- 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

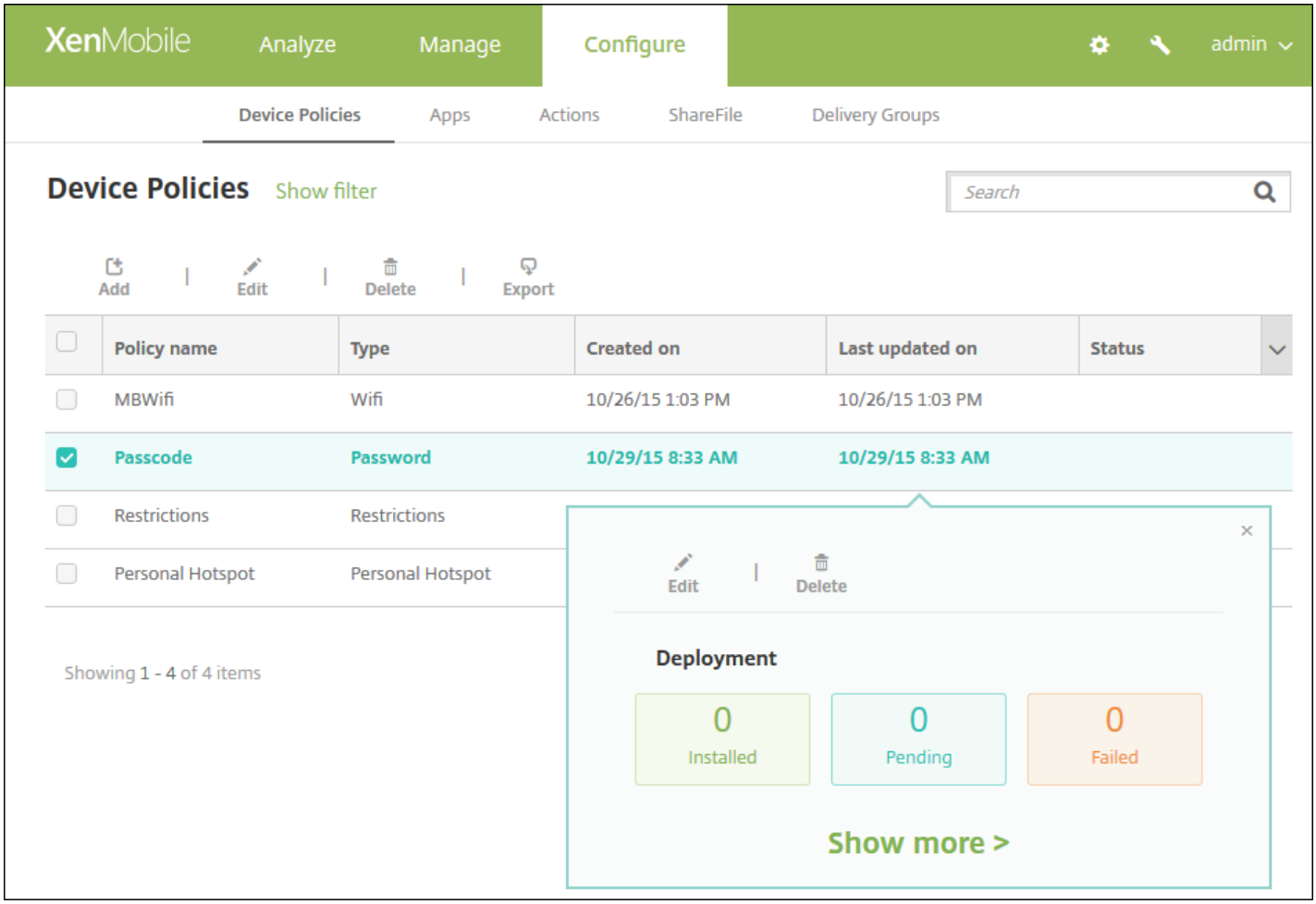


9 Haga clic en **Save**.

La directiva aparecerá en la tabla **Device Policies**.

Cómo modificar o eliminar una directiva de dispositivos

Para modificar o eliminar una directiva de dispositivos, marque la casilla ubicada junto a una directiva para que el menú de opciones aparezca sobre la lista de directivas. O bien, haga clic en una directiva de la lista para que el menú de opciones aparezca en el lado derecho de la lista.



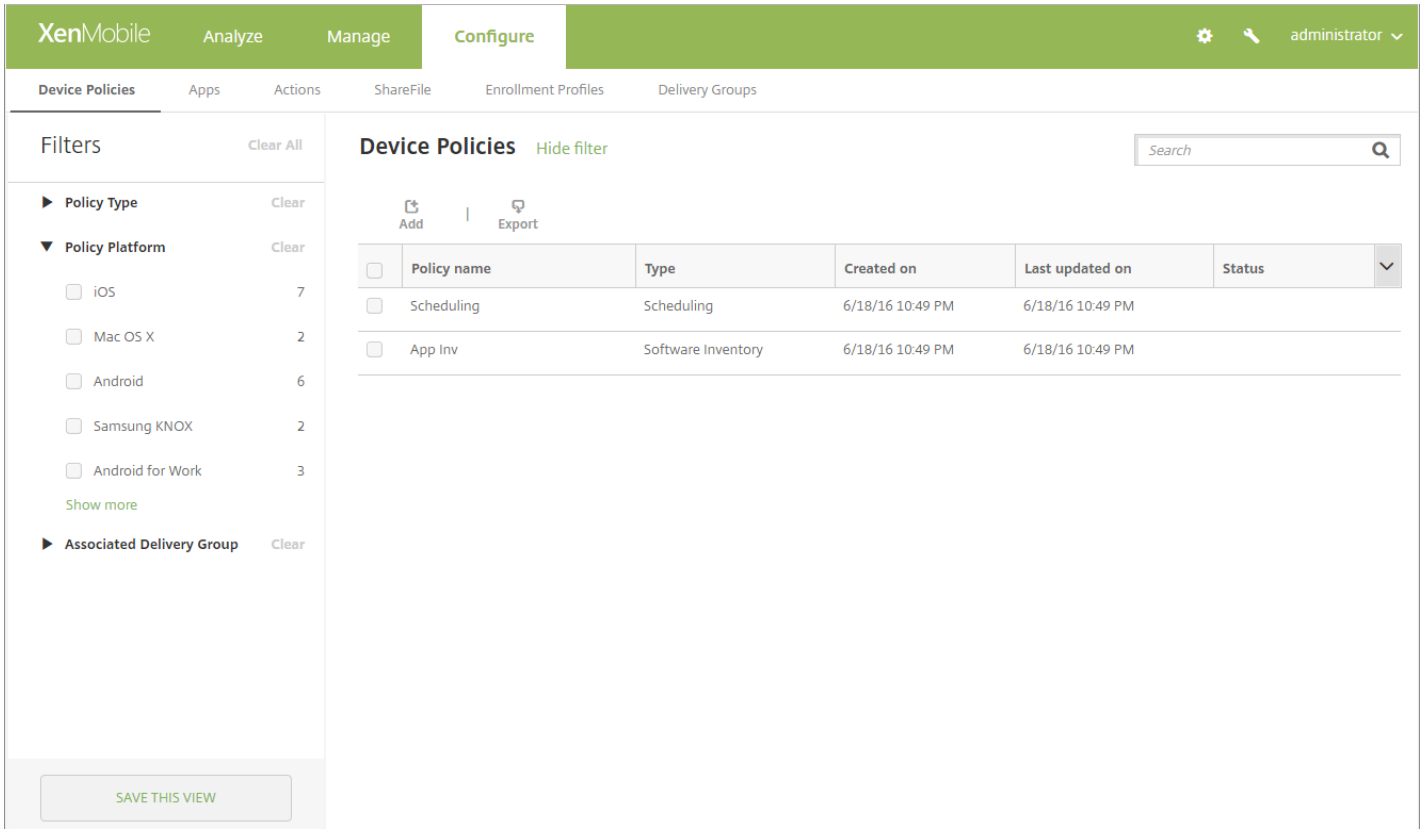
Para ver los detalles de la directiva, haga clic en **Show more**.

Para modificar toda la configuración de una directiva de dispositivos, haga clic **Edit**.

Aparecerá un cuadro de diálogo de confirmación si hace clic en **Delete**. Vuelva a hacer clic en **Delete**.

Cómo filtrar la lista de las directivas de dispositivos agregadas

Puede filtrar la lista de las directivas agregadas por tipos de directivas, plataformas y grupos de entrega asociados. En la página **Configure > Device Policies**, haga clic en **Show Filter**. En la lista, marque las casillas de los elementos que quiere ver.



Haga clic en **SAVE THIS VIEW** para guardar un filtro. Entonces, el nombre del filtro aparecerá en el botón situado debajo del botón **SAVE THIS VIEW**.

Directivas de dispositivos

Nombre de directiva de dispositivos	**Descripción de directiva de dispositivos**
AirPlay Mirroring (Duplicación AirPlay)	Esta directiva permite agregar dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) a 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	Esta directiva permite agregar impresoras AirPrint a la lista de impresoras AirPrint que aparece en los dispositivos iOS. Esta directiva facilita el respaldo de entornos en los que las impresoras y los dispositivos están en subredes diferentes. Disponible para iOS 7.0 y versiones posteriores. Nota: Compruebe que dispone de la dirección IP y de la ruta de recursos para cada impresora.
Android for Work App Restrictions (Restricciones para	Esta directiva permite modificar las restricciones asociadas a aplicaciones Android. Sin embargo, para poder modificarlas, debe cumplir los siguientes requisitos previos: • Complete, en Google, las tareas de configuración de Android. Para obtener más

aplicaciones de Android for Work)	información, consulte Android at Work. • Agregue aplicaciones Android a XenMobile. Para obtener más información, consulte Cómo agregar una aplicación de tienda pública de aplicaciones.
APN	Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. Esta directiva determina la configuración utilizada para conectar sus dispositivos al servicio GPRS (General Packet Radio Service) de un operador concreto de teléfonos. Esta configuración ya está definida en la mayoría de los teléfonos más recientes.
App Access (Acceso a aplicaciones)	Esta directiva permite definir una lista de las aplicaciones siguientes: • Aplicaciones que deben instalarse en el dispositivo • O bien, aplicaciones que pueden instalarse en el dispositivo • O bien, aplicaciones 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 (Atributos de aplicaciones)	Esta directiva permite especificar atributos (por ejemplo, un ID de paquete de aplicación administrada o un identificador de red VPN para cada aplicación) para dispositivos iOS.
App Configuration (Configuración de aplicaciones)	Esta directiva permite configurar de forma remota varias opciones y comportamientos de las aplicaciones que admiten la configuración administrada. Para ello, debe implementar un archivo de configuración XML (llamado lista de propiedades o plist) en dispositivos iOS. O bien, puede implementar pares de clave y valor en escritorios, tabletas o teléfonos Windows 10.
App Inventory (Inventario de aplicaciones)	Esta directiva permite realizar un inventario de las aplicaciones presentes en los dispositivos administrados. Una vez realizado, XenMobile compara el inventario con las directivas de acceso a aplicaciones que se hayan implementado en esos dispositivos. De esta forma, puede detectar aplicaciones permitidas o prohibidas (incluidas en la lista blanca o negra, respectivamente) y actuar en consecuencia.
App Lock (Bloqueo de aplicaciones)	Esta directiva permite definir una lista de las aplicaciones que los usuarios pueden o no ejecutar en un dispositivo. Puede configurar esta directiva para dispositivos Android y iOS, pero su funcionamiento difiere según la plataforma. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS. La directiva de bloqueo de aplicaciones funciona en la mayoría de los dispositivos Android L y M. Sin embargo, esta directiva no funciona en dispositivos Android N o versiones posteriores porque Google dejó de utilizar la API requerida. En dispositivos iOS, solo se puede elegir una aplicación iOS por cada directiva. En

	consecuencia, los usuarios pueden utilizar el dispositivo solamente para ejecutar una 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 (Uso de red de las aplicaciones)	Esta directiva permite definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas deben usar, 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. Las aplicaciones administradas no incluyen estas aplicaciones: • Aplicaciones que los usuarios descargan directamente en sus dispositivos. Es decir, las aplicaciones que no se implementan a través de XenMobile. • Aplicaciones ya instaladas en los dispositivos cuando los dispositivos se inscribieron en XenMobile.
App Restrictions (Restricciones de aplicaciones)	Esta directiva permite crear listas negras para las aplicaciones que quiere impedir que los usuarios instalen en dispositivos Samsung KNOX. También puede crear listas blancas para las aplicaciones que quiera permitir instalar a los usuarios.
App Uninstall (Desinstalación de aplicaciones)	Esta directiva permite quitar aplicaciones de los dispositivos del usuario por varias razones. Por ejemplo, puede que no quiera respaldar ciertas aplicaciones. O bien, puede que su empresa quiera reemplazar las aplicaciones existentes por aplicaciones similares de otros proveedores. 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 (Restricciones de desinstalación de aplicaciones)	Esta directiva permite especificar las aplicaciones que los usuarios pueden o no pueden desinstalar.
Browser (Explorador Web)	Esta directiva permite definir si los dispositivos de los usuarios pueden usar el explorador Web o limitar las funciones de explorador que se puedan usar. En dispositivos Samsung, puede inhabilitar 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.
Calendario (CalDav)	Esta directiva permite agregar una cuenta de calendario (CalDAV) a dispositivos iOS o Mac OS X. La cuenta de CalDAV permite a los usuarios sincronizar datos de programación con cualquier servidor compatible con CalDAV.

Cellular (Móvil)	Esta directiva permite configurar los parámetros de red de telefonía móvil.
Connection Manager (Administrador de conexiones)	Esta directiva permite 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.
Contactos (CardDAV)	Esta directiva permite agregar una cuenta iOS de contactos (CardDAV) a dispositivos iOS o Mac OS X. La cuenta de CardDAV permite a los usuarios sincronizar datos de contacto con cualquier servidor compatible con CardDAV.
Copy apps to Samsung Container (Copiar aplicaciones al contenedor de Samsung)	Esta directiva permite que las aplicaciones que ya están instaladas en un dispositivo se copien a un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles. Las aplicaciones que se copien al contenedor SEAMS estarán disponibles en la pantalla de inicio del dispositivo. Las aplicaciones que se copien al contenedor KNOX solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.
Credenciales	Esta directiva permite la autenticación integrada con la configuración de PKI en XenMobile. Por ejemplo, con una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor. Para obtener información acerca de las credenciales, consulte Certificados y autenticación. Cada plataforma de dispositivo requiere un conjunto diferente de valores, que se describen en el artículo sobre la directiva de credenciales.
Custom XML (XML personalizado)	Esta directiva personaliza las siguientes características: • El aprovisionamiento (configurar el dispositivo y habilitar o inhabilitar las funciones) • La configuración de dispositivos (permitir o no a los usuarios cambiar la configuración y los parámetros de sus dispositivos) • Las actualizaciones de software (proporcionar o no 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 (recibir 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. El uso de 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.
Defender	Esta directiva permite configurar Windows Defender para tabletas y escritorios Windows 10.
Delete Files and Folders (Eliminar archivos y carpetas)	Esta directiva permite eliminar archivos o carpetas concretas de los dispositivos Windows Mobile/CE.

Delete Registry Keys and Values (Eliminar claves y valores del Registro)	Esta directiva permite eliminar, de los dispositivos Windows Mobile/CE, claves y valores específicos del Registro.
Device Health Attestation (Atestación del estado de dispositivos)	Esta directiva requiere a los dispositivos Windows 10 que informen de su estado. Para ello, deben enviar datos concretos e información del tiempo de ejecución al servicio Health Attestation Service (HAS) para el 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 éste, puede implementar las acciones automatizadas que haya configurado. Para obtener información, consulte la página Device HealthAttestation CSP de Microsoft.
Device Name (Nombre del dispositivo)	Esta directiva permite definir nombres para dispositivos iOS y Mac OS X de forma que pueda reconocerlos. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Para obtener información acerca de las macros, consulte Macros.
Enterprise Hub	Esta directiva para dispositivos Windows Phone permite distribuir aplicaciones a través de la tienda Enterprise Hub de la empresa. XenMobile solo admite una directiva Enterprise Hub por modo de Windows Phone Secure Hub. Por ejemplo, no debe crear varias directivas Enterprise Hub con versiones diferentes de Secure Home para XenMobile Enterprise Edition. Solo puede implementar la directiva Enterprise Hub inicial durante la inscripción del dispositivo.
Exchange	XenMobile ofrece dos opciones para entregar el correo electrónico. Puede utilizar esta directiva MDM para habilitar el correo electrónico de ActiveSync para el cliente de correo electrónico nativo en el dispositivo. O bien, se puede entregar correo electrónico de ActiveSync mediante la aplicación Secure Mail del contenedor.
Files (Archivos)	Esta directiva permite agregar, a XenMobile, scripts que realizan determinadas funciones para los usuarios. O bien, puede agregar archivos de documento a los que quiere que los usuarios de dispositivos Android tengan acceso en sus dispositivos. Cuando agregue el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo. Por ejemplo, para enviar un documento o archivo PDF de la compañía a los usuarios Android, implemente el archivo en el dispositivo. A continuación, informe a los usuarios de la ubicación del archivo.
Font (Fuente)	Esta directiva permite agregar más fuentes a dispositivos iOS y Mac OS X. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.oft). No se admiten las colecciones de fuentes (.ttc u .otc). Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.
Home screen layout	

(Diseño de la pantalla de inicio)	Esta directiva permite especificar la distribución de aplicaciones y carpetas en la pantalla de inicio de iOS en iOS 9.3 y versiones posteriores de los dispositivos supervisados.
Import iOS and Mac OSx Profile (Importar perfil de iOS y Mac OS X)	Esta directiva permite 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 (Quiosco)	Esta directiva permite restringir el uso de aplicaciones en dispositivos Samsung SAFE. Puede limitar las aplicaciones disponibles a una aplicación o aplicaciones específicas. 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 está en modo quiosco.
Launcher Configuration (Configuración de Launcher)	Esta directiva para dispositivos Android permite especificar lo siguiente para Citrix Launcher: • Las aplicaciones permitidas • Una imagen personalizada de logotipo para el icono de Citrix Launcher • Una imagen personalizada de fondo para Citrix Launcher • Requisitos de contraseña para salir de Citrix Launcher
LDAP	Esta directiva para dispositivos iOS permite proporcionar información sobre el servidor LDAP a utilizar, incluida la información de cuenta necesaria (como el nombre de host del servidor LDAP). La directiva también ofrece un conjunto de directivas de búsquedas LDAP a usar cuando se consulta el servidor LDAP.
Location (Localización)	Esta directiva permite ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado GPS para Secure Hub. Después de implementar esta directiva en el dispositivo, puede enviar el comando "locate" desde el servidor XenMobile. El dispositivo responde con sus coordenadas de ubicación. XenMobile también admite directivas de geocerca y seguimiento geográfico.
Mail (Correo)	Esta directiva permite configurar una cuenta de correo electrónico en dispositivos iOS o Mac OS X.
Managed Domains (Dominios administrados)	Esta directiva permite 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 en dispositivos supervisados iOS 8 y versiones posteriores.

MDM Options (Opciones de MDM)	Esta directiva permite 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 Inscripción en masa de dispositivos iOS y macOS.
Organization Info (Información sobre la organización)	Esta directiva permite especificar la información de la organización para los mensajes de alertas que XenMobile implementa en los dispositivos iOS. Disponible en iOS 7 y versiones posteriores.
Passcode (Código de acceso)	Esta directiva permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Además, puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.
Personal Hotspot (Hotspot personal)	Esta directiva permite a los usuarios conectarse a Internet cuando no tienen una red Wi-Fi al alcance. Los usuarios se conectan a través de una conexión de datos móviles en su dispositivo iOS con la funcionalidad de hotspot personal. Disponible en iOS 7.0 y versiones posteriores.
Profile Removal (Eliminación de perfiles)	Una vez implementada, esta directiva elimina el perfil de aplicación de los dispositivos iOS o Mac OS X.
Provisioning Profile (Perfil de aprovisionamiento)	Esta directiva permite indicar un perfil de aprovisionamiento de distribución empresarial que se envía a los dispositivos. Cuando desarrolla y firma el código de una aplicación iOS de empresa, generalmente incluye un perfil de aprovisionamiento. Apple requiere ese perfil para que la aplicación se pueda ejecutar en un dispositivo iOS. Si falta o ha caducado un perfil de aprovisionamiento, la aplicación se bloquea cuando un usuario toca en ella para abrirla.
Provisioning Profile Removal (Eliminación de perfiles de aprovisionamiento)	Esta directiva elimina perfiles de aprovisionamiento de iOS. Para obtener información acerca de los perfiles de aprovisionamiento, consulte Directiva de dispositivos de perfil de aprovisionamiento.
Proxy	Esta directiva permite especificar la configuración global de proxy HTTP en dispositivos que ejecutan Windows Mobile/CE y iOS 6.0 o versiones posteriores. Puede implementar solamente una directiva global de proxy HTTP por dispositivo.
Registry (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. Esta directiva permite definir los valores y las claves de Registro que le permitirán administrar dispositivos Windows Mobile/CE.
Remote Support (Asistencia remota)	Esta directiva permite el acceso remoto a dispositivos Samsung KNOX.

Restrictions (Restricciones)	Esta directiva ofrece numerosas opciones para bloquear y controlar características y funcionalidades en los dispositivos administrados. Ejemplos de opciones de restricción: inhabilitar la cámara o el micrófono, aplicar reglas de roaming o pedir el acceso a servicios externos, como tiendas de aplicaciones.
Roaming	Esta directiva permite configurar si se permite el roaming de voz y de datos en los dispositivos iOS o Windows Mobile/CE. Si se inhabilita la movilidad de voz, la movilidad de datos se inhabilita automáticamente. En el caso de iOS, esta directiva está disponible para iOS 5.0 y versiones posteriores.
Samsung SAFE Firewall (Firewall de Samsung SAFE)	Esta directiva permite configurar los parámetros del firewall para dispositivos Samsung. Puede proporcionar 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 éste.
Samsung MDM License Key (Clave de licencia MDM de Samsung)	Esta directiva permite indicar la clave integrada de Samsung Enterprise License Management (ELM) que debe implementar en un dispositivo para poder implementar después directivas y restricciones de SAFE. XenMobile respalda y extiende directivas de Samsung for Enterprise (SAFE) y Samsung KNOX.
Scheduling (Programación)	Esta directiva es necesaria para que los dispositivos Android y Windows Mobile se conecten de vuelta al servidor XenMobile para la administración MDM, el envío de aplicaciones y la implementación de directivas. Si no envía esta directiva y no habilita Google FCM, el dispositivo no podrá volver a conectarse al servidor.
SCEP	Esta directiva permite configurar dispositivos iOS y Mac OS X para obtener un certificado desde un servidor SCEP externo. También puede entregar un certificado al dispositivo mediante SCEP de una PKI que está conectada a XenMobile. Para ello, cree un proveedor PKI y una entidad PKI en el modo distribuido. Para obtener más información, consulte Entidades de infraestructura PKI.
SSO Account (Cuenta SSO)	Esta directiva permite 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. 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 es compatible con la autenticación Kerberos. Disponible para iOS 7.0 y versiones posteriores.
Storage Encryption (Cifrado de almacenamiento)	Esta directiva permite cifrar almacenamiento interno y externo. En algunos dispositivos, esta directiva impide que los usuarios usen una tarjeta de almacenamiento en sus dispositivos.

Subscribed Calendars (Calendarios suscritos)	Esta directiva permite agregar un calendario suscrito a la lista de calendarios en dispositivos iOS. La lista de los calendarios públicos a los que se puede suscribir está disponible en www.apple.com/downloads/macosx/calendars. 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 (Términos y condiciones)	Esta directiva permite requerir que los usuarios acepten las directivas específicas de la empresa que regulan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos en 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.
Tunnel (Túnel)	Esta directiva permite 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 se dirigirá primero a XenMobile. A continuación, el tráfico se redirigirá al servidor que ejecuta la aplicación.
VPN	Esta directiva permite acceder a sistemas back-end que utilizan tecnología antigua de puerta de enlace VPN. Esta directiva ofrece datos de conexión de puerta de enlace VPN que se pueden implementar en los dispositivos. XenMobile es compatible con varios proveedores de VPN, como 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 admita esta opción).
Wallpaper (Fondo de pantalla)	Esta directiva 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 para 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.
Web Content Filter (Filtro de contenido Web)	Esta directiva permite filtrar el contenido Web en dispositivos iOS. XenMobile utiliza la función Autofiltro de Apple y los sitios que usted agregue a las listas blancas y negras. Disponible para iOS 7.0 y versiones posteriores solo en dispositivos supervisados. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte Cómo colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

Webclip (Clip Web)	Esta directiva permite colocar accesos directos (o clips Web) que acceden a sitios 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.
Wi-Fi	Esta directiva permite a los administradores implementar datos del enrutador Wi-Fi en los dispositivos administrados. Los datos de enrutador son: el SSID, los datos de autenticación y los datos de configuración.
Windows CE Certificate (Certificado de Windows CE)	Esta directiva permite 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 y autenticación.
XenMobile Store	Esta directiva permite especificar si aparecerá un clip Web de XenMobile Store en la pantalla de inicio de los dispositivos de usuario.
XenMobile Options (Opciones de XenMobile)	Esta directiva permite configurar el comportamiento de Secure Hub al conectarse a XenMobile desde dispositivos Android y Windows Mobile/CE.
XenMobile Uninstall (Desinstalación de XenMobile)	Esta directiva permite 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.

Directivas de dispositivo por plataforma

Mar 29, 2017

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**.

La versión más reciente de XenMobile admite directivas de dispositivo para las plataformas siguientes:

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android Work
- Android
- Android Sony
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows Phone 8.1
- Teléfono Windows 10
- Escritorio o tableta Windows 10
- Windows Mobile/CE

Para obtener más información sobre dispositivos respaldados en la versión más reciente de XenMobile, consulte Plataformas de dispositivos respaldados.

> ## Nota
>
> Si su entorno está configurado con objetos de directiva de grupo (GPO):
>
> Cuando configure directivas de dispositivos de XenMobile para Windows 10, tenga en cuenta la siguiente regla. Si una directiva de uno o varios dispositivos Windows 10 inscritos entra en conflicto con otra, tendrá prioridad la directiva que se ajuste al GPO.

Directiva de duplicación AirPlay

Feb 27, 2017

La función AirPlay de Apple permite a los usuarios reproducir contenido de un dispositivo iOS en 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.

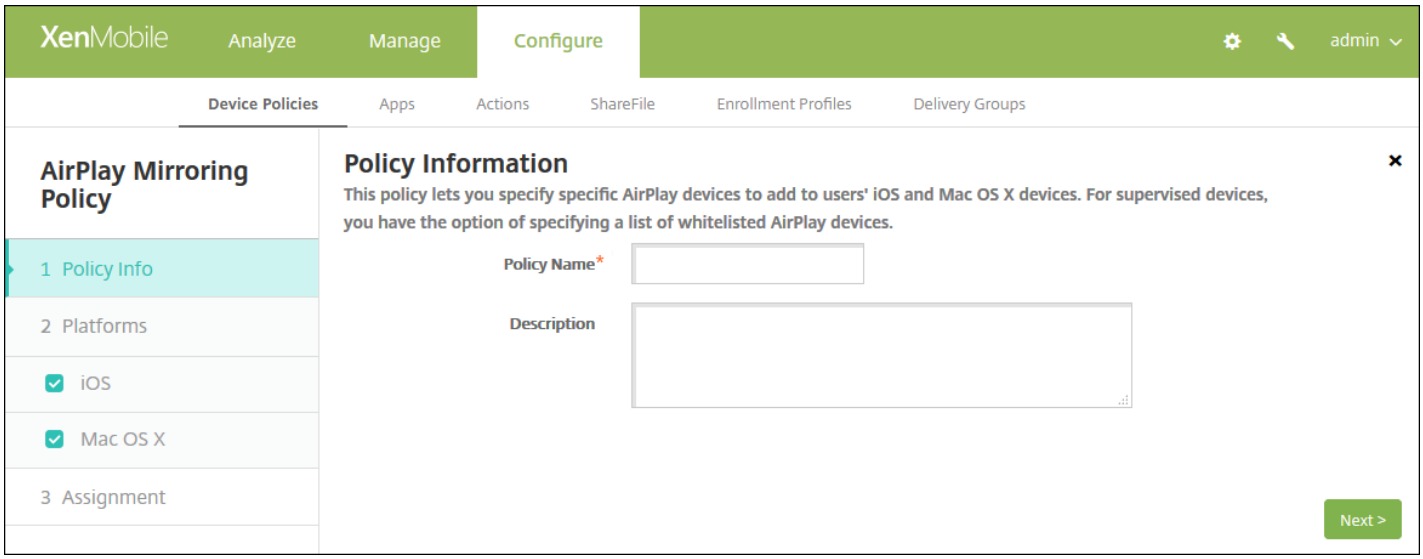
En XenMobile, puede agregar una directiva de dispositivos para agregar dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) en los dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos permitidos supervisados, lo que limitará a los usuarios a utilizar 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:

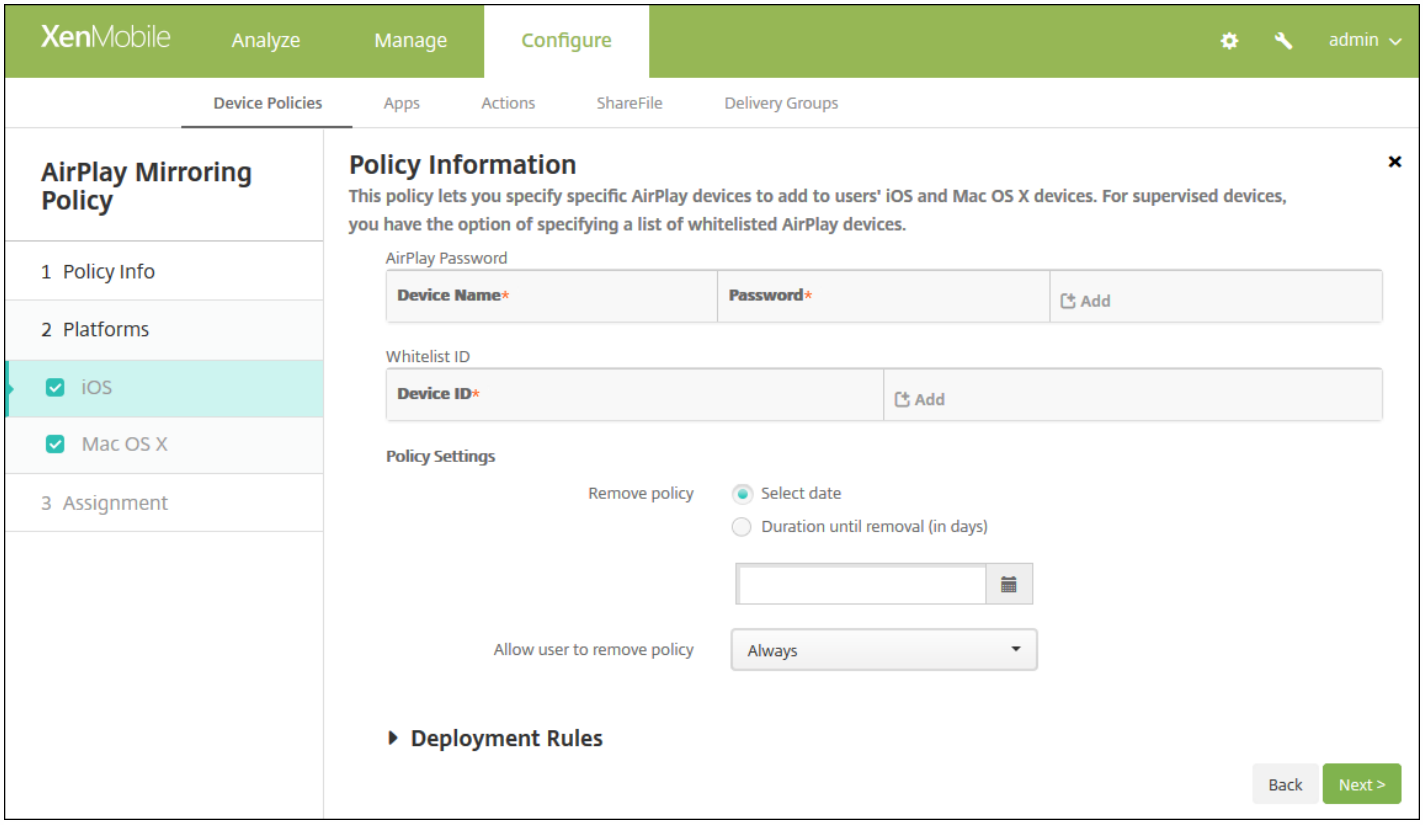
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

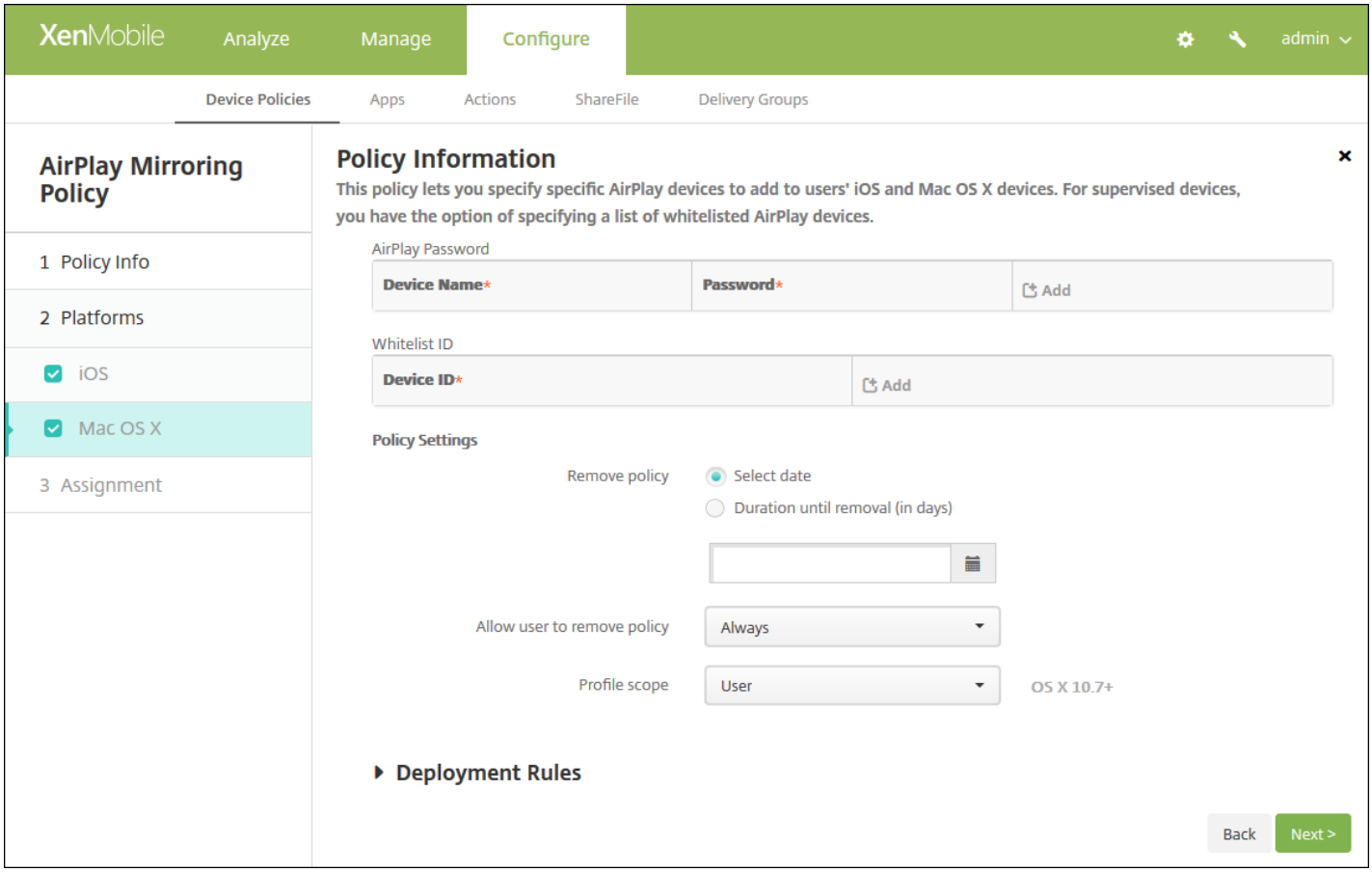
    Nota: Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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 guardarlos, o bien en **Cancel** para descartarlos.

- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, introduzca 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.

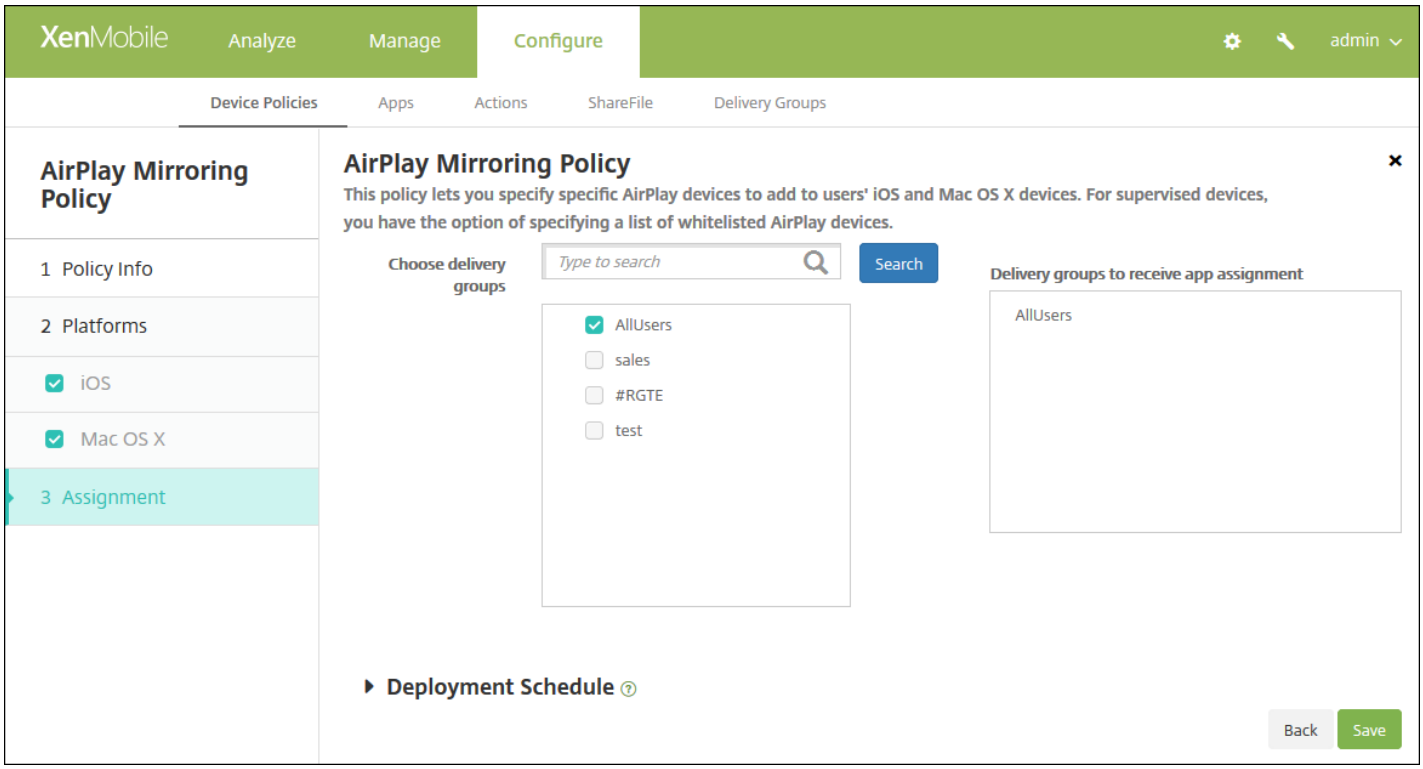
    Nota: Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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 guardarlos, o bien en **Cancel** para descartarlos.

- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 AirPrint

Feb 27, 2017

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.

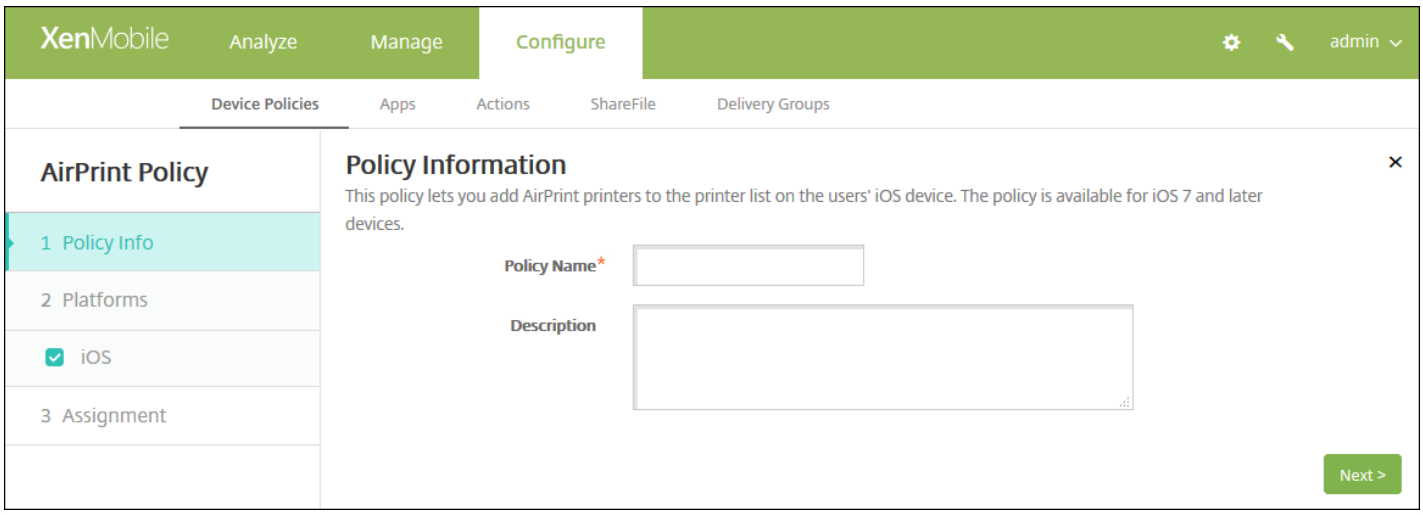
Nota:

- 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**.

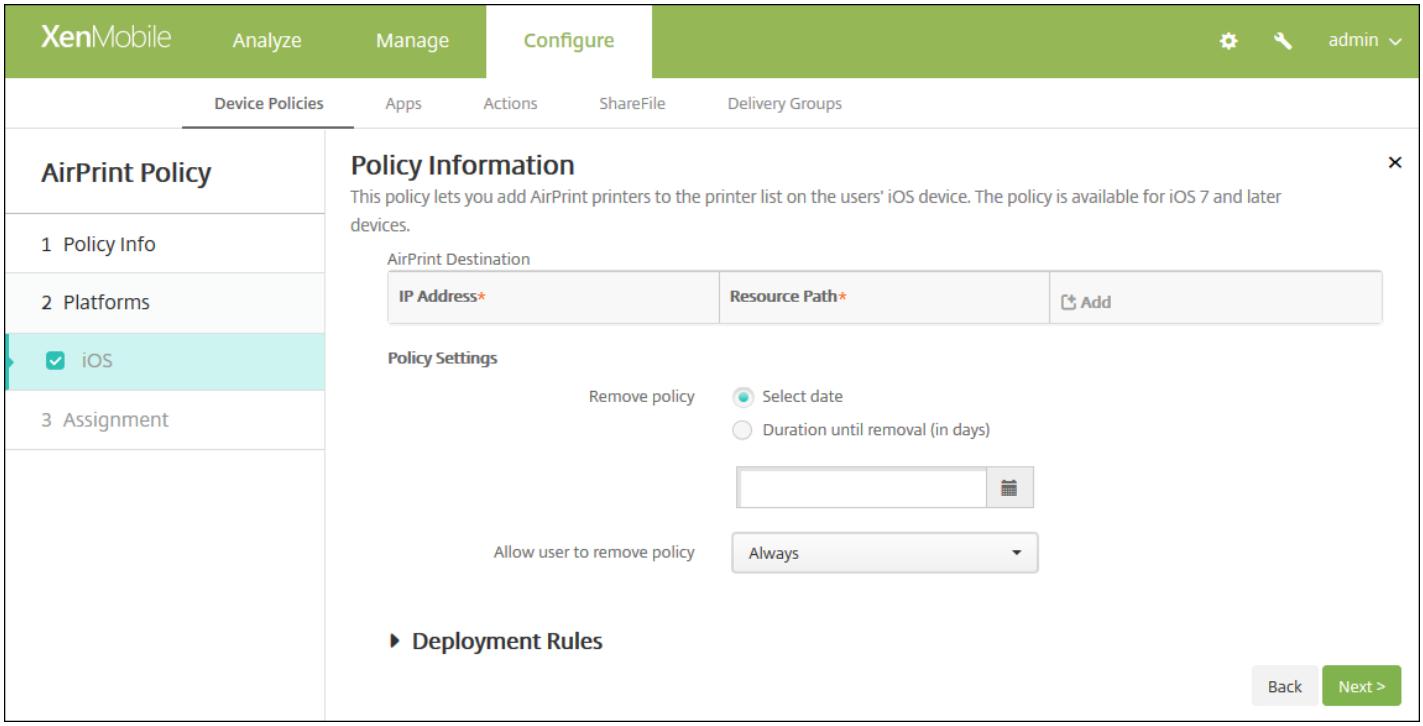
3. Haga clic en **More** y, en **End user**, haga clic en **AirPrint**. Aparecerá la página **AirPrint Policy**.



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 de información de la plataforma **iOS**.



6. Configure estos 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 _ipps.tcp de Bonjour. 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.

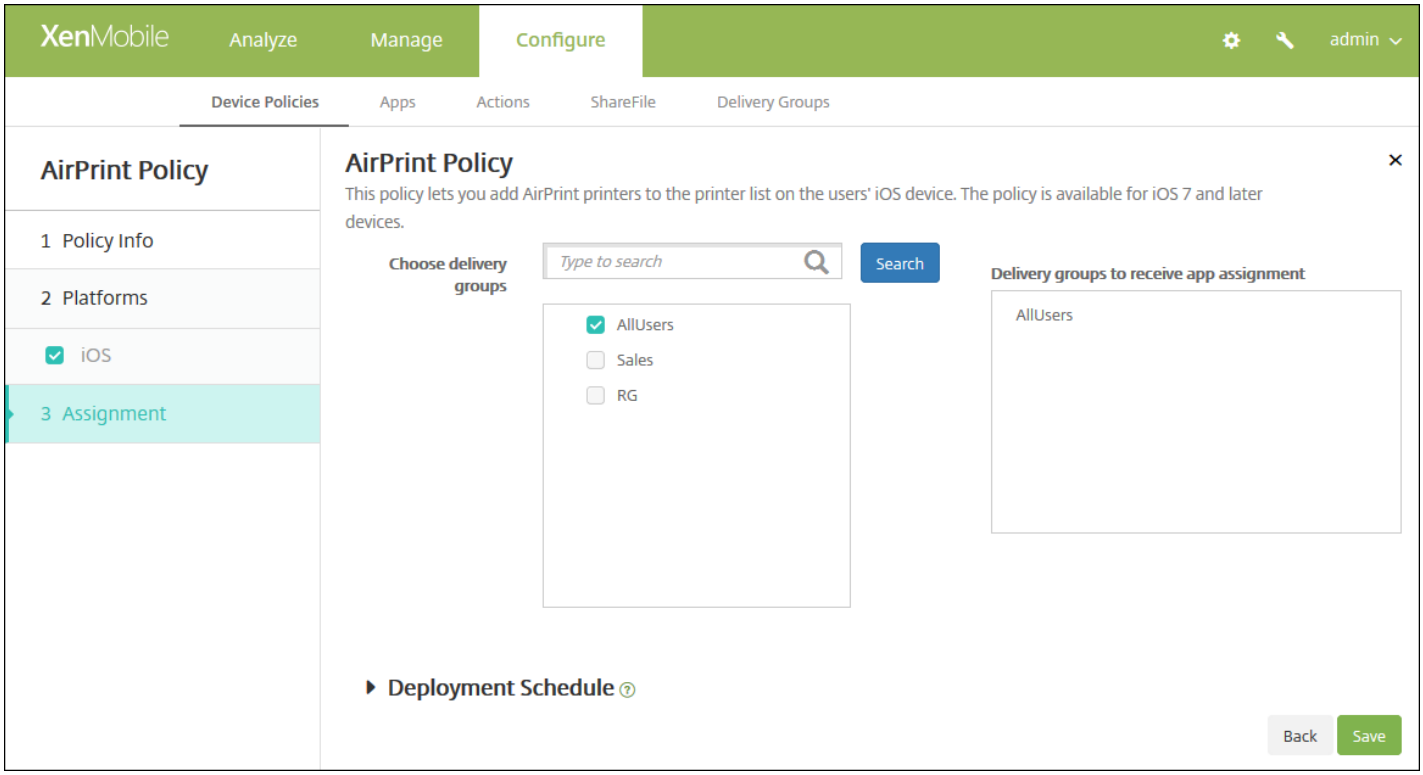
    Nota: Para eliminar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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

Feb 27, 2017

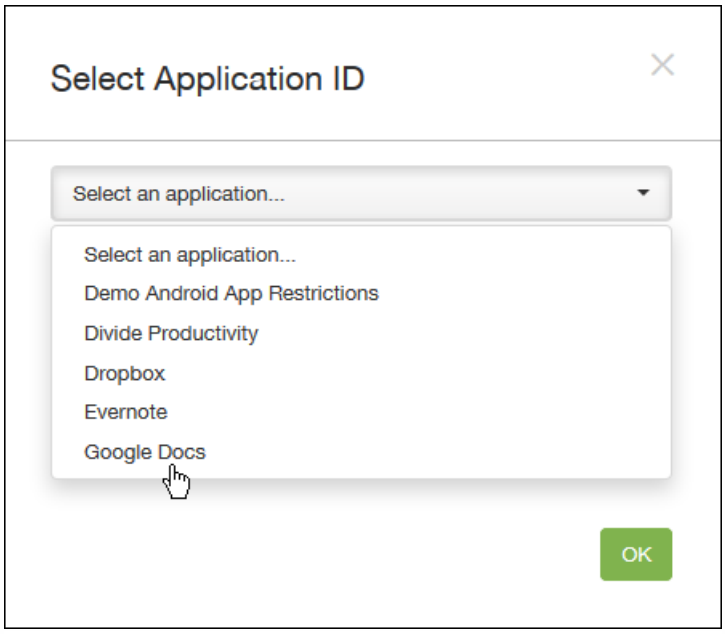
Puede modificar las restricciones asociadas a aplicaciones Android for Work. Sin embargo, antes de modificarlas, debe cumplir los siguientes requisitos previos:

- Complete, en Google, las tareas de configuración de Android for Work. Para obtener más información, consulte Administración de dispositivos con Android for Work.
- Cree 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**.

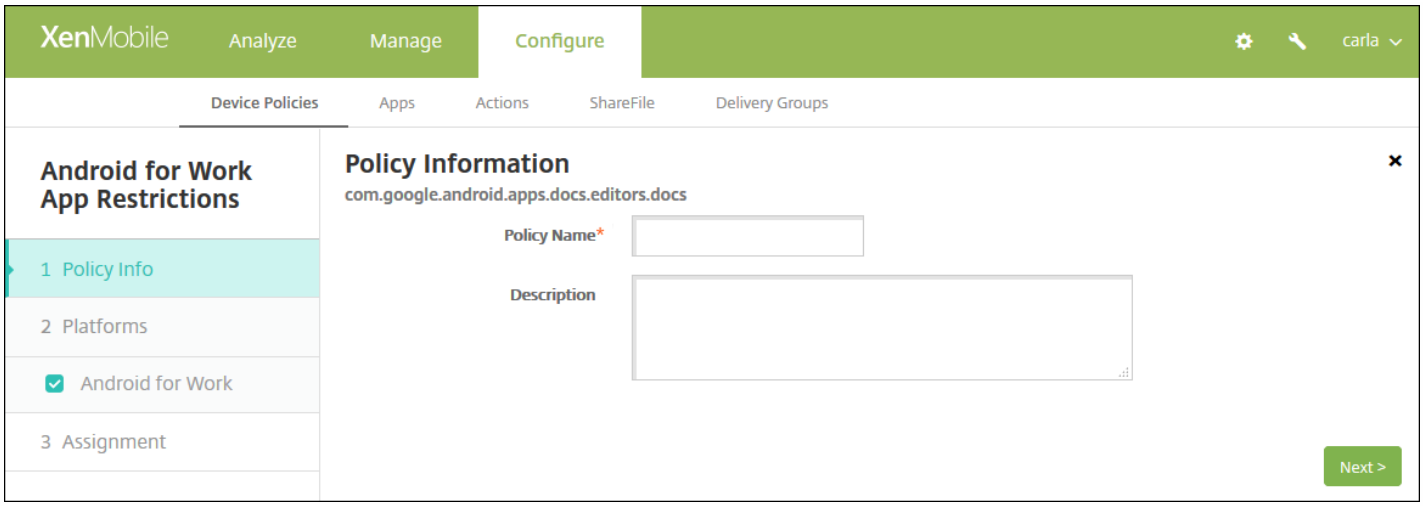
2. Haga clic en **Add** para agregar una nueva directiva. Aparecerá la página **Add a New Policy**.

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**.

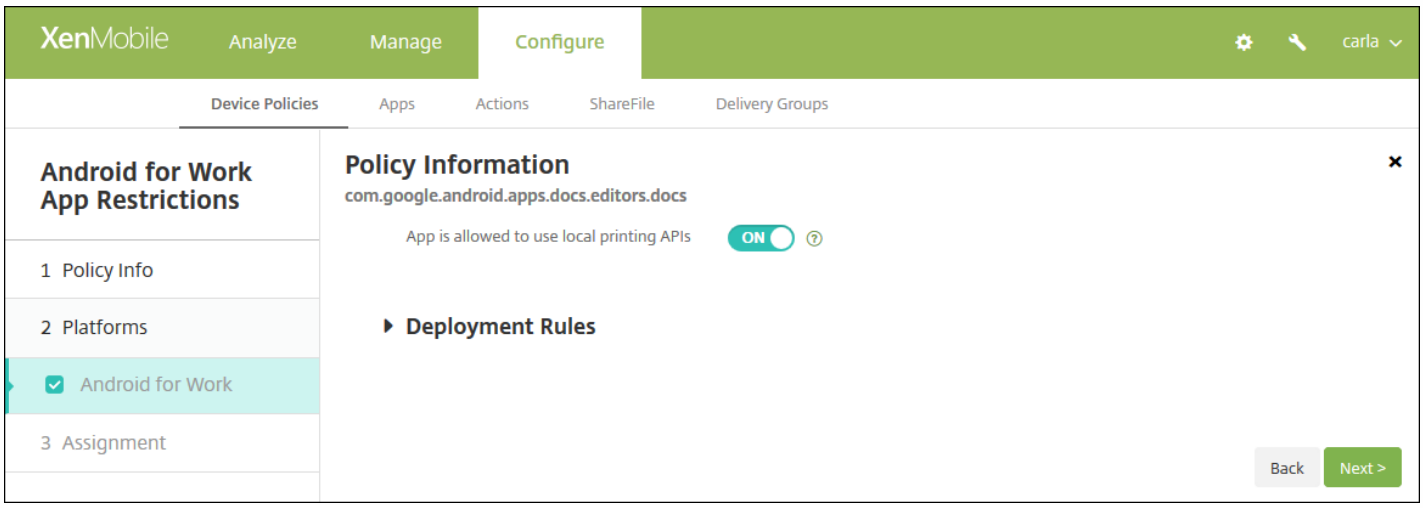
- Si no hay aplicaciones Android for Work que agregar a XenMobile, no podrá continuar. Para obtener más información sobre cómo agregar aplicaciones a XenMobile, consulte Incorporación de aplicaciones a XenMobile.
- Si la aplicación no tiene restricciones asociadas a ella, aparece una notificación a ese 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.

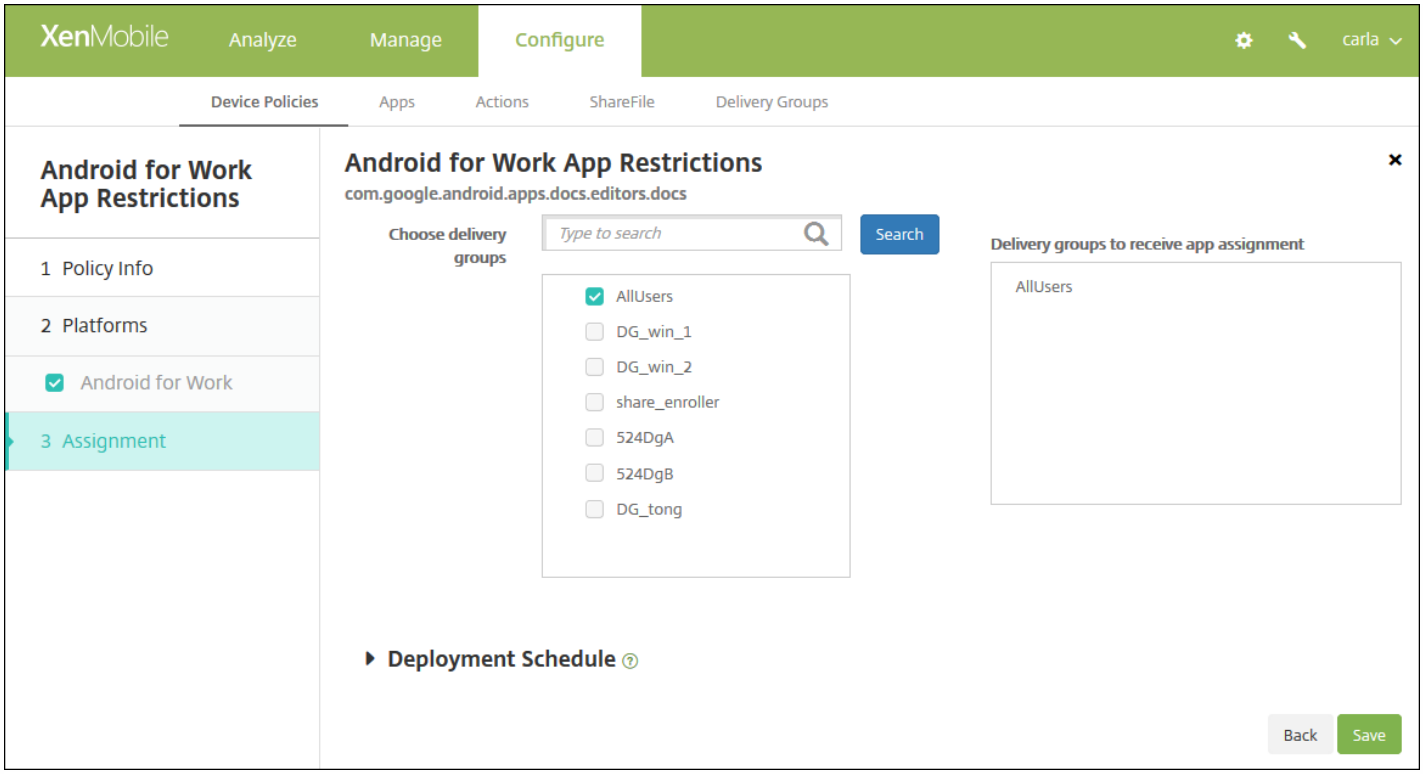
6. Haga clic en **Next**. Aparecerá la página referente a la plataforma **Android for Work**.



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 de la directiva **Android for Work App Restrictions**.



10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

12. Haga clic en **Save**.

Directivas de APN

Feb 27, 2017

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

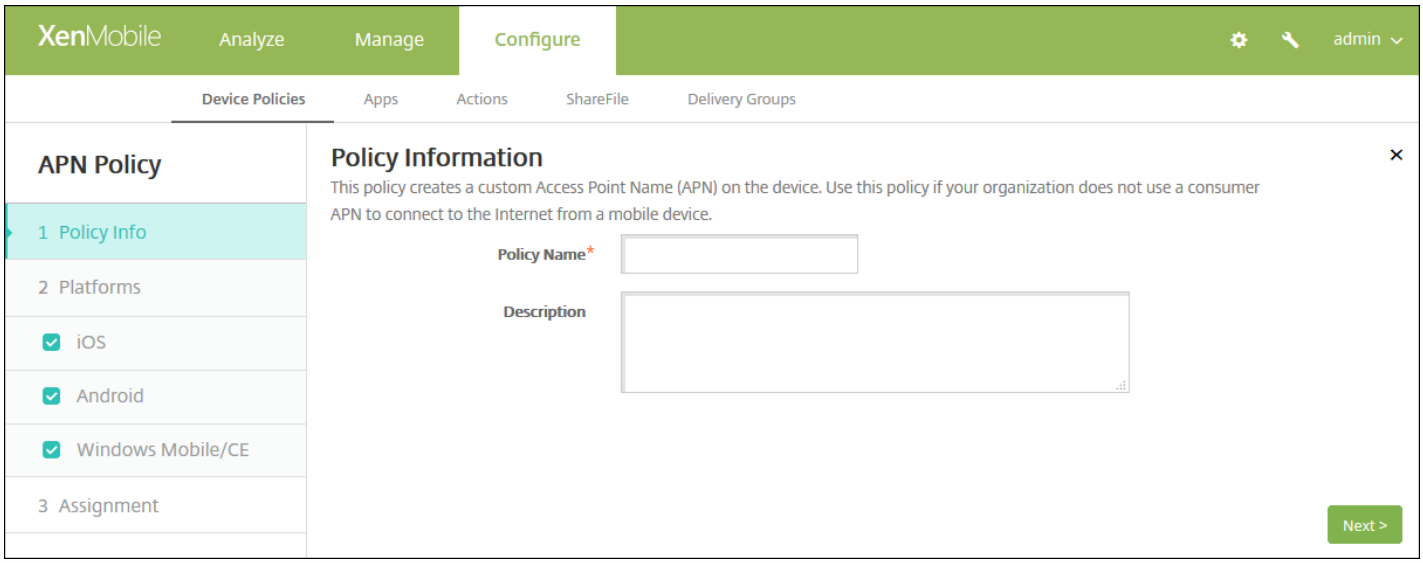
Configuración de Android

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 **APN Policy information**.



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.

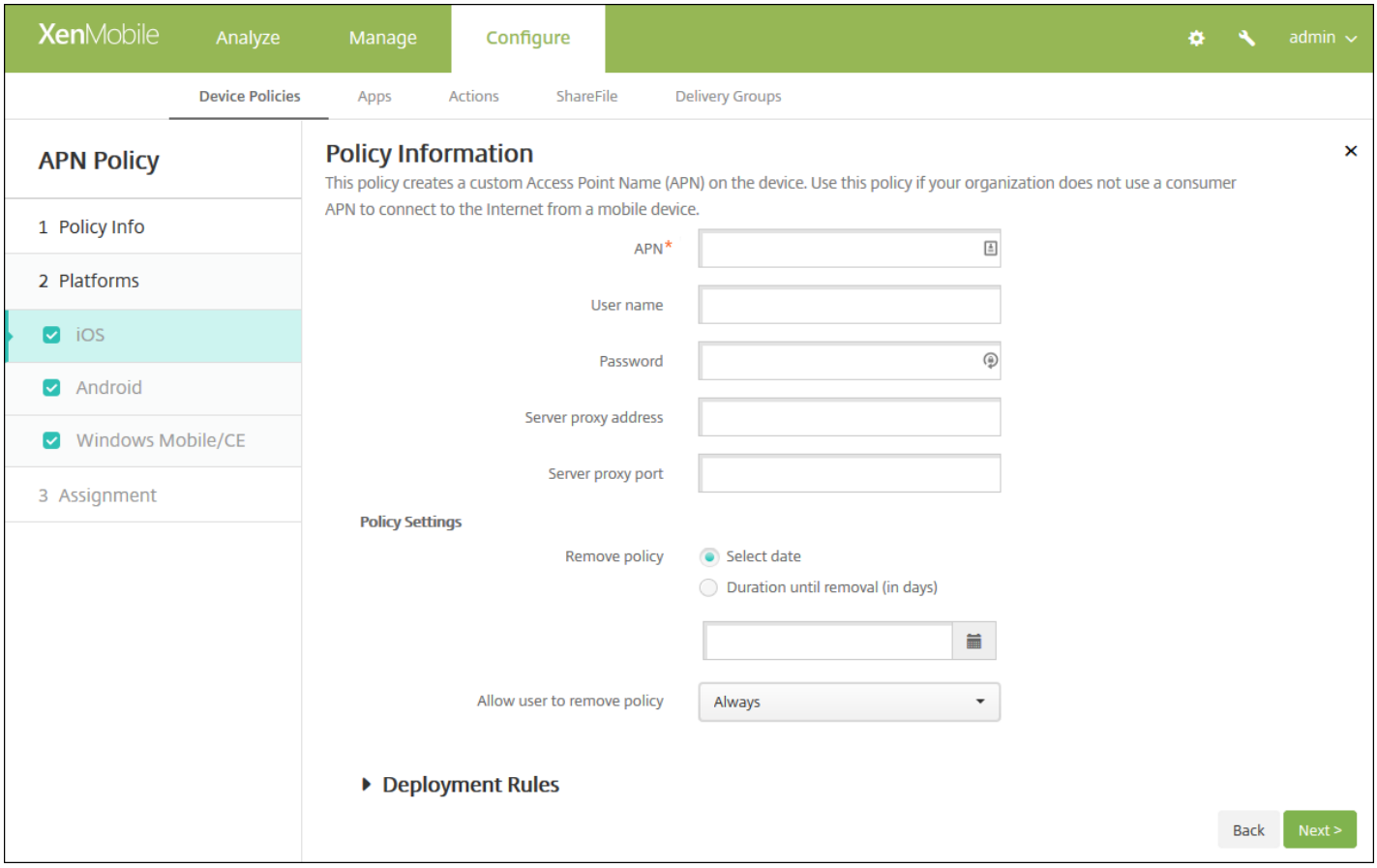
5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

Nota: Al aparecer la página **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.

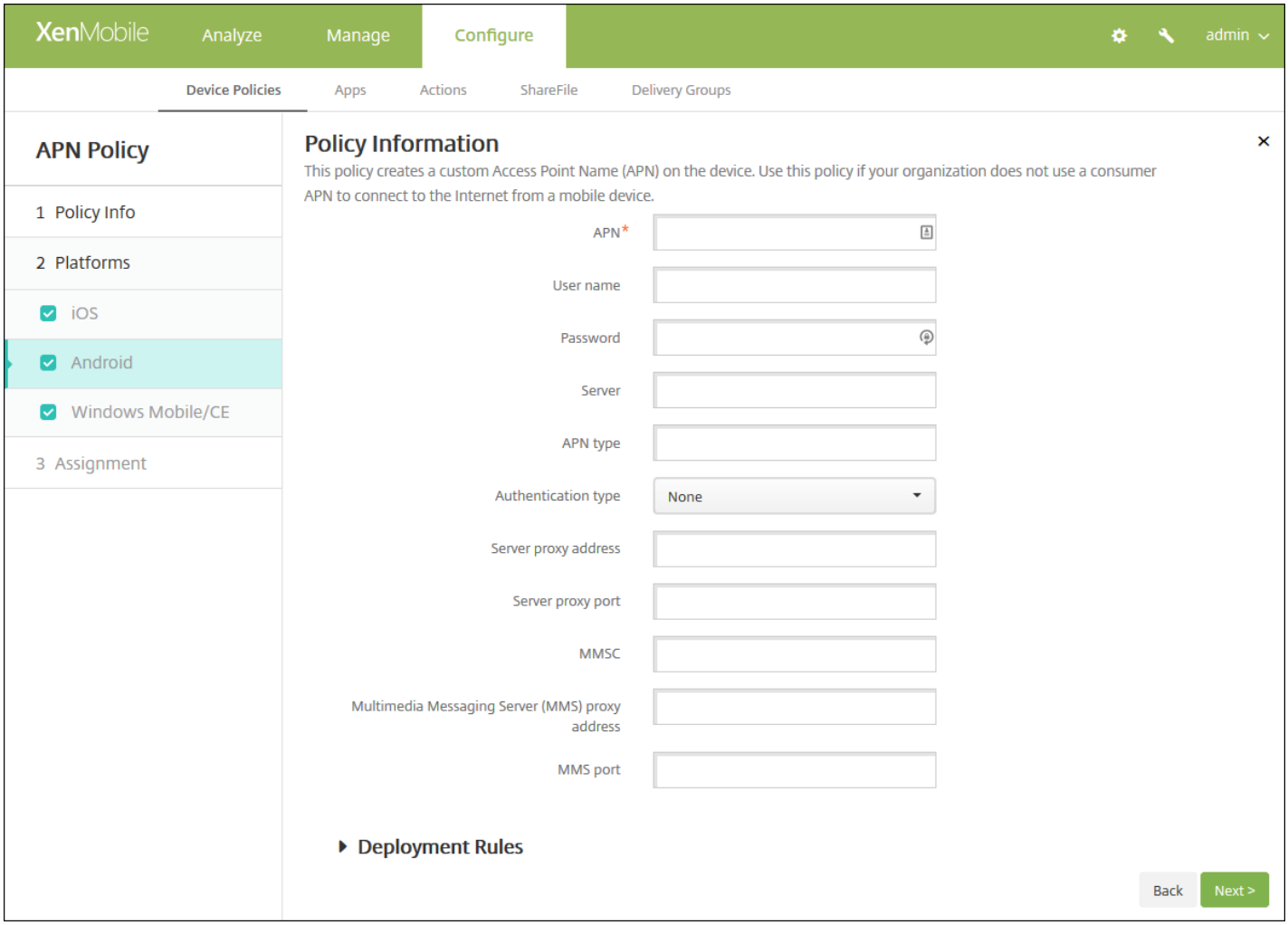
Configuración de los parámetros de iOS



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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Android



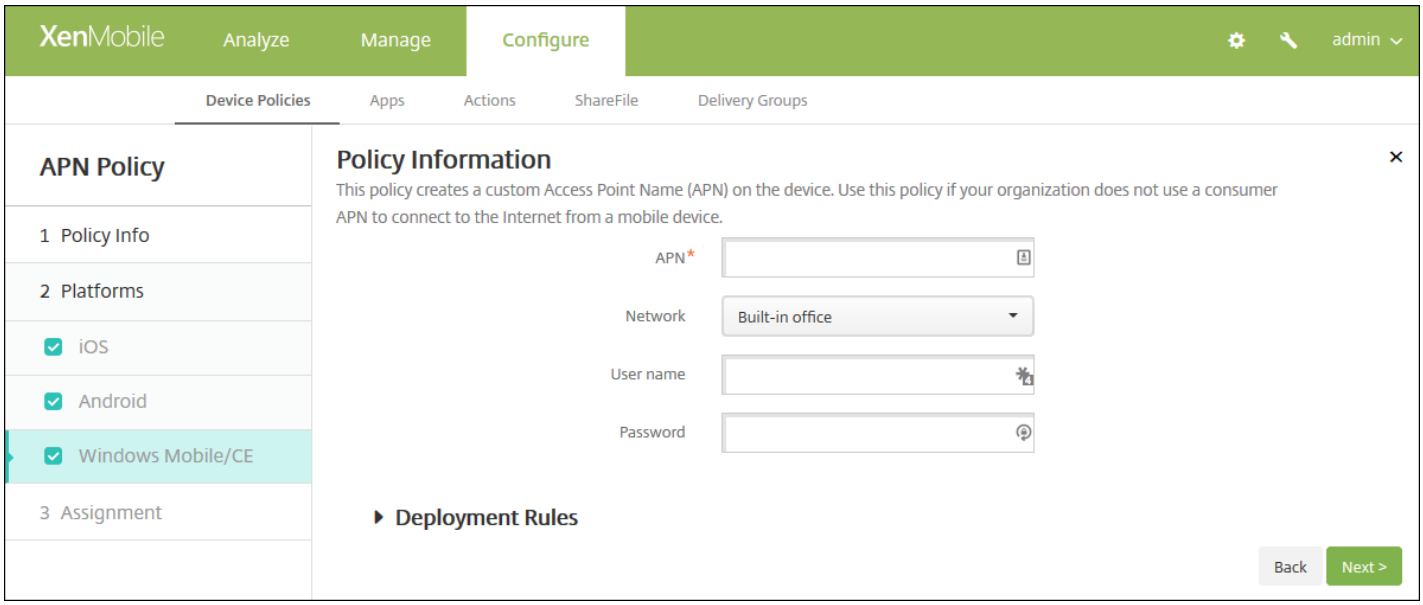
Configure estos parámetros:

- **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

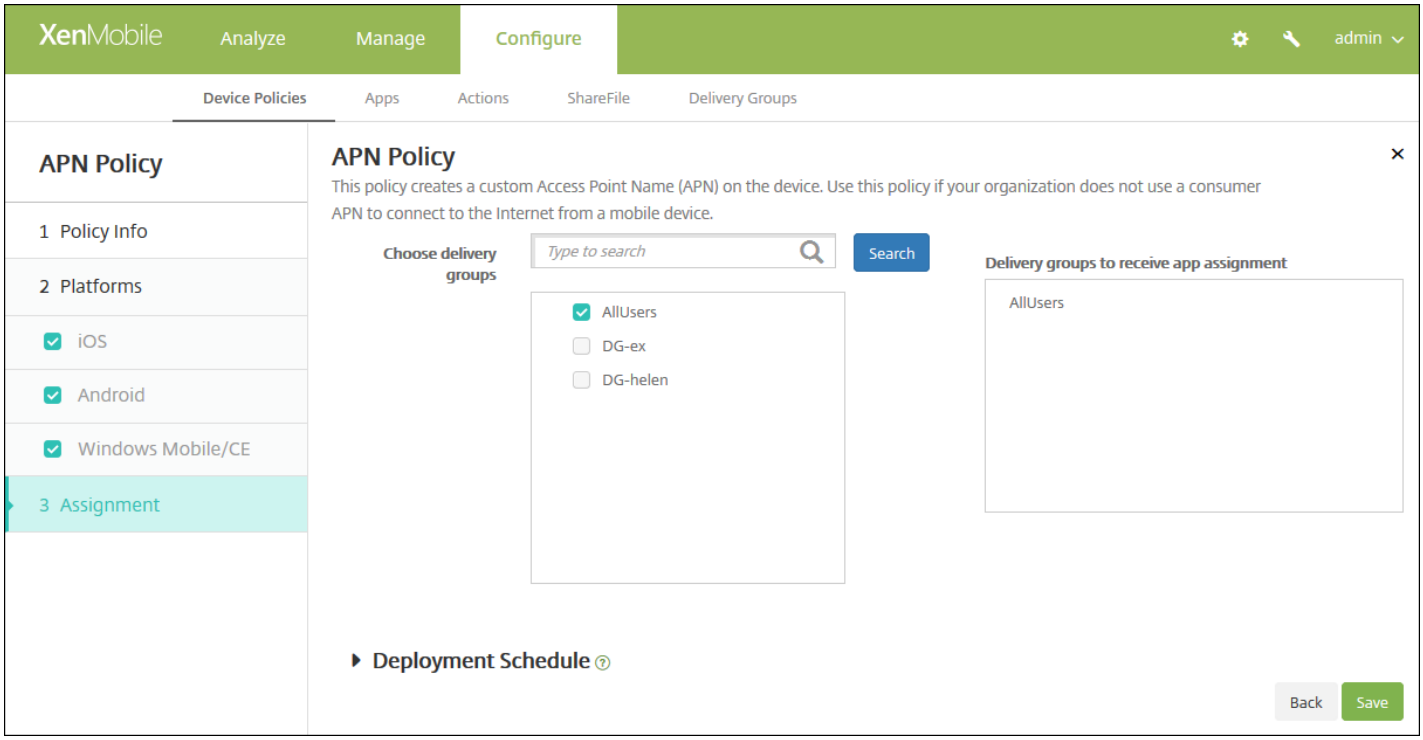


Configure los siguientes parámetros:

- **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 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.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página **Assignment** de la directiva de APN.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 acceso a aplicaciones

Feb 27, 2017

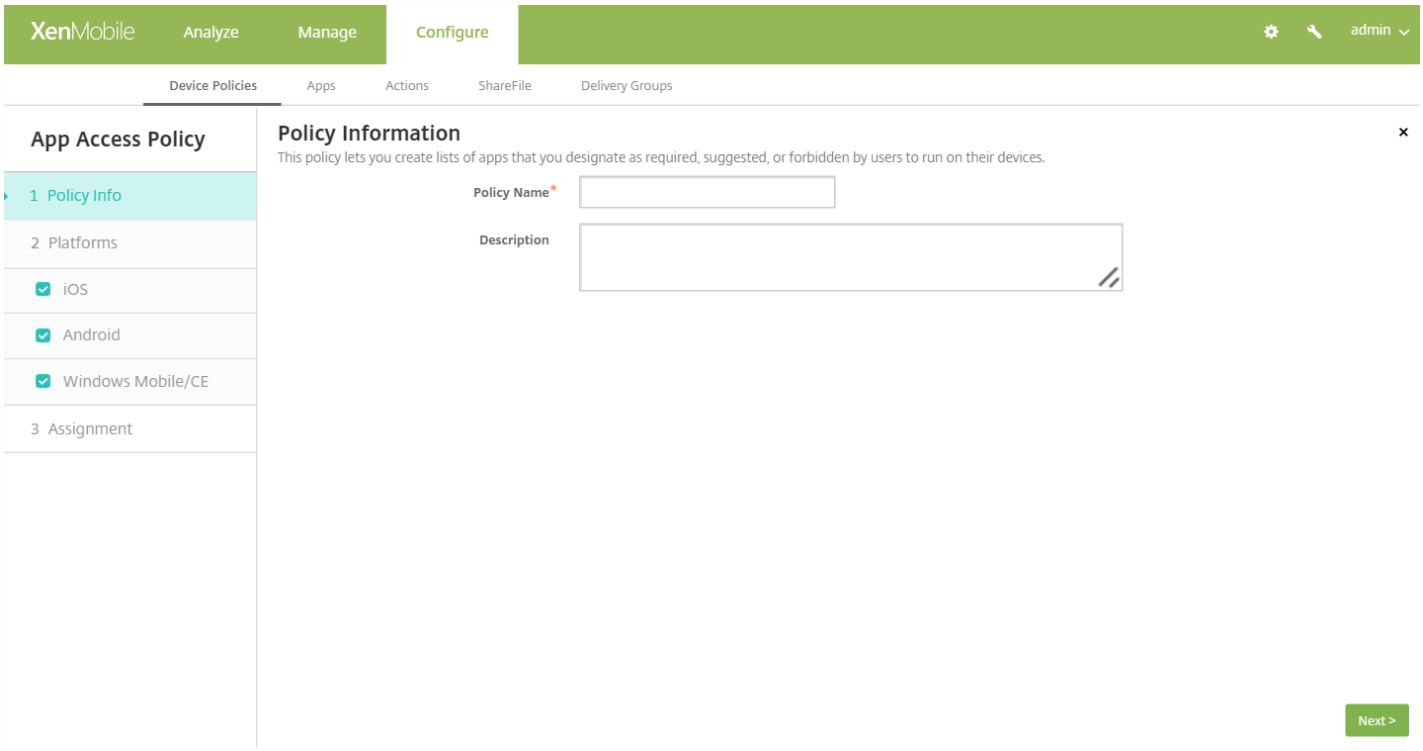
En XenMobile, la directiva de acceso de aplicaciones permite definir una lista de las aplicaciones que deben estar instaladas en el dispositivo, pueden estar instaladas en el dispositivo o no deben estar instaladas en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento 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**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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 guardarlos, o bien en **Cancel** para descartarlos.

7. Configure las reglas de implementación.

8. Haga clic en Next. Aparecerá la página de la plataforma siguiente o la página de asignación de **App Access Policy**.

9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 atributos de aplicaciones

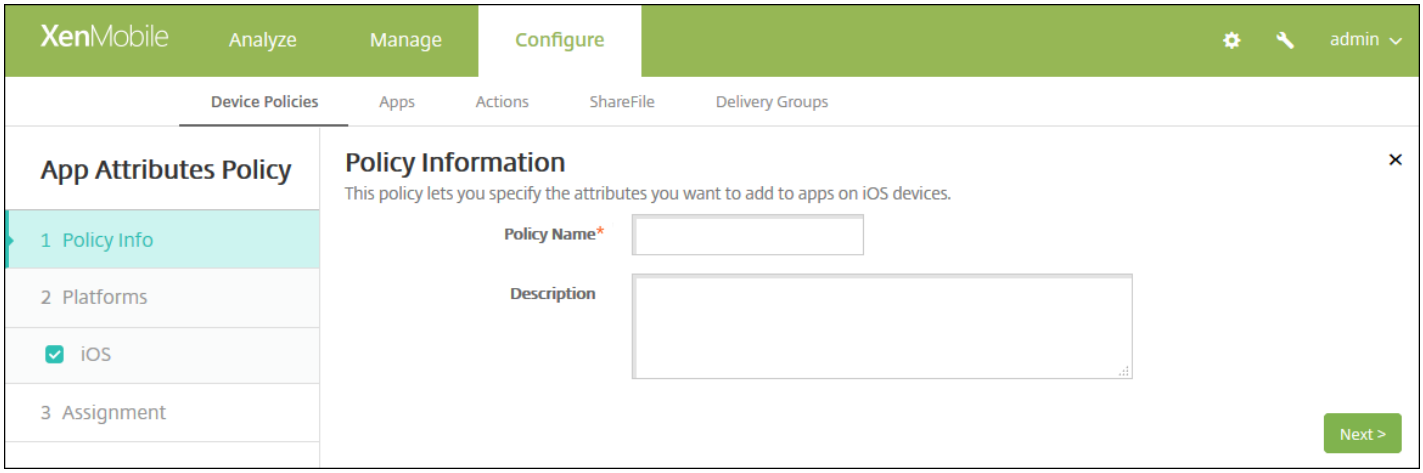
Mar 07, 2017

La directiva Atributos de aplicaciones permite especificar atributos (por ejemplo, un ID de paquete de aplicación administrada o un identificador de red VPN para cada aplicación) para dispositivos 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**.

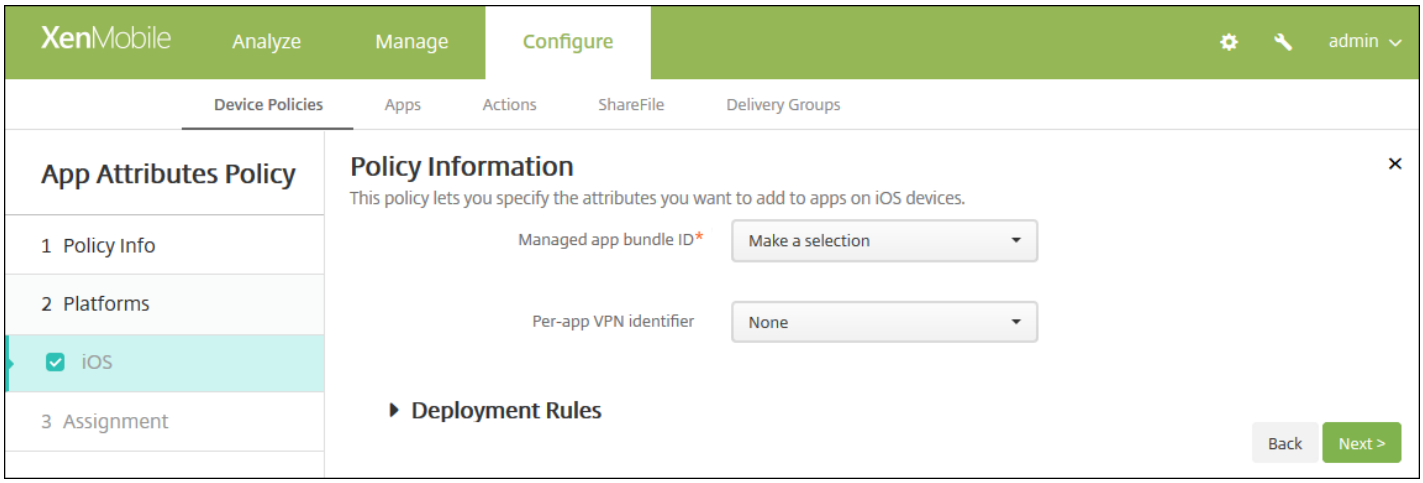
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **App Attributes**. Aparecerá la página de información **App Attributes Policy**.



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 la directiva App Attributes.

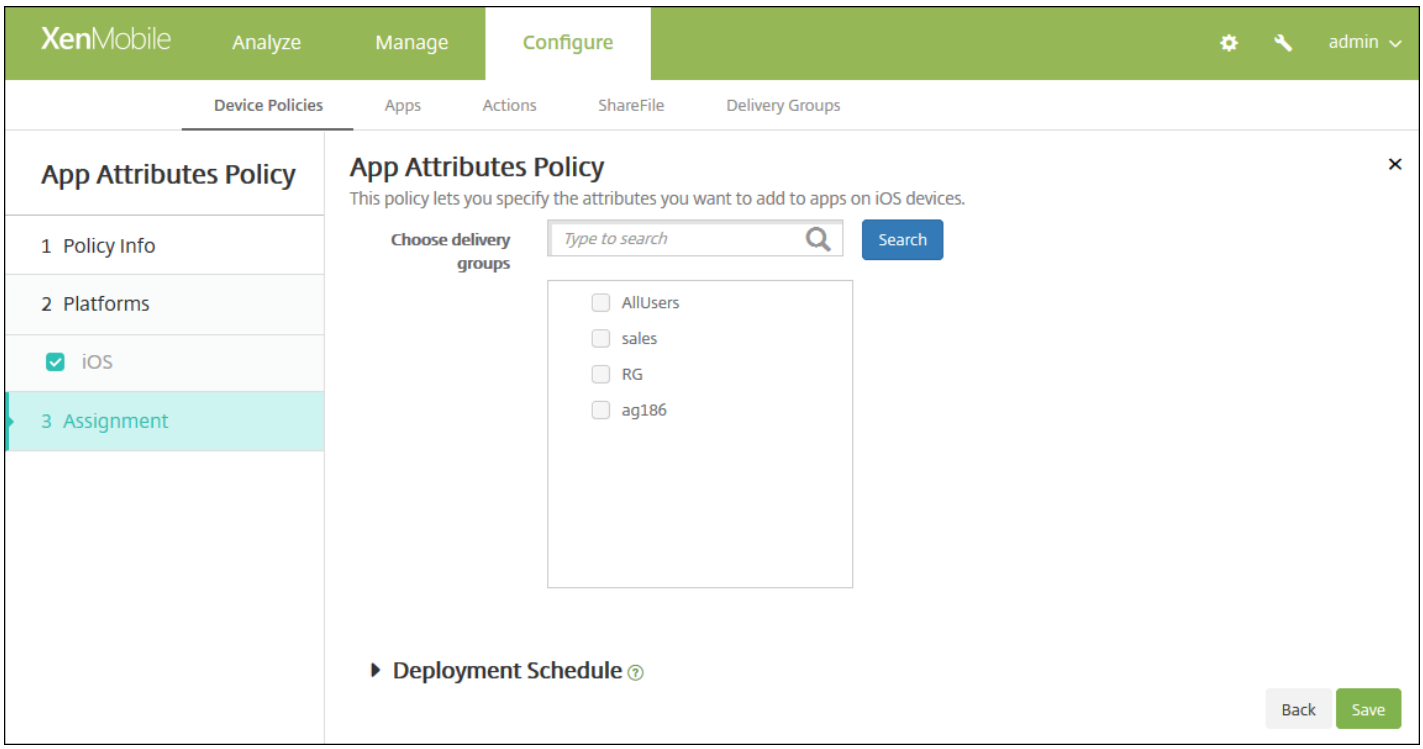


6. Configure estos parámetros:

- **Managed app bundle ID**. En la lista, haga clic en un ID del 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 para buscar un grupo de entrega. O bien, seleccione uno o varios grupos de la lista para asignarles 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 bien, haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no necesita configurar más opciones.
- 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 si se configura la clave de implementación en segundo plano para la programación desde 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

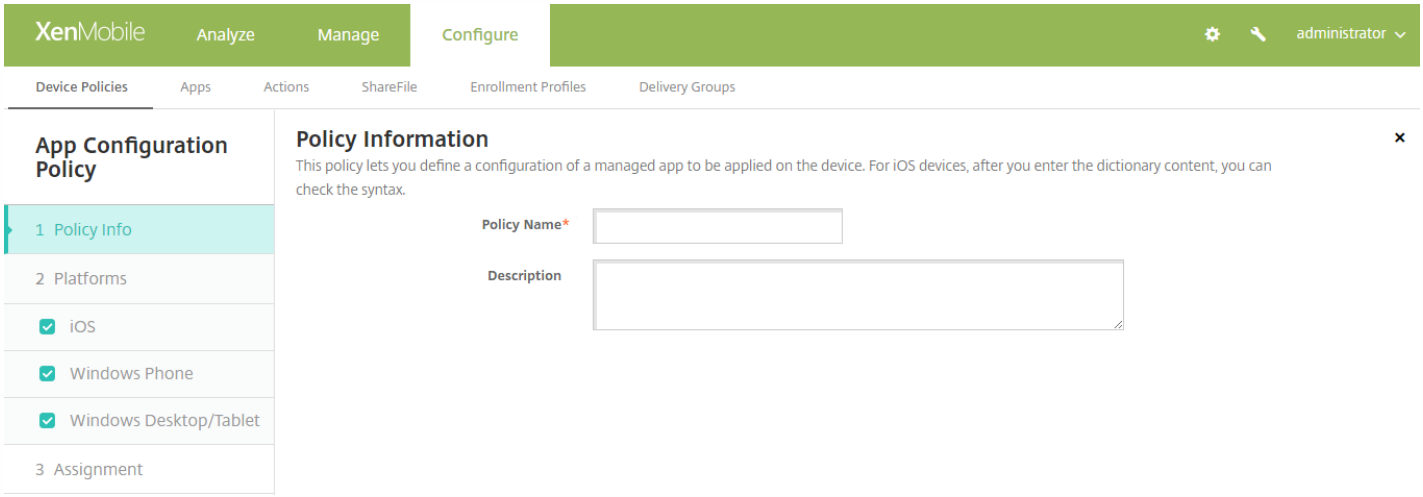
Feb 27, 2017

Puede configurar, de forma remota, aplicaciones que admitan la configuración administrada. Para ello, implemente un archivo XML de configuración (denominado "lista de propiedades" o "plist") en los dispositivos iOS de los usuarios o los pares de clave y valor en los dispositivos de teléfono, tableta o escritorio con Windows 10. La configuración permite especificar varios parámetros y comportamientos de la aplicación. XenMobile envía la configuración a los dispositivos cuando los usuarios instalan 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:

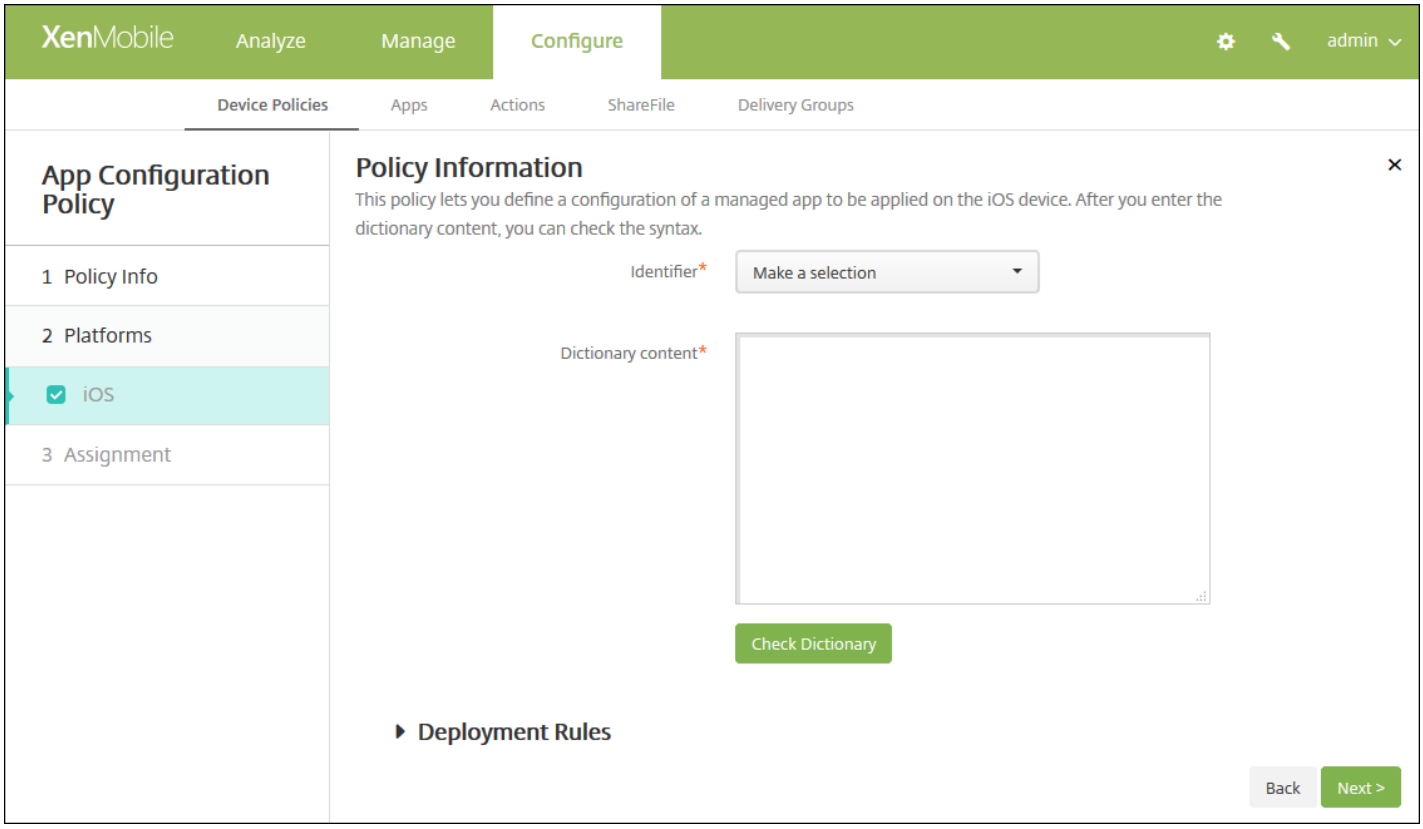
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

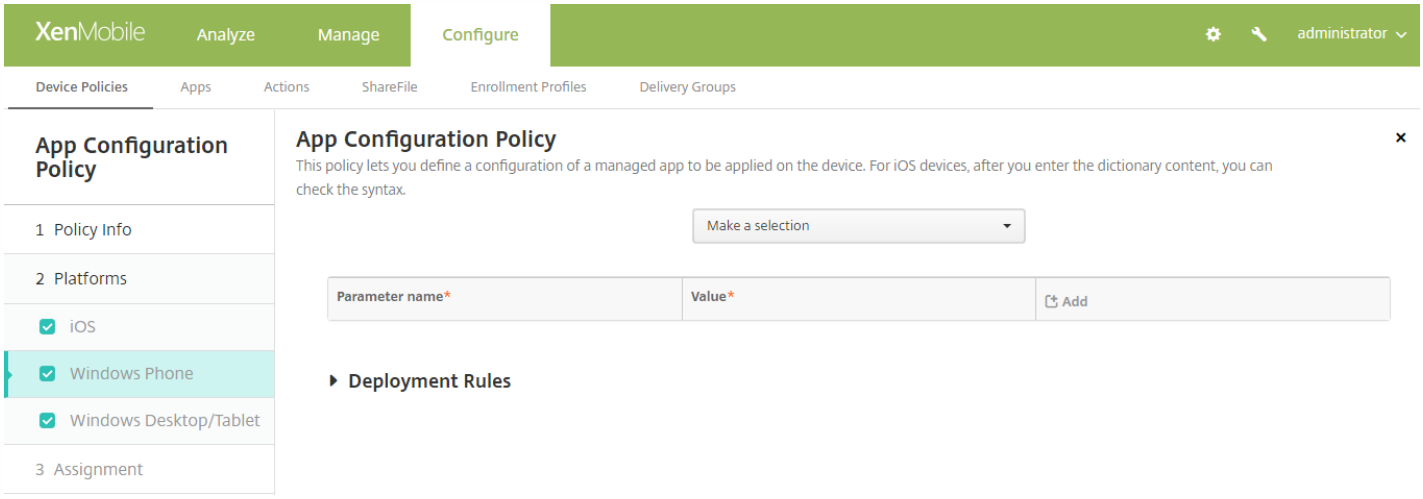
   En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

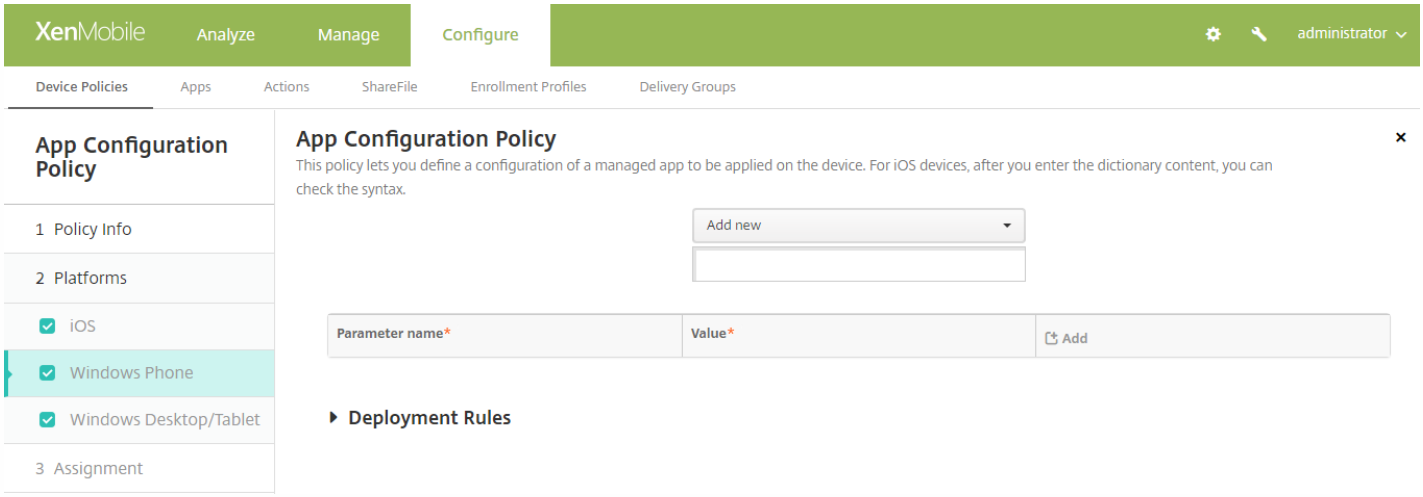
   Cuando termine de configurar los parámetros de configuración de una plataforma, consulte el paso 6 para configurar las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



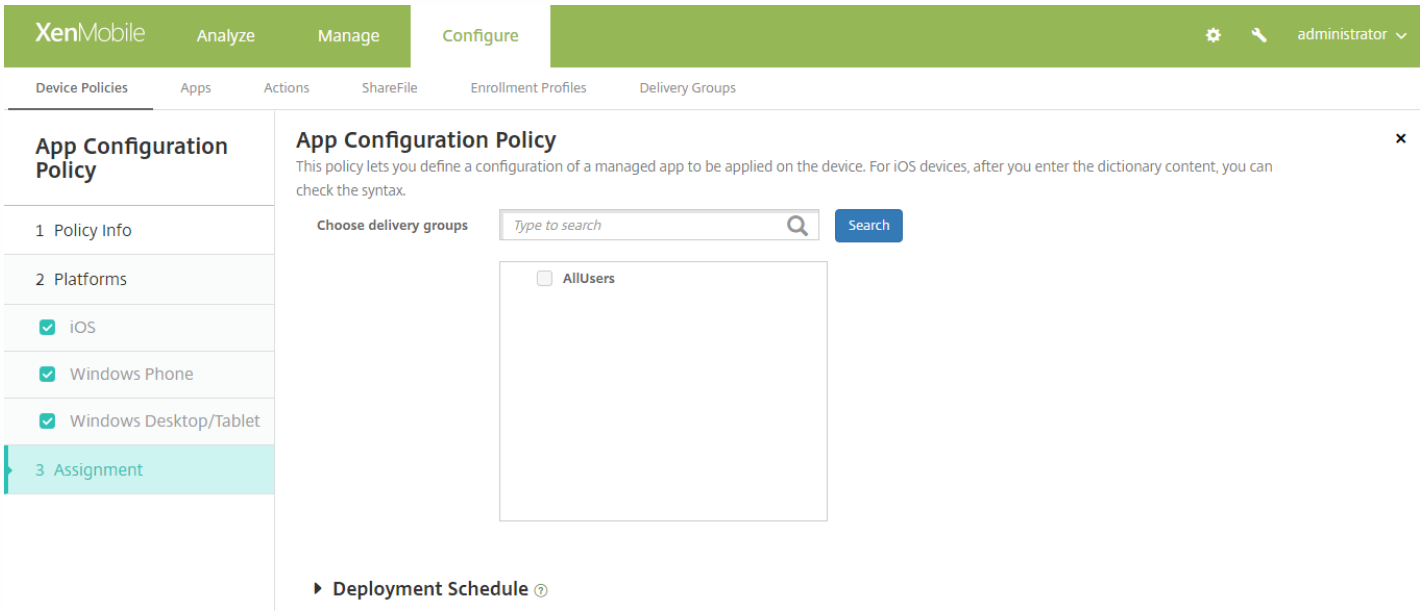
Configuración de los parámetros de teléfonos, escritorios o tabletas Windows





6. Configure las reglas de implementación.

7. Haga clic en **Next**. Aparecerá la página de asignación **App Configuration Policy**.



8. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

9 Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

10. Haga clic en **Save**.

Directiva de inventario de aplicaciones

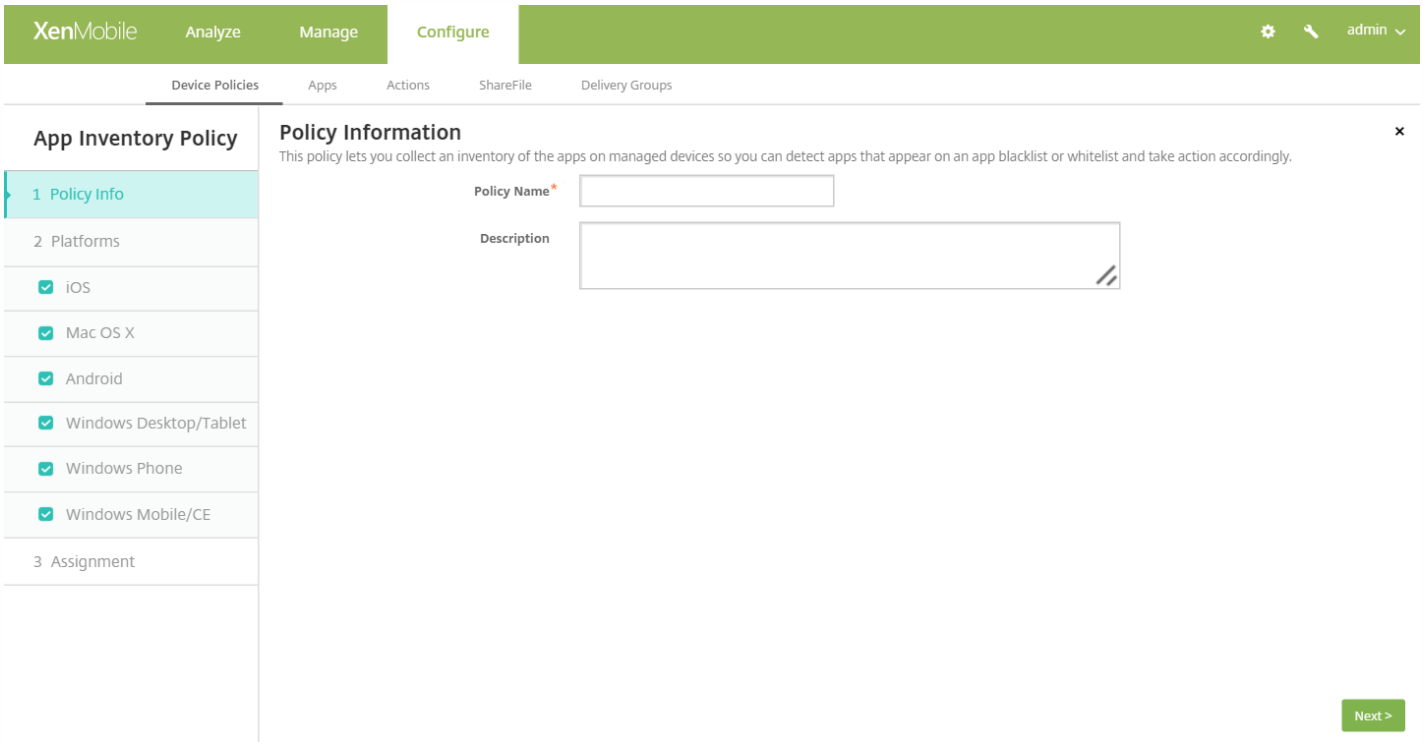
Feb 27, 2017

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 a aplicaciones) o en la lista de aplicaciones permitidas (requeridas en una directiva de acceso a 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.

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**.

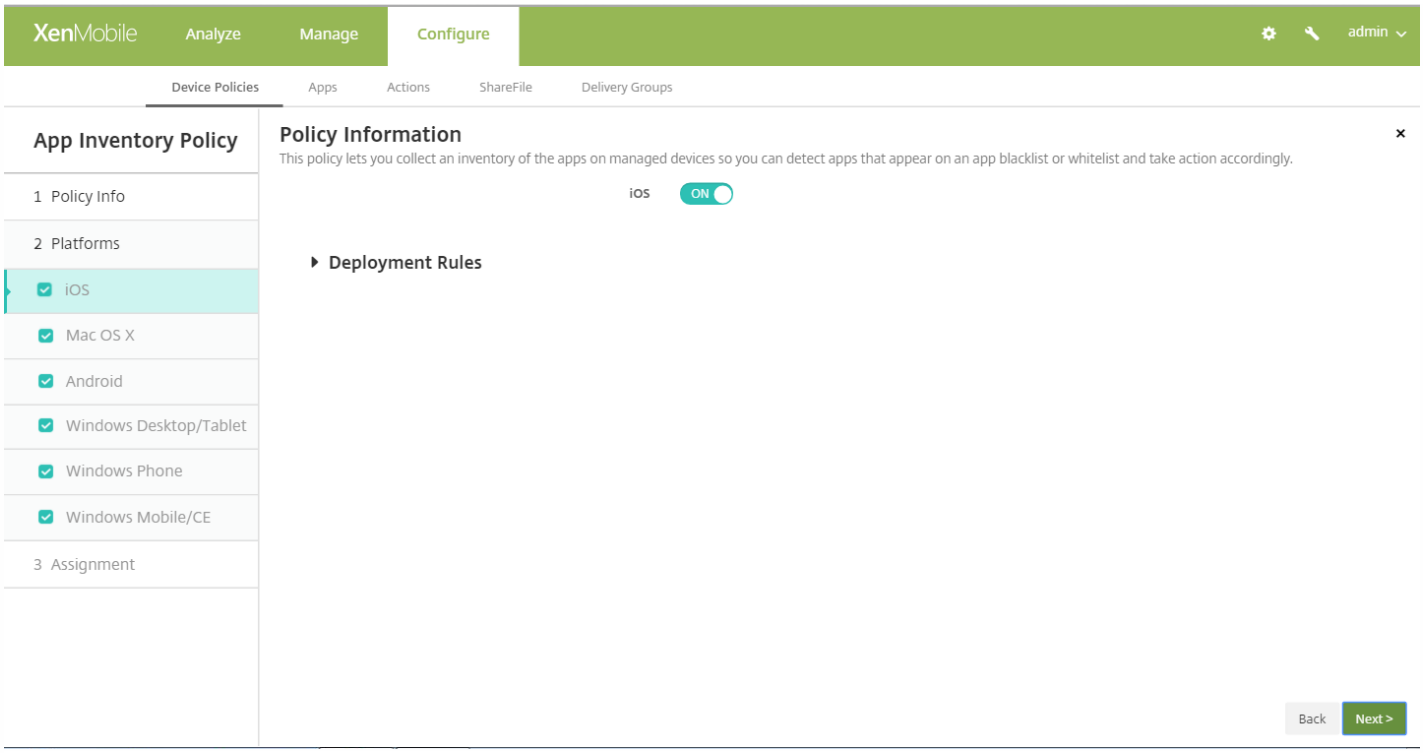
3. Expanda **More** y, en **Apps**, haga clic en **App Inventory**. Aparecerá la página **App Inventory Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



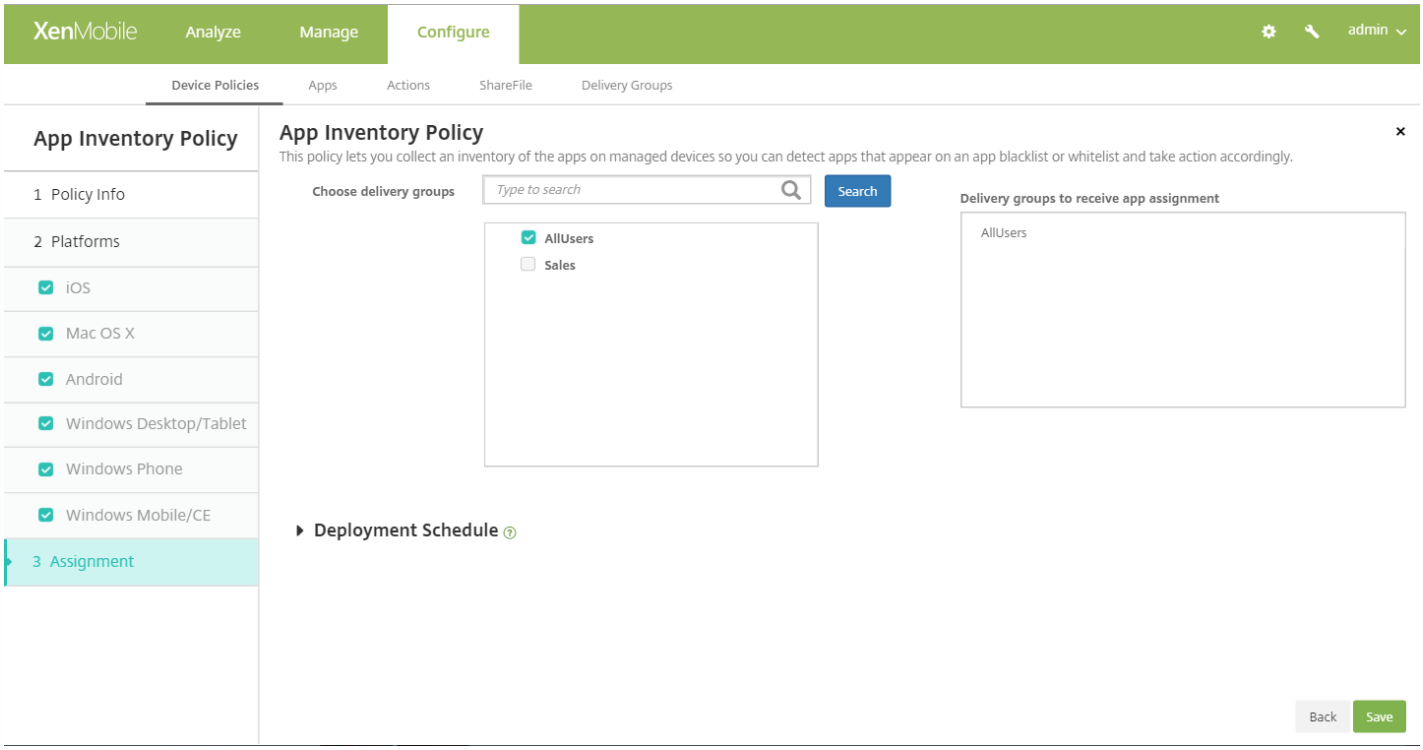
En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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.

Nota:

- Esta opción se aplica si se configura la clave de implementación en segundo plano para la programación desde **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 bloqueo de aplicaciones

Feb 27, 2017

En XenMobile, puede crear una directiva para definir una lista de las aplicaciones que se permite ejecutar en un dispositivo, o bien 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 directiva. Lo que significa que los usuarios solo pueden usar su dispositivo para ejecutar una sola aplicación. Por tanto, 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.

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.

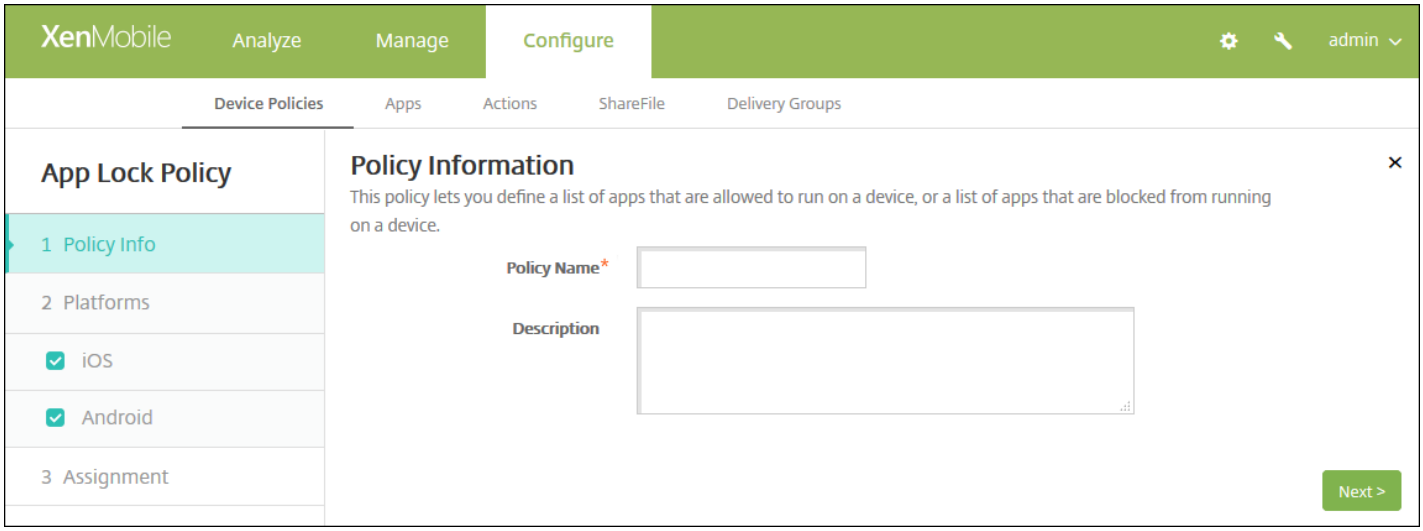
Configuración de iOS

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:

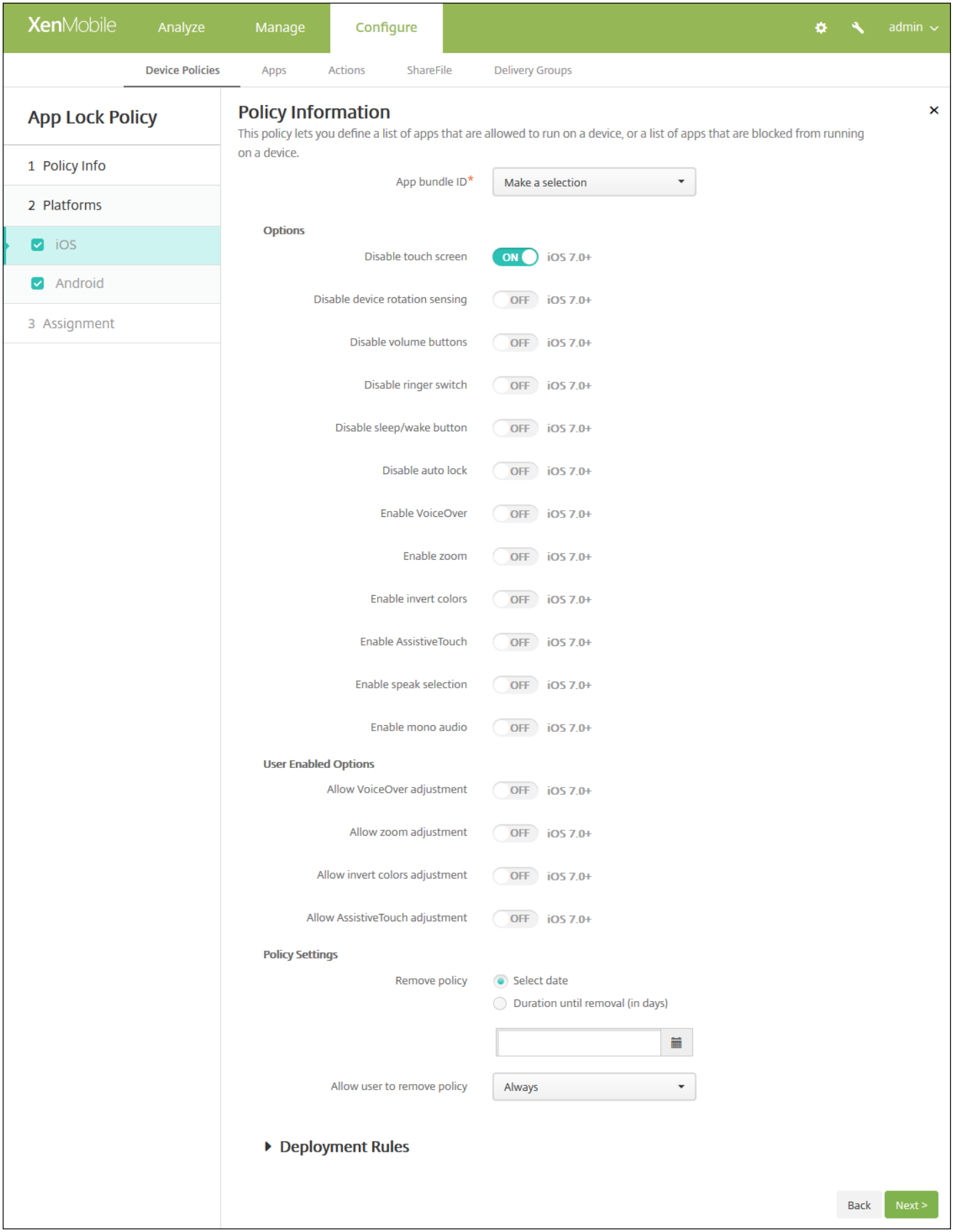
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

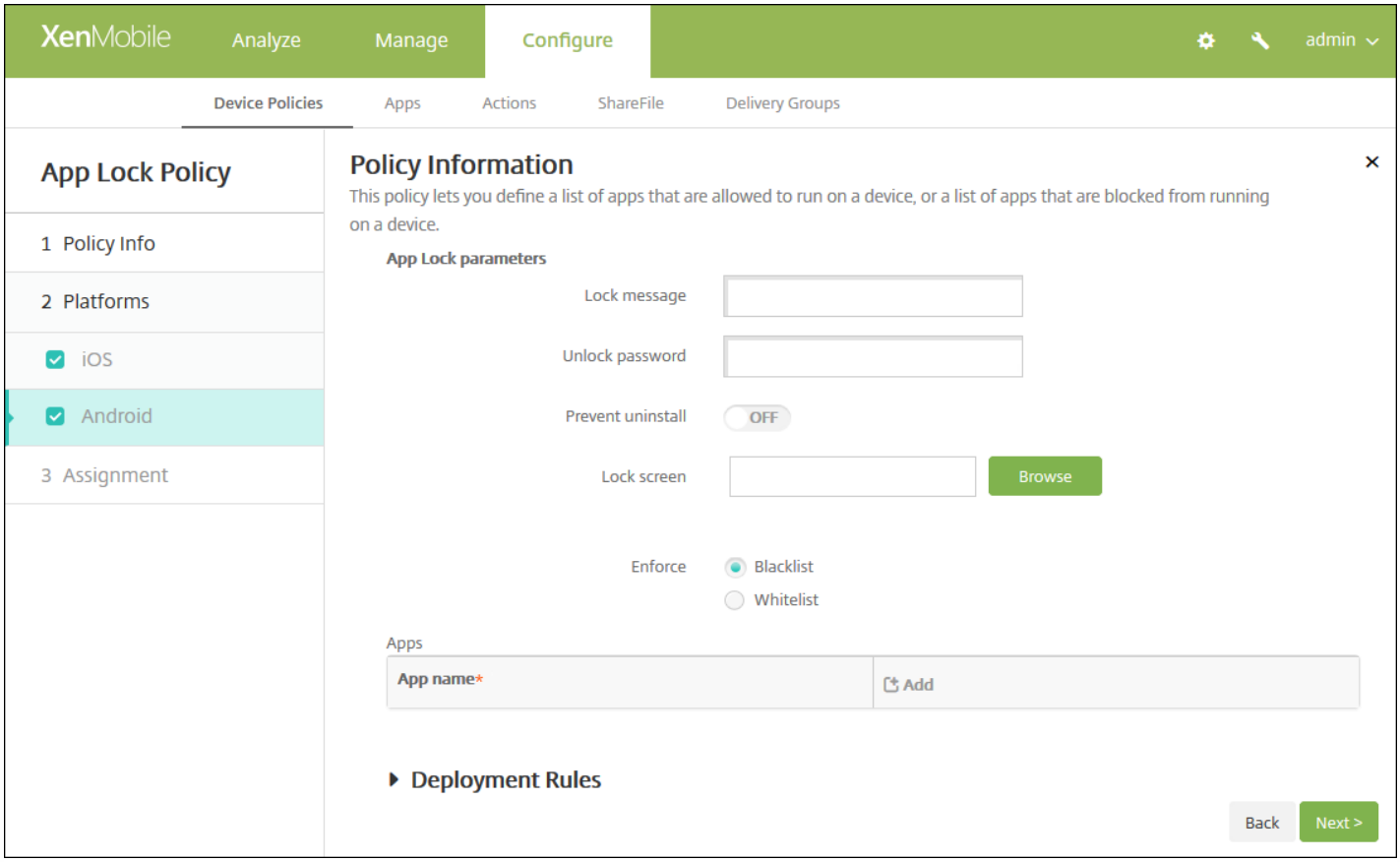
Configuración de los parámetros de iOS



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** (Opciones). Todas las opciones siguientes solo se aplican a iOS 7.0 o versiones posteriores. El valor predeterminado de todas ellas es **OFF**, excepto 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 (Inhabilitar bloqueo automático)
  - Disable VoiceOver (Habilitar 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)
- **User Enabled Options** (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**
  - - 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:

- **Parámetros de bloqueo de aplicaciones**
  - **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 las aplicaciones que no se pueden ejecutar en los dispositivos, o bien haga clic en **Whitelist** para crear una lista de las 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.

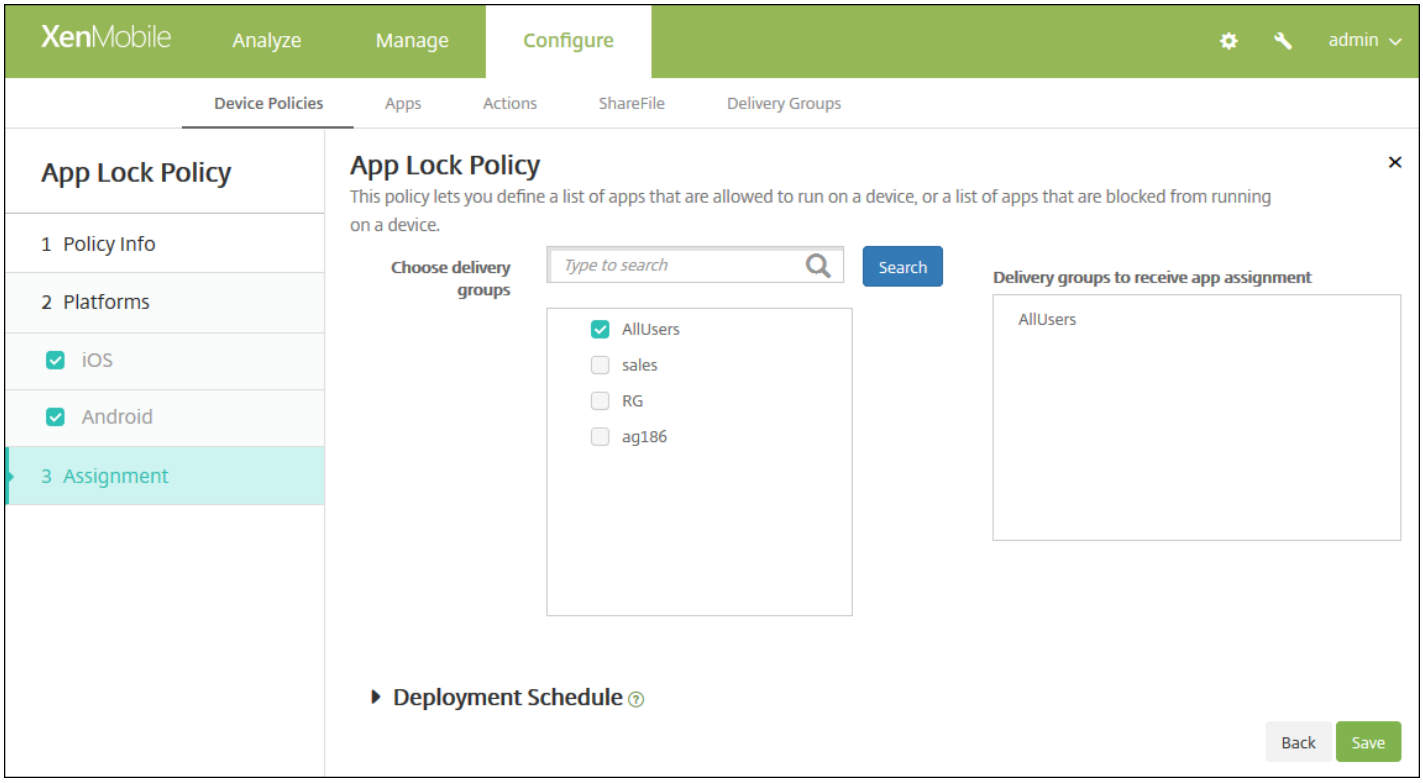
    Nota: Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para 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

guardarlos, o bien en **Cancel** para descartarlos.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **App Lock Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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

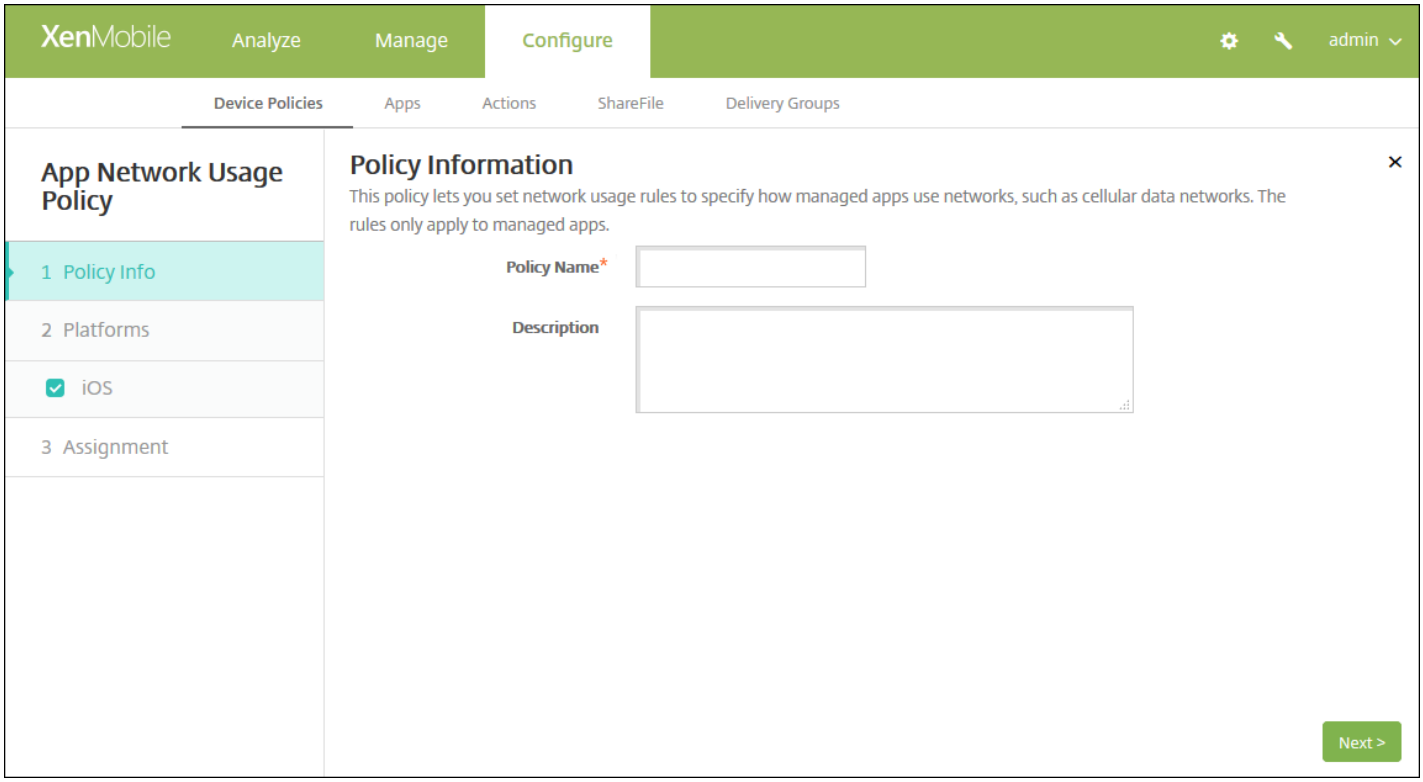
Feb 27, 2017

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**.

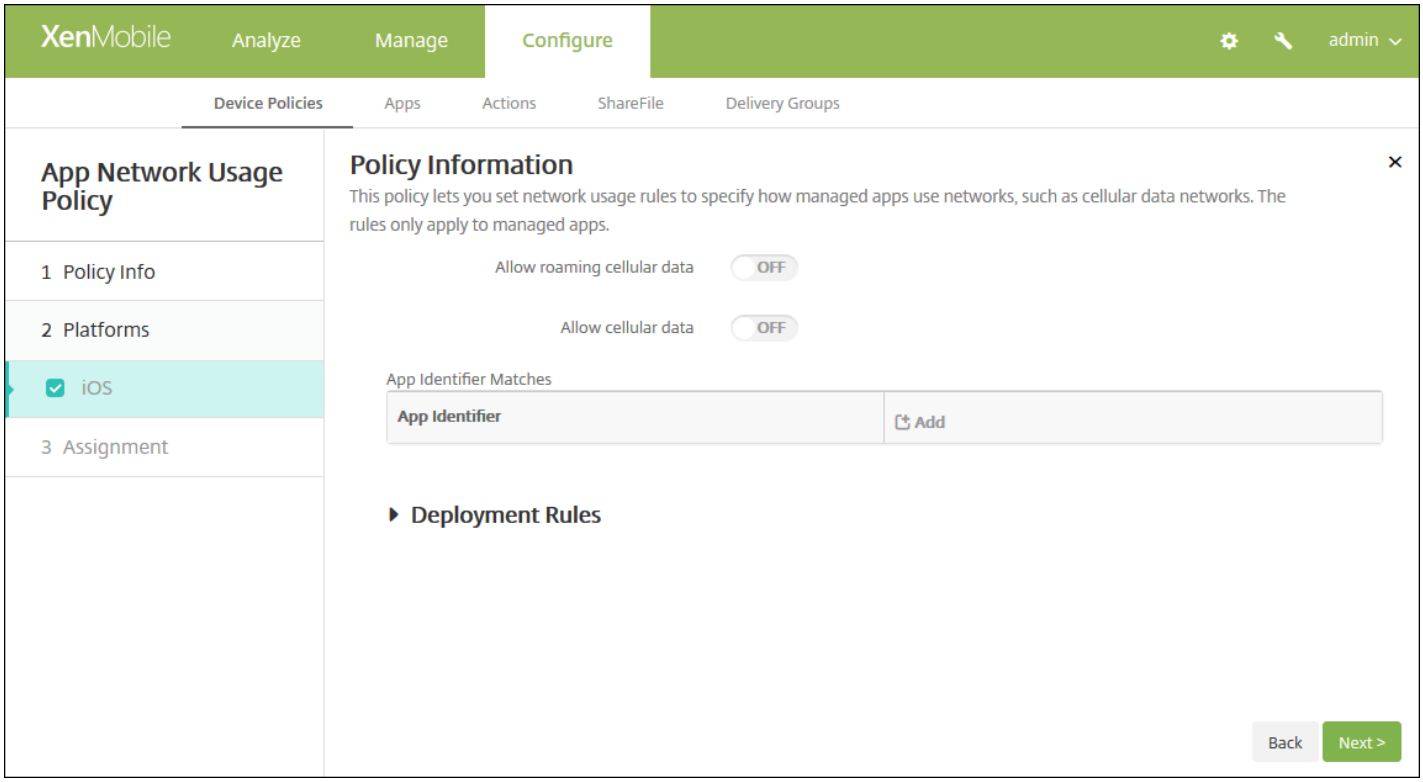
3. Expanda **More** y luego, en **Apps**, haga clic en **App Network Usage**. Aparecerá la página de información **App Network Usage Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



6. Configure estos parámetros.

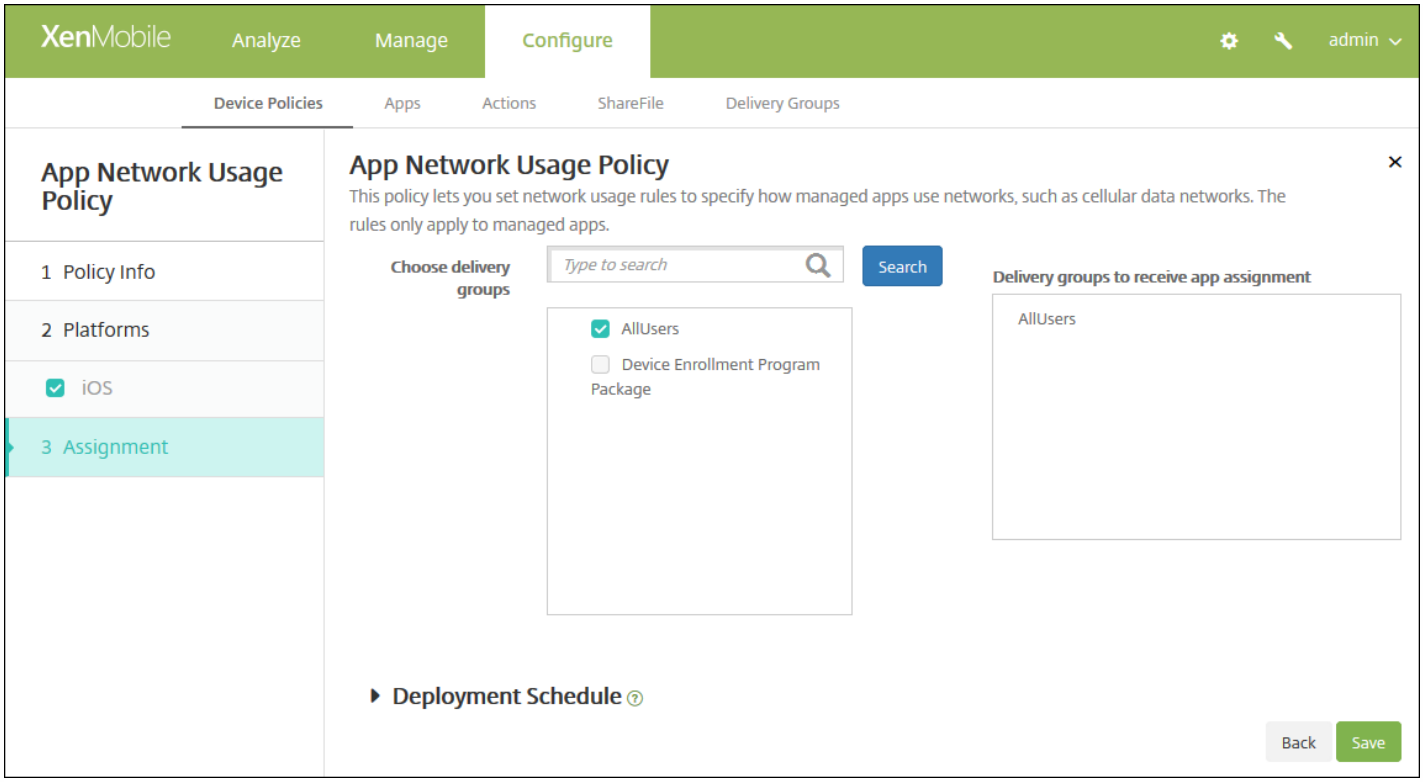
- **Allow roaming cellular data**. Seleccione si las aplicaciones indicadas pueden usar una conexión de datos móviles durante el roaming. El valor predeterminado es **OFF**.
- **Allow cellular data**. Seleccione si las aplicaciones especificadas pueden usar la conexión de datos móviles. El valor predeterminado 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 guardarlos, o bien en **Cancel** para descartarlos.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **App Network Usage Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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

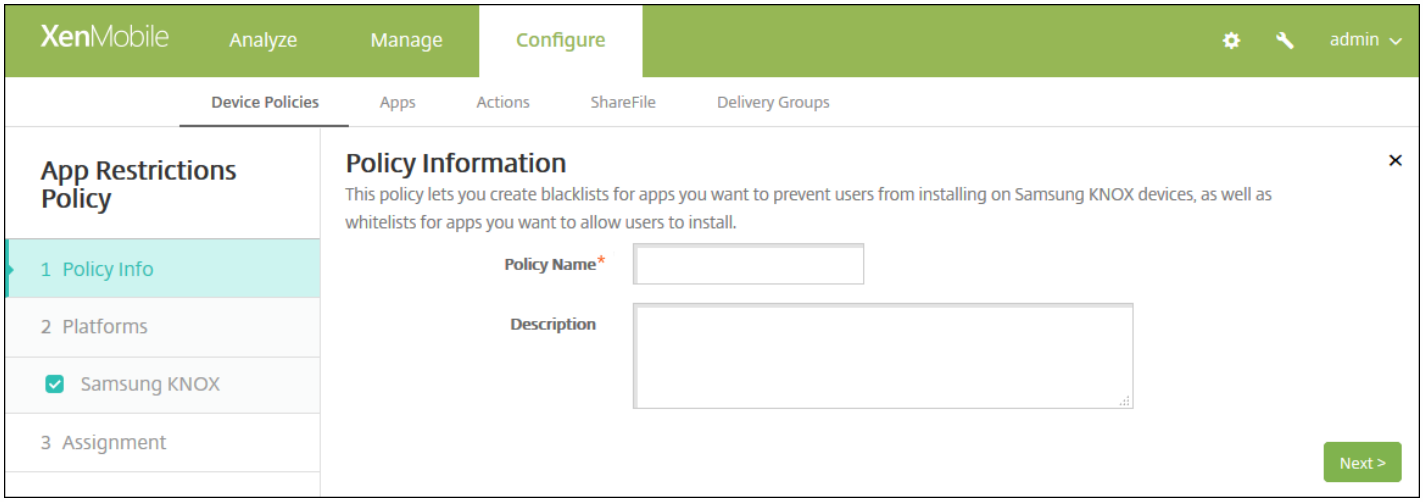
Feb 27, 2017

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**.

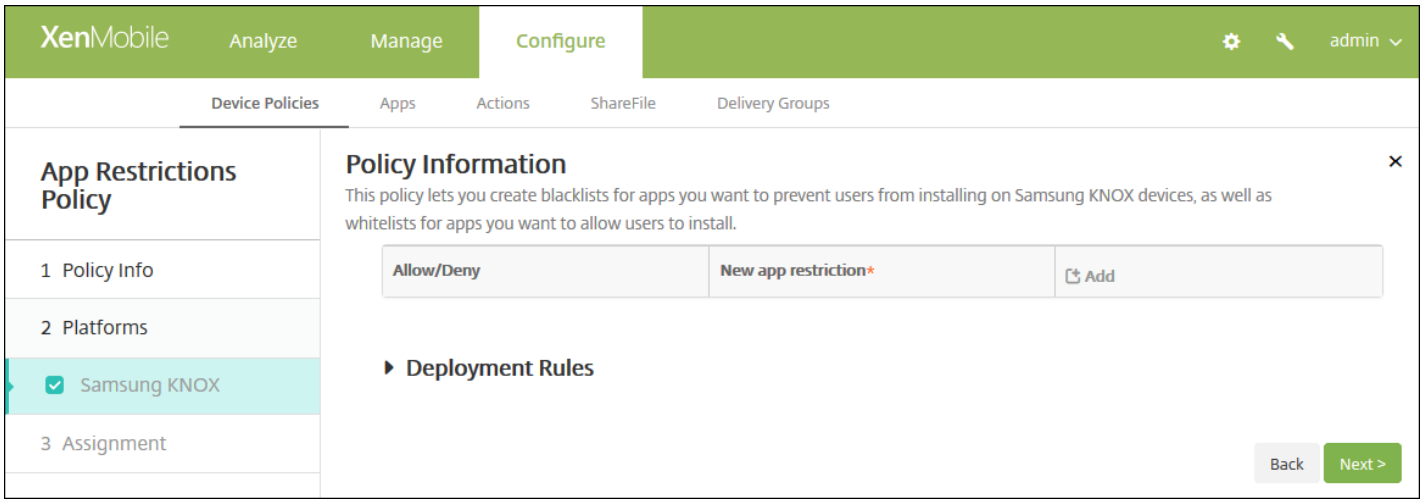
3. Expanda **More** y, a continuación, en **Security**, haga clic en **App Restrictions**. Aparecerá la página de información **App Restrictions Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Samsung KNOX**.



6. Para cada aplicación que quiera agregar a la lista Allow/Deny, haga clic en **Add** y lleve a cabo lo siguiente:

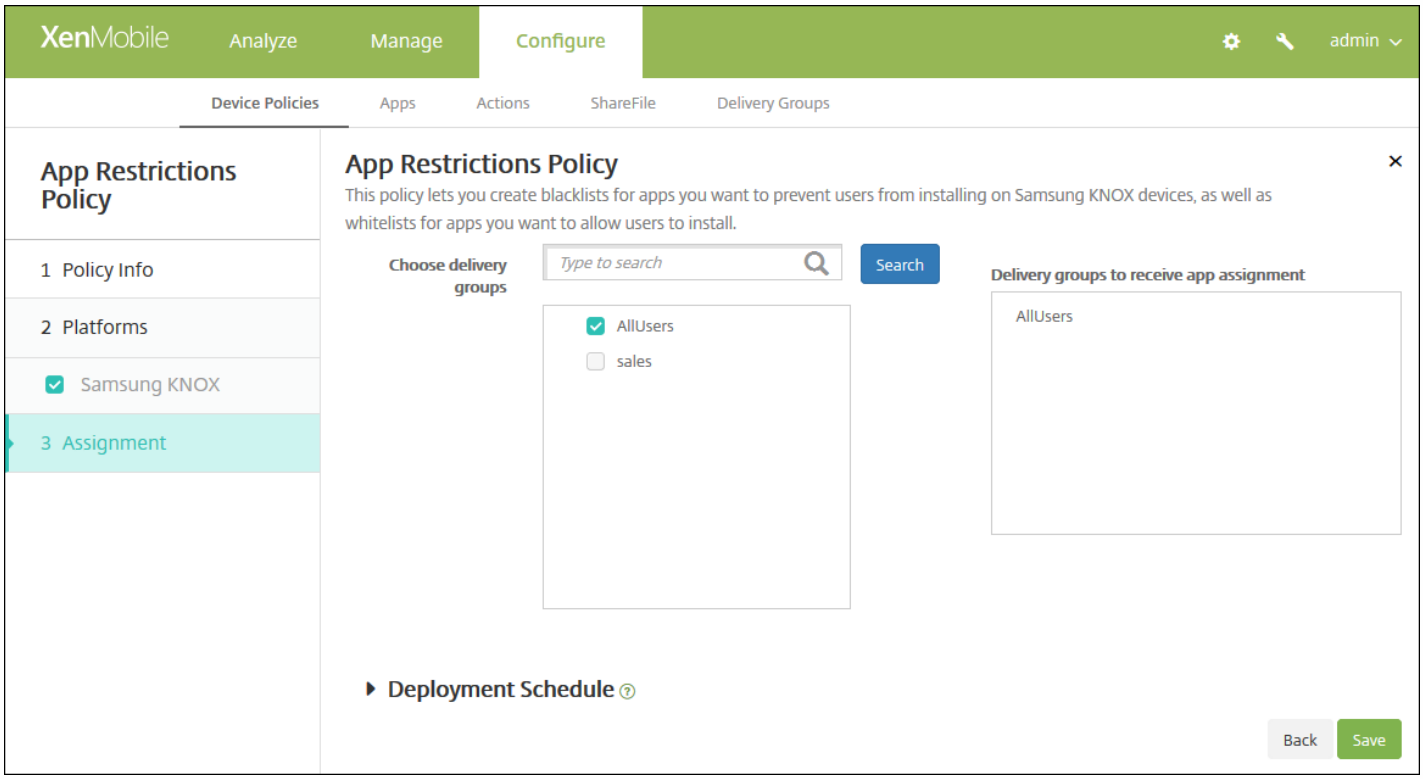
- **Allow/Deny**. Seleccione si permitir a los usuarios instalar la aplicación.
- **New app restriction**. Escriba el ID del paquete de la aplicación; por ejemplo, com.kmdm.af.crackle.
- Haga clic en **Save** para guardar la aplicación en la lista Allow/Deny, o bien haga clic en **Cancel** para no guardarla.

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 guardarlos, o bien en **Cancel** para descartarlos.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 túneles de aplicaciones

Feb 27, 2017

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.

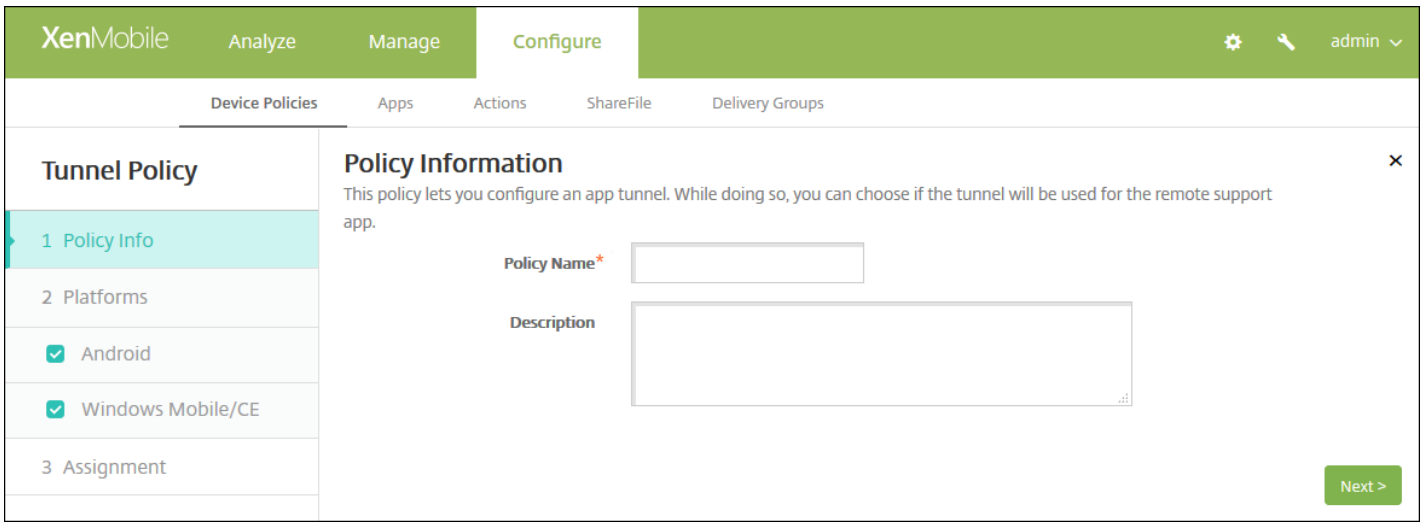
Configuración de Android

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.

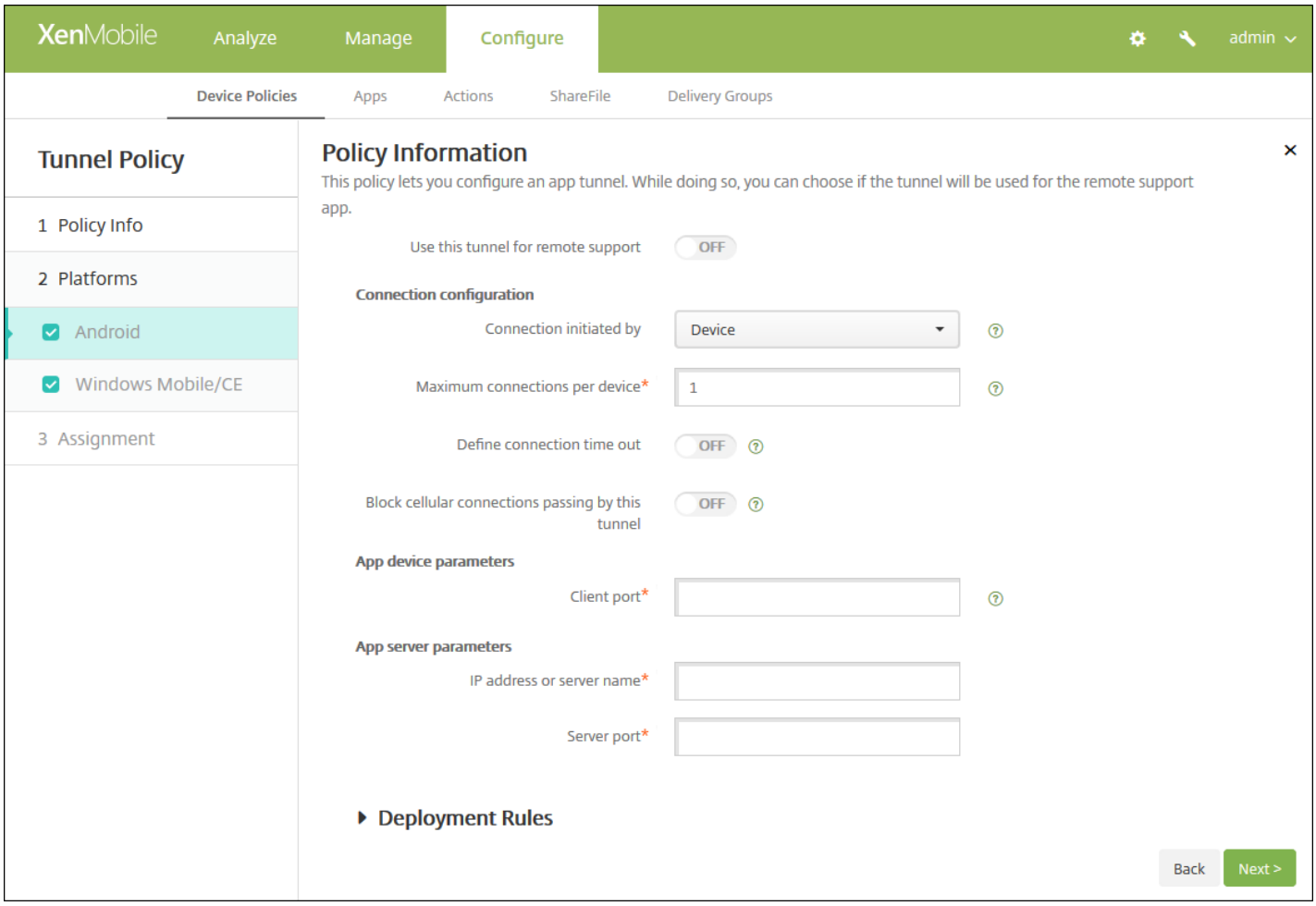
5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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 la fuente que inicia 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.

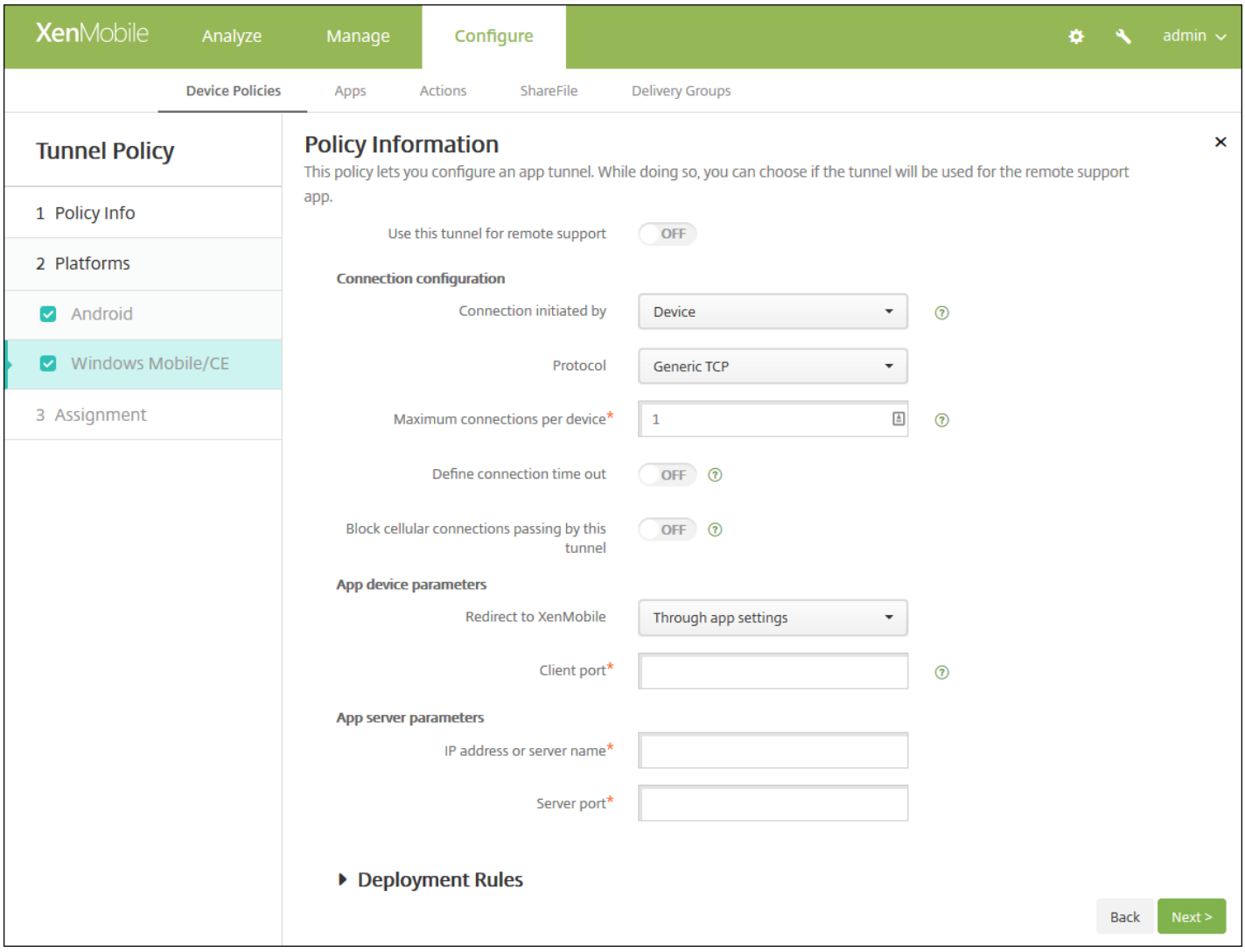
  - **Client port**. Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del

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**. Establézcalo 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 **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.

Configuración de los parámetros de Windows Mobile/CE



Configure estos parámetros:

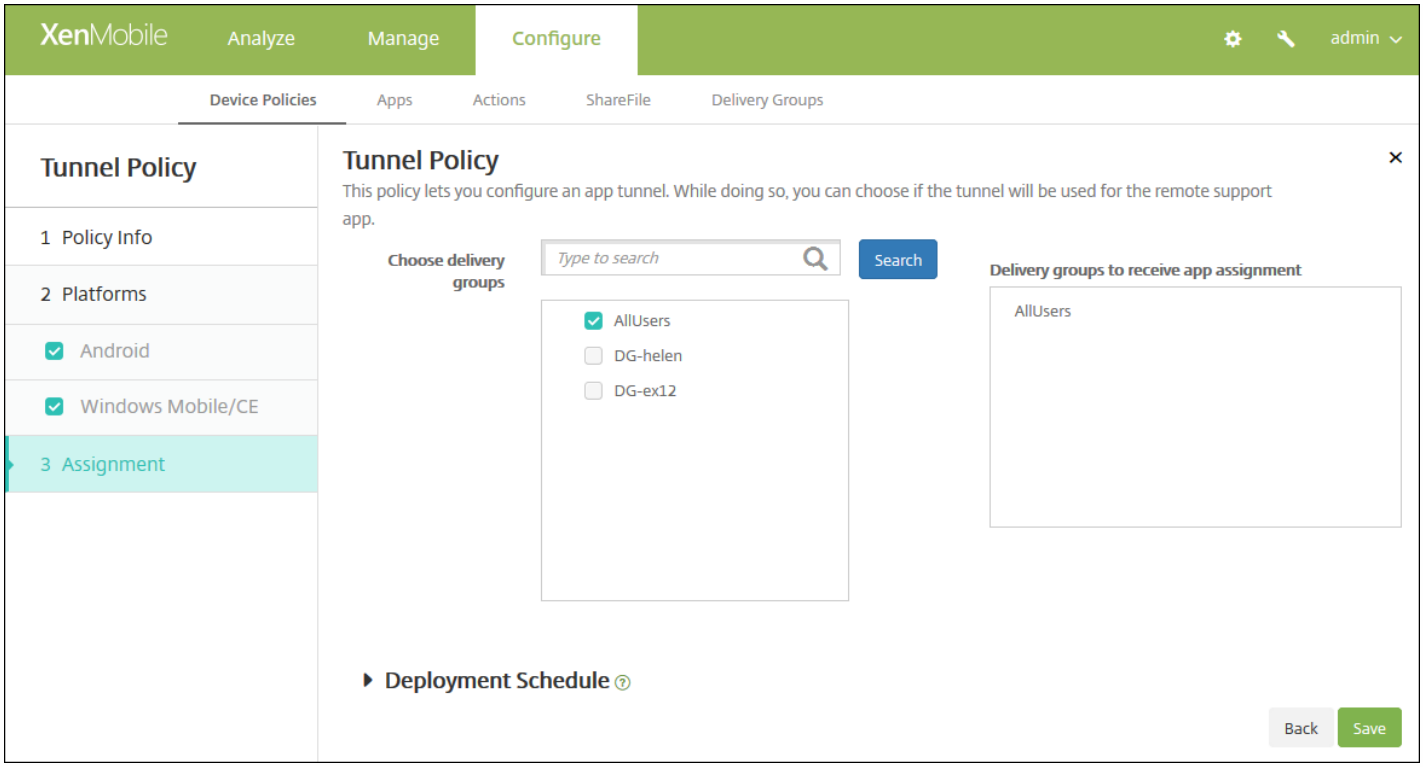
- **Use this tunnel for remote support**. Seleccione si el túnel se usará para la asistencia remota.

  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:
  - Connection **initiated by**. Haga clic en **Device** o **Server** para indicar la fuente que inicia 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**. Establézcalo 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 "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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 desinstalación de aplicaciones

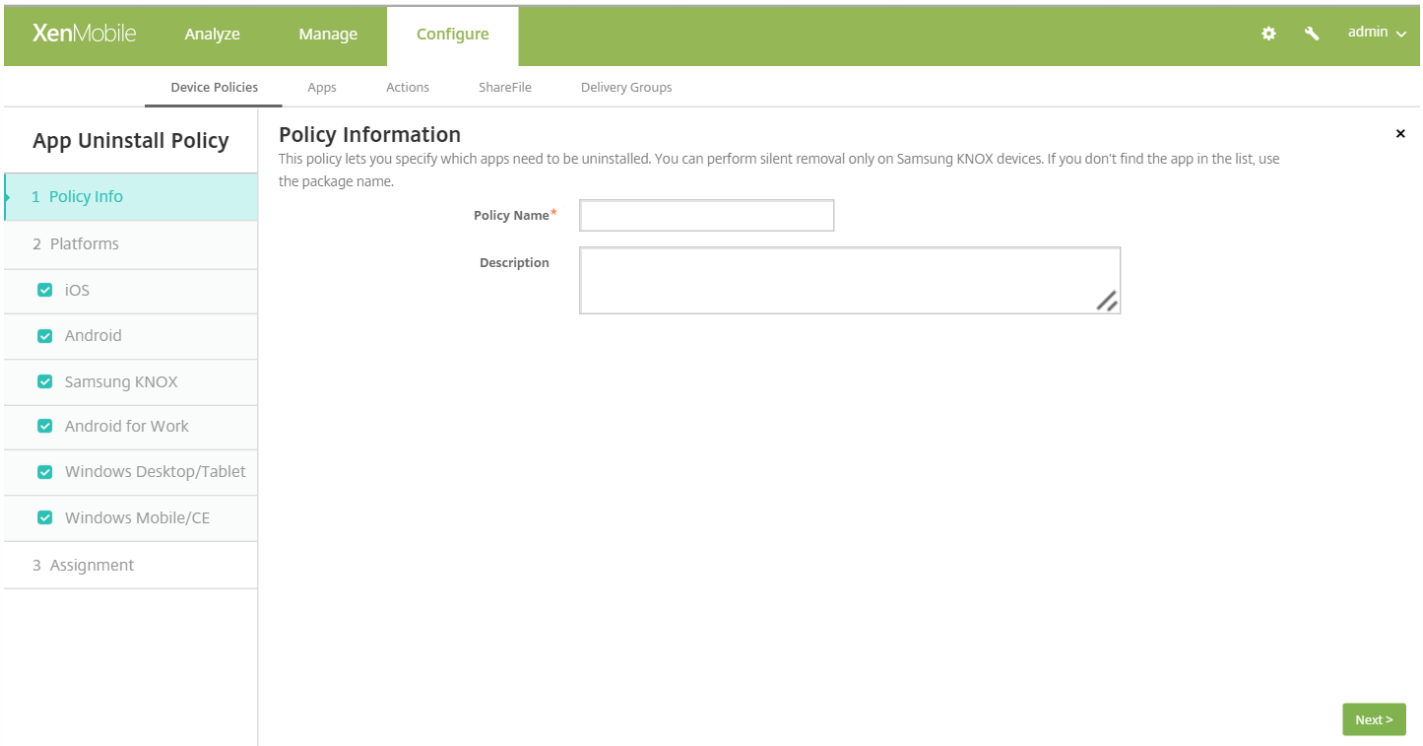
Feb 27, 2017

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**. Si quiere, escriba una descripción de la directiva.

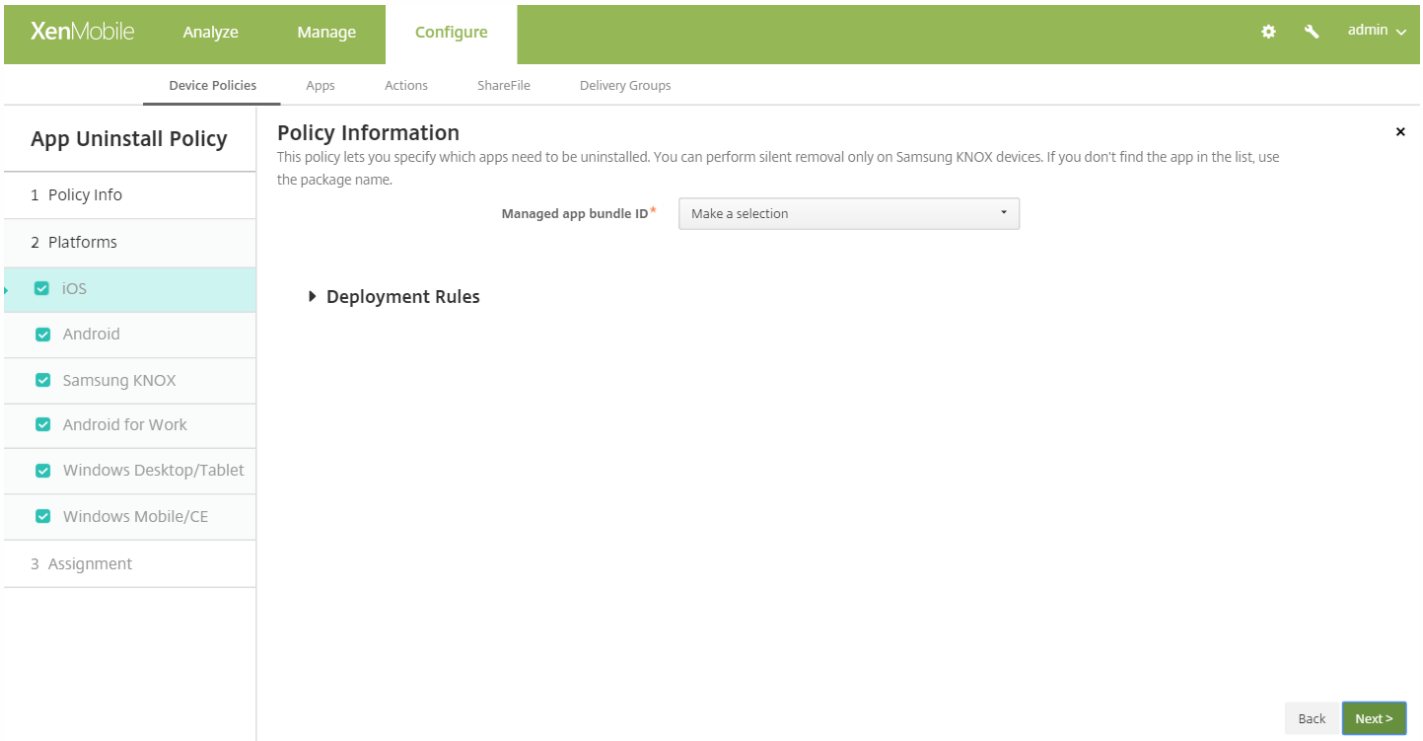
5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

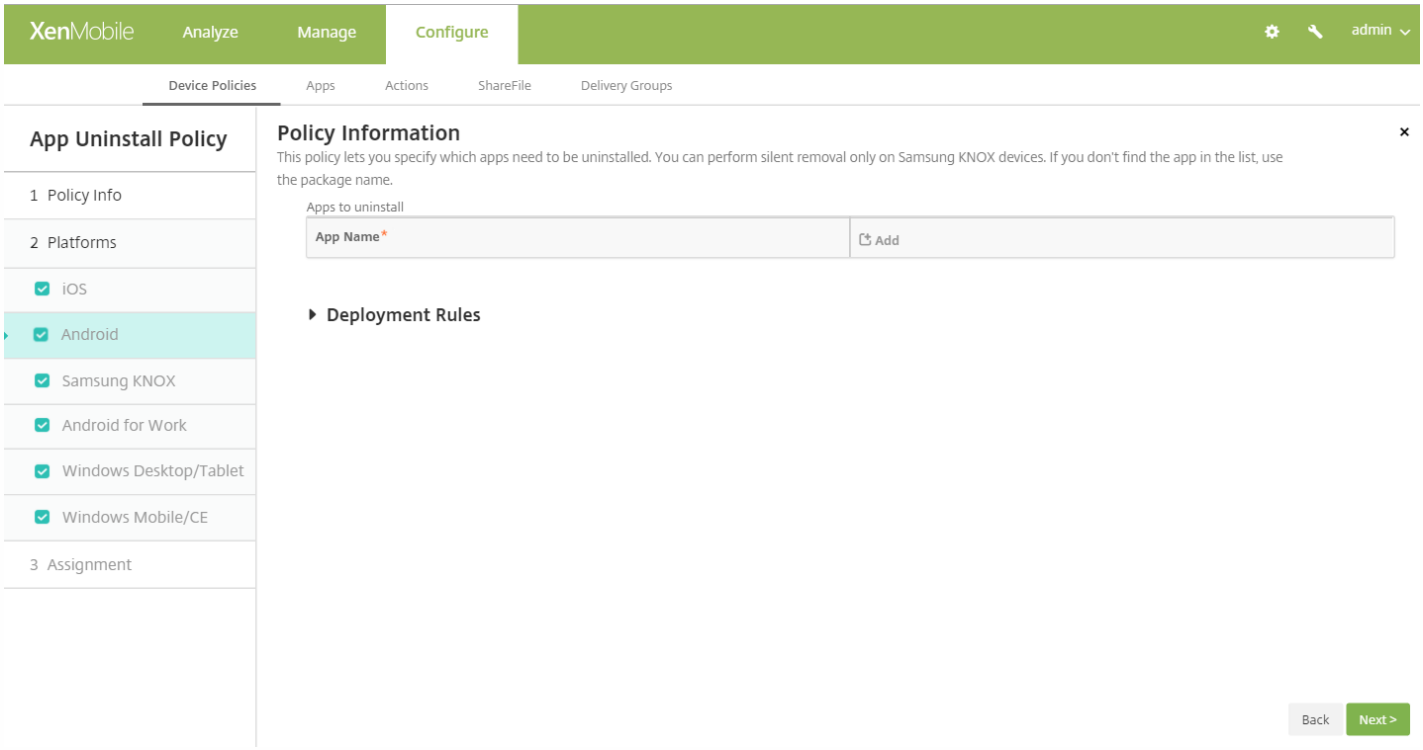
Configuración de los parámetros de iOS



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:

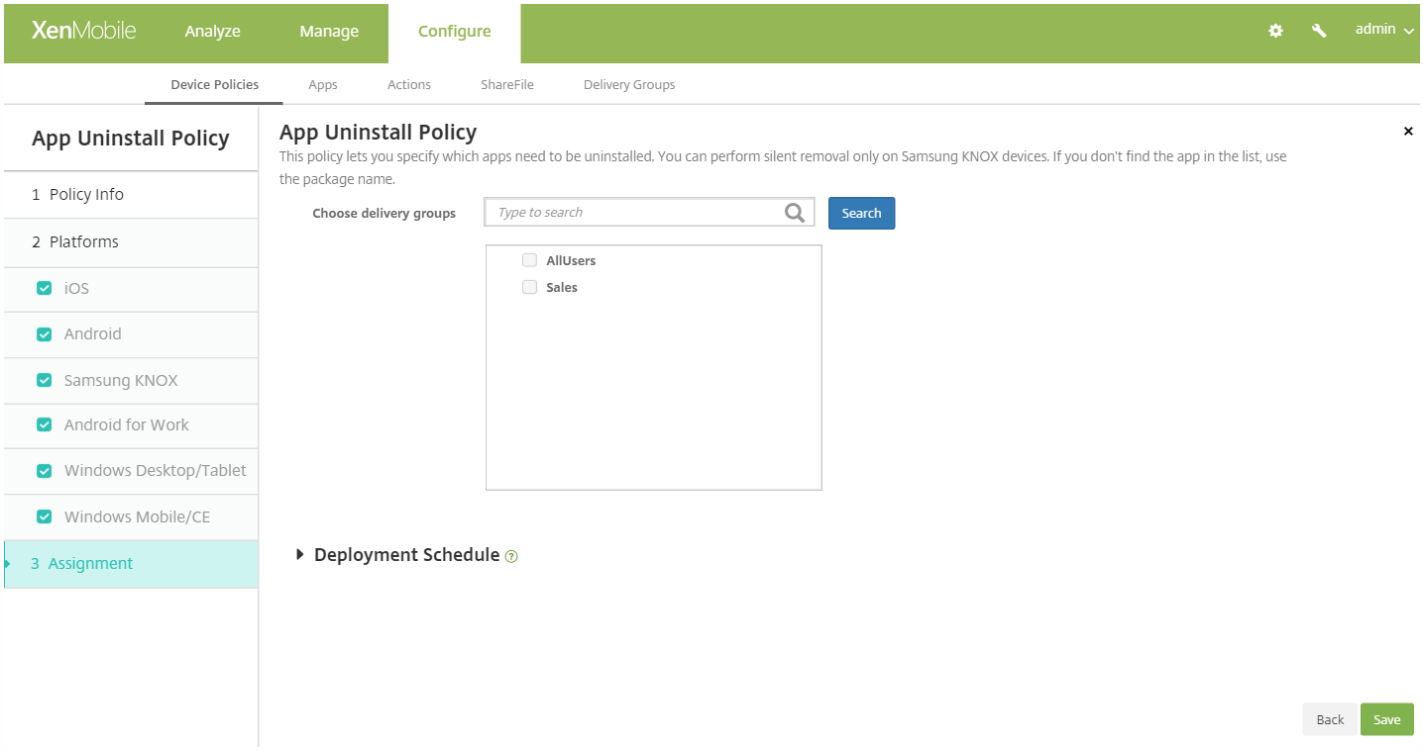
- **Apps to uninstall**. Para cada aplicación que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name**. En la lista, haga clic en una aplicación existente, o bien haga clic en **Add new** para introducir un nuevo nombre de aplicación. Si no hay ninguna aplicación configurada 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 de **App Uninstall Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 restricciones para desinstalación de aplicaciones

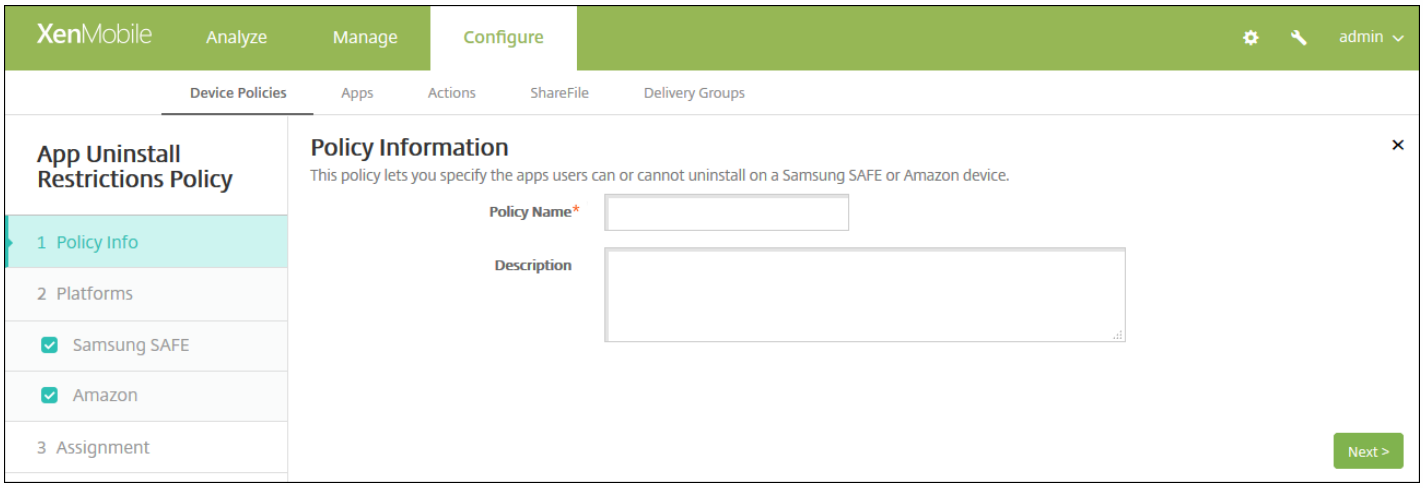
Feb 27, 2017

Puede especificar las aplicaciones que los usuarios pueden o no pueden desinstalarse de 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**.

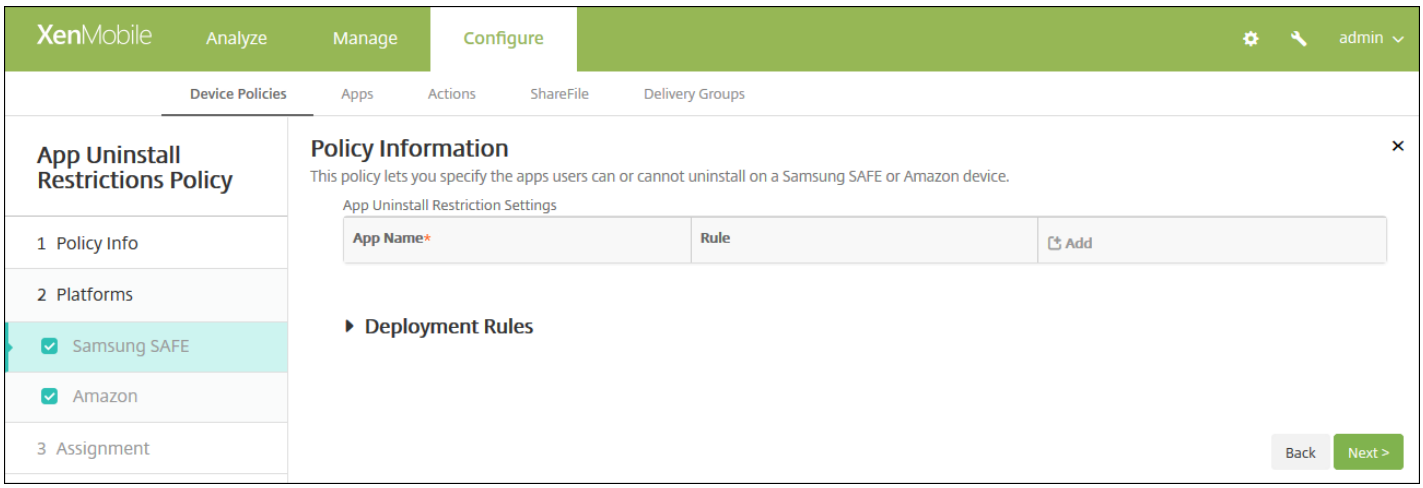
3. Expanda **More** y, en **Apps**, haga clic en **App Uninstall Restrictions**. Aparecerá la página de información **App Uninstall Restrictions Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



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:

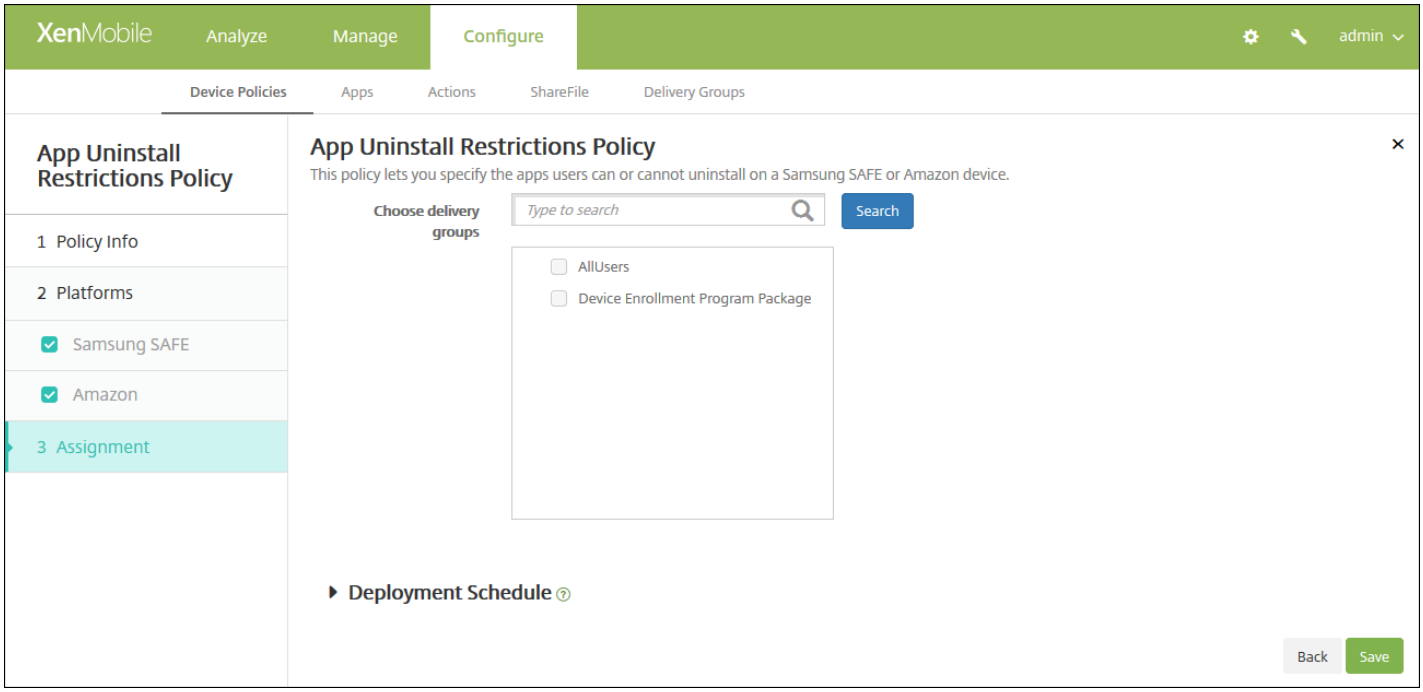
- **App Uninstall Restrictions Settings**. Para cada regla que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name**. En la lista, haga clic en una aplicación, o bien haga clic en **Add new** para introducir una nueva aplicación.
  - **Rule**. Seleccione si los usuarios pueden desinstalar la aplicación. El valor predeterminado es permitir 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 guardarlos, o bien en **Cancel** para descartarlos.

8. Configure las reglas de implementación.

9 Haga clic en **Next**. Aparecerá la página de asignación de **App Uninstall Restrictions Policy**.



10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

Directiva de exploradores Web

Feb 27, 2017

Puede crear directivas de exploradores para dispositivos Samsung SAFE y Samsung KNOX con el objetivo de definir si los dispositivos de los usuarios pueden usar el explorador, o bien, puede limitar las funciones del explorador que puedan usar los dispositivos de los usuarios.

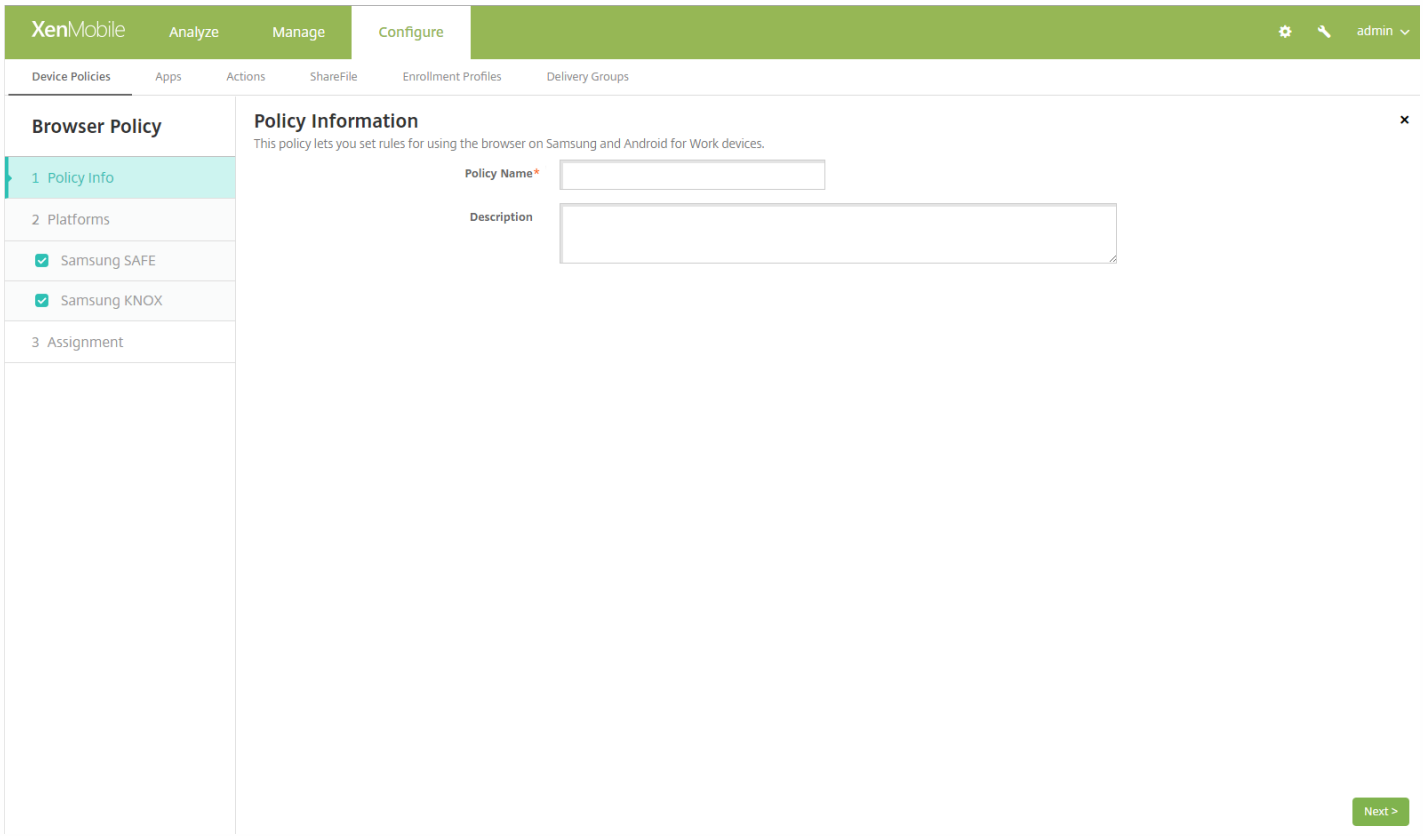
En dispositivos Samsung, puede inhabilitar completamente el explorador, puede habilitar o inhabilitar los elementos emergentes, JavaScript, las cookies, la función de completado automático, y también puede decidir si forzar advertencias de fraude.

Configuración de Samsung SAFE y Samsung KNOX

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. 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:

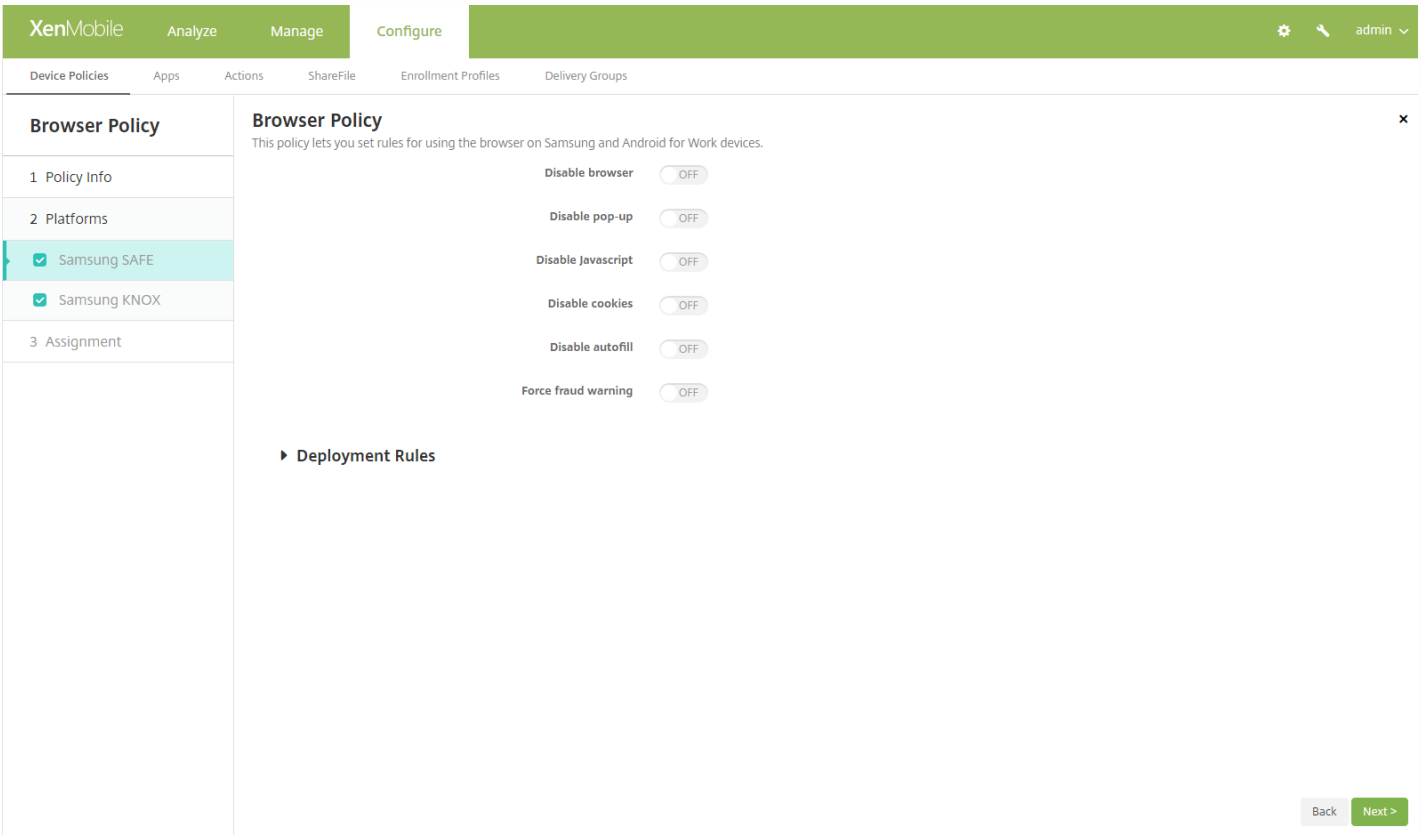
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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

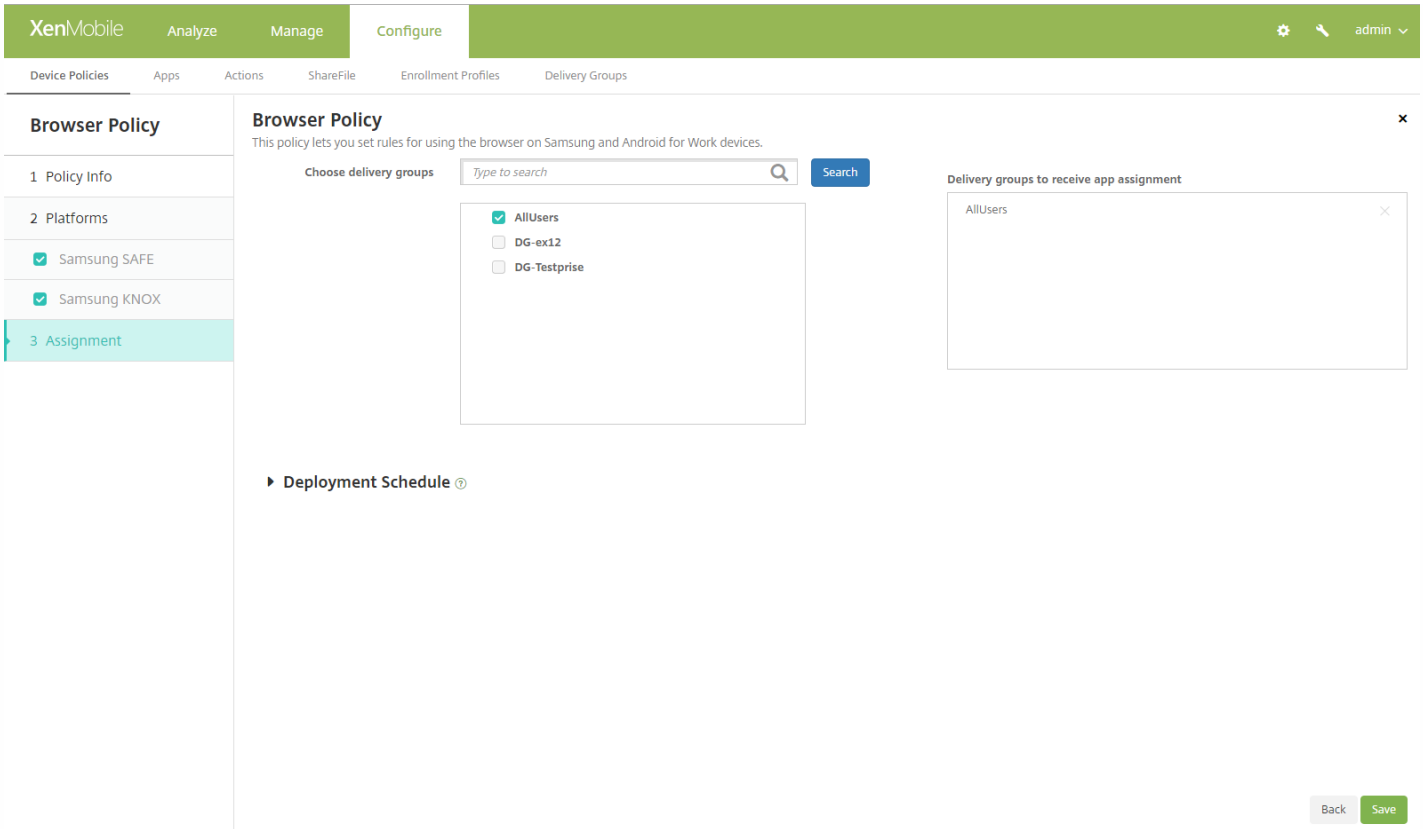


Configure estos parámetros:

- **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.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo de calendario (CalDAV)

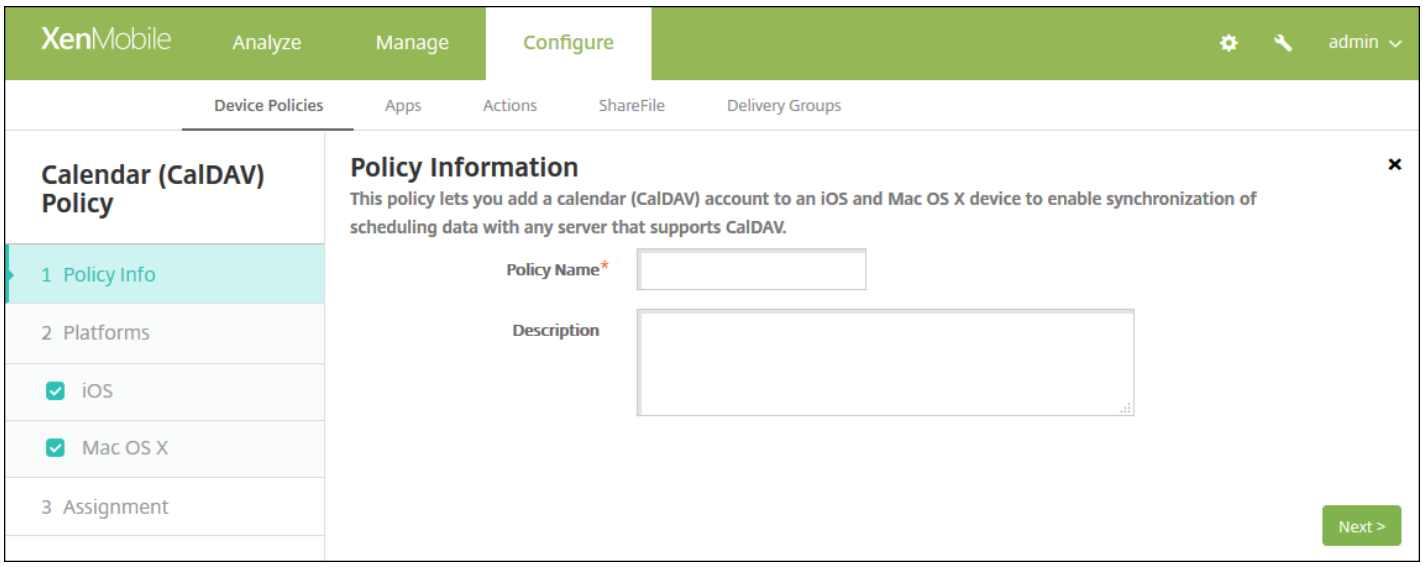
Feb 27, 2017

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:

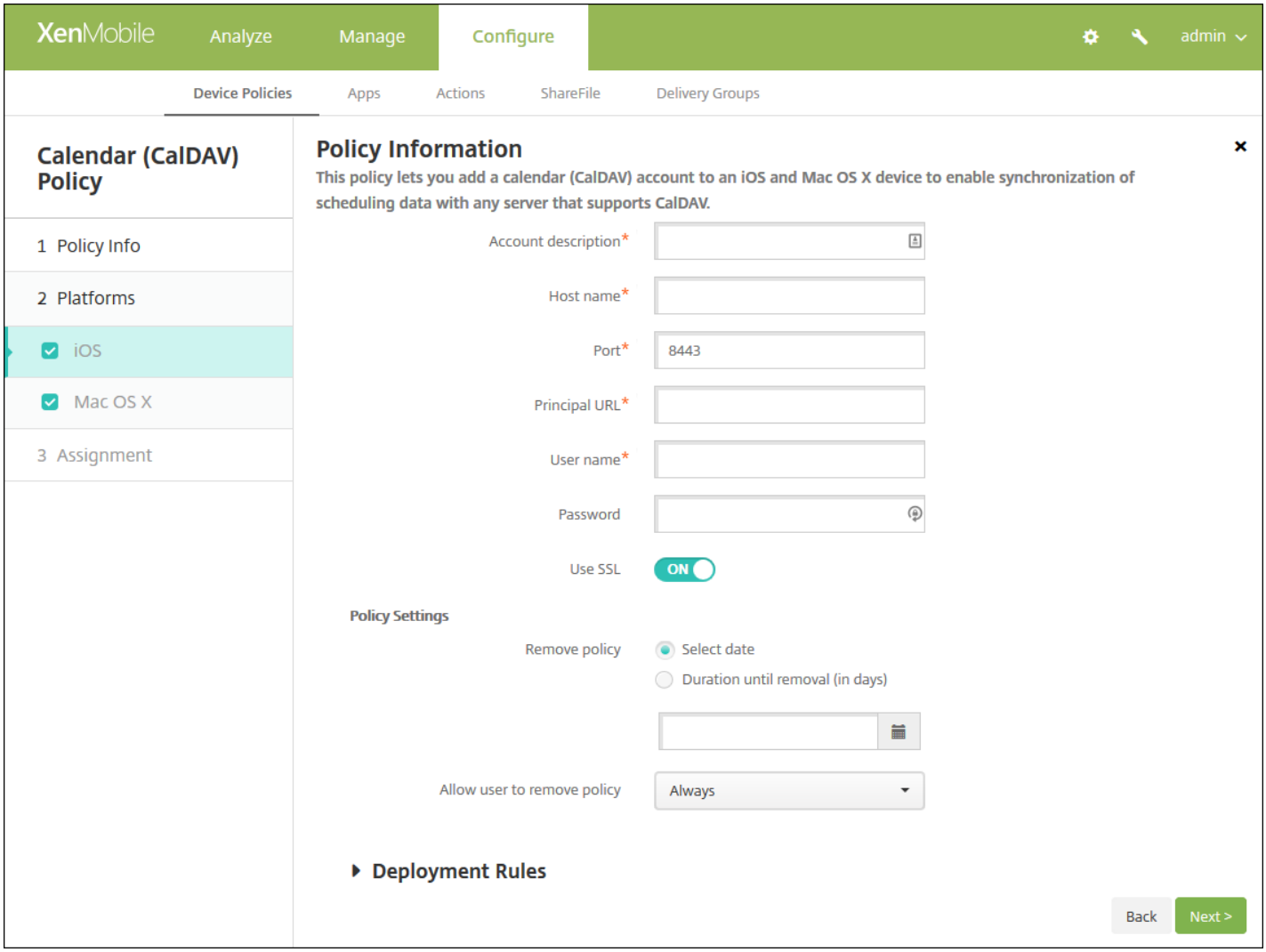
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

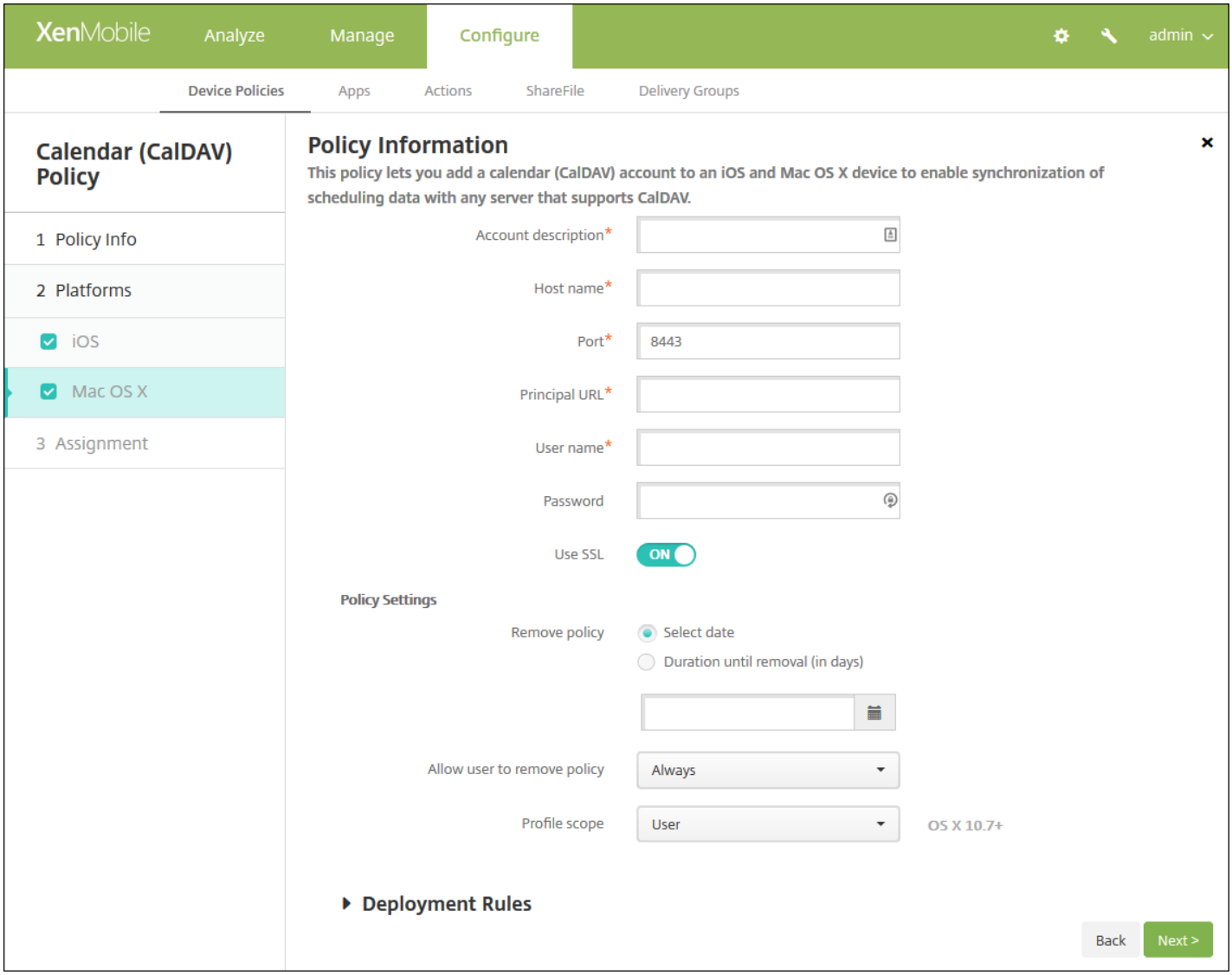
Configuración de los parámetros de iOS



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 por 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



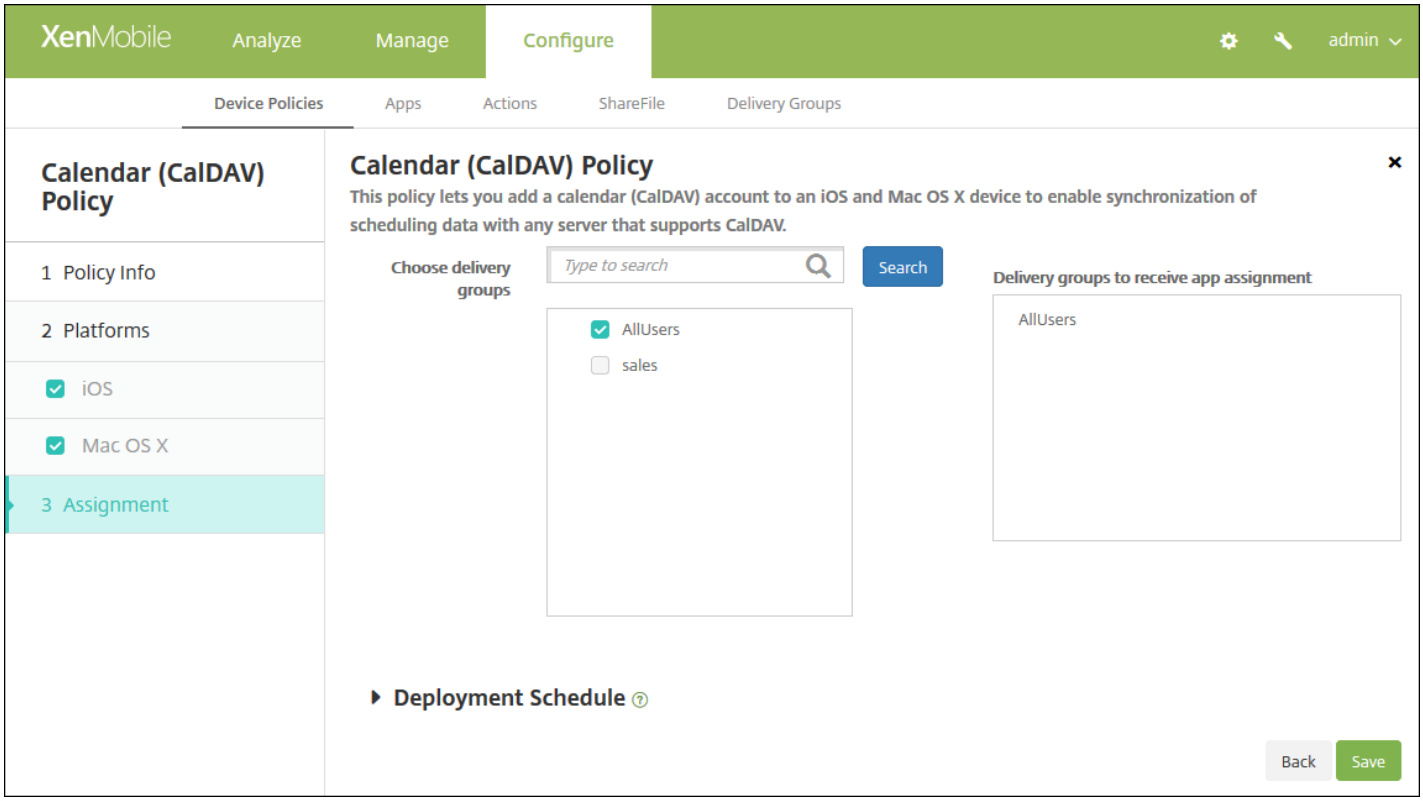
Configure los siguientes parámetros:

- **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 por 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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**.

Nota:

- Esta opción se aplica si se configura la clave de implementación en segundo plano para la programación desde **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 redes de telefonía móvil

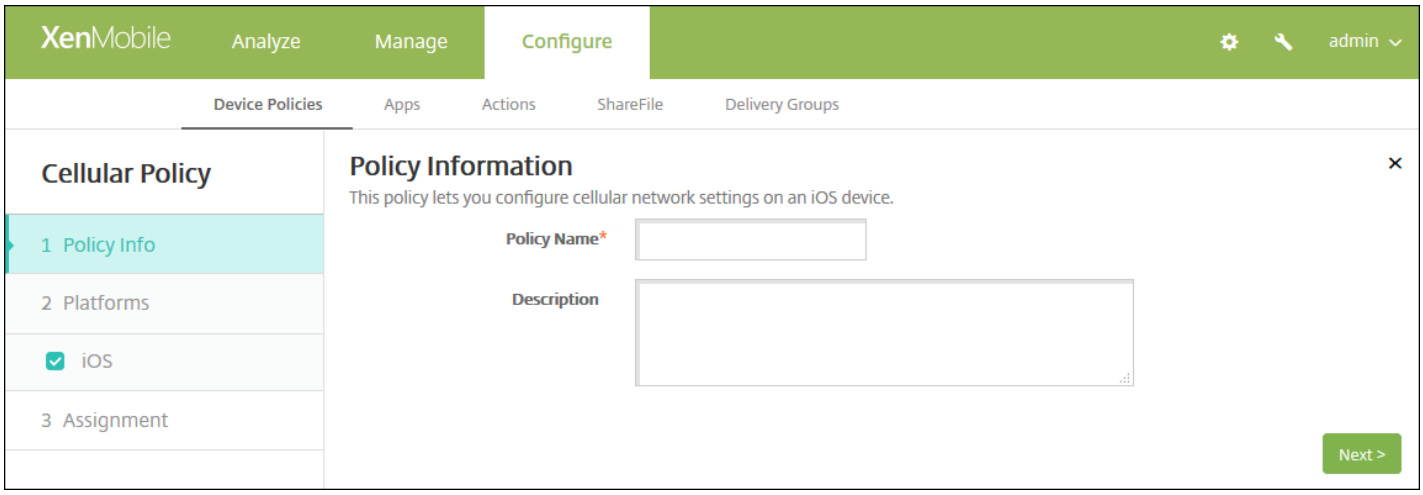
Feb 27, 2017

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**.

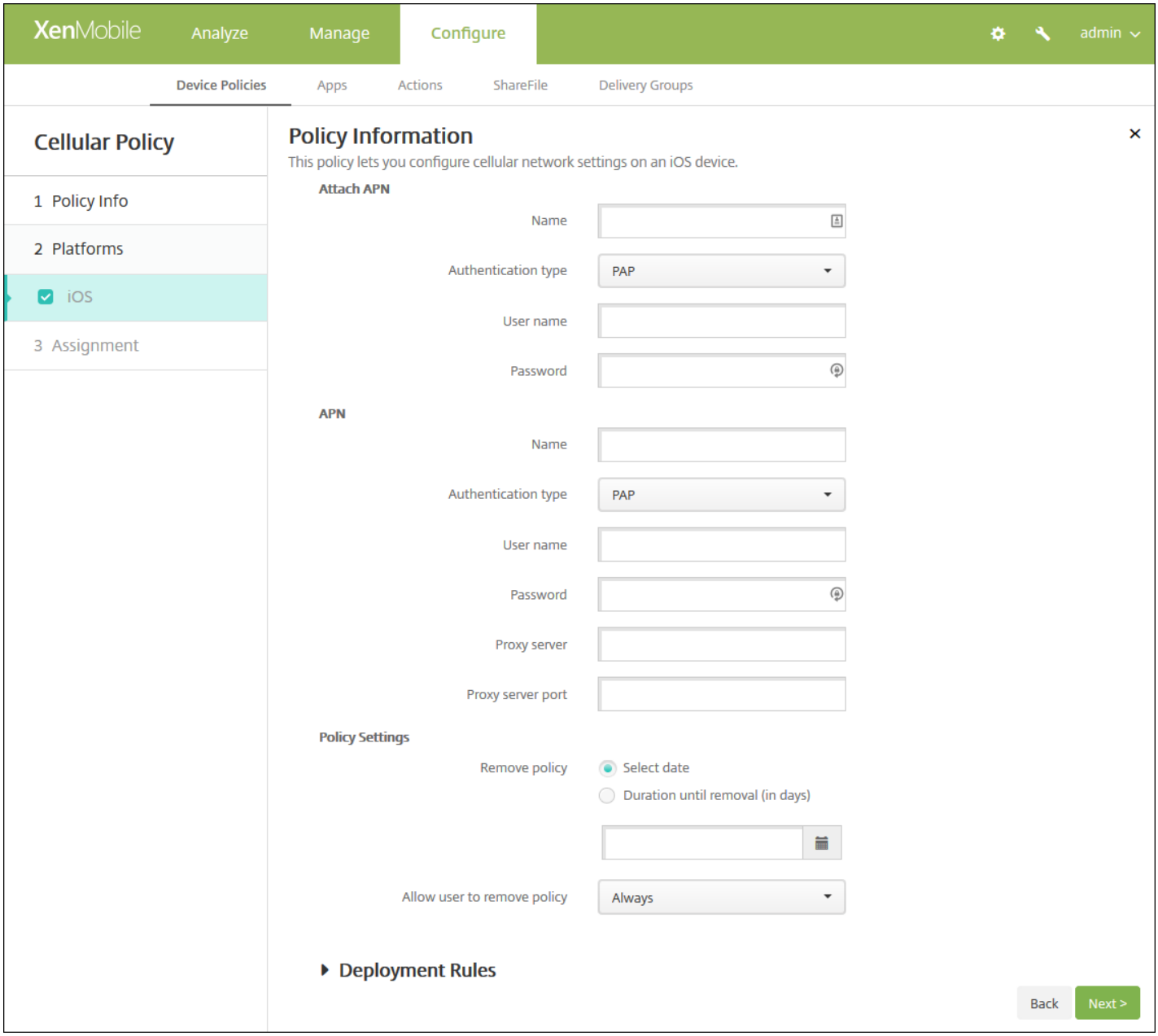
3. Expanda **More** y, a continuación, en **Network Access**, haga clic en **Cellular**. Aparecerá la página de información **Cellular Network Policy**.



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 de la plataforma **iOS**.



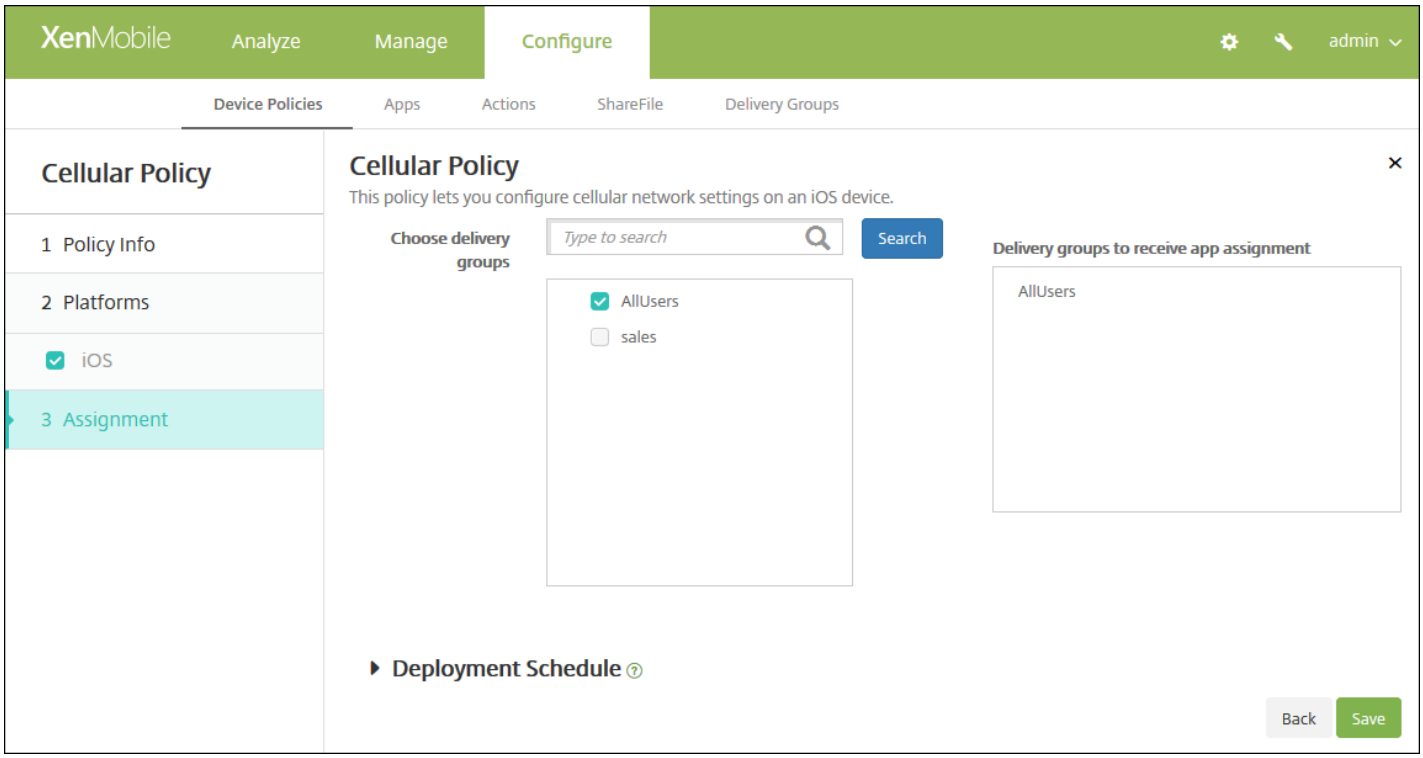
6. Configure estos parámetros:

- **Asociar 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 la contraseña que se usará 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Cellular Network Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para el administrador de conexiones

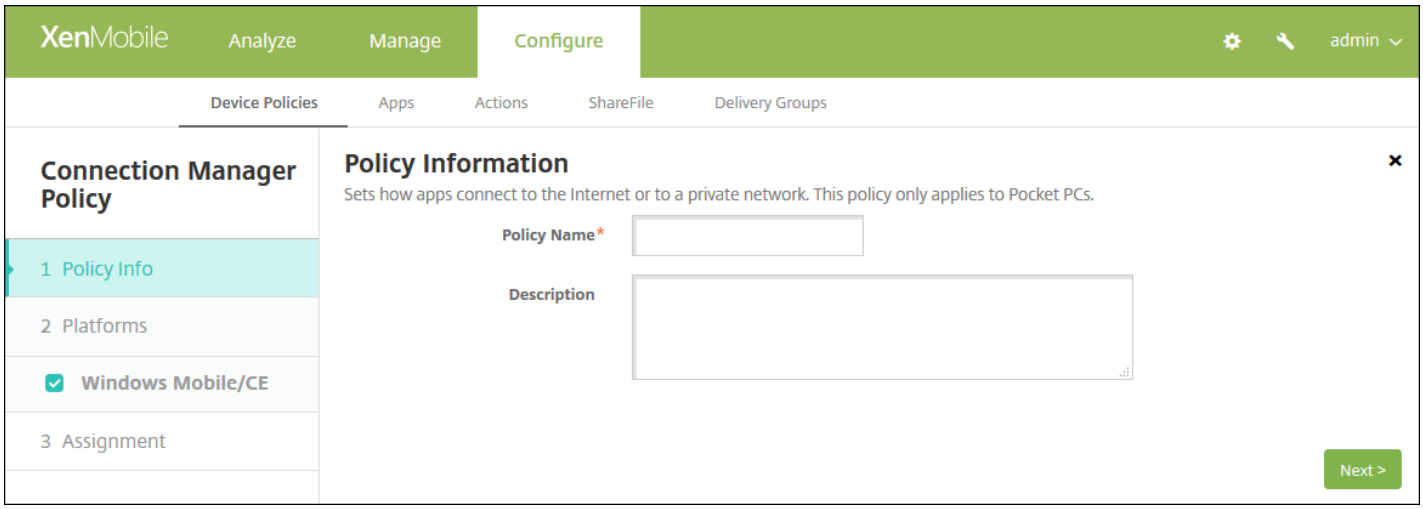
Feb 27, 2017

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**.

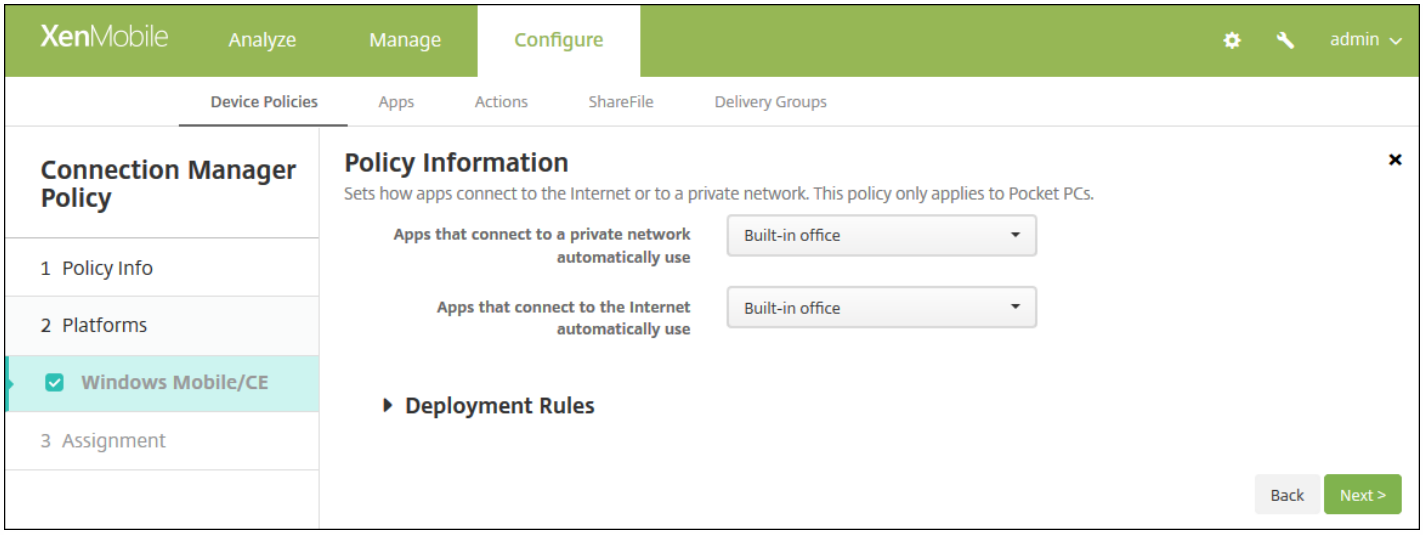
3. Haga clic en **More** y, en **Network access**, haga clic en **Connection Manager**. Aparecerá la página de información **Connection Manager Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



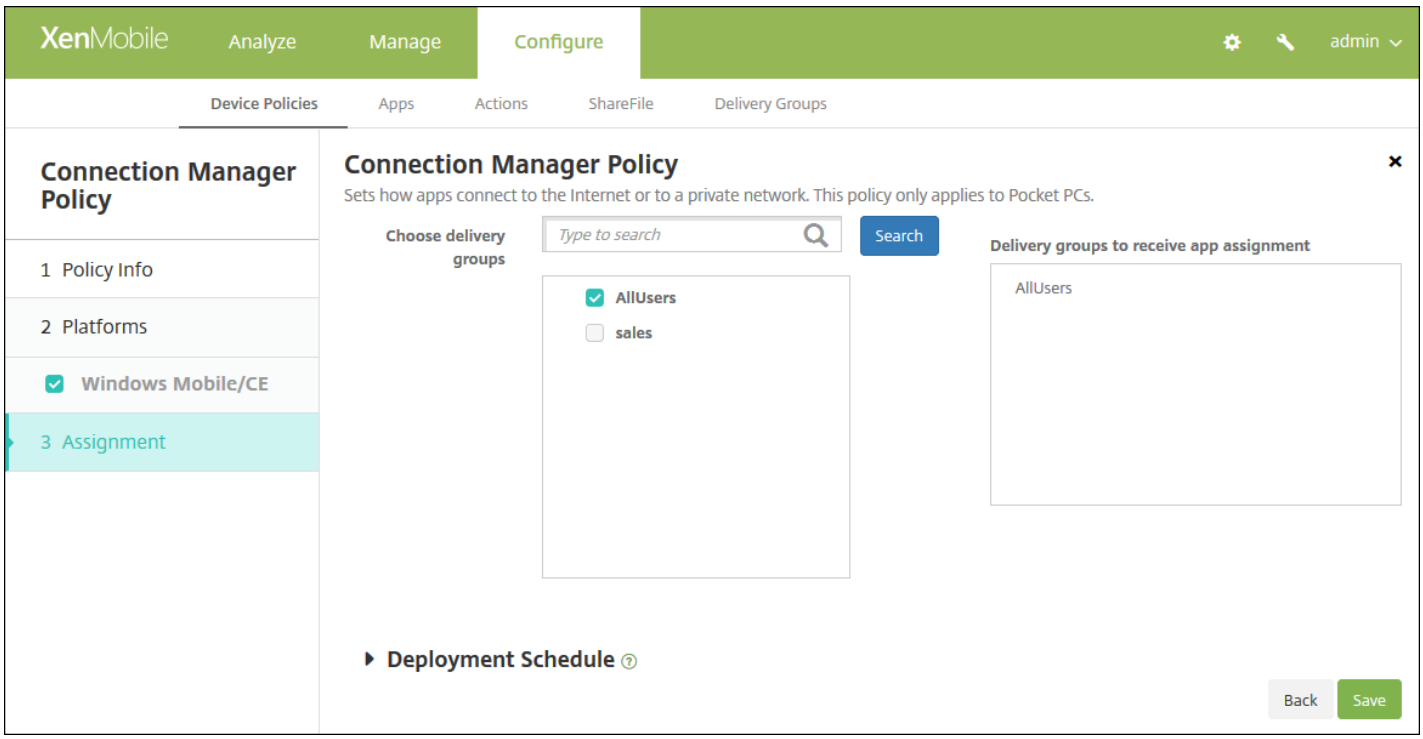
6. Configure estos parámetros.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para programación de conexiones

Feb 27, 2017

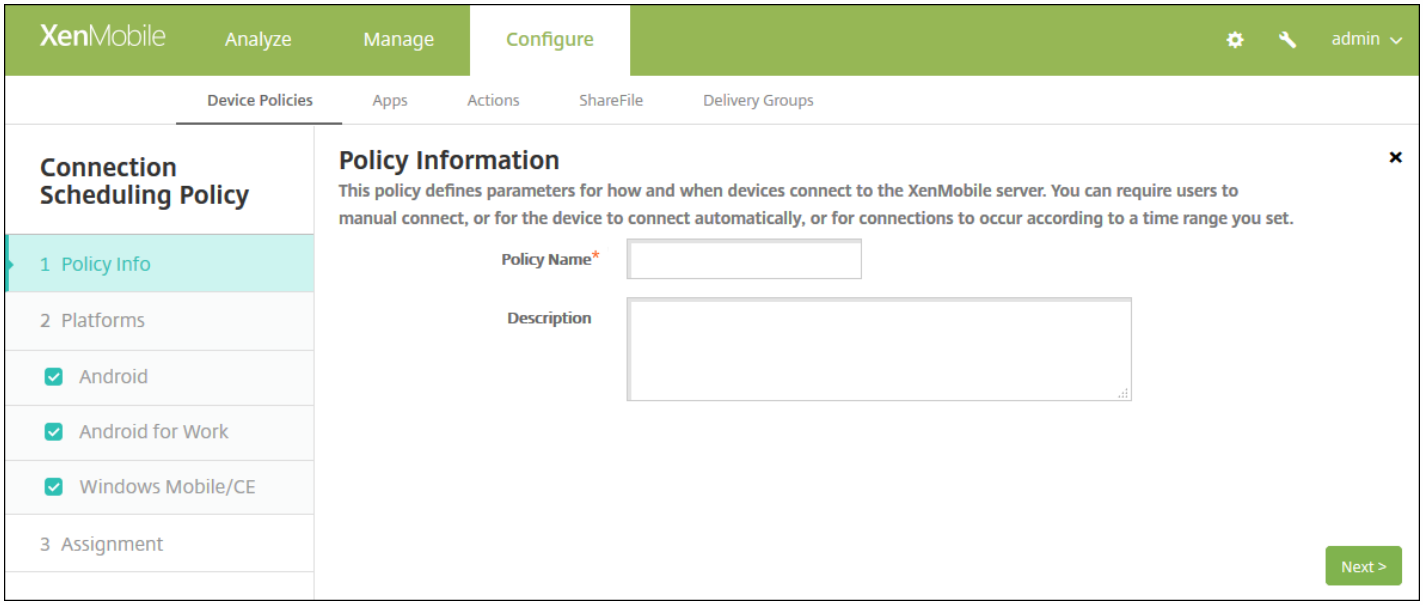
Puede crear directivas de programación de conexiones para controlar cómo y cuándo los usuarios de los dispositivos se conectan a XenMobile. Tenga en cuenta que también puede configurar esta directiva para dispositivos habilitados para Android for Work.

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**.

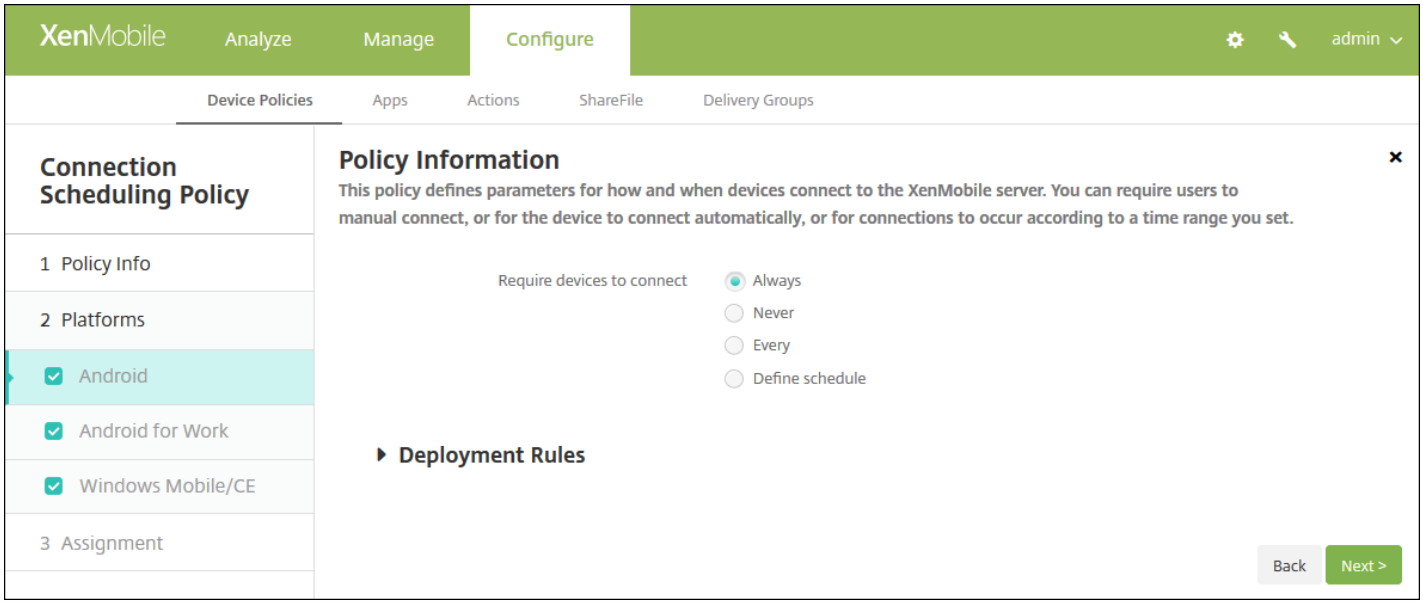
3. Haga clic en **Scheduling**. Aparecerá la página de información **Connection Scheduling Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



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 de una plataforma, consulte el paso 8 para configurar 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 optimizar la seguridad. Cuando seleccione **Always**, use también la opción **Tunnel Policy** del dispositivo, con **Define connection time-out** para 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 **Deploy for always-on connections** en **Deployment Schedule** de cada directiva implementada en el dispositivo.
  - **Never**. Se conecta manualmente. Los usuarios deben iniciar la conexión desde la instancia de XenMobile presente en sus dispositivos. Citrix no recomienda esta opción para las implementaciones de producción, ya que le impide implementar directivas de seguridad en los dispositivos; por lo tanto, los usuarios no recibirán nunca aplicaciones ni directivas nuevas.
  - **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

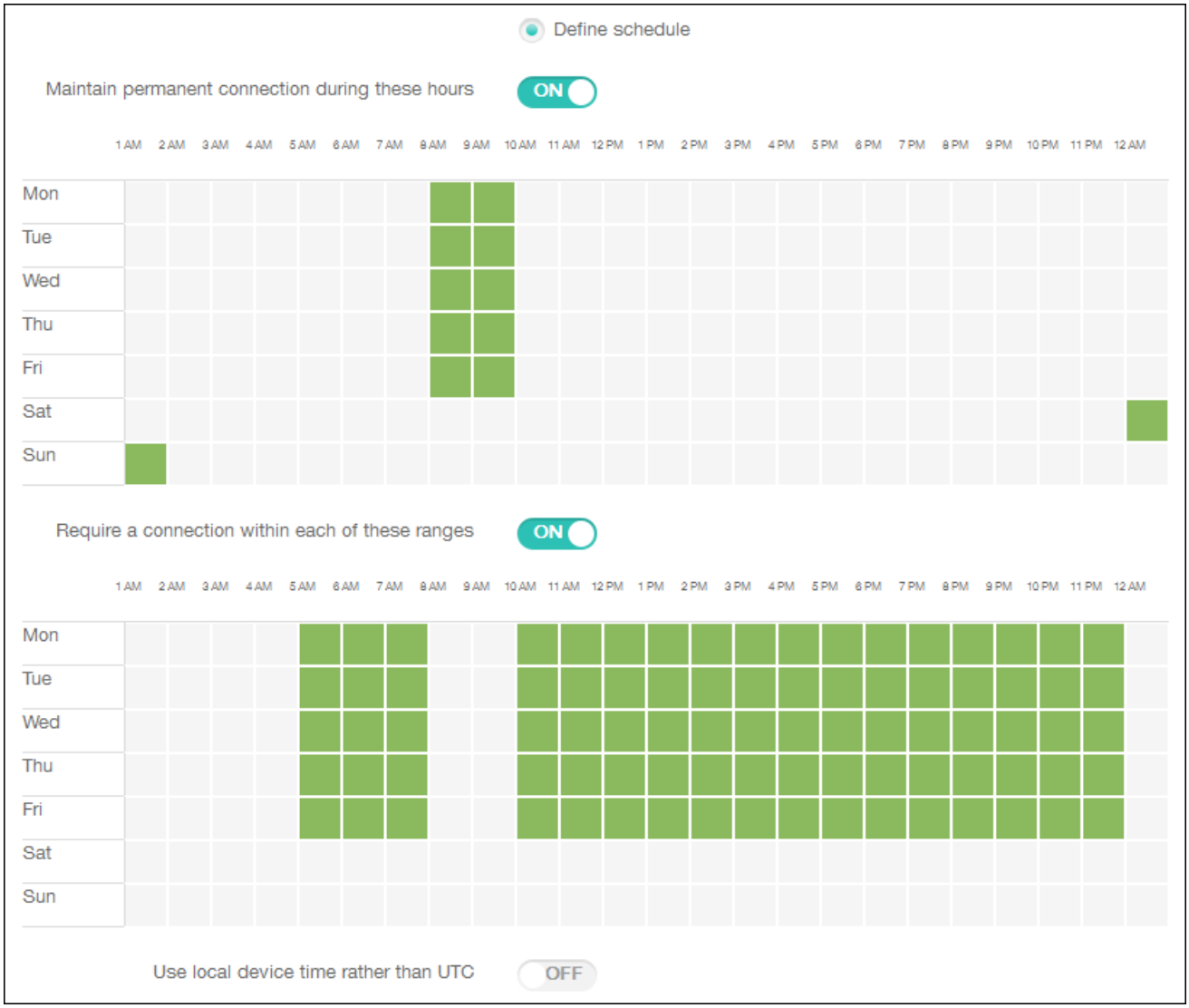
vez en cualquiera de los períodos de tiempo definidos.

- **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

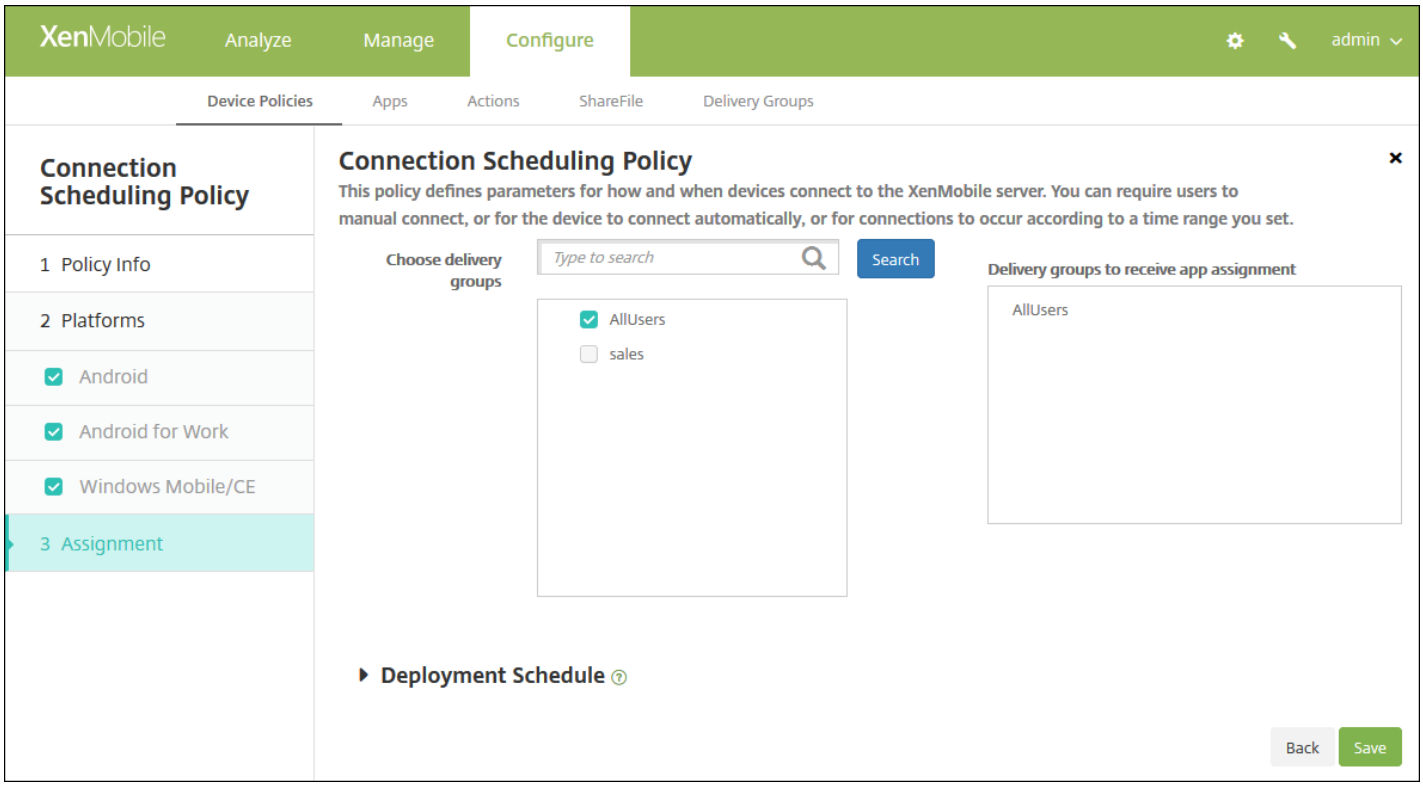
Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

Directiva de dispositivo para contactos (CardDAV)

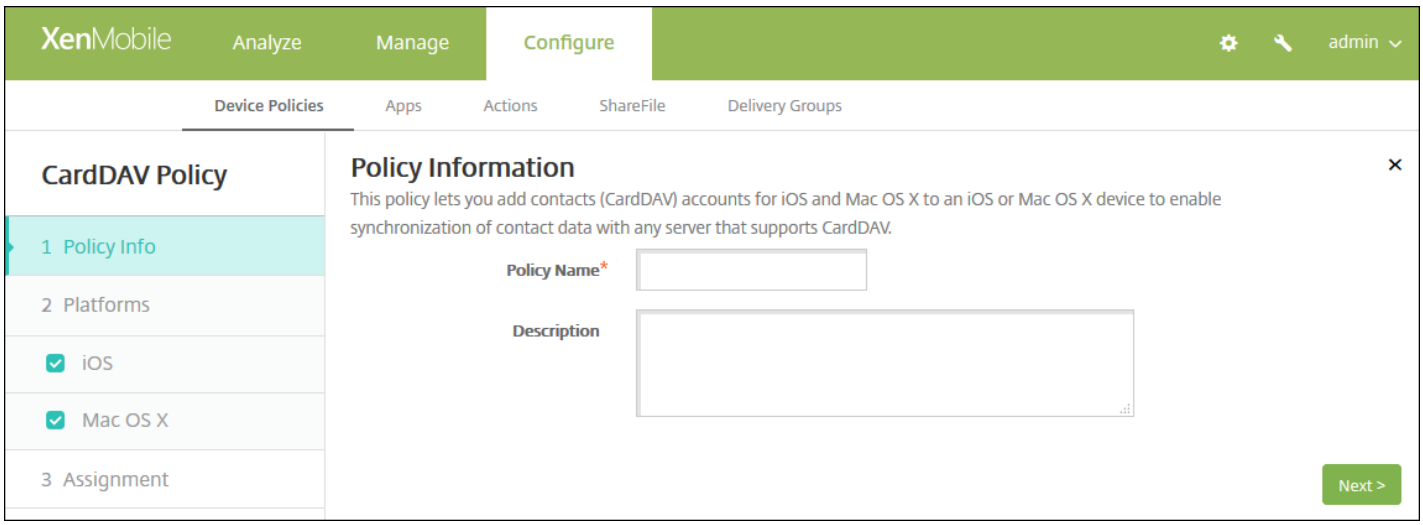
Feb 27, 2017

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:

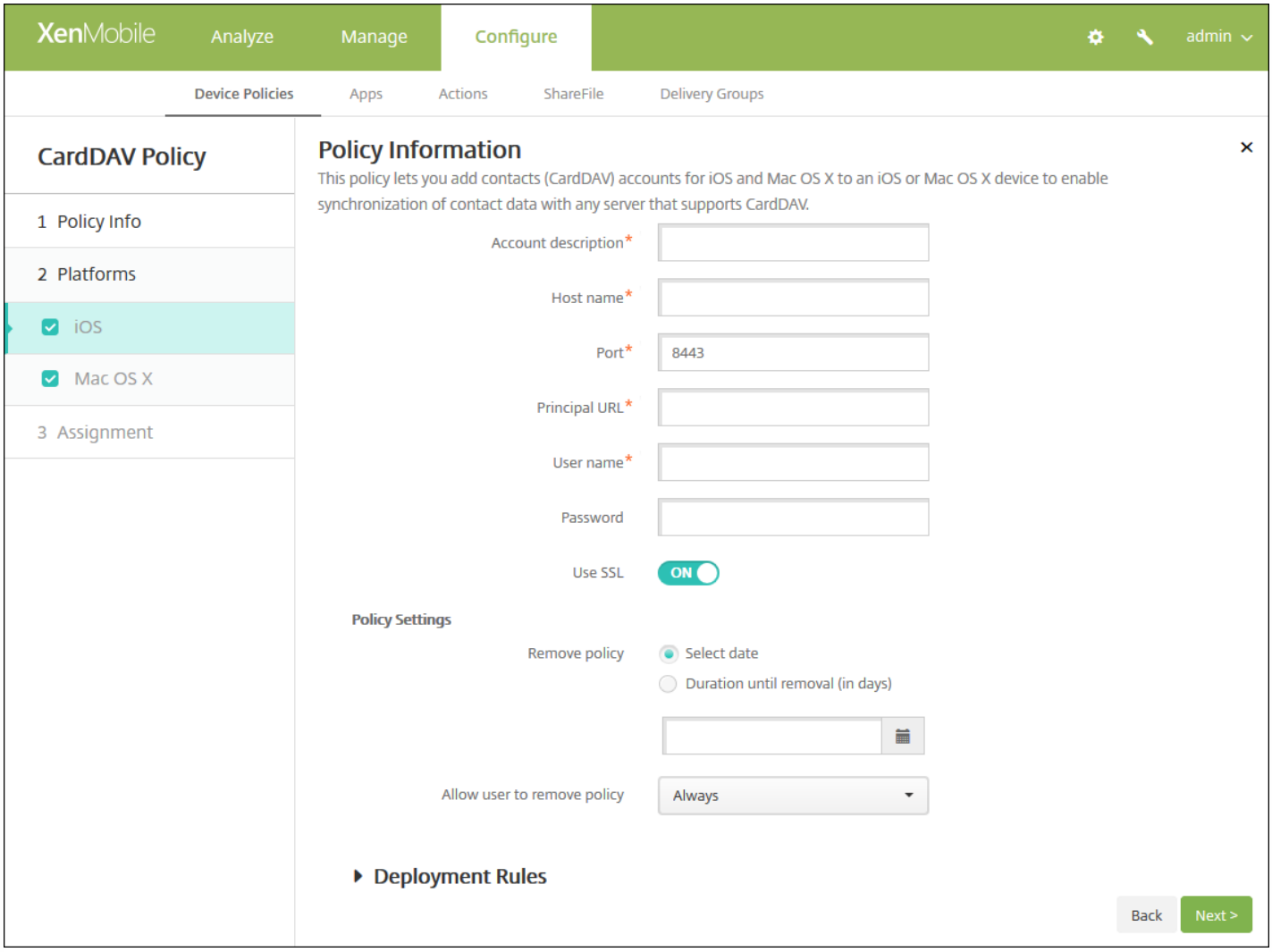
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

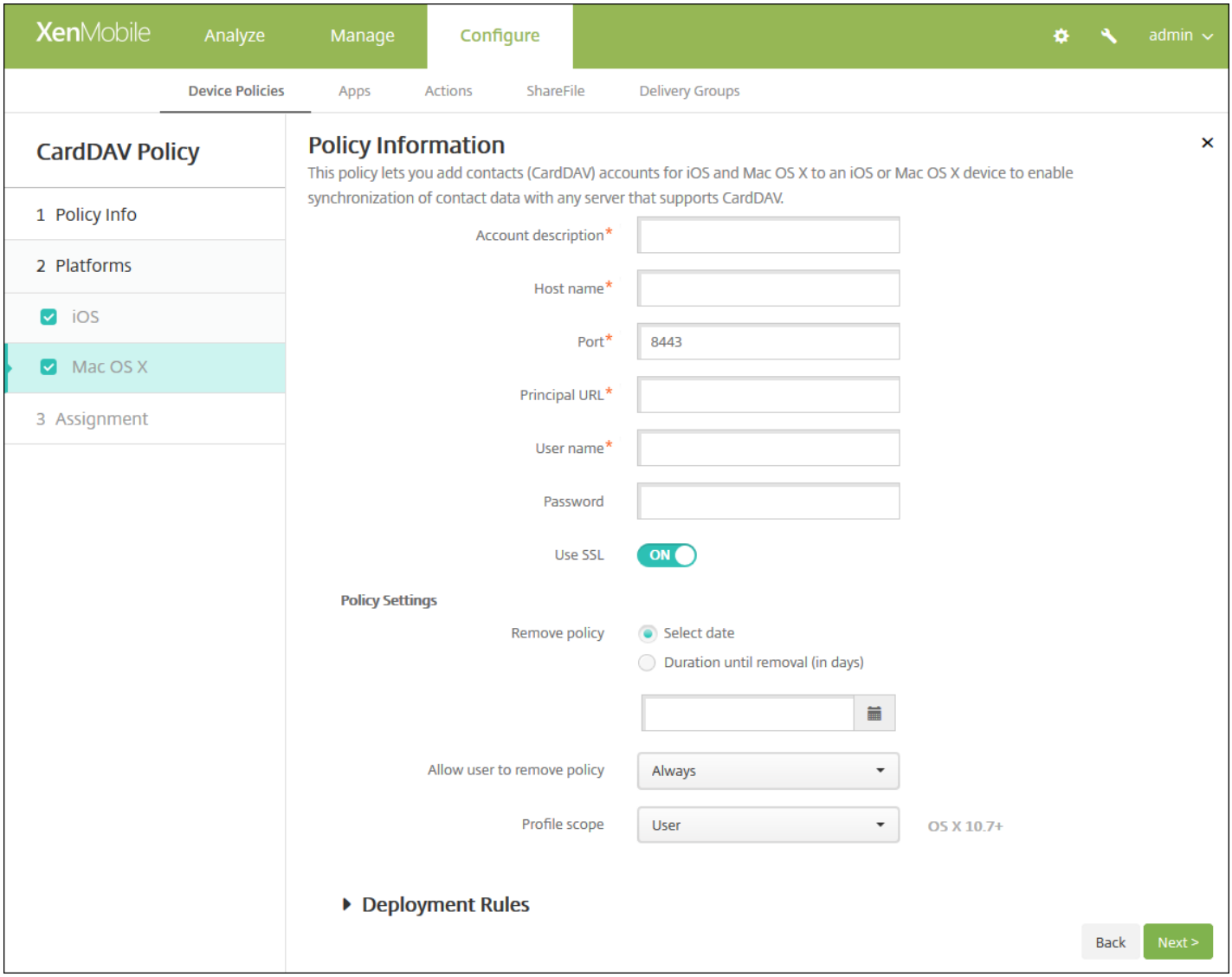
Configuración de los parámetros de iOS



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 por 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, introduzca la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



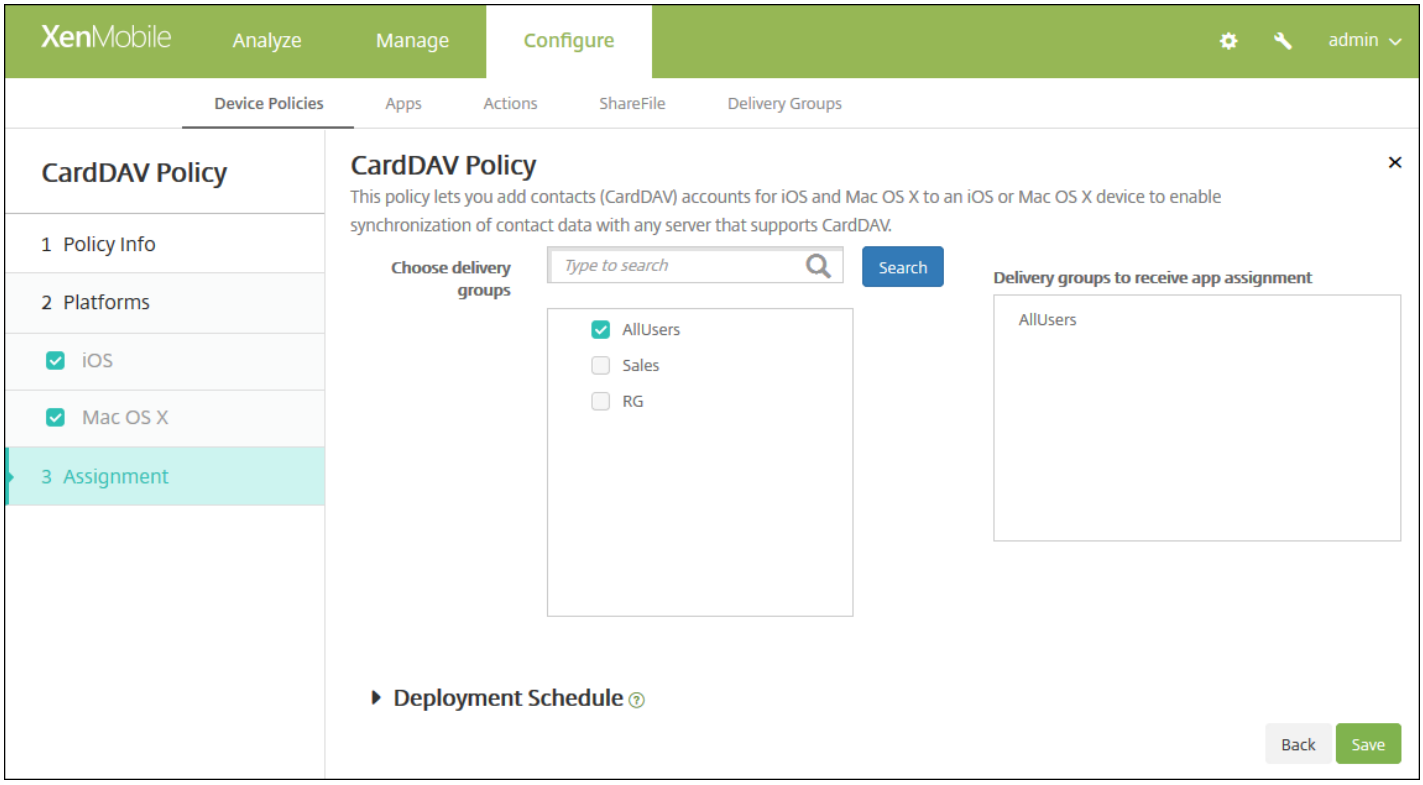
Configure estos parámetros:

- **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 por 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para copiar aplicaciones a un contenedor Samsung

Feb 27, 2017

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.

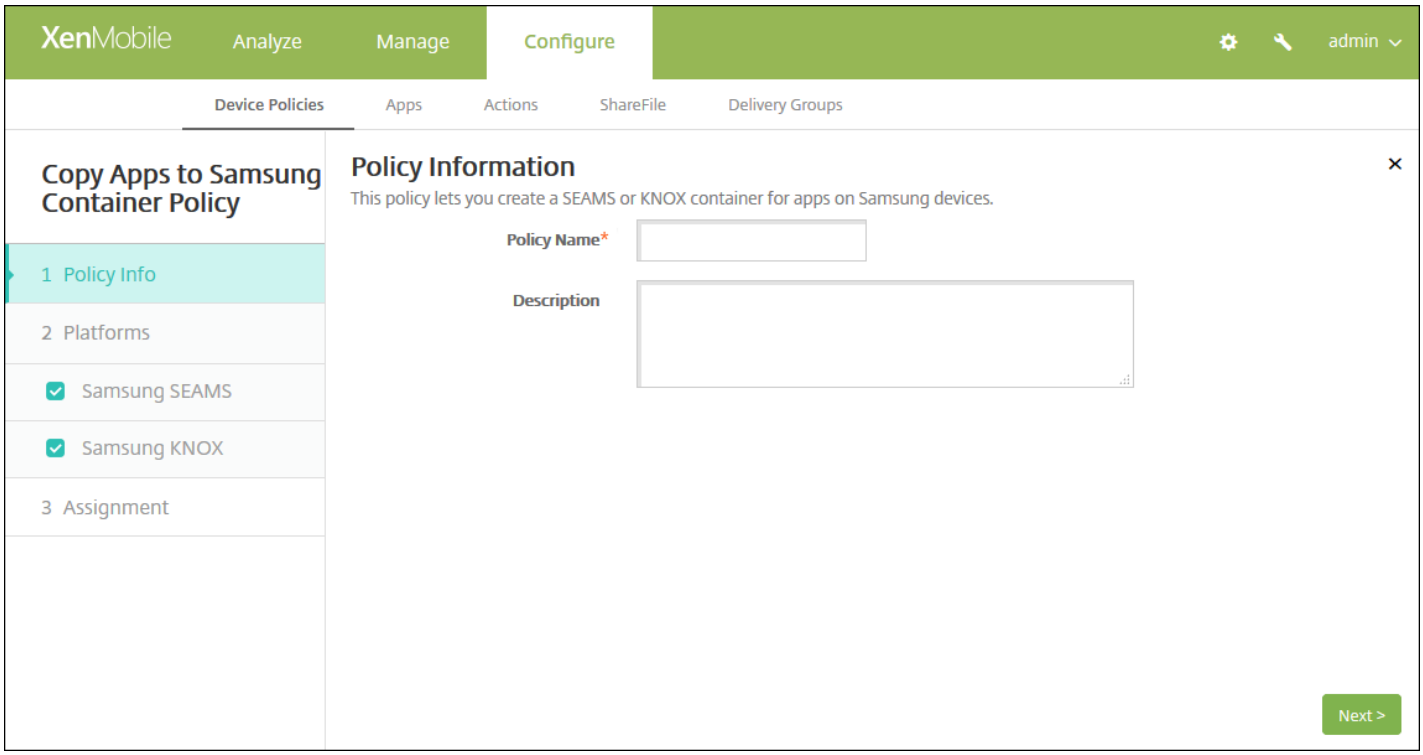
Requisitos previos:

- 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**.

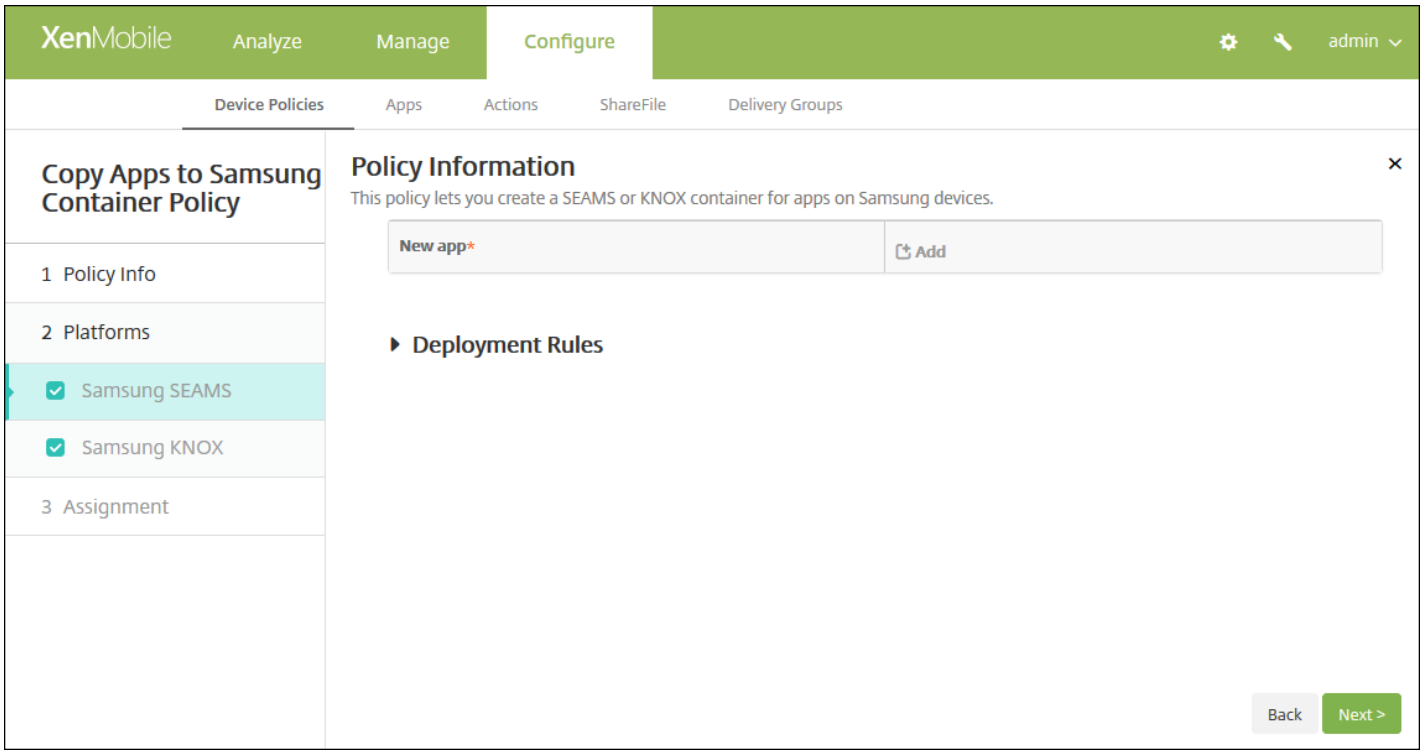
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Copy Apps to Samsung Container**. Aparecerá la página de información **Copy Apps to Samsung Container Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



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 de una plataforma, consulte el paso 8 para configurar las reglas de implementación de esa plataforma.

7. Configure el siguiente parámetro para cada una de las plataformas seleccionadas.

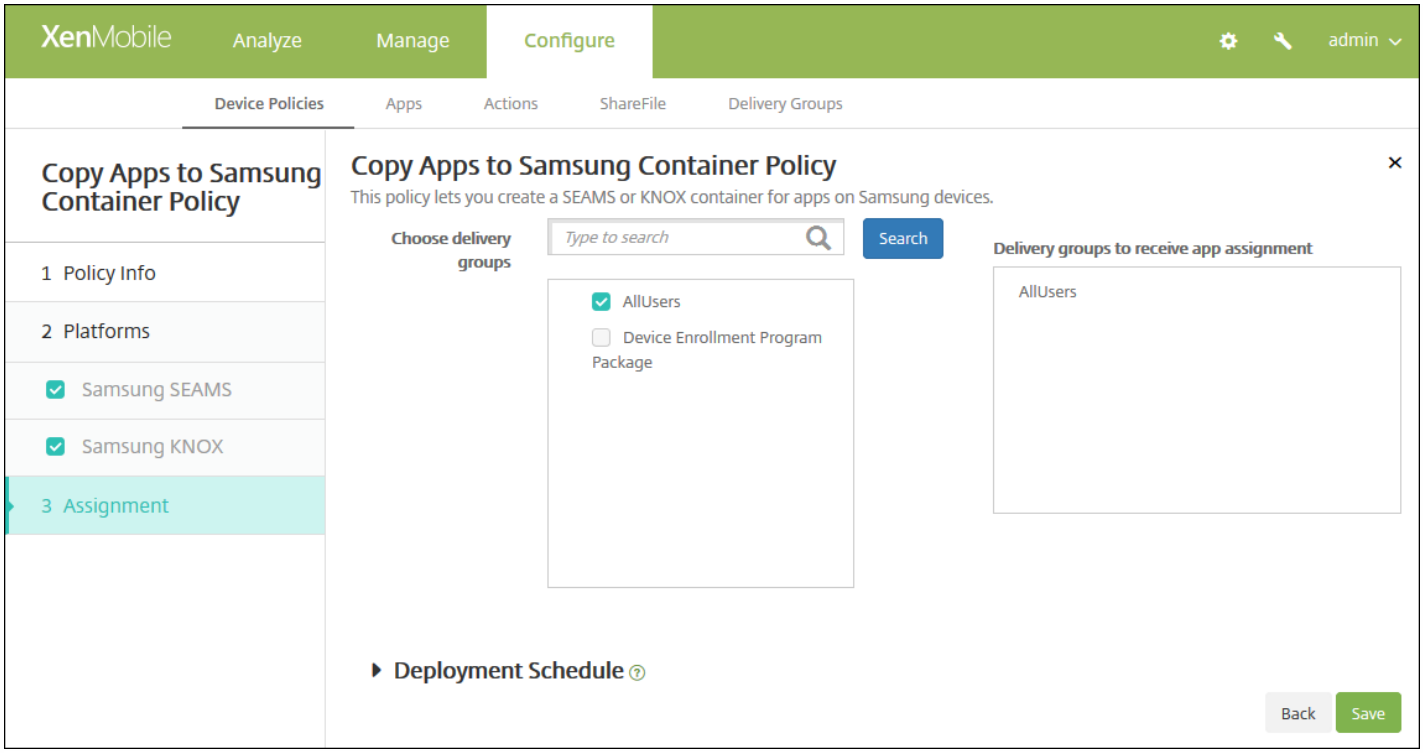
- **New App**. Para agregar cada aplicación a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - Escriba un ID de paquet, por ejemplo: com.mobiwolf.lacingart para la aplicación LacingArt.
  - Haga clic en **Save** o **Cancel**.

    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 guardarlos, o bien en **Cancel** para descartarlos.

8. Configure las reglas de implementación.

9 Haga clic en **Next**. Aparecerá la página de la plataforma siguiente, o bien la página de asignación **Copy Apps to Samsung Container Policy**.



10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde 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.

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**.

Directiva de dispositivo sobre credenciales

Feb 27, 2017

En XenMobile, puede crear directivas de credenciales para habilitar la autenticación integrada con la configuración de PKI en XenMobile, 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

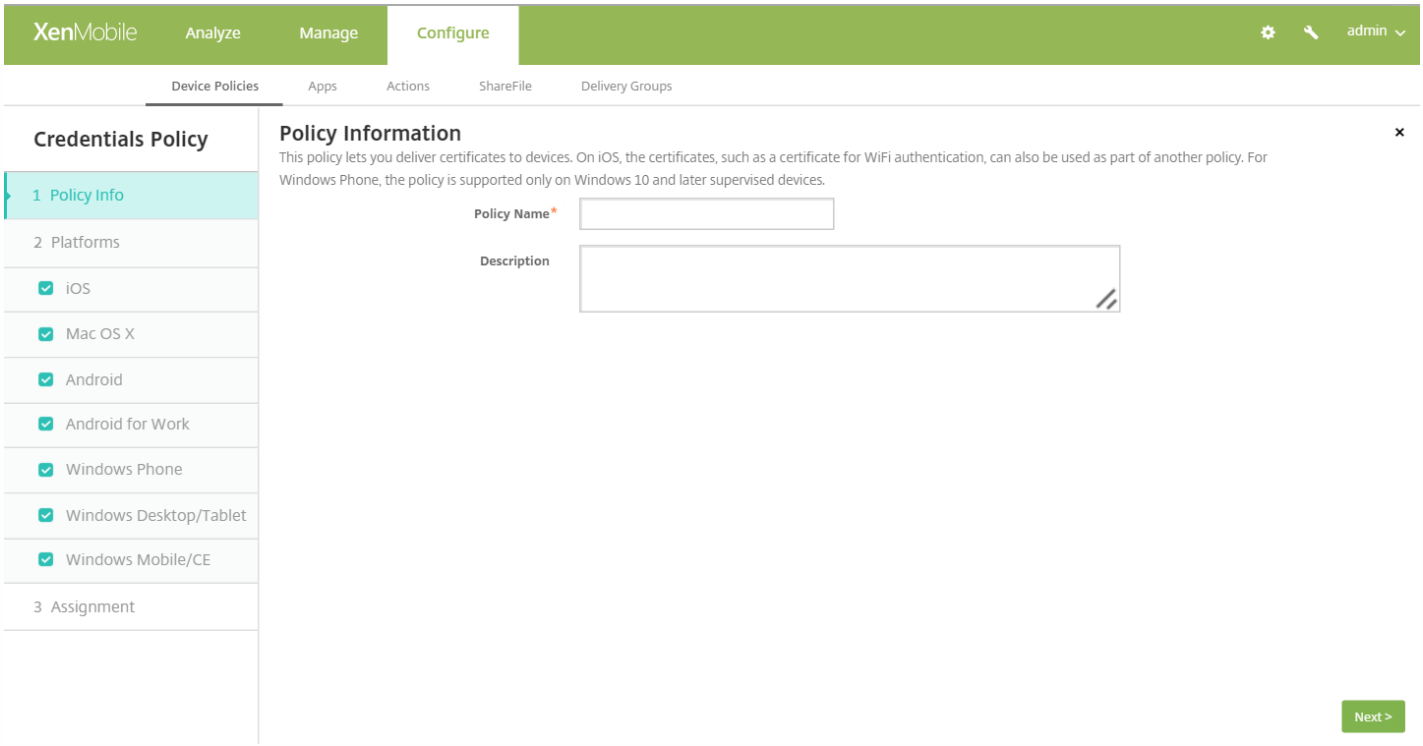
Configuración de Windows Phone

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:

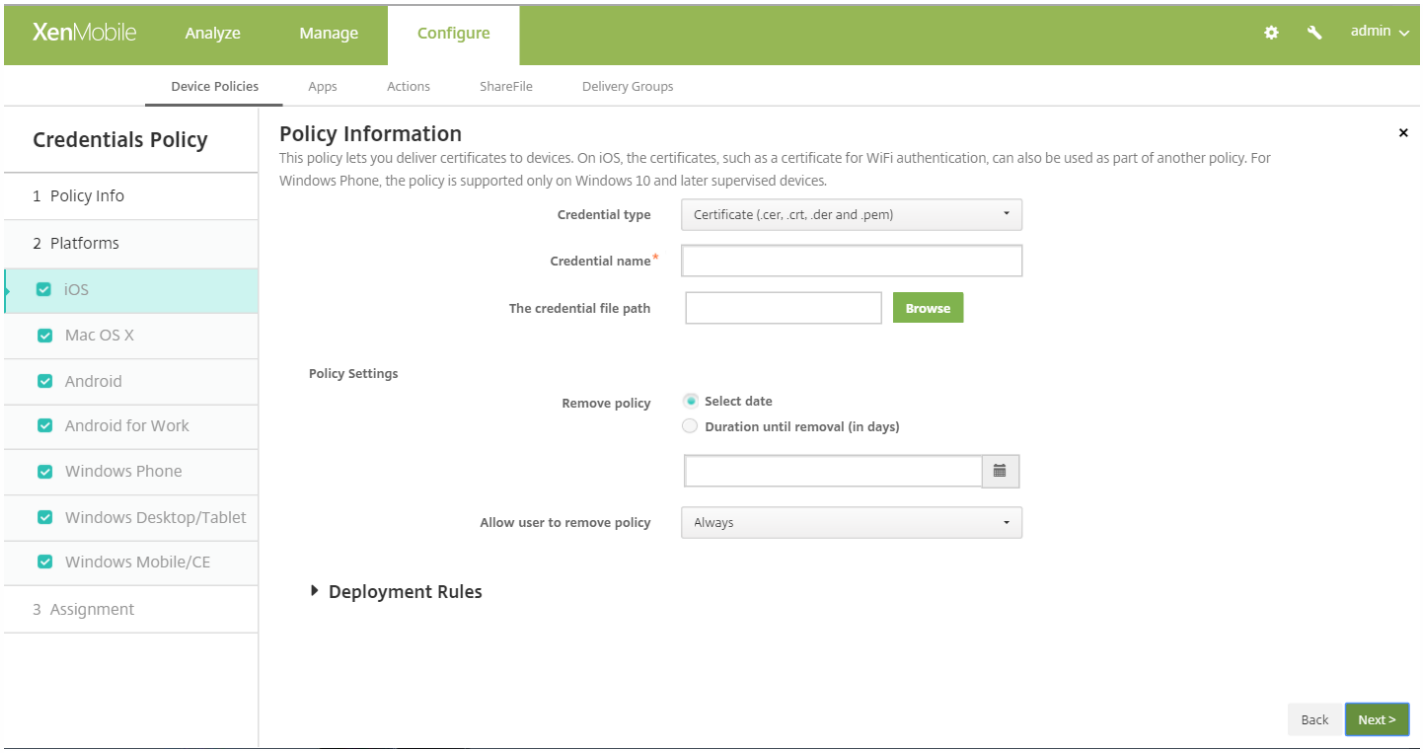
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

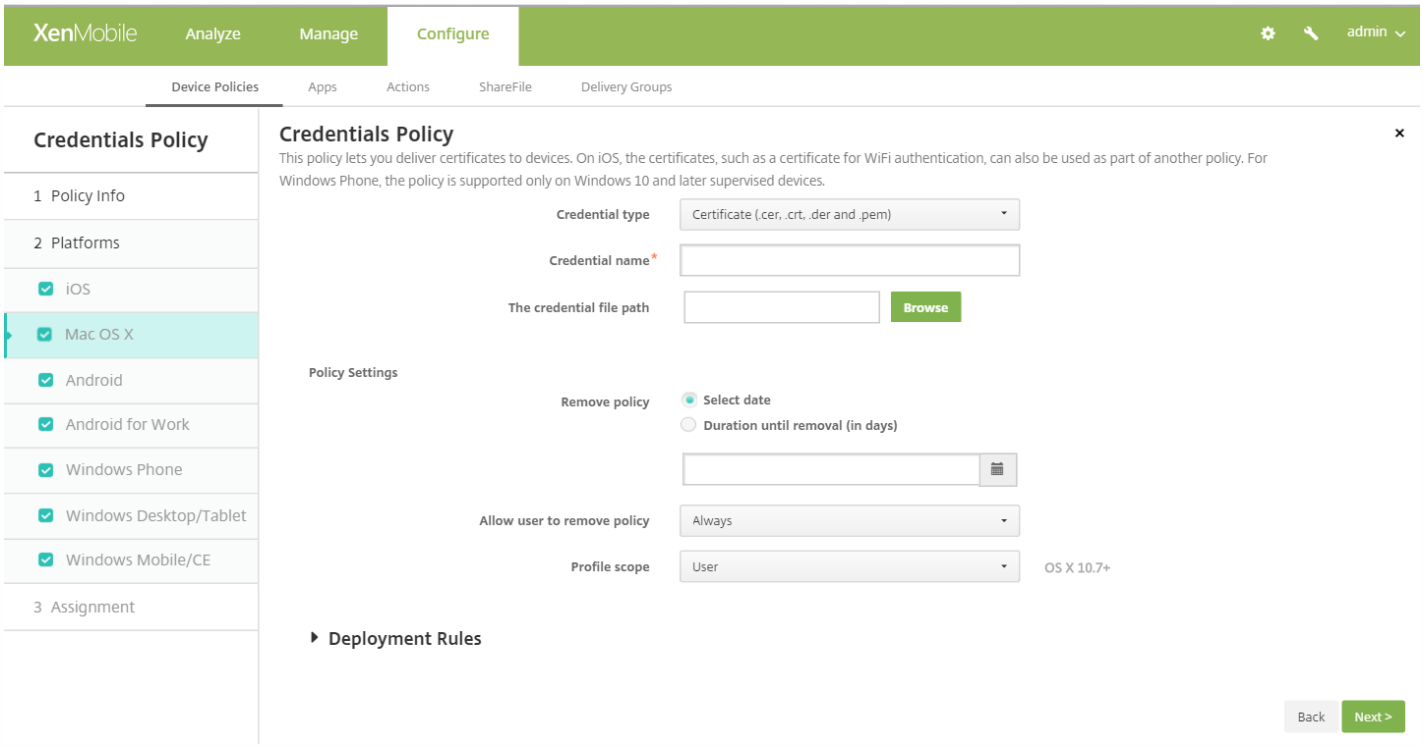
Configuración de los parámetros de iOS



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.
  - **Certificado de servidor**
    - **Server certificate**. En la lista, haga clic en el certificado que se va a utilizar.
  - **Proveedor de credenciales**
    - **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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

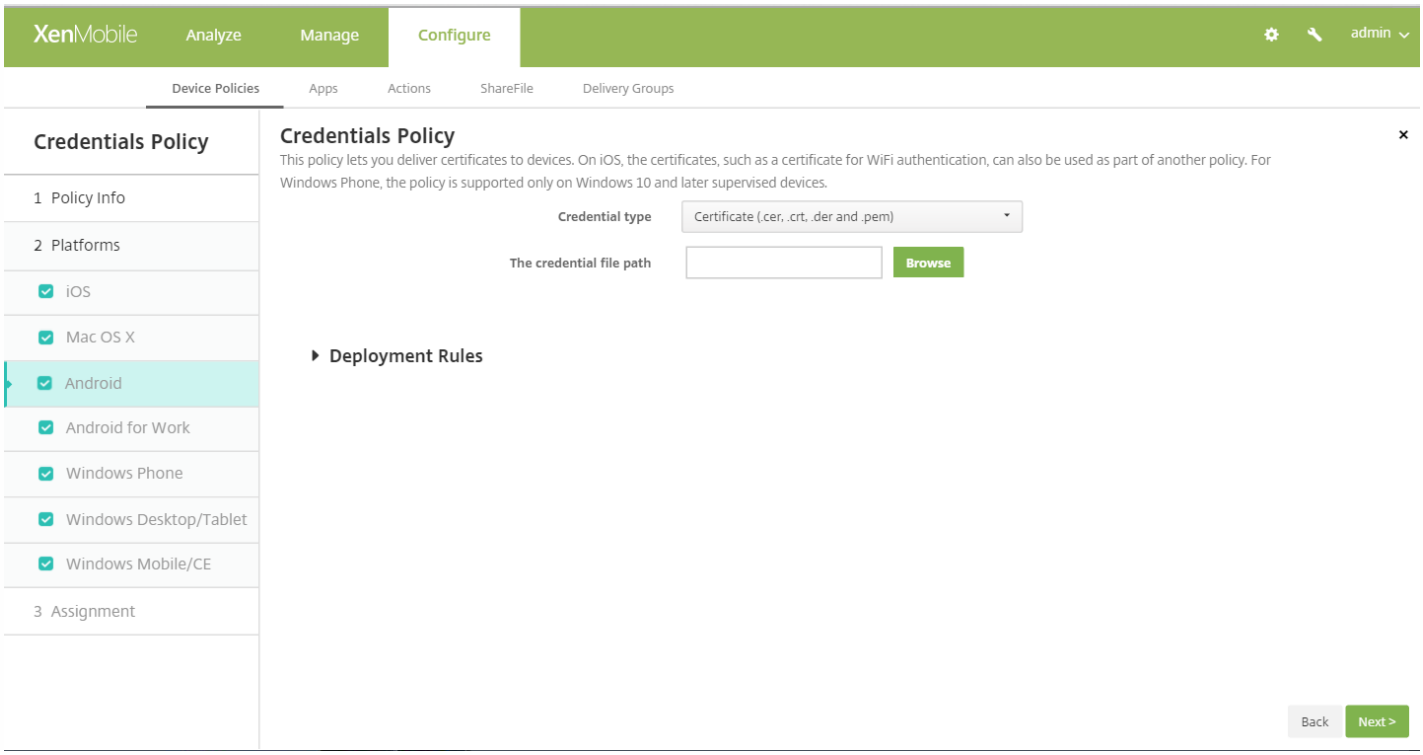
Configuración de los parámetros de Mac OS X



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.
  - **Certificado de servidor**
    - **Server certificate**. En la lista, haga clic en el certificado que se va a utilizar.
  - **Proveedor de credenciales**
    - **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** 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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.

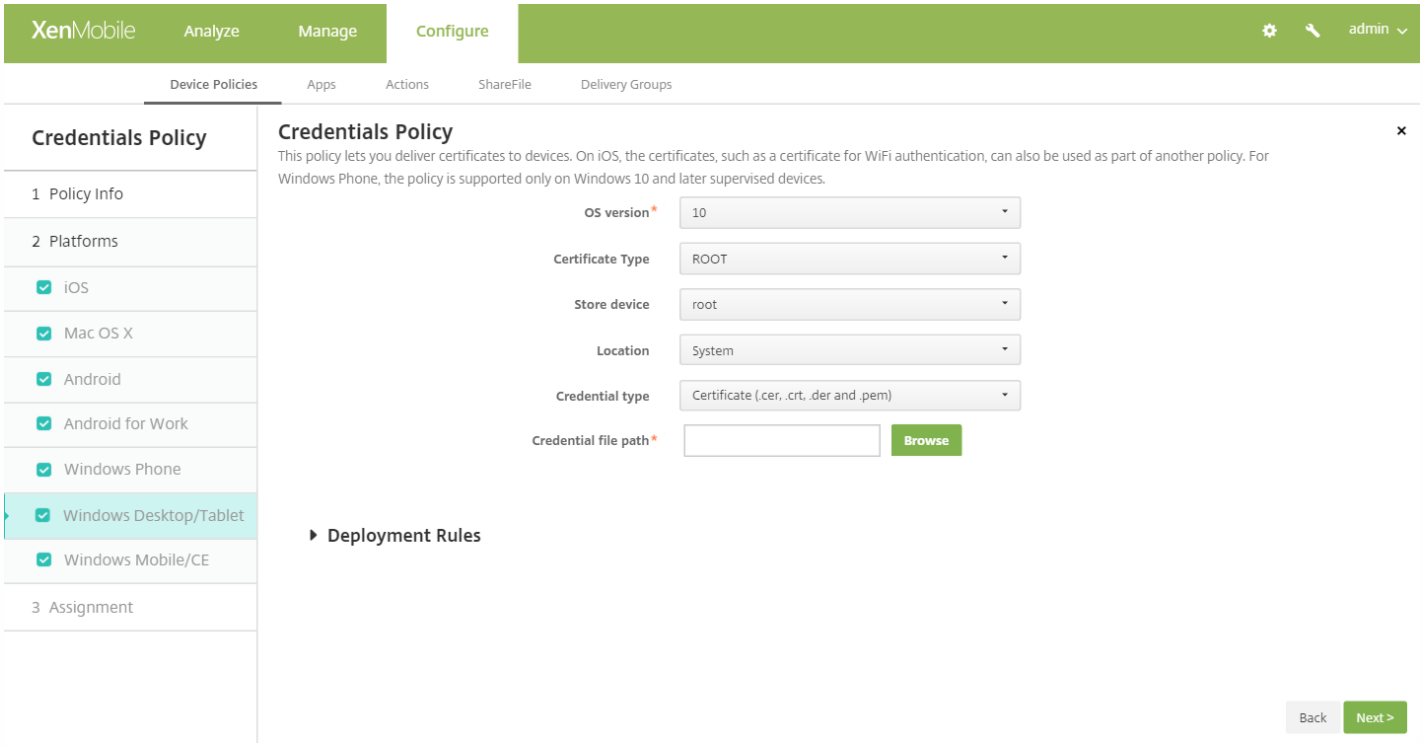
Configuración de los parámetros de Android y Android for Work



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.
  - **Certificado de servidor**
    - **Server certificate**. En la lista, haga clic en el certificado que se va a utilizar.
  - **Proveedor de credenciales**
    - **Credential provider**. En la lista, haga clic en el nombre del proveedor de credenciales.

Configuración de los parámetros de escritorios o tabletas Windows



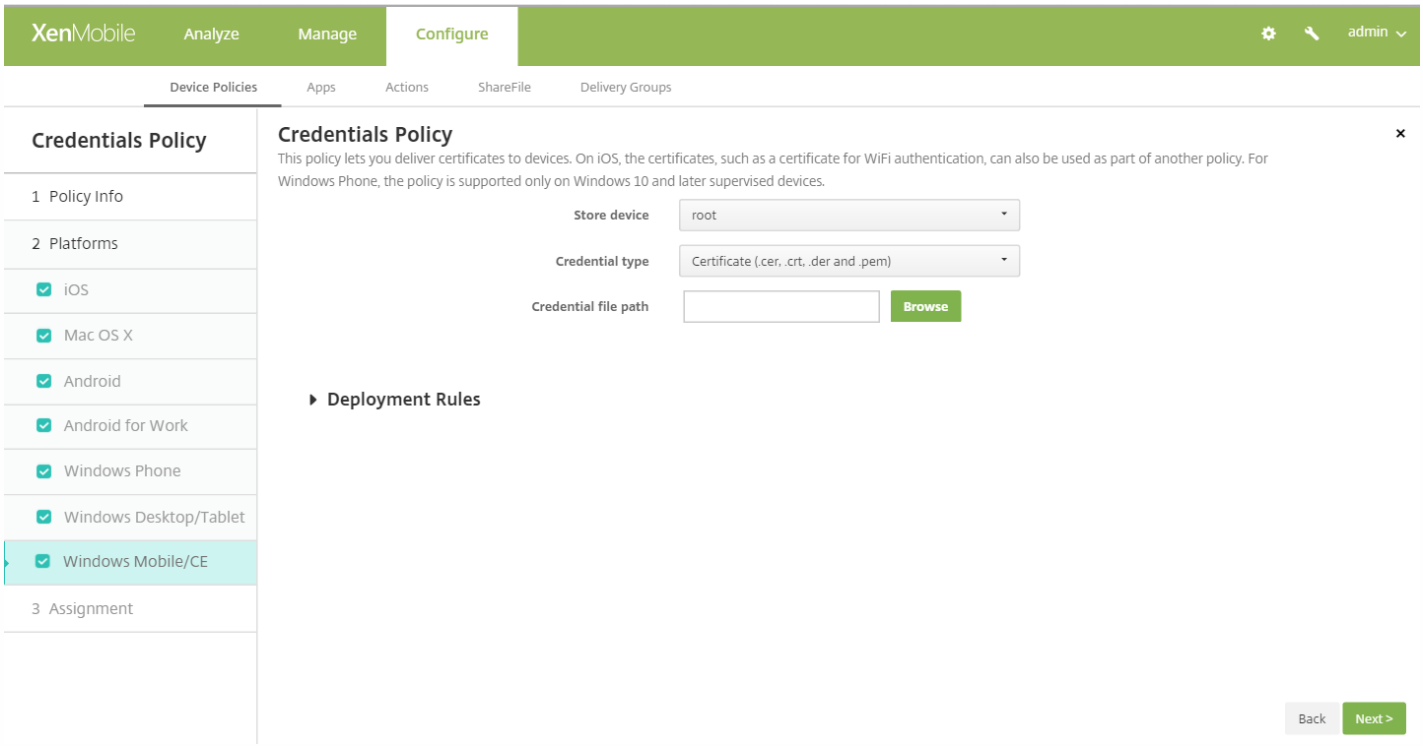
Configure los siguientes parámetros:

OS version. 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

Parámetros de Windows 8.1 Phone

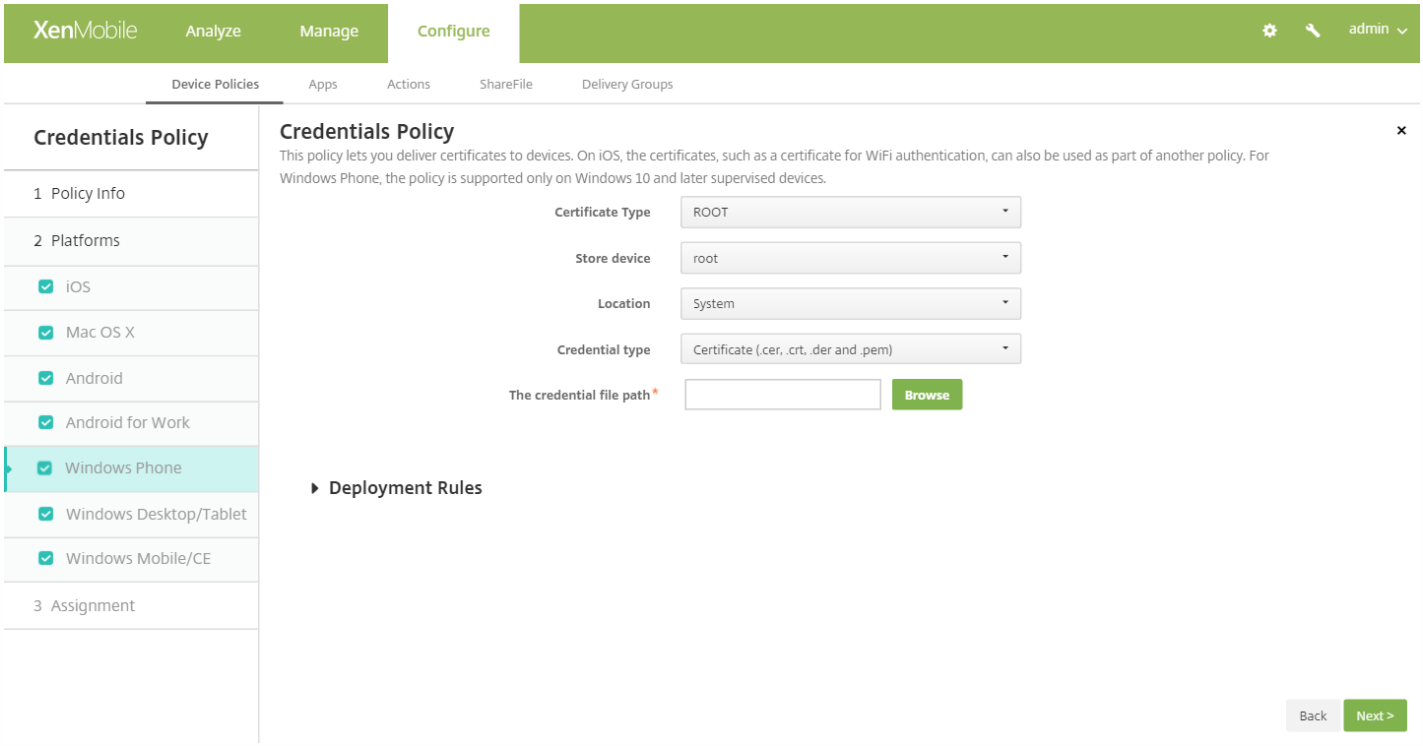
Configuración de los parámetros de Windows Mobile/CE



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 certificados 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

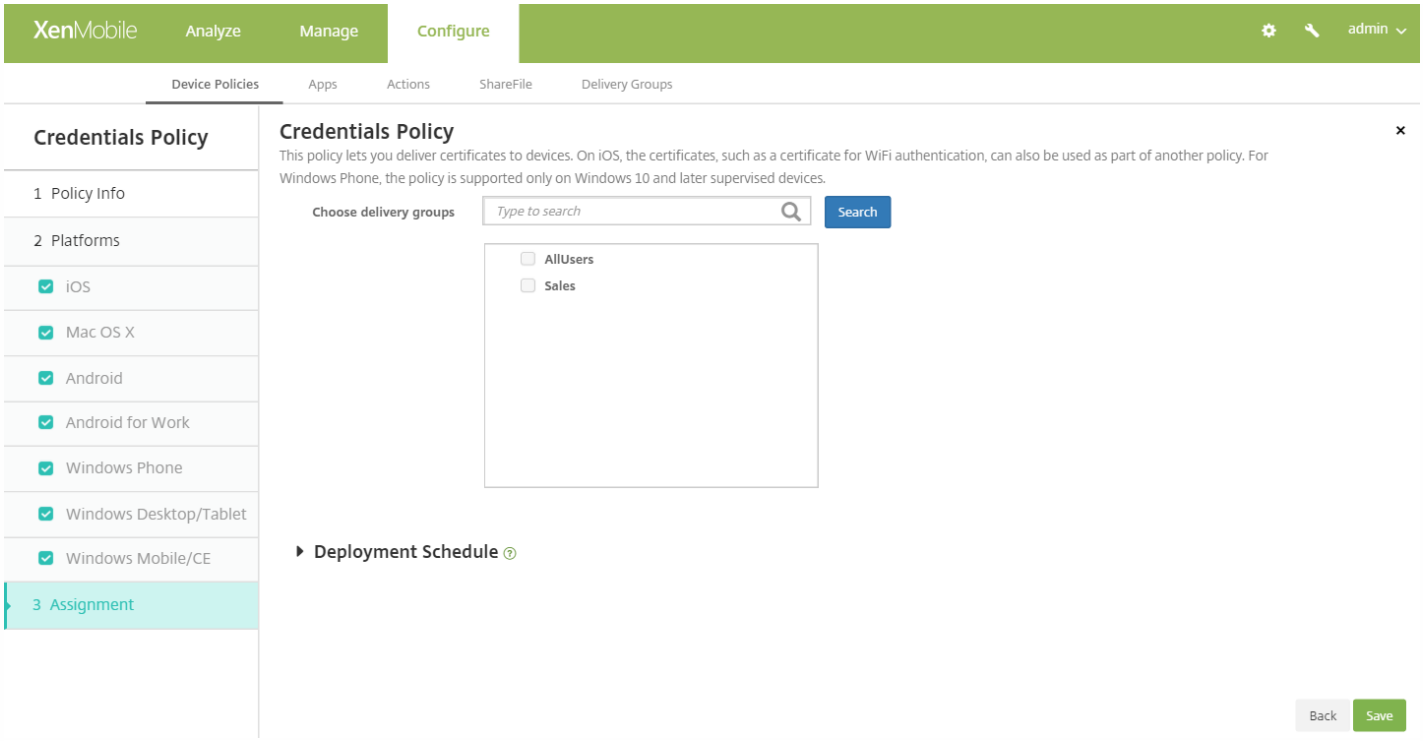


Configure los siguientes parámetros:

- **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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo de XML personalizado

Feb 27, 2017

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:

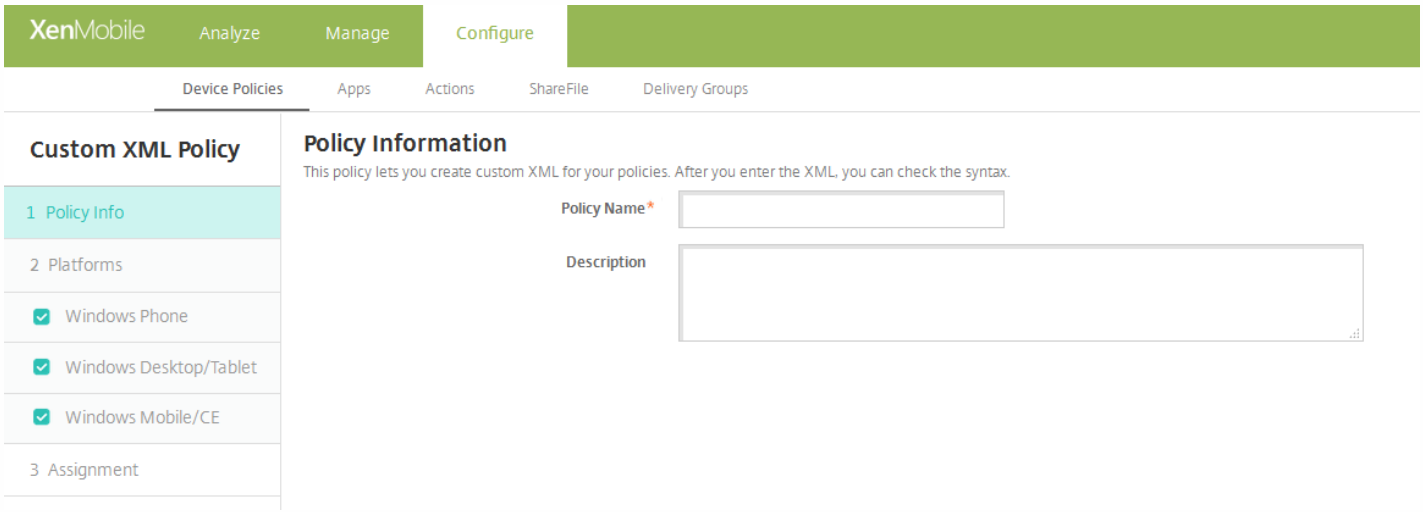
- El aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o inhabilitación de las funciones.
- La configuración de dispositivos, que incluye la capacidad para permitir a los usuarios cambiar la configuración y los parámetros de sus dispositivos.
- Las actualizaciones de software, 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 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**.

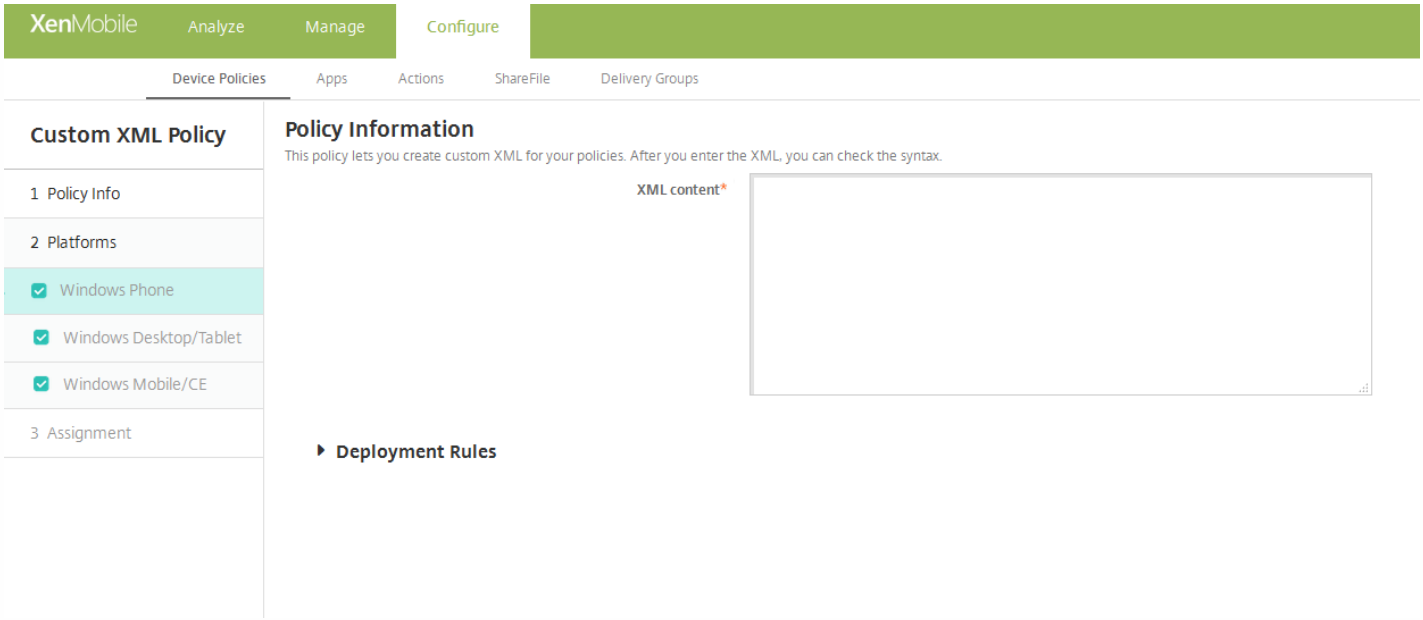
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Custom XML**. Aparecerá la página de información **Custom XML Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página **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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para Defender

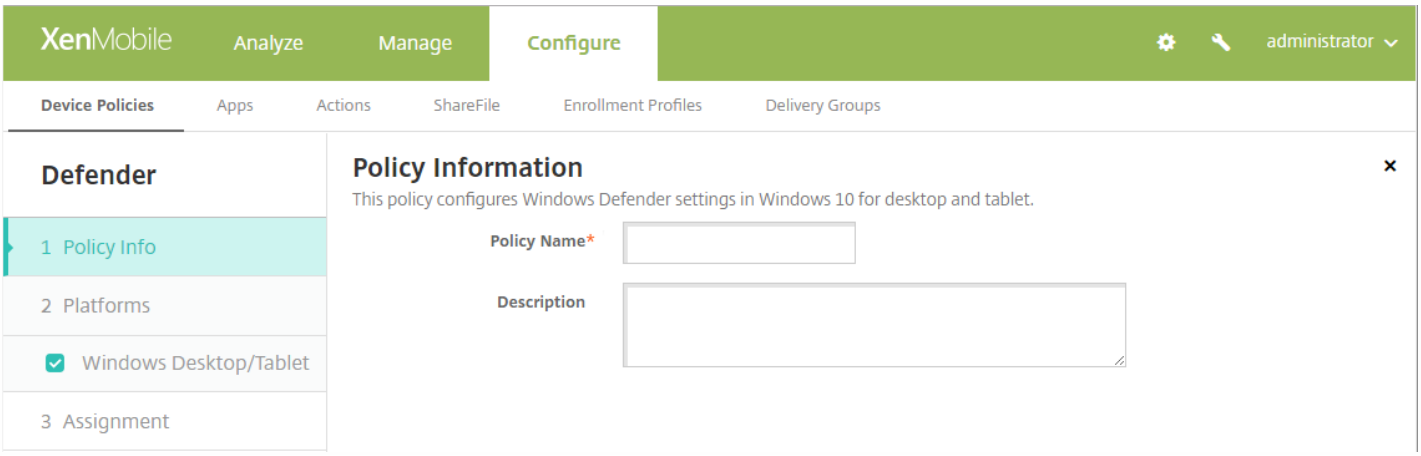
Feb 27, 2017

Windows Defender es una protección contra el software malicioso o malware incluida con Windows 10. En XenMobile, puede usar la directiva de dispositivo Defender para configurar la directiva de Microsoft Defender para Windows 10 para escritorios y tabletas.

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**.

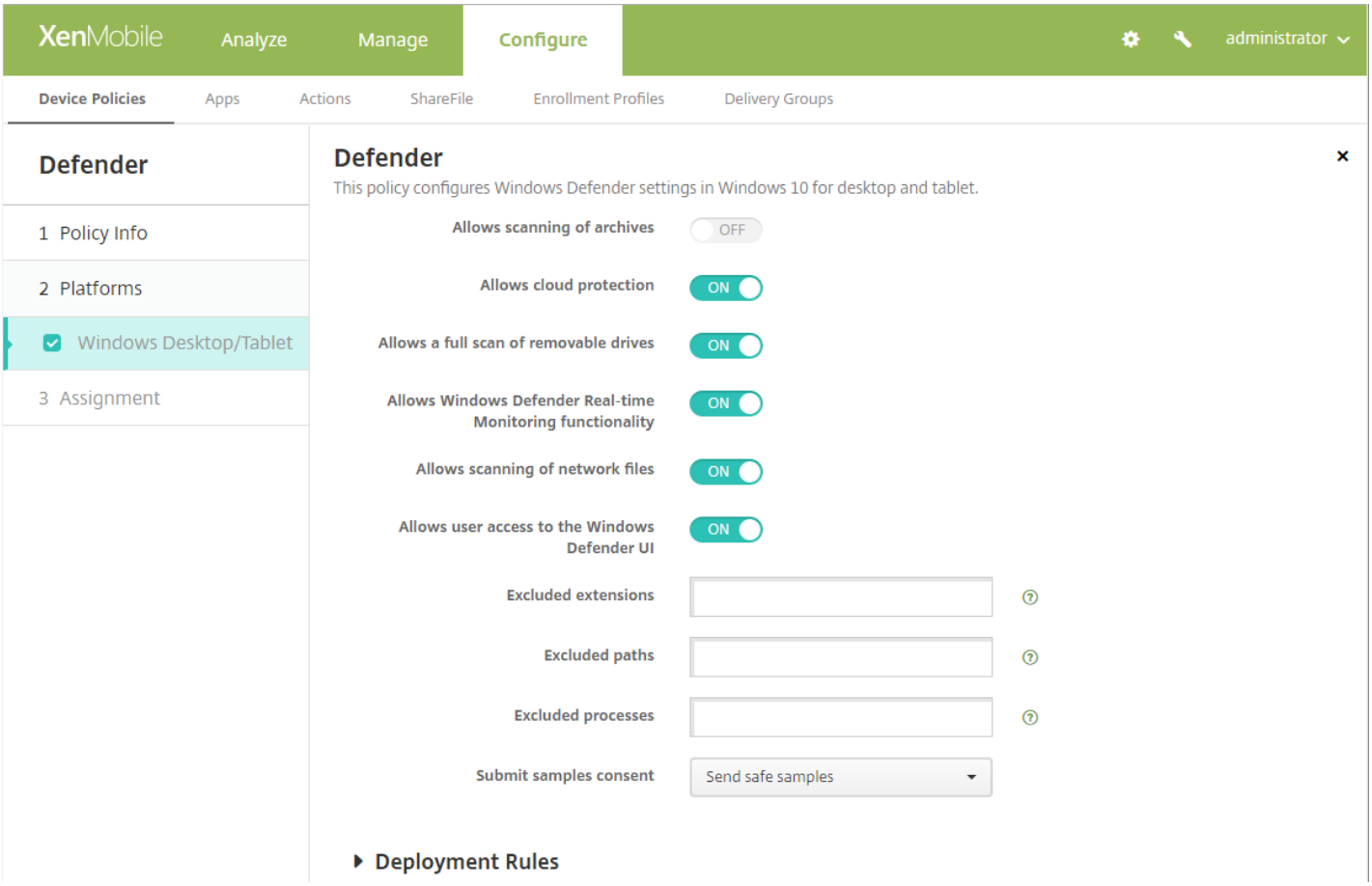
3. Empiece a teclear **Defender** y, a continuación, haga clic en ese nombre en los resultados de búsqueda. Aparecerá la página **Defender Policy Information**.



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 la directiva.



Configure estos parámetros:

- **Allows scanning of archives**. Permite o prohíbe que Defender analice archivos ya archivados. El valor predeterminado es **OFF**.
- **Allows cloud protection**. Permite o prohíbe que Defender envíe información a Microsoft sobre la actividad del malware. El valor predeterminado es **ON**.
- **Allows a full scan of removable drives**. Permite o prohíbe que Defender analice las unidades extraíbles (como lápices USB). El valor predeterminado es **ON**.
- **Allows Windows Defender Real-time Monitoring functionality**. El valor predeterminado es **ON**.
- **Allows scanning of network files**. Permite o prohíbe que Defender analice archivos de red. El valor predeterminado es **ON**.
- **Allows user access to the Windows Defender UI**. Especifica si los usuarios pueden acceder a la interfaz de usuario de Windows Defender. Este parámetro surte efecto la próxima vez que se inicia el dispositivo del usuario. Si este parámetro está en **OFF**, los usuarios no recibirán ninguna notificación de Windows Defender. El valor predeterminado es **ON**.
- **Excluded extensions**. Las extensiones a excluir de los análisis en tiempo real o programados. Para separar las extensiones, use la barra vertical **|**. Por ejemplo: "lib|obj".
- **Excluded paths**. Las rutas a excluir de los análisis en tiempo real o programados. Para separar las rutas, use la barra vertical **|**. Por ejemplo: "C:\Ejemplo|C:\Ejemplo1".
- **Excluded processes**. Los procesos a excluir de los análisis en tiempo real o programados. Para separar los procesos, use la barra vertical **|**. Por ejemplo: C:\Ejemplo.exe|C:\Ejemplo1.exe".
- **Submit samples consent**. Controla si se envían a Microsoft archivos que pueden requerir mayor análisis para determinar si son malintencionados. Opciones: **Always prompt** (Preguntar siempre), **Send safe samples** (Enviar muestras seguras),

Never send (No enviar nunca), **Send all samples** (Enviar todas las muestras). El valor predeterminado es **Send safe samples**.

6. Configure las reglas de implementación.

7. Haga clic en **Next**. Aparecerá la página de asignación **Defender**.

8. Junto a **Choose delivery groups**, escriba para buscar un grupo de entrega. Para asignar la directiva a un grupo o varios, seleccione los grupos en la lista. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

9 Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si hace clic en **OFF**, no se aplican las demás opciones.
- 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**.

10. Haga clic en **Save** para guardar la directiva.

Directiva de dispositivo para la eliminación de archivos y carpetas

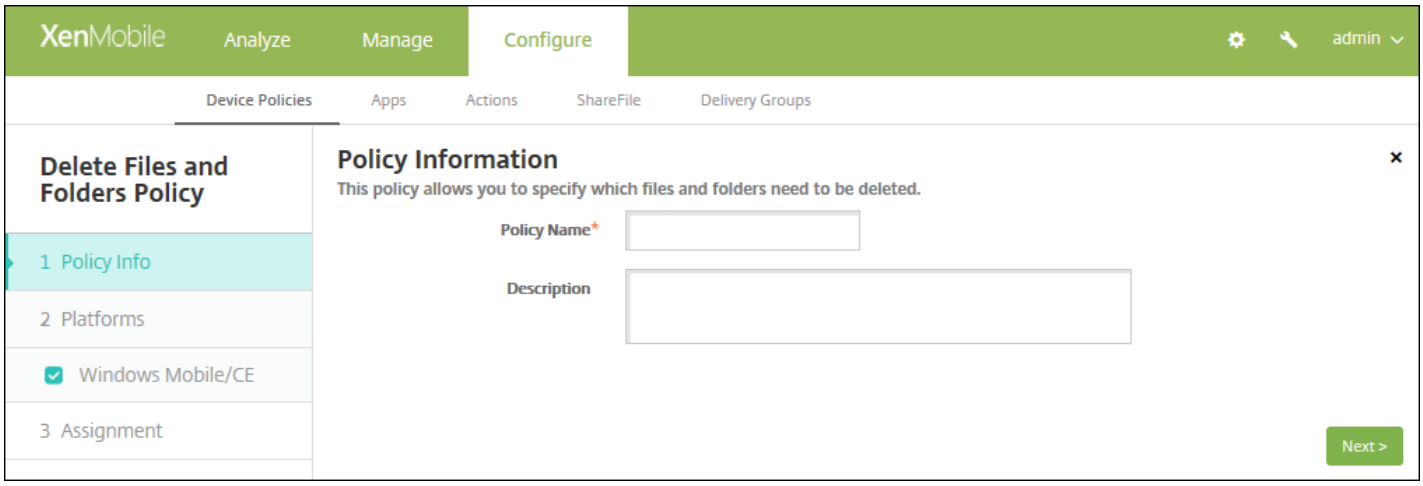
Feb 27, 2017

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**.

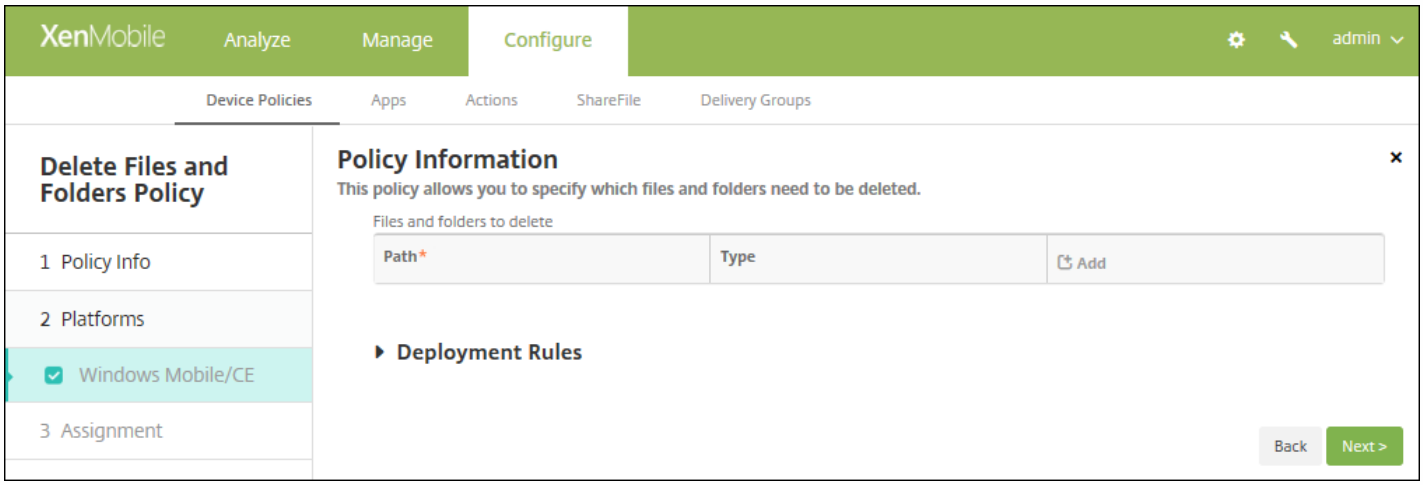
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Delete Files and Folders**. Aparecerá la página de información **Delete Files and Folders Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



6. Configure estos parámetros:

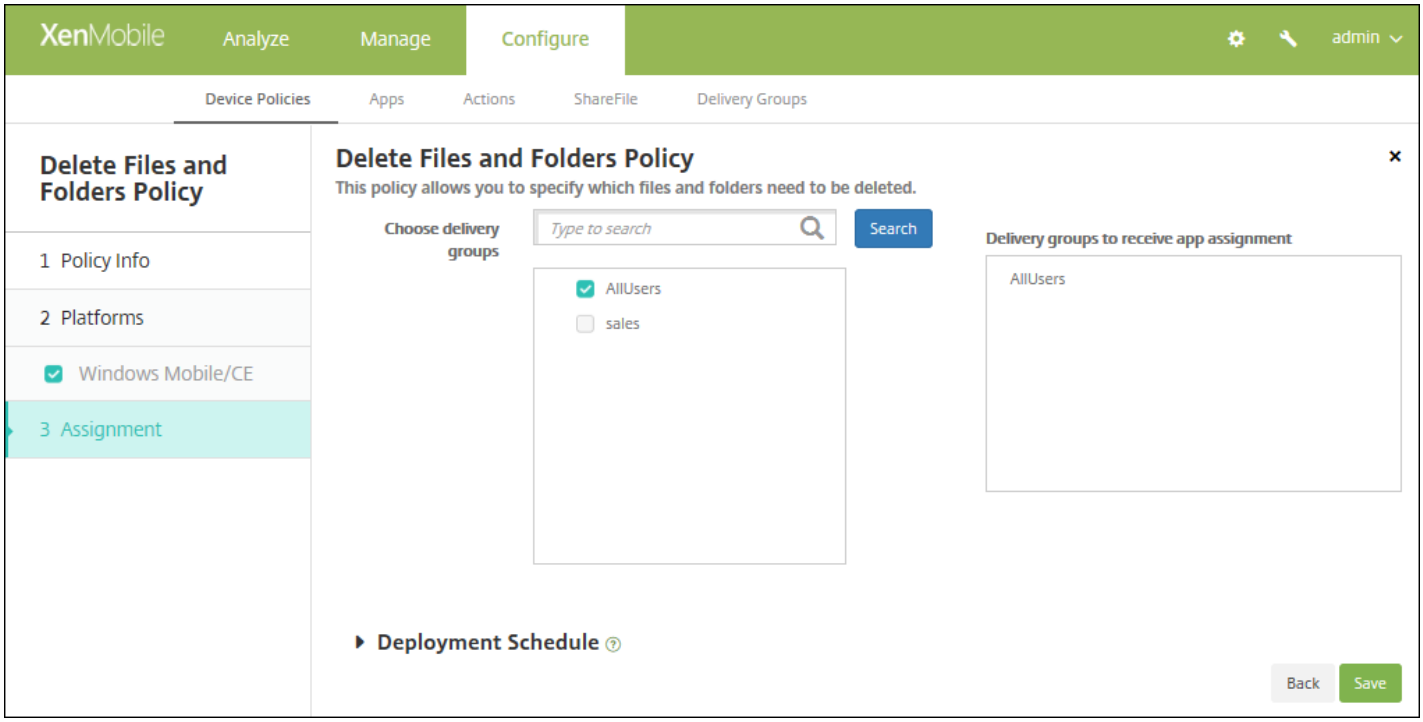
- **Files and folders to delete**. Para cada archivo o carpeta que quiera eliminar, haga clic en "Add" y lleve a cabo lo siguiente:
  - **Path**. Escriba la ruta al archivo o carpeta.
  - **Type**. En la lista, haga clic en "File" o "Folder". El valor predeterminado es File.
  - Haga clic en **Save** 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 guardarlos, o bien en **Cancel** para descartarlos.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para la eliminación de valores y claves de Registro

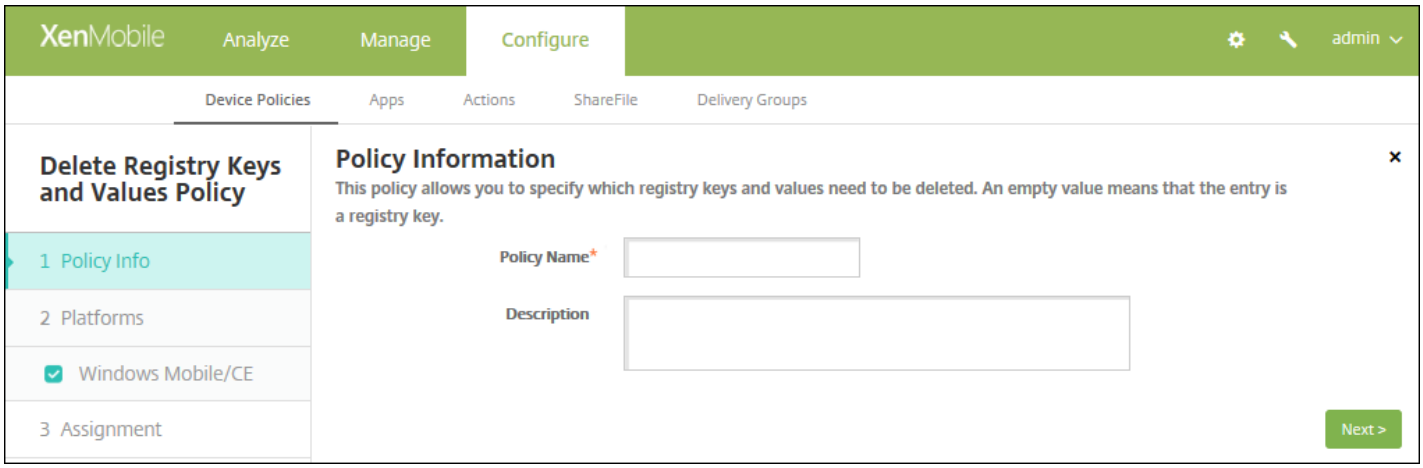
Feb 27, 2017

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**.

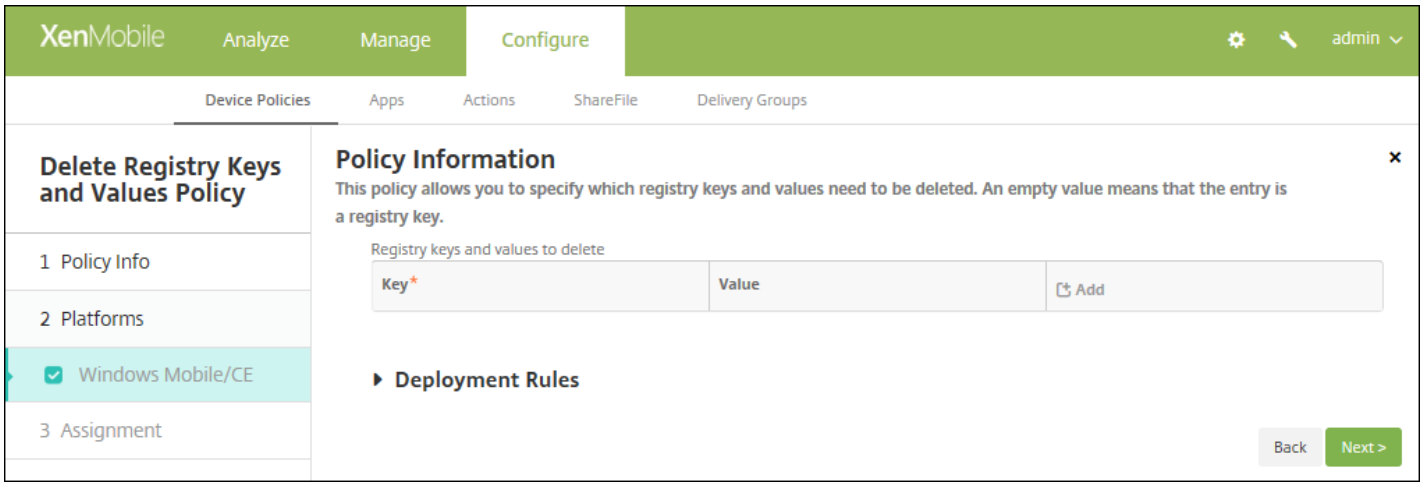
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Delete Registry Keys and Values**. Aparecerá la página de información **Delete Registry Keys and Values Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



6. Configure estos parámetros:

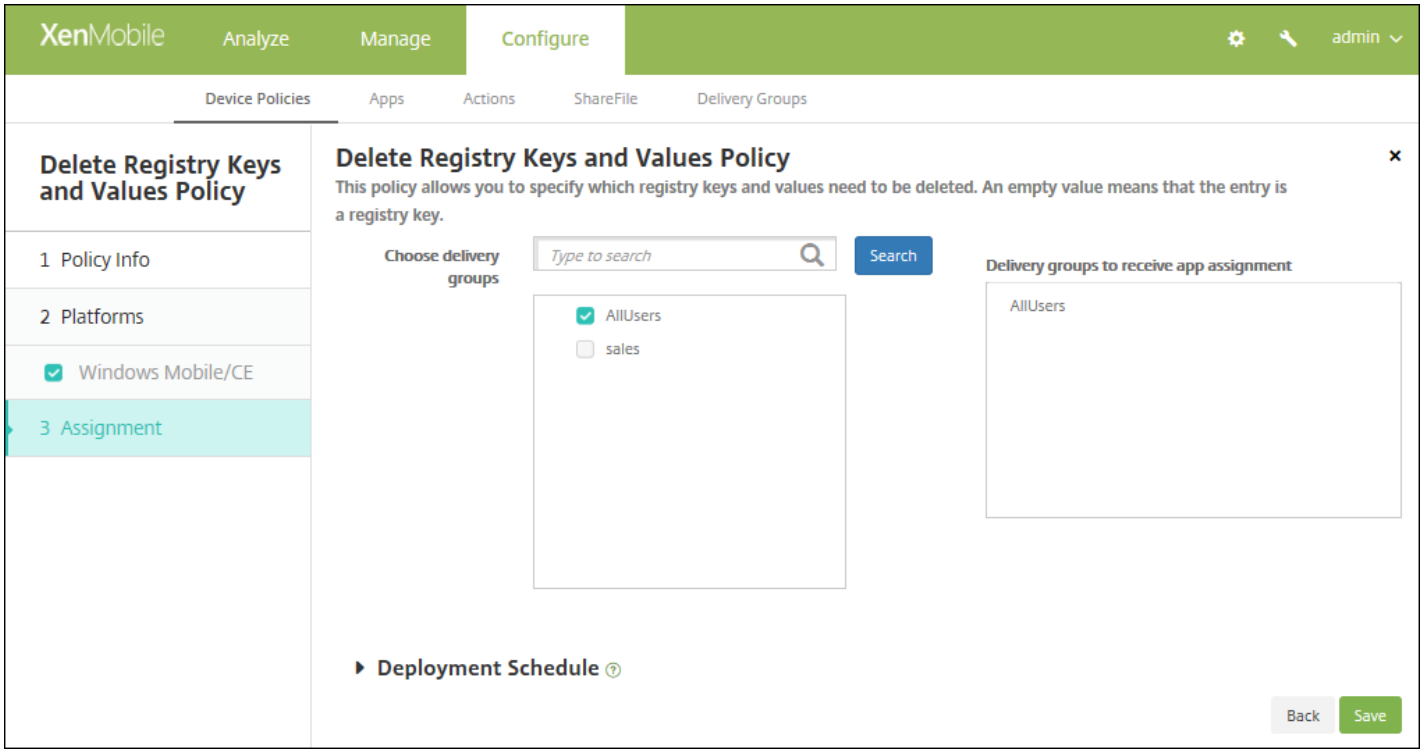
- **Registry keys and values to delete**. Para cada valor y clave del Registro que quiera eliminar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Key**. Escriba la ruta de la clave del Registro. Este campo es obligatorio. La ruta de la clave del Registro debe empezar por HKEY_CLASSES_ROOT\, 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 guardarlos, o bien en **Cancel** para descartarlos.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 del estado de dispositivos

Feb 27, 2017

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:

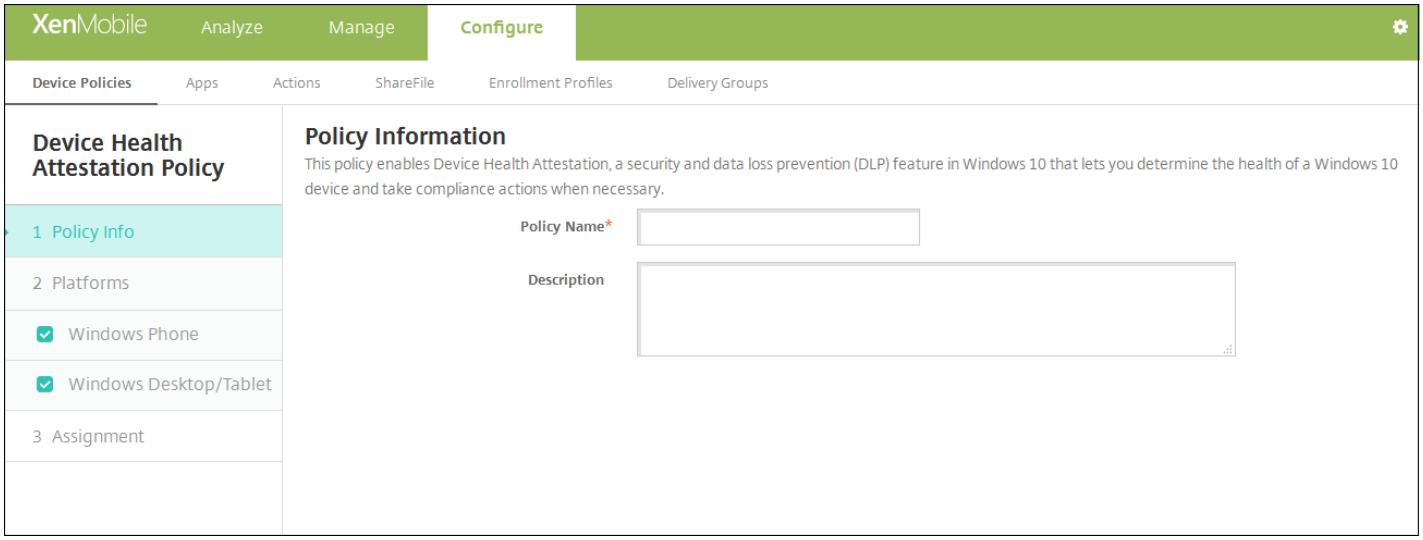
- AIKPresent
- BitLockerStatus
- BootDebuggingEnabled
- BootManagerRevListVersion
- CodeIntegrityEnabled
- CodeIntegrityRevListVersion
- DEPPolicy
- ELAMDriverLoaded
- IssuedAt
- KernelDebuggingEnabled
- PCR
- ResetCount
- RestartCount
- SafeModeEnabled
- SBCPHash
- SecureBootEnabled
- TestSigningEnabled
- VSMEnabled
- WinPEEnabled

Para obtener 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**.



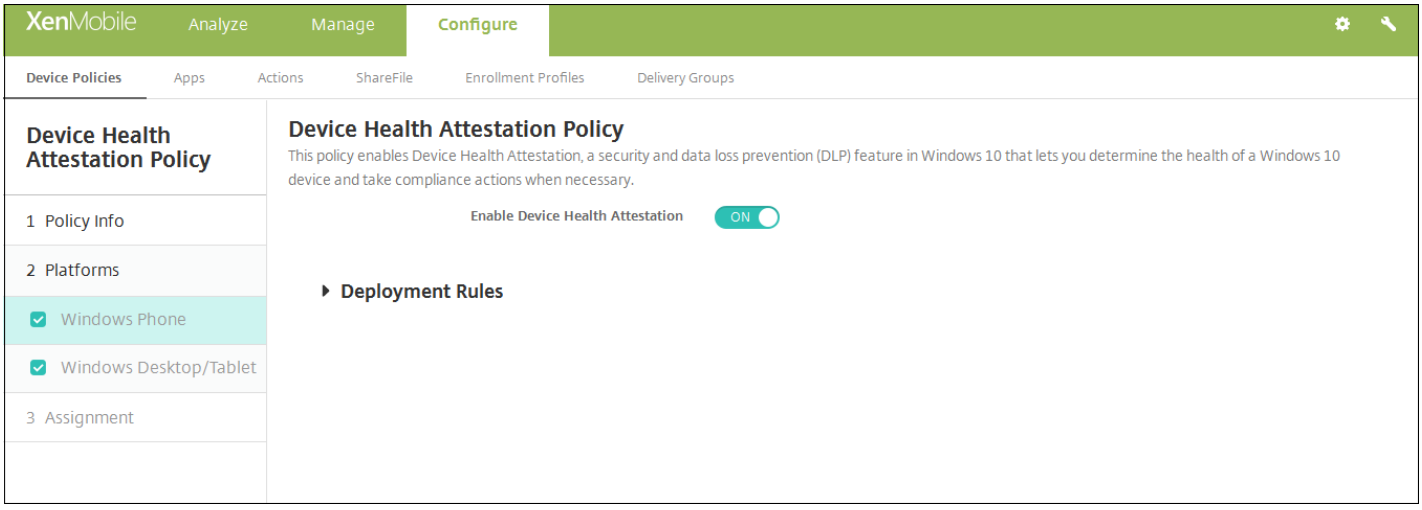
4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

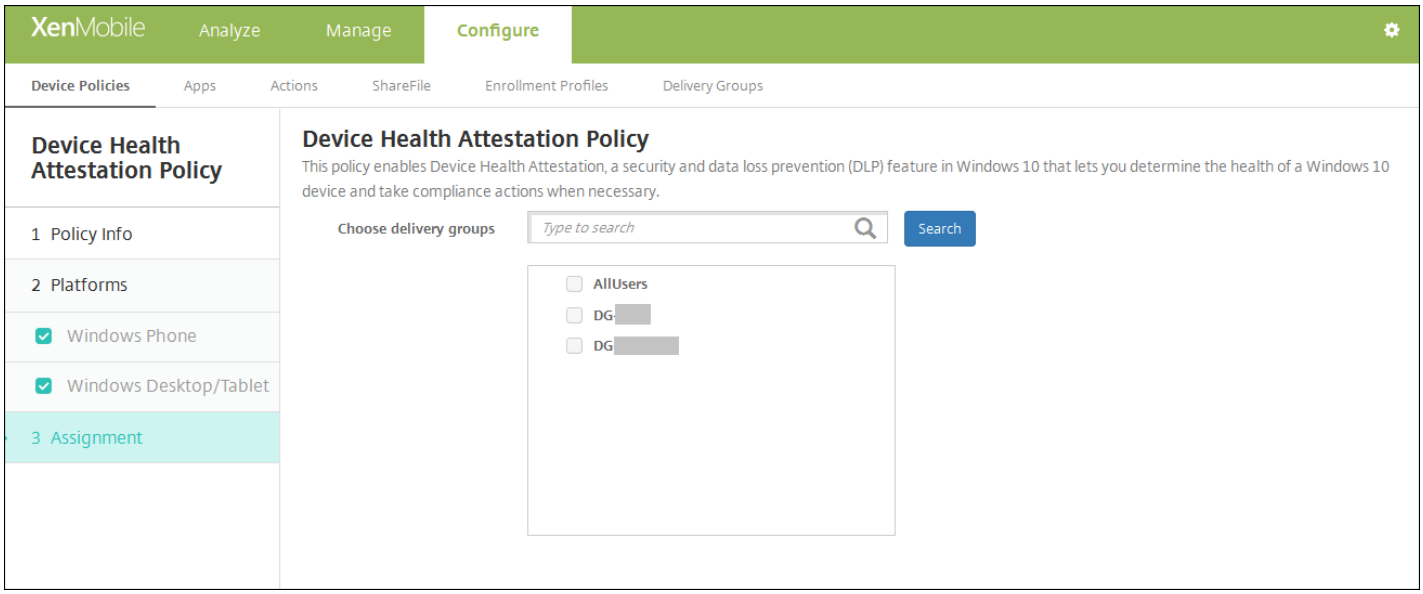


Configure este parámetro para cada plataforma seleccionada:

- **Enable Device Health Attestation**. Seleccione si se debe requerir la atestación del 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para nombres de dispositivos

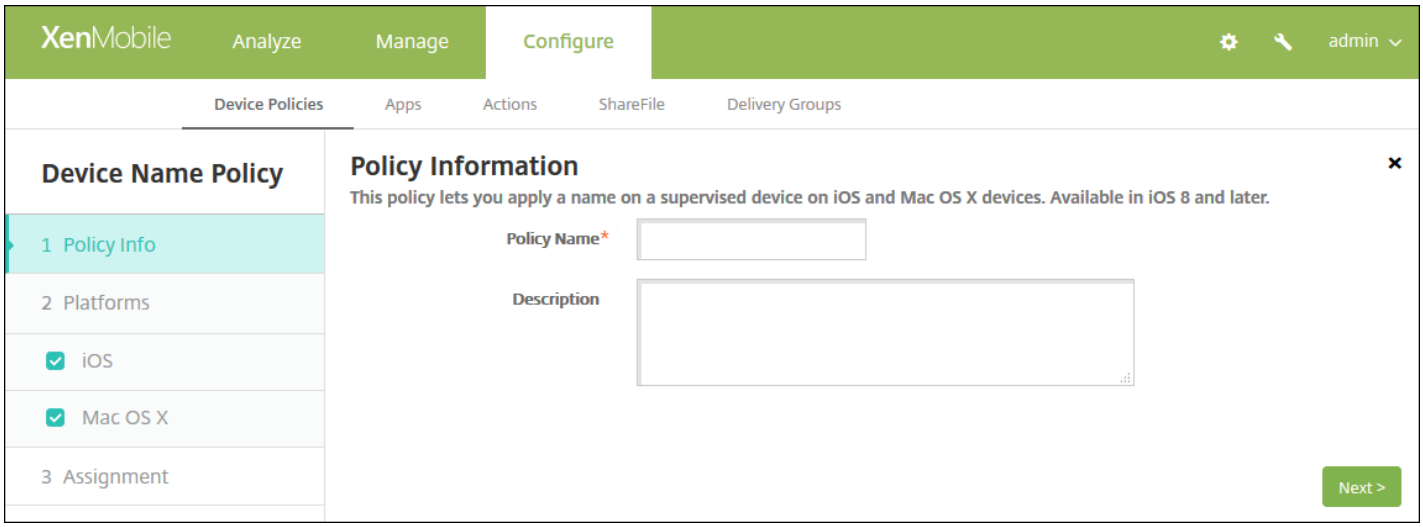
Feb 27, 2017

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 **Device Name Policy information**.



4. En el panel **Policy Information**, escriba la información siguiente:

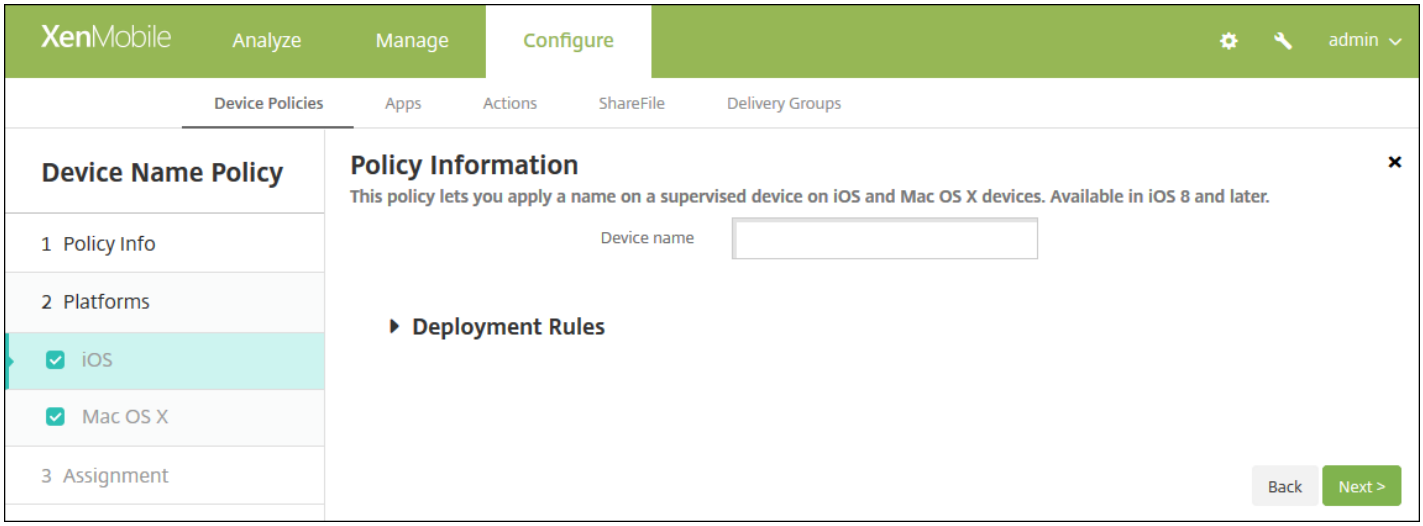
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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

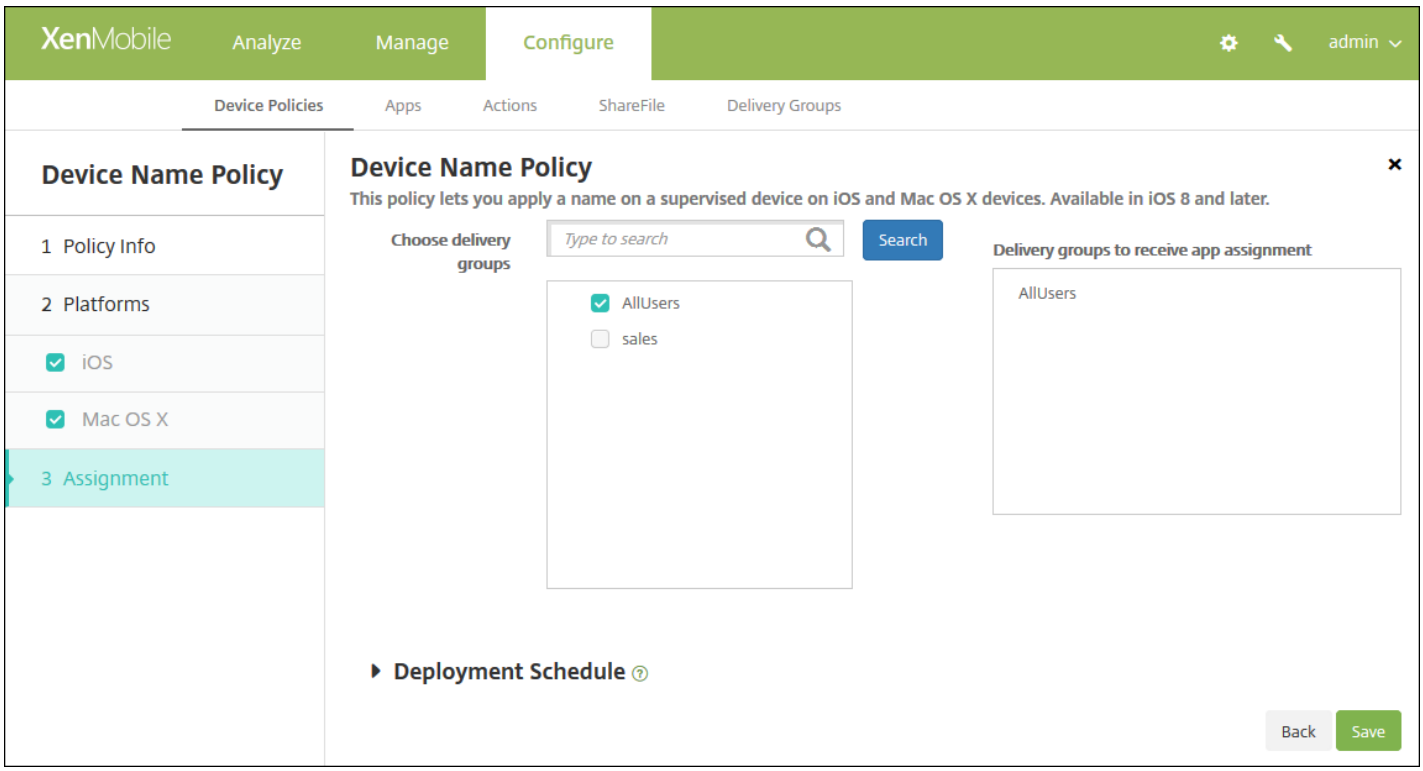


Configure este parámetro para las plataformas que elija:

- **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 de **Device Name Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un

grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo Enterprise Hub

Feb 27, 2017

Una directiva Enterprise Hub para dispositivos Windows Phone permite distribuir aplicaciones a través de la tienda Enterprise Hub de la empresa.

Antes de crear la directiva, necesita lo siguiente:

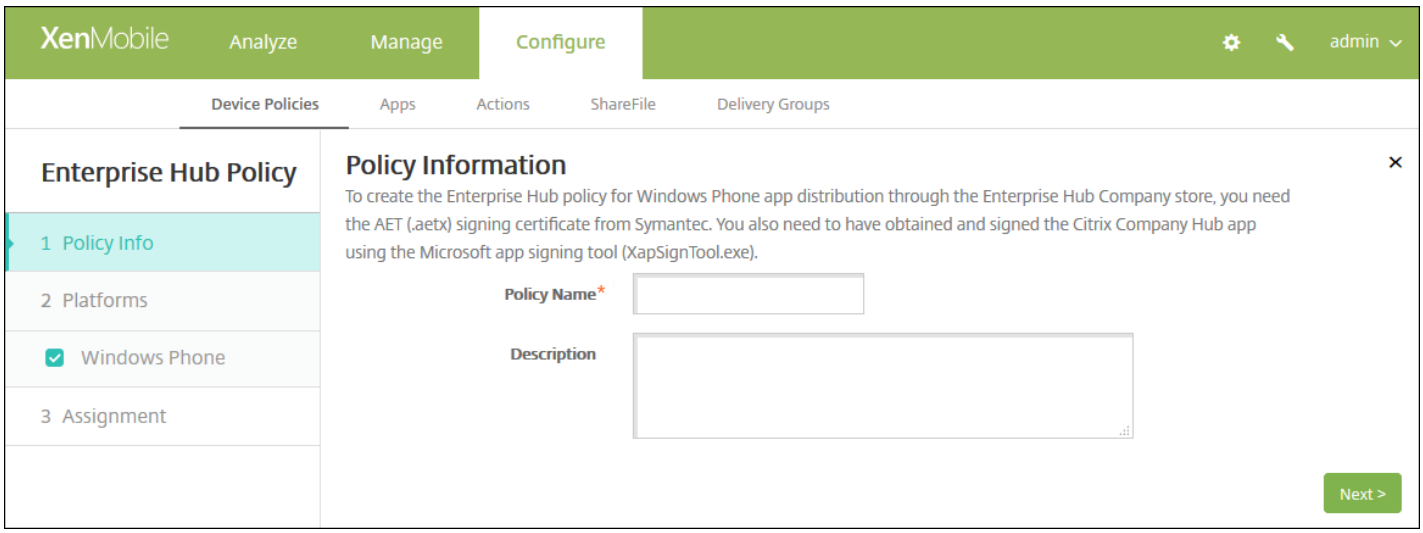
- Un certificado de firma AET (.aetx) de Symantec
- La aplicación Citrix Company Hub firmada mediante la herramienta de firma de aplicaciones de Microsoft (XapSignTool.exe)

Nota: XenMobile solo admite una directiva Enterprise Hub por modo de Windows Phone Secure Hub. Por ejemplo, para cargar Windows Phone Secure Hub en XenMobile Enterprise Edition, no debe crear varias directivas Enterprise Hub con versiones diferentes de Secure Hub 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**.

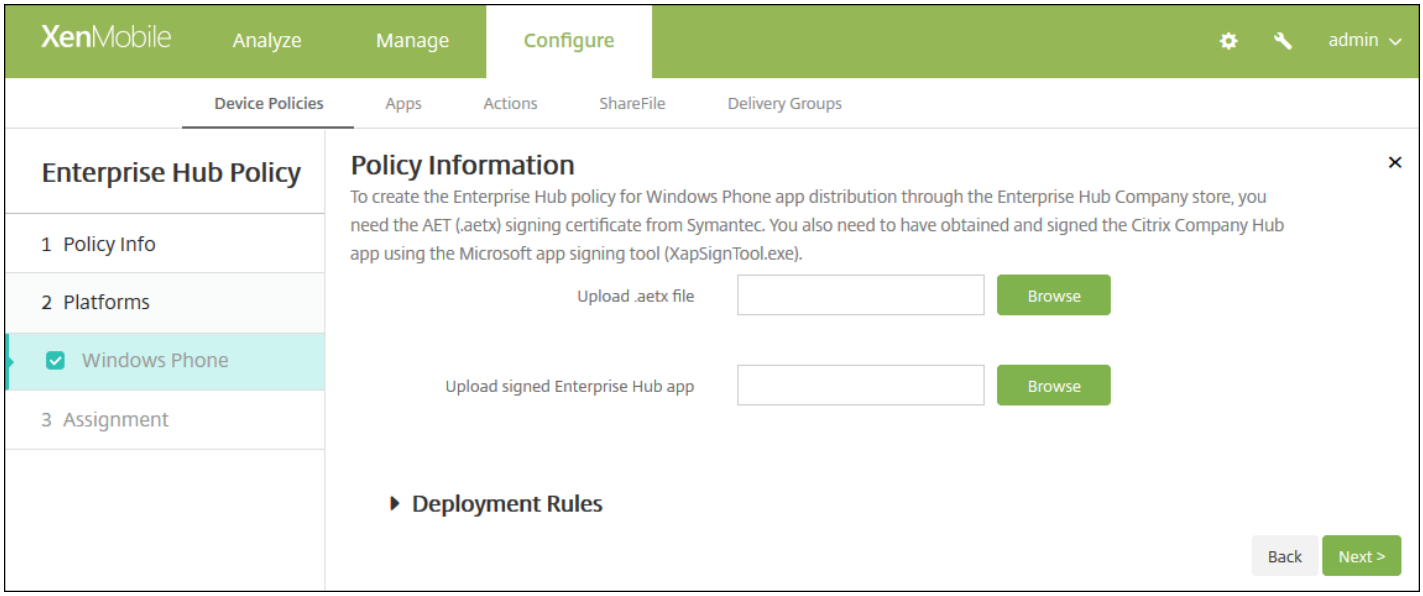
3. Haga clic en **More** y, en **XenMobile agent**, haga clic en **Enterprise Hub**. Aparecerá la página **Enterprise Hub Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de la plataforma **Windows Phone**.

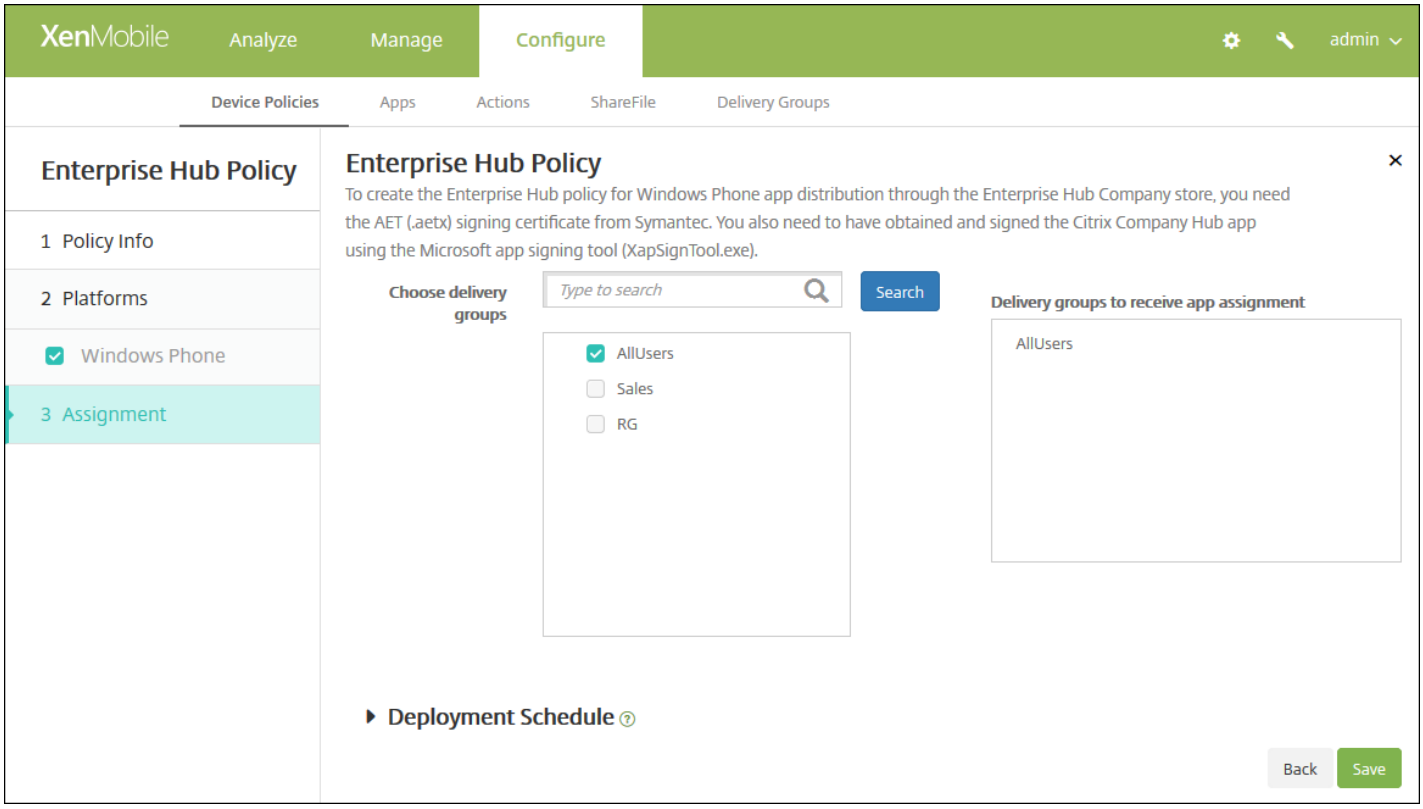


6. Configure estos parámetros:

- **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 de **Enterprise Hub Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo sobre archivos

Feb 27, 2017

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.

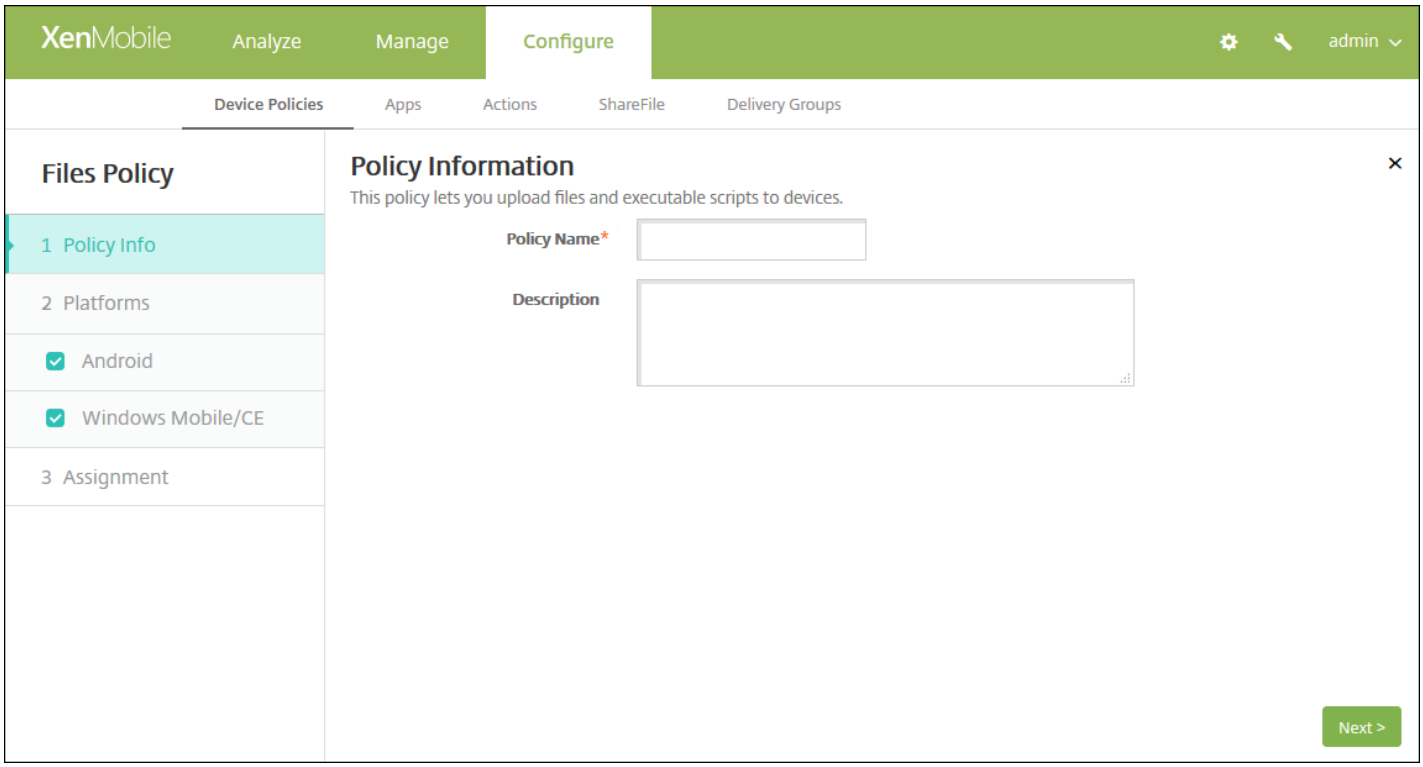
Puede agregar los siguientes tipos de archivo con esta directiva:

- 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**.

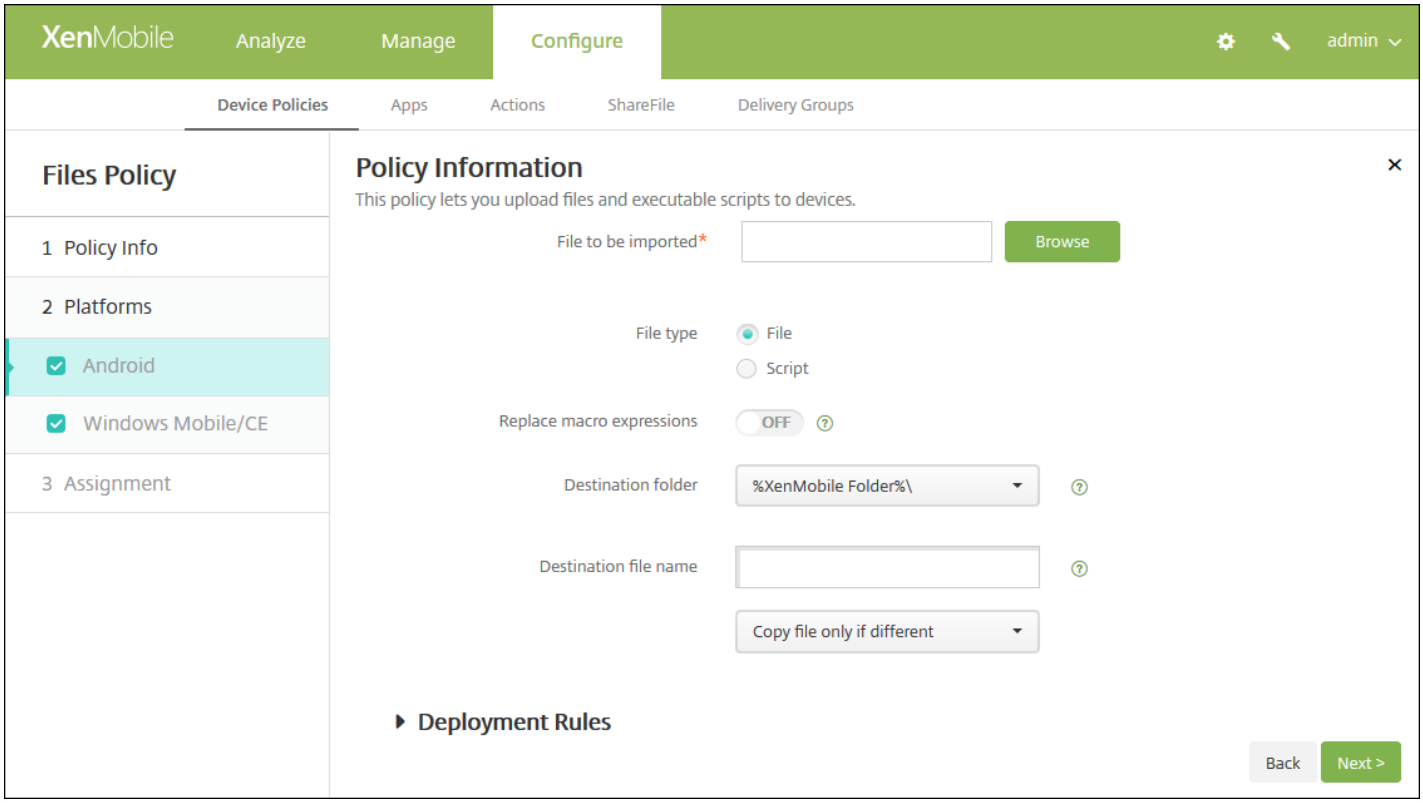
3. Expanda **More** y, en **Apps**, haga clic en **Files**. Aparecerá la página de información **Files Policy**.



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.

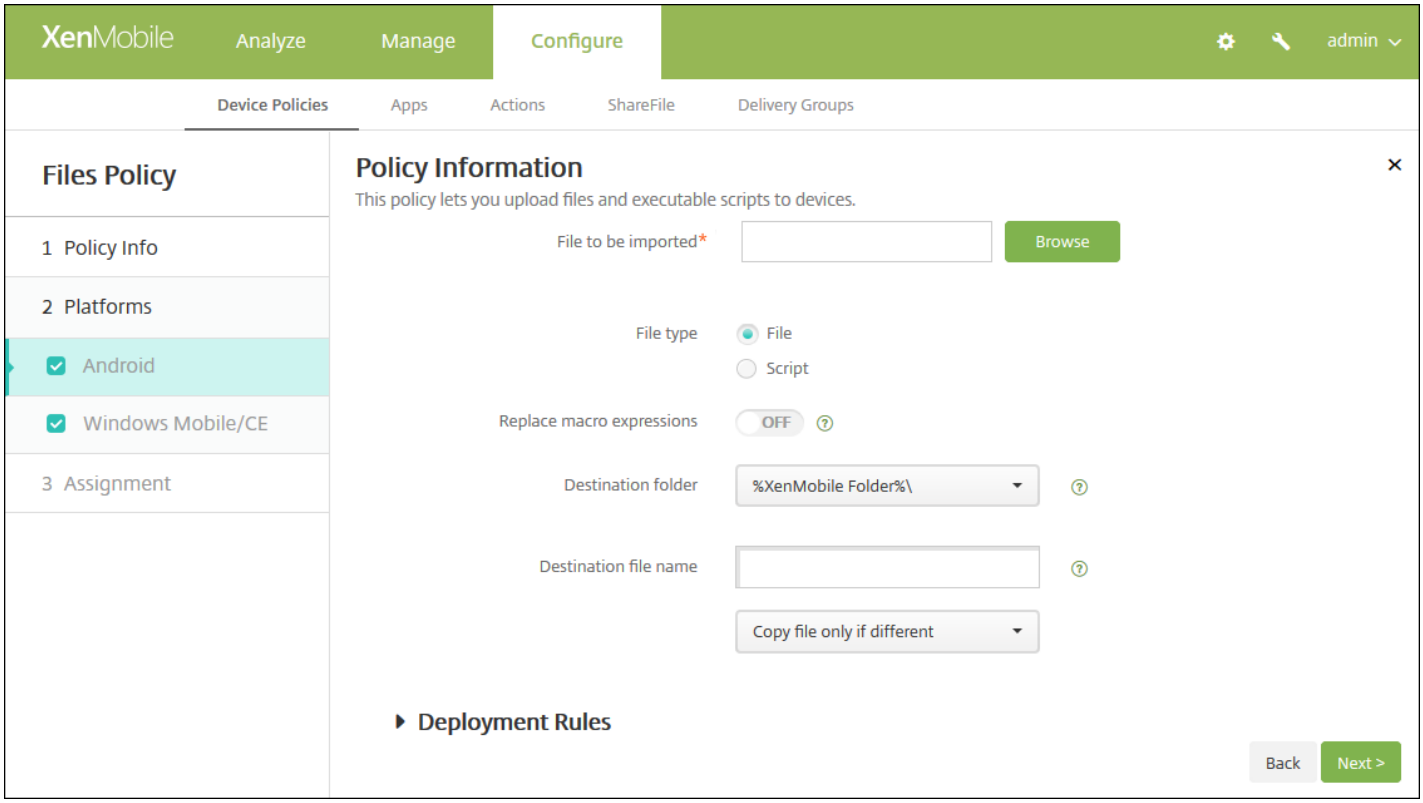
5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



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.

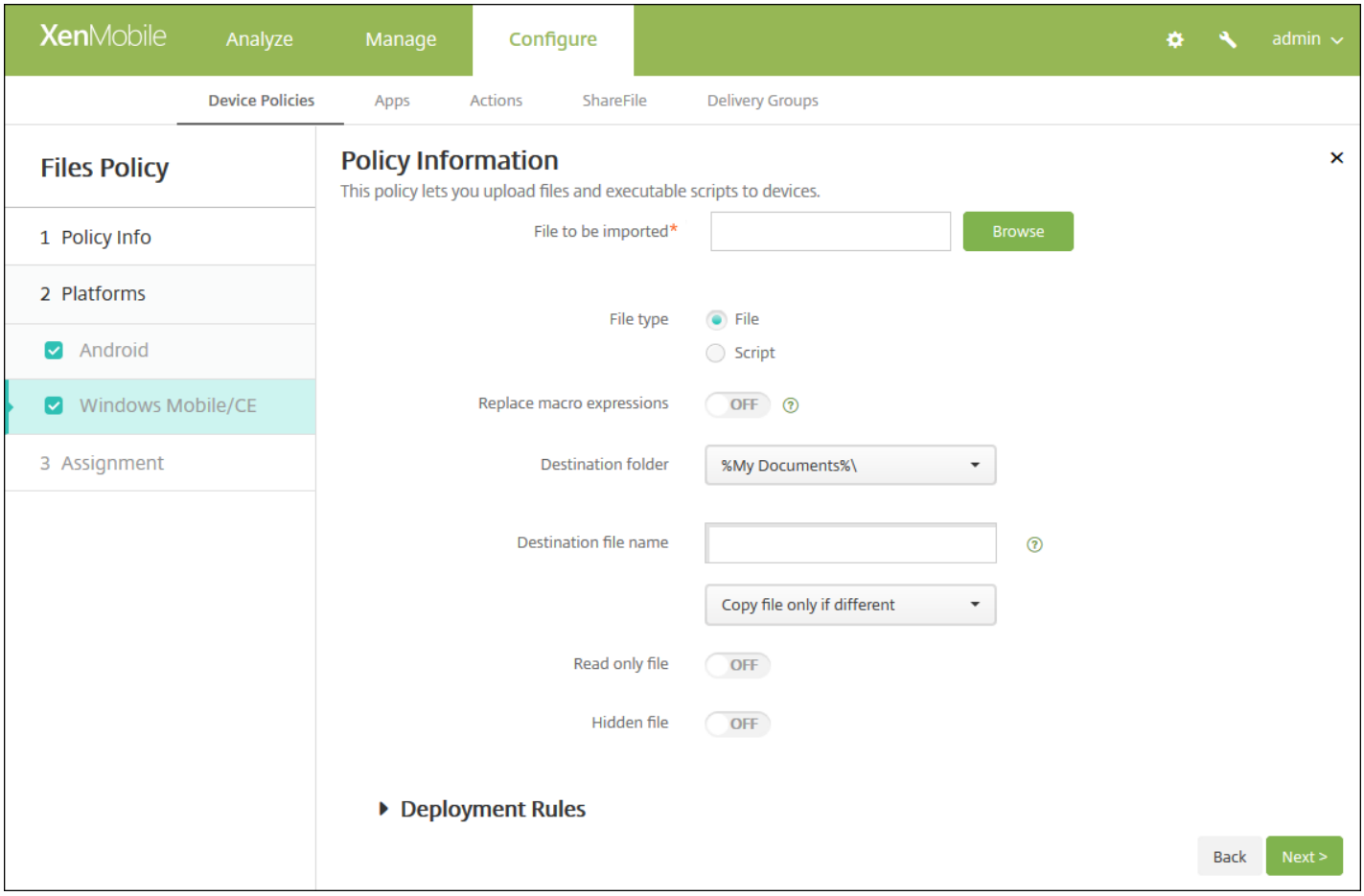
Configuración de los parámetros de Android



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 la macro en un script por 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 quiere, puede dar aquí otro nombre 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



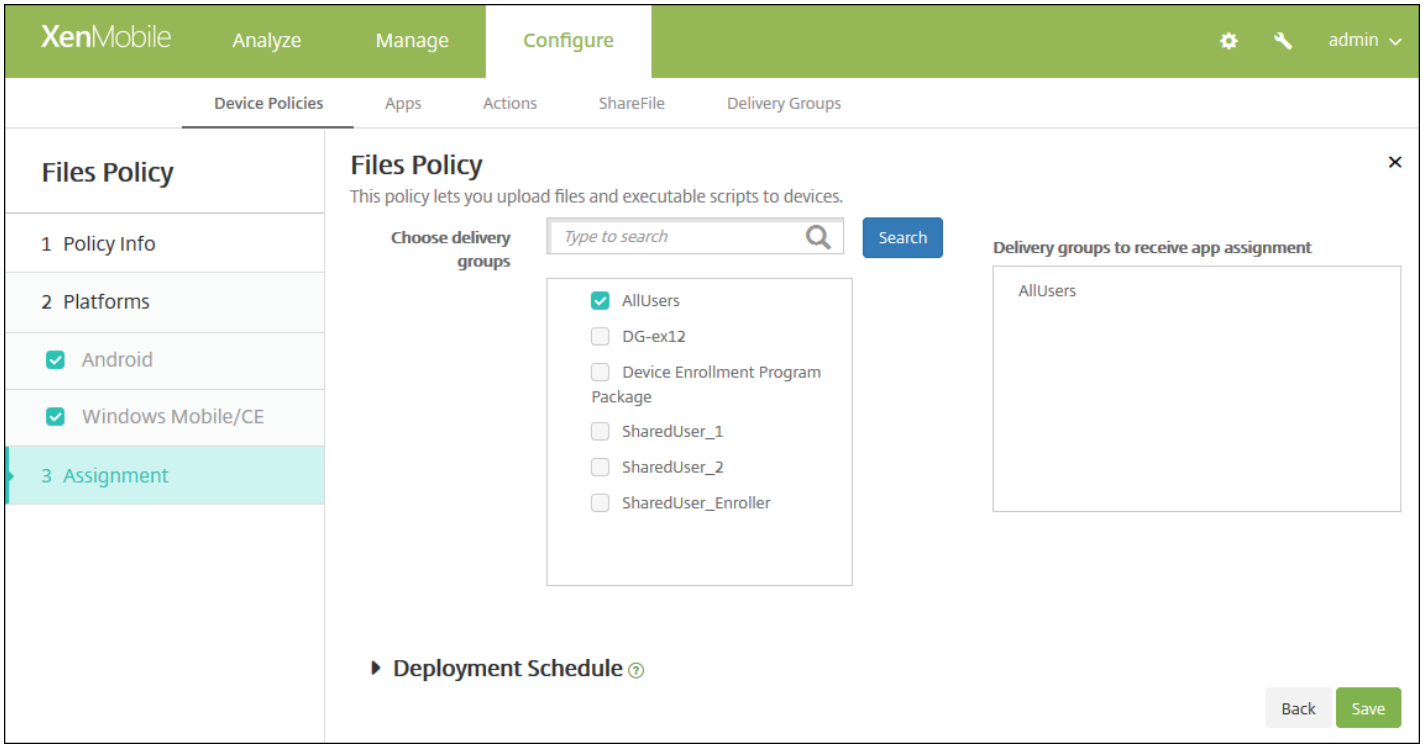
Configure los siguientes parámetros:

- **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 la macro en un script por 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:
  - %Almacenamiento Flash%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**. Si quiere, puede dar aquí otro nombre 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 de **Files Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 fuentes

Feb 27, 2017

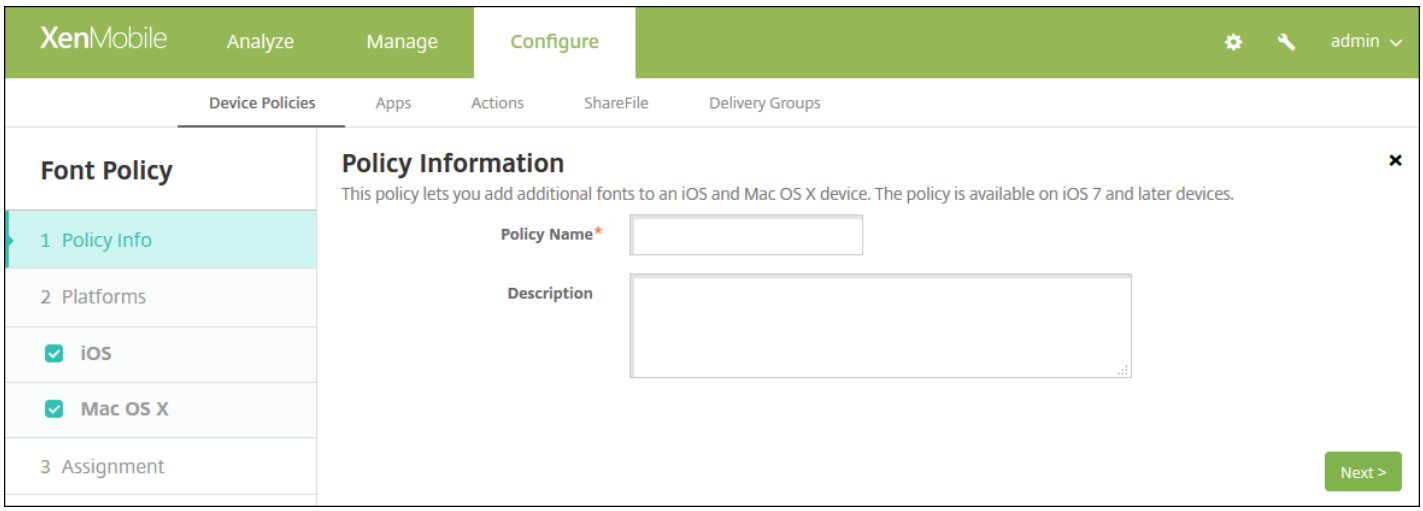
En XenMobile, puede agregar una directiva de dispositivos para agregar fuentes de texto adicionales a los dispositivos iOS y Mac OS X de los usuarios. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.oft). No se admiten las colecciones de fuentes (.ttc o .otc).

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:

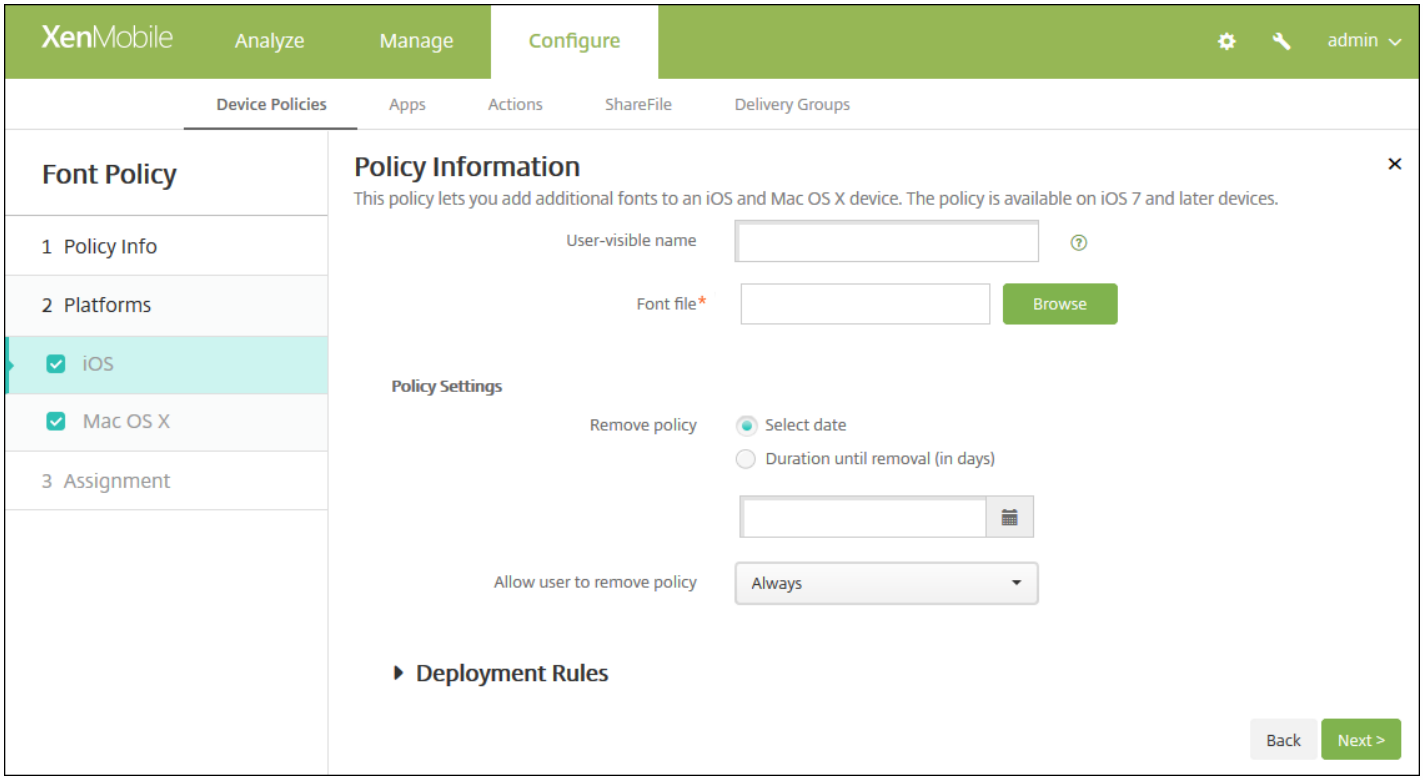
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

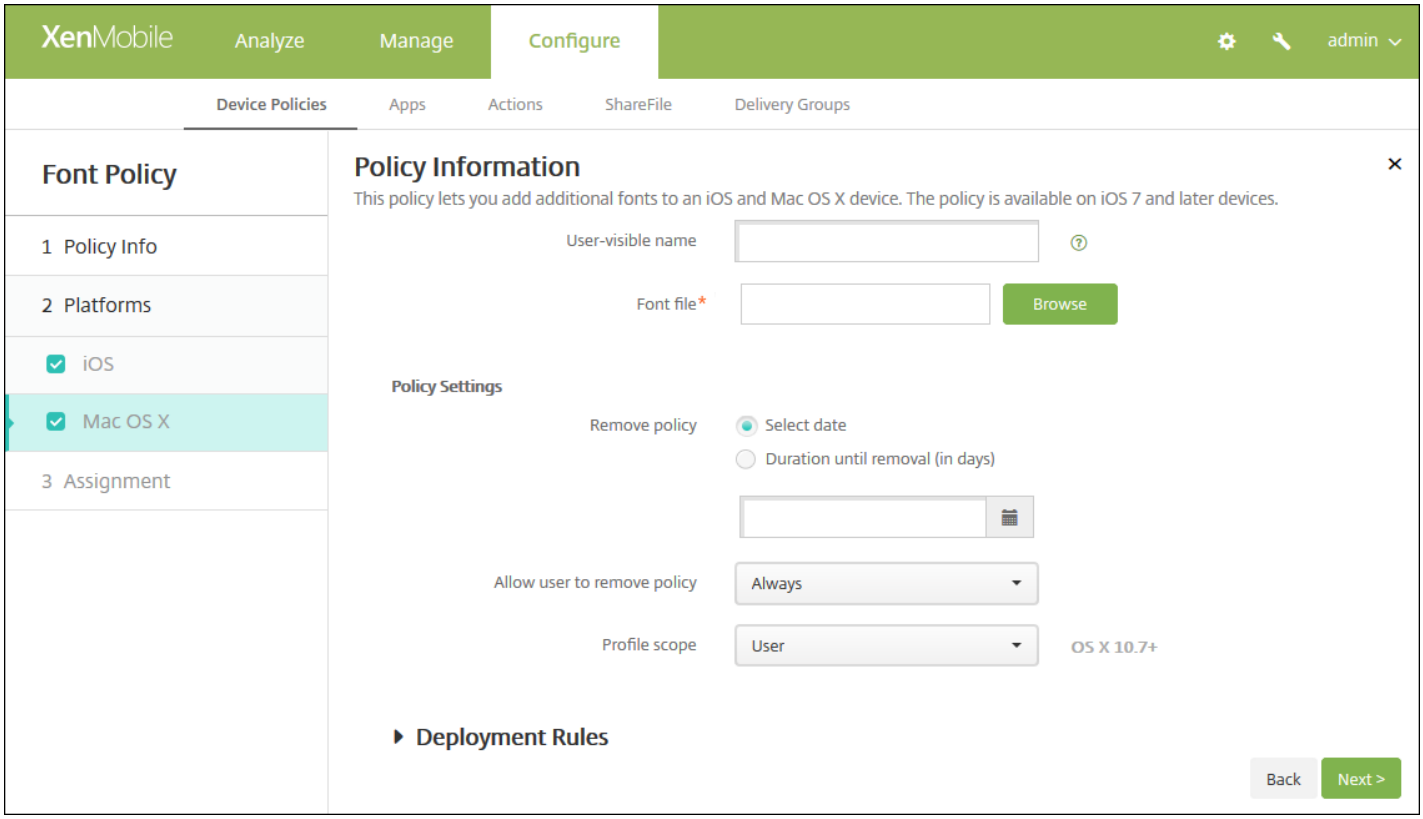
Configuración de los parámetros de iOS



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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

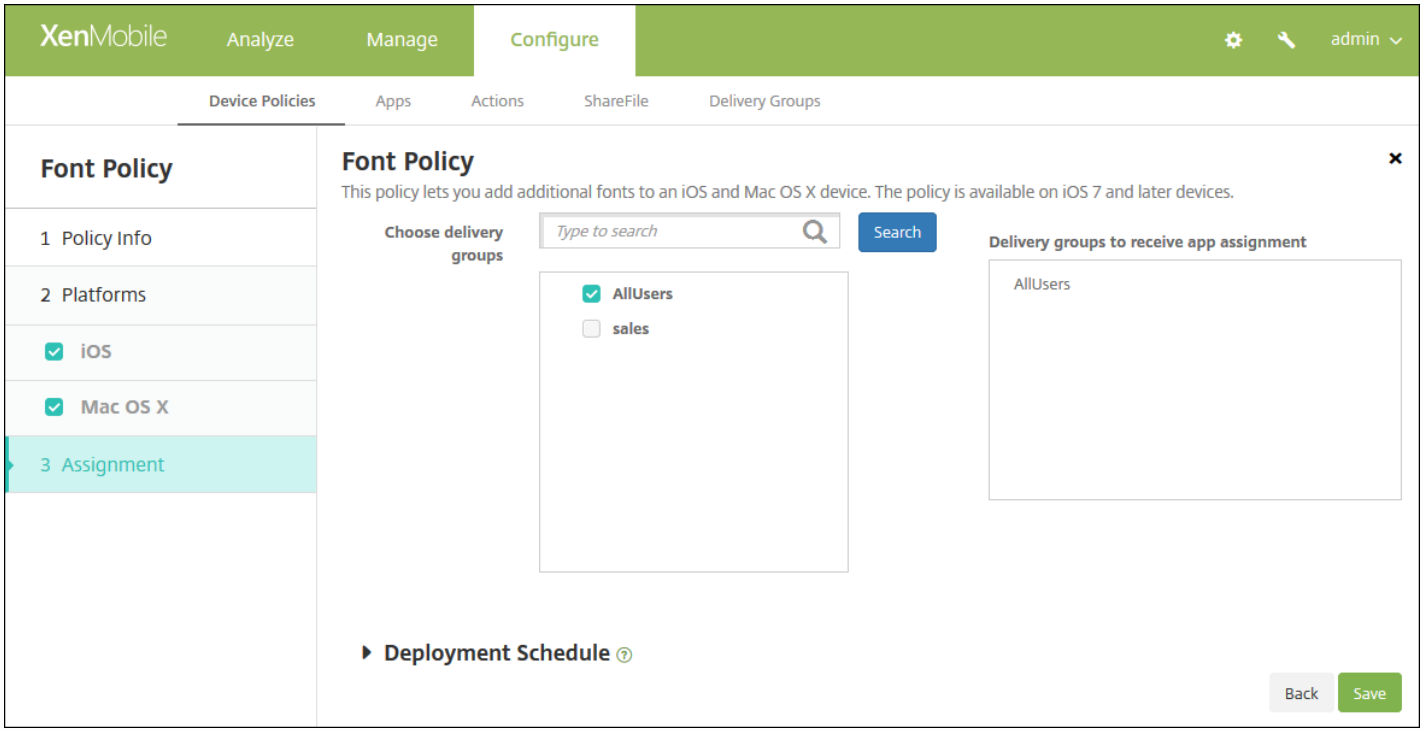


Configure los siguientes parámetros:

- **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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para el diseño de la pantalla de inicio

Feb 27, 2017

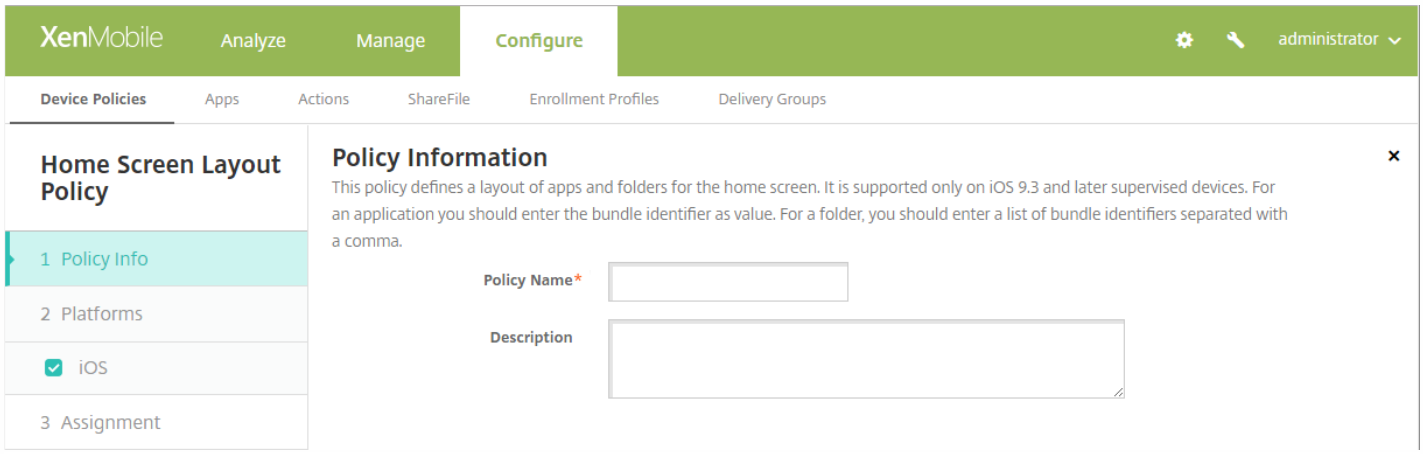
Puede especificar la distribución de las aplicaciones y las carpetas en la pantalla de inicio de iOS. La directiva de dispositivo Home screen layout (Diseño de la pantalla de inicio) es para dispositivos supervisados iOS 9.3 y versiones posteriores.

> ## Nota
>
> La implementación de varias directivas Home screen layout resulta en errores de iOS en el dispositivo. Esta limitación se aplica tanto si define el diseño de la pantalla de inicio a través de esta directiva de XenMobile o a través de 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**.

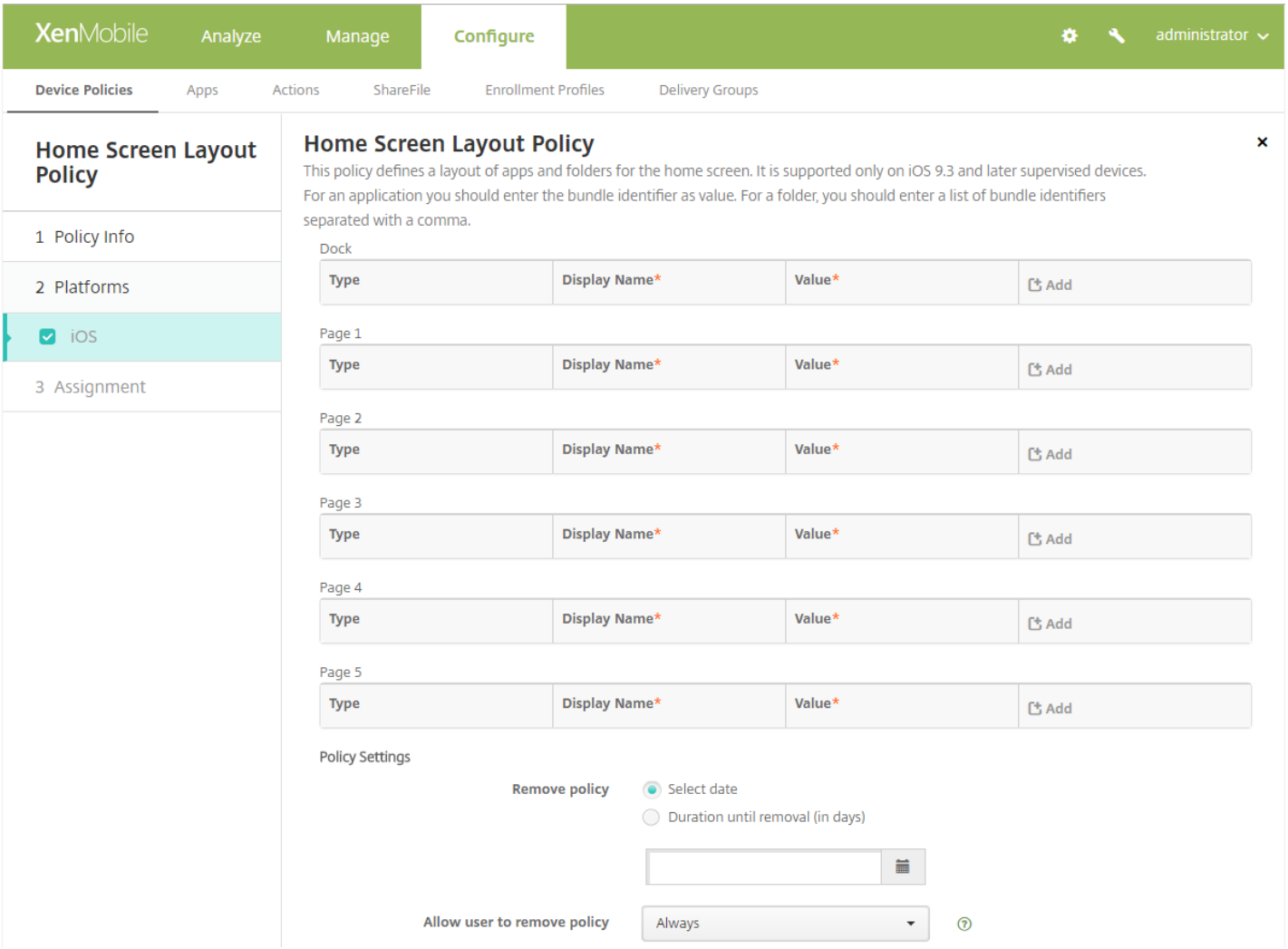
3. Empiece a teclear **Home screen layout** y, a continuación, haga clic en ese nombre en los resultados de búsqueda. Aparecerá la página de información **Home Screen Layout Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

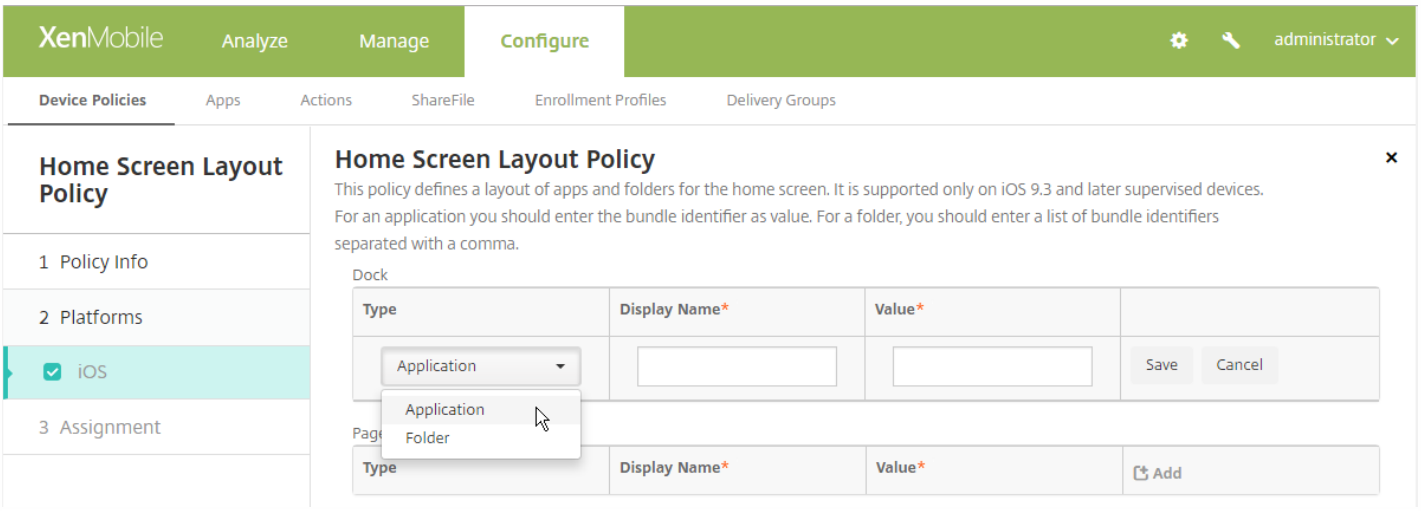
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá el panel de la plataforma **iOS**.



6. Configure estos parámetros:

- Para cada una de las áreas de la pantalla que quiere configurar (como **Dock** o **Page 1**), haga clic en **Add**.
- **Type**. Elija **Application** o **Folder**.



- **Display Name**. El nombre de la aplicación o la carpeta que aparecerá en la pantalla de inicio.
- **Value**. En caso de aplicaciones, el identificador del paquete. En caso de carpetas, una lista de identificadores de paquete, separados por comas.

Configuraciones de directivas

- **Remove policy**. Elija **Select date** y, a continuación elija una fecha del calendario, o bien, elija **Duration until removal** y especifique la cantidad de días.
- **Allow user to remove policy**. Especifique cuándo permitir que el usuario elimine la definición de la pantalla de inicio: **Always**, **Passcode required** (solo si proporciona un código de acceso) o **Never**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de la directiva **Windows Information Protection**.

9 Junto a **Choose delivery groups**, escriba para buscar un grupo de entrega. Para asignar la directiva a un grupo o varios, seleccione los grupos en la lista. 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 bien, haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si hace clic en **OFF**, no se aplican las demás opciones.
- 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para importación de perfiles de iOS y Mac OS X

Feb 27, 2017

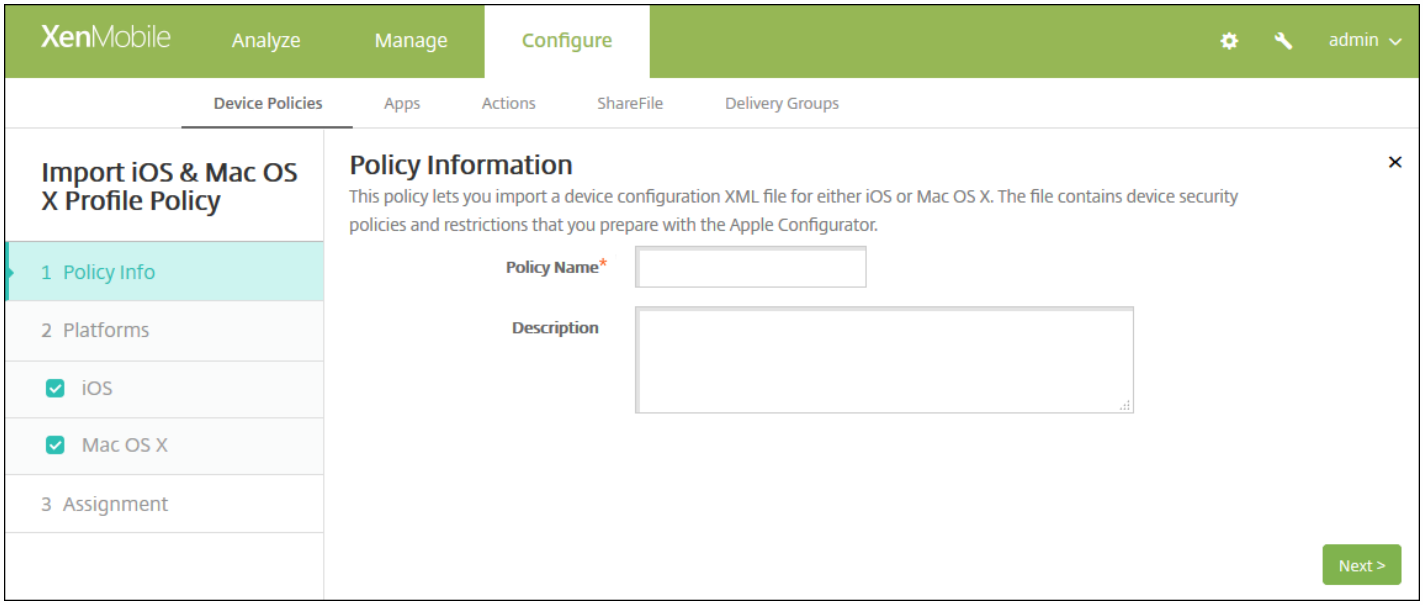
Puede importar en XenMobile archivos XML de configuración de dispositivos iOS y OS X. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator.

Puede colocar un dispositivo iOS en modo supervisado mediante Apple Configurator como se describe más adelante en este artículo. 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**.

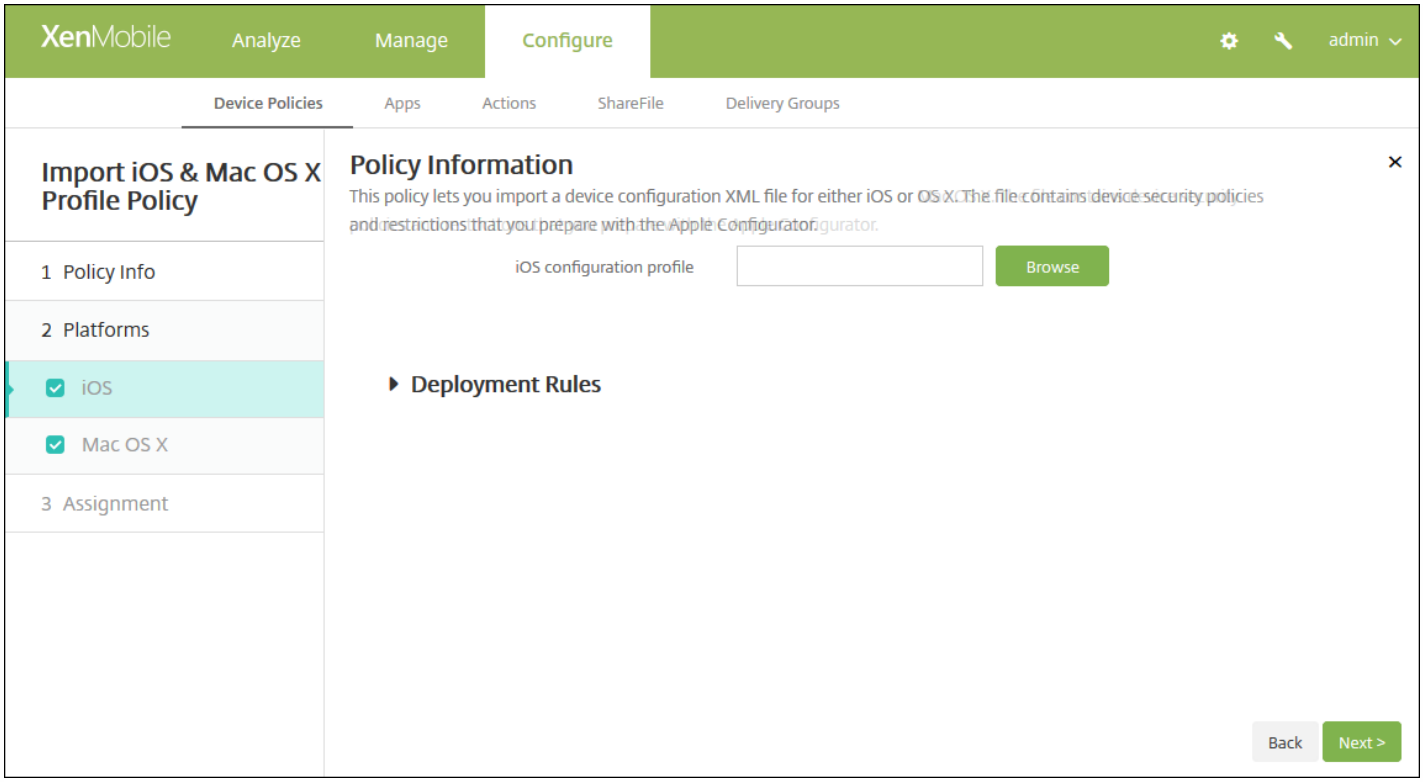
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Import iOS & Mac OS X Profile**. Aparecerá la página de información **Import iOS & Mac OS X Profile Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

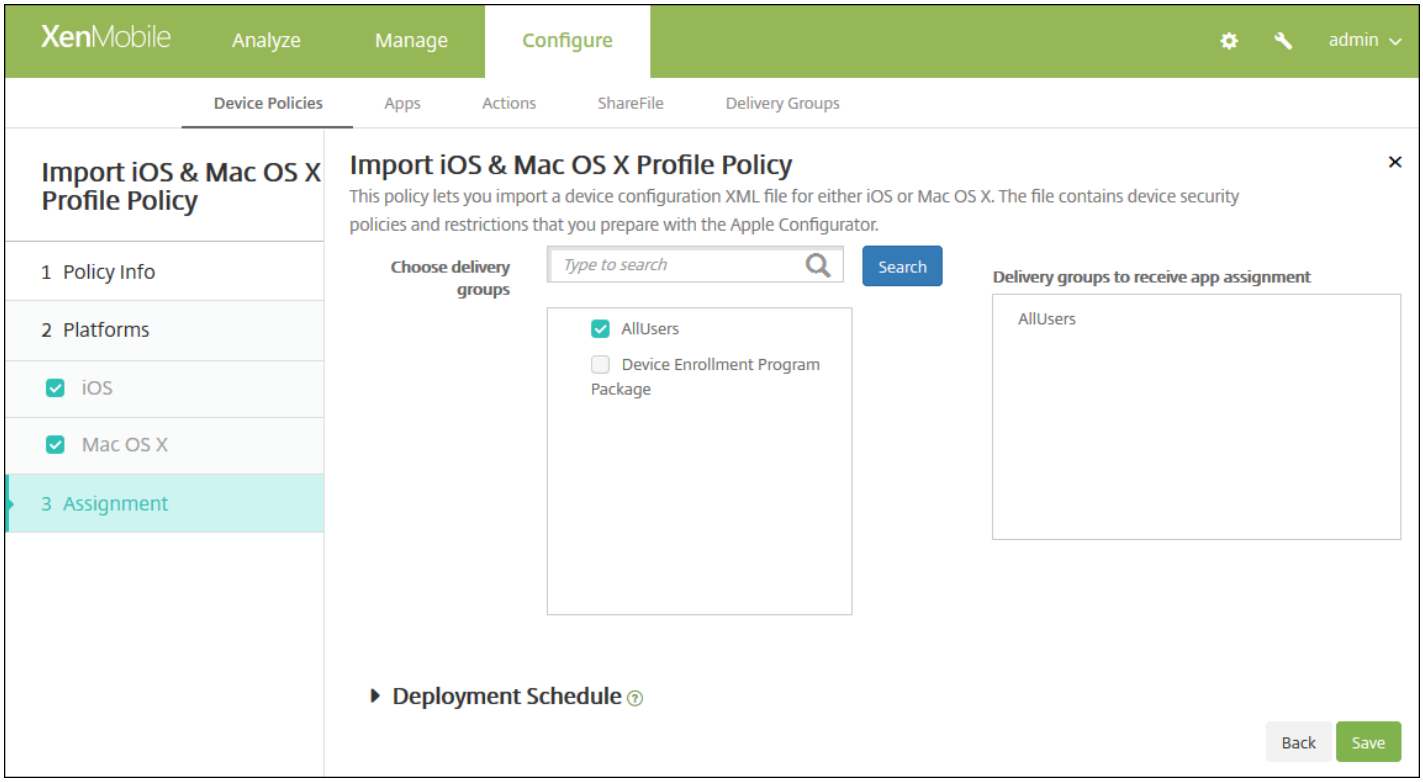
Cuando termine de configurar los parámetros de configuración de una plataforma, consulte el paso 8 para configurar las reglas de implementación de esa plataforma.

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.

9 Haga clic en **Next**. Aparecerá la página de asignación **Import iOS & Mac OS X Profile Policy**.



10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

Cómo colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

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:

a. 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.

c. Si lo prefiere, puede proporcionar un nombre para el dispositivo.

c. 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**.

Directiva de quiosco para Samsung SAFE

Feb 27, 2017

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 presente en el dispositivo móvil, como se describe en Directivas de claves de licencia para la administración de dispositivos móviles 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 quiere quitar los dispositivos del modo quiosco, cree una nueva directiva de dispositivo Kiosk que tenga el parámetro **Kiosk mode** establecido en **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

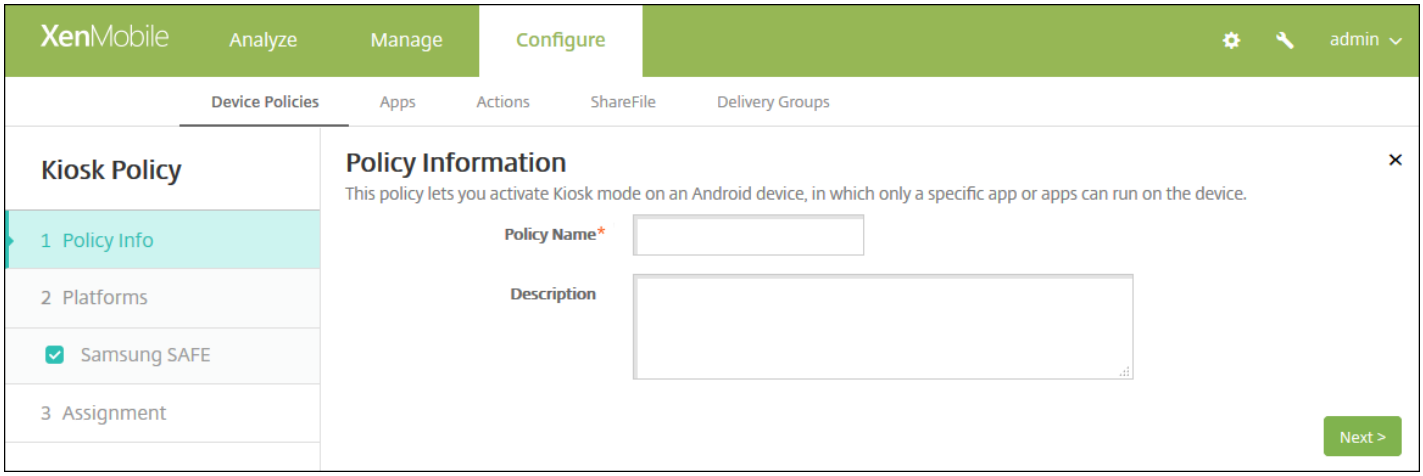
Nota:

- 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**.

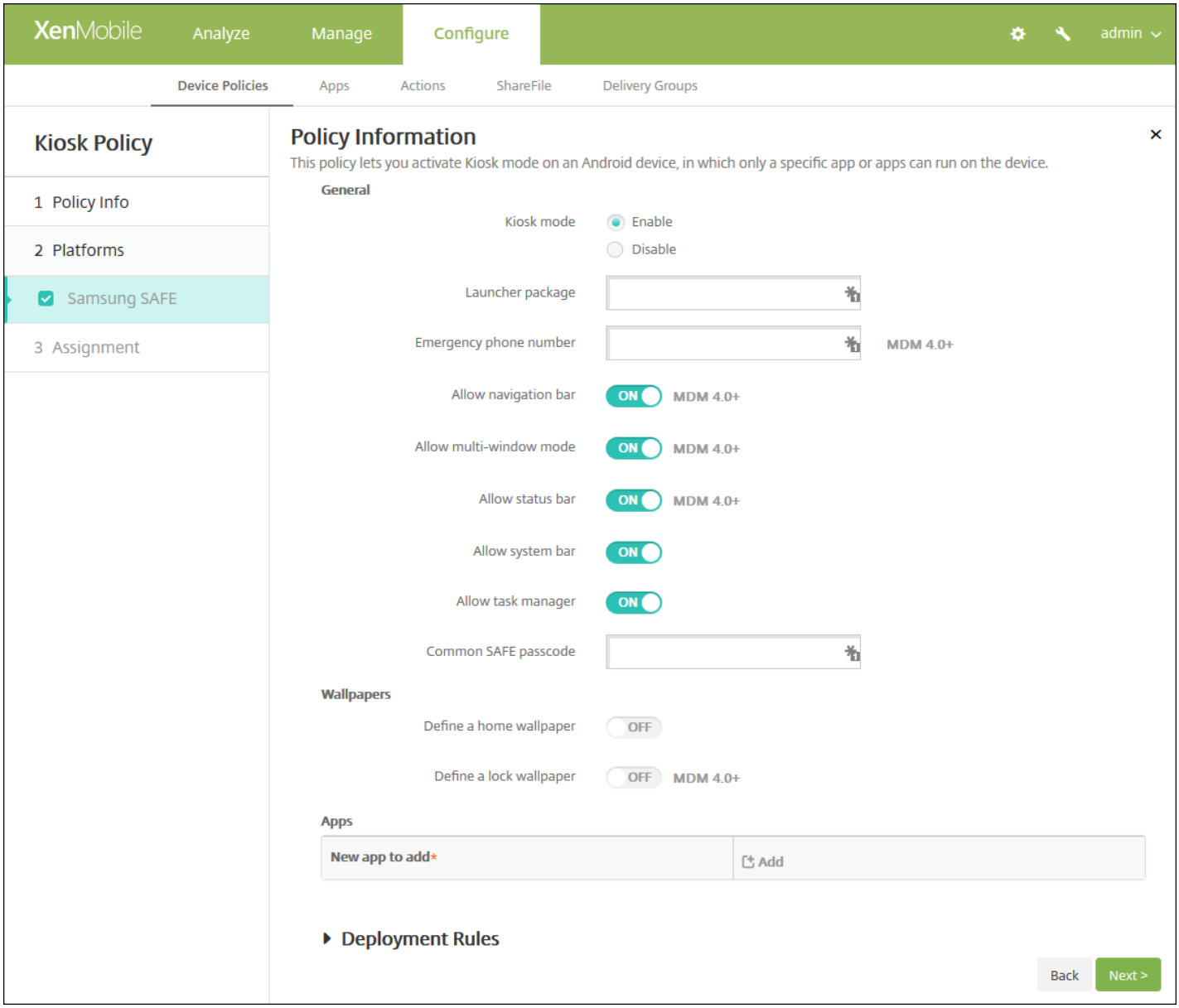
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Kiosk**. Aparecerá la página **Kiosk Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información acerca de la plataforma **Samsung SAFE**.



6. Configure estos 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 durante el modo 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 durante el modo 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 durante el modo quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.

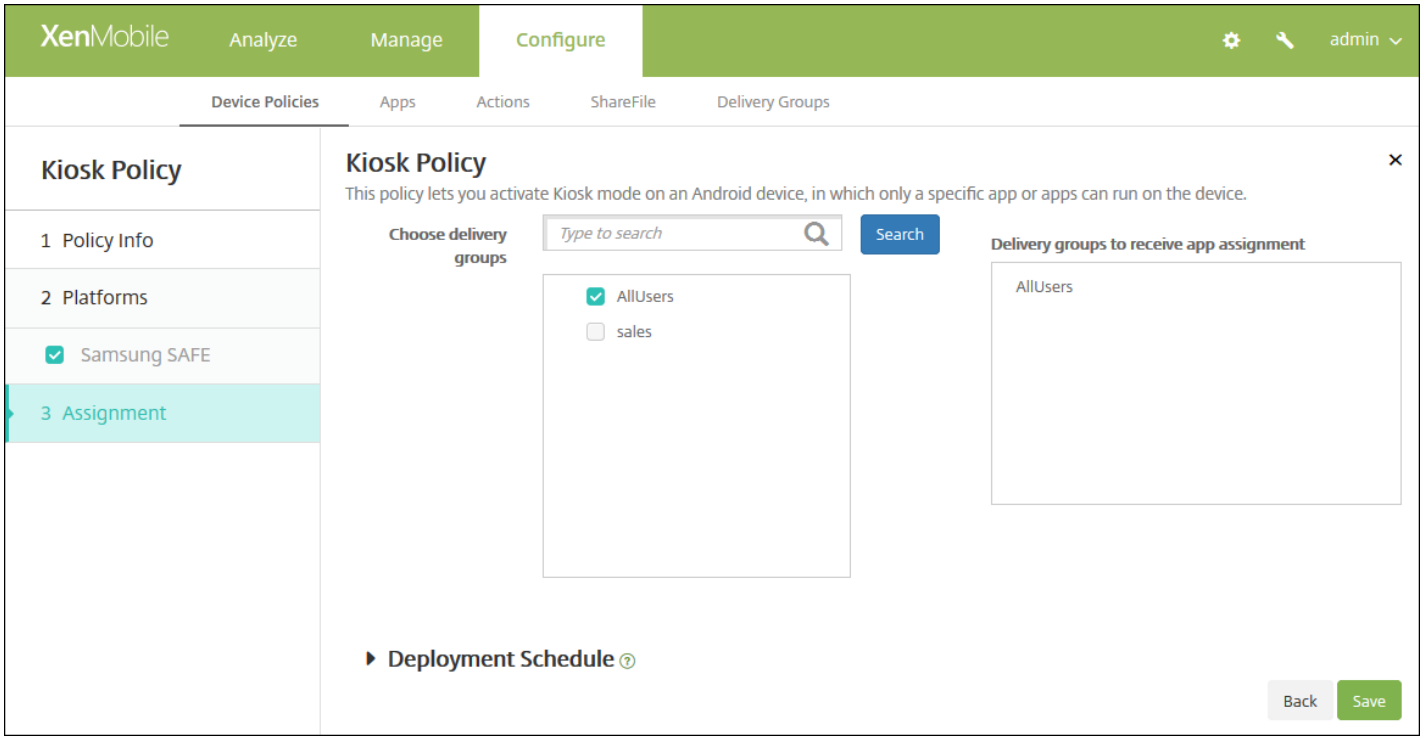
- **Allow system bar**. Seleccione si permitir que los usuarios vean la barra del sistema durante el modo quiosco. El valor predeterminado es **ON**.
- **Allow task manager**. Seleccione si permitir que los usuarios vean y usen el Administrador de tareas durante el modo quiosco. El valor predeterminado 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 el fondo de pantalla durante el modo quiosco. El valor predeterminado es **OFF**.
    - **Home image**. Si habilita **Define a home wallpaper**, seleccione un archivo de imagen. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
  - **Define a lock wallpaper**. Seleccione si utilizar una imagen personalizada para la pantalla de bloqueo durante el modo quiosco. El valor predeterminado es **OFF**. Se aplica solo a MDM 4.0 y versiones posteriores.
    - **Lock image**. Si habilita **Define a lock wallpaper**, seleccione un archivo de imagen. Para ello, haga clic en **Browse** y vaya 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 guardarlos, o bien en **Cancel** para descartarlos.

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo de configuración de Launcher para Android

Feb 27, 2017

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android implementados por XenMobile. Puede agregar una directiva de configuración de Launcher para controlar esas características de Citrix Launcher:

- Administre los dispositivos Android, de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña que los usuarios deban introducir para salir de Launcher.

Si bien Citrix Launcher permite aplicar restricciones a nivel de dispositivo, también concede a los usuarios la flexibilidad de funcionamiento que necesitan gracias al acceso integrado a las configuraciones de los dispositivos (como los parámetros de WiFi, Bluetooth y los parámetros de códigos de acceso). Citrix Launcher no está diseñado como una capa de seguridad adicional situada sobre la capa que la plataforma del dispositivo ya proporciona.

Después de implementar Citrix Launcher, XenMobile lo instala (con lo que reemplaza el programa de inicio predeterminado de Android).

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

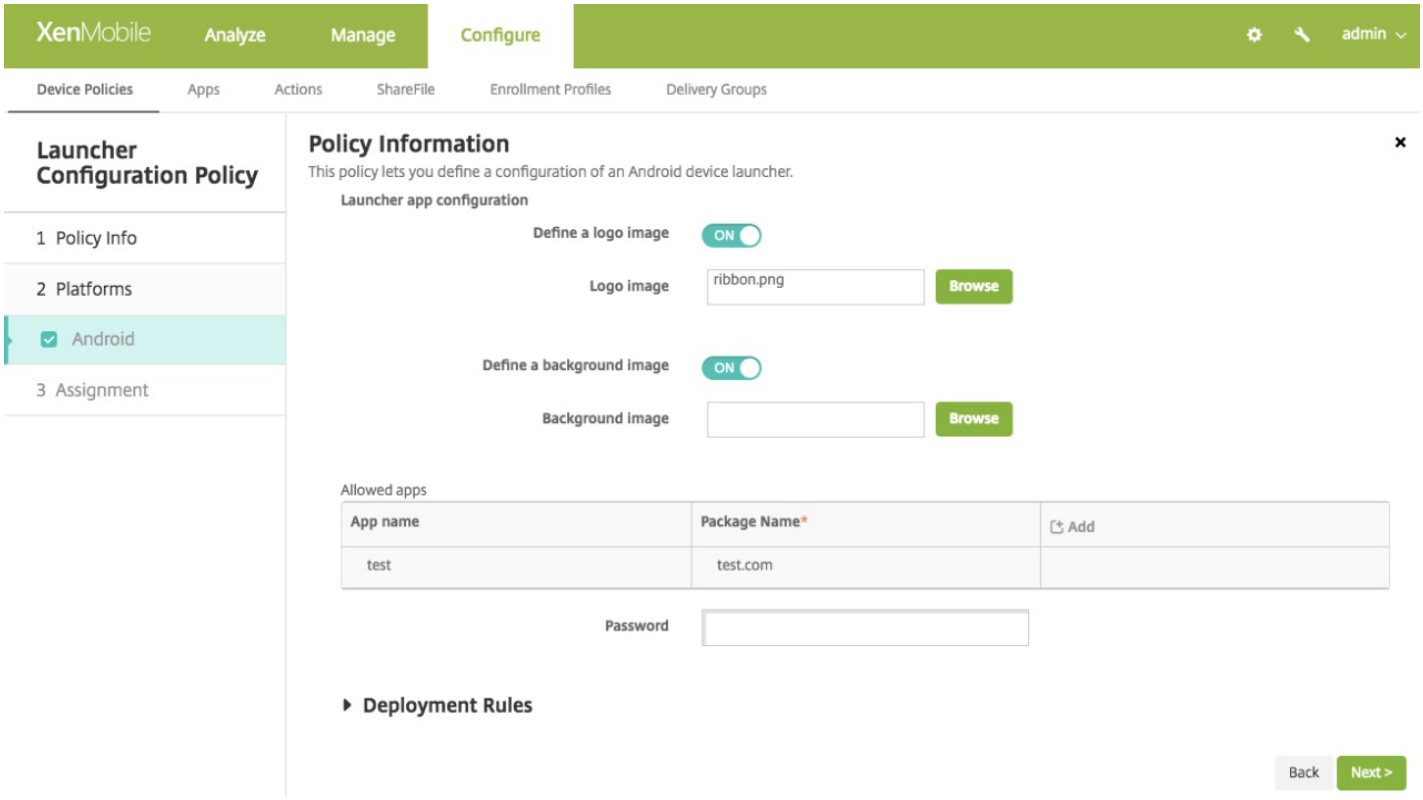
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Empiece a escribir **Launcher** y, a continuación, seleccione **Launcher Configuration** de la lista. Aparecerá la página **Launcher 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 **Android Platform**.



6. Configure estos parámetros:

- **Define a logo image**. Seleccione si utilizar una imagen personalizada como logo para el icono de Citrix Launcher. El valor predeterminado es **OFF**.
- **Logo image**. Cuando habilite **Define a logo image**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Define a background image**. Seleccione si utilizar una imagen personalizada como imagen de fondo de Citrix Launcher. El valor predeterminado es **OFF**.
- **Background image**. Cuando habilite **Define a background image**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Allowed apps**. Para cada aplicación que quiera permitir en Citrix Launcher, 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 para 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 en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

    Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardarlos, o bien en **Cancel** para descartarlos.
- **Password**. La contraseña que el usuario debe introducir para salir de Citrix Launcher.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Launcher Configuration Policy**.

9 Configure las reglas de implementación.

10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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**.

12. Haga clic en **Save**.

Directivas de dispositivo para LDAP

Feb 27, 2017

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.

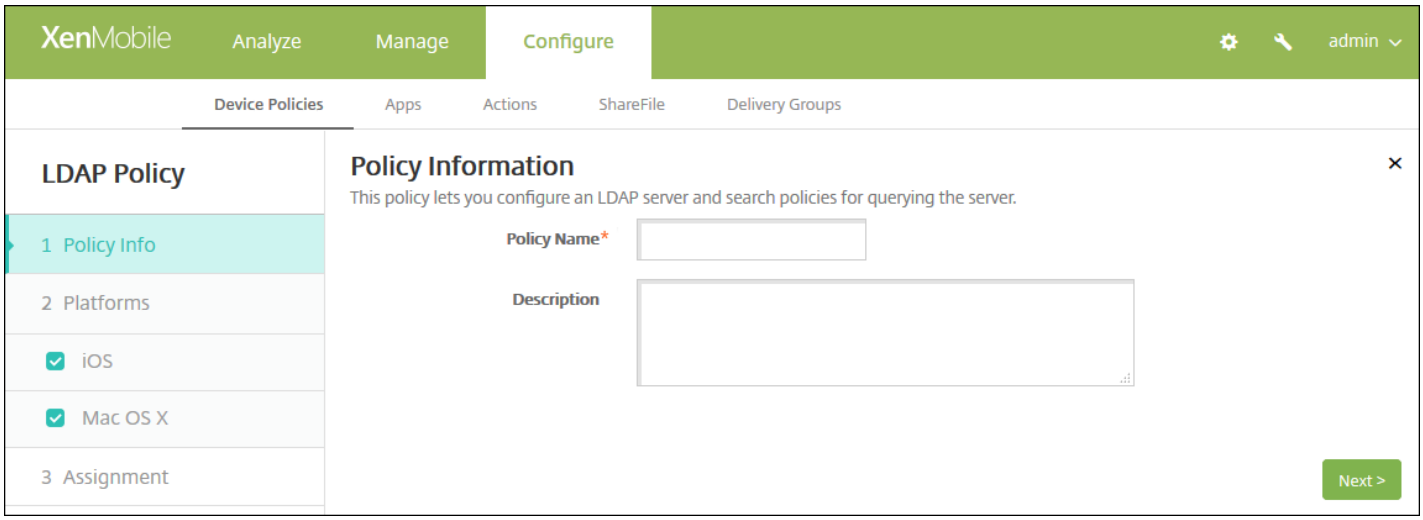
Configuración de iOS

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:

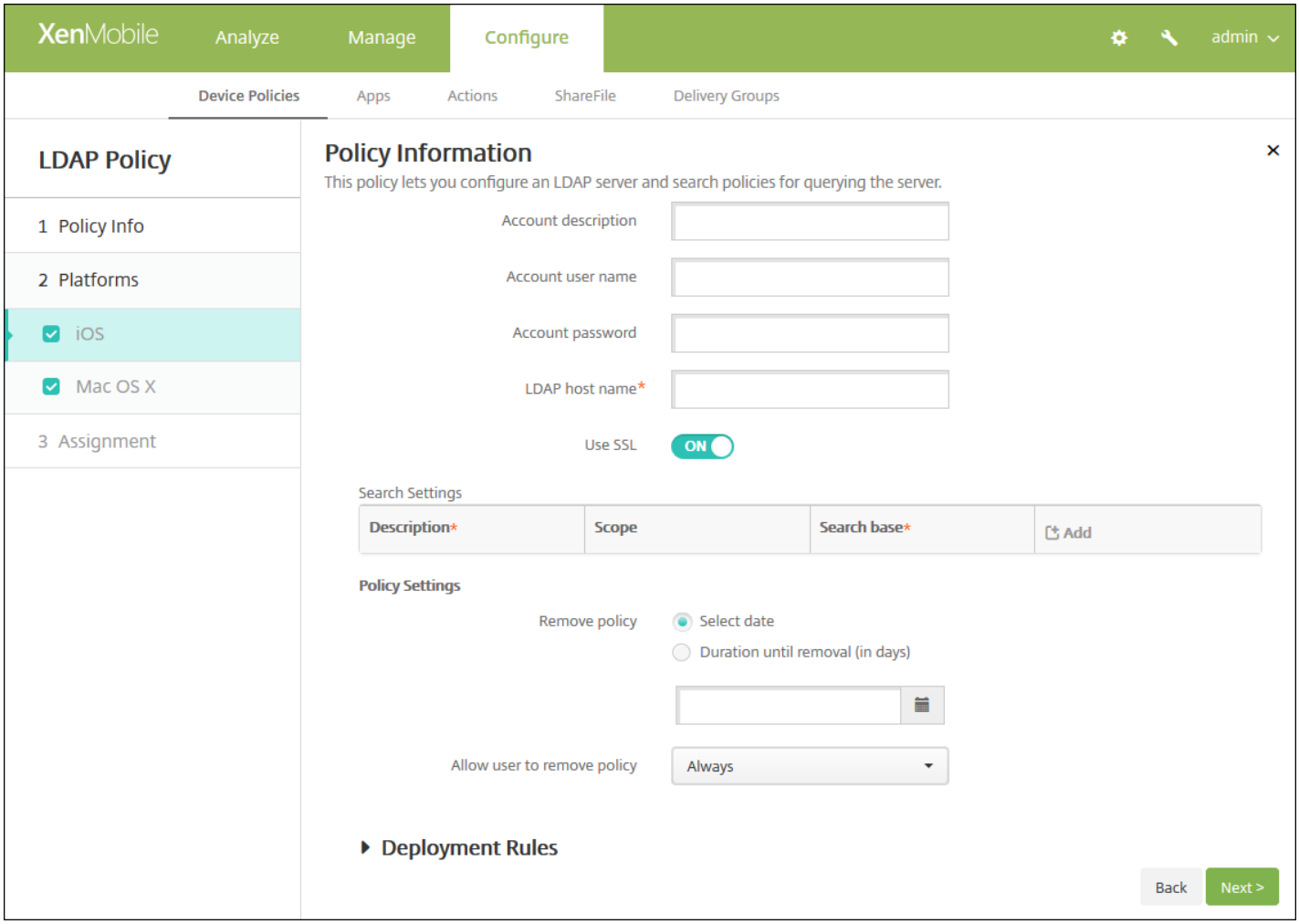
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Platforms** de la directiva.

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**. 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 capa de sockets seguros (SSL) en la conexión al 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.

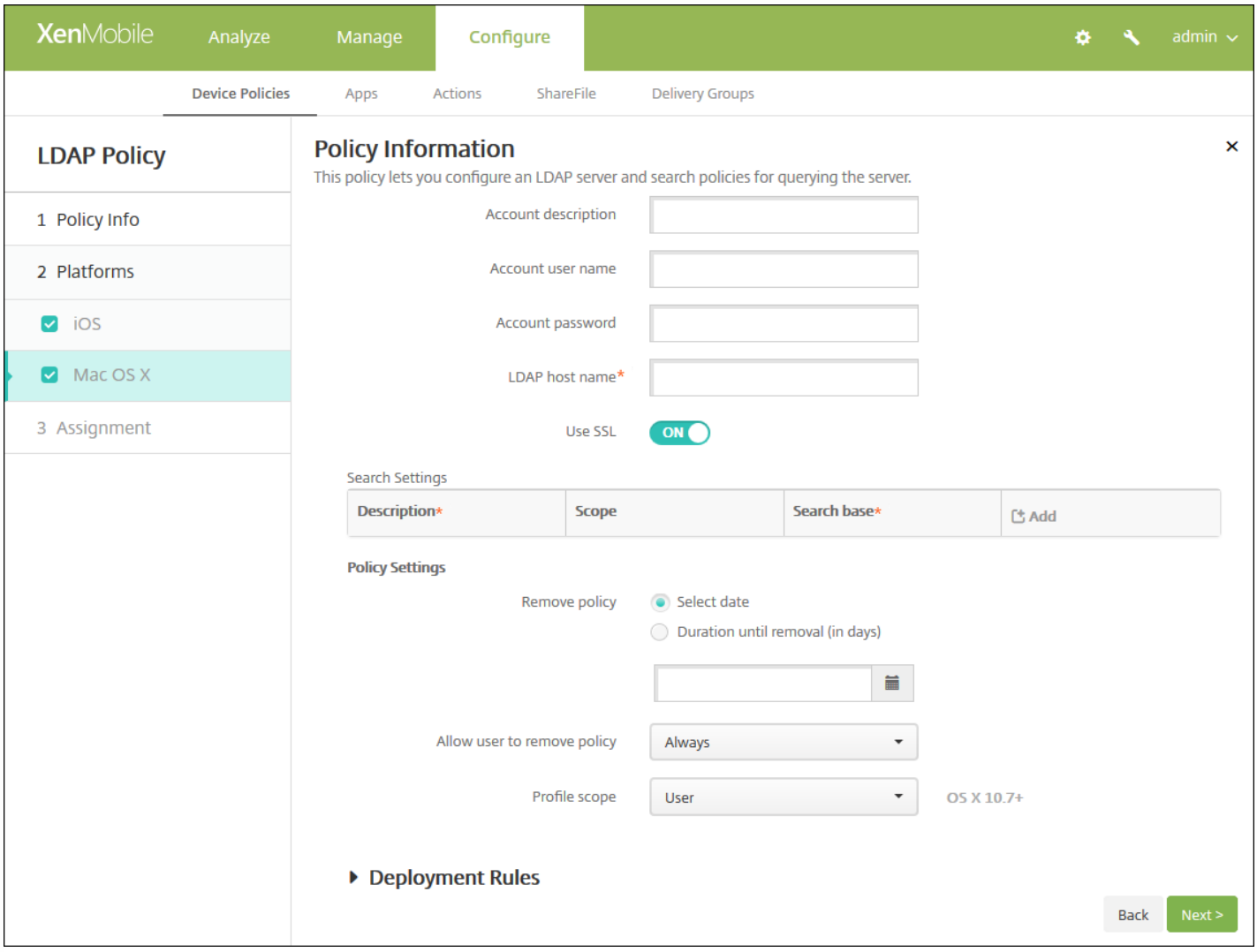
- Haga clic en **Save** para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
- Repita estos pasos para cada opción de búsqueda que quiera agregar.

  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 list**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 capa de sockets seguros (SSL) en la conexión al 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.

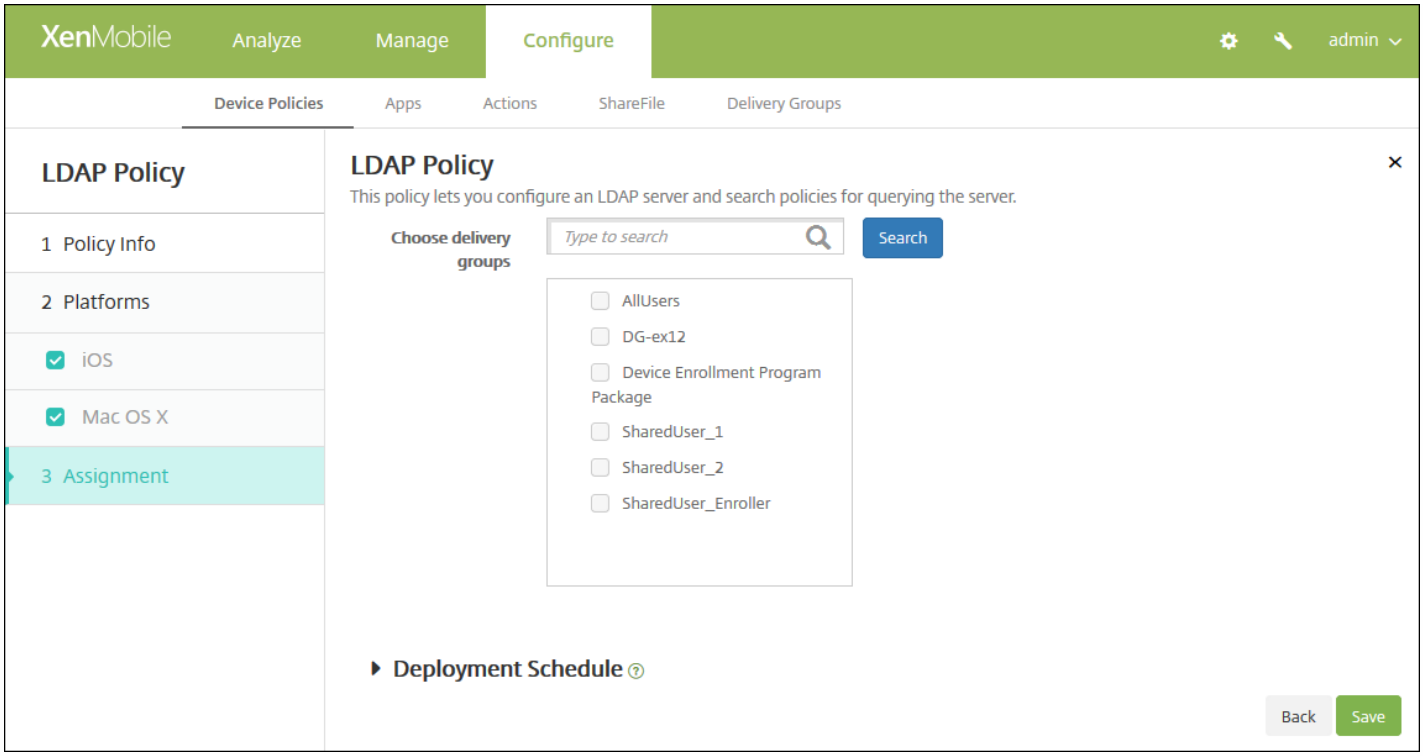
    Nota: Para eliminar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel 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 list**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 de **LDAP Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 localización

Mar 24, 2017

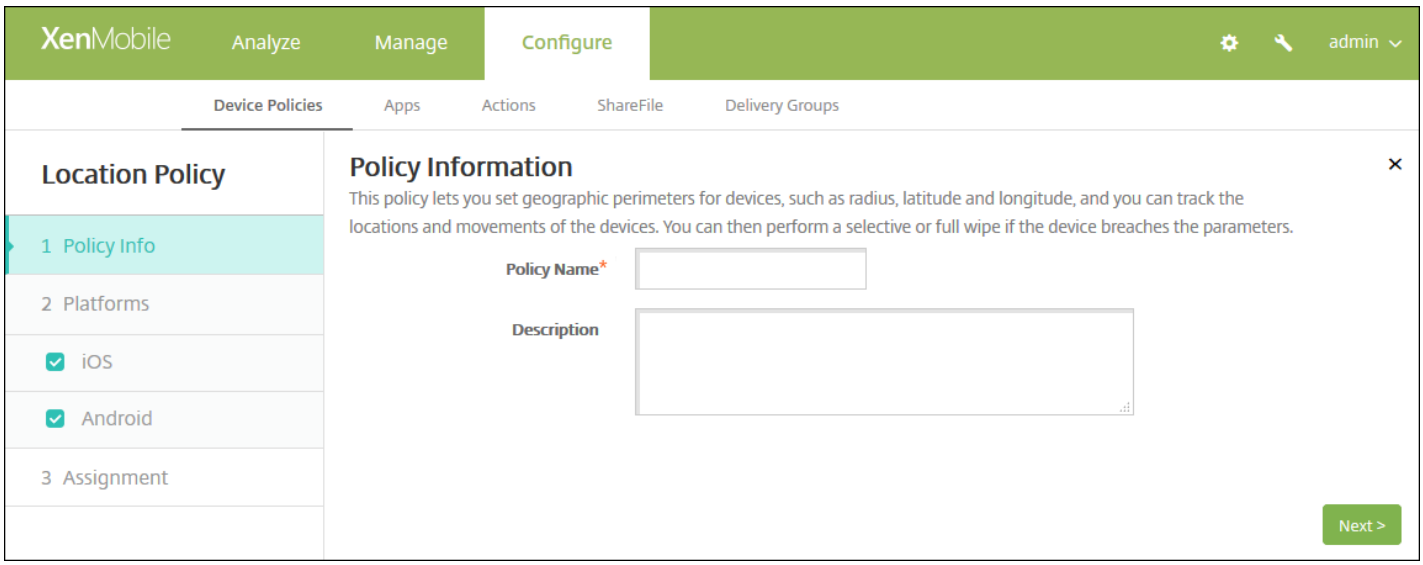
En XenMobile, puede crear directivas de dispositivos para localizaciones si quiere aplicar límites geográficos. Cuando los usuarios abandonen el límite definido, también conocido como *geocerca*, XenMobile puede realizar determinadas acciones. Por ejemplo, puede configurar la directiva para que emita un mensaje de advertencia a los usuarios cuando abandonen el perímetro definido. También puede configurar la directiva para que borre (inmediatamente o pasado un tiempo) los datos empresariales que contenga el dispositivo cuando los usuarios abandonen el perímetro. Para obtener información sobre las acciones de seguridad, como habilitar el seguimiento y localizar un dispositivo, consulte la sección de acciones de seguridad en Dispositivos.

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:

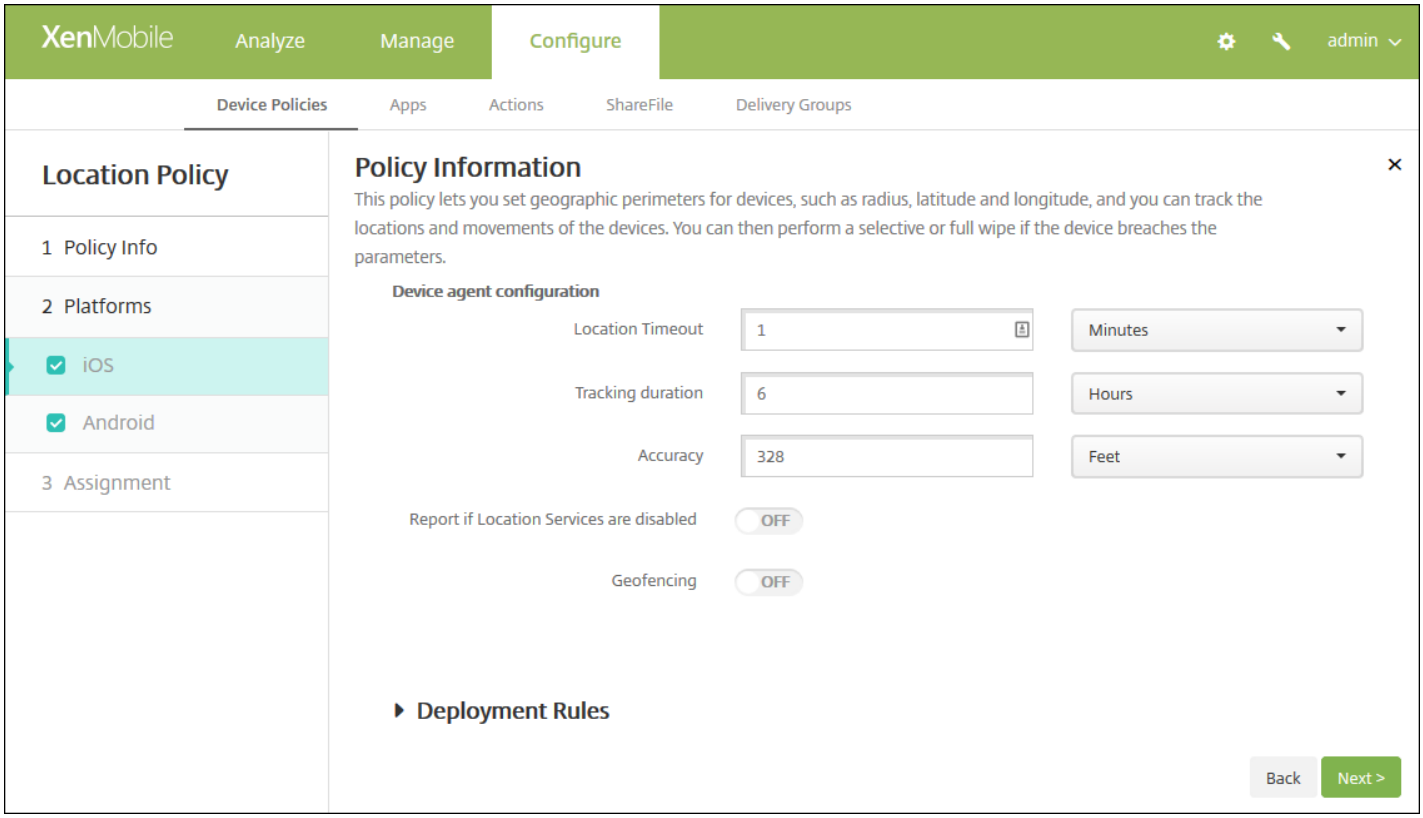
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

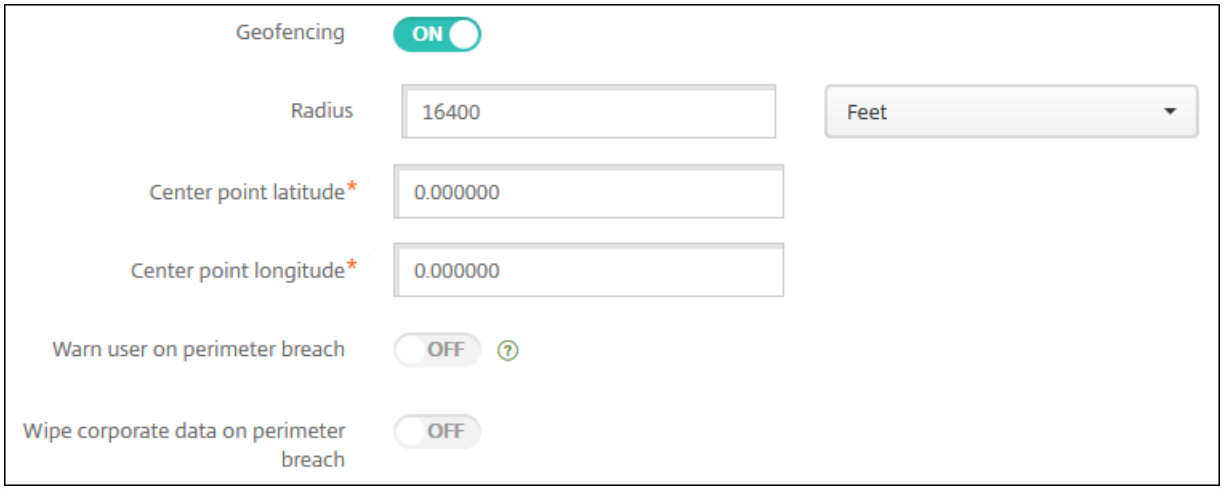
Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS



Configure estos parámetros:

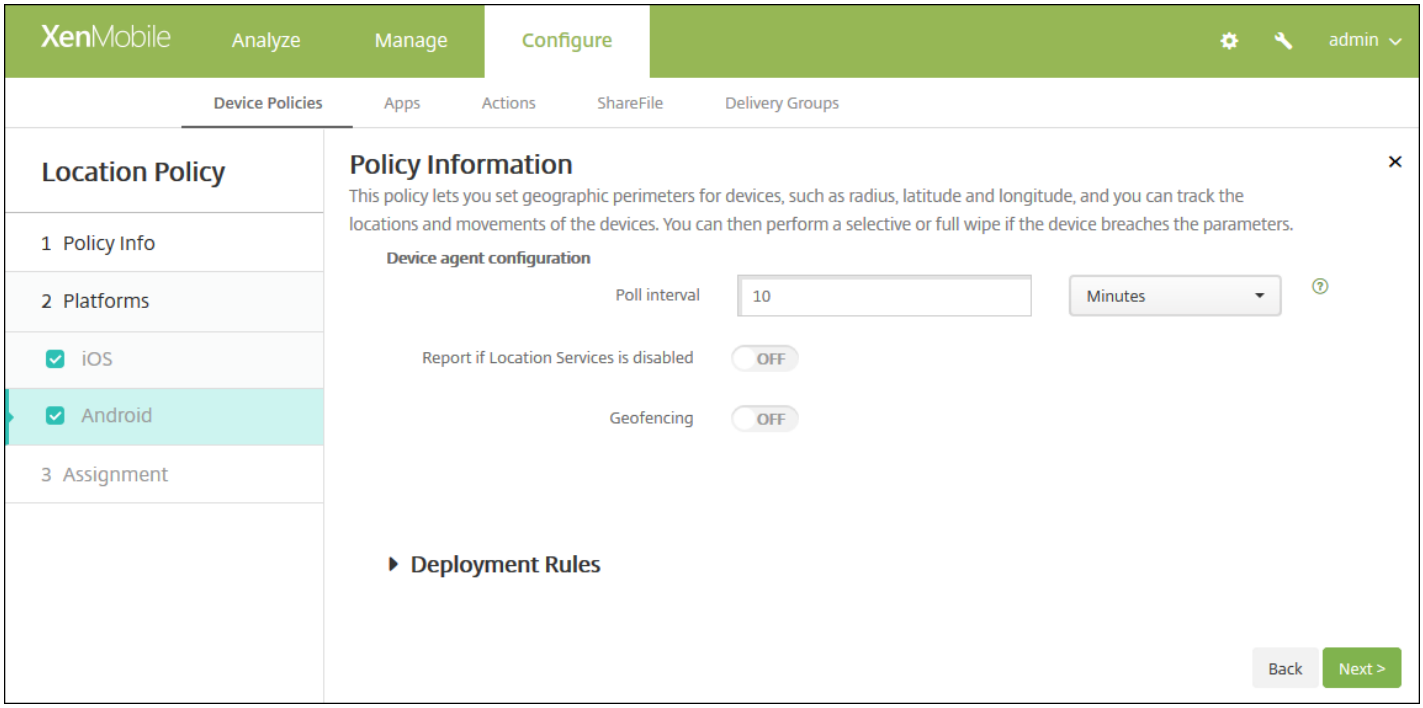
- **Location timeout**. Escriba un número y, en la lista, haga clic en **Seconds** o **Minutes** para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es de 1 minuto.
- **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** para indicar 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 15 000 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**



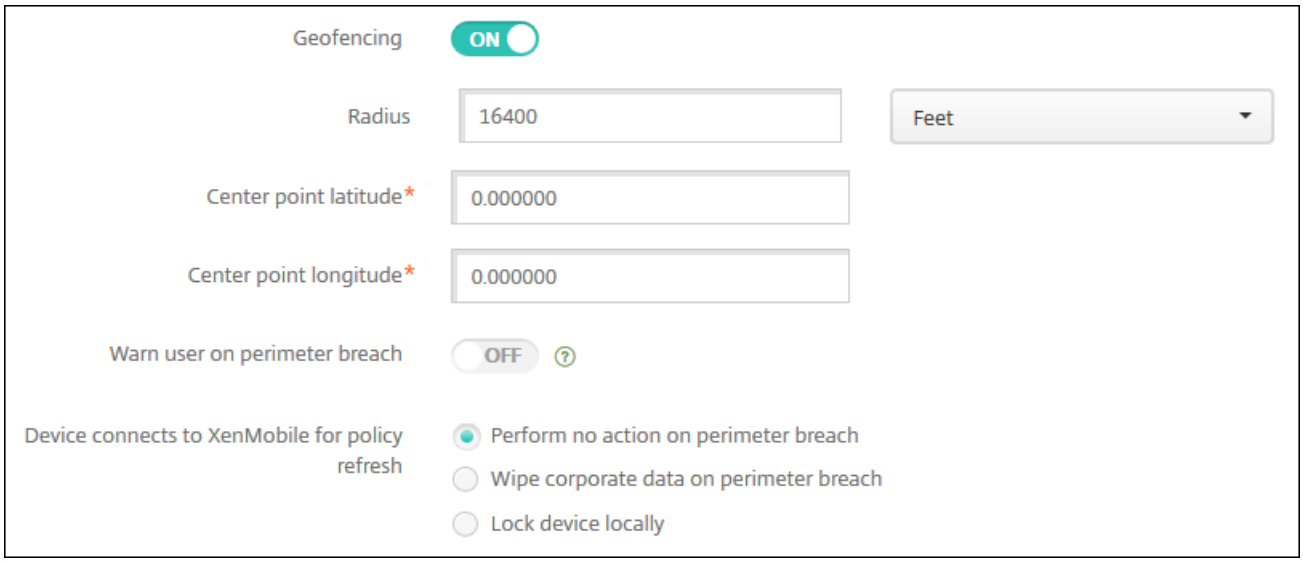
Al habilitar geocercas, configure los siguientes parámetros:

- **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 geocerca.
- **Center point longitude**. Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **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 en los dispositivos de los usuarios cuando estos abandonen el perímetro. El valor predeterminado es **OFF**. Si habilita esta opción, aparece el campo **Delay on local wipe**.
  - Escriba un número y, en la lista, haga clic en **Seconds** o **Minutes** para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.

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 cantidad 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:

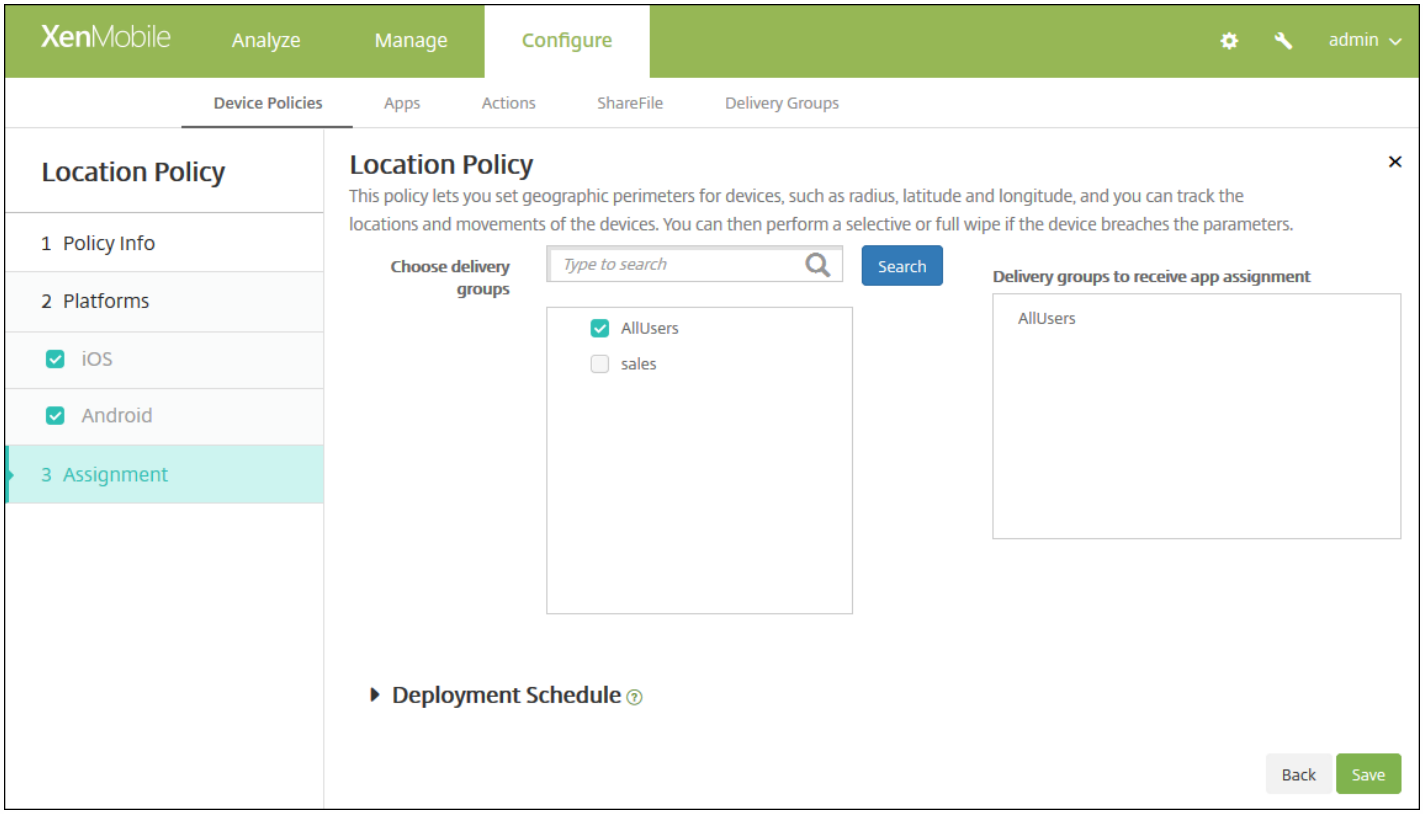
- **Radius**. Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies. Los valores válidos para el radio del perímetro son:

- 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 geocerca.
- **Center point longitude**. Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Warn user on perimeter breach**. Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **OFF**. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- **Device connects to XenMobile for policy refresh**. Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
  - **Perform no action on perimeter breach**. No hacer nada. Ésta es la opción predeterminada.
  - **Wipe corporate data on perimeter breach**. Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparece el campo **Delay on local wipe**.
    - Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.
  - **Delay on lock**. Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparece el campo **Delay on lock**.
    - Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile bloquee sus dispositivos. El valor predeterminado es de 0 segundos.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Location Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para correo

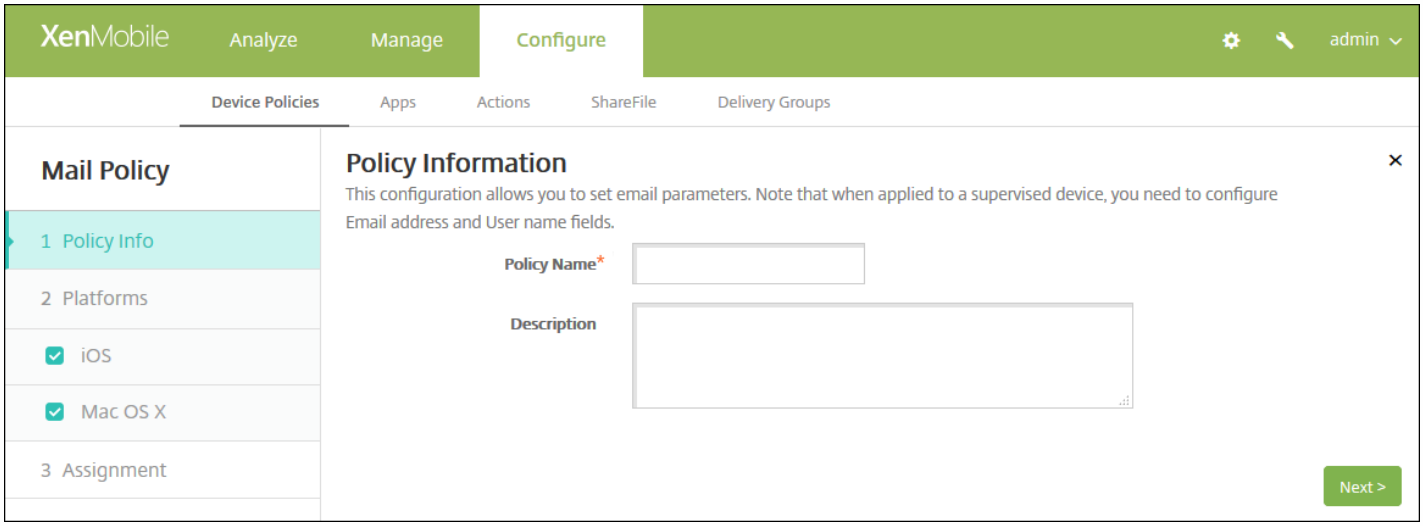
Feb 27, 2017

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**.

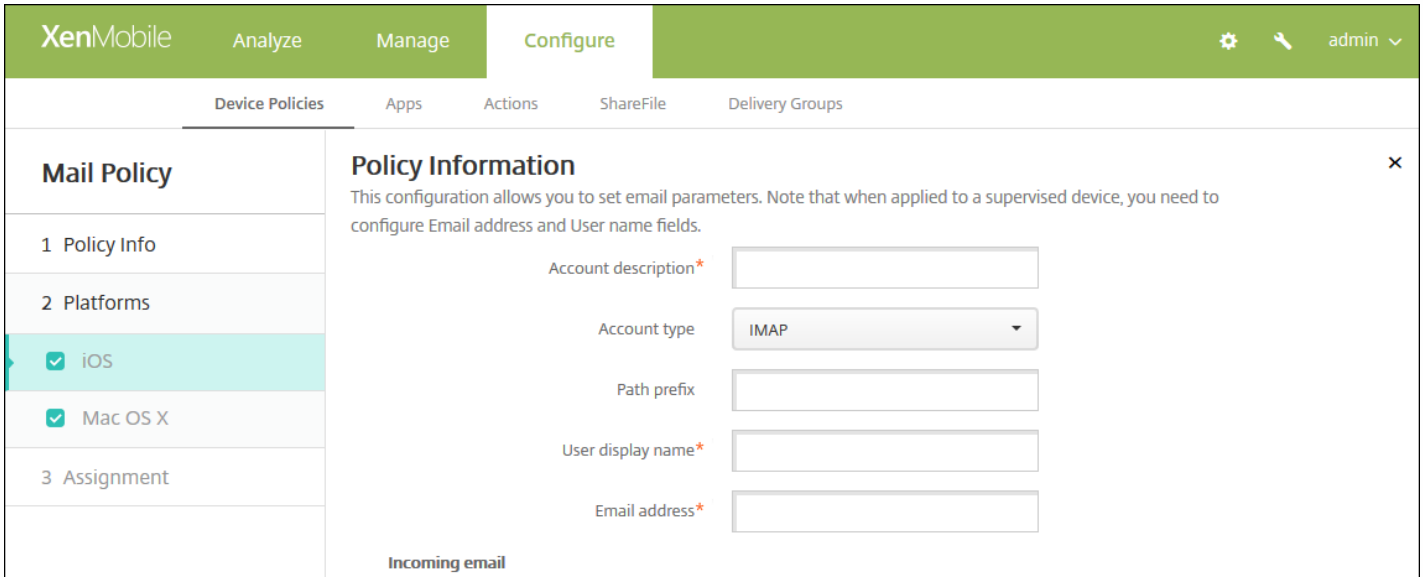
3. Haga clic en **More** y, en **End user**, haga clic en **Mail**. Aparecerá la página **Mail Policy**.

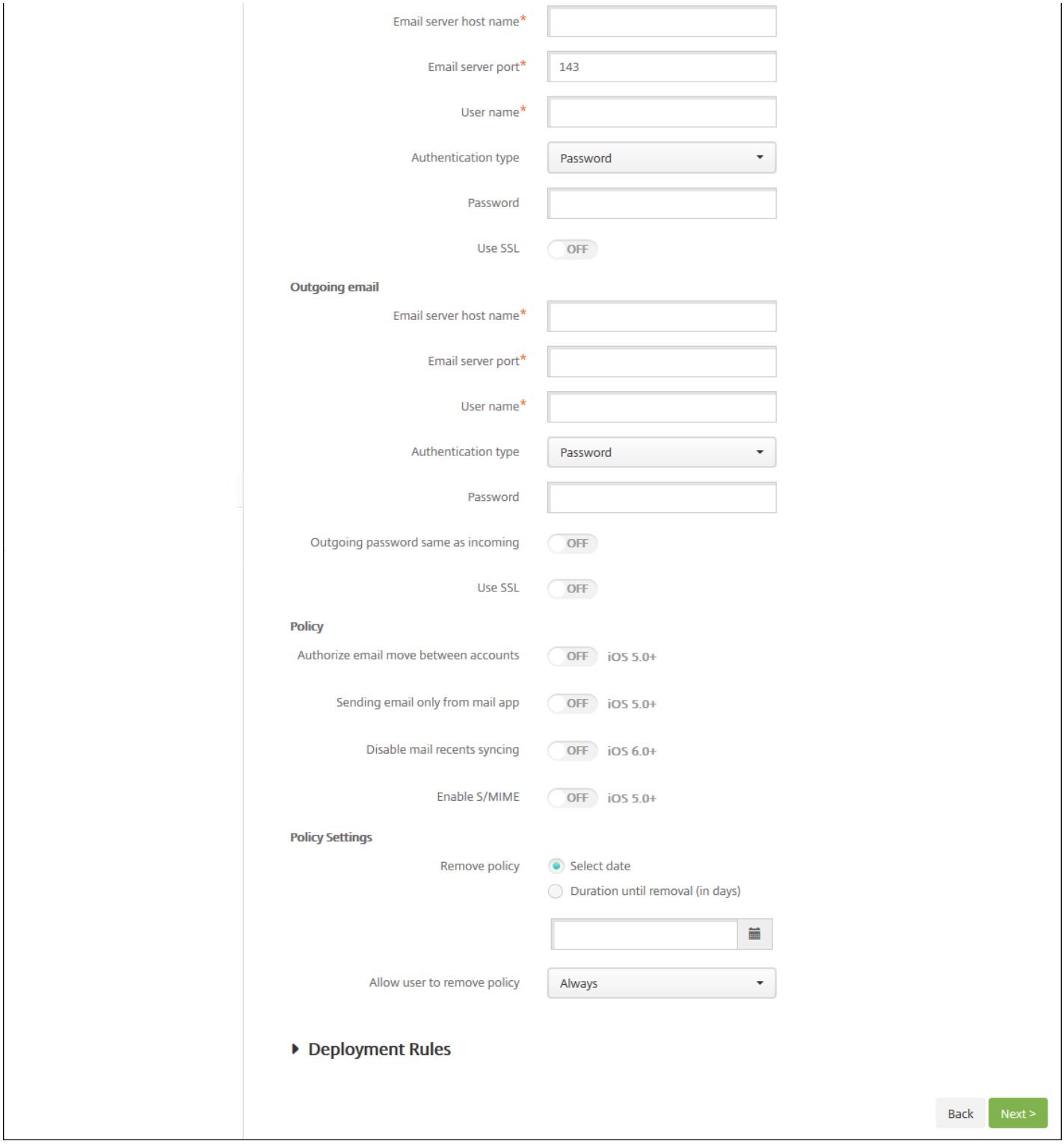


4. En el panel **Policy Information**, escriba la información siguiente:

- **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 la directiva para el correo.





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 de una plataforma, consulte el paso 8 para configurar 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 correo entrante. Este campo es obligatorio.
  - **Email server port**. Escriba el número de puerto del servidor de correo entrante. 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 **Password**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password**. Si quiere, escriba una contraseña para el servidor de correo entrante.
  - **Use SSL**. Seleccione esta opción si el servidor de correo entrante 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 de 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 correo saliente. 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 **Password**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password**. Si quiere, escriba una contraseña para el servidor de correo saliente.
  - **Outgoing password same as incoming**. Seleccione si las contraseñas de correo entrante y saliente son iguales. El valor predeterminado es OFF, lo que significa que las contraseñas son diferentes. Si se establece en **ON**, desaparece el campo **Password**.
  - **Use SSL**. Seleccione esta opción si el servidor de correo saliente 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 admite el cifrado y la autenticación S/MIME. El valor predeterminado es

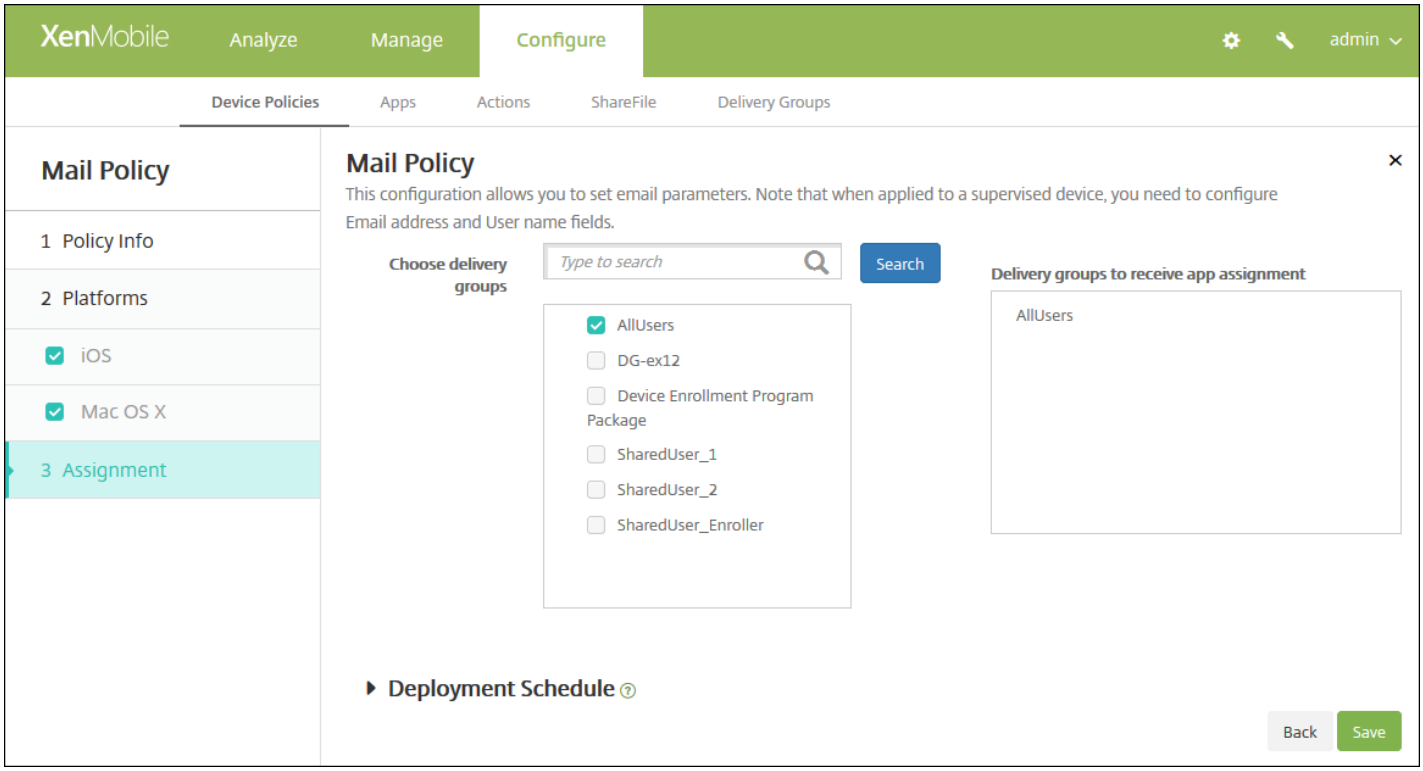
OFF. Si se establece en ON, aparecen los dos siguientes campos.

- **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 **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**, introduzca 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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

Feb 27, 2017

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 en dispositivos supervisados iOS 8 (y versiones posteriores) para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador Web. Para dispositivos supervisados iOS 9.3 y versiones posteriores, puede especificar las direcciones URL desde las que los usuarios pueden guardar contraseñas en Safari.

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.

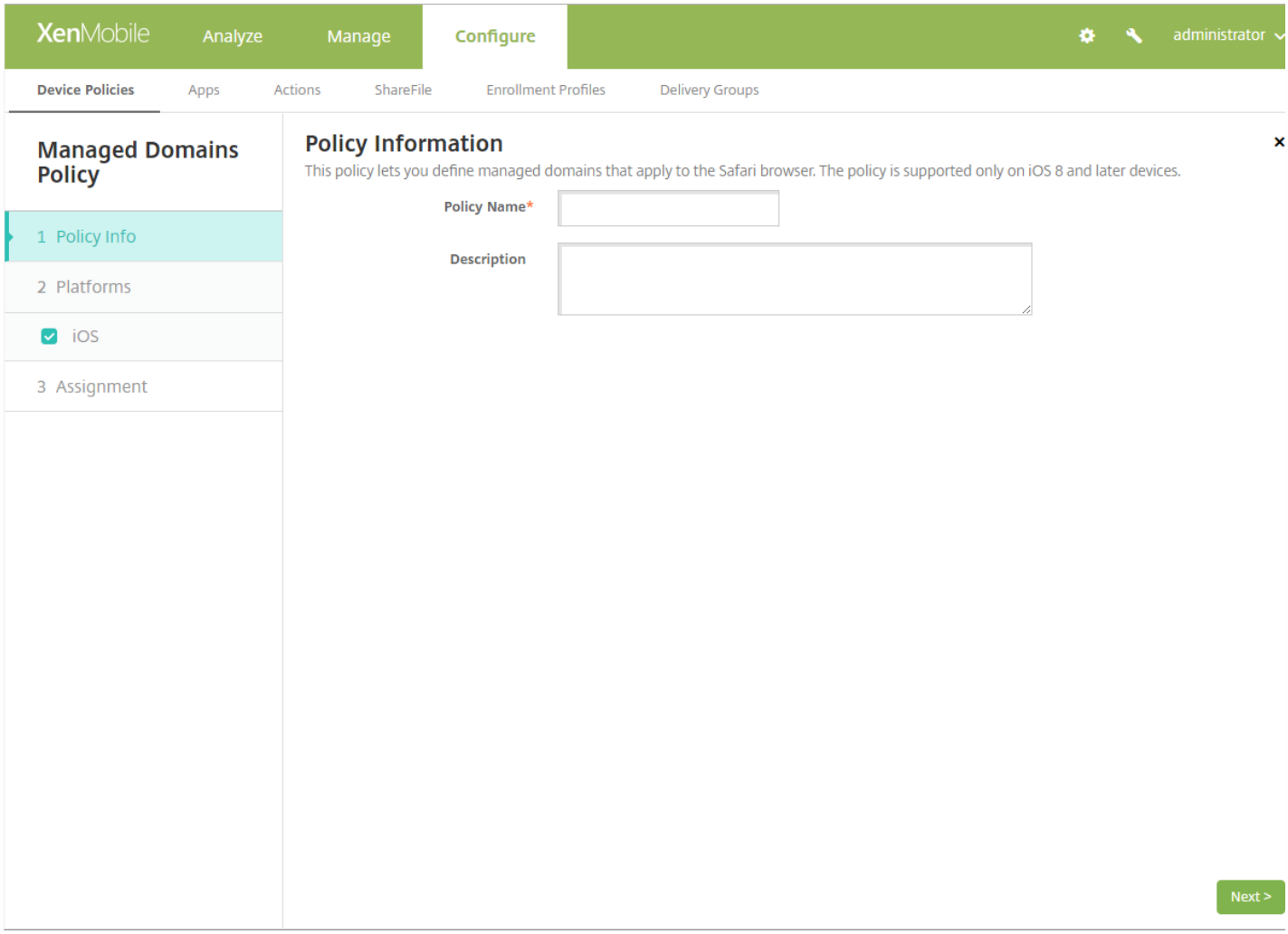
Para elementos como documentos, datos adjuntos o descargas: Cuando un usuario intente abrir un elemento (documento, adjunto o descarga) con Safari desde un dominio que conste en la lista de dominios Web administrados, la aplicación de empresa correspondiente abrirá el elemento. Si el elemento no es de un dominio Web que conste en la lista de dominios Web administrados, el usuario no podrá abrir el elemento con la aplicación de empresa. Deberá usar una aplicación personal no administrada.

En caso de dispositivos supervisados, incluso aunque no especifique dominios de Safari para el rellenado automático de contraseñas: si el dispositivo se configura como multiusuario efímero, los usuarios no podrán guardar las contraseñas. Sin embargo, si el dispositivo no está configurado como multiusuario efímero, los usuarios podrán guardar todas 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**.

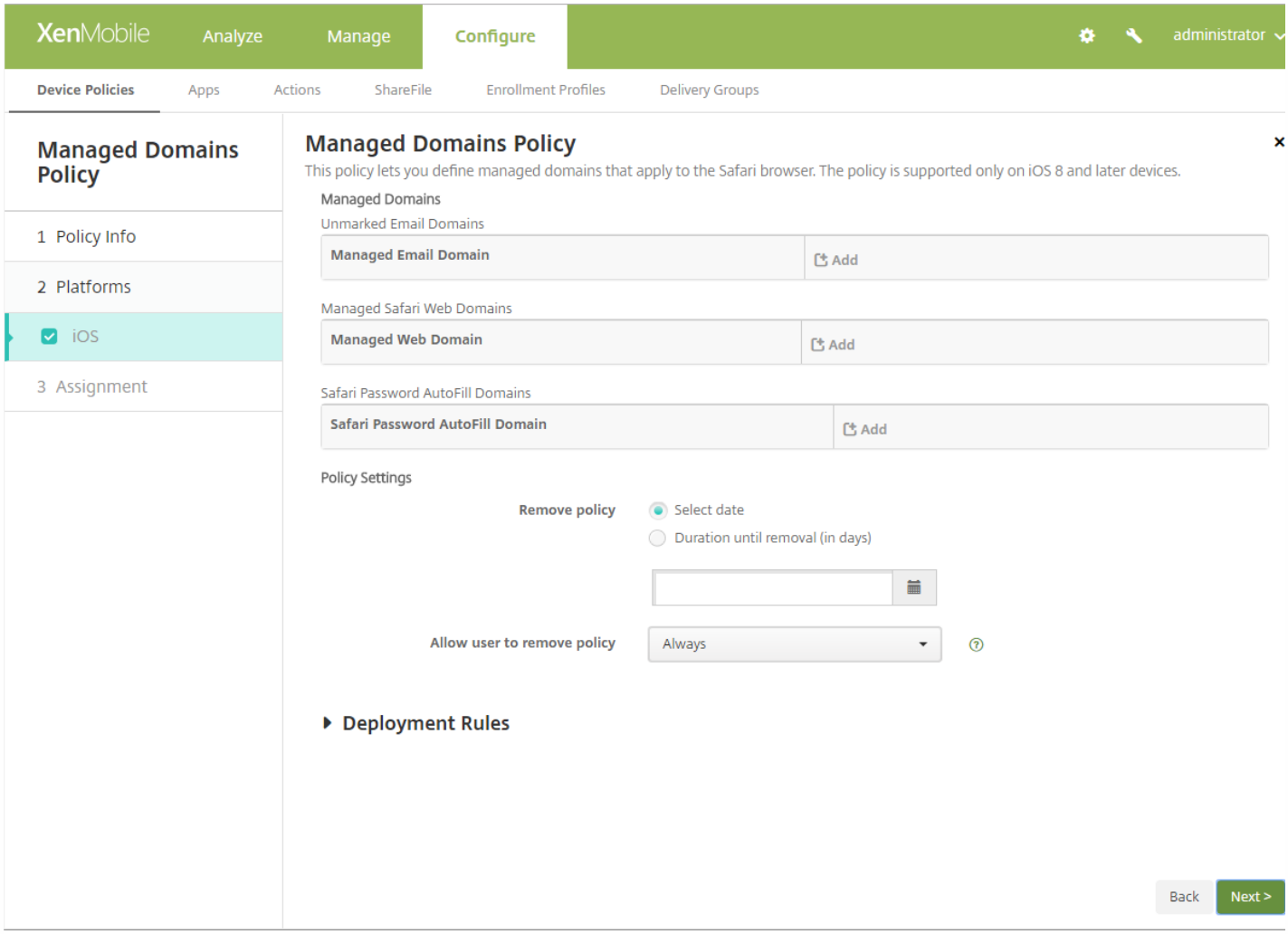
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Managed domains**. Aparecerá la página de información **Managed Domains Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de la **plataforma iOS**.



Cómo especificar dominios

6. Configure estos parámetros:

- **Dominios administrados**
  - **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.
  - **Safari Password AutoFill Domains**:
    Para cada dominio de rellenado automático que quiera incluir en la lista, haga clic en **Add** y lleve a cabo lo siguiente:
    - **Safari Password AutoFill Domain**. Escriba el dominio de rellenado automático.
    - Haga clic en **Save** para guardar el dominio de rellenado automático, 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

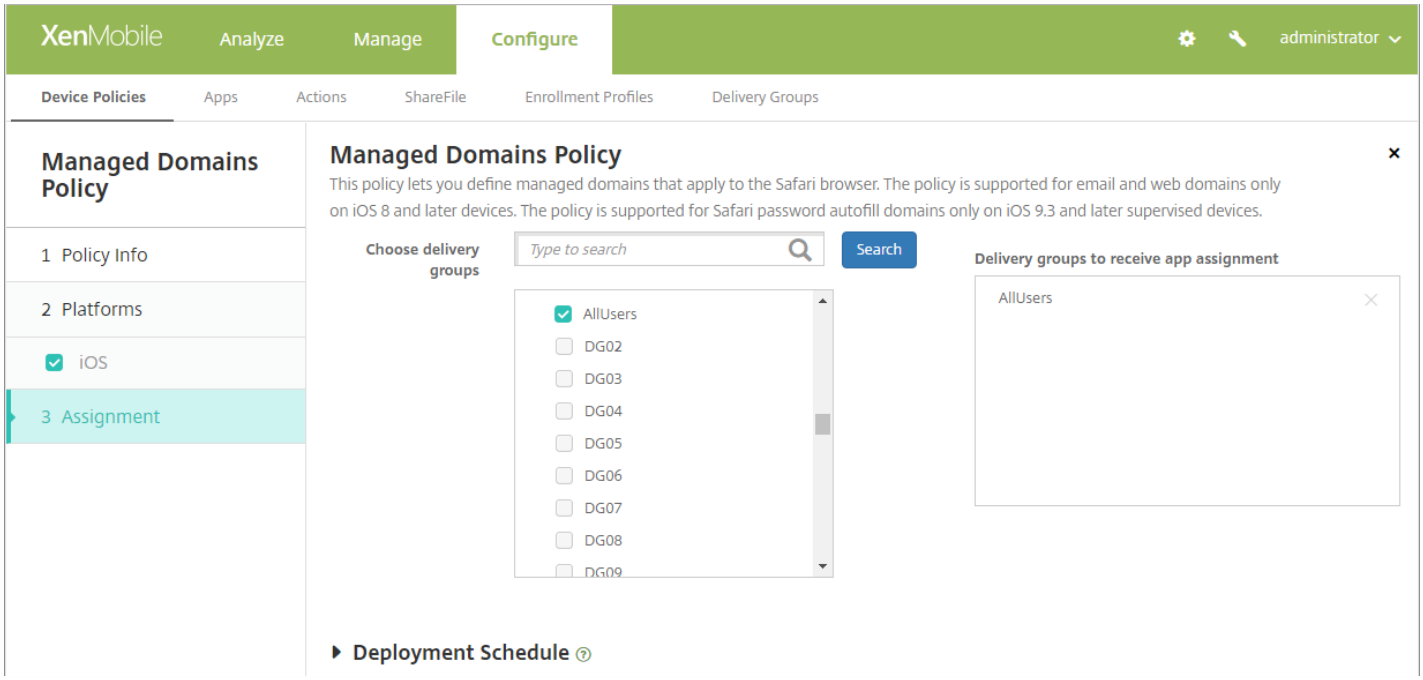
clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página **Assignment**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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

Feb 27, 2017

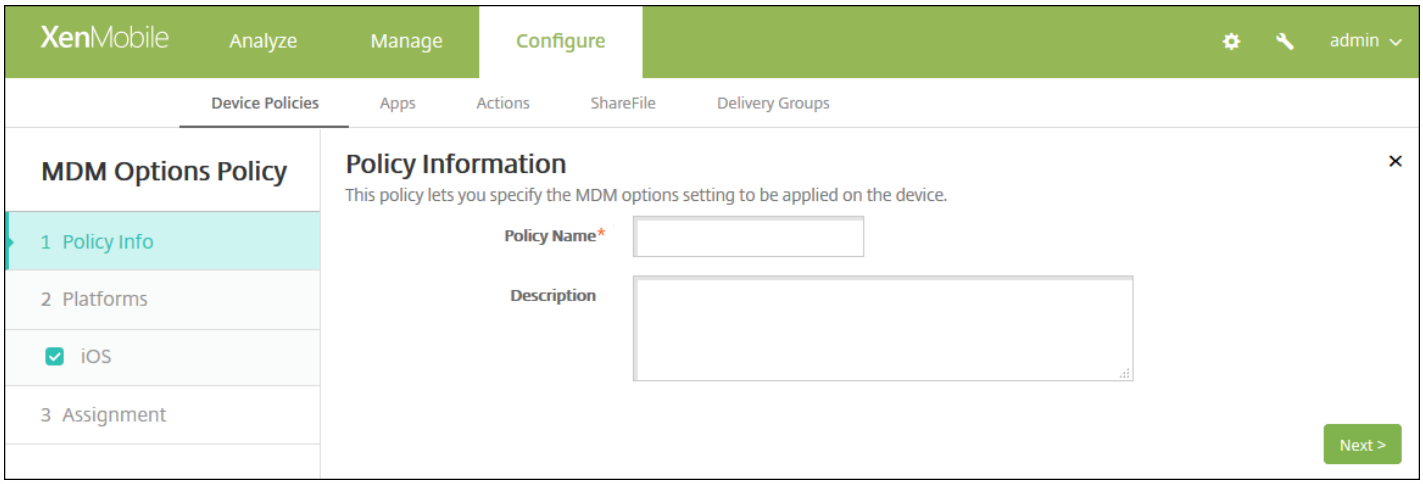
En XenMobile, puede crear una directiva de dispositivo para administrar la función Bloqueo de activación de Buscar mi iPhone/iPad en los dispositivos supervisados iOS 7.0 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

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**.

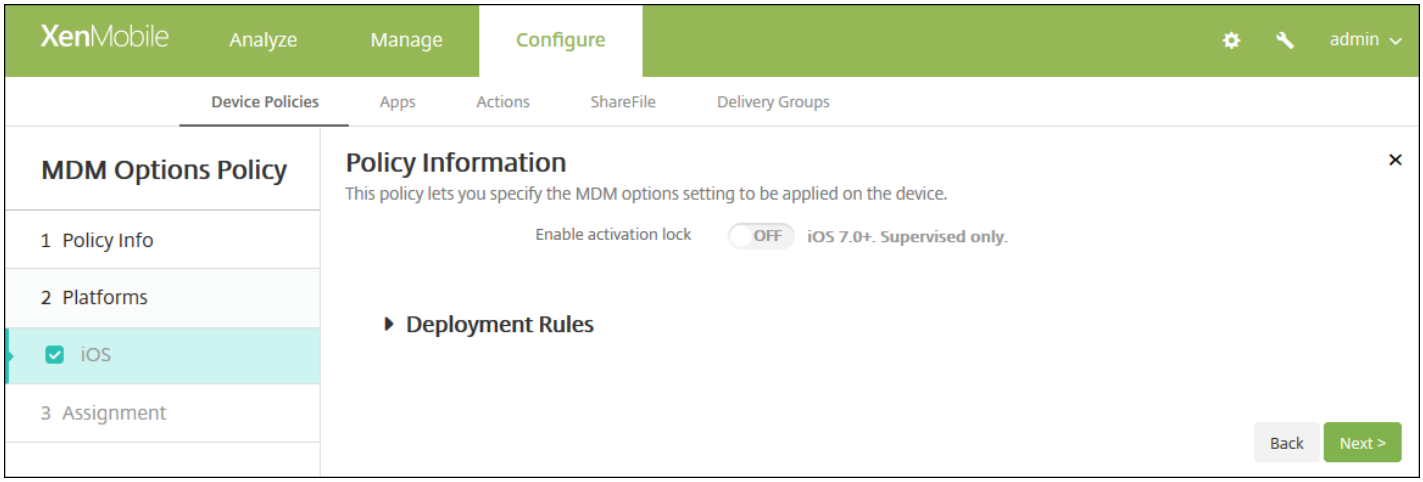
3. Expanda **More** y, en **End user**, haga clic en **MDM Options**. Aparecerá la página de información **MDM Options Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **MDM Policy Platform** de iOS.

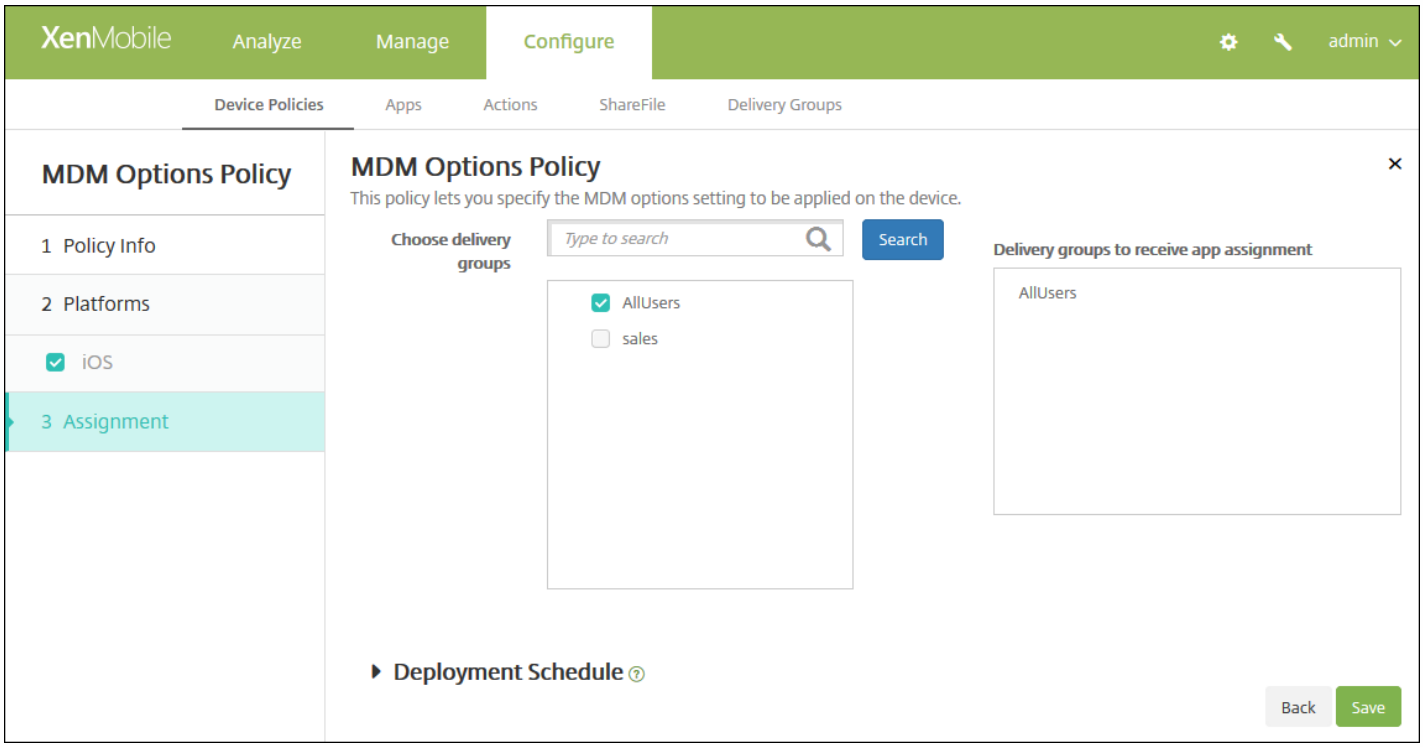


6. Configure este parámetro:

- **Enable Activation Lock**. Seleccione si quiere habilitar la función Bloqueo de activación en 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 de **MDM Options Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para Microsoft Exchange ActiveSync

Feb 27, 2017

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

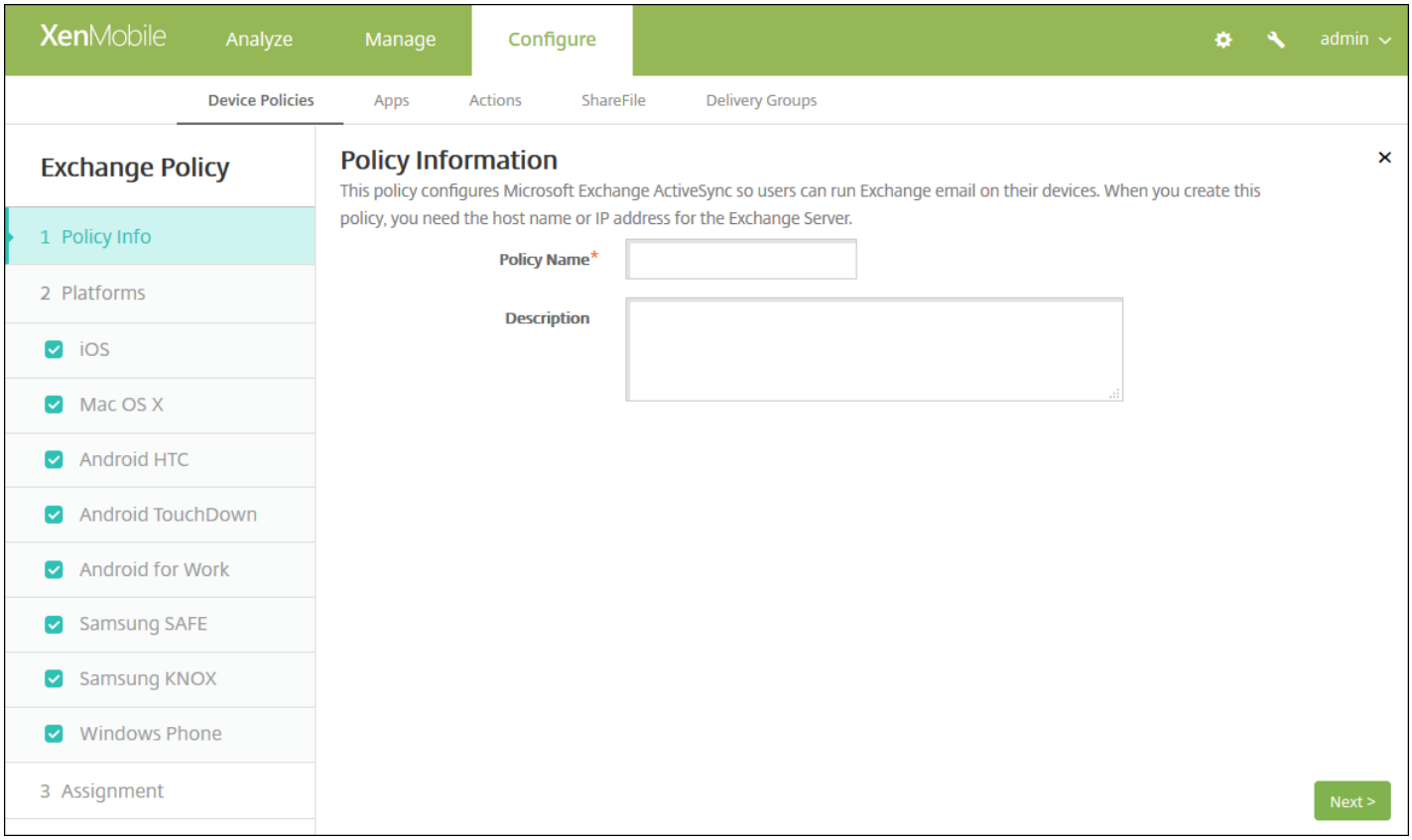
Configuración de Windows Phone

Para poder 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**.



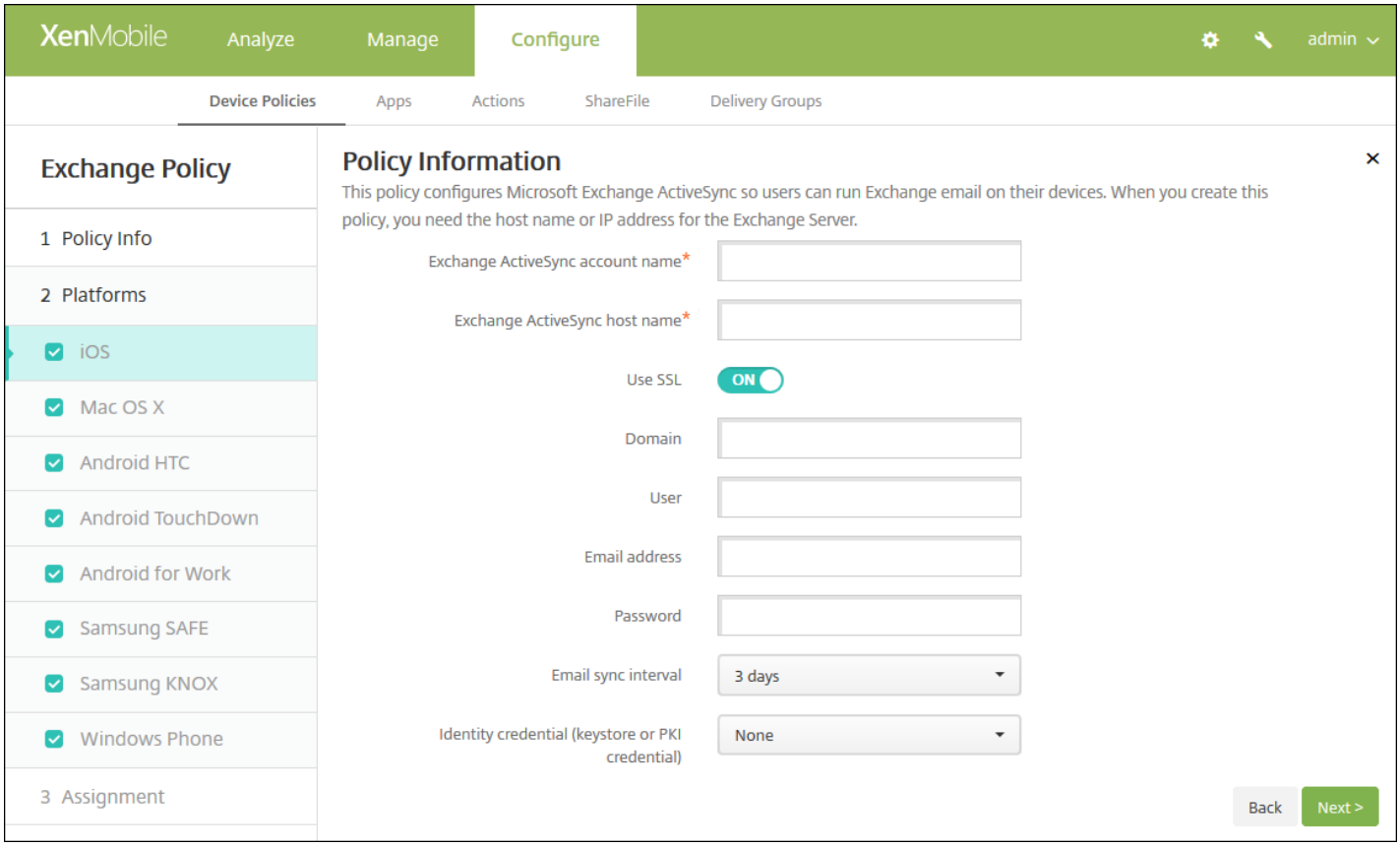
4. En el panel **Policy Information**, escriba la información siguiente:

- **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



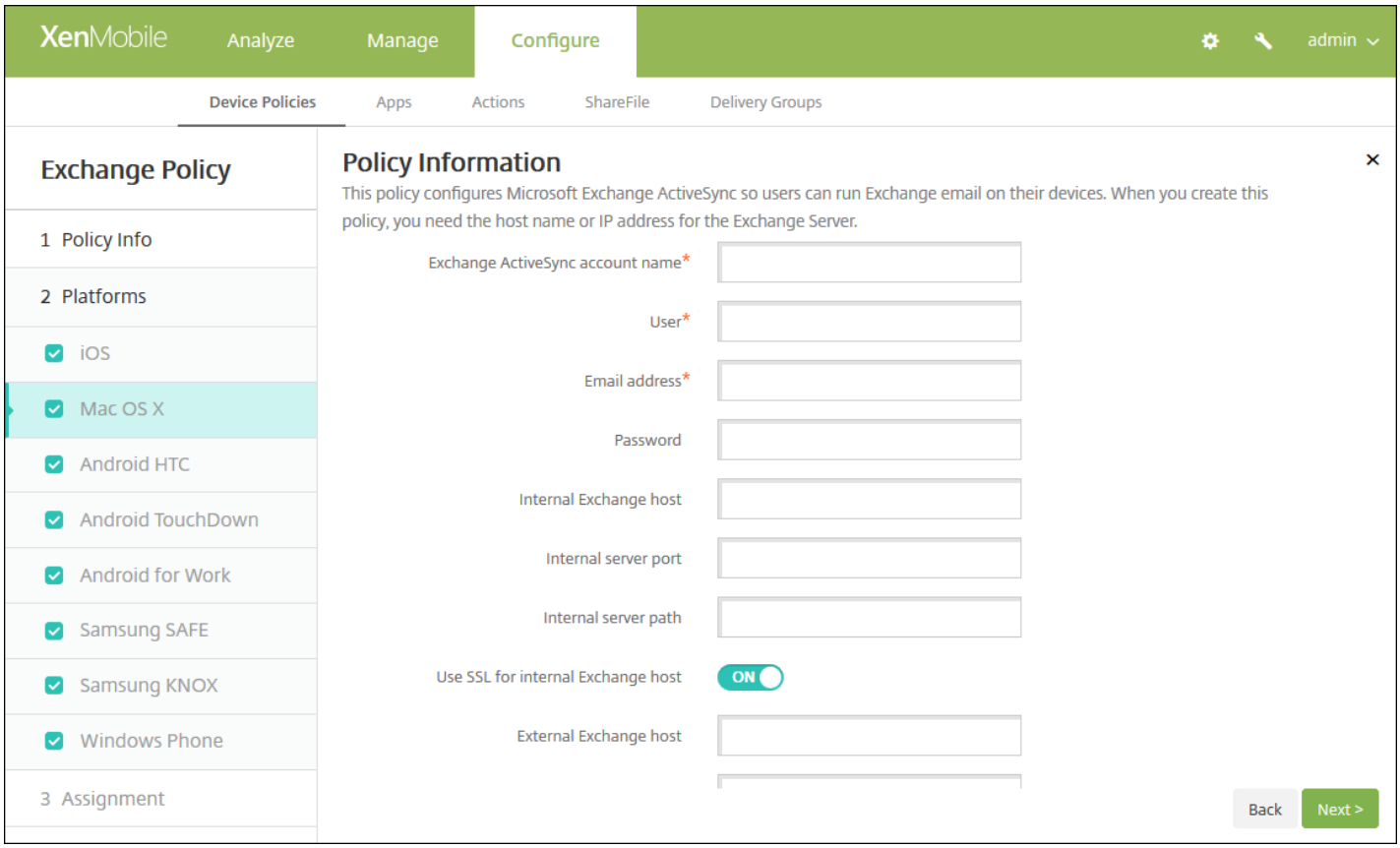
Configure estos parámetros:

- **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 donde 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**, aparecerán estos dos campos:
  - **Signing identity credential** (Credencial de identidad para firma). El valor predeterminado es **None**.
  - **Encryption identity credential** (Credencial de identidad para cifrado). 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



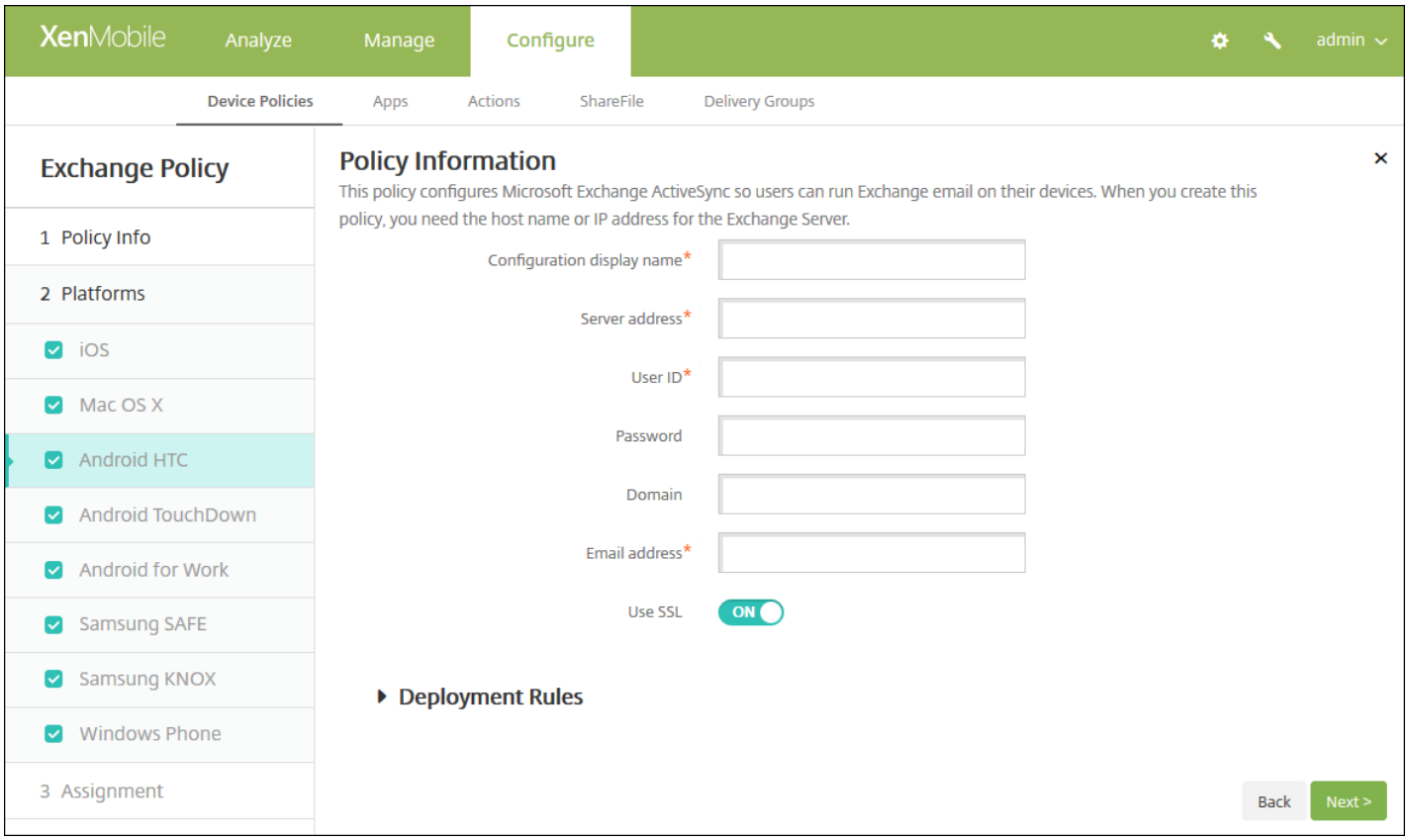
Configure estos parámetros:

- **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 para el servidor interno de Exchange.
- **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 para el servidor externo de Exchange.
- **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

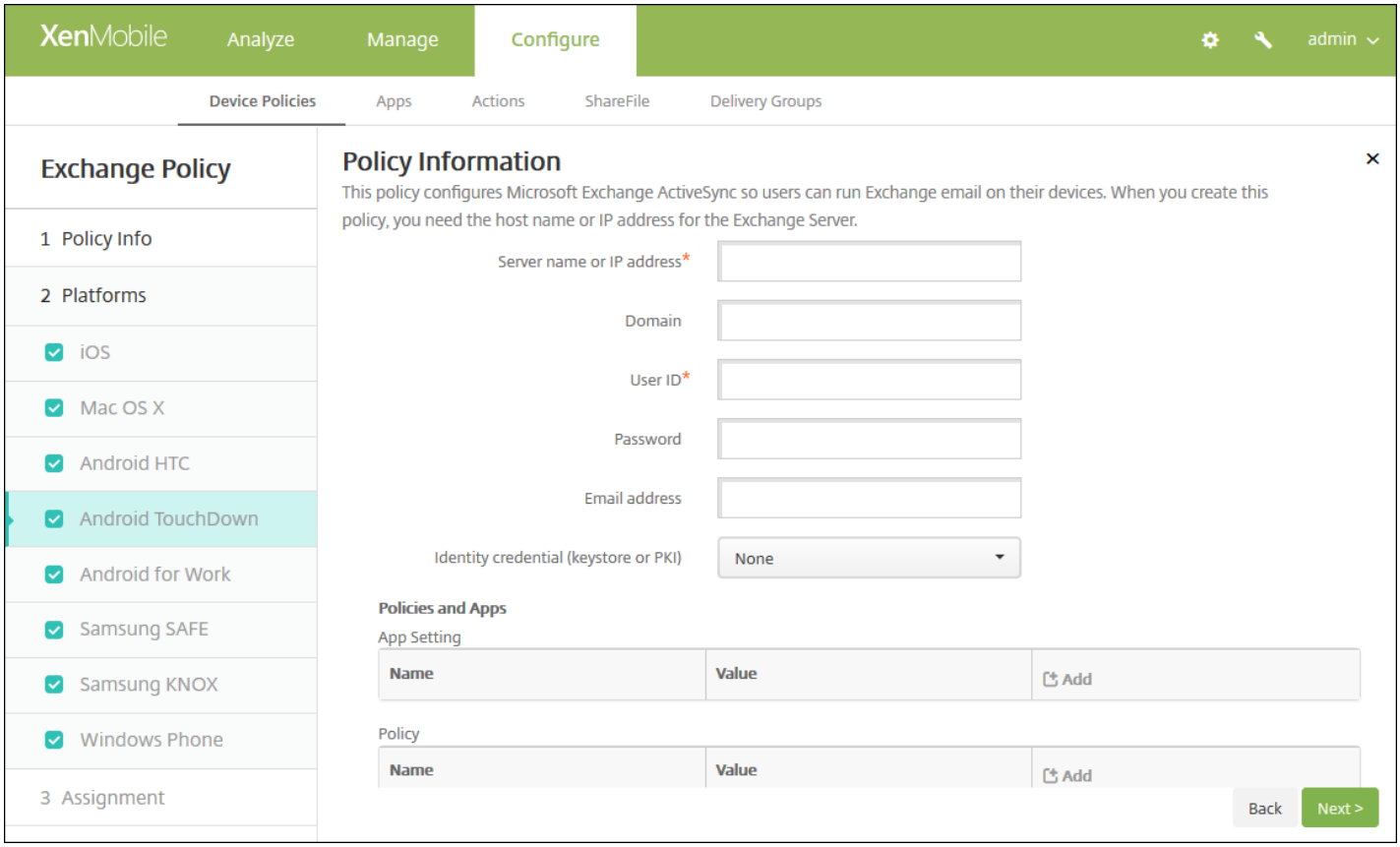


Configure estos parámetros:

- **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 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 donde 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**.

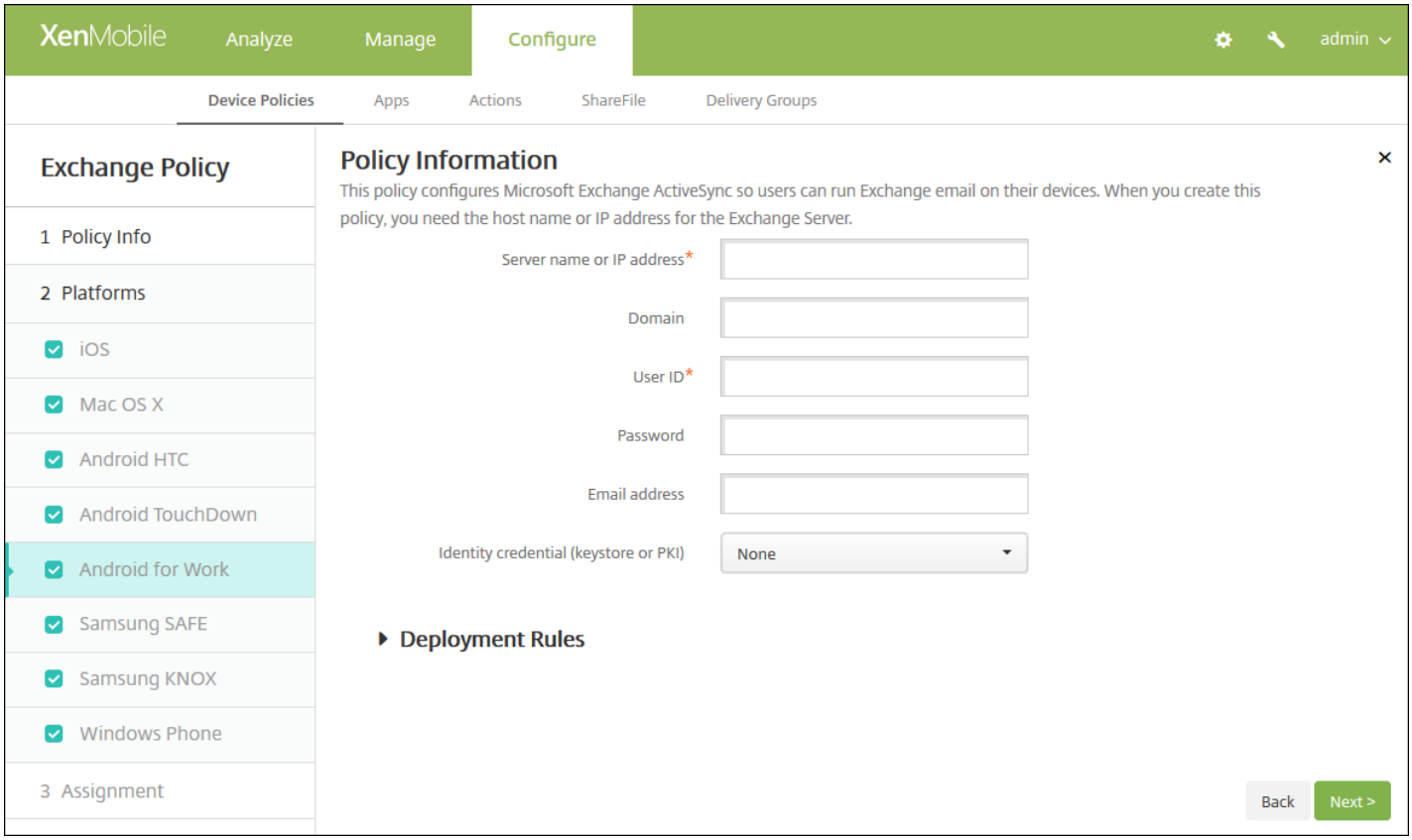
Configuración de los parámetros de Android TouchDown



Configure estos parámetros:

- **Server name or IP address**. Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain**. Escriba el dominio donde 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 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.

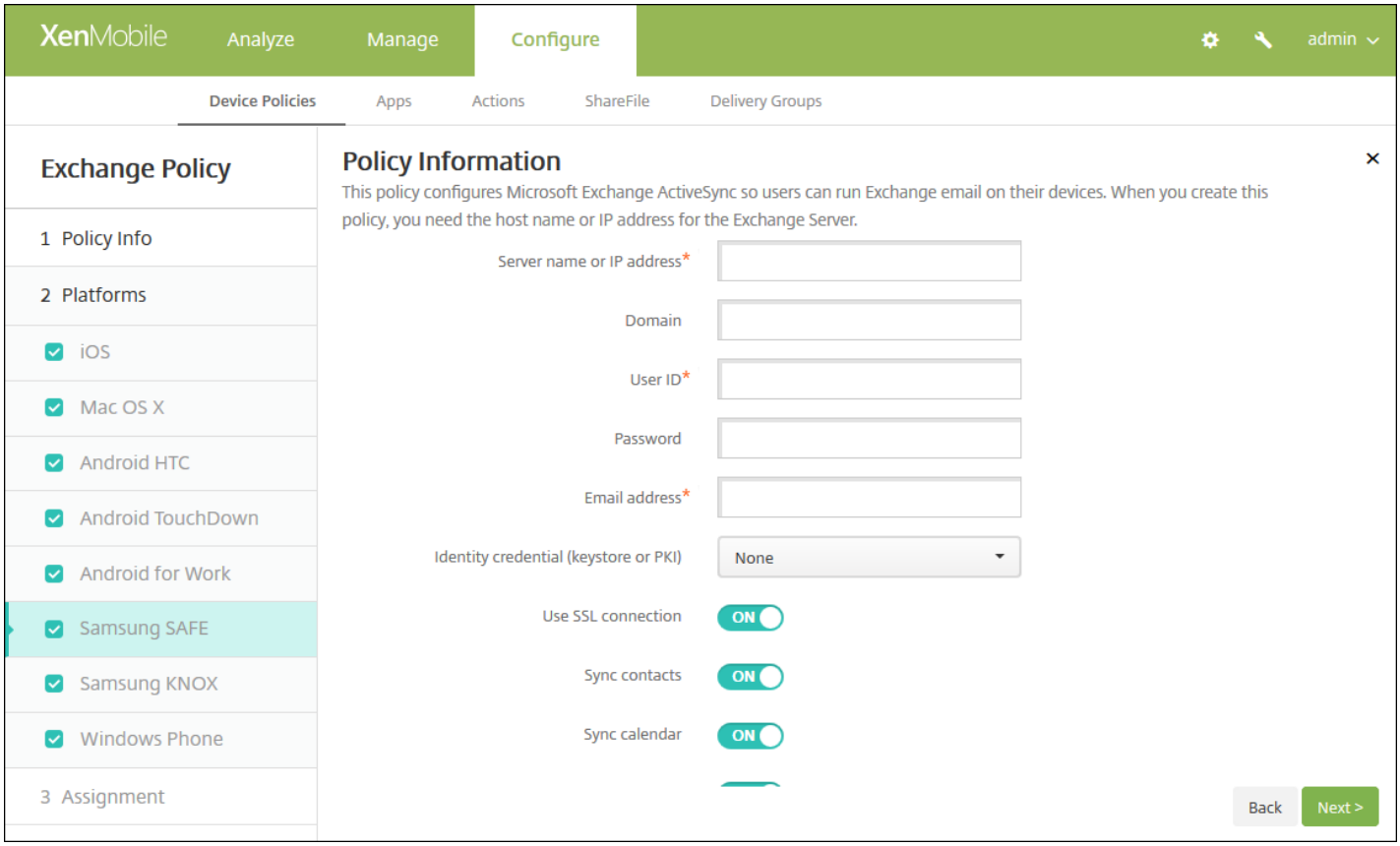
Configuración de los parámetros de Android for Work



Configure estos parámetros:

- **Server name or IP address**. Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain**. Escriba el dominio donde 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 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**.

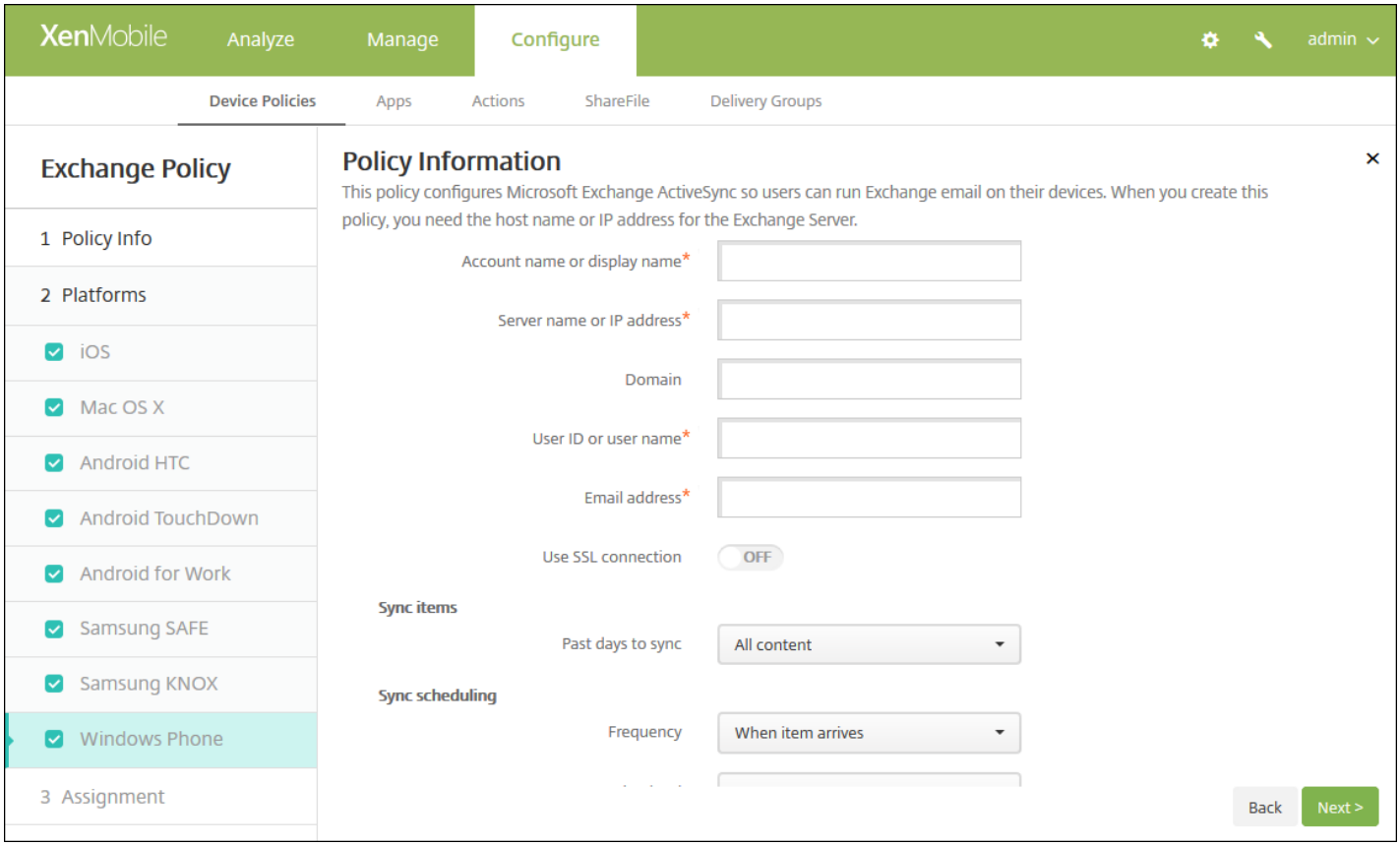
Configuración de los parámetros de Samsung SAFE y Samsung KNOX



Configure estos parámetros:

- **Server name or IP address**. Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain**. Escriba el dominio donde 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 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



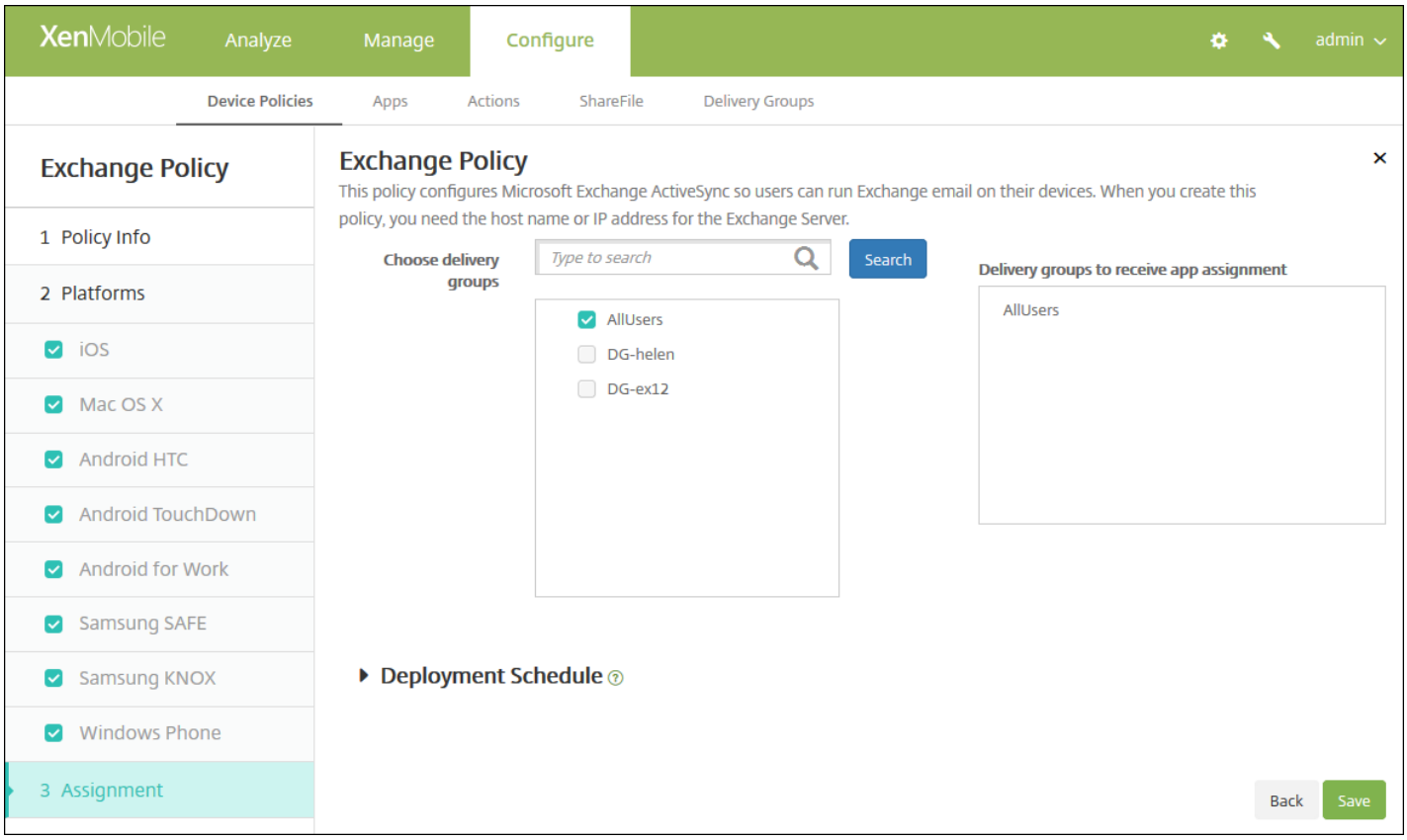
Configure estos parámetros:

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 donde 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 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 de **Exchange Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para información de la organización

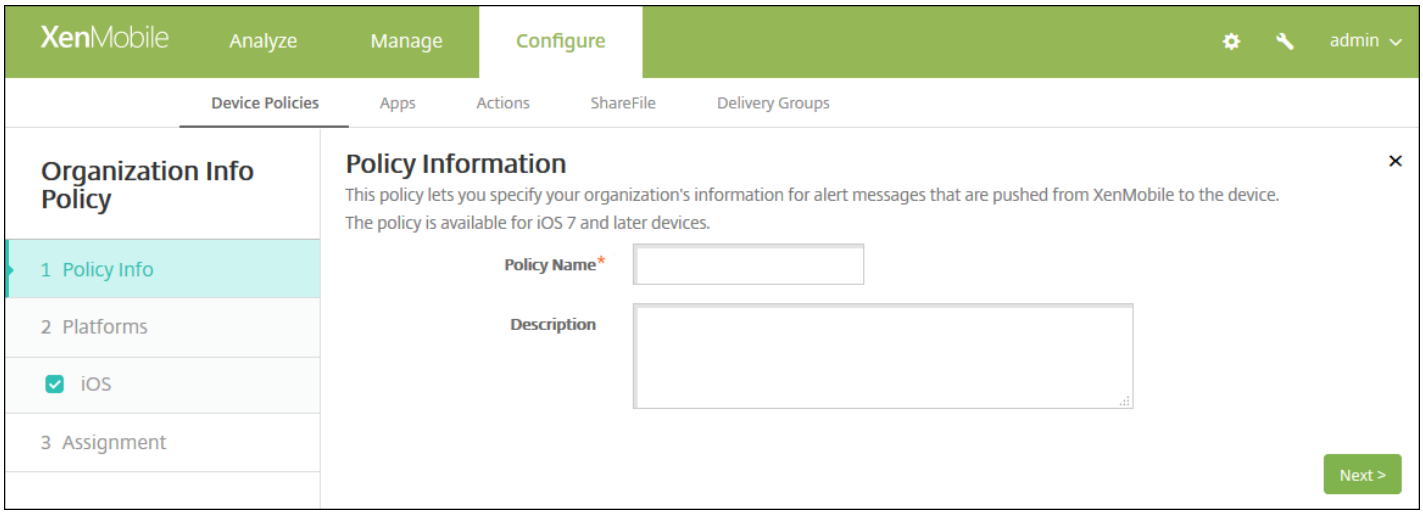
Feb 27, 2017

En XenMobile, puede agregar una directiva de dispositivos para especificar la información de su organización que se utilizará en los mensajes de alerta que envía XenMobile a dispositivos iOS. La directiva está disponible para los dispositivos iOS 7 y versiones posteriores.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

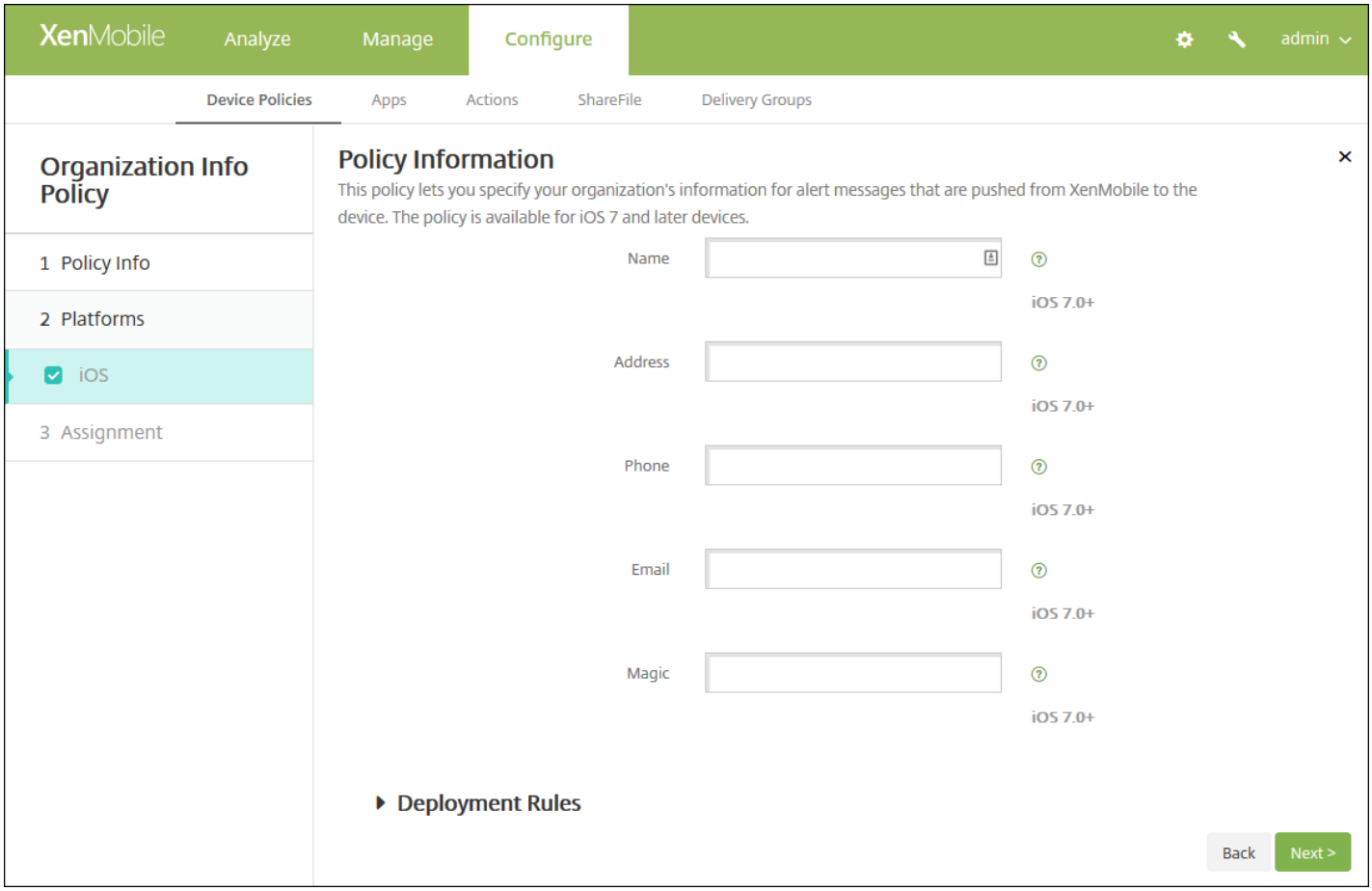
3. Haga clic en **More** y, en **End user**, haga clic en **Organization info**. Aparecerá la página **Organization Info Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **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 de la plataforma **iOS**.

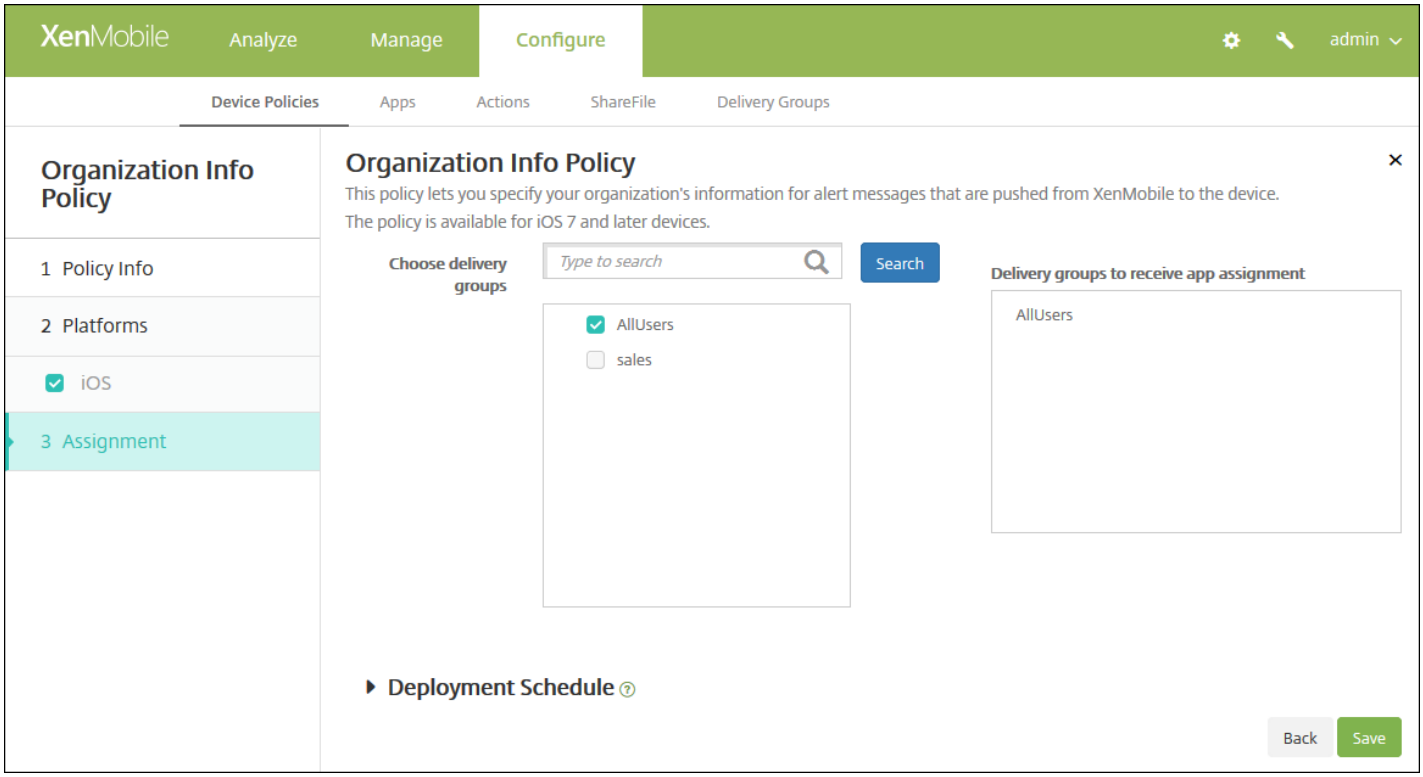


Configure estos parámetros:

- **Name**. Escriba el nombre de la organización que ejecuta XenMobile.
- **Address**. Escriba la dirección de la organización.
- **Phone**. Escriba el número de teléfono de asistencia de la organización.
- **Email**. Escriba la dirección de correo electrónico de asistencia.
- **Magic**. Escriba una palabra o frase que describa los servicios que ofrece la organización.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Organization Info Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para códigos de acceso

Feb 27, 2017

En XenMobile, puede crear una directiva de códigos de acceso en función de los requisitos de su empresa. Puede solicitar códigos de acceso en los dispositivos de los usuarios y configurar varias reglas de formatos y de códigos de acceso. Puede crear directivas para iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone y escritorios/tabletas Windows. 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

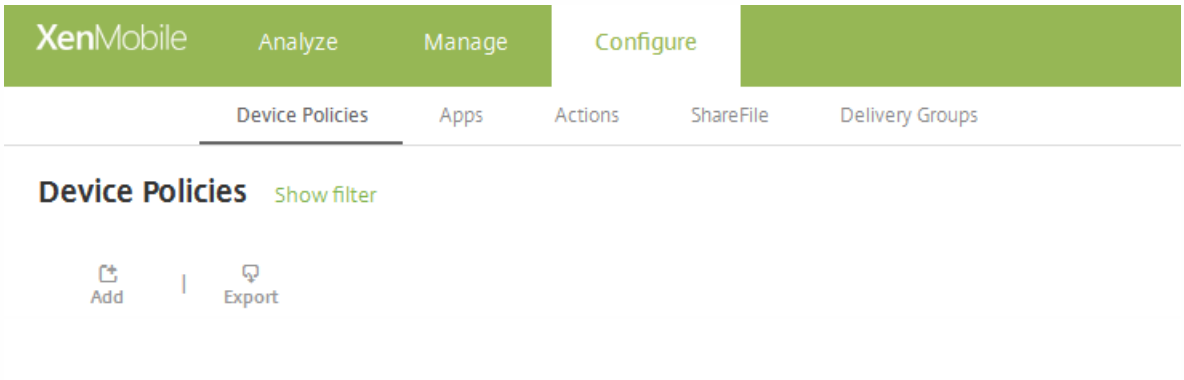
Configuración de Samsung KNOX

Configuración de Android for Work

Configuración de Windows Phone

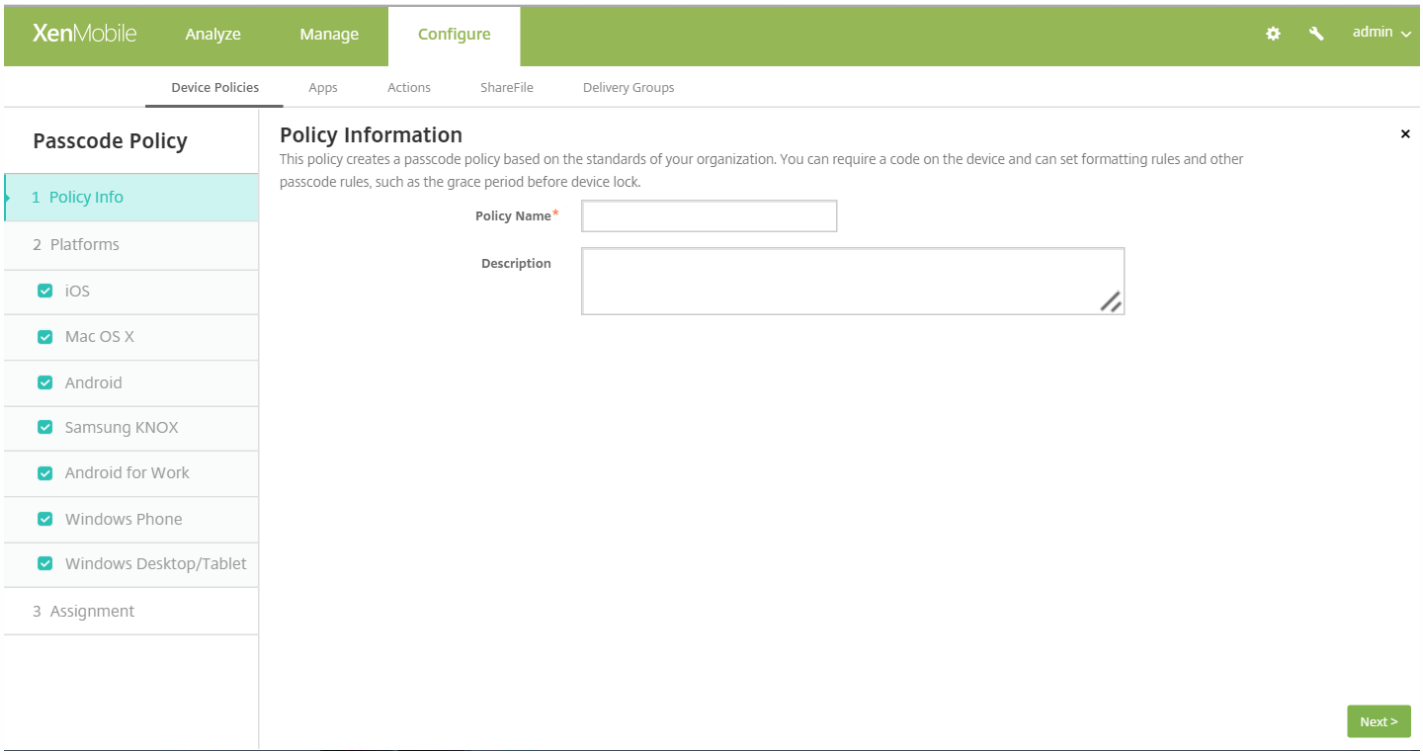
Configuración de escritorios y tabletas Windows

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.



2. Haga clic en **Add**. Aparecerá la página Add New Policy.

3. Haga clic en **Passcode**. Aparecerá la página de información Passcode Policy.



4. En el panel **Policy Information**, escriba la información siguiente:

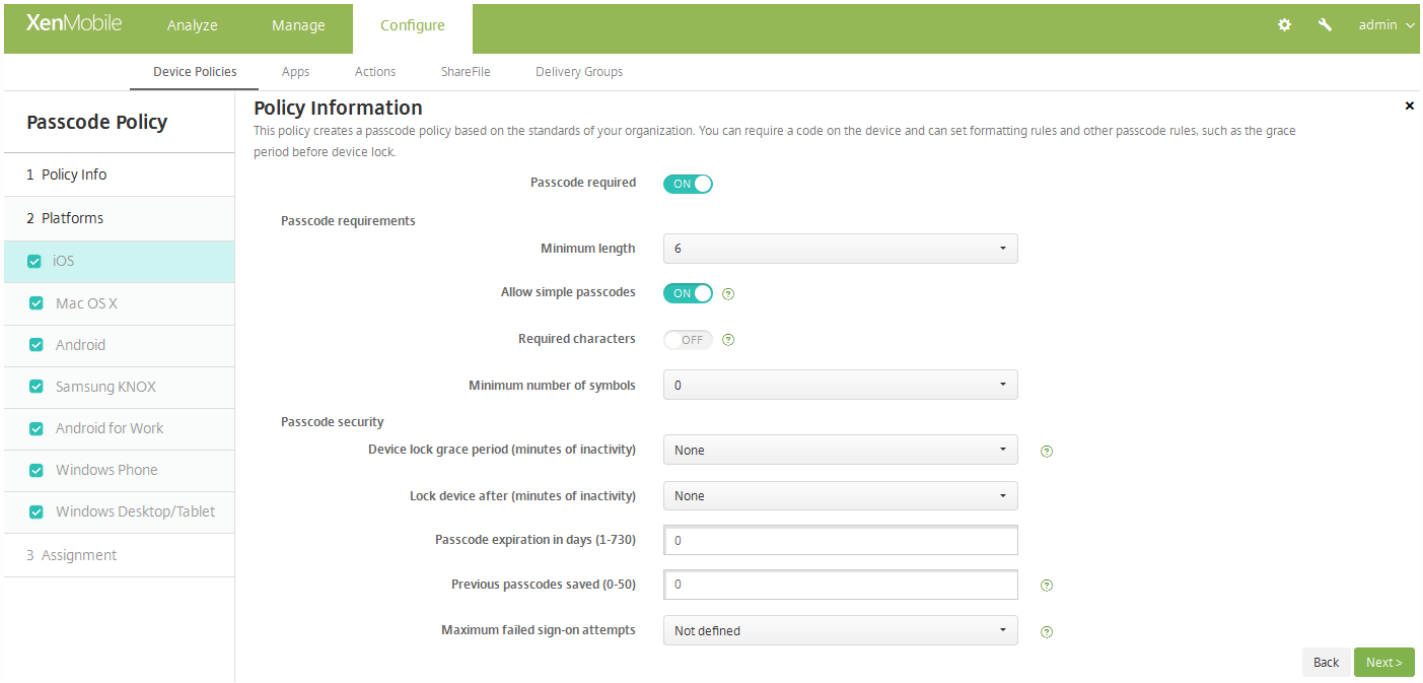
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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

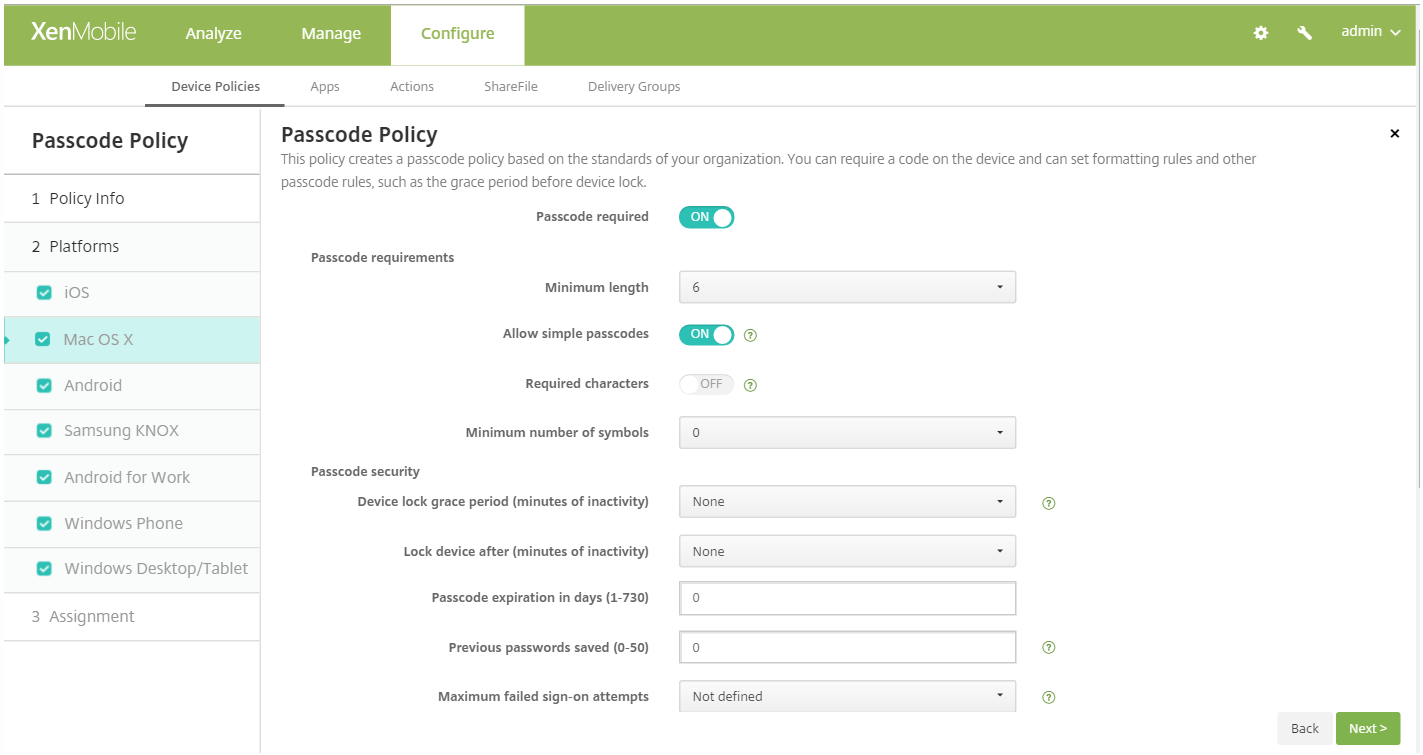


Configure los siguientes parámetros:

- **Passcode required**. Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de códigos de acceso para dispositivos iOS. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y configuraciones de directiva.
- **Requisitos de códigos de acceso**
  - **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Allow simple passcodes**. Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es **ON**.
  - **Required characters**. Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. El valor predeterminado es **OFF**.
  - **Minimum number of symbols**. En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **0**.
- **Seguridad de códigos de acceso**
  - **Device lock grace period (minutes of inactivity)**. En la lista, haga clic en el período de tiempo que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **None**.
  - **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es None.
  - **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
  - **Maximum failed sign-on attempts**. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se borre completamente el contenido del dispositivo. El valor predeterminado es **Not defined**.
- **Configuraciones de directivas**

- 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 list**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure estos parámetros:

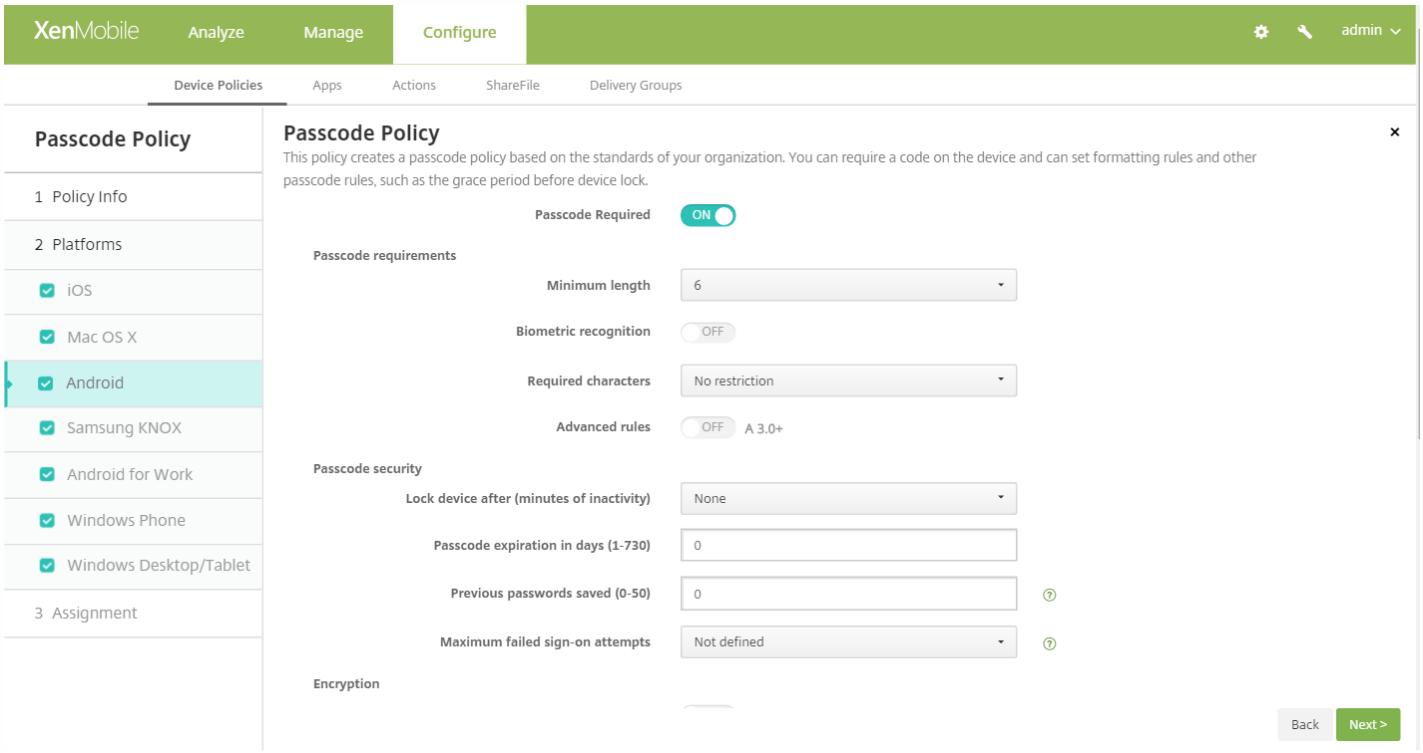
- **Passcode required**. Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de códigos de acceso para dispositivos iOS. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y configuraciones de directiva.
- Si no habilita **Passcode required**, junto a **Delay after failed sign-on attempts, in minutes**, escriba la cantidad de minutos de espera antes de permitir que los usuarios vuelvan a introducir sus códigos de acceso.
- Si habilita **Passcode required**, configure los siguientes parámetros:
- **Requisitos de códigos de acceso**
  - **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Allow simple passcodes**. Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es **ON**.
  - **Required characters**. Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. El valor predeterminado es **OFF**.
  - **Minimum number of symbols**. En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **0**.
- **Seguridad de códigos de acceso**
  - **Device lock grace period (minutes of inactivity)**. En la lista, haga clic en el período de tiempo que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor

predeterminado es **None**.

- **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
- **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
- **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Maximum failed sign-on attempts**. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se bloquee el dispositivo. El valor predeterminado es **Not defined**.
- **Delay after failed sign-on attempts, in minutes**. Escriba la cantidad de minutos de espera antes de permitir que un usuario vuelva a escribir un código de acceso.

- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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:

Nota: El valor predeterminado para Android es **OFF**.

- **Passcode required**. Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de

configuración de una directiva de códigos de acceso para dispositivos Android. La página se expande para que pueda definir las opciones de configuración de Samsung SAFE, los requisitos de los códigos de acceso, la seguridad de dichos códigos y el cifrado.

- **Requisitos de códigos de acceso**
  - **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.
  - **Biometric recognition**. Seleccione si habilitar el reconocimiento biométrico. Si se habilita esta opción, se oculta el campo Required characters. El valor predeterminado es **OFF**.
  - **Required characters**. En la lista, haga clic en "No Restriction", "Both numbers and letters", "Numbers only" o "Letters only" para definir la composición de los códigos de acceso. El valor predeterminado es No restriction.
  - **Advanced rules**. Seleccione si aplicar reglas avanzadas de códigos de acceso. Esta opción está disponible para Android 3.0 y versiones posteriores. El valor predeterminado es **OFF**.
  - Si habilita **Advanced rules**, en cada una de las siguientes listas, haga clic en la cantidad mínima de cada tipo de carácter que debe contener un código de acceso:
    - **Symbols**. La cantidad mínima de símbolos.
    - **Letters**. La cantidad mínima de letras.
    - **Lowercase letters**. La cantidad mínima de minúsculas.
    - **Uppercase letters**. La cantidad mínima de mayúsculas.
    - **Numbers or symbols**. La cantidad mínima de números o símbolos.
    - **Numbers**. La cantidad mínima de números.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
  - **Maximum failed sign-on attempts**. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se borre el contenido del dispositivo. El valor predeterminado es **Not defined**.
- **Cifrado**
  - **Enable encryption**. Seleccione si habilitar el cifrado. Esta opción está disponible para Android 3.0 y versiones posteriores. La opción está disponible independientemente de la opción de configuración **Passcode required**.

    Nota: Para cifrar los dispositivos, los usuarios deben empezar el proceso con la batería cargada y deben mantener el dispositivo enchufado durante el tiempo que tarde el cifrado. Si interrumpen el proceso de cifrado, pueden perder alguno o todos los datos de los dispositivos. Una vez cifrado el dispositivo, el proceso no se puede revertir excepto si se restablecen los valores de fábrica (proceso con el que se borrarán todos los datos hasta entonces almacenados en el dispositivo).

- **Samsung SAFE**
  - **Use same passcode across all users**. Seleccione si utilizar el mismo código de acceso para todos los usuarios. El valor predeterminado es **OFF**. Esta opción solo se aplica a dispositivos Samsung SAFE y está disponible independientemente de la opción de configuración **Passcode required**.
  - Cuando habilite **Use same passcode across all users**, escriba el código de acceso que utilizarán todos los usuarios en el campo **Passcode**.
  - Si habilita **Passcode required**, configure los siguientes parámetros de Samsung SAFE:
    - **Changed characters**. Escriba la cantidad de caracteres que los usuarios deben cambiar de su código de acceso

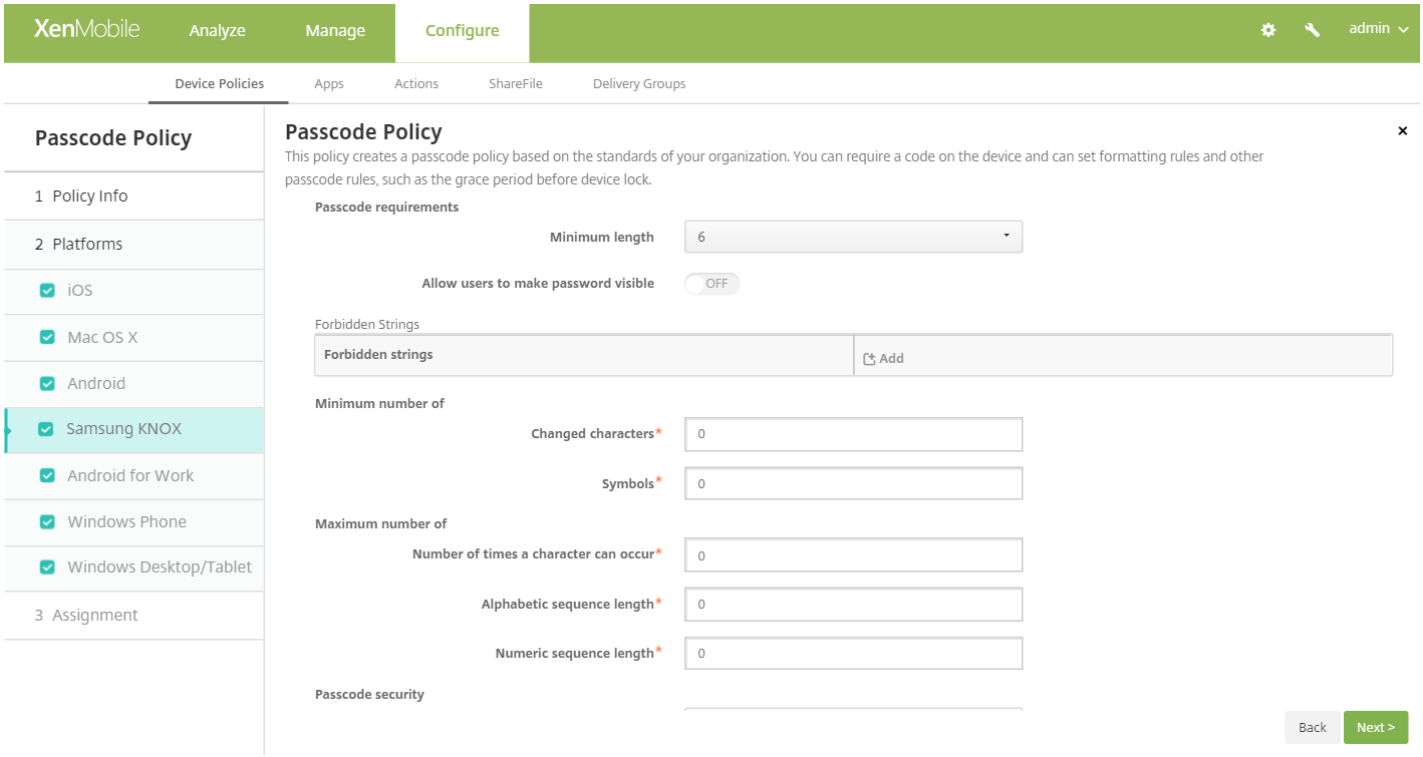
anterior. El valor predeterminado es **0**.

- **Number of times a character can occur**. Especifique la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**.
- **Alphabetic sequence length**. Escriba la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**.
- **Numeric sequence length**. Escriba la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**.
- **Allow users to make password visible**. Seleccione si los usuarios pueden hacer visibles sus códigos de acceso. El valor predeterminado es **ON**.
- **Forbidden strings**. Cree cadenas prohibidas para evitar que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como "contraseña", "contra", "bienvenida", "123456" o "111111", entre otras. Para cada cadena que quiera prohibir, haga clic en **Add** y haga lo siguiente:
  - **Forbidden strings**. Escriba la cadena que los usuarios no pueden usar.
  - Haga clic en **Save** para agregar la cadena, o bien haga clic en **Cancel** para no agregarla.

    Nota: Para eliminar una cadena 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 cadena existente, coloque el cursor sobre la línea que la contiene y haga clic en el icono de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardarlos, o bien en **Cancel** para descartarlos.

Configuración de los parámetros de Samsung KNOX



Configure estos parámetros:

- **Requisitos de códigos de acceso**

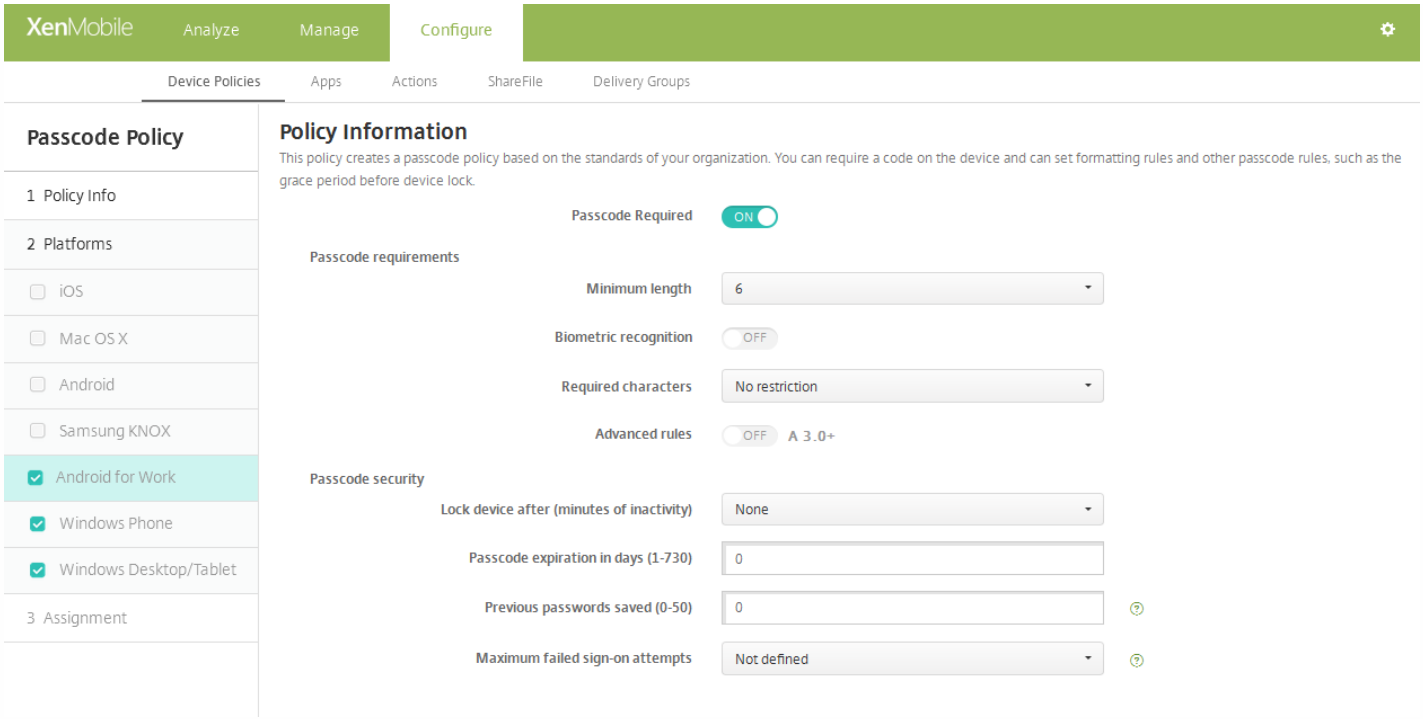
- **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
- **Allow users to make password visible**. Seleccione si los usuarios pueden hacer visibles sus contraseñas.
- **Forbidden strings**. Cree cadenas prohibidas para evitar que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como "contraseña", "contra", "bienvenida", "123456" o "111111", entre otras. Para cada cadena que quiera prohibir, haga clic en Add y haga lo siguiente:
  - **Forbidden strings**. Escriba la cadena que los usuarios no pueden usar.
  - Haga clic en **Save** para agregar la cadena, o bien haga clic en **Cancel** para no agregarla.

    Nota: Para eliminar una cadena 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 cadena existente, coloque el cursor sobre la línea que la contiene y haga clic en el icono de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardarlos, o bien en **Cancel** para descartarlos.

- **Cantidad mínima de**
  - **Changed characters**. Escriba la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
  - **Symbols**. Escriba la cantidad mínima de símbolos necesarios en un código de acceso. El valor predeterminado es **0**.
- **Cantidad máxima de**
  - **Number of times a character can occur**. Especifique la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**.
  - **Alphabetic sequence length**. Escriba la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**.
  - **Numeric sequence length**. Escriba la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de segundos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
  - **If the number of failed sign on attempts is exceeded, the device is locked**. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión antes de que se bloquee el dispositivo. El valor predeterminado es **Not defined**.
  - **If the number of failed sign on attempts is exceeded, the device is wiped**. En la lista, haga clic en la cantidad de inicios de sesión que puede fallar un usuario, antes de que el contenedor KNOX (junto con los datos de KNOX) se borre del dispositivo. Los usuarios tienen que reinicializar el contenedor KNOX después del borrado. El valor predeterminado es **Not defined**.

Configuración de los parámetros de Android for Work

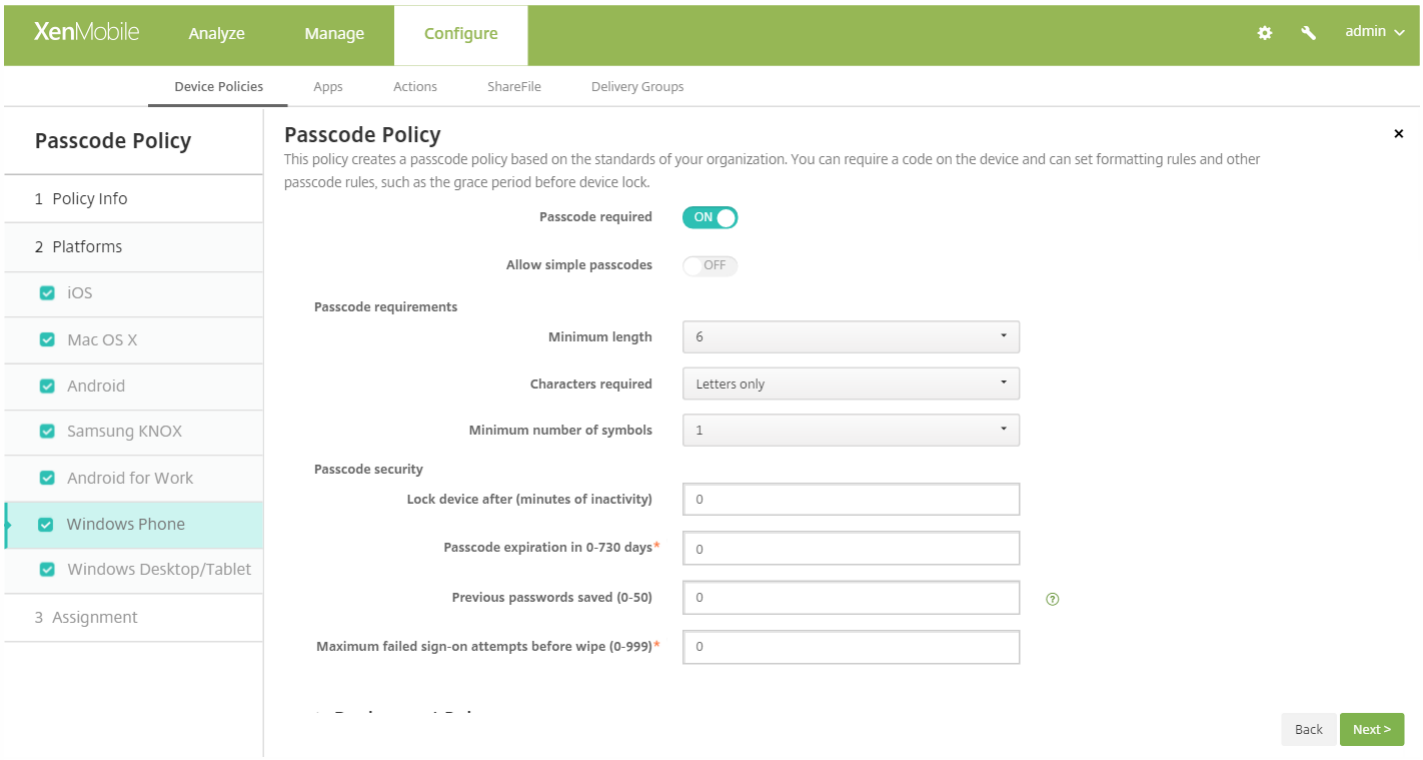


Configure estos parámetros:

- **Passcode required**. Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de códigos de acceso para dispositivos Android for Work. La página se expande para que pueda definir las opciones de configuración para los requisitos y la seguridad de los códigos de acceso.
- **Requisitos de códigos de acceso**
  - **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Biometric recognition**. Seleccione si habilitar el reconocimiento biométrico. Si se habilita esta opción, se oculta el campo **Required characters**. El valor predeterminado es **OFF**. Tenga en cuenta que esta función no se admite actualmente.
  - **Required characters**. En la lista, haga clic en **No Restriction**, **Both numbers and letters**, **Numbers only** o **Letters only** para configurar la composición de los códigos de acceso. El valor predeterminado es **No restriction**.
  - **Advanced rules**. Seleccione si aplicar reglas avanzadas de códigos de acceso. Esta opción no está disponible para dispositivos Android con versiones anteriores a Android 5.0. El valor predeterminado es **OFF**.
  - Si habilita **Advanced rules**, en cada una de las siguientes listas, haga clic en la cantidad mínima de cada tipo de carácter que debe contener un código de acceso:
    - **Symbols**. La cantidad mínima de símbolos.
    - **Letters**. La cantidad mínima de letras.
    - **Lowercase letters**. La cantidad mínima de minúsculas.
    - **Uppercase letters**. La cantidad mínima de mayúsculas.
    - **Numbers or symbols**. La cantidad mínima de números o símbolos.
    - **Numbers**. La cantidad mínima de números.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.

- **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Maximum failed sign-on attempts**. En la lista, haga clic en la cantidad de inicios de sesión que puede fallar un usuario, antes de que el contenedor KNOX (junto con los datos de KNOX) se borre del dispositivo. Los usuarios tienen que reinicializar el contenedor KNOX después del borrado. El valor predeterminado es **Not defined**.

Configuración de los parámetros de Windows Phone

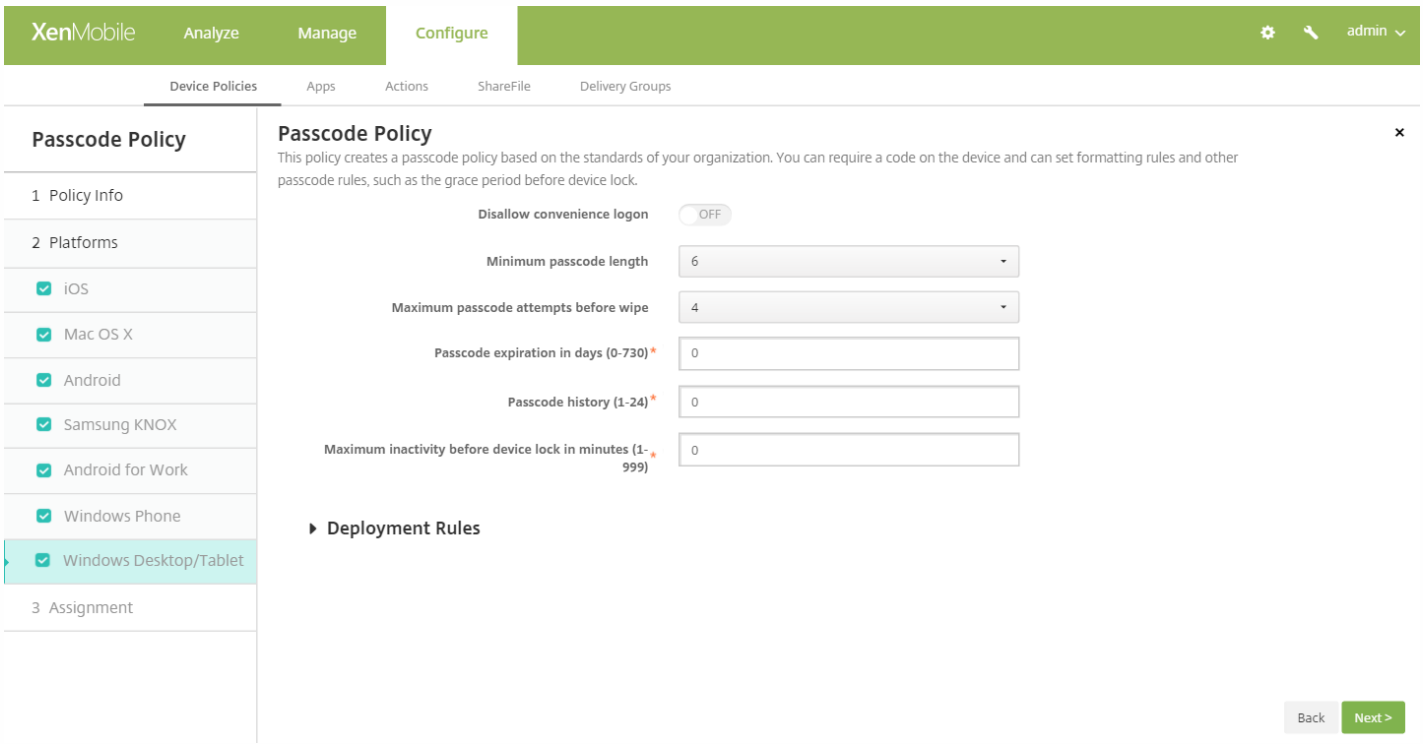


Configure estos parámetros:

- **Passcode required**. Seleccione esta opción para no requerir un código de acceso en los dispositivos Windows Phone. El parámetro predeterminado es **ON**, lo que requiere un código de acceso. La página se contrae y las siguientes opciones desaparecen cuando se inhabilita esta opción de configuración.
- **Allow simple passcodes**. Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es OFF.
- **Requisitos de códigos de acceso**
  - **Minimum length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Characters required**. En la lista, haga clic en **Numeric or alphanumeric**, **Letters only** o **Numbers only** para definir la composición de los códigos de acceso. El valor predeterminado es **Letters only**.
  - **Minimum number of symbols**. En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **1**.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity)**. En la lista, haga clic en los minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **0**.
  - **Passcode expiration in 0-730 days**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 0 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.

- **Previous passwords saved (0-50)**. Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Maximum failed sign-on attempts before wipe (0-999)**. Introduzca cuántas veces puede un usuario fallar el inicio de sesión antes de que los datos de empresa se borren del dispositivo. El valor predeterminado es **0**.

Configuración de los parámetros de escritorios o tabletas Windows

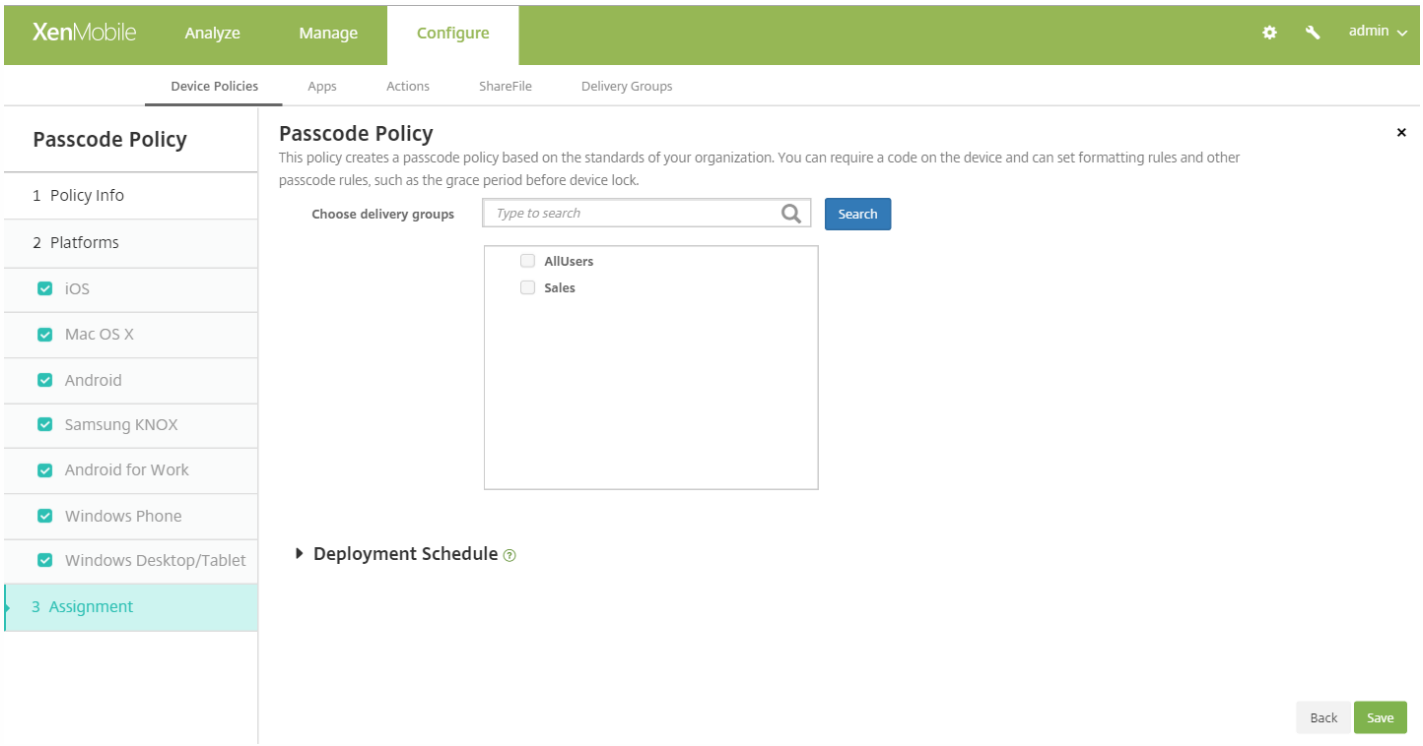


Configure estos parámetros:

- **Disallow convenience logon**. Seleccione si permitir que los usuarios accedan a sus dispositivos con contraseñas de imagen o inicios de sesión biométricos. El valor predeterminado es **OFF**.
- **Minimum passcode length**. En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
- **Maximum passcode attempts before wipe**. En la lista, haga clic en la cantidad de veces que un usuario puede fallar al iniciar sesión hasta que los datos de empresa se borren del dispositivo. El valor predeterminado es **4**.
- **Passcode expiration in days (0-730)**. Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 0 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
- **Passcode history: (1-24)**. Escriba la cantidad de códigos de acceso utilizados que se van a guardar. Los usuarios no pueden usar ningún código de acceso que esté incluido en esta lista. Cualquier valor entre 1 y 24 es válido. En este campo debe escribir un número entre 1 y 24. El valor predeterminado es **0**.
- **Maximum inactivity before device lock in minutes (1-999)**. Escriba la cantidad de tiempo (en minutos) que un dispositivo puede estar inactivo antes de bloquearse. Cualquier valor entre 1 y 999 es válido. En este campo, debe escribir un número entre 1 y 999. El valor predeterminado es **0**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Passcode Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 hotspot personal

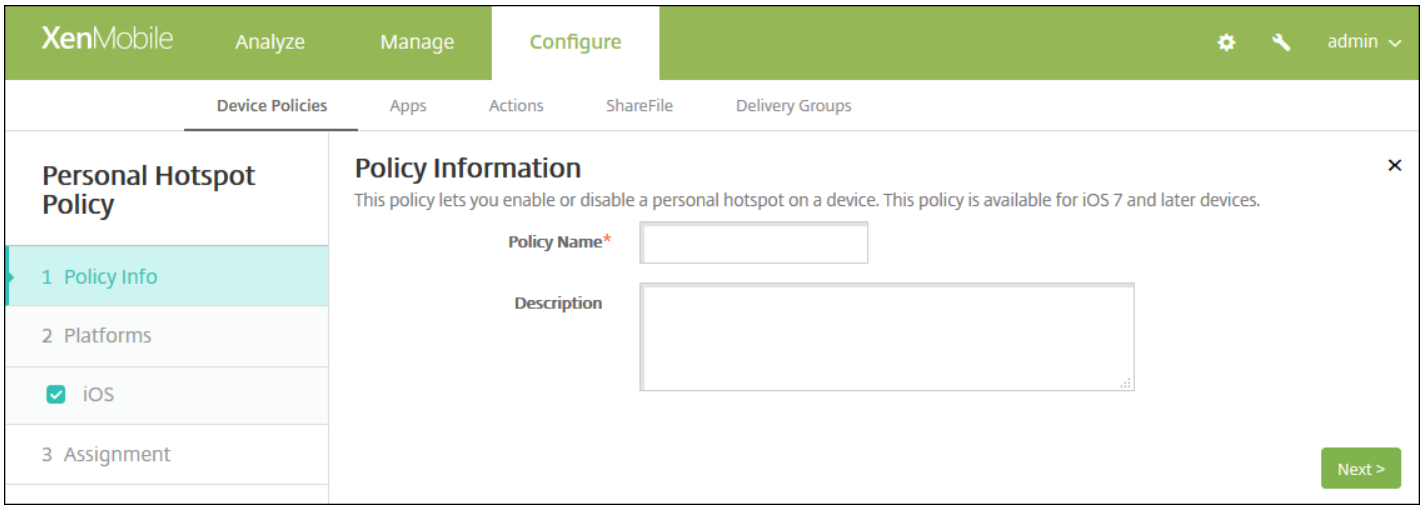
Feb 27, 2017

Puede permitir que los usuarios se conecten a Internet aunque estén fuera del alcance de una red WiFi, 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.

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**.

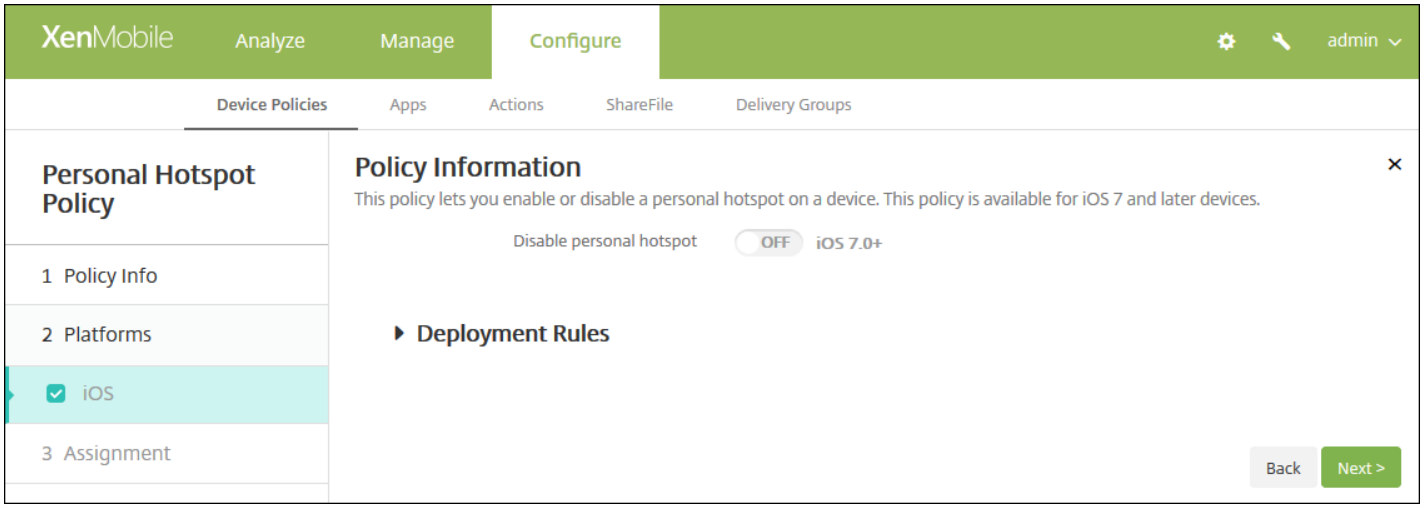
3. Expanda **More** y, a continuación, en **Network Access**, haga clic en **Personal Hotspot**. Aparecerá la página de información **Personal Hotspot Policy**.



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 de la plataforma **iOS**.

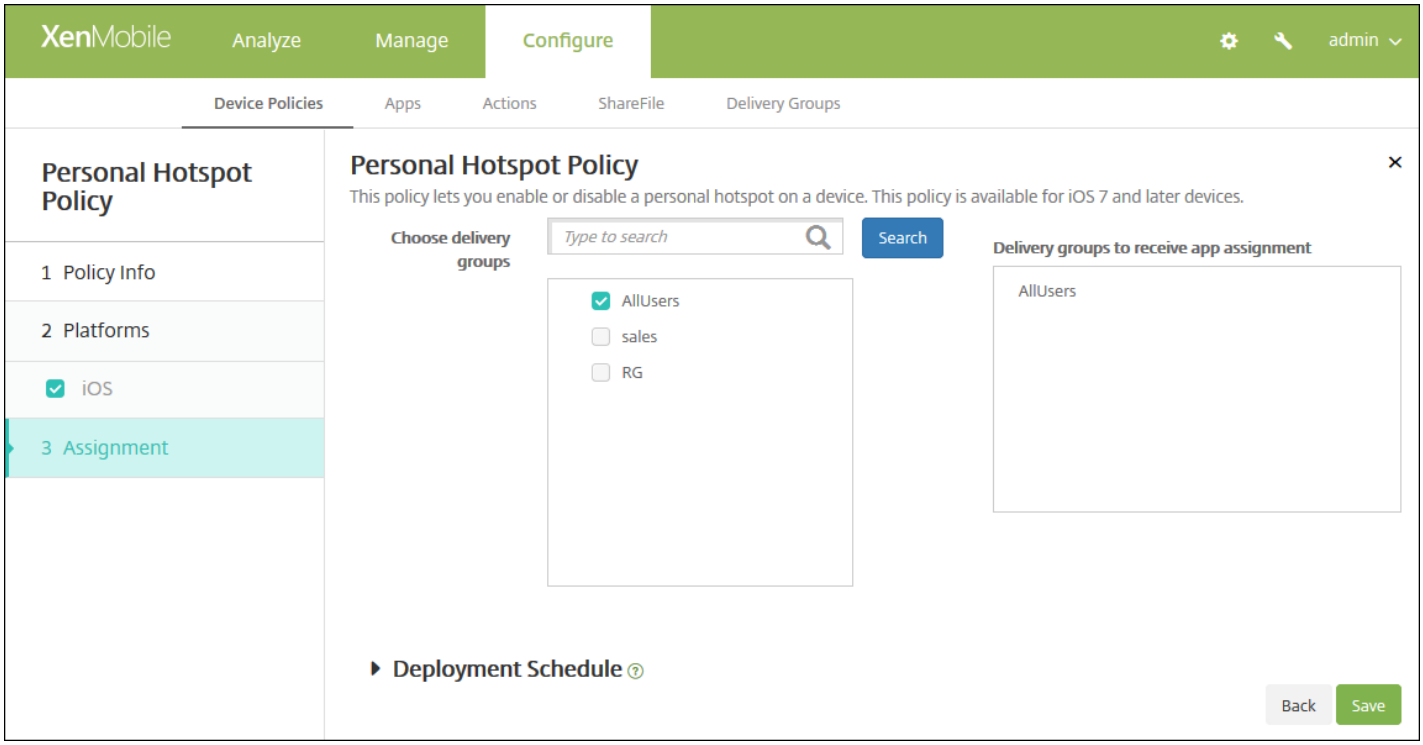


6. Configure este parámetro:

- **Disable personal hotspot**. Seleccione si quiere inhabilitar la función de hotspot personal (Compartir Internet) en los dispositivos de los usuarios. El valor predeterminado es **OFF**, lo que desactiva la función de hotspot personal (Compartir Internet) de los dispositivos de los usuarios. Esta directiva no inhabilita la función y los usuarios pueden seguir usando la función de hotspot personal (Compartir Internet) en sus dispositivos. Sin embargo, cuando se implementa la directiva, dicha función se desactiva, con lo que se cambia la opción predeterminada (seguir activa).

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Personal Hotspot Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para eliminación de perfiles

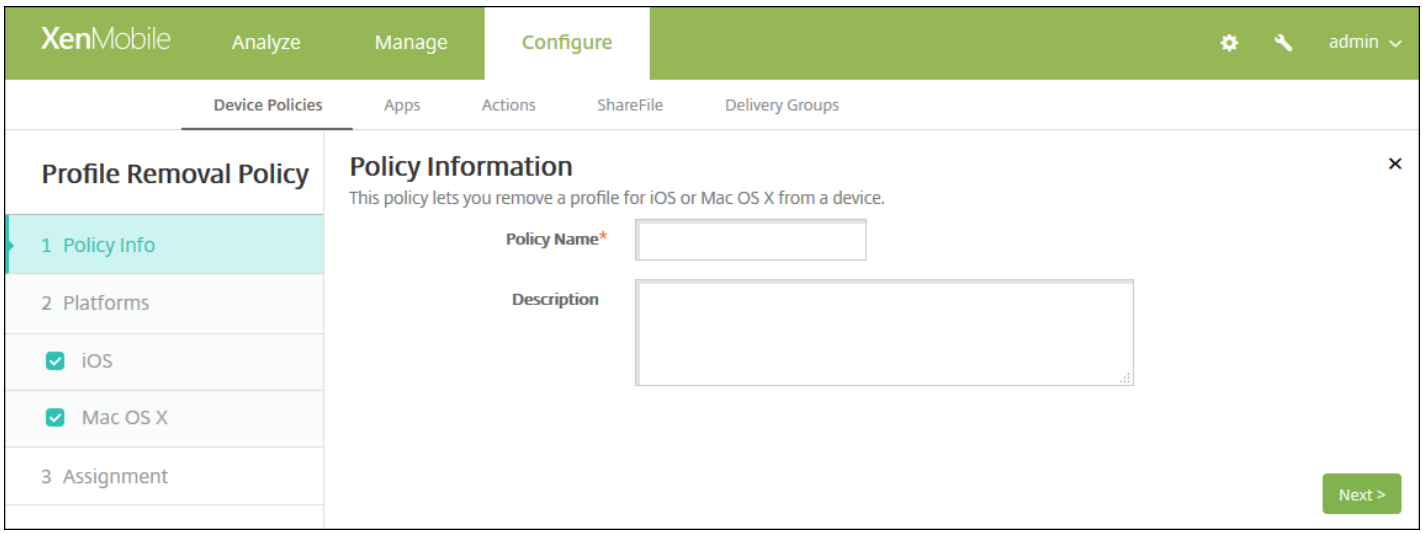
Feb 27, 2017

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.

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 **Removal**, haga clic en **Profile Removal**. Aparecerá la página de información **Profile Removal Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

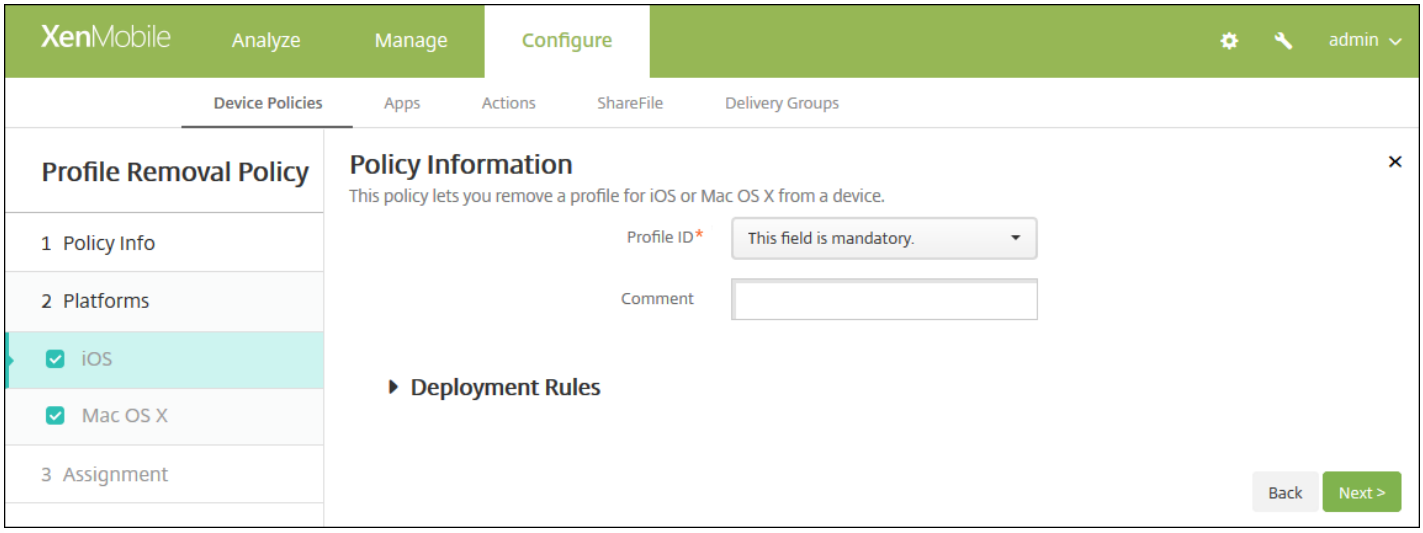
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

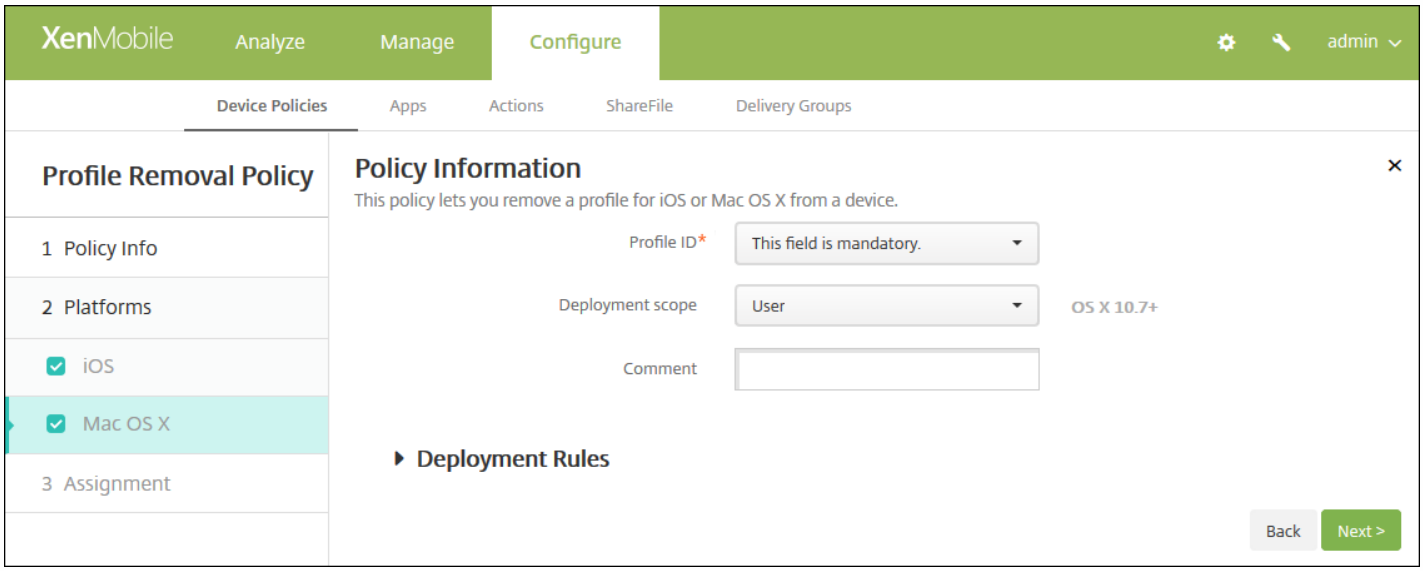
Configuración de los parámetros de iOS



Configure estos parámetros:

- **Profile ID**. En la lista, haga clic en el ID del perfil de aplicación. Este campo es obligatorio.
- **Comment**. Si quiere, escriba un comentario.

Configuración de los parámetros de Mac OS X

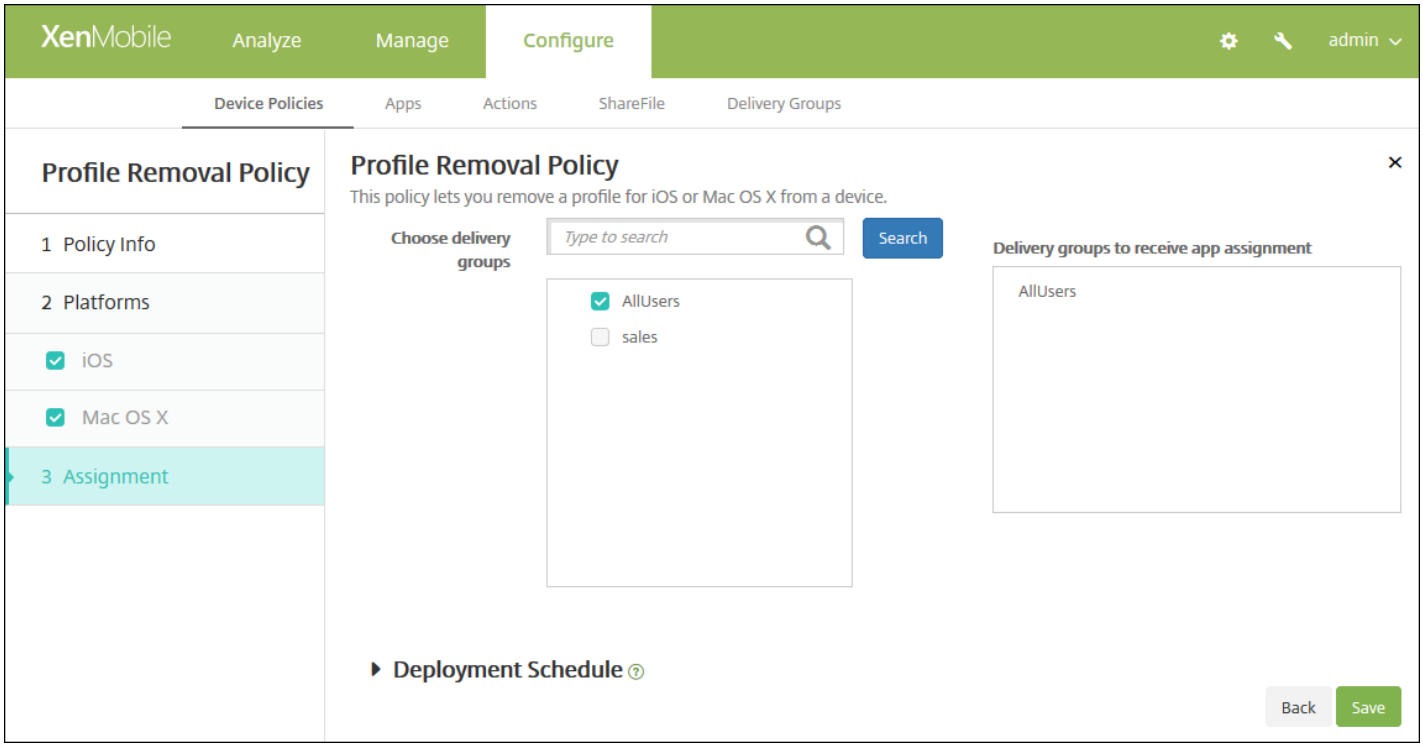


Configure estos parámetros:

- **Profile ID**. En la lista, haga clic en el ID del perfil de aplicación. Este campo es obligatorio.
- **Deployment scope**. En la lista, haga clic en **User** o **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.
- **Comment**. Si quiere, escriba un comentario.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Profile Removal Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo de Perfil de aprovisionamiento

Feb 27, 2017

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 en ella 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.

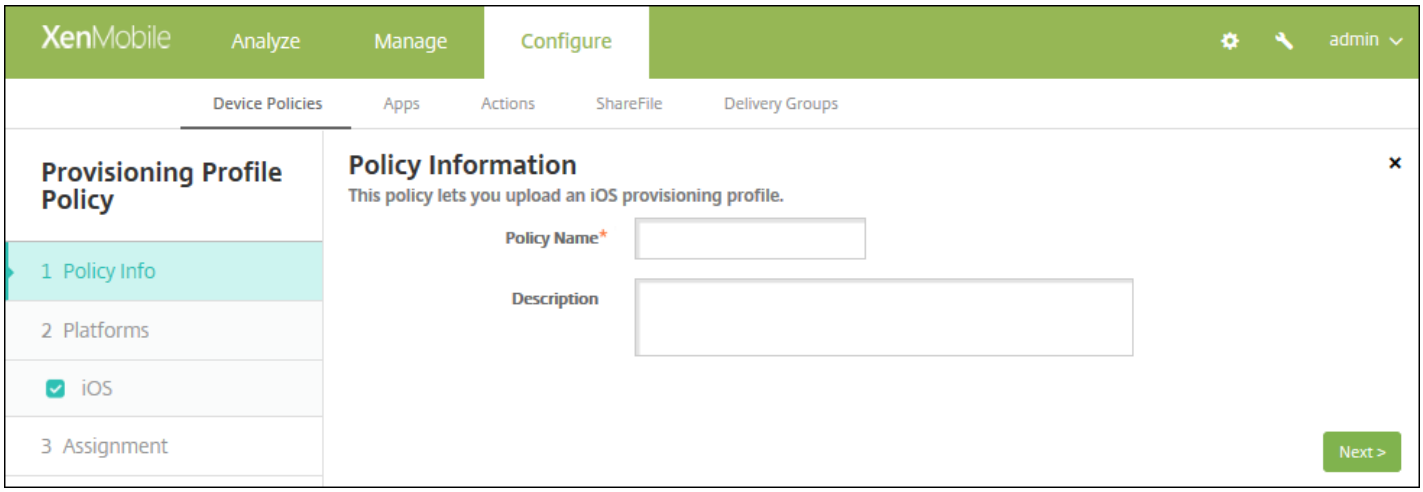
Si quiere que este proceso sea transparente para los usuarios, en XenMobile puede instalar y quitar perfiles de aprovisionamiento con directivas de dispositivo. Se quitan los perfiles que falten o hayan caducado y se instalan perfiles actualizados en los dispositivos de los usuarios, por lo que tocar una aplicación solo la abre para su uso.

Antes de crear una directiva de perfiles de aprovisionamiento, cree un archivo de perfil de aprovisionamiento. Para obtener más información, consulte Creating Provisioning Profiles en el sitio para desarrolladores 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 la página **Add a New Policy**.

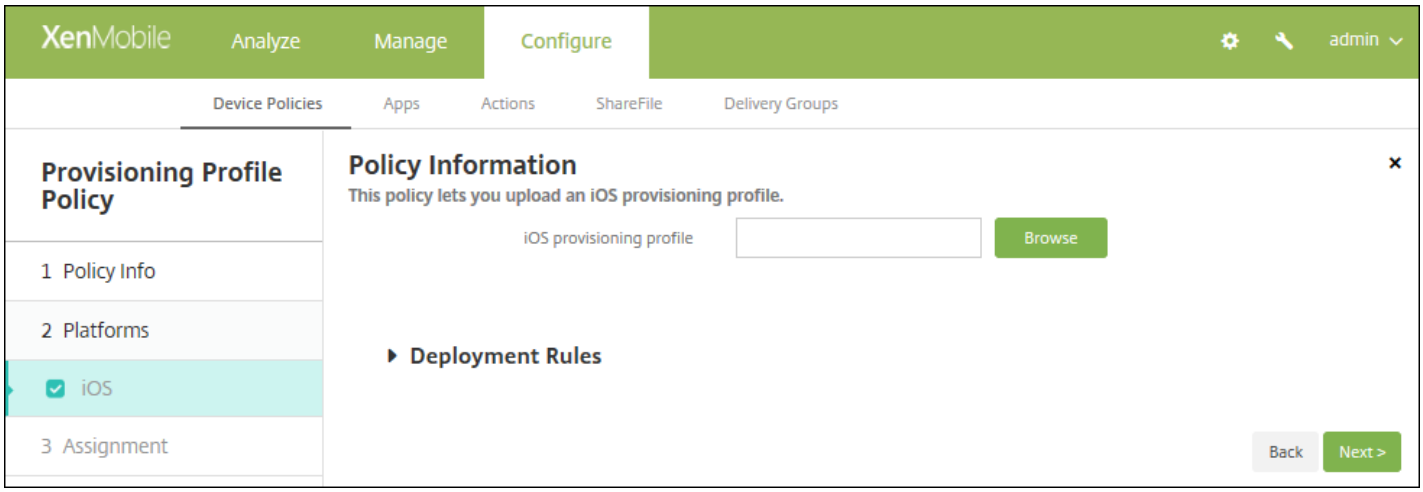
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Provisioning Profile**. Aparecerá la página de información **Provisioning Profile Policy**.



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 de la plataforma **iOS**.

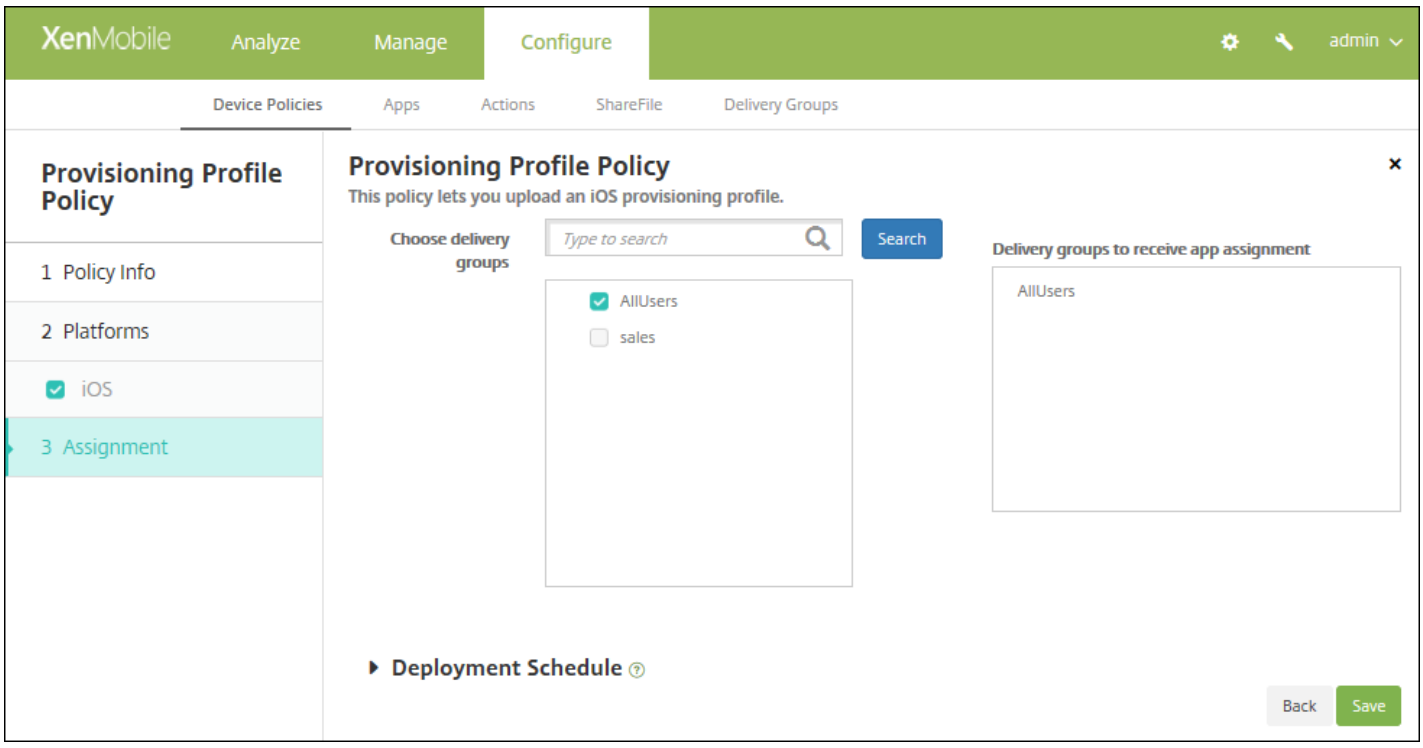


6. Configure este parámetro:

- **iOS provisioning profile**. Seleccione el archivo del perfil de aprovisionamiento que quiere importar. Para ello, haga clic en **Browse** y vaya a la ubicación de ese archivo.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Provisioning Profile Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 perfiles de aprovisionamiento

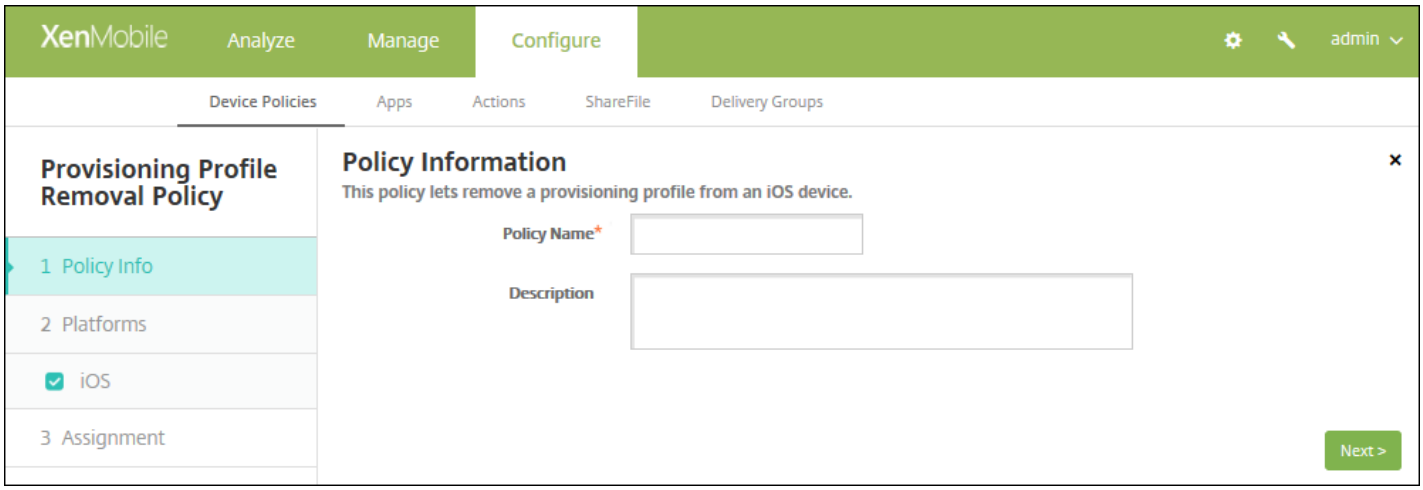
Feb 27, 2017

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.

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**.

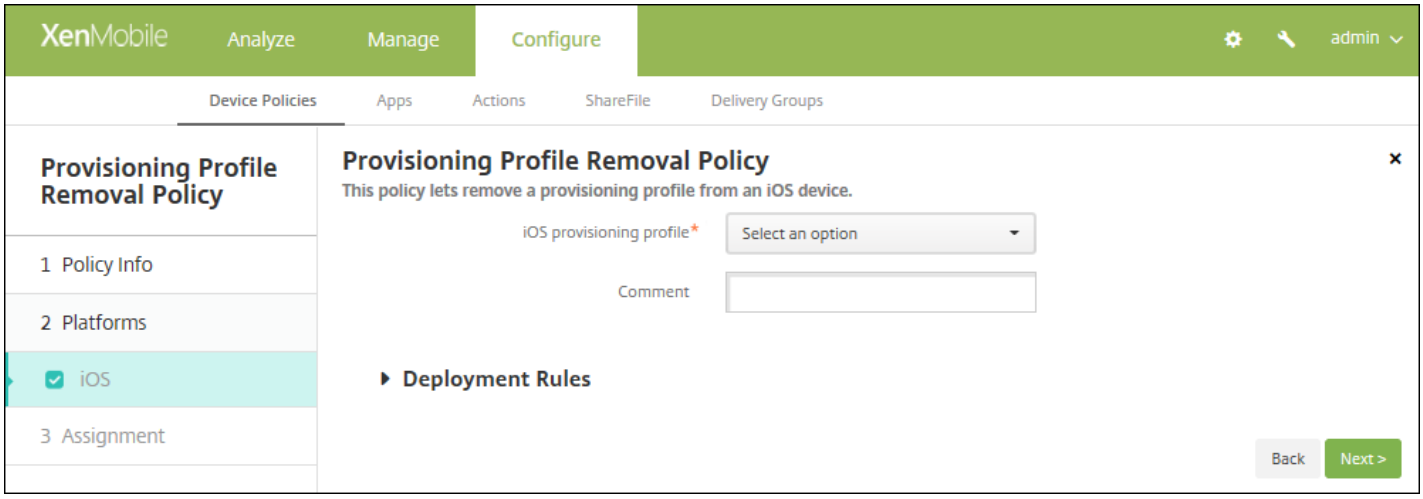
3. Expanda **More** y, a continuación, en **Removal**, haga clic en **Provisioning Profile Removal**. Aparecerá la página de información **Provisioning Profile Removal Policy**.



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**.

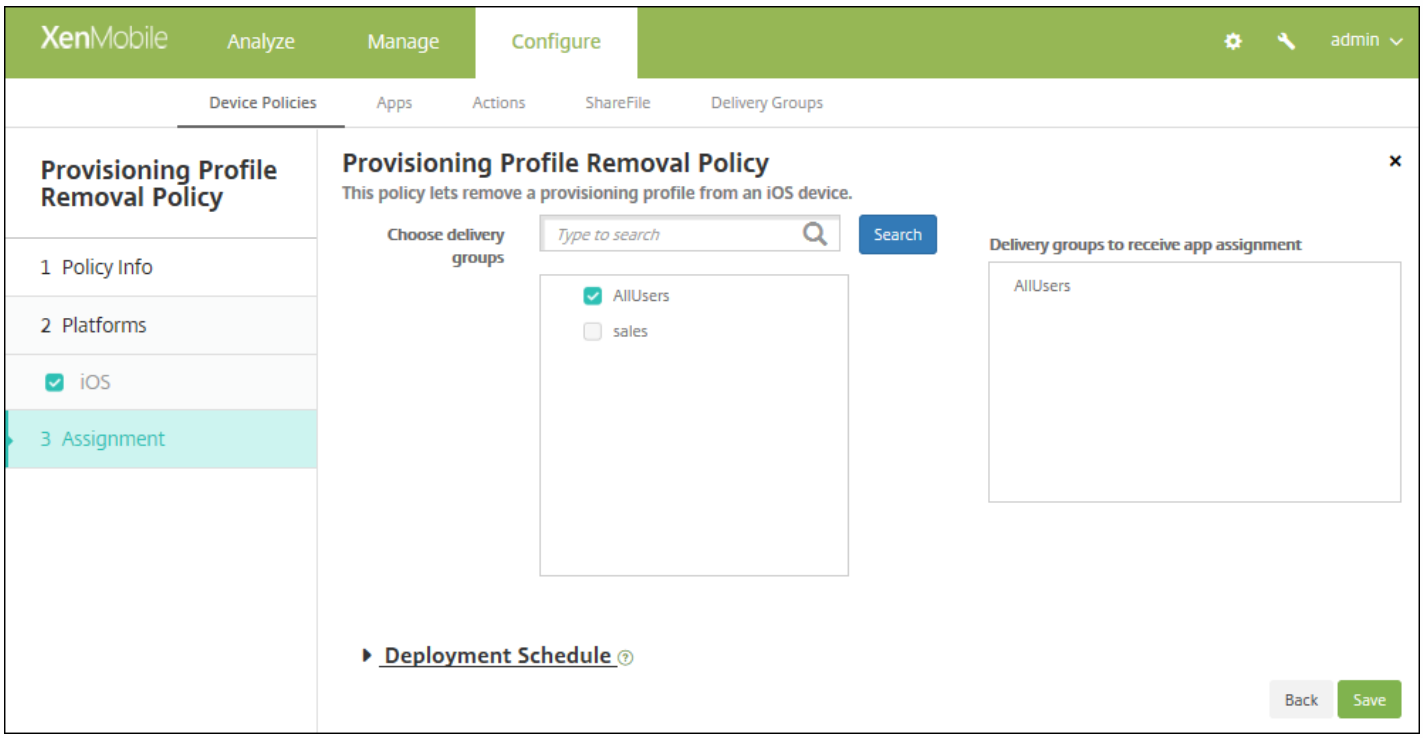


6. Configure estos parámetros:

- **iOS provisioning profile**. En la lista, haga clic en el perfil de aprovisionamiento que quiere quitar.
- **Comment**. Si lo prefiere, agregue un comentario.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Provisioning Profile Removal Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo sobre proxys

Feb 27, 2017

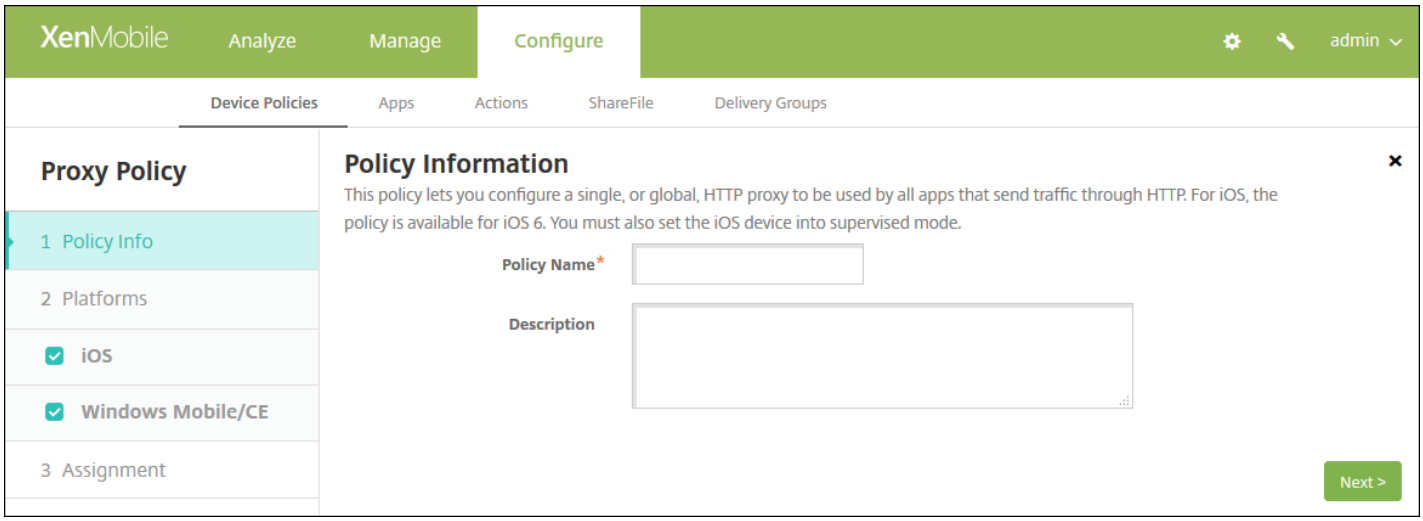
En XenMobile, puede agregar una directiva de dispositivos para especificar la configuración global de proxy HTTP en dispositivos con Windows Mobile/CE y iOS 6.0 o versiones posteriores. Puede implementar solamente una directiva global de proxy HTTP por dispositivo.

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.

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 **Proxy**. Aparecerá la página **Proxy Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

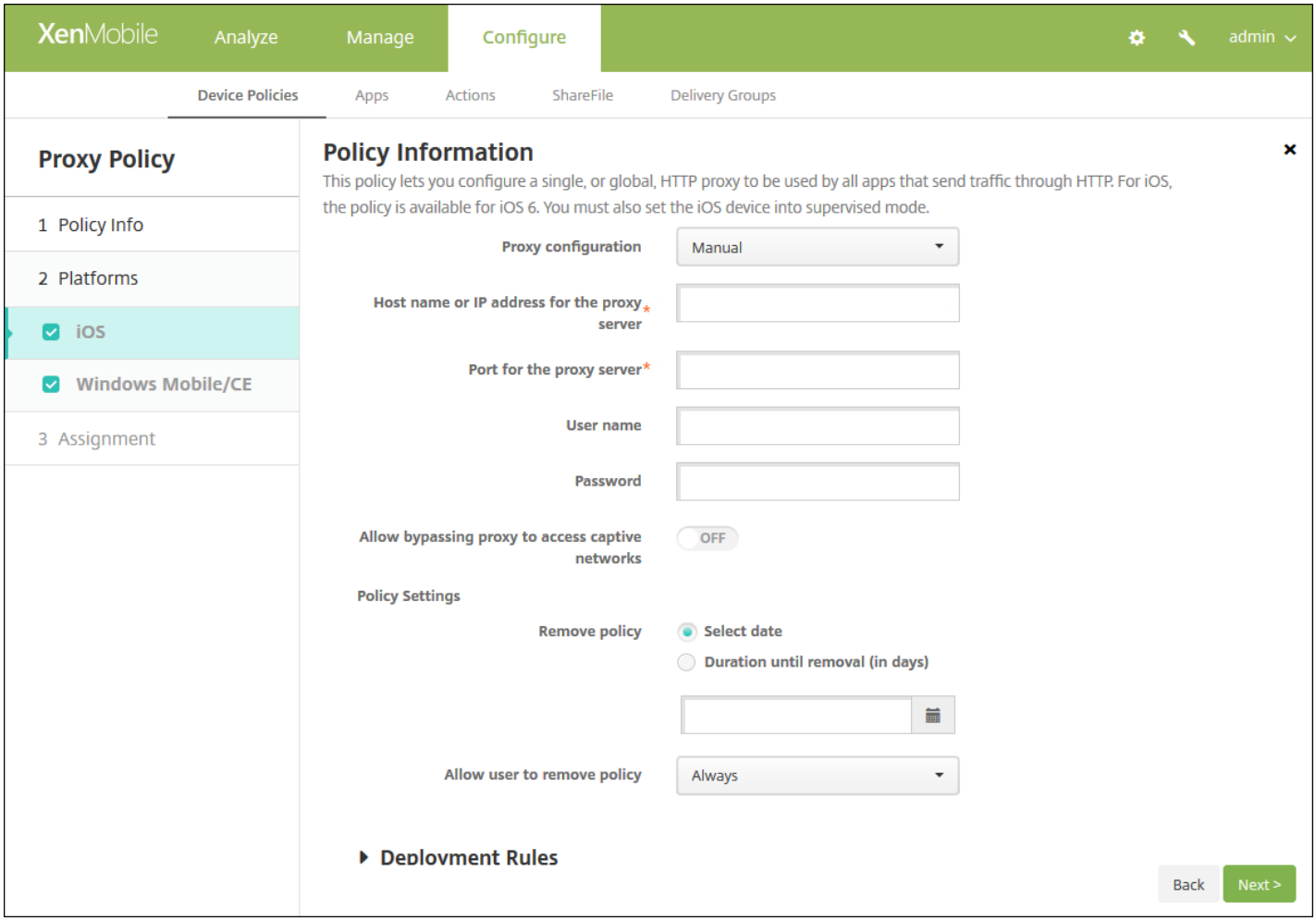
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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

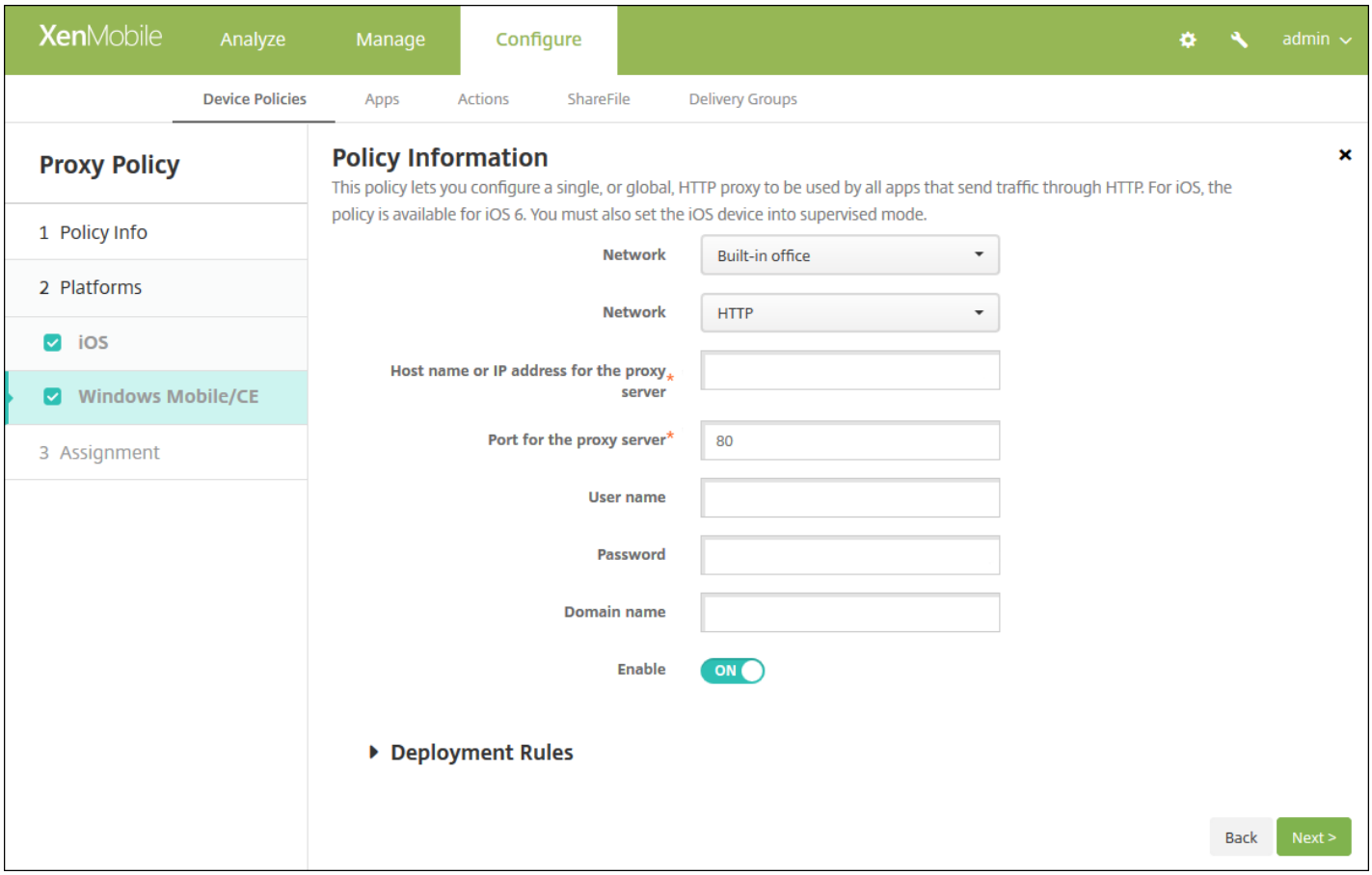


Configure estos parámetros:

- **Proxy configuration**. Haga clic en **Manual** o **Automatic** para determinar cómo se configurará el proxy en los dispositivos de los usuarios.
  - Si hace clic en **Manual**, configure los siguientes parámetros:
    - **Hostname or IP address for the proxy server**. Escriba el nombre de host o la dirección IP 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 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:
    - **Proxy PAC 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.
- **Allow bypassing proxy to access captive networks**. Seleccione si permitir que el dispositivo omita el servidor proxy y pueda acceder a redes cautivas. El valor predeterminado es **OFF**.
- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Windows Mobile/CE



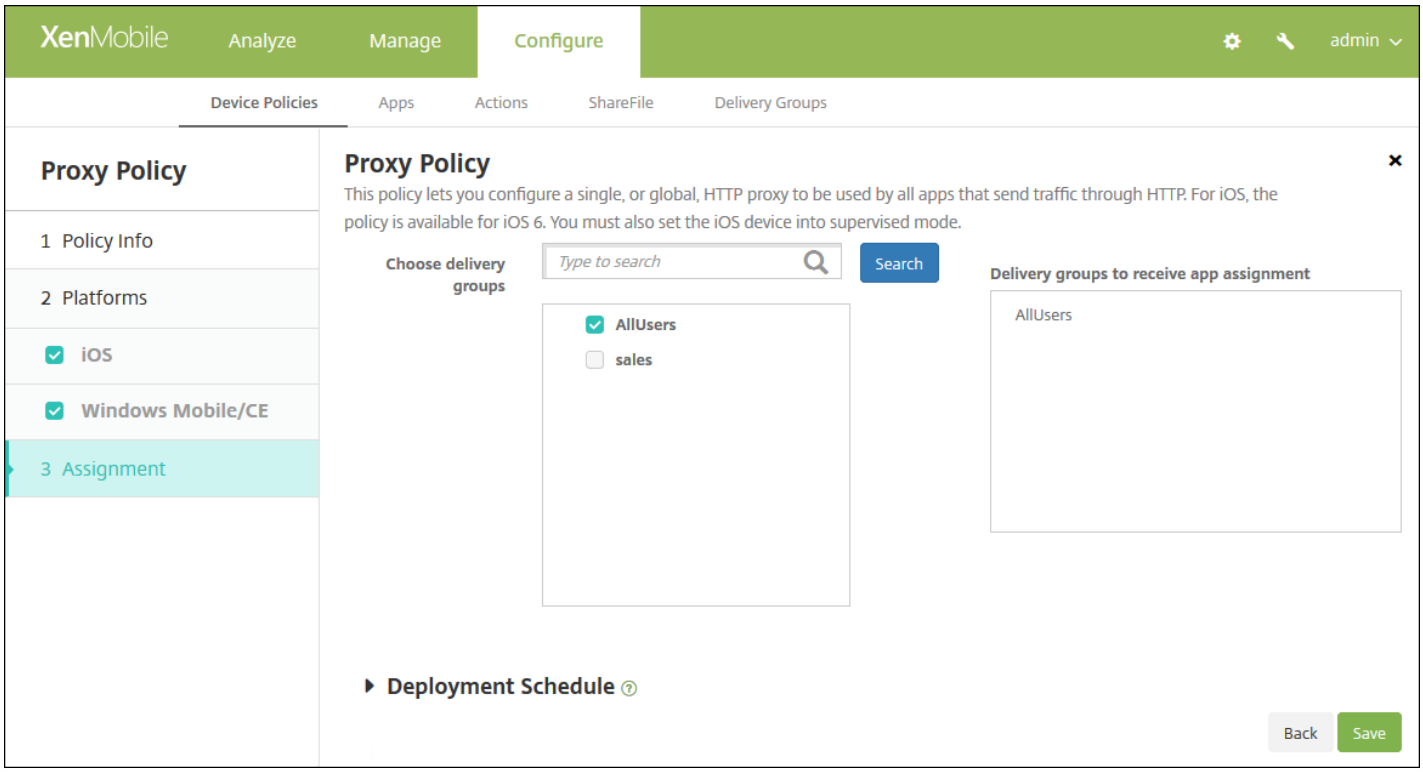
Configure estos parámetros:

- **Network**. En la lista, haga clic en el tipo de red a utilizar. El valor predeterminado es **Built-in office**. Las opciones posibles son:
  - Oficina definida por el usuario
  - Internet definido por el usuario
  - Oficina integrada
  - Internet integrado
- **Network**. En la lista, haga clic en el protocolo de conexión de red que se va a utilizar. El valor predeterminado es **HTTP**. Las opciones posibles son:
  - HTTP
  - WAP
  - SOCKS 4
  - SOCKS 5
- **Hostname or IP address for the proxy server**. Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
- **Port for the proxy server**. Escriba el número de puerto del servidor proxy. Este campo es obligatorio. El valor predeterminado es **80**.

- **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.
- **Domain name**. Si quiere, escriba un nombre de dominio.
- **Enable**. Seleccione si habilitar el proxy. El valor predeterminado es **ON**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Proxy Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 del Registro

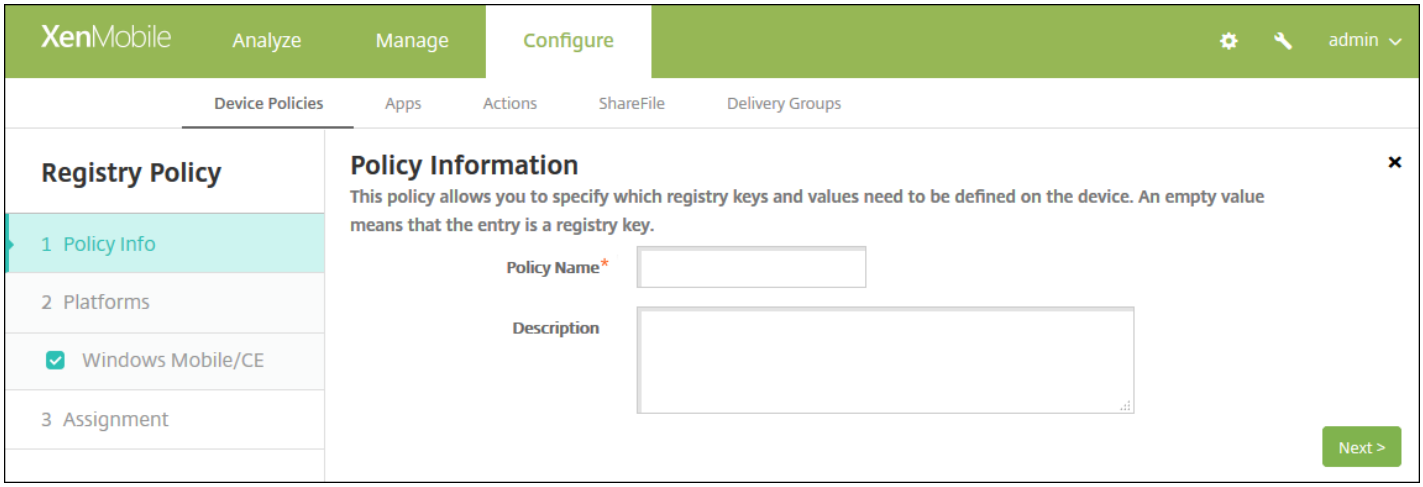
Feb 27, 2017

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.

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**.

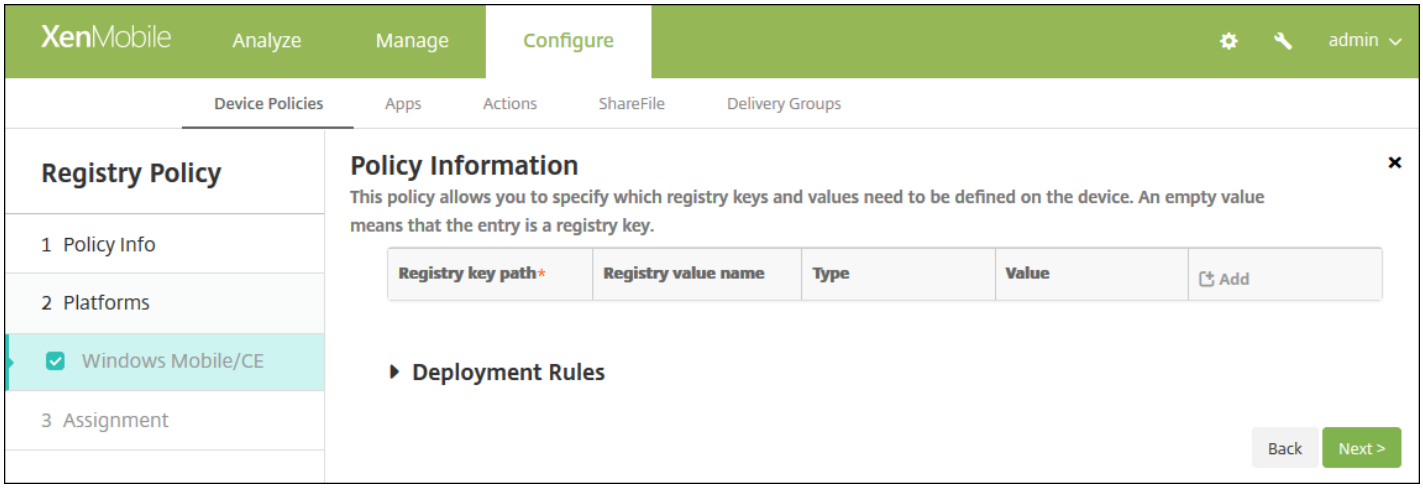
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Registry**. Aparecerá la página de información **Registry Policy**.



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 acerca de la plataforma **Windows Mobile/CE**.



6. Configure estos parámetros:

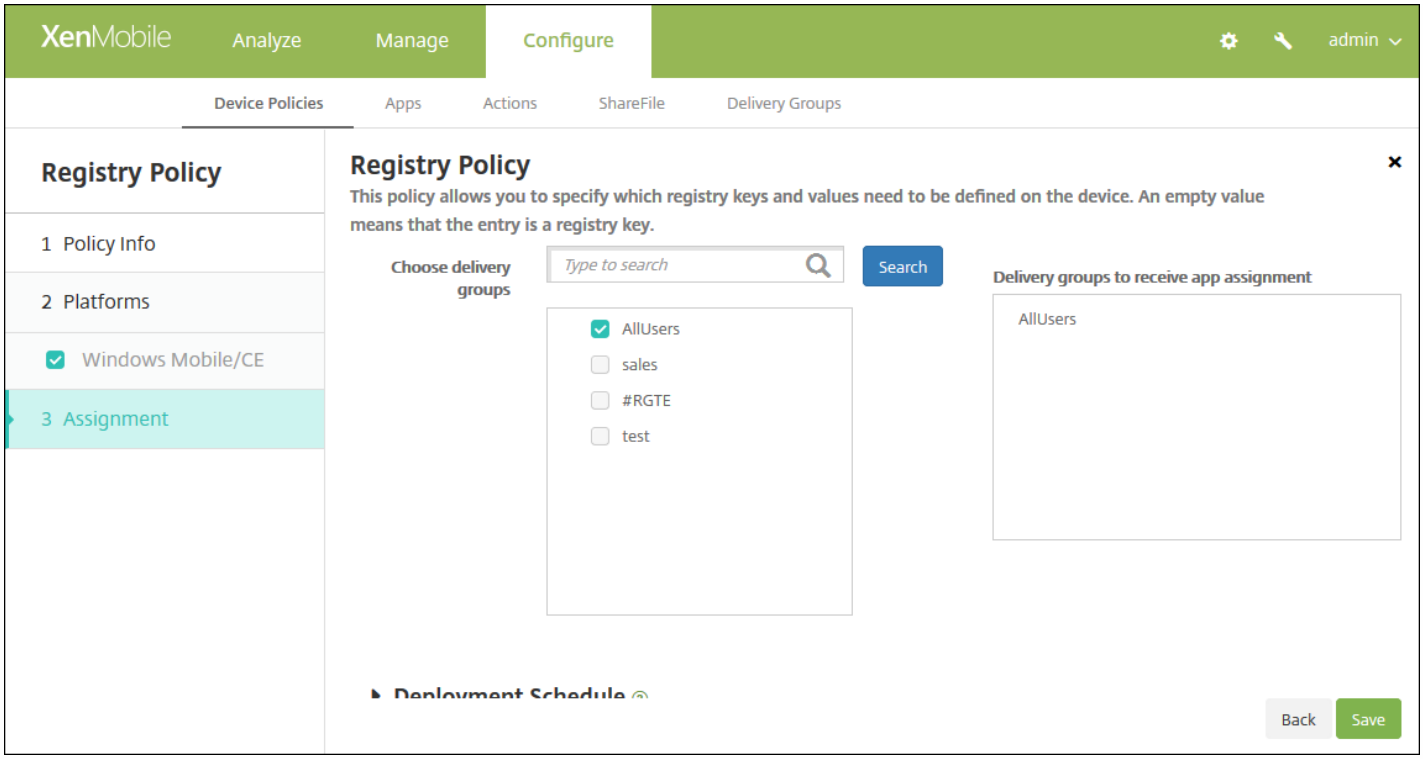
- Para cada clave de Registro o par clave/valor de Registro que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
- **Registry key path**. Escriba la ruta de acceso completa a la clave de Registro. Por ejemplo, escriba *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* para indicar la ruta a la clave de Windows desde la clave raíz HKEY_LOCAL_MACHINE.
- **Registry value name**. Escriba el nombre del valor de la clave de Registro. Por ejemplo, escriba *ProgramFilesDir* para agregar ese nombre de valor a la ruta de la clave de Registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion. Si deja este campo en blanco, significa que está agregando una clave de Registro, no una clave de Registro o un par clave de Registro/valor.
- **Type**. En la lista, haga clic en el tipo de datos del valor. El valor predeterminado es **DWORD**. Las opciones posibles son:
  - **DWORD**. Un número entero sin signo de 32 bits.
  - **String**. Cualquier cadena.
  - **Extended string**. Un valor de cadena que puede contener variables de entorno como, por ejemplo, %TEMP% o %USERPROFILE%.
  - **Binary**. Cualquier dato binario arbitrario.
- **Value**. Escriba el valor asociado al nombre del valor de Registro. Por ejemplo, para indicar el valor de ProgramFilesDir, escriba *C:\Program Files*.
- Haga clic en **Save** para guardar la información de la clave de Registro, o bien haga clic en **Cancel** para no guardarla.

  Nota: Para eliminar una clave de Registro, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

  Para modificar una clave de Registro existente, coloque el cursor sobre la línea que la 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 guardarlos, o bien en **Cancel** para descartarlos.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Registry Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 asistencia remota

Feb 27, 2017

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 y el usuario, configurar parámetros y establecer una sesión de chat entre el usuario y el departamento de asistencia.

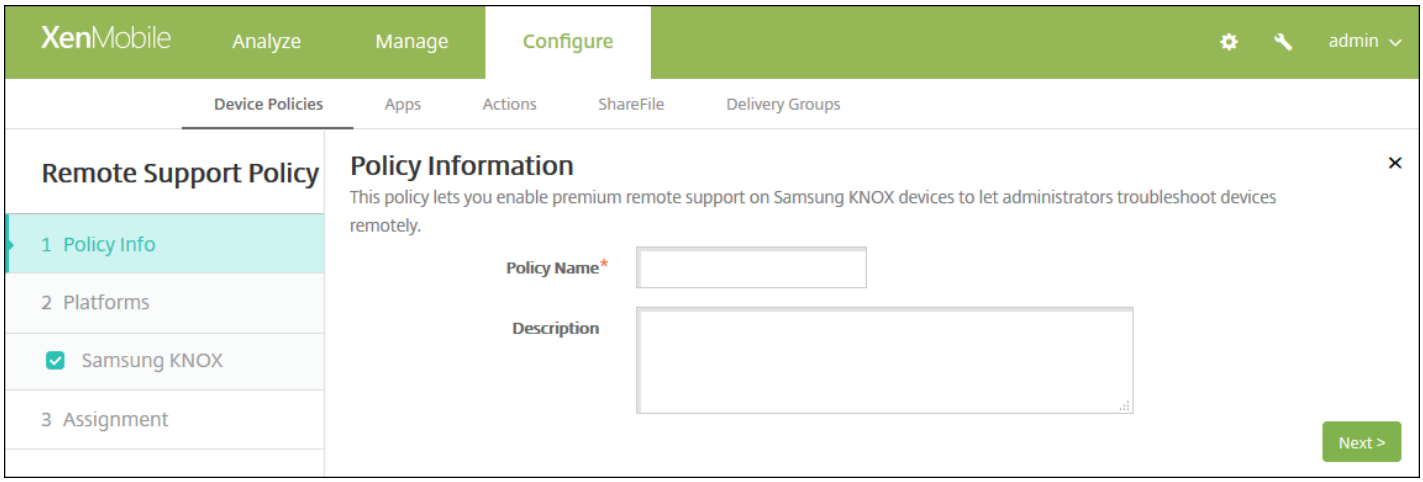
Nota: Para implementar esta directiva, debe realizar lo siguiente:

- Instalar la aplicación XenMobile Remote Support en su entorno.
- Configurar un túnel de aplicaciones para asistencia remota. Para obtener más información, consulte Directivas de túneles de aplicaciones.
- Configurar una directiva de asistencia remota para dispositivos Samsung KNOX como se describe en este apartado.
- Implementar la directiva de asistencia remota por túnel de aplicaciones y la directiva de asistencia remota de Samsung KNOX en los dispositivos de los usuarios.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

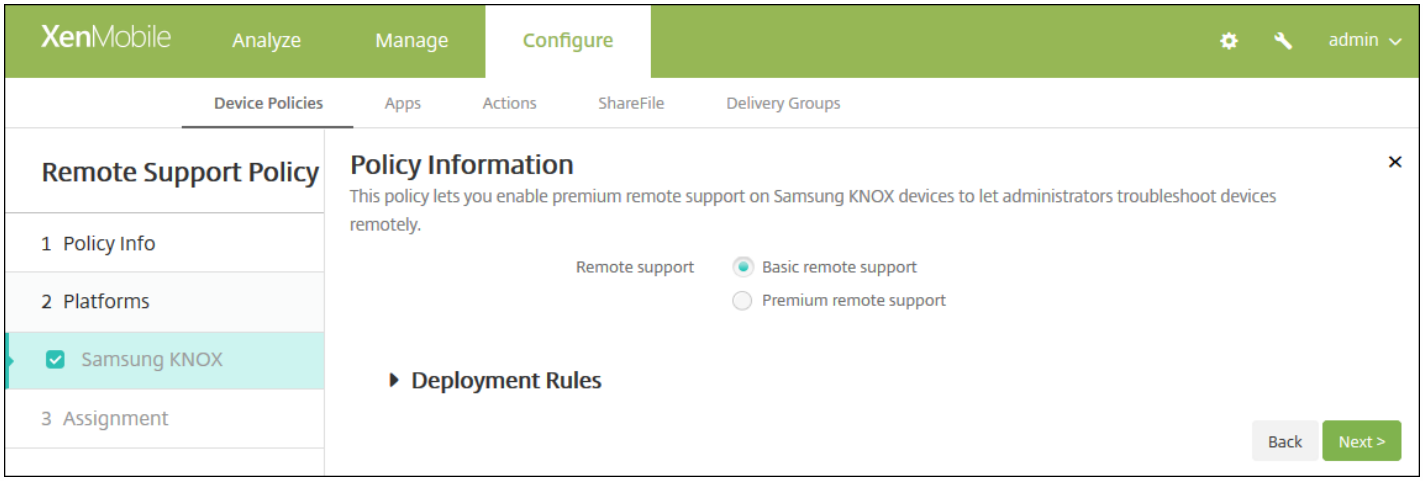
3. Expanda **More** y, en **Network access**, haga clic en **Remote Support**. Aparecerá la página **Remote Support Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **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 acerca de la plataforma **Samsung KNOX**.

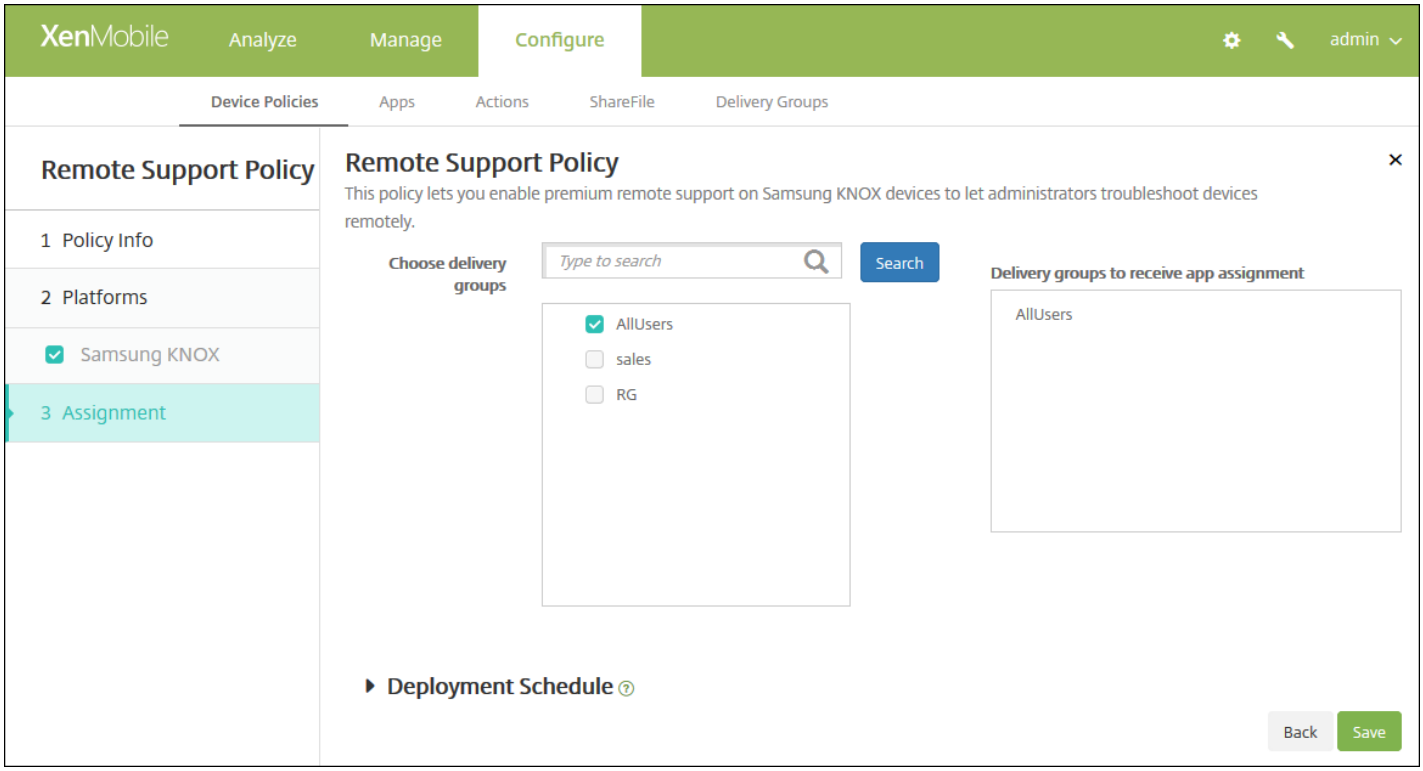


6. Configure este parámetro:

- **Remote support**. Seleccione **Basic remote support** o **Premium remote support**. El valor predeterminado es **Basic remote support**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Remote Support Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 restricciones

Feb 27, 2017

La directiva de restricciones permite o prohíbe a los usuarios utilizar funciones determinadas en sus dispositivos, como la cámara. 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*.

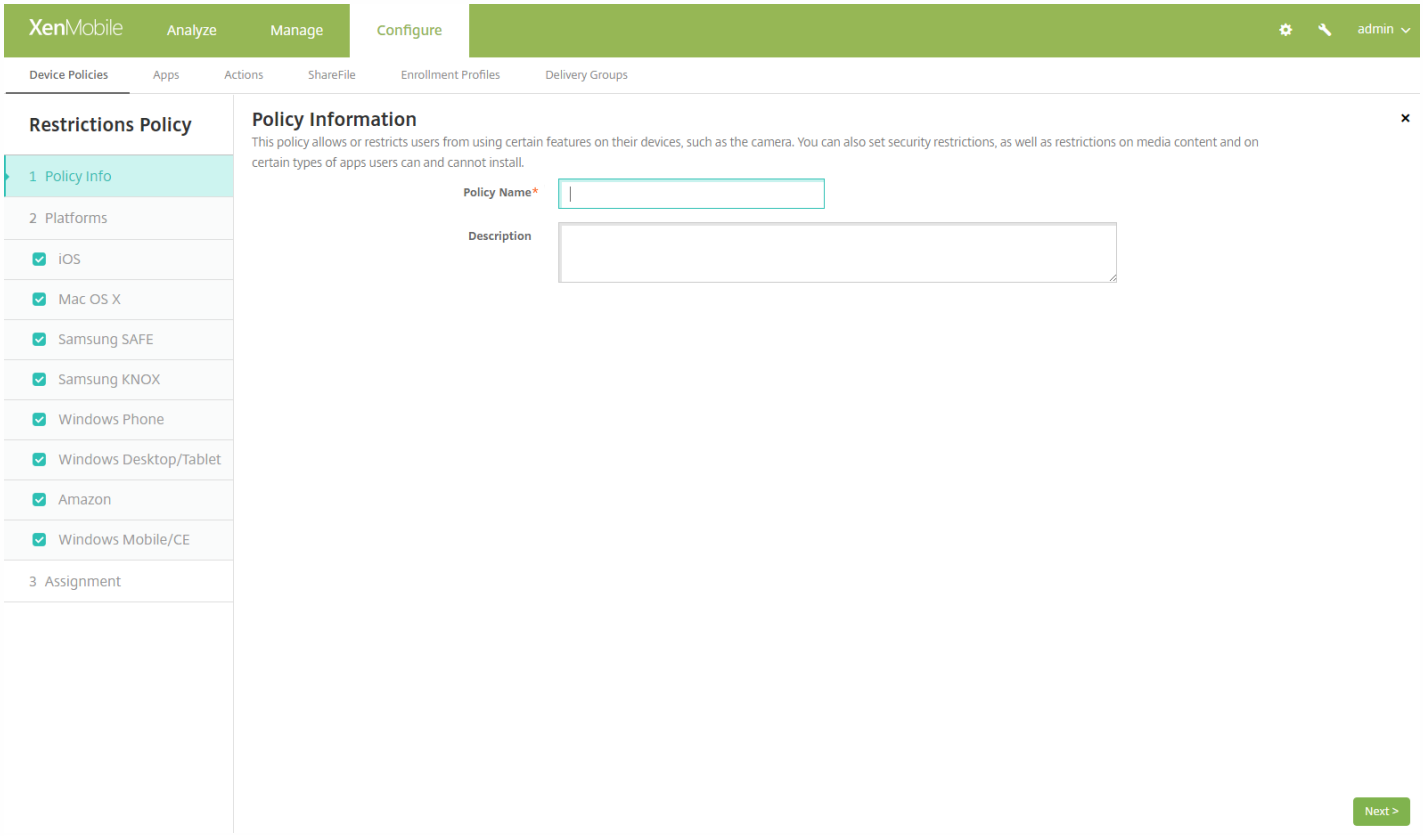
Sugerencia: Si selecciona **ON** para una opción, significa que el usuario puede realizar la operación o usar la función. Por ejemplo:

- **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.

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 **Restrictions**. Aparecerá la página de información **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.

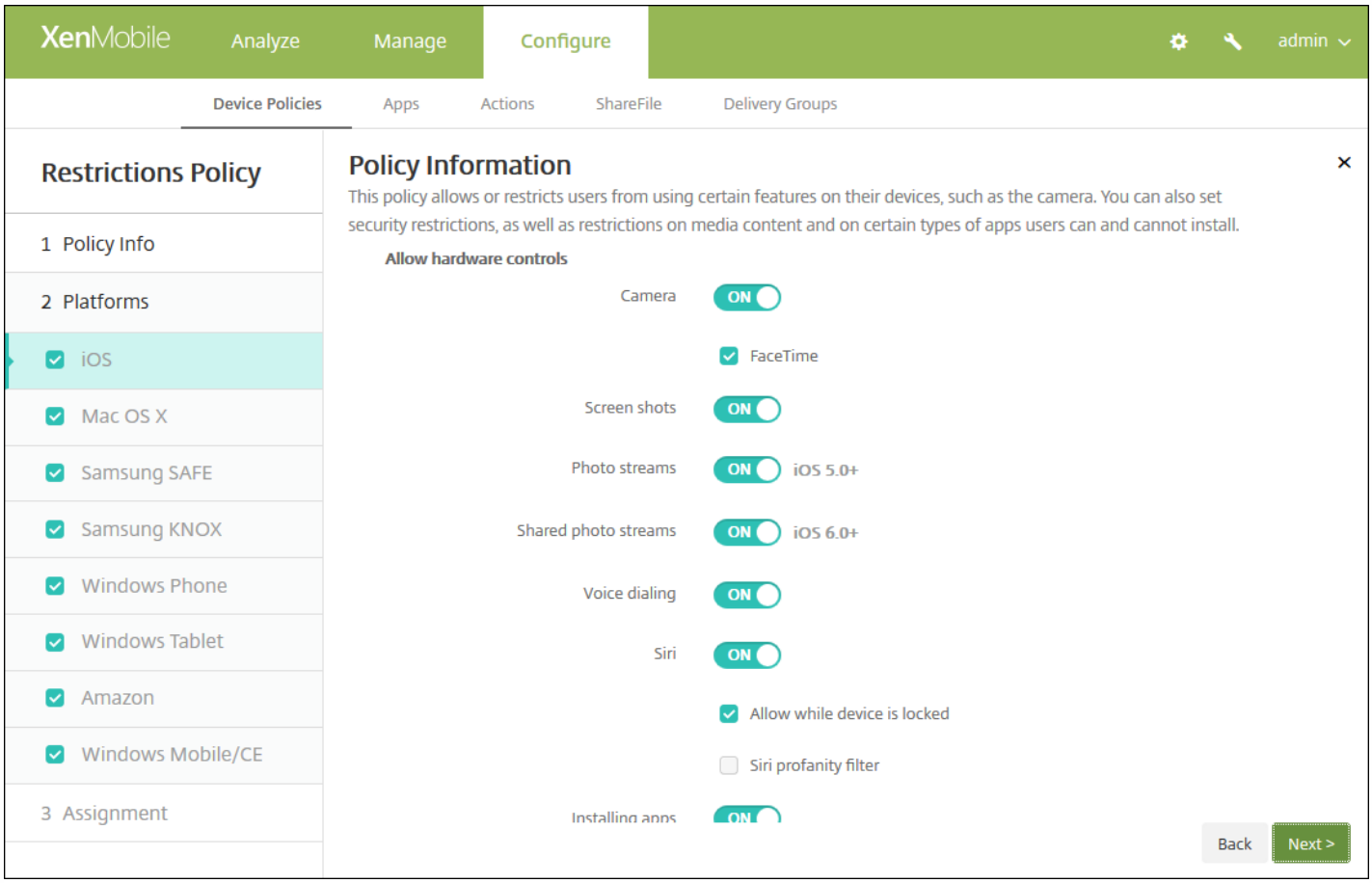
4. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

5. En **Platforms**, seleccione la plataforma o las plataformas que quiere agregar. Puede cambiar la información de la directiva para cada plataforma seleccionada. Haga clic para restringir las funciones de los siguientes apartados, con lo que cambiará la opción de configuración a **OFF**. A menos que se indique lo contrario, el valor predeterminado es habilitar la función.

Si ha seleccionado:
iOS, configure estos parámetros
Mac OS X, configure estos parámetros
Samsung SAFE, configure estos parámetros
Samsung KNOX, configure estos parámetros
Windows Phone, configure estos parámetros
Windows Tablet, configure estos parámetros
Amazon, configure estos parámetros
Windows Mobile/CE, configure estos parámetros

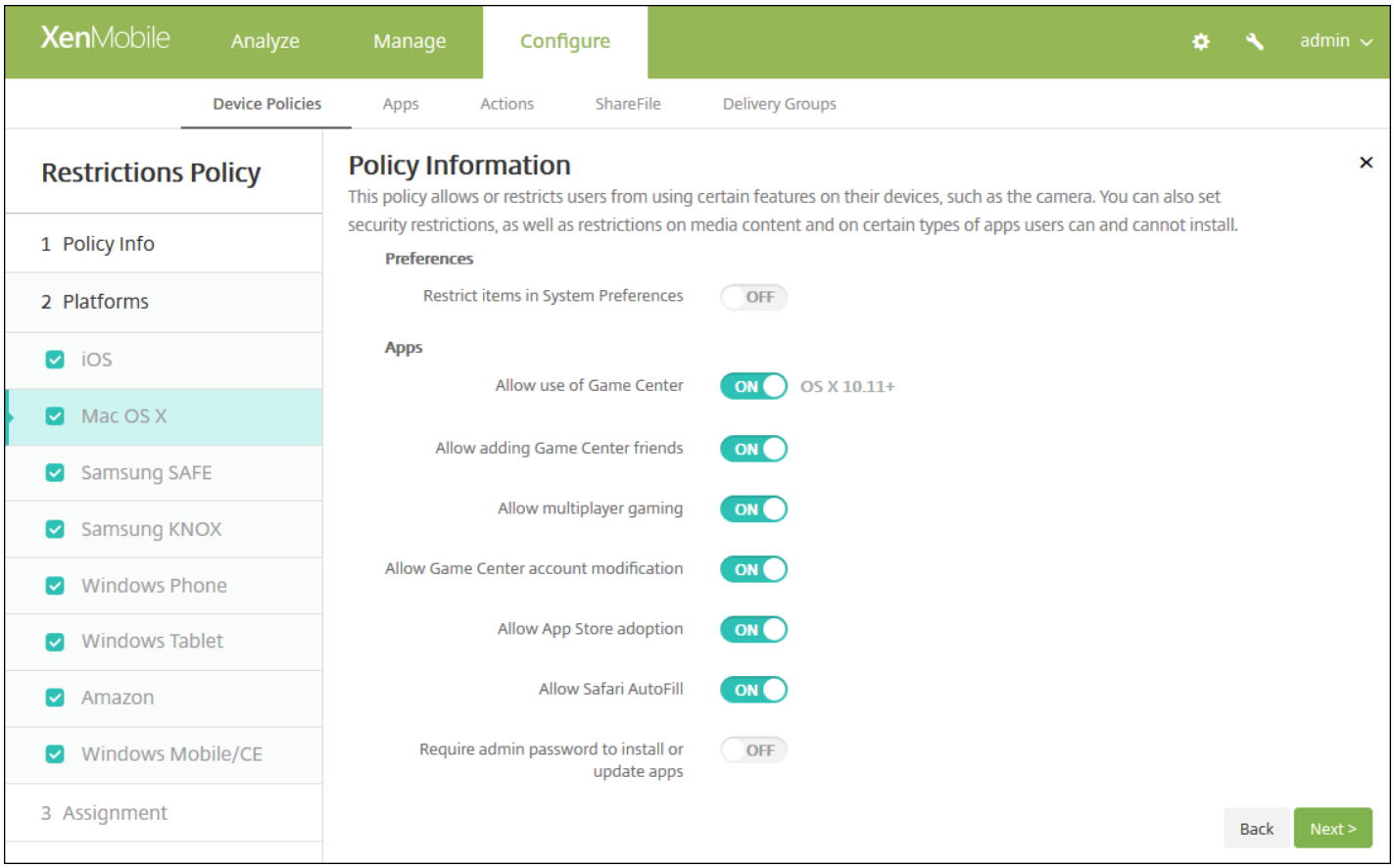
Cuando termine de configurar las restricciones para una plataforma, consulte el paso 7 más adelante en este artículo, para ver cómo definir las reglas de implementación de esa plataforma.

Si ha seleccionado iOS, configure los siguientes parámetros:



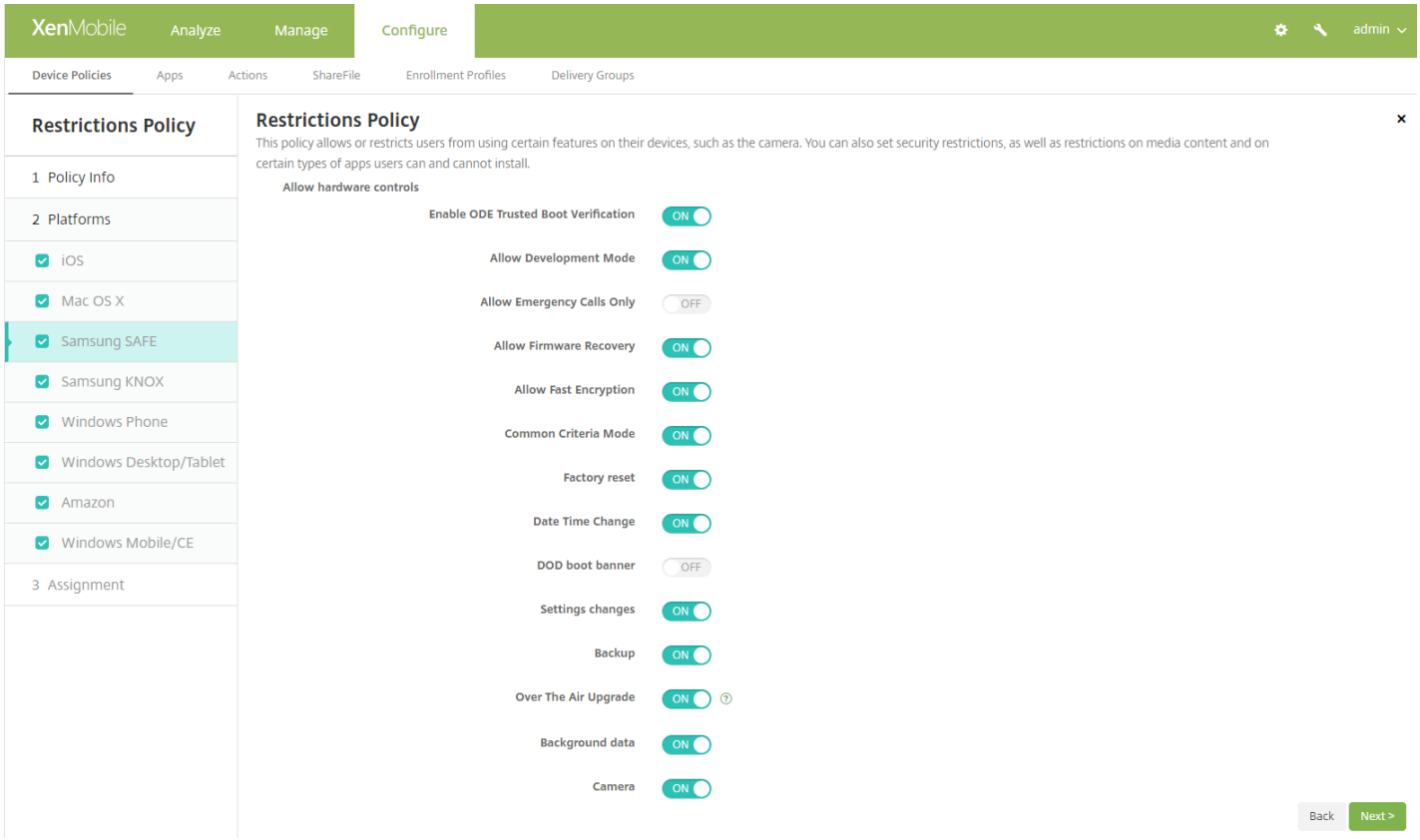
Configuración de iOS

Configuración de los parámetros de Mac OS X



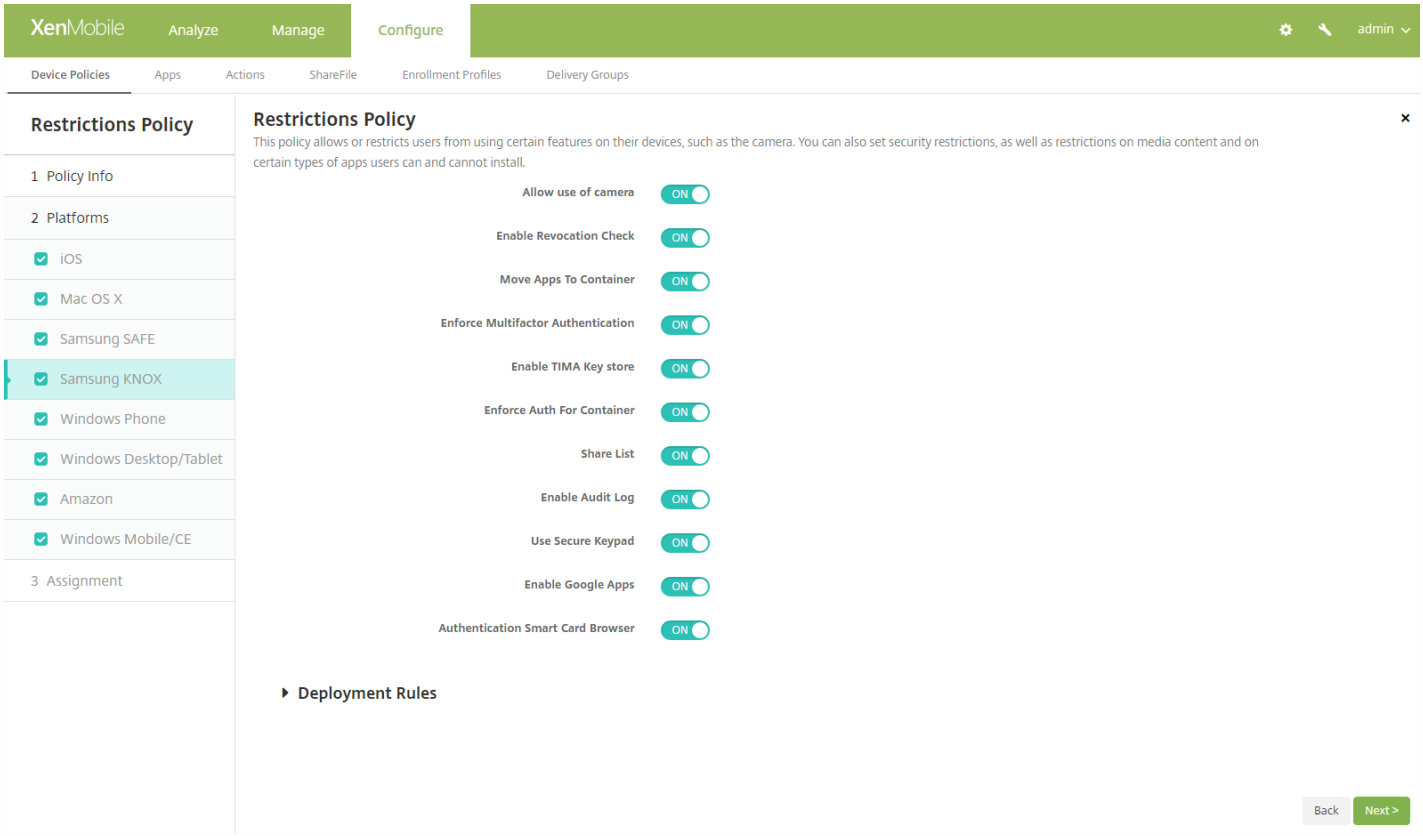
Configuración de Mac OS X

Configuración de los parámetros de Samsung SAFE



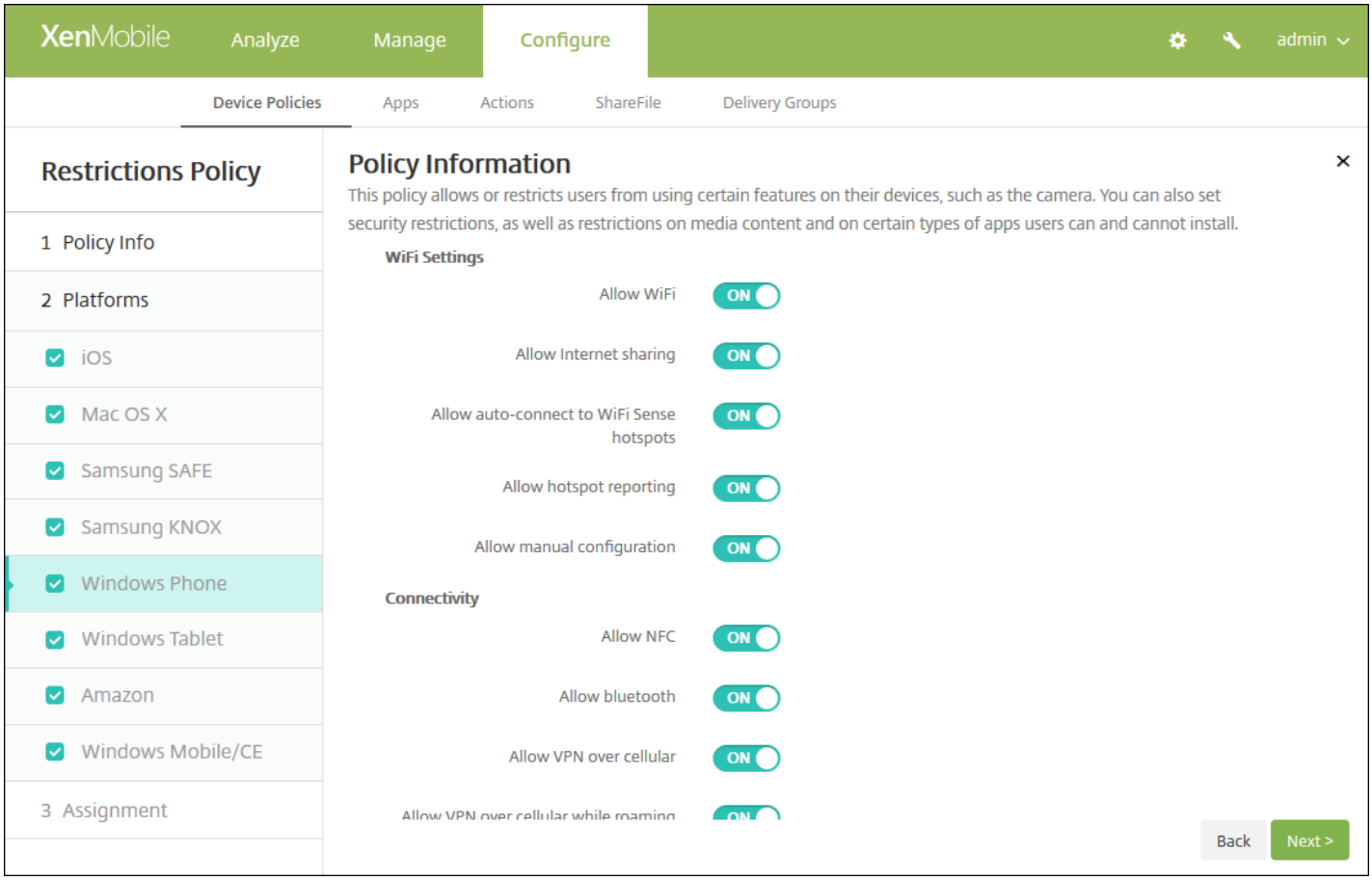
Configuración de Samsung SAFE

Configuración de los parámetros de Samsung KNOX



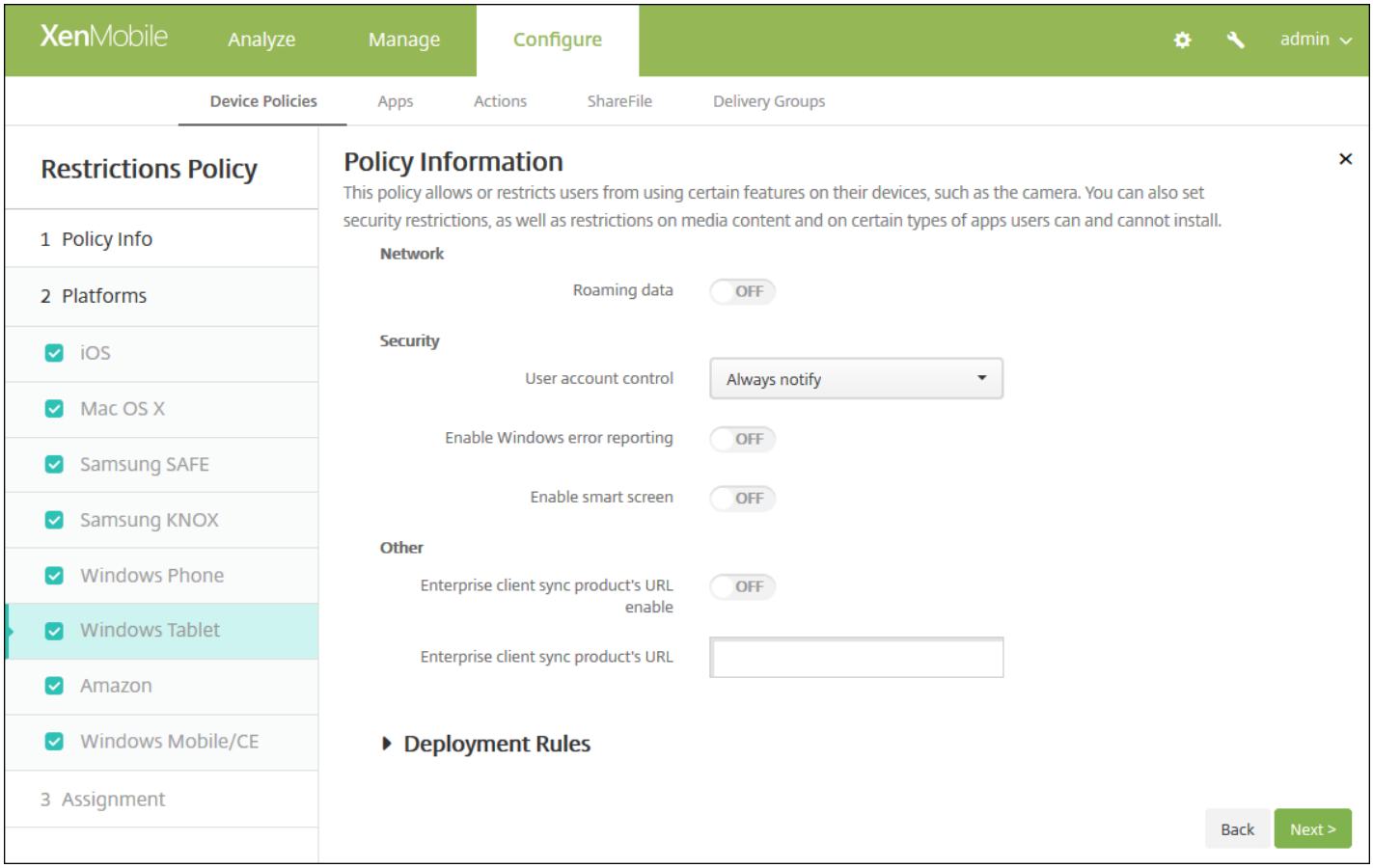
Configuración de Samsung KNOX

Configuración de los parámetros de Windows Phone



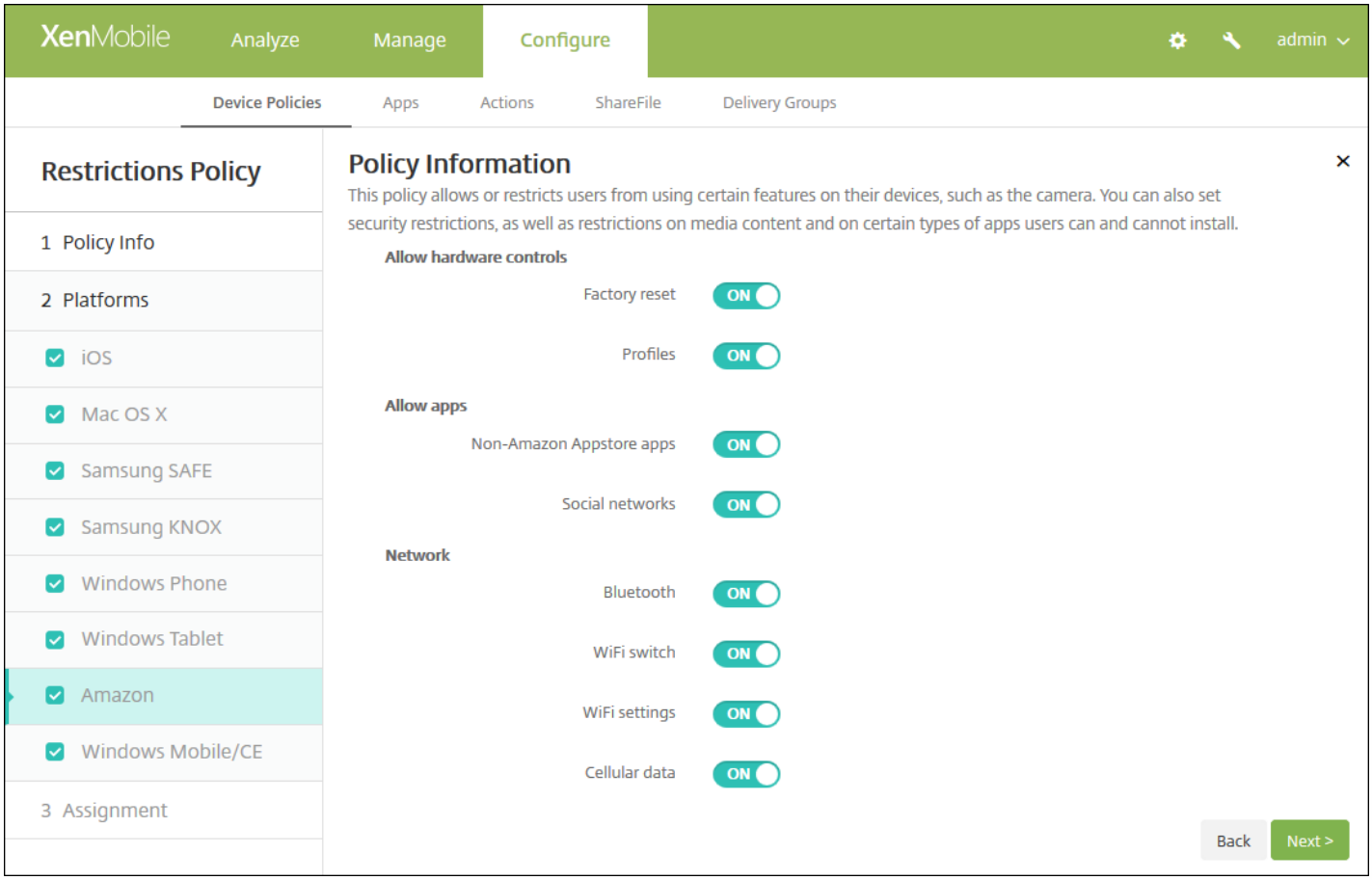
Configuración de Windows Phone

Configuración de los parámetros de escritorios o tabletas Windows



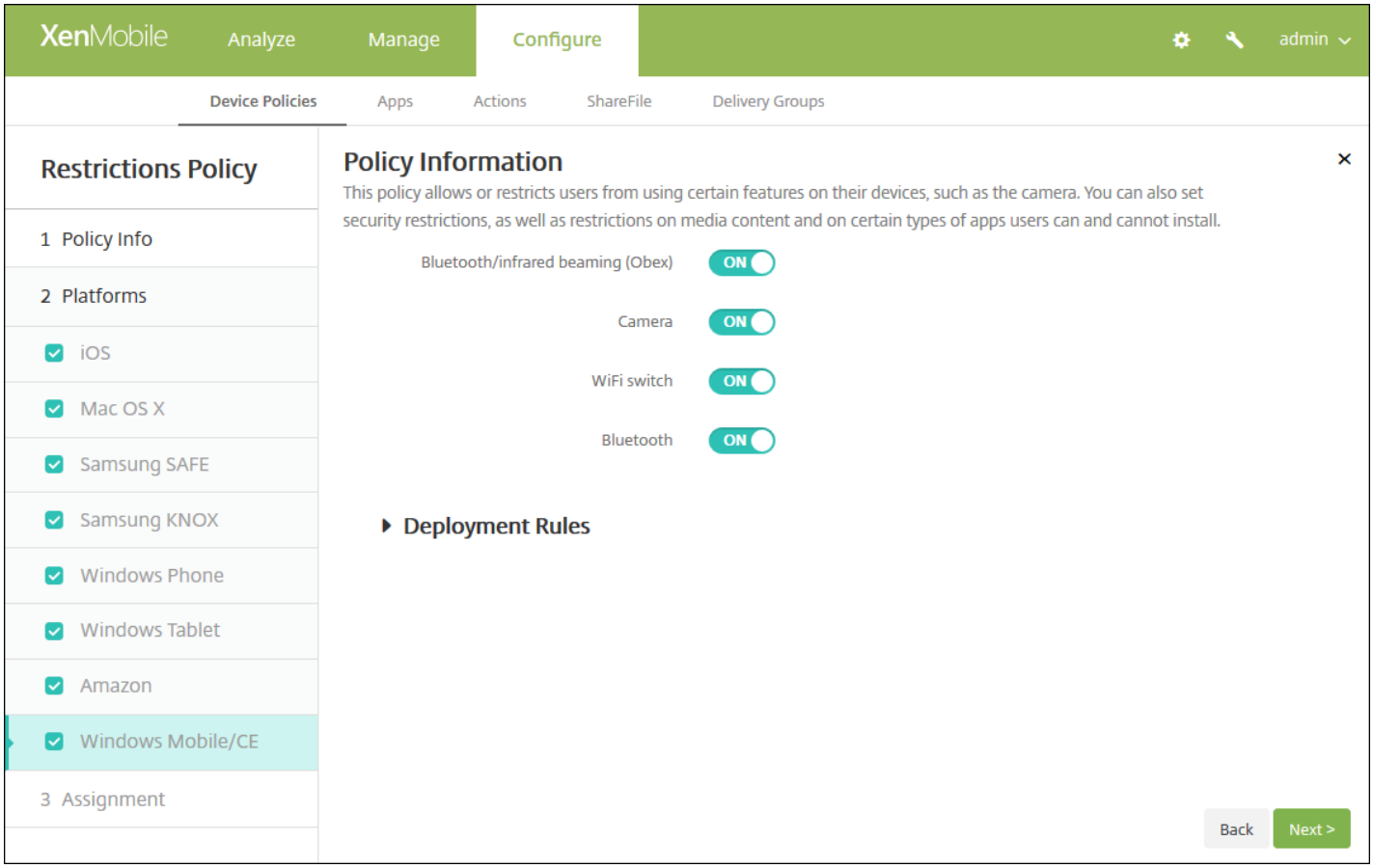
Configuración de escritorios y tabletas Windows

Configuración de los parámetros de Amazon



Configuración de Amazon

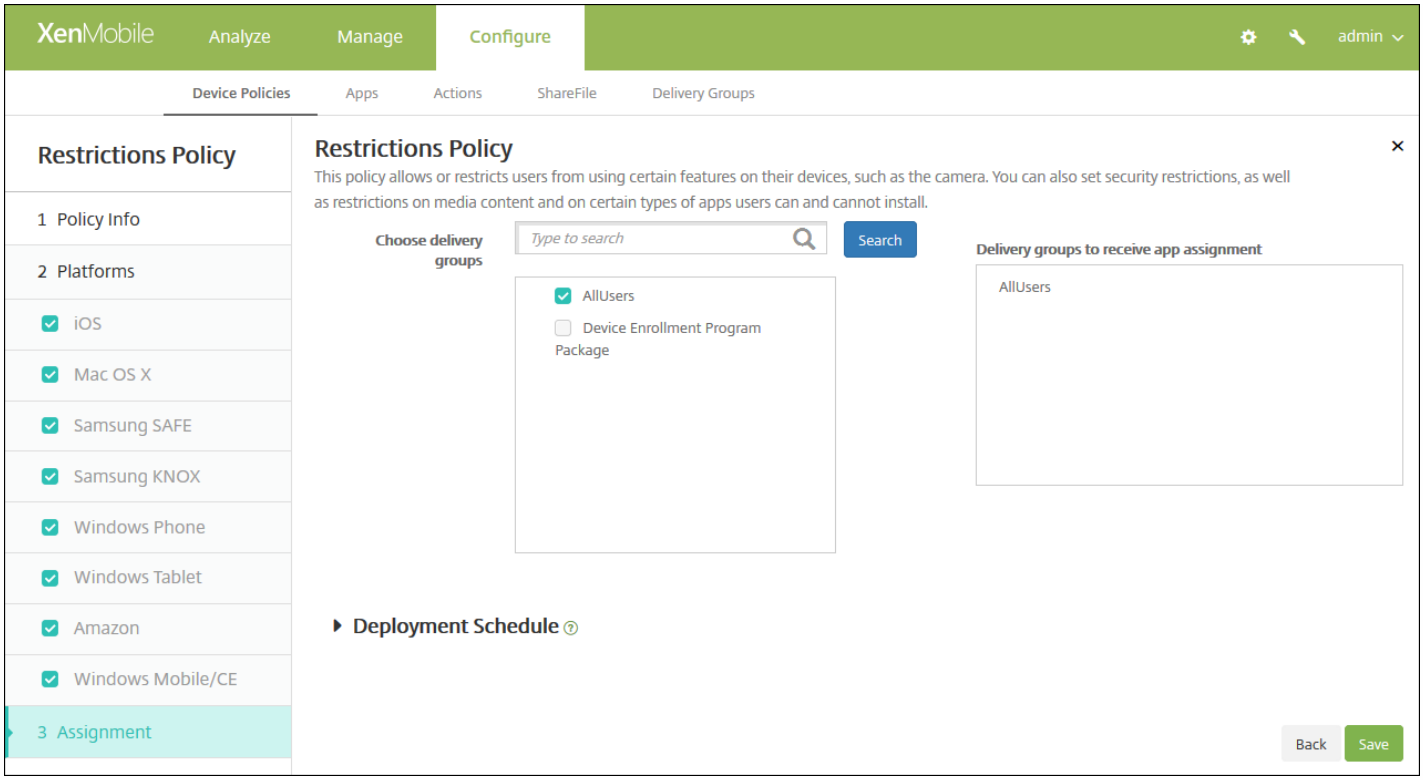
Configuración de los parámetros de Windows Mobile/CE



Configuración de Windows Mobile/CE

7. Configure las reglas de implementación.

8. Haga clic en **Next** y aparecerá la página de asignación de **Restrictions Policy**.



9 Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

10. Haga clic en **Save** para guardar la directiva.

Directiva de dispositivo para roaming

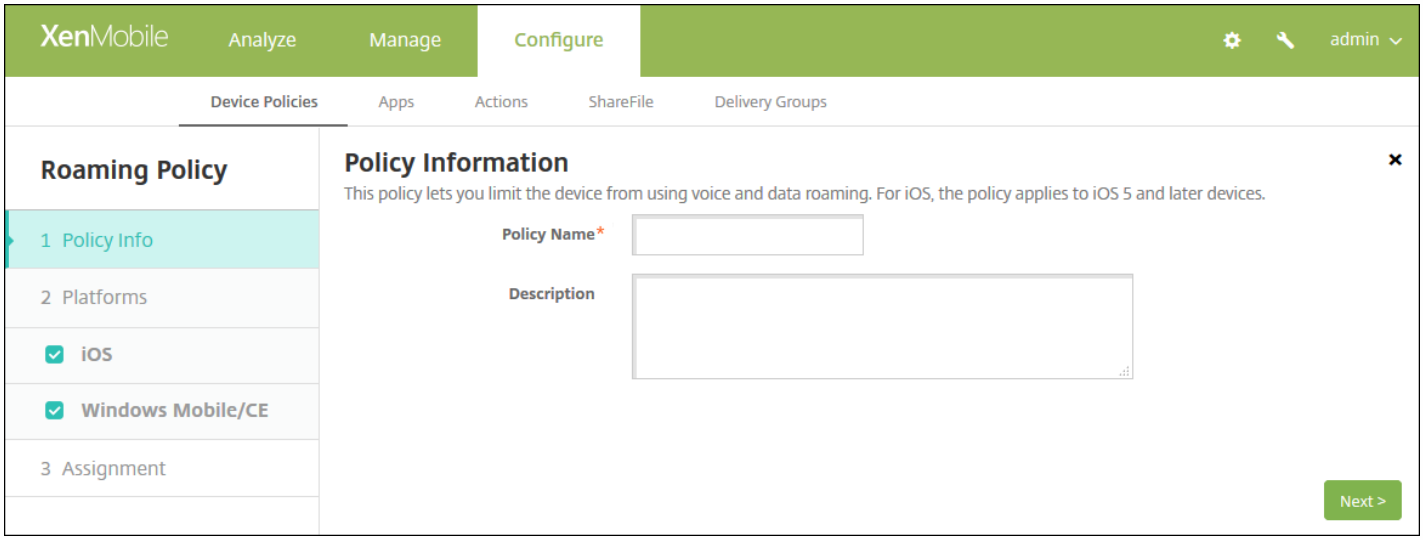
Feb 27, 2017

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.

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 **Roaming**. Aparecerá la página de información **Roaming Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

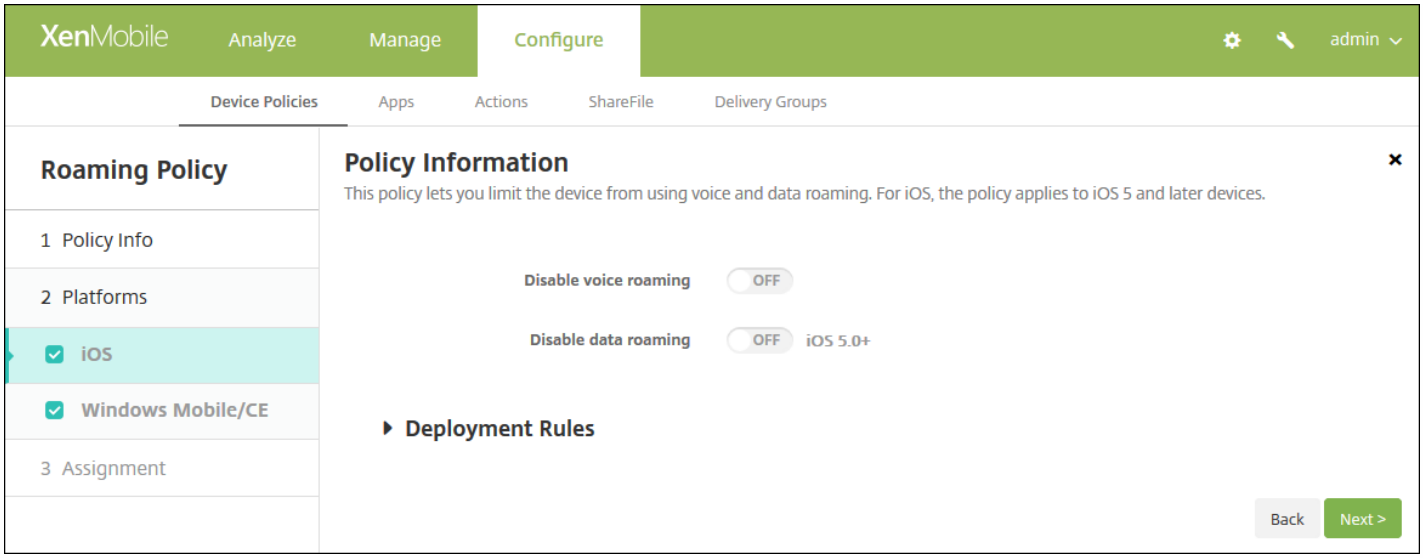
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

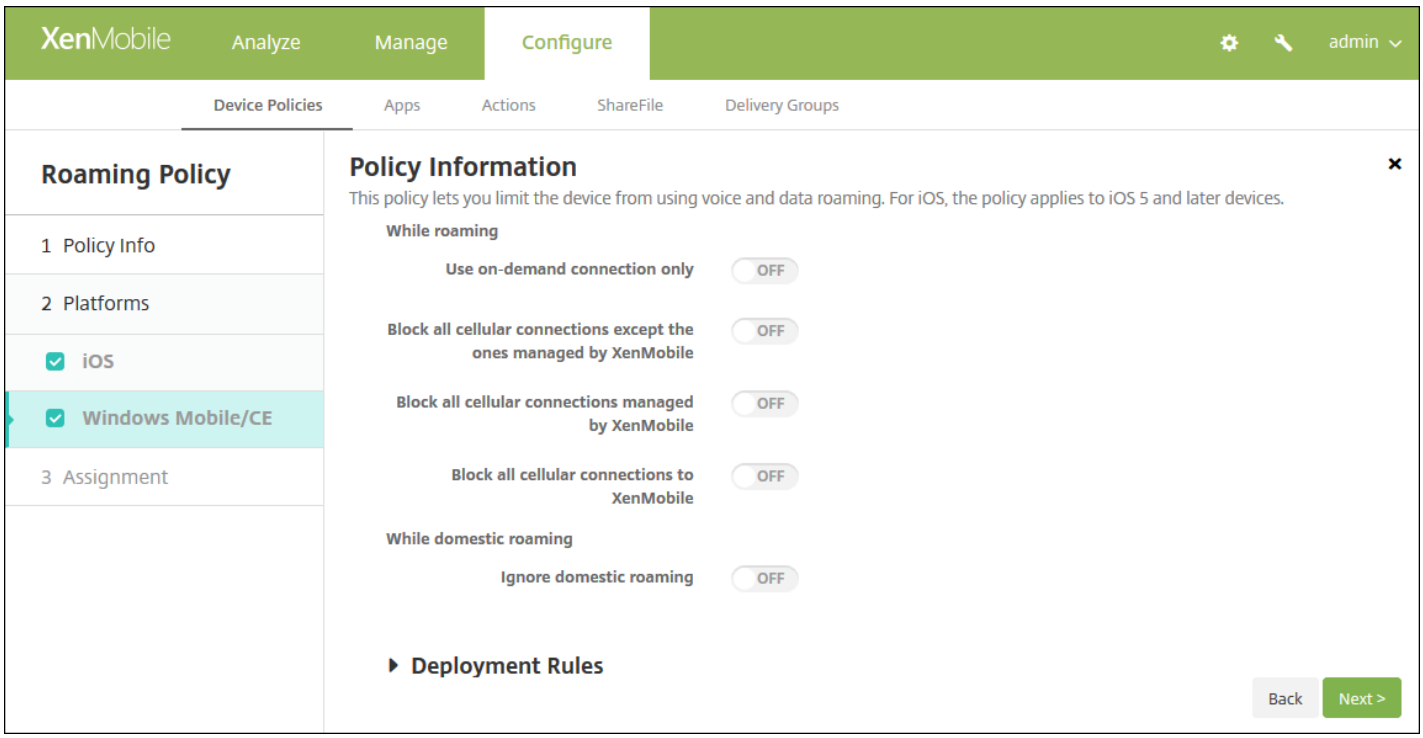
Configuración de los parámetros de iOS



Configure estos parámetros:

- **Disable voice roaming**. Seleccione si inhabilitar la movilidad de voz. Si se inhabilita esta opción, la movilidad de datos se inhabilita automáticamente. El valor predeterminado es **OFF**, lo que permite la movilidad de voz.
- **Disable data roaming**. Seleccione si inhabilitar la movilidad de datos. Esta opción solo está disponible cuando la movilidad de voz está habilitada. El valor predeterminado es **OFF**, lo que permite la movilidad de datos.

Configuración de los parámetros de Windows Mobile/CE



Configure estos parámetros:

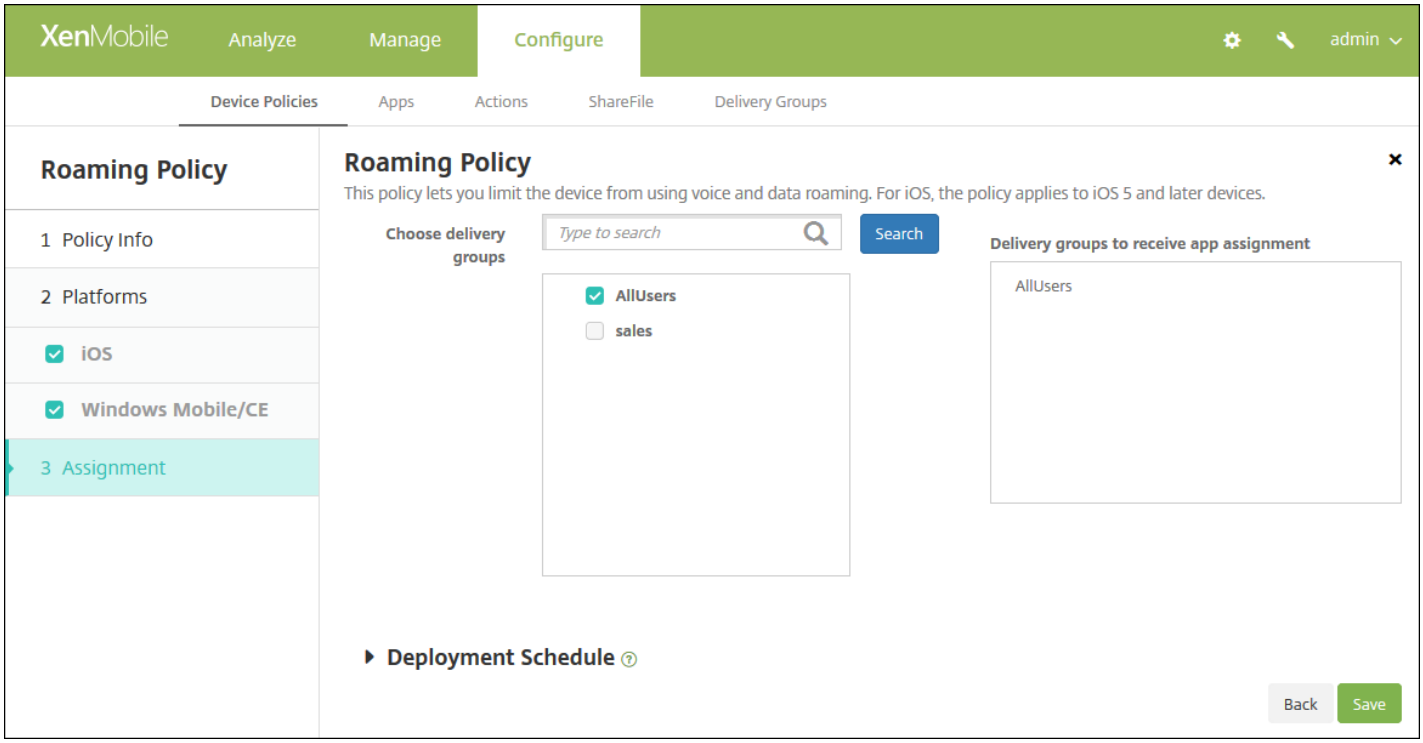
- **Mientras el dispositivo está en roaming**

- **Use on-demand connection only**. El dispositivo solo se conecta a XenMobile si el usuario activa manualmente la conexión en su dispositivo, o bien si una aplicación móvil solicita una conexión forzosa (como una solicitud push de correo si el servidor Exchange se ha configurado adecuadamente). Tenga en cuenta que esta opción inhabilita temporalmente la directiva predeterminada de programación de conexiones del dispositivo.
- **Block all cellular connections except the ones managed by XenMobile**. Excepto el tráfico de datos declarado oficialmente en un túnel de aplicaciones XenMobile u otras tareas de administración de dispositivos que lleve a cabo XenMobile, el dispositivo no enviará ni recibirá ningún dato. Por ejemplo, esta opción inhabilita todas las conexiones a Internet que se llevan a cabo mediante el explorador Web del dispositivo.
- **Block all cellular connections managed by XenMobile**. Todos los datos de aplicación que transiten a través de un túnel de XenMobile se bloquearán (incluida la aplicación Remote Support de XenMobile). Sin embargo, no se bloquea el tráfico de datos relacionado puramente con la administración de dispositivos.
- **Block all cellular connections to XenMobile**. En este caso, hasta que el dispositivo se vuelva a conectar mediante USB, WiFi o su operador predeterminado de telefonía móvil, no hay tráfico que transite entre el dispositivo y XenMobile.

- **Mientras el dispositivo está en roaming en el ámbito nacional**
  - **Ignore domestic roaming**. No se bloquean datos mientras los usuarios se muevan en el ámbito nacional.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Roaming Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo sobre claves de licencia de MDM de Samsung

Feb 27, 2017

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.

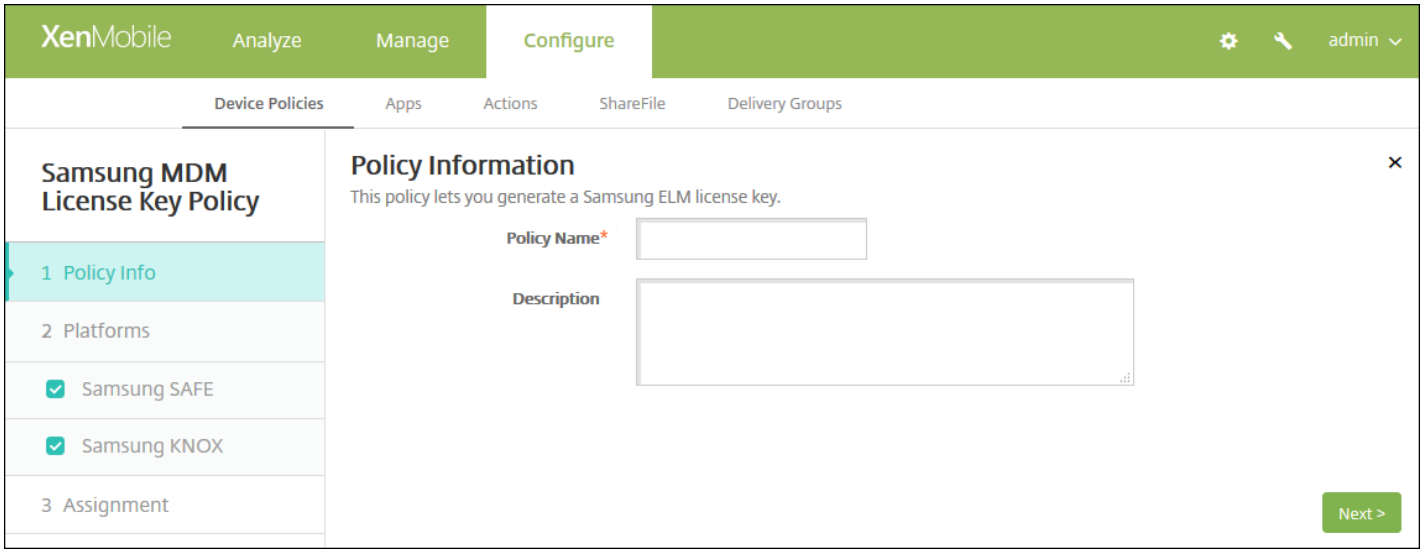
Debe habilitar las API de la solución SAFE por medio de la implementación de la clave integrada de Samsung Enterprise License Management (ELM) a un dispositivo antes de implementar directivas y restricciones de la solución SAFE. Para habilitar la API de Samsung KNOX, además de implementar la clave ELM de Samsung, también deberá adquirir una licencia de Samsung KNOX Workspace 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 Secure Hub 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 en las propiedades del dispositivo. Si la clave de Samsung ELM está implementada, el parámetro **Samsung MDM API available** tiene el valor **True**.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el diálogo **Add a New Policy**.

3. Haga clic en **More** y, a continuación, en **Security**, haga clic en **Samsung MDM License Key**. Aparecerá la página de información **Samsung MDM License Key Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

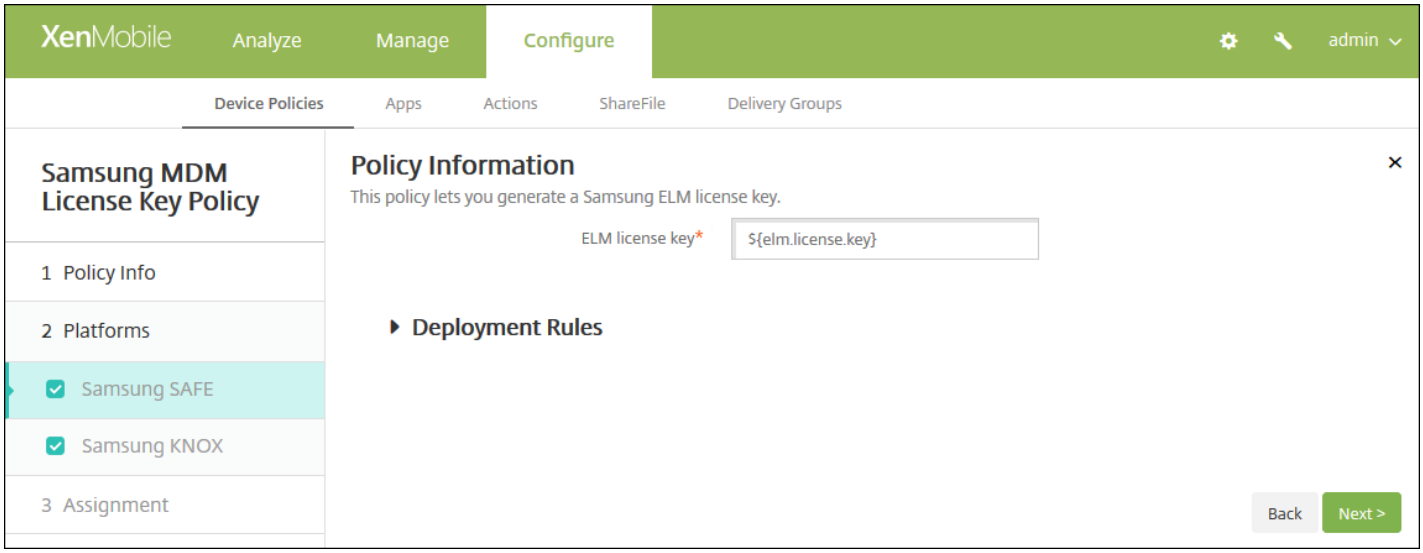
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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.

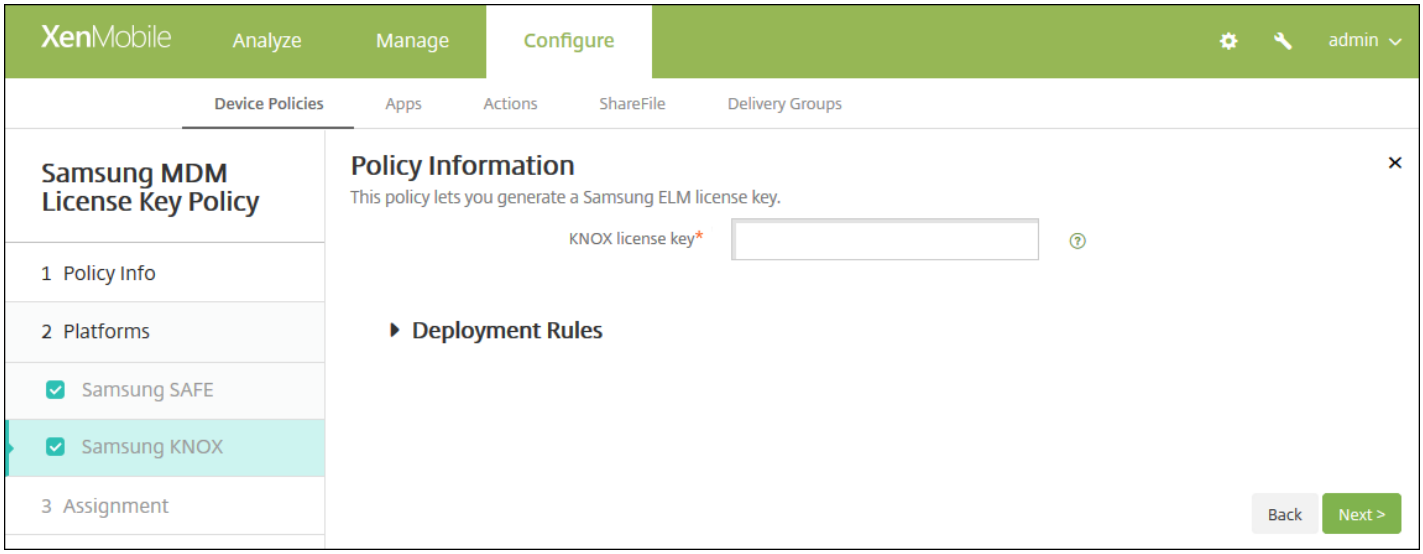
Configuración de los parámetros de Samsung SAFE



Configure este parámetro:

- **ELM License key**. Este campo ya debería contener la macro que genera la clave de licencia ELM. Si el campo está en blanco, escriba la macro ${elm.license.key}.

Configuración de los parámetros de Samsung KNOX

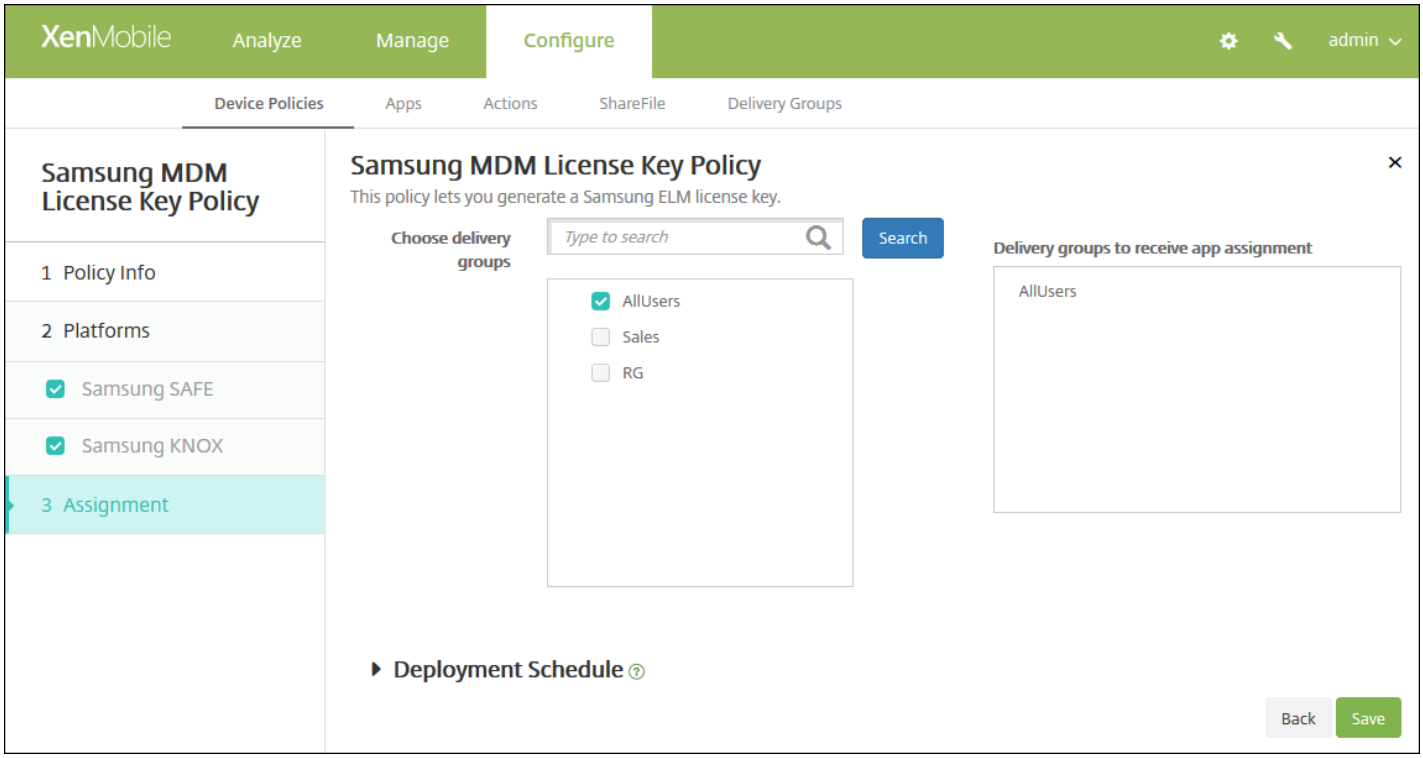


Configure este parámetro:

- **KNOX License key**. Escriba la clave de licencia KNOX compuesta de 25 dígitos que ha obtenido de Samsung.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Samsung MDM License Key Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para firewalls de Samsung SAFE

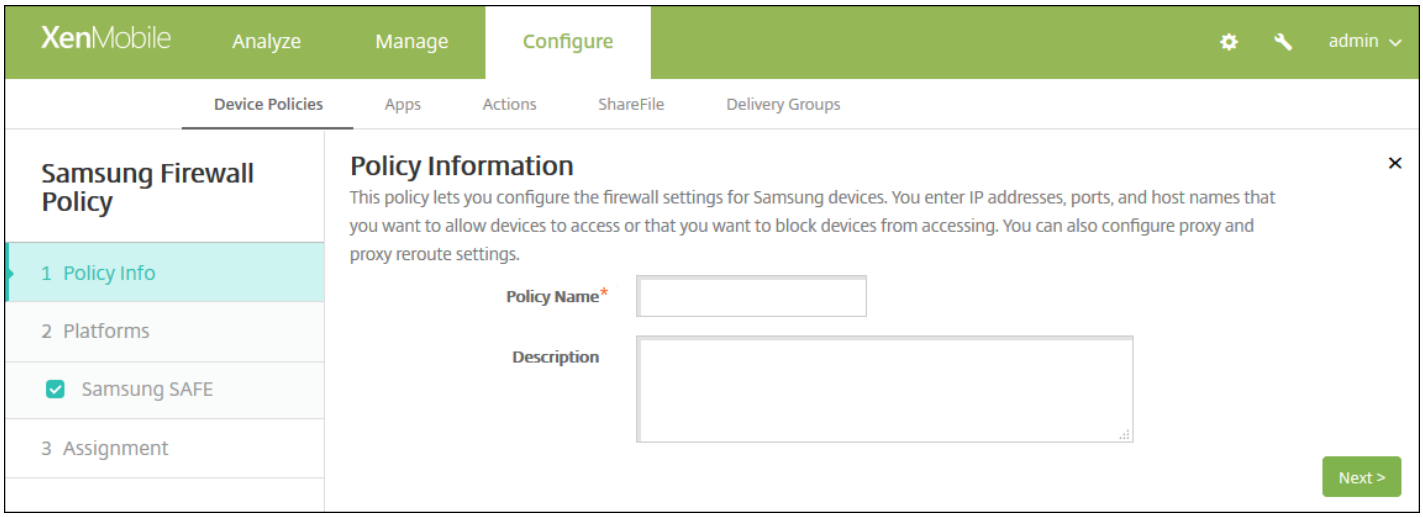
Feb 27, 2017

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.

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**.

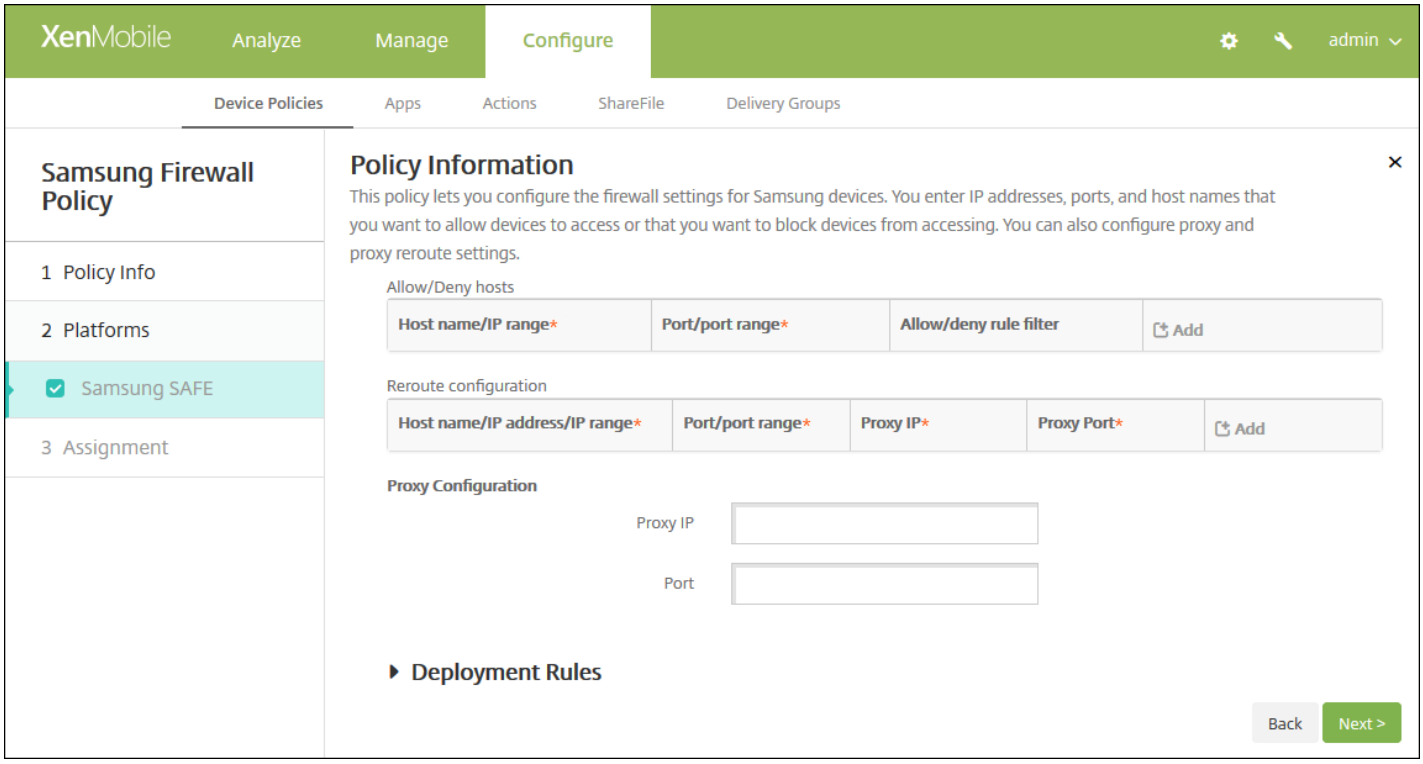
3. Expanda **More** y, en **Network access**, haga clic en **Samsung Firewall**. Aparecerá la página **Samsung Firewall Policy**.



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 acerca de la plataforma **Samsung SAFE**.



6. Configure estos parámetros:

- **Permitir/denegar hosts**
  - Para cada host al que quiera permitir o denegar el acceso, haga clic en **Add** y lleve a cabo lo siguiente:
    - **Host name/IP range**. Escriba el nombre de host o el intervalo de direcciones IP del sitio en cuestión.
    - **Port/port range**. Escriba el número de puerto o el intervalo de puertos.
    - **Allow/deny rule filter**. Seleccione "Whitelist" para permitir el acceso al sitio o "Blacklist" para negarlo.
    - Haga clic en **Save** o **Cancel**.
- **Configuración de enrutamiento**
  - Para cada proxy que quiera configurar, haga clic en **Add** y lleve a cabo lo siguiente:
    - **Host name/IP range**. Escriba el nombre de host o el intervalo de direcciones IP para el reenrutado del proxy.
    - **Port/port range**. Escriba el número de puerto o el intervalo de puertos.
    - **Proxy IP**. Escriba la dirección IP del proxy.
    - **Proxy port**. Escriba el puerto del proxy.
    - Haga clic en **Save** o **Cancel**.

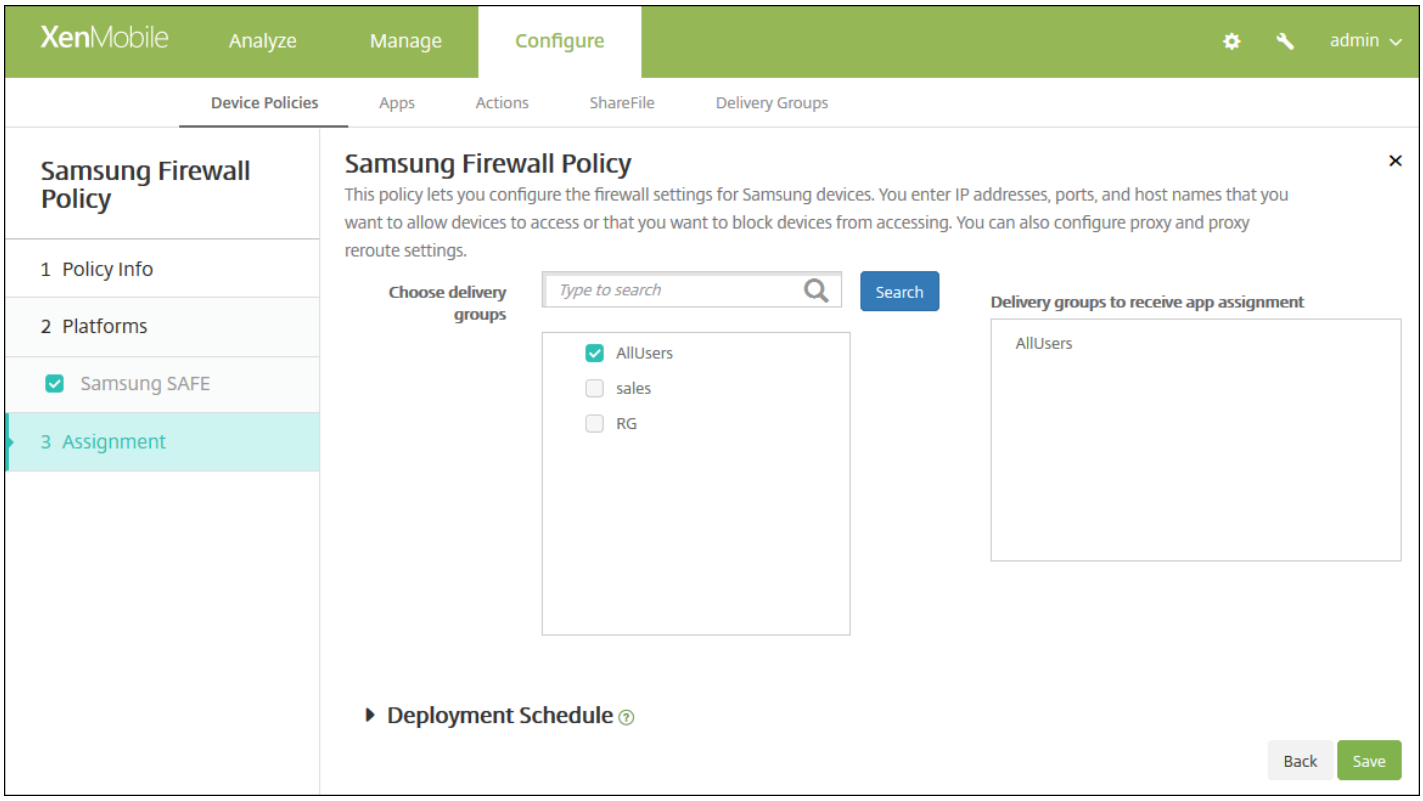
    Nota: Para eliminar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

    Para modificar un elemento 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 proxy**
  - **Proxy IP**. Escriba la dirección IP del servidor proxy.
  - **Port**. Escriba el puerto del servidor proxy.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Samsung Firewall Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 SCEP

Feb 27, 2017

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.

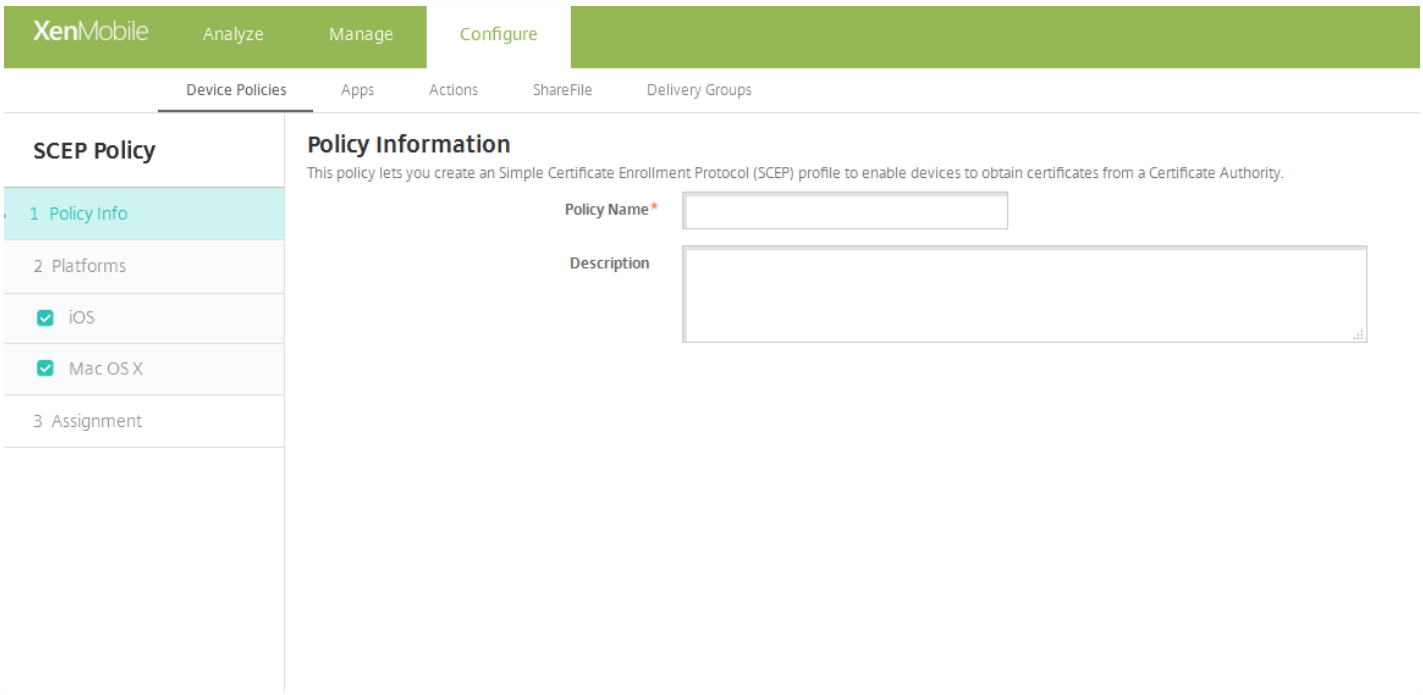
Configuración de iOS

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**. Aparecerá el cuadro de diálogo **Add New Policy**.

3. Expanda **More** y, a continuación, en **Security**, haga clic en **SCEP**. Aparecerá la página de información **SCEP 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.

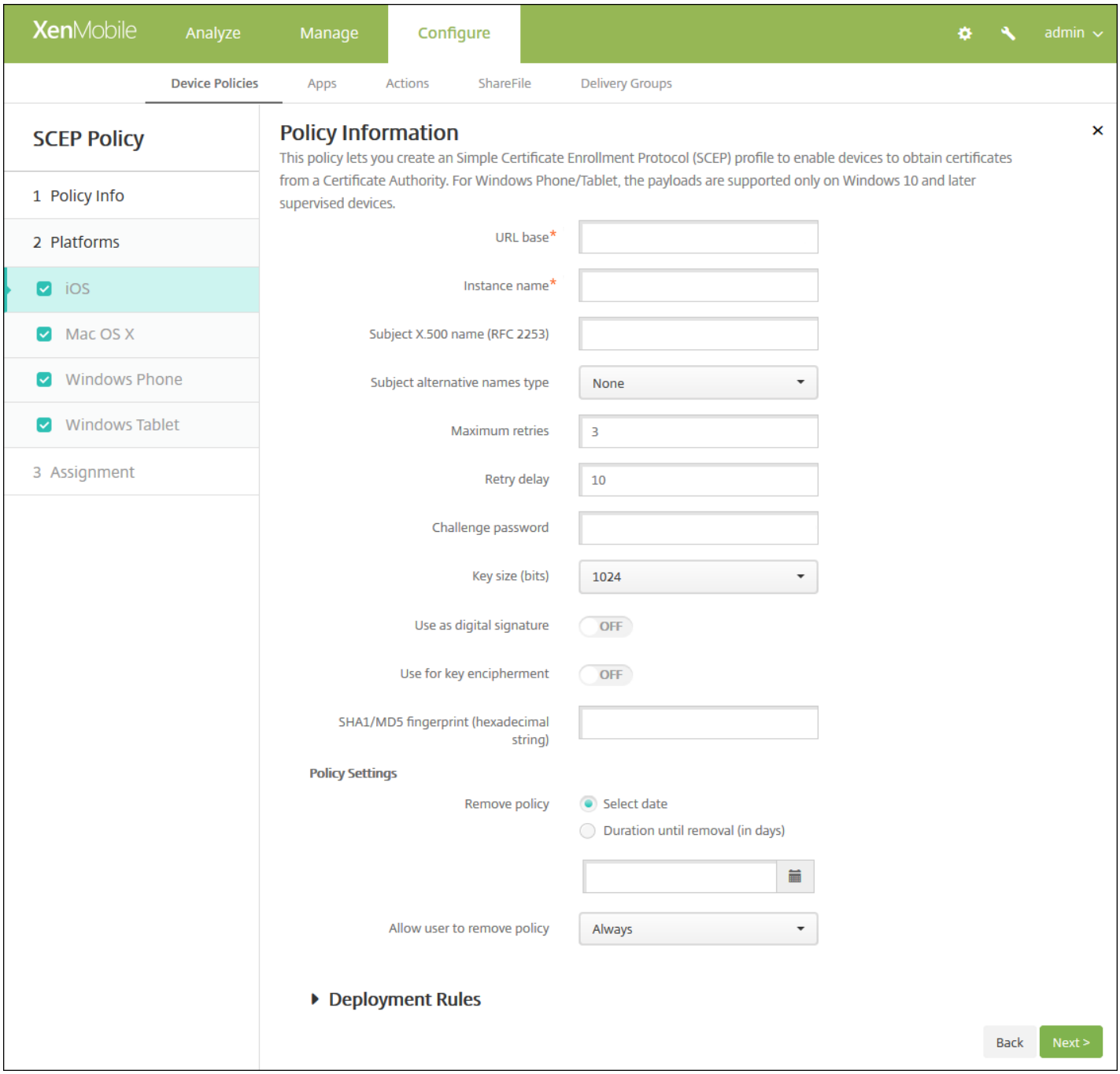
5. Haga clic en **Next**. Aparecerá la página **Platforms**.

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



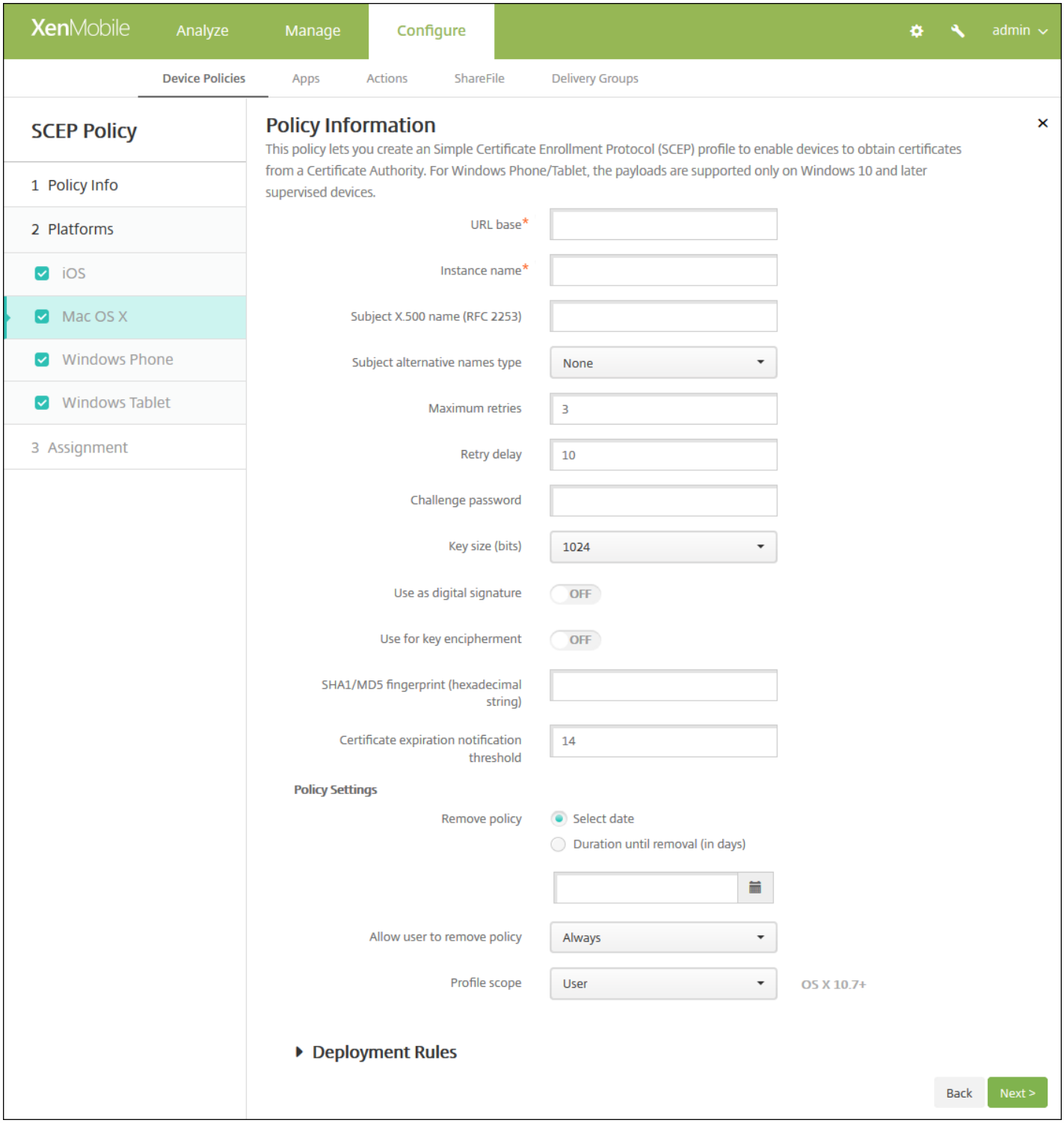
Configure estos parámetros:

- **URL base**. Escriba la dirección del servidor SCEP para definir dónde se enviarán las solicitudes SCEP, ya sea por HTTP o por HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que enviar la solicitud sin cifrar puede ser una opción segura. Sin embargo, si se permite volver a utilizar la contraseña de un solo uso, debe utilizar HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Instance name**. Escriba cualquier cadena que reconozca el servidor SCEP. Por ejemplo, puede ser un nombre de dominio, como ejemplo.org. Si una entidad de certificación dispone de varios certificados de CA, puede usar este campo para

diferenciar el dominio pertinente. Este paso es obligatorio.

- **Subject X.500 name (RFC 2253)**. Escriba la representación de un nombre de X.500 representado como una matriz de identificadores OID y valores. Por ejemplo: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se podría traducir como: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. Los identificadores OID se pueden representar como números con puntos y que disponen de accesos directos para el país (C), la localidad (L), el estado (ST), la organización (O), la unidad organizativa (OU) y el nombre común (CN).
- **Subject alternative names type**. En la lista, seleccione un tipo de nombre alternativo. Si lo prefiere, la directiva de SCEP puede especificar un tipo de nombre alternativo que proporciona los valores que requiere la entidad de certificación para emitir un certificado. Puede especificar **None**, **RFC 822 name**, **DNS name** o **URI**.
- **Maximum retries**. Escriba la cantidad de veces que un dispositivo debe volver a intentar la conexión cuando el servidor SCEP envía la respuesta PENDING. El valor predeterminado es **3**.
- **Retry delay**. Escriba el número de segundos que se deben esperar entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Challenge password**. Escriba un secreto previamente compartido.
- **Key size (bits)**. En la lista, haga clic en el tamaño de la clave en bits, ya sea **1024** o **2048**. El valor predeterminado es **1024**.
- **Use as digital signature**. Indique esta opción si quiere que el certificado se use como una firma digital. Si alguien usa el certificado para comprobar una firma digital (por ejemplo, para averiguar si el certificado ha sido emitido por una entidad de certificación), el servidor SCEP podría comprobar si ese certificado se puede usar de esa forma antes de usar la clave pública para descifrar el hash.
- **Use for key encipherment**. Indique esta opción si quiere que el certificado se use para el cifrado de clave. Si un servidor utiliza la clave pública en un certificado proporcionado por un cliente para comprobar que una parte de los datos se ha cifrado mediante la clave privada, el servidor puede comprobar primero si el certificado se puede usar para el cifrado de clave. Si no es así, la operación no se puede realizar.
- **SHA1/MD5 fingerprint (hexadecimal string)**. Si la entidad de certificación utiliza HTTP, utilice este campo para la huella digital del certificado de CA; el dispositivo se vale de él para confirmar la autenticidad de la respuesta de la entidad durante la inscripción. Puede escribir una huella digital MD5 o SHA1. También puede seleccionar un certificado para importar su firma.
- **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

Configuración de los parámetros de Mac OS X



Configure estos parámetros:

- **URL base**. Escriba la dirección del servidor SCEP para definir dónde se enviarán las solicitudes SCEP, ya sea por HTTP o por HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que enviar la solicitud sin cifrar puede ser una opción segura. Sin embargo, si se permite volver a utilizar la contraseña de un solo uso, debe utilizar HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Instance name**. Escriba cualquier cadena que reconozca el servidor SCEP. Por ejemplo, puede ser un nombre de dominio, como ejemplo.org. Si una entidad de certificación dispone de varios certificados de CA, puede usar este campo para

diferenciar el dominio pertinente. Este paso es obligatorio.

- **Subject X.500 name (RFC 2253)**. Escriba la representación de un nombre de X.500 representado como una matriz de identificadores OID y valores. Por ejemplo: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se podría traducir como: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. Los identificadores OID se pueden representar como números con puntos y que disponen de accesos directos para el país (C), la localidad (L), el estado (ST), la organización (O), la unidad organizativa (OU) y el nombre común (CN).
- **Subject alternative names type**. En la lista, seleccione un tipo de nombre alternativo. Si lo prefiere, la directiva de SCEP puede especificar un tipo de nombre alternativo que proporciona los valores que requiere la entidad de certificación para emitir un certificado. Puede especificar **None**, **RFC 822 name**, **DNS name** o **URI**.
- **Maximum retries**. Escriba la cantidad de veces que un dispositivo debe volver a intentar la conexión cuando el servidor SCEP envía la respuesta PENDING. El valor predeterminado es **3**.
- **Retry delay**. Escriba el número de segundos que se deben esperar entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Challenge password**. Escriba un secreto previamente compartido.
- **Key size (bits)**. En la lista, haga clic en el tamaño de la clave en bits, ya sea **1024** o **2048**. El valor predeterminado es **1024**.
- **Use as digital signature**. Indique esta opción si quiere que el certificado se use como una firma digital. Si alguien usa el certificado para comprobar una firma digital (por ejemplo, para averiguar si el certificado ha sido emitido por una entidad de certificación), el servidor SCEP podría comprobar si ese certificado se puede usar de esa forma antes de usar la clave pública para descifrar el hash.
- **Use for key encipherment**. Indique esta opción si quiere que el certificado se use para el cifrado de clave. Si un servidor utiliza la clave pública en un certificado proporcionado por un cliente para comprobar que una parte de los datos se ha cifrado mediante la clave privada, el servidor puede comprobar primero si el certificado se puede usar para el cifrado de clave. Si no es así, la operación no se puede realizar.
- **SHA1/MD5 fingerprint (hexadecimal string)**. Si la entidad de certificación utiliza HTTP, utilice este campo para la huella digital del certificado de CA; el dispositivo se vale de él para confirmar la autenticidad de la respuesta de la entidad durante la inscripción. Puede escribir una huella digital MD5 o SHA1. También puede seleccionar un certificado para importar su firma.
- **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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 **SCEP Policy**.

9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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**.

Nota:

- Esta opción se aplica si se configura la clave de implementación en segundo plano para la programación desde **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.

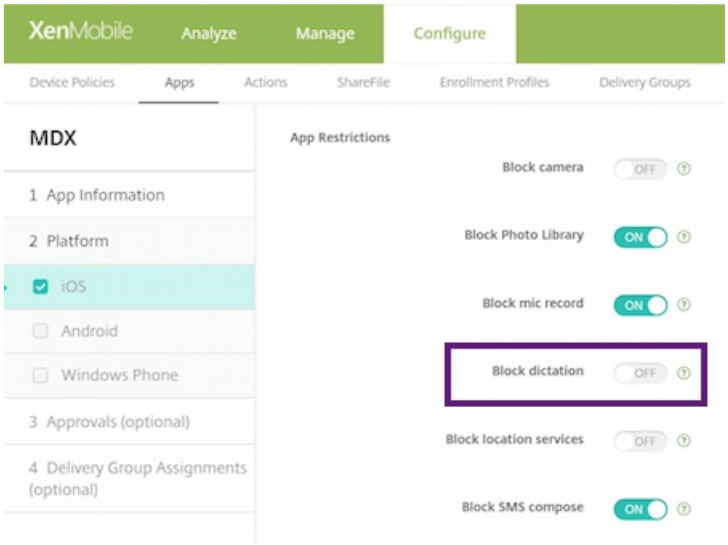
Directivas de Siri y dictado

Feb 27, 2017

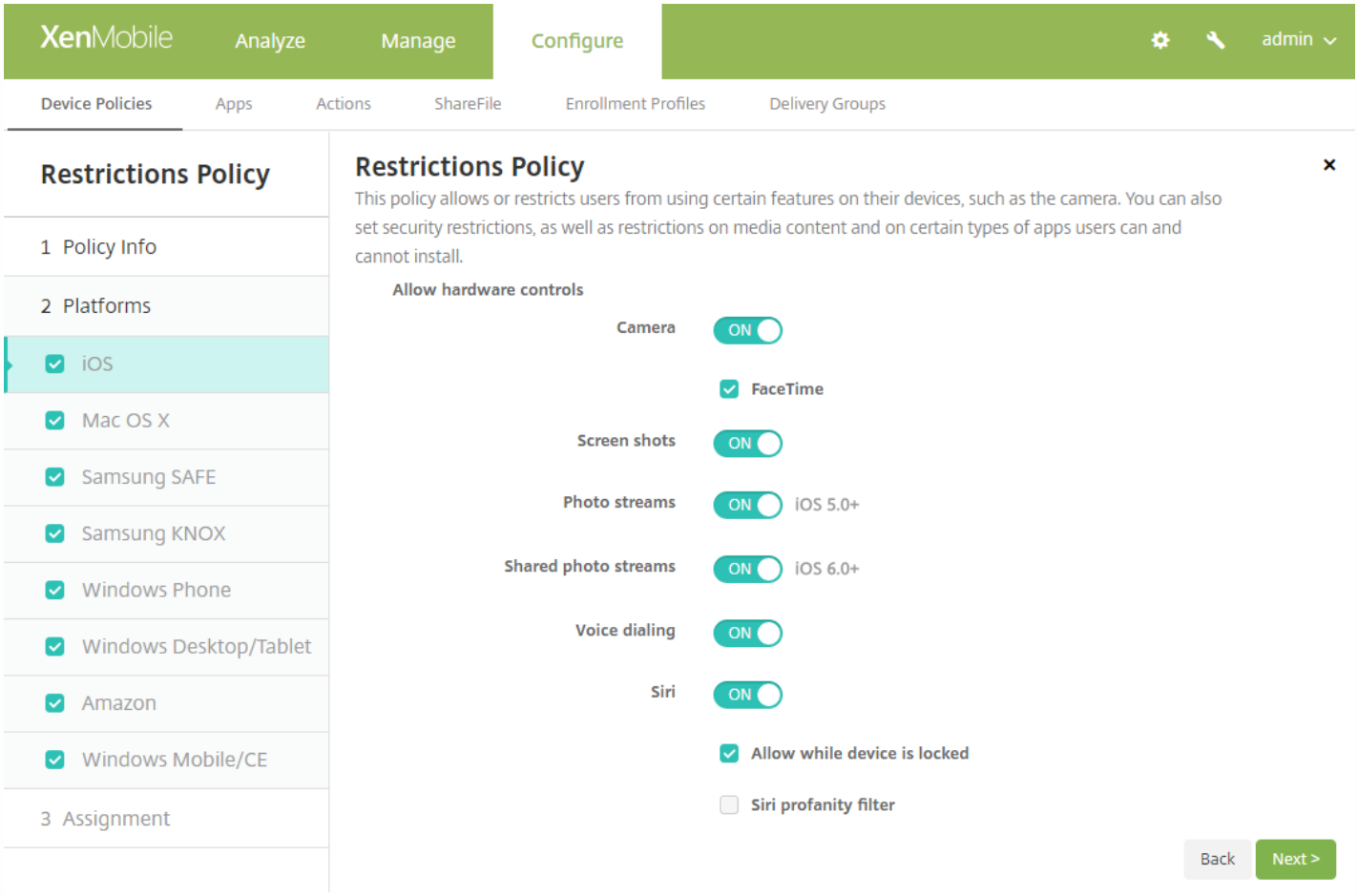
Cuando los usuarios preguntan algo a Siri o dictan texto en dispositivos iOS administrados, Apple recopila los datos de voz con el fin de mejorar Siri. Los datos de voz pasan a través de los servicios de nube de Apple, y por lo tanto existen fuera del contenedor seguro de XenMobile. El texto resultado del dictado, sin embargo, queda dentro del contenedor.

XenMobile le permite bloquear los servicios de dictado y Siri, si sus necesidades de seguridad lo exigen.

En las implementaciones de administración de aplicaciones móviles (MAM), la directiva **Block dictation** para cada aplicación tiene el valor **On** (activada) de forma predeterminada, lo que inhabilita el micrófono del dispositivo. Configúrela con el valor **Off** si quiere permitir el dictado. Puede encontrar la directiva en la consola de XenMobile, en **Configure > Apps**. Seleccione la aplicación, haga clic en **Edit** y, a continuación, haga clic en **iOS**.



En implementaciones de administración de dispositivos móviles (MDM), también puede inhabilitar Siri desde **Configure > Device Policies > Restrictions Policy > iOS**. El uso de Siri está permitido de manera predeterminada.



Hay algunas cuestiones a tener en cuenta a la hora de decidir si se permiten Siri y el dictado:

- De acuerdo con la información que Apple ha hecho pública, Apple guarda datos de clips de voz y Siri por un máximo de dos años. Se asigna un número aleatorio a los datos, para representar al usuario, y los archivos de voz se asocian con dicho número. Para obtener más información, consulte este artículo de Wired: Apple reveals how long Siri keeps your data.
- Puede consultar la directiva de privacidad de Apple en **Ajustes > General > Teclados** en cualquier dispositivo iOS, si toca el enlace de **Habilitar dictado**.

Directiva de dispositivo de cuenta SSO

Feb 27, 2017

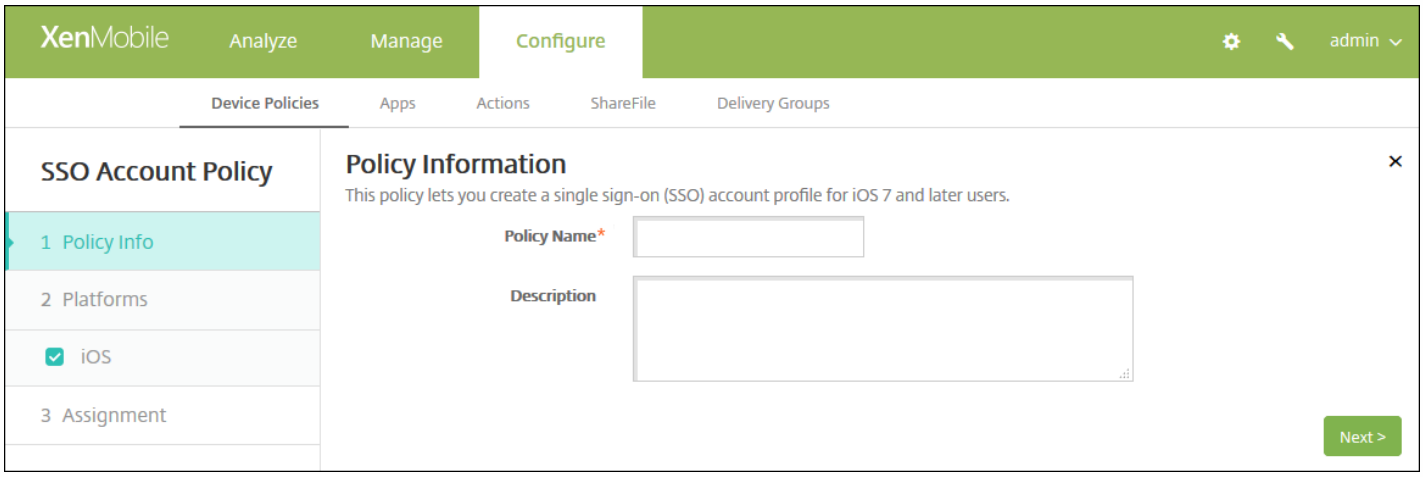
En XenMobile, puede crear cuentas de inicio de sesión único (SSO) para que los usuarios solo deban iniciar sesión una vez para acceder a XenMobile y a los recursos internos de la empresa desde varias aplicaciones. Así, no es necesario que los usuarios almacenen credenciales en el dispositivo. Las credenciales de usuario de empresa de la cuenta SSO se pueden usar en varias aplicaciones, incluidas las aplicaciones del App Store de Apple. Esta directiva está pensada para funcionar con un servidor back-end de autenticación Kerberos.

Nota: Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

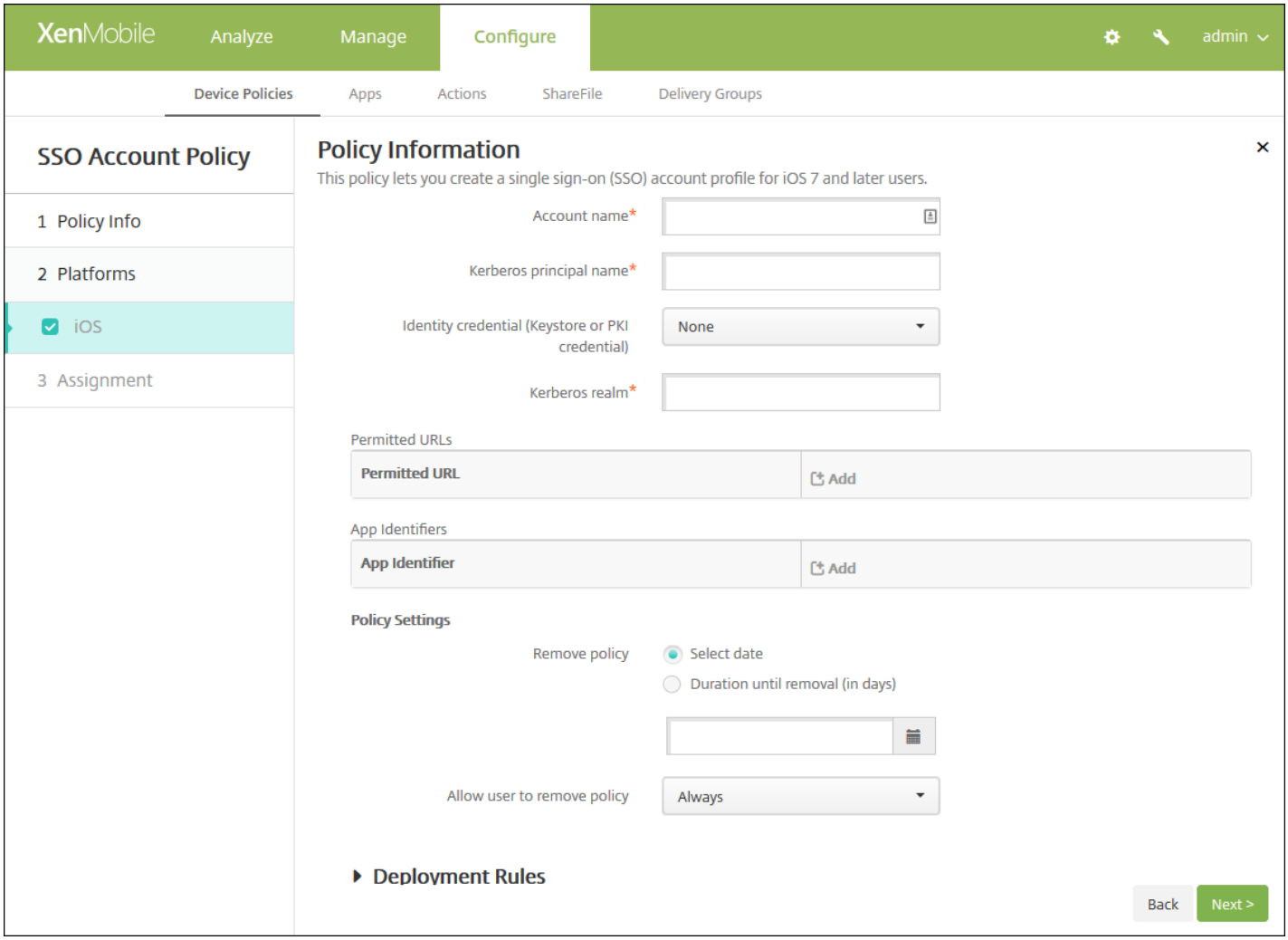
3. Haga clic en **More** y, en **End user**, haga clic en **SSO Account**. Aparecerá la página **SSO Account Policy**.



4. En el panel **SSO Account 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 de la **plataforma iOS**.



6. Configure estos parámetros:

- **Account name**. Escriba el nombre de la cuenta SSO de Kerberos que aparece en los dispositivos de los usuarios. Este campo es obligatorio.
- **Kerberos principal name**. Escriba el nombre de la entidad principal de seguridad asignada a Kerberos. Este campo es obligatorio.
- **Identity credential (Keystore or PKI credential)**. En la lista, haga clic en una de las credenciales de identidad opcionales que se pueden usar para renovar la credencial de Kerberos sin la interacción del usuario.
- **Kerberos realm**. Escriba el dominio de Kerberos designado a esta directiva. Por regla general, se trata de su nombre de dominio en letras mayúsculas (por ejemplo, EJEMPLO.COM). Este campo es obligatorio.
- **Permitted URLs**. Para agregar cada URL que deba requerir el inicio Single Sign-On, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Permitted URL**. Escriba la URL que requerirá el inicio de sesión único cuando un usuario la visite desde el dispositivo iOS. Por ejemplo: cuando un usuario intenta abrir un sitio Web y este sitio pide una comprobación de Kerberos, si ese sitio no está en la lista de direcciones URL, el dispositivo iOS no intenta el inicio de sesión Single Sign-On con el token de Kerberos que se haya almacenado en caché en el dispositivo después de un inicio de sesión Kerberos. La coincidencia debe ser exacta en la parte de host de la URL; por ejemplo: http://shopping.apple.com es correcta, pero http://*.apple.com no lo es. Además, si Kerberos no se activa en función de la coincidencia de host, la URL sigue recurriendo a una llamada de HTTP estándar. Esto puede tener varias consecuencias, incluida una comprobación de

contraseña estándar o un error de HTTP si la URL se ha configurado solo para el inicio de sesión único mediante Kerberos.
    - Haga clic en **Add** para agregar la URL, o bien haga clic en **Cancel** para cancelar la operación.
- **App Identifiers**. Para cada aplicación que pueda emplear este inicio de sesión, haga clic en **Add** y lleve a cabo lo siguiente:
    - **App Identifier**. Escriba el identificador de aplicación perteneciente a una aplicación que pueda utilizar esta credencial. Si no se agrega ningún identificador de aplicación, esta credencial coincidirá con **todos** los identificadores de aplicación.
    - Haga clic en **Add** para agregar el identificador de aplicación, o bien haga clic en **Cancel** para cancelar la operación.

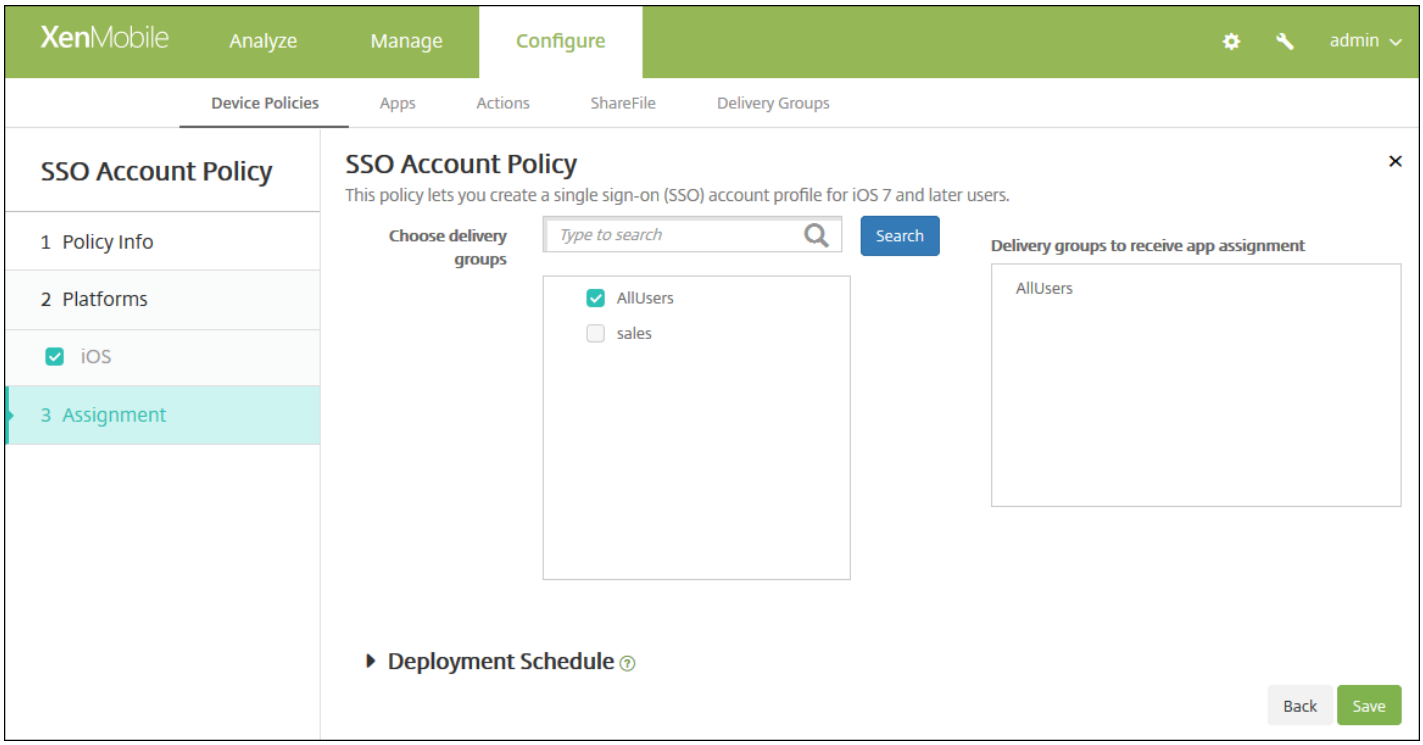
      Nota: Para eliminar una URL o un identificador de aplicación existente, coloque el cursor sobre la línea que los contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

      Para modificar una URL o un identificador de aplicación existente, coloque el cursor sobre la línea que los contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

- **Configuraciones de directivas**
    - 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 list**, haga clic en **Always**, **Password required** o **Never**.
    - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **SSO Account Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para el cifrado del almacenamiento

Feb 27, 2017

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 detalladamente en este artículo.

Configuración de Samsung SAFE

Configuración de Windows Phone

Configuración de Android Sony

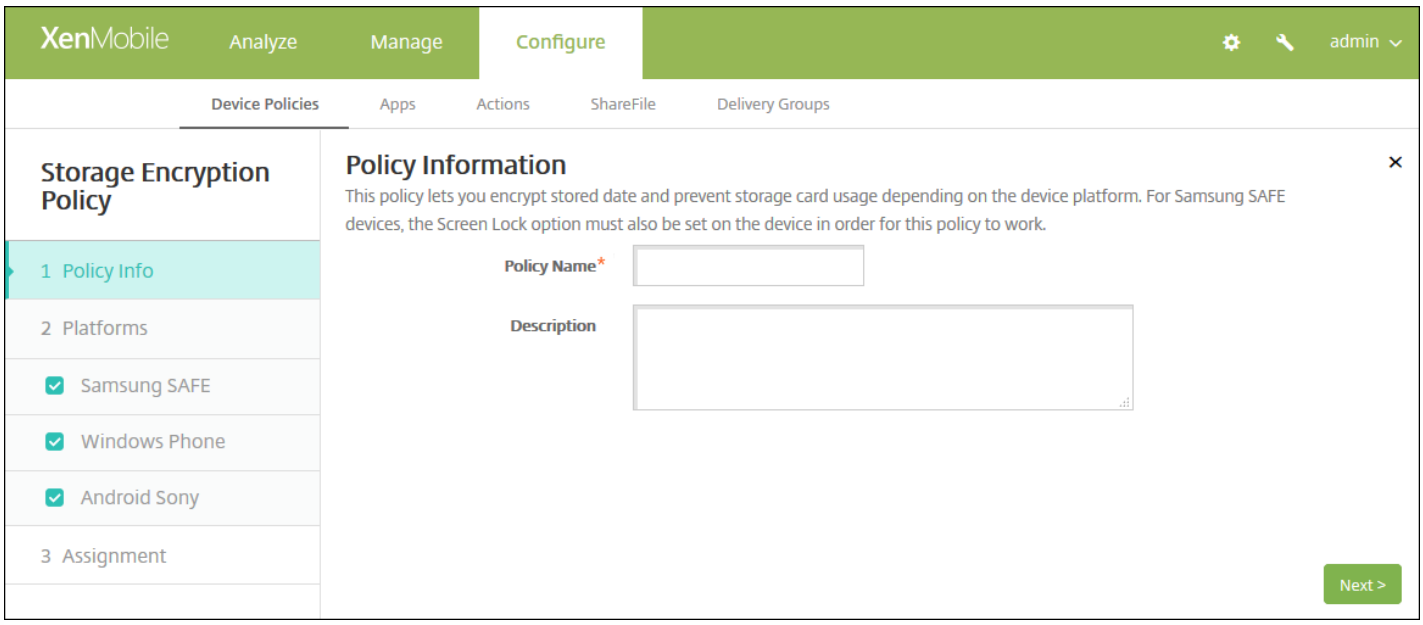
Nota: Para dispositivos Samsung SAFE, antes de configurar esta directiva, compruebe que se cumplen los siguientes requisitos:

- Debe establecer la opción de bloqueo de pantalla en los dispositivos de los usuarios.
- Los dispositivos de los usuarios deben estar conectados y cargados al 80 %.
- El dispositivo debe requerir una contraseña que contenga números y letras o símbolos.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

3. Haga clic en **More** y, a continuación, en **Security**, haga clic en **Storage Encryption**. Aparecerá la página de información **Storage Encryption Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

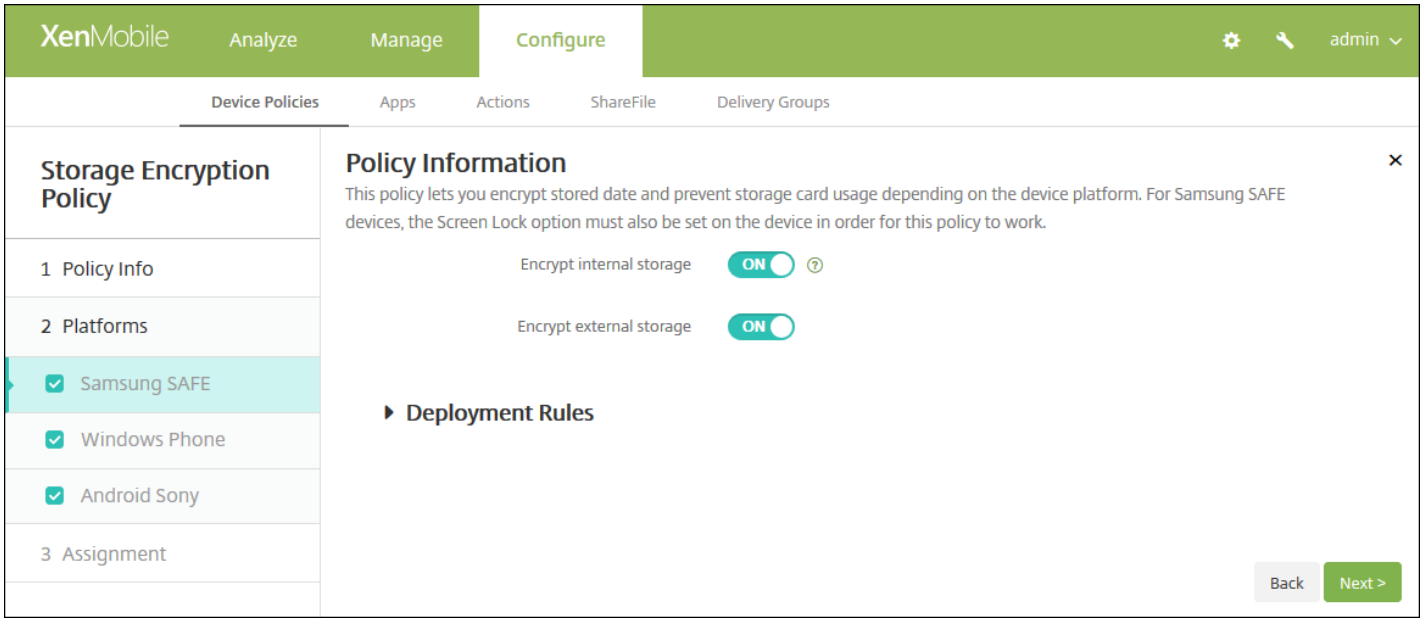
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

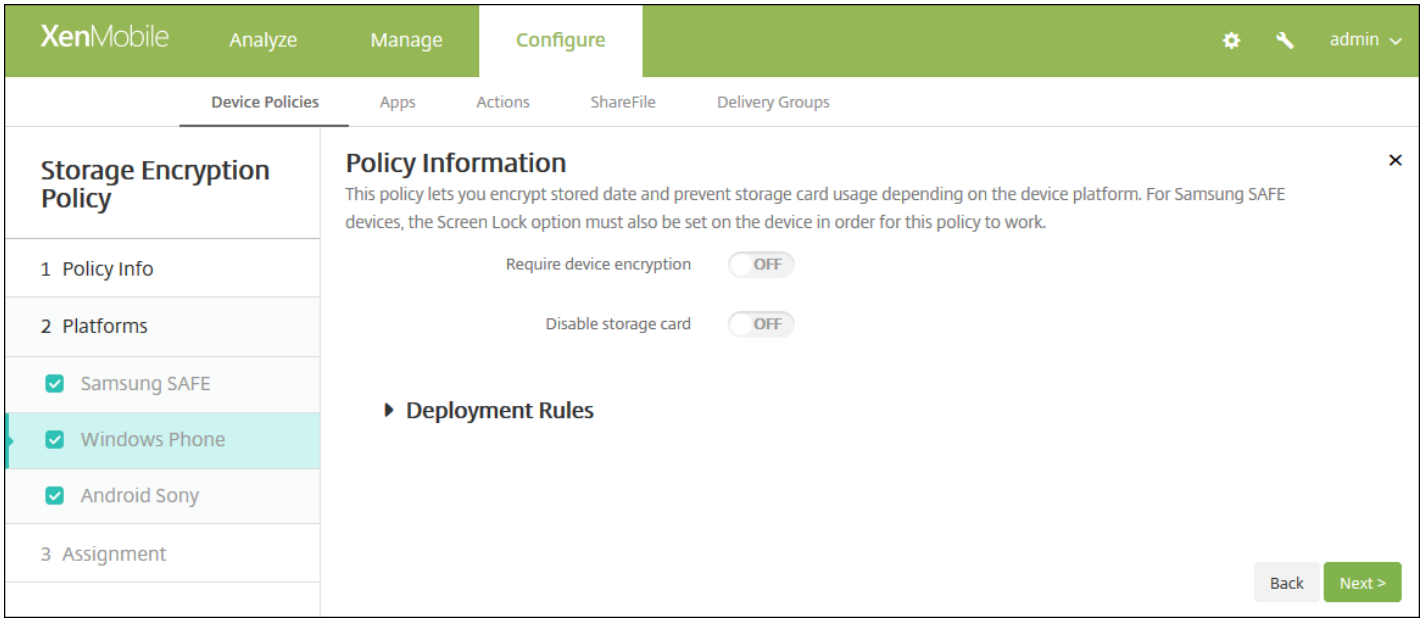
Configuración de los parámetros de Samsung SAFE



Configure estos parámetros:

- **Encrypt internal storage**. Seleccione si cifrar el almacenamiento interno en los dispositivos de los usuarios. El almacenamiento interno incluye el almacenamiento interno y la memoria del dispositivo. El valor predeterminado es **ON**.
- **Encrypt external storage**. Seleccione si cifrar el almacenamiento externo en los dispositivos de los usuarios. El valor predeterminado es **ON**.

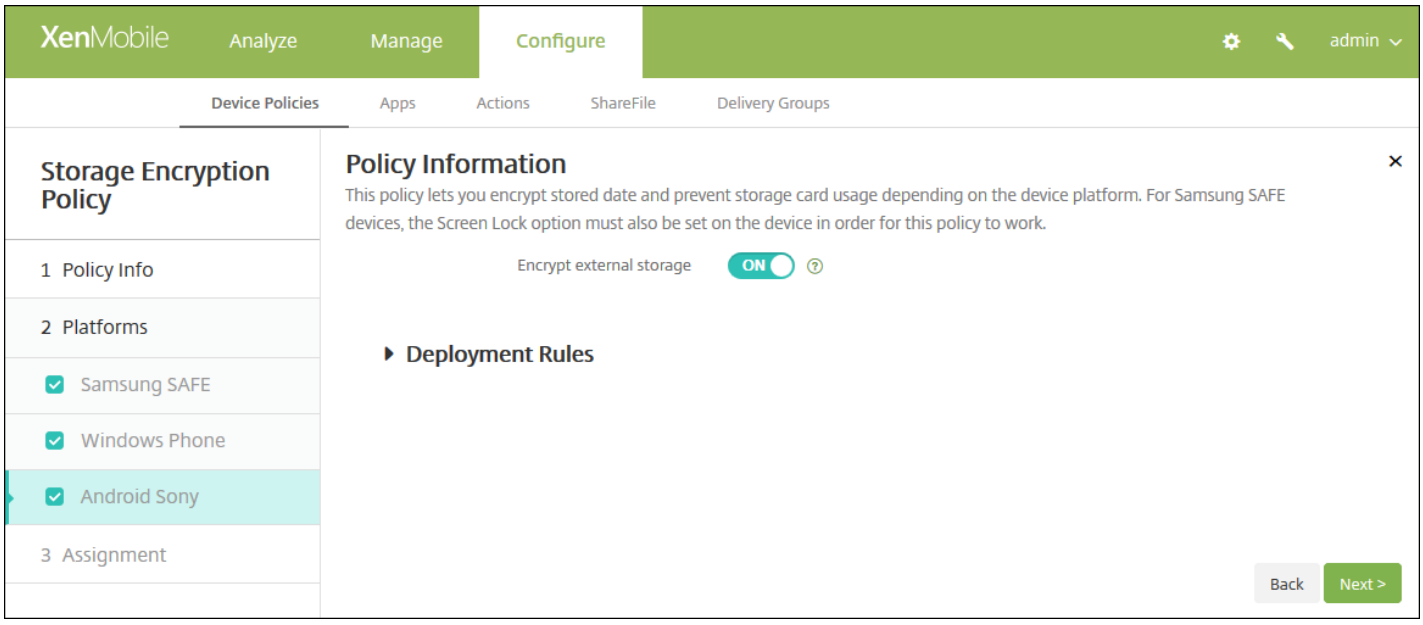
Configuración de los parámetros de Windows Phone



Configure estos parámetros:

- **Require device encryption**. Seleccione esta opción para cifrar los dispositivos de los usuarios. El valor predeterminado es **OFF**.
- **Disable storage card**. Seleccione esta opción para evitar que los usuarios utilicen tarjetas de almacenamiento en sus dispositivos. El valor predeterminado es **OFF**.

Configuración de los parámetros de Android Sony

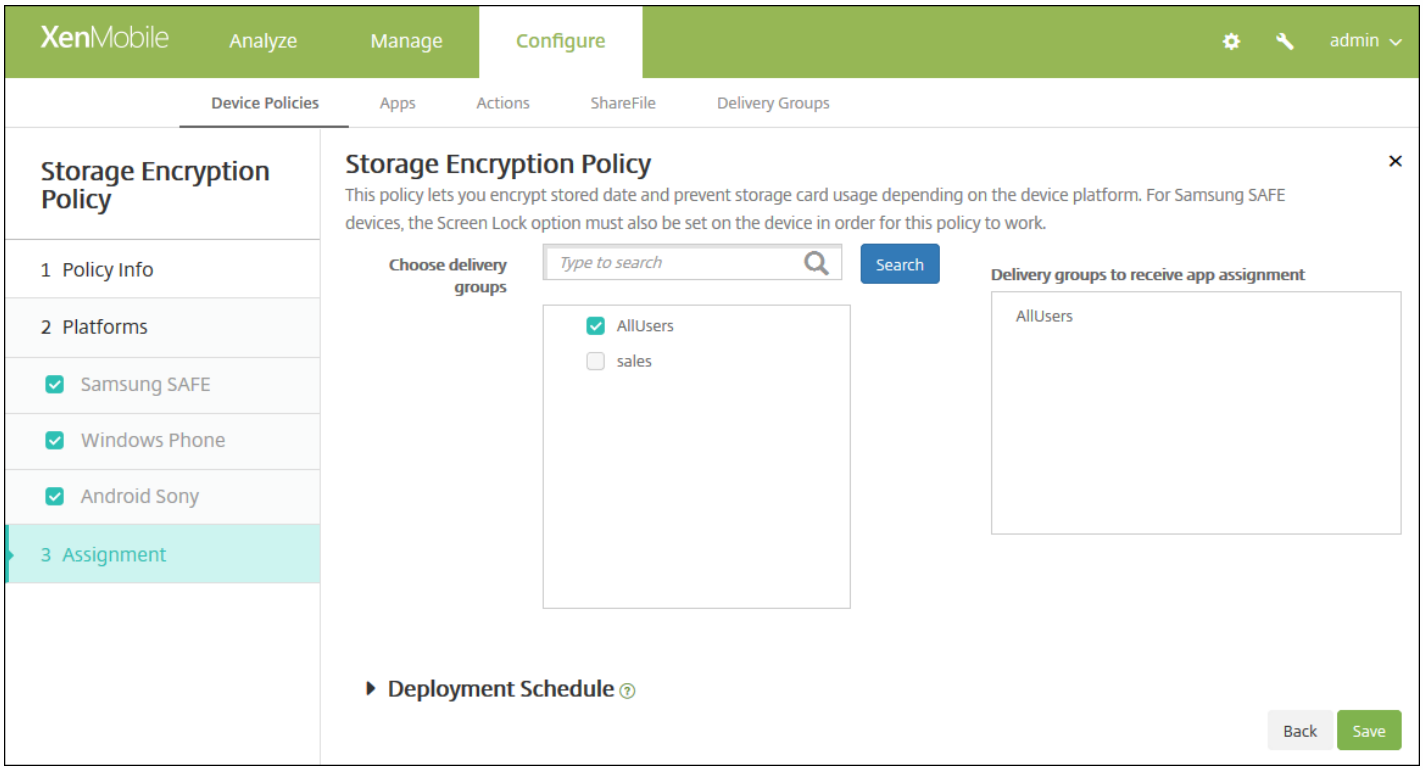


Configure este parámetro:

- **Encrypt external storage**. Seleccione si cifrar el almacenamiento externo en los dispositivos de los usuarios. El dispositivo debe requerir una contraseña que contenga números y letras o símbolos. El valor predeterminado es **ON**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Storage Encryption Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo Store

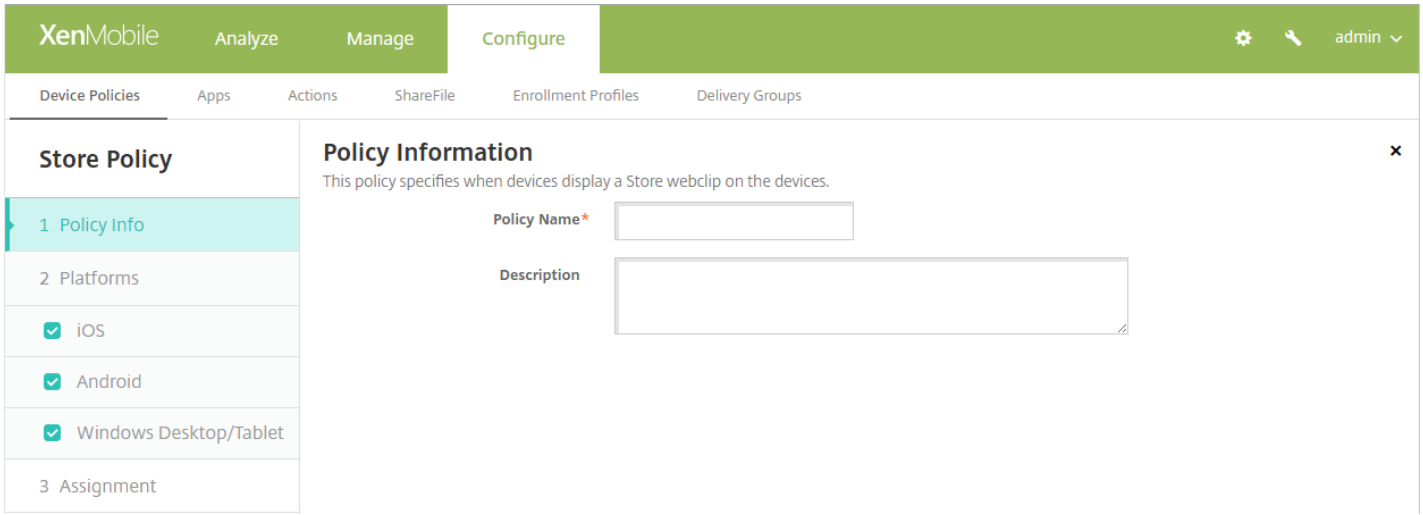
Feb 27, 2017

En XenMobile, puede crear una directiva para especificar si los dispositivos iOS, Android o tabletas Windows mostrarán un clip Web de XenMobile 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**.

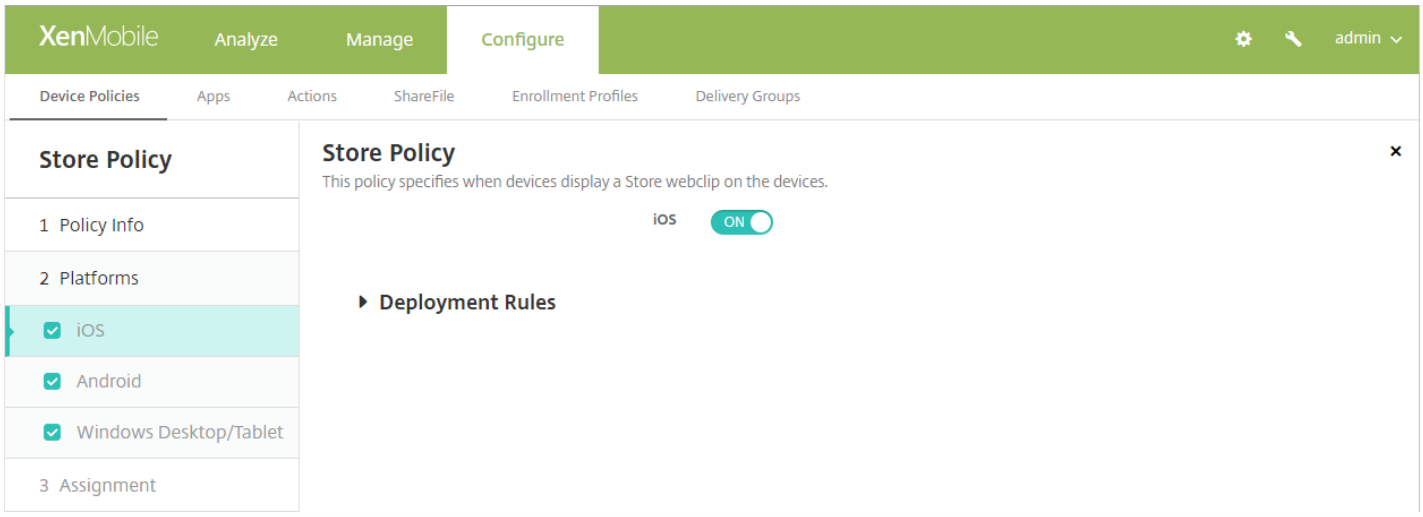
3. Expanda **More** y, a continuación, en **Apps**, haga clic en **Store**. Aparecerá la página **Store Policy**.



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 XenMobile 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 de **XenMobile Store Policy**.

10. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

Directiva de dispositivo para calendarios suscritos

Feb 27, 2017

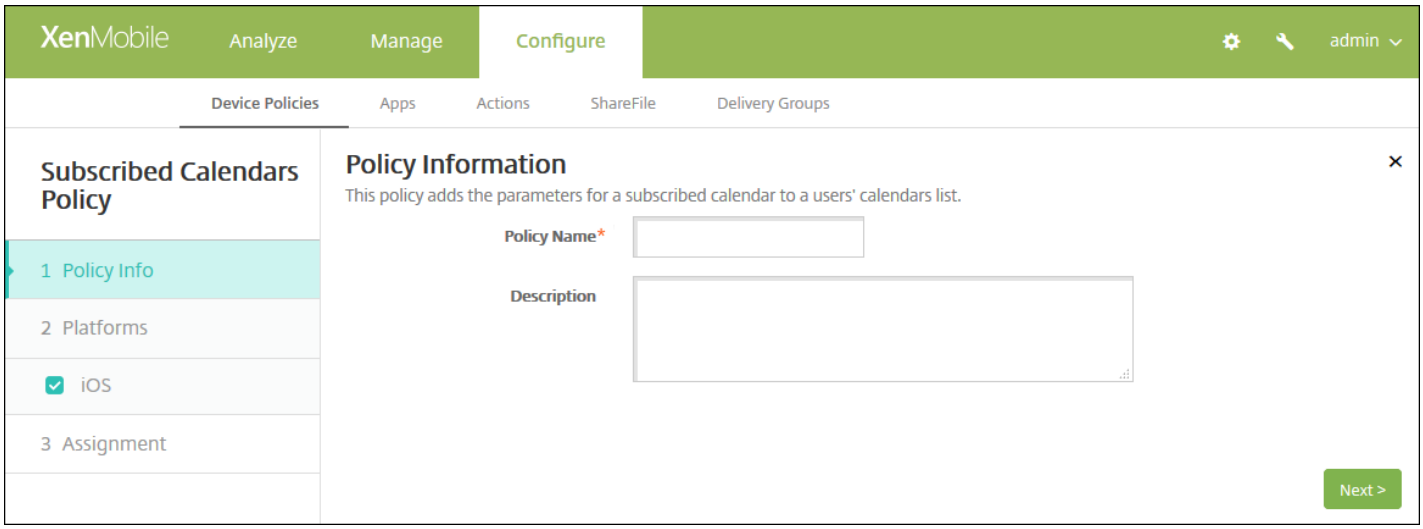
En XenMobile, puede agregar una directiva de dispositivos para agregar un calendario suscrito a la lista de calendarios en los dispositivos iOS de los usuarios. La lista de los calendarios públicos a los que se puede suscribir está disponible en www.apple.com/downloads/macosx/calendars.

Nota: Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

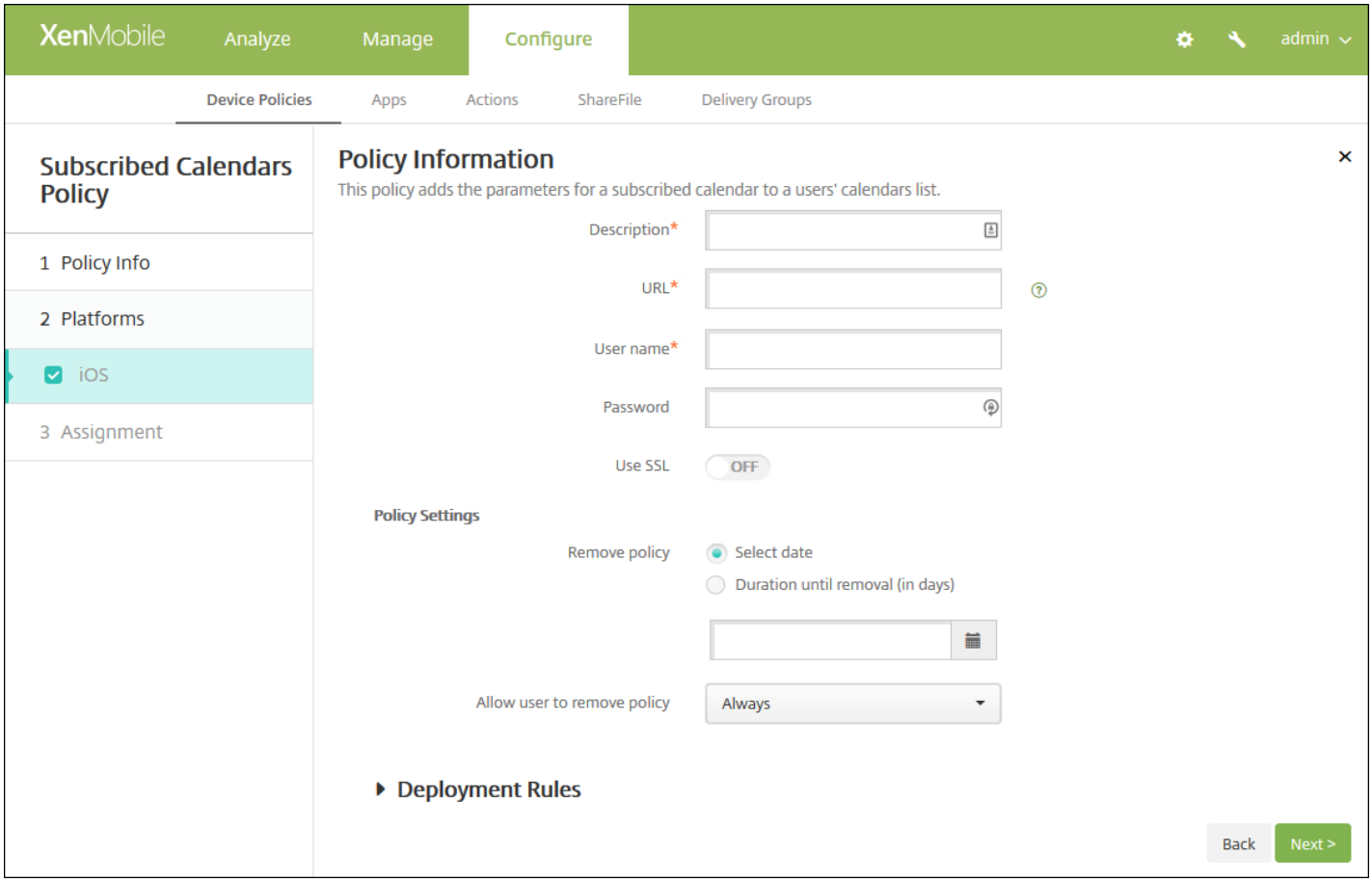
3. Haga clic en **More** y, en **End user**, haga clic en **Subscribed Calendars**. Aparecerá la página **Subscribed Calendars Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **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 de la plataforma **iOS**.

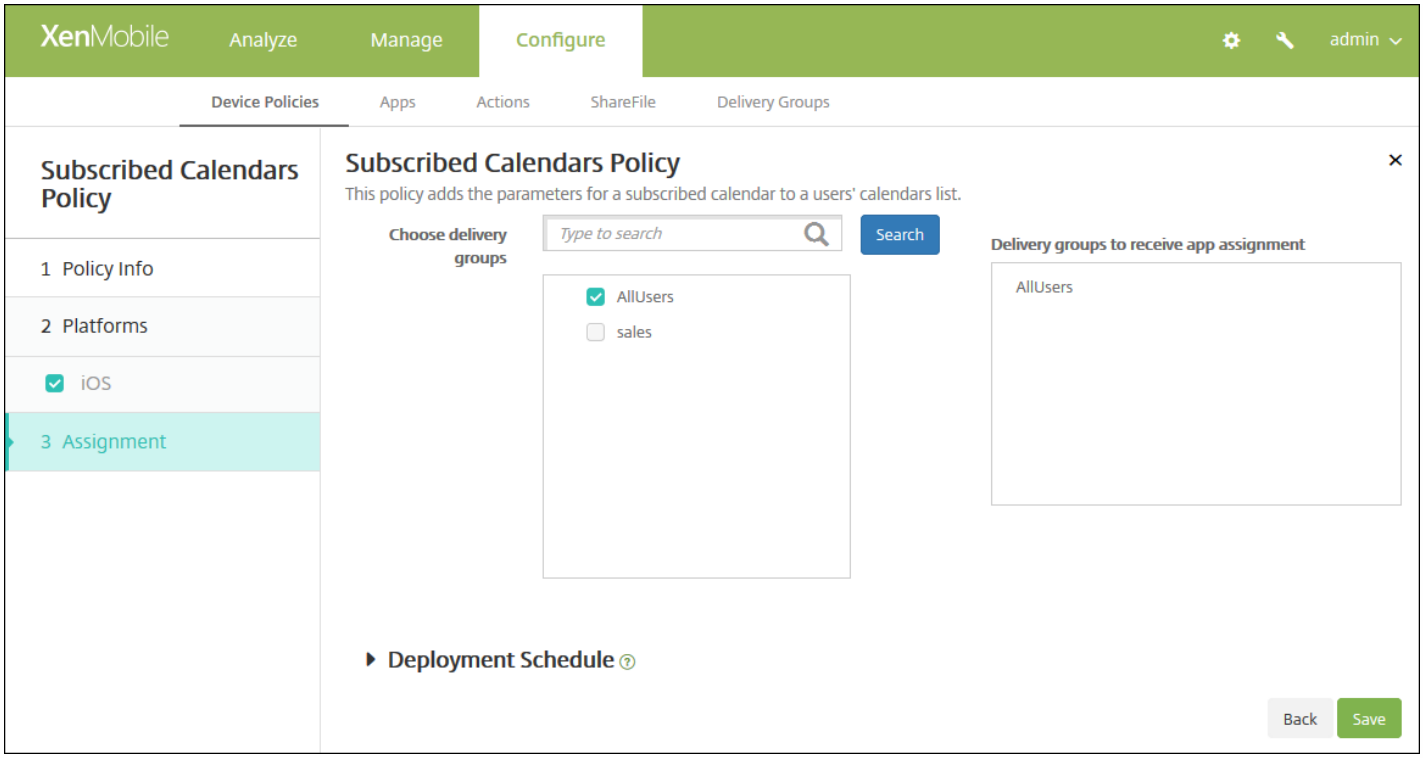


6. Configure estos parámetros:

- **Description**. Introduzca una descripción del calendario. Este campo es obligatorio.
- **URL**. Introduzca la dirección URL del calendario. Puede introducir una dirección URL webcal:// o un enlace http:// a un archivo de iCalendar (.ics). Este campo es obligatorio.
- **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 calendario. El valor predeterminado es Desactivado.
- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Subscribed Calendars Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para términos y condiciones

Feb 27, 2017

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.

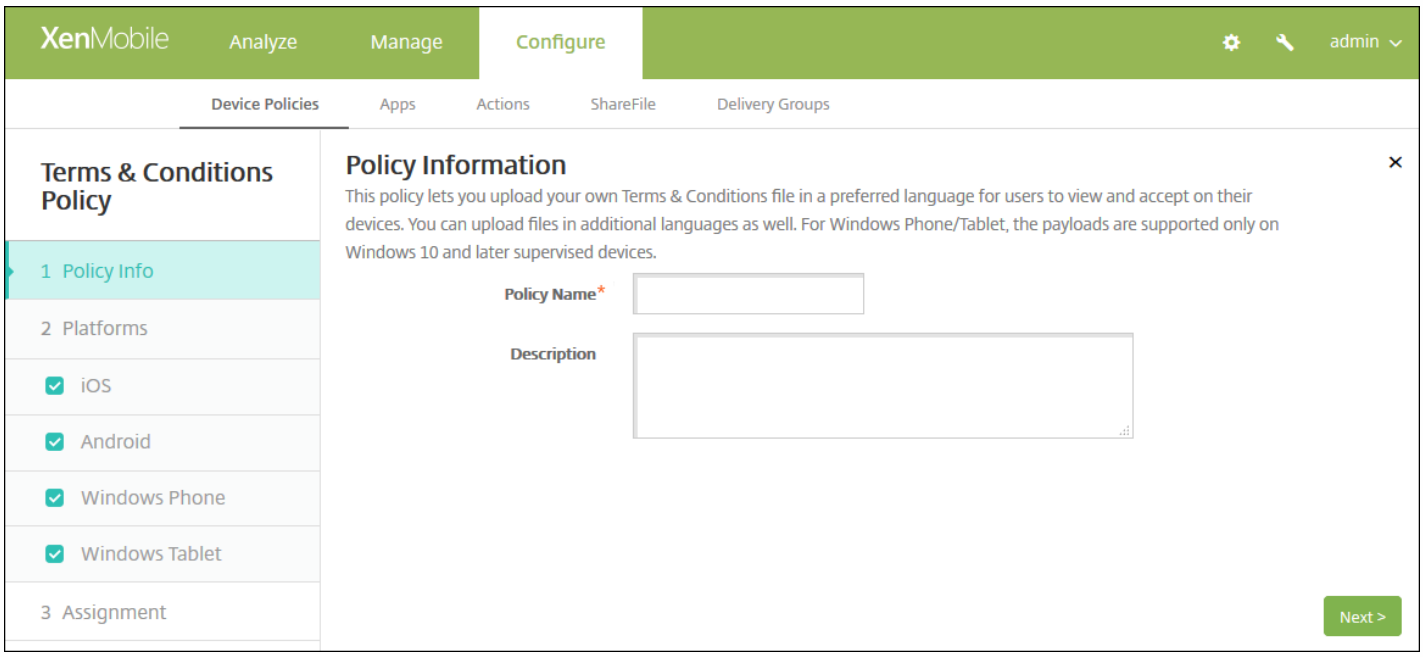
Configuración de iOS y Android

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**.

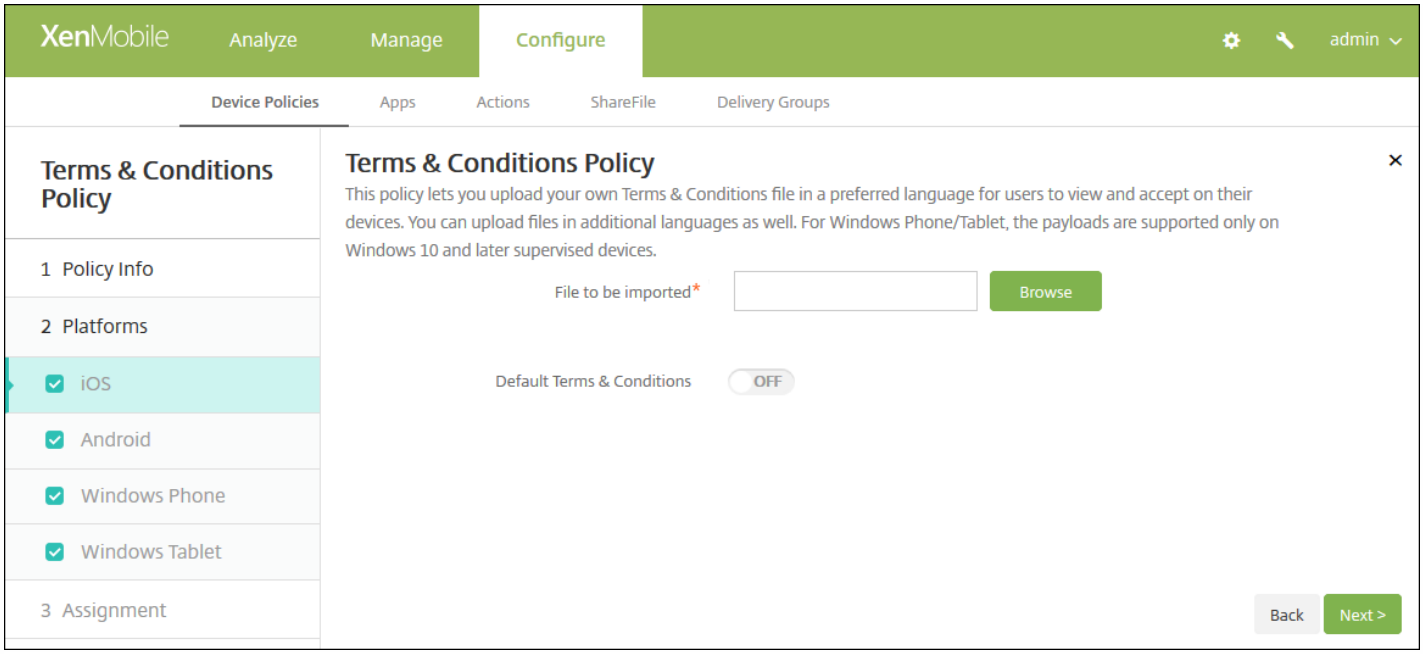
3. Haga clic en **Terms & Conditions**. Aparecerá la página **Terms & Conditions Policy**.



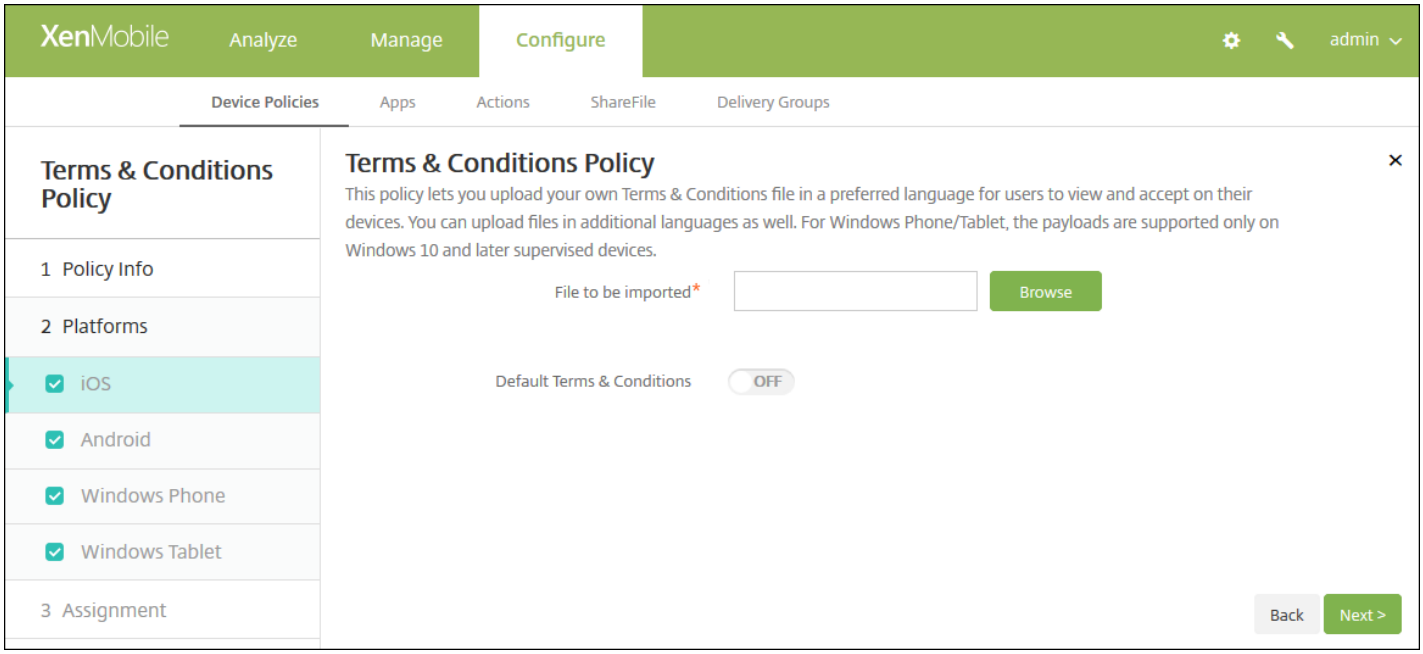
4. En el panel **Policy Information**, escriba la información siguiente:

- **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 **Platforms de Terms & Conditions Policy**.



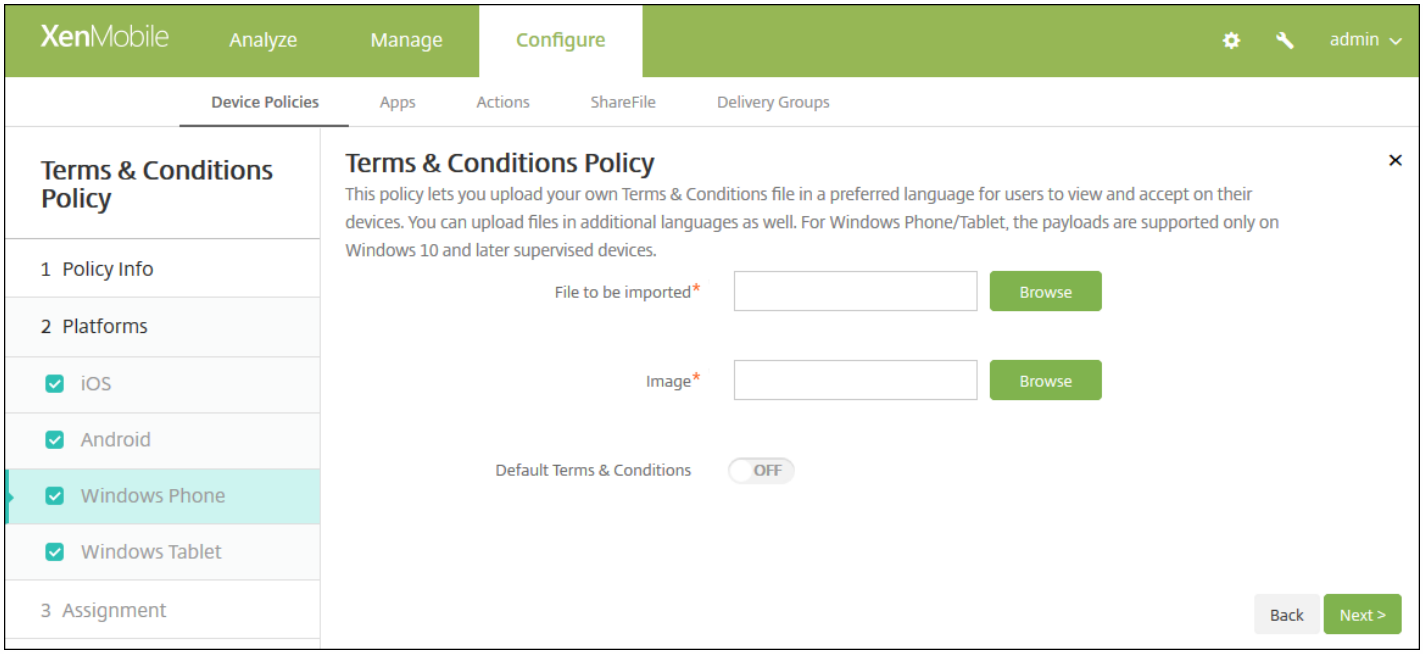
Configuración de iOS y Android



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**.

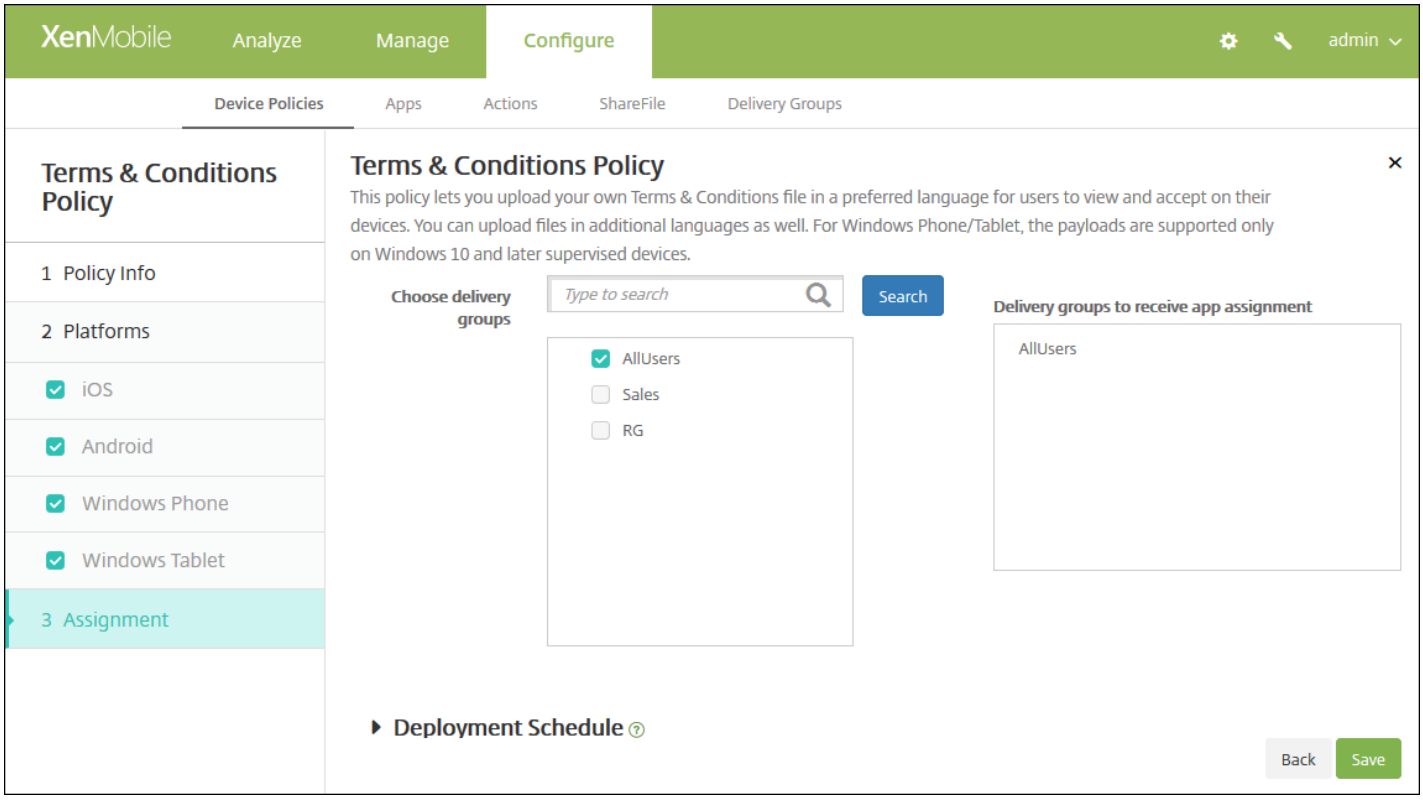
Configuración de Windows Phone y tabletas Windows



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 de **Terms & Conditions Policy**.



7. Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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.

8. Haga clic en **Save**.

Directiva de redes privadas virtuales (VPN)

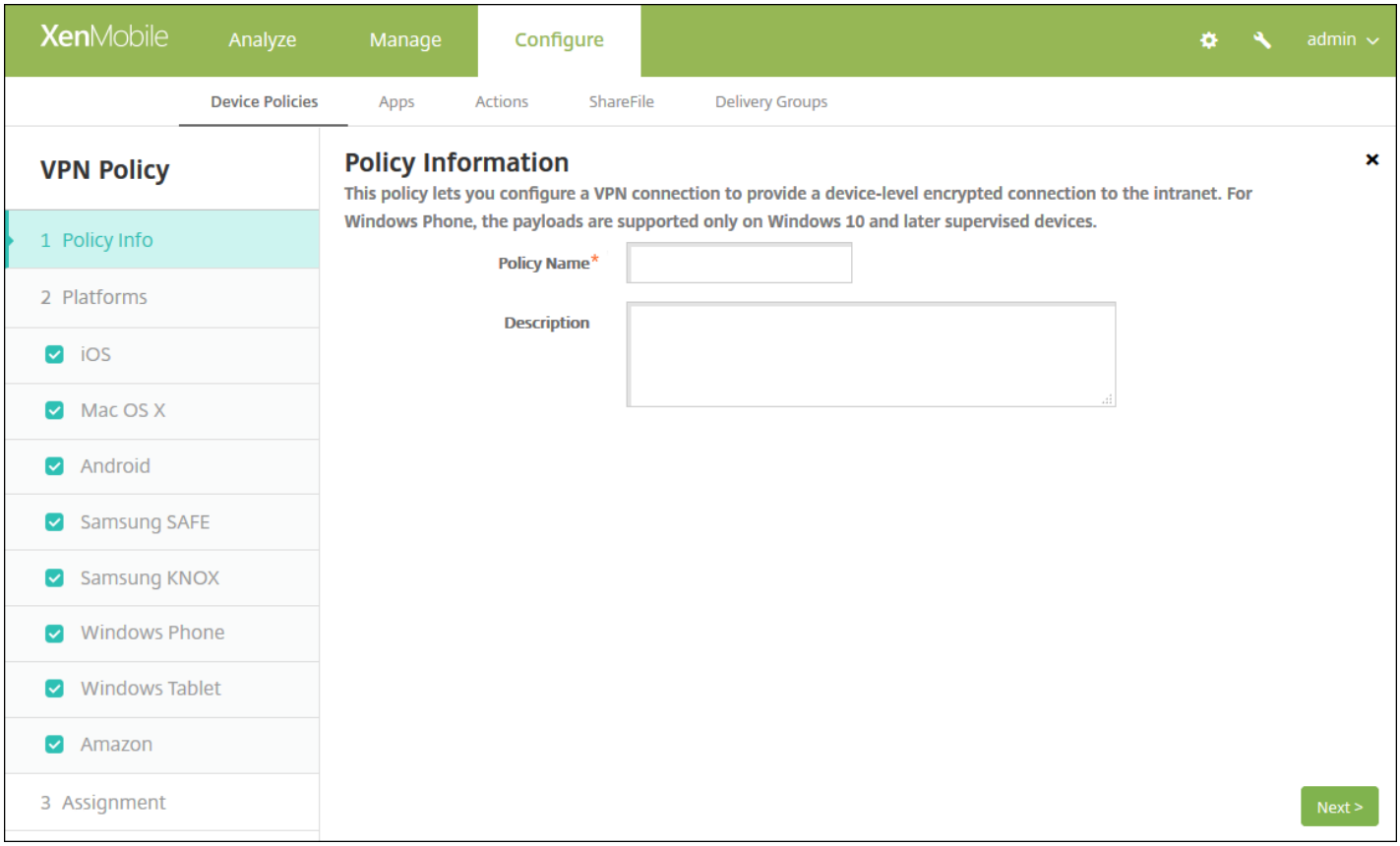
May 07, 2017

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:

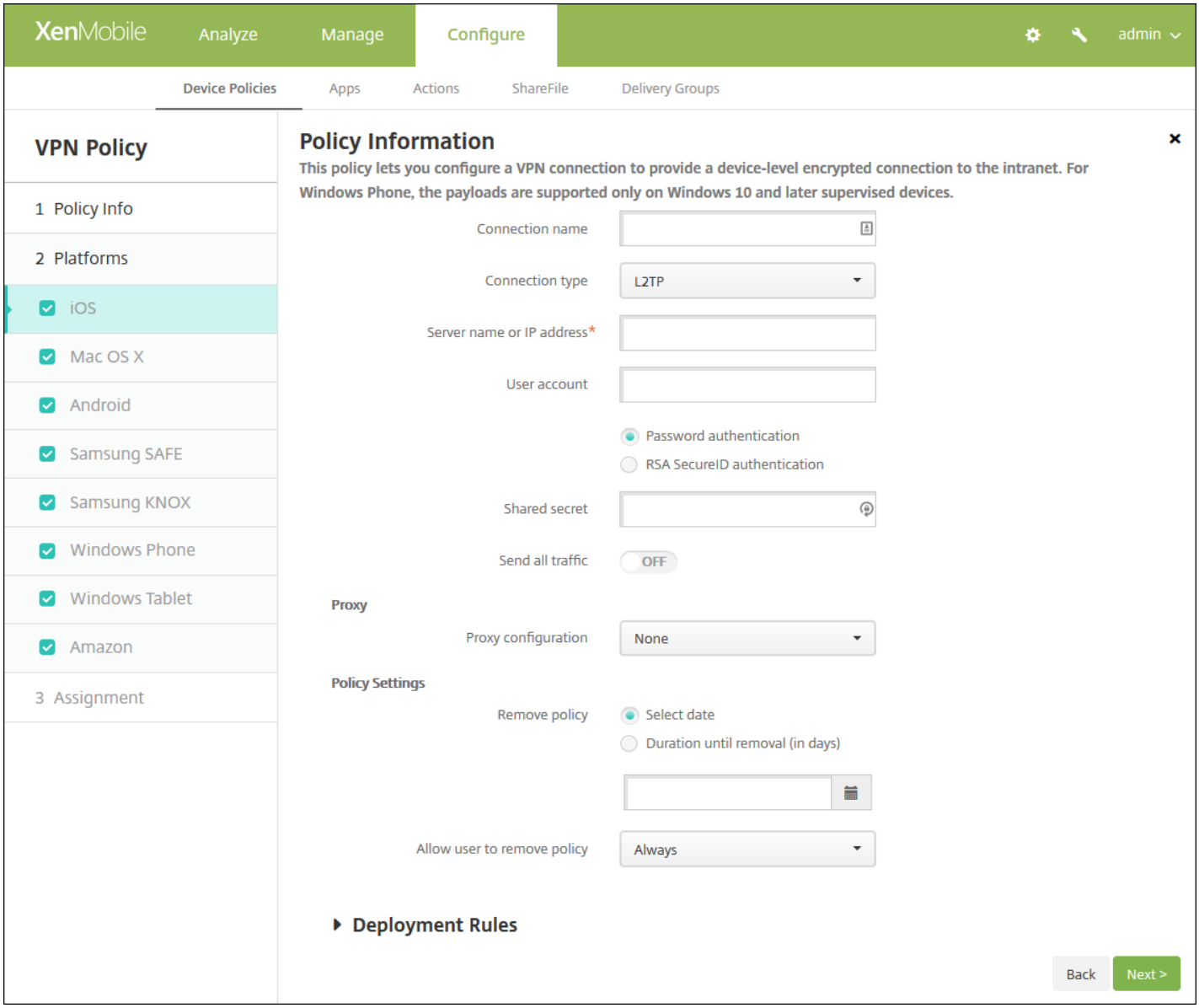
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva. Al aparecer la página **Platforms** de la directiva, 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 de protocolos IKEv2

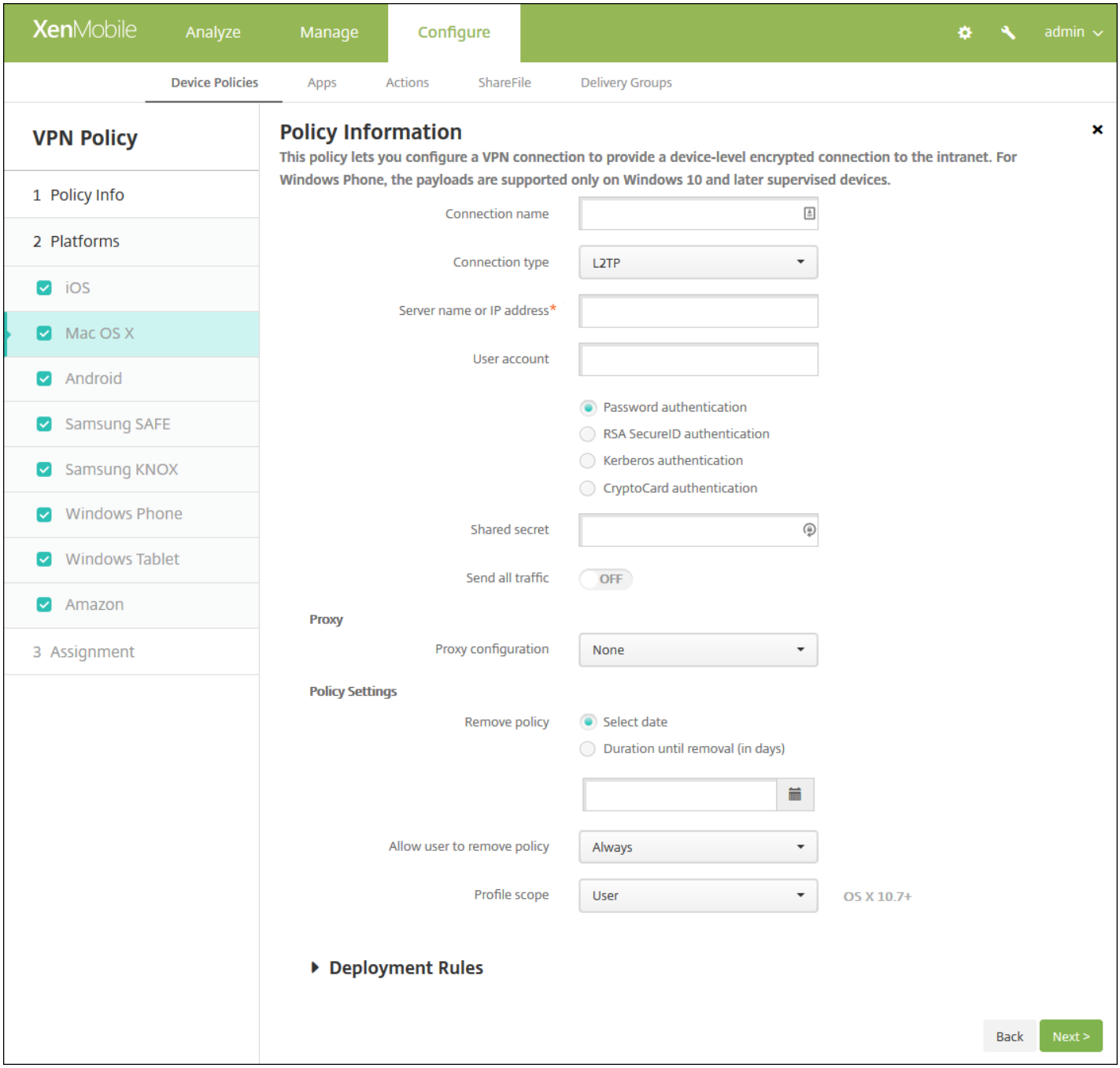
Configuración del protocolo VPN de Citrix

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 de host o la dirección IP 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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

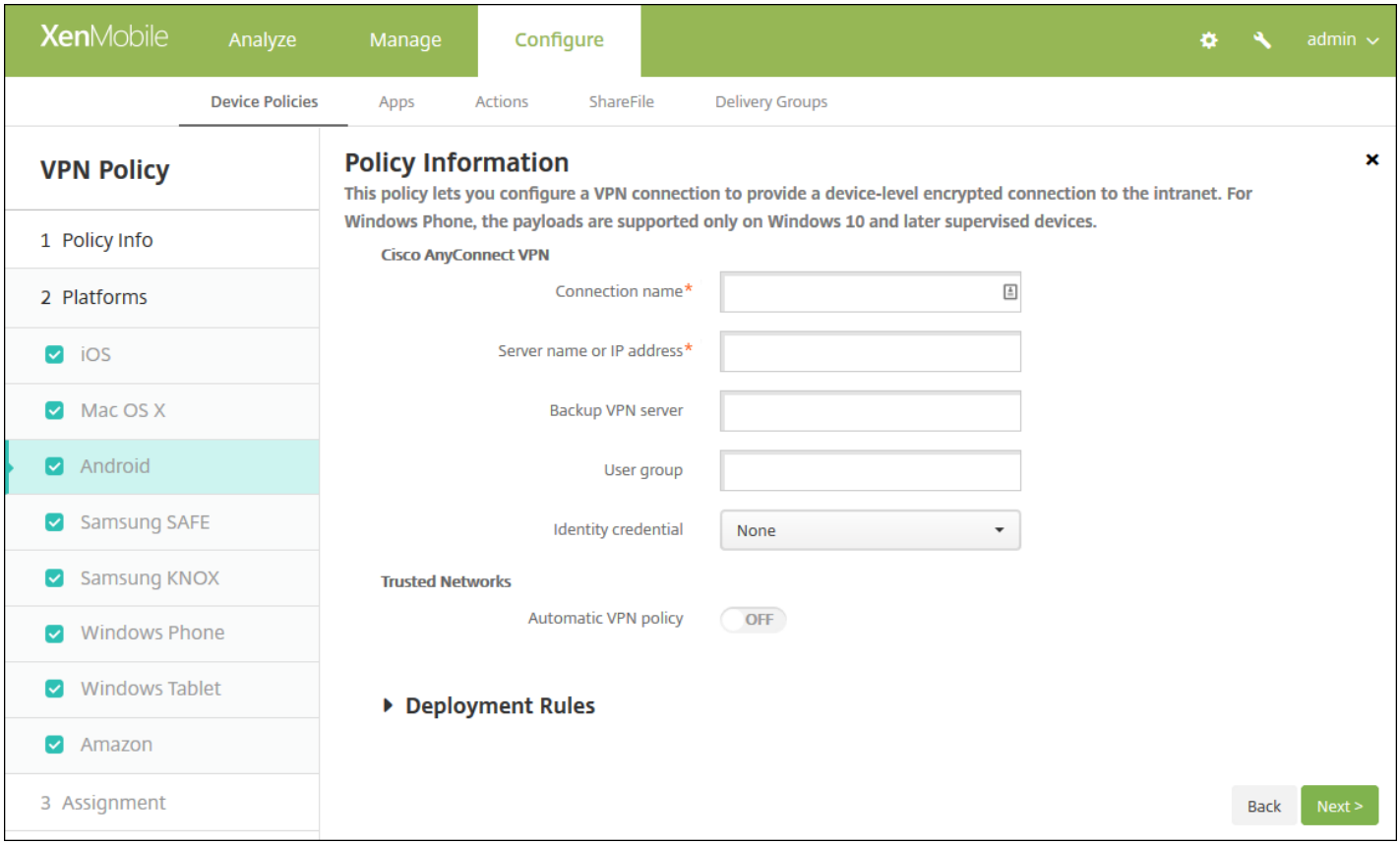
Configuración del protocolo VPN de Citrix

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 de host o la dirección IP 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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:

- **VPN de Cisco AnyConnect**
  - **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.
- **Redes de confianza**
  - **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:

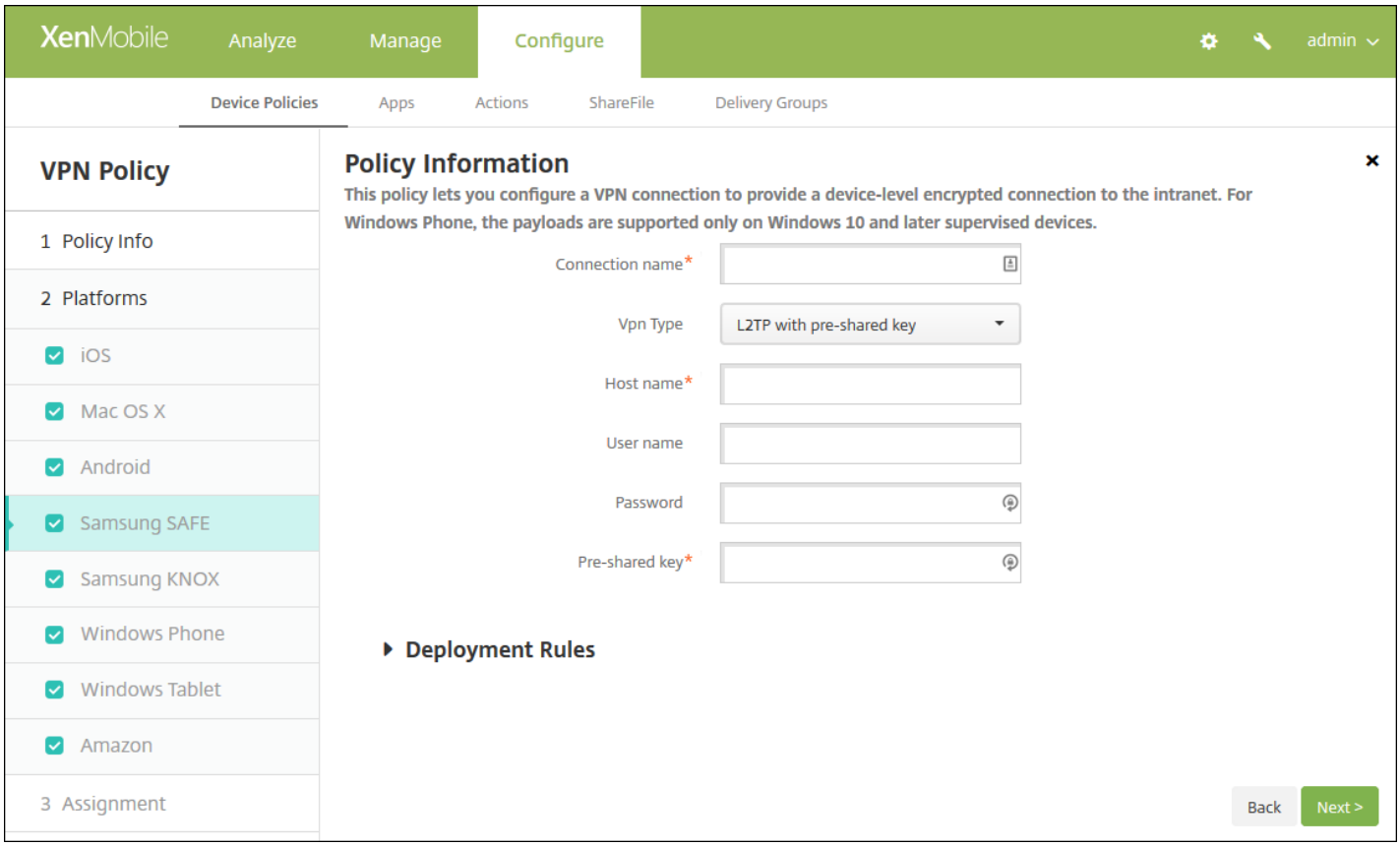
- **Connect**. El cliente inicia una conexión VPN en una red que no es de confianza.
- **Do Nothing**. El cliente inicia una conexión VPN en una red que no es de confianza. Esta opción inhabilita la opción Always-on VPN.

- **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 guardarlos, o bien en **Cancel** para descartarlos.

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

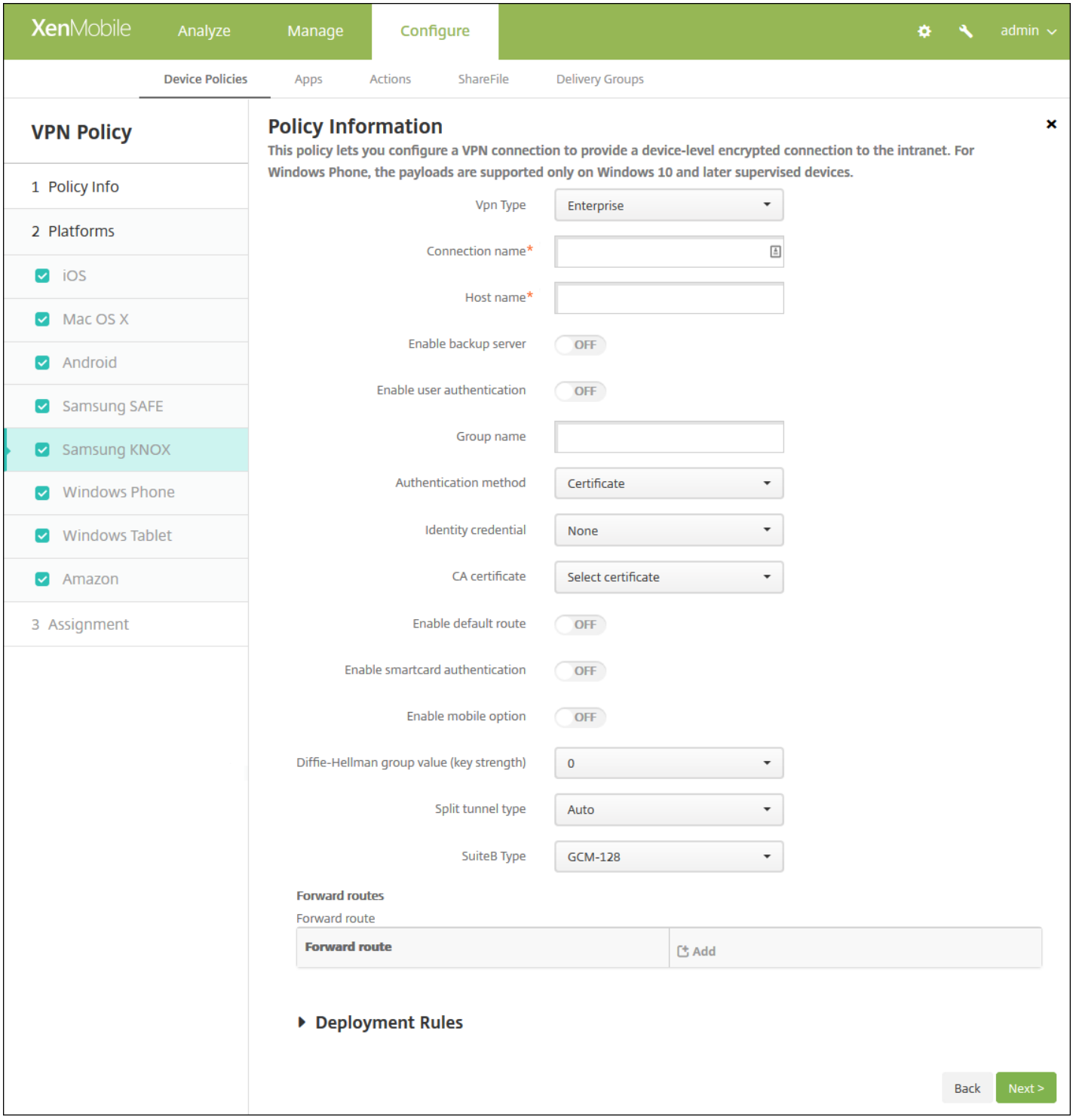
Configuración del protocolo L2TP con certificado

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:

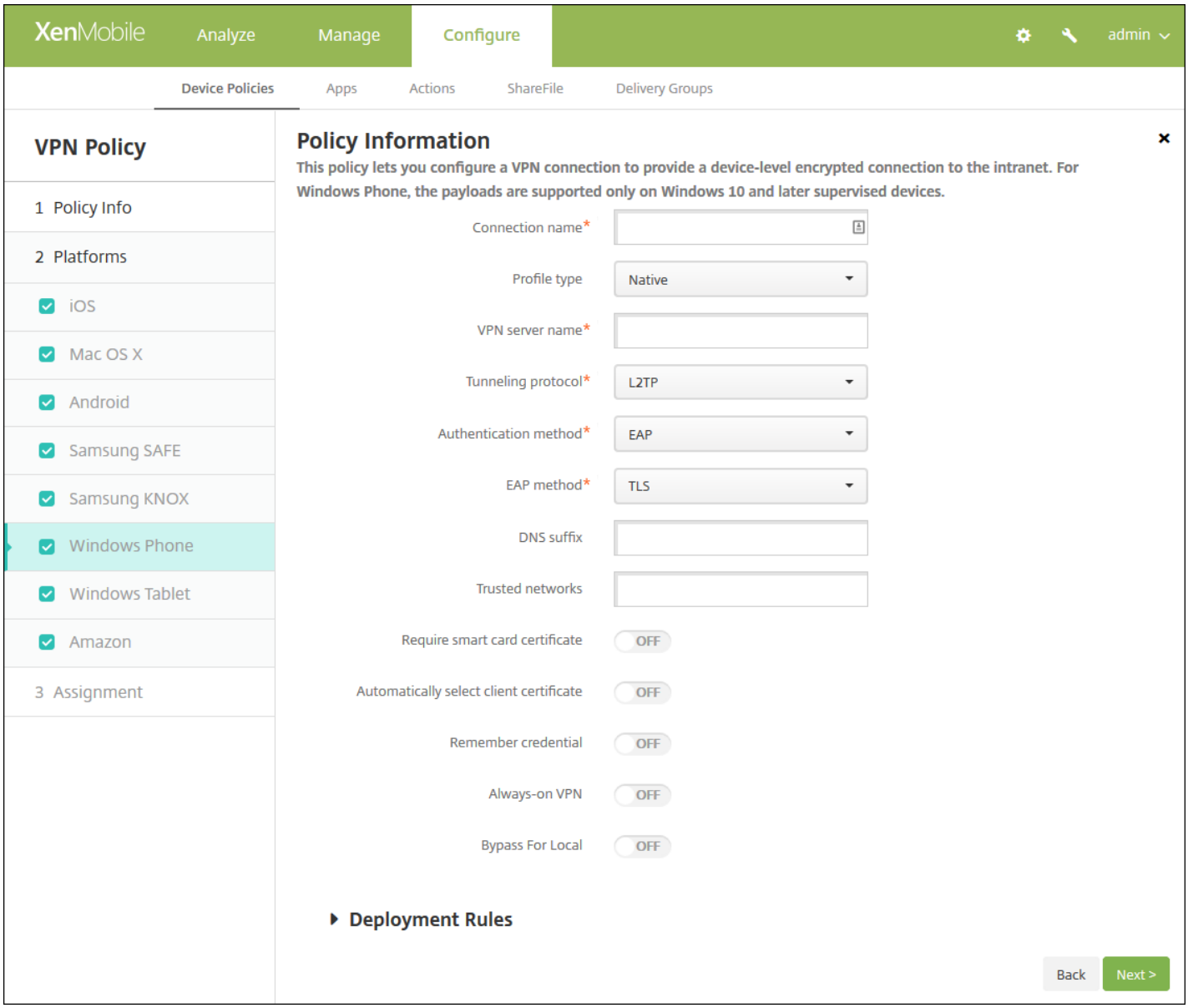
- **Vpn Type**. En la lista, haga clic en el tipo de conexión VPN a configurar, **Enterprise** (se aplica a las versiones KNOX anteriores a 2.0) o **Generic** (se aplica a KNOX 2.0 o versiones posteriores). El valor predeterminado es **Enterprise**.

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:

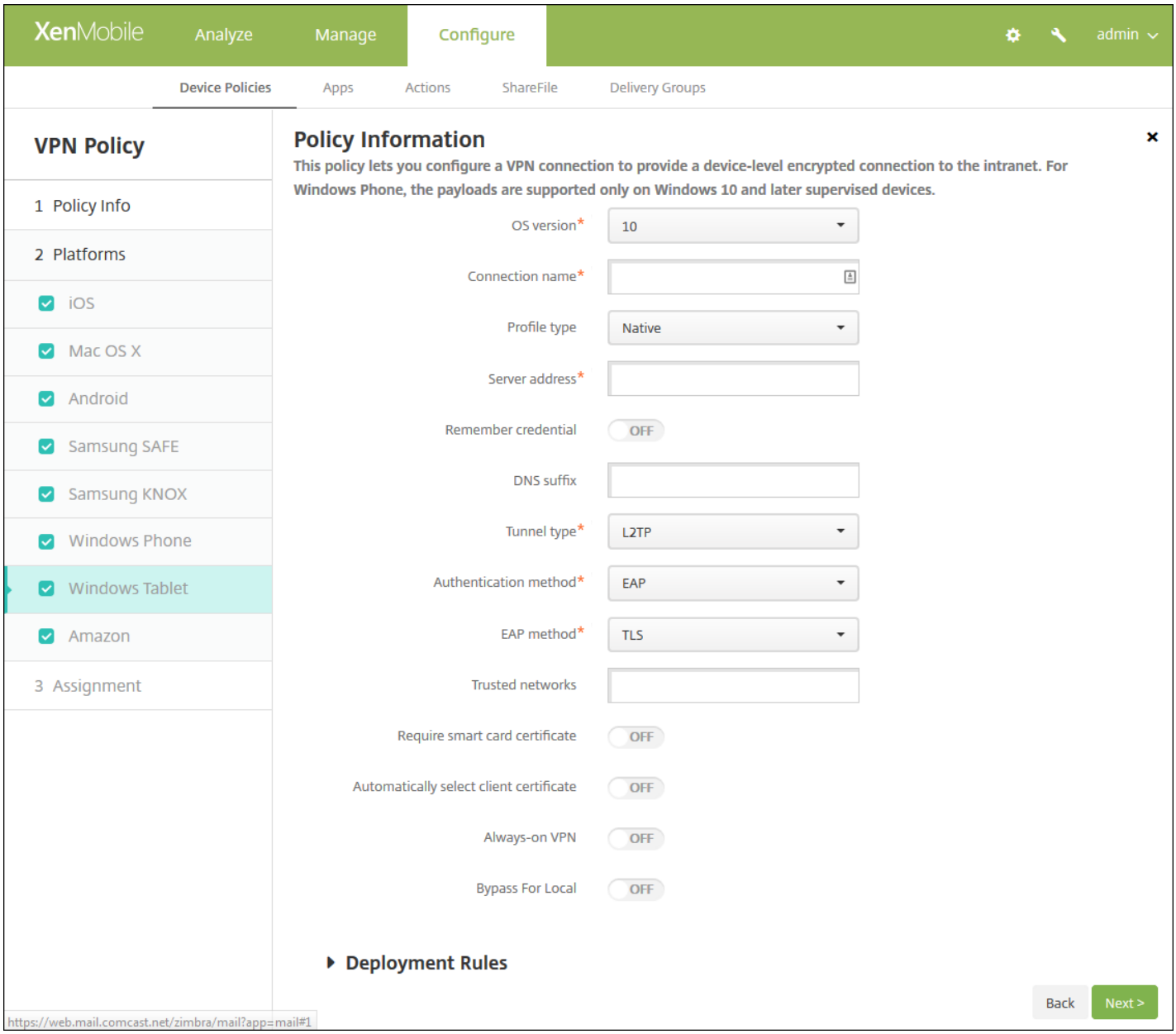
- **Connection name**. Escriba el nombre de la conexión. Este campo es obligatorio.
- **Profile type**. En la lista, haga clic en **Native** o **Plugin**. El valor predeterminado es **Native**. En los siguientes apartados, se describe la configuración de cada una de las opciones.
- **Configure Native 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 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 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.

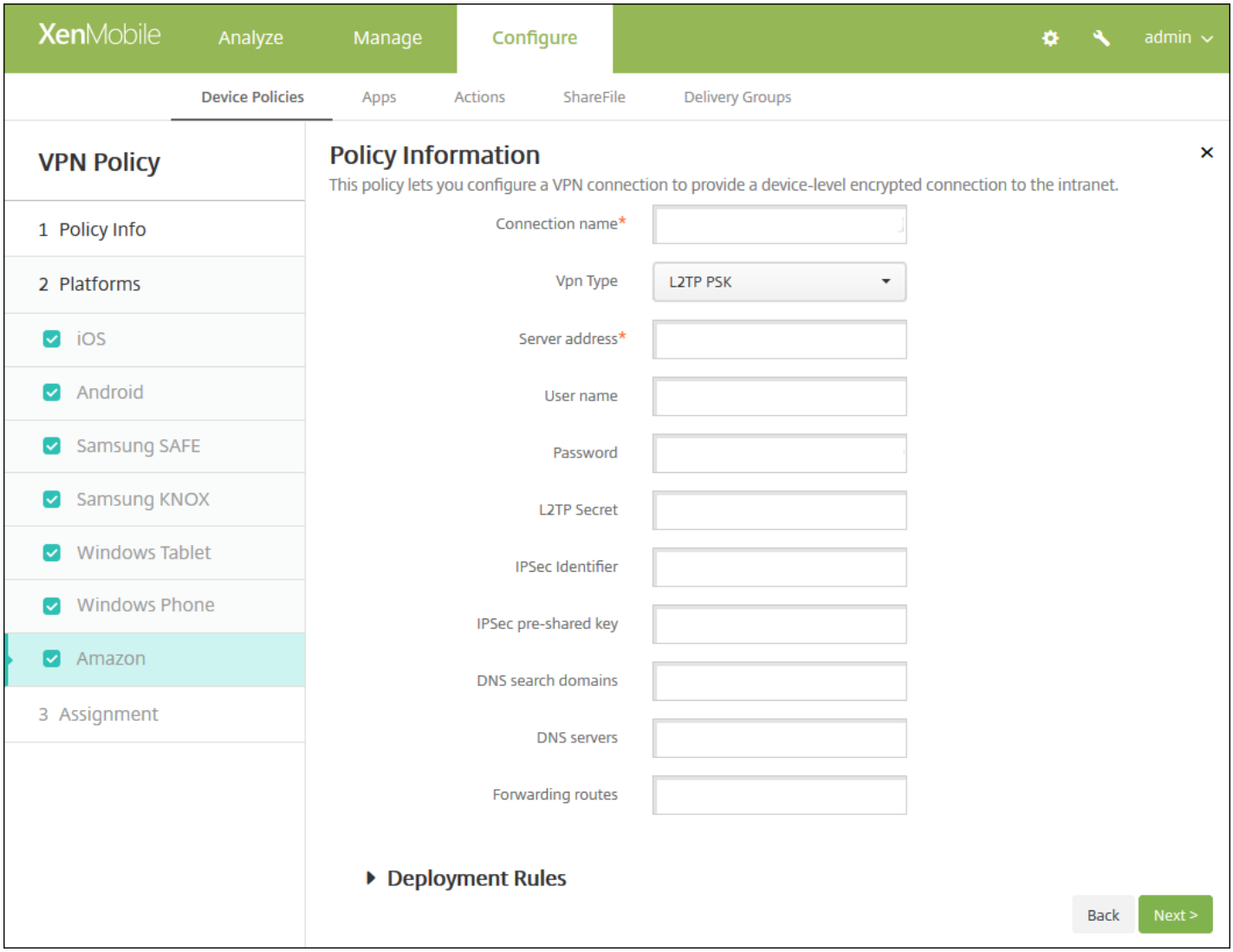
Configuración de los parámetros de tabletas Windows



Configure estos parámetros:

Configuración de los parámetros de Windows 10

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

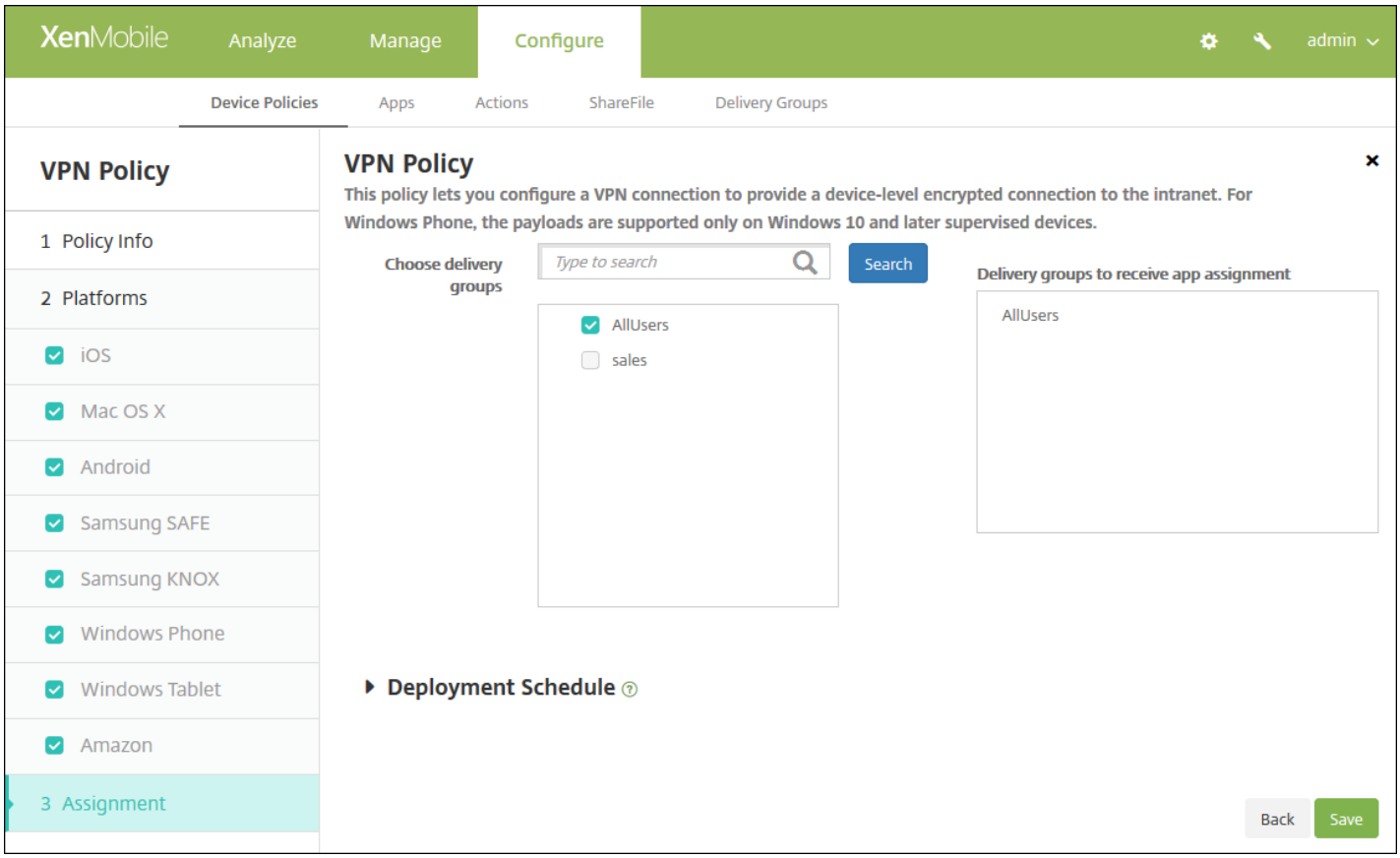
Configuración de los parámetros de RSA para AUTH de IPsec

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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota:

- Esta opción se aplica si se configura la clave de implementación en segundo plano para la programación desde **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

Feb 27, 2017

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 escritorio 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**.

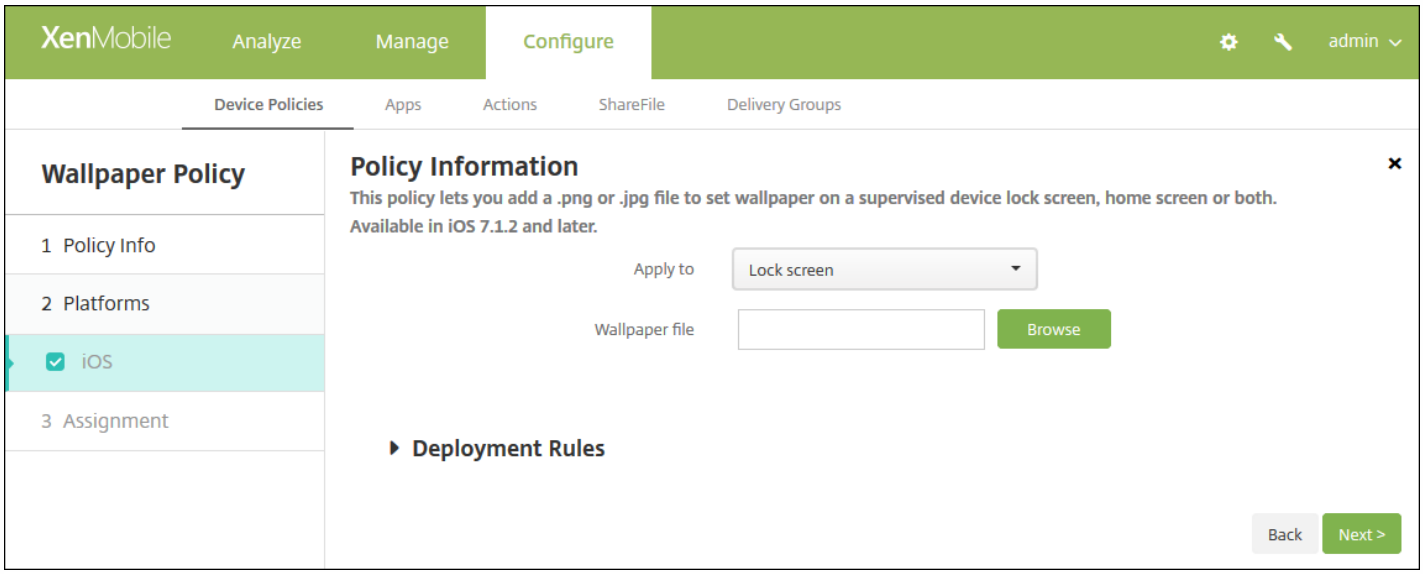
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.

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**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

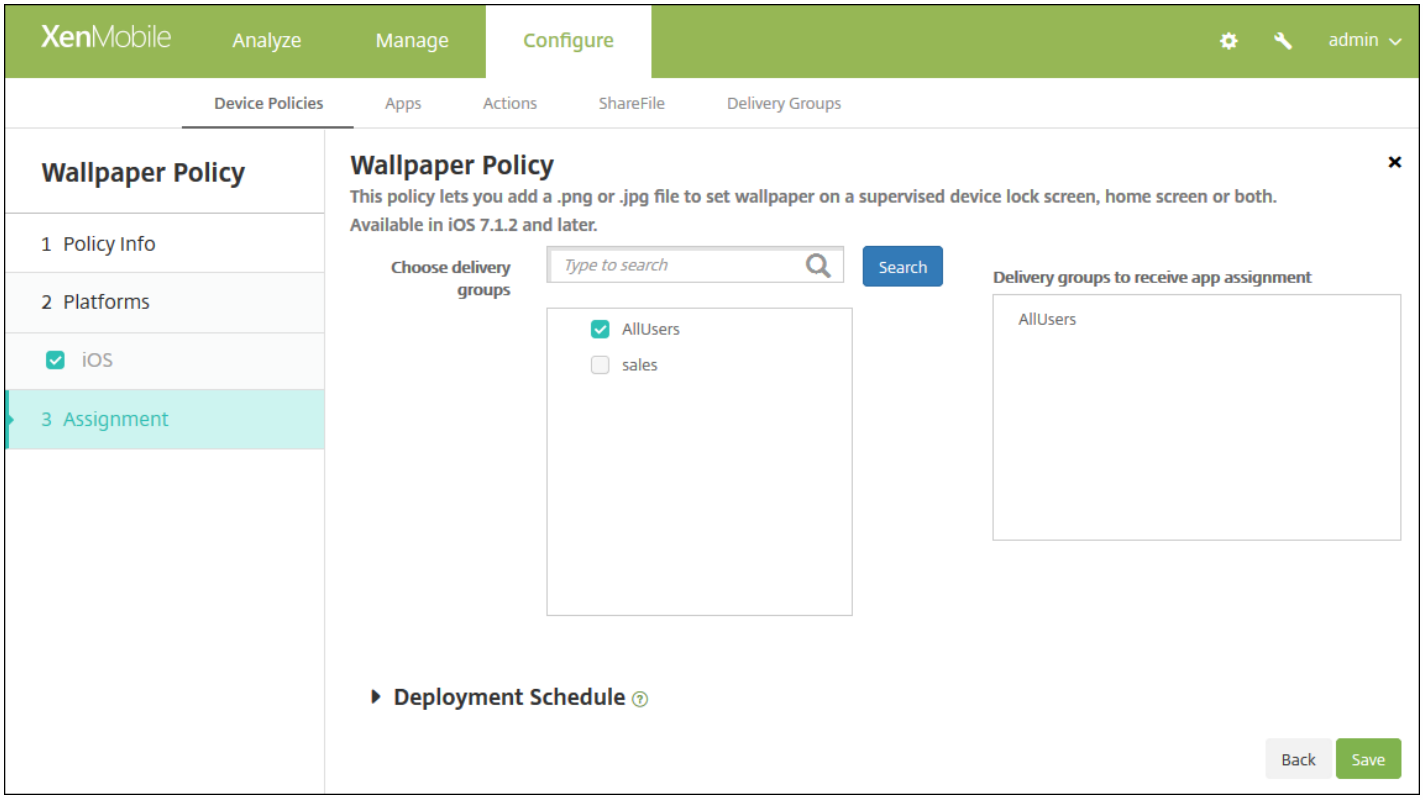


Configure estos parámetros:

- **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 de **Wallpaper Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para filtrar el contenido Web

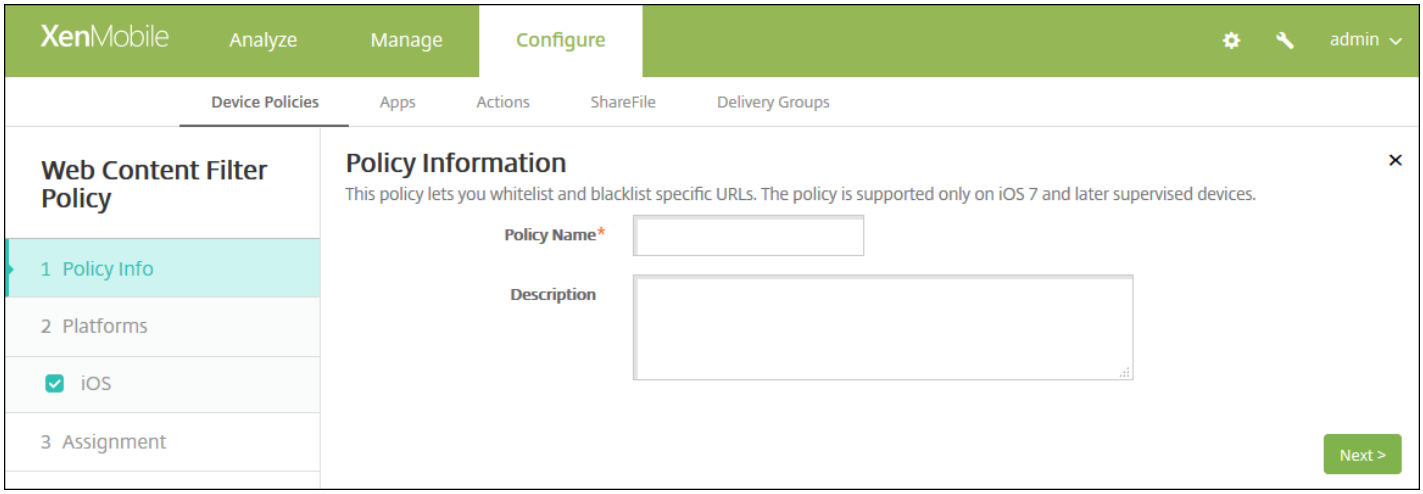
Feb 27, 2017

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**.

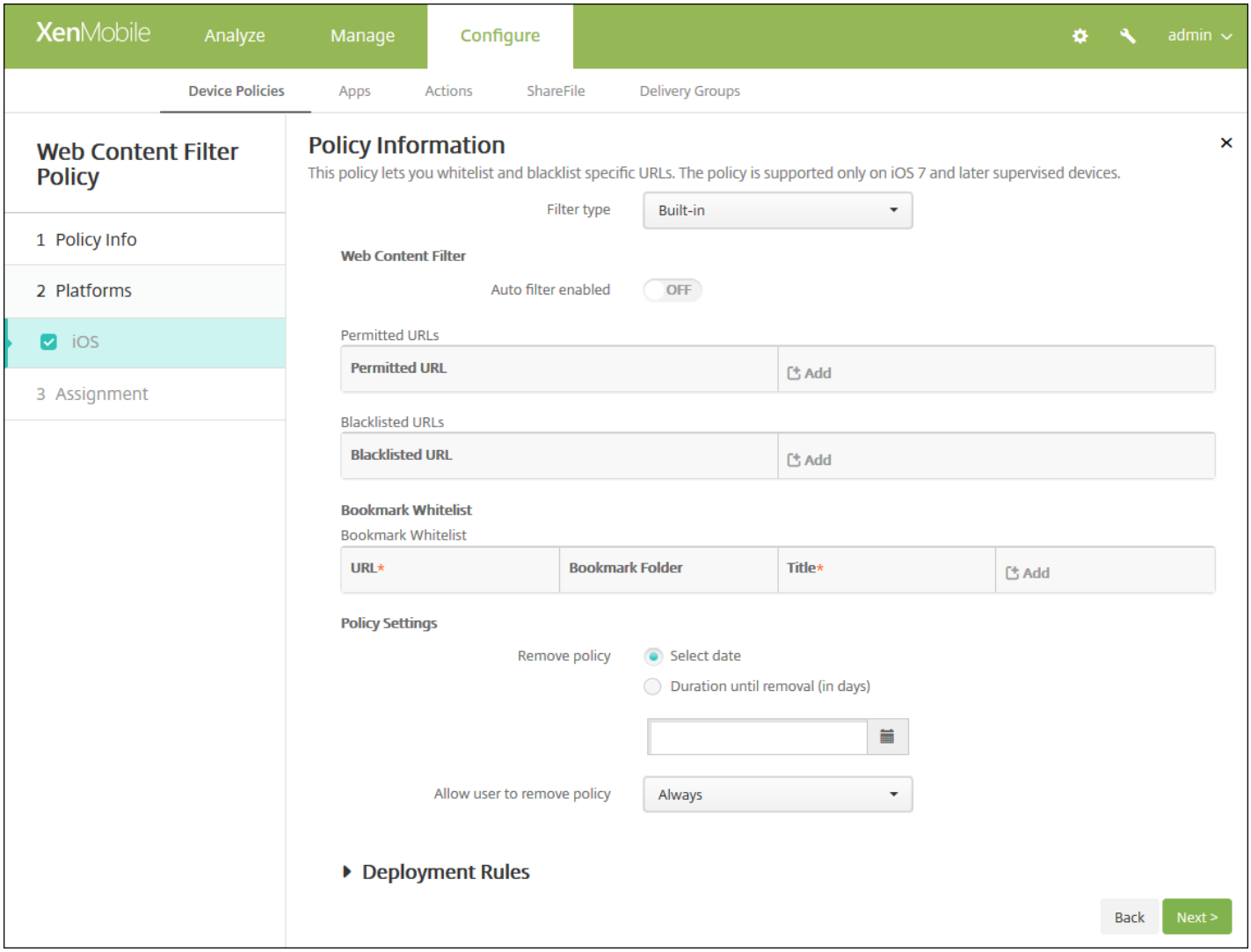
3. Haga clic en **More** y, a continuación, en el apartado **Security**, haga clic en **Web Content Filter**. Aparecerá la página **Web Content Filter Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **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 de la **plataforma iOS**.



6. Configure estos 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**.

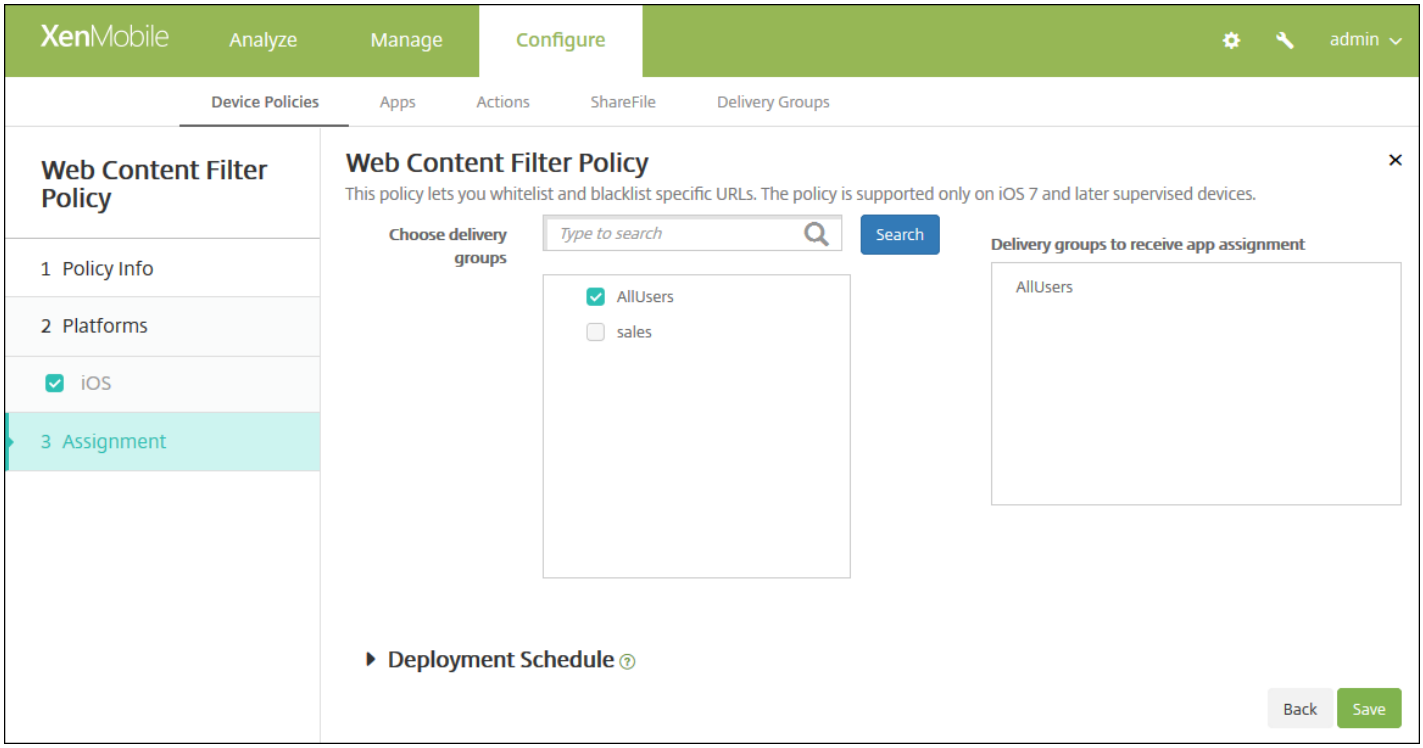
Configuración del tipo de filtro integrado

Configuración del tipo de filtro plug-in

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación de **Web Content Filter Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo sobre clips Web

Feb 27, 2017

Puede colocar accesos directos, o clips Web, para que los sitios Web aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede indicar iconos propios 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

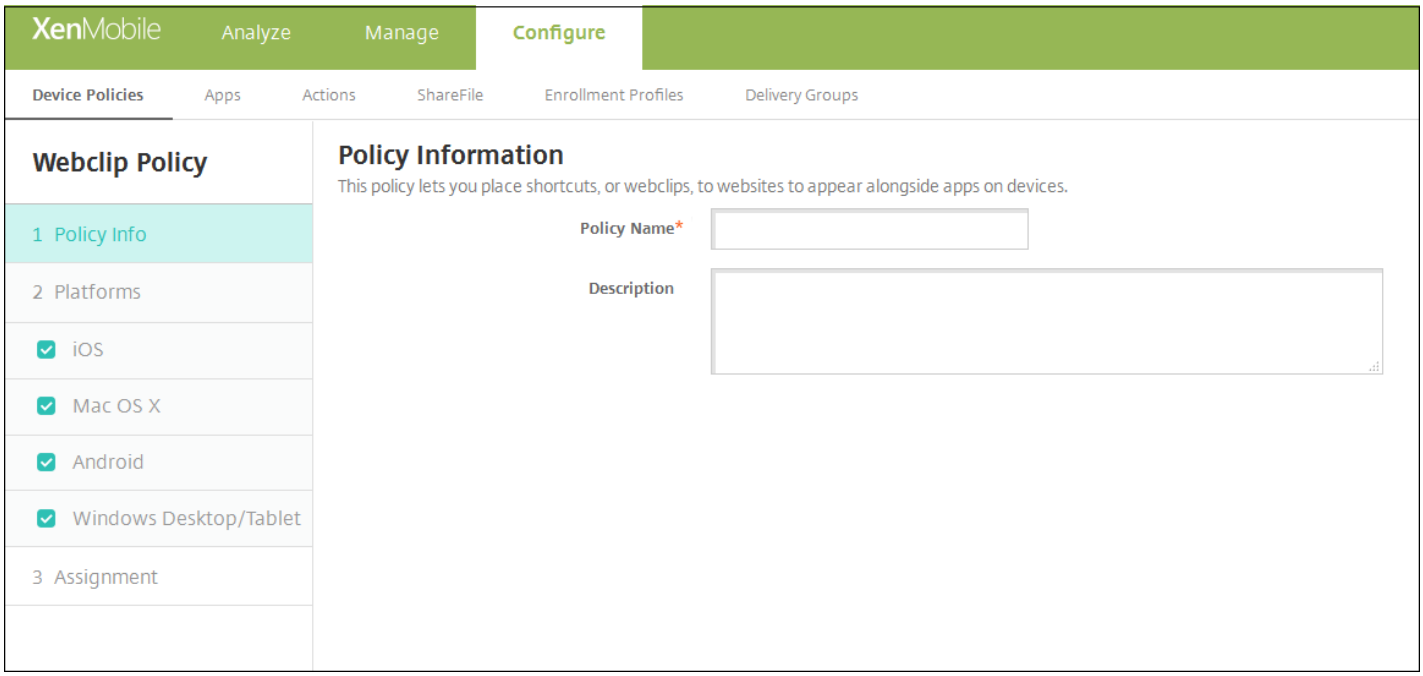
Configuración de Android

Configuración de escritorios 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. Expanda **More** y, a continuación, en **Apps**, haga clic en **Webclip**. Aparece la página **Webclip Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

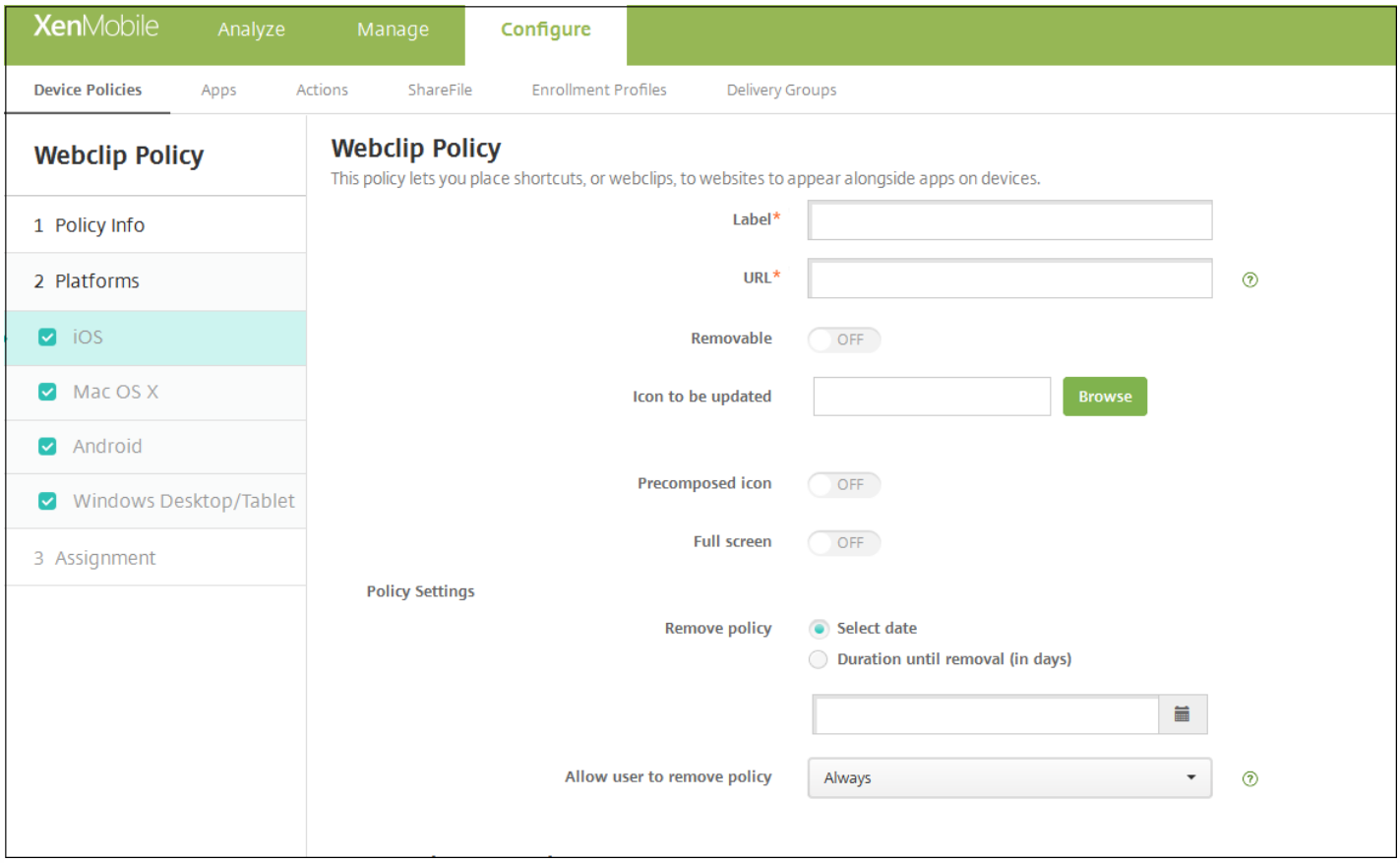
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

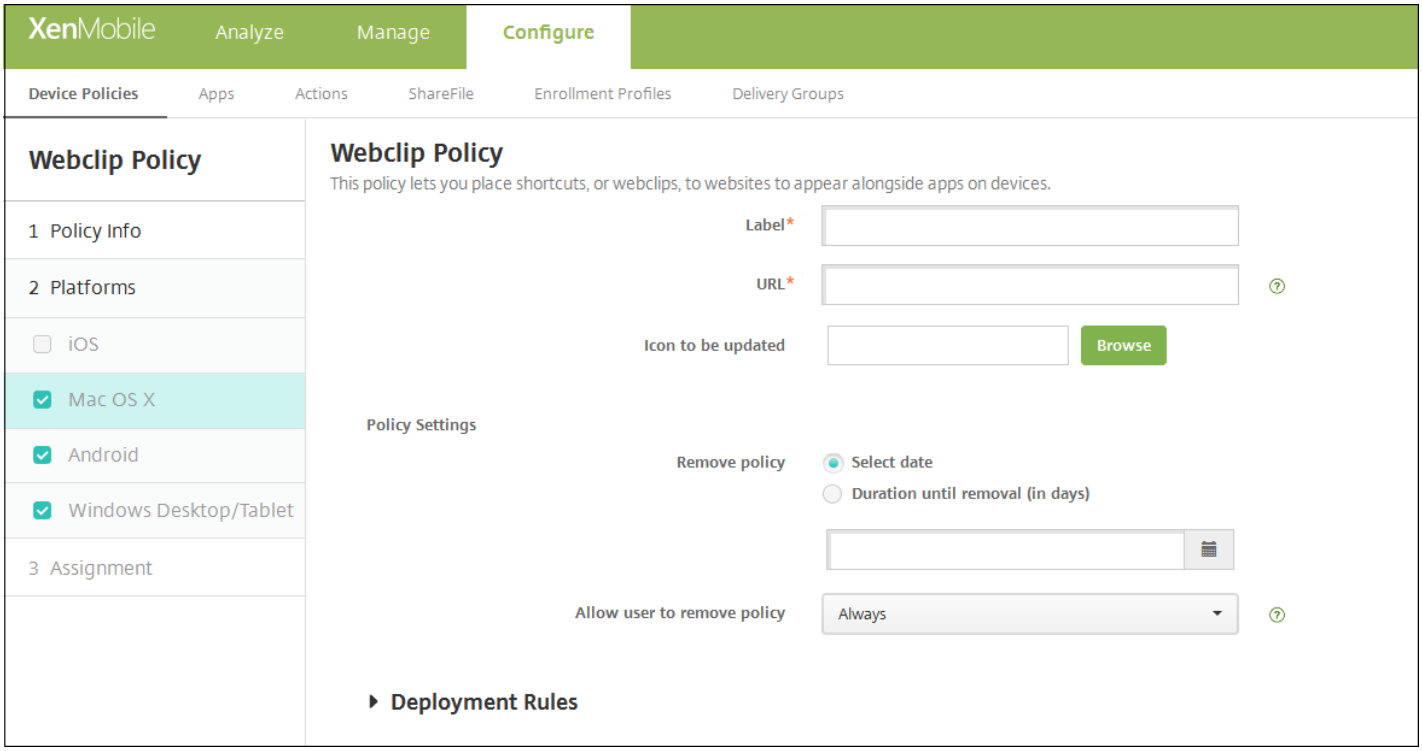
Configuración de los parámetros de iOS



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 que se utilizará para el clip Web. Para ello, haga clic en **Browse** para ir a 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 **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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.

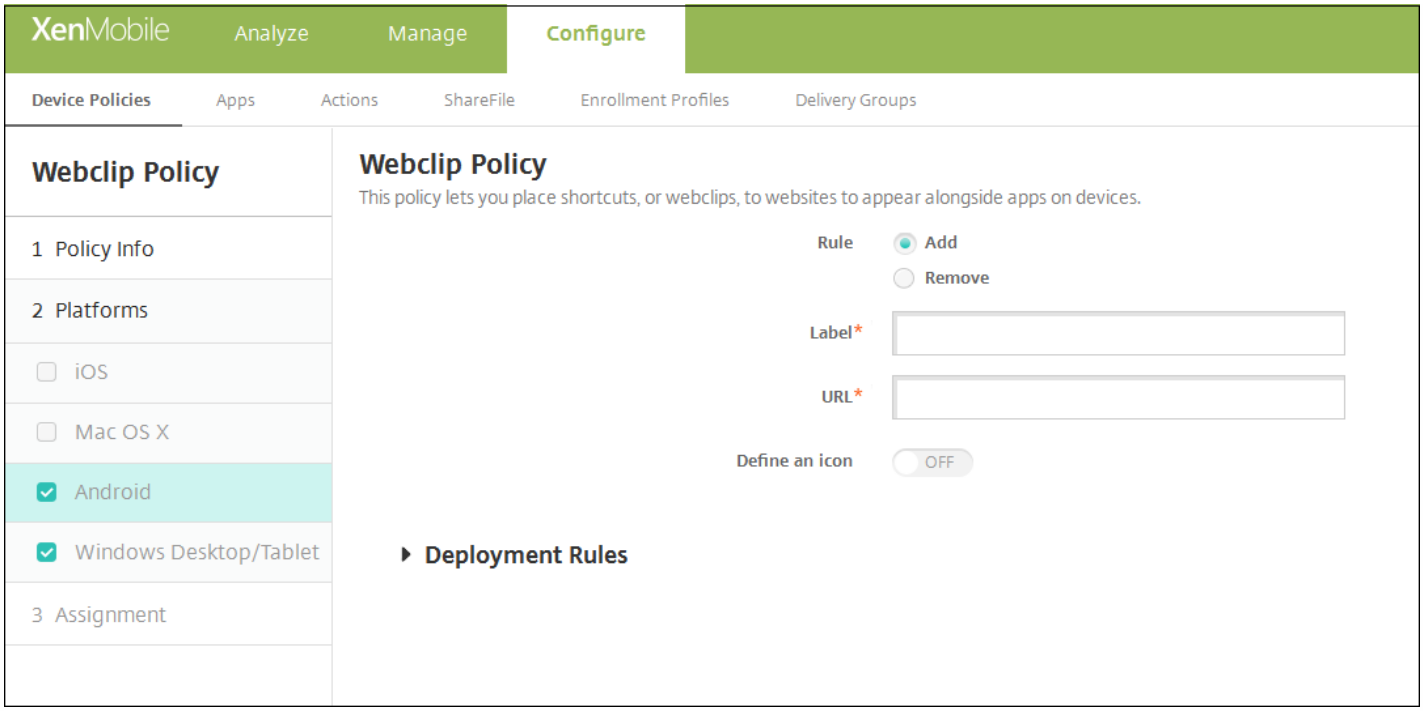
Configuración de los parámetros de Mac OS X



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 que se utilizará para el clip Web. Para ello, haga clic en Browse para ir a la ubicación del archivo.
- **Configuraciones de directivas**
  - 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 list**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, introduzca 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.

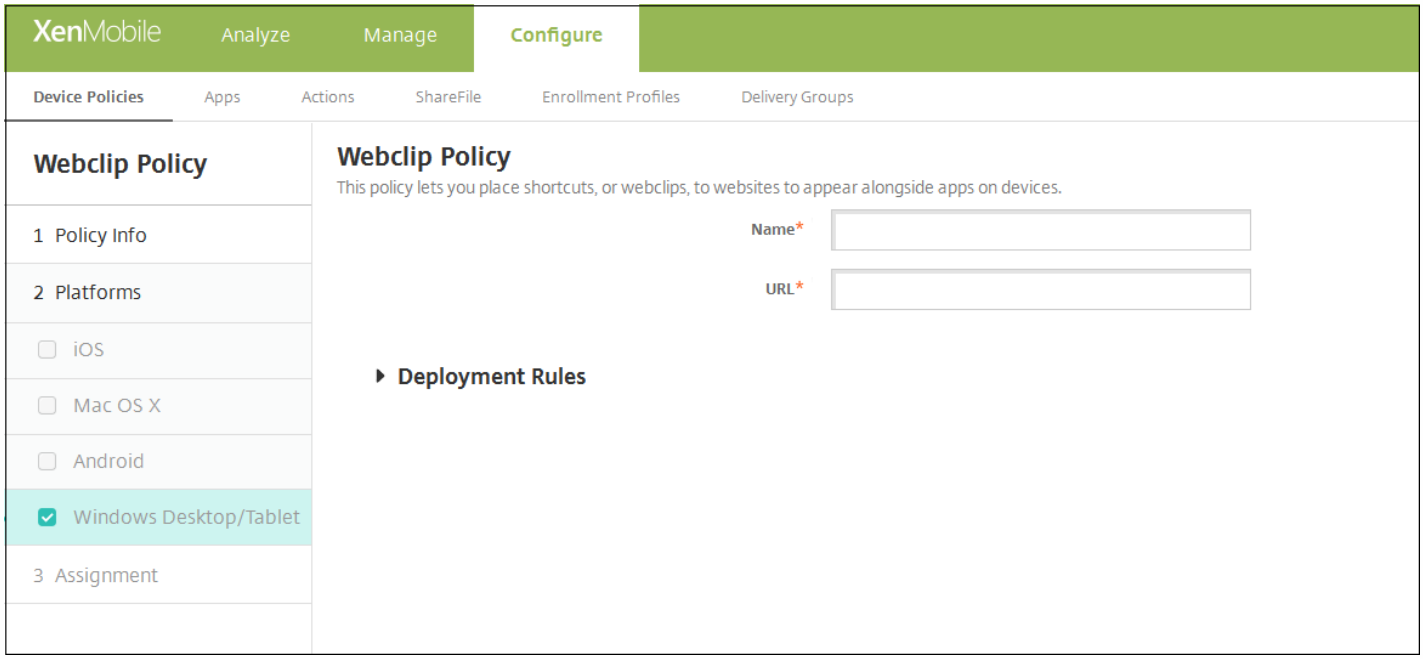
Configuración de los parámetros de Android



Configure estos parámetros:

- **Rule**. Seleccione si esta directiva agrega o quita clips 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 escritorios o tabletas Windows

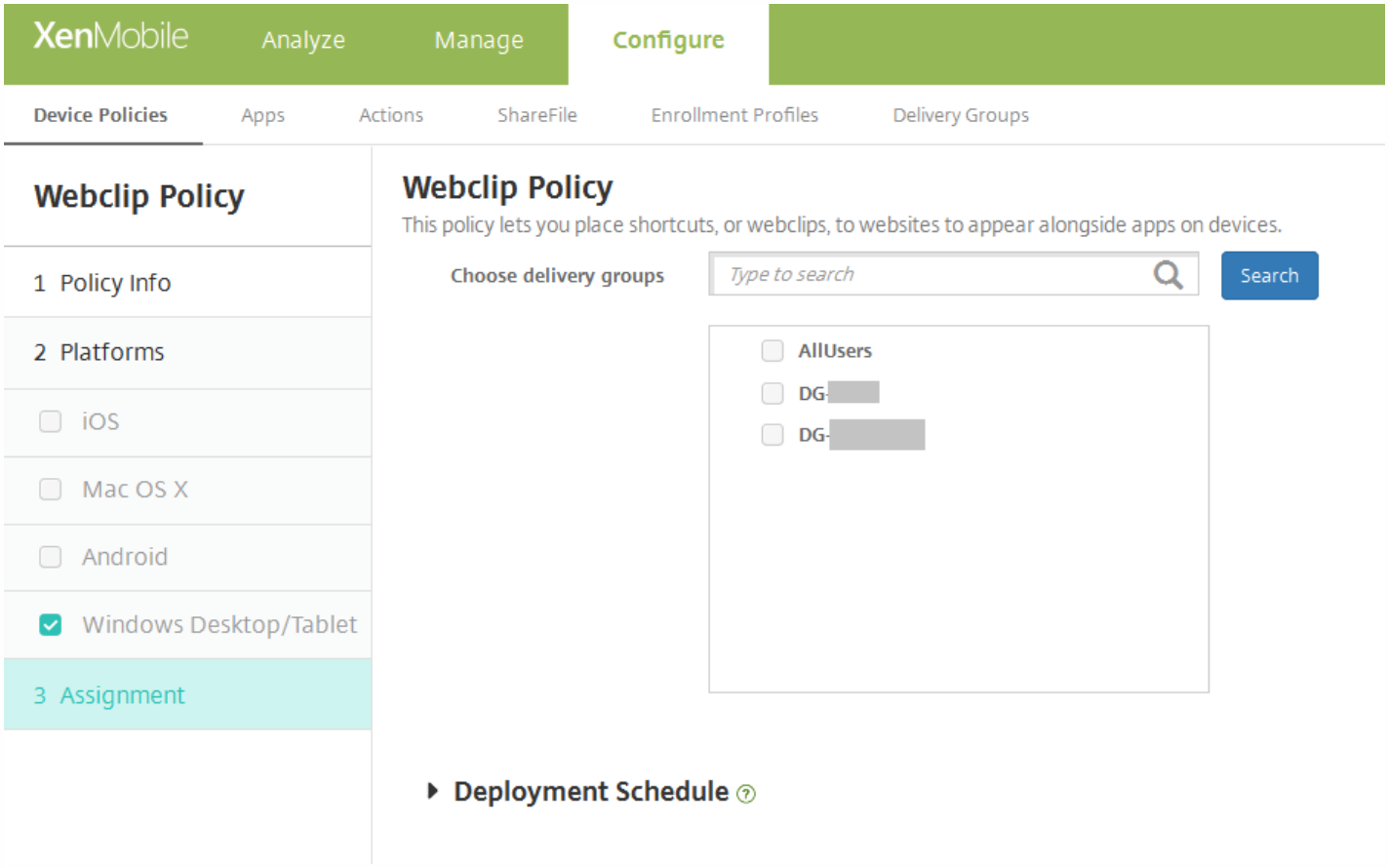


Configure estos parámetros:

- **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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 redes Wi-Fi

Apr 24, 2017

En XenMobile, puede crear o modificar las directivas de Wi-Fi desde la página **Configure > Device Policies** de la consola de XenMobile. Las directivas de redes Wi-Fi permiten administrar el modo en que los usuarios conectan sus dispositivos a las redes inalámbricas. Para ello, deberá definir los siguientes elementos:

- Tipos y nombres de red
- Directivas de autenticación y seguridad
- Uso de servidores proxy
- Otros datos relacionados con redes WiFi

Puede configurar parámetros de red inalámbrica WiFi para los usuarios de las plataformas siguientes. 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 (incluidos los dispositivos habilitados para Android for Work)

Configuración de Windows Phone

Configuración de escritorios y tabletas Windows

Important

Antes de crear una directiva, debe:

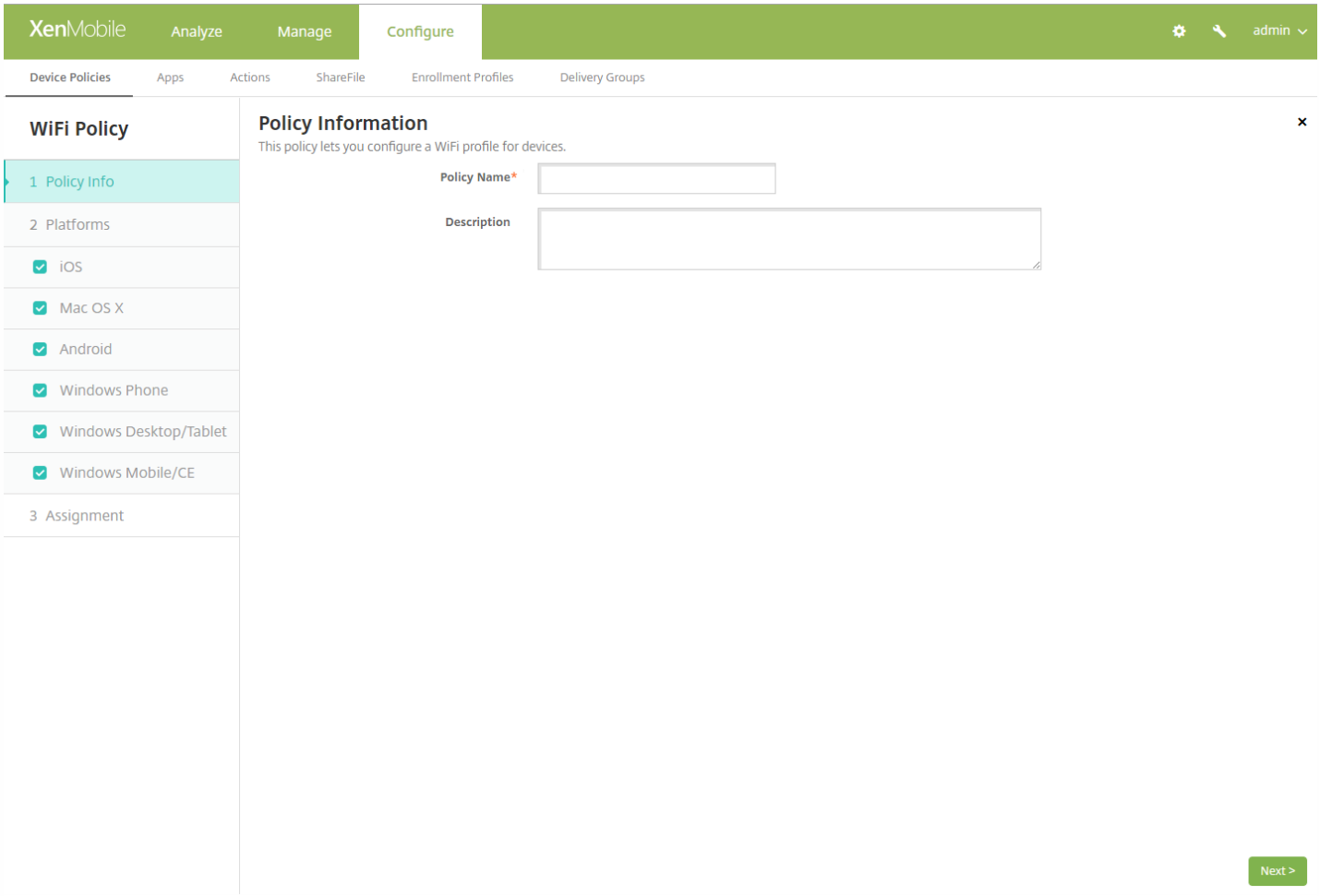
- Crear los grupos de entrega que se van a utilizar.
- Saber el nombre y el tipo de red.
- Conocer los tipos de seguridad o de autenticación que se van a utilizar.
- Conocer cualquier información del servidor proxy que pueda necesitar.
- Instalar los certificados de CA necesarios.
- Disponer de todas las claves compartidas necesarias.
- Crear una entidad PKI para la autenticación basada en certificados.
- Configurar proveedores de credenciales.

Para obtener más información, consulte Autenticación y sus apartados.

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:

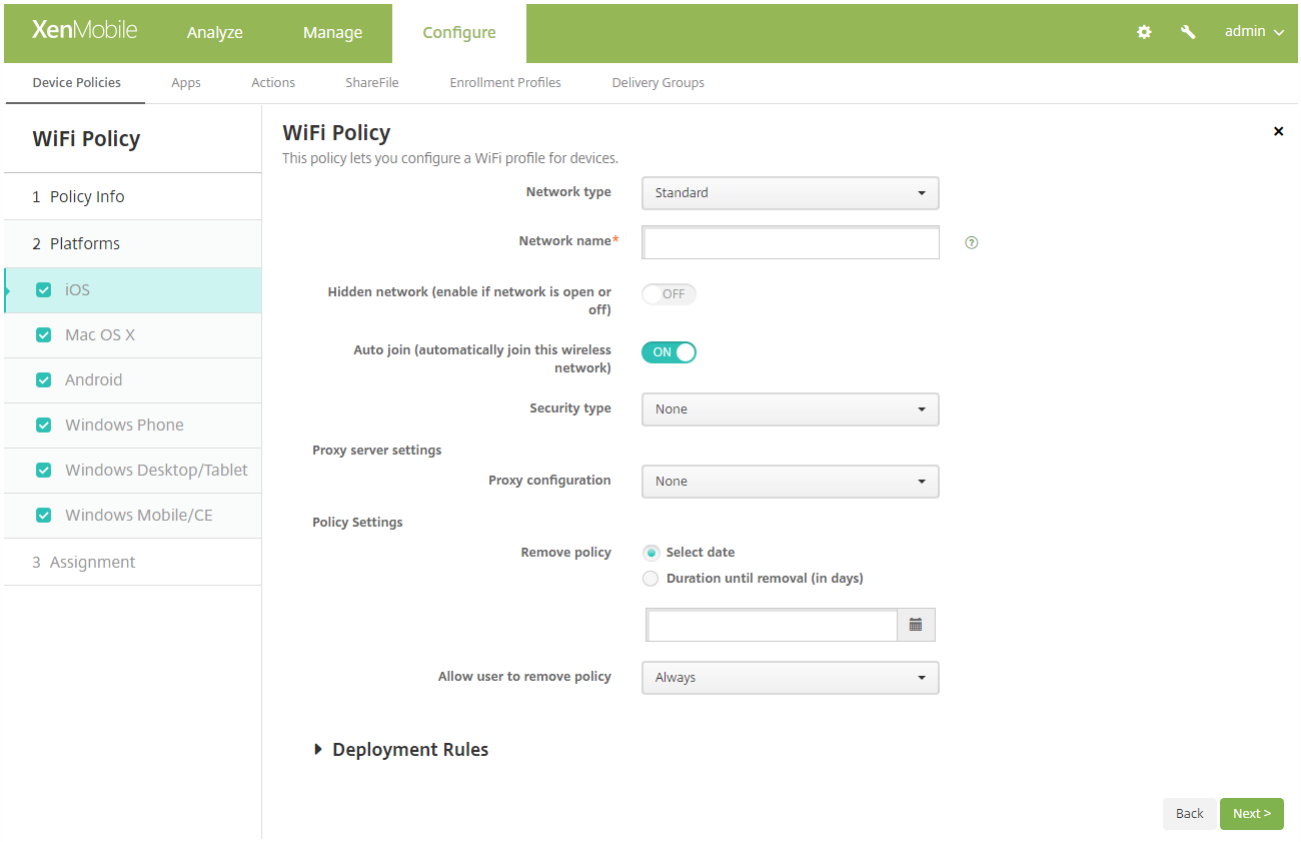
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

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 o WPA2 Enterprise. Para la versión más reciente de Windows 10, usar WPA2 Enterprise requiere que se configure SCEP. Así, XenMobile puede enviar el certificado a los dispositivos para autenticarse en el servidor WiFi. Para configurar SCEP, vaya a la página Distribution de **Settings > Credential Providers**. Para obtener más información, consulte Proveedores de credenciales.
  - Cualquiera (Enterprise)

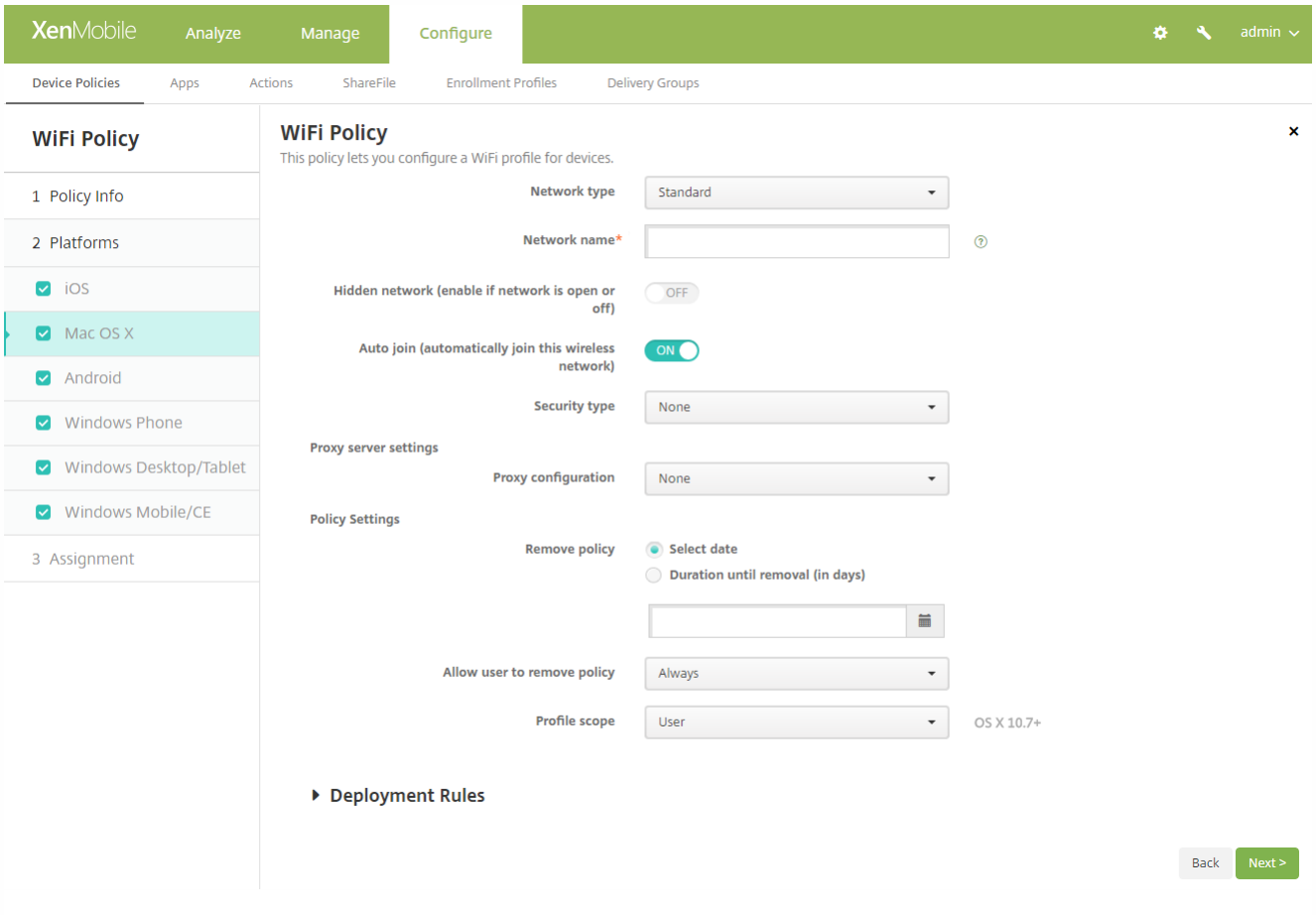
  En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

WPA, WPA Personal, Any (personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise)

- **Parámetros del servidor proxy**
  - **Proxy configuration**. En la lista, elija **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 de host o la dirección IP 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**. Elija si 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.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, elija **Select date** o **Duration until removal (in days)**.
  - Si elige **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy list**, elija **Always**, **Password required** o **Never**.
  - Si elige **Password required**, junto a **Removal password**, introduzca 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.

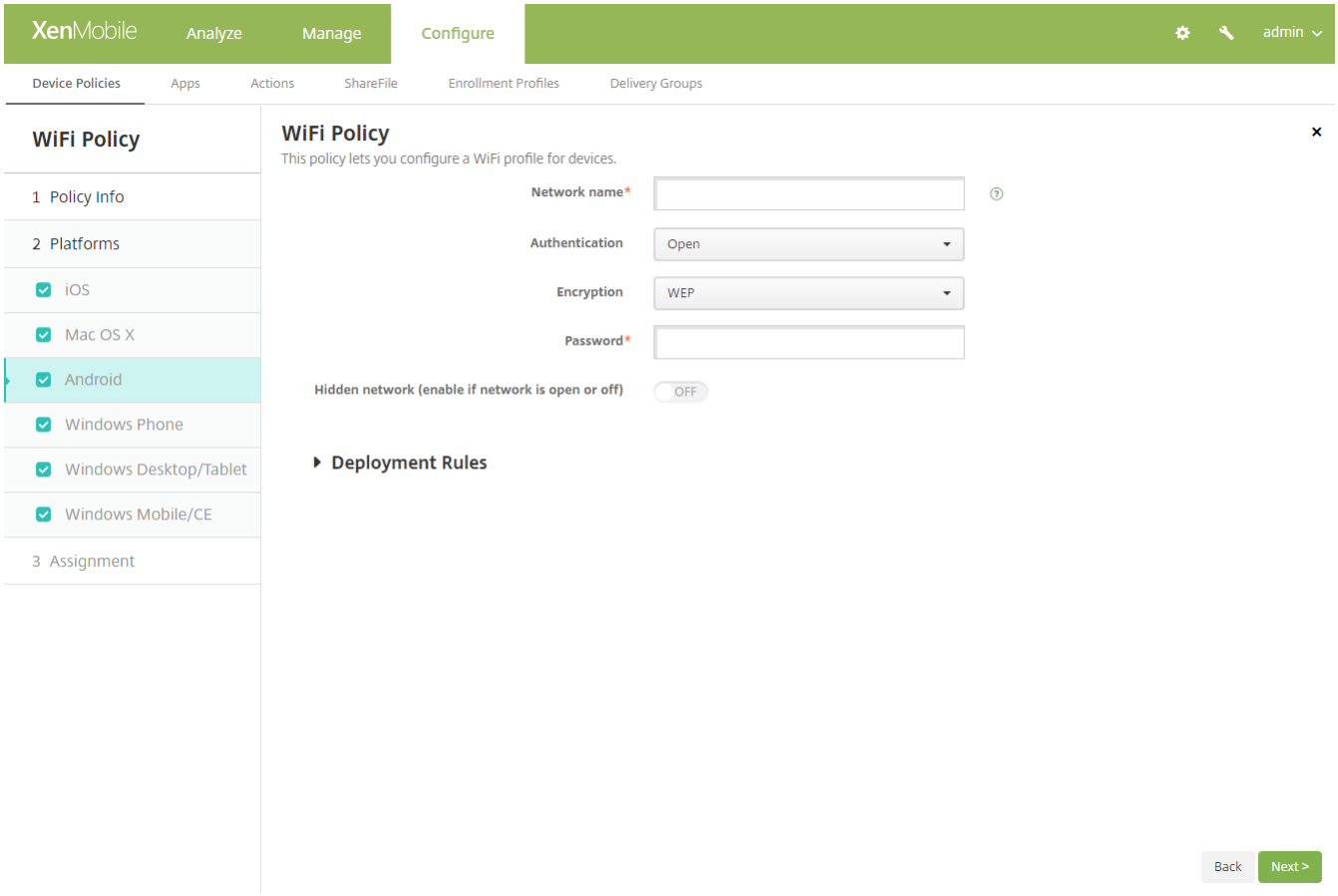
WPA, WPA Personal, WPA 2 Personal, Cualquiera (Personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise)

- **Use as a Login Window configuration**. Elija 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, elija **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 de host o la dirección IP 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**. Elija si 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.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, elija **Select date** o **Duration until removal (in days)**.

- Si elige **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy list**, elija **Always**, **Password required** o **Never**.
- Si elige **Password required**, junto a **Removal password**, introduzca la contraseña en cuestión.
- Junto a **Profile scope**, elija **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, elija el tipo de seguridad que se va a utilizar en la conexión WiFi.
  - 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.

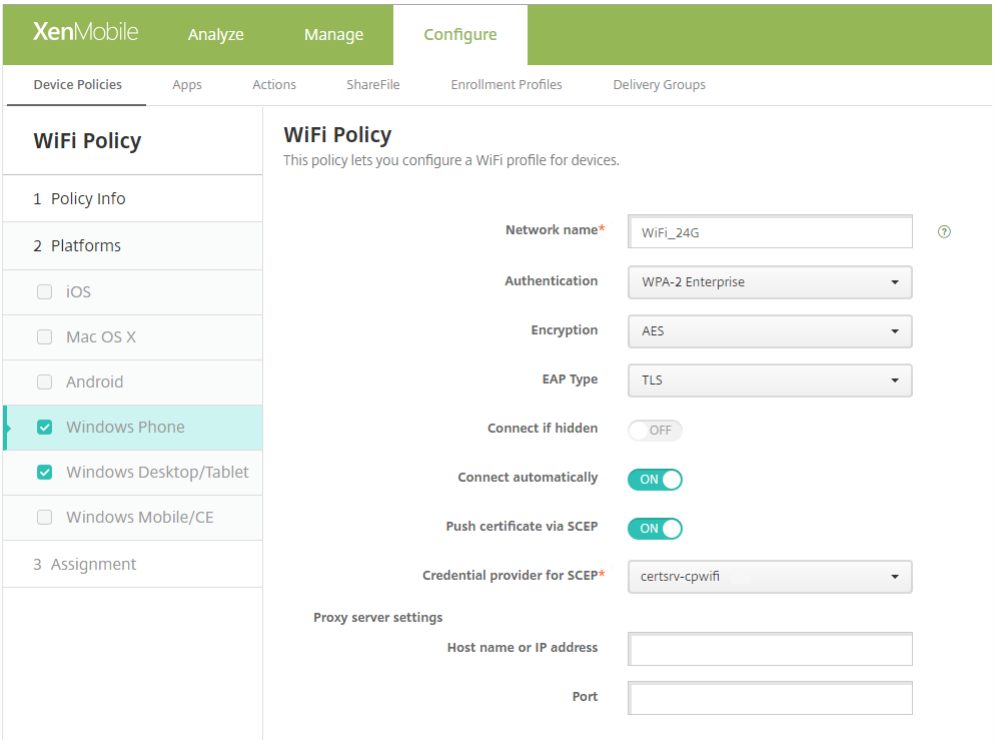
Abierta, Compartida

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, elija el tipo de seguridad que se va a utilizar en la conexión WiFi.
  - Abierta
  - WPA personal
  - WPA2 personal
  - WPA-2 Enterprise. Para la versión más reciente de Windows 10, usar WPA-2 Enterprise requiere que se configure SCEP. Así, XenMobile puede enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página **Distribution** de **Settings > Credential Providers**. Para obtener más información, consulte Proveedores de credenciales.

    En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

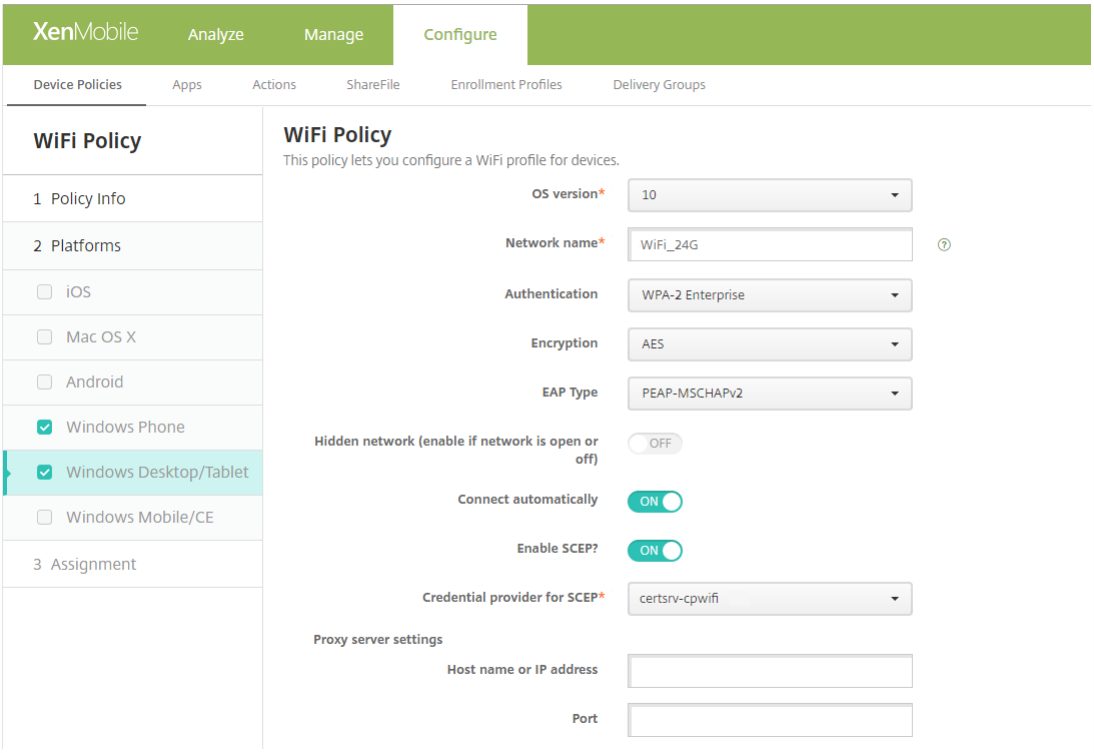
Abierta

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 escritorios o tabletas Windows



Configure los siguientes parámetros:

Configuración de Windows 10

- **Authentication**. En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión WiFi.
  - Abierta
  - WPA personal
  - WPA2 personal
  - WPA de empresa
  - WPA-2 Enterprise. Para la versión más reciente de Windows 10, usar WPA-2 Enterprise requiere que se configure SCEP. Así, XenMobile puede enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página **Distribution** de **Settings > Credential Providers**. Para obtener más información, consulte Proveedores de credenciales.

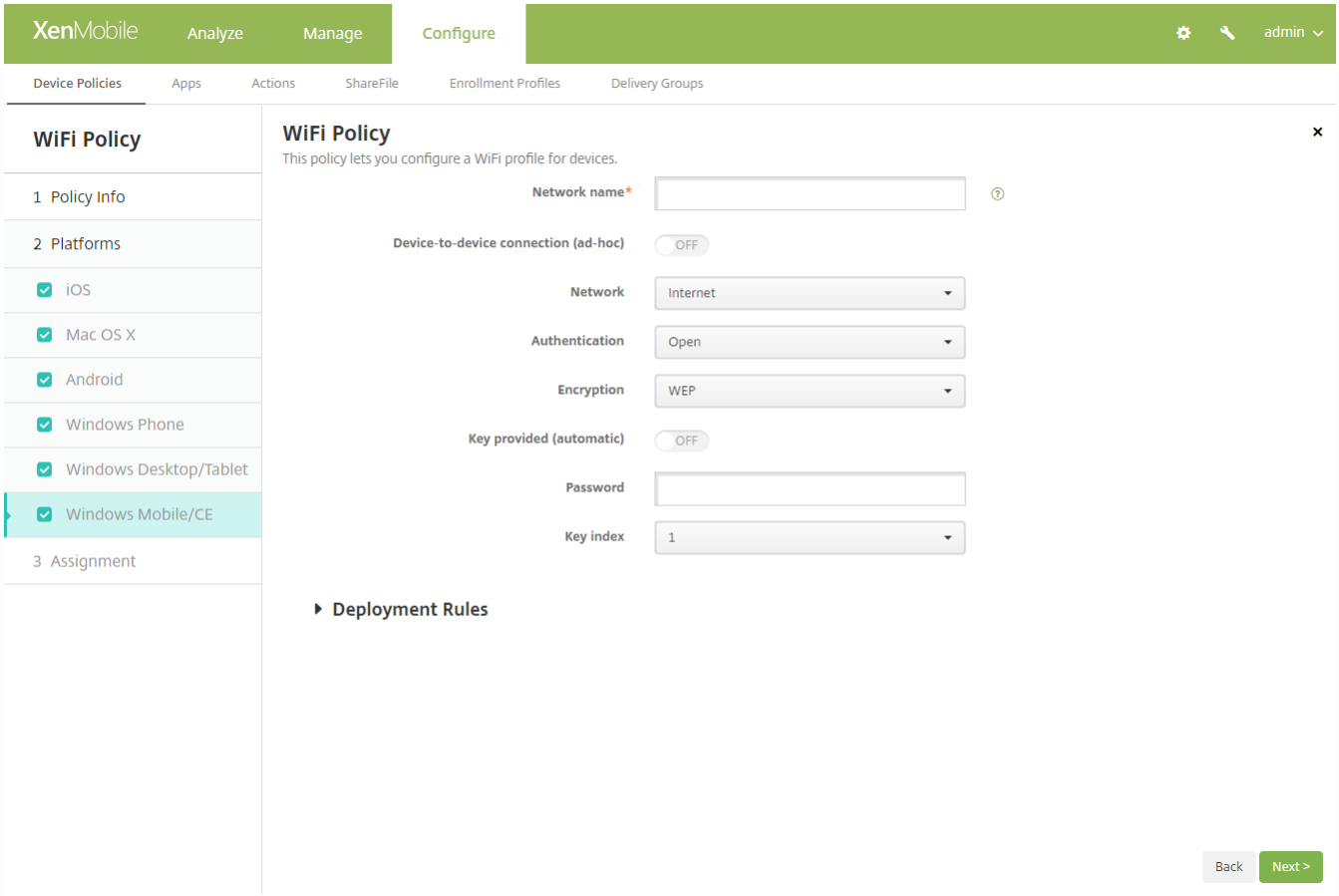
    En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Abierta

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

Configuración de Windows Mobile/CE



Configure estos parámetros:

- **Network name**. Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Device-to-device connection (ad-hoc)**. Permite que dos dispositivos se conecten directamente. La opción predeterminada es **Off**.
- **Network**. Seleccione si el dispositivo está conectado a un origen de Internet externo o a una red de intranet de la oficina.
- **Authentication**. En la lista, elija el tipo de seguridad que se va a utilizar en la conexión WiFi.
  - Abierta
  - WPA personal
  - WPA2 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

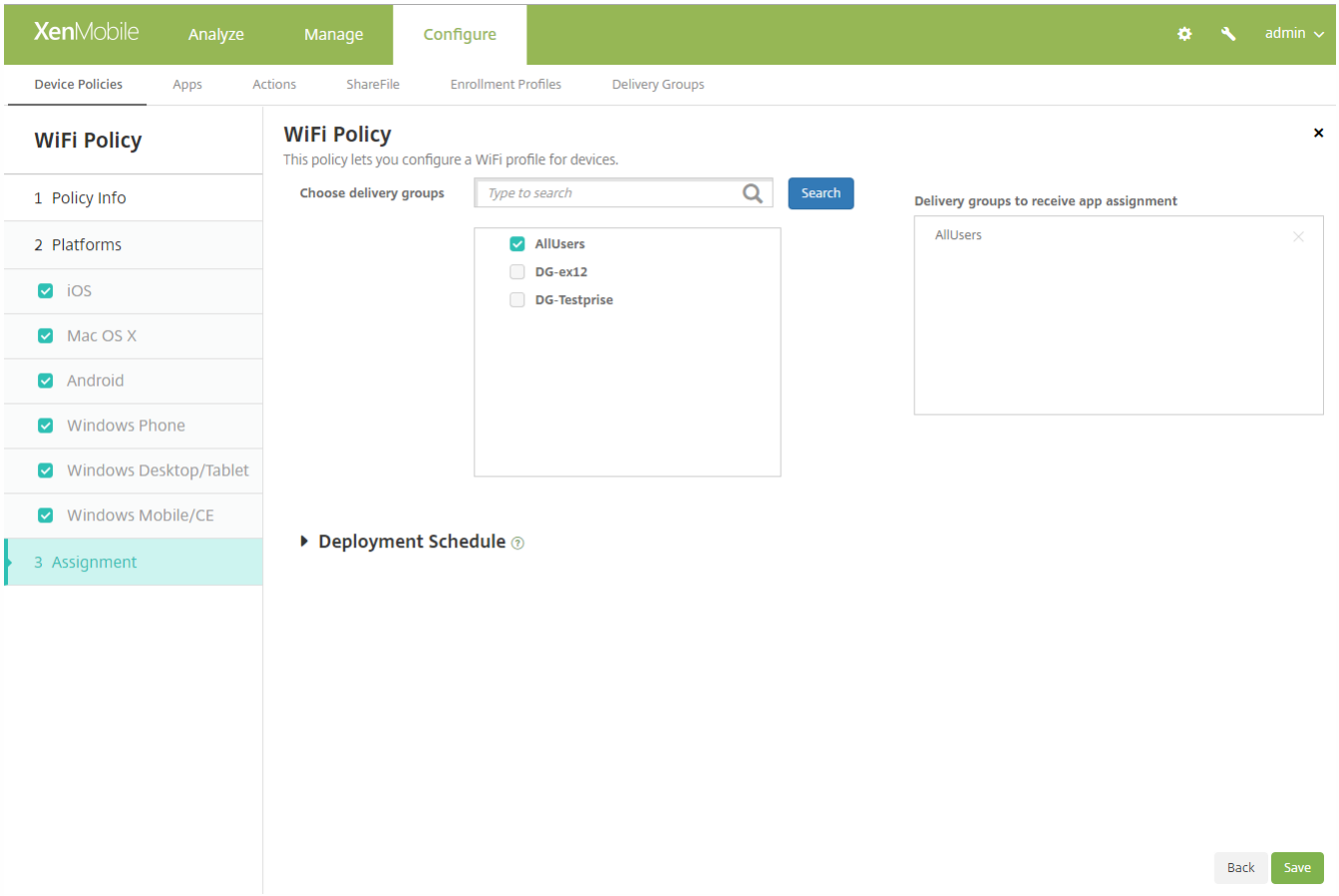
WPA-2 Enterprise

- **Key provided (automatic)**. Seleccione si la clave se suministra automáticamente o no. La opción predeterminada es **Off**.
- **Password**. Introduzca la contraseña en este campo.
- **Key index**. Elija el índice de la clave. Las opciones disponibles son: **1**, **2**, **3** y **4**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página **Assignment** de la **directiva WiFi**.

8. Haga clic en **Next**. Aparecerá la página **Assignment** de la directiva WiFi.
8. Haga clic en **Next**. Aparecerá la página **Assignment** de la directiva WiFi.
8. Haga clic en **Next**. Aparecerá la página **Assignment** de la directiva WiFi.



9 Junto a **Choose delivery groups**, escriba para buscar un grupo de entrega o seleccione un grupo o varios. 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 bien, haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**.
- 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para certificados de Windows CE

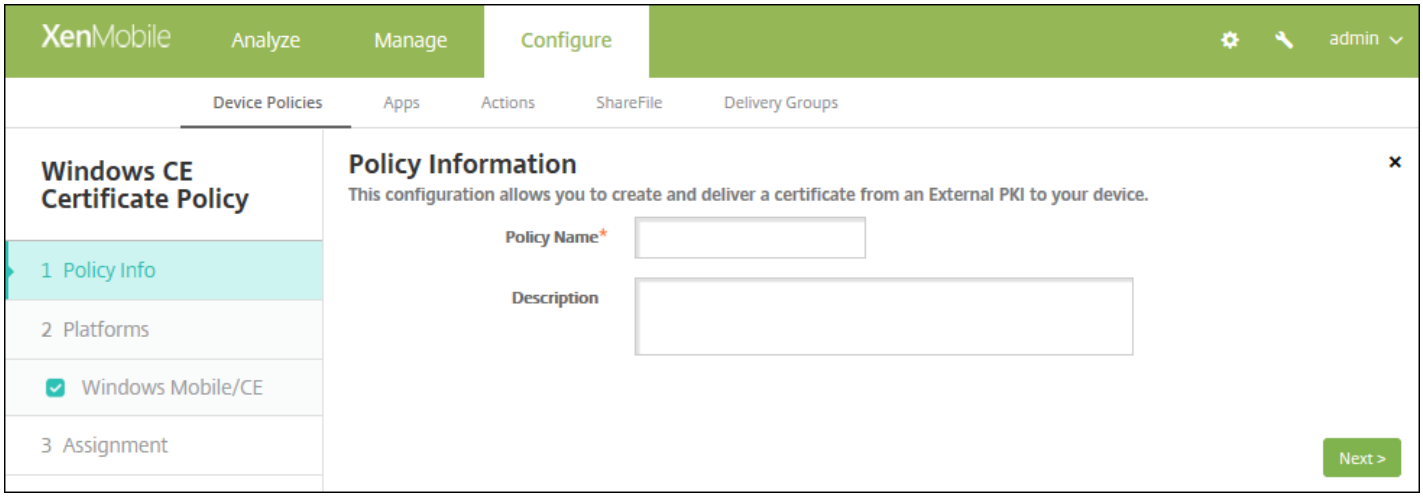
Feb 27, 2017

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**.

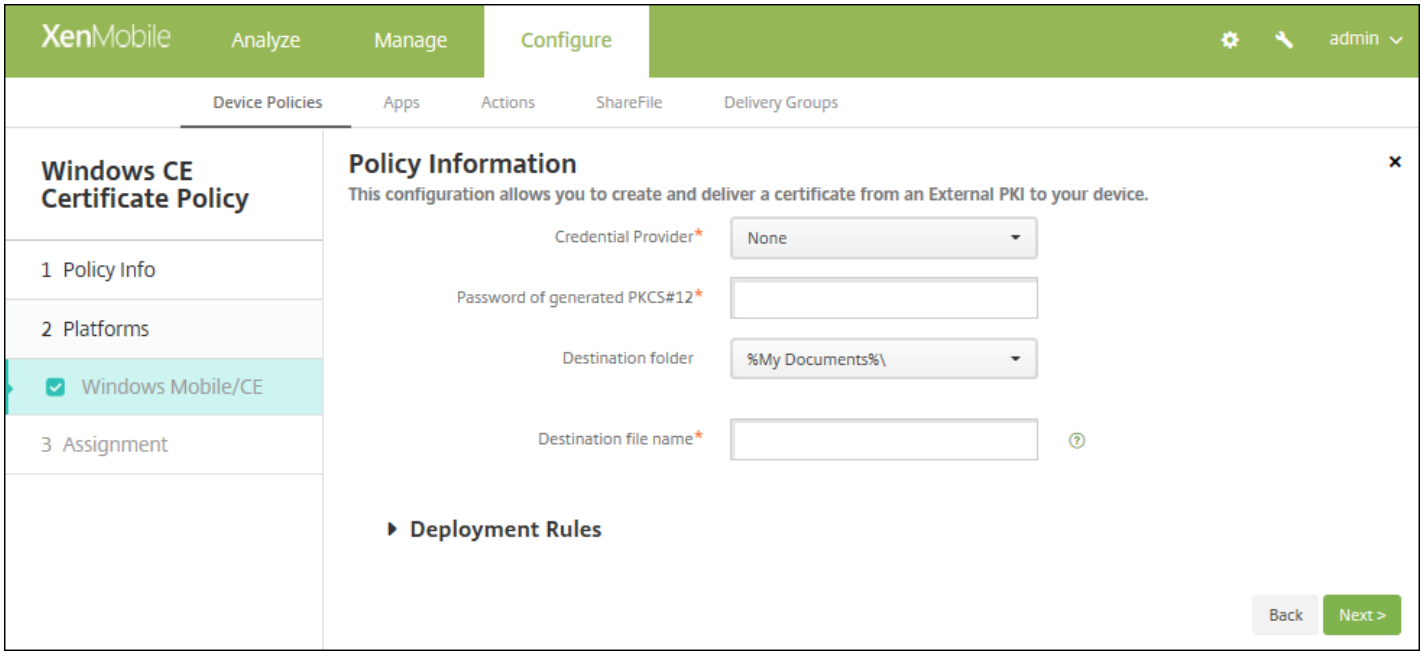
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Windows CE Certificate**. Aparecerá la página de información **Windows CE Certificate Policy**.



4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Windows CE Certificate Policy Platforms**.

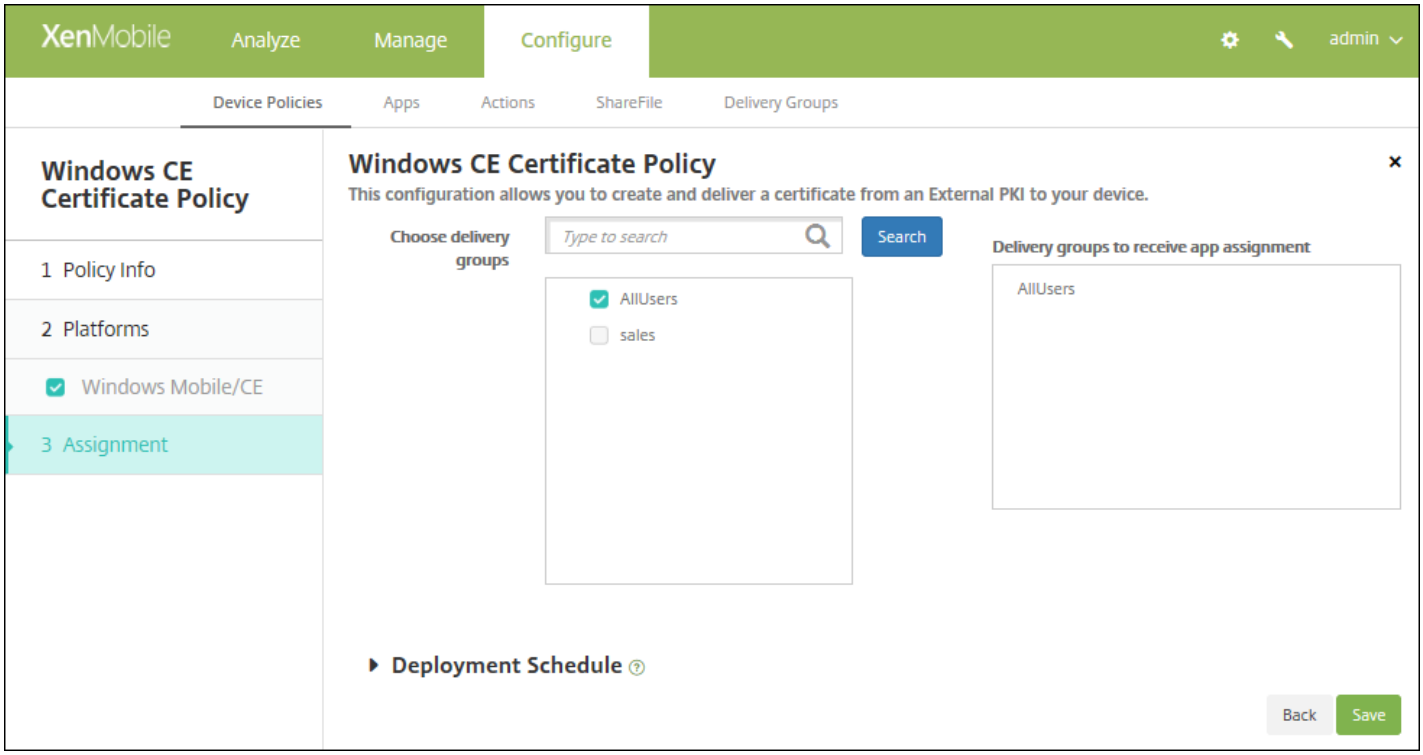


6. Configure estos parámetros:

- **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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 opciones de XenMobile

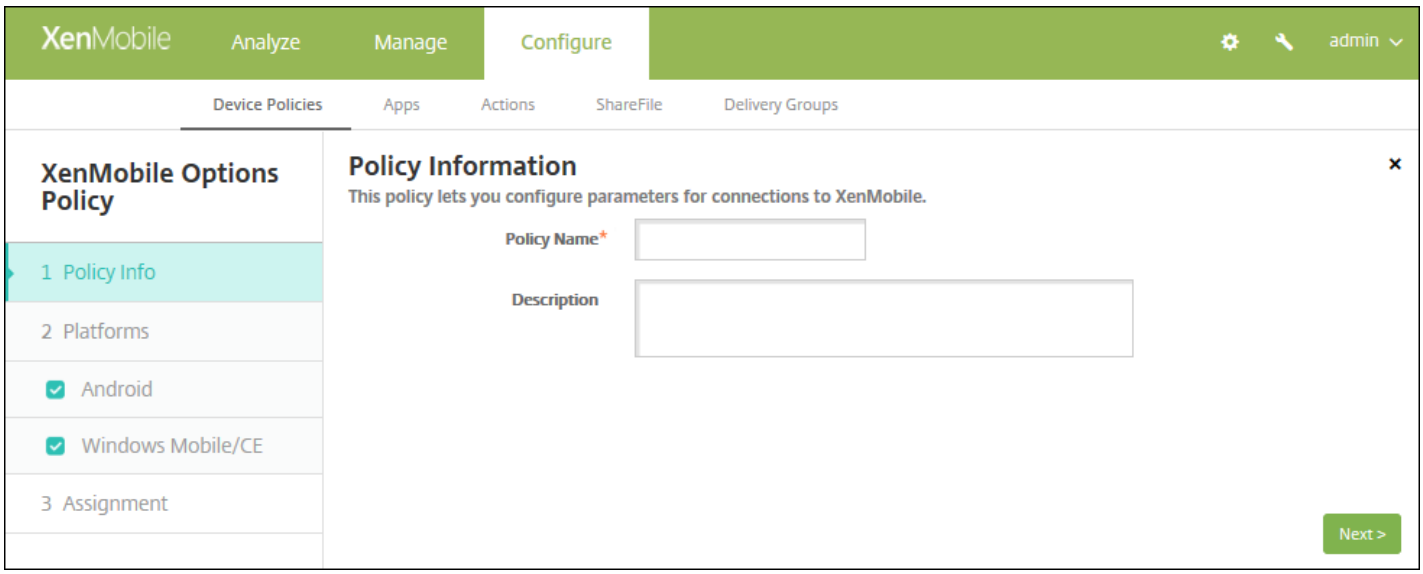
Feb 27, 2017

Puede agregar una directiva de opciones de XenMobile para configurar el comportamiento de Secure Hub 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:

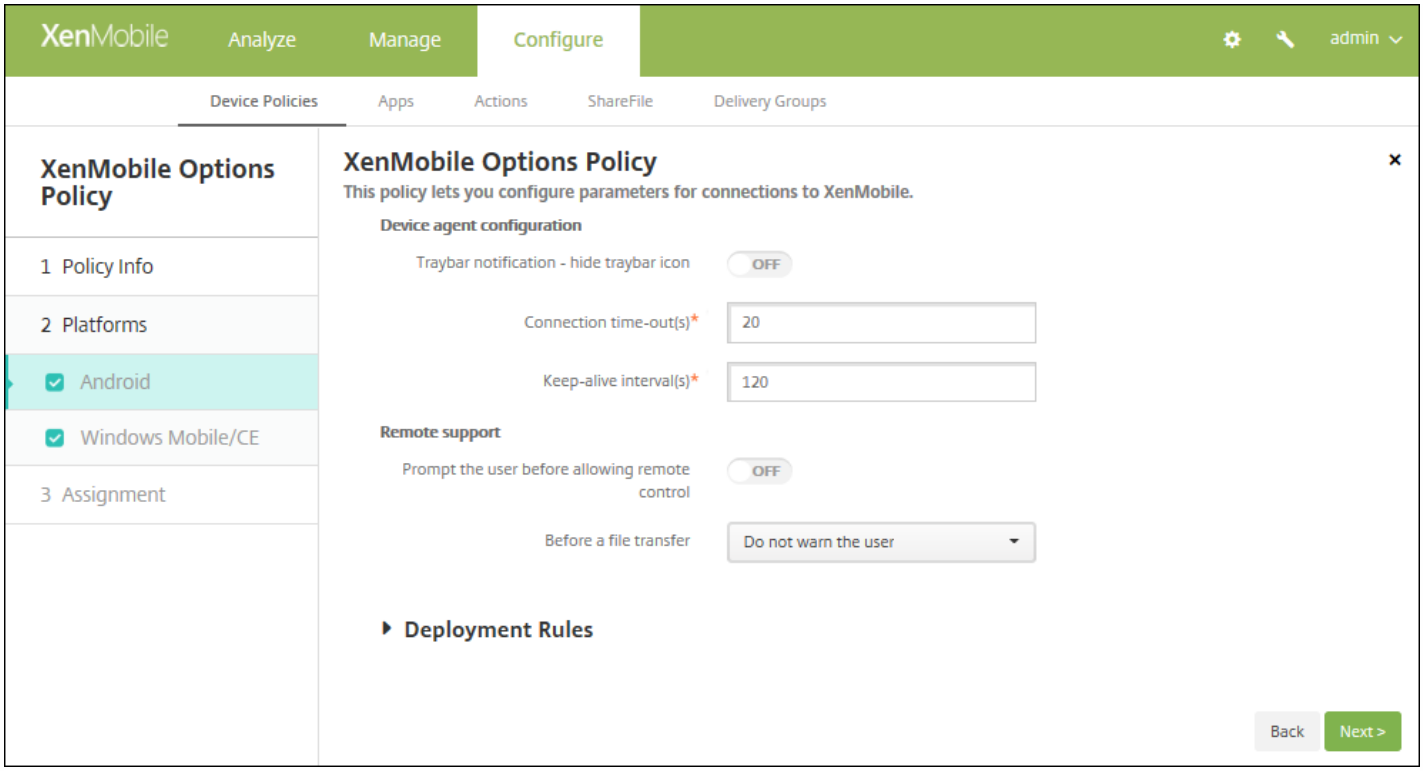
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Platforms** de la directiva.

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.

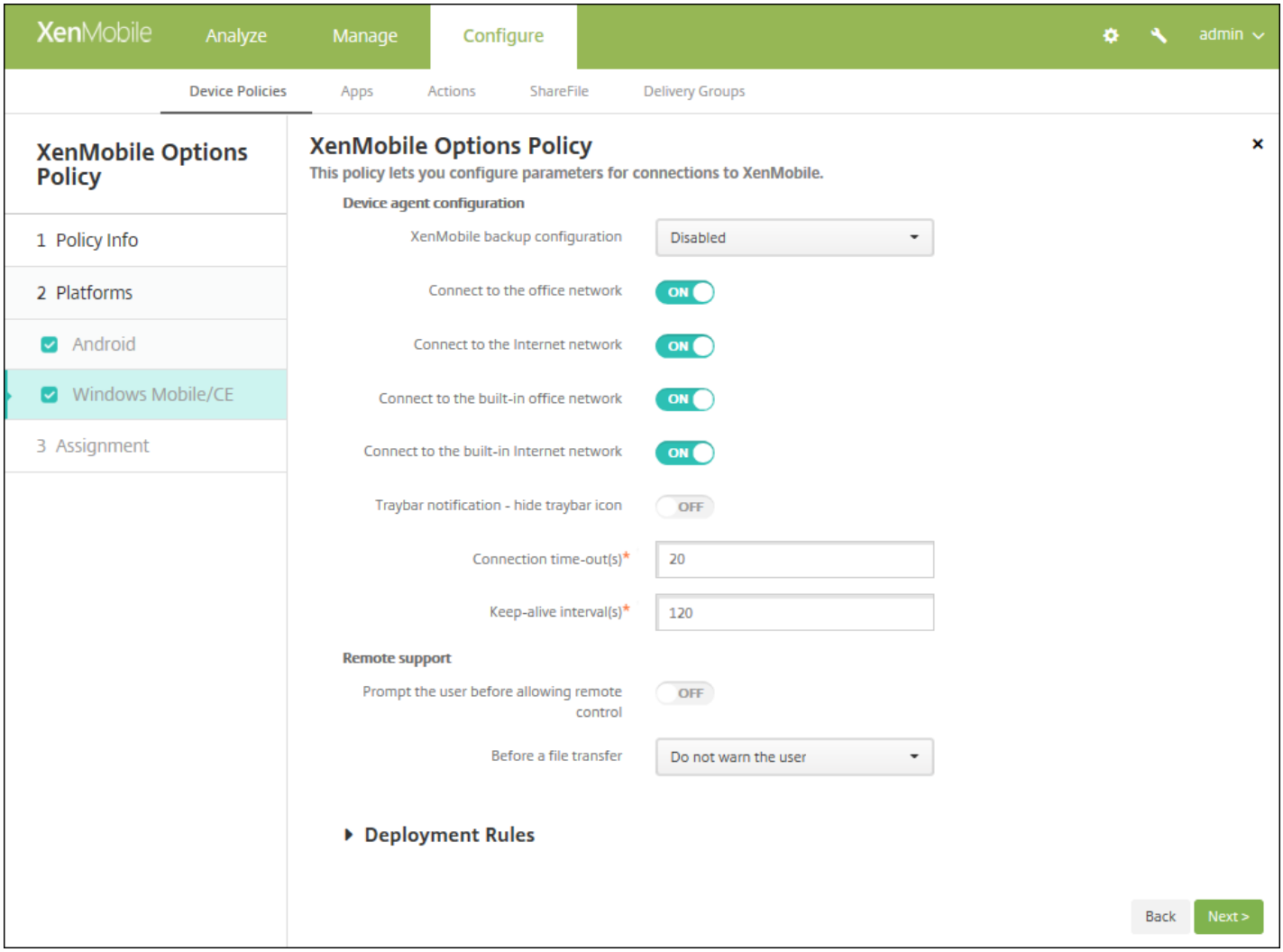
Configuración de los parámetros de Android



Configure estos parámetros:

- **Traybar notification - hide traybar icon**. Seleccione si el icono 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.
- **Prompt the user before allowing remote control**. Seleccione si pedir confirmación al usuario antes de permitir que el equipo de asistencia remota tome el control. 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:

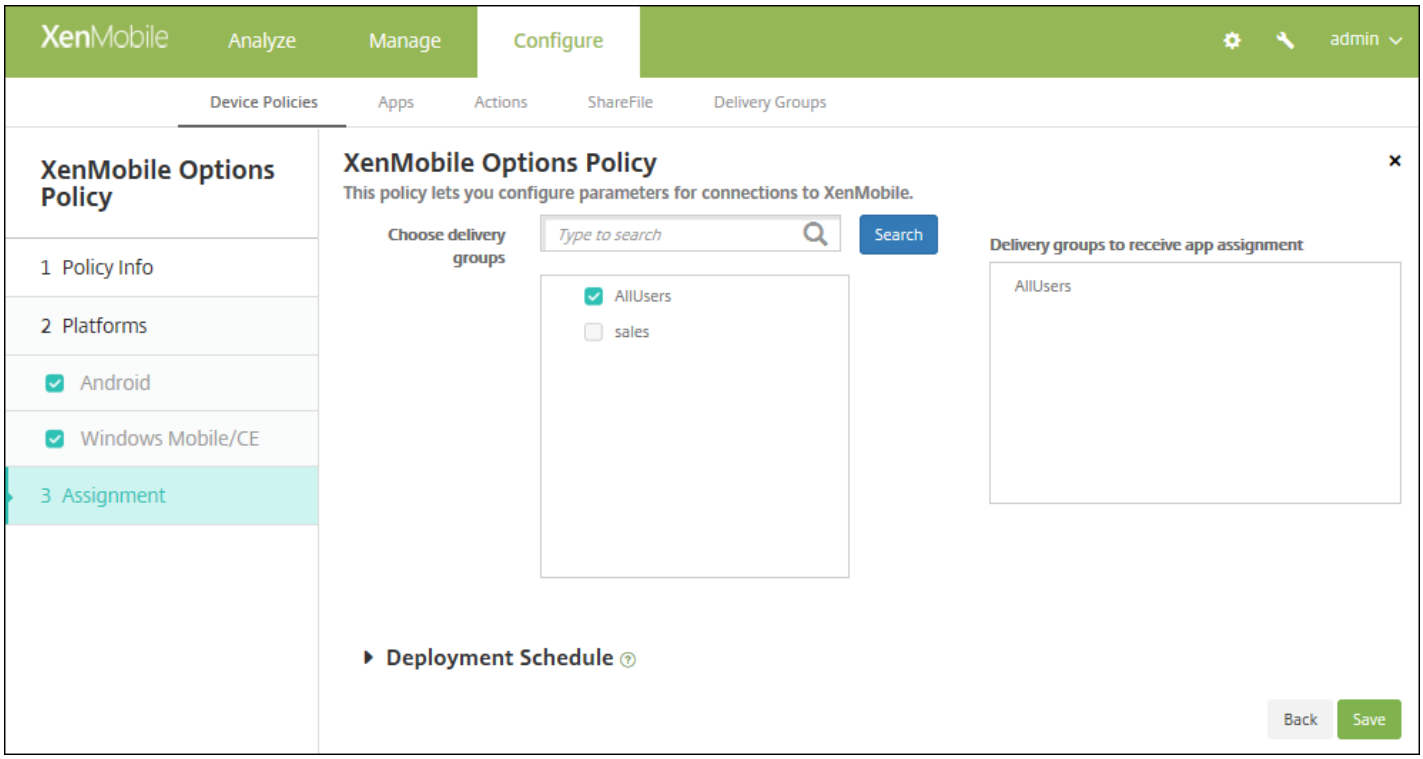
- **Configuración del agente del dispositivo**
  - **XenMobile backup configuration**. En la lista, haga clic en una opción para la copia de seguridad de la configuración de XenMobile en los dispositivos de los usuarios. El valor predeterminado es **Disabled**. Las opciones disponibles son:
    - Disabled (Inhabilitado)
    - At first connection after XenMobile installation (En la primera conexión después de instalar XenMobile)
    - At first connection after each device reboot (En la primera conexión después de cada reinicio del dispositivo)
  - **Connect to the office network (Conectar a la red de la oficina)**
  - **Connect to the Internet network (Conectar a la red de Internet)**
  - **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.

- **Asistencia remota**
  - **Prompt the user before allowing remote control**. Seleccione si pedir confirmación al usuario antes de permitir que el equipo de asistencia remota tome el control. 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 el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 dispositivo para la desinstalación de XenMobile

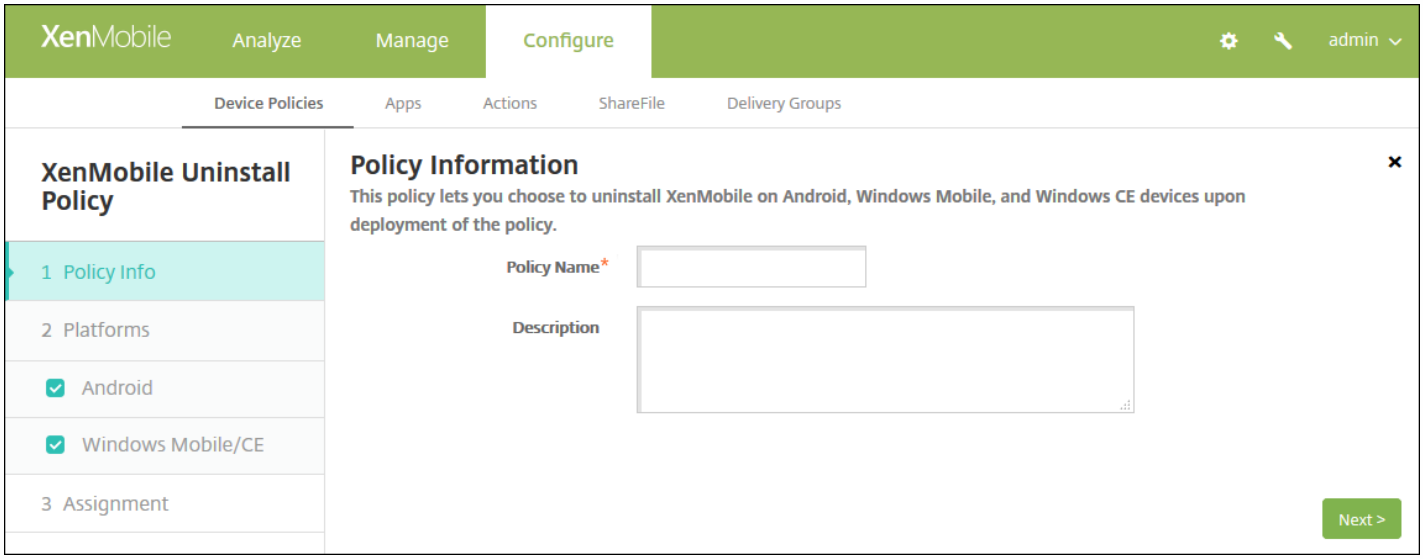
Feb 27, 2017

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:

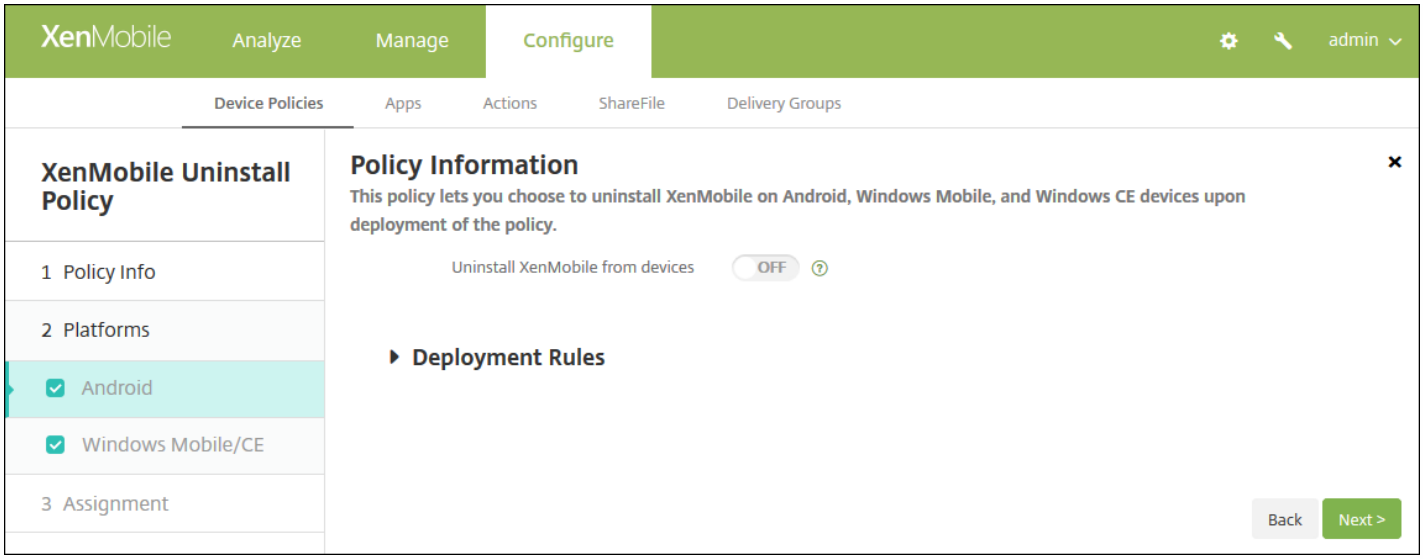
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **Platforms** de la directiva.

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

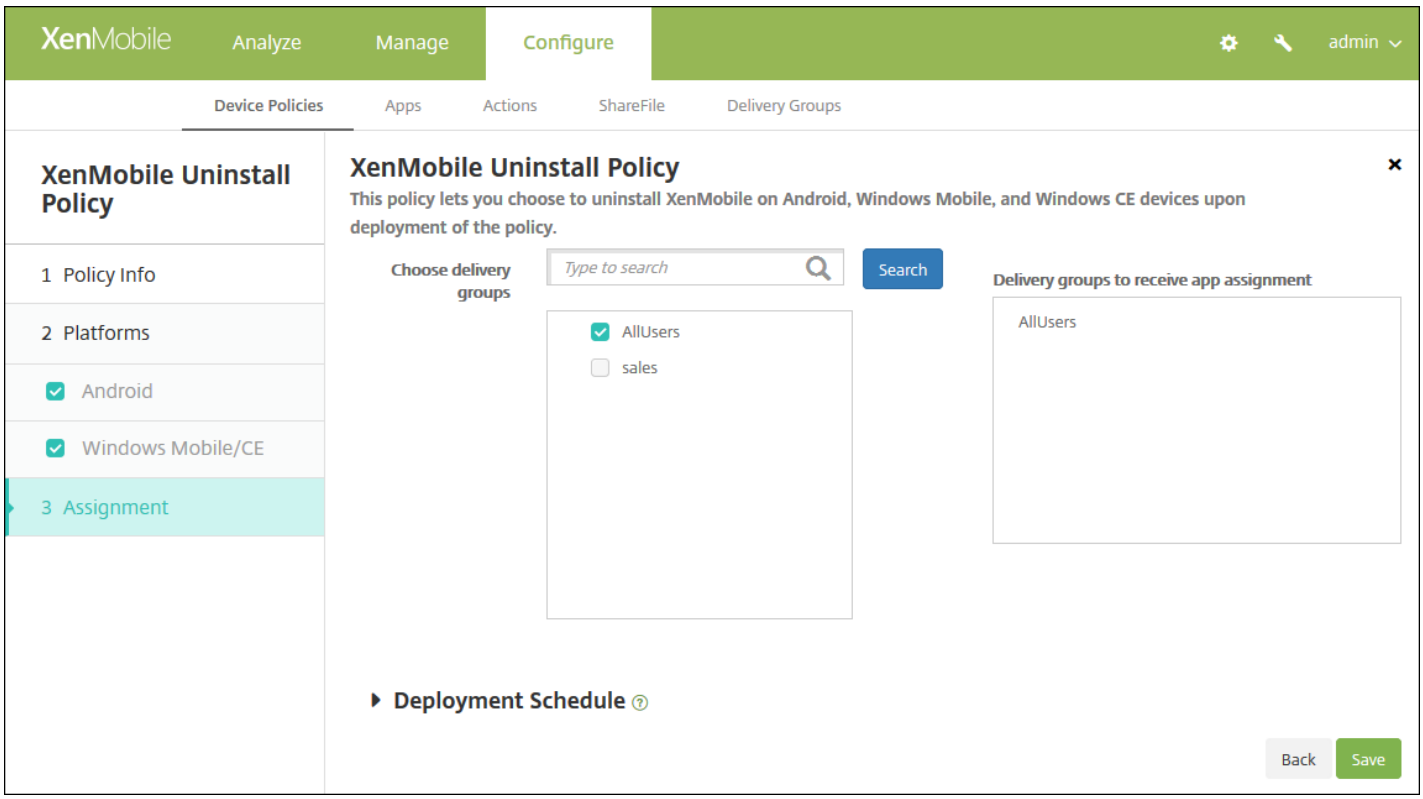


Configure este parámetro para cada plataforma seleccionada:

- **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 de **XenMobile Uninstall Policy**.



9 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un

grupo o varios 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

Cómo agregar aplicaciones

May 10, 2017

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 tiendas internas y de tiendas públicas.
- **Tienda pública de aplicaciones**. Estas aplicaciones incluyen aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como iTunes o Google Play. Por ejemplo, GoToMeeting.
- **Web y 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.
- **Empresarial**. Estas aplicaciones son aplicaciones nativas que no están empaquetadas con la herramienta MDX Toolkit y no contienen las directivas asociadas a aplicaciones MDX.
- **Enlace Web**. 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. 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, coloque el dispositivo iOS administrado en modo supervisado. Para obtener más información, consulte Directivas de importación de perfiles de iOS y Mac OS X.
> - Para las aplicaciones Android, habilite las directivas de Samsung for Enterprise (SAFE) o KNOX en el dispositivo. Para ello, configure la directiva de clave de licencia 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, Android y Windows, incluidas las aplicaciones XenMobile (como Secure Hub, Secure Mail y Secure Web) 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 XenMobile, 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.

Para distribuir aplicaciones XenMobile para iOS y Android, hay que descargar de Citrix los archivos MDX de la tienda pública, cargar esos archivos en la consola de XenMobile (**Configure > Apps**), actualizar las directivas MDX según sea necesario y luego cargar los archivos MDX en las tiendas públicas de aplicaciones. Para obtener más información, consulte Cómo agregar una aplicación MDX en este artículo.

Para distribuir aplicaciones XenMobile para Windows, hay que descargar de Citrix los archivos de aplicaciones, empaquetarlos con MDX Toolkit, cargarlos en la consola de XenMobile, actualizar las directivas MDX según sea necesario, y entregar las aplicaciones en los dispositivos de usuario a través de grupos de entrega. Para obtener más información, consulte Entrega de aplicaciones XenMobile mediante tienda pública de aplicaciones en la documentación de las aplicaciones XenMobile.

Citrix ofrece la herramienta MDX Toolkit, la cual empaqueta aplicaciones para dispositivos iOS, 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. En algunos casos, es posible configurar las plantillas para la administración y la creación 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.

Para obtener más información, consulte Cómo agregar una aplicación Web o SaaS en este artículo.

Funcionamiento de las aplicaciones de empresa

Las aplicaciones de empresa normalmente residen en la red interna. Los usuarios se pueden conectar a las aplicaciones mediante Secure Hub. Al agregar una aplicación de empresa, XenMobile crea el conector de aplicación correspondiente. Para obtener más información, consulte Cómo agregar una aplicación de empresa en este artículo.

Funcionamiento de la tienda pública 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 obtiene de la tienda la información de la aplicación, XenMobile sobrescribe el nombre y la descripción existentes. Para obtener más información, consulte Cómo agregar una aplicación de tienda pública de aplicaciones en este artículo.

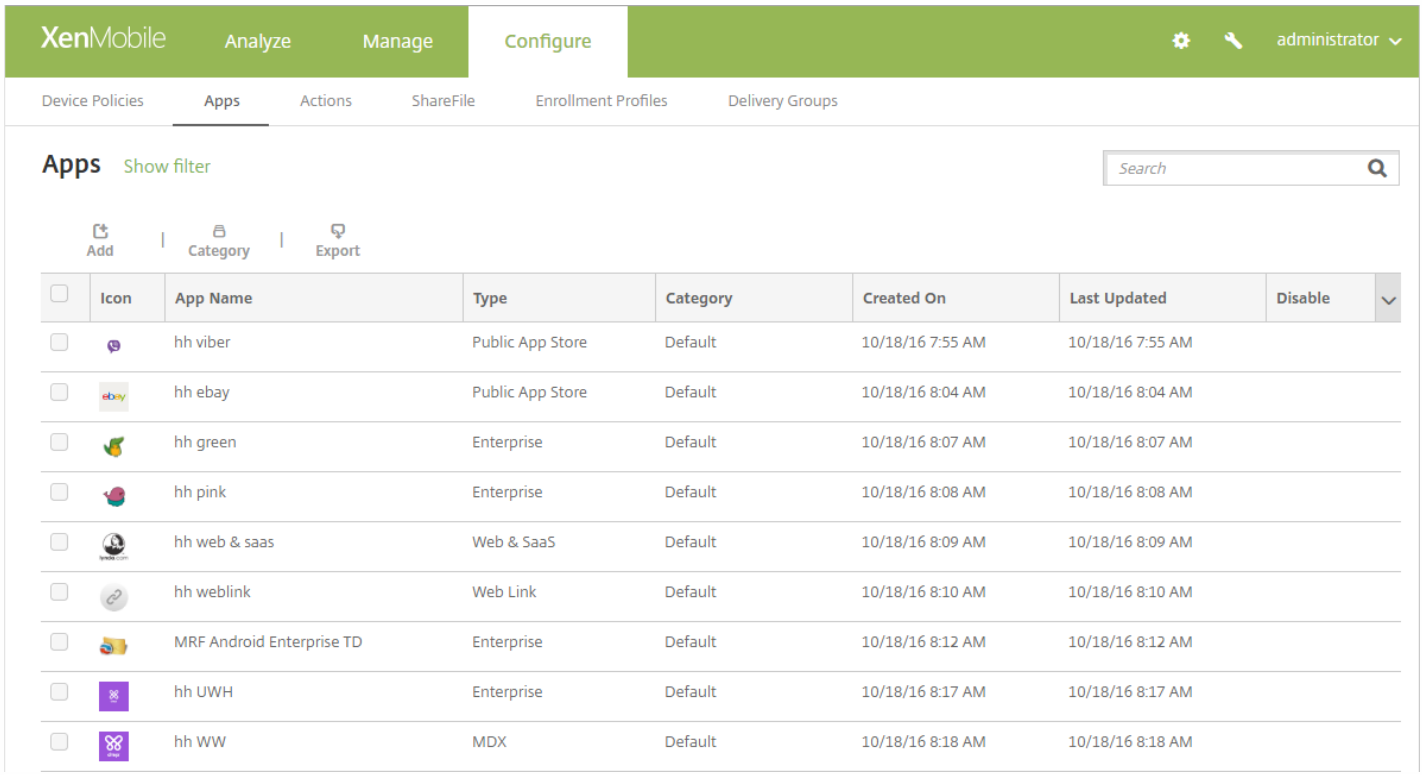
Funcionamiento de los enlaces Web

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, aparecerá como un icono en XenMobile Store. Cuando los usuarios inician sesión en Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles. Para obtener más información, consulte Cómo agregar una aplicación de enlace Web en este artículo.

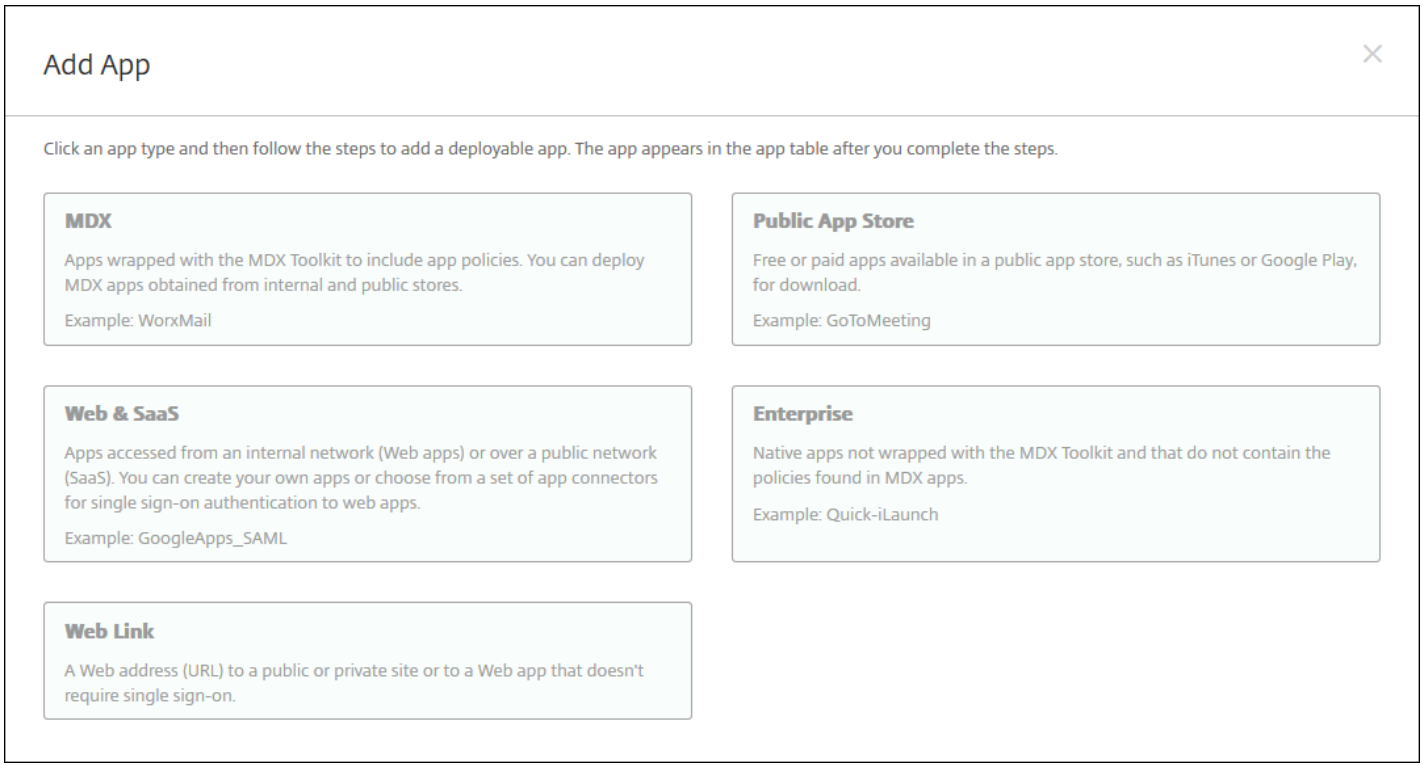
Cómo agregar una aplicación MDX

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 sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivo, consulte Vista general de las directivas MDX. También encontrará descripciones detalladas de las directivas en esa sección.

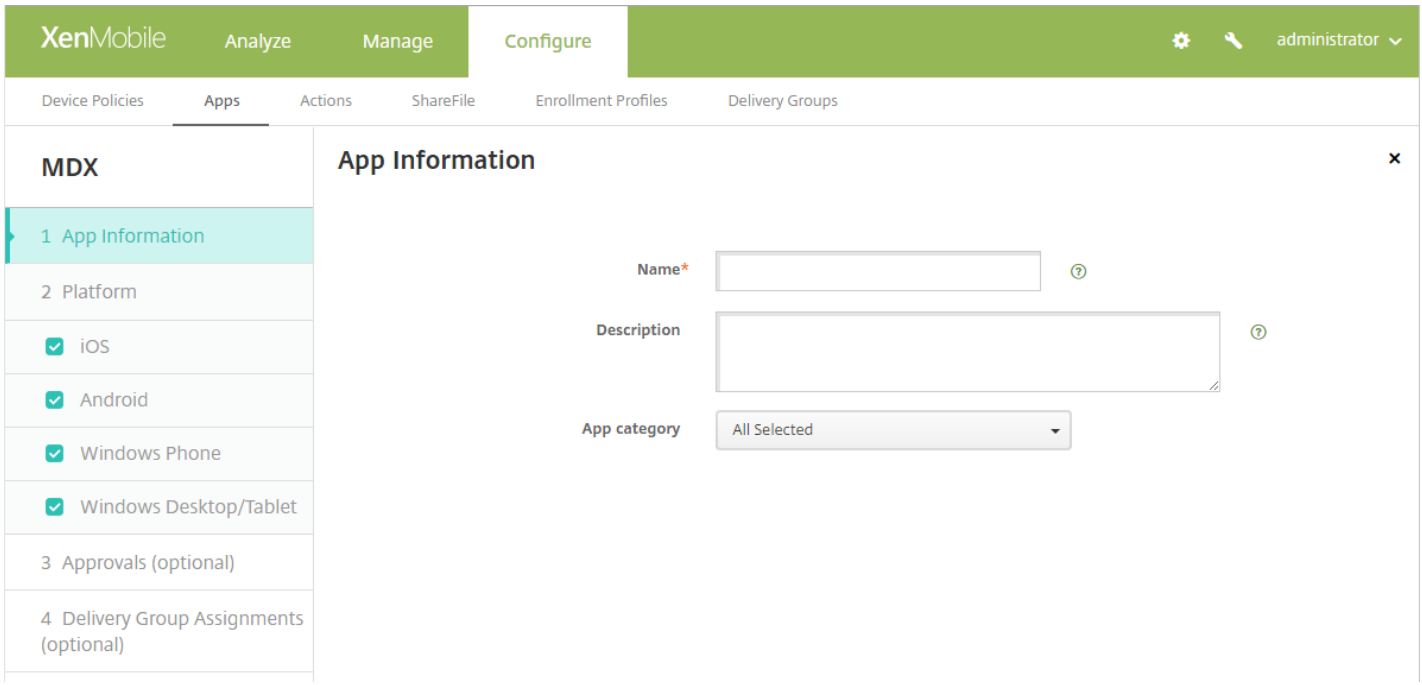
1. En la consola de XenMobile, haga clic en **Configure** > **Apps**. Aparecerá la página **Apps**.



2. Haga clic en **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.

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 de una plataforma, consulte el paso 11 para configurar 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 PCV B2B de iOS, haga clic en **Your application is a VPP B2B application?** y, en la lista, haga clic en la cuenta B2B de PCV a utilizar.

8. Haga clic en **Next**. Aparecerá la página de datos detallados de la aplicación.

9 Configure estos parámetros:

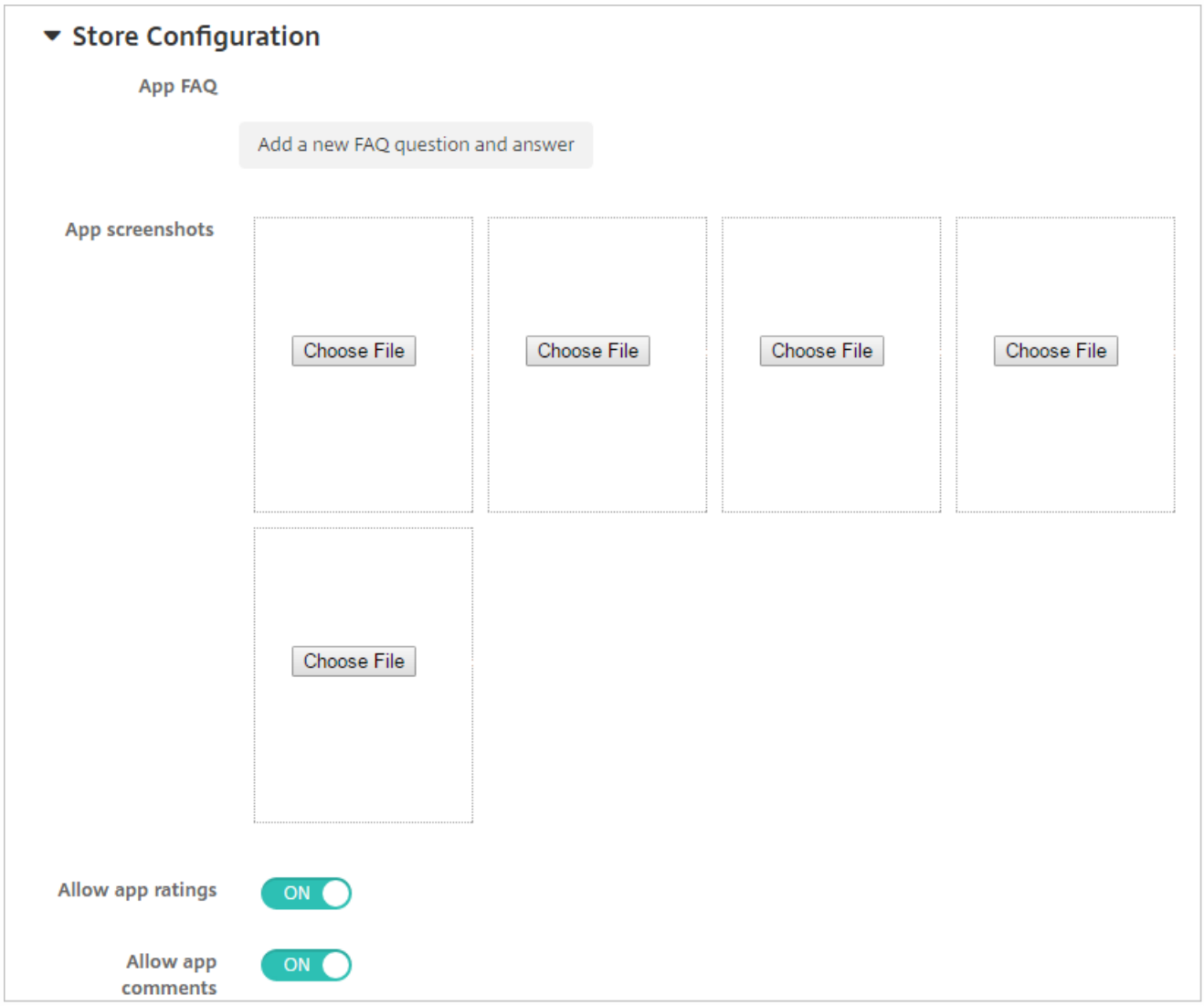
- **File name**. Escriba el nombre del archivo asociado a la aplicación.
- **App Description**. Escriba una descripción de la aplicación.
- **App version**. Si quiere, escriba el número de versión de la aplicación.
- **Minimum OS version**. Si quiere, escriba la versión más antigua del sistema operativo 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, cifrado, interacción de las aplicaciones y restricciones de aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener más información acerca de directivas de aplicaciones MDX, incluida una tabla en la que se muestran las directivas que se aplican a cada plataforma, consulte Vista general de las directivas MDX.

11. Configure las reglas de implementación.

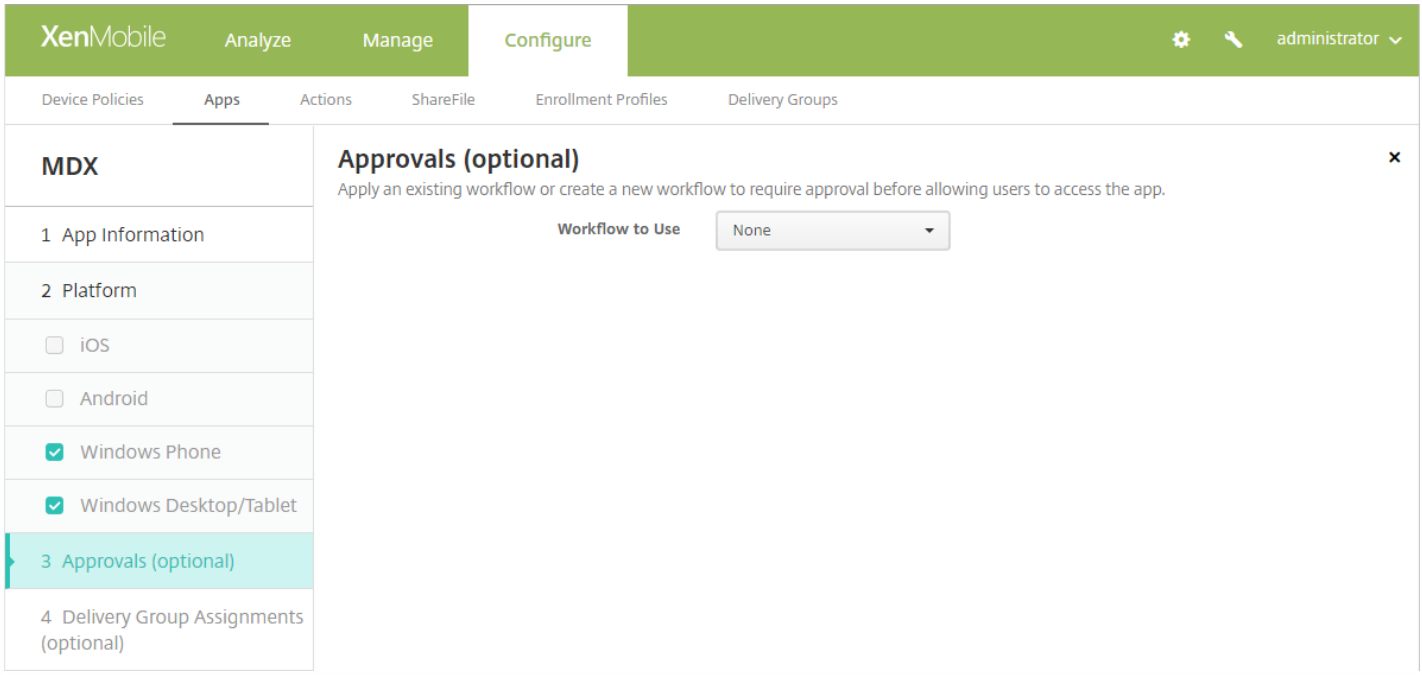
12. Expanda **XenMobile Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en XenMobile 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 XenMobile 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. La opción predeterminada es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. La opción predeterminada 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.

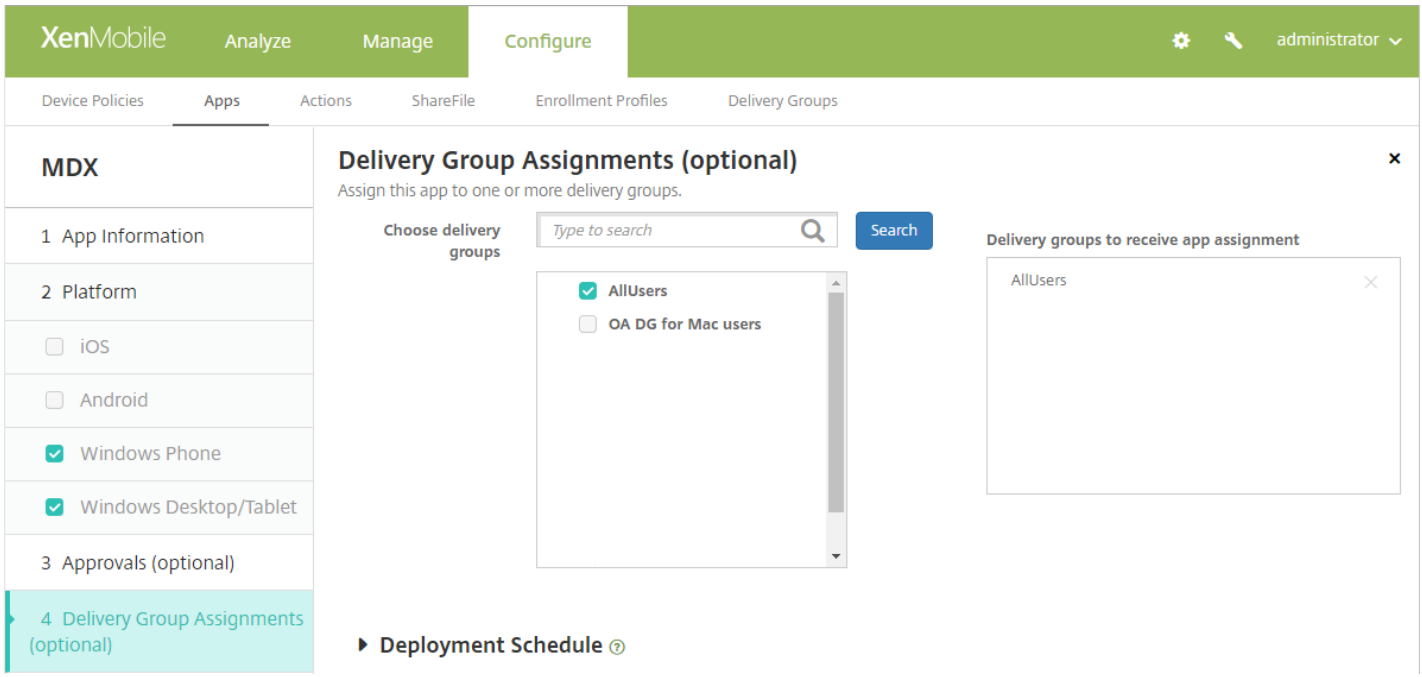
Configure esta opción si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use**. En la lista, haga clic en un flujo de trabajo existente o haga clic en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros. Para obtener más información, consulte Creación y administración de flujos de trabajo.
  - **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 al flujo de trabajo. 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:

- No se necesita
- 1 nivel
- 2 niveles
- 3 niveles

- **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 Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

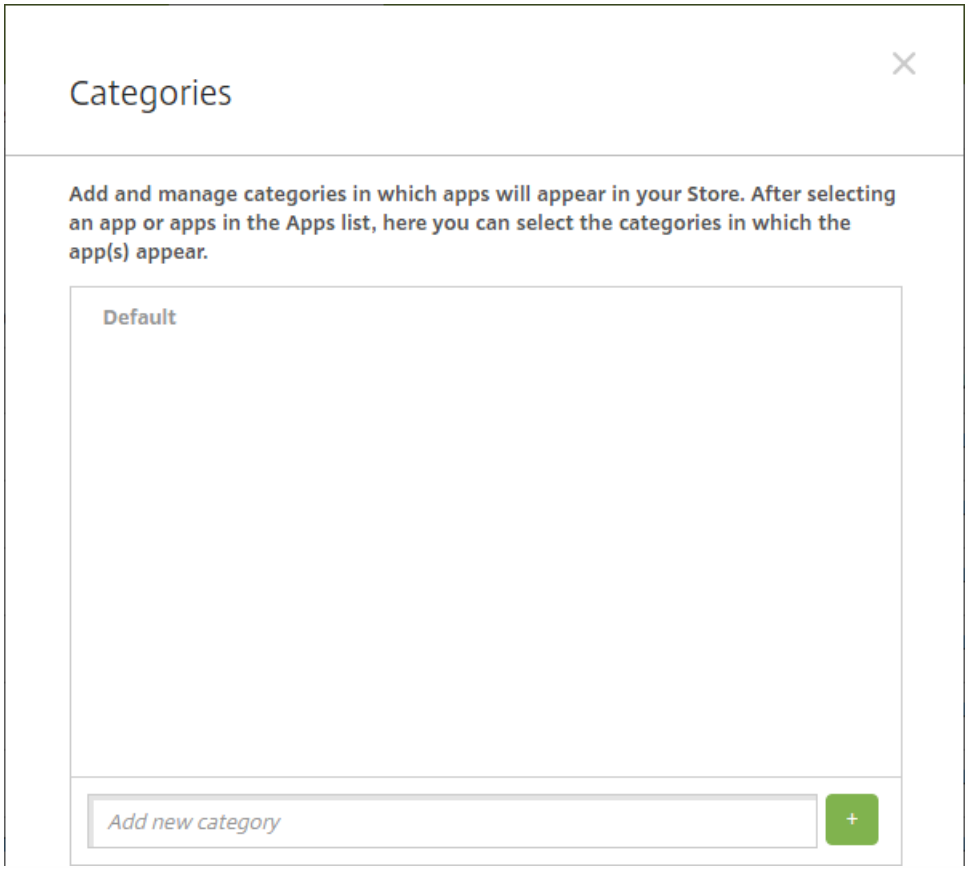
Creación de categorías de aplicaciones

Cuando los usuarios inician sesión en Secure Hub, reciben una lista de las aplicaciones, los enlaces Web y las tiendas que se hayan agregado a XenMobile y configurado en él. Puede usar categorías de aplicaciones para que los usuarios accedan únicamente a aquellas aplicaciones, tiendas 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 una tienda, puede agregarlos a una de las categorías que haya configurado.

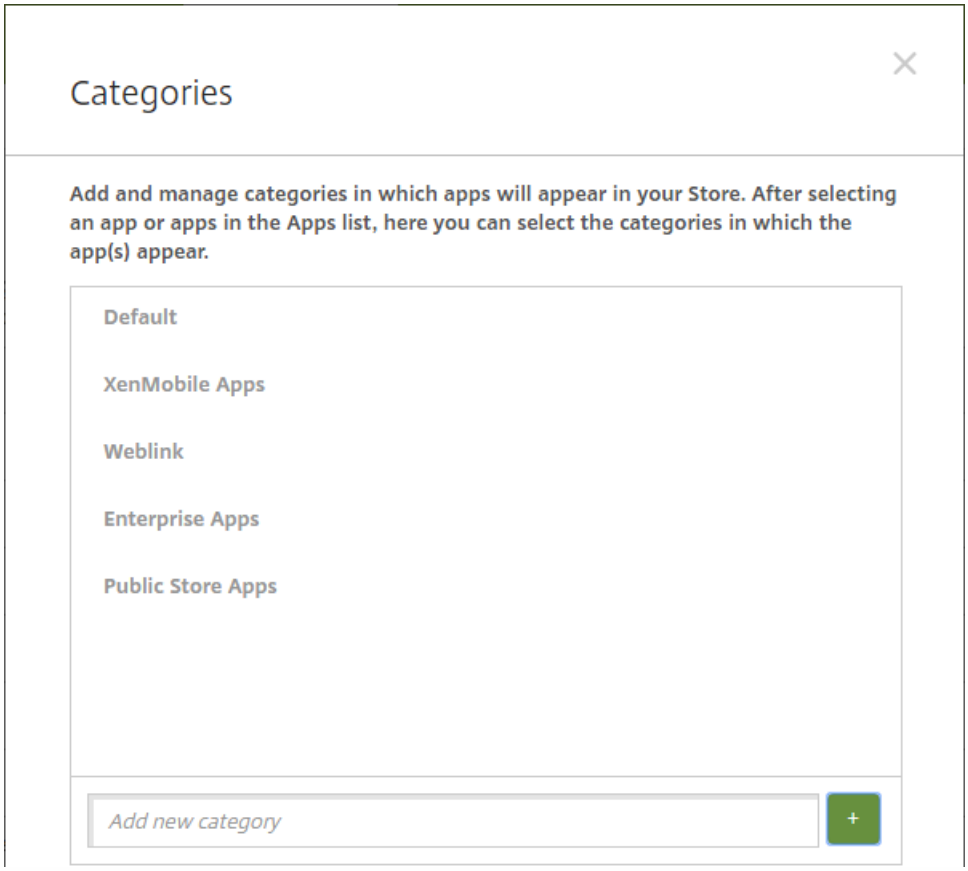
1. En la consola de XenMobile, haga clic en **Configure** > **Apps**. Aparecerá la página **Apps**.

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**.

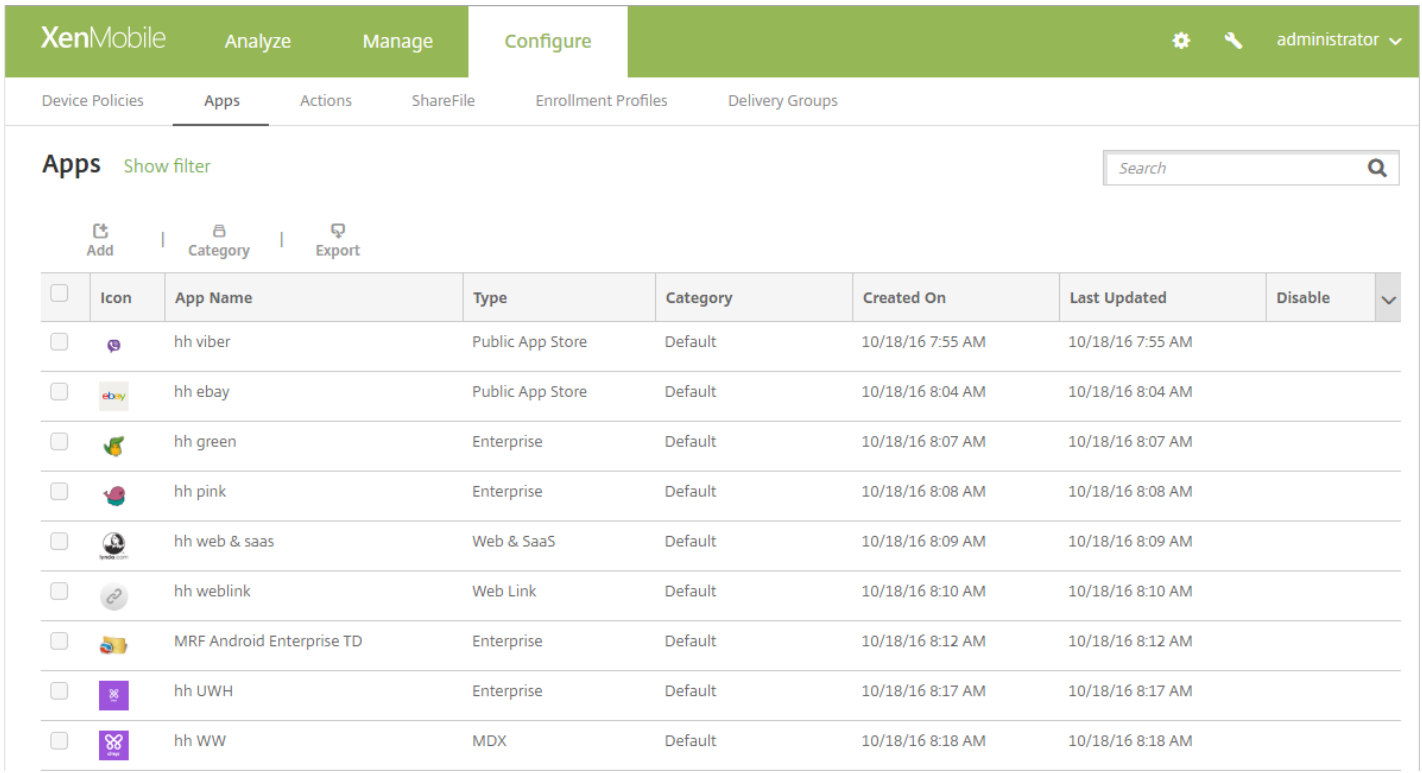
5. En la página **Apps**, puede colocar una aplicación existente en una categoría nueva.

- 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 Group Assignments** o haga clic en **Next** en las páginas restantes de la configuración de la aplicación.
- Haga clic en **Save** en la página **Delivery Group Assignments** para aplicar la nueva categoría. La nueva categoría se aplicará a la aplicación y aparecerá en la tabla **Apps**.

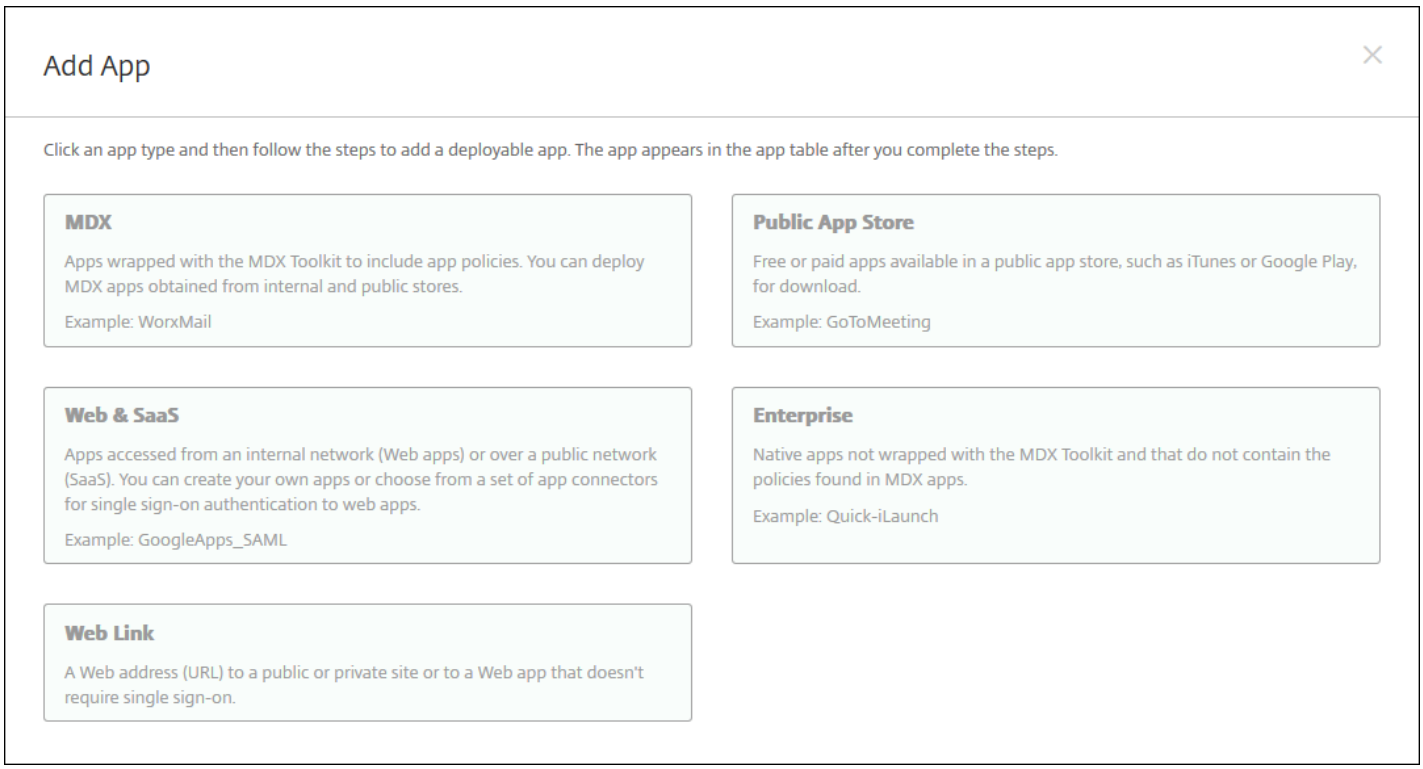
Cómo agregar una aplicación de tienda pública

Se pueden agregar a XenMobile tanto aplicaciones gratuitas como de pago, que estén disponibles en una tienda pública 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:

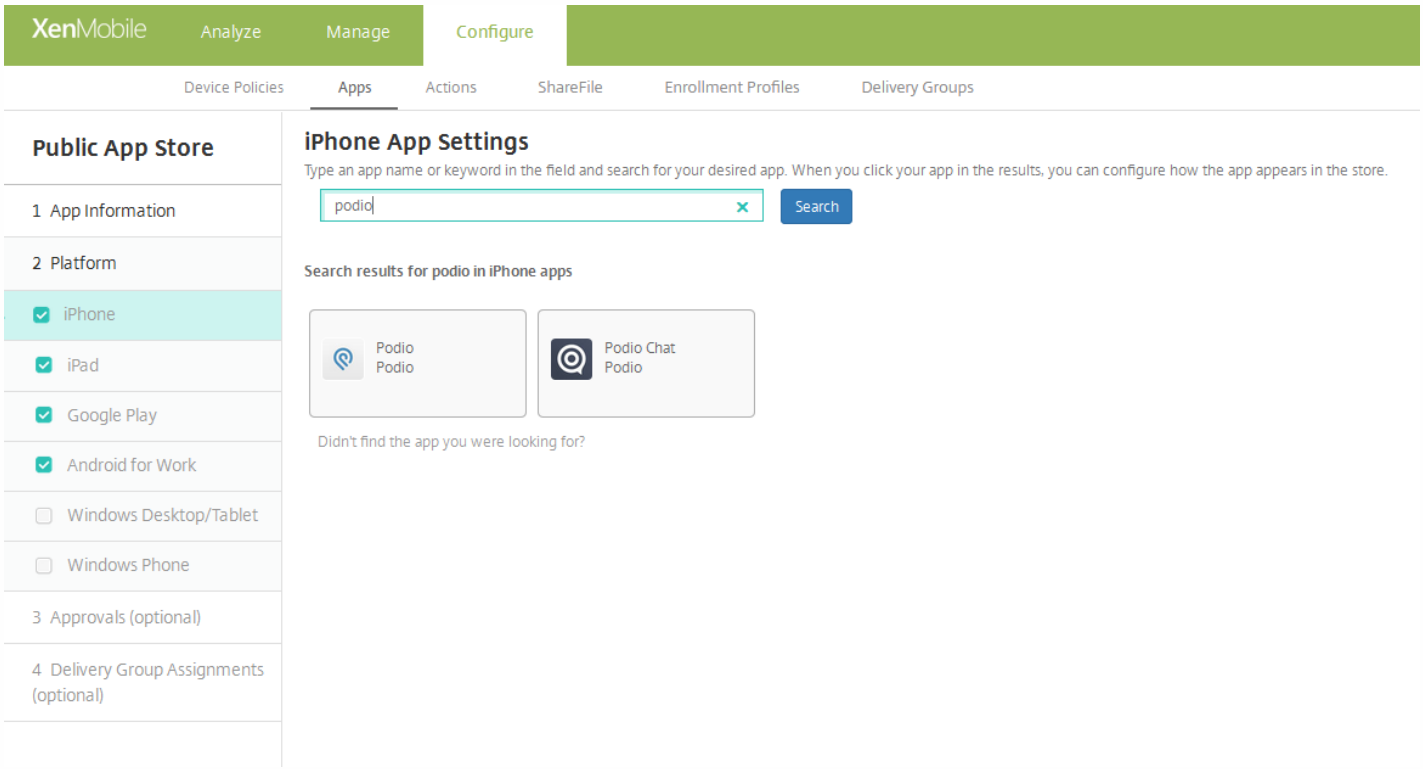
- **Name**. Escriba un nombre descriptivo para la aplicación. Este figurará en **App Name**, en la tabla **Apps**.
- **Description**. Escriba, si quiere, una descripción de la aplicación.
- **App category**. Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Creación de categorías de aplicaciones.

5. Haga clic en **Next**. Aparecerá la página **App Platforms**.

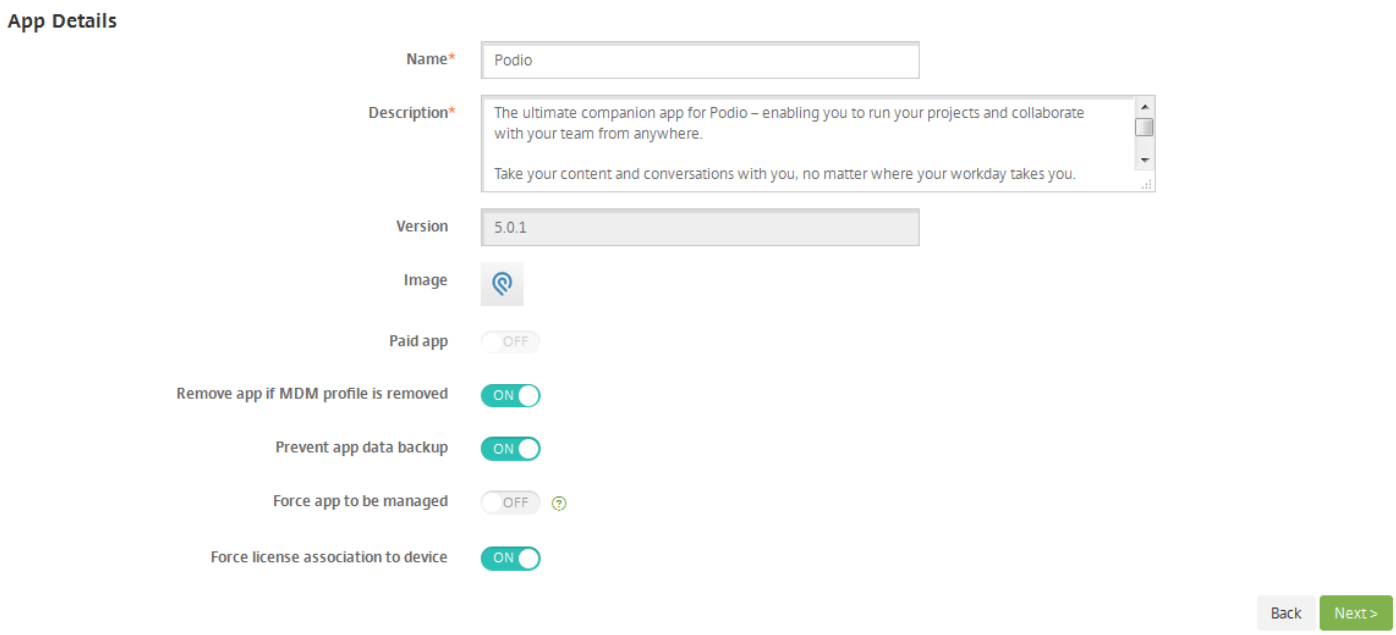
6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración de una plataforma, consulte el paso 10 para configurar 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 de "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).

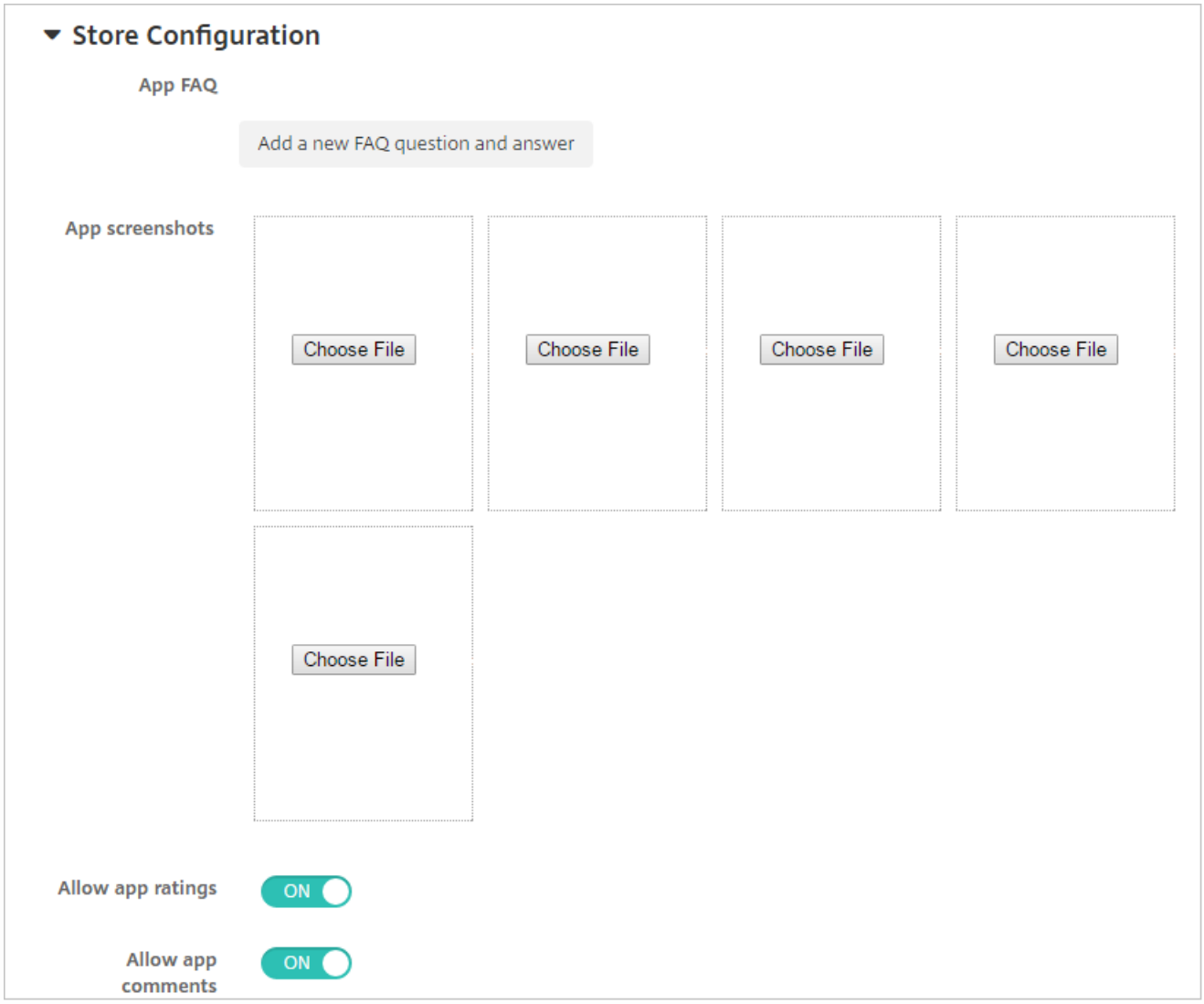


9 Configure estos parámetros:

- 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 **XenMobile Store Configuration**.

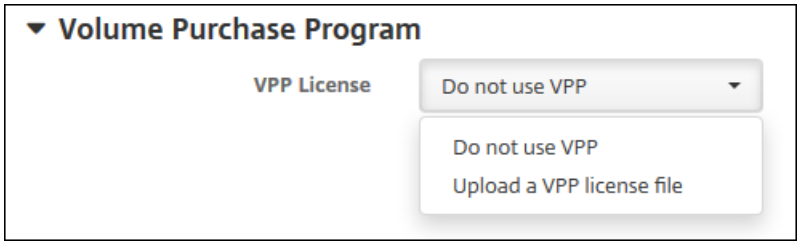


Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en XenMobile Store. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- 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 XenMobile 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. La opción predeterminada 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**.

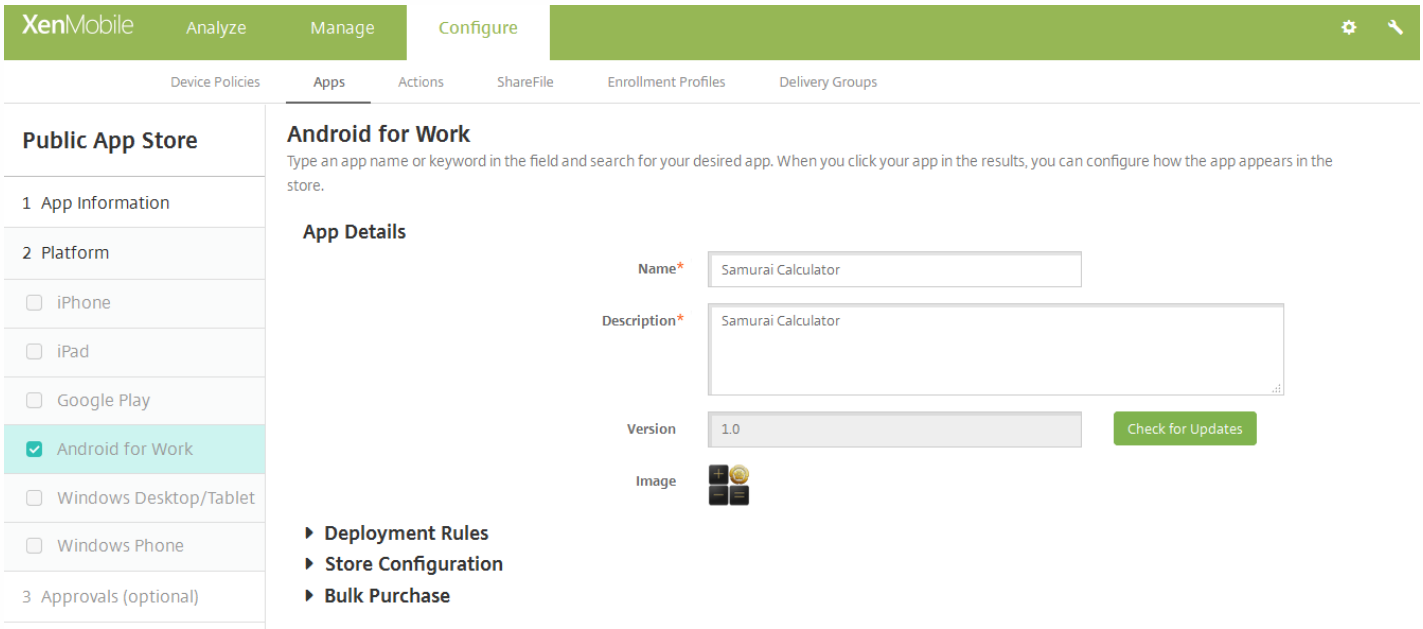
Para el programa Volume Purchase Program de compras por volumen, complete los pasos siguientes.



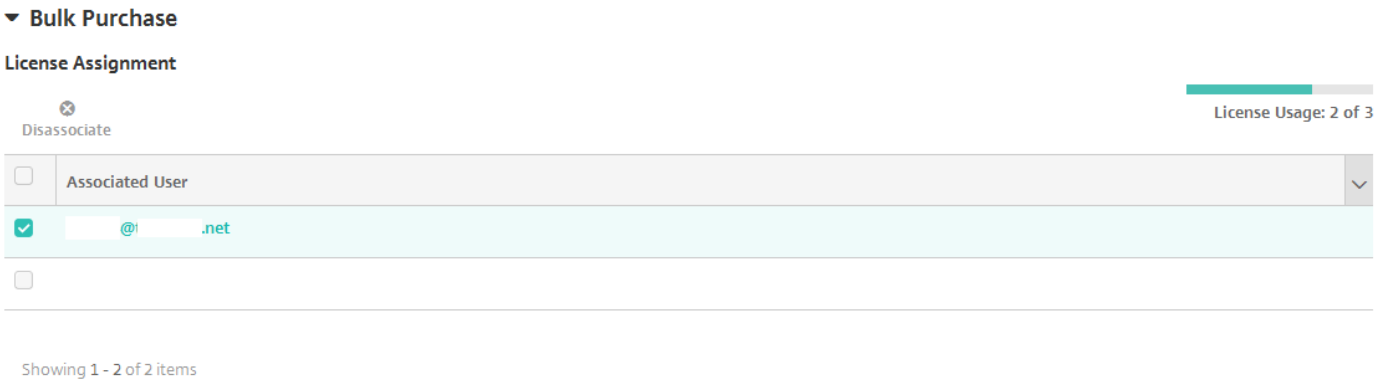
a. En la lista **VPP license**, haga clic en **Upload a VPP license file** si quiere permitir que XenMobile aplique una licencia de PCV a la aplicación.

b. En el cuadro de diálogo que aparecerá, 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**. Aparecerá 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 estos parámetros 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 al flujo de trabajo. 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:
    - No se necesita
    - 1 nivel
    - 2 niveles
    - 3 niveles
  - **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 Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

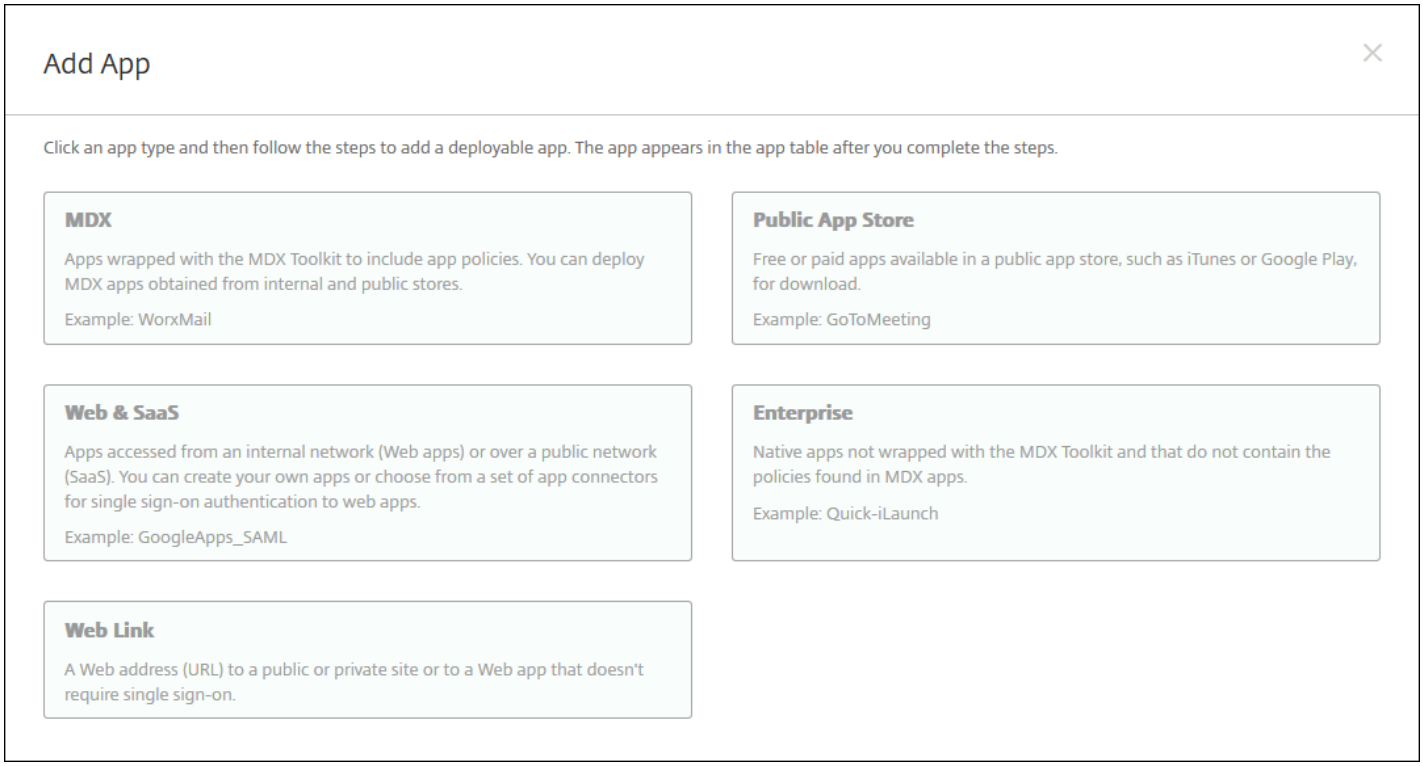
Cómo agregar una aplicación Web o SaaS

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 Tipos de conectores de aplicaciones. También puede crear su propio conector en XenMobile cuando agregue una aplicación Web o SaaS.

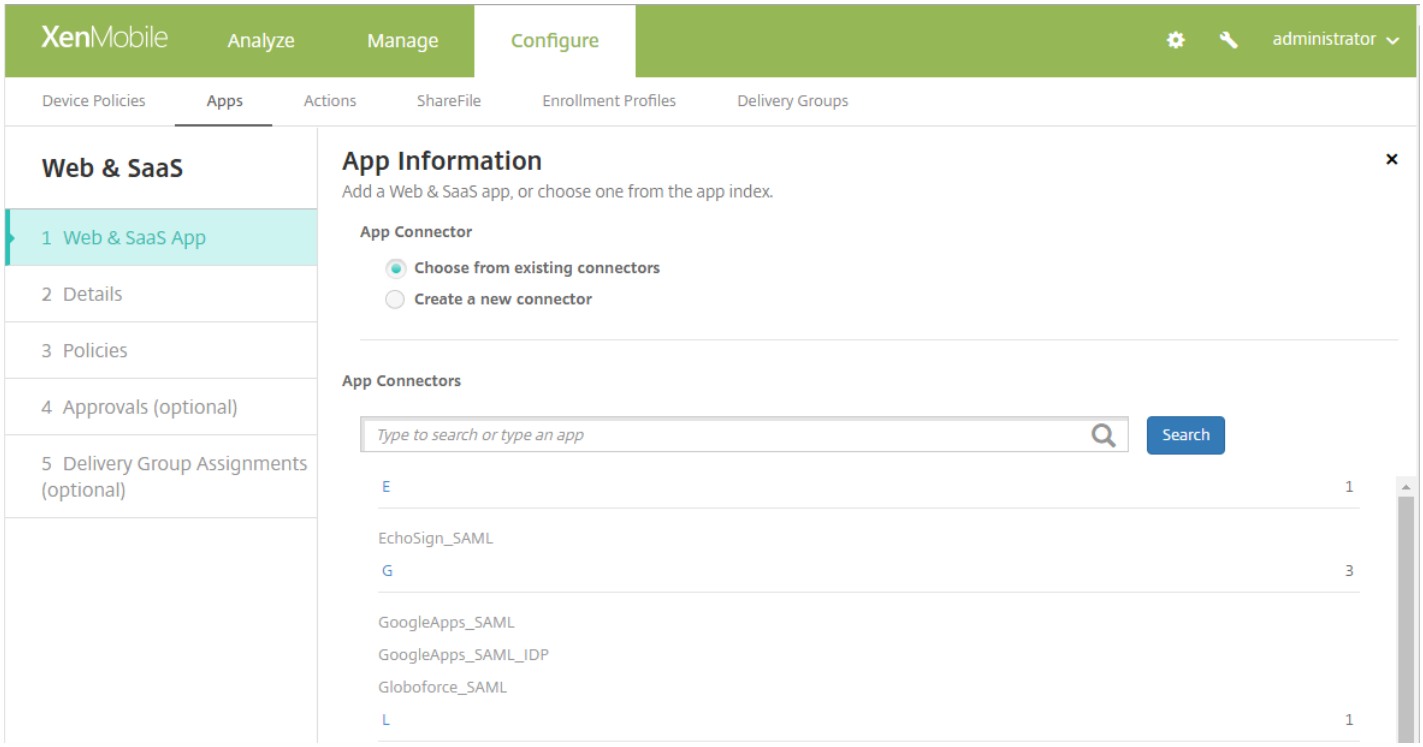
Si una aplicación solo está disponible para SSO, al finalizar la configuración de los parámetros anteriores, guárdelos para que la aplicación aparezca en la ficha **Apps** de la consola de XenMobile.

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 un conector de aplicación nuevo o existente, como se muestra a continuación.

Para configurar un conector de aplicación existente

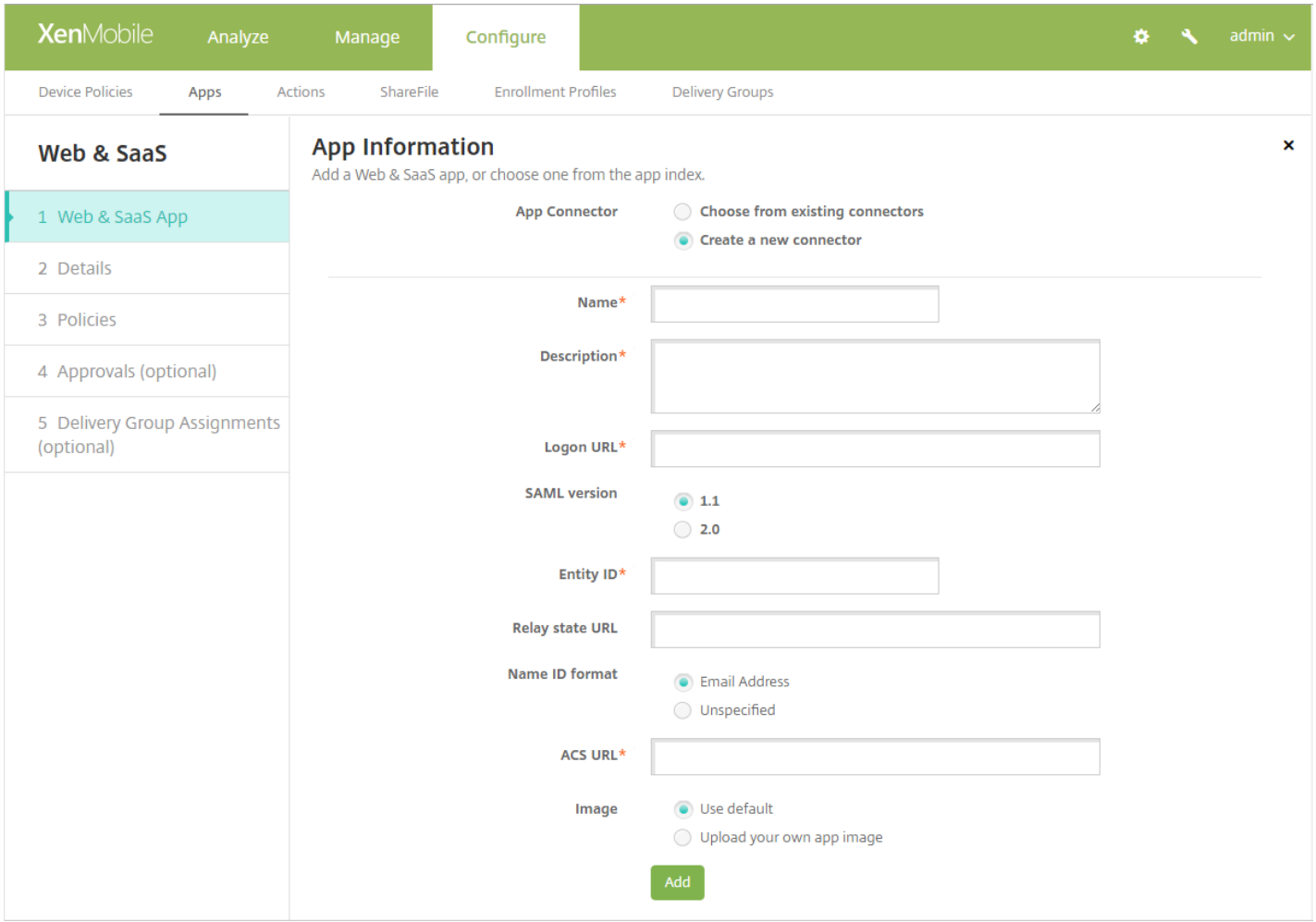
En la página **App Information**, la opción **Choose from existing connectors** ya está seleccionada, como se muestra arriba. En la lista **App Connectors**, haga clic en el conector que quiera usar. Aparecerá la información del conector de aplicaciones.

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 corresponde, 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:
  - **Cuenta de servicio**
    - **User Name**. Escriba el nombre del administrador de la aplicación. Este campo es obligatorio.
    - **Password**. Escriba la contraseña del administrador de la aplicación. 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. La opción predeterminada es Inhabilitar la cuenta (Disable account). Las opciones posibles son:
      - Inhabilitar la cuenta
      - Conservar la cuenta
      - Quitar la cuenta
  - **Regla de nombre de usuario**
    - 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.
- **Requisito de contraseña**
  - **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 los que la contraseña será 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, los usuarios no pueden abrir la aplicación después de que caduquen sus contraseñas.

Para configurar un nuevo conector de aplicaciones

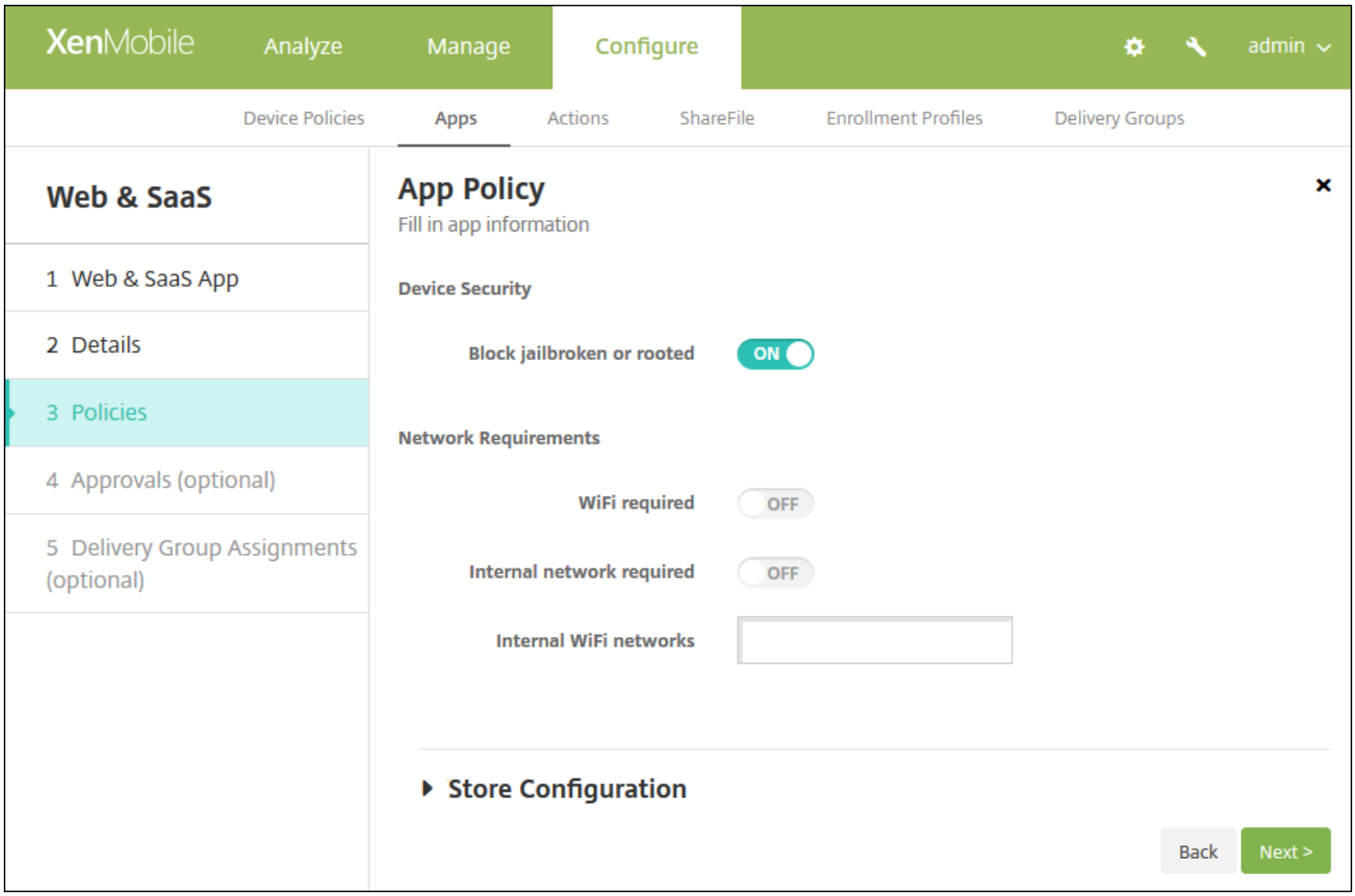
En la página **App Information**, seleccione **Create a new connector**. Aparecerán los campos de información del conector de aplicación.



Configure estos parámetros:

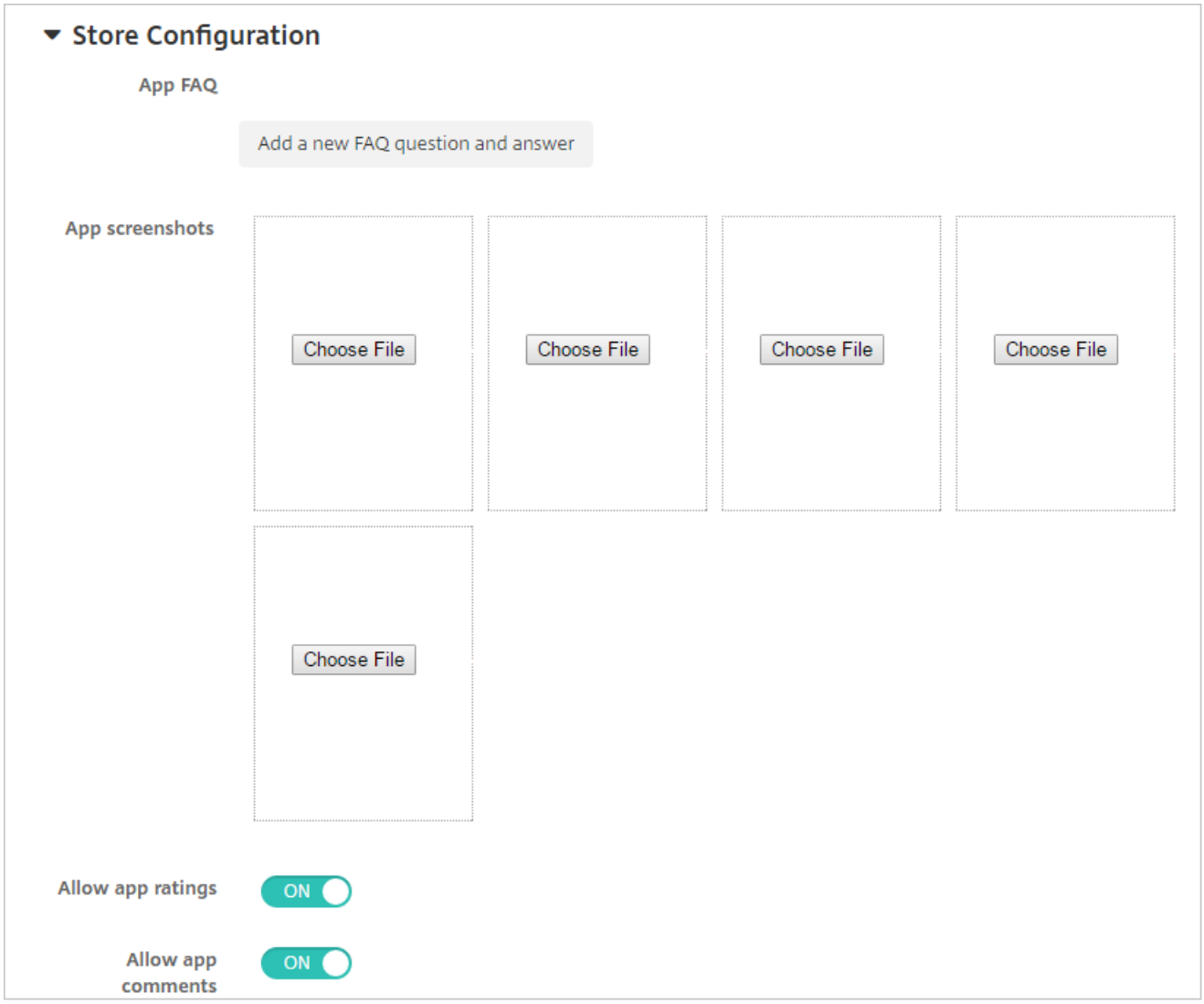
- **Name**. Escriba un nombre para el conector. Este campo es obligatorio.
- **Description**. Escriba una descripción para el conector. Este campo es obligatorio.
- **Logon URL**. Escriba o copie y pegue la URL donde los usuarios inician sesión en el sitio. Por ejemplo, si la aplicación que quiere agregar tiene una página de inicio de sesión, abra un explorador Web y vaya a la página de inicio de sesión de la aplicación. Por ejemplo, puede ser http://www.ejemplo.com/inicio. 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 selecciónelo. El archivo debe ser PNG. No puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.
  - Cuando haya terminado, haga clic en **Add**. Aparecerá la página **Details**.

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. La opción predeterminada es **ON**.
  - **Requisitos de la red**
    - **WiFi required**. Seleccione si se necesita una conexión WiFi para ejecutar la aplicación. La opción predeterminada es **OFF**.
    - **Internal network required**. Seleccione si se necesita una red interna para ejecutar la aplicación. La opción predeterminada es **OFF**.
    - **Internal WiFi networks**. Si habilitó la opción para requerir WiFi, escriba las redes WiFi internas que se van a usar.

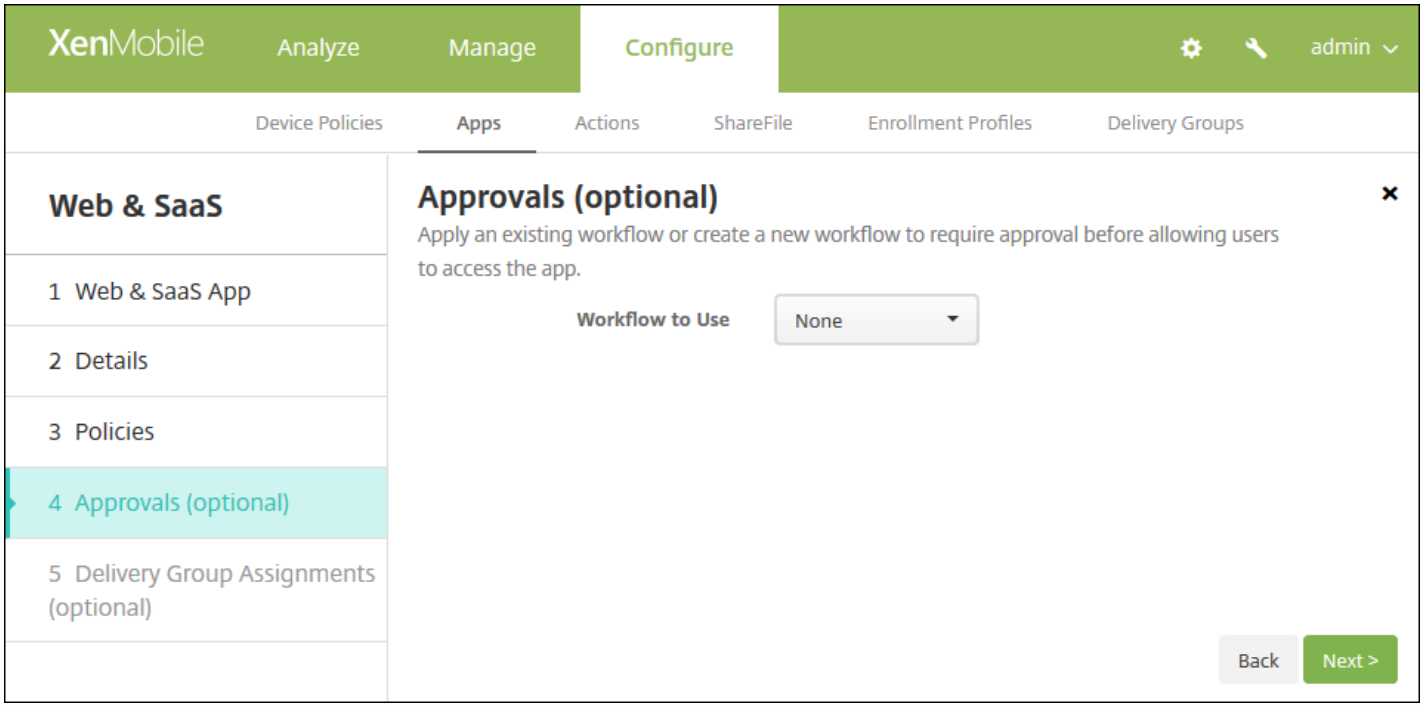
6. Expanda **XenMobile Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en XenMobile 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 XenMobile 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. La opción predeterminada es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. La opción predeterminada es **ON**.

7. Haga clic en **Next**. Aparecerá la página **Approvals**.



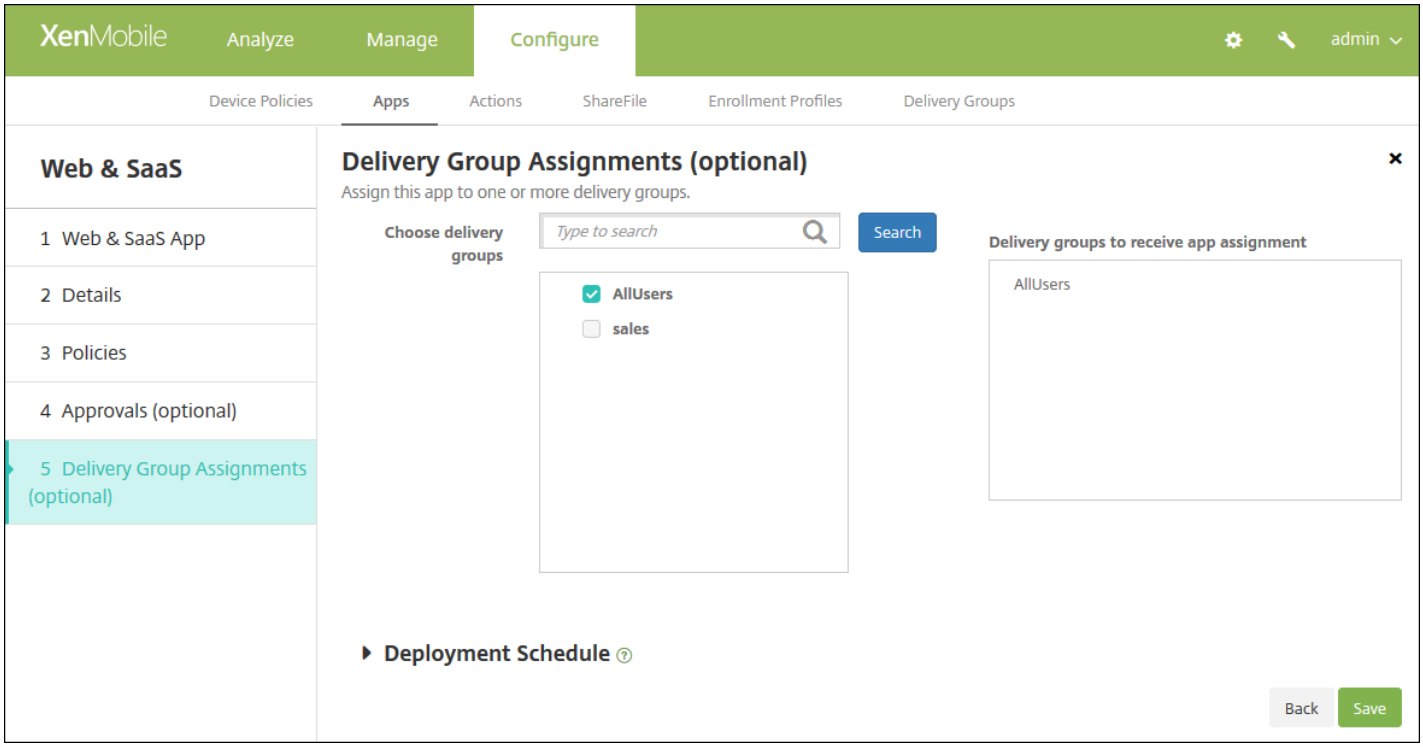
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 8.

Configure estos parámetros 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 al flujo de trabajo. 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:
    - No se necesita
    - 1 nivel
    - 2 niveles
    - 3 niveles
  - **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 Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

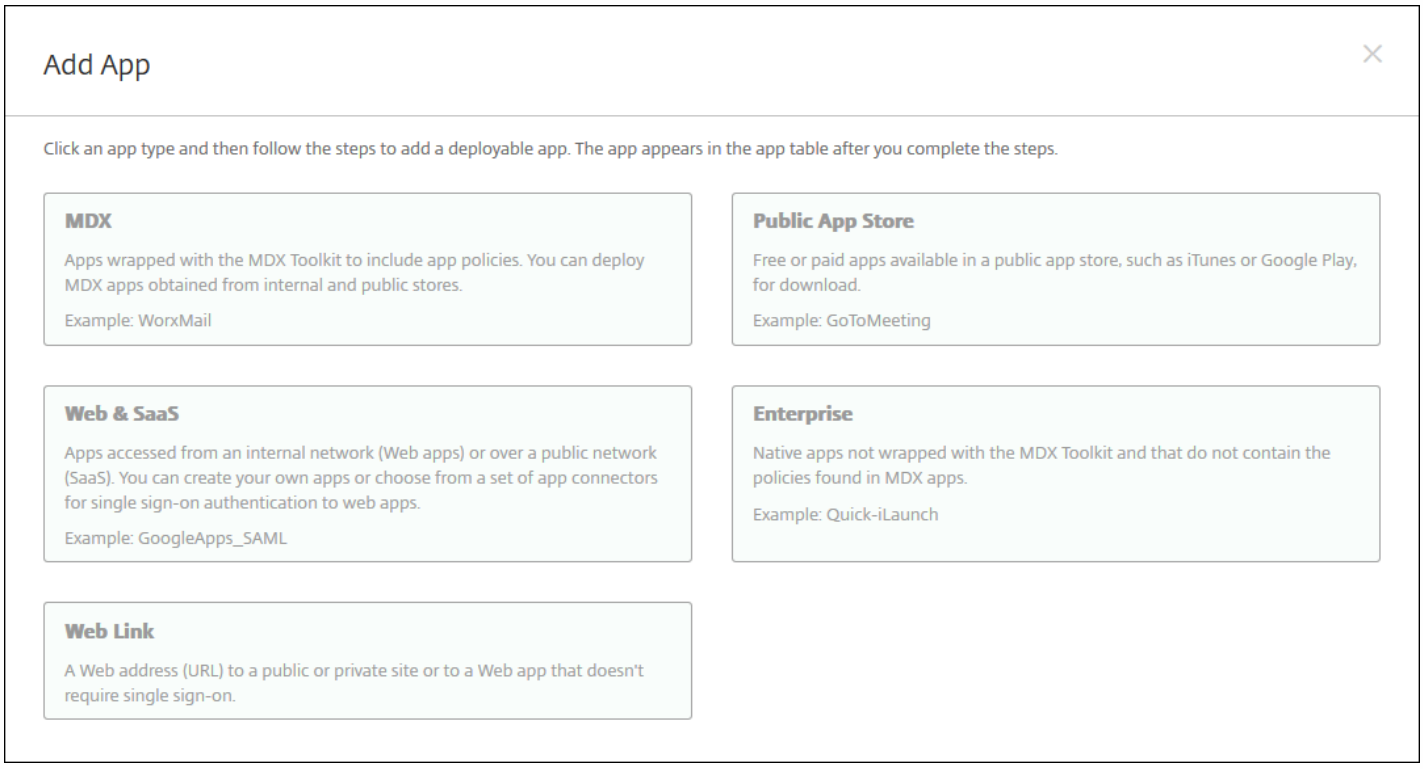
Cómo agregar una aplicación de empresa

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 desde la ficha **Apps** de la consola de XenMobile. Las aplicaciones de empresa admiten las siguientes plataformas (y sus tipos de archivo correspondientes):

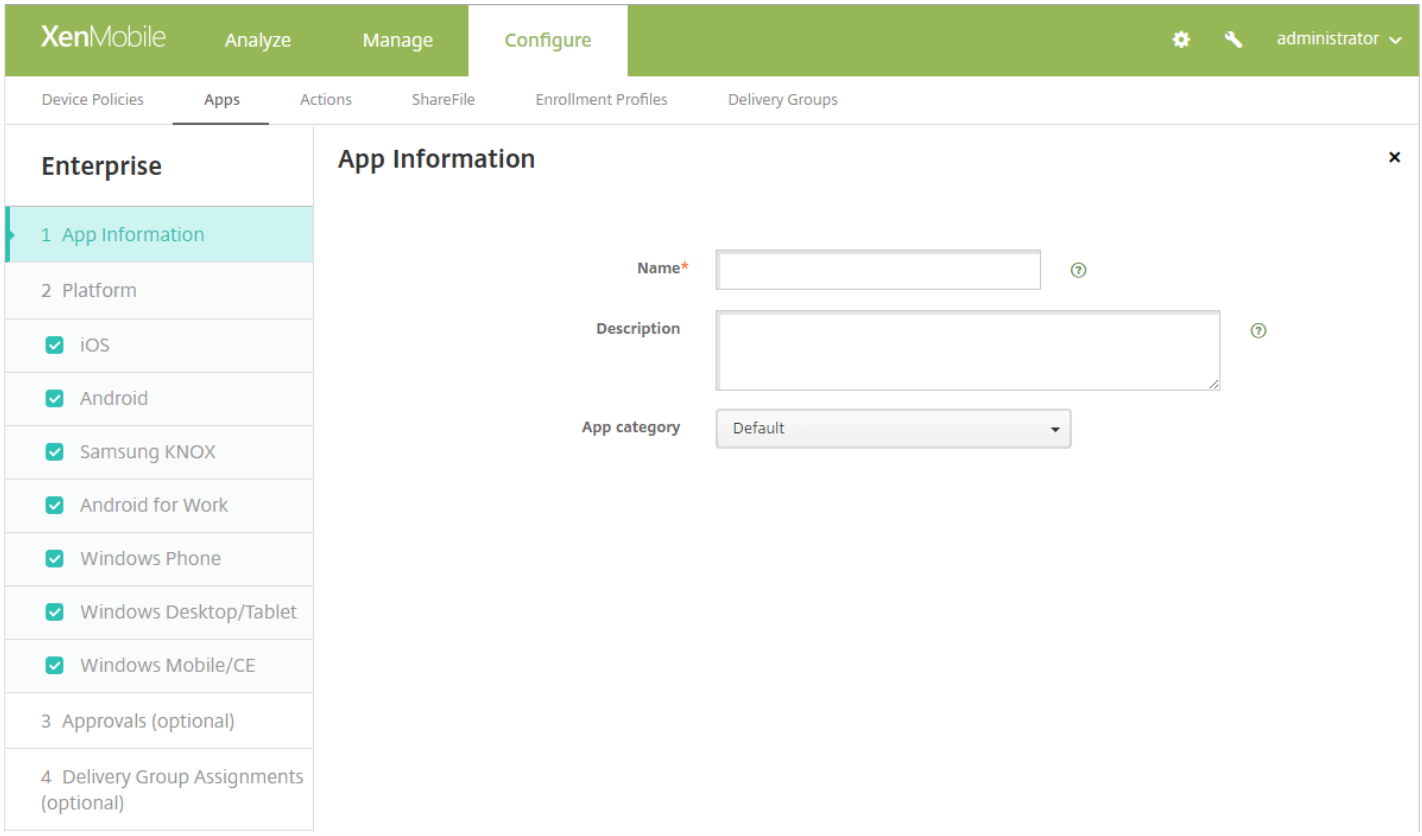
- iOS (archivo .ipa)
- Android (archivo .apk)
- Samsung KNOX (archivo .apk)
- Android for Work (archivo .apk)
- Windows Phone (archivo .xap o .appx)
- Tableta Windows (archivo .appx)
- Windows Mobile/CE (archivo .cab)

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 de una plataforma, consulte el paso 10 para configurar 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.

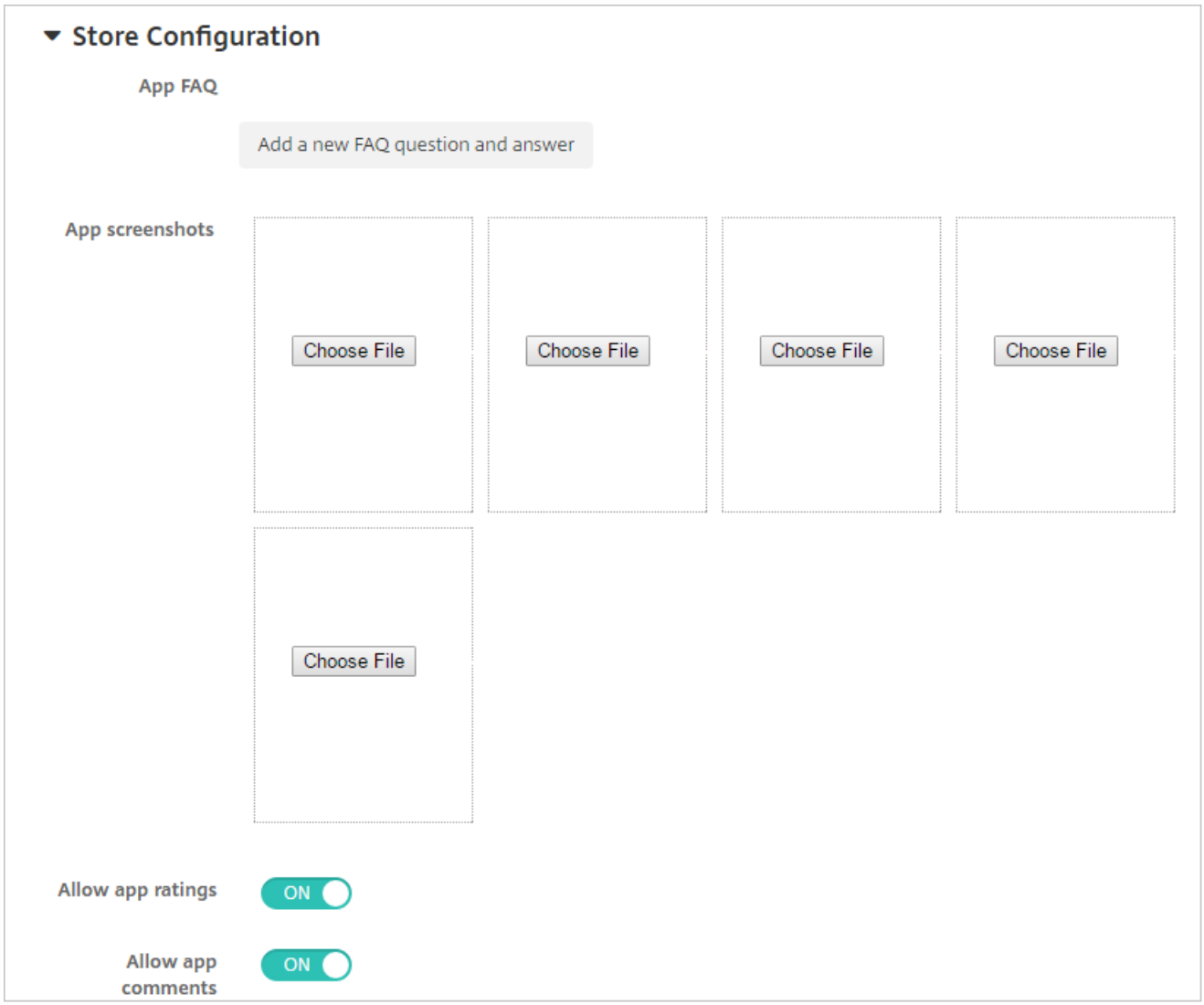
9 Configure los parámetros para el tipo de plataforma, como:

- **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**. 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 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 administrará. Esta configuración se aplica a dispositivos iOS 9.x.

10. Configure las reglas de implementación.

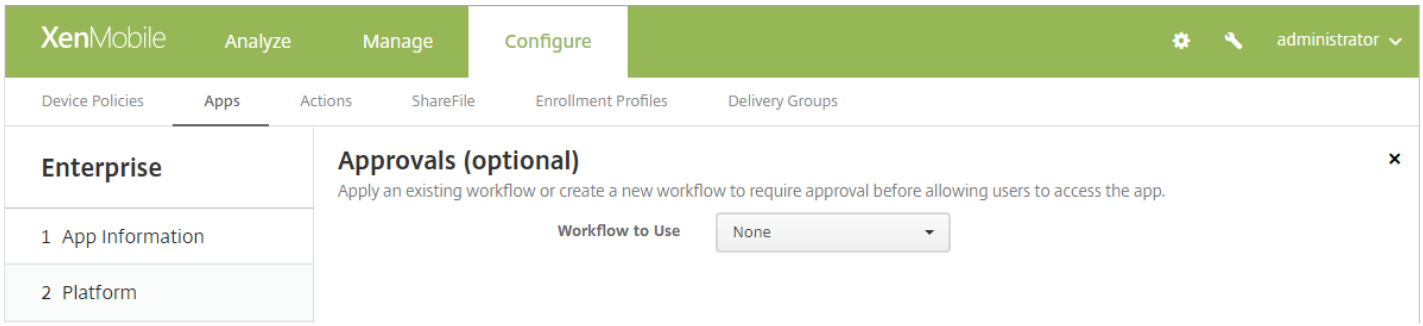
11. Expanda **XenMobile Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en XenMobile 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 XenMobile 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. La opción predeterminada es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. La opción predeterminada es **ON**.

12. Haga clic en **Next**. Aparecerá la página **Approvals**.



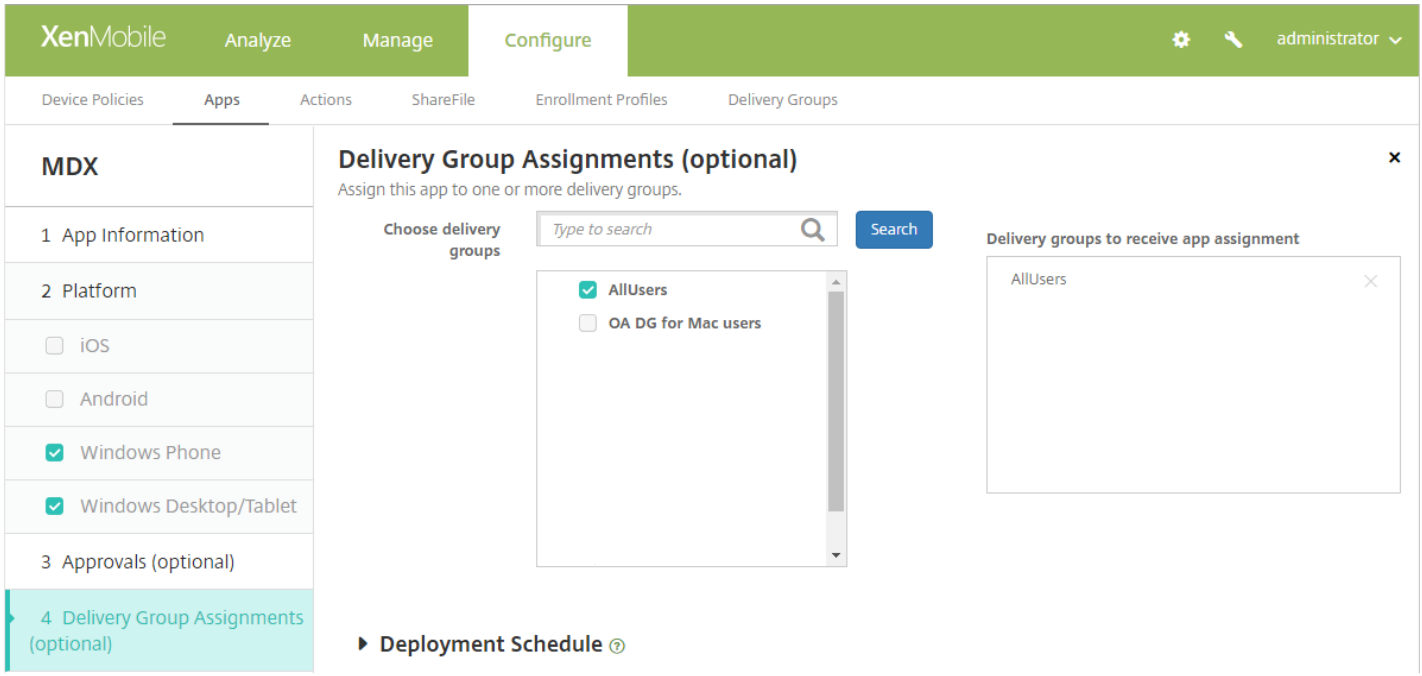
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 13.

Configure estos parámetros 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 al flujo de trabajo. 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:
    - No se necesita
    - 1 nivel
    - 2 niveles
    - 3 niveles
  - **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. Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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 un enlace Web

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).

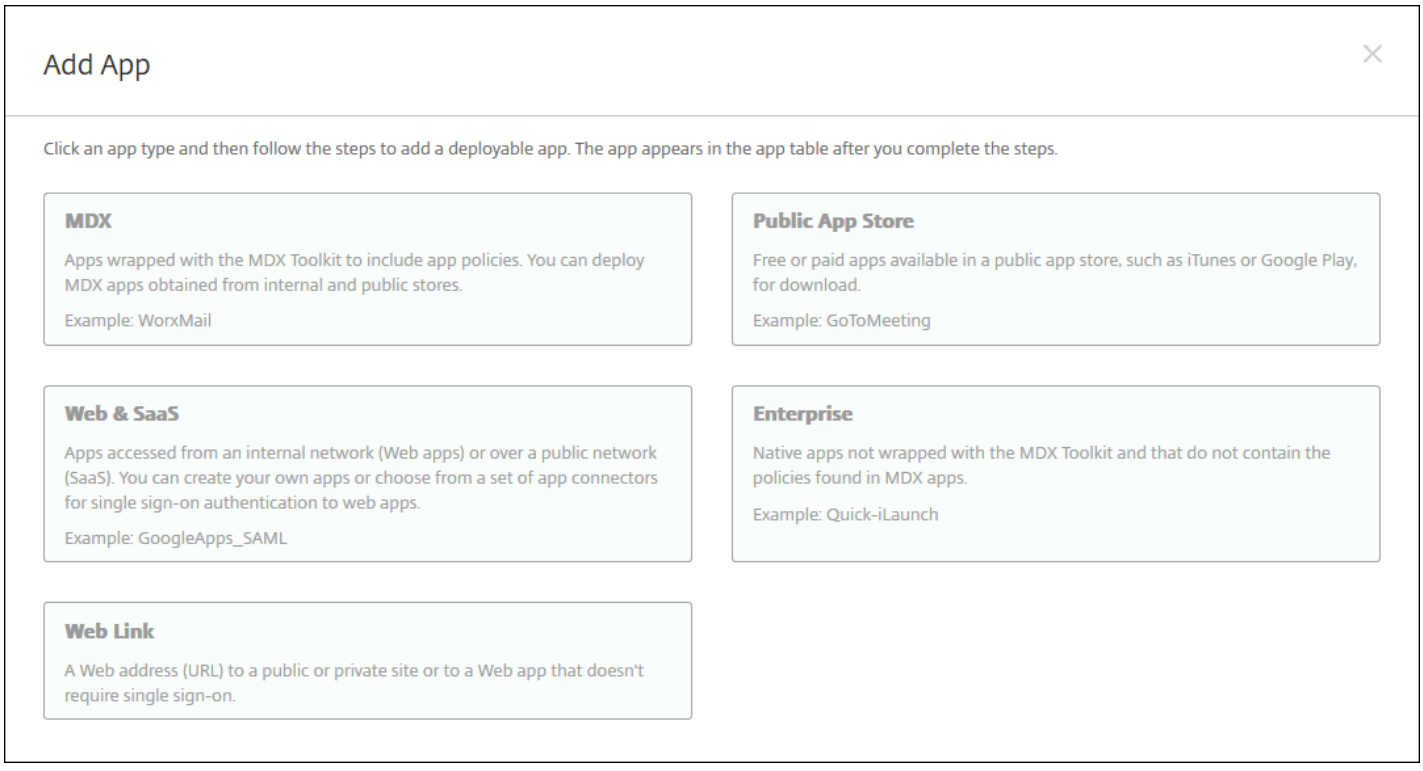
Puede configurar enlaces Web desde la ficha **Apps** de la consola de XenMobile. Una vez configurado el enlace Web, este aparece como un icono de enlace en la lista de la tabla **Apps**. Cuando los usuarios inician sesión en Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Para agregar el enlace, debe proporcionar la siguiente información:

- Nombre del 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**.

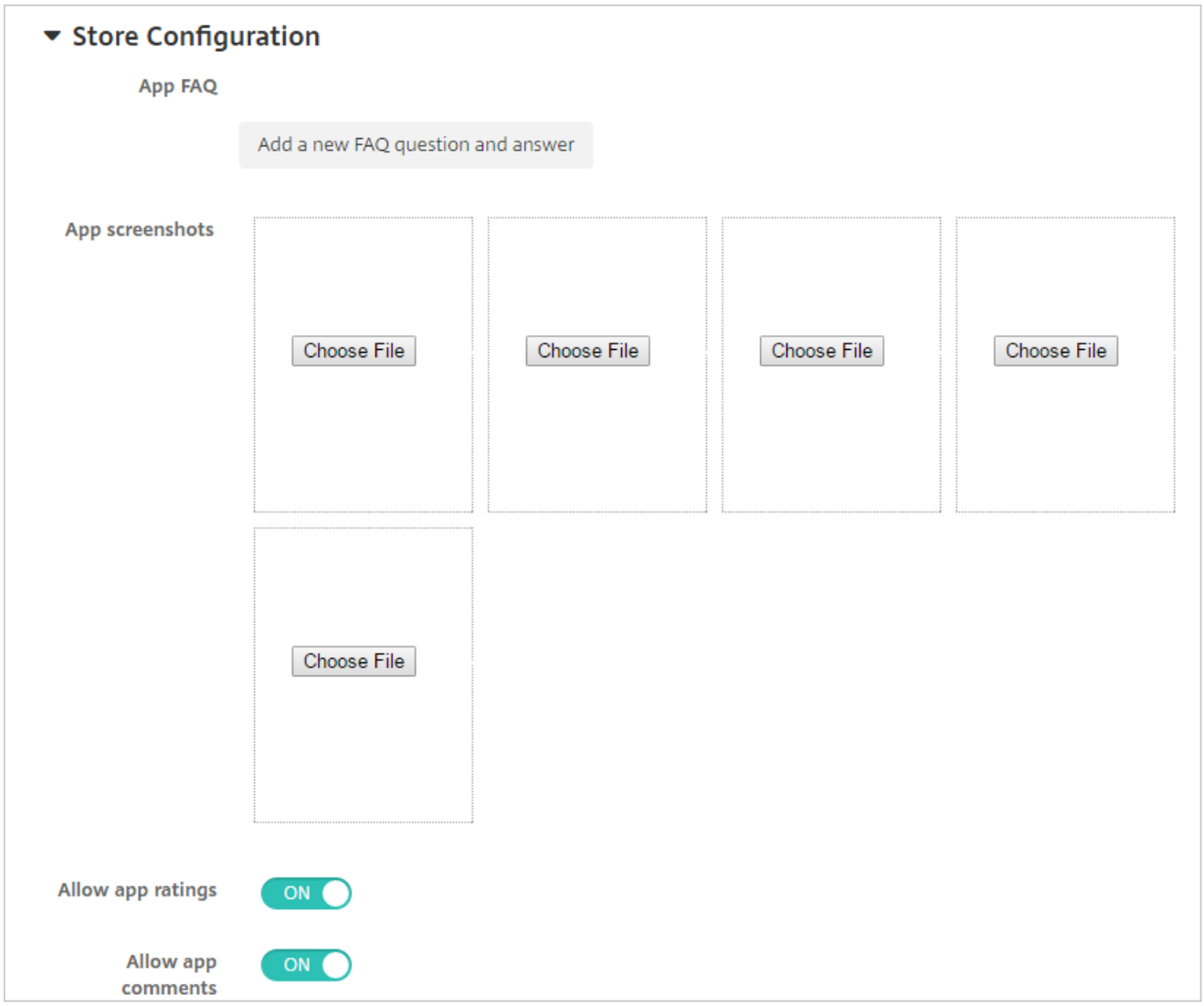


3. Haga clic en **Web Link**. Aparecerá la página **App Information**.

4. Configure 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.
- **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 selecciónelo. 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 **XenMobile Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en

XenMobile 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 XenMobile 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. La opción predeterminada es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. La opción predeterminada es **ON**.

6. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.

7. Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. 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 bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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**.

Cómo habilitar aplicaciones de Microsoft 365

Puede abrir el contenedor MDX para permitir a Secure Mail, Secure Web y ShareFile que transfieran documentos y datos a las aplicaciones de Microsoft Office 365. Para obtener más información, consulte Interacción segura con aplicaciones Office 365.

Creación y administración de flujos de trabajo

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.

Al configurar XenMobile por primera vez, se definen los parámetros de correo electrónico referentes al flujo de trabajo; estos parámetros se deben establecer antes de utilizar los 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.

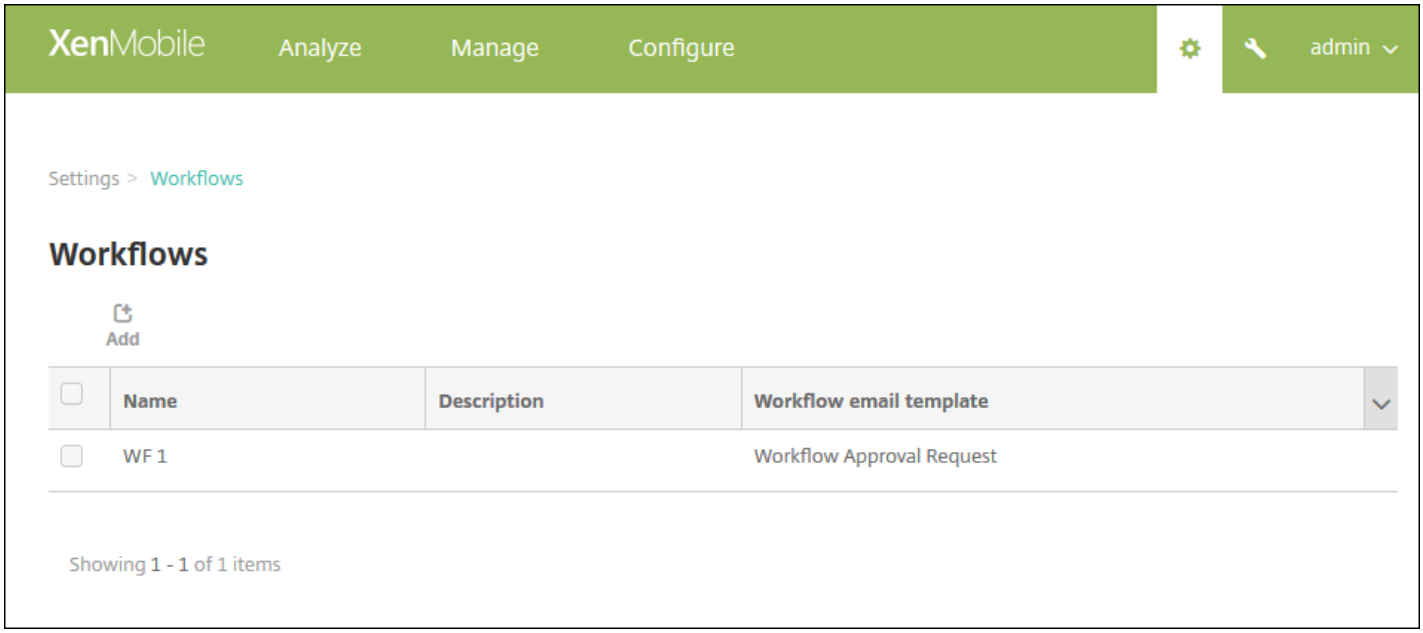
Puede configurar flujos de trabajo en dos lugares de XenMobile:

- 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 solicitudes de cuentas de usuario.

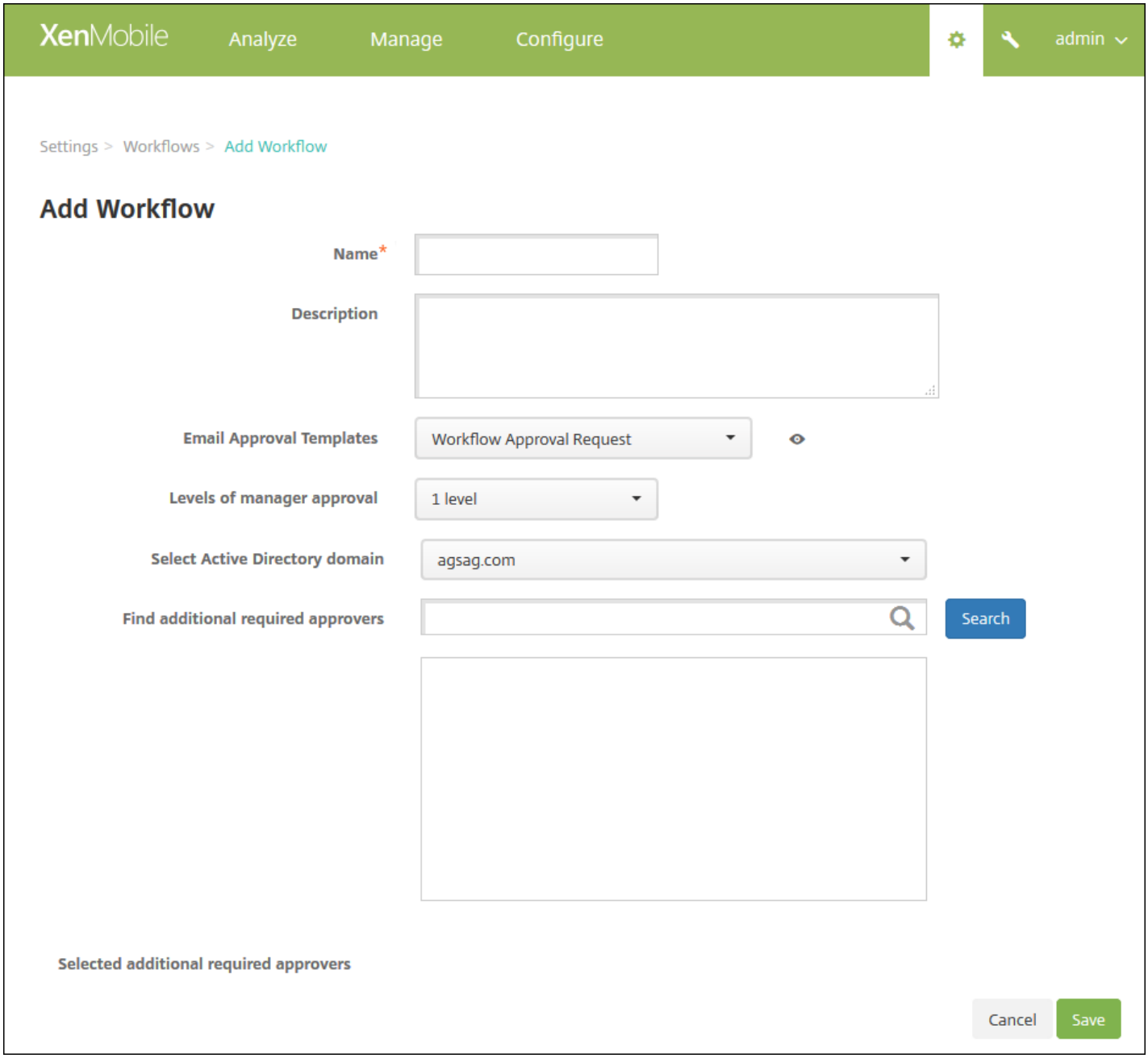
Se puede asignar hasta tres niveles de la aprobación del tipo administrador para cuentas de usuario. Si necesita que otras personas aprueben la cuenta de usuario, puede buscar y seleccionar aprobadores adicionales por nombre o dirección de correo electrónico de la persona. Cuando XenMobile las encuentre, 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 el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.

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

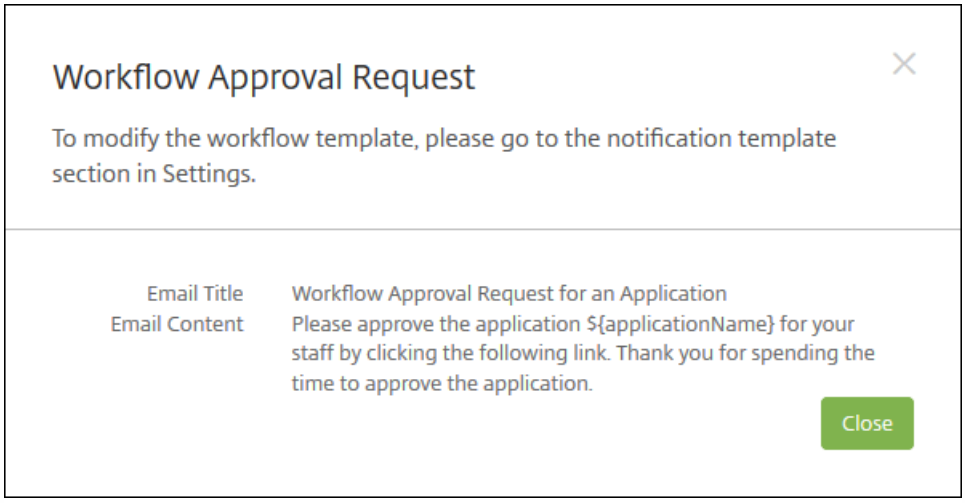


3. Haga clic en **Add**. Aparecerá la página **Add Workflow**.



4. Configure estos 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 al flujo de trabajo. En la consola de XenMobile, puede crear plantillas de correo electrónico en la sección Notification Templates, en Settings. Cuando haga clic en el icono con forma de ojo situado a la derecha del campo, aparece el siguiente cuadro de diálogo.



- **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:
  - No se necesita
  - 1 nivel
  - 2 niveles
  - 3 niveles
- **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.

5. 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 a él.

2. Para eliminar un flujo de trabajo, haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Delete**.

Importante: Esta operación no se puede deshacer.

Tipos de conectores de aplicaciones

Feb 27, 2017

La tabla siguiente muestra los conectores y los tipos de conectores que están disponibles en XenMobile cuando se agrega una aplicación Web o SaaS. También puede agregar un conector nuevo a XenMobile cuando agregue una aplicación Web o SaaS.

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 SSO.
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

Actualización de aplicaciones MDX o de empresa

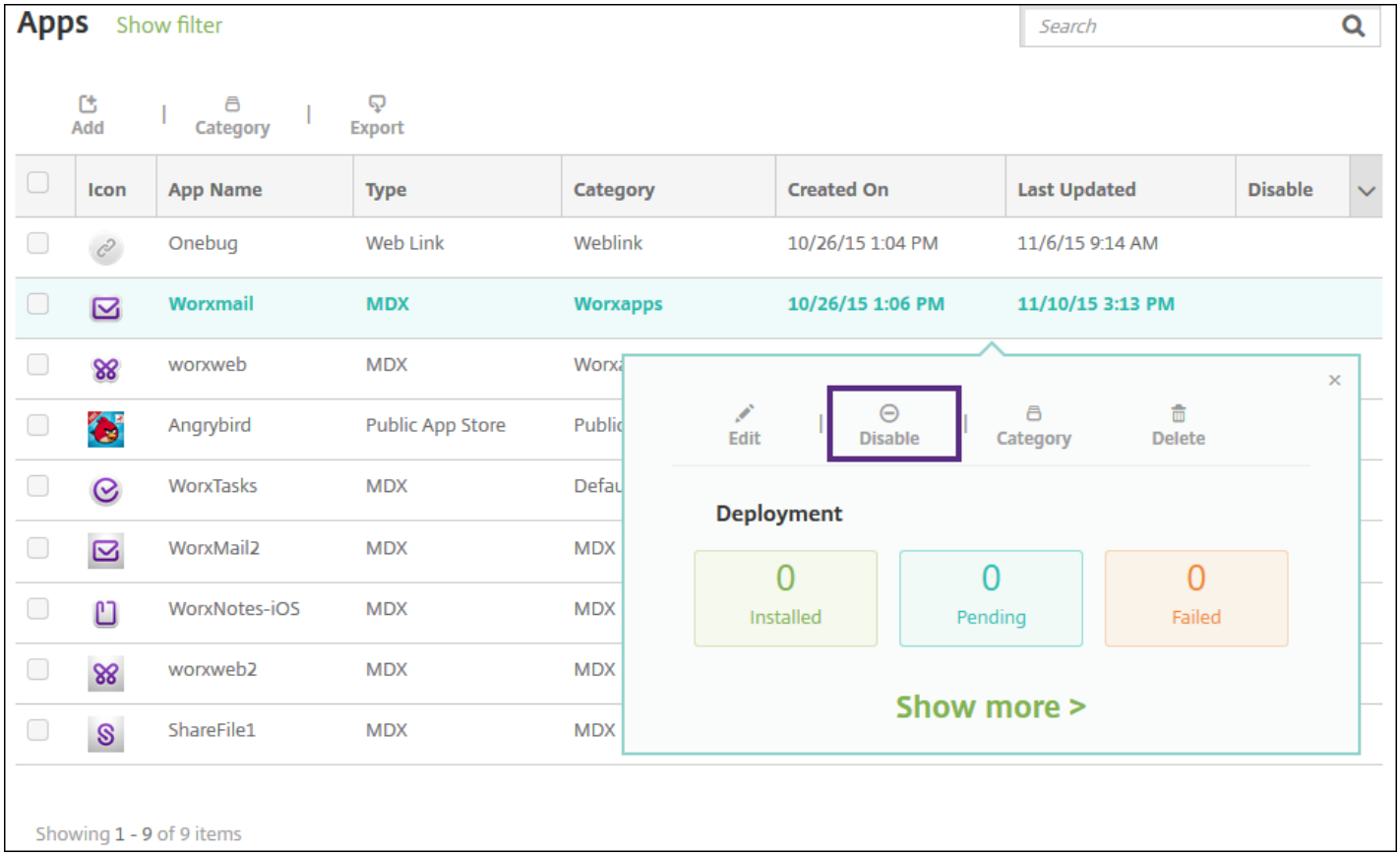
Feb 27, 2017

En XenMobile, para actualizar una aplicación MDX o de empresa, puede inhabilitarla en la consola de XenMobile y cargar luego la nueva versión de esta.

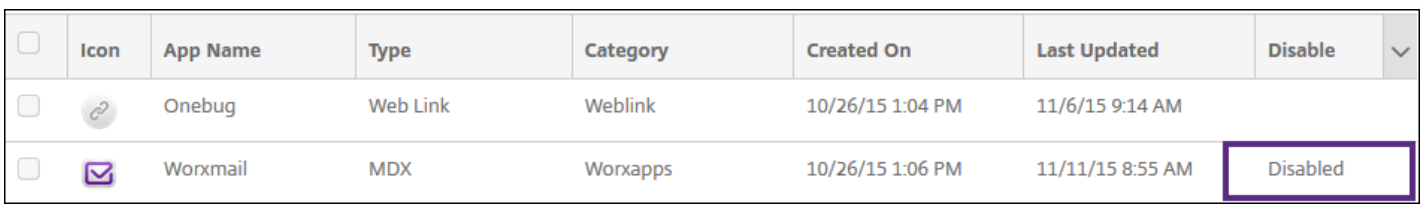
1. En la consola de XenMobile, haga clic en **Configure > Apps**. Aparecerá la página **Apps**.

2. En el caso de dispositivos administrados (dispositivos inscritos en XenMobile para la administración de dispositivos móviles), vaya directamente al paso 3. En el caso de dispositivos no administrados (dispositivos inscritos en XenMobile solo para la administración de aplicaciones de empresa), lleve a cabo lo siguiente:

- Para actualizar una aplicación, en la tabla **Apps**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.
- Haga clic en **Disable** en el menú que aparecerá.



- Haga clic en **Disable** en el cuadro de diálogo de confirmación. Aparecerá la etiqueta *Disabled* en la columna **Disable** de la aplicación.



Nota: Inhabilitar una aplicación significa colocarla en modo de mantenimiento. Mientras la aplicación está inhabilitada, los usuarios no pueden volver a conectarse a ella después de cerrar sesión. Inhabilitar una aplicación es opcional, aunque se recomienda inhabilitarla para evitar problemas de funcionalidad. Por ejemplo, pueden ocurrir problemas debido a actualizaciones de directivas o si los usuarios solicitan una descarga al mismo tiempo que se carga la aplicación en XenMobile.

3. Para actualizar una aplicación, en la tabla **Apps**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.

4. Haga clic en **Edit** en el menú que aparecerá. Aparecerá la página **App Information**, con las plataformas que eligió en su momento para la aplicación seleccionada.

5. Configure estos parámetros:

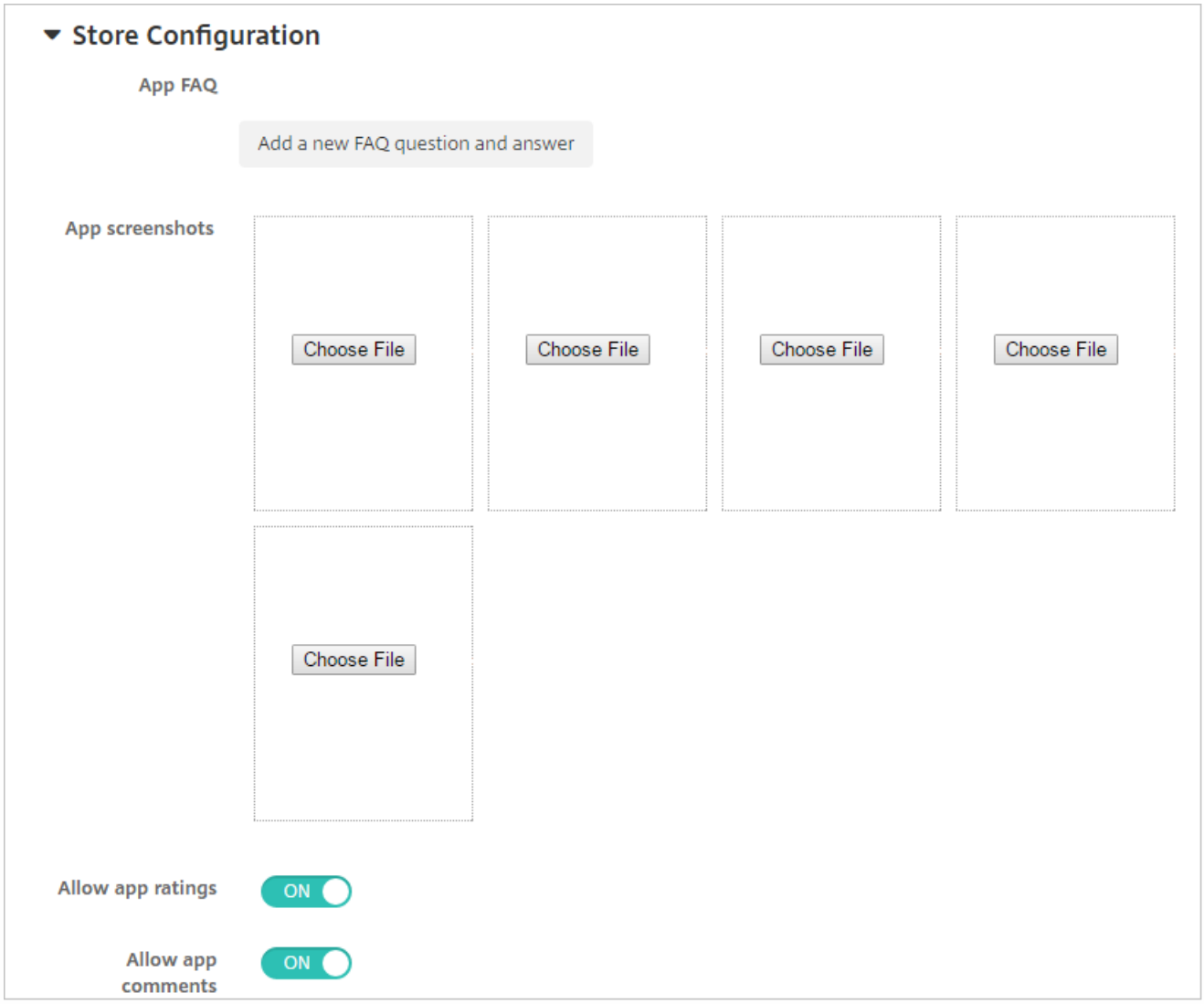
- **Name**. Si quiere, puede cambiar el nombre de la aplicación.
- **Description**. Si quiere, puede cambiar la descripción de la aplicación.
- **App category**. Si quiere, puede cambiar la categoría de aplicación.

6. Haga clic en **Next**. Aparecerá la página de la primera plataforma seleccionada. Lleve a cabo lo siguiente para cada plataforma seleccionada:

- Elija el archivo de sustitución que quiera cargar. Para ello, haga clic en **Upload** y vaya a la ubicación del archivo. La aplicación se cargará en XenMobile.
- Si quiere, puede cambiar los datos de la aplicación y la configuración de directiva para la plataforma.
- También puede configurar reglas de implementación (consulte el paso 7) y configuraciones de XenMobile Store (consulte el paso 8).

7. Configure las reglas de implementación.

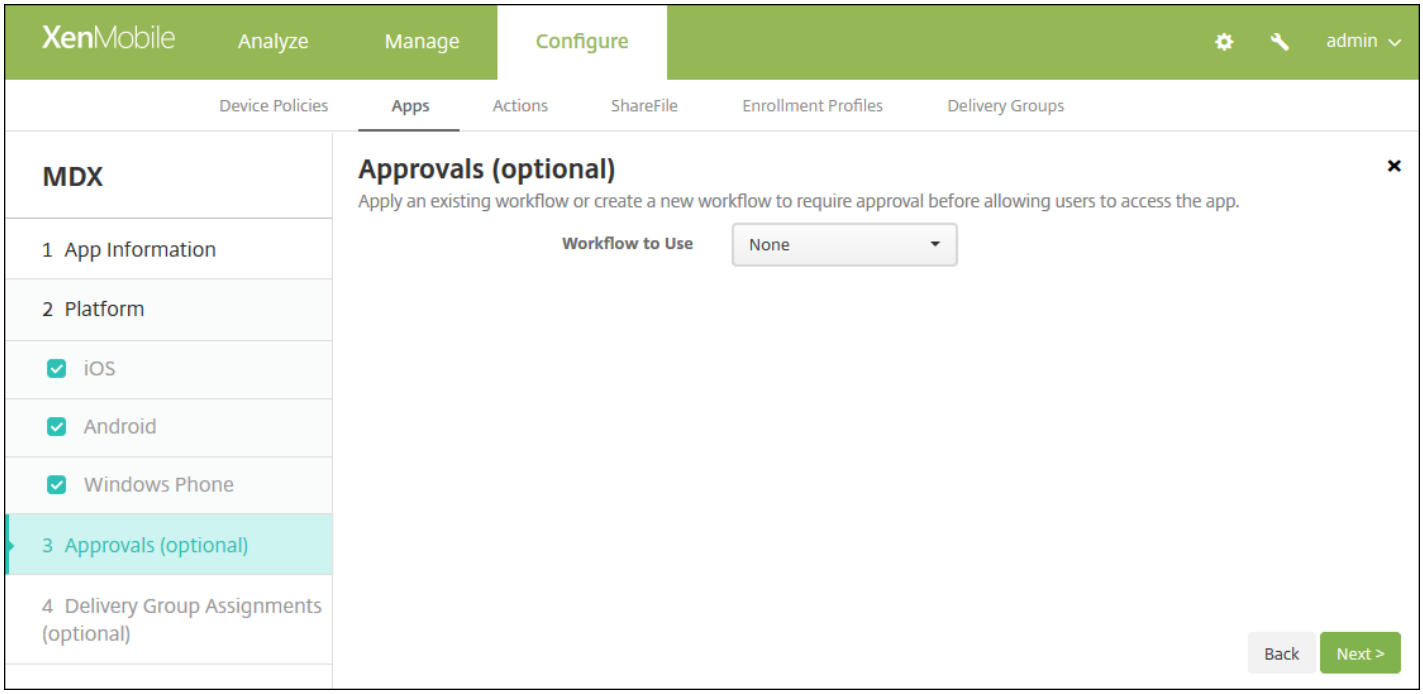
8. Expanda **Store Configuration**.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en XenMobile 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 XenMobile 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. La opción predeterminada es **ON**.
  - **Allow app comments**. Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. La opción predeterminada es **ON**.

9 Haga clic en **Next**. Aparecerá la página **Approvals**.



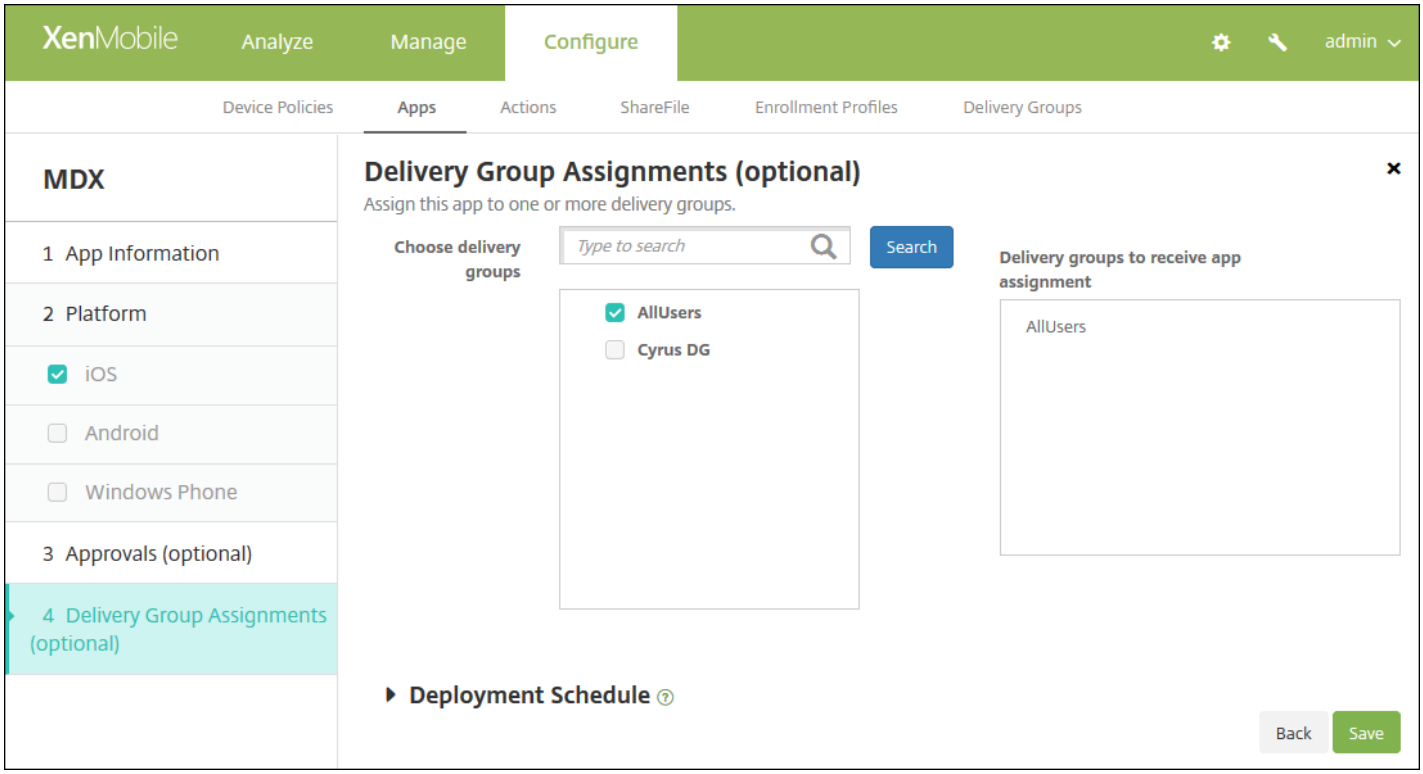
10. Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 11.

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 al flujo de trabajo. 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:
    - No se necesita
    - 1 nivel
    - 2 niveles
    - 3 niveles
  - **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.

11. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.



12. Escriba en **Choose delivery groups** para buscar un grupo de entrega o seleccione uno o varios grupos de la lista a los que quiera asignar la aplicación. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

13. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **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.

14. Haga clic en **Save**. Aparecerá la página **Apps**.

15 Si ha inhabilitado la aplicación en el paso 2, haga lo siguiente:

- En la ficha **Apps**, haga clic para seleccionar la aplicación actualizada y, en el menú que aparecerá, haga clic en **Enable**.
- En el cuadro de confirmación que aparece, haga clic en **Enable**. Ahora, los usuarios podrán acceder a la aplicación y recibir una notificación que les pedirá actualizarla.

Directivas de aplicaciones MDX

Feb 27, 2017

Para ver una lista de las directivas de aplicación MDX para iOS, Android y Windows con notas sobre las restricciones aplicables y las recomendaciones de Citrix, consulte Vista general de las directivas de aplicaciones MDX en la documentación de MDX Toolkit.

Personalización de marca en XenMobile Store y Citrix Secure Hub

Feb 27, 2017

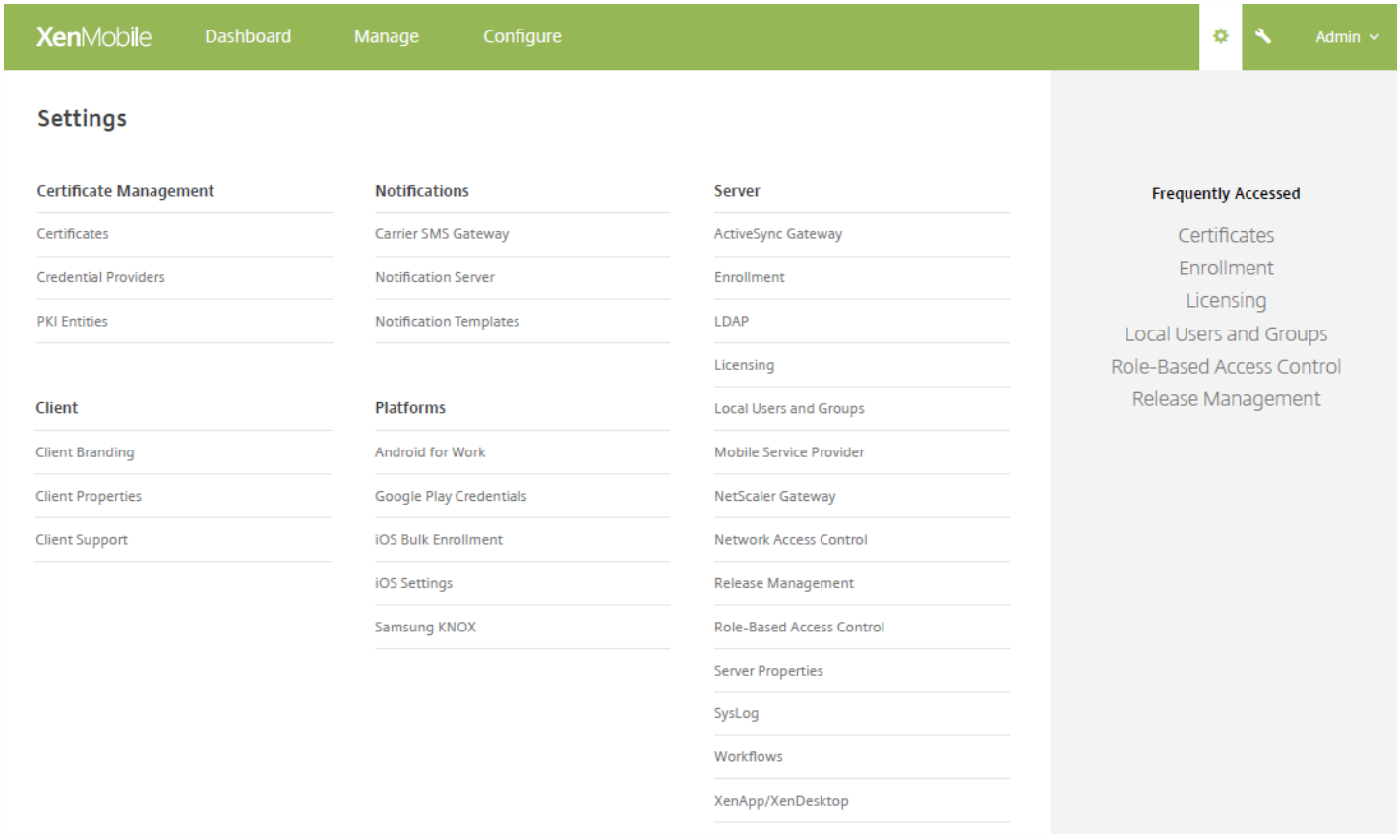
Puede configurar el modo en que aparecen las aplicaciones en la tienda de aplicaciones y agregar un logo de su propia marca en Secure Hub y XenMobile Store. Estas funciones de personalización están disponibles para dispositivos iOS y Android.

Nota: Antes de comenzar, compruebe que la imagen de personalización está preparada y se puede acceder a ella.

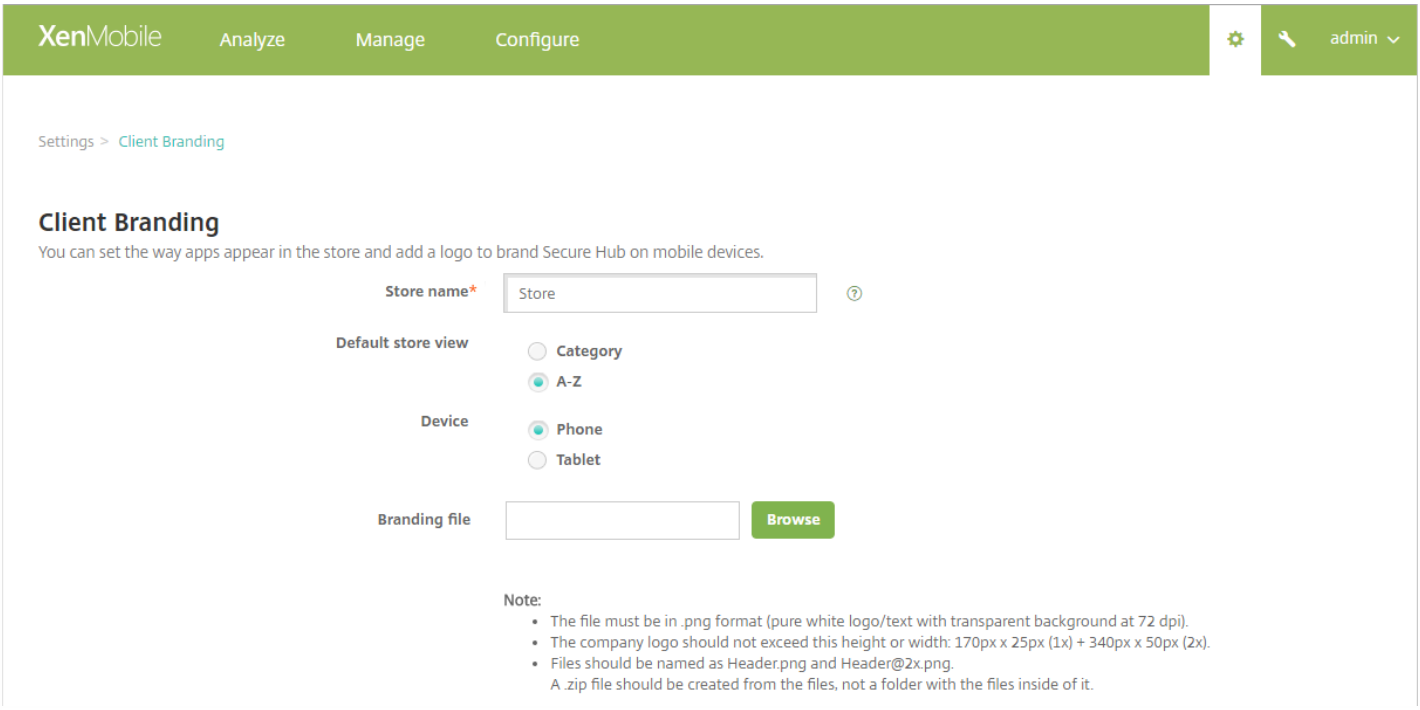
La imagen personalizada debe cumplir los siguientes requisitos:

- El archivo debe estar en formato PNG.
- Use un texto o logotipo blancos puros con un fondo transparente de 72 ppp.
- El logotipo de empresa no debe superar el alto o el ancho de 170 píxeles x 25 píxeles (1x) ni 340 píxeles x 50 píxeles (2x).
- Establezca el nombre de los archivos como Header.png y Header@2x.png.
- Cree un archivo ZIP con los archivos, no una carpeta con los archivos en ella.

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



2. En **Client**, haga clic en **Client Branding**. Aparecerá la página **Client Branding**.



Configure los siguientes parámetros:

- **Store name**. El nombre de tienda que aparecerá en la información de la cuenta de usuario. Si cambia el nombre, también se cambia la URL que se usa para acceder a los servicios de tienda. Por lo general, no es necesario cambiar el nombre predeterminado.
- **Default store view**. Seleccione **Category** o **A-Z**. El valor predeterminado es **A-Z**.
- **Device option**. Seleccione **Phone** o **Tablet**. El valor predeterminado **Phone**.
- **Branding file**. Seleccione un archivo o un ZIP con las imágenes que se van a usar para la personalización. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

3. Haga clic en **Save**.

Para implementar este paquete en los dispositivos de los usuarios, debe crear un paquete de implementación e implementarlo en los dispositivos.

Citrix Launcher

Feb 27, 2017

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android implementados por XenMobile. La versión mínima de Android que se admite para que Secure Hub administre Citrix Launcher es Android 4.0.3. Puede agregar la **directiva de configuración de Launcher** para controlar estas características de Citrix Launcher:

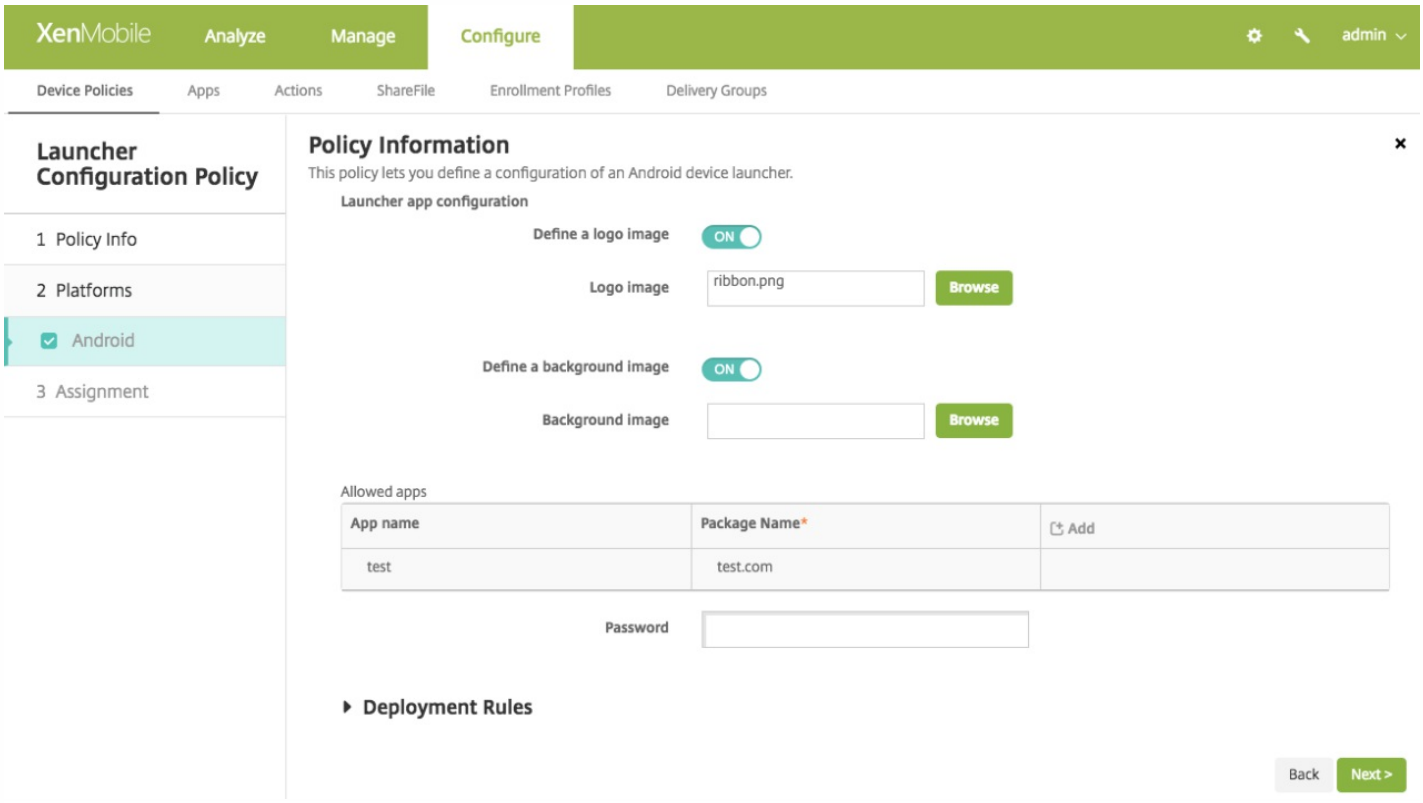
- Administre los dispositivos Android, de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña que los usuarios deban introducir para salir de Launcher.

Si bien Citrix Launcher permite aplicar restricciones a nivel de dispositivo, también concede a los usuarios acceso integrado a las configuraciones de los dispositivos (como los parámetros de WiFi, Bluetooth y los parámetros de códigos de acceso). Citrix Launcher no está diseñado como una capa de seguridad adicional situada sobre la capa que la plataforma del dispositivo ya proporciona.

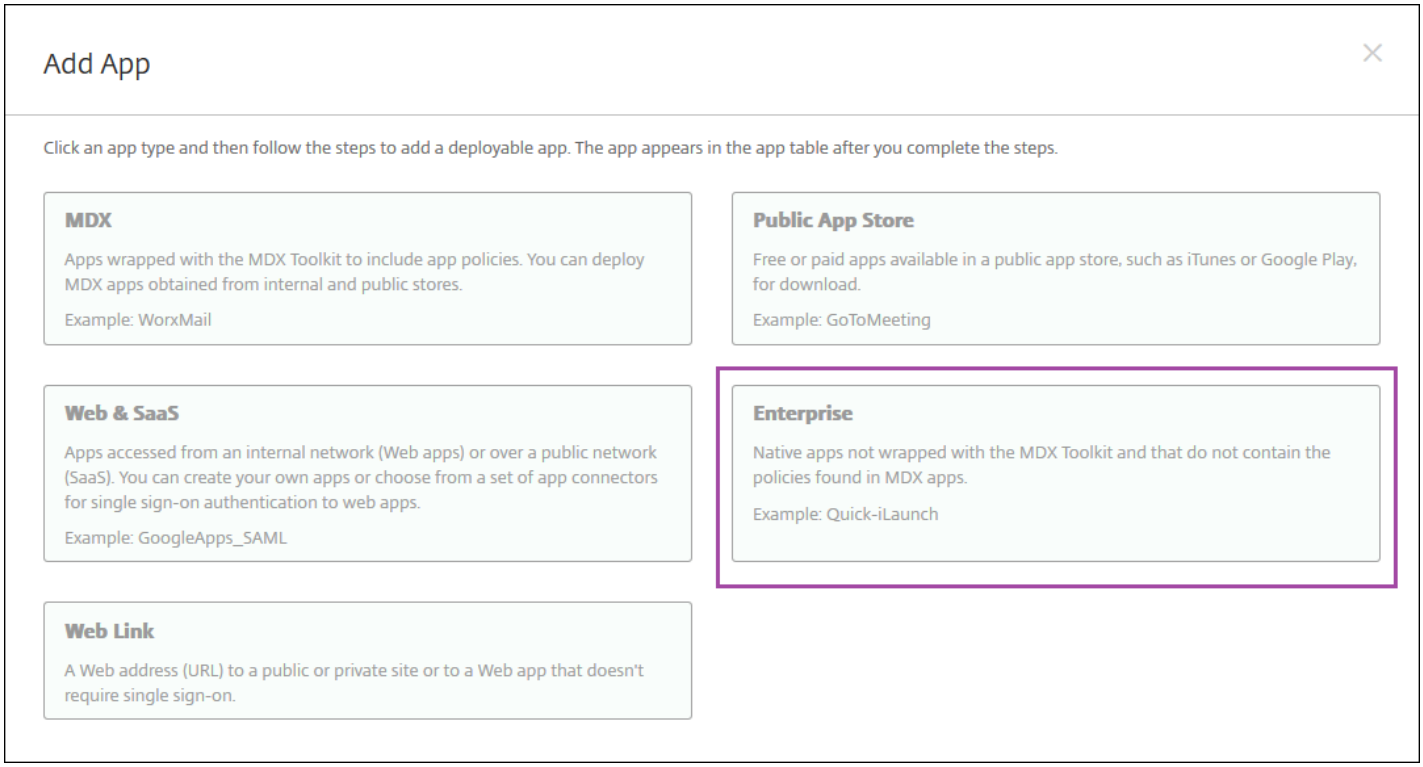
Para proporcionar Citrix Launcher a dispositivos Android, siga estos pasos generales.

1. Descargue la aplicación Citrix Launcher desde la página de descargas de Citrix XenMobile de su edición de XenMobile. El nombre del archivo es CitrixLauncher.apk. El archivo está listo para cargarlo en XenMobile y no requiere empaquetado.

2. Agregue la directiva de dispositivo **Launcher Configuration Policy**: Vaya a **Configure > Device Policies**, haga clic en **Add** y, en el cuadro de diálogo **Add a New Policy**, empiece a teclear **Launcher**. Para obtener más información, consulte Launcher Configuration Policy.

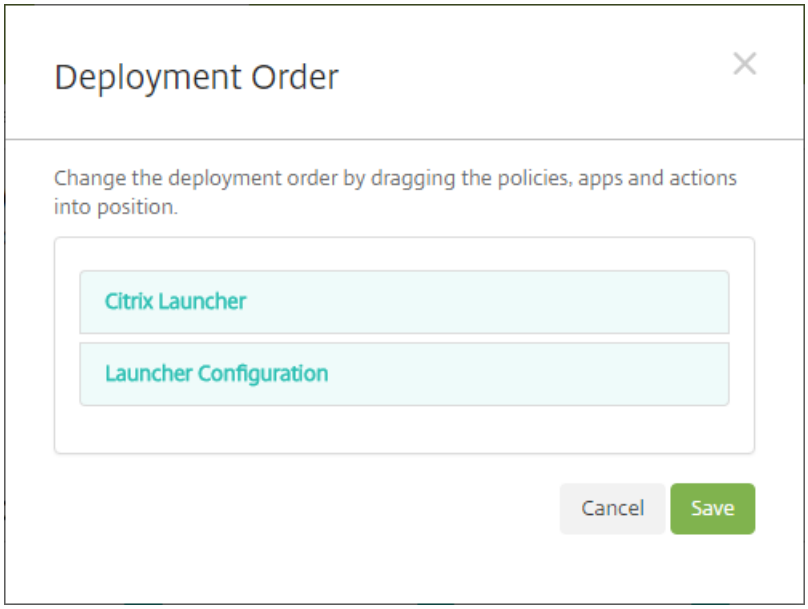


3. Agregue la aplicación Citrix Launcher a XenMobile como una aplicación de empresa. Puede hacerlo desde **Configure > Apps**, donde deberá hacer clic en **Add** y, a continuación, en **Enterprise**. Para obtener información más detallada, consulte Cómo agregar una aplicación de empresa.



4. Cree un grupo de entrega de Citrix Launcher con la siguiente configuración en **Configure > Delivery groups**:

- En la página **Policies**, agregue **Launcher Configuration Policy**.
- En la página **Apps**, arrastre **Citrix Launcher** a **Required Apps**.
- En la página **Summary**, haga clic en **Deployment Order** y compruebe que la aplicación **Citrix Launcher** precede a la directiva **Launcher Configuration**.



Para obtener más información, consulte Implementación de recursos.

Programa de Compras por Volumen de iOS

Apr 04, 2017

Puede administrar las licencias de las aplicaciones iOS mediante el Programa de Compras por Volumen (VPP) de Apple. El programa VPP simplifica el proceso de búsqueda, compra y distribución de aplicaciones (y otros datos) de forma masiva en una organización.

Con VPP, puede usar XenMobile para distribuir aplicaciones de tienda pública. El programa VPP no se respalda para las aplicaciones XenMobile ni para las aplicaciones empaquetadas con MDX Toolkit. Aunque puede distribuir las aplicaciones XenMobile desde la tienda pública mediante VPP, la implementación no es la óptima. Se requieren más mejoras en el servidor XenMobile y el almacén de Secure Hub para solucionar las limitaciones. Para obtener una lista de los problemas conocidos a la hora de implementar las aplicaciones XenMobile desde la tienda pública vía VPP y las posibles soluciones a esos problemas, consulte este artículo en Support Knowledge Center de Citrix.

Con VPP, puede distribuir directamente las aplicaciones adecuadas en los dispositivos. O bien, puede asignar contenido a los usuarios mediante códigos de canje. En XenMobile, puede configurar parámetros específicos del Programa de Compras por Volumen de iOS.

Periódicamente, XenMobile vuelve a importar licencias del Programa de Compras por Volumen (VPP) desde Apple para que estas reflejen todos los cambios. Se trata de cambios como, por ejemplo, la eliminación manual de una aplicación importada del programa VPP. De forma predeterminada, XenMobile actualiza el punto de referencia para licencias VPPcada 720 minutos como mínimo. Puede cambiar el intervalo del punto de referencia desde la propiedad de servidor "VPP baseline interval" (vpp.baseline). Para obtener más información, consulte Propiedades de servidor.

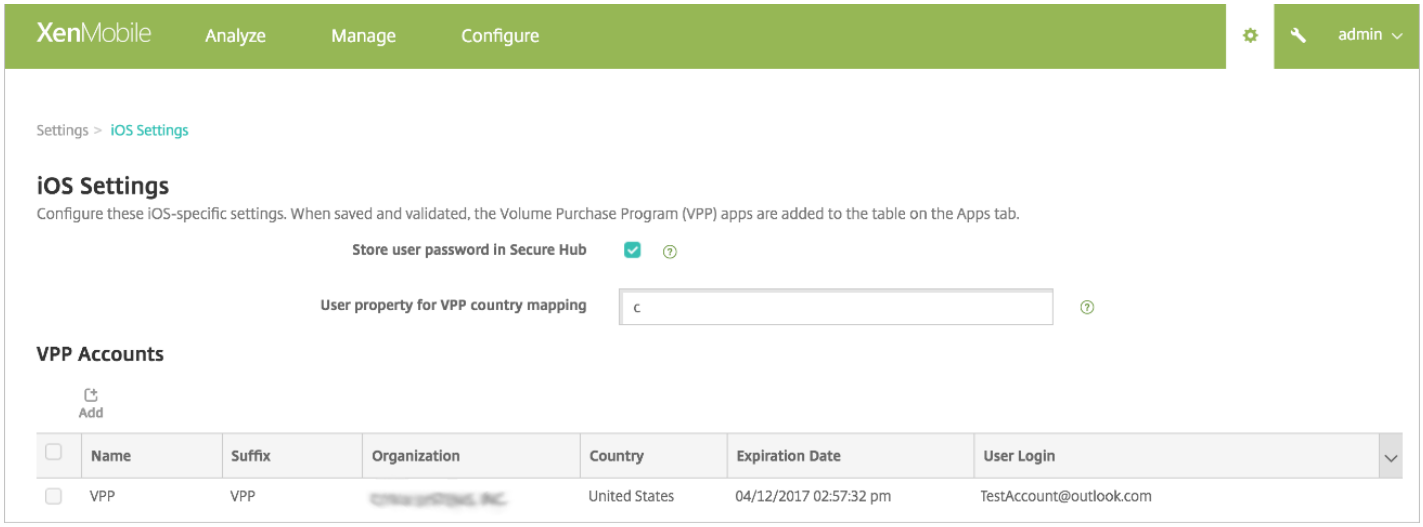
En este artículo, se describe exhaustivamente el uso de VPP con licencias administradas, lo que permite utilizar XenMobile para distribuir aplicaciones. Si ahora utiliza códigos de canje y quiere cambiar a una distribución administrada, consulte este documento de asistencia de Apple Pasar de códigos de canje a la distribución gestionada con el Programa de Compras por Volumen.

Para obtener información acerca del Programa de Compras por Volumen de iOS, consulte http://www.apple.com/business/vpp/. Para inscribirse en VPP, vaya a https://deploy.apple.com/qforms/open/register/index/avs. Para acceder a su tienda VPP en iTunes, vaya a https://vpp.itunes.apple.com/?l=en.

Después de guardar la configuración del programa VPP de iOS en XenMobile, las aplicaciones adquiridas aparecen en la página **Configure > Apps** de la consola de XenMobile.

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

2. En **Platform**, haga clic en **iOS Settings**. Aparecerá la página de configuración **iOS Settings**.



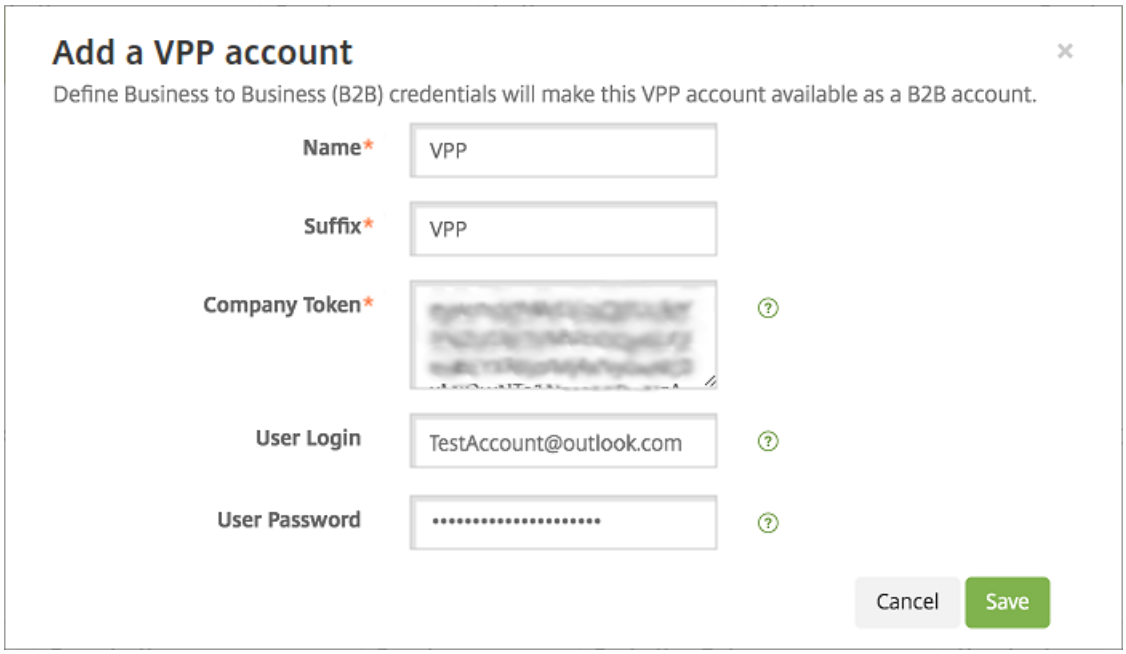
3. Configure estos parámetros:

- **Store user password in Secure Hub**. Seleccione si quiere almacenar de forma segura un nombre de usuario y la contraseña correspondiente en Secure Hub para la autenticación en XenMobile. El valor predeterminado es almacenar los datos con este método seguro.
- **User property for VPP country mapping**. Escriba un código para que los usuarios puedan descargar aplicaciones desde las tiendas de aplicaciones específicas de cada país.

  XenMobile utiliza esta asignación para elegir la agrupación de propiedades del programa VPP. Por ejemplo, si la propiedad del usuario es Estados Unidos, dicho usuario no puede descargarse aplicaciones si el código del programa VPP de estas es para el Reino Unido. Póngase en contacto con el administrador de planes del programa VPP para obtener más información acerca del código de asignación de país.

Cuentas VPP

- Para cada cuenta VPP que quiera agregar, haga clic en **Add**. Aparecerá el cuadro de diálogo **Add VPP account**.



Configure estos valores para cada cuenta que quiera agregar:

Nota: Si utiliza Apple Configurator 1, cargue un archivo de licencias de este modo: vaya a **Configure > Apps**, vaya a una página de plataforma y expanda **Volume Purchase Program**.

- **Name**. Escriba el nombre de la cuenta del programa VPP.
- **Suffix**. Escriba el sufijo que aparecerá en los nombres de las aplicaciones que se obtengan mediante la cuenta del programa VPP. Por ejemplo, si introduce **VPP**, la aplicación Secure Mail aparecerá en la lista de aplicaciones como **Secure Mail - VPP**.
- **Company Token**. Copie y pegue el token de servicio del programa VPP obtenido de Apple. Para obtener el token, en la página **Account Summary** del portal del programa VPP de Apple, haga clic en el botón **Download** para generar y descargar el archivo del programa VPP. Ese archivo contiene el token de servicio, además de otra información (como la caducidad y el código de país). Guarde el archivo en una ubicación segura.
- **User Login**. Introduzca un nombre de administrador optativo para la cuenta VPP autorizada a importar aplicaciones B2B personalizadas.
- **User Password**. Introduzca la contraseña del administrador de la cuenta VPP.

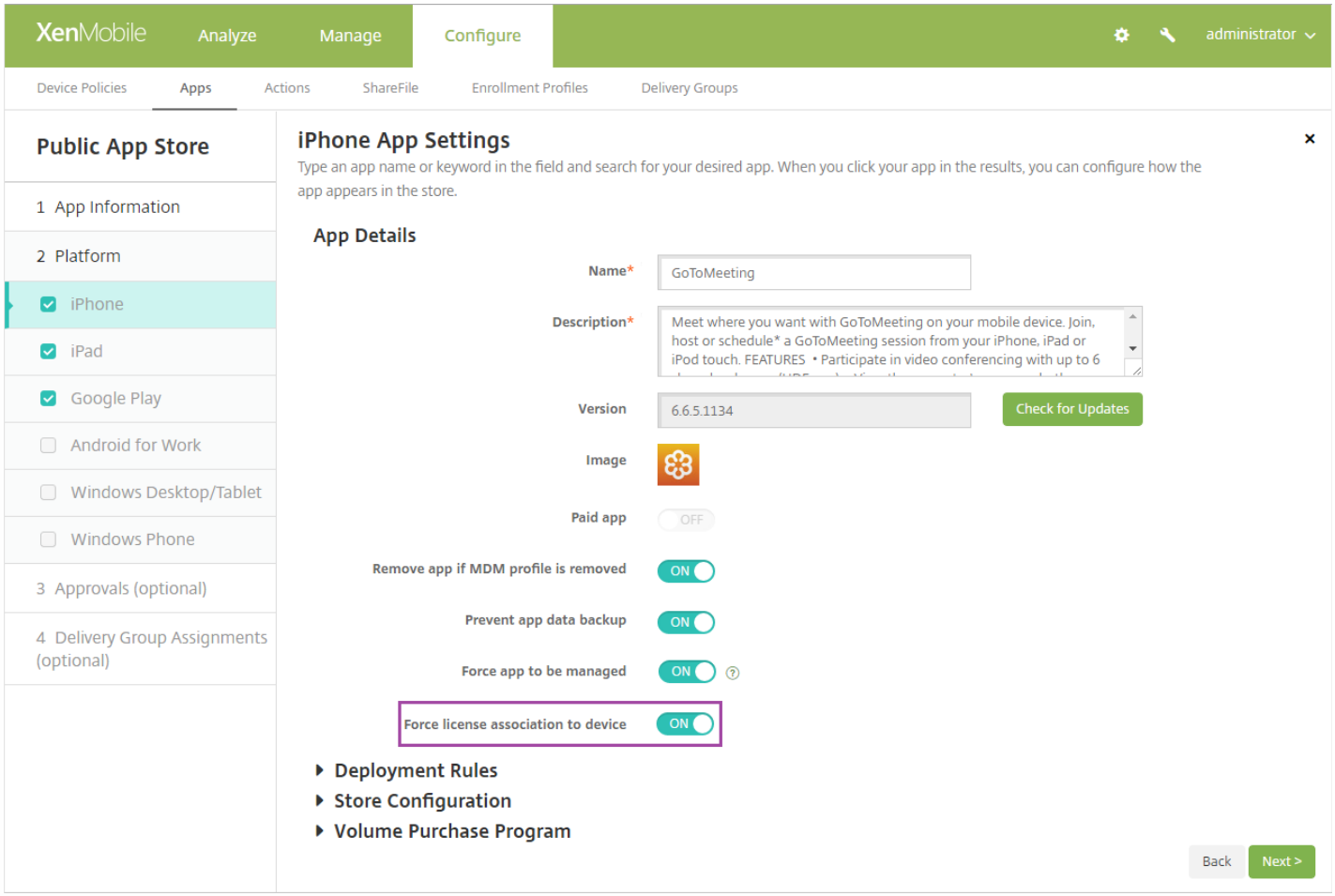
5. Haga clic en **Save** para cerrar el cuadro de diálogo.

6. Haga clic en **Save** para guardar la configuración de iOS.

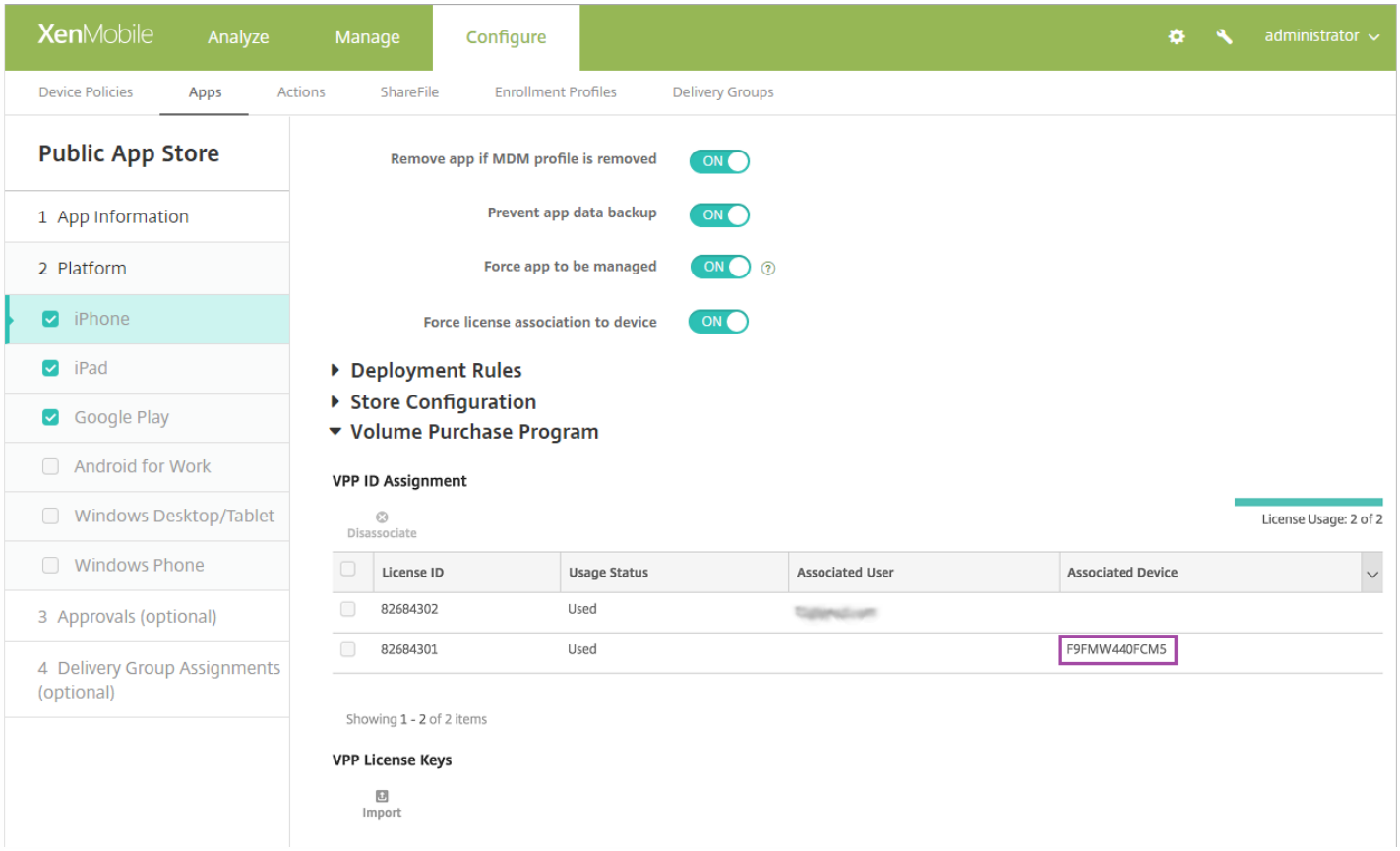
Aparecerá un mensaje para informarle de que XenMobile agregará las aplicaciones a la lista de la página **Configure > Apps**. En la página Configure > Apps, tenga en cuenta que los nombres de las aplicaciones extraídas de su cuenta de VPP contienen el sufijo que proporcionó en la configuración anterior.

Ya puede configurar los parámetros de aplicación del programa VPP y ajustar los parámetros del grupo de entrega y de la directiva de dispositivo a las aplicaciones del programa VPP. Después de completar esas configuraciones, los usuarios podrán inscribir sus dispositivos. Las siguientes notas contienen aspectos a tener en cuenta en dichos procesos.

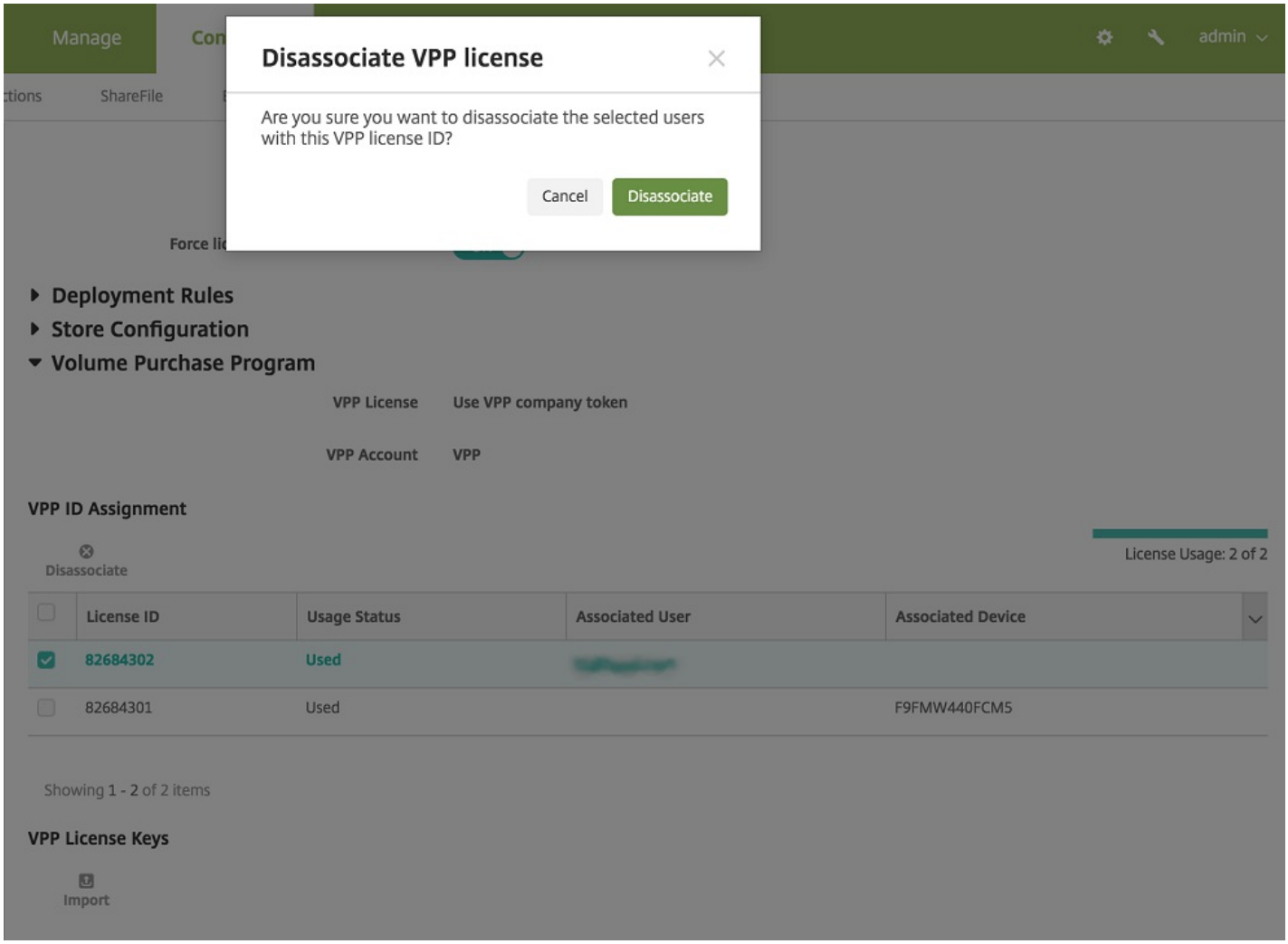
- Al configurar los parámetros de aplicación del programa VPP (**Configure > Apps**), habilite **Force license association to device** (Forzar asociación de licencia con el dispositivo). Una de las ventajas de usar el programa VPP de Apple y DEP con dispositivos supervisados es la capacidad de utilizar XenMobile para asignar la aplicación a nivel de dispositivo (en lugar de usuario). Por eso, no es necesario usar un ID de dispositivo Apple. Además, los usuarios no reciben invitación para participar en el programa VPP. Los usuarios también pueden descargar las aplicaciones sin iniciar sesión en sus cuentas de iTunes.



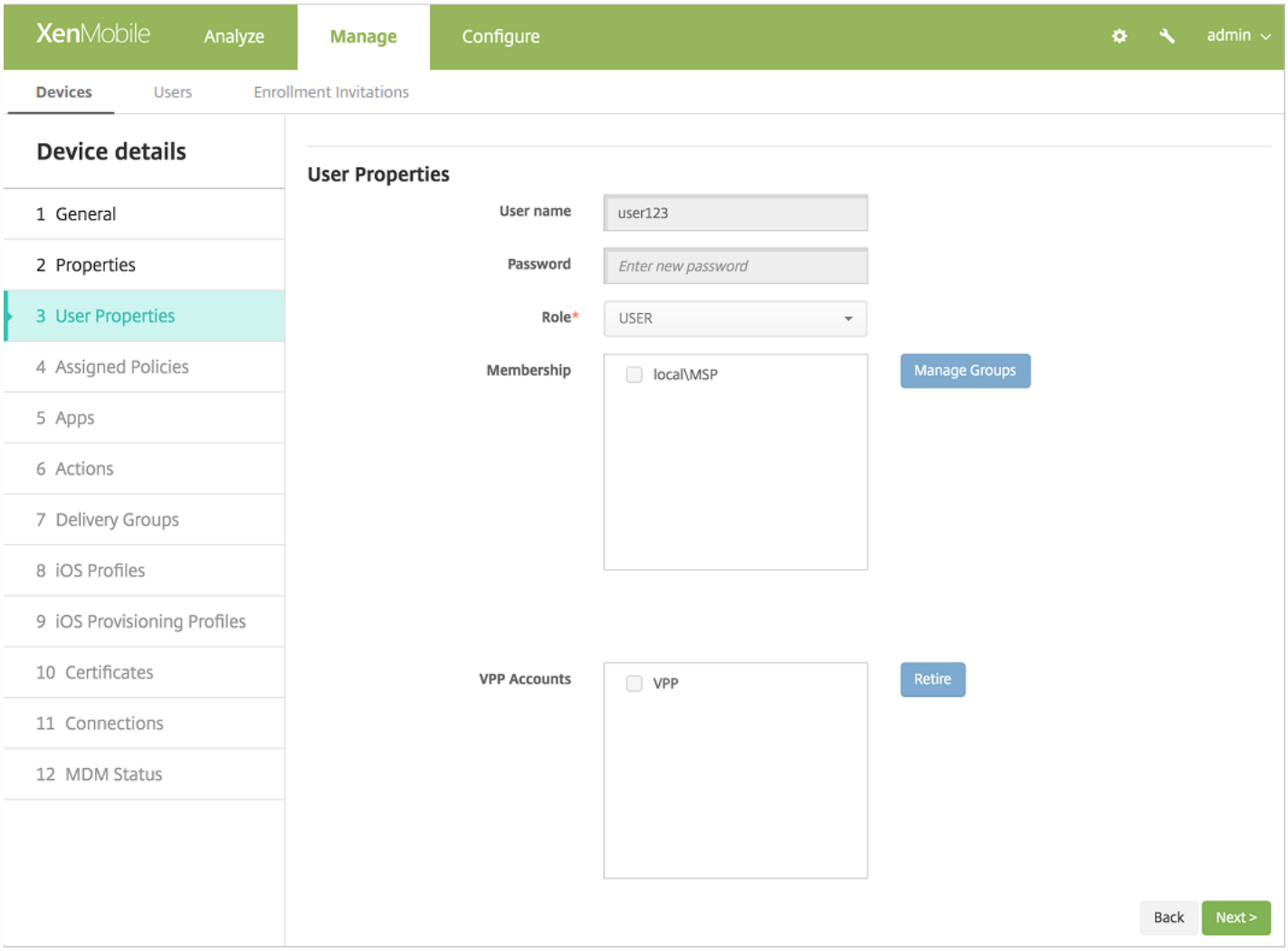
Para ver la información del programa VPP para esa aplicación, expanda **Volume Purchase Program**. Tenga en cuenta que, en la tabla **VPP ID Assignment**, la licencia está asociada con un dispositivo. El número de serie del dispositivo aparece en la columna **Associated Device**. Si el usuario quita el token y lo importa de nuevo, aparecerá la palabra **Hidden** en lugar del número de serie, debido a las restricciones de privacidad de Apple.



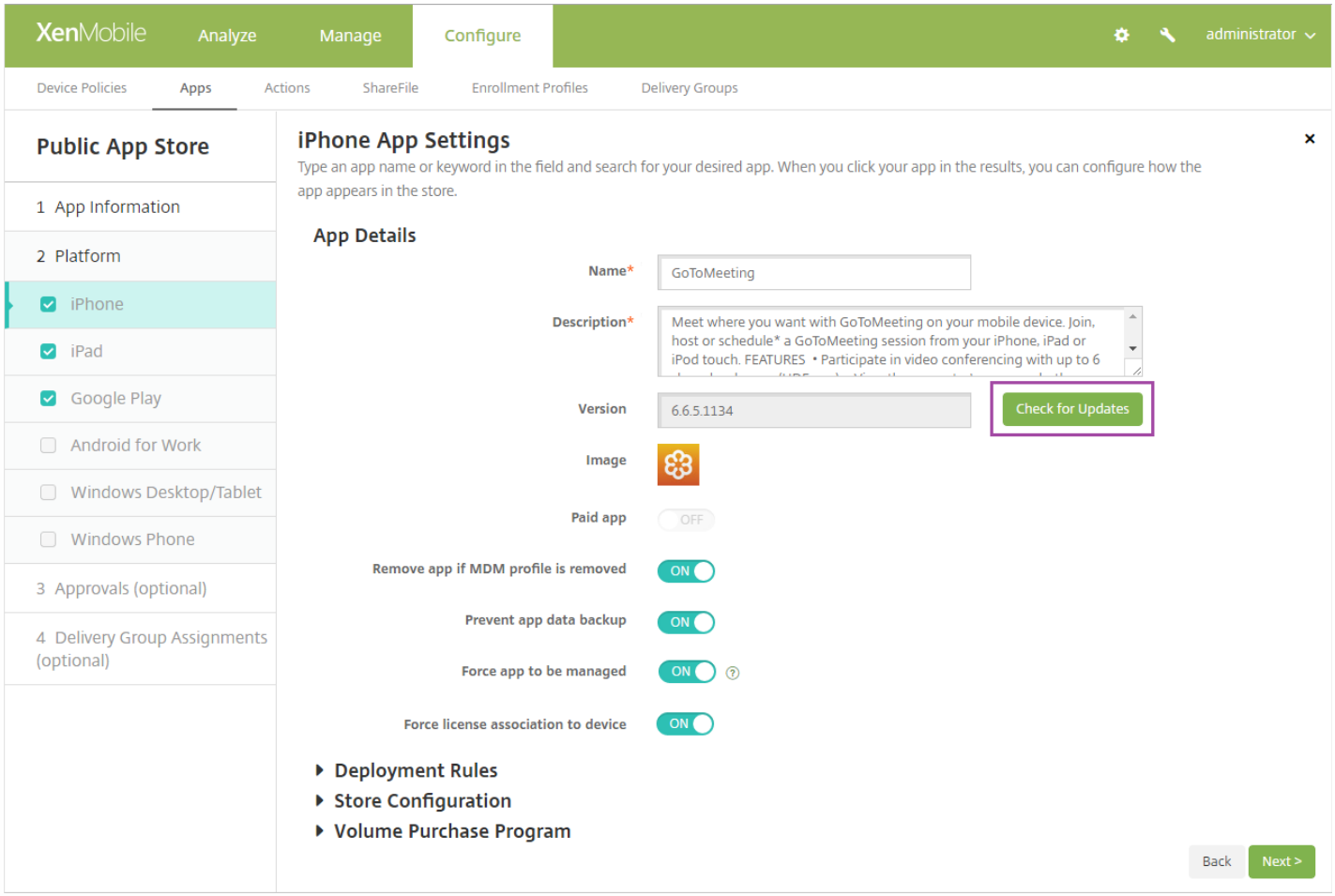
Para desvincular una licencia, haga clic en la fila de la licencia y en **Disassociate**.



Si asocia licencias del programa VPP con los usuarios, XenMobile integra a los usuarios en la cuenta del programa VPP y asocia sus ID de iTunes con la cuenta del programa VPP. Los ID de iTunes de los usuarios nunca son visibles para la empresa ni para el servidor XenMobile. Apple crea de forma transparente la asociación para mantener la privacidad de los usuarios. Puede retirar a un usuario del programa VPP, para desasociar todas las licencias de la cuenta del usuario. Para retirar a un usuario, vaya a **Manage > Devices**.



- Cuando asigna una aplicación a un grupo de entrega, XenMobile la identifica de forma predeterminada como una aplicación opcional. Para que XenMobile la implemente en los dispositivos, vaya a **Configure > Delivery Groups.** En la página **Apps**, mueva la aplicación a la lista **Required Apps**.
- Cuando está disponible una actualización para una aplicación de tienda pública y esa aplicación se ha enviado por medio del programa VPP, la aplicación no se actualiza automáticamente en los dispositivos hasta que usted busque las actualizaciones y las aplique. Para enviar una actualización de Secure Hub, si se ha asignado al dispositivo y no al usuario, haga lo siguiente. En **Configure > Apps**, en una página de plataforma, haga clic en **Check for Updates** e instale la actualización.



XenApp y XenDesktop desde Citrix Secure Hub

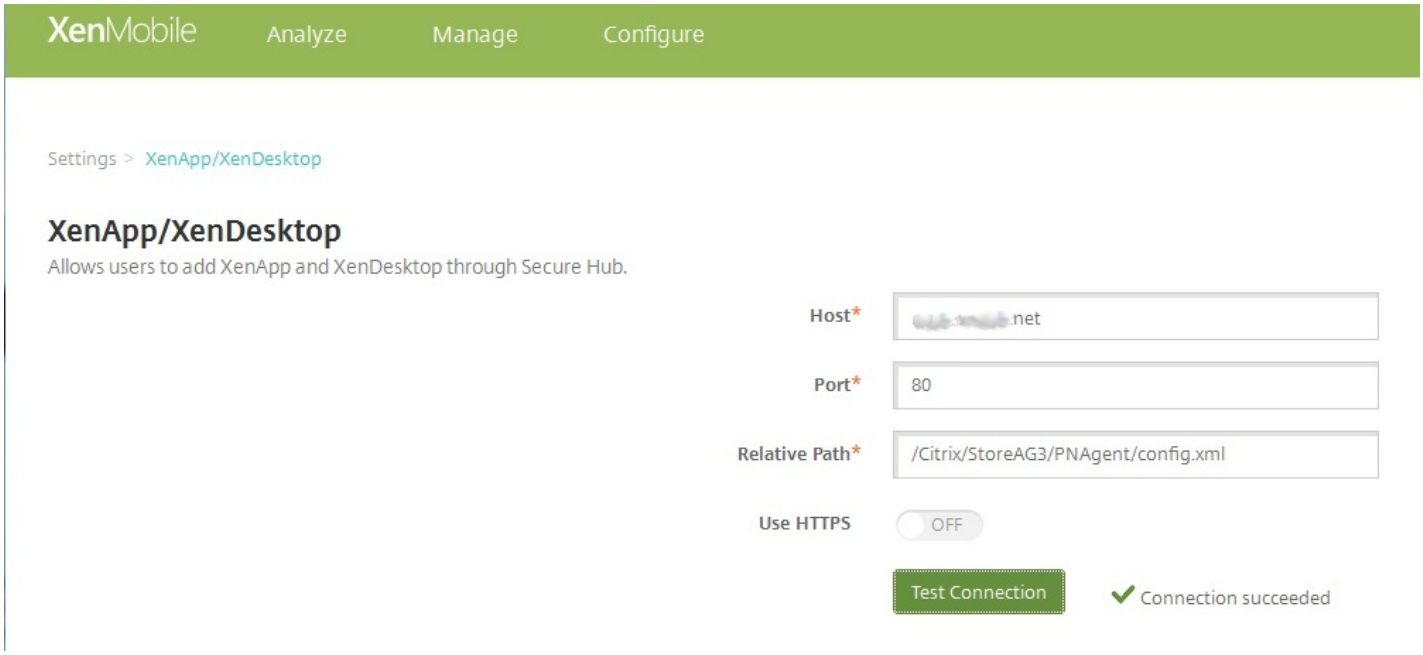
Feb 27, 2017

XenMobile puede recopilar aplicaciones desde XenApp y XenDesktop y ponerlas a disposición de los usuarios de dispositivos móviles desde XenMobile Store. Los usuarios se suscriben a las aplicaciones directamente desde XenMobile Store y las inician desde Secure Hub. Citrix 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 estos 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 **Test Connection** para verificar que XenMobile puede conectarse al servidor XenApp y XenDesktop especificado.

5. Haga clic en **Save**.

Uso de ShareFile con XenMobile

Apr 24, 2017

XenMobile dispone de dos opciones para integrarse con ShareFile: ShareFile Enterprise y conectores StorageZone. La integración con ShareFile Enterprise o conectores StorageZone requiere XenMobile Enterprise Edition.

ShareFile Enterprise

Si dispone de XenMobile Enterprise Edition, puede configurar XenMobile para proporcionar acceso a su cuenta de ShareFile Enterprise. Esa configuración:

- Permite a los usuarios móviles acceder al conjunto de las funcionalidades de ShareFile (como compartir archivos, sincronizarlos y StorageZone Connector).
- Puede ofrecer a ShareFile el aprovisionamiento de cuentas de usuario basado en AD, la autenticación Single Sign-On para usuarios de aplicaciones XenMobile y unas directivas completas de control de acceso.
- Ofrece la configuración, la supervisión del nivel de servicio y la supervisión del uso de licencias de ShareFile desde la consola de XenMobile.

Para obtener más información sobre cómo configurar XenMobile para ShareFile Enterprise, consulte SAML para Single Sign-On con ShareFile.

Conectores StorageZone

Puede configurar XenMobile para que solo ofrezca acceso a los conectores StorageZone que haya creado desde la consola de XenMobile. Esa configuración:

- Ofrece un acceso móvil seguro a los repositorios del almacenamiento local existente, como sitios de SharePoint y archivos compartidos de red.
- No se requiere que configure un subdominio de ShareFile ni aprovisione usuarios a ShareFile ni aloje datos de ShareFile.
- Proporciona a los usuarios acceso móvil a los datos a través de las aplicaciones XenMobile de ShareFile para iOS y Android. Los usuarios pueden modificar documentos de Microsoft Office. Los usuarios también pueden obtener vistas previas y escribir notas en archivos PDF de Adobe desde dispositivos móviles.
- Cumple las restricciones de seguridad contra la filtración de la información de usuarios fuera de la red corporativa.
- Proporciona una configuración simple de conectores StorageZone Connector a través de la consola de XenMobile. Si posteriormente decide usar la funcionalidad completa de ShareFile con XenMobile, puede cambiar la configuración en la consola de XenMobile.
- Requiere la edición XenMobile Enterprise.

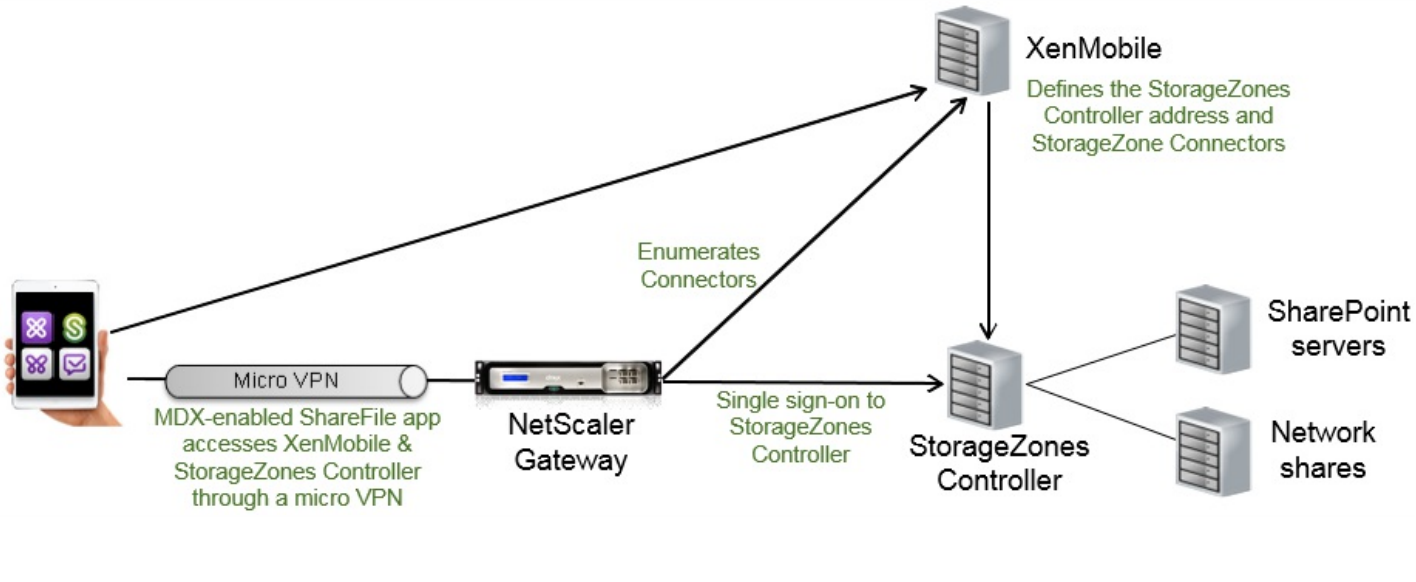
Para integrar XenMobile solo con conectores StorageZone:

- ShareFile utiliza su configuración de inicio de sesión único SSO en NetScaler Gateway para autenticarse en

StorageZones Controller.

- XenMobile no se autentica a través de SAML porque no se utiliza el plano de control de ShareFile.

En el siguiente diagrama, se muestra la arquitectura de alto nivel para usar XenMobile con conectores StorageZone.



Requisitos

- Versiones mínimas de los componentes:
  - XenMobile Server 10.5 (local)
  - ShareFile para iOS (MDX) 5.3
  - ShareFile para Android (MDX) 5.3
  - ShareFile StorageZones Controller 5.0
    Este artículo contiene instrucciones para configurar ShareFile StorageZones Controller 5.0
- Compruebe que el servidor que ejecutará StorageZones Controller cumple los requisitos del sistema. Para conocer los requisitos, consulte las siguientes secciones en "Requisitos del sistema" de la documentación de StorageZones Controller para ShareFile:
  - StorageZones Controller
  - StorageZone Connector para SharePoint
  - StorageZone Connector para recursos compartidos de red

    Los requisitos de StorageZones para datos de ShareFile y para StorageZones restringidas no se aplican a la integración de XenMobile con solo conectores de StorageZone.

    XenMobile no respalda conectores Documentum.

- Para ejecutar scripts de PowerShell:
  - Ejecute los scripts en la versión de 32 bits (x86) de PowerShell.

Tareas de instalación

Complete las siguientes tareas en el orden indicado para instalar y configurar StorageZones Controller. Los pasos siguientes son para integrar XenMobile solo con conectores StorageZone. Algunos de estos artículos se encuentran en la documentación de StorageZones Controller.

1. Configuración de NetScaler para StorageZones Controller

Puede utilizar NetScaler como un proxy DMZ para StorageZones Controller.

2. Instalación de un certificado SSL

   Un StorageZones Controller que aloja zonas estándar requiere un certificado SSL. Un StorageZones Controller que aloja zonas restringidas y usa una dirección interna no requiere ningún certificado SSL.

3. Preparación del servidor

   Se requiere la configuración de IIS y ASP.NET para conectores StorageZone.

4. Instalación de StorageZones Controller

5. Preparación de StorageZones Controller para que solo se pueda usar con conectores StorageZone

6. Indicación de un servidor proxy para StorageZones

   La consola de StorageZones Controllers permite especificar un servidor proxy para los StorageZones Controllers. También puede especificar un servidor proxy utilizando otros métodos.

7. Configuración del controlador de dominio para que confíe en el StorageZones Controller para la delegación

   Configure el controlador de dominio para que admita la autenticación NTLM o Kerberos en recursos compartidos de red o sitios de SharePoint.

8. Unión de un StorageZones Controller secundario a una StorageZone

   Para configurar una StorageZone de alta disponibilidad, debe conectar al menos dos StorageZones Controllers a ella.

Instalación de StorageZones Controller

1. Descargue e instale el software de StorageZones Controller:

   a. Desde la página de descargas de ShareFile en http://www.citrix.com/downloads/sharefile.html, inicie sesión y descargue el programa de instalación más reciente de StorageZones Controller.

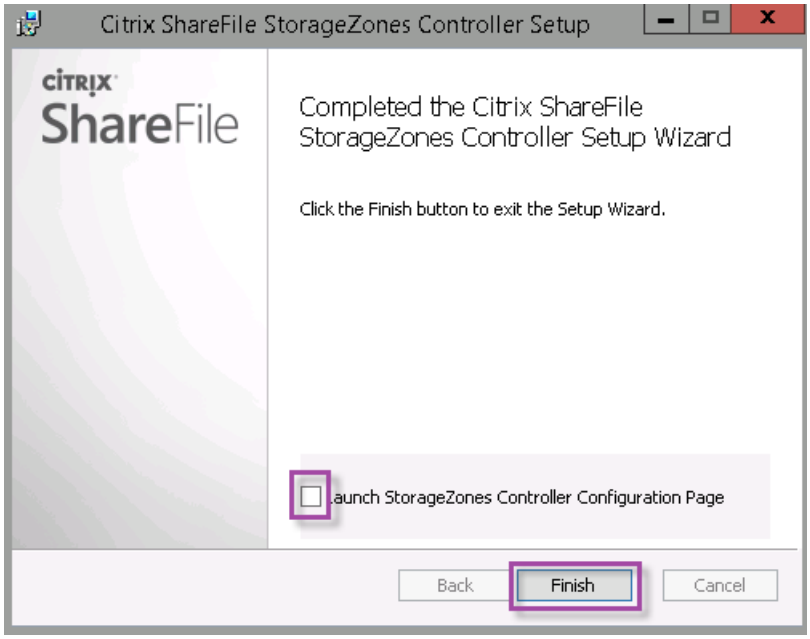
   b. Instalar StorageZones Controller cambia el sitio Web predeterminado en el servidor a la ruta de instalación del Controller. Habilite **Anonymous Authentication** en el sitio Web predeterminado.

2. En el servidor donde quiere instalar StorageZones Controller, ejecute StorageCenter.msi.

   Se iniciará el Asistente para la instalación de StorageZones Controller para ShareFile.

3. Responda a las solicitudes del sistema:

- En la página **Destination Folder**, si Internet Information Services (IIS) está instalado en la ubicación predeterminada, deje los valores predeterminados. Si no es así, vaya a la ubicación de instalación de IIS.
- Cuando finalice la instalación, desmarque la casilla **Launch StorageZones Controller Configuration Page** y, a continuación, haga clic en **Finish**.



4. Cuando se le pida, reinicie el StorageZones Controller.

5. Para comprobar si la instalación es correcta, vaya a http://localhost/. Si la instalación ha sido correcta, aparecerá el logotipo de ShareFile.

Si no aparece el logotipo de ShareFile, borre la caché del explorador y vuelva a intentarlo.

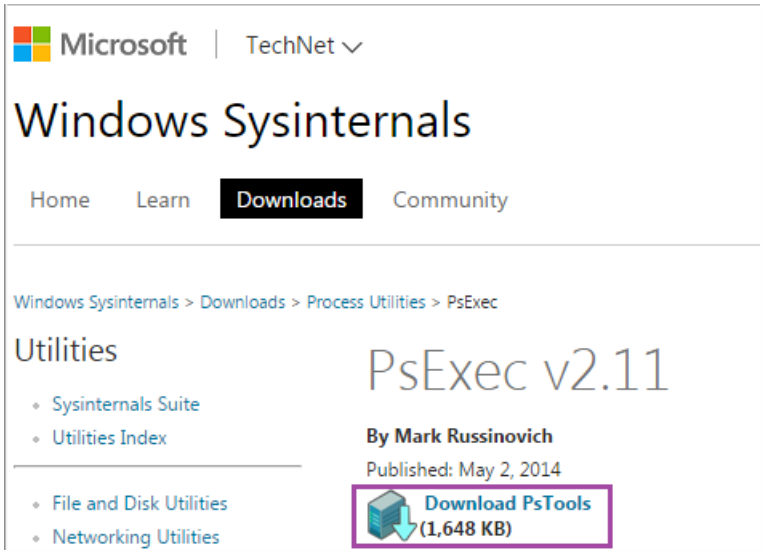
> ## Important
>
> Si va a clonar el StorageZones Controller, capture la imagen de disco antes de continuar con la configuración del StorageZones Controller.

Preparación de StorageZones Controller para que solo se pueda usar con conectores StorageZone

Para una integración solo con conectores StorageZone, no use la consola administrativa de StorageZones Controller. Esa interfaz requiere una cuenta de administrador de ShareFile, que no es necesaria para esta solución. Por eso, ejecute un script de PowerShell para preparar StorageZones Controller para usarlo sin el plano de control de ShareFile. El script hace lo siguiente:

- Registra el StorageZones Controller actual como el Controller principal de StorageZones. Más adelante, puede unir Controllers secundarios de StorageZones al Controller principal.
- Crea una zona y establece la frase secreta para ella.

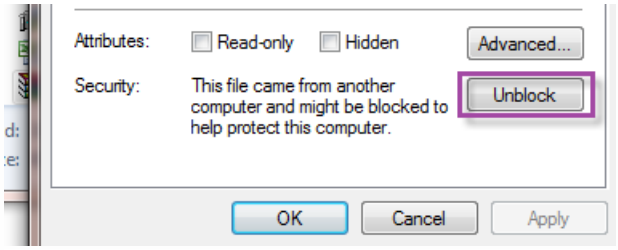
1. Desde el servidor de StorageZone Controller, descargue la herramienta PsExec: vaya a Microsoft Windows Sysinternals y, a continuación, haga clic en **Download PsTools**. Extraiga la herramienta en la raíz de la unidad C.



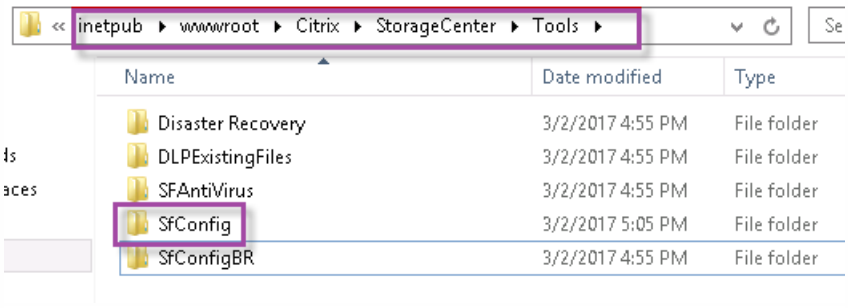
2. Descargue SfConfig.zip: Vaya a https://labs.sharefile.com/d-sf083d50048a4e408 en el sitio de ShareFile Labs y haga clic en **Download**.

3. Guarde SfConfig.zip en C:\inetpub\wwwroot\Citrix\StorageCenter\Tools.

4. Haga clic con el botón secundario en SfConfig.zip. Elija **Properties** y haga clic en **Unlock** para quitar el bloqueo de seguridad.



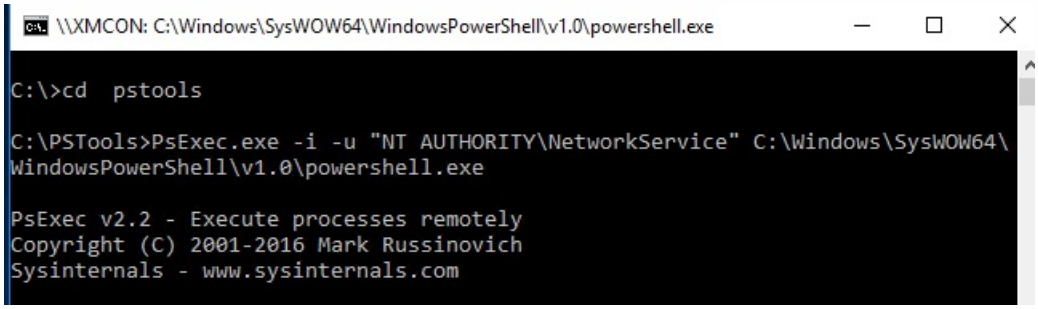
5. Extraiga el archivo ZIP en C:\inetpub\wwwroot\Citrix\StorageCenter\Tools.



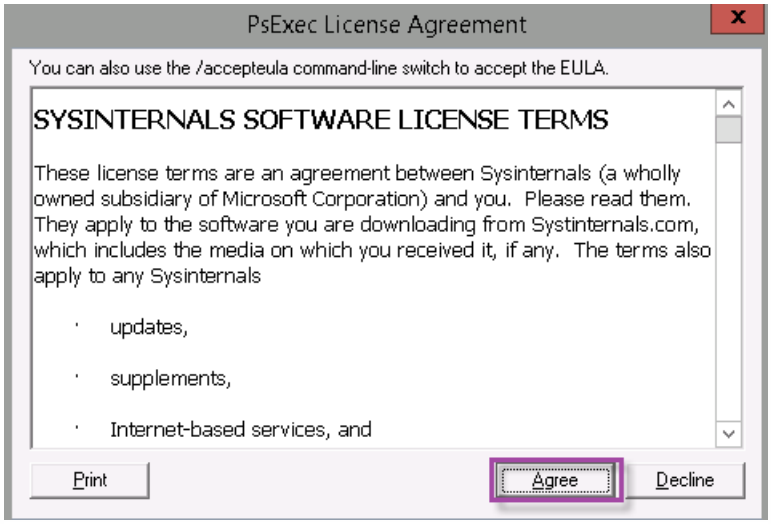
6. Ejecute la herramienta PsExec: Abra el símbolo del sistema como el usuario administrador y escriba lo siguiente:

comando COPIAR

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



7. Cuando se le pida, haga clic en **Agree** para ejecutar la herramienta Sysinternals.



Se abrirá una ventana de PowerShell.

8. En la ventana de PowerShell, escriba lo siguiente:

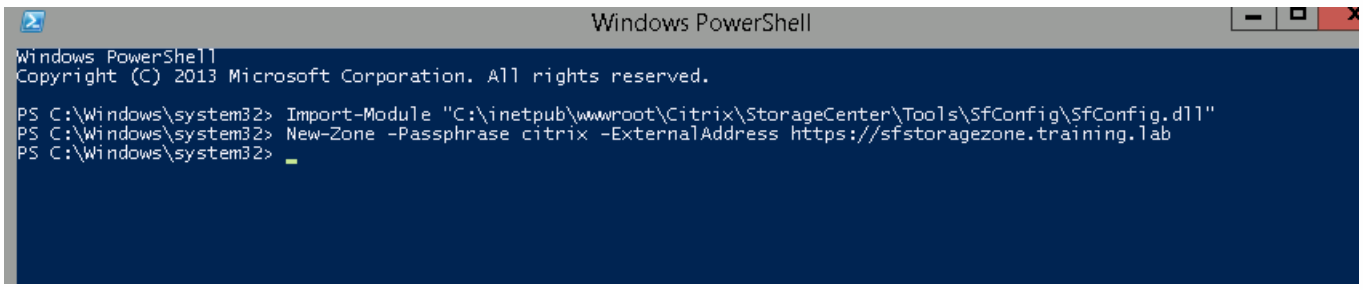
comando COPIAR

```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone  -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

Donde:

Passphrase. Es la frase secreta que quiere asignar al sitio. Apúntela. No podrá recuperar esta frase secreta desde el Controller. Si pierde la frase secreta, no podrá volver a instalar StorageZones ni unir más StorageZones Controllers a la StorageZone ni recuperar la StorageZone si se produce un error en el servidor.

ExternalAddress. Es el nombre de dominio completo externo del servidor StorageZones Controller.



Ya está listo el StorageZones Controller principal.

Antes de iniciar sesión en XenMobile para crear conectores de StorageZone, debe completar la configuración siguiente, si

procede:

Indicación de un servidor proxy para StorageZones

Configuración del controlador de dominio para que confíe en el StorageZones Controller para la delegación

Unión de un StorageZones Controller secundario a una StorageZone

Para crear conectores StorageZone, consulte Definición de conexiones de StorageZones Controller en XenMobile.

Unión de un StorageZones Controller secundario a una StorageZone

Para configurar una StorageZone de alta disponibilidad, debe conectar al menos dos StorageZones Controllers a ella. Para unir un StorageZones Controller secundario a una zona, instale StorageZones Controller en un segundo servidor. A continuación, una ese Controller a la zona del Controller principal.

1. Abra una ventana de PowerShell en el servidor de StorageZones Controller que quiere unir al servidor principal.

2. En la ventana de PowerShell, escriba lo siguiente:

Join-Zone -Passphrase -PrimaryController

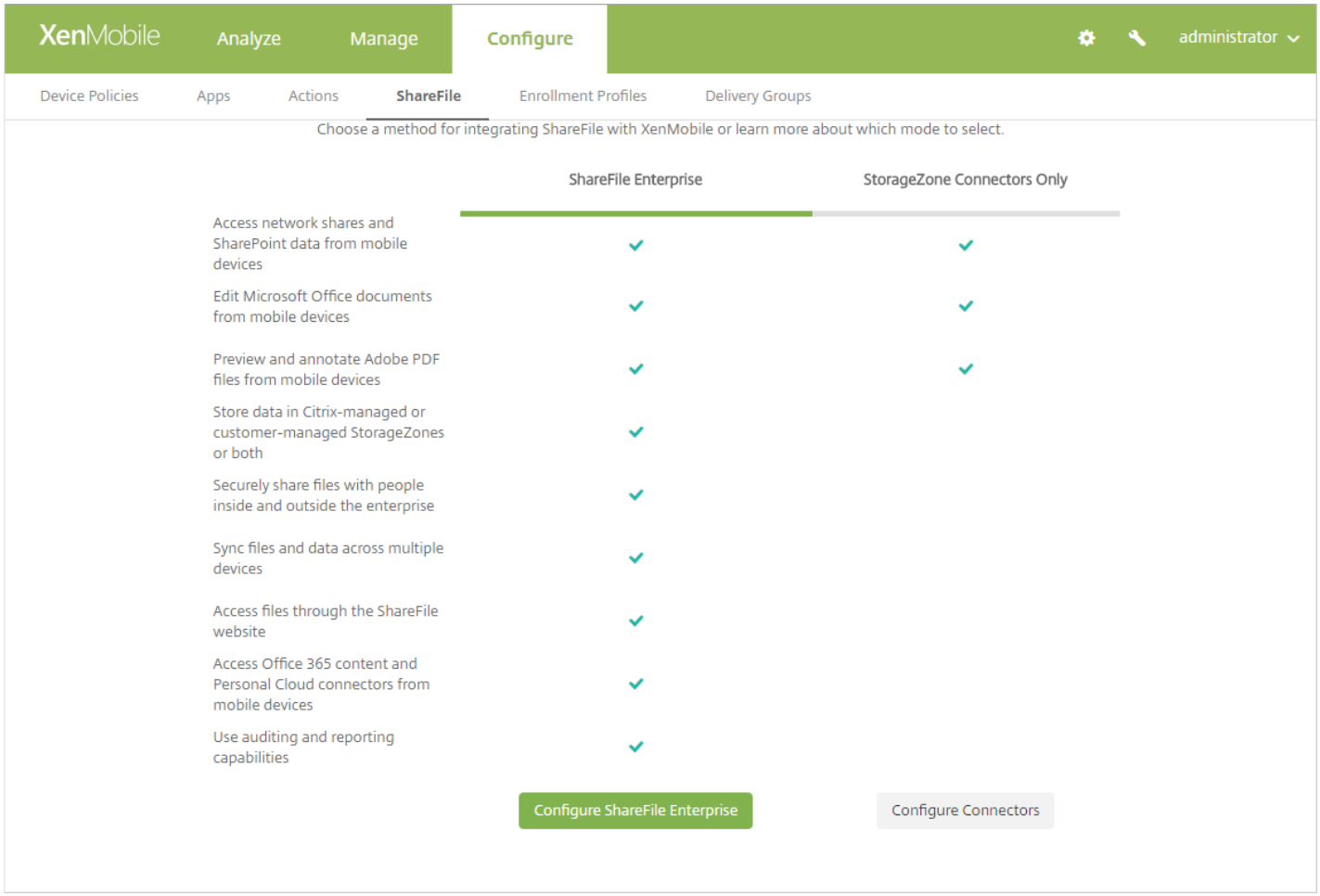
Por ejemplo:

Join-Zone -Passphrase secreto123 -PrimaryController 10.10.110.210

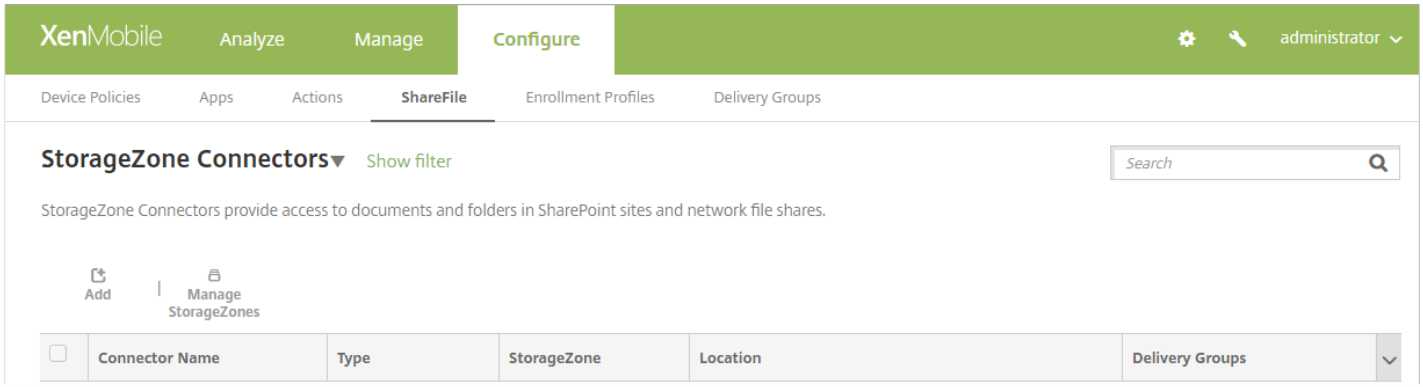
Definición de conexiones de StorageZones Controller en XenMobile

Antes de agregar conectores StorageZone Connector, debe definir la información de conexión para cada StorageZones Controller habilitado para StorageZone Connector. Los StorageZones Controllers se pueden definir como se describe en esta sección, o al agregar un conector.

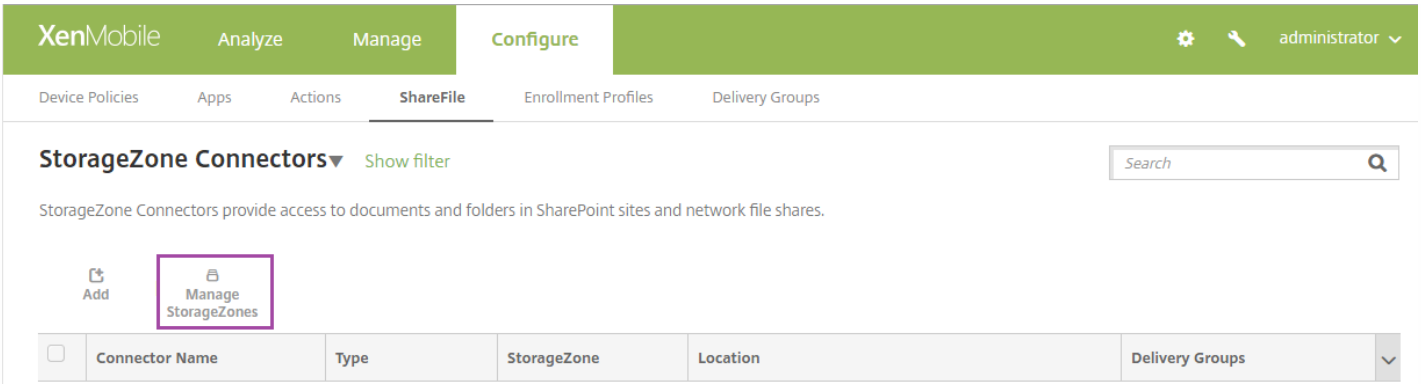
En su primera visita a la página **Configure > ShareFile**, se resumen en la página las diferencias entre usar XenMobile con ShareFile Enterprise y con conectores StorageZone.



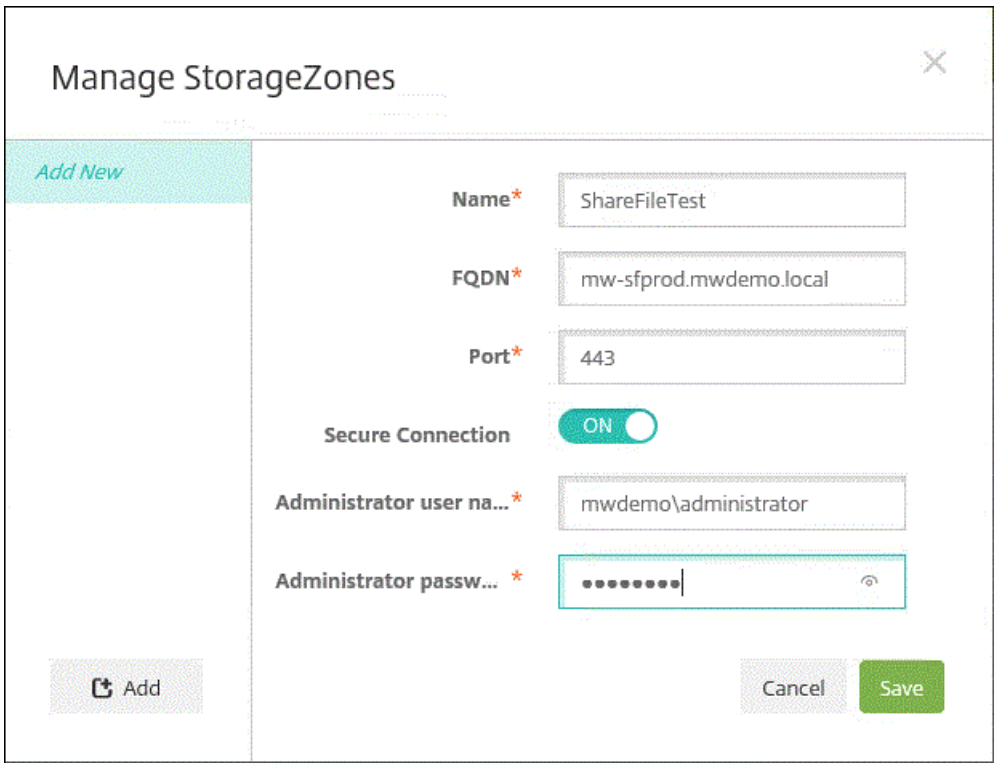
Haga clic en **Configure Connectors** para continuar con los pasos de configuración de este artículo.



1. En **Configure > ShareFile**, haga clic en **Manage StorageZones**.



2. En **Manage StorageZones**, agregue la información de conexión.



- **Name**. Un nombre descriptivo para la StorageZone, que sirva para identificarla en XenMobile. No incluya espacios ni caracteres especiales en el nombre.
- **FQDN and Port**. El nombre de dominio completo y el número de puerto del StorageZones Controller al que se puede acceder desde el servidor XenMobile.
- **Secure Connection**. Si usa SSL para las conexiones a StorageZones Controller, use el parámetro predeterminado, ON. Si no utiliza SSL para las conexiones, cambie este parámetro a OFF.
- **Administrator user name** y **Administrator password**. El nombre de usuario de la cuenta del administrador del servicio (en el formato dominio\admin) y la contraseña. Como alternativa, una cuenta de usuario con permisos de lectura y escritura en los StorageZones Controllers.

3. Haga clic en **Save**.

4. Para probar la conexión, compruebe que el servidor XenMobile puede establecer conexión con el nombre de dominio

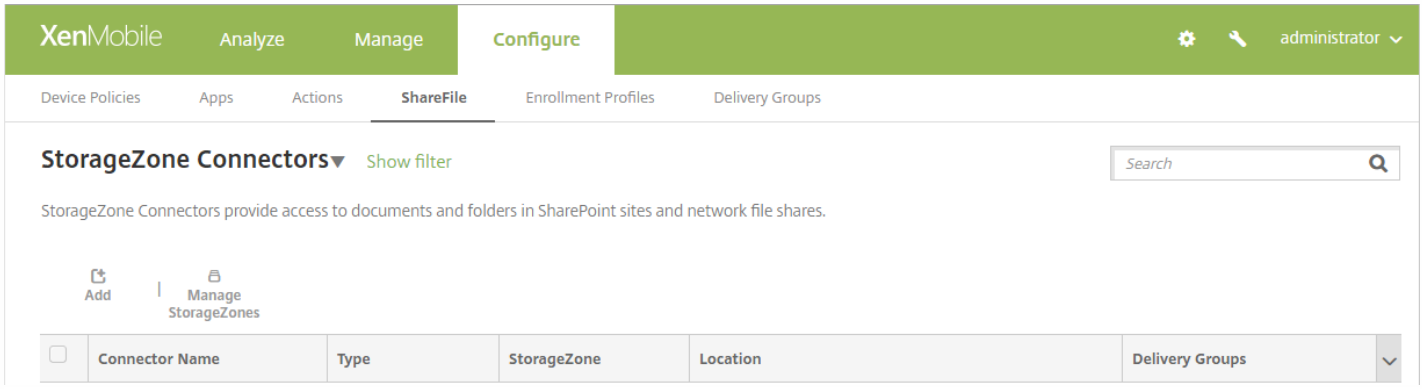
completo del StorageZones Controller en el puerto 443.

5. Para definir otra conexión de StorageZones Controller, haga clic en el botón **Add** en **Manage StorageZones**.

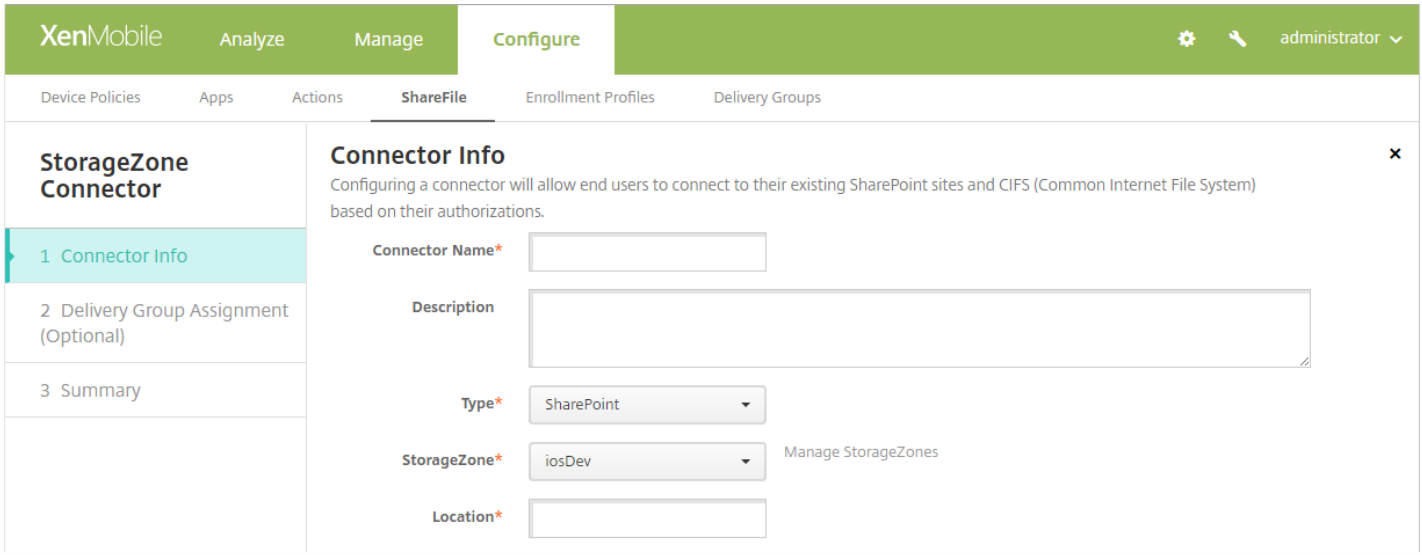
Para modificar o eliminar la información para una conexión de StorageZones Controller, seleccione el nombre de la conexión en **Manage StorageZones**. Haga clic en **Edit** o **Delete**.

Cómo agregar un StorageZone Connector en XenMobile

1. Vaya a **Configure > ShareFile** y, a continuación, haga clic en **Add**.

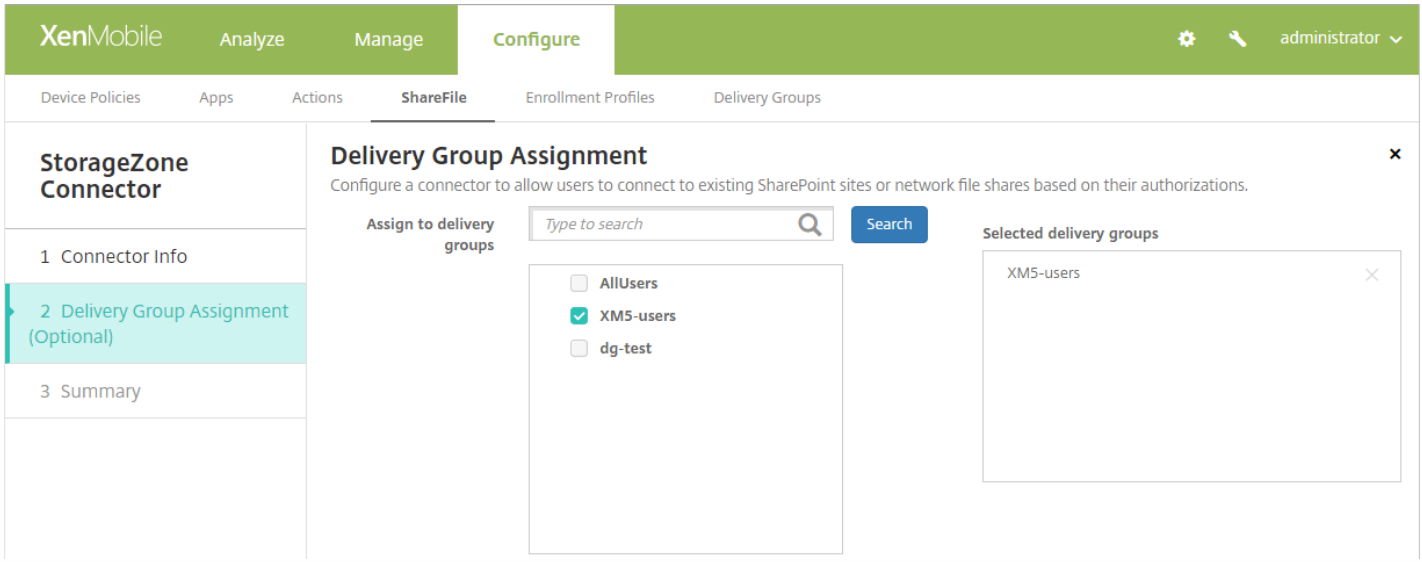


2. En la página **Connector Info**, configure los siguientes parámetros:



- **Connector Name**. Un nombre que identifica el StorageZone Connector en XenMobile.
- **Description**. Notas opcionales sobre este conector.
- **Type**. Elija **SharePoint** o **Network**.
- **StorageZone**. Seleccione la zona StorageZone asociada al conector. Si no aparece StorageZone, haga clic en **Manage StorageZones** para definir el StorageZones Controller.
- **Location**. Para SharePoint, especifique la URL del sitio en el nivel raíz de SharePoint, la colección del sitio, o la biblioteca de documentos (en el formato https://sharepoint.company.com). Para un recurso compartido de red, especifique el nombre de dominio completo de la ruta UNC (en el fomato \\servidor\recurso).

3. Si quiere, en la página **Delivery Group Assignment**, puede asignar el conector a grupos de entrega. De forma alternativa, puede asociar conectores a grupos de entrega desde **Configure > Delivery Groups**.



4. En la página **Summary**, puede revisar las opciones que ha configurado. Para ajustar la configuración, haga clic en **Back**.

5. Haga clic en **Save** para guardar el conector.

6. Pruebe el conector:

a. Al empaquetar clientes ShareFile, realice lo siguiente:

- Establezca la directiva Network access con el valor **Tunneled to the internal network**.

  En este modo de funcionamiento, el marco de trabajo de XenMobile MDX intercepta todo el tráfico de red desde el cliente ShareFile. Redirige el tráfico a través de NetScaler Gateway mediante una micro VPN específica de la aplicación.

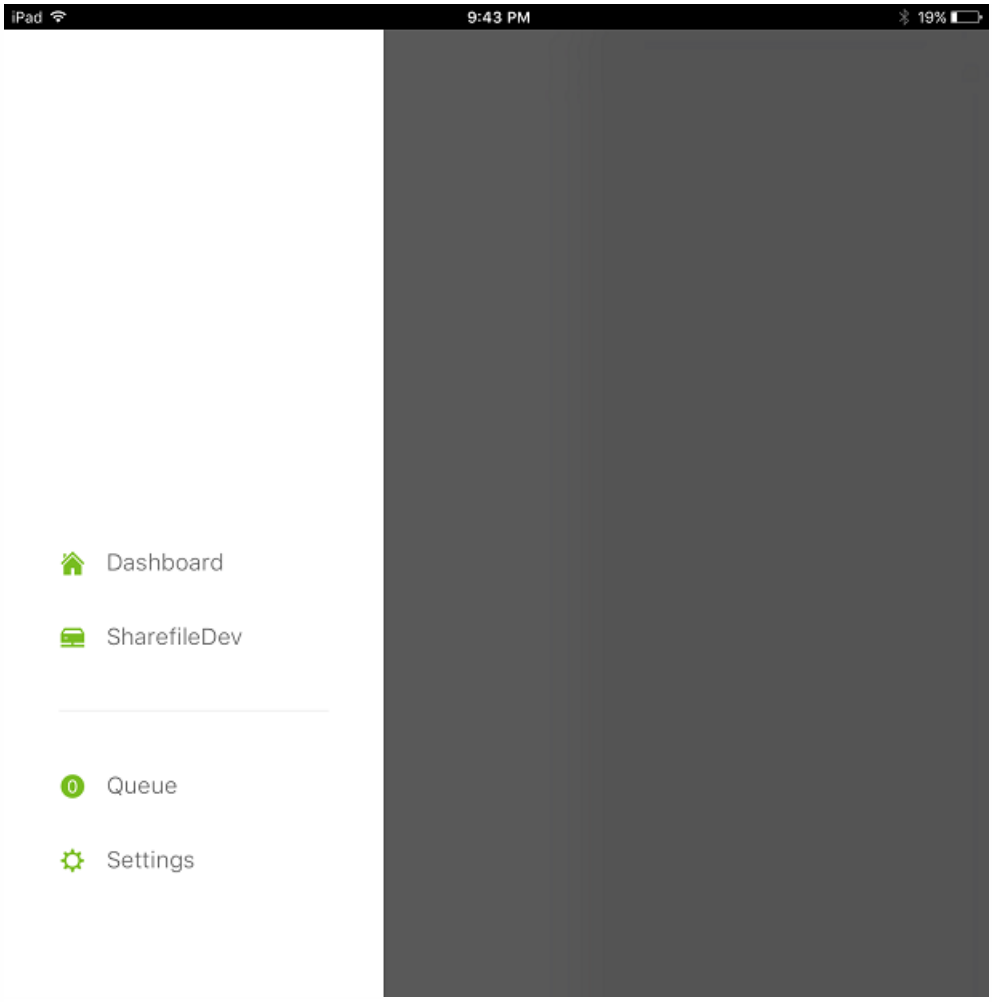
- Establezca la directiva Preferred VPN mode con el valor **Secure browse**.

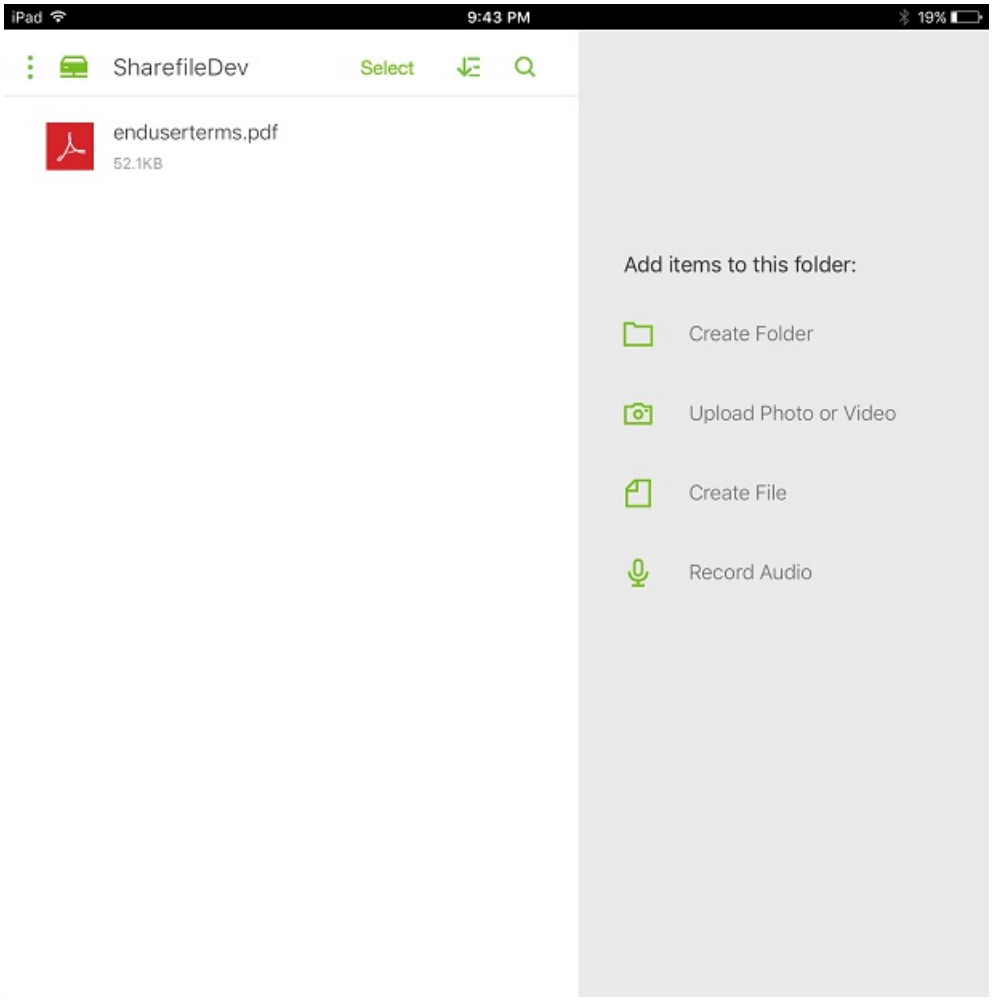
  En este modo de canalización por túnel, el marco MDX finaliza el tráfico SSL/HTTP desde una aplicación MDX. A continuación, MDX inicia conexiones nuevas con conexiones internas en nombre del usuario. Esta configuración de directiva permite que el marco de MDX detecte y responda a los desafíos de autenticación emitidos por servidores Web.

b. Agregue los clientes ShareFile a XenMobile. Para obtener más información, consulte Para agregar clientes ShareFile a XenMobile.

c. Desde un dispositivo compatible, compruebe el inicio de sesión único SSO para ShareFile y los conectores.

En los ejemplos siguientes, SharefileDev es el nombre de un conector.

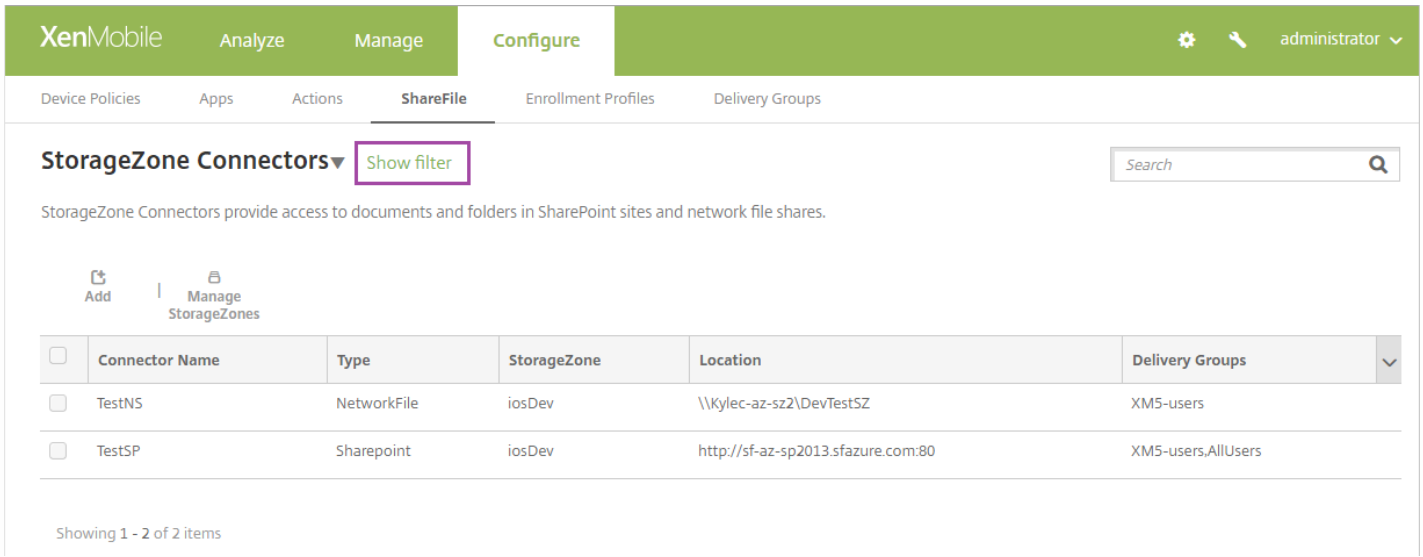




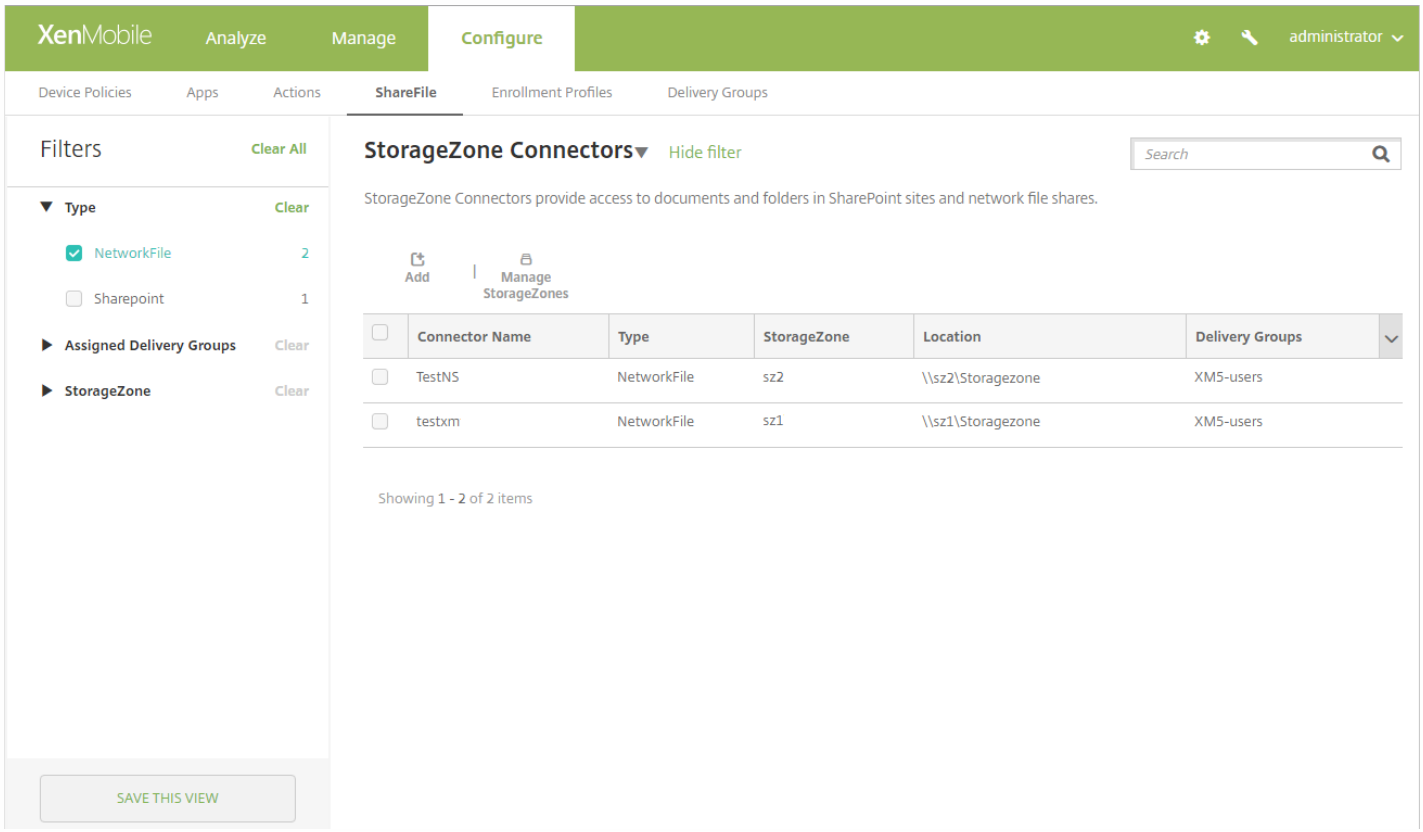
Cómo filtrar la lista de conectores StorageZone Connector

Puede filtrar la lista de conectores de StorageZone por tipo de conector, grupos de entrega asignados y zona StorageZone.

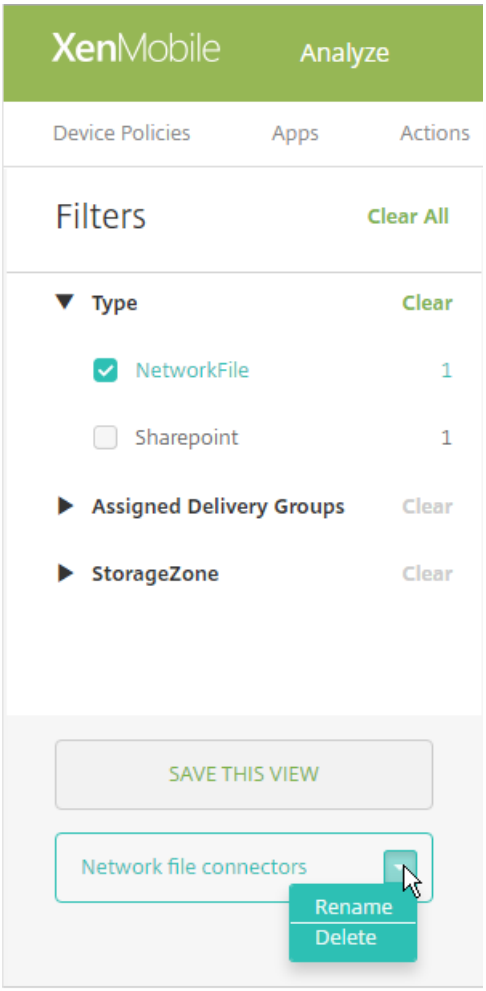
1. Vaya a **Configure > ShareFile** y, a continuación, haga clic en **Show filter**.



2. Expanda los encabezados de filtro para realizar selecciones. Para guardar un filtro, haga clic en **SAVE THIS VIEW**, escriba el nombre del filtro y haga clic en **Save**.



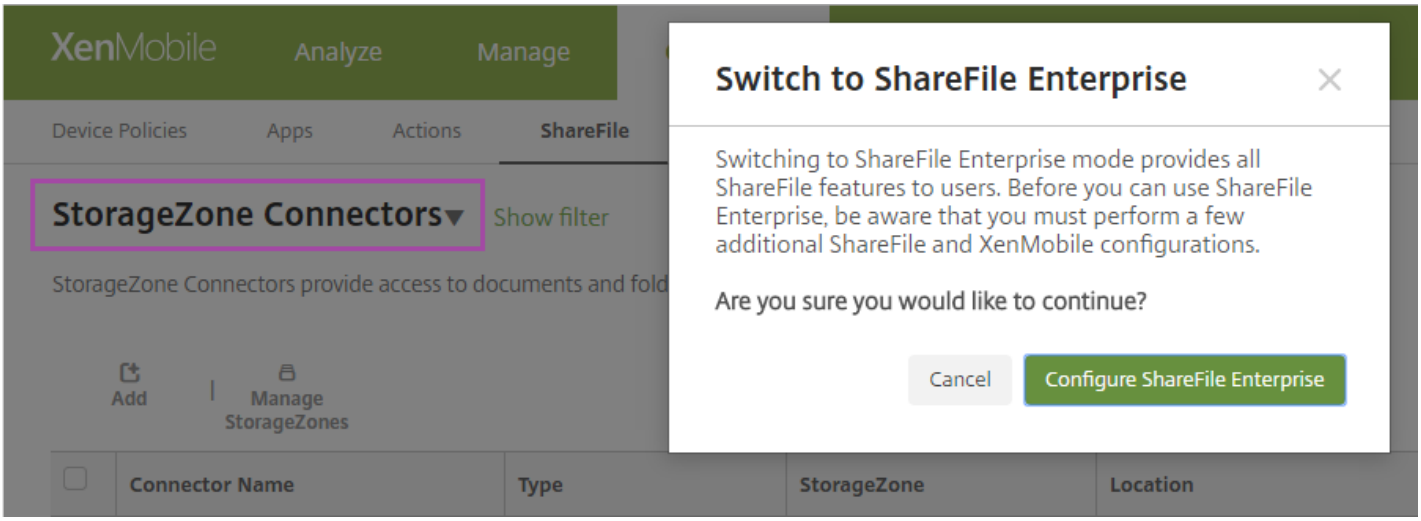
3. Para cambiar el nombre de un filtro o eliminarlo, haga clic en el icono de flecha situado junto al nombre del filtro.



Cambiar a ShareFile Enterprise

Después de integrar conectores StorageZone Connector con XenMobile, puede cambiar al conjunto de funcionalidades de ShareFile Enterprise. El conjunto de funcionalidades de ShareFile Enterprise requiere XenMobile Enterprise Edition. XenMobile conserva los parámetros existentes de integración de StorageZone Connector.

Vaya a **Configure > ShareFile**, haga clic en el menú desplegable **StorageZone Connectors** y, a continuación, haga clic en **Configure ShareFile Enterprise**.



Para obtener información sobre cómo configurar ShareFile Enterprise, consulte SAML para Single Sign-On con ShareFile.

SmartAccess para aplicaciones HDX

Feb 27, 2017

Esta funcionalidad permite controlar el acceso a las aplicaciones HDX en función de las propiedades del dispositivo, las propiedades del usuario de un dispositivo o las aplicaciones instaladas en un dispositivo. Para utilizar esta funcionalidad, se configuran acciones automatizadas que marcan el dispositivo como no conforme para denegarle el acceso. Las aplicaciones HDX utilizadas con esta funcionalidad se configuran en XenApp y XenDesktop a través de una directiva de SmartAccess que deniega el acceso a los dispositivos no conformes. XenMobile comunica el estado del dispositivo a StoreFront por medio de una etiqueta firmada y cifrada. StoreFront permite o deniega el acceso en función de la directiva de control del acceso de la aplicación.

Para usar esta función, se requiere una implementación de:

- XenApp y XenDesktop 7.6
- StoreFront 3.7 o 3.8
- XenMobile Server configurado con aplicaciones HDX agrupadas desde un servidor StoreFront
- XenMobile Server configurado con un certificado SAML que se utilizará para firmar y cifrar las etiquetas. El mismo certificado sin clave privada se carga en el servidor StoreFront.

Para empezar a usar esta funcionalidad:

- Configuración del certificado en el almacén de StoreFront
- Configure al menos un grupo de entrega de XenApp y XenDesktop con la directiva de SmartAccess requerida
- Establezca la acción automatizada en XenMobile

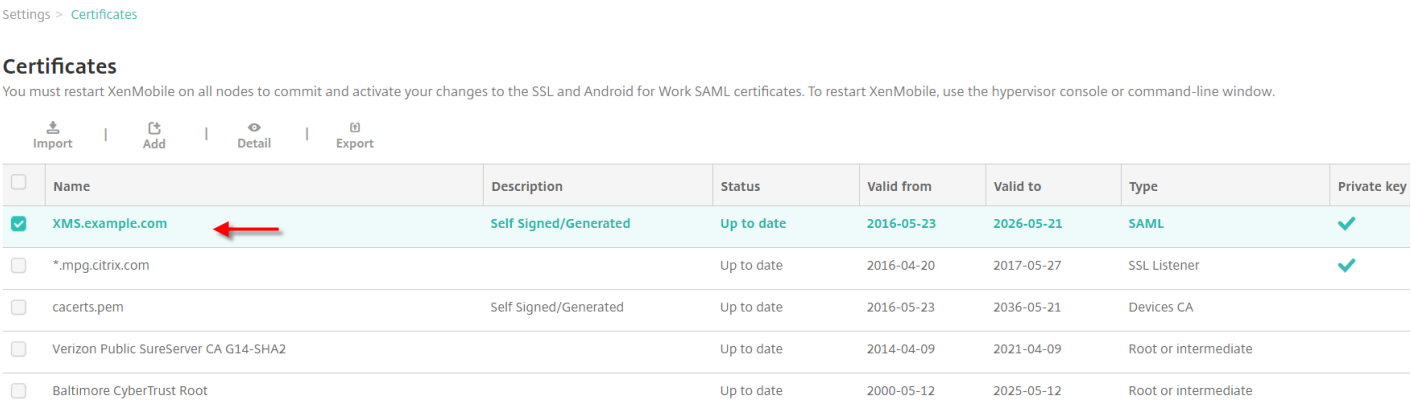
Exportación y configuración del certificado de XenMobile Server para cargarlo en el almacén de StoreFront

SmartAccess usa etiquetas cifradas y firmadas para la comunicación entre los servidores de XenMobile y StoreFront. Para habilitar esta comunicación, agregue el certificado del servidor XenMobile al almacén de StoreFront.

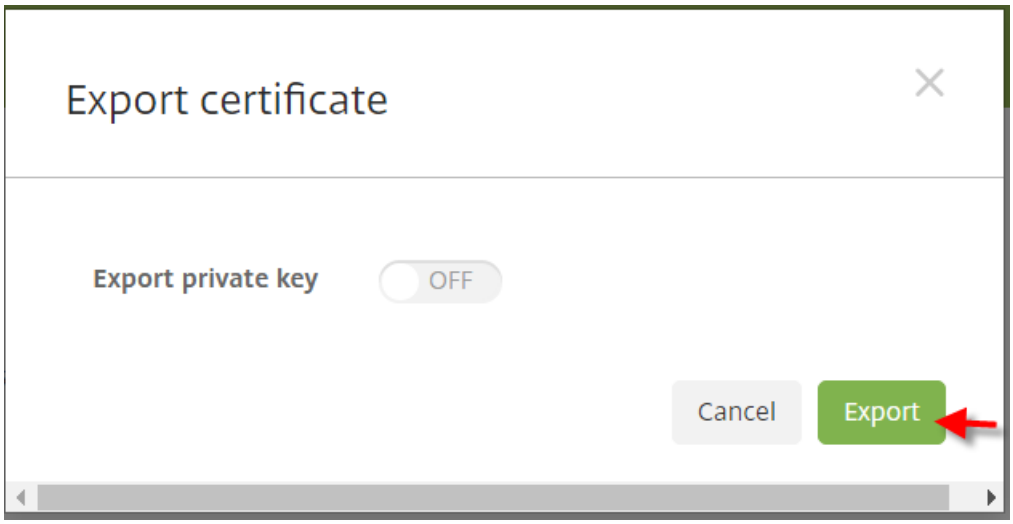
Exportación del certificado SAML desde el servidor XenMobile

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**. Haga clic en **Certificates**.

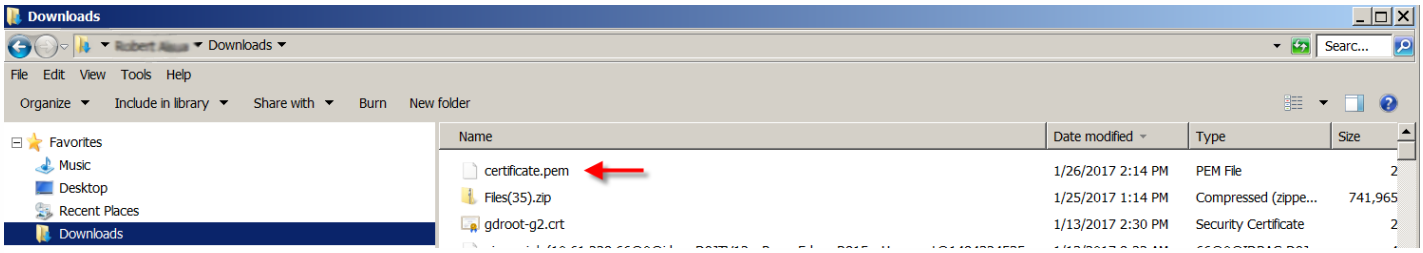
2. Busque el certificado SAML del servidor XenMobile.



3. Compruebe que **Export private key** está establecido en **Off**. Haga clic en **Export** para exportar el certificado a su directorio de descarga.

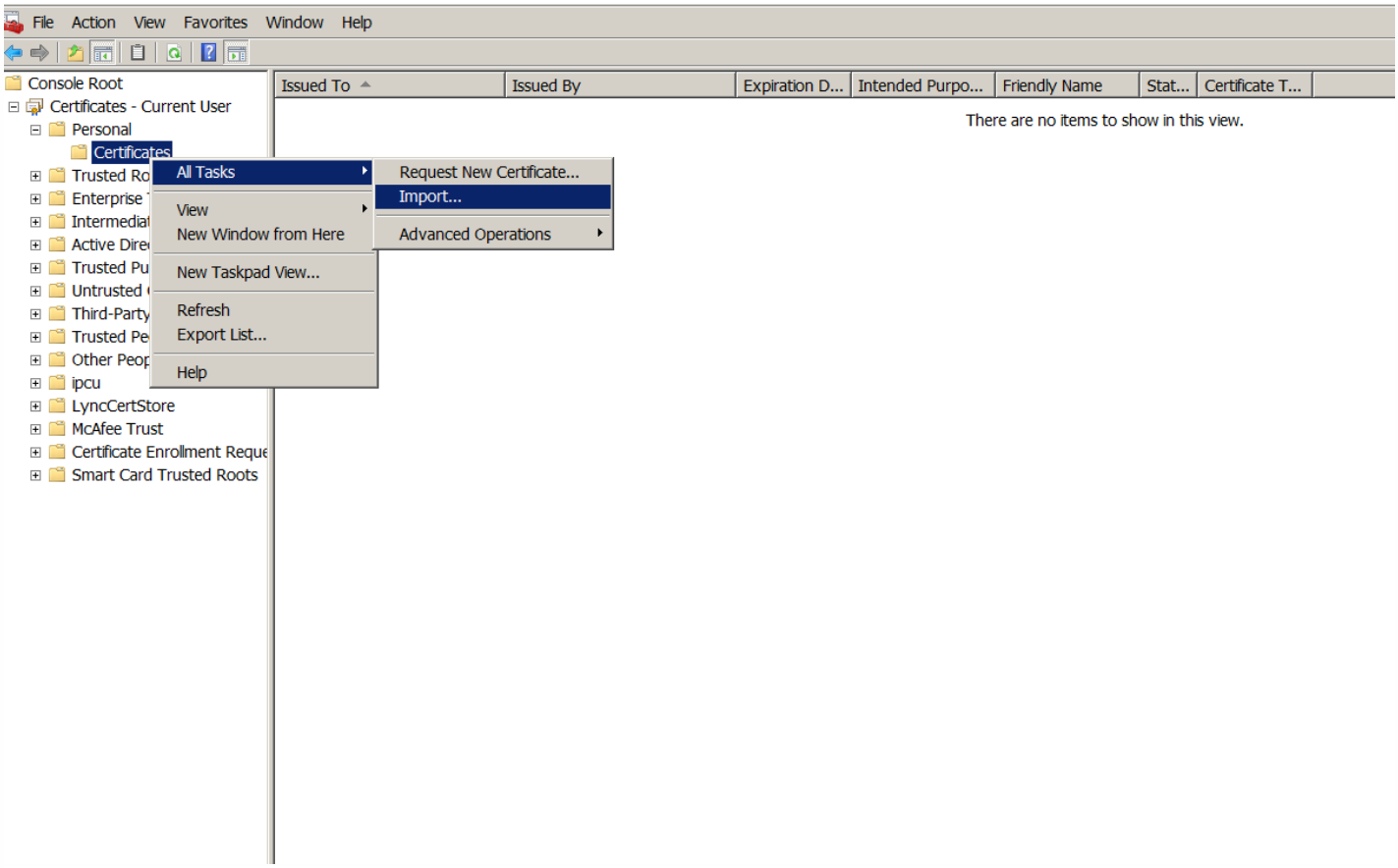


4. Busque el certificado en el directorio de descarga. El certificado está en formato PEM.



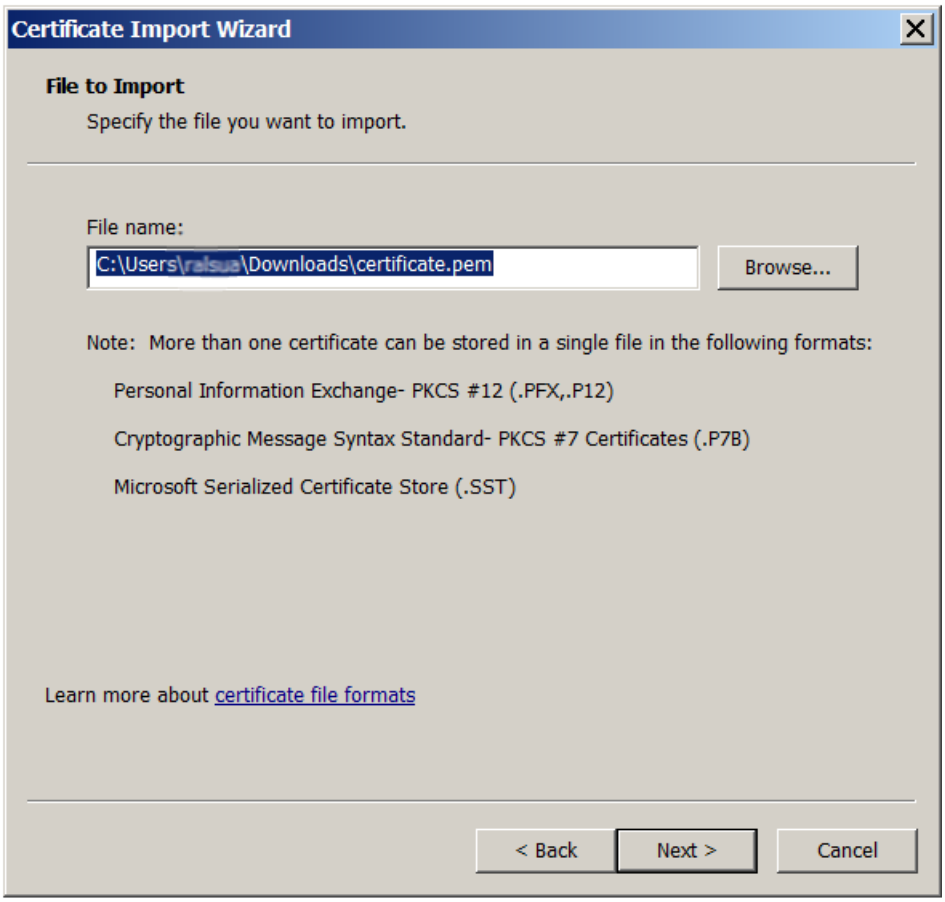
Conversión del certificado de PEM a CER

1. Abra Microsoft Management Console (MMC) y haga clic con el botón secundario en **Certificados > Todas las tareas > Importar**.

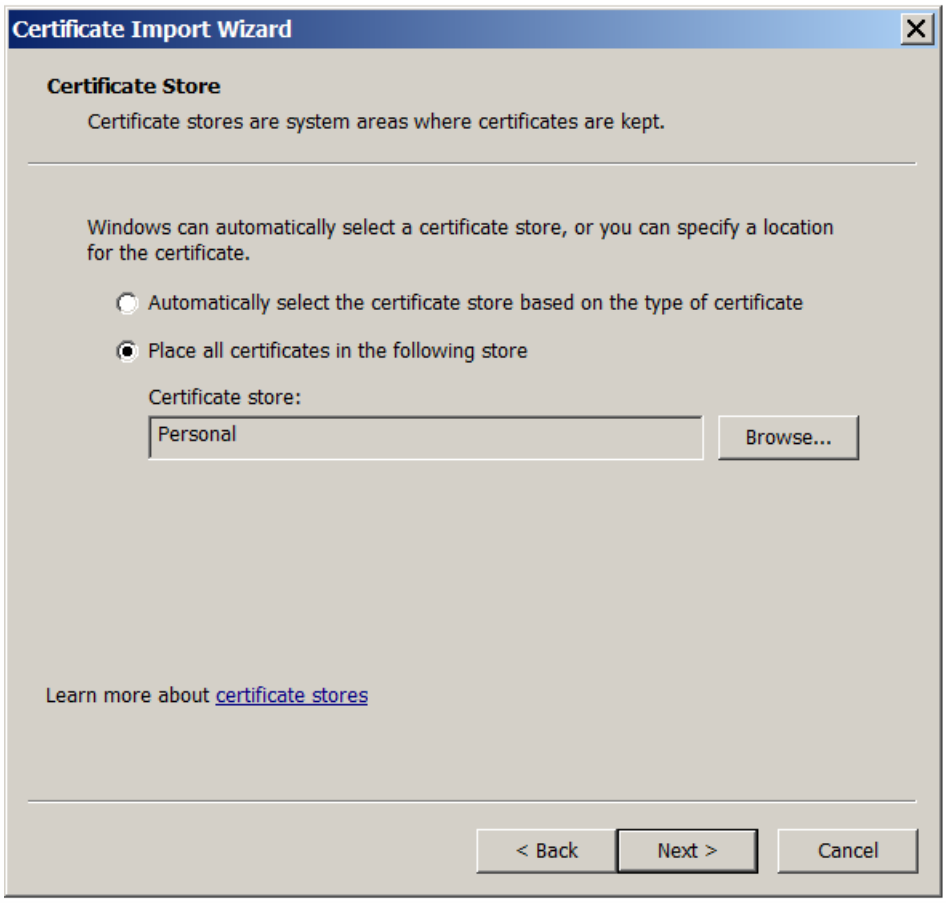


2. Cuando aparezca el Asistente para importación de certificados, haga clic en **Siguiente**.

3. Vaya al certificado en el directorio de descarga.

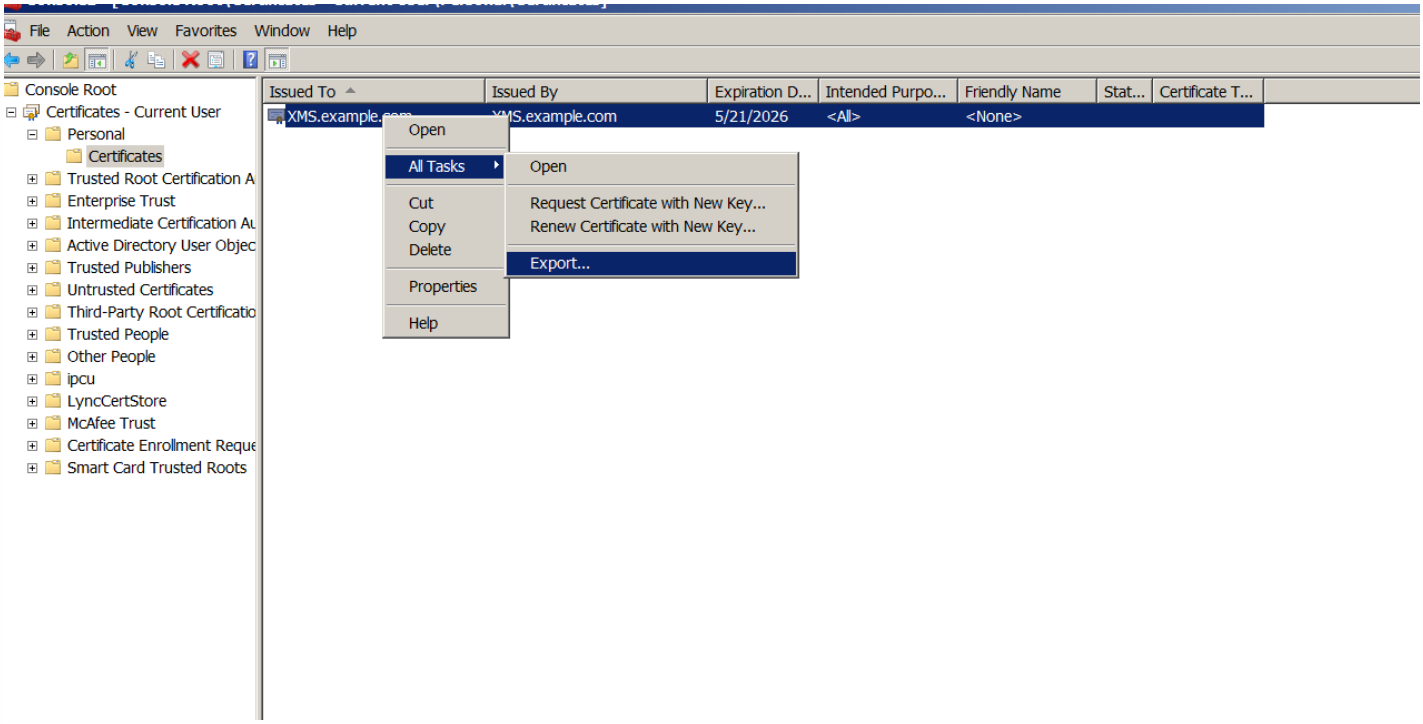


4. Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, seleccione **Personal** como almacén de certificados. Haga clic en **Siguiente**.



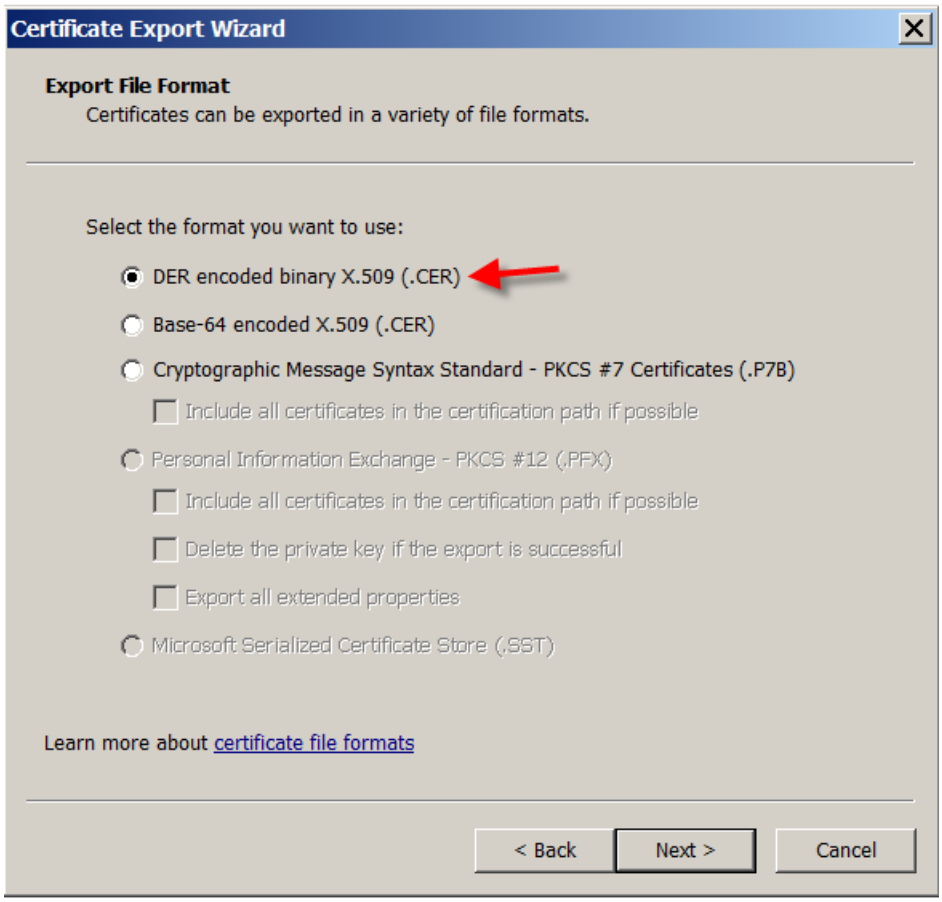
5. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** para cerrar la ventana de confirmación.

6. En la consola MMC, haga clic con el botón secundario en el certificado y seleccione **Todas las tareas > Exportar**.

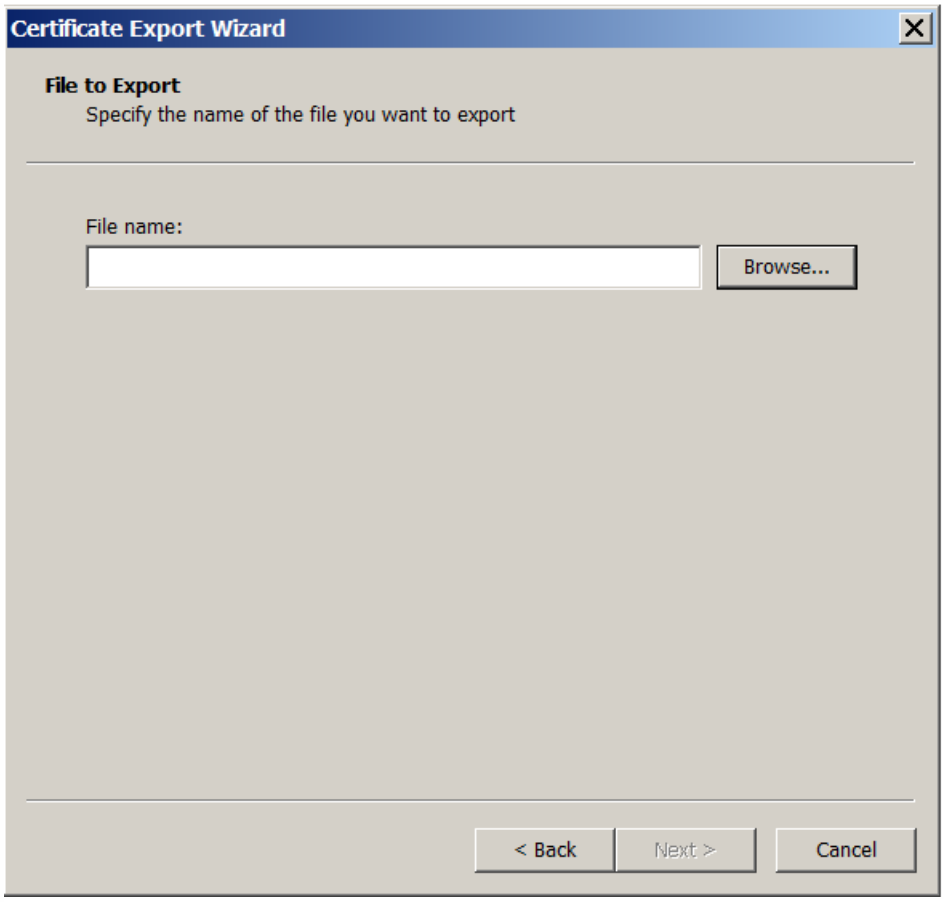


7. Cuando aparezca el Asistente para exportación de certificados, haga clic en **Siguiente**.

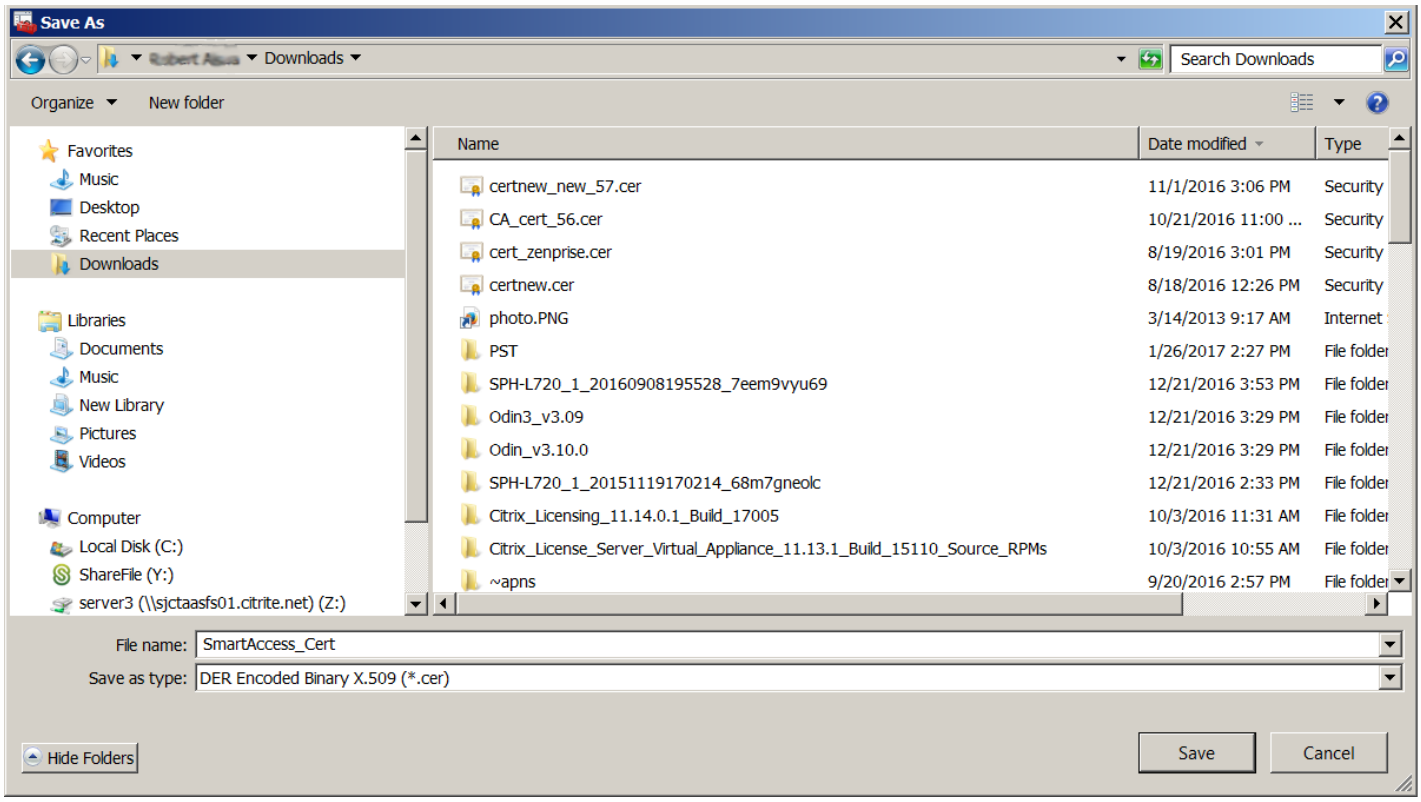
8. Seleccione el formato **DER binario codificado X.509 (.CER)**. Haga clic en **Siguiente**.



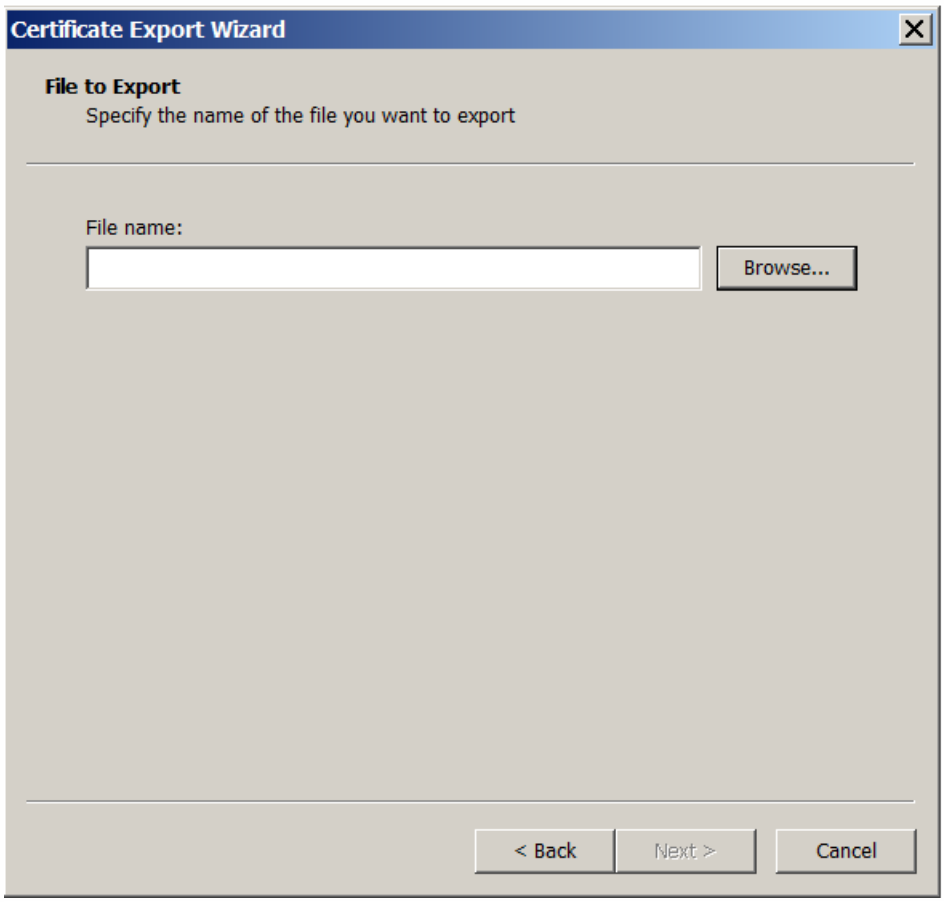
9 Vaya al certificado. Escriba un nombre para el certificado y haga clic en **Siguiente**.



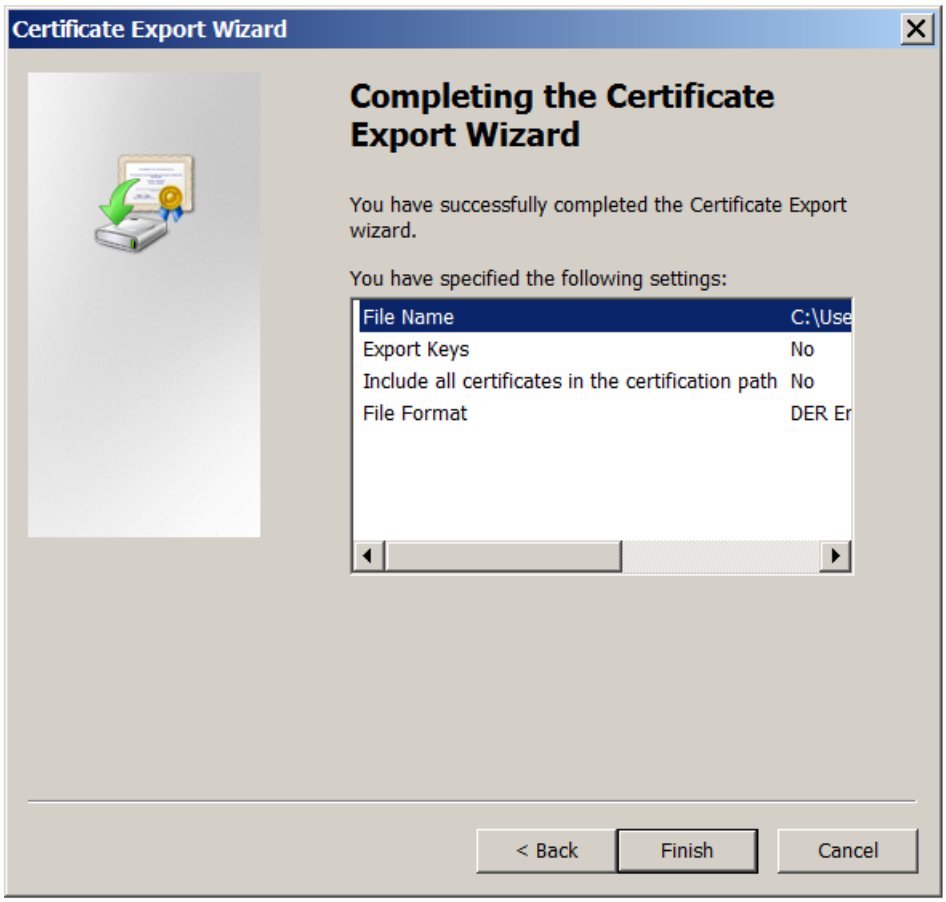
10. Guarde el certificado.



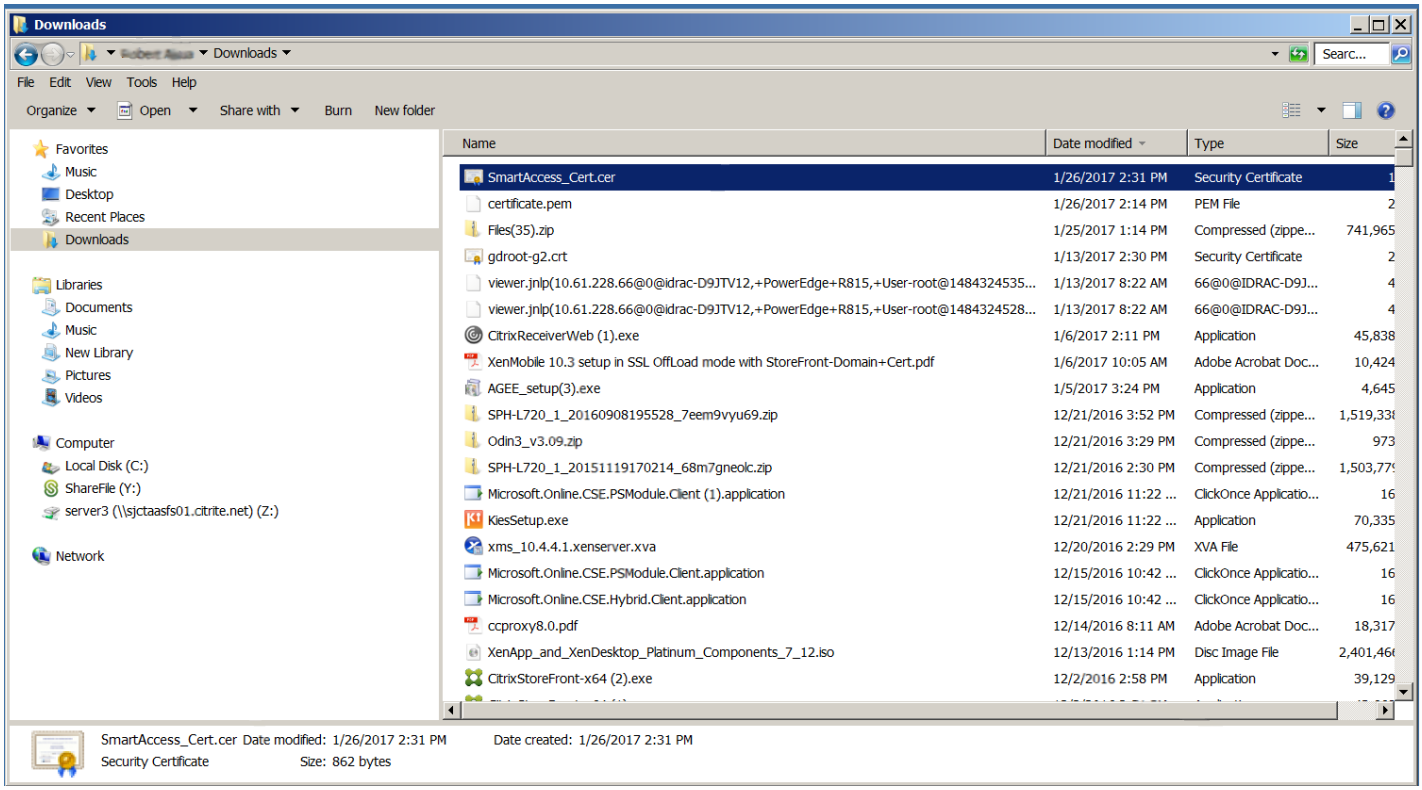
11. Vaya al certificado y haga clic en **Siguiente**.



12. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** para cerrar la ventana de confirmación.



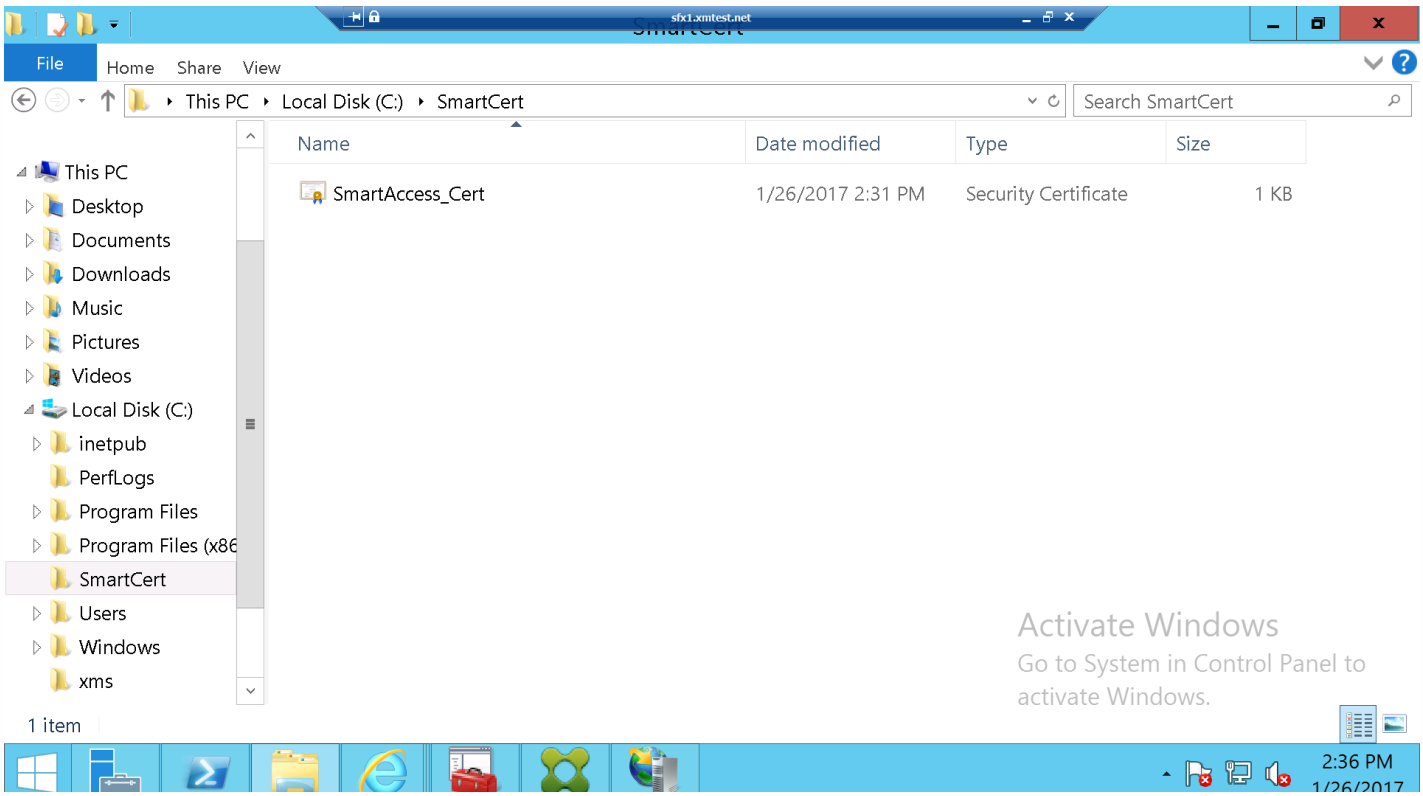
13. Busque el certificado en el directorio de descarga. Tenga en cuenta que el certificado tiene el formato CER.



Copia del certificado al servidor StoreFront

1. En el servidor StoreFront, cree una carpeta llamada **SmartCert**.

2. Copie el certificado a la carpeta **SmartCert**.

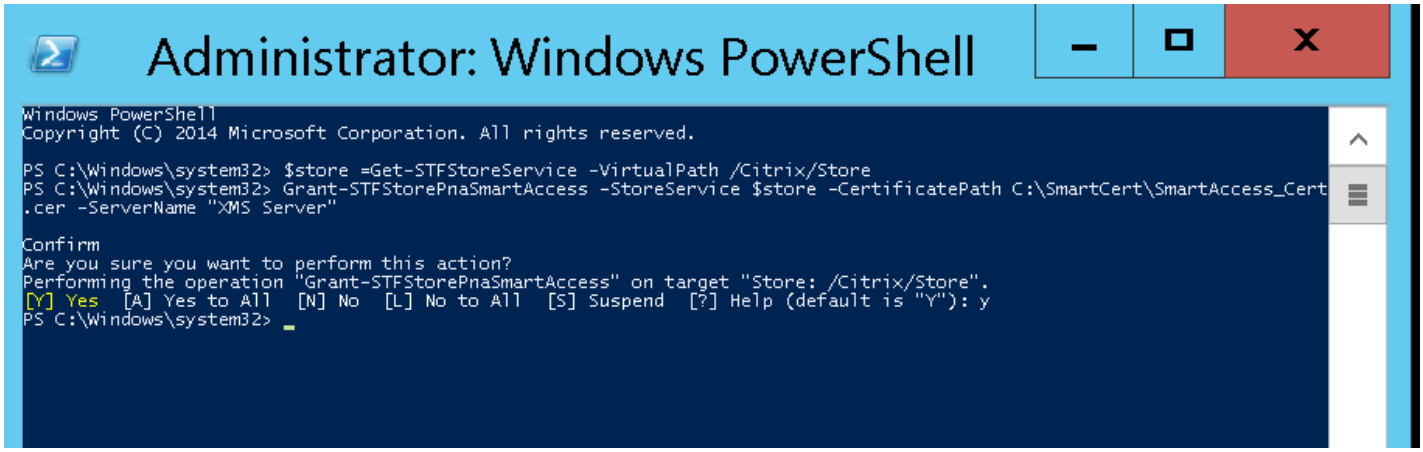


Configuración del certificado en el almacén de StoreFront

En el servidor StoreFront, ejecute el siguiente comando de PowerShell para configurar el certificado de XenMobile Server convertido que se encuentra en el almacén:

comando COPIAR

```
Grant-STFStorePnaSmartAccess -StoreService $store -CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
```



Si ya hay certificados existentes en el almacén de StoreFront, ejecute este comando de PowerShell para revocarlos:

comando COPIAR

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

De forma alternativa, puede ejecutar cualquiera de estos comandos de PowerShell en el servidor StoreFront para revocar los certificados existentes en el almacén de StoreFront:

- Revocar por nombre:

comando COPIAR

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server”
```

- Revocar por huella digital:

comando COPIAR

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess -StoreService $store -CertificateThumbprint "1094821dec7834d5d42 bb456329efe4fca8
```

- Revocar por objeto de servidor:

comando COPIAR

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess -StoreService $store

Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess $access.AccessConditionsTrusts[0]
```

Configuración de la directiva de SmartAccess para XenApp y XenDesktop

Para agregar la directiva pertinente de SmartAccess al grupo que entrega la aplicación HDX:

1. En el servidor XenApp y XenDesktop, abra Citrix Studio.

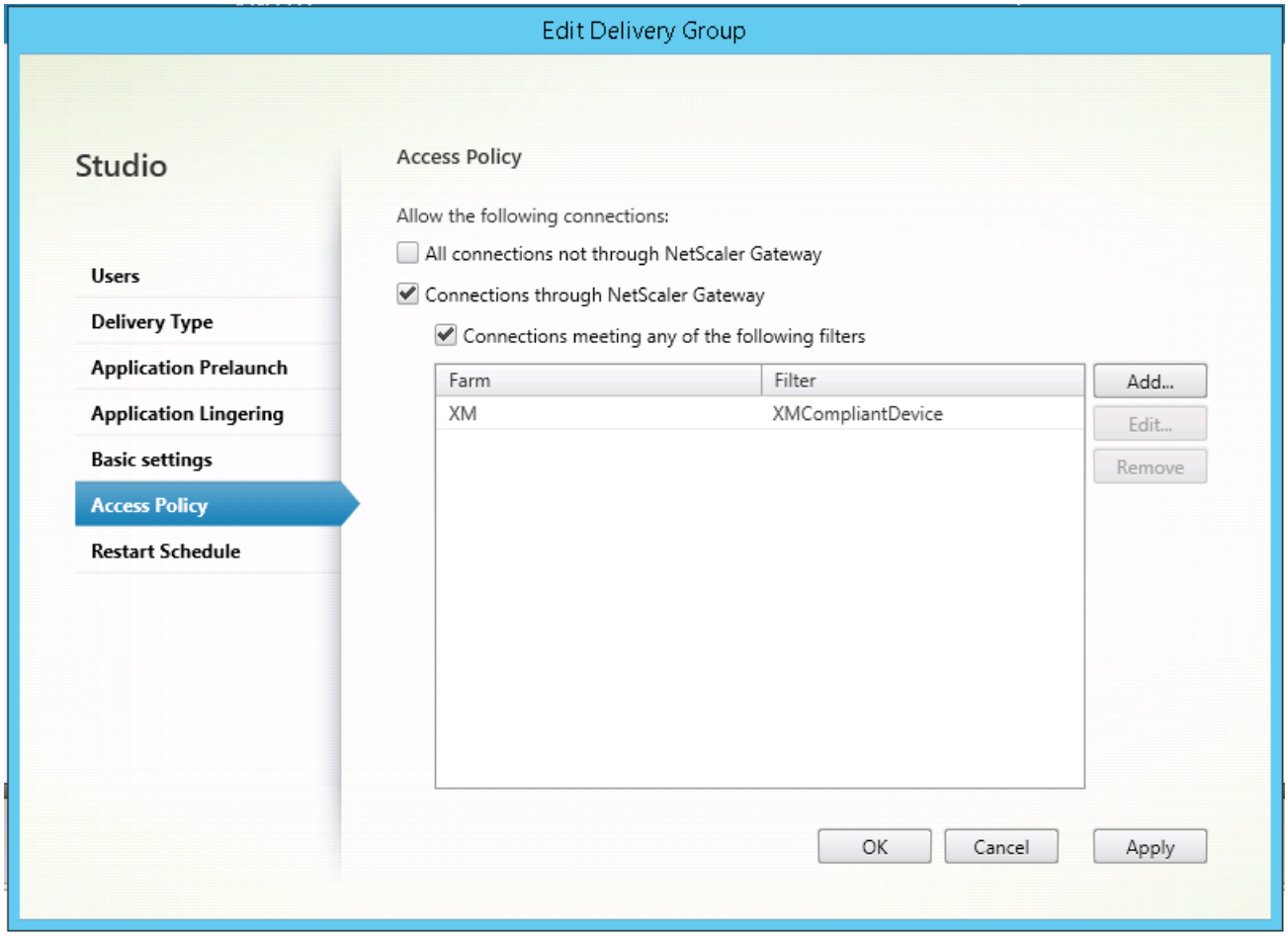
2. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

3. Seleccione un grupo que entrega la aplicación o aplicaciones cuyo acceso quiere controlar. Seleccione **Modificar grupo de entrega** en el panel **Acciones**.

4. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway** y **Conexiones que cumplan cualquiera de estos filtros**.

5. Haga clic en **Agregar**.

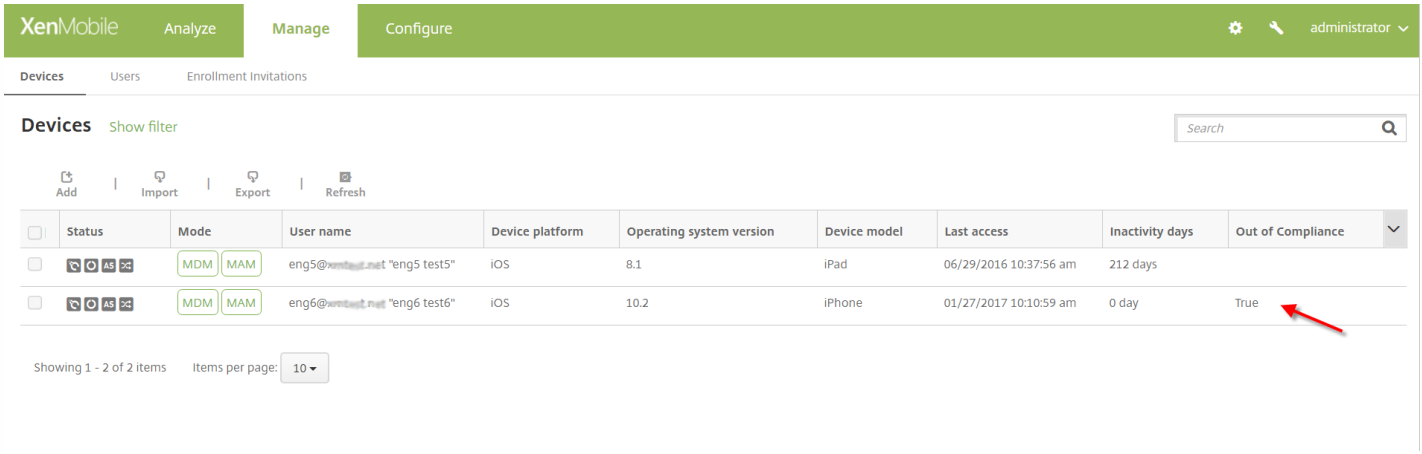
6. Agregue una directiva de acceso donde **Comunidad** es **XM** y **Filtro** es **XMCompliantDevice**.



7. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Configuración de acciones automatizadas en XenMobile

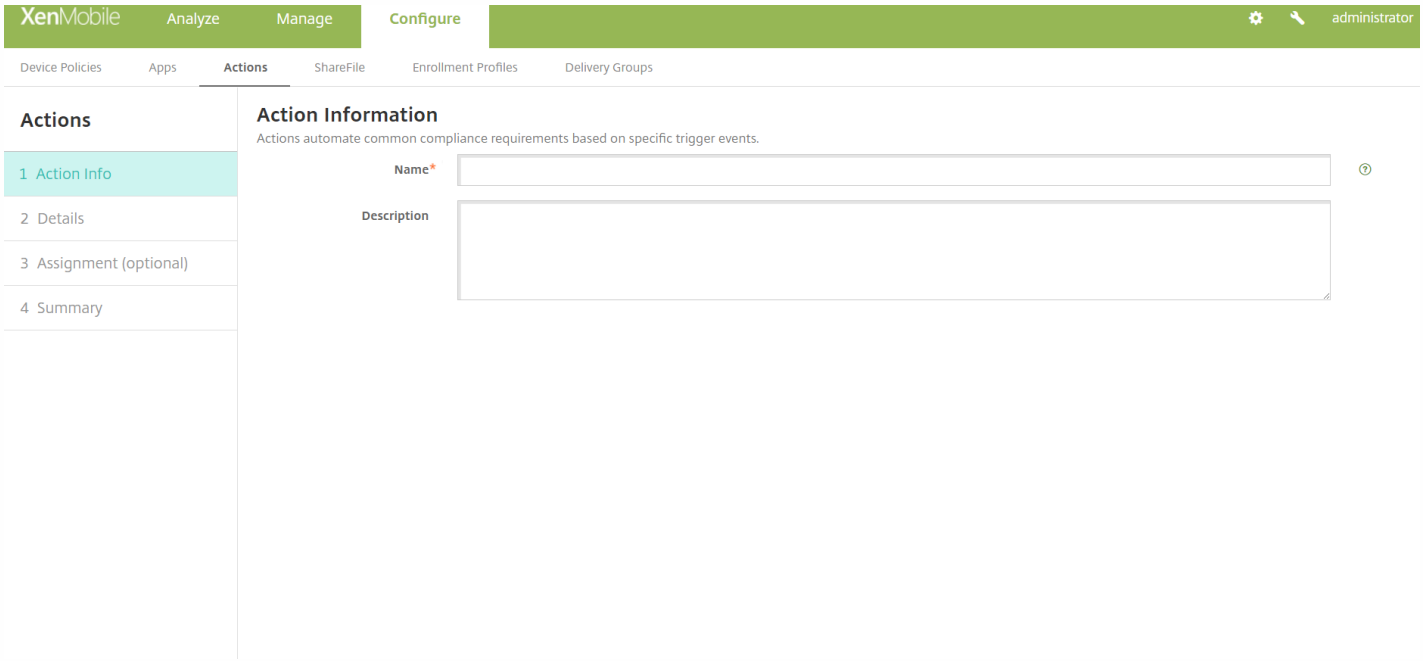
La directiva SmartAccess configurada en el grupo de entrega para una aplicación HDX deniega el acceso a un dispositivo cuando este no cumple los requisitos. Utilice acciones automatizadas para marcar el dispositivo como no conforme.



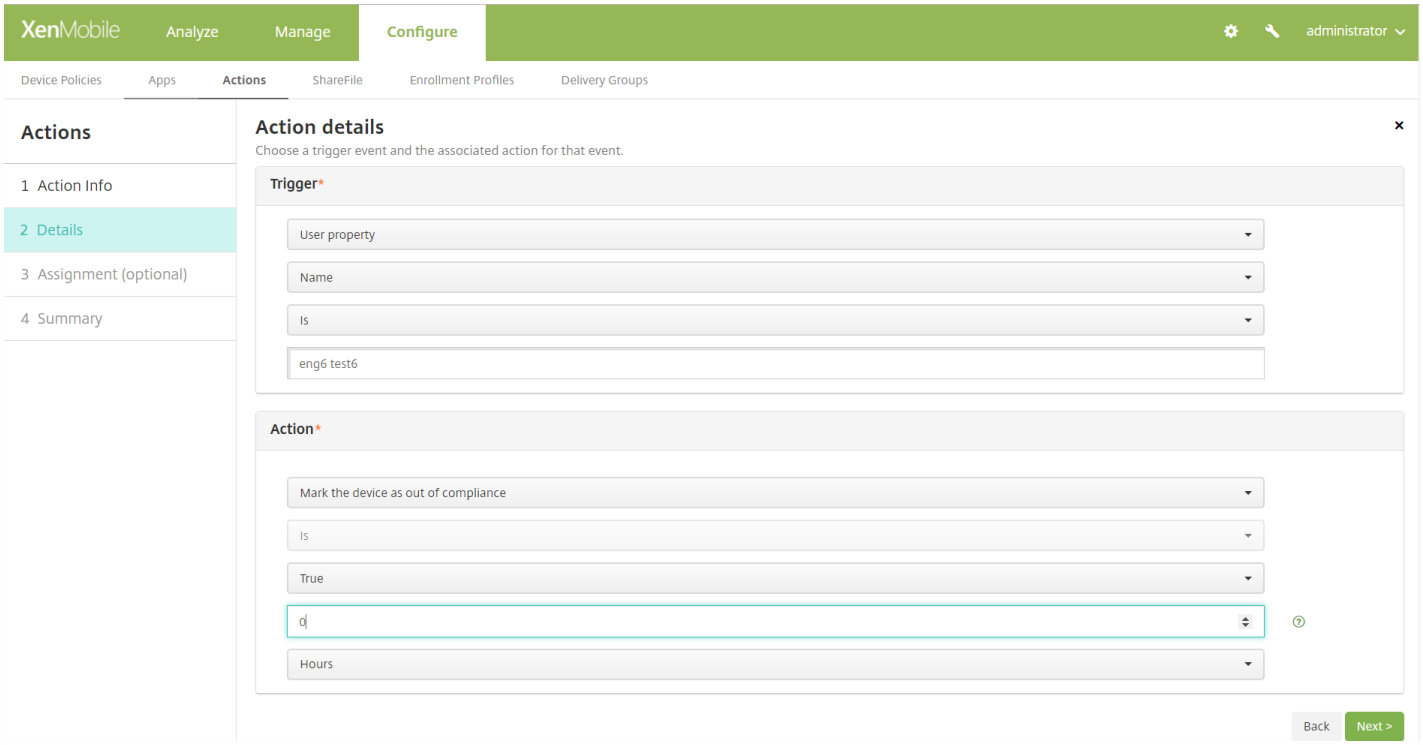
1. En la consola de XenMobile, haga clic en **Configure > Actions**. Aparecerá la página **Actions**.

2. Haga clic en **Add** para agregar una nueva acción. Aparecerá la página **Action Information**.

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



4. Haga clic en **Next**. Aparecerá la página **Action details**. En el ejemplo siguiente, se crea un desencadenador que marca inmediatamente dispositivos como no conformes si tienen el nombre de la propiedad de usuario **eng5** o **eng6**.

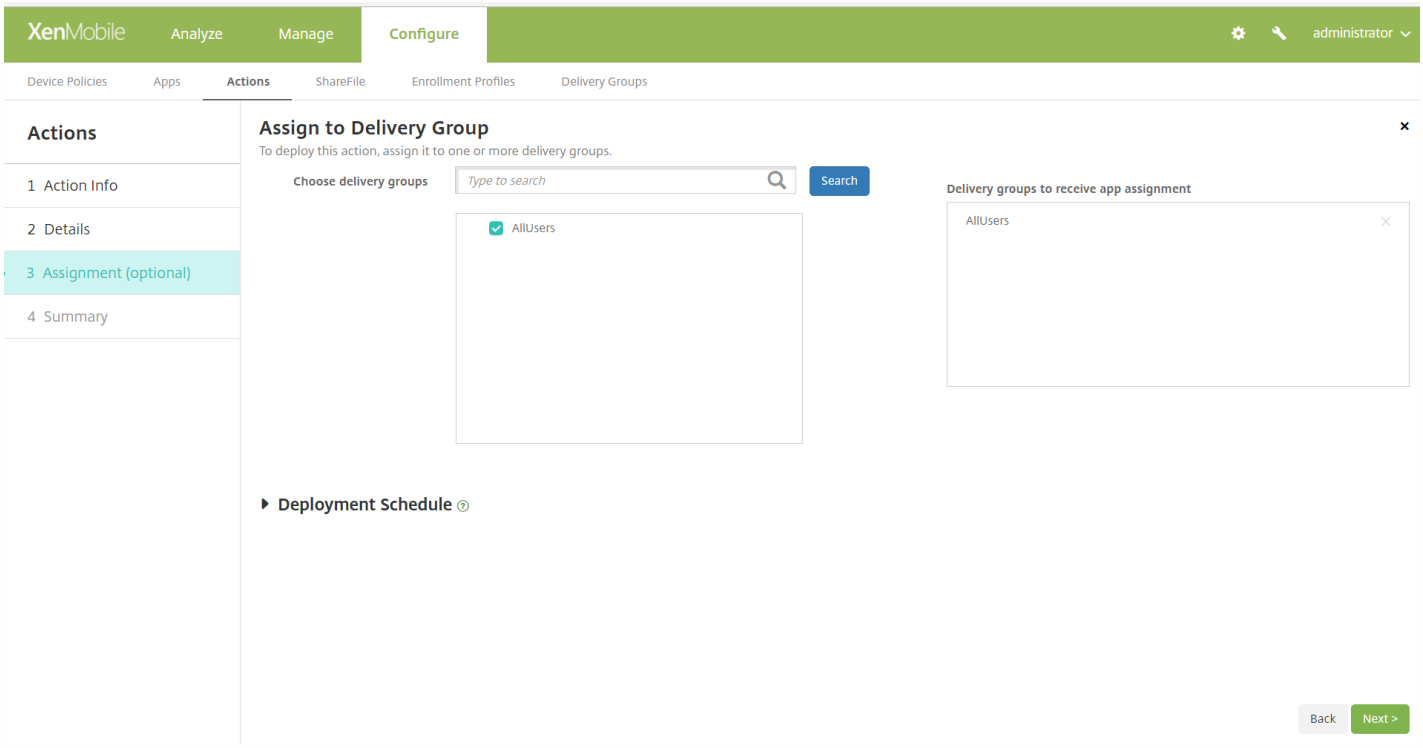


5. En la lista **Trigger**, elija **Device property**, **User property** o **Installed app name**. SmartAccess no admite desencadenadores de sucesos.

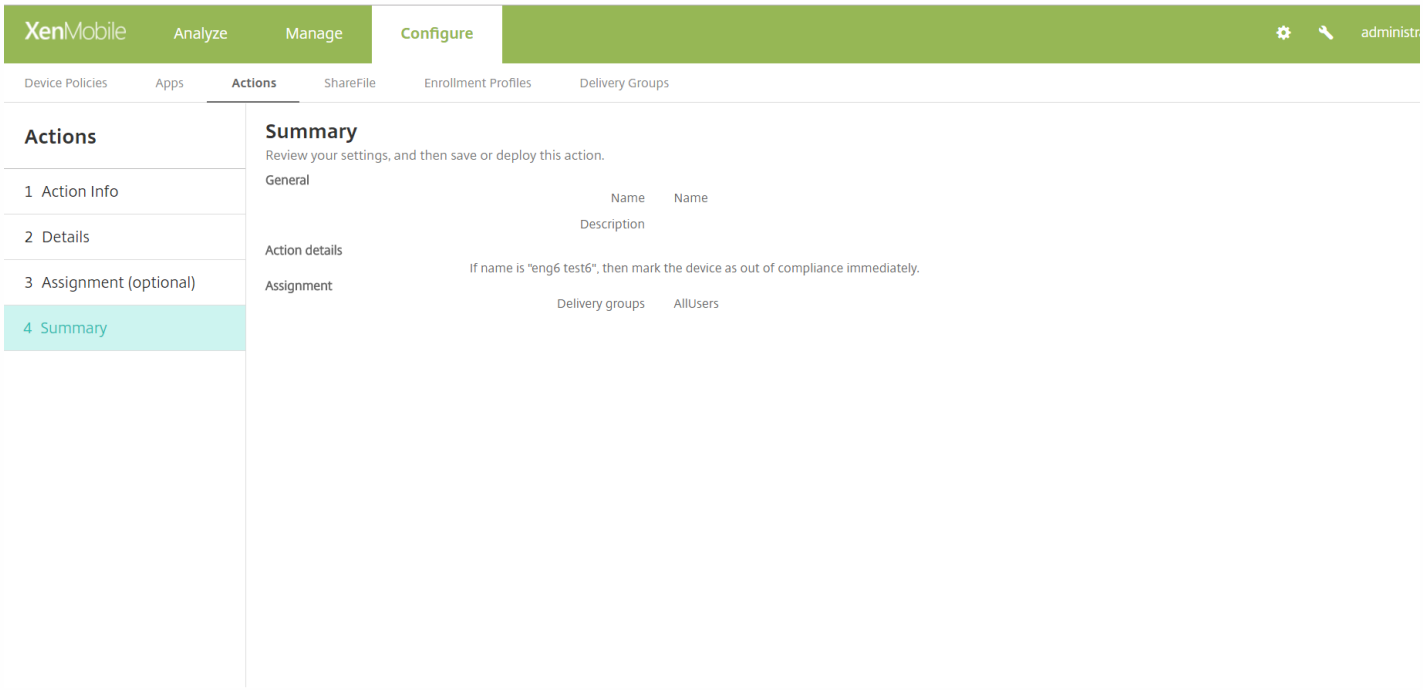
6. En la lista **Action**:

- Seleccione **Mark the device as out of compliance.**
- Elija **Is**.
- Elija **True**.
- Para que la acción de marcar el dispositivo como no conforme cuando se cumpla la condición del desencadenador sea inmediata, establezca el período de tiempo en **0**.

7. Elija el grupo o grupos de entrega de XenMobile a los que aplicar esta acción.



8. Revise el resumen de la acción.

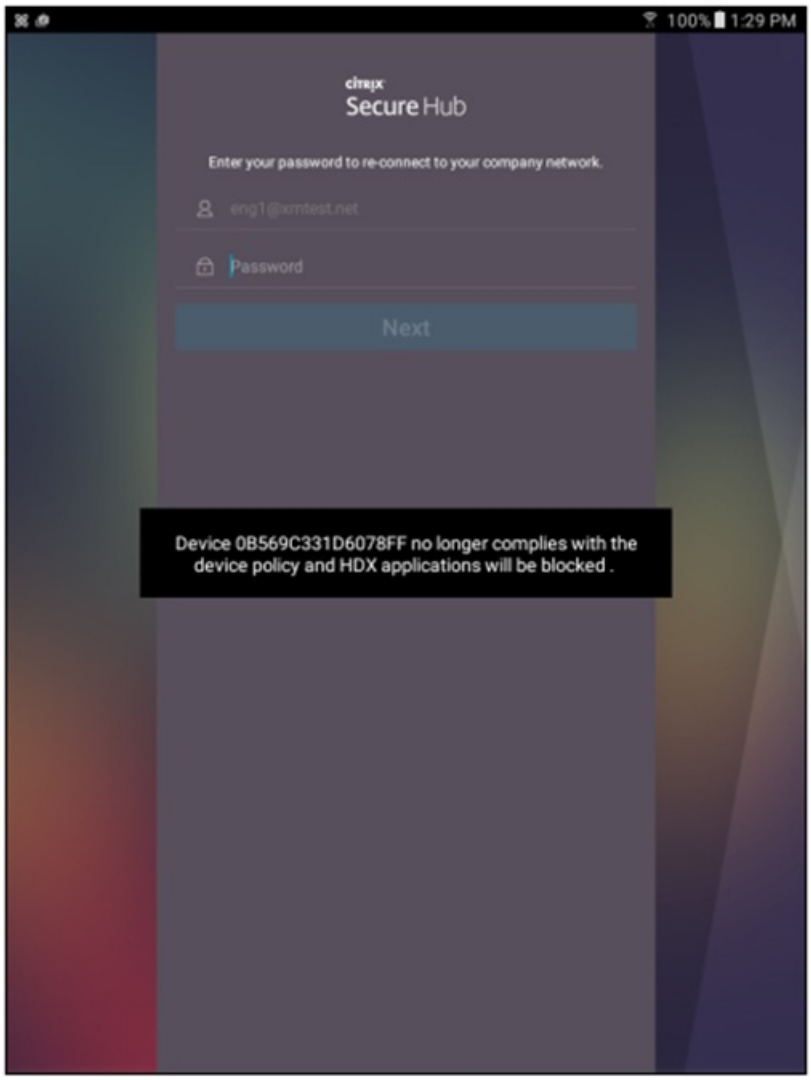


9 Haga clic en **Next** y, a continuación, haga clic en **Save**.

Cuando el dispositivo se marca como no conforme, las aplicaciones HDX ya no aparecen en la tienda de Secure Hub. El usuario ya no se suscribe a las aplicaciones. No se envía ninguna notificación al dispositivo y, en la tienda de Secure Hub, no hay nada que indique que las aplicaciones HDX estaban disponibles.

Si quiere notificar a los usuarios cuando un dispositivo se marque como no conforme, cree una notificación y, a continuación, cree una acción automatizada para enviar esa notificación.

En este ejemplo, se crea y se envía la siguiente notificación cuando un dispositivo se marca como no conforme: "Deviceserial number or telephone number no longer complies with the device policy and HDXapplications will be blocked" (El número de serie del dispositivo o el número de teléfono ya no cumple las condiciones de la directiva de dispositivo, por lo tanto se bloquearán las aplicaciones HDX).



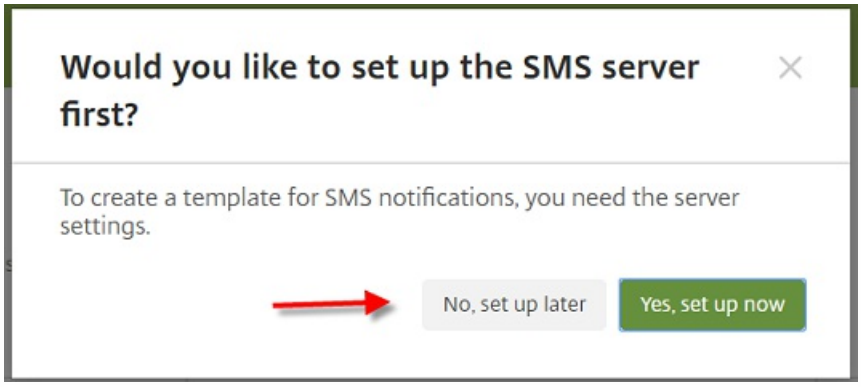
Creación de la notificación que ven los usuarios cuando un dispositivo se marca como no conforme

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**.

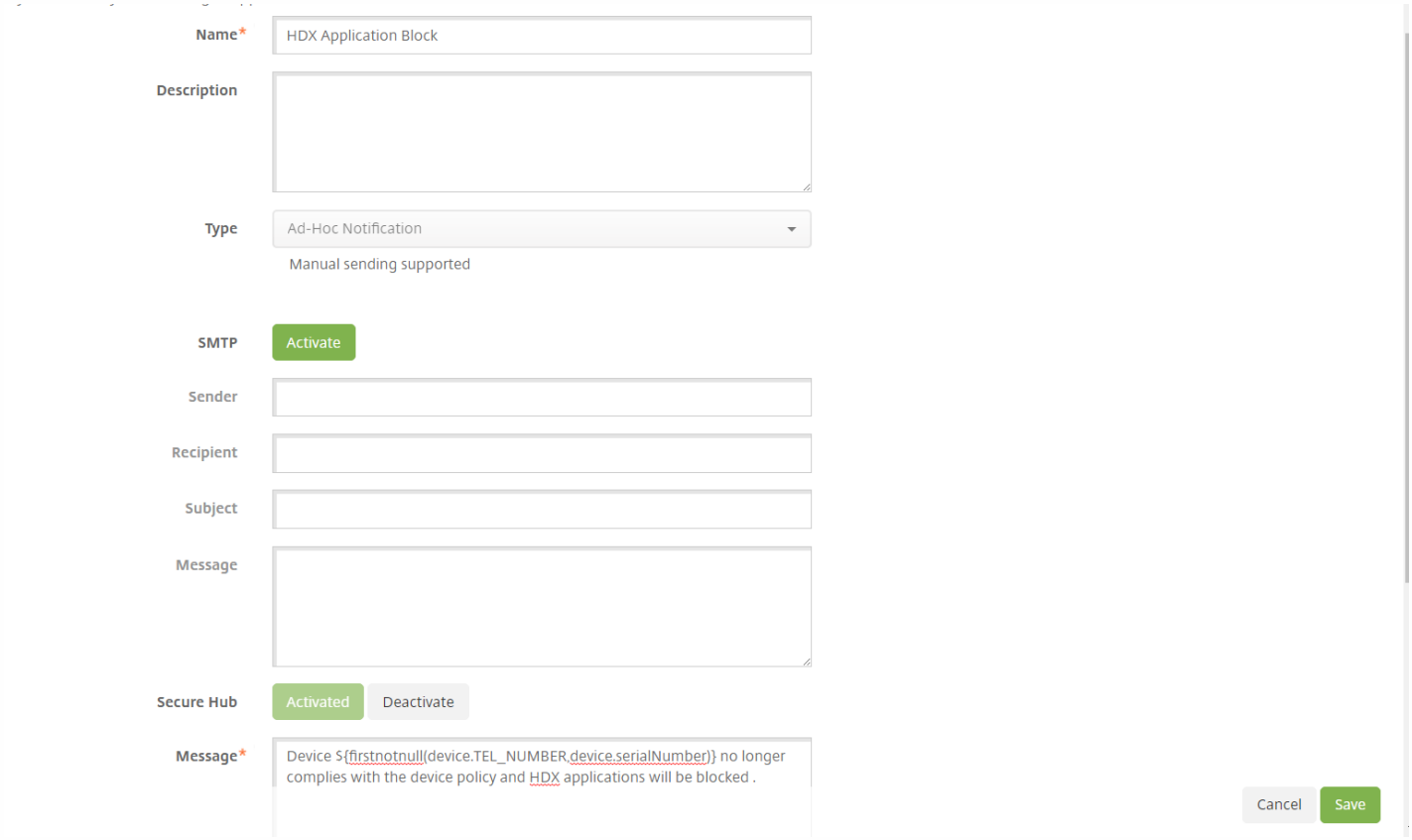
3. Haga clic en **Add** para agregar una nueva plantilla de notificaciones en la página **Notification Templates**.

4. Cuando se le solicite configurar primero el servidor SMS, haga clic en **No, set up later**.



5. Configure estos parámetros:

- **Name**. Bloqueo de aplicaciones HDX
- **Description**. Notificación del agente cuando el dispositivo no es conforme
- **Type**. Notificación Ad Hoc
- **Secure Hub**. Activado
- **Message**. El dispositivo ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} ya no cumple la directiva de dispositivo: se bloquearán las aplicaciones HDX. (Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.)



6. Haga clic en **Save**.

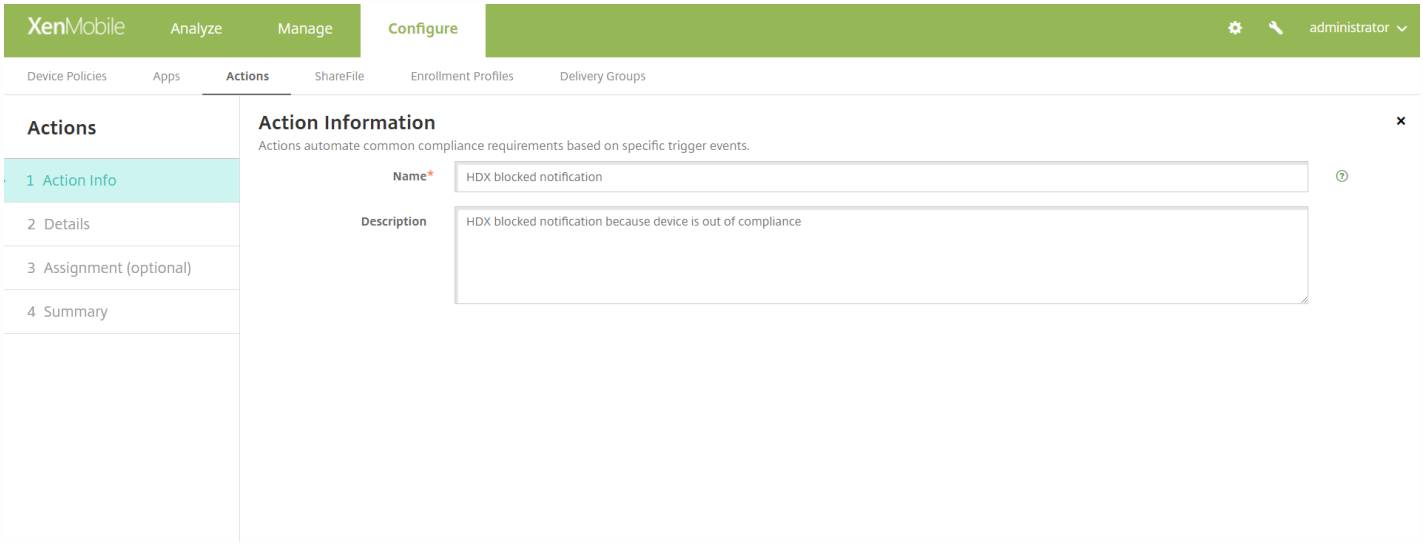
Creación de la acción que envía la notificación cuando un dispositivo se marca como no conforme

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

2. Haga clic en **Add** para agregar una nueva acción. Aparecerá la página **Action Information**.

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

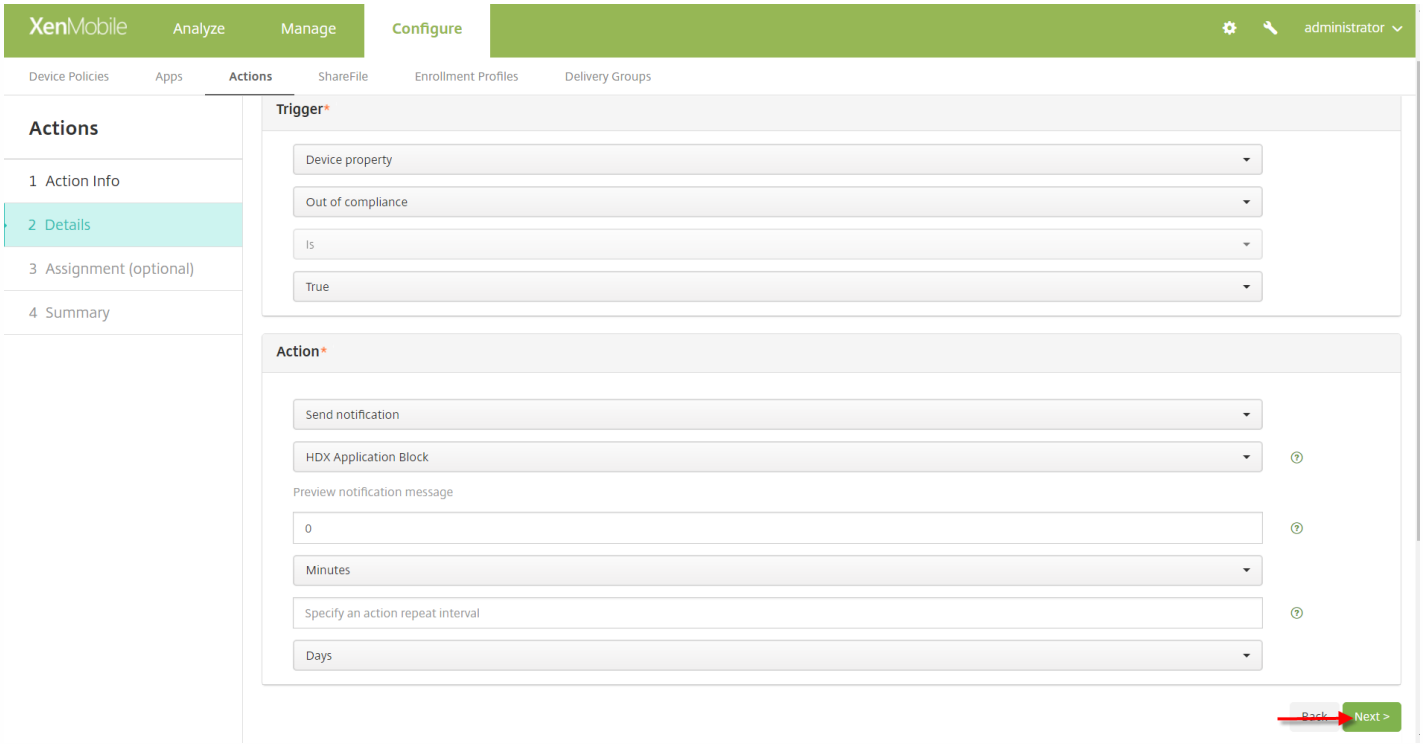
- Name: Notificación de HDX bloqueado
- **Description**. Notificación de HDX bloqueado porque el dispositivo no es conforme



4. Haga clic en **Next**. Aparecerá la página **Action details**.

5. En la lista **Trigger**:

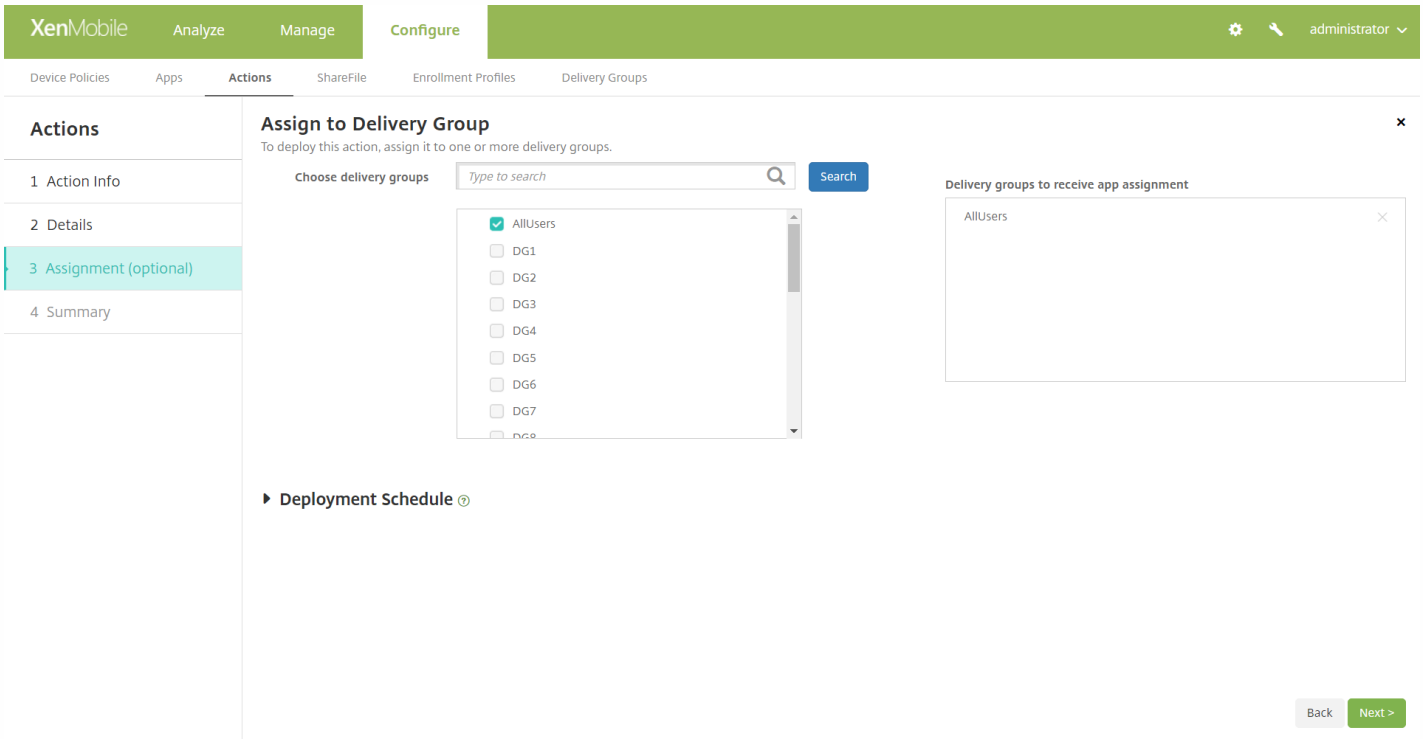
- Elija **Device property**.
- Elija **Out of compliance.**
- Elija **Is**.
- Elija **True**.



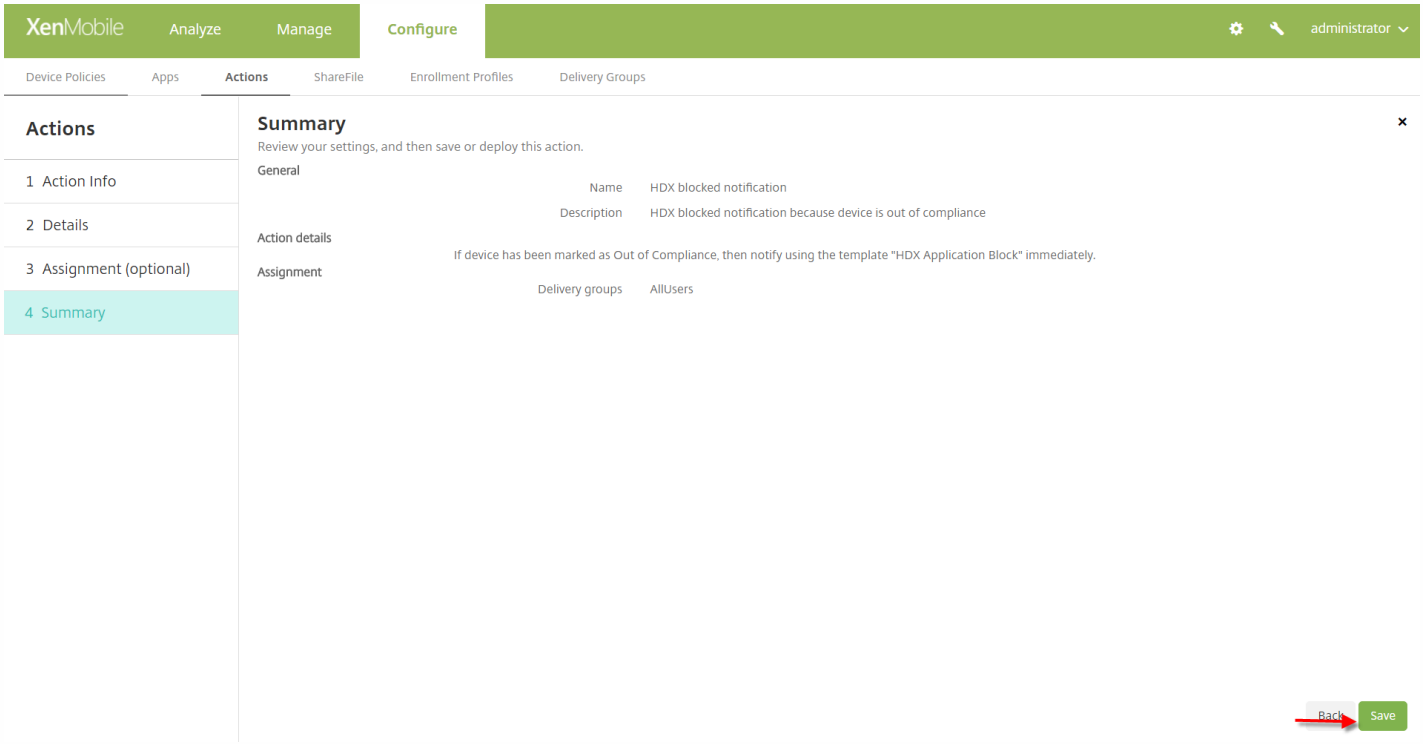
6. En la lista **Action**, especifique las acciones que ocurren cuando se cumplen las condiciones del desencadenador:

- Elija **Send notification**.
- Elija **HDX Application Block, the notification you created**.
- Elija **0**. Si este valor es 0, la notificación se enviará tan pronto como se cumpla la condición del desencadenador.

7. Elija el grupo o grupos de entrega de XenMobile a los que aplicar esta acción. En este ejemplo, elija **AllUsers**.



8. Revise el resumen de la acción.



9 Haga clic en **Next** y, a continuación, haga clic en **Save**.

Para obtener información detallada sobre cómo configurar acciones automatizadas, consulte Acciones automatizadas.

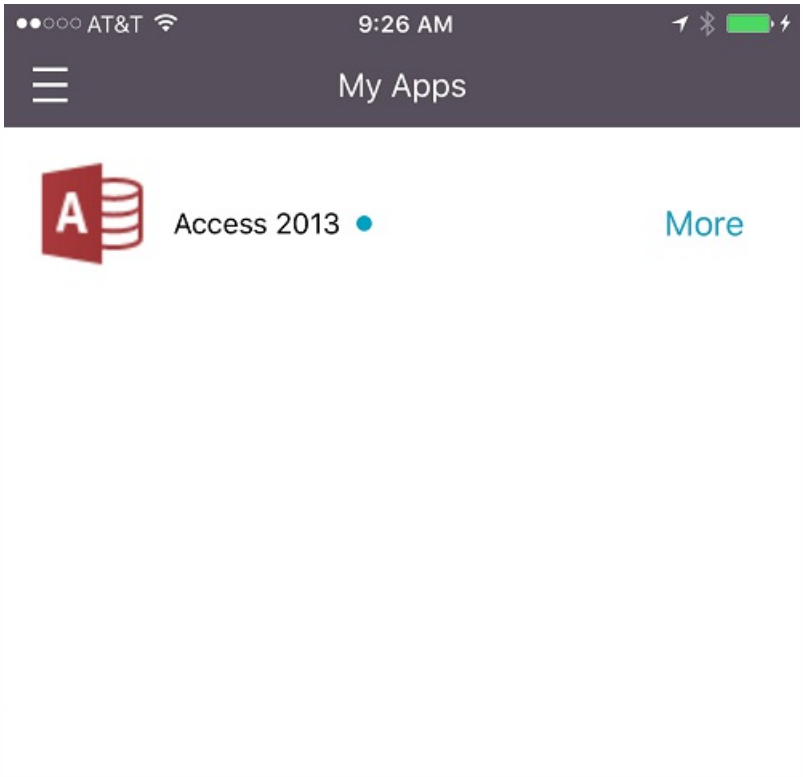
Cómo los usuarios vuelven a tener acceso a aplicaciones HDX

Los usuarios pueden volver a obtener acceso a las aplicaciones HDX una vez que el dispositivo vuelve a estar conforme:

1. En el dispositivo, vaya a la tienda de Secure Hub para actualizar las aplicaciones que contiene la tienda.

2. Vaya a la aplicación y toque en **Agregar** a la aplicación.

Una vez agregada, la aplicación aparece en Mis aplicaciones, con un punto azul porque es una aplicación recién instalada.



Implementación de recursos

Feb 27, 2017

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*. En este artículo, se describe cómo agregar, administrar e implementar grupos de entrega; cómo cambiar el orden de implementación de los recursos y las acciones en 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 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 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
Apps (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
Delivery group (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 ordenarlos es el siguiente:

a. Colocar los recursos de los grupos de entrega que tengan un orden de implementación definido 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.

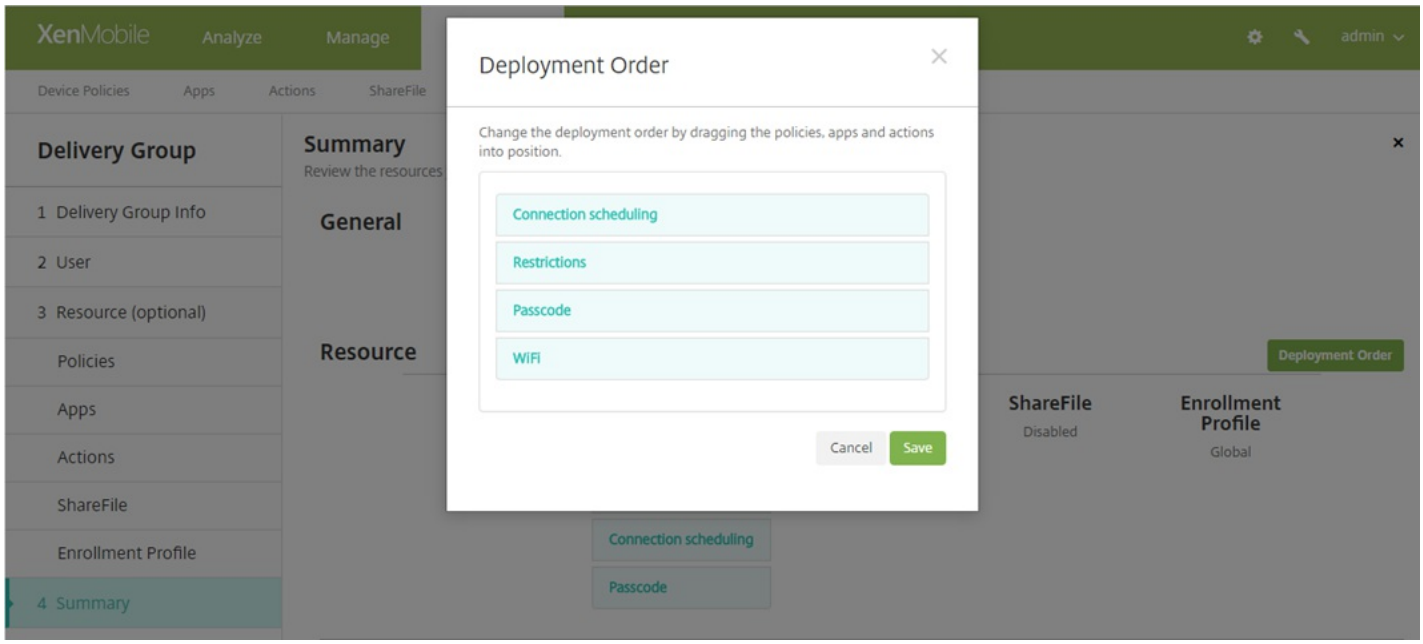
c. Durante el proceso de ordenamiento, se mantiene el orden de implementación especificado para los recursos de un grupo de entrega, si lo hubiera. Si no lo hay, los recursos del grupo de entrega se ordenan por nombre de recurso.

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. Como se indica en los pasos anteriores, el algoritmo de cálculo elimina los recursos innecesarios y solo entrega el primer recurso de esta lista. Cuando se quitan los recursos duplicados de este 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, quiere entregar la directiva **Passcode** antes que la directiva **WiFi**.



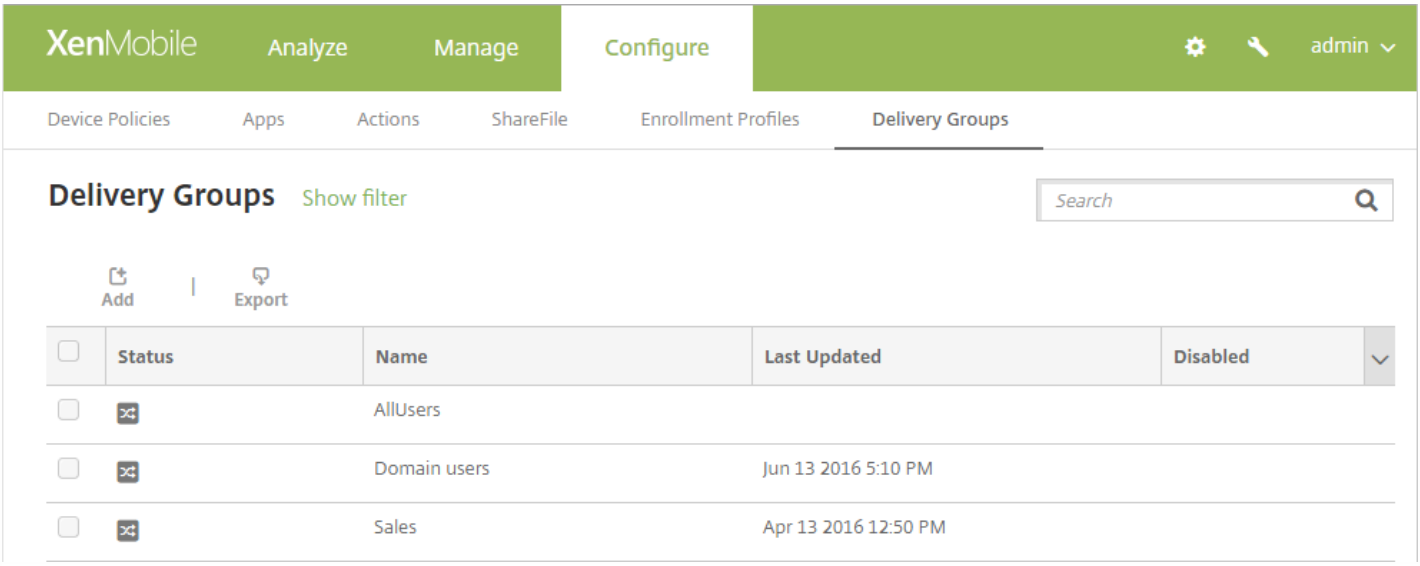
Si el algoritmo de cálculo ordenara los grupos de implementación solo por nombre, XenMobile realizaría la implementación en este orden, empezando por el grupo de entrega Gestores de cuentas 1: **WiFi**, **Passcode**, **Connection scheduling** y **Restrictions**. XenMobile omitiría **Passcode** y **WiFi**, 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

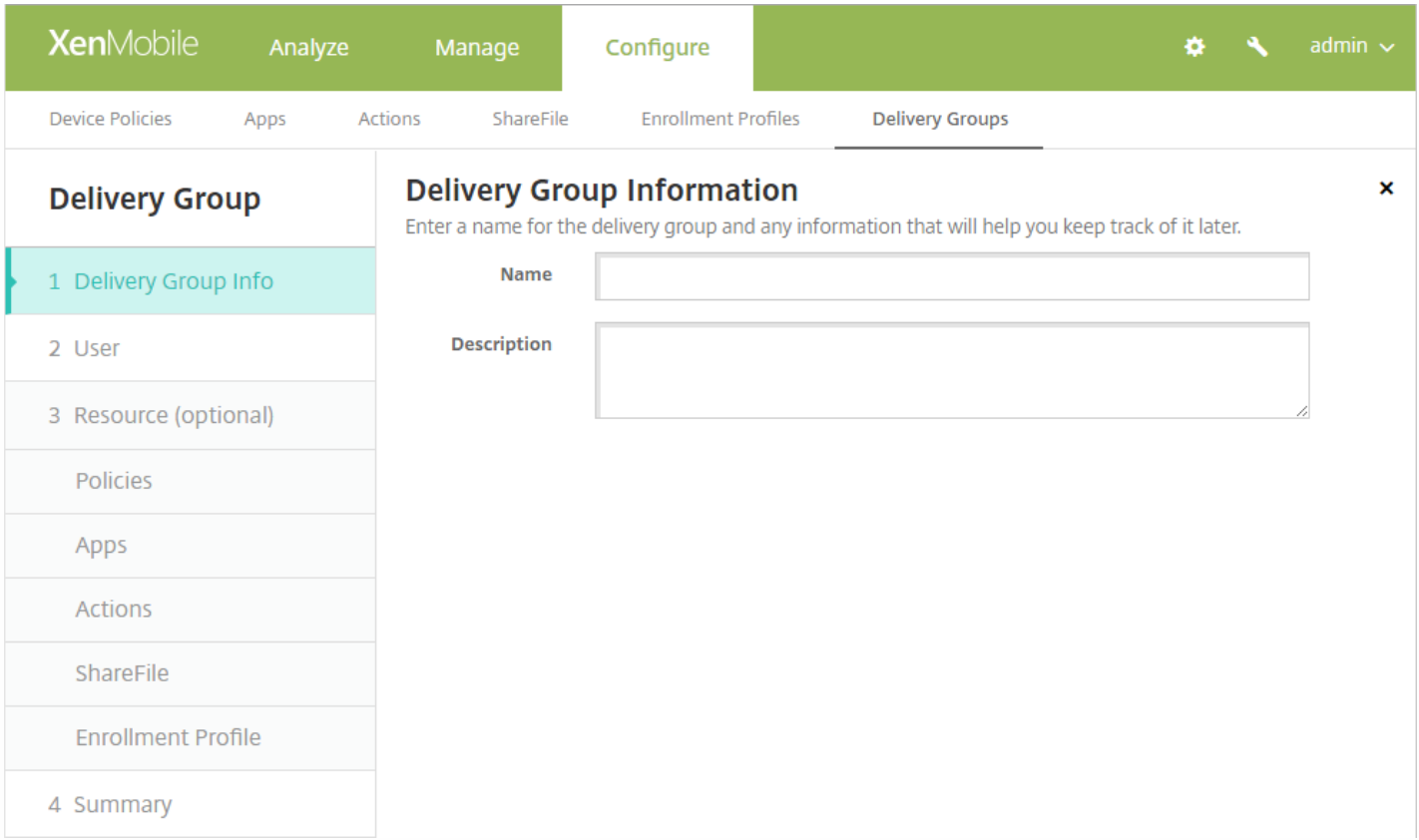
administrador, el algoritmo de cálculo coloca los recursos del grupo de entrega Gestores de cuentas 2 por encima de los recursos del grupo de entrega Gestores de cuentas 1 en la lista. Como resultado de ello, XenMobile implementa las directivas en este orden: **Connection scheduling**, **Restrictions**, **Passcode** y **WiFi**. XenMobile ignora 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**.



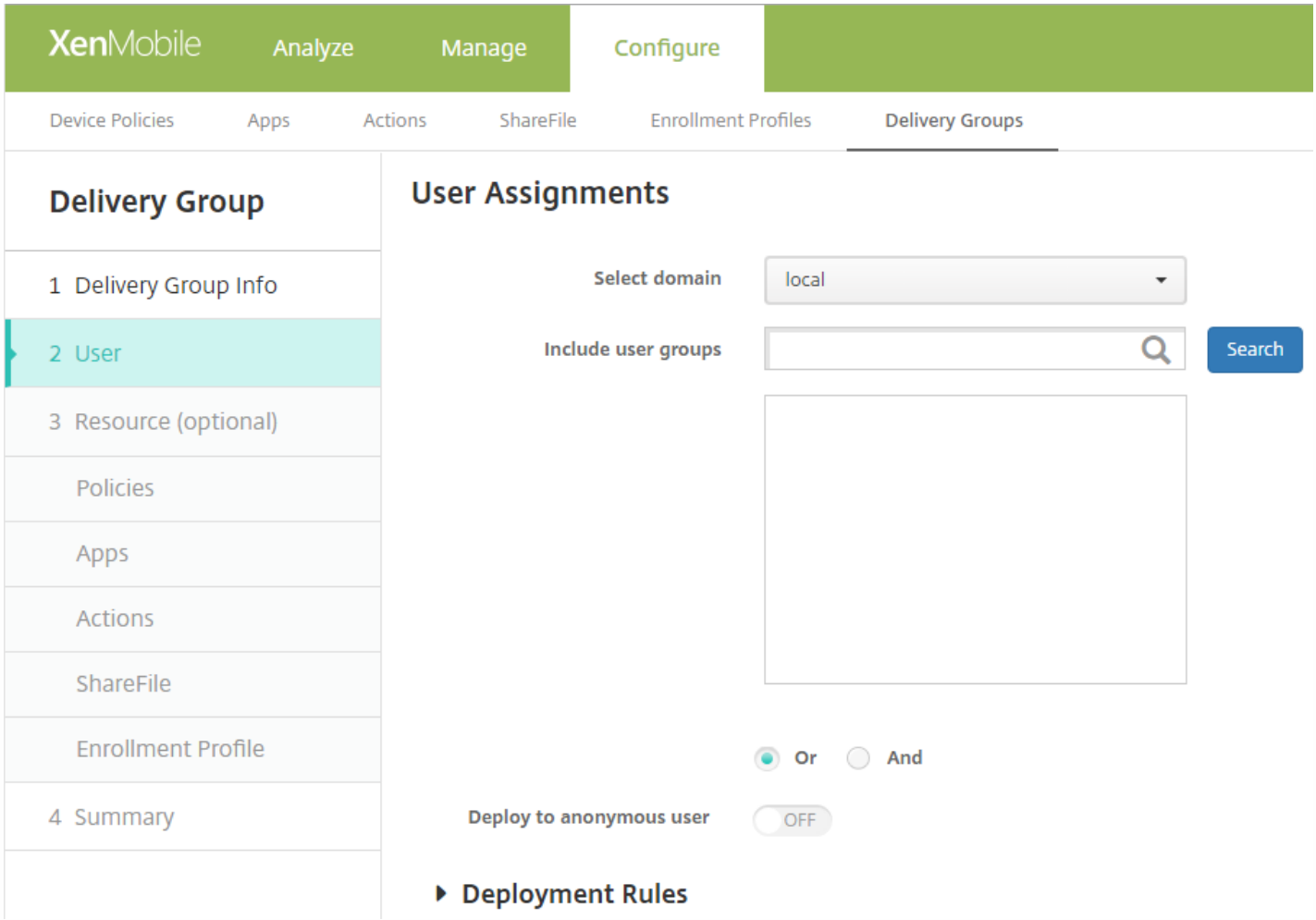
2. En la página **Delivery Groups**, haga clic en **Add**. Aparecerá la página **Delivery Group Information**.



3. En la página **Delivery Group Information**, introduzca la información siguiente:

- **Name**. Indique un nombre descriptivo para el grupo de entrega.
- **Description**. Escriba una descripción opcional del grupo de entrega.

4. Haga clic en **Next**. Aparecerá la página **User Assignments**.



5. Configure estos 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 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 que existen en el 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** situada junto a cada uno de los grupos que quiera quitar.
      - Haga clic en **Search** para ver una lista de todos los grupos de usuarios del dominio seleccionado. Desplácese por la lista y desmarque la casilla de cada grupo 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 en sus dispositivos.
- **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

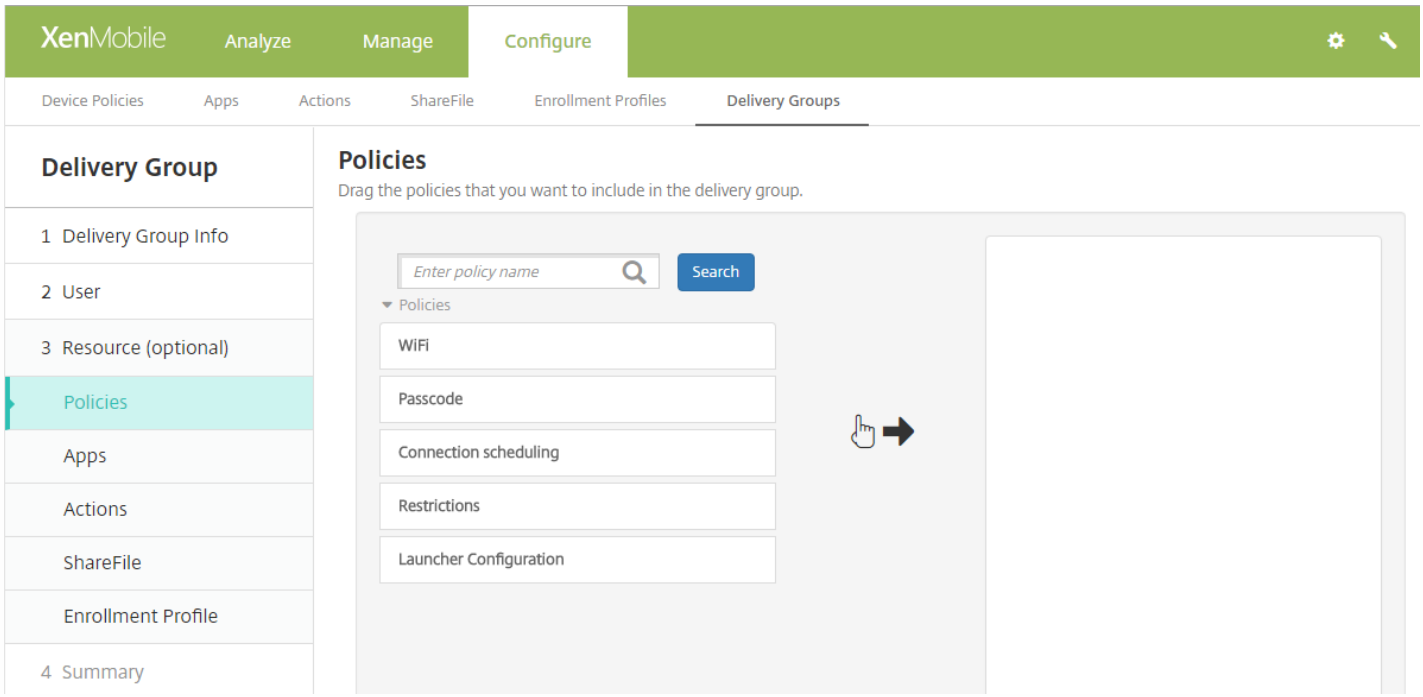
permitido conectarse a XenMobile de todas formas.

6. Configure las reglas de implementación.

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 la incorporación de un recurso, haga clic en **Summary**.

Incorporación de directivas



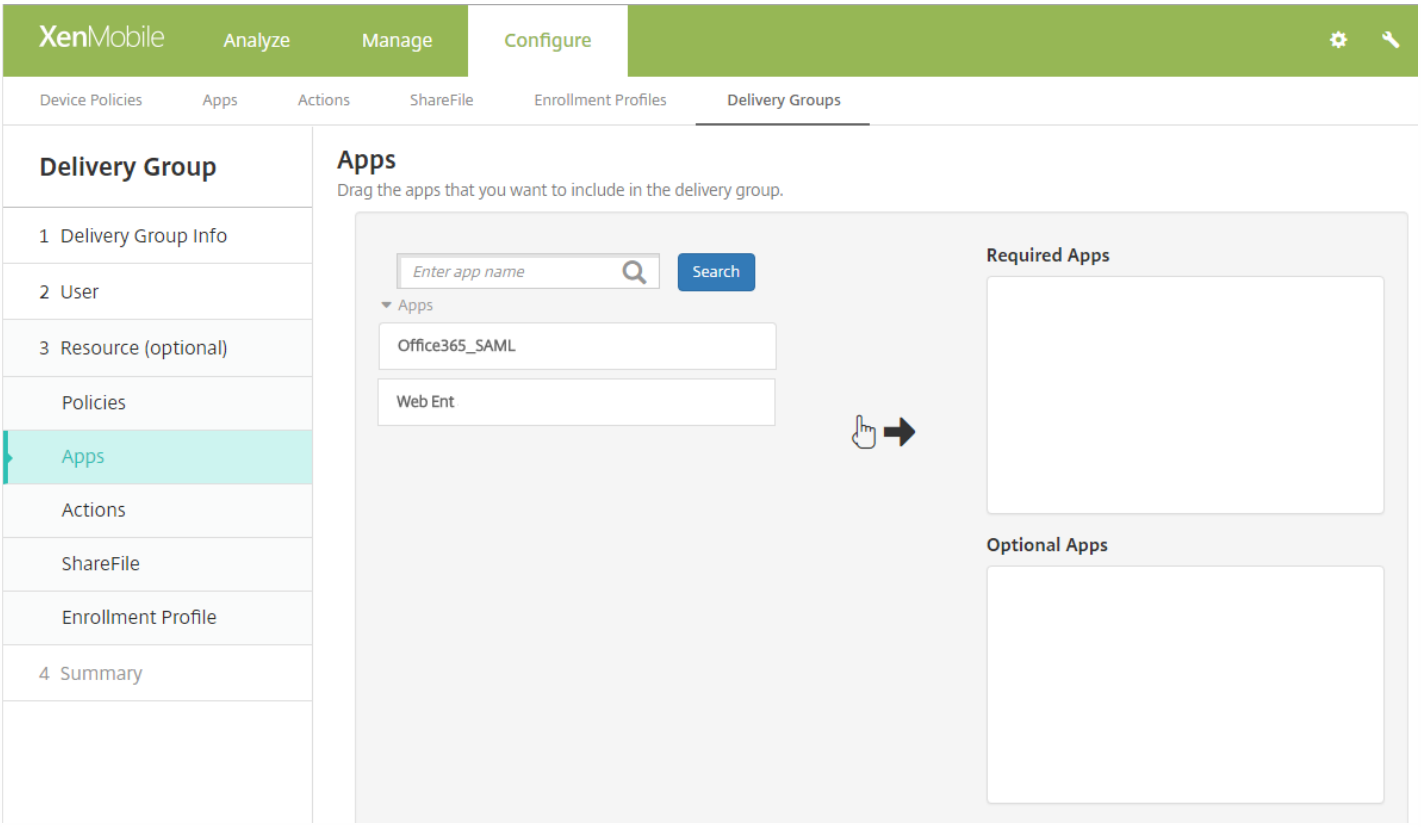
1. Para cada directiva que quiera agregar, lleve a cabo lo siguiente:

- 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 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**.

Cómo agregar aplicaciones



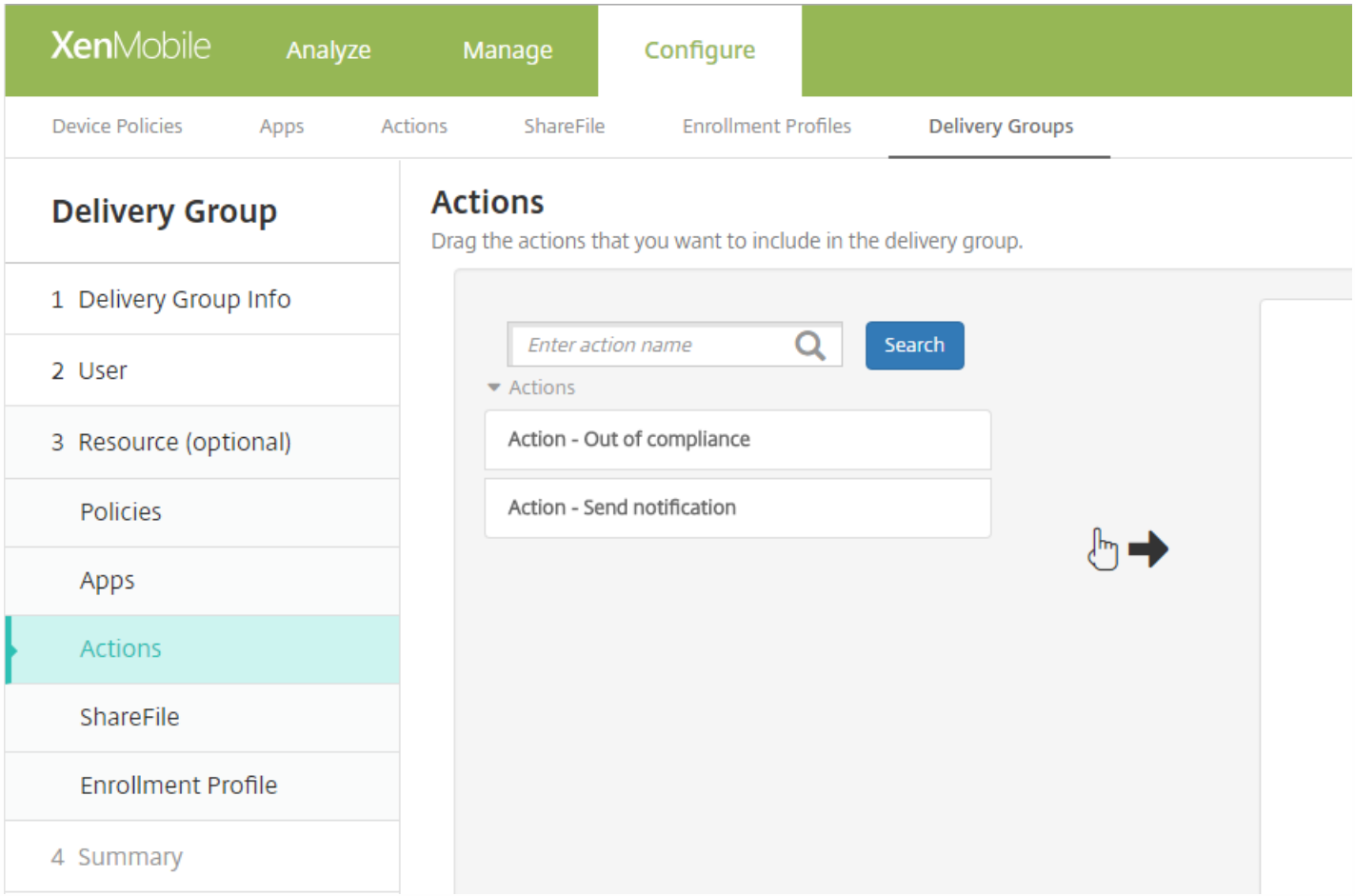
1. Para cada aplicación que quiera agregar, lleve a cabo lo siguiente:

- 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 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**.

Cómo agregar acciones



1. Para cada acción que quiera agregar, lleve a cabo 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 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.

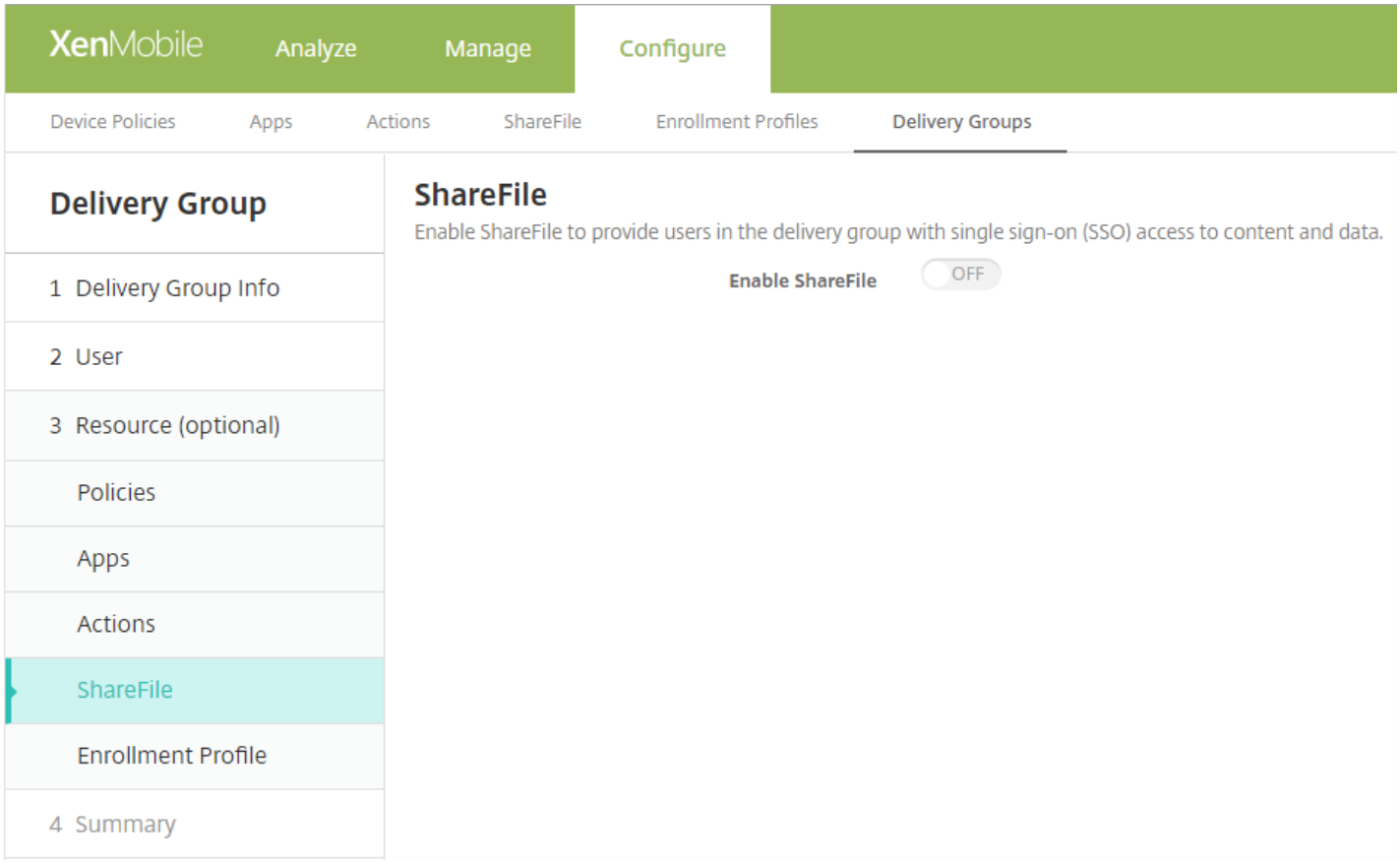
Nota: Para quitar una acción, haga clic en la **X** situada junto al nombre de esa acción en el cuadro de la derecha.

2. Haga clic en **Next**. Aparecerá la página **ShareFile**.

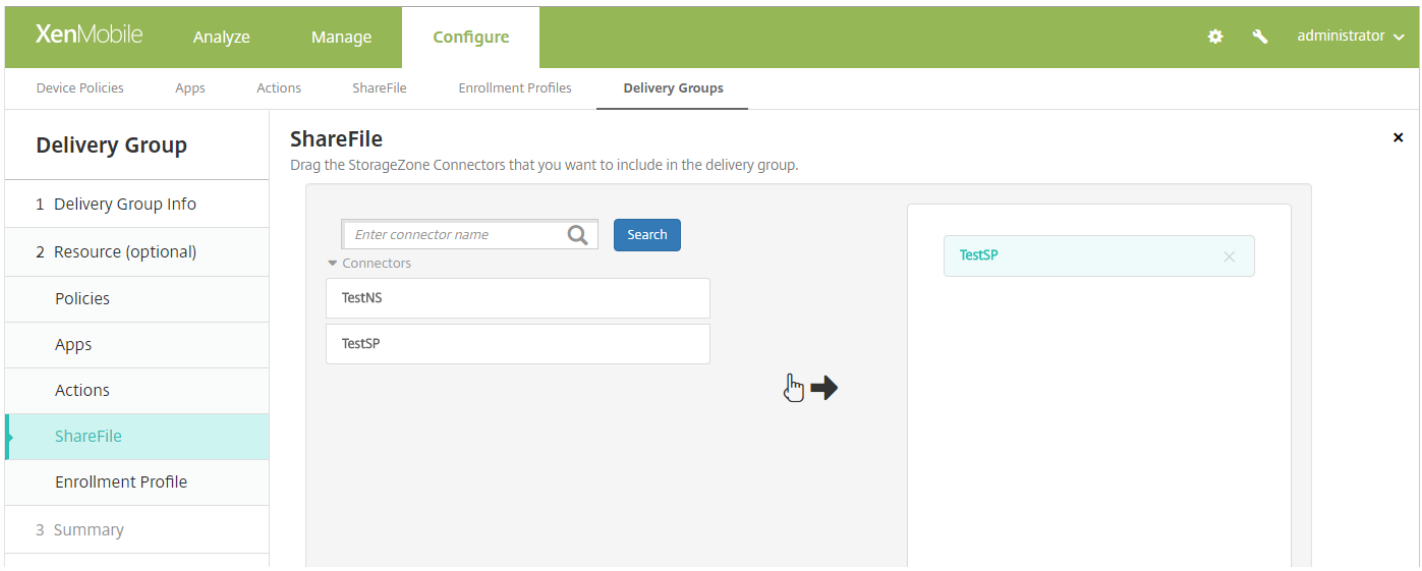
Cómo aplicar la configuración de ShareFile

La página ShareFile varía según si XenMobile (**Configure > ShareFile**) se ha configurado para ShareFile Enterprise o StorageZone Connectors.

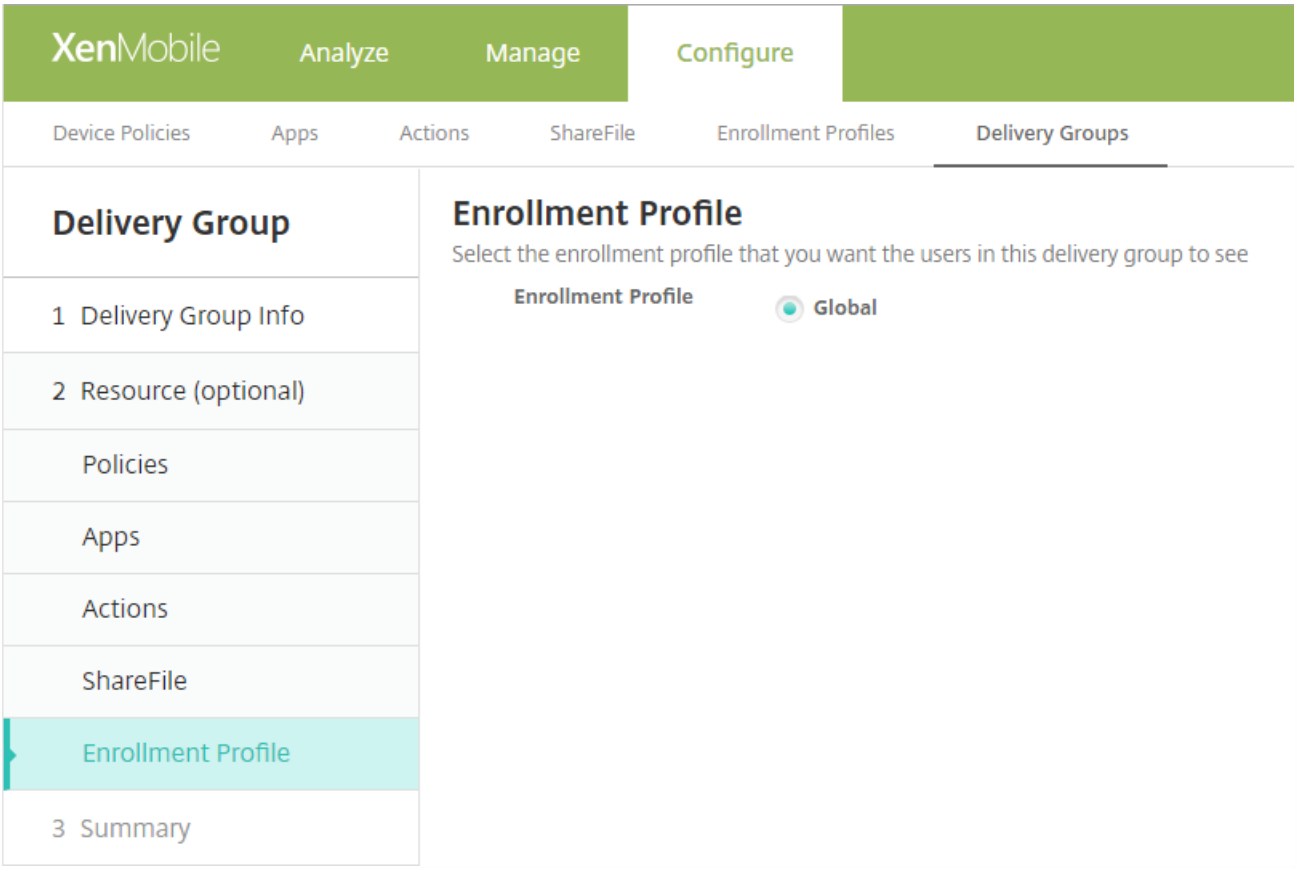
Si ha configurado ShareFile Enterprise para usarlo con XenMobile, establezca **Enable ShareFile** en **ON** para conceder al grupo de entrega acceso Single Sign-On a datos y al contenido de ShareFile.



En cambio, si ha configurado conectores StorageZone para usarlos con XenMobile, seleccione los conectores StorageZone que se incluirán en el grupo de entrega.



Perfil de inscripción

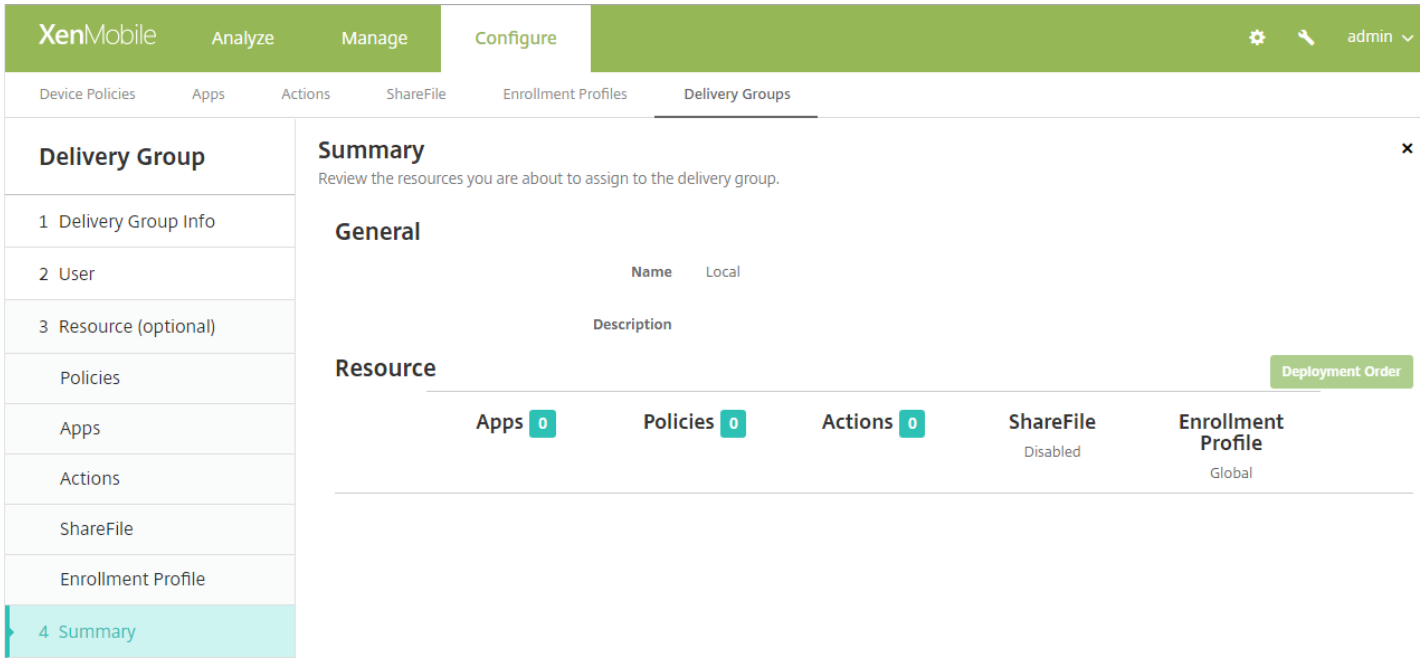


1. Configure este parámetro:

- **Enrollment Profile**. Seleccione un perfil de inscripción. Para crear un perfil de inscripción, consulte Límite de inscripción de dispositivos.

2. Haga clic en **Next**. Aparecerá 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.

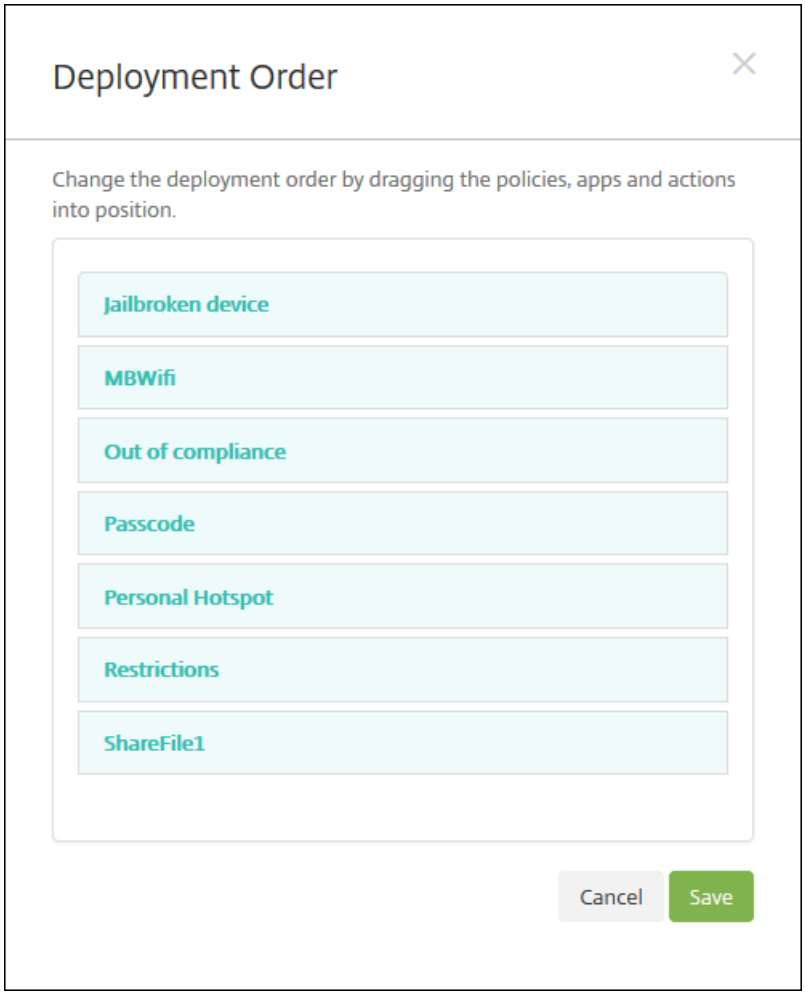
1. Haga clic en **Back** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.

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 desea 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

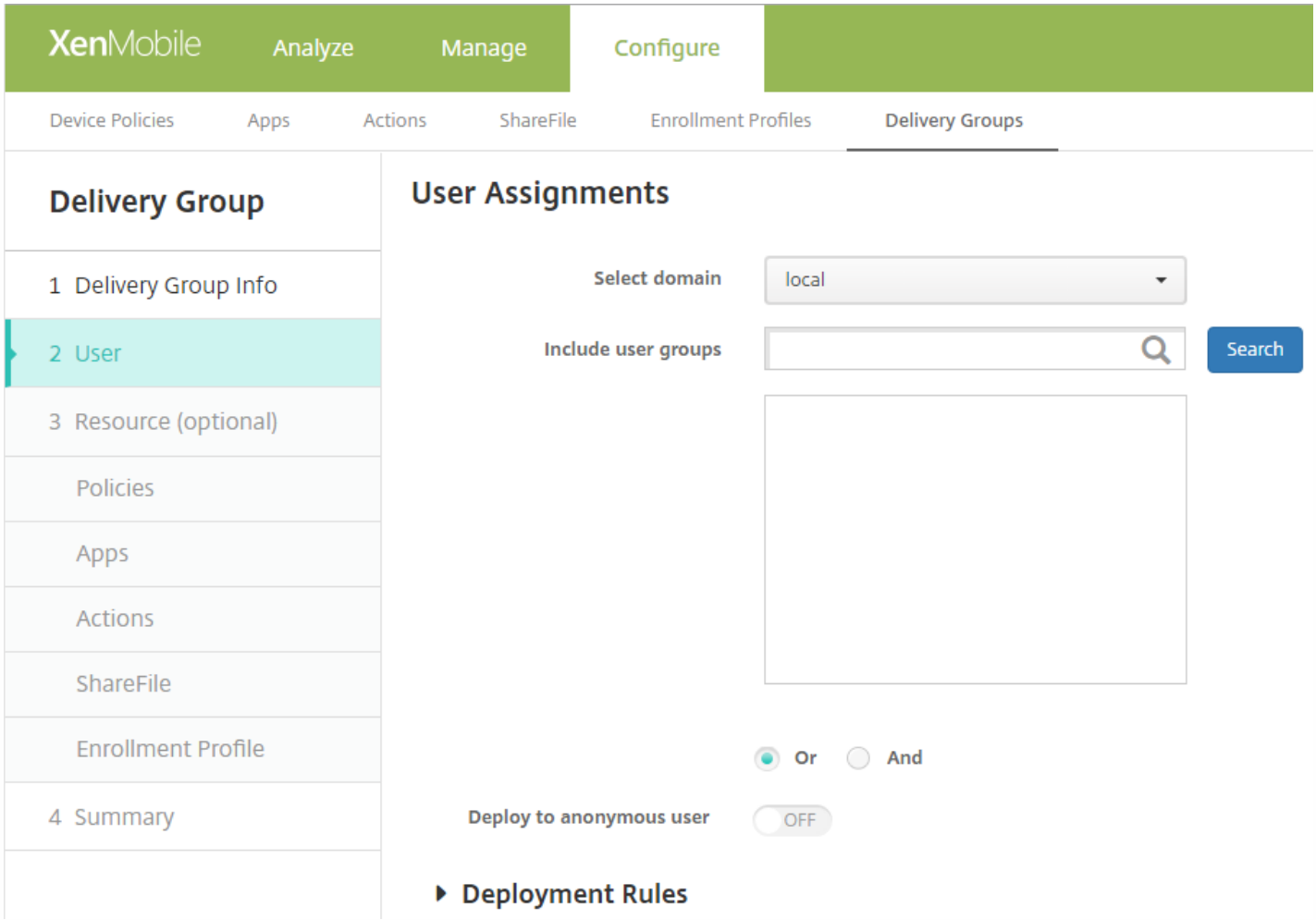
1. En la página **Delivery Groups**, seleccione el grupo de entrega que quiera modificar. Puede seleccionarlo de dos maneras: marcando la casilla de verificación que aparece junto a su nombre o haciendo clic en la línea que contiene su nombre y luego en **Edit**. Aparecerá la página para modificar la información de grupos de entrega **Delivery Group Information**.

> **Nota**
>
> Según cómo haya seleccionado el grupo de entrega, el comando **Edit** aparecerá 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 de entrega 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 que existen en el 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 la implementación.
- **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 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 situada junto al nombre **AllUsers** o haciendo clic en la línea que contiene AllUsers. A continuación, lleve a cabo una de las siguientes acciones:

Nota: Según cómo haya seleccionado el grupo de entrega AllUsers, los comandos **Enable** o **Disable** aparecerán encima o a la derecha del grupo de entrega AllUsers.

- Haga clic en **Disable** para inhabilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está habilitado (valor predeterminado). Una vez inhabilitado, aparecerá bajo el encabezado **Disabled** en la tabla del grupo de entrega.
- Haga clic en **Enable** para habilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está inhabilitado. Una vez habilitado, desaparecerá del encabezado **Disabled** de la tabla del grupo de entrega.

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 la instancia de XenMobile Store presente en los dispositivos Android de los usuarios, primero debe implementar una directiva de inventario de aplicaciones en los dispositivos de los usuarios.

1. En la página **Delivery Groups**, lleve a cabo 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.

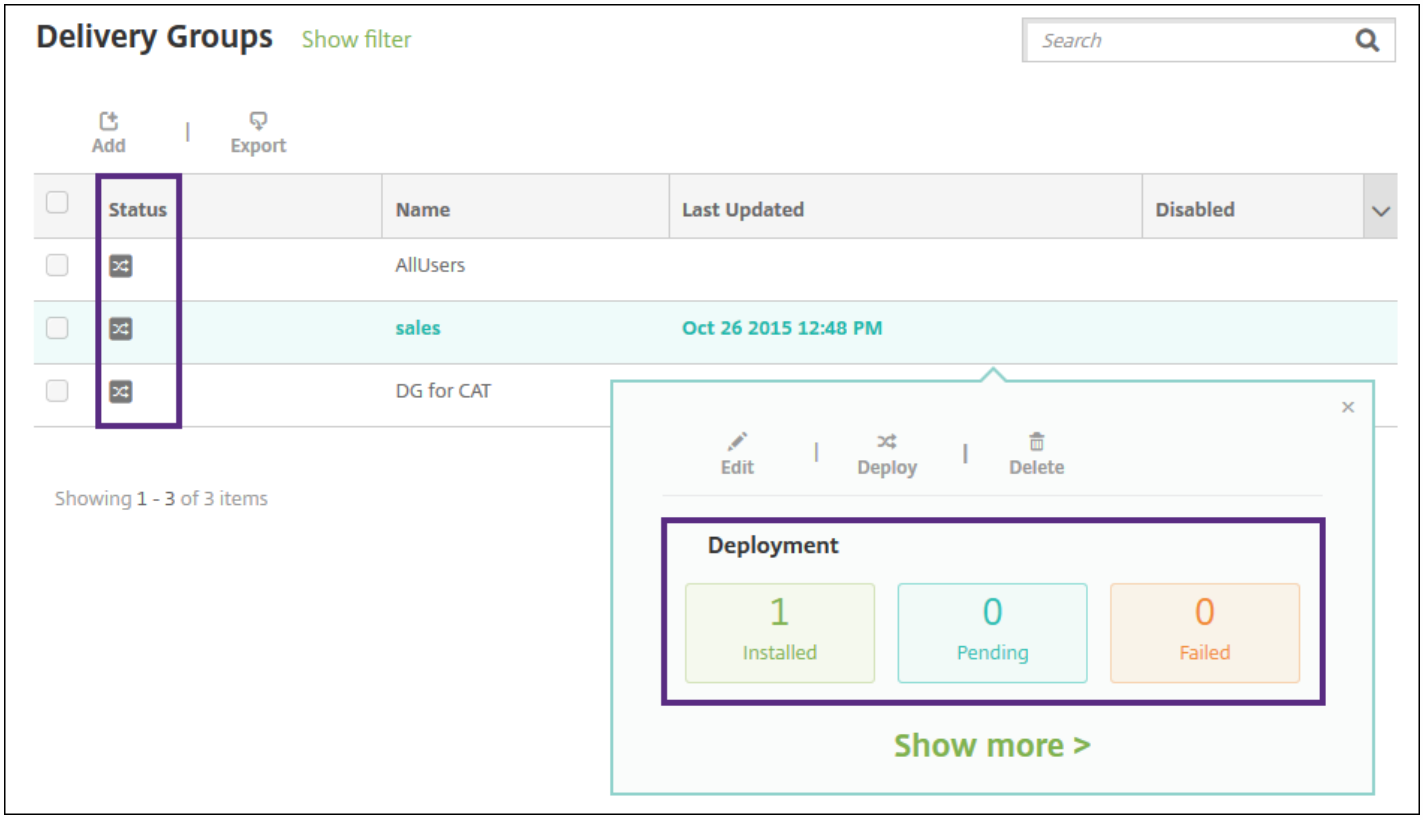
2. Haga clic en **Deploy**.

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 se van a implementar aplicaciones, directivas y acciones se encuentran en la lista y, a continuación, haga clic en **Deploy**. Las aplicaciones, las directivas y las acciones se implementan en los grupos seleccionados en función de la plataforma de los dispositivos y de la directiva de programación.

Puede consultar el estado de la implementación en la página **Delivery Groups** de una de las siguientes maneras:

- Mire el icono de implementación, en el encabezado **Status** del grupo de entrega, que indica si ha habido algún error en la implementación.
- Haga clic en la línea que contiene el grupo de entrega para ver una etiqueta superpuesta donde se indica si la implementación se ha instalado (**Installed**), está pendiente (**Pending**) o ha fallado (**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**, lleve a cabo 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 sobre 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.

Macros

Feb 27, 2017

XenMobile pone a su disposición potentes macros para rellenar datos de propiedad de usuario o de dispositivo en los campos de texto de un perfil, una directiva, una notificación o una plantilla de inscripción (para algunas acciones), entre otros usos. Con las macros, puede configurar una sola directiva, para implementarla a un usuario básico, además de definir que aparezcan valores específicos por usuario para cada usuario de destino. Por ejemplo, puede rellenar de antemano el valor del buzón de correo relativo a un solo usuario en un perfil de Exchange entre miles de usuarios.

Por el momento, esta función solo está disponible en el contexto de configuraciones y plantillas para dispositivos iOS y Android.

Definición de macros de usuario

Las siguientes macros de usuario siempre están disponibles:

- loginname (nombre de usuario y nombre de dominio)
- username (loginname menos el dominio, si existe alguno)
- domainname (nombre de dominio o el dominio predeterminado)

Las siguientes propiedades definidas por el administrador pueden estar disponibles:

- c
- cn
- company
- companyname
- department
- description
- nombre simplificado
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename

- postalcode
- postofficebox
- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (reemplaza la propiedad descrita anteriormente)

Además, si el usuario está autenticado mediante un servidor de autenticación (como LDAP), están disponibles todas las propiedades asociadas al usuario en esa tienda.

Sintaxis de macros

Una macro puede presentar el siguiente formato:

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

Como regla general, todos los elementos de sintaxis posteriores al signo de dólar ($), deben estar entre llaves ({ }).

- Los nombres de propiedad calificados hacen referencia ya sea a una propiedad de usuario, una propiedad de dispositivo o a una propiedad personalizada.
- Los nombres de propiedad calificados se componen de un prefijo, seguido del nombre en sí de la propiedad.
- Las propiedades de usuario presentan el formato ${user.[PROPERTYNAME] (prefix="user.")}.
- Las propiedades de dispositivo presentan el formato ${device.[PROPERTYNAME] (prefix="device.")}.

Por ejemplo, ${user.username} rellena el valor de nombre de usuario en el campo de texto de una directiva. Esto es útil para configurar perfiles de Exchange ActiveSync y otros perfiles utilizados por varios usuarios.

Para macros personalizadas (propiedades que usted define), el prefijo es ${custom}. Puede omitir el prefijo.

Nota: Los nombres de propiedad distinguen mayúsculas de minúsculas.

Acciones automatizadas

Feb 27, 2017

En XenMobile, puede crear acciones automatizadas para programar una respuesta ante determinados eventos, ante propiedades de dispositivo o de usuario, o bien ante la existencia de ciertas aplicaciones en los dispositivos de usuario. Cuando se crea una acción automatizada, se establece el efecto en el dispositivo del usuario cuando este se conecta a XenMobile. Este efecto se establece según los desencadenadores de la acción. Cuando un evento tiene lugar, usted puede enviar una notificación al usuario para corregir el problema antes de tomar medidas más terminantes.

Por ejemplo: si quiere detectar una aplicación que ya haya bloqueado (por ejemplo, Words with Friends), puede especificar un desencadenador que establezca un dispositivo de usuario como dispositivo que no cumple los requisitos cuando se detecte Words with Friends en él. La acción notifica a dicho usuario de que debe quitar la aplicación para que su dispositivo vuelva a cumplirlos. Puede establecer un límite de tiempo de espera antes del cual el usuario debe cumplir los requisitos antes de tomar medidas más terminantes, como borrar el dispositivo de forma selectiva.

En los casos en que el dispositivo de un usuario no cumpla los requisitos establecidos y el usuario arregle el dispositivo para que cumpla los requisitos, deberá configurar una directiva para implementar un paquete que restablezca el dispositivo a un estado de cumplimiento.

Los efectos automáticos que establezca varían entre:

- Borrar totalmente o de forma selectiva el dispositivo.
- Establecer el dispositivo como dispositivo que no cumple los requisitos.
- Revocar el dispositivo.
- Enviar una notificación al usuario para corregir el problema antes de tomar medidas más terminantes.

En este artículo, se explica cómo agregar, modificar y filtrar las acciones automatizadas en XenMobile, así como la forma de configurar las acciones de bloqueo y borrado de aplicaciones para el modo solo MAM.

> ## Nota
>
> Para notificar a los usuarios, primero debe configurar los servidores de notificaciones en Settings para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes (consulte Notificaciones en XenMobile Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificación, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.

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

2. En la página **Actions**, lleve a cabo una de estas acciones:

- Haga clic en **Add** para agregar una nueva acción.
- Seleccione una acción existente para modificarla o eliminarla. Haga clic en la opción pertinente.

Nota: Si marca la casilla situada junto a una acción, el menú de opciones aparecerá encima de la lista de acciones. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.

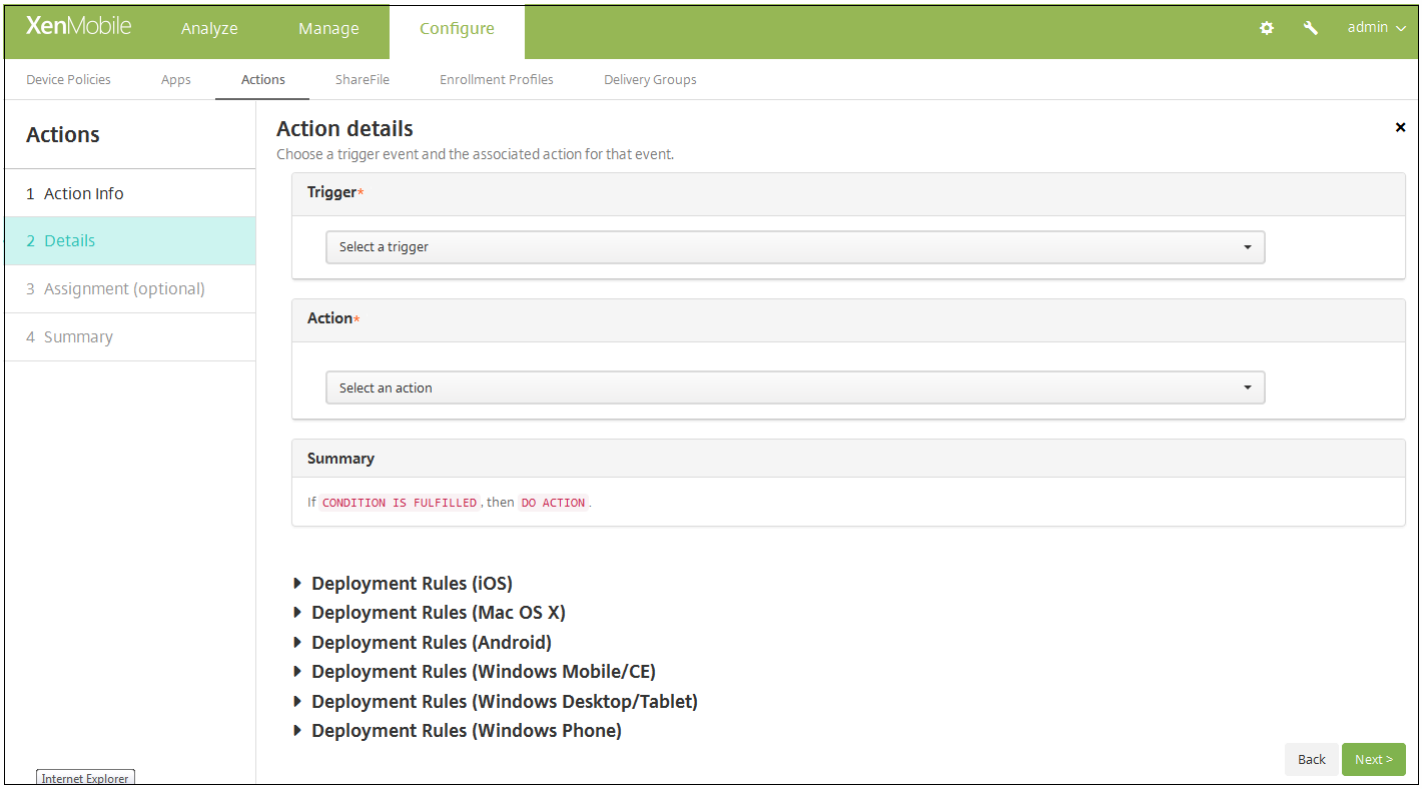
3. Aparecerá la página **Action Information**.

4. En la página **Action Information**, escriba o modifique la información siguiente:

- **Name**. Escriba un nombre para identificar de forma exclusiva la acción. Este campo es obligatorio.
- **Description**. Describa en qué consiste la acción.

5. Haga clic en **Next**. Aparecerá la página **Action details**.

Nota: En el siguiente ejemplo se muestra cómo configurar un desencadenador de **eventos**. Si selecciona otro activador, las opciones resultantes serán distintas a las mostradas aquí.



6. En la página **Action details**, escriba o modifique la información siguiente:

- En la lista **Trigger**, haga clic en el tipo de desencadenador de eventos para esta acción. El significado de cada desencadenador es el siguiente:
  - **Event**. Reacciona ante un evento predefinido.
  - **Device property**. Comprueba un atributo de dispositivo en el dispositivo recopilado en el modo de administración de dispositivos móviles y reacciona ante él.
  - **User property**. Reacciona ante un atributo de usuario, generalmente de Active Directory.
  - **Installed app name**. Reacciona ante una aplicación instalada. No se aplica al modo solo MAM. Requiere que la directiva de inventario de aplicaciones esté habilitada en el dispositivo. De forma predeterminada, la directiva de inventario de aplicaciones está habilitada en todas las plataformas. Para obtener más información, consulte Para agregar una directiva de inventario de aplicaciones.

7. En la siguiente lista, haga clic en la respuesta del desencadenador.

8. En la lista **Action**, haga clic en la acción que se debe realizar cuando se cumplan los criterios del desencadenador. A excepción de **Send notification**, puede elegir un intervalo de tiempo en que los usuarios puedan resolver el problema que haya activado el desencadenador. Si el problema no se resuelve en ese período de tiempo, se llevará a cabo la acción

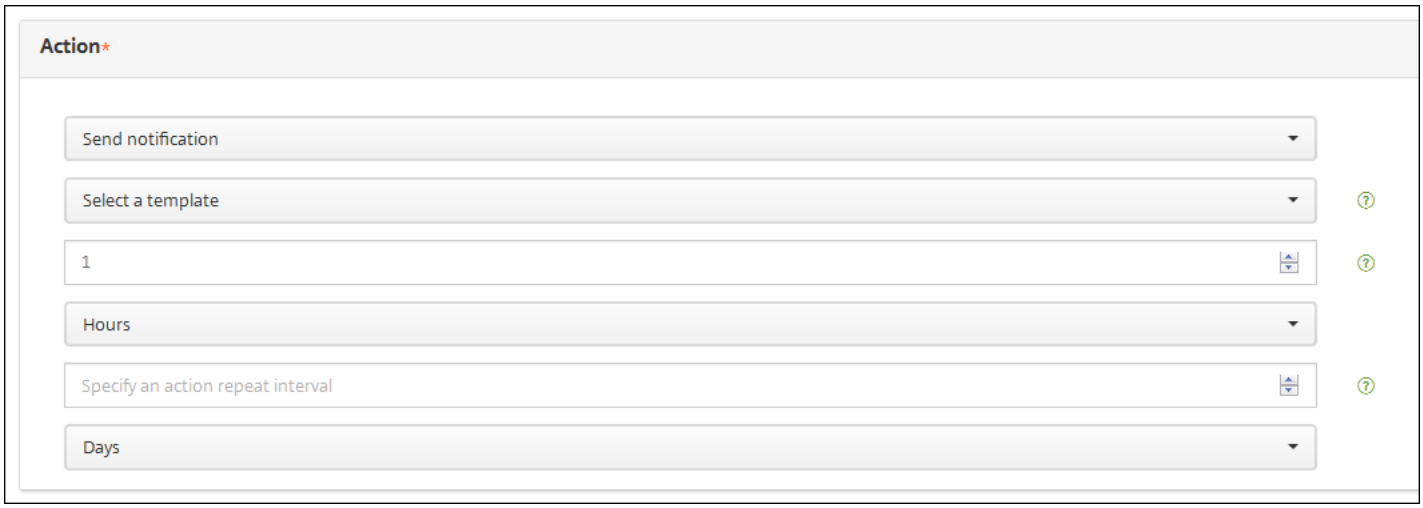
seleccionada. Las acciones disponibles son las siguientes:

- **Selectively wipe the device**. Borra todas las aplicaciones y datos empresariales de un dispositivo, pero no afecta a las aplicaciones y datos personales.
- **Completely wipe the device**. Borra todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria (si el dispositivo las tuviera).
- **Revoke the device**. Prohíbe a un dispositivo que se conecte a XenMobile.
- **App lock**. Deniega el acceso a todas las aplicaciones de un dispositivo. En Android, los usuarios no podrán iniciar sesión en XenMobile. En iOS, los usuarios sí podrán iniciar sesión, pero no podrán acceder a aplicaciones. Para obtener más información, consulte "Acciones de bloqueo y borrado de aplicaciones en el modo de solo MAM" más adelante en este artículo.
- **App wipe**. En Android, elimina la cuenta de XenMobile del usuario. En iOS, esto elimina la clave de cifrado que los usuarios necesitan para acceder a las características de XenMobile. Para obtener más información, consulte "Acciones de bloqueo y borrado de aplicaciones en el modo de solo MAM" más adelante en este artículo.
- **Mark the device as out of compliance**. Establece el dispositivo en estado de no cumplimiento.
- **Send notification**. Envía un mensaje al usuario.

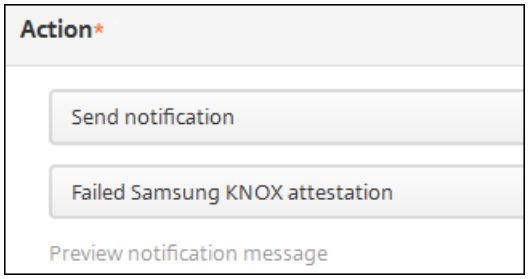
Si elige **Send notification**, el resto de este procedimiento explica cómo enviar una acción de notificación.

9 En la siguiente lista, seleccione la plantilla a utilizar para la notificación. Aparecerán las plantillas de notificaciones correspondientes al evento seleccionado, a menos que no haya ninguna plantilla para ese tipo de notificación. En ese caso, se le solicitará que configure una plantilla con el mensaje: No hay ninguna plantilla para este tipo de evento. Cree una plantilla desde la sección **Notification Template** de **Settings**.

Nota: Para notificar a los usuarios, primero debe configurar los servidores de notificaciones en Settings para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes (consulte Notificaciones en XenMobile Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificación, consulte Para crear o actualizar plantillas de notificaciones en XenMobile.



Nota: Después de seleccionar la plantilla, puede obtener una vista previa de la notificación cuando hace clic en **Preview notification message**.



10. En los siguientes campos, establezca el tiempo que debe transcurrir en días, horas y minutos antes de tomar medidas, así como el intervalo en el que la acción se repite hasta que el usuario resuelva la situación.

11. En **Summary**, verifique que la acción automatizada que ha creado es la acción esperada.

12. Después de configurar los datos de la acción, puede configurar las reglas de implementación para cada plataforma individualmente. Para ello, siga el paso 13 para cada plataforma seleccionada.

13. Configure las reglas de implementación.

14. Tras configurar las reglas de implementación de las plataformas para la acción, haga clic en **Next**. Aparecerá de asignación de acciones **Actions assignment**, en la que puede asignar la acción a un grupo o grupos de entrega. Este paso es opcional.

15 Junto a **Choose delivery groups**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione, de la lista, un grupo o varios 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.

16. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación, o bien, 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 si se configura la clave de implementación en segundo plano para la programación desde **Settings** > **Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

Nota: La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always-on connection**, que no se aplicará para iOS.

17. Haga clic en **Next**. Aparecerá la página **Summary**, donde puede comprobar la configuración de la acción.

18. Haga clic en **Save** para guardar la acción.

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

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.

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 pertinente.

5. En **Action**, seleccione una acción.

Para este paso, no olvide las siguientes condiciones:

Si el tipo de desencadenador es **Event** y el valor no es **Active Directory disabled user**, las acciones **App wipe** y **App lock** no aparecerán.

Si el tipo de desencadenador es **Device property** y el valor es **MDM lost mode enabled**, aparecerán las siguientes acciones:

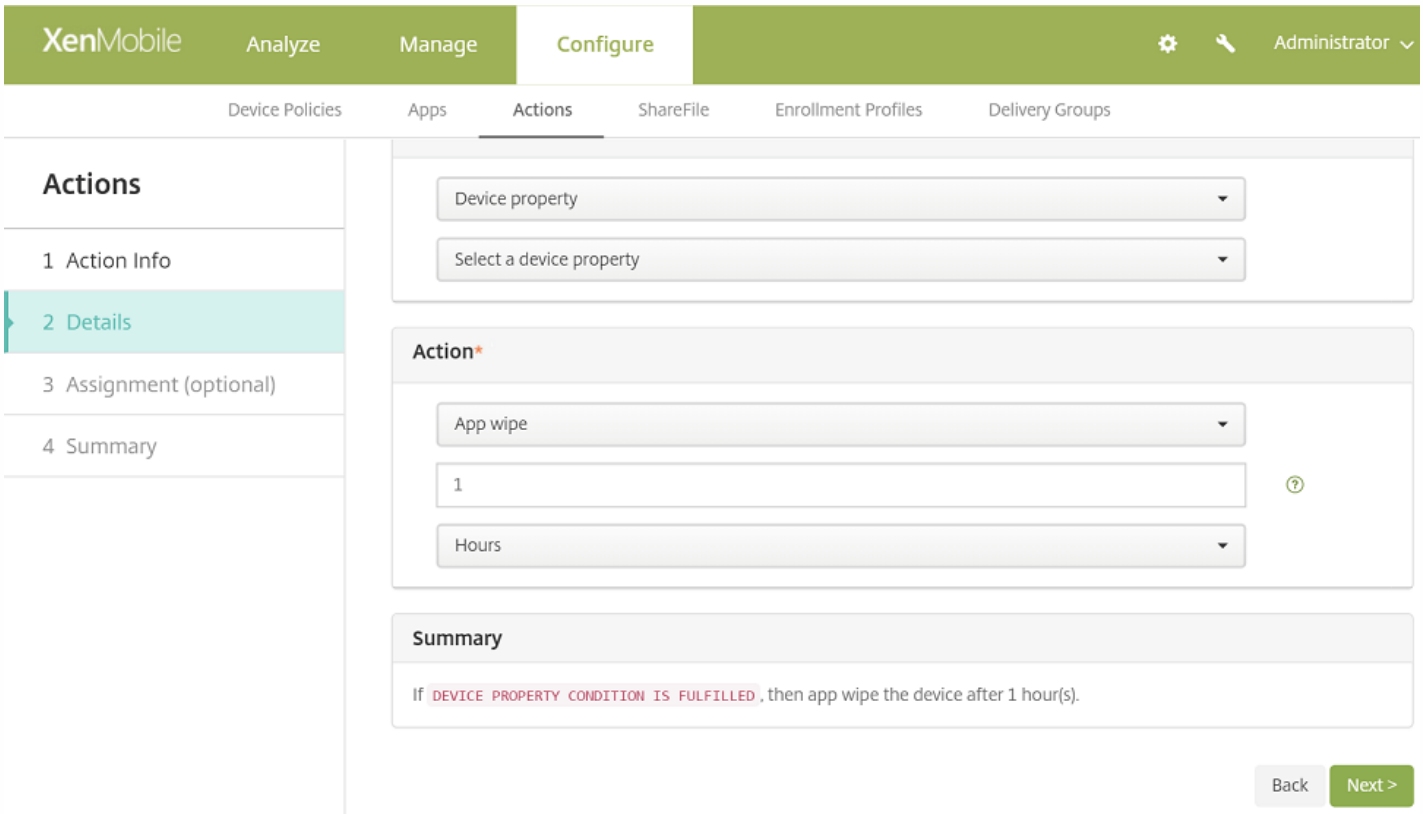
- Borrar datos selectivamente del dispositivo
- Borrar datos completamente del dispositivo
- Revocar el dispositivo

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 Configuración de roles con RBAC.

> **Nota**
>
> Si establece el desencadenador en **Event**, el intervalo de repetición es automáticamente 1 hora como mínimo. Para recibir la notificación en el dispositivo, deben actualizarse las directivas en él, es decir, debe estar sincronizado con el servidor. Por lo general,

un dispositivo se sincroniza con el servidor cuando los usuarios inician sesión o actualizan manualmente sus directivas a través de Secure Hub.

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.



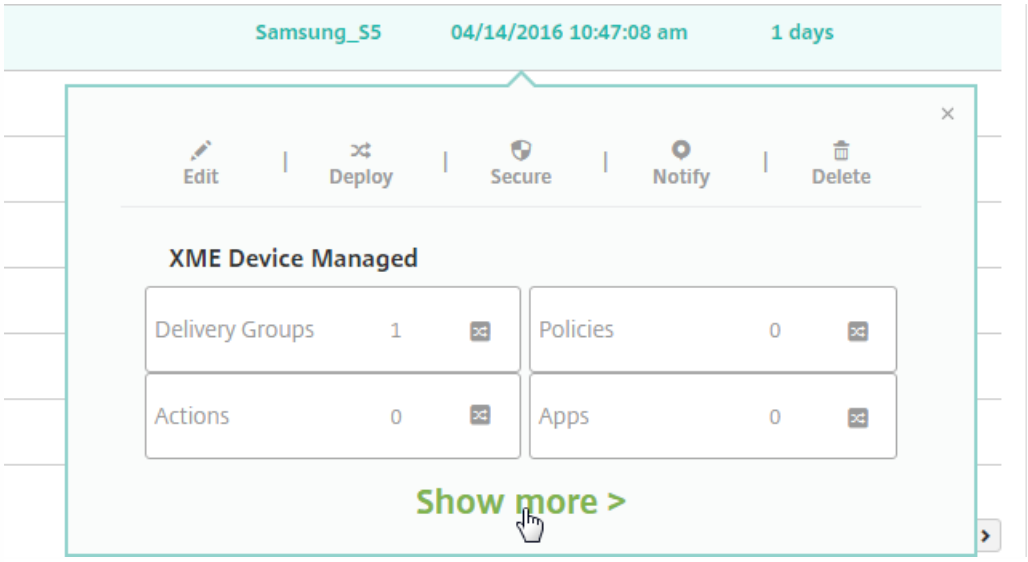
6. Configure las reglas de implementación y, a continuación, haga clic en **Next**.

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

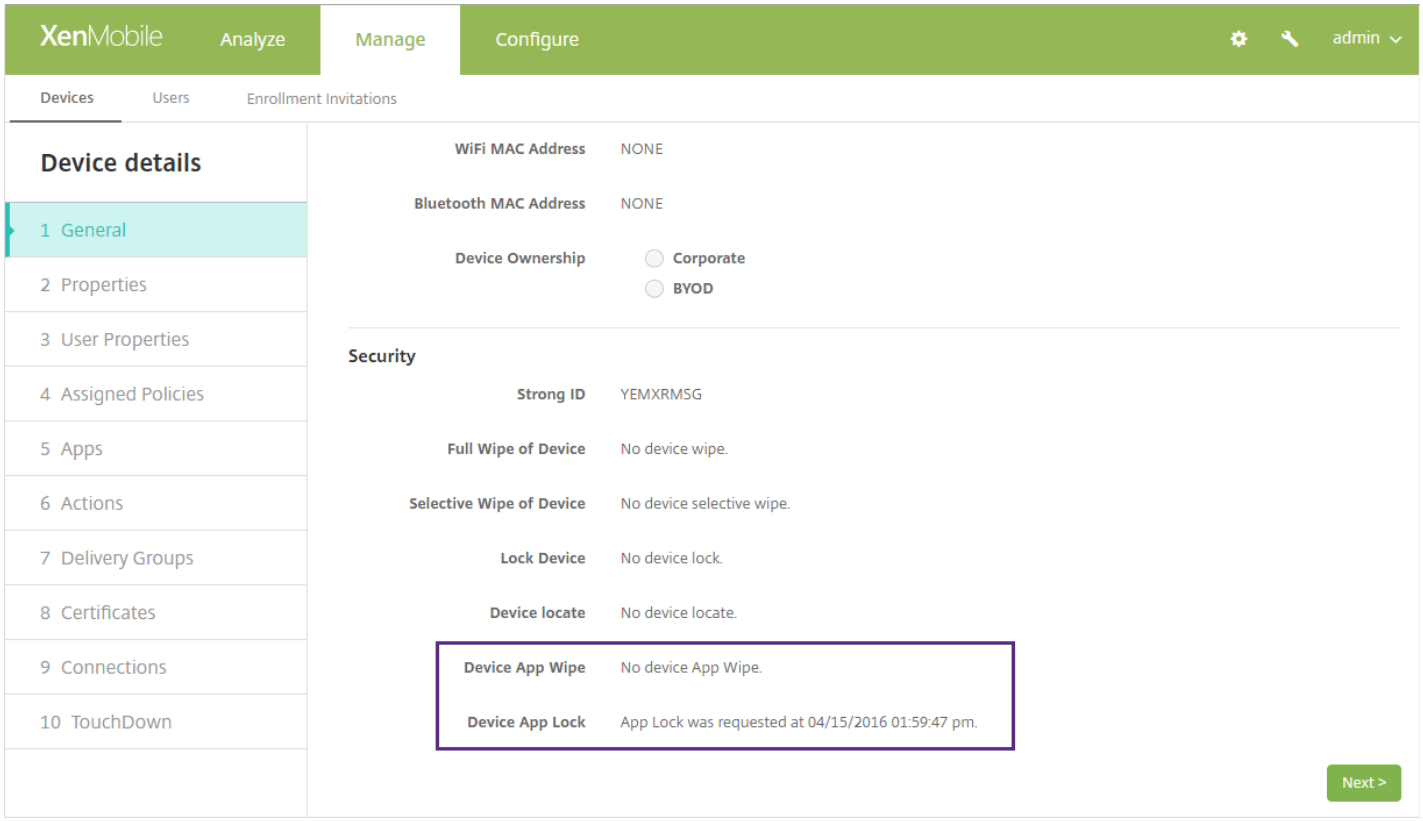
8. Haga clic en **Save**.

Para comprobar el estado del bloqueo o borrado de las aplicaciones

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



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



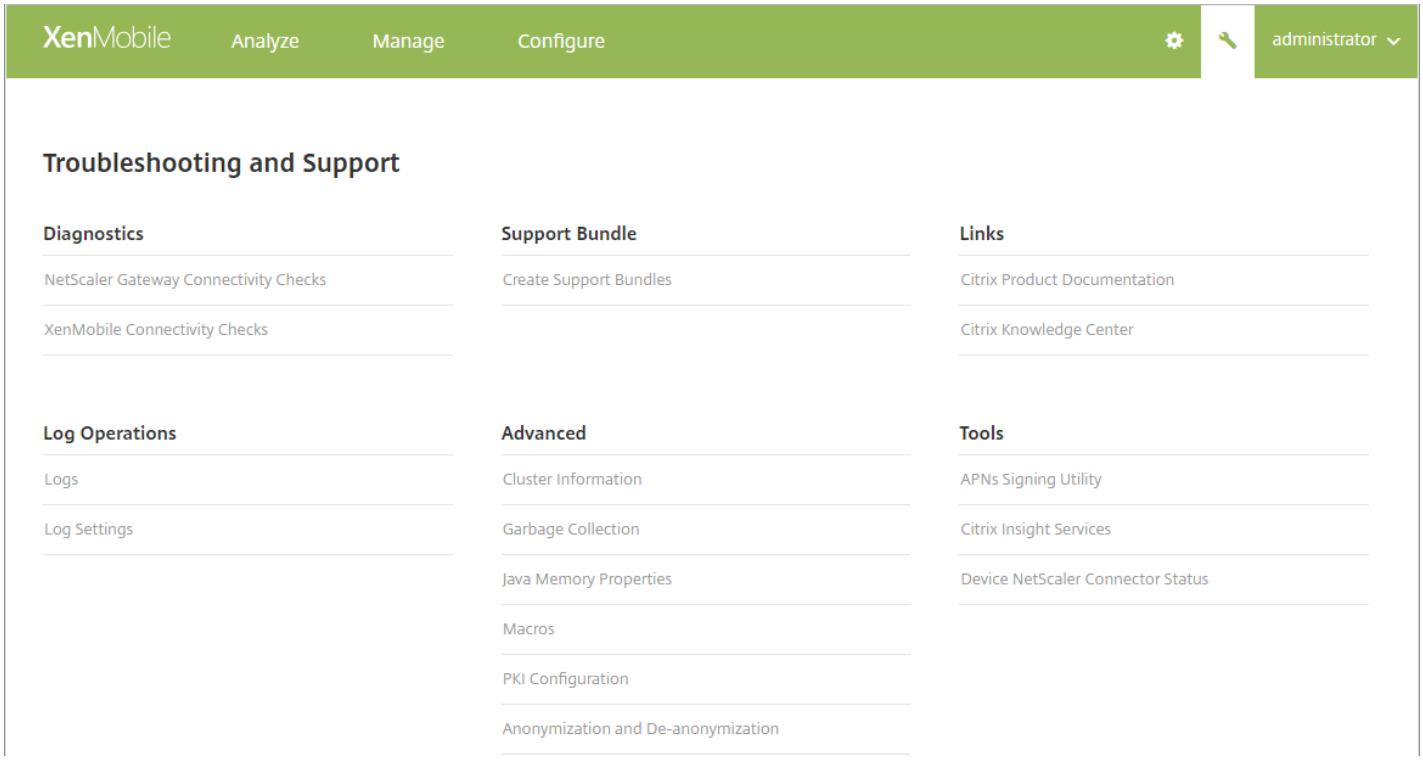
Supervisión y asistencia

May 10, 2017

Puede utilizar el panel de mandos de XenMobile y la página "Support" de XenMobile para supervisar y solucionar los problemas que presente su servidor XenMobile. Use la página "Support" de XenMobile para acceder a un repertorio de datos 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 la consola de XenMobile, haga clic en el icono con forma de llave inglesa, situado en la esquina superior derecha de la consola.

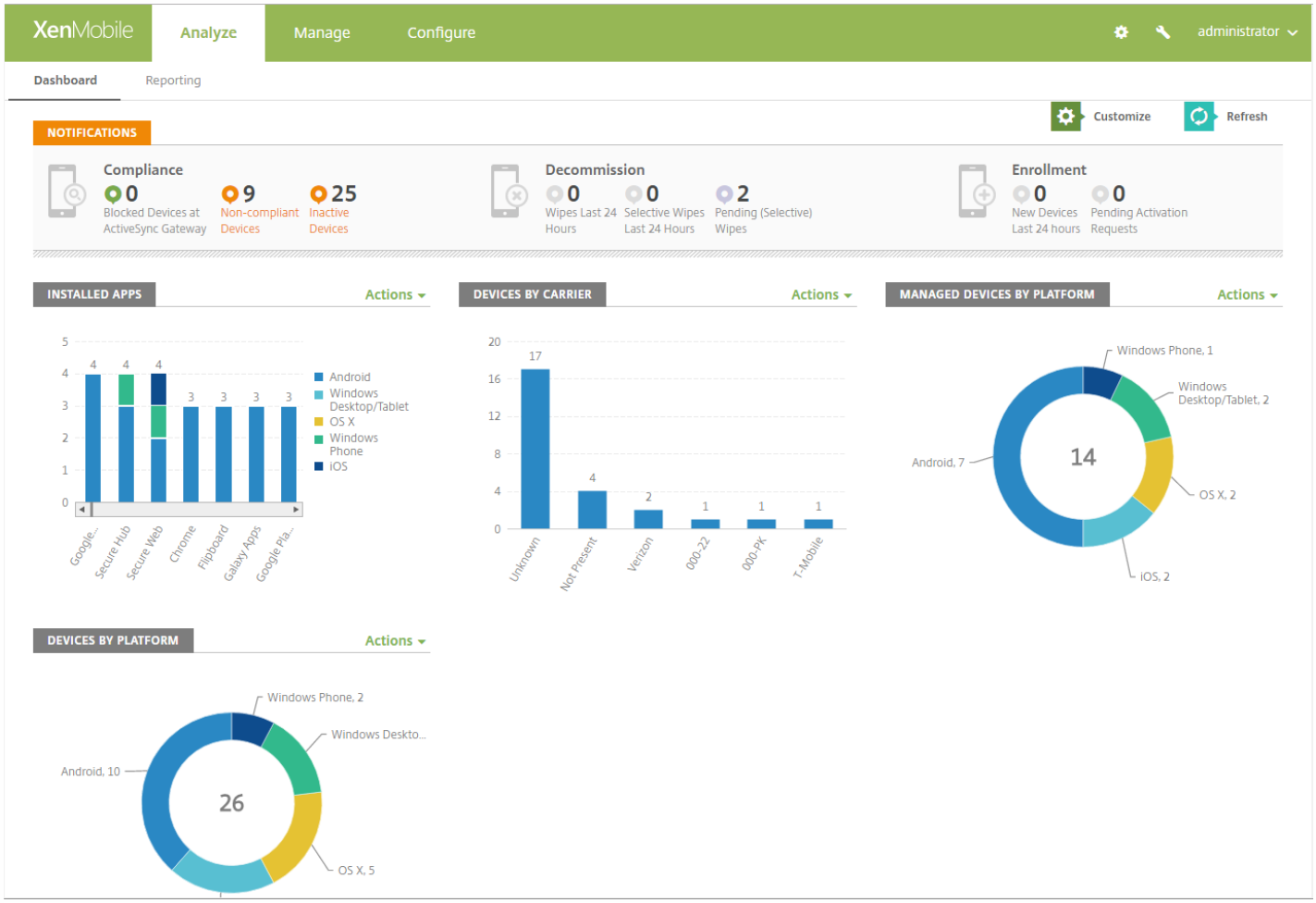
Aparecerá la página Support.



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

Asimismo, puede ver toda la información de un vistazo desde su panel de mandos en la consola de XenMobile. En esta información, puede utilizar widgets para ver rápidamente los problemas y las operaciones correctas que se hayan producido.



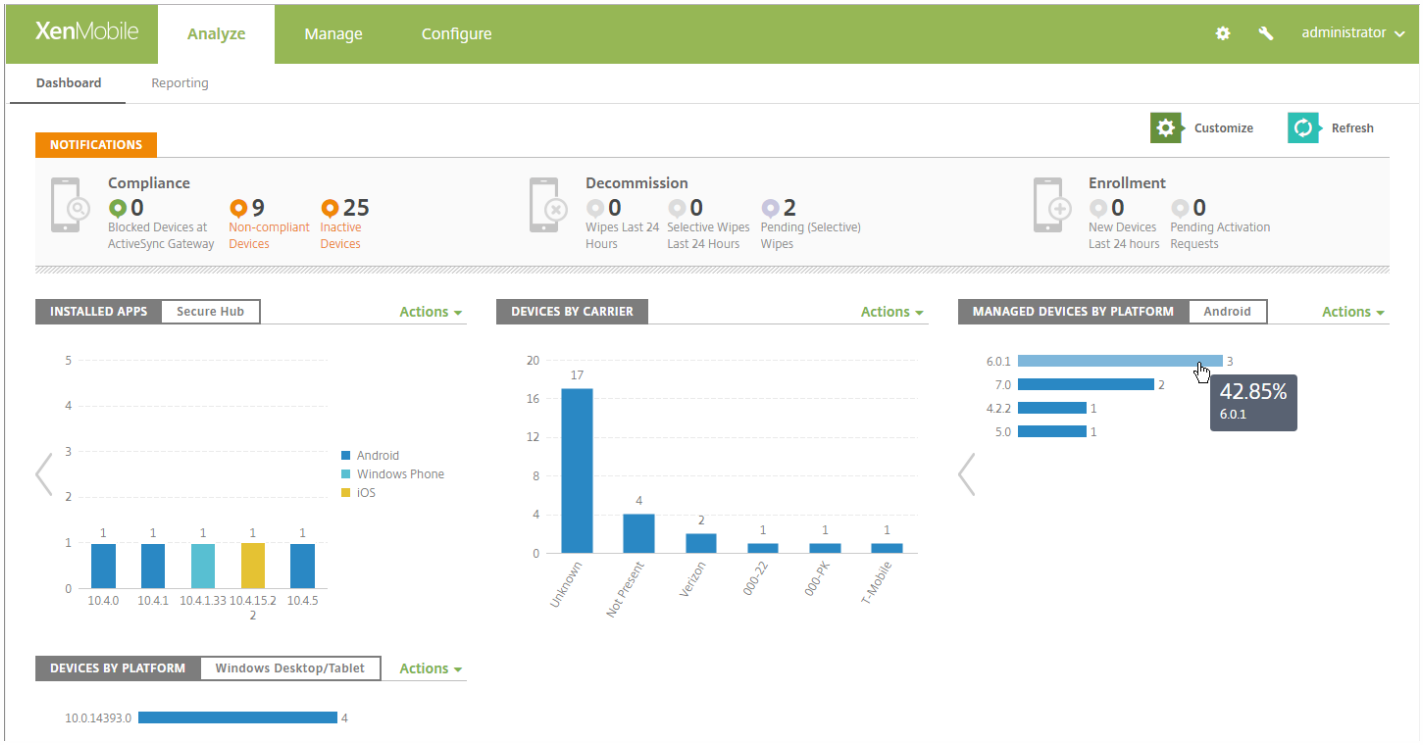
Por regla general, el panel de mandos es la pantalla que aparece al iniciar sesión por primera vez en la consola de XenMobile. Para acceder al panel de mandos desde cualquier otro sitio de la consola, haga clic en **Analyze**. Haga clic en **Customize** en el panel de mandos para modificar el diseño de la página y para modificar los widgets que aparecen.

- **My Dashboards**. Puede guardar hasta cuatro paneles de mandos diferentes. Puede seleccionar cada panel guardado para verlo y modificarlo por separado.
- **Layout Style**. En esta fila, puede seleccionar la cantidad de widgets que aparecerán en el panel de mandos y cómo se etiquetarán.
- **Widget Selection**. Puede elegir qué información se mostrará en el panel de mandos.
  - **Notifications**. Marque la casilla situada encima de los números en la parte izquierda para agregar una barra de notificaciones encima de los widgets. Esta barra muestra la cantidad de dispositivos conformes, dispositivos inactivos, dispositivos borrados o dispositivos inscritos en las últimas 24 horas.
  - **Devices by Platform**. Muestra la cantidad de dispositivos administrados y no administrados por plataforma.
  - **Devices by Carrier**. Muestra la cantidad de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
  - **Managed Devices by Platform**. Muestra la cantidad de dispositivos administrados por plataforma.
  - **Unmanaged Devices by Platform**. Muestra la cantidad de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero se han borrado o se les pueden

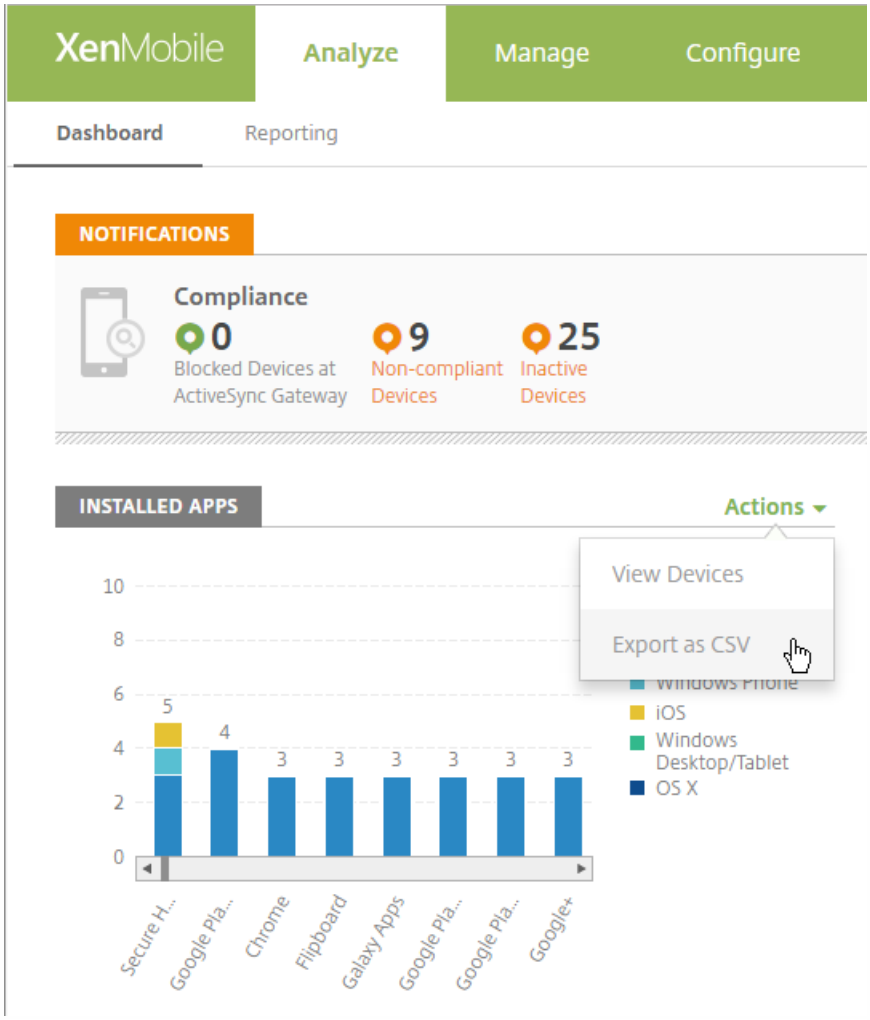
haber revocados los privilegios.

- **Devices By ActiveSync Gateway Status**. Muestra la cantidad de dispositivos agrupados por estado de ActiveSync Gateway. La información se muestra como estado Blocked (Bloqueado), Allowed (Permitido) o Unknown (Desconocido). Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Devices By Ownership**. Muestra la cantidad de dispositivos agrupados por propietario. La información se muestra como propiedad de la empresa, del empleado o propietario desconocido.
- **Android TouchDown License Status**. Muestra la cantidad de dispositivos que tienen una licencia de TouchDown.
- **Failed Delivery Group Deployments**. Muestra la cantidad total de implementaciones fallidas desglosadas por paquete. Solo se muestran los paquetes de implementaciones con errores.
- **Devices By Blocked Reason**. Muestra la cantidad de dispositivos bloqueados por ActiveSync.
- **Installed Apps**. Con este widget, puede escribir el nombre de una aplicación y aparece un gráfico con información sobre esa aplicación.
- **VPP Apps License Usage**. Muestra estadísticas sobre el uso de licencias por parte de las aplicaciones provenientes del Programa de Compras por Volumen (PCV) de Apple.

En cada widget, puede hacer clic en partes individuales para ampliar la información mostrada.



También puede exportar la información como archivo CSV. Para ello, haga clic en la lista desplegable **Action**.



Informes

Feb 27, 2017

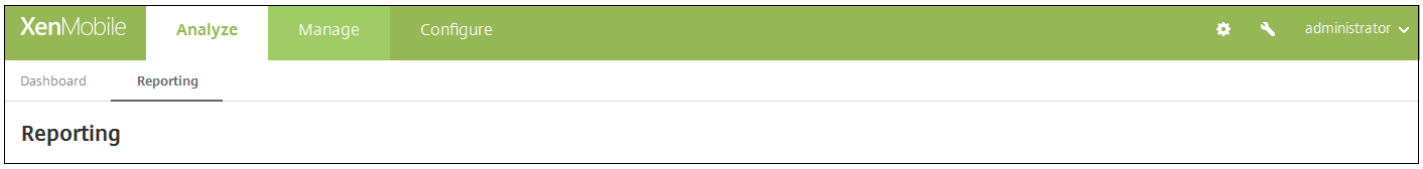
XenMobile ofrece los siguientes informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones:

- **Apps by Devices & User** (Aplicaciones por dispositivo y usuario). Ofrece una lista de las aplicaciones administradas que los usuarios tienen en sus dispositivos. Este informe no incluye las aplicaciones personales instaladas en un dispositivo.
- **Terms & Conditions** (Términos y condiciones). Ofrece una lista de los usuarios que han aceptado o rechazado los contratos de términos y condiciones.
- **Top 25 Apps (25 aplicaciones principales).** Ofrece una lista de un máximo de 25 aplicaciones que tienen la mayoría de los usuarios en sus dispositivos.
- **Jailbroken/Rooted Devices** (Dispositivos liberados por jailbreak o root). Ofrece una lista de los dispositivos iOS liberados por jailbreak y de los dispositivos Android liberados por root.
- **Top 10 Apps - Failed Deployment** (10 aplicaciones principales: implementación fallida). Ofrece una lista de las aplicaciones que no se pudieron implementar.
- **Inactive Devices** (Dispositivos inactivos). Ofrece una lista de los dispositivos que hayan estado inactivos durante un período de tiempo especificado.
- **Apps by Type & Category** (Aplicaciones por tipo y categoría). Ofrece una lista de las aplicaciones según su versión, tipo o categoría.
- **Device Enrollment** (Inscripción de dispositivos). Ofrece una lista de todos los dispositivos inscritos.
- **Apps by Platform** (Aplicaciones por plataforma). Ofrece una lista de las aplicaciones y sus versiones según la plataforma y la versión del dispositivo.
- **Blacklisted Apps by Device & User** (Aplicaciones prohibidas por dispositivo y usuario). Ofrece una lista de las aplicaciones prohibidas (incluidas en la lista negra) que los usuarios tienen en sus dispositivos.
- **Devices & Apps** (Dispositivos y aplicaciones). Ofrece una lista de los dispositivos que ejecutan aplicaciones administradas.

Los informes se presentan en formato CSV, y se pueden abrir con programas como Microsoft Excel.

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**.



Cada tipo de informe contiene una descripción de la información que recopila el informe, así como los datos específicos de informe, como se muestra en el ejemplo siguiente:

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.

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.

En la siguiente imagen, se muestra parte de un informe "Top 25 apps" como aparece en Microsoft Excel:

	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store

Important

Aunque es posible utilizar SQL Server para crear informes personalizados, Citrix no recomienda este método. Usar la base de datos de SQL Server de esta manera puede acarrear consecuencias imprevistas en la implementación de XenMobile. Si decide seguir este método para generar informes, compruebe que las consultas SQL se ejecutan mediante una cuenta de solo lectura.

Proveedor de servicios móviles

Feb 27, 2017

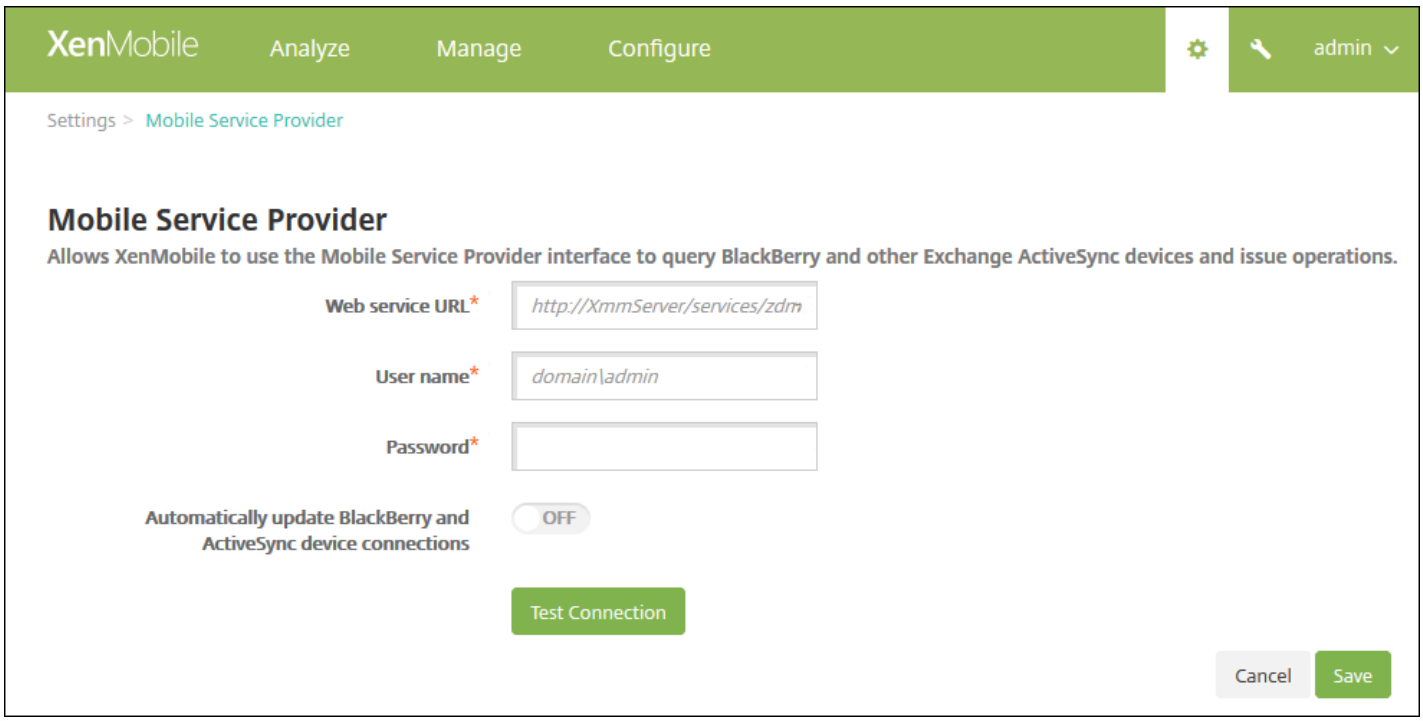
Puede habilitar XenMobile para que utilice la interfaz del proveedor de servicios móviles, para enviar consultas a dispositivos BlackBerry y Exchange ActiveSync y emitir operaciones.

Por ejemplo, suponga que en su organización hay más de mil usuarios y cada usuario usa uno o varios dispositivos distintos. Después de notificar a cada usuario que debe inscribir sus dispositivos en XenMobile para ser administrados, la consola de XenMobile indica la cantidad de dispositivos que inscriben los usuarios. Mediante la configuración de este parámetro, puede determinar la cantidad de dispositivos que se conectan a Exchange Server. De este modo, puede hacer lo siguiente:

- Determinar si los usuarios aún tienen que inscribir sus dispositivos.
- Emitir comandos para los dispositivos de usuario que se conectan a un servidor Exchange Server; por ejemplo, un comando de borrado de datos.

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 **Mobile Service Provider**. Aparece la página **Mobile Service Provider**.



3. Configure estos parámetros:

- **Web service URL**. Escriba la dirección URL del servicio Web. Por ejemplo: http://XmmServer/services/xdmservice.
- **User name**. Escriba el nombre de usuario con el formato dominio\admin.
- **Password**. Escriba la contraseña.
- **Automatically update BlackBerry and ActiveSync device connections**. Seleccione si quiere actualizar automáticamente las conexiones de los dispositivos. El valor predeterminado es **OFF**.
- Haga clic en **Test connection** para comprobar la conexión.

4. Haga clic en **Save**.

SysLog

Apr 13, 2017

Puede configurar XenMobile (solo local) para enviar archivos de registro 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:

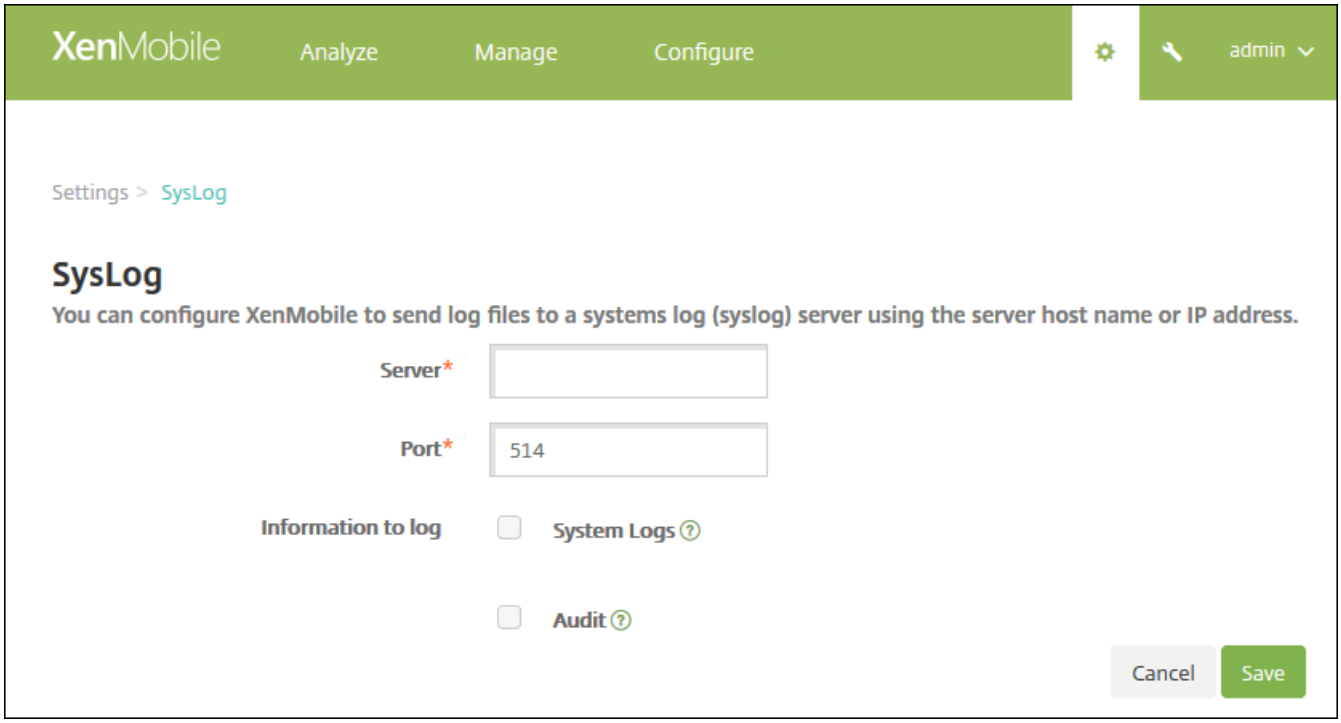
- La dirección IP del dispositivo que generó el mensaje de registro
- Una marca de tiempo
- El tipo de mensaje
- El nivel de registro asociado a un evento (crítico, error, aviso, advertencia, informativo, depuración, alerta o emergencia)
- La información del mensaje

Puede usar esta información para analizar el origen de la alerta y, si fuera necesario, realizar las correcciones oportunas.

> ## Nota
>
> En implementaciones de XenMobile Service (nube), 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 **Download All** 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**.

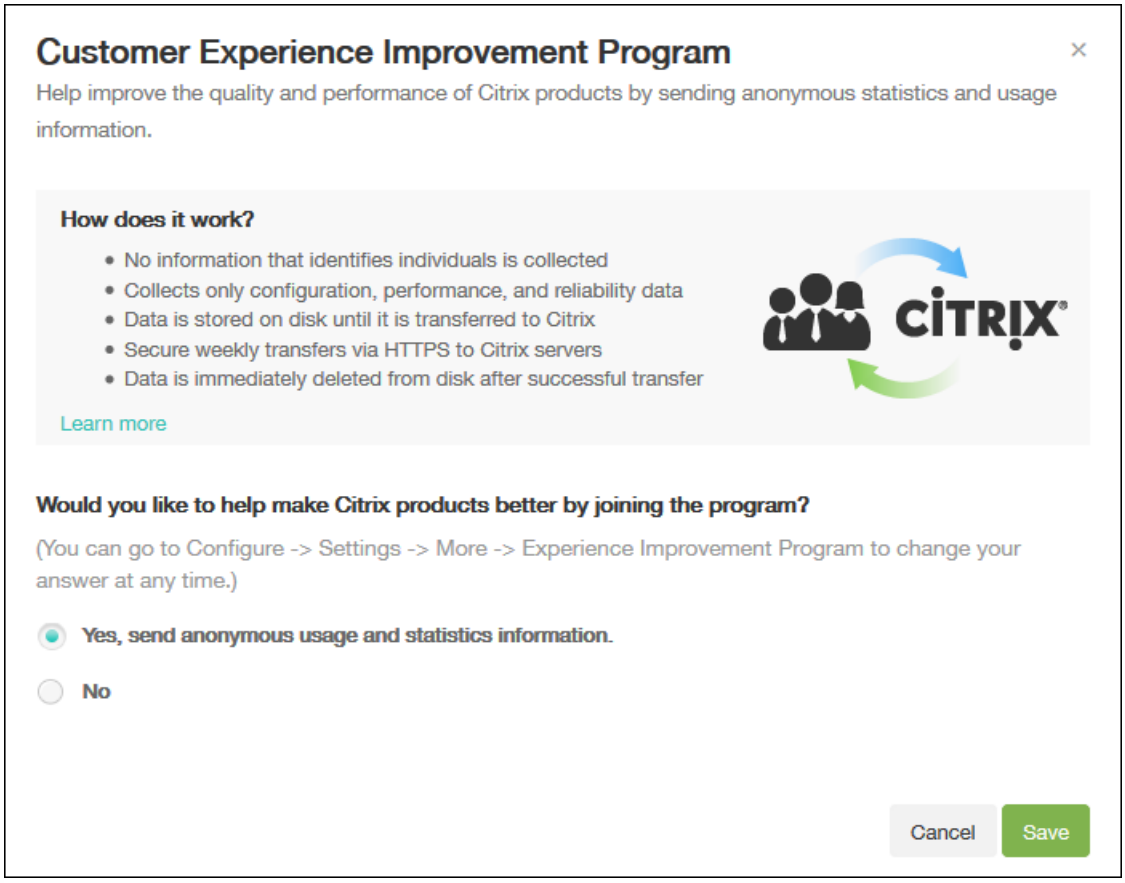
2. Haga clic en **Syslog**. Aparecerá la página **Syslog**.

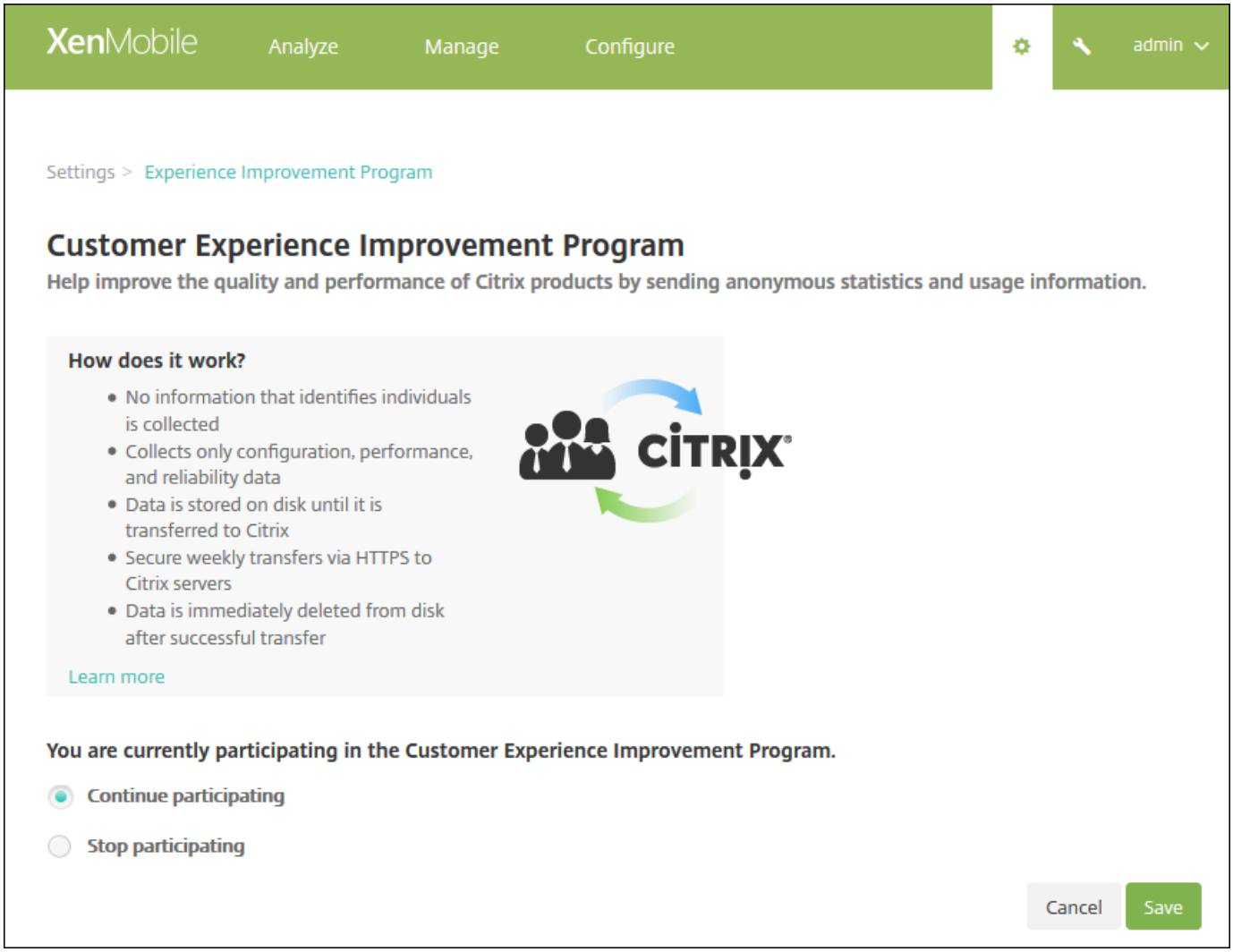


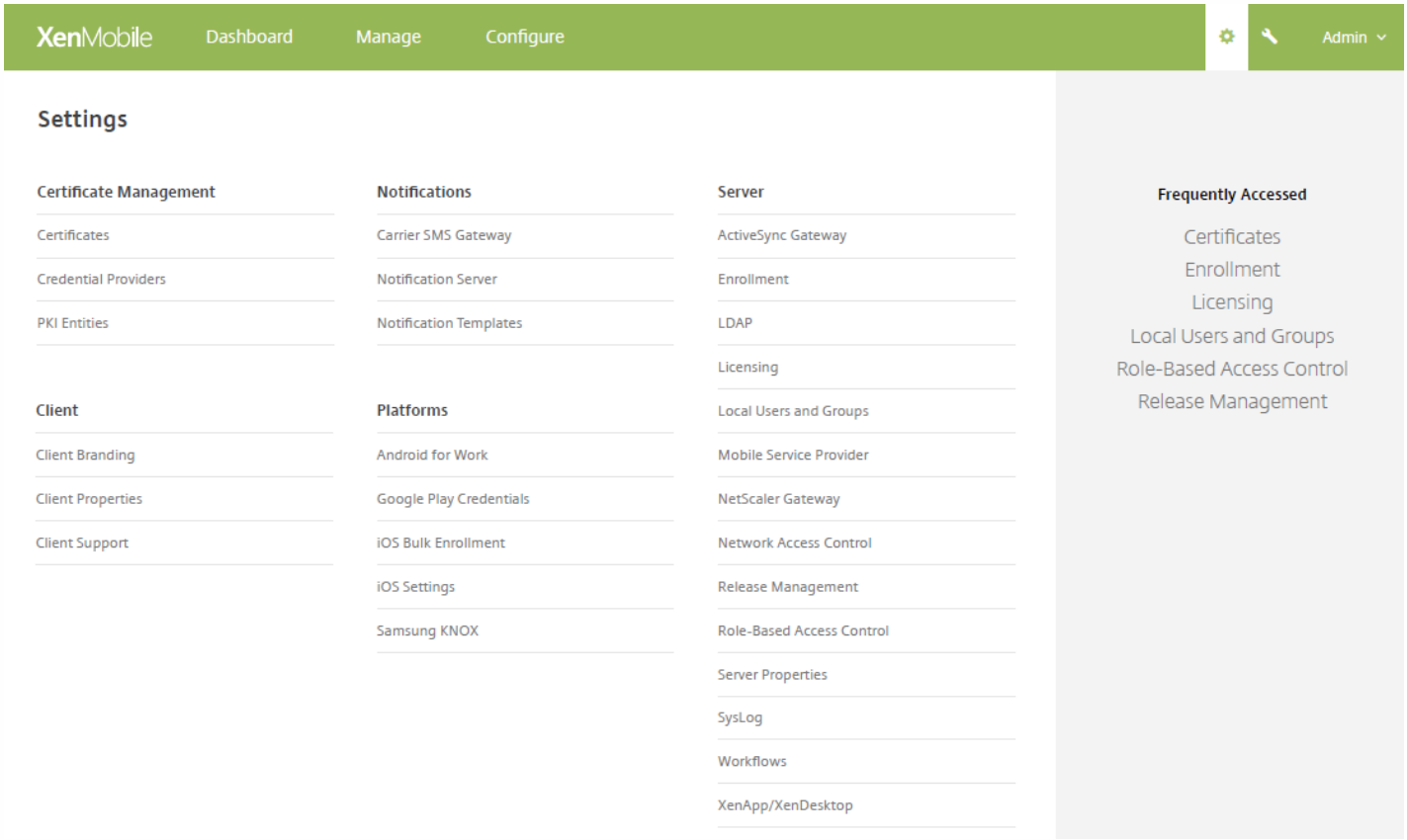
3. Configure estos parámetros:

- **Server**. 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 que lleva a cabo XenMobile.
  - Los registros de auditoría contienen un registro cronológico de las actividades del sistema para XenMobile.

4. Haga clic en **Save**.

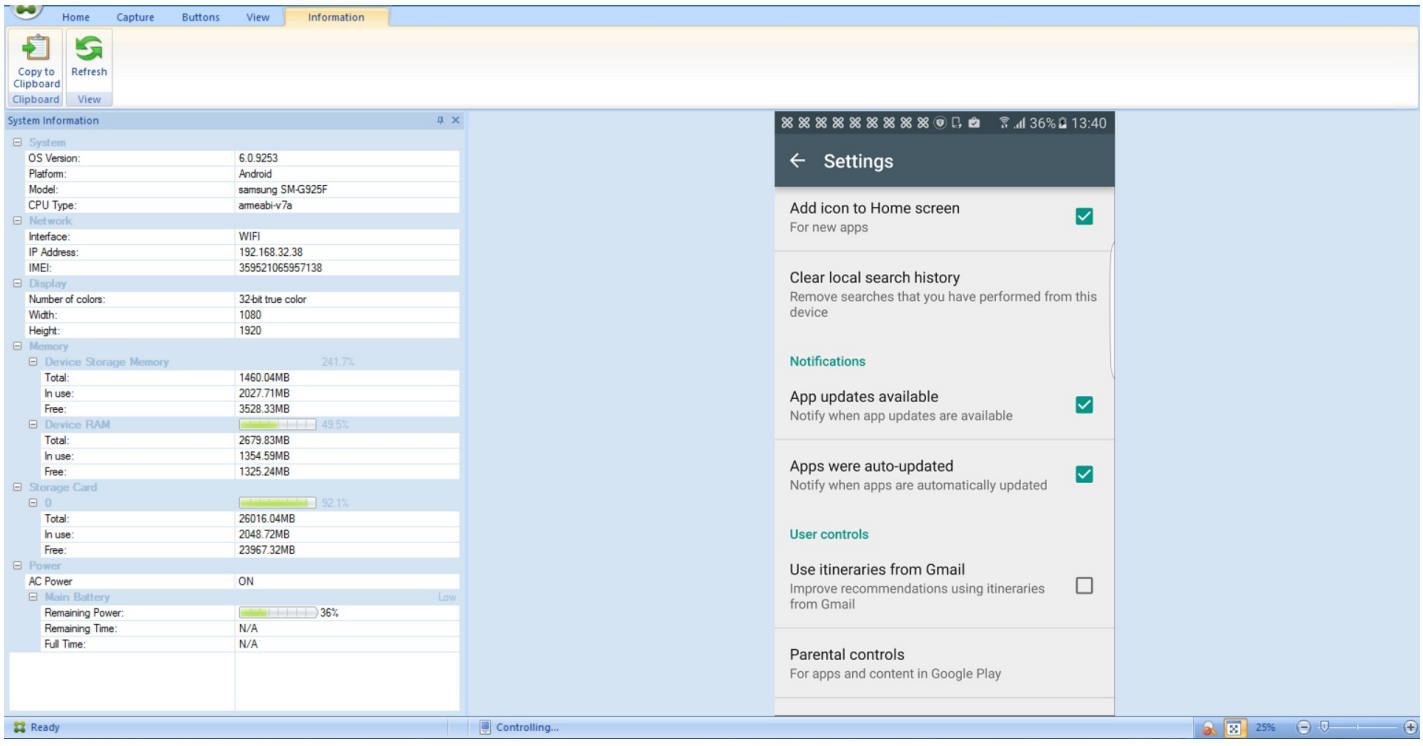






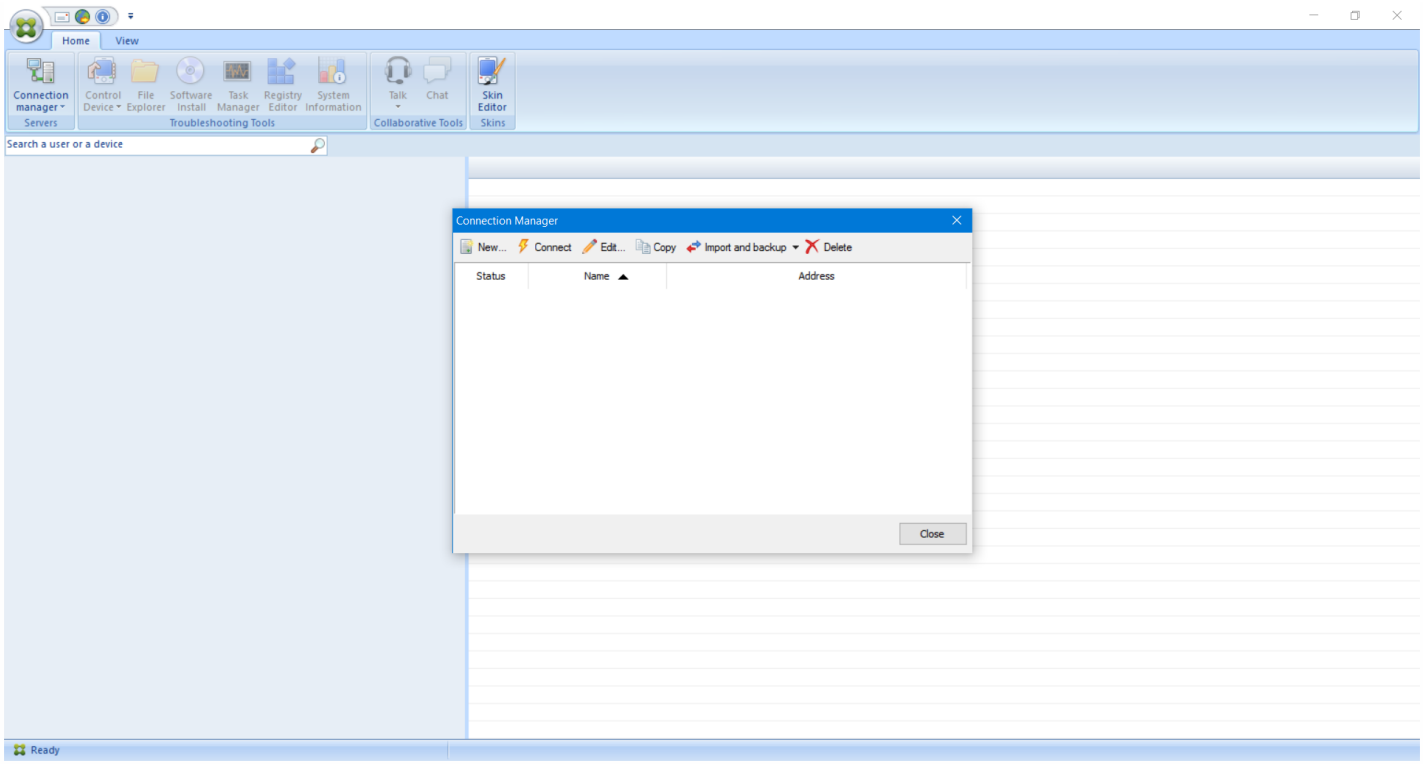
-
-
-

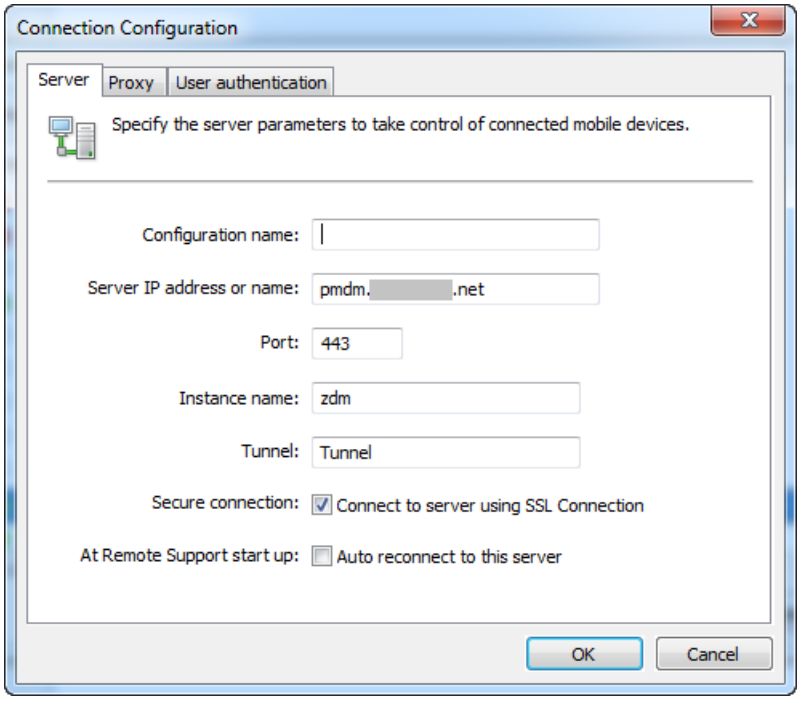
-
-
-

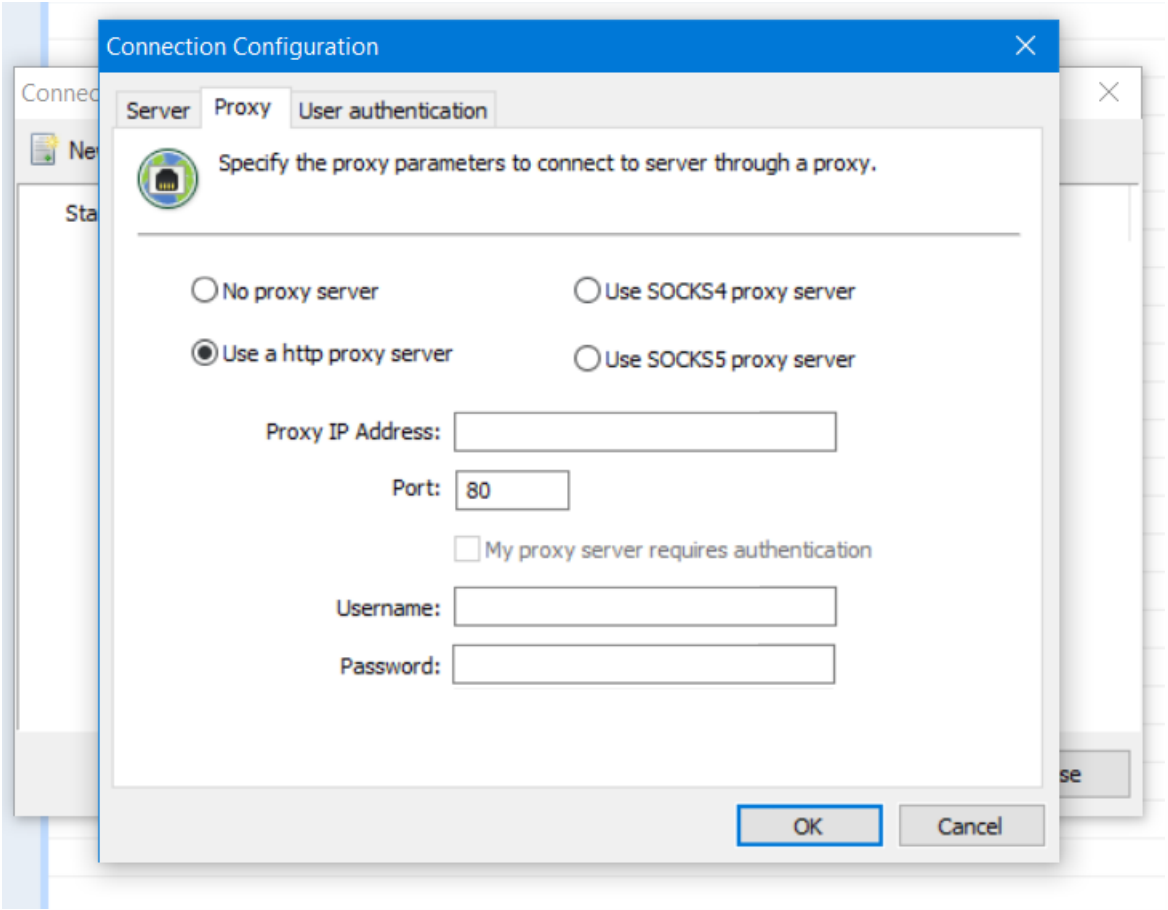


-
-
-
-
-
-
-

-
-

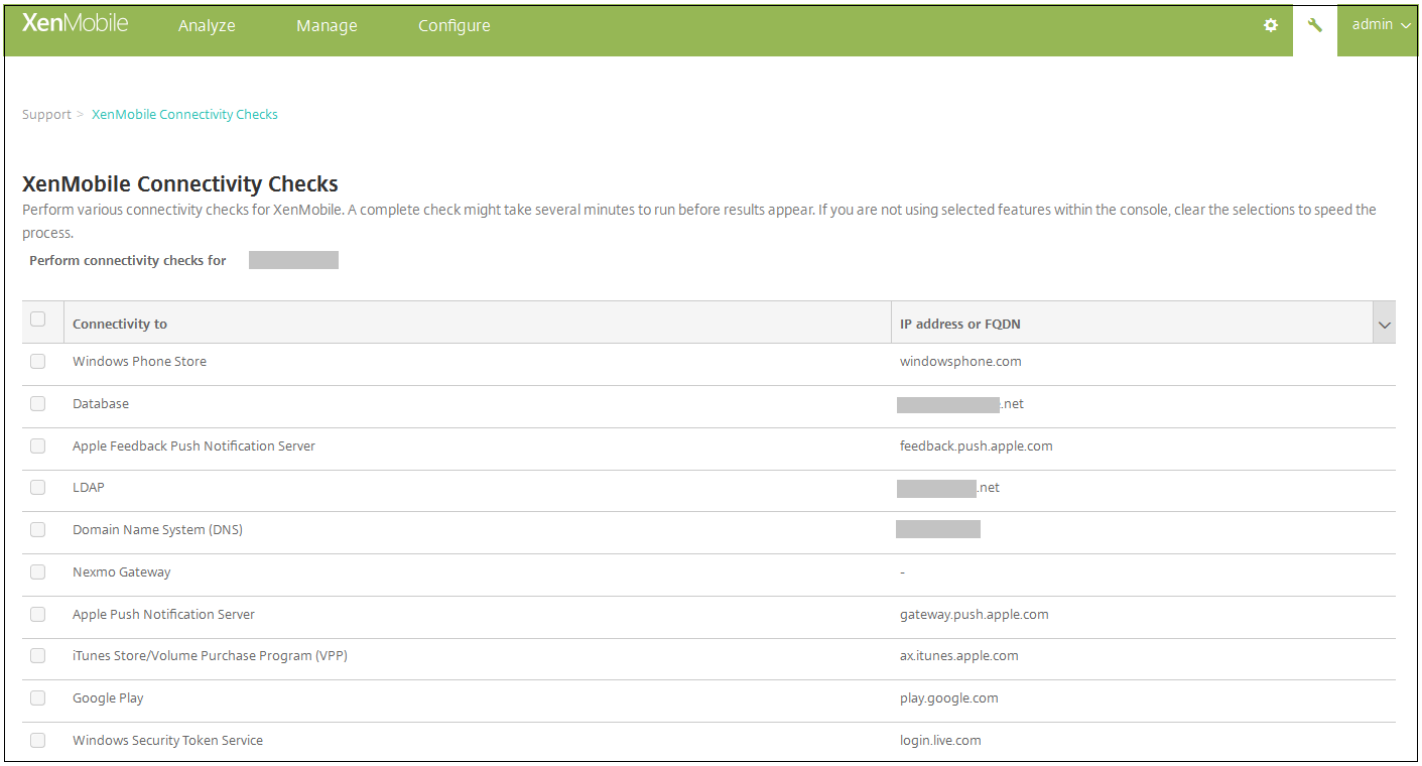


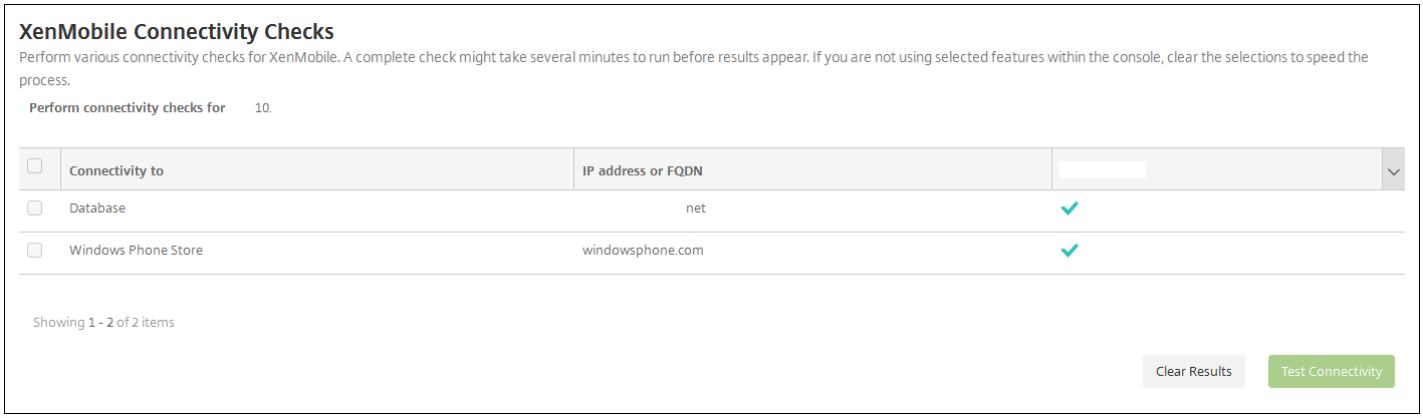


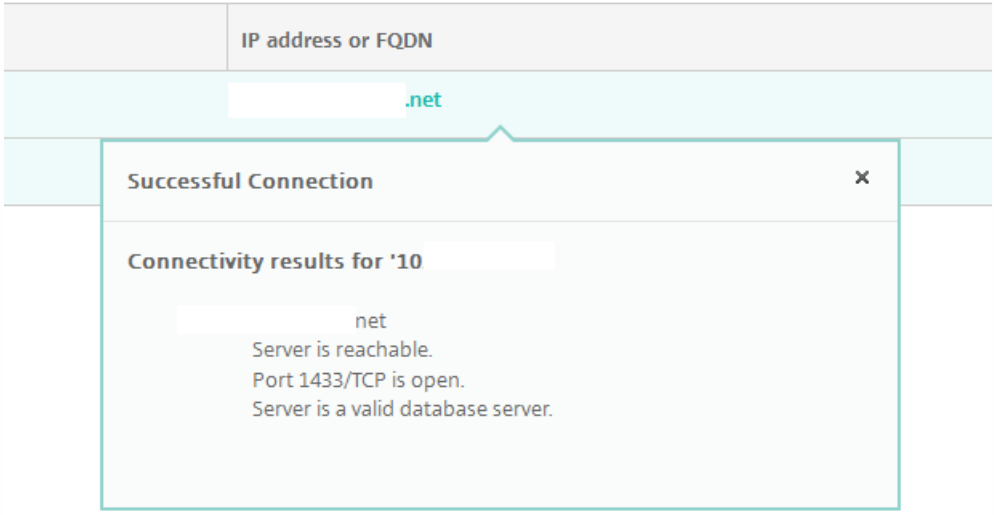


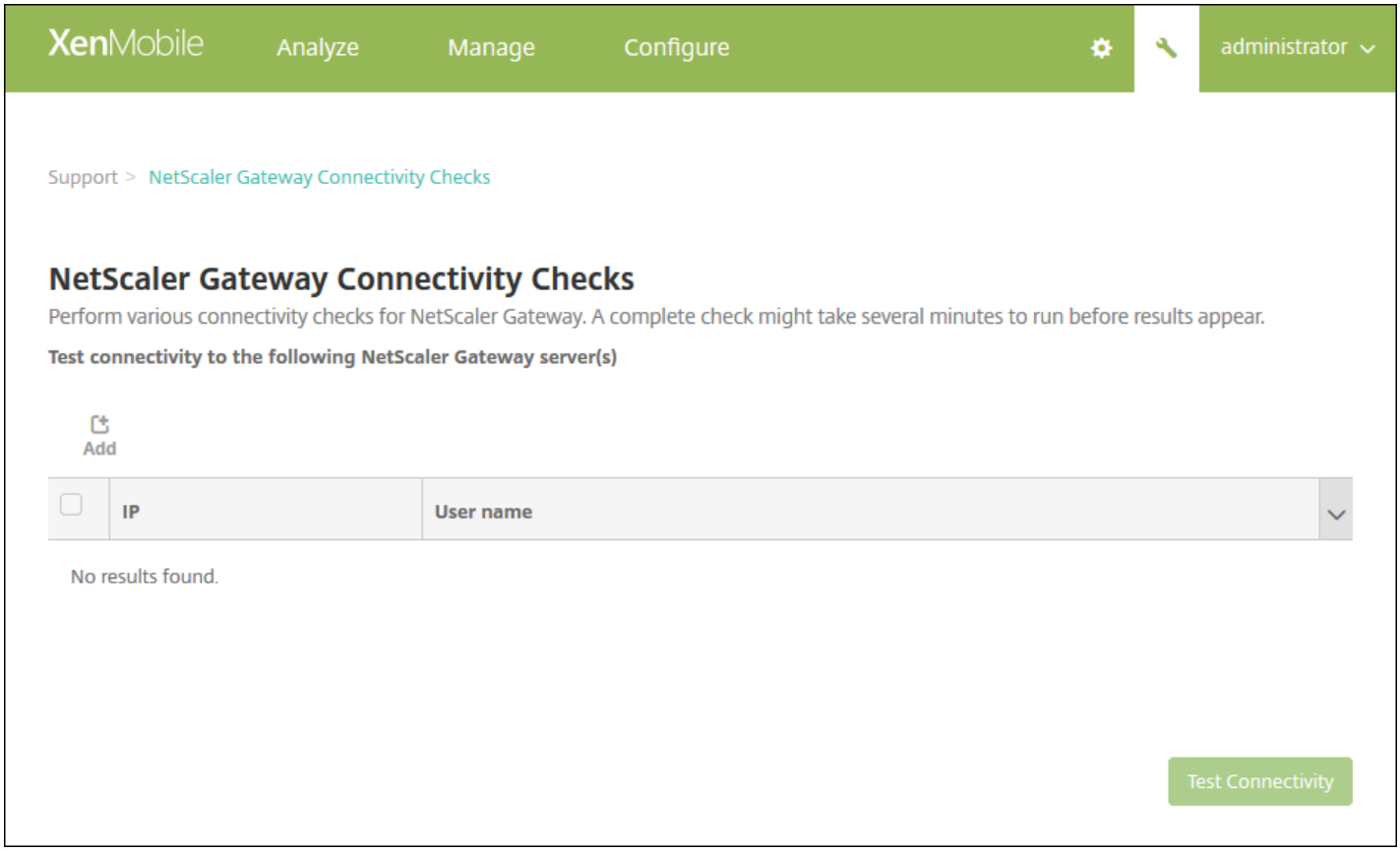
-
-

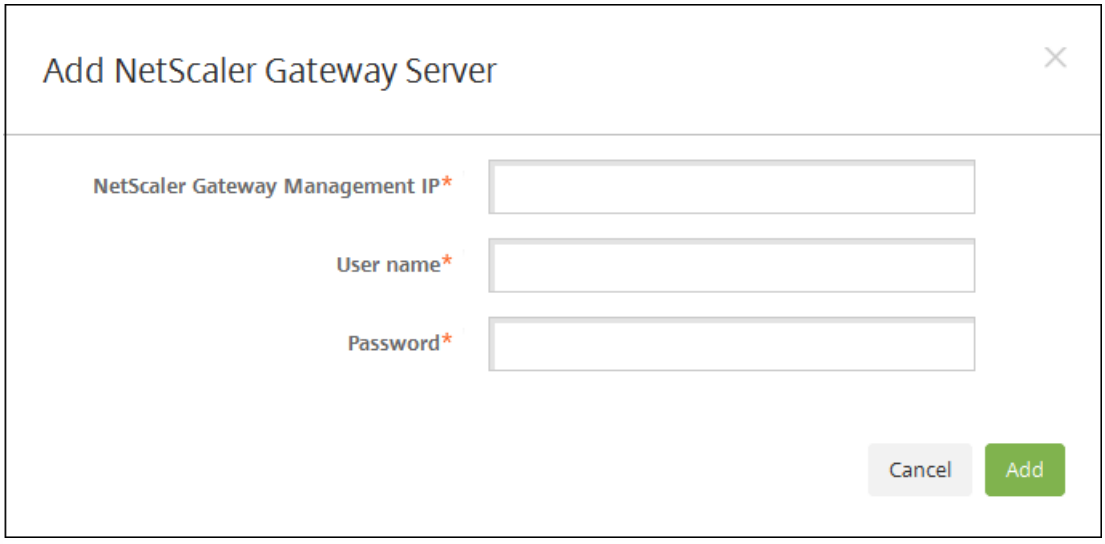
-
-
-
-
-
-
-
-

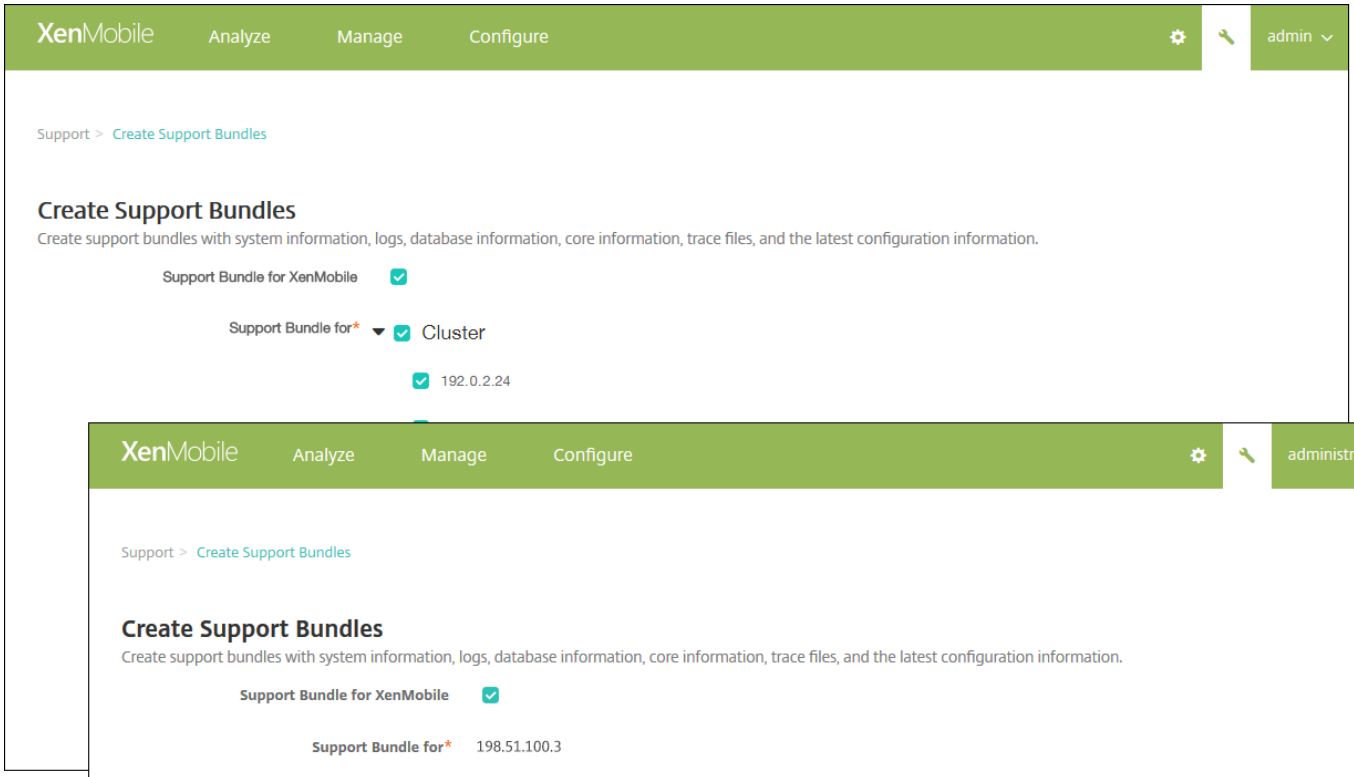


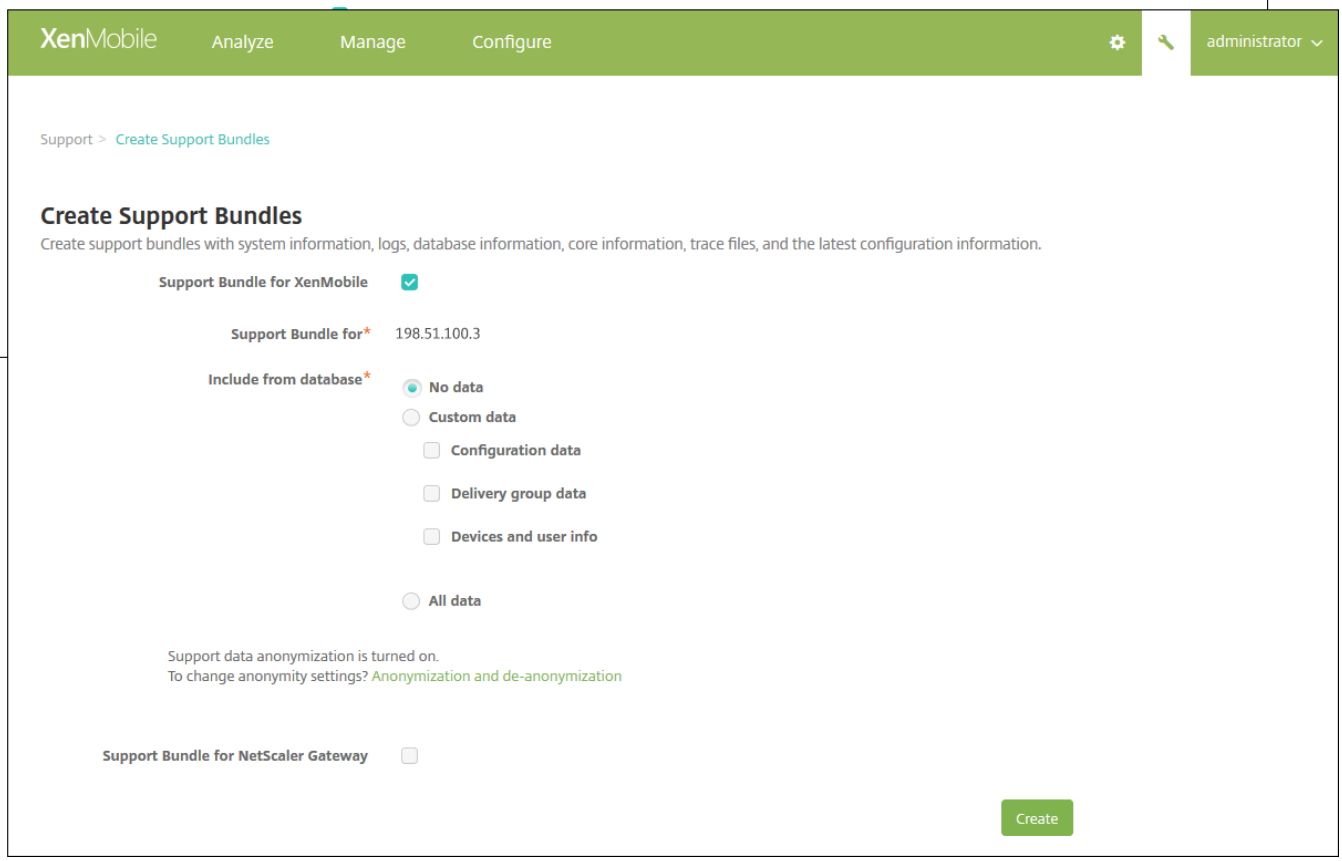




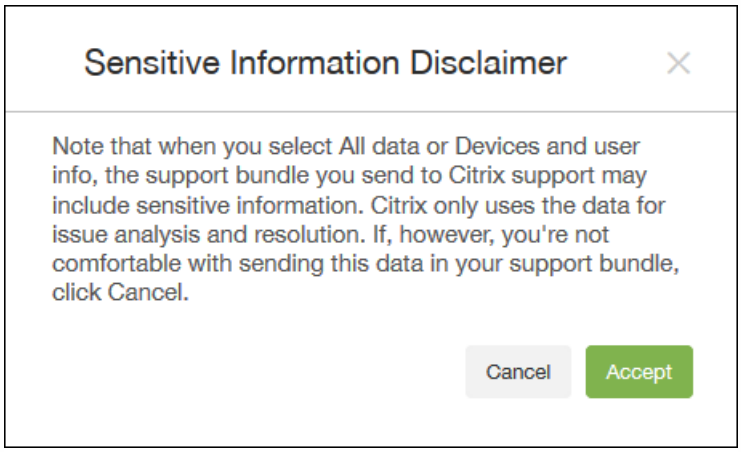


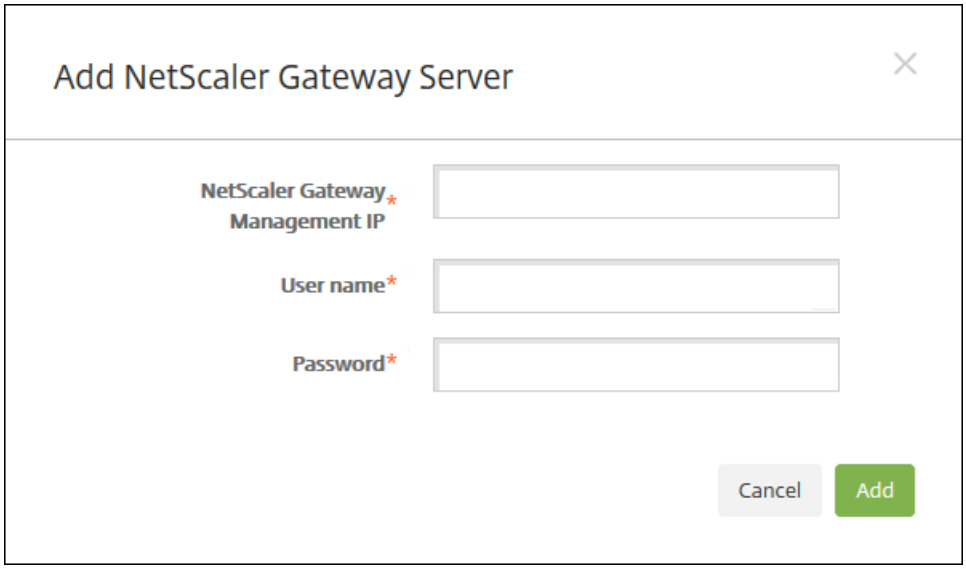


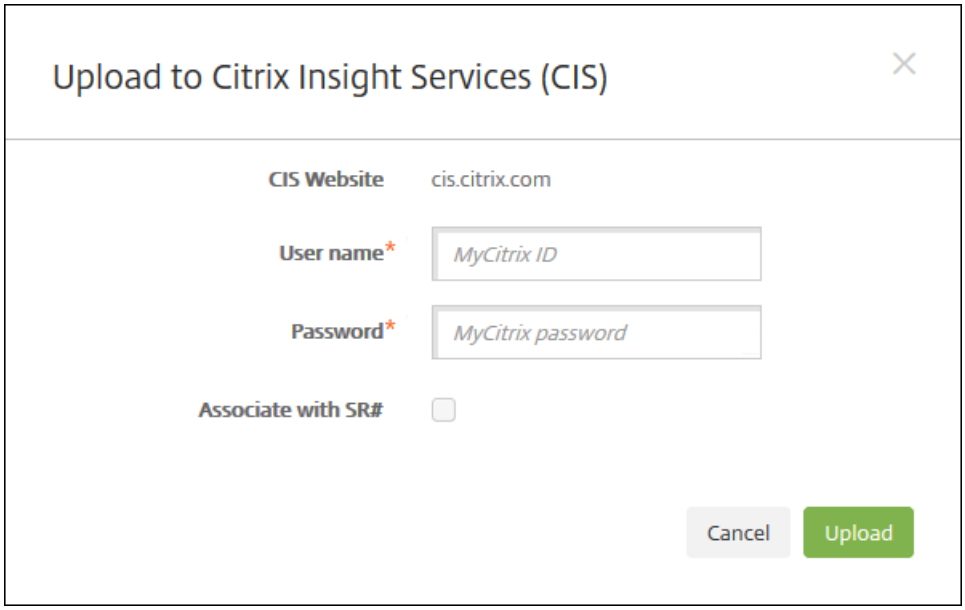




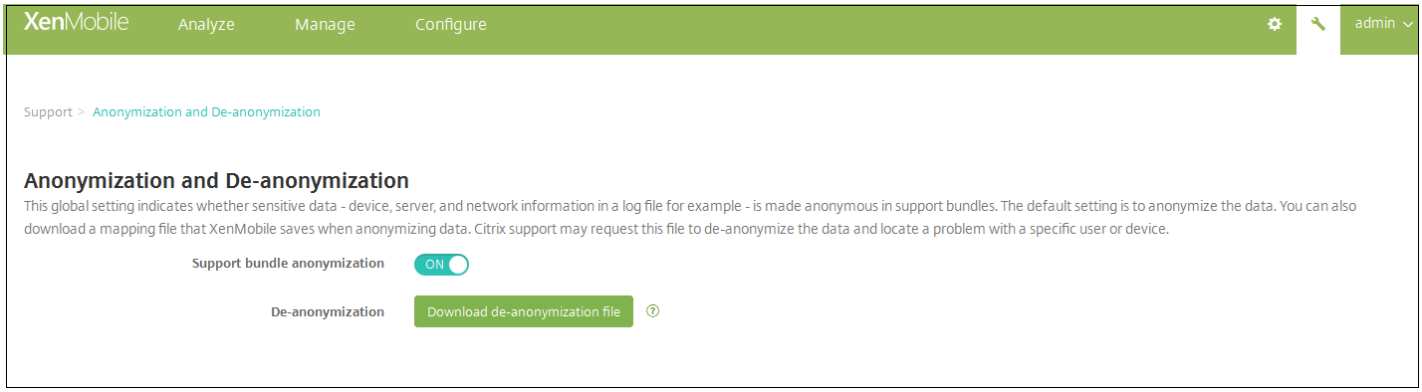
-
-
  -
  -
  -
-

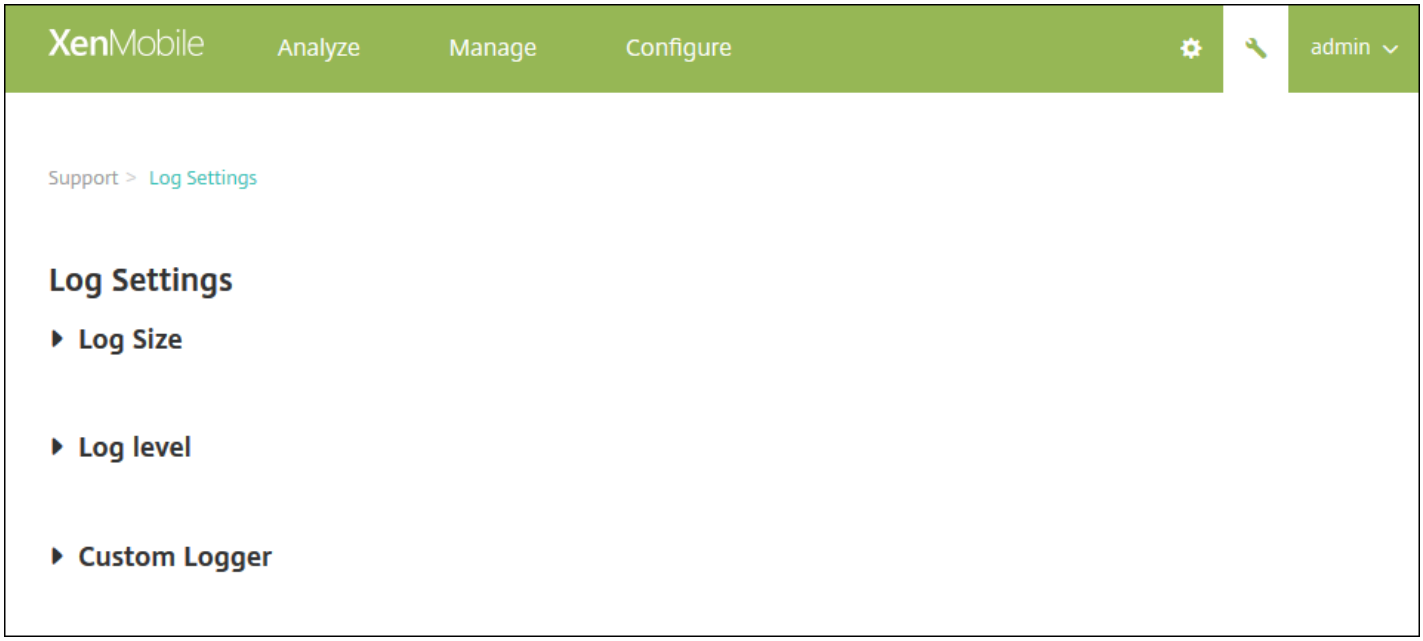




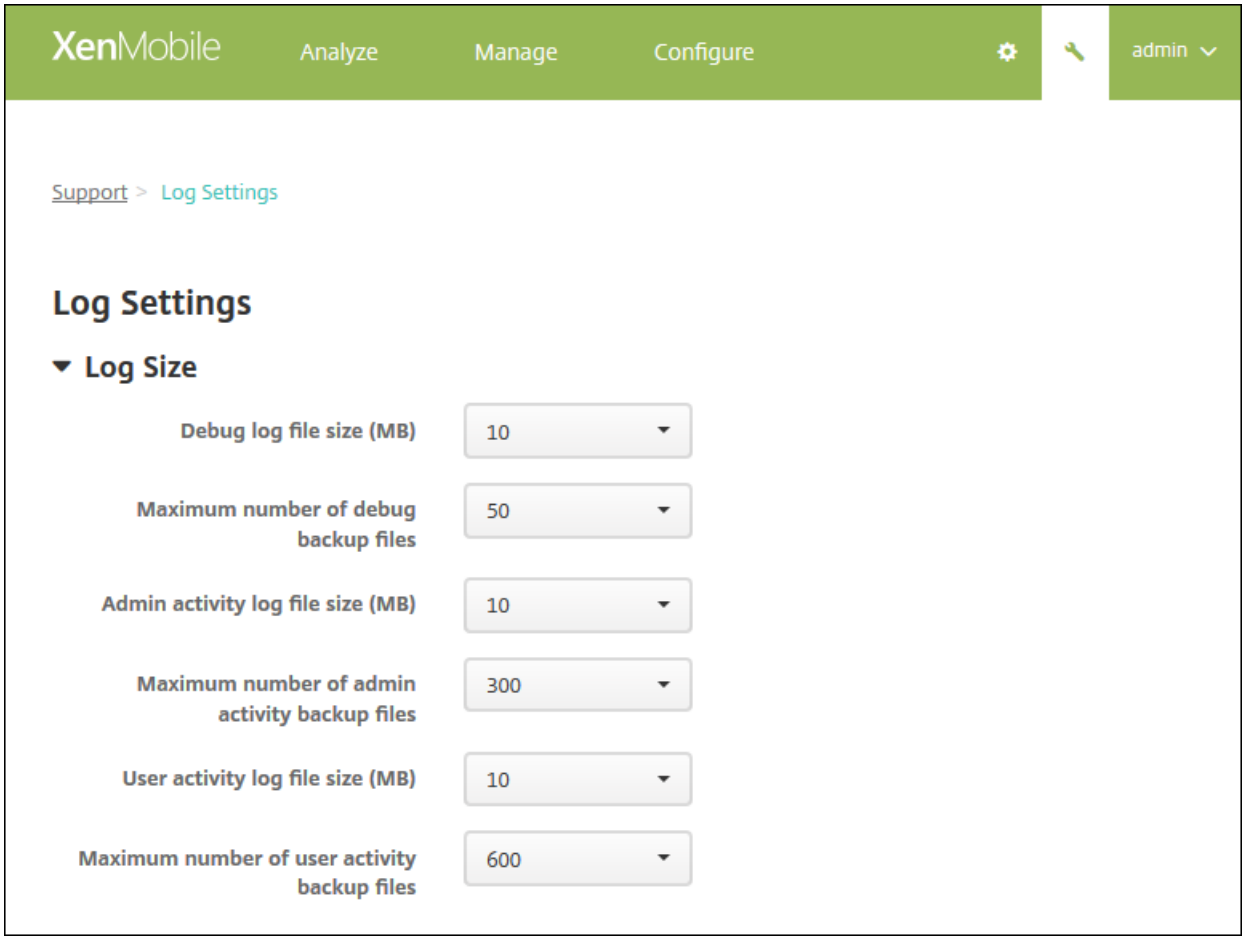


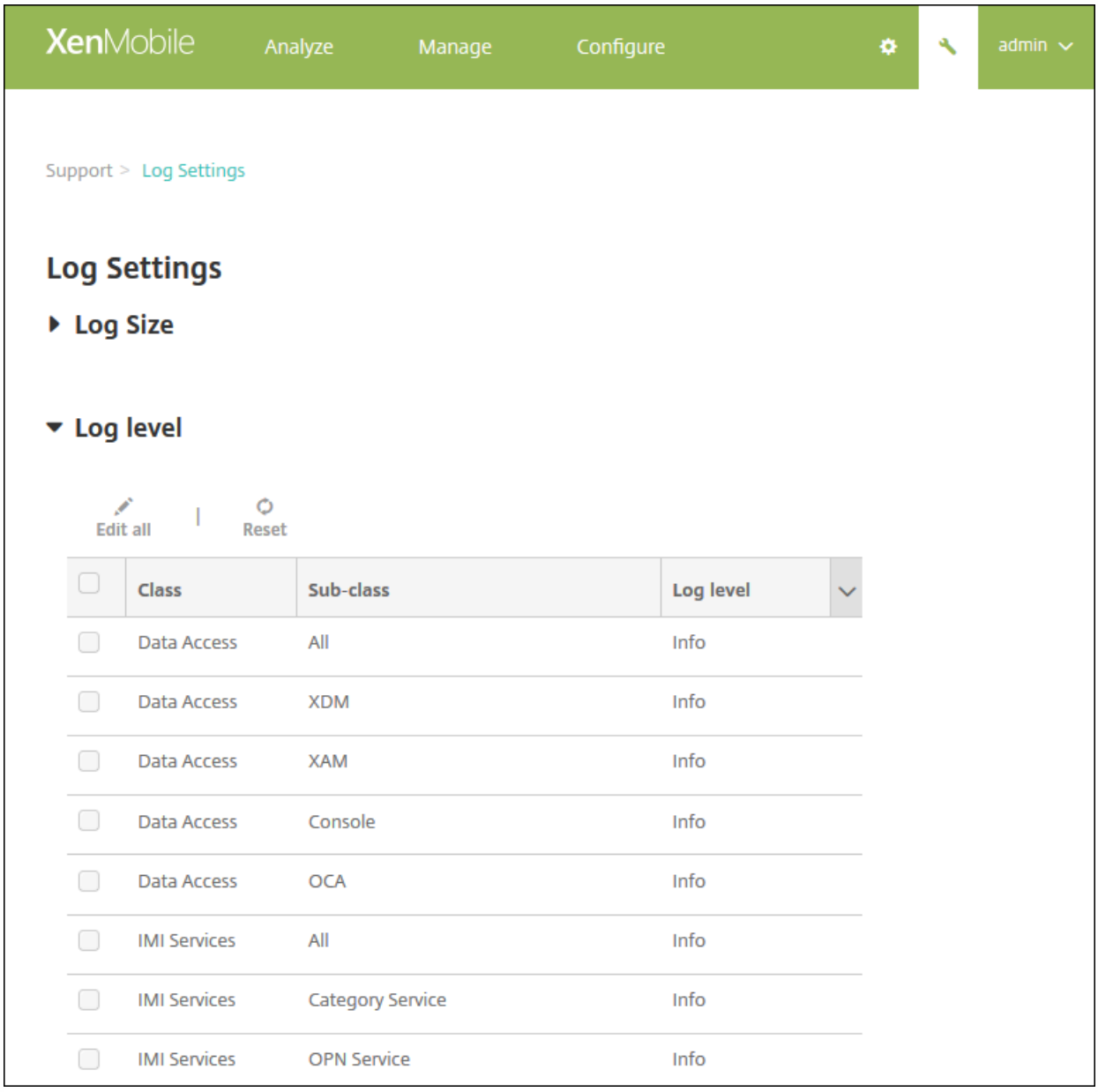
-
-



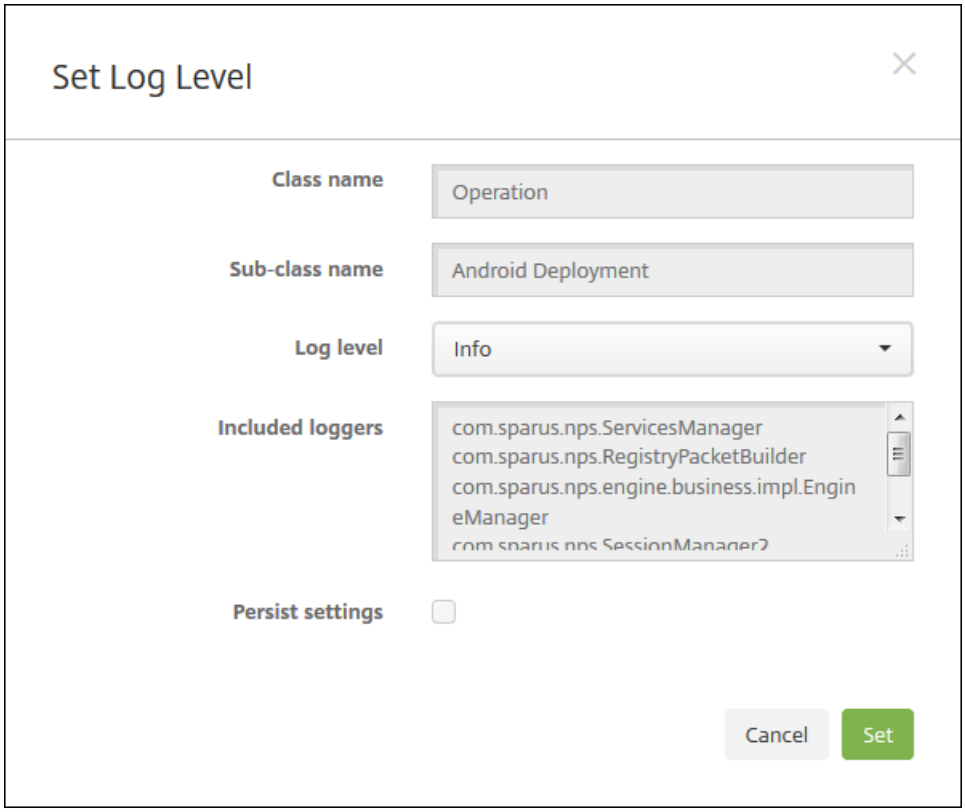


-
-
-

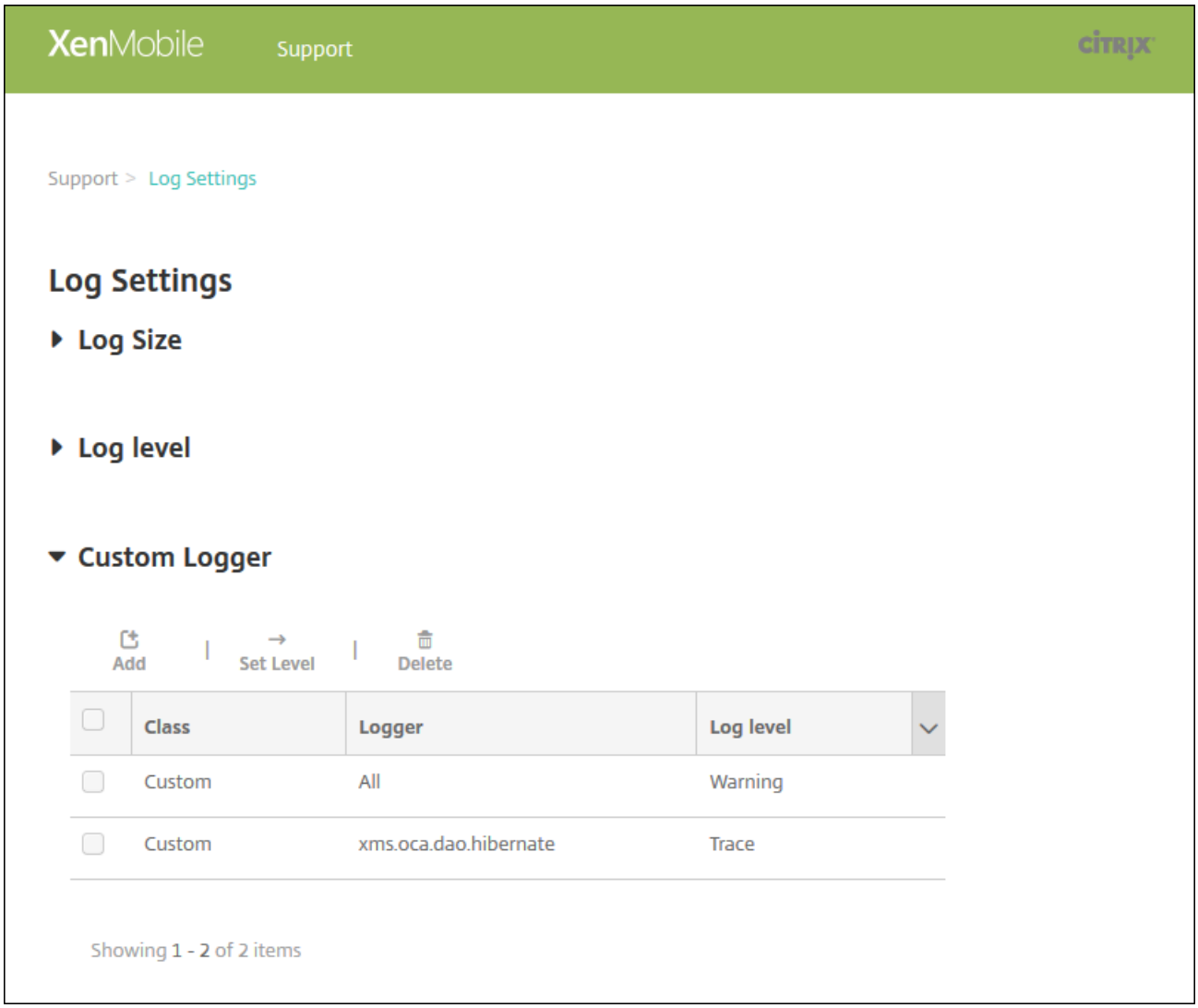


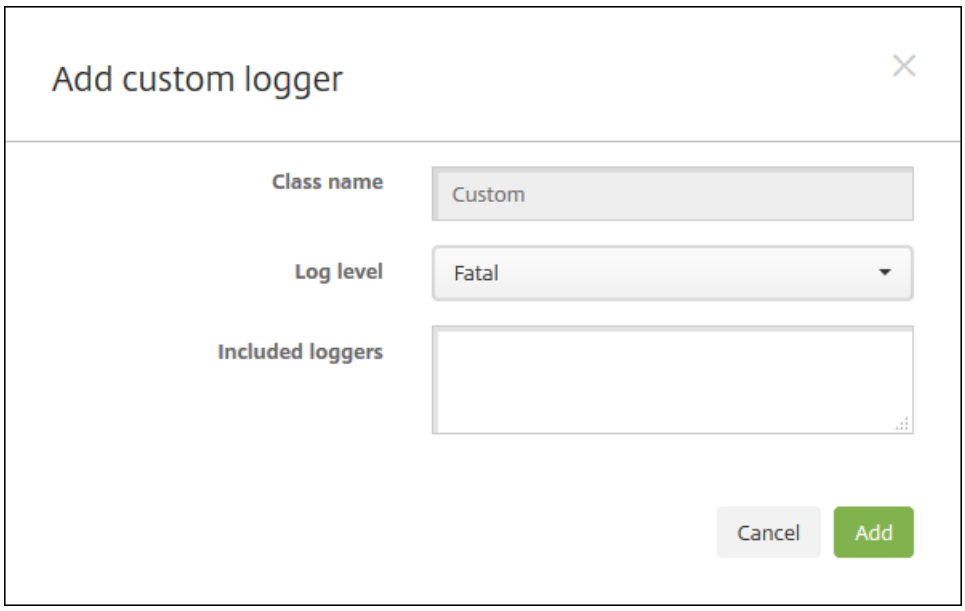


-
-

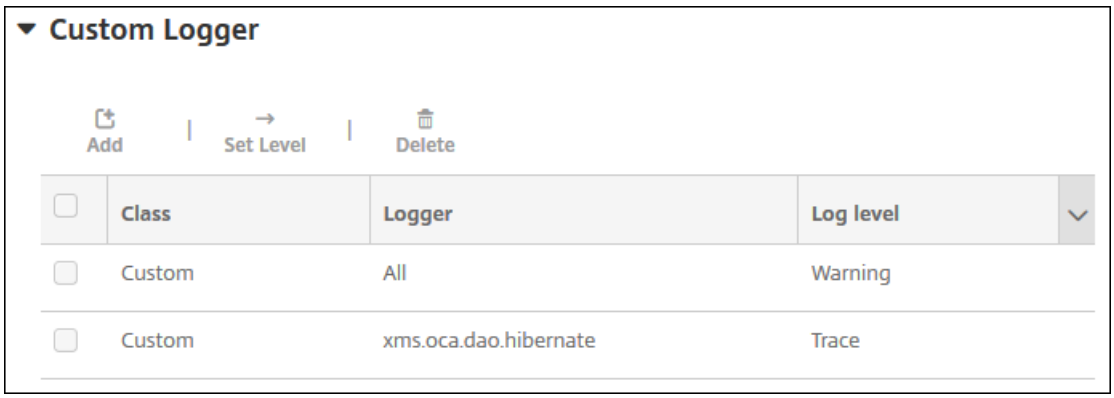


-
-
-
  -
  -
  -
  -
  -
  -
  -
-
-





-
-
  -
  -
  -
  -
  -
  -
  -
  -
-

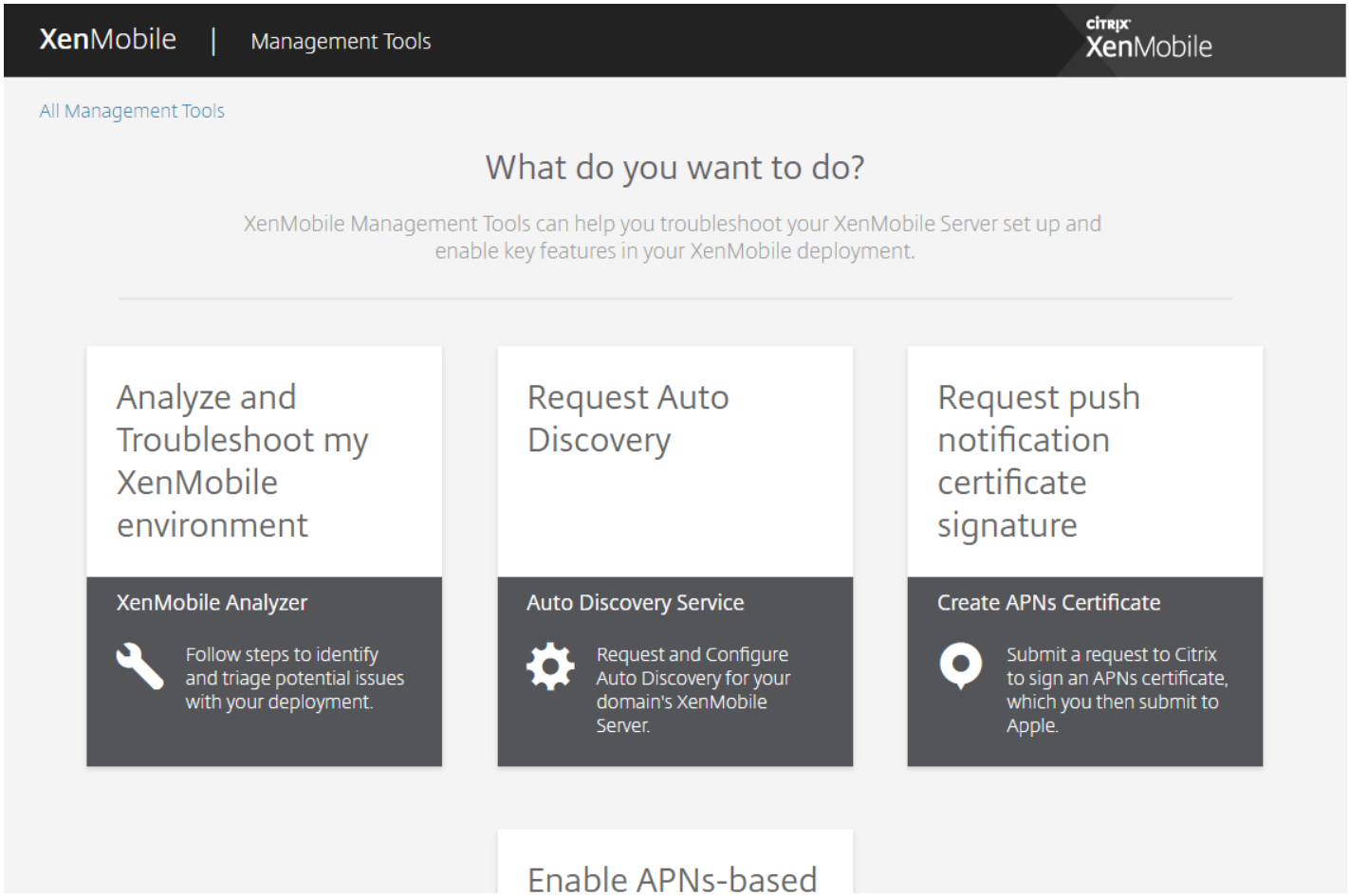


-
-
-
-
-

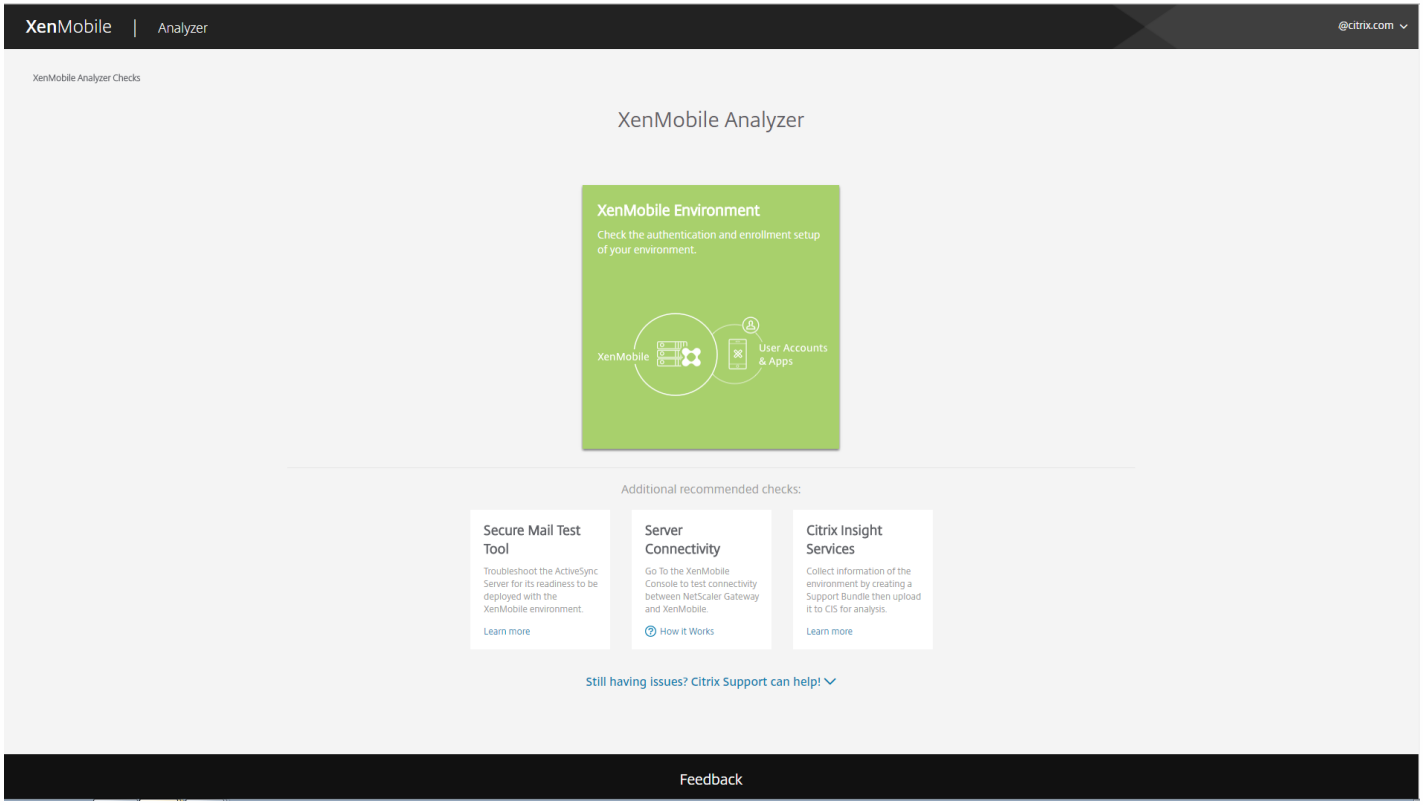
-

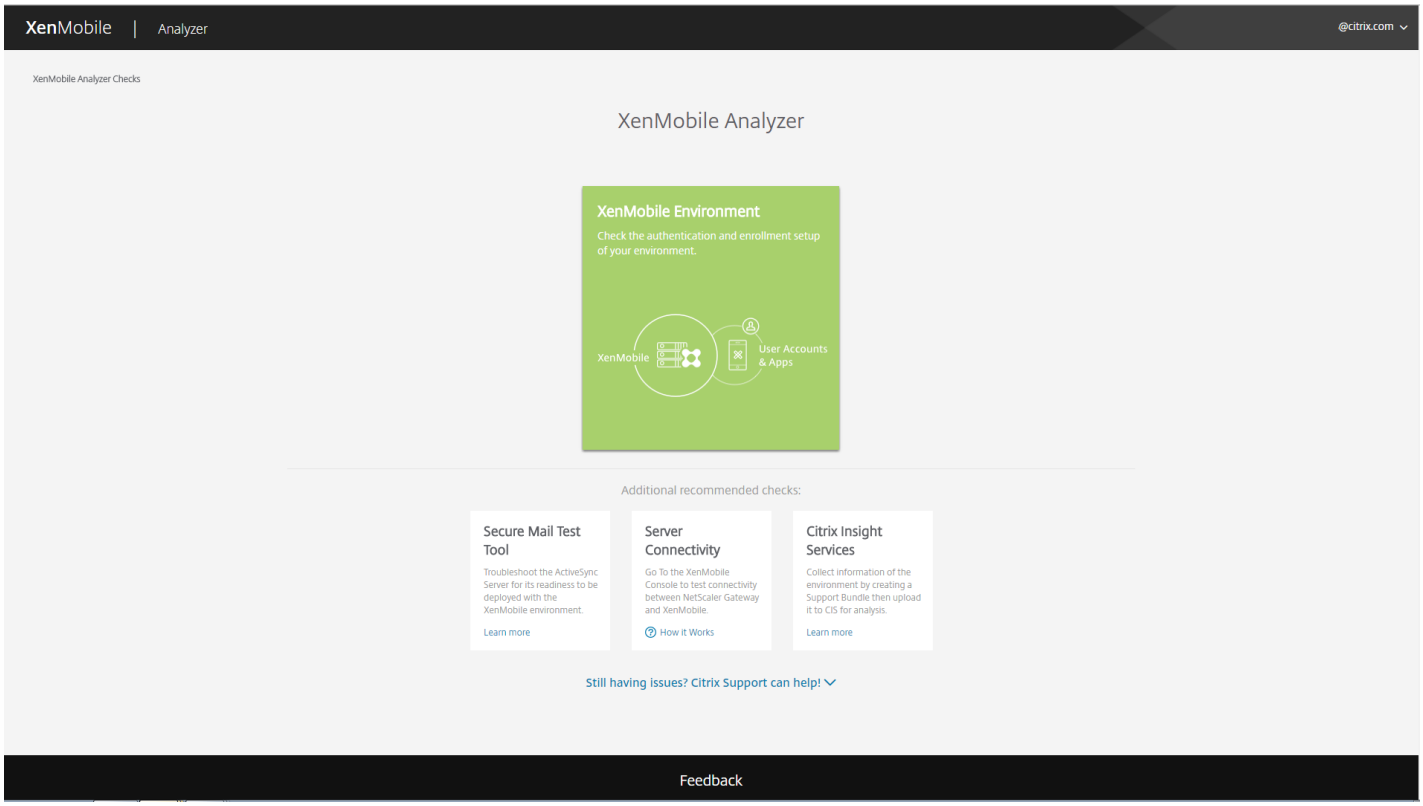
-
-

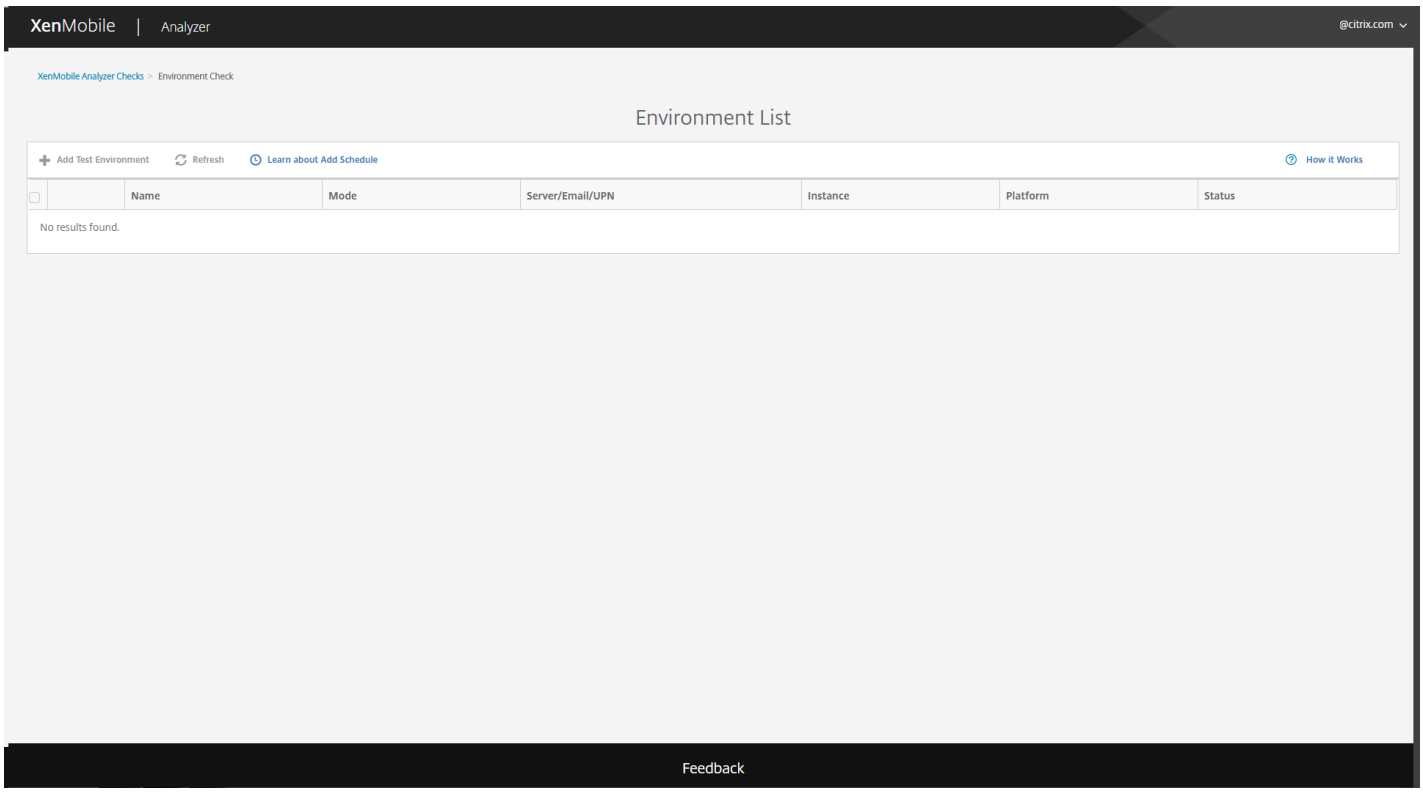
-
-
-
-
-
-

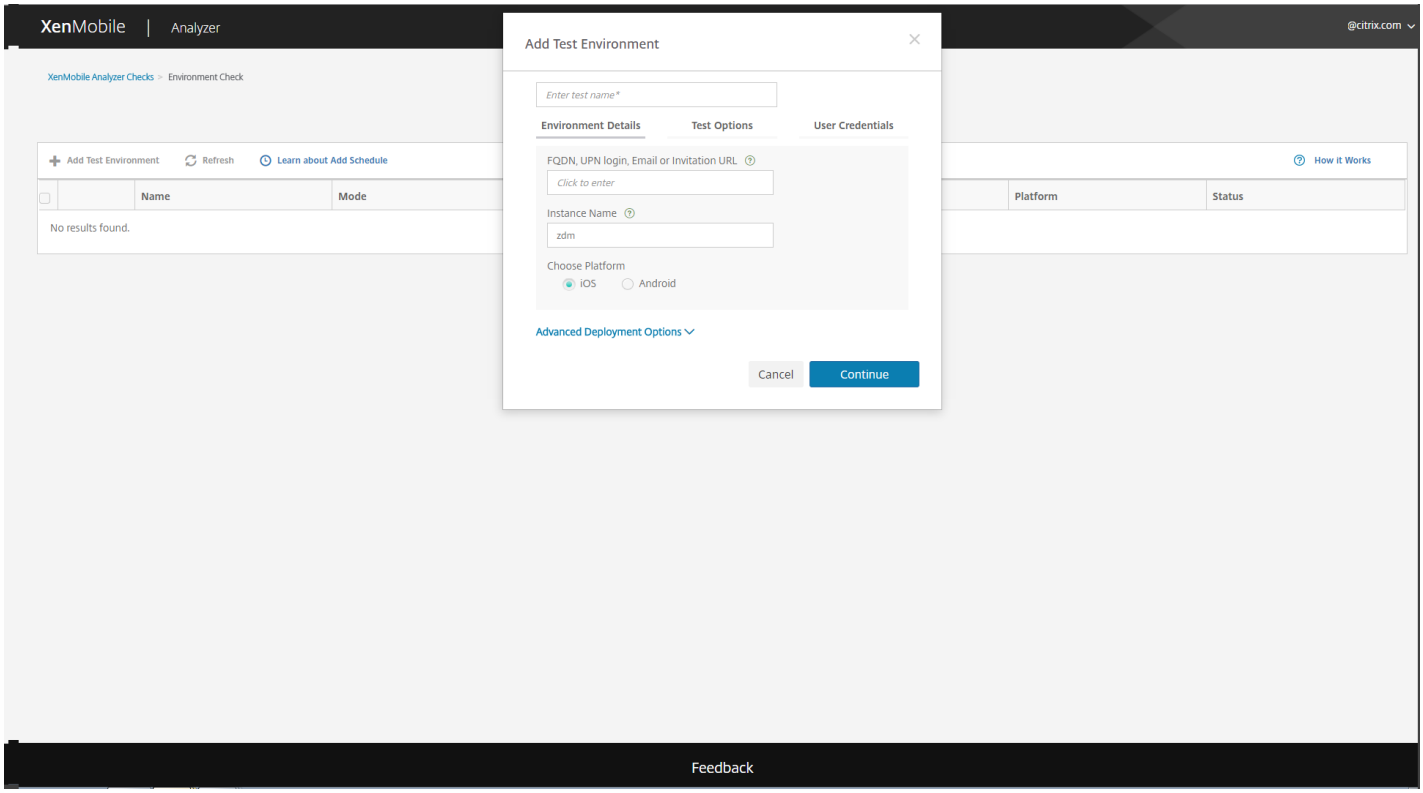


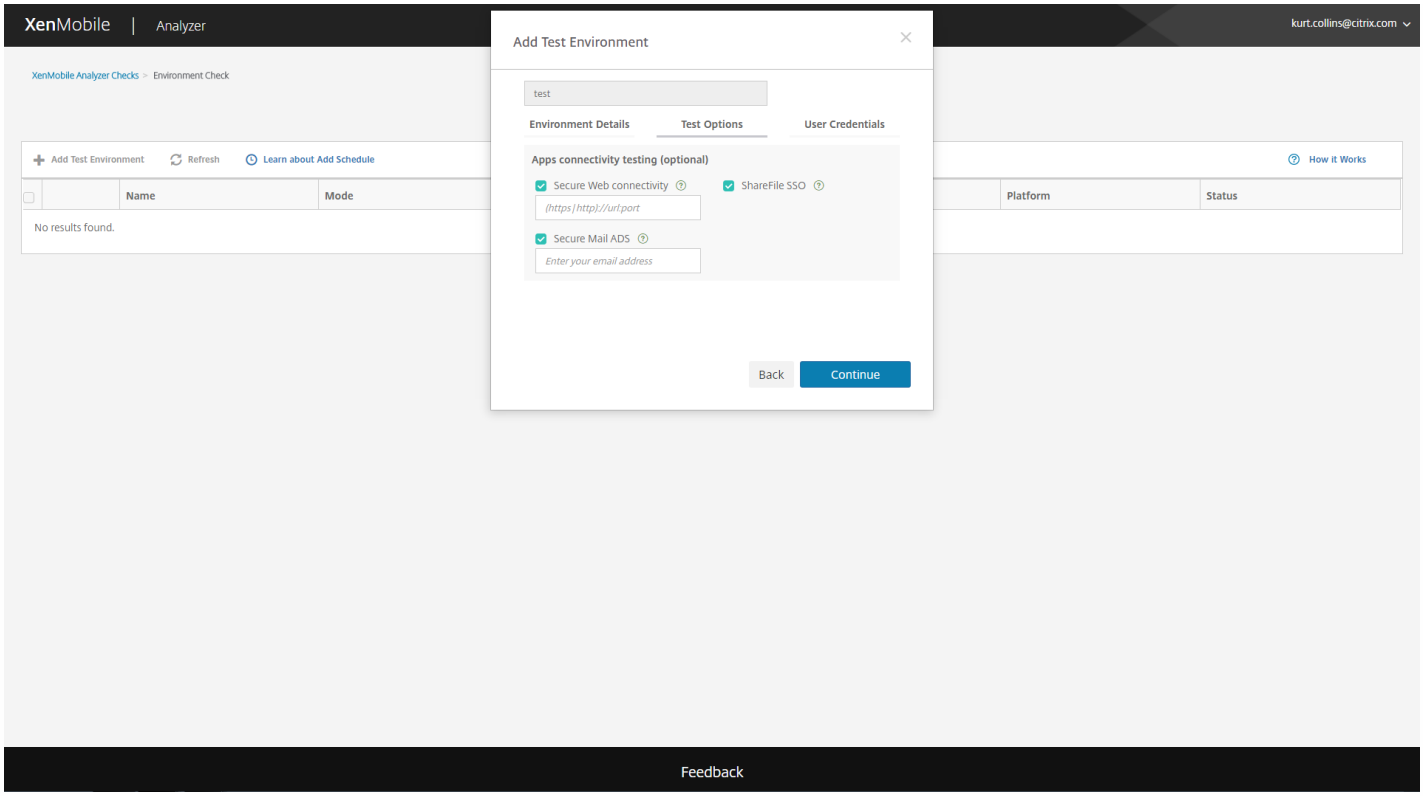
-
-
-
-
-

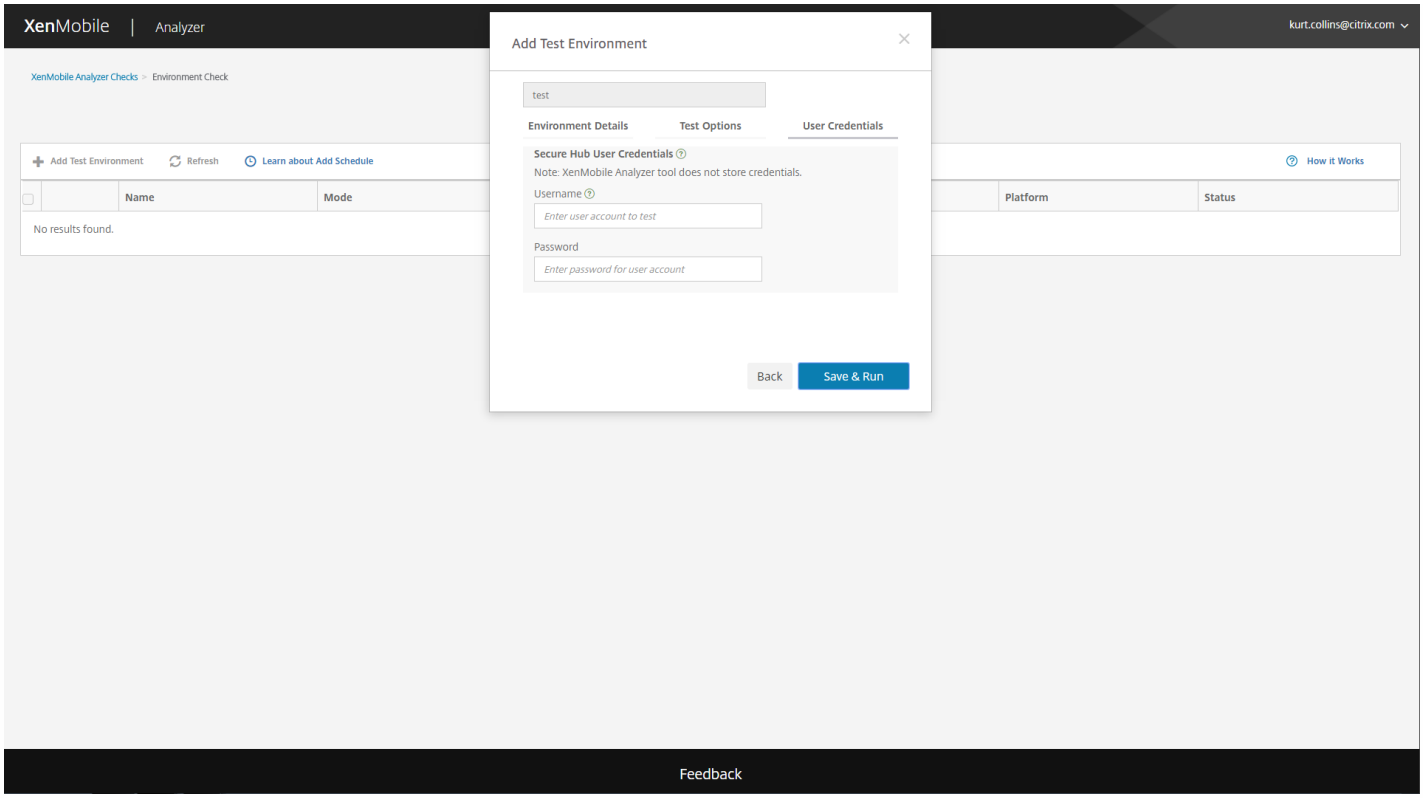
- 

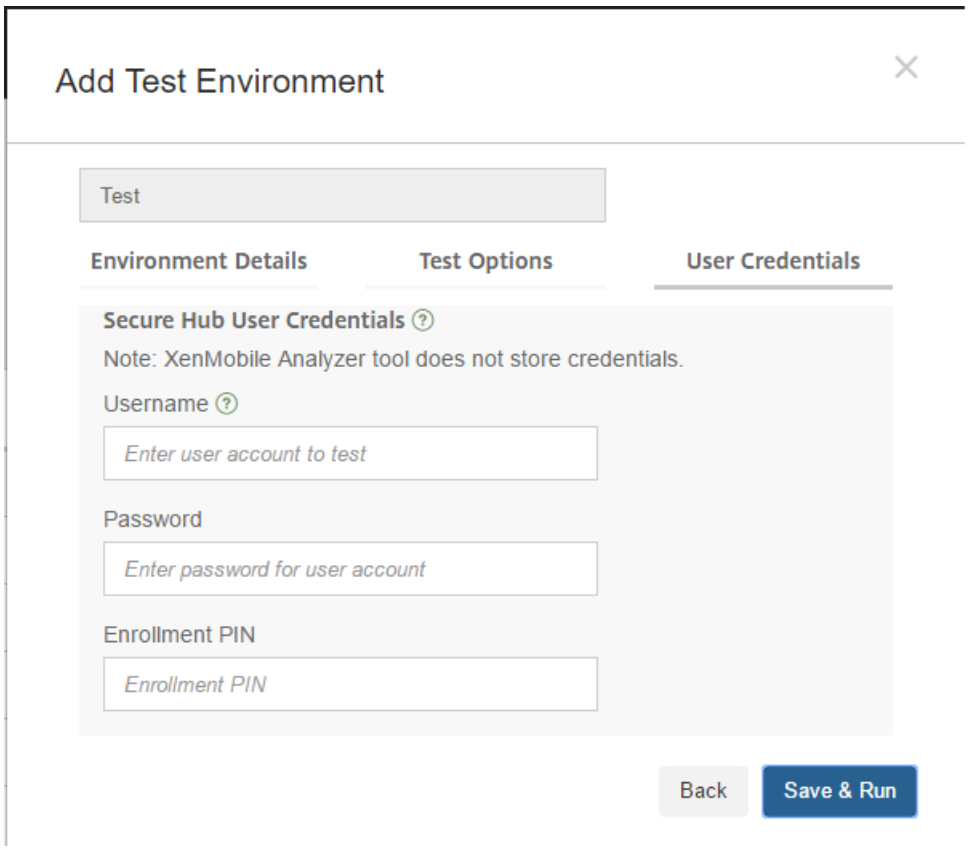


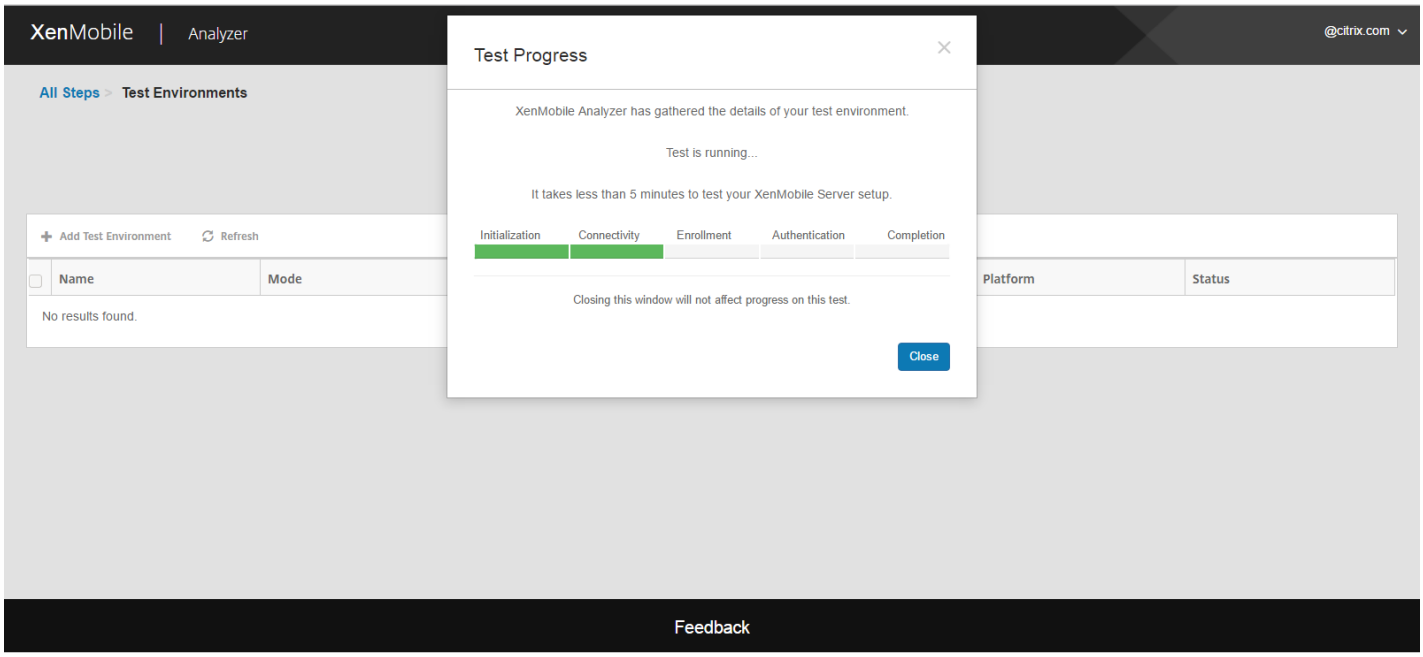


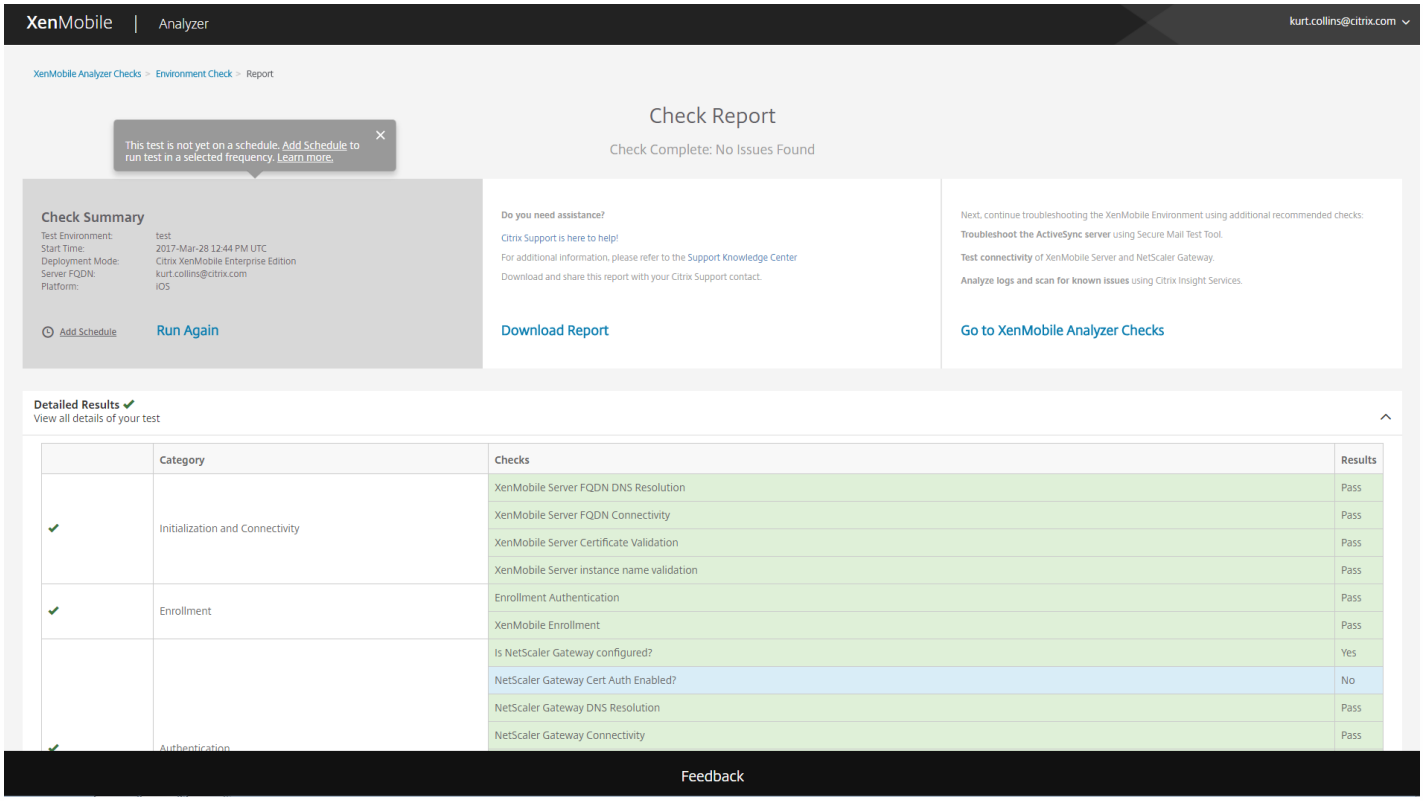


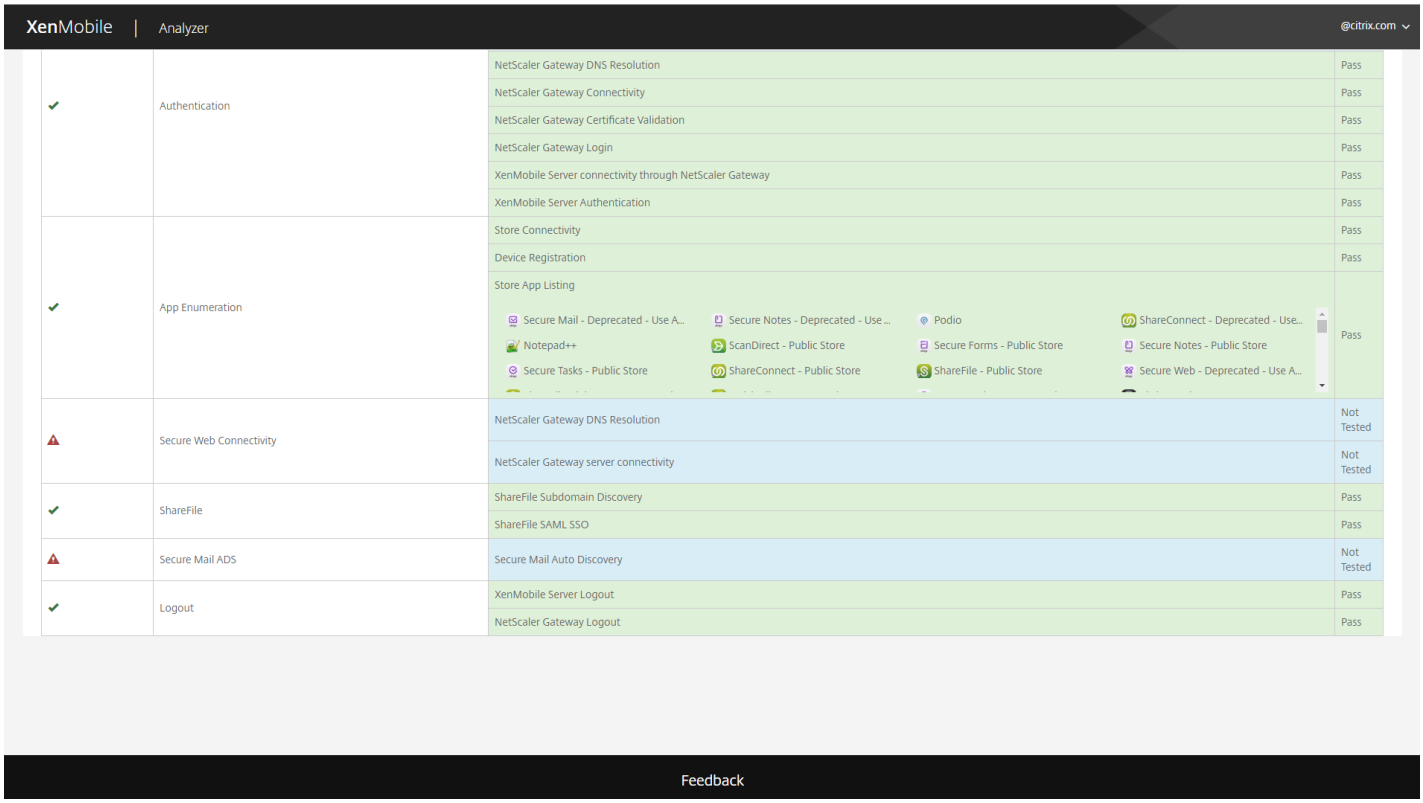


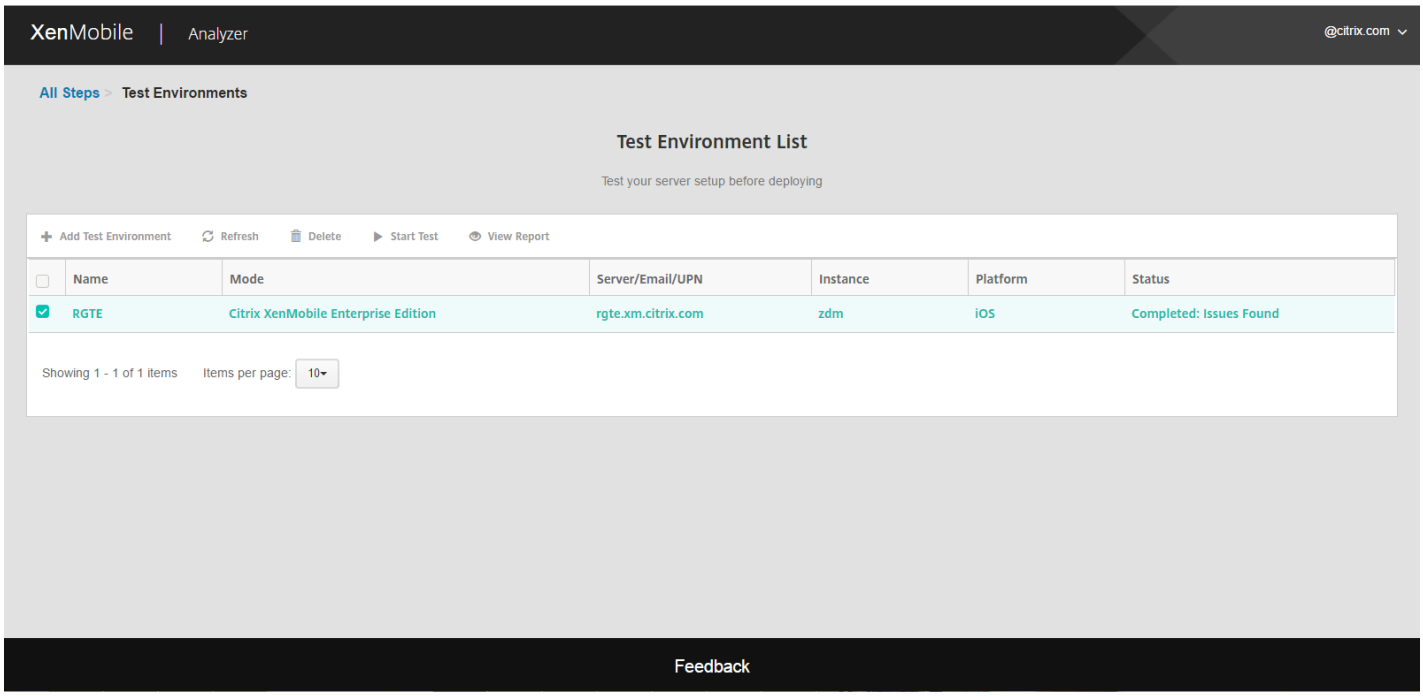


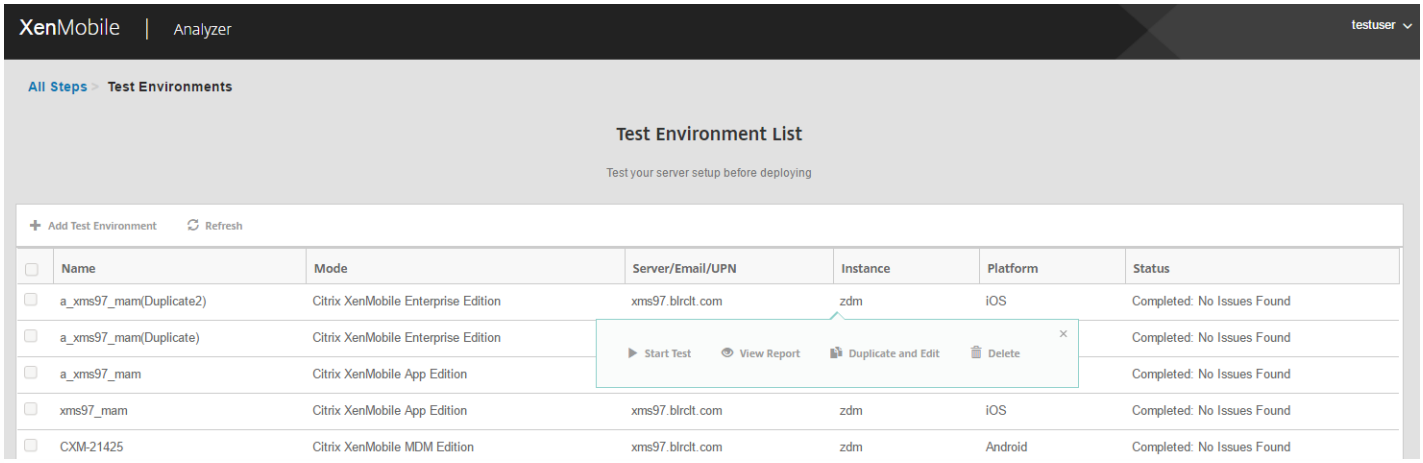


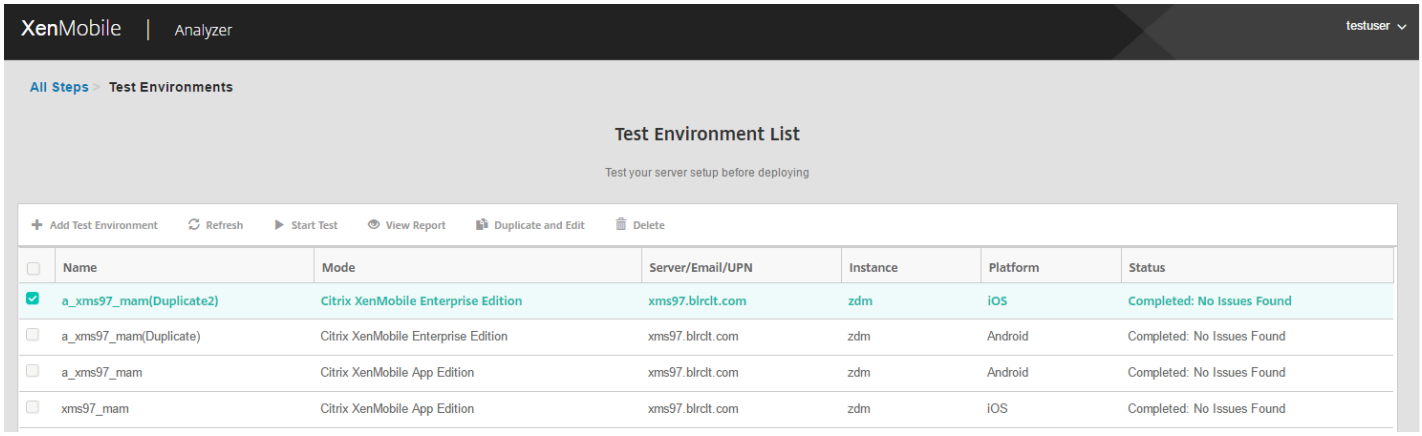


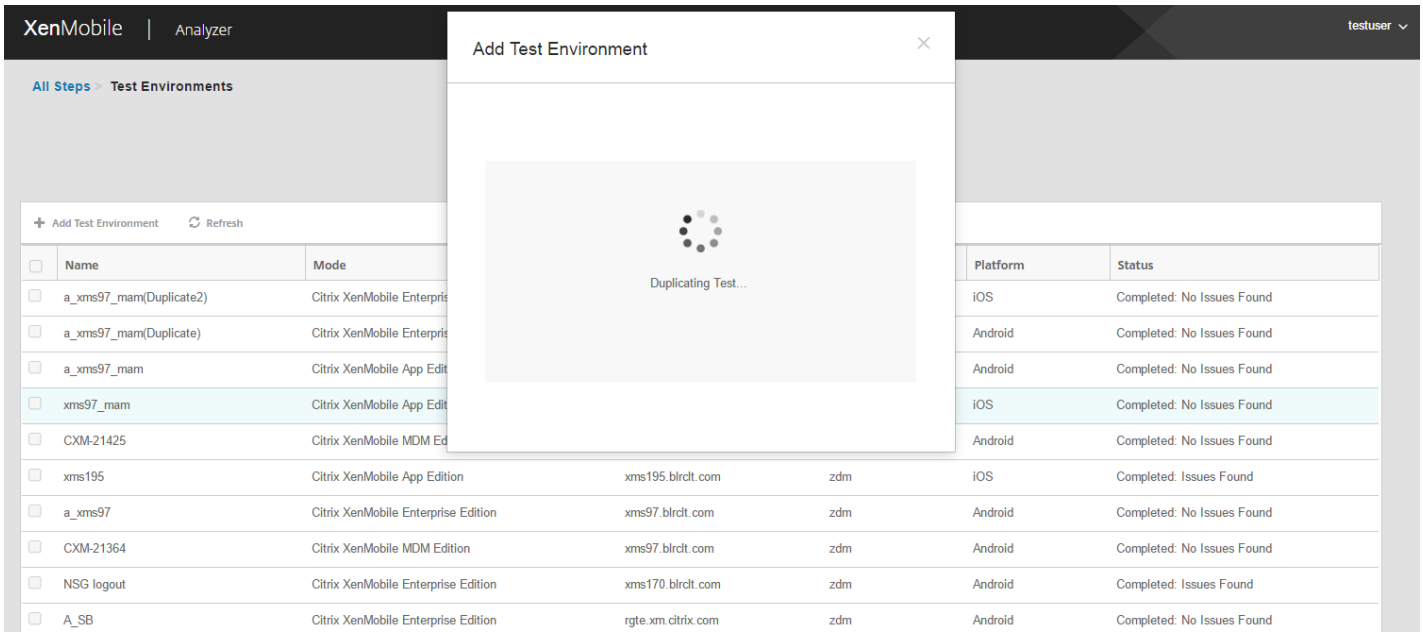


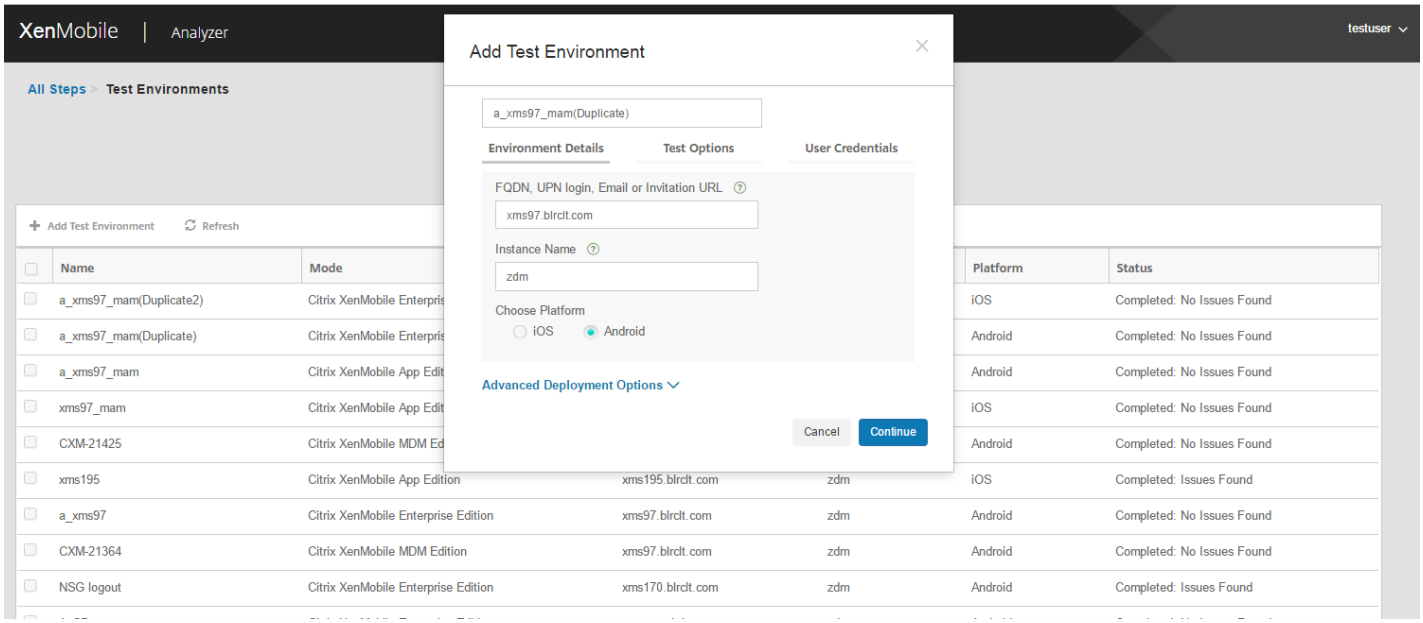


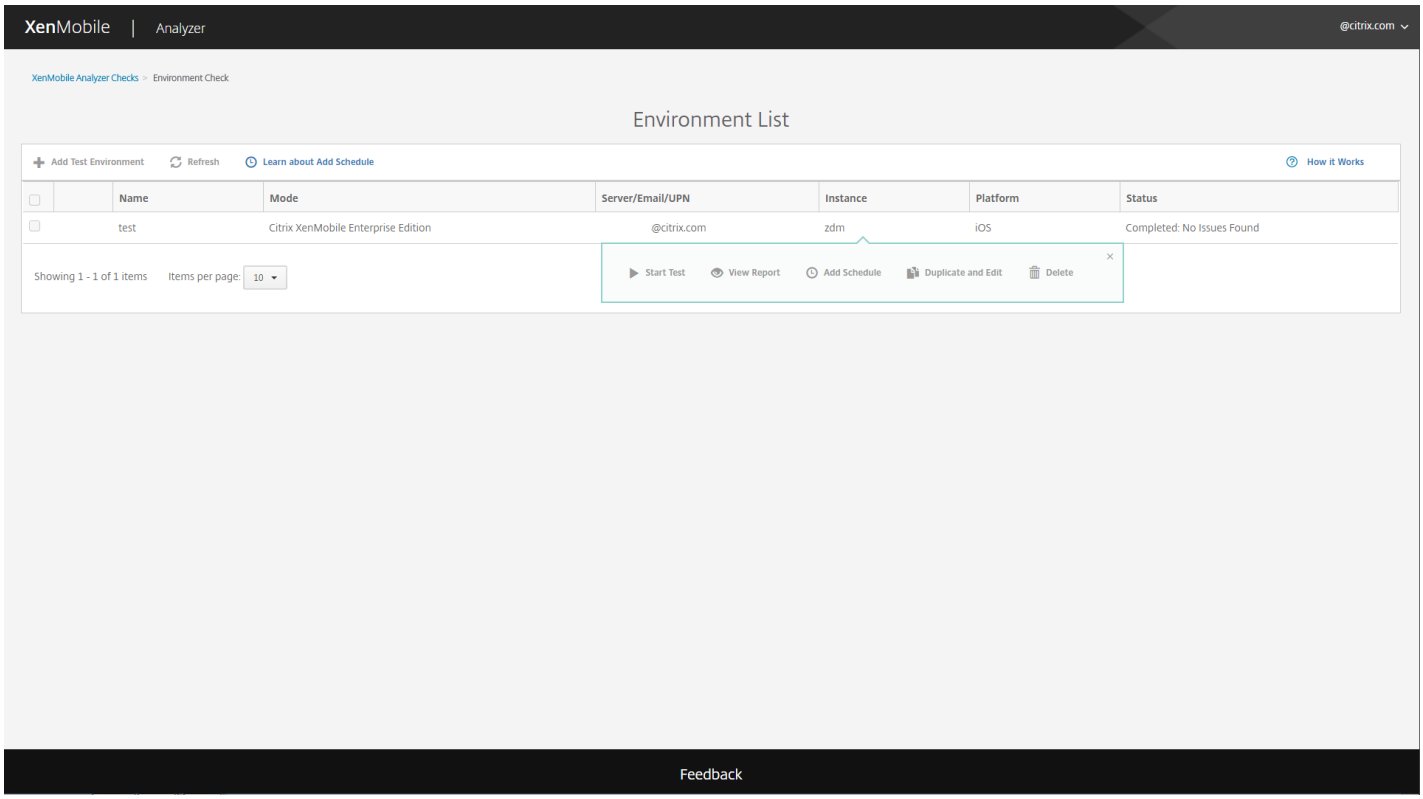


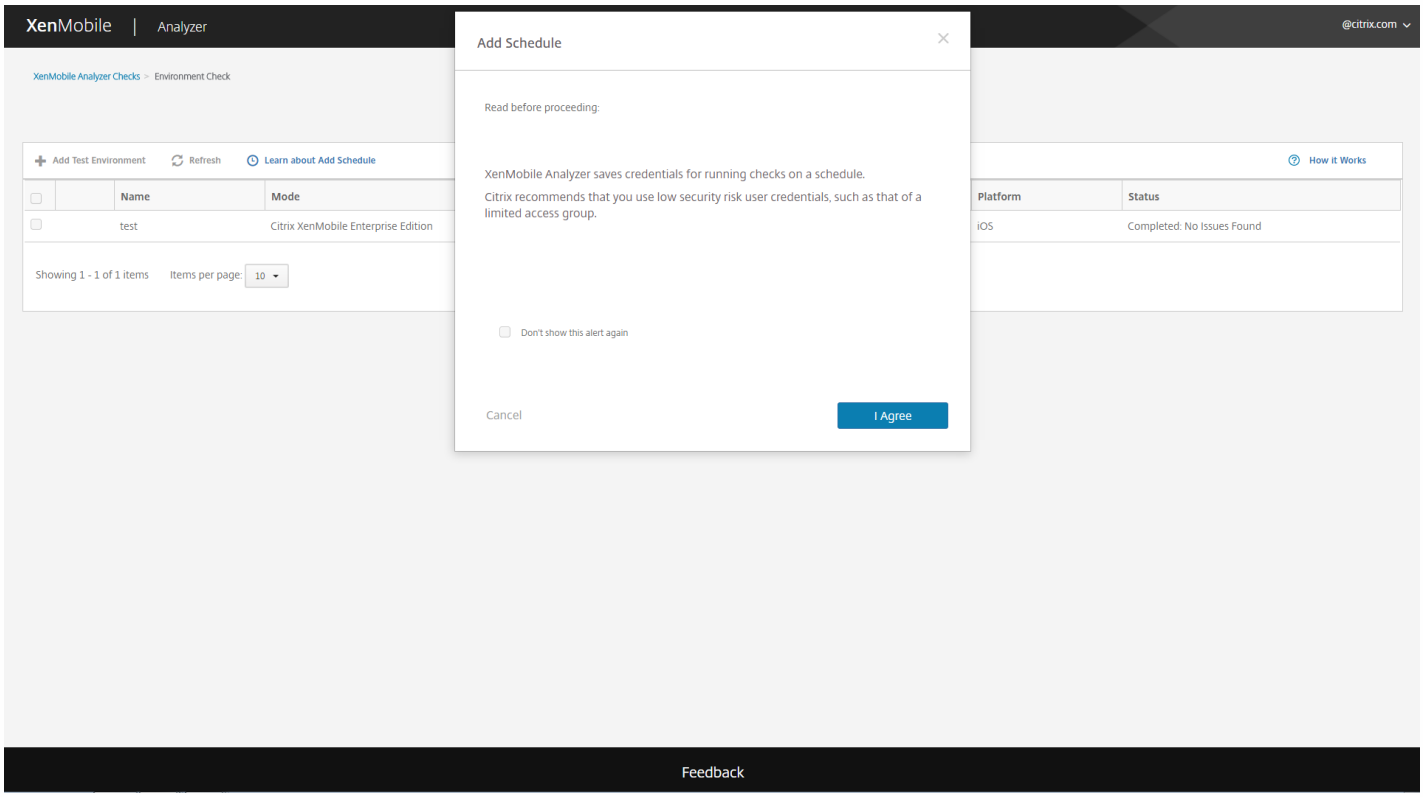


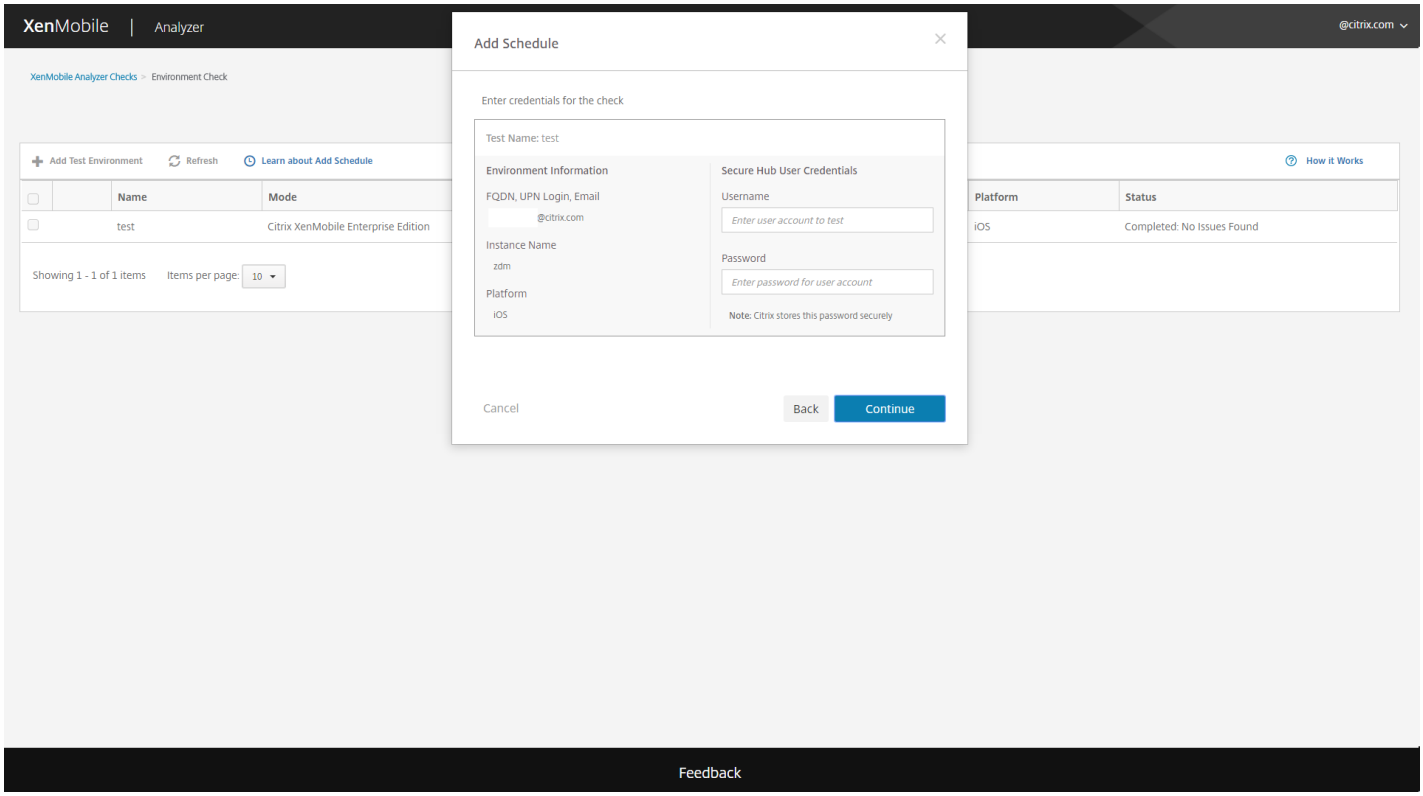


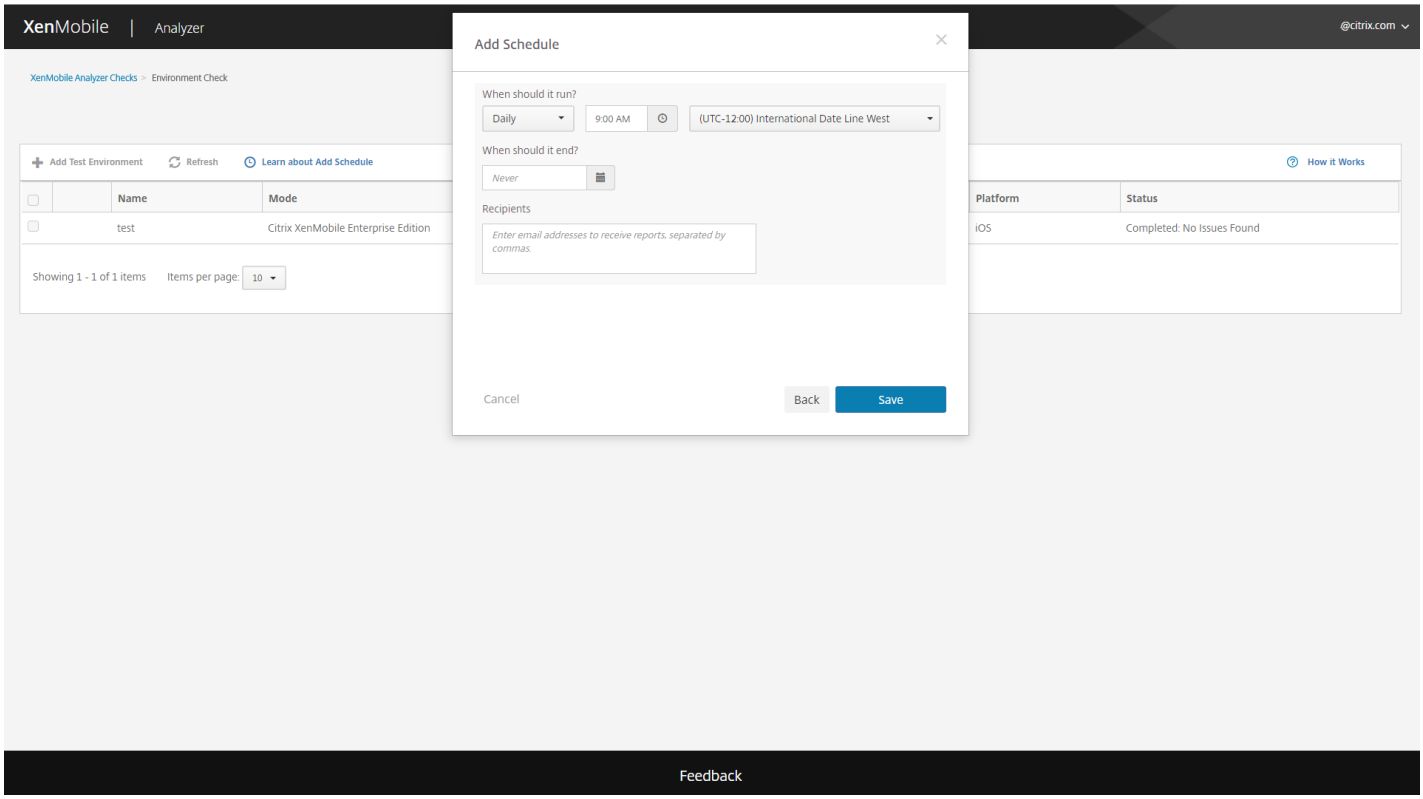


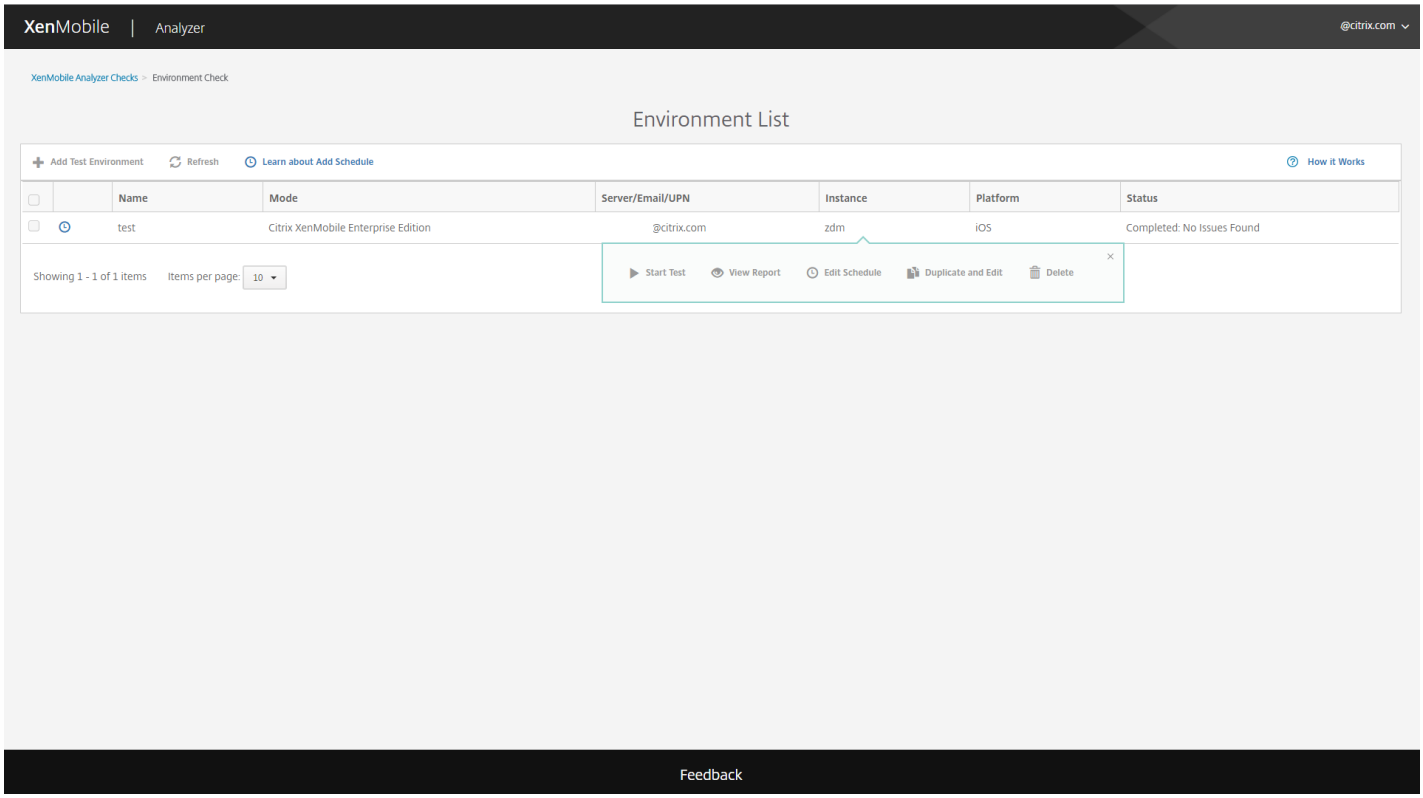


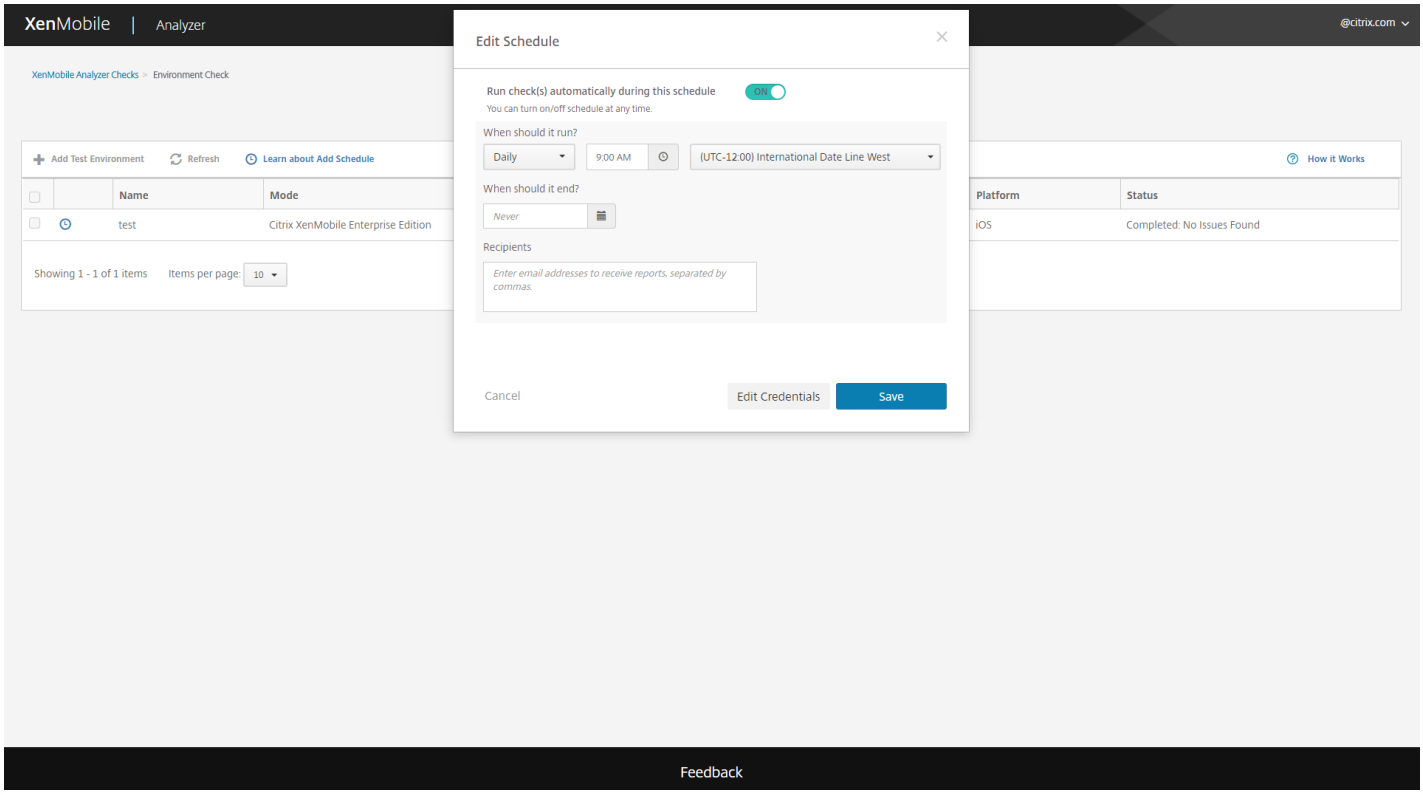


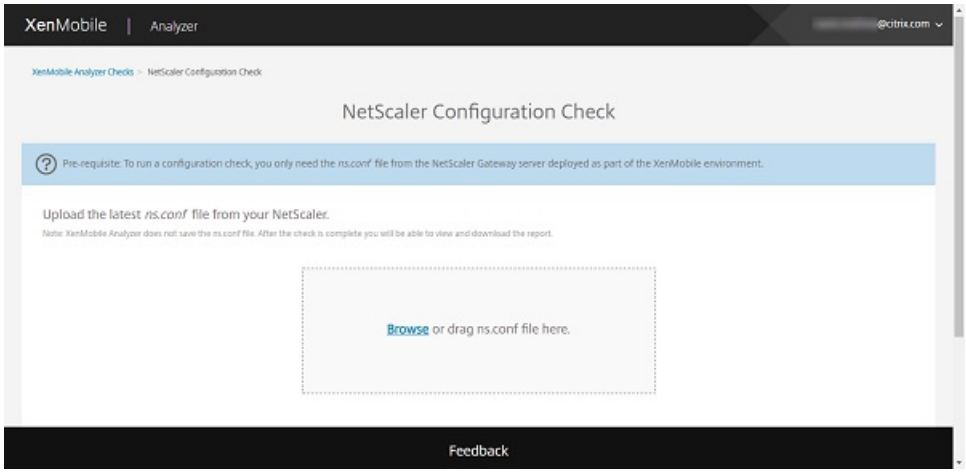


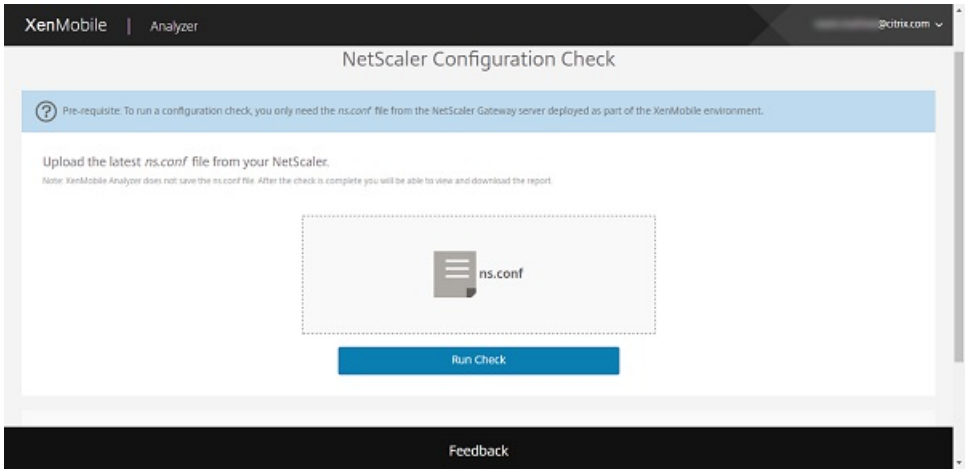




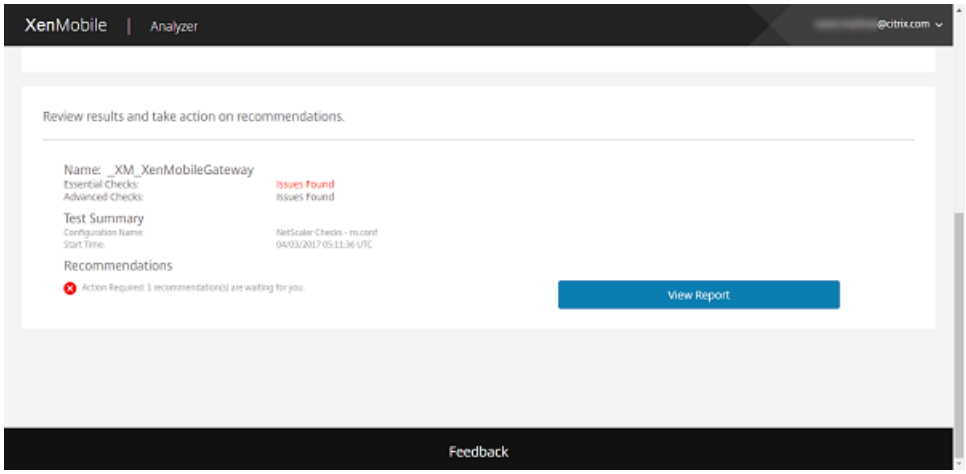


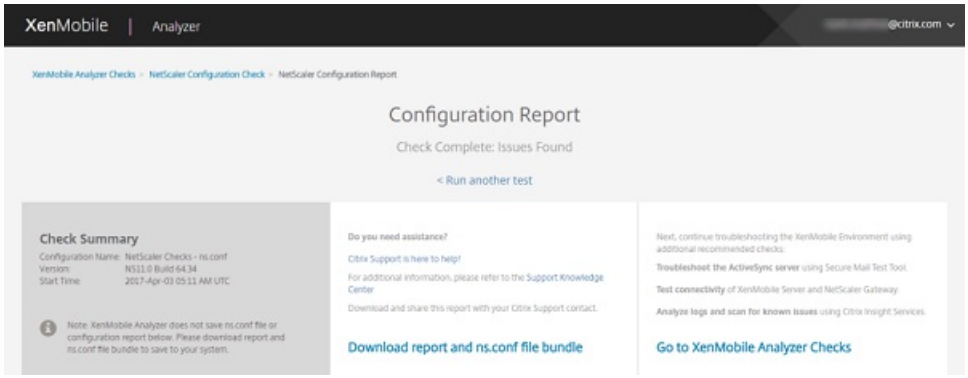


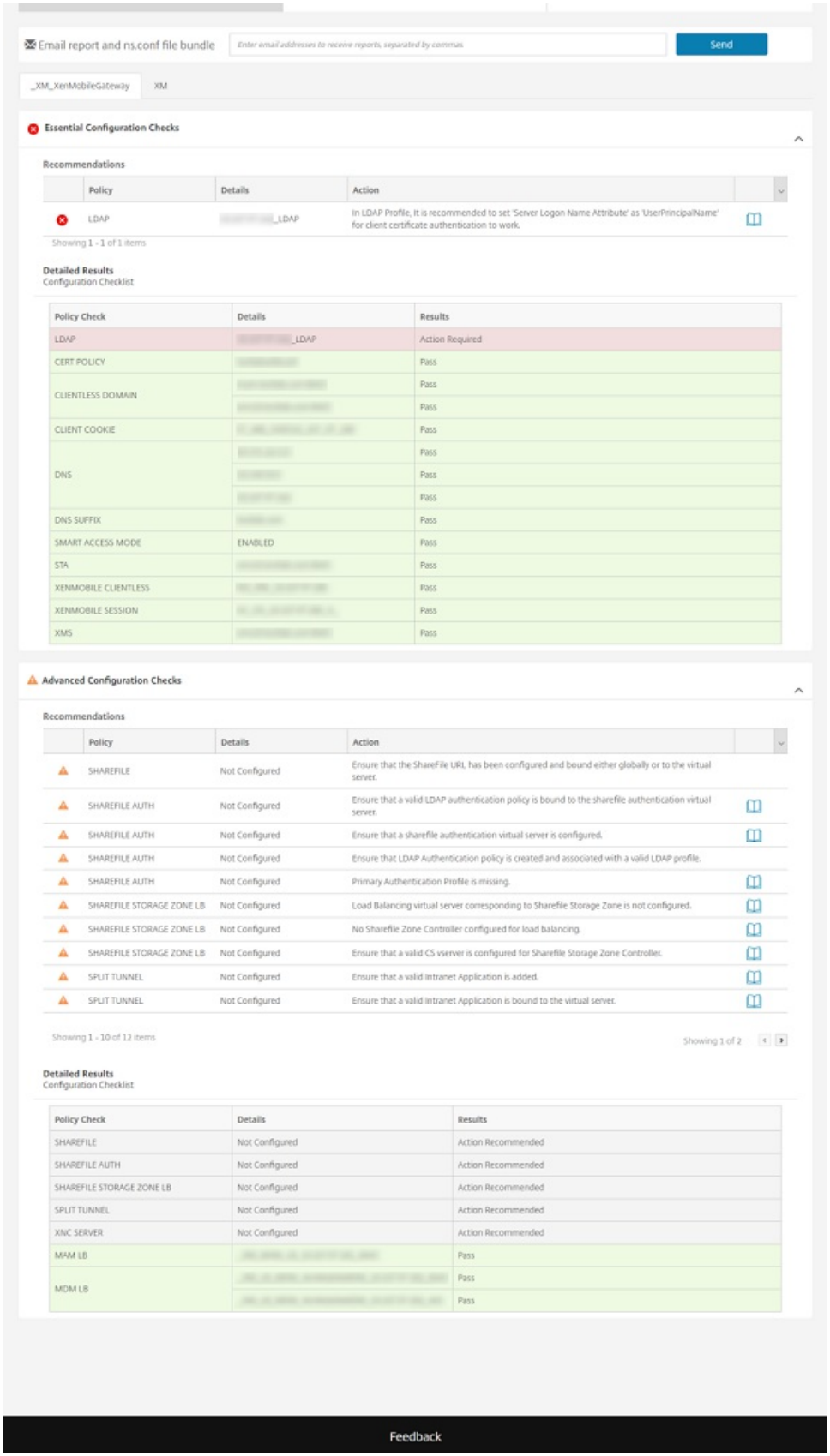




-
-

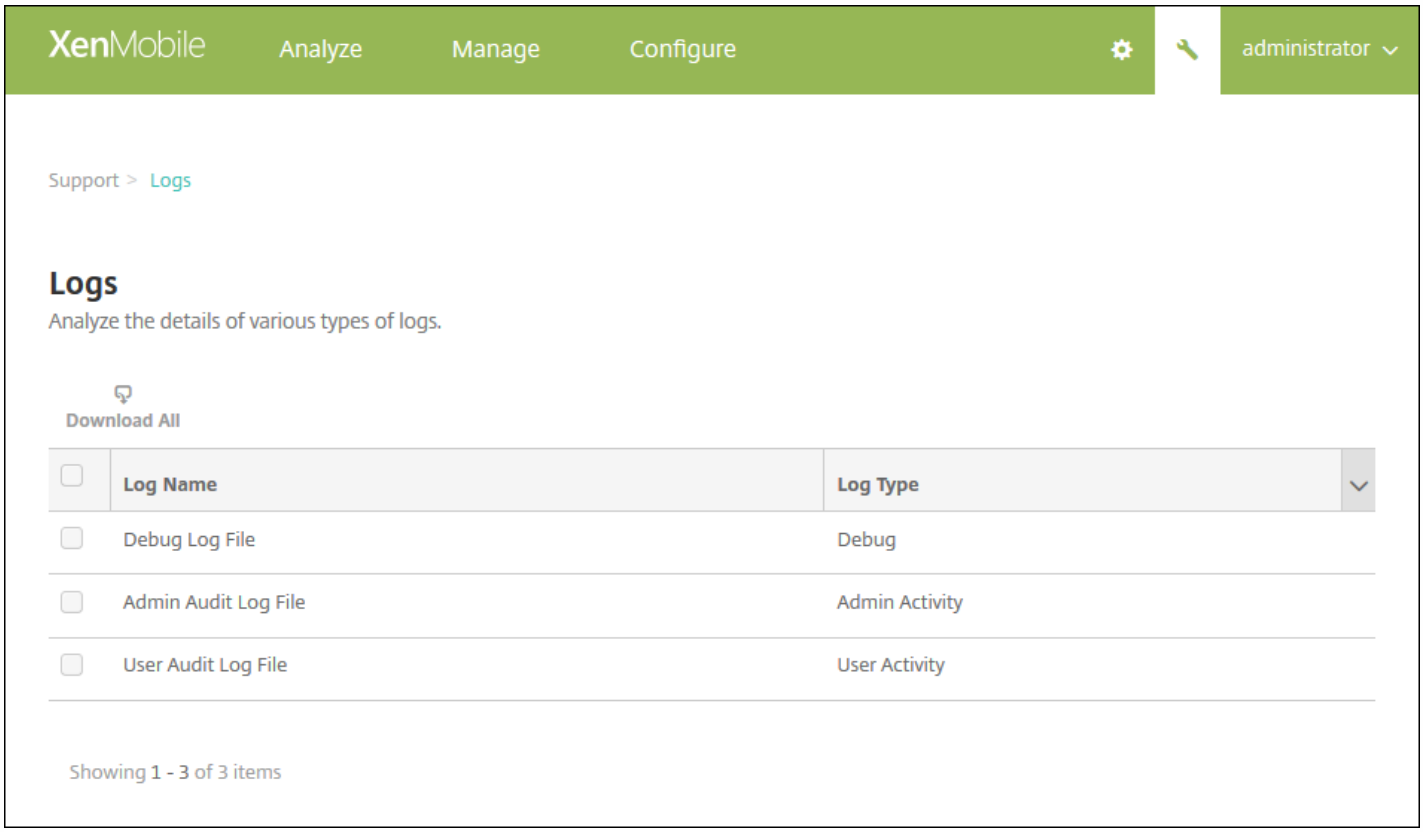


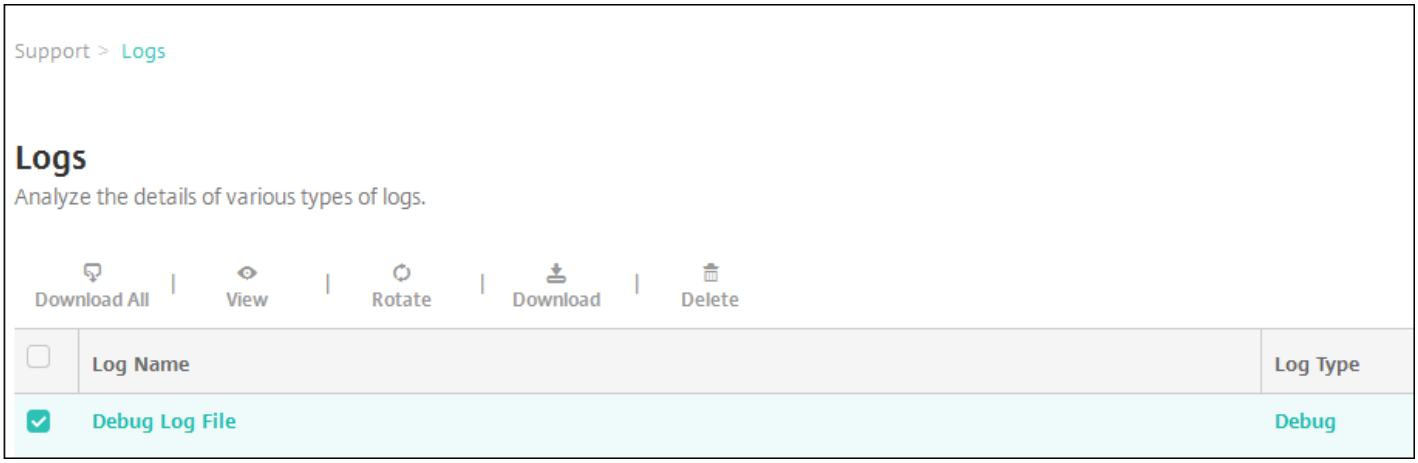




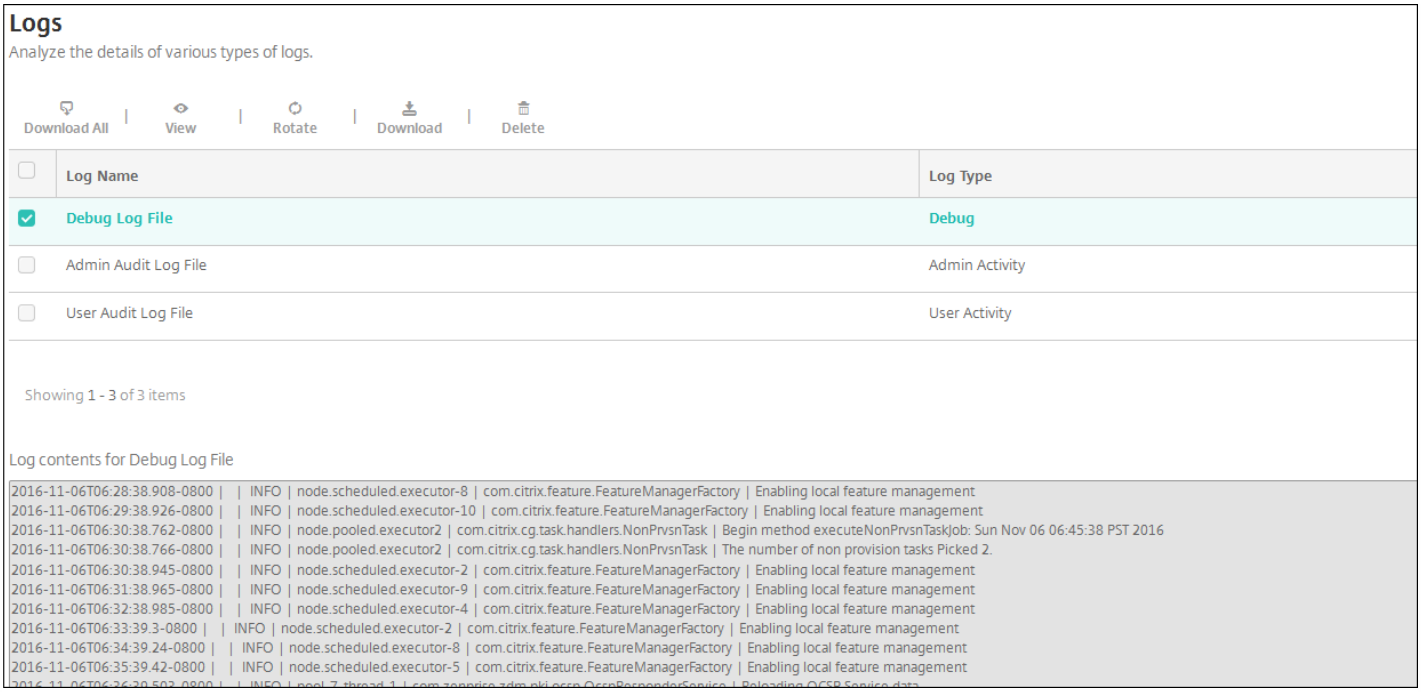
-
-
-
-

-
-
-
-
-

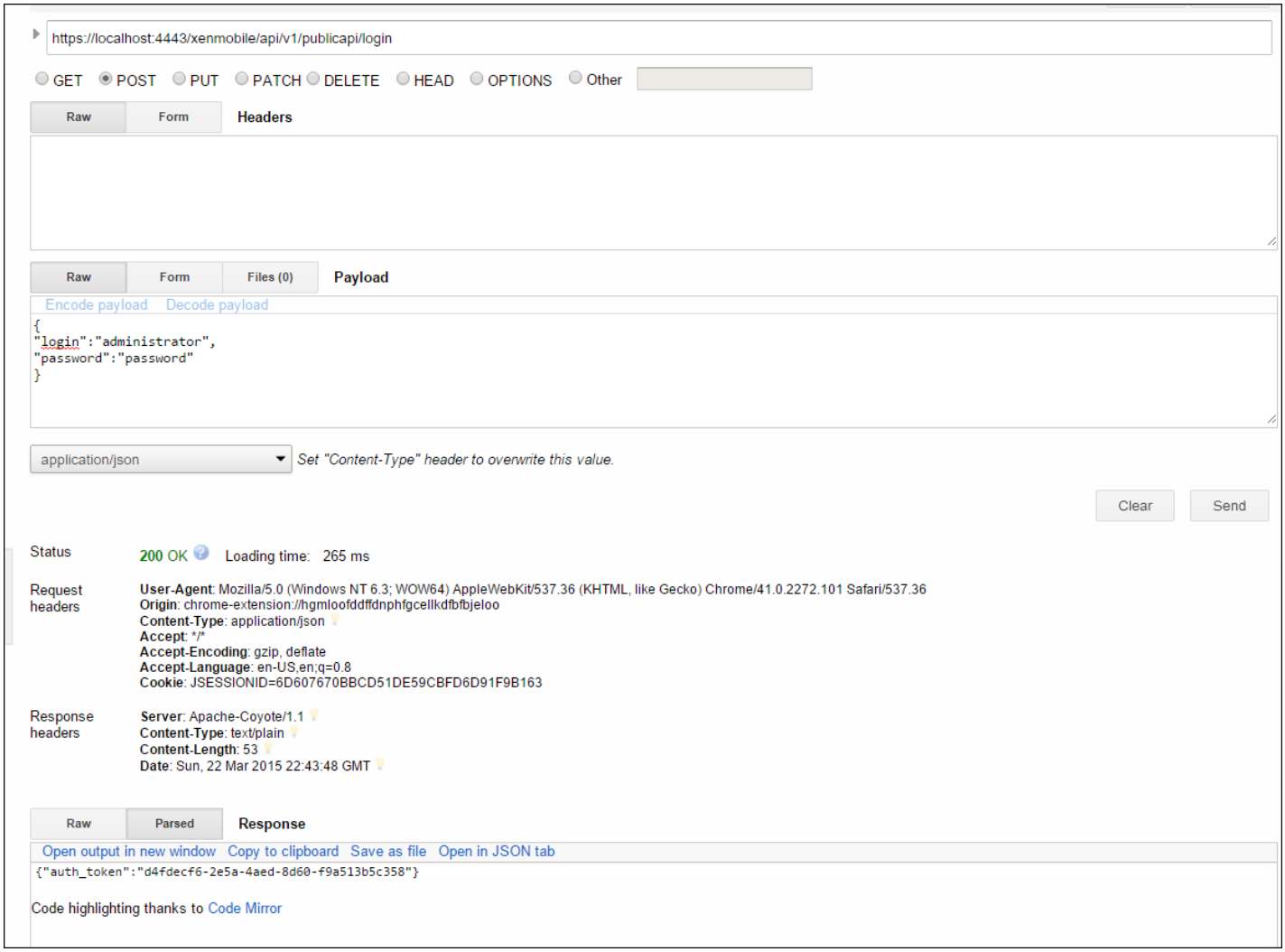




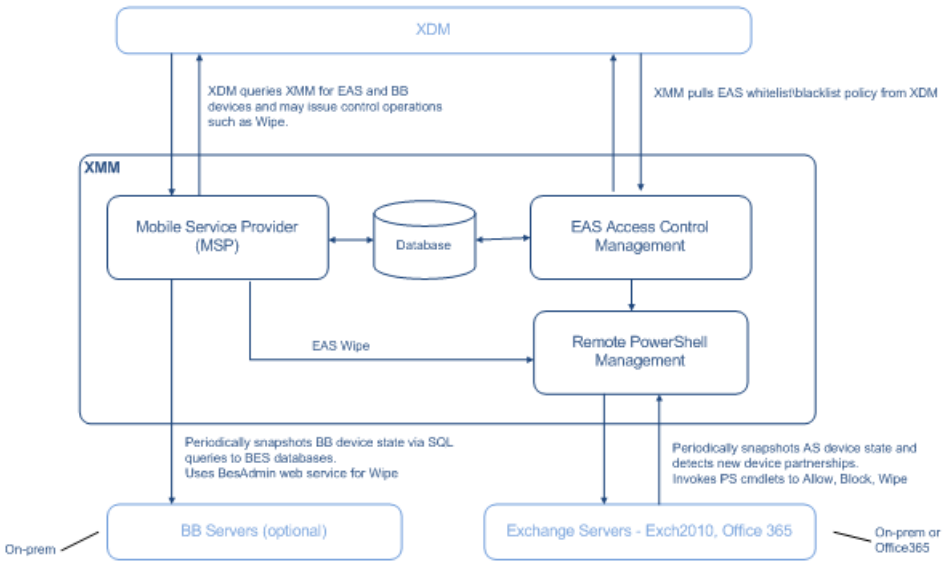
-
-
-
-
-
-
-



-
-



-
-
-
-
-
-
-



-
-
-

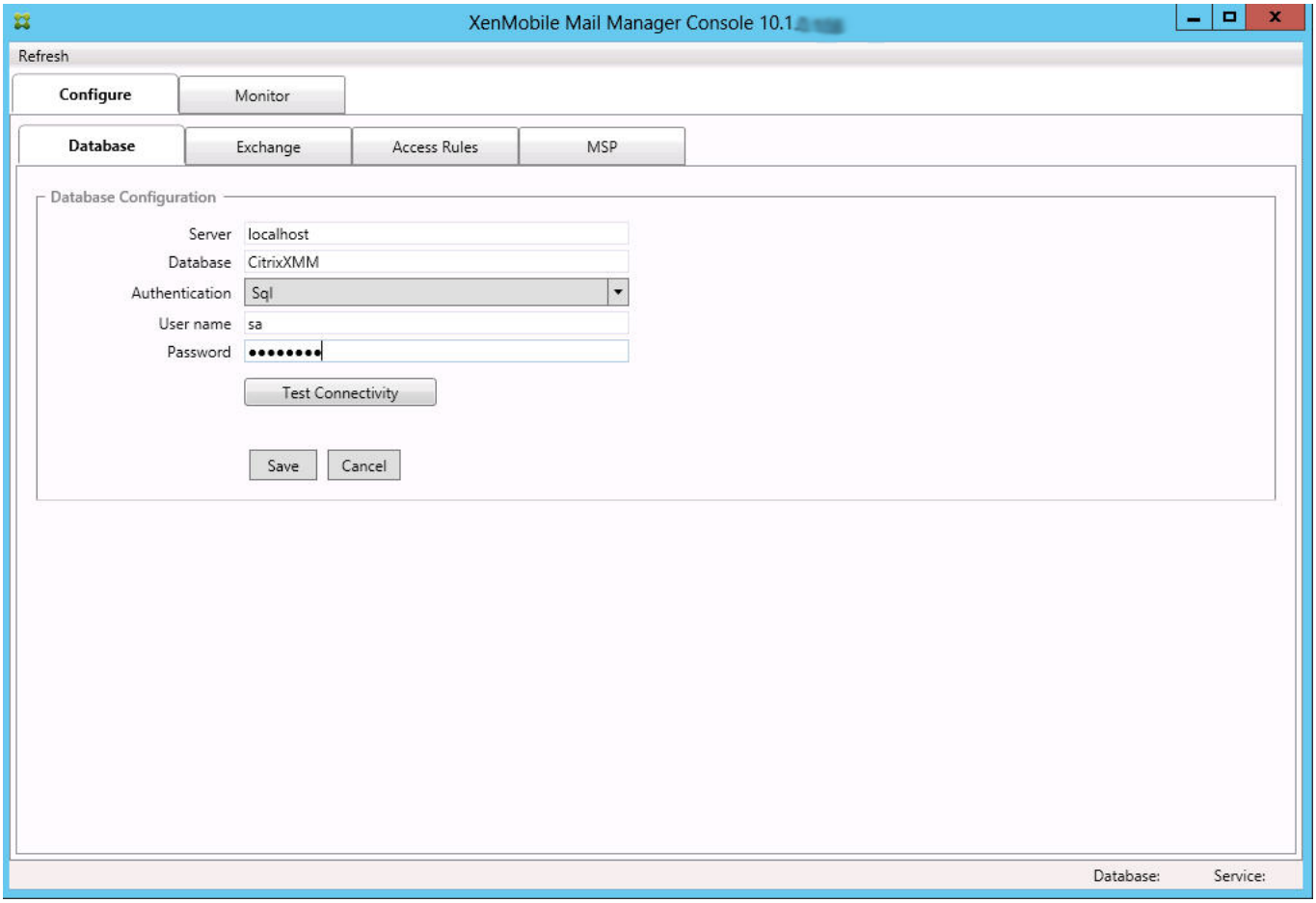
- **Para Exchange Server 2010 SP2:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics

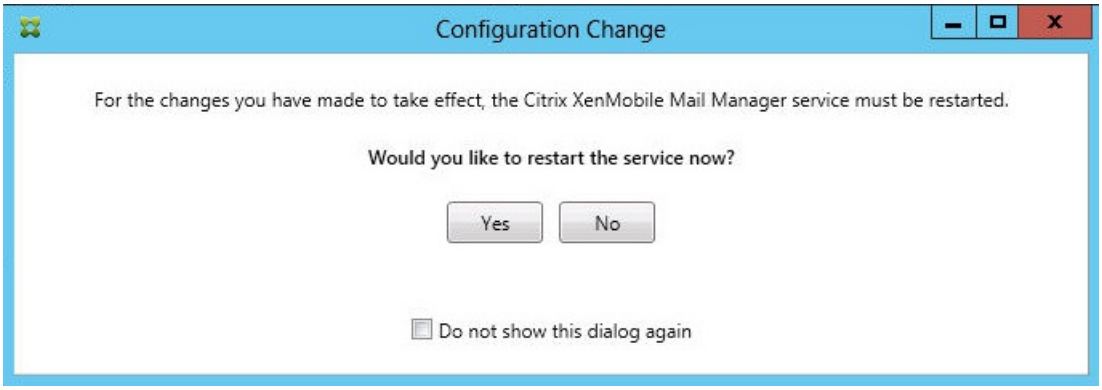
    - Clear-ActiveSyncDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
- **Para el servidor Exchange Server 2013 y Exchange Server 2016:**
    - Get-CASMailbox
    - Set-CASMailbox
    - Get-Mailbox
    - Get-MobileDevice
    - Get-MobileDeviceStatistics
    - Clear-MobileDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment

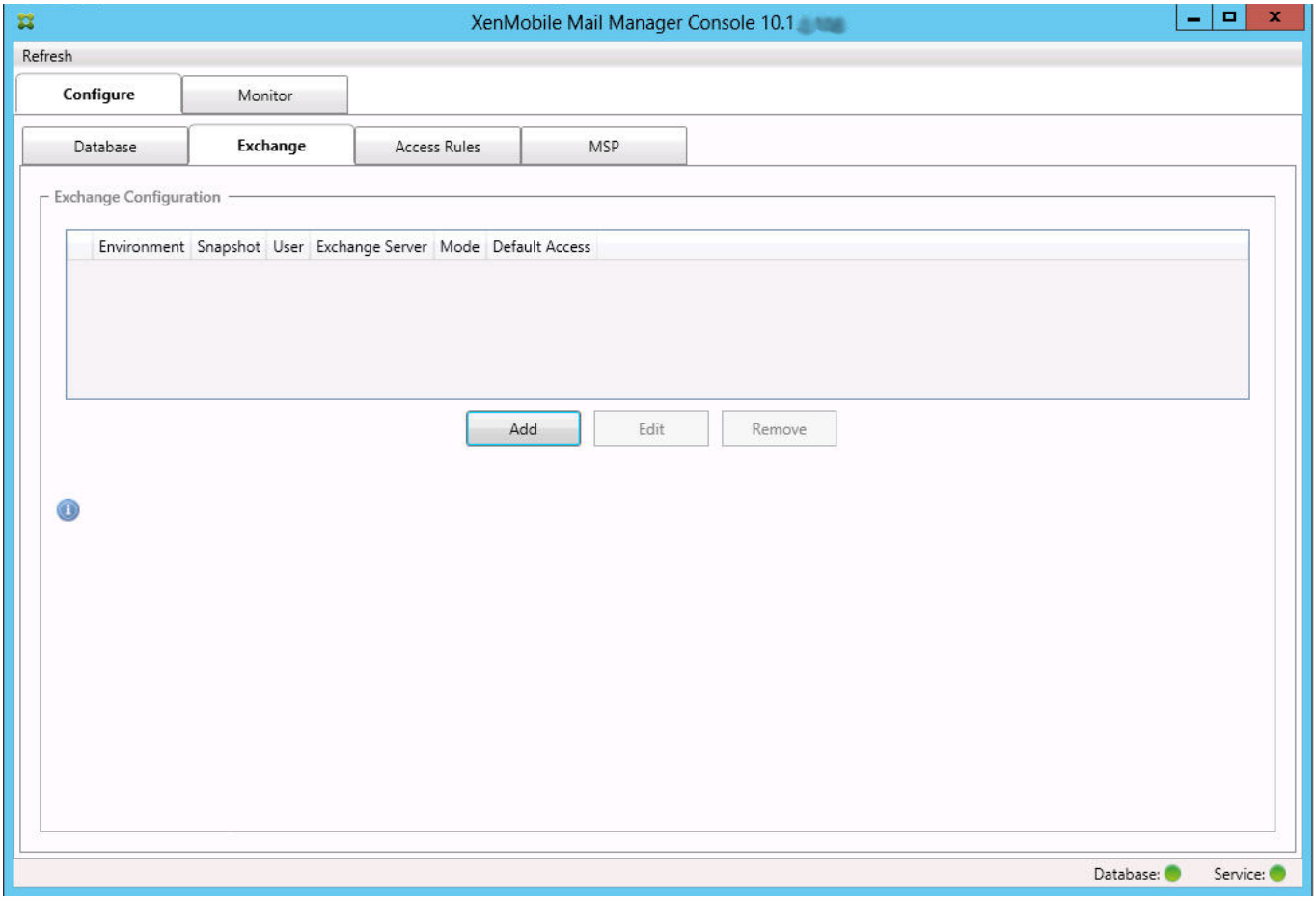
- Si XenMobile Mail Manager está configurado para ver todo el bosque, se debe haber concedido permiso para ejecutar: Set-AdServerSettings -ViewEntireForest $true.
- Las credenciales suministradas deben contar con derecho a conectarse al servidor Exchange mediante el shell remoto. De forma predeterminada, 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 este post de blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands, se puede usar Set-PSSessionConfiguration 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 alcanza el límite de conexiones, XenMobile Mail Manager no se puede conectar 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.

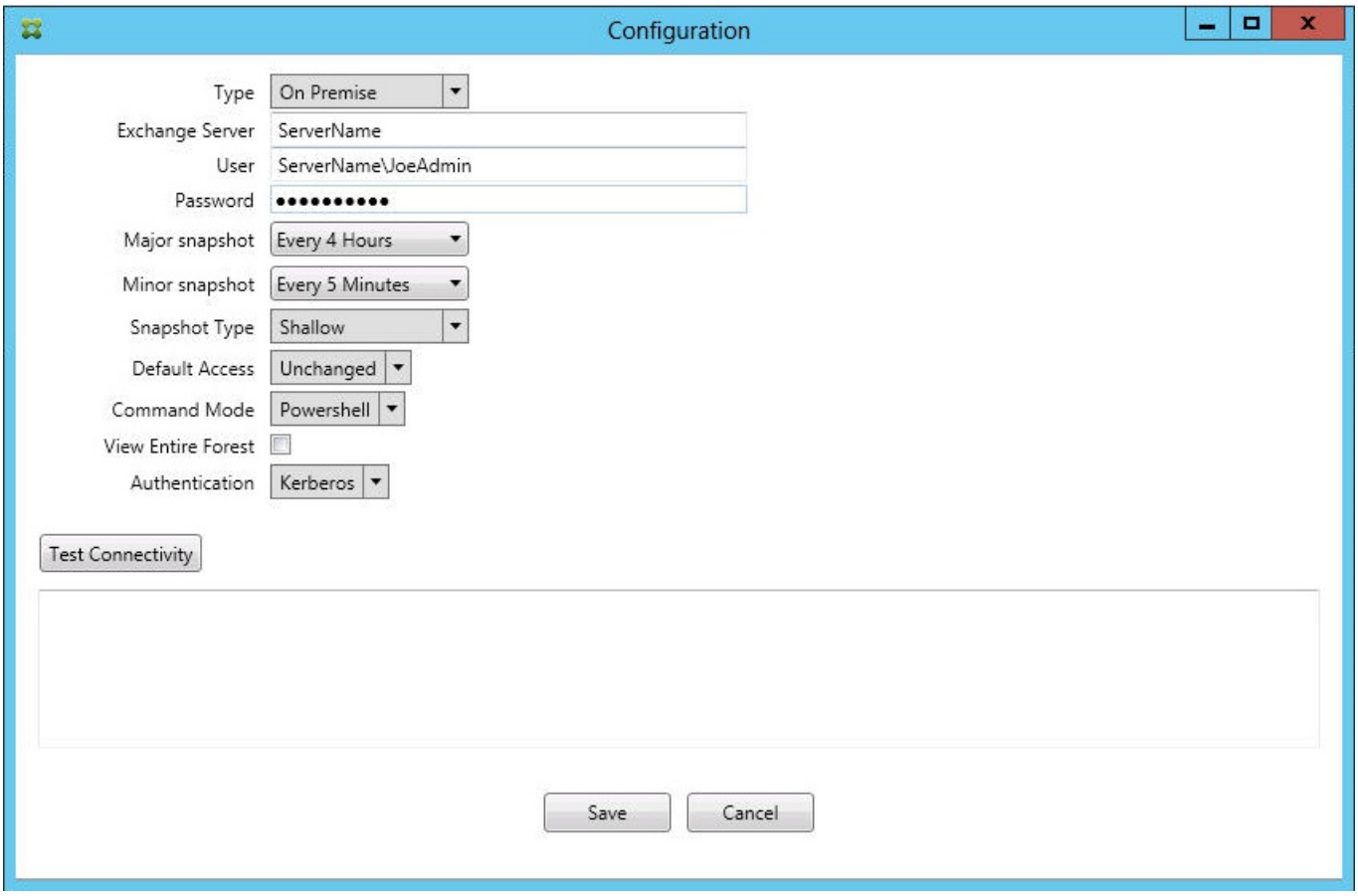
- **Permisos**. Las credenciales especificadas en la interfaz de usuario de la configuración de Exchange deben permitir la conexión a Office 365 y deben tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange:
    - Get-CASMailbox
    - Set-CASMailbox
    - Get-Mailbox
    - Get-MobileDevice
    - Get-MobileDeviceStatistics
    - Clear-MobileDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
- **Privilegios** 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.
- **Directivas de limitaciones**. 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 alcanza el límite de conexiones, XenMobile Mail Manager no se puede conectar 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.

-
-

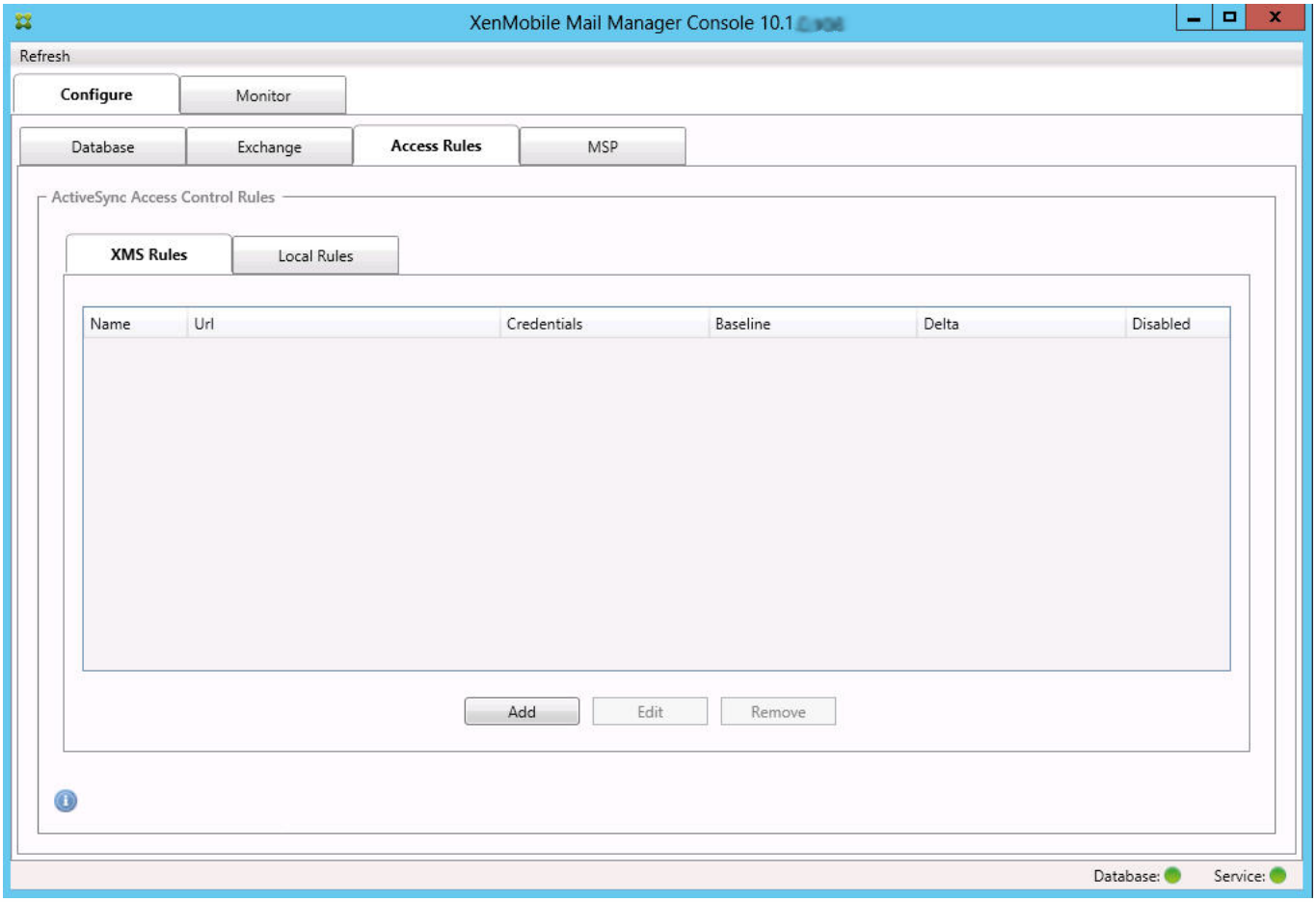


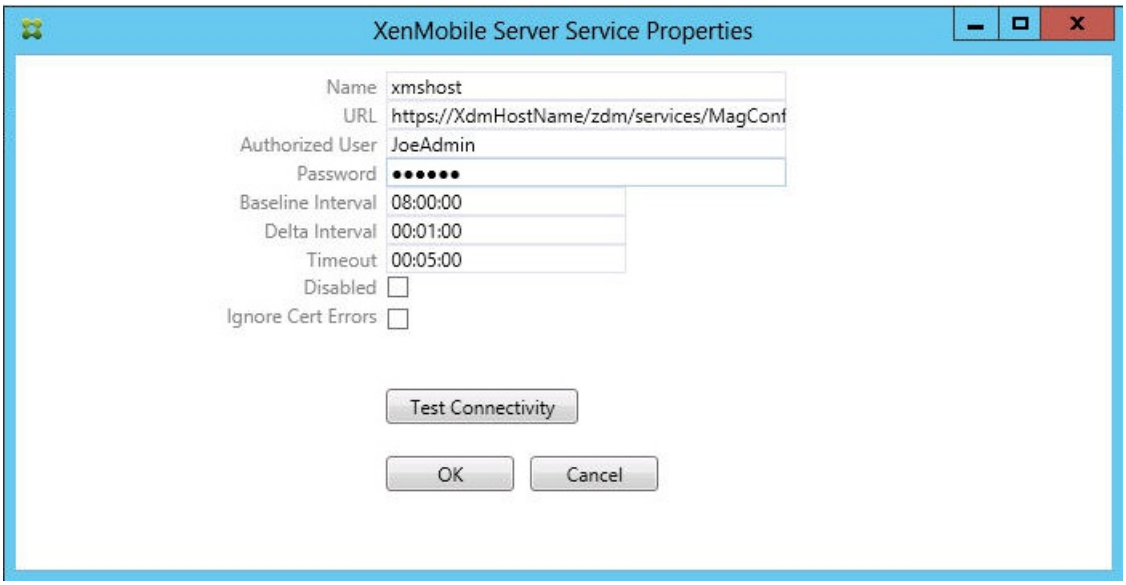


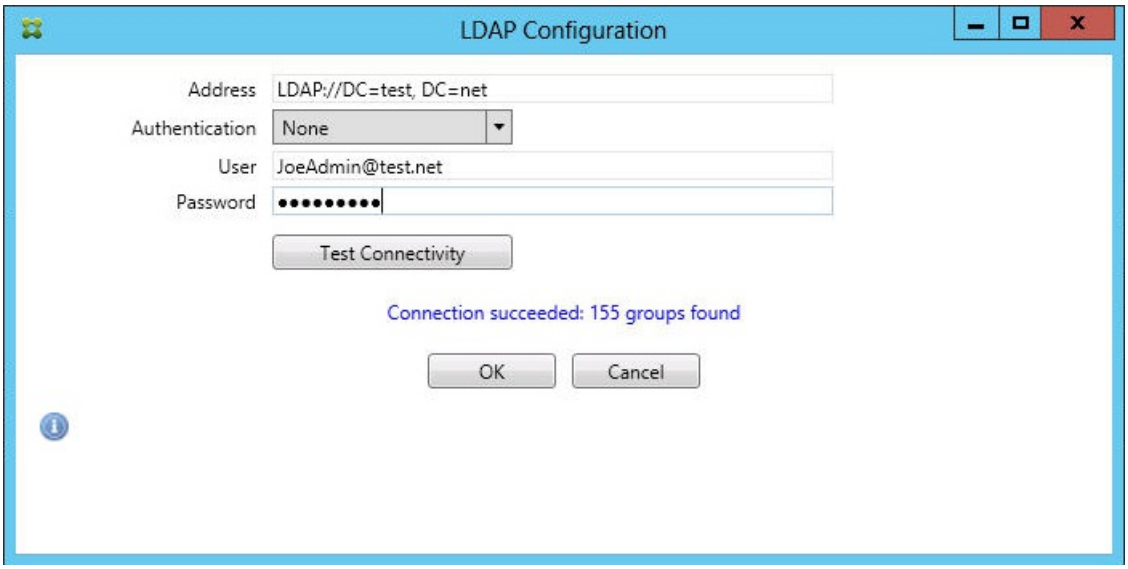


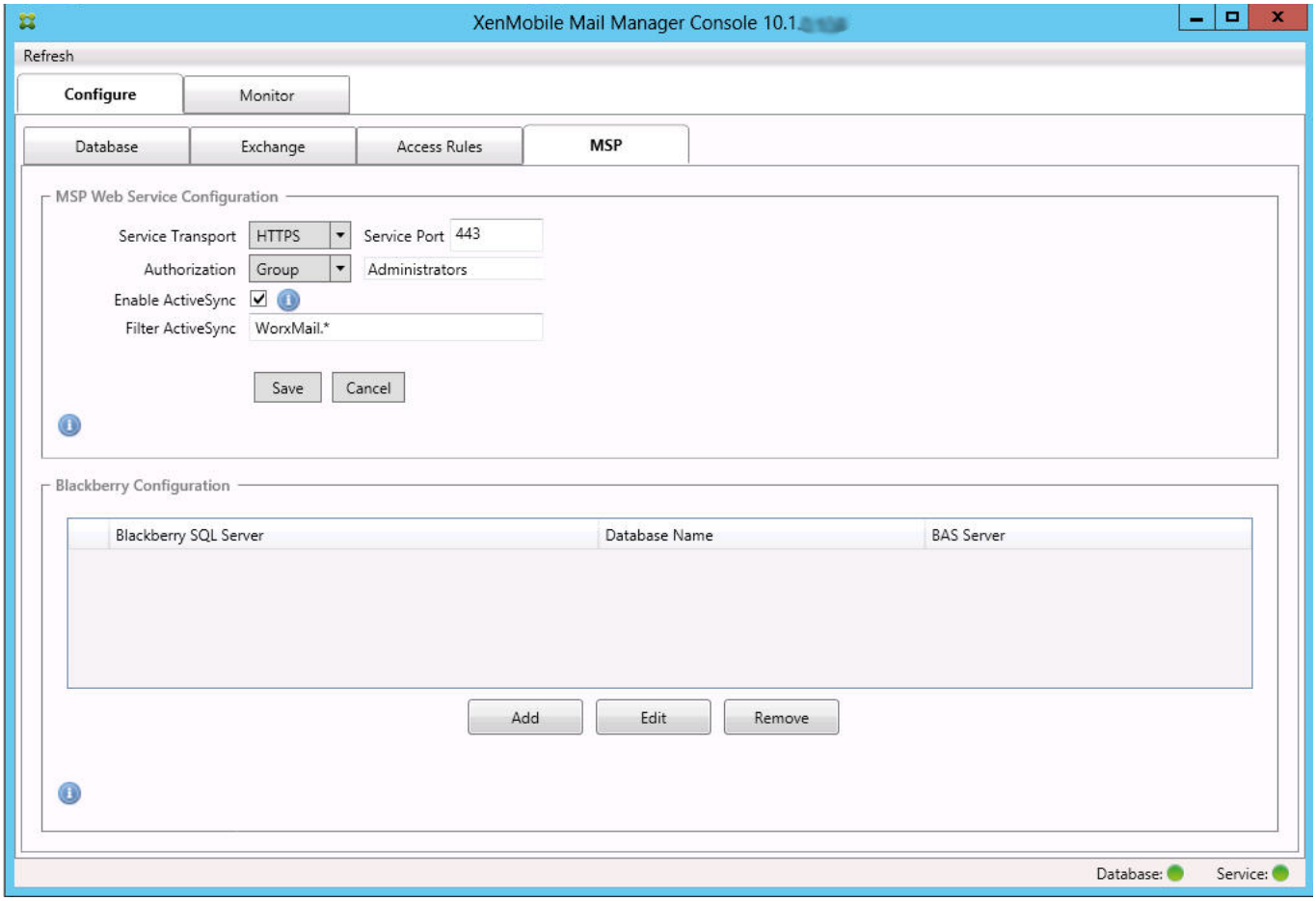


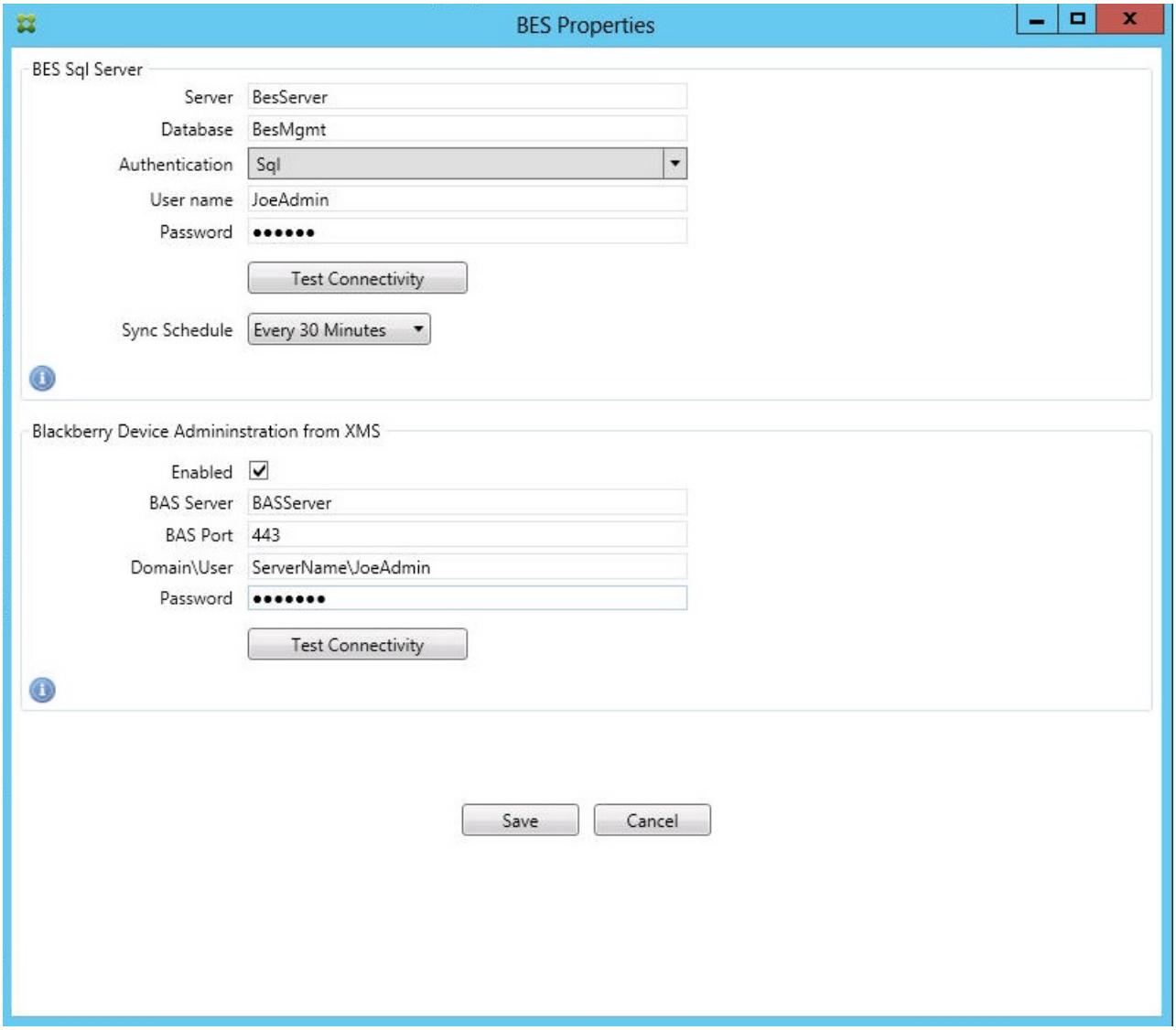
-
-

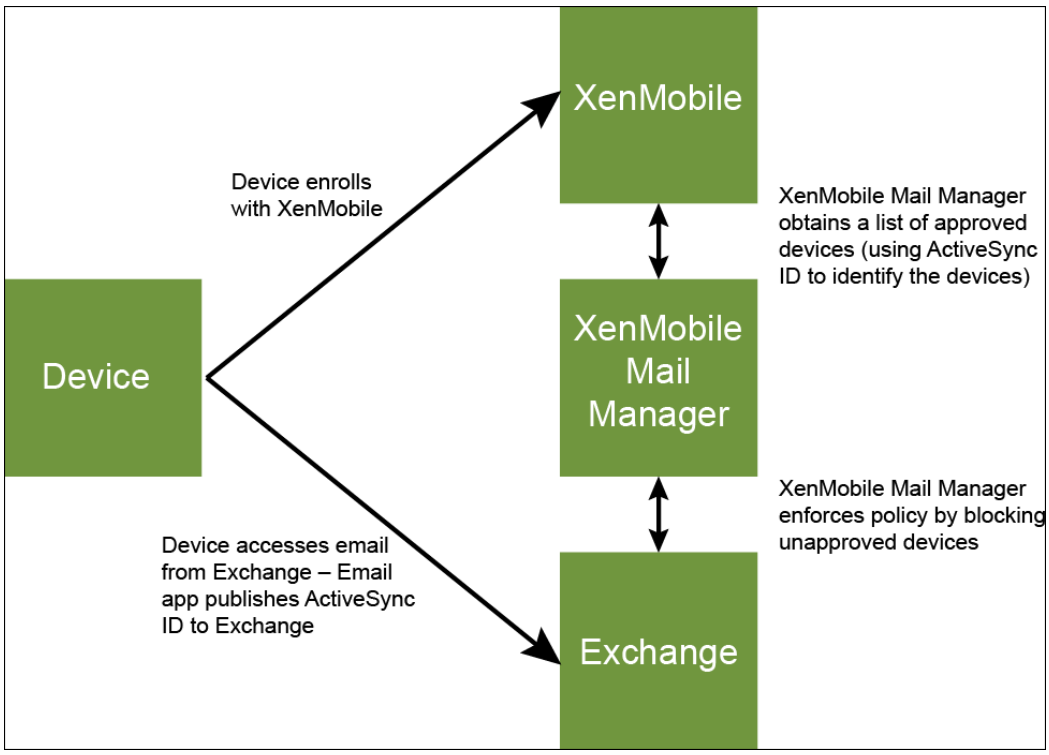










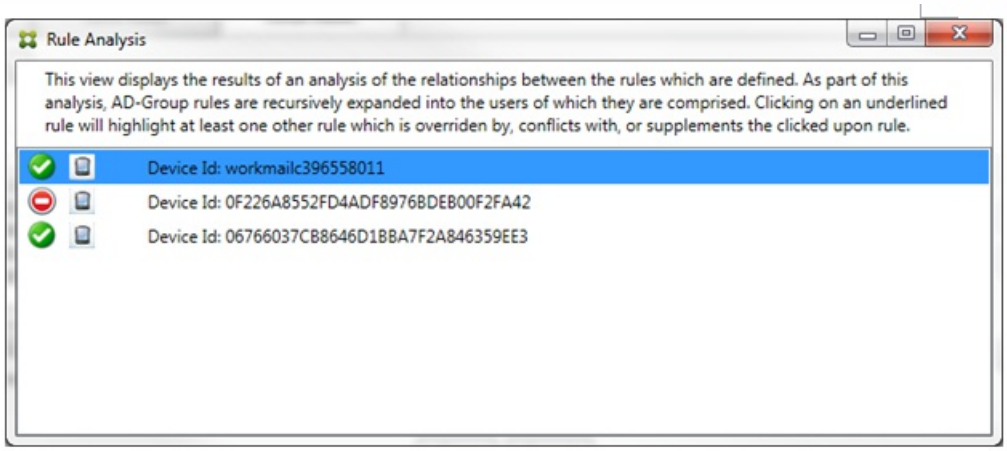


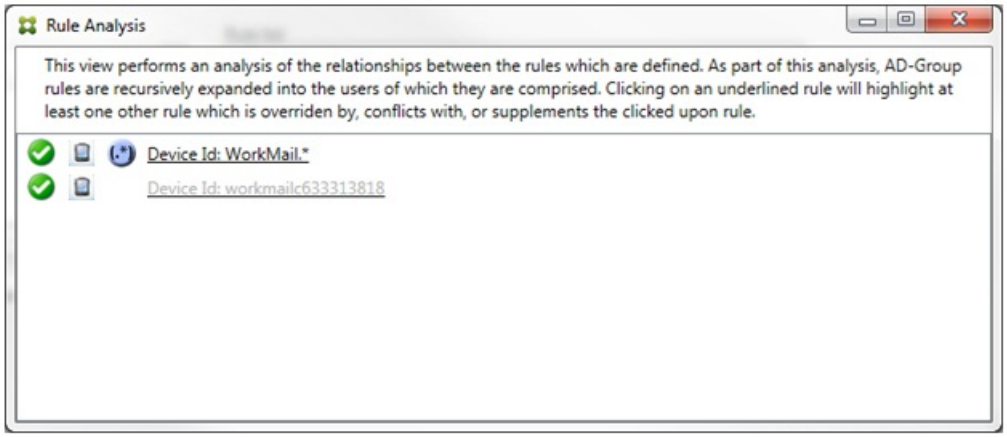
-
-

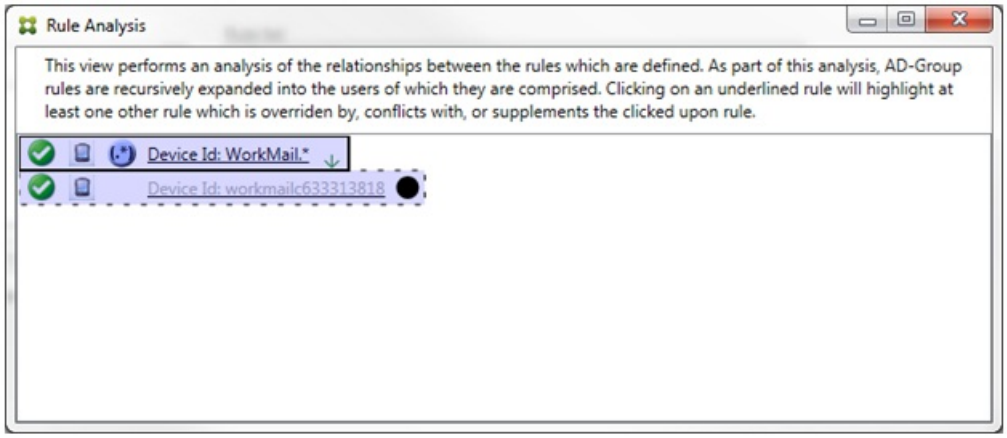
-
-
-
-

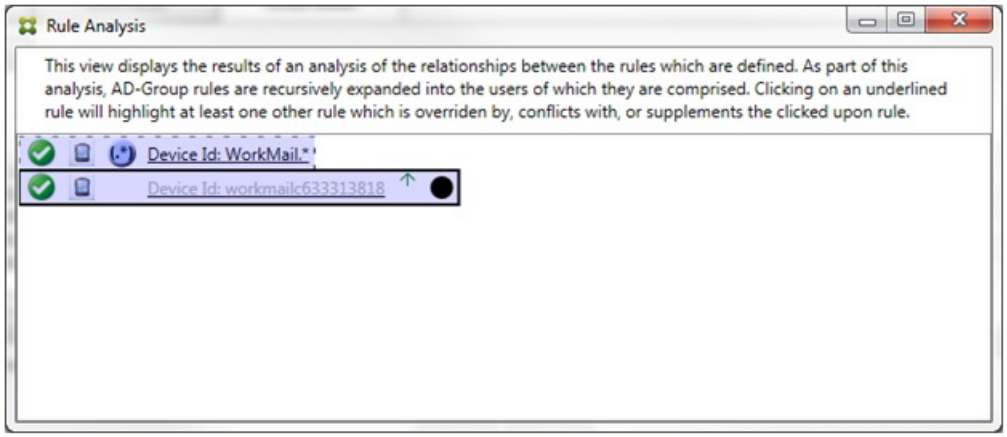
-
-
-
-
-
-

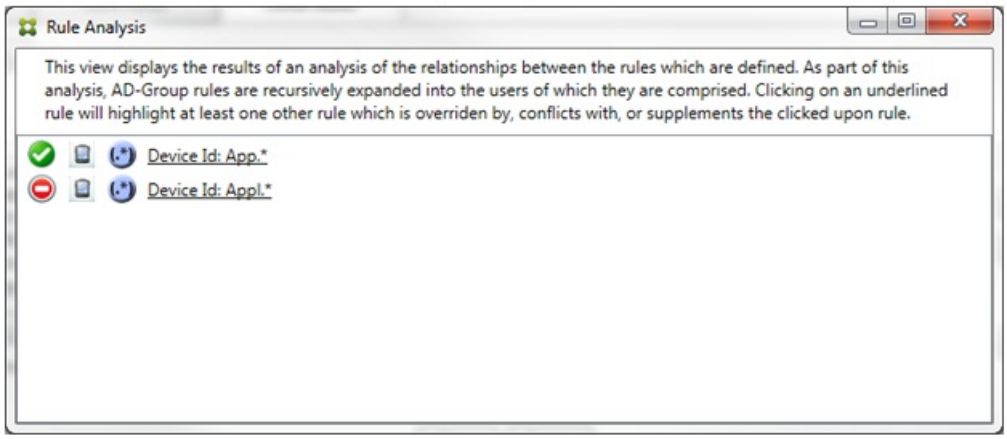
-
-
-
-
-

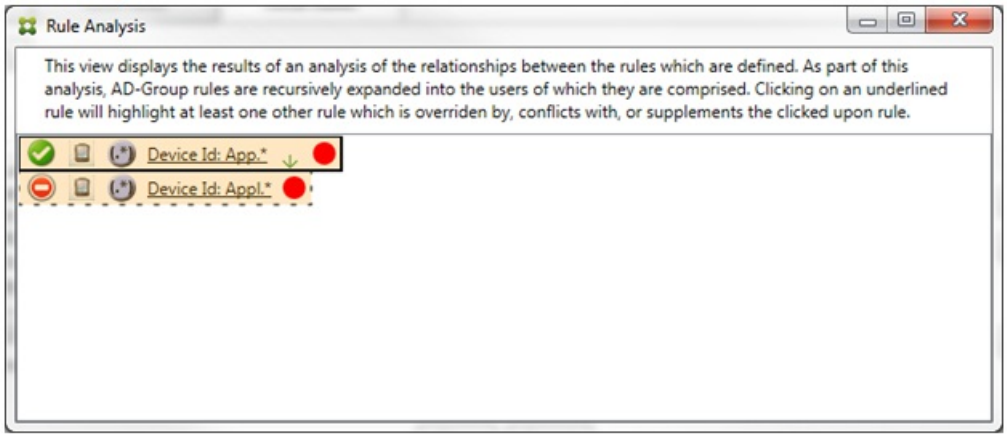


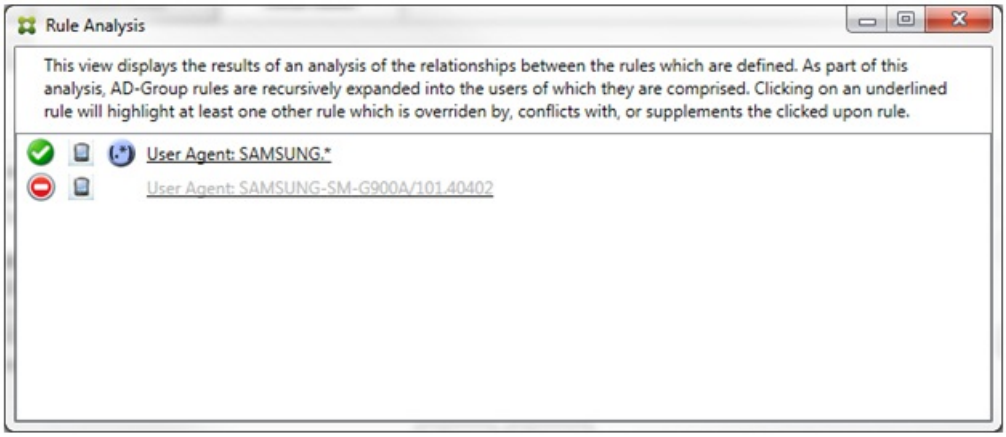


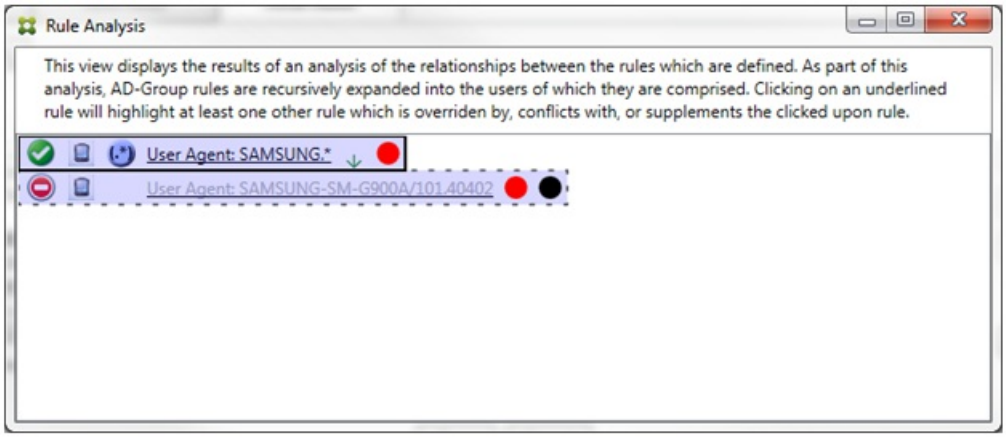


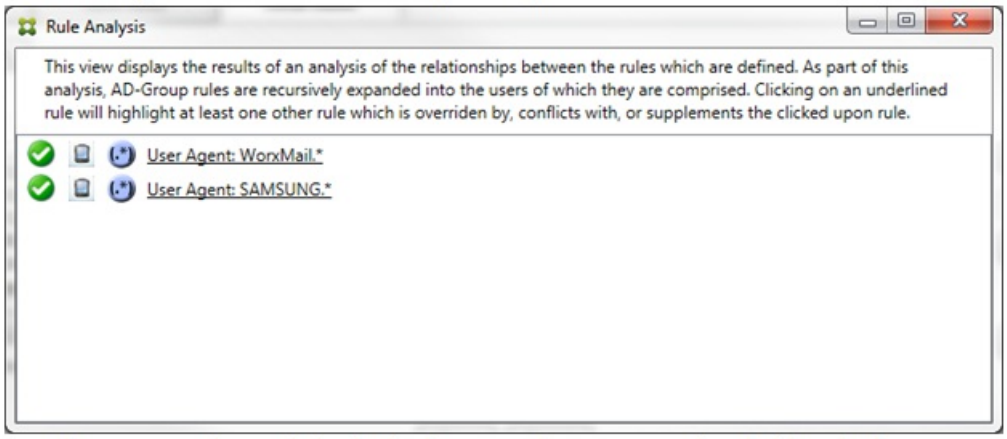


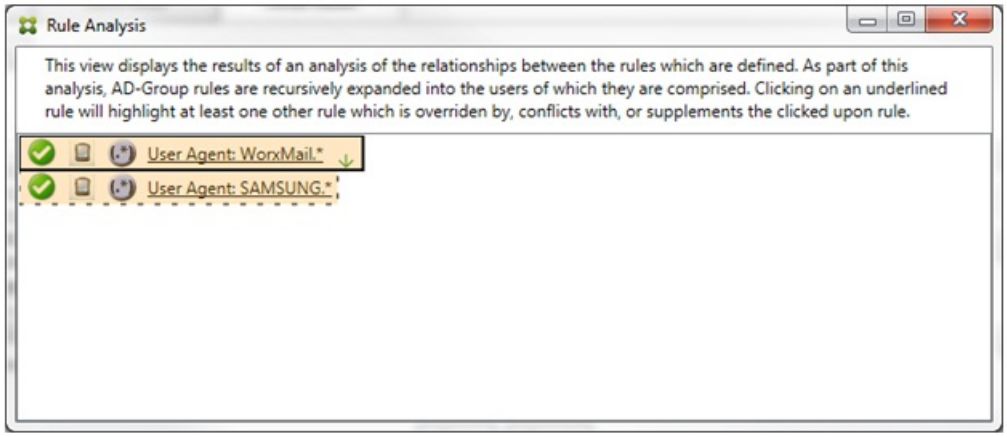


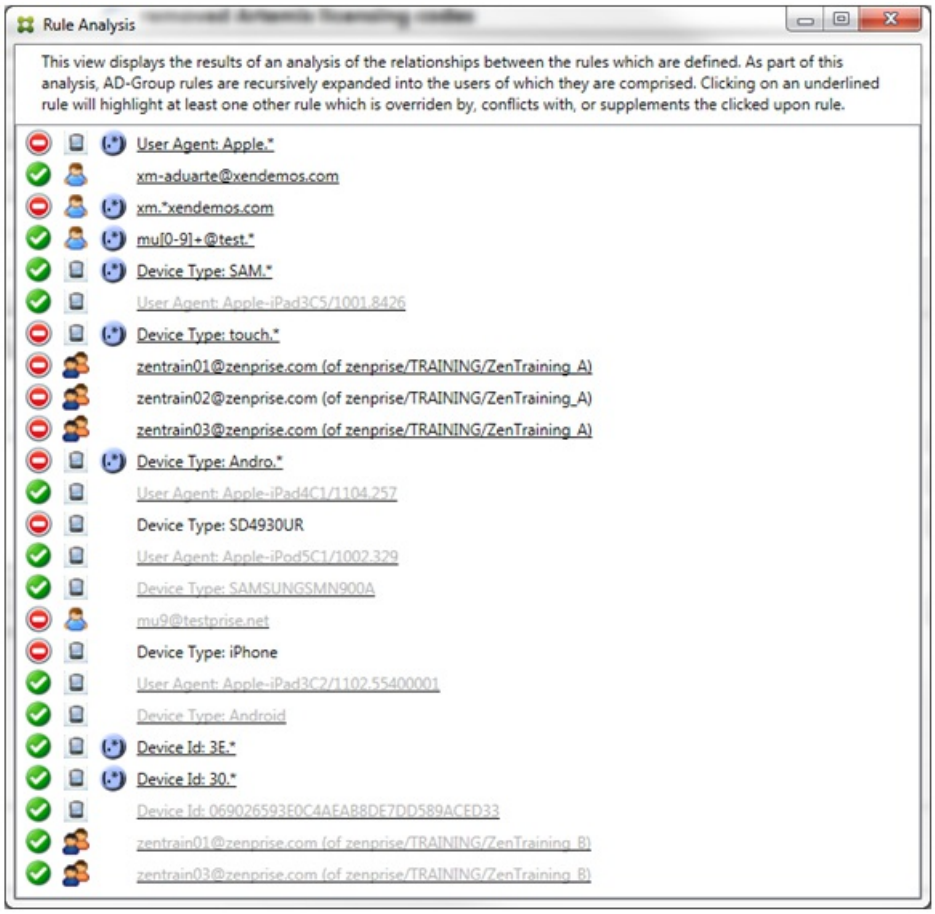


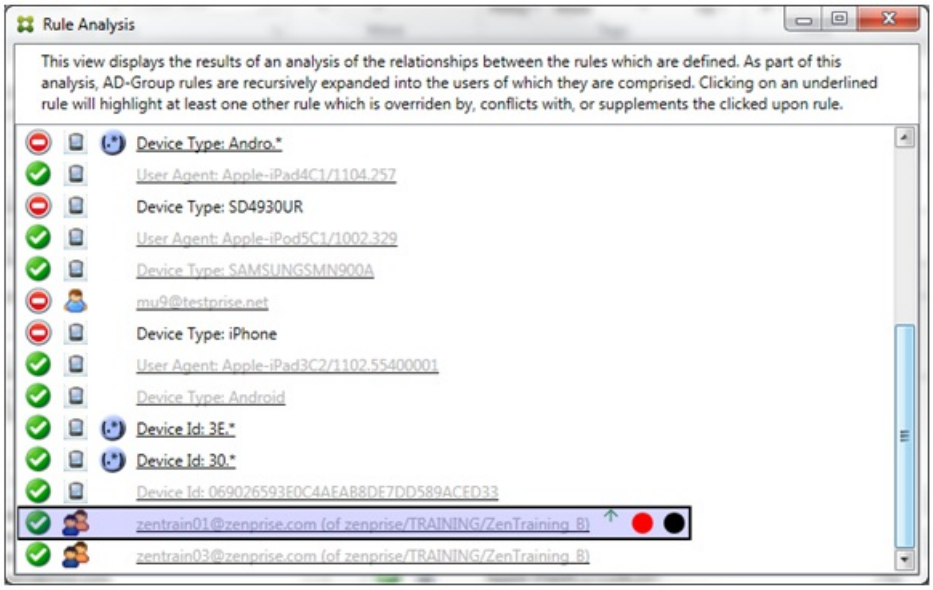




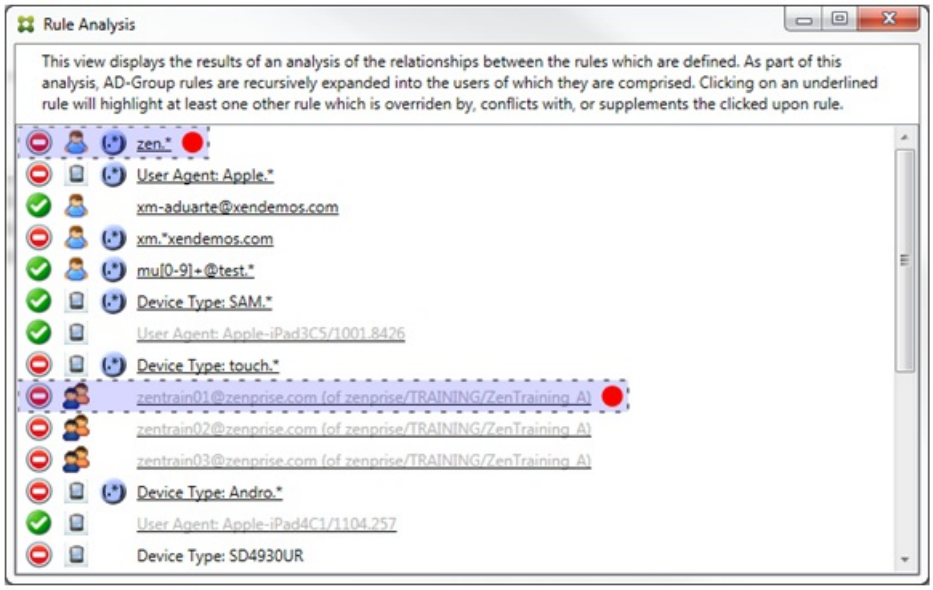


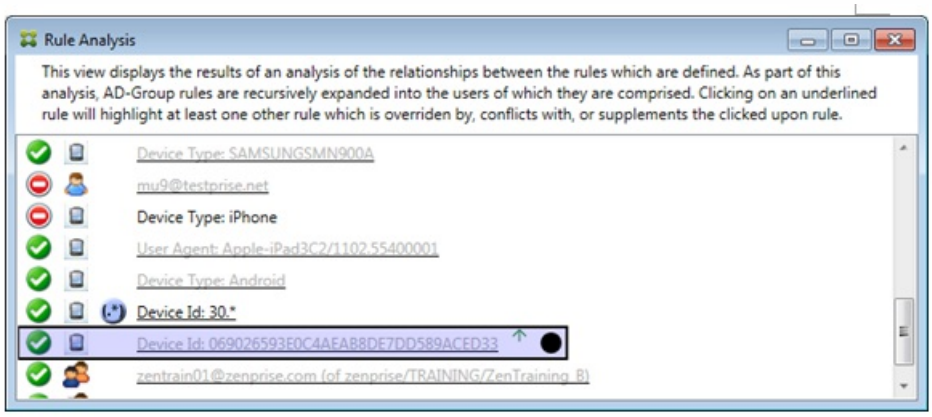




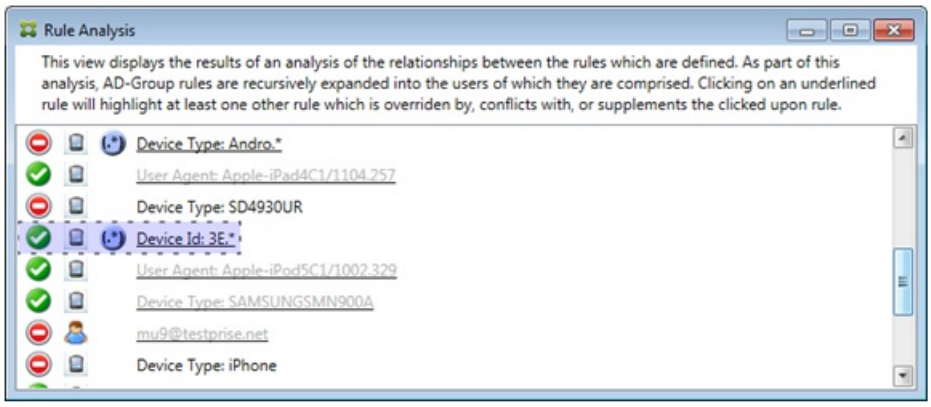


-
-
-



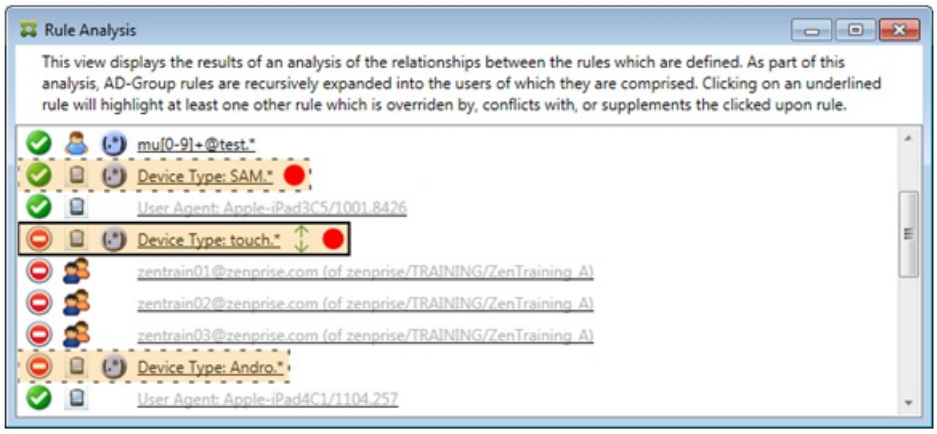


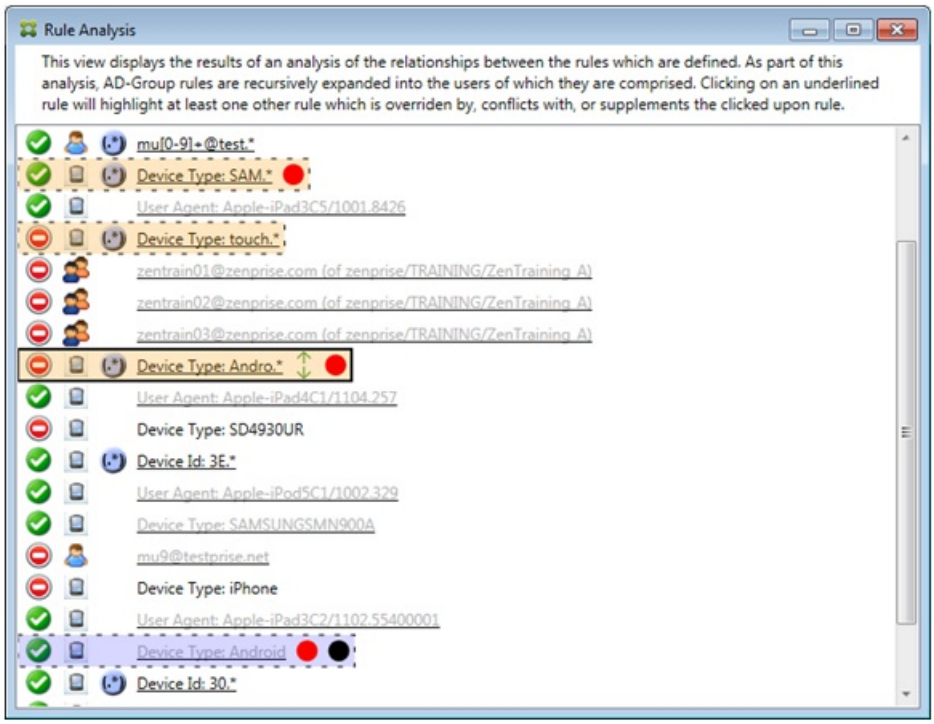
-
-
-

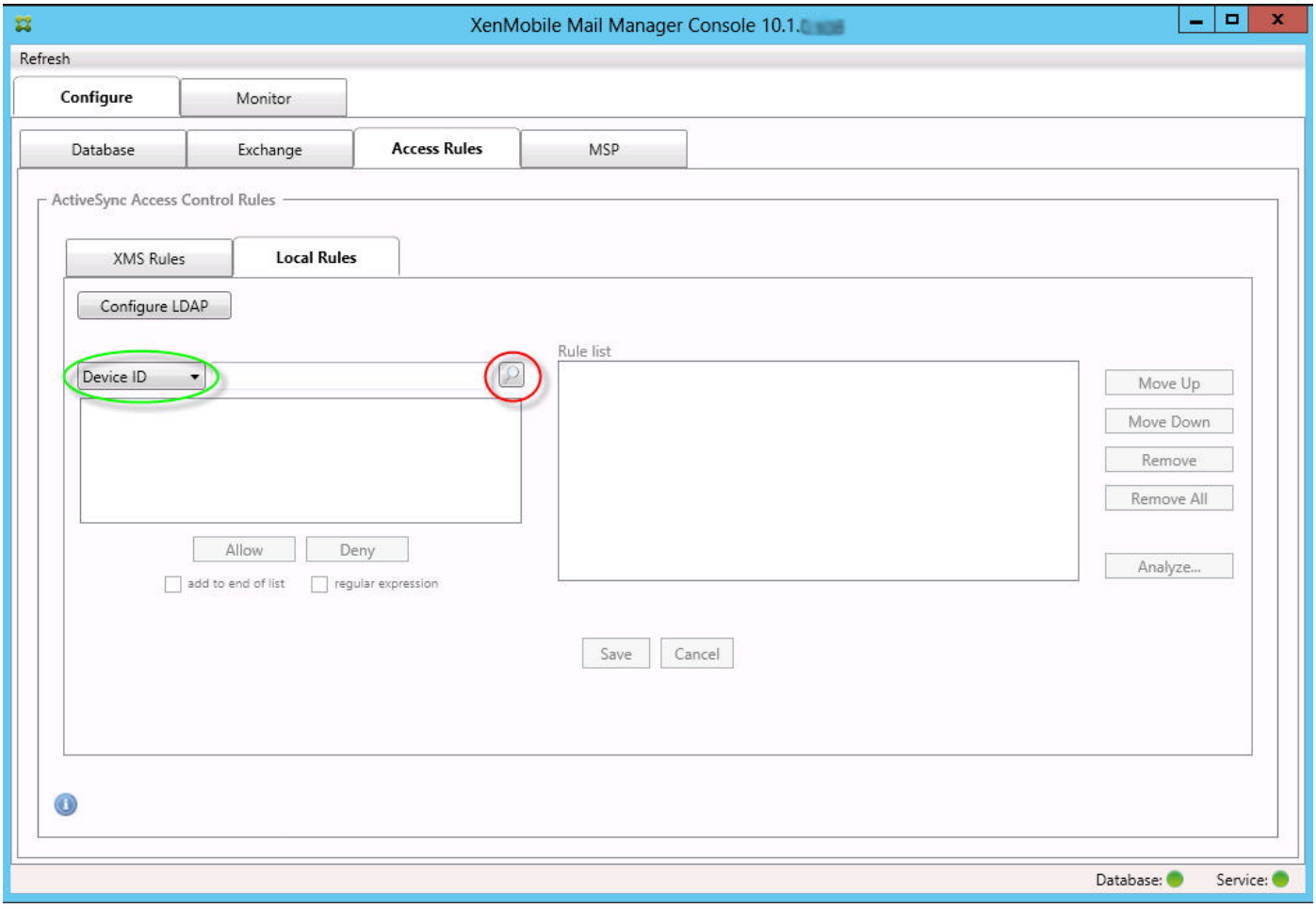


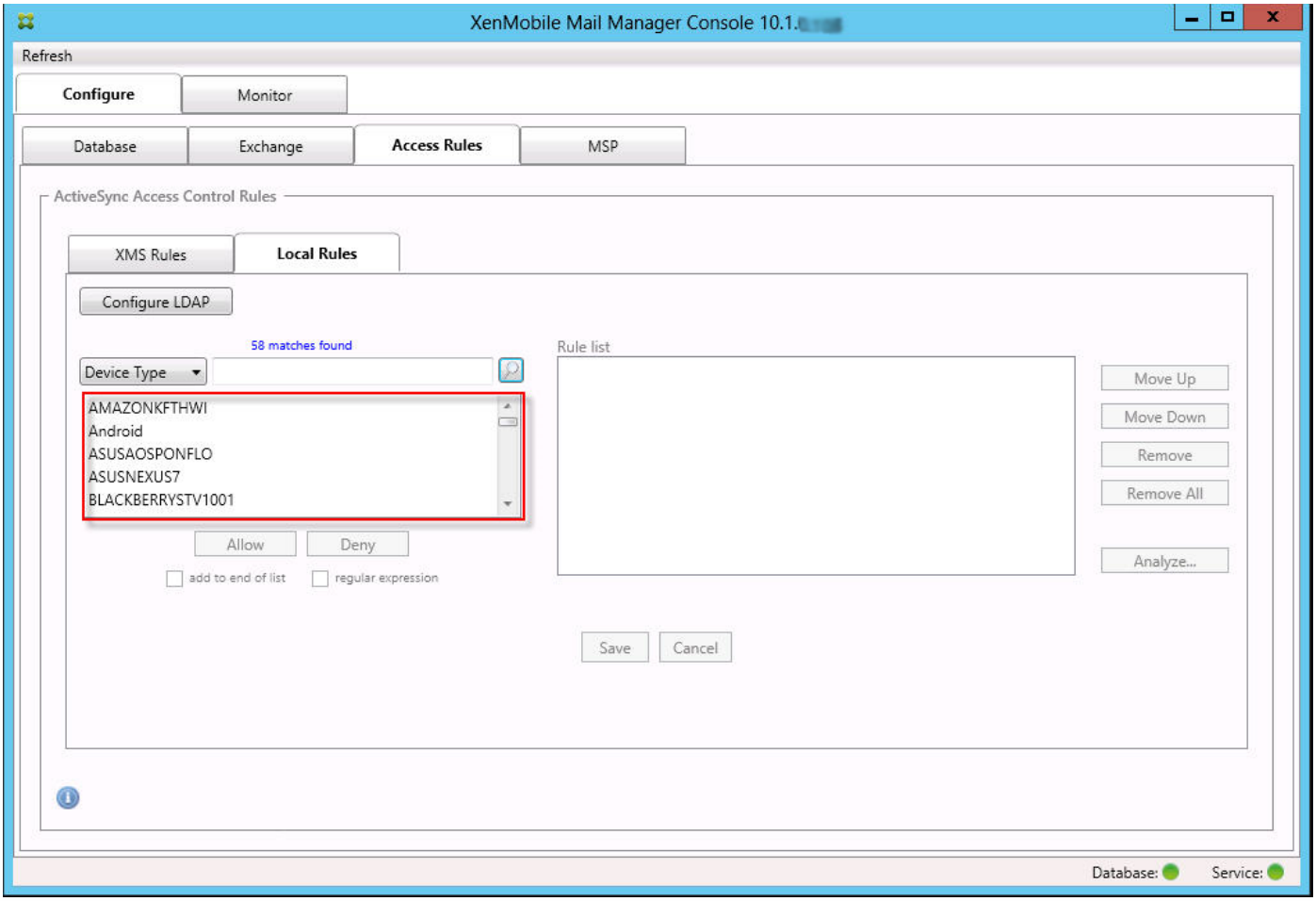
-

-
-
-
-
-
-

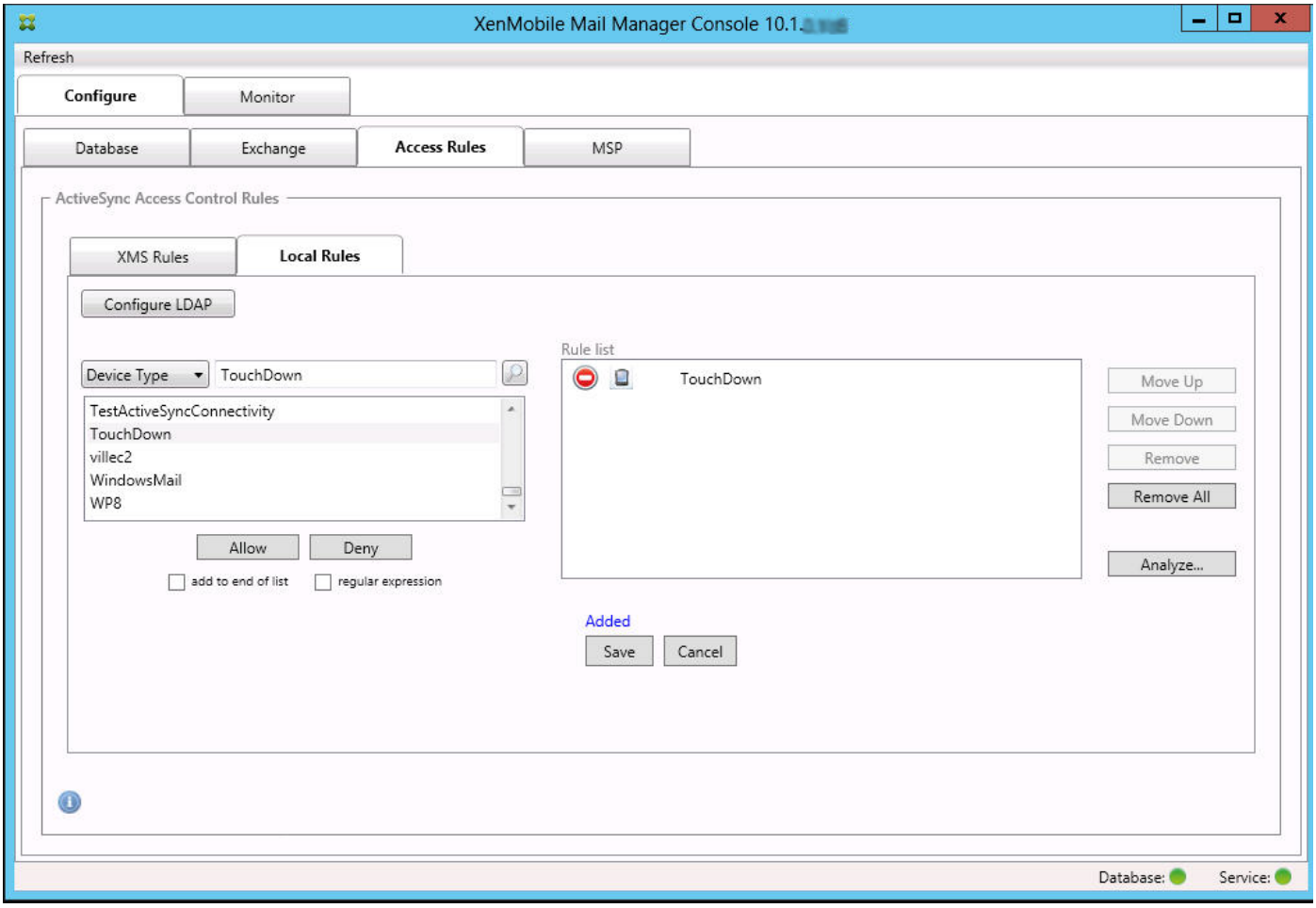


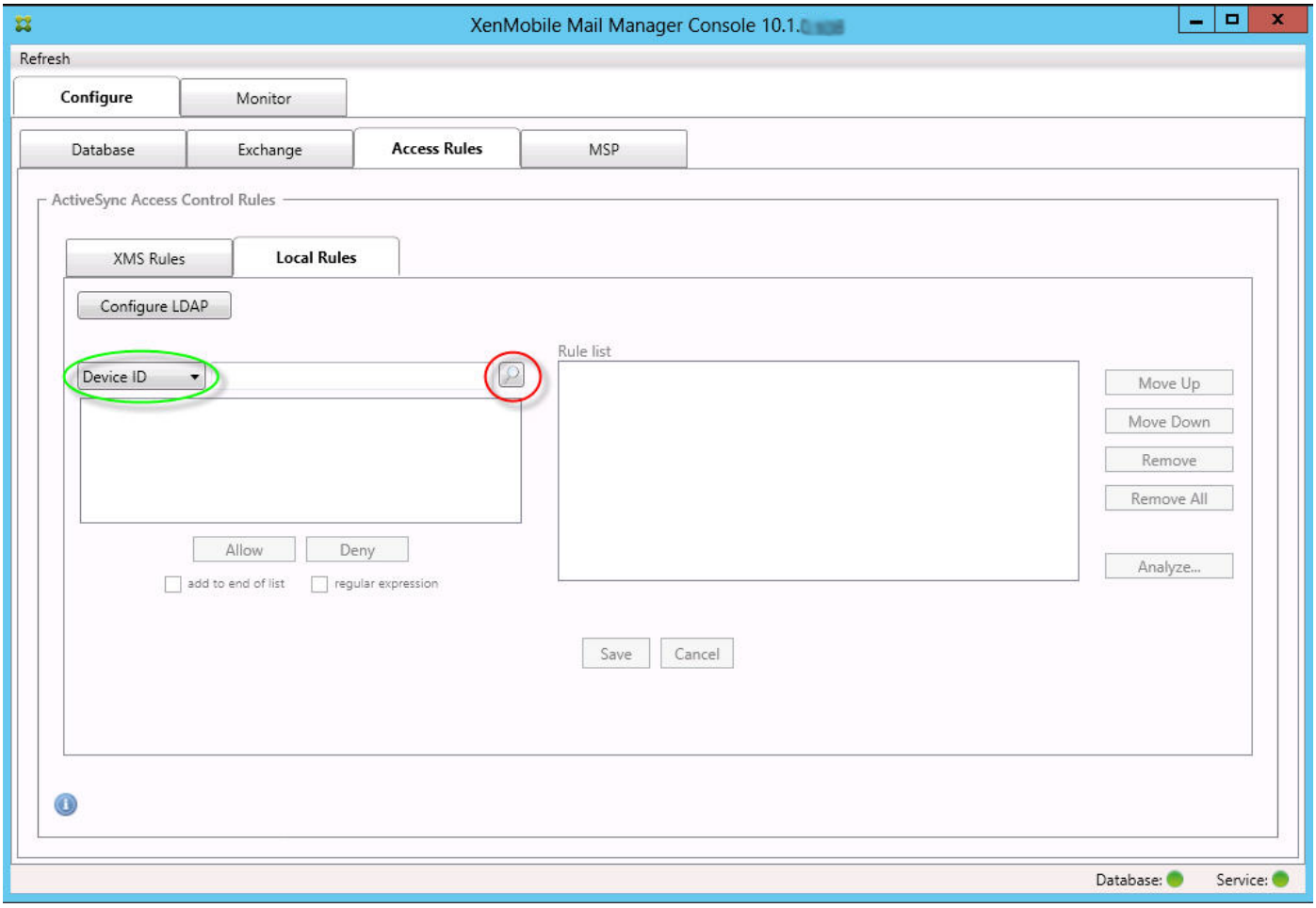


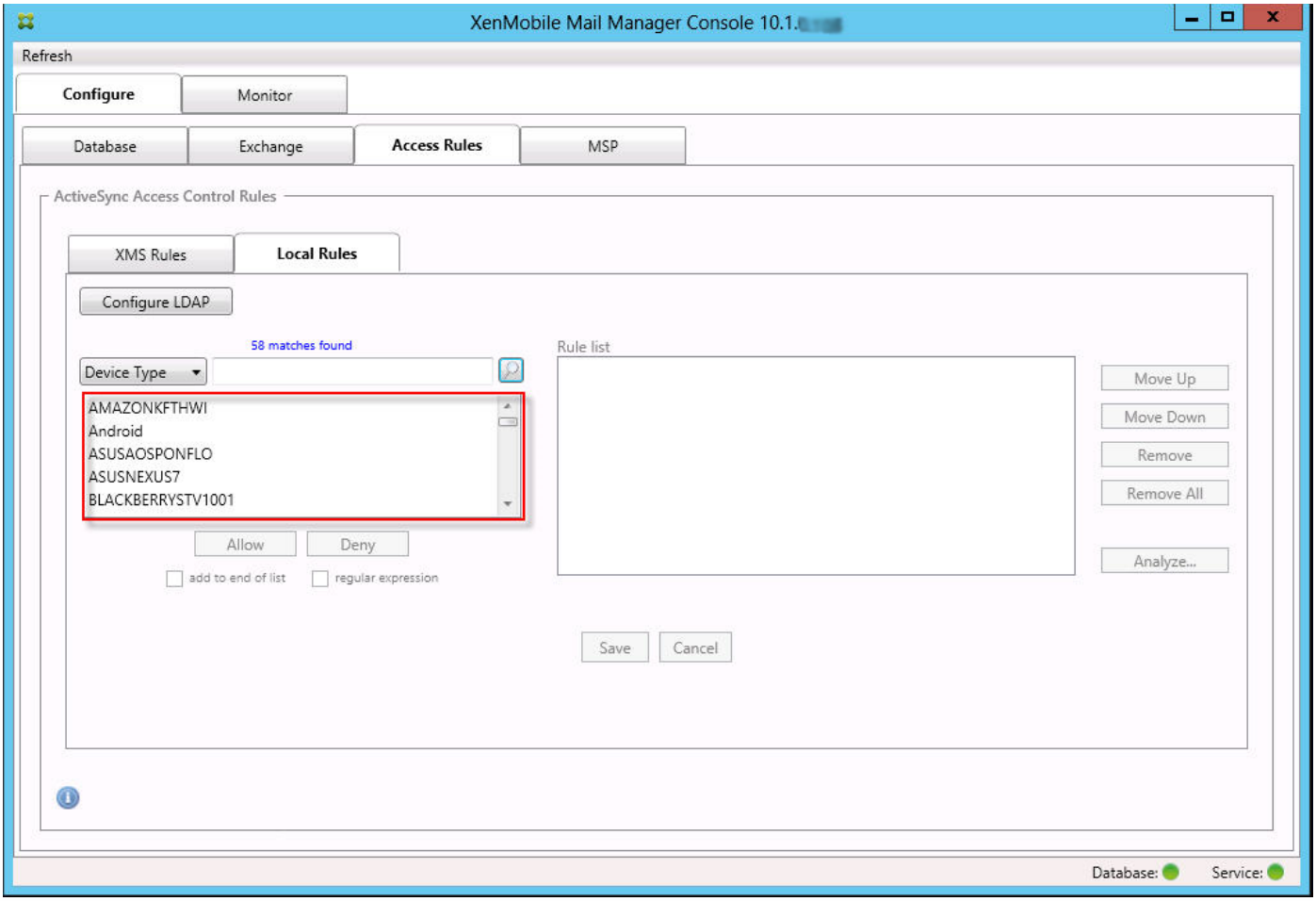


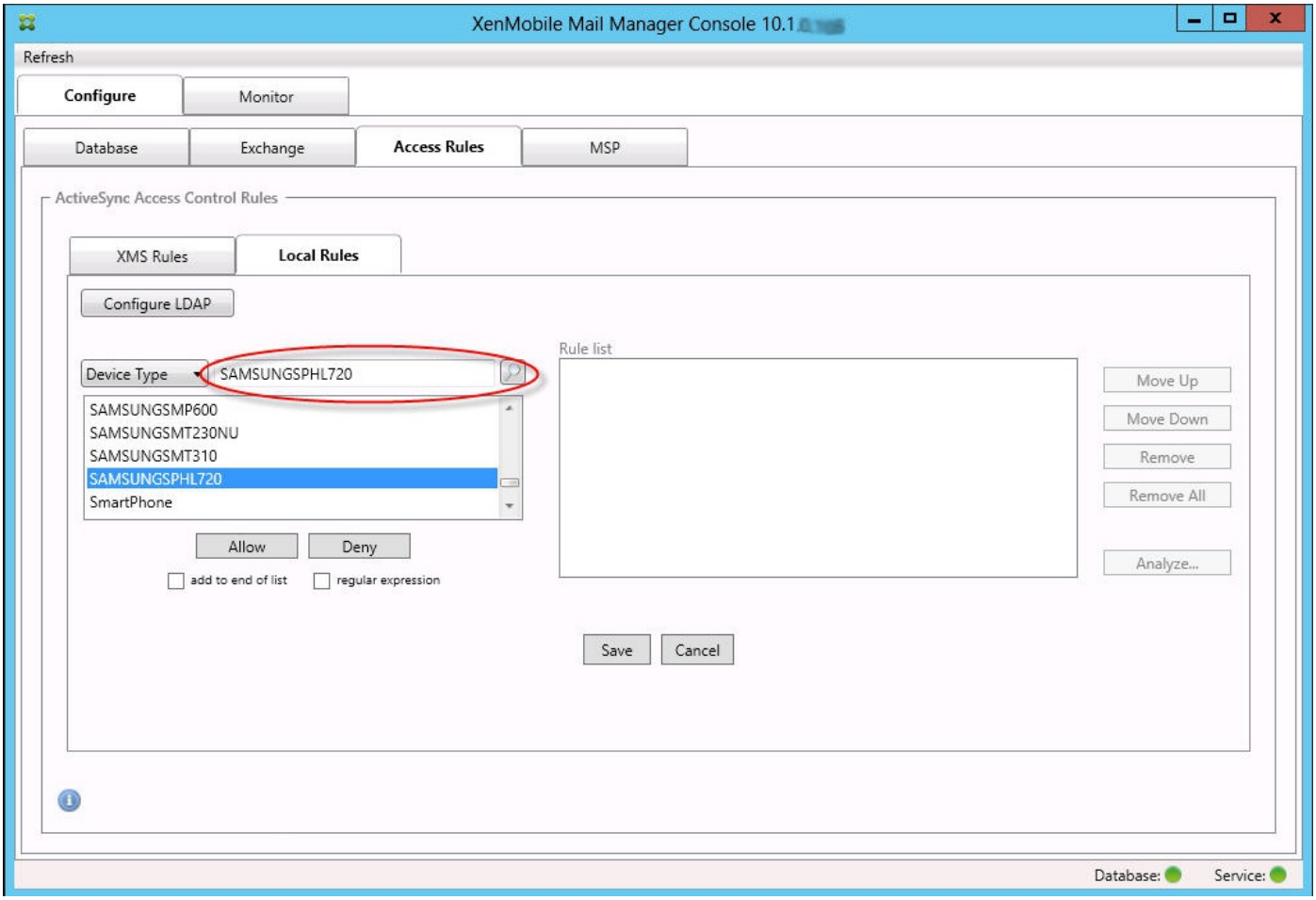


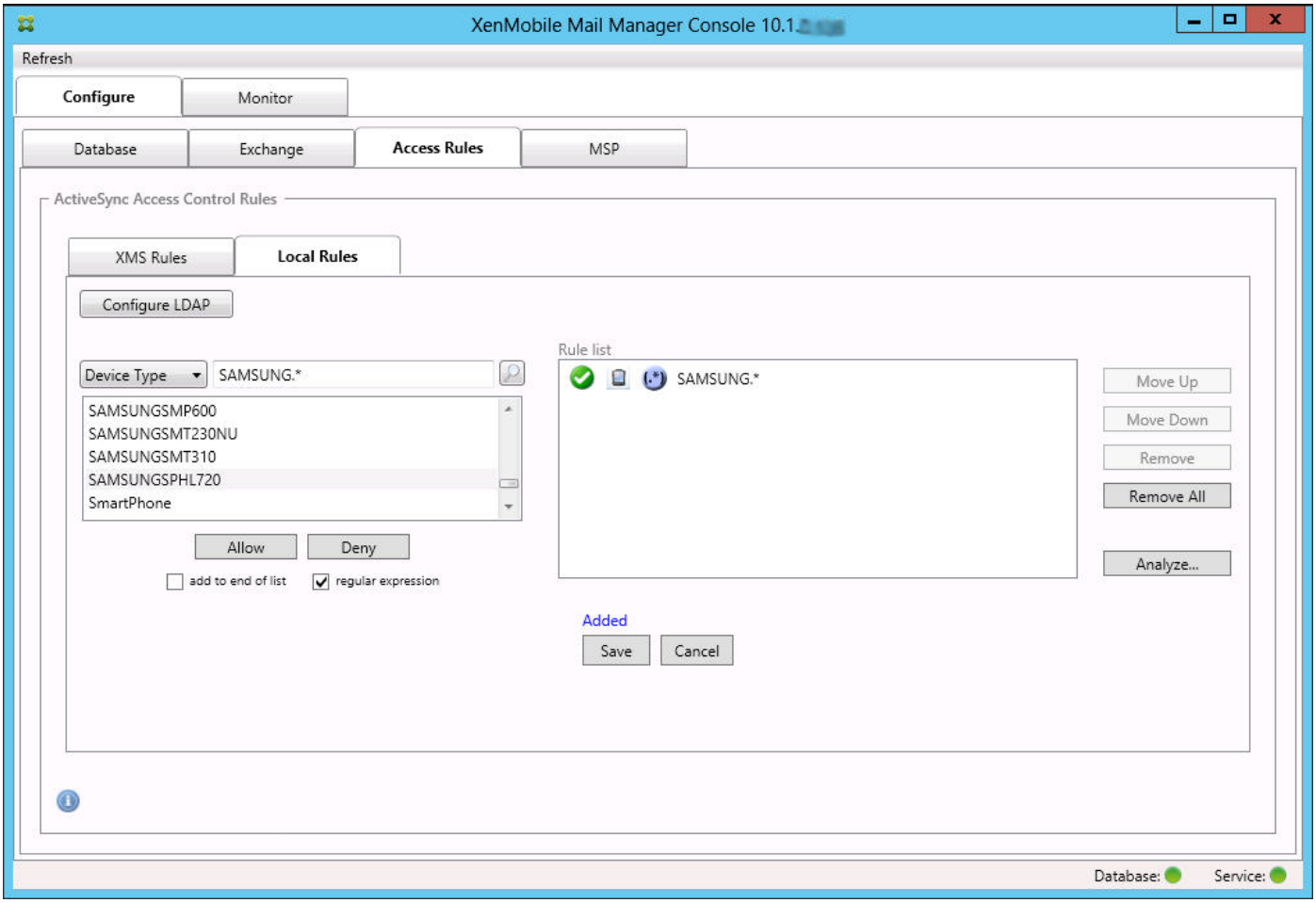
-
-

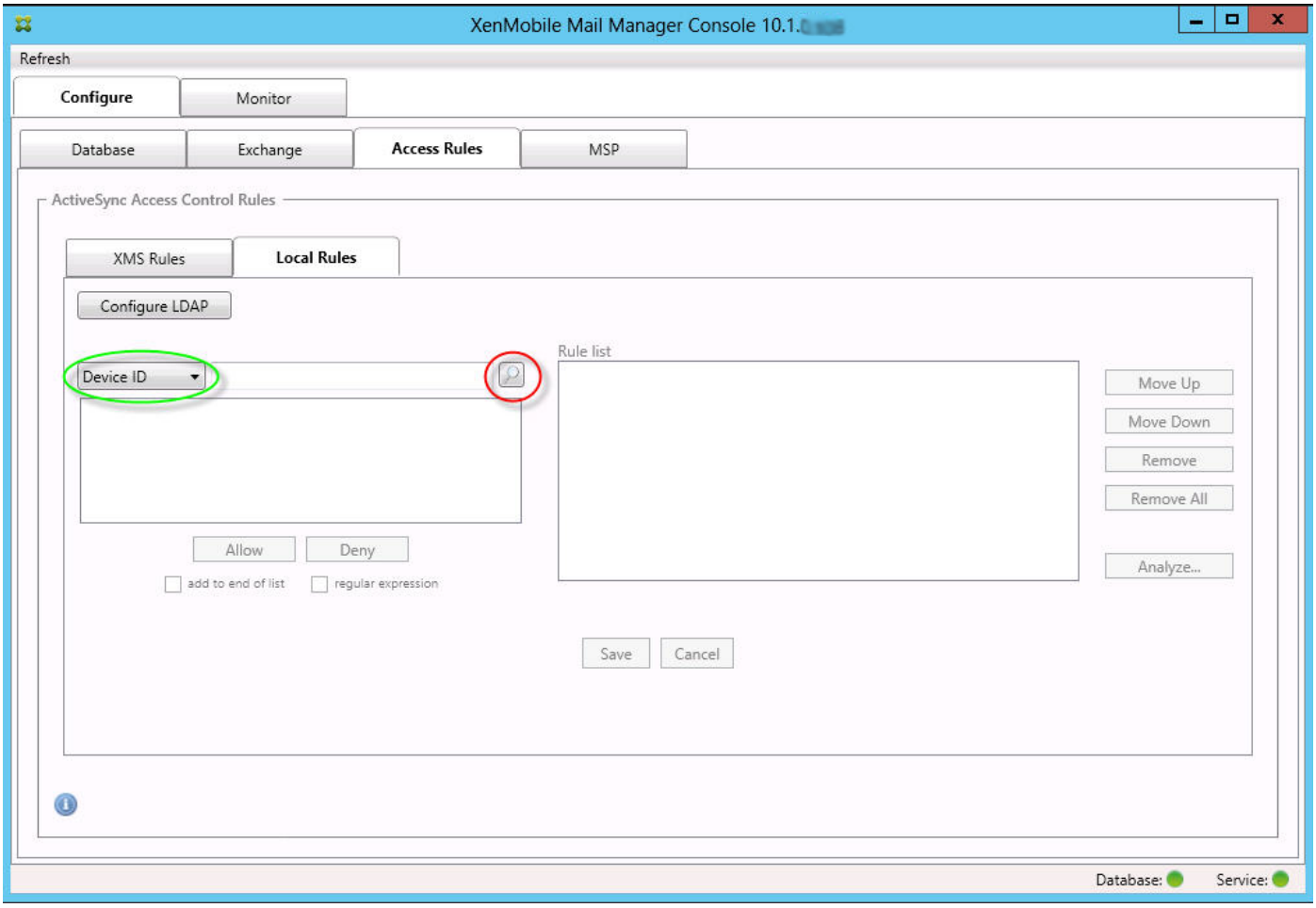


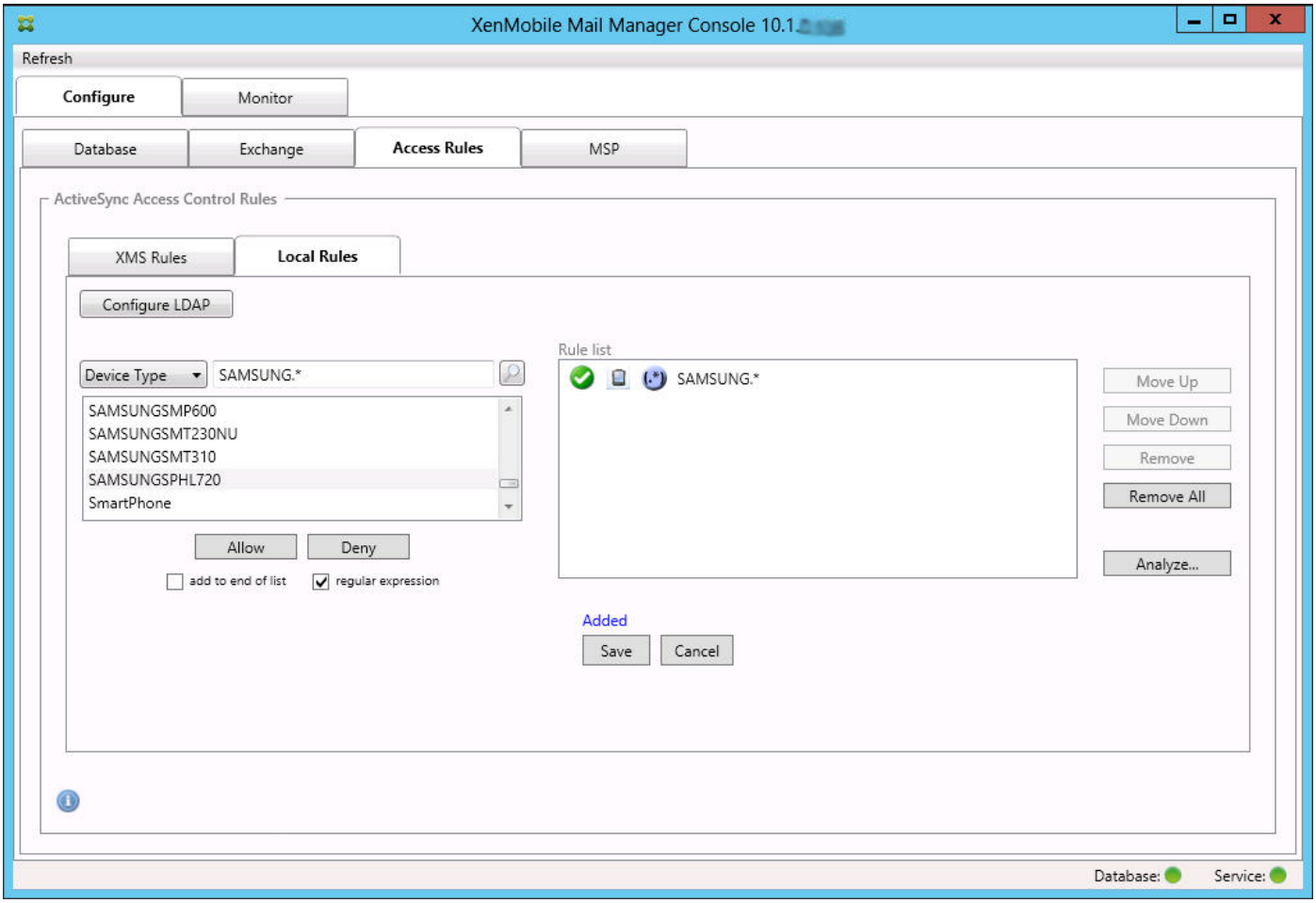


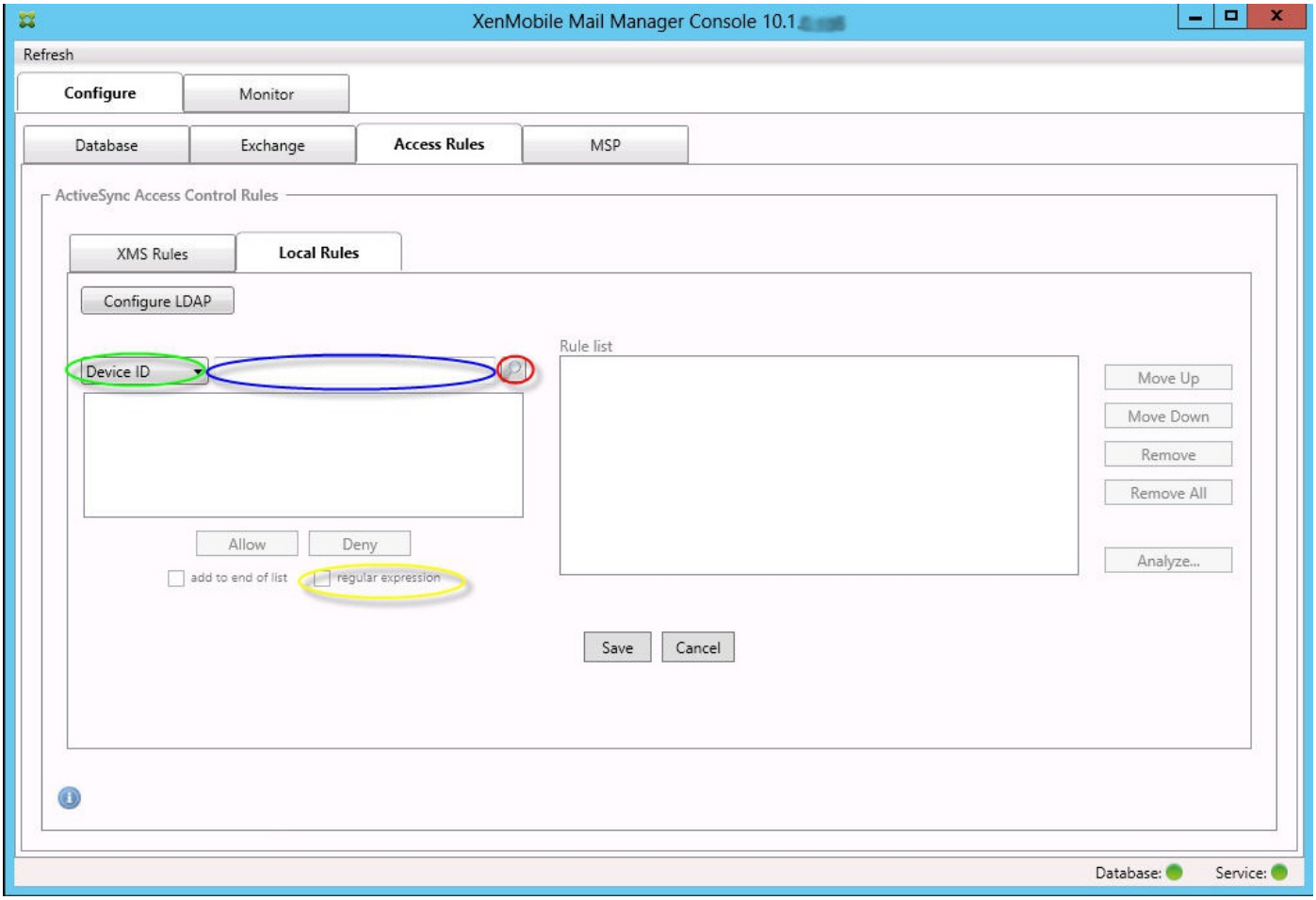


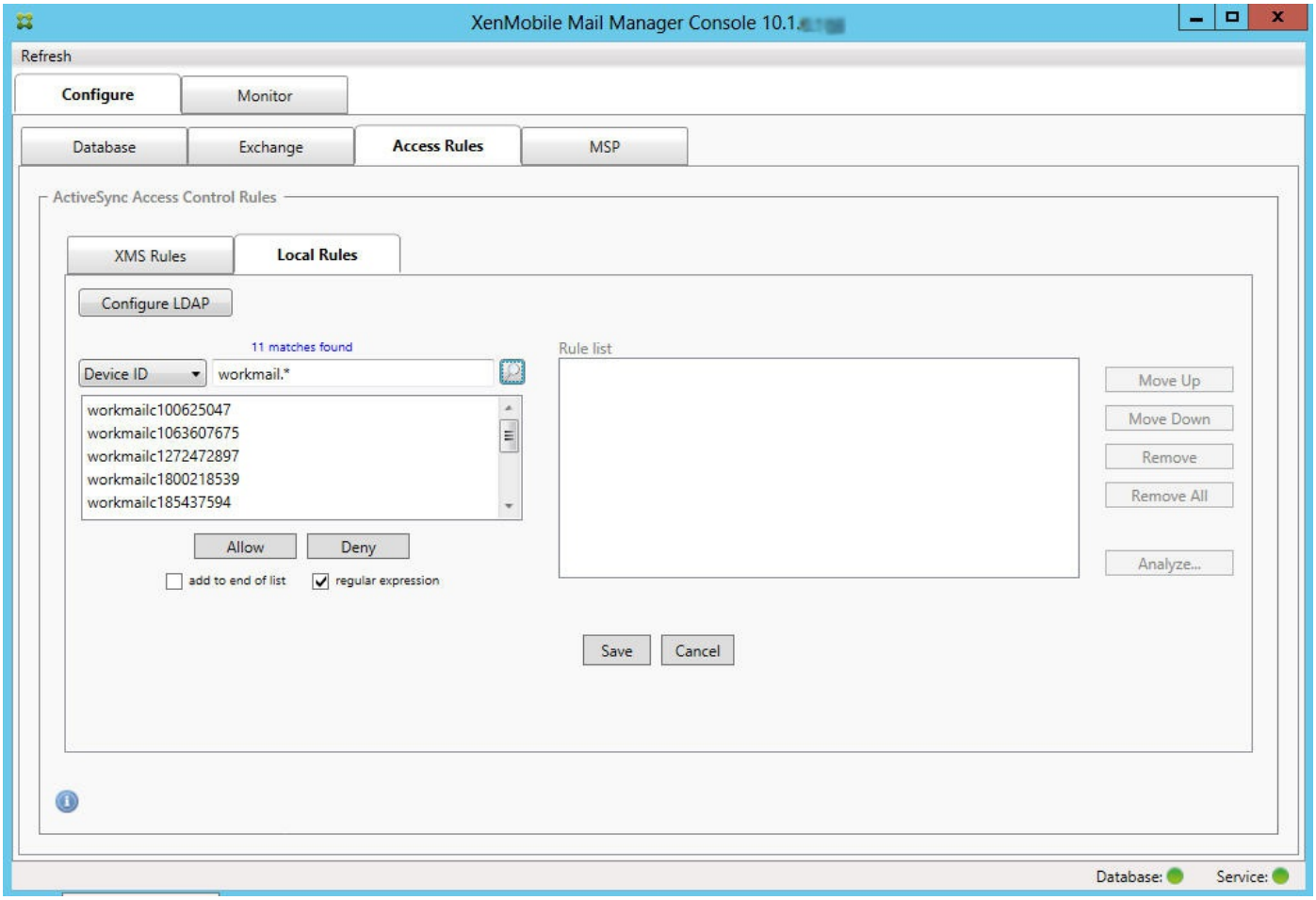


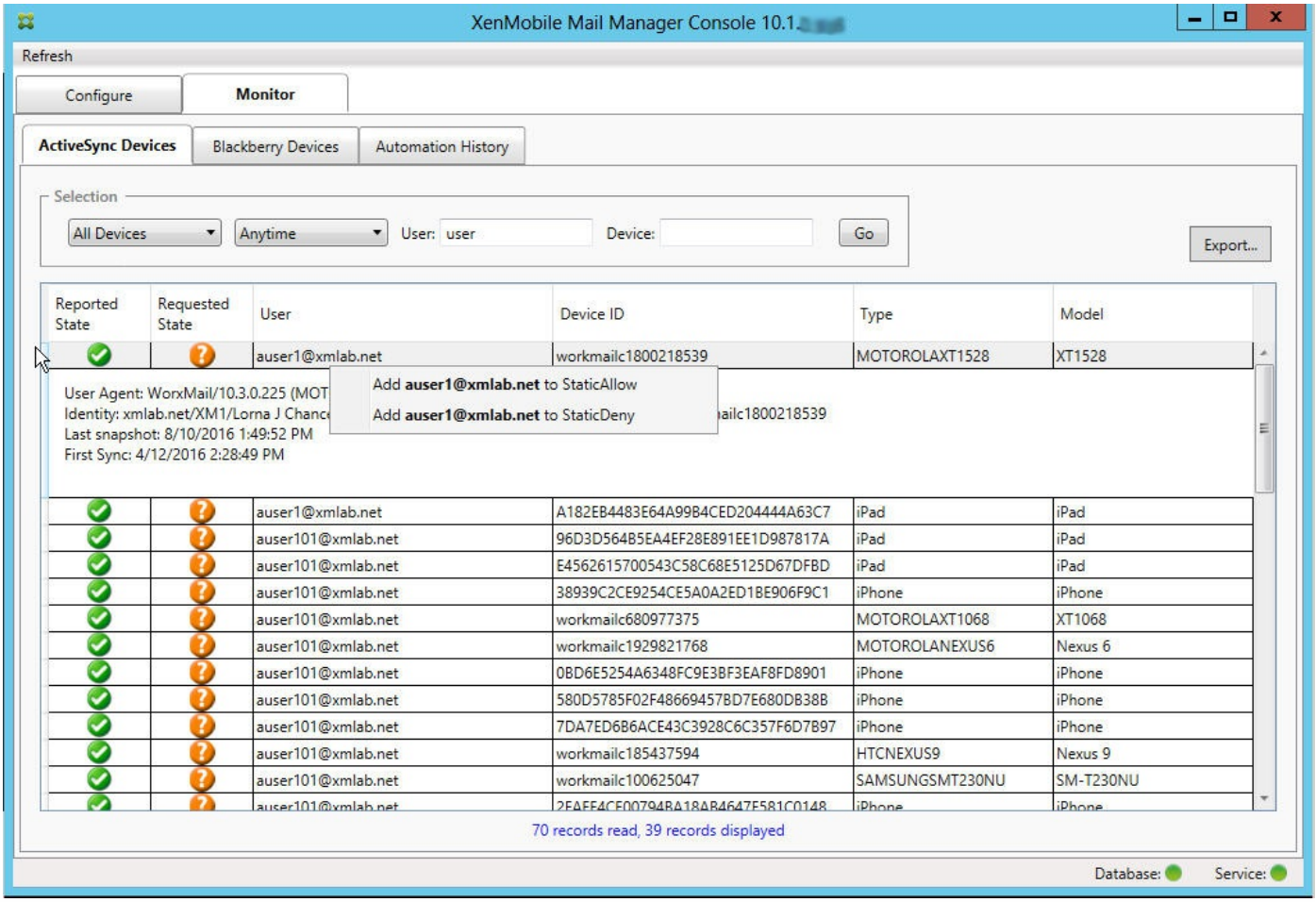






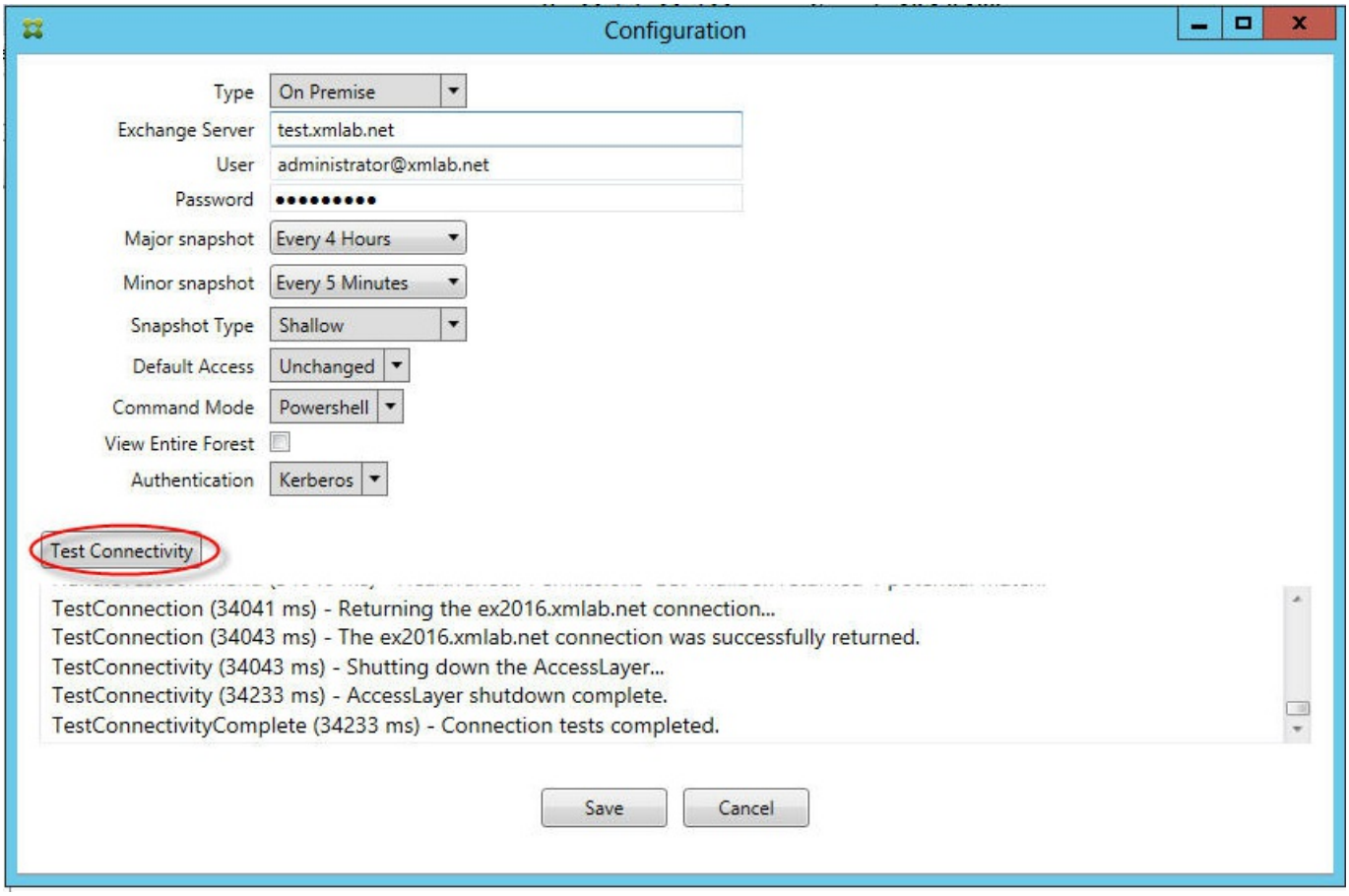






-
  -
  -
  -
-
-
-
-

-
  -
  -
-



-
-

Interacción del XenMobile instalado localmente con Active Directory

Siddartha Vuppala , | Aug 09, 2017

En este artículo, se explica la interacción entre XenMobile Server y Active Directory. XenMobile Server interactúa con Active Directory directas y en segundo plano. En las secciones siguientes, se ofrece más información sobre las operaciones directas y en segundo plano que implican una interacción con Active Directory.

> ## Nota
>
> Este artículo es una introducción de la interacción y no cubre detalles concretos. Para obtener más información sobre cómo configurar Active Directory y LDAP desde la consola de XenMobile, consulte Autenticación de dominio o dominio + token de seguridad.

Interacciones directas

XenMobile Server se comunica con Active Directory según los parámetros LDAP que configura un administrador. La configuración recupera información sobre usuarios y grupos. A continuación, se presentan las operaciones que provocan la interacción entre XenMobile Server y Active Directory.

1. **Configuración de LDAP.** La configuración de Active Directory en sí resulta en una interacción con Active Directory. XenMobile Server intenta validar la información cotejándola con Active Directory. Para ello, el servidor utiliza el protocolo de Internet, el puerto y las credenciales de la cuenta de servicio proporcionadas. Una vinculación satisfactoria indica que la conexión se ha configurado correctamente.

2. **Interacciones de grupos.**

   a. Buscar uno o varios grupos durante el control de acceso basado en roles (RBAC) y crear una definición de grupos de entrega. El administrador de XenMobile Server introduce una cadena de texto de búsqueda en la consola de XenMobile. XenMobile Server busca todos los grupos que contienen la subcadena proporcionada en el dominio seleccionado. A continuación, XenMobile Server recupera los atributos objectGUID, samAccountName y Nombre distintivo de los grupos identificados en la búsqueda.

   > ## Nota
   >
   > Esta información no se almacena en la base de datos de XenMobile Server.

   b. Agregar o actualizar RBAC y definiciones de grupos de implementación. El administrador de XenMobile Server selecciona los grupos de Active Directory relevantes para la búsqueda anterior y los incluye en la definición de grupos de implementación. XenMobile Server busca el grupo específico, uno por uno, en Active Directory. XenMobile Server busca el atributo objectGUID y recupera los atributos seleccionados, incluida la información de pertenencia a grupos. La información de pertenencia a grupos ayuda a determinar la pertenencia entre el grupo obtenido y los usuarios o grupos existentes en la base de datos de XenMobile Server. Realizar cambios en la pertenencia al grupo deriva en cambios en

RBAC y en grupos de implementación de los miembros afectados, lo que provoca asignaciones nuevas de usuarios.

> **Nota**
>
> A su vez, realizar cambios en la definición de grupos de implementación puede provocar cambios en los derechos a aplicaciones o directivas cuando se trate de los usuarios afectados.

c. **Invitaciones de PIN de un solo uso (OTP)**. El administrador de XenMobile Server selecciona un grupo de la lista de grupos de Active Directory presente en la base de datos de XenMobile Server. Para este grupo, todos los usuarios (tanto directos como indirectos), se recuperan de Active Directory. Las invitaciones OTP se envían a los usuarios que se hayan identificado en el paso anterior.

> **Nota**
>
> Las tres interacciones anteriores implican que las interacciones de grupos se activan tras cambios en la configuración de XenMobile Server. Cuando no hay cambios en la configuración, no hay interacciones con Active Directory. También implican que no hay necesidad de tareas en segundo plano para capturar la parte del grupo de los cambios periódicos.

3. **Interacción de usuarios.**

a. Autenticación de usuarios. El proceso de autenticación de usuarios provoca dos interacciones con Active Directory:

- Para autenticar al usuario con las credenciales proporcionadas.
- Para agregar o actualizar atributos de usuario en la base de datos de XenMobile Server, incluida la pertenencia directa a grupos, objectGUID, Nombre distintivo y sAMAccountName. Realizar cambios en la pertenencia al grupo provoca cambios en los derechos de acceso, aplicación y directiva.

El usuario puede autenticarse desde el dispositivo o desde la consola de XenMobile Server. En ambos casos, la interacción con Active Directory presenta el mismo comportamiento.

b. Acceso a la tienda de aplicaciones y actualización. Una actualización de la tienda provoca una actualización de los atributos de usuario, incluida la pertenencia directa a grupos. Esta acción provoca cambios en los derechos de los usuarios.

c. Conexiones de dispositivos. En la consola de XenMobile, los administradores pueden configurar conexiones periódicas de dispositivos. Cada vez que un dispositivo se conecta, se actualizan los atributos correspondientes de usuario, incluidas las pertenencias directas a grupos. Estas conexiones provocan cambios en los derechos de los usuarios.

d. Invitaciones OTP por grupo. El administrador de XenMobile Server selecciona un grupo de la lista de grupos de Active Directory presente en la base de datos de XenMobile Server. Los miembros, directos e indirectos (debido a la anidación de usuarios), se recuperan de Active Directory y se guardan en la base de datos de XenMobile Server. Las invitaciones OTP se envían a los usuarios miembro que se hayan identificado en el paso anterior.

e. Invitaciones OTP por usuario. El administrador introduce una cadena de texto de búsqueda en la consola de XenMobile. XenMobile Server consulta Active Directory y devuelve los registros de usuario que coincidan con la cadena de texto introducida. El administrador selecciona el usuario al que enviar la invitación OTP. XenMobile Server recupera los

datos del usuario de Active Directory y los actualiza en la base de datos antes de enviar la invitación al usuario.

Interacciones en segundo plano

Una conclusión de la comunicación directa con Active Directory es que las interacciones del grupo se activan tras ciertos cambios en la configuración de XenMobile Server. Cuando no hay cambios en la configuración, no hay interacciones relativas a grupos de Active Directory.

Esta interacción requiere tareas en segundo plano de sincronización periódica con Active Directory para actualizar los cambios correspondientes que haya en los grupos pertinentes.

A continuación, se presentan las tareas en segundo plano que interactúan con Active Directory.

1. **Tarea de sincronización de grupos**. El propósito de esta tarea es consultar Active Directory sobre los grupos relevantes para saber si ha habido cambios en los atributos de nombre distintivo o sAMAccountName. Estas consultas se realizan uno por uno (un grupo a la vez). La consulta de búsqueda en Active Directory utiliza el atributo objectGUID del grupo relevante para obtener los valores actuales de los atributos de nombre distintivo y sAMAccountName. Los cambios realizados en el nombre distintivo o en sAMAccountName de los grupos relevantes se actualizan en la base de datos.

   > **Nota**
   >
   > Esta tarea no actualiza la información de pertenencia del usuario al grupo.

2. **Tarea de sincronización de grupos anidados**. Esta tarea actualiza los cambios en la jerarquía de anidamiento de los grupos relevantes. XenMobile Server permite que los miembros directos e indirectos de un grupo obtengan derechos. La pertenencia directa de los usuarios se actualiza durante las interacciones directas de los usuarios. Ejecutada en segundo plano, esta tarea realiza un seguimiento de las pertenencias indirectas. Las pertenencia indirectas son aquellas en que un usuario es miembro de un grupo que es a su vez miembro de un grupo relevante.

   Esta tarea recopila la lista de grupos de Active Directory desde la base de datos de XenMobile Server. Estos grupos forman parte de la definición de RBAC o del grupo de implementación. XenMobile Server obtiene a los miembros de cada grupo de la lista. Los miembros de un grupo son una lista de nombres distintivos que representan a usuarios y grupos. XenMobile Server realiza otra consulta a Active Directory para obtener solo a los usuarios miembro del grupo relevante. La diferencia entre las dos listas permite determinar a los miembros del grupo relevante. Los cambios en los grupos de miembros se actualizan en la base de datos. Se repite el mismo proceso para todos los grupos de la jerarquía.

   Los cambios de anidamiento provocan el procesamiento de los usuarios afectados para determinar los cambios de derechos.

3. **Comprobación de usuarios inhabilitados**. Esta tarea solo se ejecuta si el administrador de XenMobile crea una acción para comprobar si existen usuarios inhabilitados. La tarea se ejecuta en el ámbito de una tarea de sincronización de grupos. La tarea consulta el estado inhabilitado de los usuarios relevantes en Active Directory; un usuario a la vez.

Preguntas frecuentes

¿Qué es la frecuencia predeterminada de ejecución de las tareas en segundo plano?

¿Para qué se necesita una tarea de sincronización de grupos?

¿Se puede desactivar una tarea de sincronización de grupos?

¿Para qué se necesita una tarea en segundo plano de procesamiento de grupos anidados?

¿Se puede desactivar una tarea de procesamiento de grupos anidados?