

# Problemas resueltos

Mar 02, 2017

Se han resuelto los siguientes problemas en XenMobile 10.4. Los problemas resueltos de la herramienta de actualización aparecerán bajo el título "XenMobile Upgrade Tool 10.4" al final de este artículo.

**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](#).

Cuando intente agregar una aplicación de tienda pública de aplicaciones para Windows Phone e introduce una URL de Microsoft Store, la carga fallará. [CXM-13468]

Para algunas configuraciones, después de actualizar desde XenMobile 9 a 10.3.6, los dispositivos que se habían inscrito en XenMobile 9 no pueden abrir aplicaciones instaladas ni descargar las nuevas aplicaciones desde WorxStore. Asimismo, las aplicaciones desaparecen de Worx Home y los usuarios no pueden acceder a WorxStore. [CXM-13708]

Cuando se crea una directiva de WiFi con una contraseña definida de WiFi que incluye caracteres especiales, como un símbolo de menor (<), mayor (>) o la "Y" comercial (&), se solicita a los usuarios que introduzcan su contraseña de WiFi. [CXM-13717]

Cuando intenta cargar una aplicación de empresa para iOS, aparece el error "no se ha encontrado el icono" si el tamaño del icono supera 1000 KB. [CXM-13729]

Si está habilitada la agrupación en clústeres y se envía un borrado a un dispositivo desconectado, el dispositivo se borrará cuando se vuelva a conectar, según lo previsto. Sin embargo, si el dispositivo se vuelve a inscribir o se conecta a otro nodo del clúster, XenMobile volverá a borrar el dispositivo. [CXM-13793]

El permiso de inscripción de dispositivos compartidos está habilitado de forma predeterminada para el rol "Admin" de RBAC en implementaciones en la nube del servicio XenMobile. Por eso, todos los dispositivos que pertenezcan a usuarios con el rol "Admin" se inscriben como dispositivos compartidos. [CXM-15203]

No se produce la inscripción cuando configura la autenticación de certificados de cliente y la opción "Require Server Name Indication" está habilitada en el servidor de la entidad de certificación. [CXM-15312]

Al buscar aplicaciones de Google Play Store desde la consola de XenMobile, la búsqueda no devolverá las aplicaciones basadas en el sistema operativo Android en el dispositivo registrado. Por ejemplo, las aplicaciones que requieren un sistema operativo mínimo de 4.4 no aparecen en el panel de resultados. [CXM-15653]

Si crea un usuario local asignado a un grupo local, cuando el usuario intente registrarse con un dispositivo Windows 10, la inscripción falla. [CXM-16895]

Si crea una directiva de Citrix Launcher, los usuarios podrán inscribir un dispositivo Android, pero, si cambia una configuración de directiva, no podrán salir de Citrix con la contraseña que haya definido en la directiva. Como solución temporal, es necesario volver a introducir la contraseña en los parámetros de la directiva y actualizarla. [CXM-17157]

En XenMobile, cuando se inhabilita la opción Habilitar ShareFile, en Secure Mail para Android, los usuarios no pueden acceder a ningún tipo de archivos adjuntos. [CXM-17887]

Al actualizar desde XenMobile 10.3.6 con Rolling Patch 1 a XenMobile 10.4, los tipos de licencias permanentes caducan con

un mensaje de error. [CXM-17900]

Al actualizar desde XenMobile 10.3.6 a XenMobile 10.4, aunque la licencia de tipo permanente siga siendo válida, aparecerá el mensaje de error de una licencia caducada. [CXM-17987]

Si introduce manualmente la URL de una tienda pública de aplicaciones Windows y esa URL no es de una tienda de EE.UU., aparece un error en la consola de XenMobile. Cuando se usa la URL de una tienda de aplicaciones de EE.UU., se carga correctamente. [CXM-18013]

Cuando los usuarios reciben invitaciones de contraseña de uso único para enlaces de IMEI (nombre de usuario y contraseña) y notificaciones SMTP y SMS, el primer perfil se instala correctamente y la instalación del segundo perfil falla con el mensaje de error "Profile Installation Fails. A connection to the server could not be established". En dispositivos iPhone 6 e iPhone 6 Plus, hay un número IMEI y un número MEID y la contraseña de un solo uso se vincula con el número MEID en lugar de hacerlo con el número IMEI. Puede reemplazar el número IMEI con el identificador único de dispositivo (UDID) de iPhone o usar un número de teléfono normal. [#606162]

El intento de descargar una solicitud de firma de certificado (CSR) desde Internet Explorer y Firefox falla, con el error: "The Webpage cannot be displayed". La descarga de la solicitud CSR desde Chrome sí que funciona. [#609552]

Si inicia sesión en la consola de XenMobile, va a **Analyze > Reporting** y hace clic en **Inactive Devices**, aparecerá una pantalla en blanco en lugar de descargarse el archivo. [#609649]

XenMobile NetScaler Connector no obtiene los dispositivos Samsung 5.x de una sincronización con ActiveSync. [#613522]

Cuando crea una directiva de dispositivo WiFi para Android con un tipo de autenticación de protocolo de autenticación extensible (EAP) 802.1x, el campo Contraseña ya no es obligatorio. [#614932]

Esta corrección soluciona una vulnerabilidad de seguridad. Para obtener más información, consulte el boletín de seguridad <http://support.citrix.com/article/CTX207824>.

**Nota:** Para que esta corrección de seguridad funcione, se requiere un segundo reinicio del servidor XenMobile. [#624347]

Por ahora, 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]

A veces, la inscripción de Windows Phone no puede iniciar Worx Home. [#633884]

Las aplicaciones HDX inhabilitadas no aparecen en Worx Store. [#634110]

El servidor XenMobile muestra datos de usuario incorrectos en el archivo de registros. [#636754]

Después de actualizar XenMobile de 10.3.1 a 10.3.6, el tipo de archivo y la carpeta de destino en las propiedades de la directiva Archivos no se muestran correctamente en la consola de XenMobile. [#640334]

La longitud máxima del cuadro de texto para el token de VPP es de 256 caracteres. [#640692]

Los usuarios de Windows Phone no pueden inscribir un dispositivo con una cuenta SAM. [#640847]

Después de quitar los usuarios ya inscritos del subsistema de control de ShareFile, los usuarios inscritos pueden aparecer en el archivo de registro de auditoría del usuario en la consola de XenMobile. [#641342]

Después de actualizar XenMobile Server de 10.1 a 10.3.x y hacer clic en <https://zdm/enrollmdm.html>, la plataforma de iOS

no aparece como selección de plataforma. [#641771]

Al inscribir un dispositivo en Worx Home para iOS, es posible que la inscripción MDM se realice correctamente, pero la inscripción MAM falle. [#644892]

La eliminación de los grupos anidados nunca se refleja. [#647557]

Si **Manage > Enrollment** tiene más de 2000 entradas, después de hacer clic en **Export**, la página se queda vacía y el informe no se genera. [#647855]

Los administradores de XenMobile que intentan acceder a la consola de XenMobile, en vez de ello pueden ser redirigidos al portal Self-Help Portal de XenMobile. Esto puede ocurrir cuando se han creado grupos de administradores de XenMobile con acceso basado en roles y se mueve un grupo desde una unidad organizativa de Active Directory a otra. [#647987]

No se pueden cargar aplicaciones para iOS; aparece el error: "La aplicación móvil cargada no es válida. No se encontró el icono de la aplicación". [#649574]

El servidor XenMobile puede dejar de responder con un error de memoria insuficiente. [#650490]

Problemas con el borrado de dispositivos por la mensajería en clústeres. [#650555]

Al configurar una directiva de redes VPN para dispositivos, no se puede especificar un número de puerto. [#650972]

Después de actualizar el servidor XenMobile con la agrupación en clústeres habilitada, pueden producirse varios bloqueos. El servidor puede dejar de responder. [#651122]

La consola de XenMobile no muestra datos de número de serie cuando se le solicita confirmar la eliminación de un dispositivo. [#651185]

En XenMobile Server 10.3.6, la directiva de cuentas SSO no funciona según lo previsto. Sigue solicitándose la contraseña a los usuarios. [#651860]

No se puede inhabilitar la asociación de aplicaciones para iPad en XenMobile 10.3.6 para aplicaciones VPP. [#652280]

Si elimina un grupo de entrega de una directiva de dispositivo, XenMobile no guarda el cambio y el grupo de entrega permanece asignado a la directiva. [#652321]

La cuenta de SSO no puede guardar un nombre de dominio completo que sea corto. [#652704]

Cuando un usuario quita los derechos de administración desde su dispositivo Android, XenMobile cambia el estado de los dispositivos inscritos como MDX y MAM a "Naranja/No administrado" y el usuario pierde el acceso a todas las aplicaciones MDX. El estado de MAM debería seguir siendo "Verde/Administrado". [#655180]

## XenMobile Upgrade Tool 10.4

Si el parámetro de dispositivo en XenMobile 9.0 para la versión máxima o mínima de sistema operativo se establece como 10 o posterior, y para dispositivos excluidos para aplicaciones MDX y de empresa, después de actualizar la regla no se migra correctamente. Aparecen aplicaciones que no deberían verse, y viceversa, no se ven aplicaciones que sí deberían aparecer. [#603412]

Si el servidor Microsoft SQL se ha configurado con la distinción entre mayúsculas y minúsculas, la actualización resulta en error si la tabla "Id\_Generator" se especifica como "id\_generator". [#623300]

Después de actualizar XenMobile de 9 a 10, el tipo de valor de la directiva Personal Hotspot es booleano en lugar de una cadena. [#633337]

Si el nombre de un grupo de Active Directory contiene el carácter arroba (@), falla la actualización. [#633718]

Si su servidor Device Manager 9.0 está configurado con Local PostgreSQL y usa localhost como una referencia para el servidor de bases de datos, la actualización fallará. Como solución temporal, edite el archivo ew-config.properties en el servidor Device Manager 9.0 y reemplace todas las referencias a localhost por la dirección IP del servidor de la base de datos de Device Manager. Después, continúe con los requisitos previos para la actualización. [#635023]

En XenMobile 9.0, cuando se define la **unidad organizativa de los usuarios (OU)** en los parámetros de conexión de LDAP, después de actualizar a XenMobile 10, el contexto raíz completo no se añade a la unidad organizativa de los usuarios. Por ejemplo, OU=MDMUsers, OU=SALES debería ser OU=MDMUsers, OU=SALES, DC=citrite, DC=com. Por eso, es necesario hacerlo manualmente en XenMobile 10. [#635981]

Durante una actualización, a la hora de cargar el paquete de asistencia, aparece el error "MAM set up failed, see the logs for details" y la herramienta Upgrade Tool conserva datos MAM dañados. [#638062]

Si el nombre de un grupo de Active Directory contiene un punto (.), un rol migrado como grupo de entrega pierde su asociación de grupo. [#647590]

En App Controller, si el proxy Web contiene una barra diagonal invertida (\), no se puede iniciar el servidor XenMobile 10.1 y aparece el mensaje "Starting main app..." mientras el servidor sigue reiniciándose. [#647919]

Después de actualizar XenMobile de 9 a 10, las aplicaciones VPP de pago no se instalan desde la tienda de XenMobile (Worx) a menos que la configuración de la aplicación requiera la instalación. [#668102]

En una configuración de autenticación en varios dominios, después de actualizar XenMobile a 10.3.6, los dispositivos que se habían inscrito en XenMobile 9 no pueden abrir aplicaciones instaladas ni descargar las nuevas aplicaciones desde la tienda Worx (XenMobile) ni acceder a ella. [CXM-13708]

Después de actualizar XenMobile de 9 a 10, las aplicaciones provenientes de tiendas públicas aparecen como no suscritas en la tienda de XenMobile (Worx). [CXM-17936]

Si la URL de la conexión de base de datos es localhost, ya no se debe modificar el archivo ew-config.properties.

Tras la actualización, si tiene roles RBAC configurados con acceso restringido a LDAP y Active Directory (o a cualquiera de los elementos secundarios), cuando usted inicia sesión en la consola de XenMobile como administrador, no se seleccionan las mismas configuraciones.

# Problemas conocidos

Mar 02, 2017

A continuación, se describen los problemas conocidos de XenMobile 10.4.

Cuando configura Citrix Launcher, la opción **Just Once** no funciona. Debe hacer clic en la opción **Always**. [CXM-13413]

En ocasiones, cuando los usuarios vuelven a inscribir un dispositivo Android, se produce un borrado selectivo de forma inesperada. [CXM-13716]

Si configuró aplicaciones públicas en la consola de XenMobile, después de actualizar a XenMobile 10.4 y, a continuación, implementar Secure Hub en una tableta Windows 10, los usuarios no pueden ver las aplicaciones públicas. [CXM-16516]

Con Citrix Launcher, en modo MDM, cuando los usuarios abren XenMobile Store, la tienda se abre en un explorador Web predeterminado aunque se hubiera indicado un explorador distinto en la lista blanca. [CXM-17097]

Citrix Launcher no puede descargar imágenes de fondo y de logotipo desde un servidor que tenga un certificado autofirmado. [CXM-17159]

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

## XenMobile Upgrade Tool 10.4

### Problemas con datos y directivas

Después de actualizar, los datos de configuración de servidor de syslog no se migran al servidor XenMobile. [#558539]

Algunas configuraciones de la directiva de restricciones quedaron obsoletas en la versión 10.1. Por lo tanto, XenMobile 10.4 no puede implementar toda la directiva de restricciones en Windows 10 Phone después de actualizar desde XenMobile 9 a XenMobile 10.4. No obstante, si se abre y se guarda la configuración de directivas en XenMobile 10.4, la directiva se implementa con éxito. [#608541]

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 se colocan en 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]

### Aplicaciones de Google Play

Si incluye una aplicación pública de Google Play para dispositivos Android con el icono predeterminado, después de la migración, ese icono predeterminado no aparece en la consola de XenMobile. Para que aparezca la imagen, deberá modificar y guardar la aplicación, o bien hacer clic en Check for Updates. [#557996]

### Servidor SQL

Si usa una base de datos PostgreSQL, los dispositivos MAM no pueden reinscribirse después de la actualización. Para solucionar este problema, elimine las entradas de los dispositivos de XenMobile y envíe notificaciones de inscripción a los usuarios. [#632831]

## RBAC

Surgen problemas con las configuraciones de RBAC después de la actualización:

- Si tiene configurado un rol de superadministrador, se seleccionan todos los permisos de forma predeterminada. Después de actualizar, solo se seleccionan tres permisos: RBAC, Enrollment y Release Management.
- Si ha creado un rol personalizado de superadministrador, todos los permisos de asistencia deberían estar seleccionados de forma predeterminada. Después de actualizar, no se selecciona ninguna de las configuraciones de los permisos de asistencia. Para solucionar este problema, cree el permiso de asistencia después de la actualización. [#569350, #569395, #569423]

## Citrix Secure Hub y Citrix Store

Antes de actualizar desde XenMobile 9 a XenMobile 10.4, si su tienda de WorxStore tiene un nombre personalizado, pueden ocurrir problemas con la inscripción, el acceso a Worx Home y el acceso a Worx Store. Como solución temporal, cambie la tienda al nombre predeterminado **Store** antes de actualizar. Para obtener información detallada sobre una solución alternativa a este requisito previo, consulte [Requisitos previos de Upgrade Tool](#). [#619458]

Los usuarios que tengan dispositivos de solo MAM no podrán autenticarse en Citrix Secure Hub después de actualizar desde XenMobile 9.0 a XenMobile 10.4 y establecer la opción **User search by** en **sAMAccountName**. [#628233]

## Android for Work

Después de una actualización, el inicio de sesión de SAML para Android for Work falla porque el certificado SAML tiene la extensión .pem, que el servidor XenMobile no puede importar. [#631795]

Como solución temporal, asegúrese de que XenMobile tiene el certificado SAML correcto, de este modo:

1. Exporte el certificado SAML desde XenMobile 9 App Controller con una clave privada ([AppController.ejemplo.com](#)). Ese certificado tiene el formato PEM y la extensión .pem.
2. Use el comando openssl para generar un archivo PFX a partir del archivo PEM:  

```
openssl pkcs12 -export -out certificate.pfx -in certificate.pem
```
3. Importe el archivo PFX en XenMobile 10.3 como almacén de claves SAML.
4. Exporte el certificado SAML sin la clave privada desde XenMobile 10.4 y después cárguelo en el dominio de Android for Work.

# Arquitectura

Mar 02, 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, quiere conceder a los usuarios de la organización acceso remoto a las aplicaciones para móvil y necesita realizar un seguimiento de los tipos de dispositivos a los que se conectan los usuarios. En este caso, implementaría XenMobile con NetScaler Gateway. Con XenMobile puede administrar aplicaciones y dispositivos, mientras que NetScaler Gateway permite a los usuarios conectarse a la red.

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

- Conexiones a la red interna. Si se trata de usuarios remotos, pueden conectarse mediante una conexión VPN o Micro VPN a través de NetScaler Gateway para acceder a aplicaciones y escritorios de la red interna.
- Inscripción de dispositivos. Los usuarios pueden inscribir dispositivos móviles en XenMobile para que estos se puedan administrar en la consola de XenMobile que se conecta a los recursos de red.
- Aplicaciones Web, SaaS y para móvil. Los usuarios pueden acceder a 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 todas o algunas de estas funciones, Citrix recomienda implementar componentes de XenMobile en el siguiente orden:

- NetScaler Gateway. Puede configurar parámetros en NetScaler Gateway para habilitar la comunicación con XenMobile, StoreFront o la Interfaz Web mediante el asistente de configuración rápida. Antes de usar el asistente de configuración rápida en NetScaler Gateway, debe instalar XenMobile, StoreFront o la Interfaz Web para poder establecer la comunicación con él.
- XenMobile. Después de instalar XenMobile, puede configurar las directivas y los parámetros en la consola de XenMobile, lo que permite a los usuarios inscribir sus dispositivos móviles. También puede configurar aplicaciones Web, SaaS y para móvil. Las aplicaciones para móvil pueden incluir aplicaciones procedentes del App Store o de Google Play. Los usuarios también pueden conectarse a aplicaciones para móvil empaquetadas con MDX Toolkit y cargadas en la consola.
- MDX Toolkit. MDX Toolkit puede empaquetar de forma segura 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 respalda una solución integrada que ofrece la administración de dispositivos y la administración de aplicaciones

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

En un entorno de producción, Citrix recomienda implementar la solución XenMobile en una configuración de clúster. Con ello, se obtiene escalabilidad y redundancia de servidores. Además, aprovechar la funcionalidad de la descarga de SSL de NetScaler puede reducir más la carga del servidor XenMobile y aumentar el rendimiento. Para obtener más información sobre cómo instalar una agrupación en clústeres en XenMobile 10.x configurando dos direcciones IP virtuales de equilibrio de carga en NetScaler, consulte [Agrupación en clústeres](#).

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

En las siguientes secciones, se describen las diferentes arquitecturas de referencia para la implementación de XenMobile. Para obtener más información acerca de los diagramas de arquitectura, consulte los artículos [Reference Architecture for On-Premises Deployments](#) y [Reference Architecture for Cloud Deployments](#) en "XenMobile Deployment Handbook". Para ver una lista completa de los puertos, consulte [Requisitos de puertos](#).

### **Modo de administración de dispositivos móviles (MDM)**

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

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

### **Modo de administración de aplicaciones móviles (MAM)**

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

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

### **Modo MDM+MAM**

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

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

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

# Requisitos del sistema y compatibilidad

Mar 02, 2017

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

- [Compatibilidad de XenMobile](#)
- [Plataformas de dispositivos respaldados](#)
- [Requisitos de puertos](#)
- [Escalabilidad](#)
- [Licencia](#)
- [Cumplimiento del estándar FIPS 140-2](#)
- [Respaldo para idiomas](#)

Para ejecutar XenMobile 10.4, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 7.0, 6.5.x o 6.2.x); para obtener información más detallada, consulte [XenServer](#).
  - VMware (versiones compatibles: ESXi 5.1, ESXi 5.5 o ESXi 6.0). Para obtener información más detallada, consulte [VMware](#).
  - 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
- 50 GB de espacio en disco

XenMobile 10.4.x requiere el servidor de licencias de Citrix 11.12.1 o una versión posterior.

## Requisitos del sistema para NetScaler Gateway

Para ejecutar NetScaler Gateway con XenMobile 10.4, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - XenServer (versiones respaldadas: 6.2.x, 6.1.x o 6.0.x)
  - VMware (versiones respaldadas: ESXi 4.1, ESXi 5.1, ESXi 5.5 o ESXi 6.0)
  - Hyper-V (versiones respaldadas: Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2)
- Dos CPU virtuales
- 2 GB de RAM
- 20 GB de espacio en disco

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

## Requisitos de base de datos para XenMobile 10.4

XenMobile requiere una de las siguientes bases de datos:

- Microsoft SQL Server

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

Server, consulte [Microsoft SQL Server](#)):

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

XenMobile 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 información acerca de SQL Server 2014. Si usa otra versión de servidor, selecciónela en la lista **Otras versiones**:

[Configuración del servidor: cuentas de servicio](#)

[Configurar los permisos y las cuentas de servicio de Windows](#)

[Roles de nivel de servidor](#)

- PostgreSQL

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

**Nota:** Todas las ediciones de XenMobile admiten Remote PostgreSQL 9.5.2 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 3.6  
StoreFront 3.5  
StoreFront 3.0  
StoreFront 2.6  
Interfaz Web 5.4  
XenApp y XenDesktop 7.9  
XenApp y XenDesktop 7.8  
XenApp y XenDesktop 7.7  
XenApp y XenDesktop 7.6  
XenApp y XenDesktop 7.5  
XenApp 6.5

Requisitos de servidor de correo de XenMobile 10.4

XenMobile 10.4 respalda el uso de los siguientes servidores de correo:

- Exchange 2016
- Exchange 2013
- Exchange 2010

# Requisitos de puertos

Mar 02, 2017

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

## Apertura de puertos de NetScaler Gateway y XenMobile para administrar aplicaciones

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

Puerto TCP	Descripción	Origen	Destino
21 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	El puerto XML y Secure Ticket Authority (STA) se usa para la enumeración, la generación de tickets y la autenticación.	Tráfico de red XML de StoreFront y de la Interfaz Web	XenDesktop o XenApp
443	Citrix recomienda el uso del puerto 443.	STA de NetScaler Gateway	
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 para móvil (MAM).	XenMobile NetScaler Gateway Dispositivos Internet	XenMobile
4443	Se utiliza para que un administrador acceda a la consola de XenMobile a través del explorador.	Punto de acceso (explorador)	XenMobile
	Se utiliza para la descarga de registros y paquetes de asistencia de todos los nodos en clúster de XenMobile desde un nodo.	XenMobile	XenMobile
27000	Puerto predeterminado utilizado para acceder al servidor de licencias de Citrix externo.	XenMobile	Citrix License Server

7279	Puerto predeterminado utilizado para registrar o anular licencias de Citrix.	XenMobile	Demonio de proveedor de Citrix
------	--	-----------	--------------------------------

## Apertura de puertos de XenMobile para administrar dispositivos

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

<b>Puerto TCP</b>	<b>Descripción</b>	<b>Origen</b>	<b>Destino</b>
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	<p>iTunes App Store de Apple (ax.itunes.apple.com y *.mzstatic.com)</p> <p>Programa de compras por volumen de Apple (vpp.itunes.apple.com)</p> <p>Para Windows Phone: login.live.com y *.notify.windows.com</p> <p>Google Play (play.google.com)</p>
80 ó 443	Se utiliza para las conexiones salientes entre XenMobile y la retransmisión de notificaciones SMS de Nexmo.	XenMobile	Servidor de retransmisión de SMS de Nexmo
389	Se usa para conexiones de protocolo LDAP no seguras.	XenMobile	Servidor de autenticación LDAP o Active Directory
443	Se usa para la inscripción y la instalación de agentes para Android y Windows Mobile.	Internet	XenMobile
	Se utiliza para la inscripción y la instalación de agentes en el caso de dispositivos Android y Windows, la consola Web de XenMobile y el cliente Remote Support para la administración	Wi-Fi o red LAN interna	

MDM.

1433	Se utiliza para las conexiones a un servidor remoto de bases de datos (optativo).	XenMobile	Servidor SQL
2195	Se usa para las conexiones salientes del servicio de notificaciones push de Apple (APNs) a gateway.push.apple.com para notificaciones de dispositivos iOS y la inserción de directivas de dispositivo.	XenMobile	Internet (hosts APNs con la dirección IP pública 17.0.0.0/8)
2196	Se usa para las conexiones salientes APNs hacia feedback.push.apple.com para notificaciones de dispositivos iOS y la inserción de directivas de dispositivo.		
5223	Se usa para las conexiones salientes de APNs desde dispositivos iOS en redes Wi-Fi a *.push.apple.com.	Dispositivos iOS en redes Wi-Fi	Internet (hosts APNs con la dirección IP pública 17.0.0.0/8)
8081	Se utiliza para los túneles de aplicaciones desde el cliente optativo Remote Support Client para MDM. El valor predeterminado es 8081.	Remote Support Client	Internet, para túneles de aplicaciones hacia dispositivos de usuario (Android y Windows solamente)
8443	Utilizado para la inscripción de dispositivos iOS y Windows Phone.	Internet  Red LAN y Wi-Fi	XenMobile

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

Esta configuración de puerto garantiza que los dispositivos Android que se conectan desde Secure Hub para Android 10.2 y 10.3 pueden acceder al servicio de detección automática de Citrix ADS (Auto Discovery Service) desde dentro de la red interna. La capacidad de acceder a ADS es importante en el momento de descargar las actualizaciones de seguridad que están disponibles a través del servicio ADS.

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

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

- **Obtener certificados para el servidor XenMobile y NetScaler.** Los certificados deben estar en formato PEM y deben ser un certificado público y no la clave privada.

- **Póngase en contacto con la asistencia técnica de Citrix y solicite la habilitación de la fijación de certificados.**

Durante este proceso, se le pedirán los certificados.

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

Para que Secure Hub 10.2 para Android acceda al servicio ADS, abra el puerto 443 para el nombre de dominio completo (FQDN) y las direcciones IP siguientes:

<b>FQDN</b>	<b>IP address</b>
	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
discovery.mdm.zenprise.com	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

# Escalabilidad y rendimiento

Mar 02, 2017

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 poder determinar los requisitos de infraestructura para el rendimiento y la escalabilidad de implementaciones pequeñas, medianas y grandes locales de XenMobile 10.4.

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 reconectar con 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 de sesión pueden reconectarse con 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 llevaron a cabo usando NetScaler Gateway 7500 (para implementaciones de un máximo de 10 000 dispositivos) y NetScaler Gateway 5550 (para implementaciones de más de 10 000 dispositivos). 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	Hasta 60000 dispositivos	
Tasa de inicio de sesión	Velocidad de reconexión de los usuarios existentes	Un máximo de 7500 dispositivos por hora
Configuración	NetScaler Gateway	MPX 7500, MPX 5550
	XenMobile Enterprise Edition	Clúster de 5 nodos del servidor XenMobile
	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.

<b>Cantidad de dispositivos</b>	10000	30.000	45.000	60.000
<b>Tasa de reconexión de dispositivos existentes por hora</b>	833	3750	5.625	7500
<b>Modo del servidor XenMobile</b>	Autónomo	Clúster	Clúster	Clúster
<b>Clúster de servidores XenMobile</b>	N/D	3	4	5
<b>Dispositivo virtual de servidor XenMobile</b>	Memoria = 12 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 6	Memoria = 24 GB de RAM Unidades vCPU = 8	Memoria = 24 GB de RAM Unidades vCPU = 8
<b>Active Directory</b>	Memoria = 8 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 4	Memoria = 16 GB de RAM Unidades vCPU = 4
<b>Base de datos externa de Microsoft SQL Server</b>	Memoria = 32 GB de RAM Unidades vCPU = 16	Memoria = 32 GB de RAM Unidades vCPU = 12	Memoria = 48 GB de RAM Unidades vCPU = 4, con 4 núcleos cada una	Memoria = 48 GB de RAM Unidades vCPU = 4, con 4 núcleos cada una

Para implementaciones de 45000 dispositivos, el servidor SQL Server se ha optimizado para aumentar el número de subprocesos de trabajo a 2000. Para implementaciones de 60.000 dispositivos, el servidor SQL Server se ha optimizado para aumentar el número de subprocesos de trabajo a 3.000. (Para obtener información sobre cómo establecer el número de subprocesos de trabajo de SQL Server, consulte el artículo de Microsoft, [Configure the max worker threads Server Configuration Option](#)).

## Perfil de escalabilidad

Estas tablas resumen el perfil de prueba utilizado para derivar los datos descritos en este artículo:

--	--

Configuración de Active Directory	Perfil utilizado
Usuarios	100000
Grupos	200.000
Niveles de anidamiento	5

Configuración del servidor XenMobile	Total	Por usuario
Directivas	20	20
Apps	270	50
Aplicación pública	200	0
MDX	50	30
Web & SaaS	20	20
Acciones	50	
Grupos de entrega	20	
Grupos de Active Directory por grupo de entrega	10	

SQL	
Número 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 nodos del servidor XenMobile están sujetos a condiciones de carga más altas de las normales, porque los dispositivos que se reconectan obtienen todas las directivas de seguridad que les corresponden. 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 servidor XenMobile.

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 "Arquitectura de referencia de núcleo MDM + MAM" 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 probó la plataforma Windows.
- El envío de directivas se ha probó en dispositivos iOS y Android.
- Cada nodo de servidor XenMobile admite un máximo de 10000 dispositivos de forma simultánea.

# Licencia

Mar 02, 2017

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

Para obtener más información sobre el sistema de licencias de NetScaler Gateway, consulte [Licencias](#) en la documentación de NetScaler Gateway. XenMobile usa Citrix Licensing para administrar las licencias. Para obtener más información acerca de Citrix Licensing, consulte [El sistema de licencias de Citrix](#).

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

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

## Nota

XenMobile 10.4.x requiere Citrix License Server 11.12.1 o una versión posterior; las versiones anteriores del servidor de licencias no funcionan con XenMobile 10.4.x.

## Important

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

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

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

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

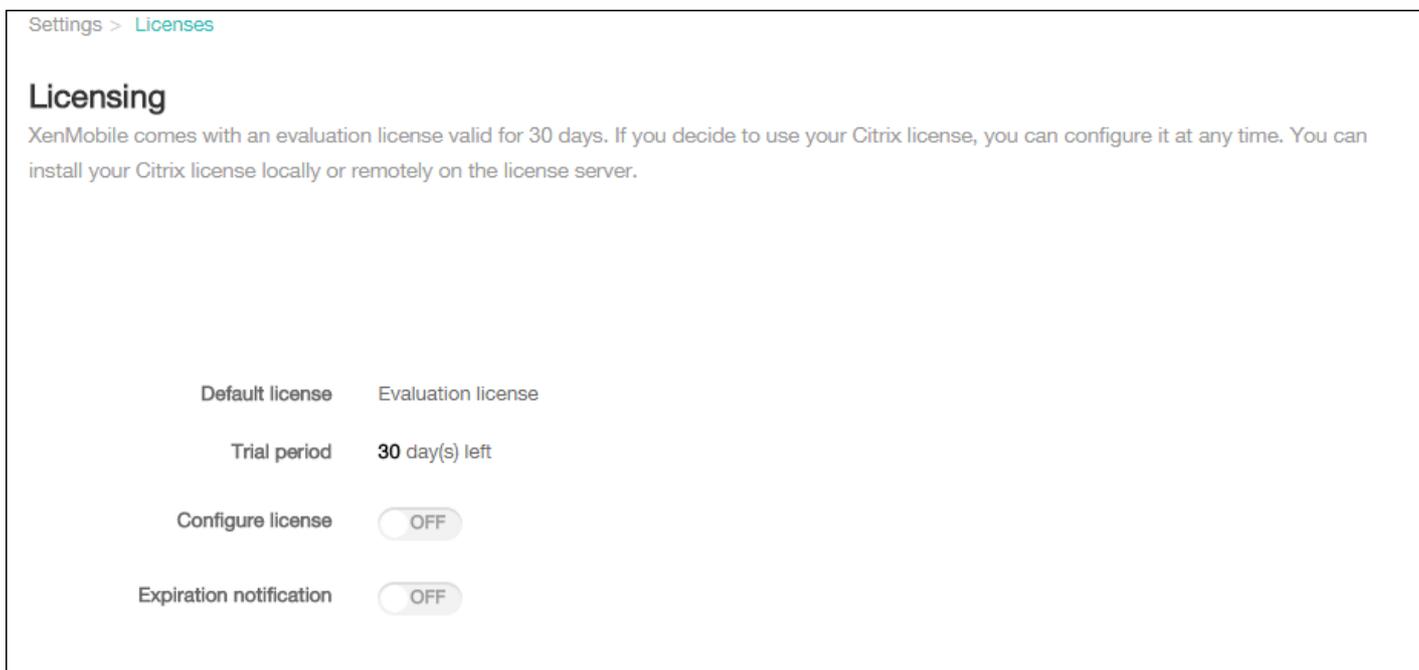
Aunque XenMobile permite cargar varias licencias, solo se puede activar una licencia en un momento dado.

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

dispositivos. Por ejemplo, no se pueden inscribir usuarios o dispositivos nuevos, además de que las configuraciones y las aplicaciones implementadas en los dispositivos inscritos no se pueden actualizar. Para obtener más información acerca de los programas y los modelos de licencia de XenMobile, consulte las [licencias de XenMobile](#).

Para encontrar la página Licensing en la consola de XenMobile

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



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

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

Para agregar una licencia local

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

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

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

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

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

4. Establezca **Configure license** en **On**. Aparecerán la lista **License type**, el botón **Add** y la tabla **Licensing**. La tabla **Licensing** contiene las licencias que haya usado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.

Settings > Licenses

### Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

Default license: Evaluation license

Trial period: 30 day(s) left

Configure license: **ON**

License type: Local license

Add

Product Name	Active	Total number of licenses	Number used	Type	Expires on
No results found.					

Expiration notification: OFF

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**.

### Add New License

License File: Choose File No file chosen

Cancel Upload

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.

The screenshot shows the Citrix Licensing interface. At the top, there is a 'License type' dropdown menu set to 'Local license'. Below it are 'Add' and 'Delete All' buttons. A table displays the following data:

Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition Device	✓	15002	0	Retail	01-DEC-2015

Below the table, it says 'Showing 1 - 1 of 1 items' and 'Expiration notification' is set to 'OFF'.

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

Para agregar una licencia remota

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

1. En la página **Licensing**, establezca **Configure license** en **On**. Aparecerán la lista **License type**, el botón **Add** y la tabla **Licensing**. La tabla **Licensing** contiene las licencias que haya usado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.

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

The screenshot shows the Citrix Licensing interface for configuring a remote license. The 'License type' dropdown is set to 'Remote license'. There are input fields for 'License server\*' and 'Port\*' (set to 27000). A green 'Test Connection' button is visible. Below the form is a table with the following data:

Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

4. Configure los siguientes parámetros:

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

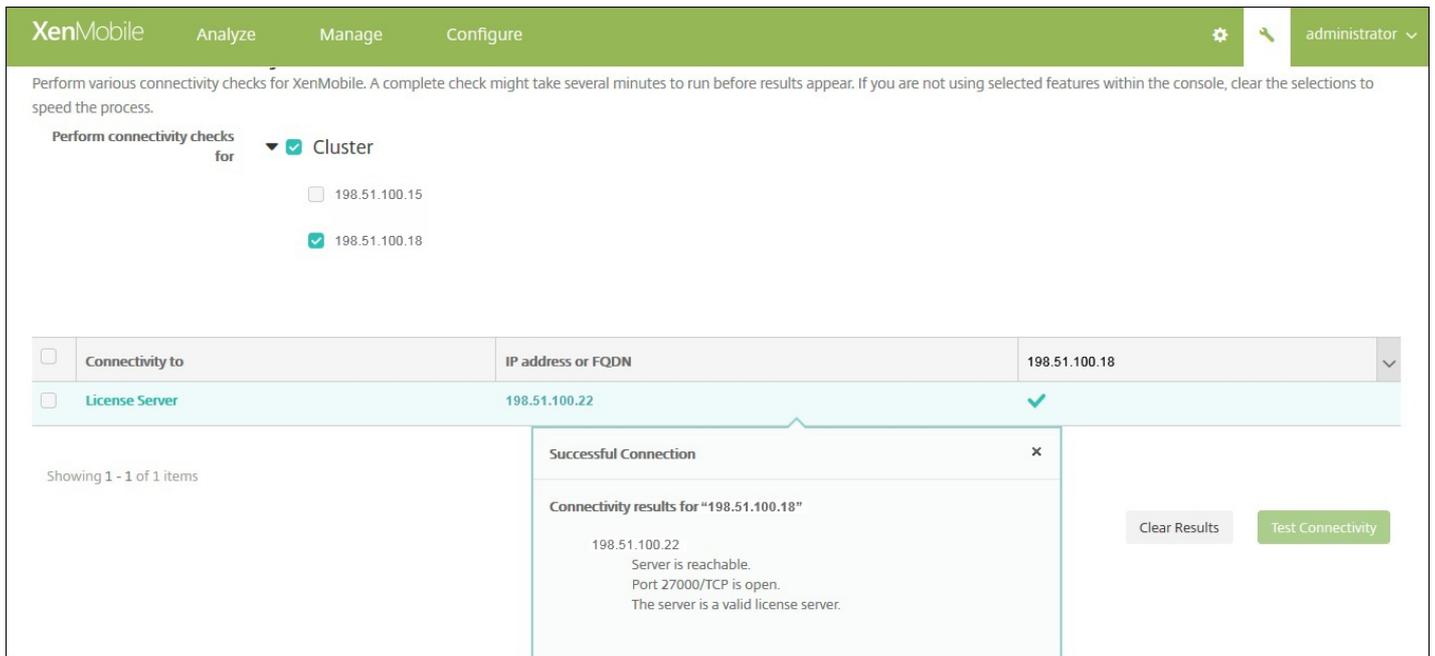
5. Haga clic en **Test Connection**. Si la conexión es satisfactoria, XenMobile se conecta al servidor de Citrix Licensing, y la

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

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

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

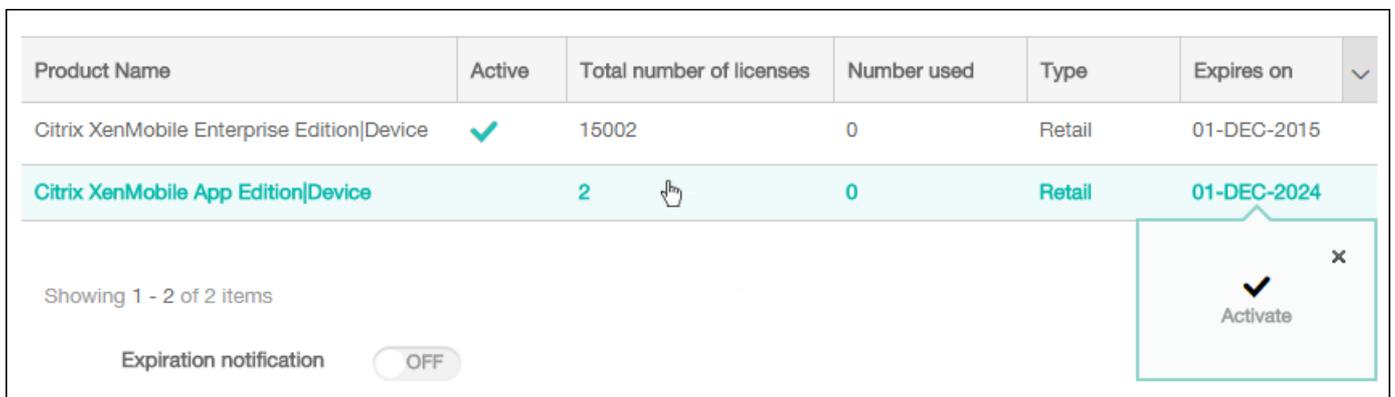
Si no se puede establecer la conexión, revise el mensaje de error que se muestra, realice las correcciones necesarias y, a continuación, haga clic en **Test Connection**.



## Para activar una licencia diferente

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

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



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

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

## Important

Si activa la licencia seleccionada, la licencia actualmente activa se desactiva.

### Para automatizar una notificación de caducidad

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

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

The screenshot shows the 'Expiration notification' configuration page. At the top, there is a toggle switch labeled 'Expiration notification' which is currently turned 'ON'. Below this, there are three main configuration sections:

- Notify every\***: A text input field containing the number '7', followed by the text 'day(s)'. To the right of this is another text input field containing the number '60', followed by the text 'day(s) before expiration'.
- Recipient\***: A text input field with the placeholder text 'Enter email address(es)'.
- Content\***: A large text area containing the text 'License expiry notice'.

2. Configure los siguientes parámetros:

- En **Notify every**, escriba:
  - La frecuencia con que se enviarán las notificaciones; por ejemplo, cada 7 días.
  - Cuándo se comienza a enviar la notificación; por ejemplo, 60 días antes de que caduque la licencia.
- **Recipient**. Escriba su dirección de correo electrónico o la de la persona responsable de la licencia.
- **Content**. Escriba el mensaje de notificación de caducidad que el destinatario verá en la notificación.

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

# Cumplimiento del estándar FIPS 140-2

Mar 02, 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: Solo puede habilitar el modo FIPS de XenMobile durante la instalación inicial.

Nota: Los modos de XenMobile de solo administración de dispositivos móviles (MDM) o de solo administración de aplicaciones para móvil (MAM), así como XenMobile Enterprise, cumplen el estándar FIPS mientras no se usen aplicaciones HDX.

En iOS, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" utilizan módulos de cifrado certificados por FIPS que proporcionan OpenSSL y Apple. En Android, todas las operaciones de cifrado de "Data in Transit" y de "Data at Rest" desde el dispositivo móvil a NetScaler Gateway utilizan módulos de cifrado certificados por FIPS que proporciona OpenSSL.

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

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

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

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

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

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

# Respaldo para idiomas

Mar 02, 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 traducida al idioma preferido del usuario. Para obtener más información sobre el respaldo para globalización para todos los productos Citrix, consulte <http://support.citrix.com/article/CTX119253>.

Este artículo indica los idiomas respaldados en XenMobile 10.4.

## Consola de XenMobile

- Francés
- Alemán
- Coreano
- Portugués
- Chino simplificado

## Aplicaciones XenMobile

Una "X" indica que la aplicación está disponible en ese idioma concreto. Actualmente, 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	Solo iOS
Ruso	X	X	X	X	X	X

## 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

La tabla siguiente resume el respaldo para texto de idiomas de Oriente Medio, para cada aplicación. La "X" indica que la característica está disponible para esa plataforma. El respaldo para idiomas escritos de derecha a izquierda no está

disponible para dispositivos Windows.

	<b>iOS</b>	<b>Android</b>
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

Mar 02, 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	

<p>Identifique y escriba el nombre de host de NetScaler Gateway.</p> <p>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.</p>	<p>NetScaler Gateway</p>	
<p>Escriba la dirección IP de XenMobile.</p> <p>Reserve una dirección IP si instala una instancia de XenMobile.</p> <p>Si configura un clúster, escriba todas las direcciones IP que necesita.</p>	<p>XenMobile</p>	
<ul style="list-style-type: none"> <li>• Una dirección IP pública configurada en NetScaler Gateway</li> <li>• Una entrada DNS externa para NetScaler Gateway</li> </ul>	<p>NetScaler Gateway</p>	
<p>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).</p> <p>Nota: Puede utilizar el sAMAccountName o el nombre principal de usuario (UPN) al configurar el nombre de usuario para el proxy Web.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
<p>Escriba la dirección IP de la puerta de enlace predeterminada.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
<p>Escriba la dirección IP del sistema (NSIP) y la máscara de subred.</p>	<p>NetScaler Gateway</p>	
<p>Escriba la dirección IP de subred (SNIP) y la máscara de subred.</p>	<p>NetScaler Gateway</p>	
<p>Escriba la dirección IP del servidor virtual de NetScaler Gateway y el nombre de dominio completo (FQDN) del certificado.</p> <p>Si necesita configurar varios servidores virtuales, escriba todas las direcciones IP virtuales y los nombres FQDN de los certificados.</p>	<p>NetScaler Gateway</p>	
<p>Escriba las redes internas a las que pueden acceder los usuarios a través de NetScaler Gateway.</p> <p>Ejemplo: 10.10.0.0/24.</p>	<p>NetScaler Gateway</p>	

	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 [El sistema de licencias de Citrix](#).

•	Requisitos previos	Componente	Escriba la ubicación
	Obtenga licencias universales del <a href="#">sitio Web de Citrix</a> . Para obtener información más detallada, consulte <a href="#">Licencias</a> 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
	<p>Puerto y dirección IP de Microsoft SQL Server.</p> <p>Compruebe que la cuenta de servicio de SQL Server que se va a usar en XenMobile tiene el permiso del rol DBcreator.</p>	XenMobile	

## Parámetros de Active Directory

•	Requisitos previos	Componente	Escriba el parámetro
	<p>Escriba el puerto y la dirección IP de Active Directory de los servidores principales y secundarios.</p> <p>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.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
	<p>Escriba el nombre de dominio de Active Directory.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
	<p>Escriba la cuenta de servicio de Active Directory, que requiere un ID de usuario, una contraseña y un alias de dominio.</p> <p>La cuenta de servicio de Active Directory es la cuenta que XenMobile utiliza para consultar a Active Directory.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
	<p>Escriba el DN base de usuario.</p> <p>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.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	
	<p>Escriba el DN base de grupo.</p> <p>Este es el nivel de directorio en el que se encuentran los grupos.</p>	<p>XenMobile</p> <p>NetScaler Gateway</p>	

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 seguir los siguientes pasos. Para obtener más información, consulte la documentación de [XenServer](#) o [VMware](#).

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

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

- Instale Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2 con Hyper-V y sus roles habilitados en un equipo que disponga de los recursos de sistema adecuados. Cuando instale el rol Hyper-V, asegúrese de que especifica las tarjetas de interfaz de red (NIC) en el servidor que Hyper-V usará para crear las redes virtuales. Puede reservar algunas tarjetas para el host.
- Elimine el archivo Virtual Machines/<UUID de compilación específico>.xml
- Mueva el archivo Legacy/<UUID de compilación específico>.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 una sesión con su cuenta.
3. Haga clic en la ficha Descargas.
4. En la página Descargas, en la lista de selección de productos, haga clic en XenMobile.



5. Haga clic en Go. Aparecerá la página XenMobile.
6. Expanda XenMobile 10.
7. Haga clic en XenMobile 10.0 Server.
8. En la página XenMobile 10.0 Server, haga clic en Download, situado junto a la imagen virtual apropiada que hay que usar para instalar XenMobile en XenServer, VMware o Hyper-V.
9. Siga las instrucciones en pantalla para descargar el software.

## Para descargar el software de NetScaler Gateway

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

1. Vaya al [sitio Web de Citrix](#).
2. Si todavía no ha iniciado sesión en el sitio Web de Citrix, haga clic en Iniciar sesión junto al cuadro de búsqueda e inicie una sesión con su cuenta.
3. Haga clic en la ficha Descargas.
4. En la página Descargas, en la lista de productos, haga clic en NetScaler Gateway.
5. Haga clic en Go. Aparecerá la página NetScaler Gateway.
6. En la página NetScaler Gateway, expanda la versión de NetScaler Gateway que se está ejecutando.
7. Debajo de Firmware, haga clic en la versión del software de dispositivo que desea descargar.  
Nota: También puede hacer clic en Virtual Appliances para descargar NetScaler VPX. Cuando se selecciona esta opción, se recibe una lista de software para la máquina virtual para cada hipervisor.
8. Haga clic en la versión de software del dispositivo que desea descargar.
9. En la página de software del dispositivo correspondiente a la versión que quiere descargar, haga clic en Download para descargar el dispositivo virtual.
10. Siga las instrucciones en pantalla para descargar el software.

## Configuración de XenMobile para el primer uso

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

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

### Nota

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

## Configuración de XenMobile en la ventana del símbolo del sistema

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

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the initial configuration of XenMobile. Accept options offered by pressing Enter/Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the command prompt.
Username: admin
New password: █
```

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

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

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

```
Network settings:
IP address: 192.0.2.0
Netmask: 225.225.225.128
Default gateway: 203.0.113.3
Primary DNS server: 192.0.2.4
Secondary DNS server [optional]: 192.0.2.5
Commit settings [y/n]: y
```

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

5. Introduzca 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 pulsar 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, debe facilitar su propia frase secreta. No se puede ver la frase secreta si se ha seleccionado una frase secreta aleatoria.

```
Encryption passphrase:
Generate a random passphrase to secure the server data? [y/n]: y
```

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](#).

```
Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:
```

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

```
Database connection:
Local or remote [l/r]: r
Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
Use SSL [y/n]: n
Server: 198.0.2.10
Port: 5432
Username: postgres
Password:
```

1. La base de datos puede ser local o remota. Introduzca l para local, o r para remota.

2. Seleccione el tipo de base de datos. Introduzca m para Microsoft SQL o introduzca 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, introduzca 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 la base de datos si es diferente del número de puerto predeterminado. El puerto predeterminado para Microsoft SQL es 1433 y el puerto predeterminado para PostgreSQL es 5432.

6. Introduzca el nombre de usuario del administrador de la base de datos.

7. Introduzca la contraseña del administrador de la base de datos.

8. Introduzca el nombre de la base de datos.

9. Presione **Entrar** para confirmar los parámetros de la base de datos.

8. Si quiere, introduzca y para habilitar la organización en clúster de nodos o instancias de XenMobile.

Importante: Si habilita un clúster de XenMobile, después de completarse la configuración del sistema, abra el puerto 80 para habilitar la comunicación en tiempo real entre miembros del clúster. Esto debe hacerse en todos los nodos del clúster.

9. Introduzca el nombre de dominio completo (FQDN) del servidor XenMobile.

```
XenMobile hostname:  
Hostname: justan.example.com
```

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).

```
HTTP [80]: 80  
HTTPS with certificate authentication [443]: 443  
HTTPS with no certificate authentication [8443]: 8443  
HTTPS for management [4443]: 4443
```

12. Omita la siguiente pregunta acerca de la actualización de una versión anterior de XenMobile ya que está instalando XenMobile por primera vez.

13. Introduzca 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](#).

```
The wizard will now generate an internal Public Key Infrastructure (PKI):  
- A root certificate  
- An intermediate certificate to issue device certificates during enrollment  
- An intermediate certificate to issue an SSL certificate  
- An SSL certificate for your connectors  
Do you want to use the same password for all the certificates of the PKI [y]:  
New password:  
Re-enter new password:
```

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.

```
XenMobile console administrator account:  
This is the user name and password you use when logging on to the XenMobile console through a web browser.  
Username [administrator]: administrator  
Password:  
Re-enter new password:
```

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.

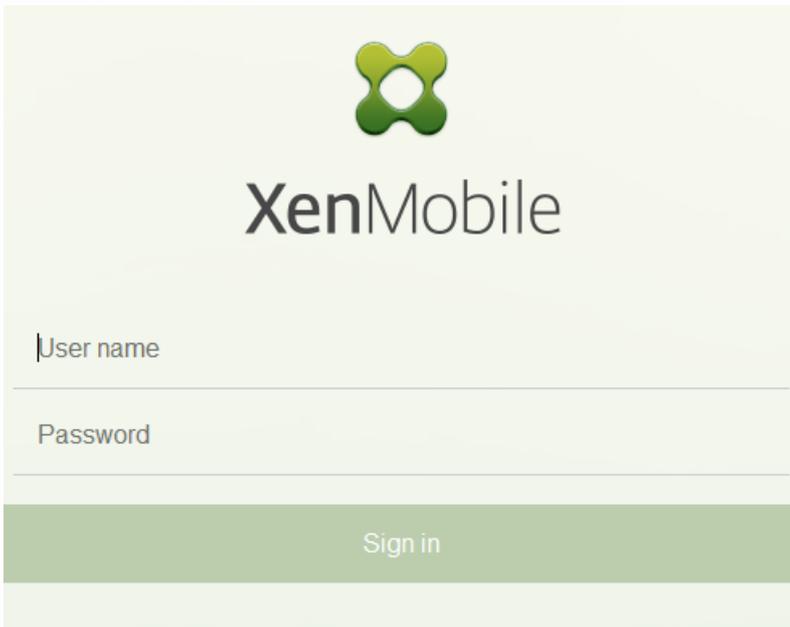
```
Writing iptables configuration...  
Restarting iptables...  
  
Initial system configuration complete!  
  
Upgrade:  
Upgrade from previous release (y/n) [n]:  
  
Stopping configuration app... [ OK ]  
Starting configuration app... [ OK ]  
  application started successfully  
Stopping main app... [ OK ]  
Starting main app...  
  this may take a few minutes.....  
.....  
  application started successfully [ OK ]  
  
To access the console, from a web browser, go to the following location and  
log on with your console credentials:  
https://203.0.113.8:4443/  
  
Starting monitoring... [ OK ]
```

## 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.

En el explorador Web, vaya a la ubicación proporcionada al final de la configuración en la ventana del símbolo del sistema.

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.

The image shows the XenMobile login interface. At the top center is the XenMobile logo, a green four-lobed shape. Below the logo is the text "XenMobile" in a dark grey font. Underneath, there are two input fields: "User name" and "Password", both with light green borders. Below the password field is a green button with the text "Sign in" in white.

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 el certificado de escucha de SSL y APNs. 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 de 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

Mar 02, 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 Server, consulte los [Manuales de SQL Server](#).
- Para la comunicación SSL segura se necesita instalar un certificado SSL en el servidor SQL Server. El certificado SSL puede ser un certificado público de una entidad de certificación (CA) comercial, o un certificado autofirmado de una CA interna. SQL Server 2014 no puede aceptar un certificado comodín. Por tanto, Citrix recomienda solicitar un certificado SSL con el nombre de dominio completo (FQDN) del servidor SQL Server.
- Si usa un certificado autofirmado para el servidor SQL Server, necesitará una copia del certificado raíz de la CA que emitió su certificado autofirmado. El certificado raíz de la CA debe importarse en el servidor XenMobile durante la instalación.

## Configuración del modo FIPS

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

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

1. Durante la instalación inicial, habilite **FIPS mode**.
2. Cargue el certificado raíz de la CA para el servidor SQL Server. Si usó un certificado SSL autofirmado en lugar de un certificado público en el servidor SQL Server, elija **Yes** para esta opción, y lleve a cabo una de las acciones siguientes:
  - a. Copie y pegue el certificado de la CA.
  - b. Importe el certificado de la CA. Para importar el certificado de la CA, debe publicar el certificado en un sitio Web que sea accesible desde el servidor XenMobile a través de una URL con HTTP. Para obtener más información, consulte la sección [Importación de certificados](#) más adelante en este artículo.
3. Especifique el nombre del servidor y el puerto del servidor SQL Server, las credenciales para iniciar sesión en SQL Server y el nombre de la base de datos que se debe crear para XenMobile.

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

4. Para usar una cuenta de Active Directory, introduzca las credenciales con el formato dominio\nombre-de-usuario.
5. Una vez completados estos pasos, continúe con la instalación inicial de XenMobile.

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

### Importación de certificados

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

## Requisitos previos de SQL

1. La conexión con la instancia SQL desde XenMobile necesita ser segura y la versión debe ser SQL Server 2012 o SQL Server 2014. Para proteger la seguridad de la conexión, consulte [Cómo habilitar el cifrado SSL para una instancia de SQL Server usando Microsoft Management Console](#).
2. Si el servicio no se reinicia correctamente, compruebe lo siguiente: Abra **Services.msc**.
  - a. Copie la información de cuenta de inicio de sesión utilizada para el servicio SQL Server.
  - b. Abra MMC.exe en SQL Server.
  - c. Vaya a **Archivo > Agregar o quitar complemento** y luego haga doble clic en el elemento Certificados para agregar el complemento Certificados. Seleccione Cuenta de equipo y Equipo local en las dos páginas siguientes del asistente.
  - d. Haga clic en **Aceptar**.
  - e. Expanda **Certificados (Equipo local) > Personal > Certificados** y busque el certificado SSL importado.
  - f. Haga clic con el botón secundario en el certificado importado (seleccionado en el Administrador de configuración de SQL Server) y haga clic en **Todas las tareas > Administrar claves privadas**.
  - g. En **Nombres de grupos o usuarios**, haga clic en **Agregar**.
  - h. Introduzca el nombre de la cuenta del servicio SQL que copió en uno de los pasos anteriores.
  - i. Deje sin marcar la casilla de **Permitir control total**. De manera predeterminada, la cuenta del servicio recibe permisos de Control total y Leer, pero en realidad solo necesita leer la clave privada.
  - j. Cierre **MMC** e inicie el servicio SQL.
3. Asegúrese de que el servicio SQL se inicia correctamente.

## Requisitos previos de Internet Information Services (IIS)

1. Descargue el certificado raíz (base 64).
2. Copie el certificado raíz en el sitio Web predeterminado del servidor IIS, C:\inetpub\wwwroot.
3. Marque la casilla **Autenticación** para el sitio predeterminado.
4. Defina el parámetro **Anónimo** como **habilitado**.

5. Marque la casilla de reglas de **Seguimiento de solicitudes con error**.
6. Asegúrese de que .cer no esté bloqueado.
7. Busque la ubicación del archivo .cer en Internet Explorer desde el servidor local, <http://localhost/nombre-certificado.cer>. El texto de certificado raíz aparecerá en el explorador Web.
8. Si el certificado raíz no aparece en Internet Explorer, asegúrese de que ASP está habilitado en el servidor IIS, de este modo.
  - a. Abra Administrador del servidor.
  - b. Vaya al asistente **Administrar > Agregar roles y características**.
  - c. En los roles del servidor, expanda **Servidor web (IIS)**, expanda **Servidor web**, expanda **Desarrollo de aplicaciones** y después seleccione **ASP**.
  - d. Haga clic en **Siguiente** hasta que se complete la instalación.
9. Abra Internet Explorer y vaya a <http://localhost/cert.cer>.

Para obtener más información, consulte [Internet Information Services \(IIS\) 8.5](#).

## Nota

Puede usar la instancia de IIS de la CA para este procedimiento.

## Importación del certificado raíz durante la configuración inicial de FIPS

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

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

# Configuración de la agrupación en clústeres

Mar 02, 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.

```
*****
*           Citrix XenMobile           *
*   (in First Time Use mode)         *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password: _
```

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

```

Network settings:
IP address []: 10.147.75.51
Netmask []: 255.255.255.0
Default gateway []: 10.147.75.1
Primary DNS server []: 10.147.75.240
Secondary DNS server (optional) []:

Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps

```

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

```

Encryption passphrase:
Generate a random passphrase to secure the server data (y/n) [y]:

```

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

```

Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [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".

```

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

```

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

```

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server [l]: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:

```

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

```

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
y
New password:
Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
this may take a few seconds..... [ OK ]
application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes....._

```

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

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

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds.....
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  this may take a few minutes.....^ [ .....
.....
  application started [ OK ]

To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://10.147.75.59:4443/

Starting monitoring... [ OK ]
xms51.wg.lab login: |
```

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**.

XenMobile Analyze Manage Configure administrator

## Support

Diagnostics	Support Bundle	Links
NetScaler Gateway Connectivity Checks XenMobile Connectivity Checks	Create Support Bundles	Citrix Product Documentation Citrix Knowledge Center
Log Operations	Advanced	Tools
Logs Log Settings	Cluster Information Garbage Collection Java Memory Properties Macros PKI Configuration Anonymization and De-anonymization	APNs Signing Utility Citrix Insight Services Device NetScaler Connector Status

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.

XenMobile Support citrix

Support > Cluster Information

### Cluster Information

Provides information about each of the nodes in the cluster.

Cluster Members

Node ID	Node name	Status	Role	First check-in	Next check-in
177425211		ACTIVE	null	2019-04-22 14:40:34.877	2019-04-22 01:02:06.293
177425203		ACTIVE	OLDEST	2019-04-22 14:30:08.47	2019-04-22 02:09:02.61

Showing 1 - 2 of 2 items

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**.

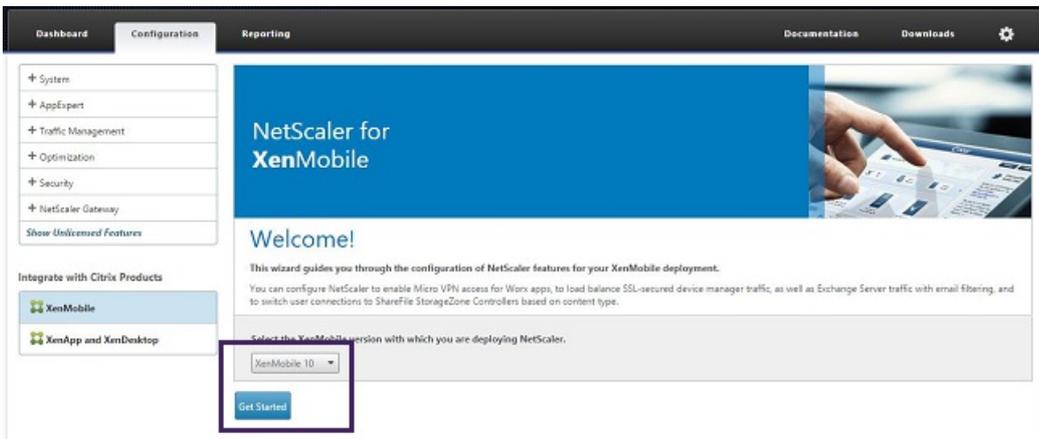
Para configurar el equilibrio de carga para el clúster de XenMobile en NetScaler

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.

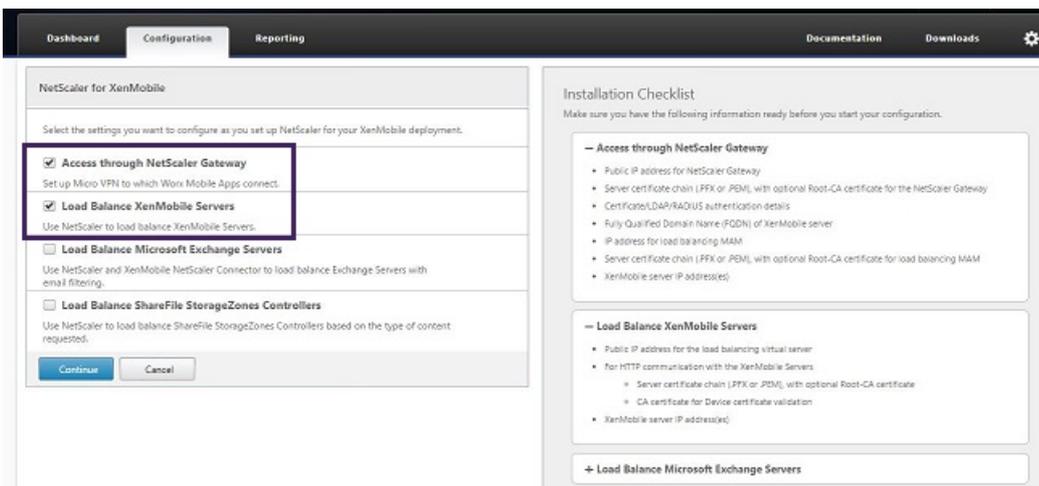
1. Inicie sesión en NetScaler.



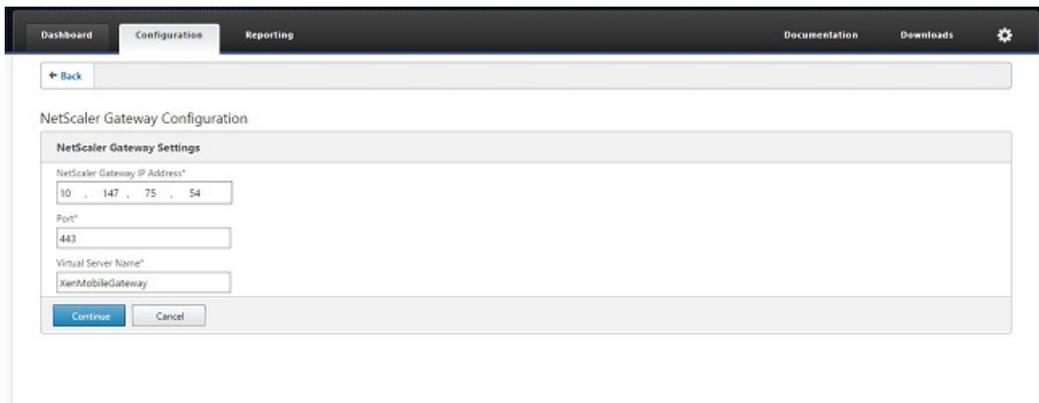
2. En la ficha Configuration, haga clic en XenMobile y en Get Started.



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



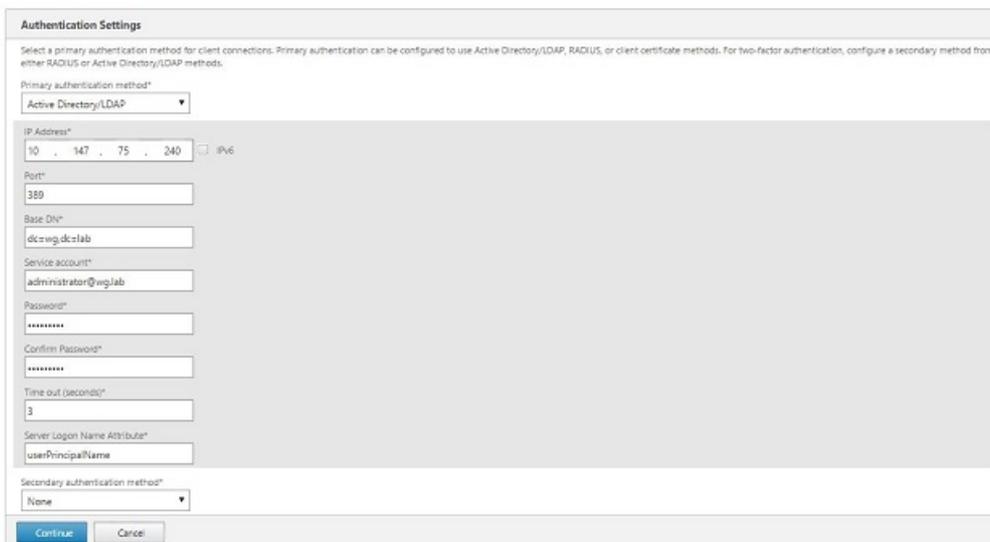
4. Introduzca la dirección IP de NetScaler Gateway y haga clic en Continue.



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 Continúe.
  - 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 Continúe.



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

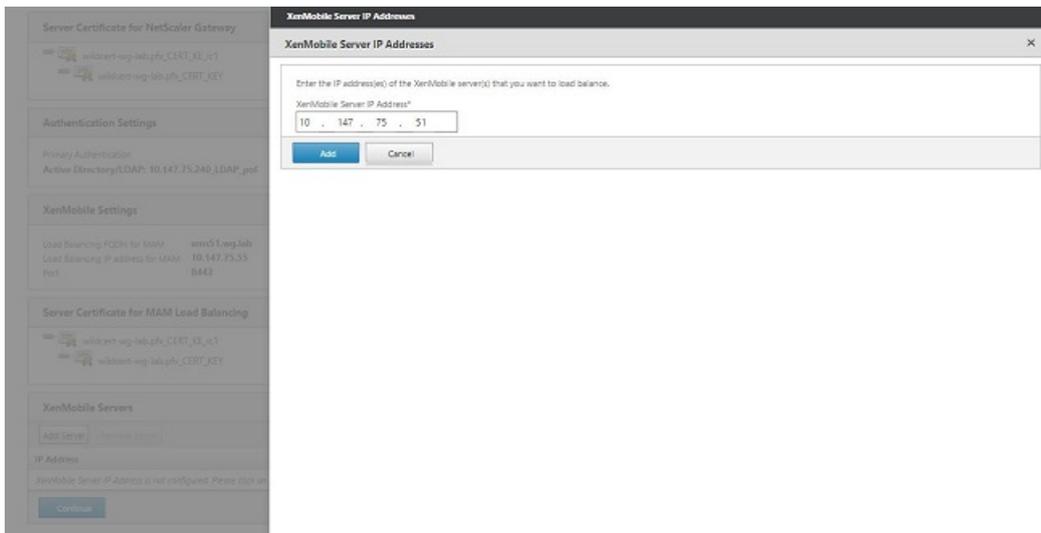
7. En XenMobile Settings, rellene el campo Load Balancing FQDN for MAM y, a continuación, haga clic en Continúe.

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

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

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

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



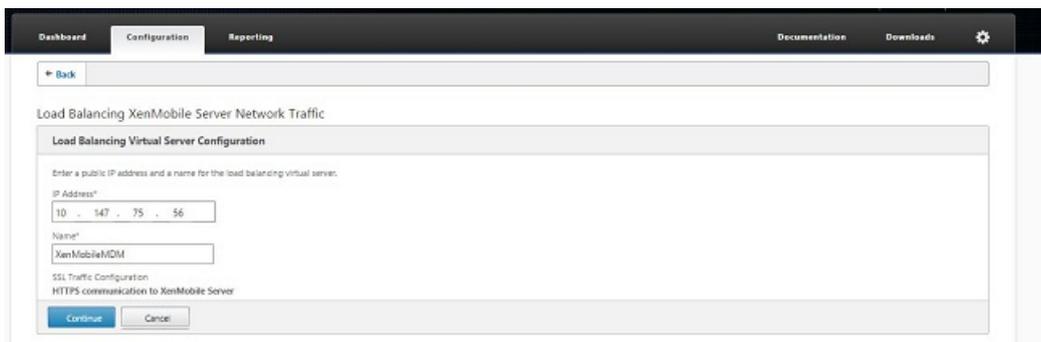
12. Repita los pasos 10 y 11 para agregar nodos de XenMobile adicionales que formen parte del clúster de XenMobile. Verá todos los nodos de XenMobile que haya agregado. Haga clic en Continuar.



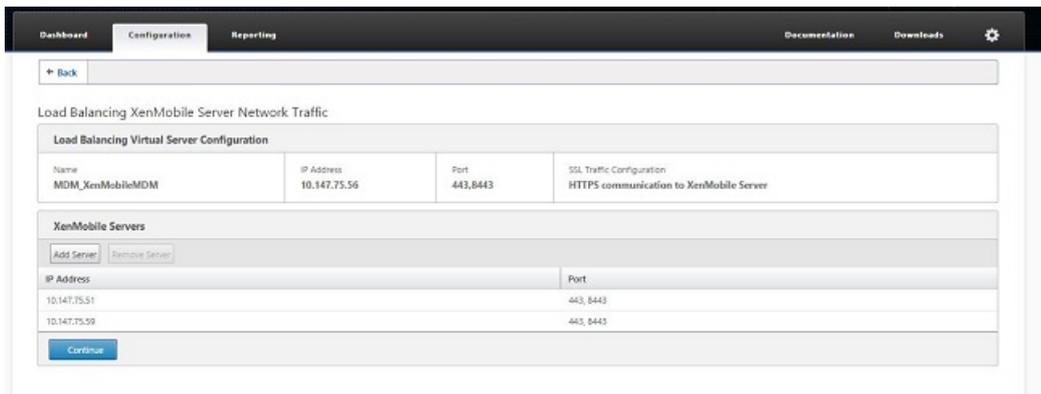
13. Haga clic en Load Balance Device Manager Servers para continuar con la configuración del equilibrio de carga para MDM.



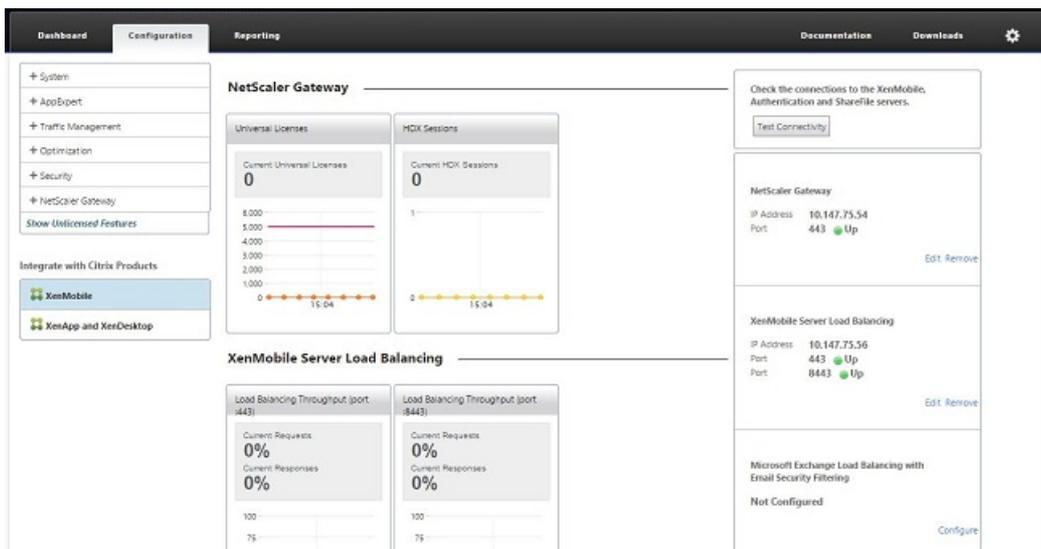
14. Introduzca la dirección IP que se utilizará como la IP de equilibrio de carga para MDM y, a continuación, haga clic en Continue.



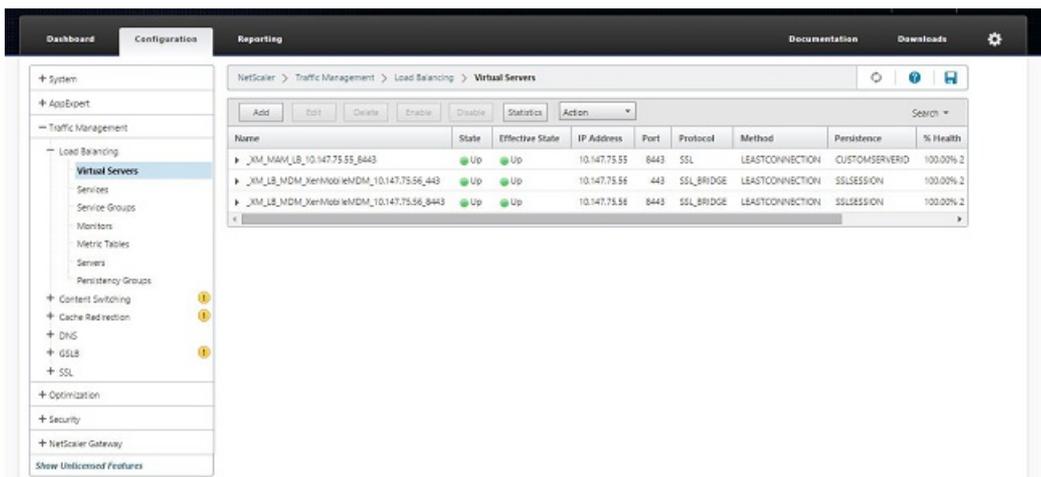
15. Una vez que vea los nodos de XenMobile en la lista, haga clic en Continuar y, a continuación, en Done para finalizar el proceso.



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



- 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.

Dashboard Configuration Reporting Documentation Downloads

NetScaler > Traffic Management > DNS > Records > Address Records

Add Delete Search

Host Name	IP Address	TTL (secs)	Type	OS/B Virtual Server Name
lroot-servers.net	199.7.93.42	3600000	ADNS	-N/A-
lroot-servers.net	192.228.79.201	3600000	ADNS	-N/A-
droot-servers.net	199.7.91.13	3600000	ADNS	-N/A-
jroot-servers.net	192.58.128.93	3600000	ADNS	-N/A-
hroot-servers.net	128.63.2.53	3600000	ADNS	-N/A-
froot-servers.net	192.5.5.241	3600000	ADNS	-N/A-
xms01.wg.lab	10.147.75.55	3600	ADNS	-N/A-
kroot-servers.net	193.0.14.129	3600000	ADNS	-N/A-
aroot-servers.net	198.41.0.4	3600000	ADNS	-N/A-
eroot-servers.net	192.35.4.12	3600000	ADNS	-N/A-
mroot-servers.net	202.12.27.33	3600000	ADNS	-N/A-
lroot-servers.net	192.36.148.17	3600000	ADNS	-N/A-
groot-servers.net	192.112.36.4	3600000	ADNS	-N/A-
e1root-servers.net	192.209.230.10	3600000	ADNS	-N/A-

System  
AppExpert  
Traffic Management  
Load Balancing  
Content Switching  
Cache Redirection  
DNS  
Zones  
Name Servers  
DNS Suffix  
Keys  
Views  
Policy Labels  
Policies  
Actions  
Records  
Address Records  
Canonical Records  
Mail Exchange Records  
Name Server Records  
SOA Records  
SRV Records  
PTR Records

# Guía de recuperación ante desastres

Mar 02, 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

Mar 02, 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, introduzca **2** para seleccionar el menú de sistema.
2. En el menú de sistema, introduzca **6** para seleccionar el menú de servidor proxy.

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

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

```
-----
Choice: [0 - 10] 6
-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

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

```

-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 1

Enter socks proxy information
Address [1]: 203.0.113.23
Port[1]: 1080
Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]: █

```

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

```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 2

Enter https proxy information
Address [1]: 203.0.113.23
Port[]: 4443
Configure username & password [y/n]: y
Username: Justaname
Password:

Target - WEB
WEB proxy configured. Override proxy settings?[y/n]:
```

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

# Propiedades de servidor

Mar 02, 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, editar o eliminar propiedades de servidor.

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**.

### Audit Log Cleanup Execution Time

La hora a la que debe comenzar la limpieza del registro de auditoría, con el formato HH: MM AM/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 el servidor XenMobile debe conservar los registros de auditoría. El valor predeterminado es **1**.

### Audit Logger

Si es **False**, no registra eventos de interfaz de usuario (UI). El valor predeterminado es **False**.

### Audit Log Retention (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de auditoría. El valor predeterminado es **7**.

### 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 se define con un valor de 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 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, es posible aumentar este valor a 60 segundos o más. Un servidor de certificados que no responda al cabo de 120 segundos necesita algún trabajo de mantenimiento. El valor predeterminado es **15000** milésimas de segundo (15 segundos).

### Deploy Log Cleanup (in Days)

La cantidad de días que el servidor XenMobile debe conservar los registros de implementación. El valor predeterminado

es 7.

### **Disable SSL Server Verification**

Si el valor es **True**, se inhabilita la validación de certificado de servidor SSL cuando se cumplen todas las condiciones siguientes: Se ha habilitado la autenticación basada en certificados en el servidor XenMobile, el servidor de la CA de Microsoft es el emisor del certificado y el certificado ha sido firmado por una CA interna cuya raíz no es de confianza para el servidor XenMobile. El valor predeterminado es **True**.

### **Enable/Disable Hibernate statistics logging for diagnostics**

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.

### **Inactivity Timeout in Minutes**

Si la propiedad del servidor **WebServices timeout type** es **INACTIVITY\_TIMEOUT**, esta propiedad define la cantidad de minutos que deben transcurrir antes de que XenMobile cierre la sesión de un administrador inactivo que usó la API pública del servidor XenMobile para acceder a la consola de XenMobile o a una aplicación de terceros. Un tiempo de espera de **0** significa que no se cerrará la sesión del 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 tendrán que 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 introduce sus credenciales durante la inscripción de dispositivos, este valor de propiedad especifica durante cuánto tiempo se espera antes de mostrar un mensaje para pedir la instalación del 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 de 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, cuando 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.

### **MAM\_MACRO\_SUPPORT**

Configura el servidor XenMobile para las implementaciones de solo MAM, de modo que los usuarios con dispositivos iOS o Android que se inscriban en Secure Hub con credenciales de correo electrónico se inscriban automáticamente en Secure Mail. Lo que significa que los usuarios no tienen que introducir información adicional ni realizar pasos adicionales para inscribirse en Secure Mail. Agregue esta clave personalizada y use el valor predeterminado **True** para permitir la inscripción automática con correo electrónico. También se requieren las propiedades de cliente `ENABLE_CREDENTIAL_STORE` y `SEND_LDAP_ATTRIBUTES`.

La primera vez que se usa Secure Mail, este obtiene el ID, el dominio y la dirección de correo electrónico del usuario desde Secure Hub. Secure Mail usa la dirección de correo electrónico para la detección automática. XenMobile identifica al servidor Exchange por el dominio y el ID de usuario, lo que permite a Secure Mail autenticar automáticamente al usuario. XenMobile solicita al usuario que introduzca una contraseña si la directiva está configurada para no transferirla automáticamente, pero no es necesario que el usuario introduzca ninguna información adicional.

### **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 al servidor 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**.

### **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, es posible aumentar este valor a 60 segundos o más. Un servidor de certificados que no responda al cabo de 120 segundos necesita algún trabajo de mantenimiento. El valor predeterminado es **15000** milésimas de segundo (15 segundos).

### **Session Log Cleanup (in Days)**

La cantidad de días que el servidor XenMobile debe conservar los registros de sesiones. El valor predeterminado es **7**.

### **Server Mode**

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.

<b>Sus licencias son para esta edición</b>	<b>Quiere que los dispositivos se registren en este modo</b>	<b>Defina la propiedad Server Mode con el valor</b>
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 el modo de servidor se cambia 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](#).

### **Static Timeout in Minutes**

Si la propiedad del servidor **WebServices timeout type** es **STATIC\_TIMEOUT**, esta propiedad define la cantidad de minutos que deben transcurrir antes de que XenMobile cierre la sesión de un administrador que usó la API pública del servidor XenMobile para acceder a la consola de XenMobile o a una aplicación de terceros. 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**.

### 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**.

### XAM One-Time Ticket

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

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

El tiempo, en minutos, transcurrido el cual XenMobile cierra la sesión de un usuario inactivo en el Self Help Portal de XenMobile. Si especifica un tiempo de espera de **0**, el usuario inactivo permanece conectado, no se cierra su sesión. El valor predeterminado es **30**.

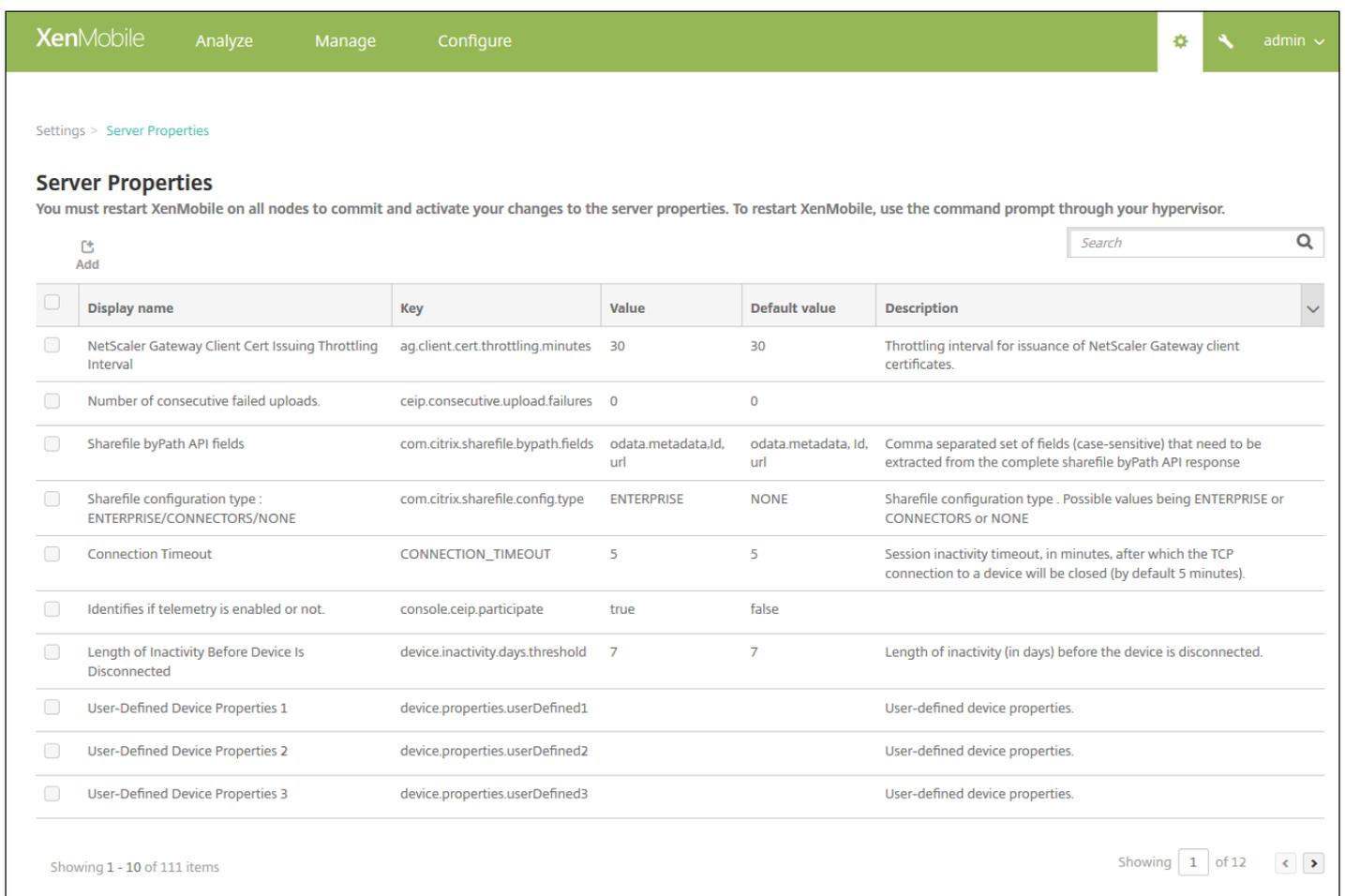
# Cómo agregar, editar o eliminar propiedades de servidor

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

## Nota

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

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.
2. En **Server**, haga clic en **Server Properties**. Aparecerá la página **Server Properties**. Puede agregar, modificar o eliminar propiedades de servidor desde esta página.



XenMobile Analyze Manage Configure admin

Settings > Server Properties

### Server Properties

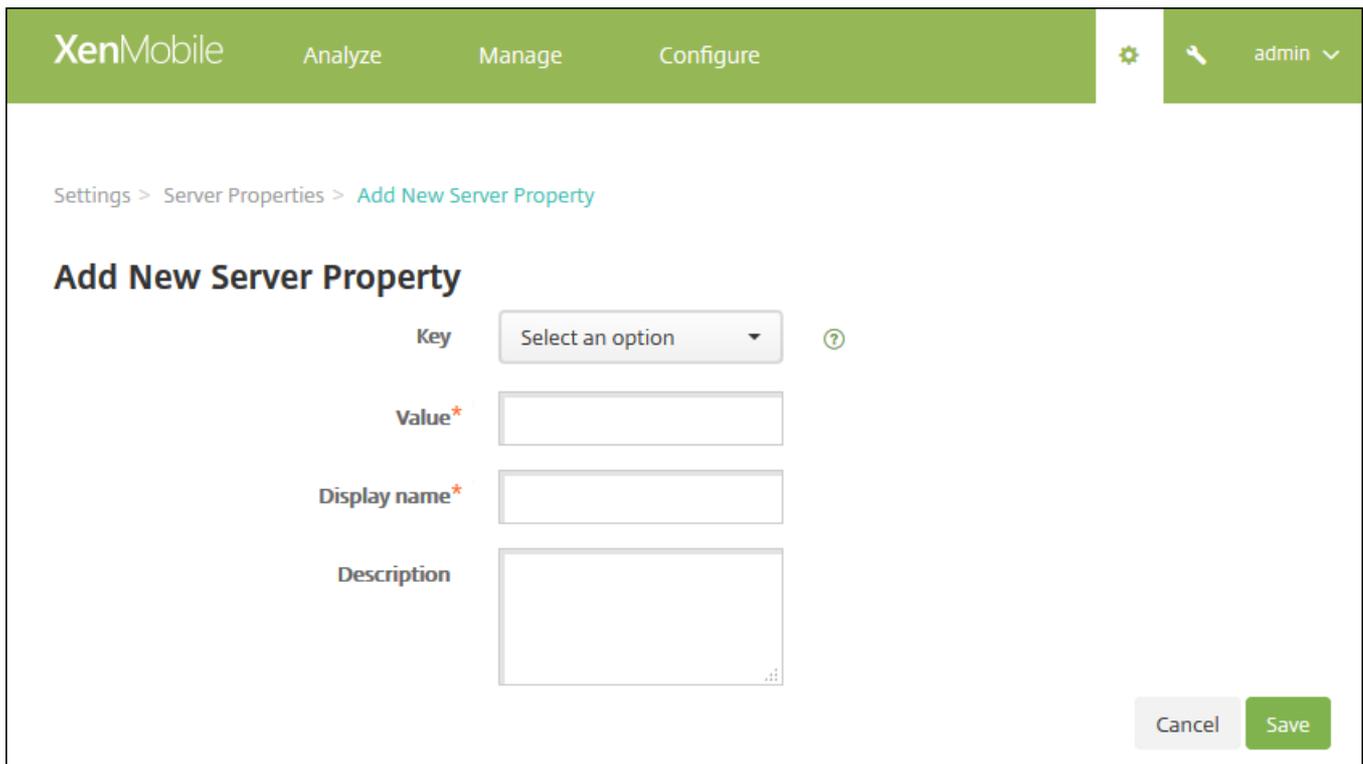
You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata,Id, url	odata.metadata, Id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Showing 1 - 10 of 111 items Showing 1 of 12

Para agregar una propiedad de servidor

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



The screenshot shows the XenMobile interface. At the top, there is a green navigation bar with the XenMobile logo and menu items: Analyze, Manage, and Configure. On the right side of the bar, there are icons for settings and a user profile labeled 'admin'. Below the navigation bar, the breadcrumb trail reads 'Settings > Server Properties > Add New Server Property'. The main heading is 'Add New Server Property'. The form contains four fields: 'Key' is a dropdown menu with 'Select an option' and a help icon; 'Value\*' is a text input field; 'Display name\*' is a text input field; and 'Description' is a larger text area. At the bottom right, there are 'Cancel' and 'Save' buttons.

2. Configure los siguientes parámetros:

- **Key.** En la lista, seleccione la clave apropiada. Las claves distinguen mayúsculas y minúsculas. Debe ponerse en contacto con el servicio de asistencia técnica de Citrix antes de realizar cambios o de solicitar una clave especial.
- **Value.** Escriba un valor en función de la clave seleccionada.
- **Display name.** Especifique el nombre del nuevo valor de propiedad que aparece en la tabla **Server Properties**.
- **Description.** Si quiere, escriba una descripción de la nueva directiva de servidor.

3. Haga clic en **Save**.

Para modificar una propiedad de servidor

1. En la tabla **Server Properties**, seleccione la propiedad de servidor que quiere modificar.

**Nota:** Si marca la casilla situada junto a una propiedad de servidor, el menú de opciones aparecerá encima de la lista de propiedades de servidor. En cambio, si hace clic en cualquier lugar de la lista, el menú de opciones aparecerá a la derecha de la lista.

2. Haga clic en **Edit**. Aparecerá la página **Edit New Server Property**.

XenMobile Analyze Manage Configure

Settings > Server Properties > Edit New Server Property

### Edit New Server Property

**Key** ag.client.cert.throttling.mi

**Value\*** 30

**Display name\*** NetScaler Gateway Client

**Description** Throttling interval for issuance of NetScaler Gateway client certificates.

Cancel Save

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

Mar 02, 2017

Puede acceder a las opciones de la interfaz de línea de comandos (CLI) en cualquier momento del siguiente modo:

- En el hipervisor en que se haya instalado XenMobile: Citrix XenServer, Microsoft Hyper-V o VMware ESXi. 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 una gran variedad de 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.

```
-----  
Main Menu  
-----  
[0] Configuration  
[1] Clustering  
[2] System  
[3] Troubleshooting  
[4] Help  
[5] Log Out  
-----
```

## Opciones de Configuration

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

```
-----  
Configuration Menu  
-----  
[0] Back to Main Menu  
[1] Network  
[2] Firewall  
[3] Database  
[4] Listener Ports  
-----
```

### [1] Network (Red)

```
Reboot is required to save the changes.  
Do you want to proceed? (y/n) [y]: y  
IP address [10.207.87.75]: 10.200.87.75  
Netmask [255.255.254.0]: 255.255.254.0  
Default gateway [10.207.86.1]: 10.200.86.1  
Primary DNS server [10.207.86.50]: 10.200.86.50  
Secondary DNS server (optional) []:  
  
Applying network settings...  
  
Are you sure to restart the system? [y/n]: █
```

### [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.

```
-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----
```

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

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

### [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)

```
Current White List:
- 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

Please enter hosts or networks to be white listed:
```

### [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 variada a nivel del sistema, reiniciar o apagar el servidor, o bien acceder a **Advanced Settings**.

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
```

## [12] Advanced Settings (Parámetros avanzados)

```
***** WARNING *****
Please only modify these options if you are
in contact with Citrix Support
*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] Reset SSL Certificate
[4] Reset pki.xml
[5] Server Tuning
-----
```

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

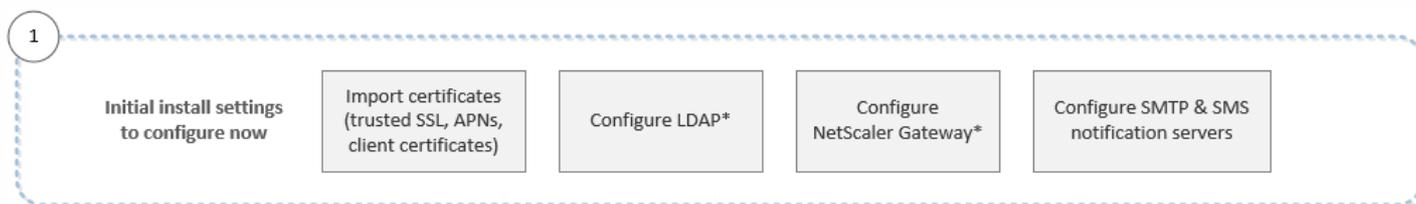
Mar 02, 2017

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 necesita instalar XenMobile, consulte [Instalación de XenMobile](#). Para obtener más información acerca de los exploradores Web que admiten la consola de XenMobile, consulte [Respaldo para exploradores Web](#) en el artículo de 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. Como no se puede volver a las pantallas de configuración iniciales, si en ese momento omitió alguna configuración de instalación, puede establecer los siguientes parámetros en la consola. Antes de empezar a agregar usuarios, aplicaciones y dispositivos, debe plantearse completar estos parámetros de instalación. Para empezar, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola.

**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 [Getting Started with Publishing](#) en Google Play.
- Cree una cuenta de administrador de Android for Work. Para obtener más información, consulte [Android for Work](#).
- Verifique su nombre de dominio con Google. Para obtener más información, consulte [Verify your domain for Google Apps](#).
- Habilite las API y cree una cuenta de servicio para Android for Work. Para obtener más información, consulte la [ayuda de Android for Work](#).

### 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). Necesitará un certificado APNs de Apple si va a administrar dispositivos iOS con la implementación de XenMobile Service (nube) y si quiere utilizar notificaciones push para la implementación de WorxMail. Para obtener más información, 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](#).

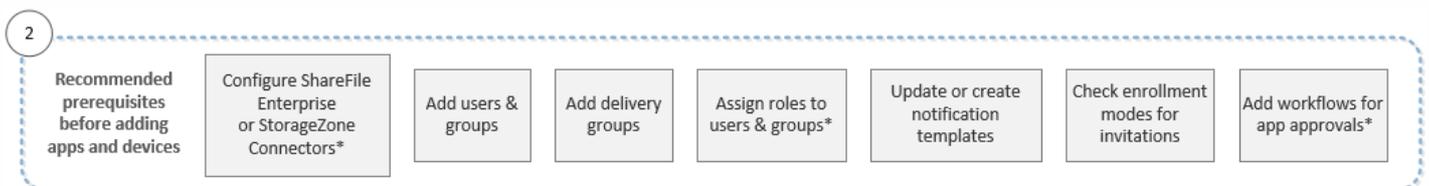
## Windows

- 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, asegúrese de 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 recomendados que puede configurar antes de agregar aplicaciones y dispositivos.

**Nota:** Los elementos con asterisco son optativos.



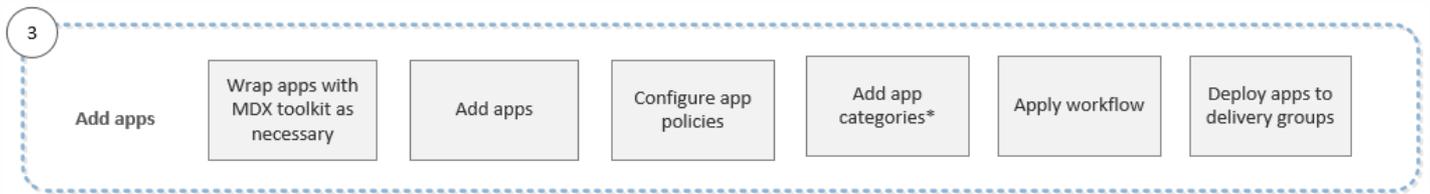
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- [Inscripción, roles y cuentas de usuario](#)
- [Implementación de recursos](#)
- [Configuración de roles con RBAC](#)
- [Notificaciones](#)
- [Creación y administración de flujos de trabajo](#)

## 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](#)
- [Plataformas de dispositivos respaldados](#)
- [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.



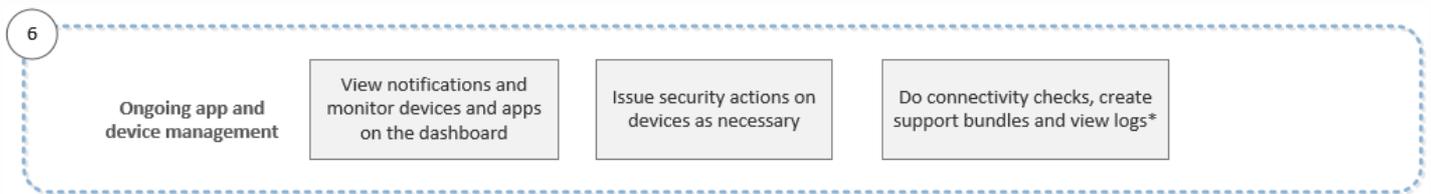
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- [Inscripción, roles y cuentas de usuario](#)
- [Notificaciones](#)

### Flujo de trabajo para la administración continua de dispositivos y aplicaciones

Este flujo de trabajo muestra las actividades recomendadas de la administración continua 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](#) y sus apartados.

# Autenticación

Mar 02, 2017

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

- **Servidor XenMobile.** La seguridad de la inscripción, así como la experiencia de la inscripción, se definen desde 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, 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. Si 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 los aspectos a tener en cuenta a la hora de decidir cómo configurar la autenticación, incluida una descripción general de los métodos 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.

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

La autenticación con certificados de cliente proporciona una capa de seguridad adicional para las aplicaciones móviles y permite que los usuarios pueden acceder sin problemas a aplicaciones HDX. Cuando se configura la autenticación con certificados de cliente, el usuario introduce su PIN de 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. <b>Importante:</b> XenMobile Server no respalda certificados con la extensión .pem. Use el comando openssl en una herramienta de conversión SSL de terceros para generar un archivo .p12 o .pfx desde un archivo PEM, tal como <a href="https://www.sslshopper.com/ssl-converter.html">https://www.sslshopper.com/ssl-converter.html</a> Por ejemplo, para convertir a .pfx, el comando sería: openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX (PKCS#12)	SSL, raíz

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

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

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

## Carga de certificados en XenMobile

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

Esta sección ofrece instrucciones generales para cargar certificados. Para obtener más información 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 importar un almacén de claves y luego identificar la entrada en el repositorio del almacén de claves que quiere instalar, a menos que esté cargando un formato PKCS#12.
- Puede hacer clic para importar un certificado.

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

### 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**.

XenMobile Analyze Manage Configure   admin 

Settings > Certificates

## Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

 Import |  Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key	
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML		
<input type="checkbox"/>	*.agsag.com		 Expired	2013-10-23	2015-10-23	SSL Listener		
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA		
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate		
<input type="checkbox"/>	APSP:3623302e-7c6e-4df8-aa91		 22 days left	2015-09-30	2016-09-29	APNs		

Showing 1 - 5 of 5 items

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

4. Configure los siguientes parámetros:

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

## Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file\***  Browse

**Password\***

**Description**

Cancel
Import

- **Keystore type:** Seleccione **PKCS#12** en la lista.
- **Use as:** En la lista, haga clic en la forma en que se usará el certificado. Las opciones disponibles son:
  - **Server.** Los certificados de servidor son aquellos que usa el servidor XenMobile de manera funcional, que se cargan en la consola Web de XenMobile. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Este uso se aplica especialmente a certificados de entidades de certificación utilizados para establecer una relación de confianza en el dispositivo.
  - **SAML.** La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On (SSO) a los servidores, los sitios Web y las aplicaciones.
  - **APNs.** Los certificados del servicio de notificaciones push de Apple (APNs) permiten la administración de dispositivos móviles a través de Apple Push Network.
  - **SSL Listener.** La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.
- **Keystore file:** 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 de la entrada del almacén de claves forman una cadena; por ejemplo, si cada certificado de la cadena es el emisor del anterior.

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

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, haga clic en **Certificates**.
2. En la página **Certificates**, haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
3. En el cuadro de diálogo **Import**, en **Import**, si no se ha seleccionado ya, haga clic en **Certificate**.
4. El cuadro de diálogo **Import** cambiará para reflejar las opciones de certificado disponibles. En **Use as**, haga clic en la forma en que se usará el almacén de claves. Las opciones disponibles son:
  - **Server**. Los certificados de servidor son aquellos que usa el servidor XenMobile de manera funcional, que se cargan en la consola Web de XenMobile. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Esta opción se aplica especialmente a entidades de certificación utilizadas para establecer una relación de confianza en el dispositivo.
  - **SAML**. La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On (SSO) a los servidores, los sitios Web y las aplicaciones.
  - **SSL Listener**. La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.
5. Busque el almacén de claves que quiere importar del tipo de archivo .p12 (o .pfx en equipos Windows).
6. Si quiere, busque el archivo de clave privada del certificado. Junto con el certificado, la clave privada se usa para el cifrado y el descifrado.
7. Si quiere, escriba una descripción del certificado que le ayude a distinguirlo de otros certificados.
8. Haga clic en **Import**. El certificado se agrega a la tabla **Certificates**.

### Actualización de un certificado

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

La forma más eficaz de actualizar los certificados es: en la consola de XenMobile, haga clic en el icono con forma de engranaje, ubicado en la esquina superior derecha, y abra la página **Settings**; a continuación, haga clic en **Certificates**. En el cuadro de diálogo **Import**, importe el 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 hacer un seguimiento de los certificados que utilice en la implementación de XenMobile, sobre todo de sus fechas de caducidad y sus contraseñas respectivas. El objetivo de esta sección es facilitarle la tarea de administración de certificados en XenMobile.

Su entorno puede contener alguno o todos los certificados siguientes:

### **XenMobile Server**

Certificado SSL para FQDN de MDM

Certificado SAML (para ShareFile)

Certificados de CA raíz e intermedios para los certificados anteriores y otros recursos internos (StoreFront, Proxy, etc.)

Certificado APNs para la administración de dispositivos iOS

Certificado APNs interno para notificaciones de Secure Hub en el servidor XenMobile

Certificado de usuario PKI para la conectividad con PKI

### **MDX Toolkit**

Certificado de desarrollador de Apple

Perfil de aprovisionamiento de Apple (por aplicación)

Certificado APNs de Apple (para usar con Citrix Secure Mail)

Archivo JKS de Android

Certificado Windows Phone – Symantec

### **NetScaler**

Certificado SSL para FQDN de MDM

Certificado SSL para FQDN de Gateway

Certificado SSL para FQDN de StorageZones Controller de ShareFile

Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)

Certificado SSL para el equilibrio de carga con StoreFront

Certificados de CA raíz e intermedios para los certificados anteriores

### Directiva de caducidad de certificados en XenMobile

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

## Nota

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

### Certificado APNs para Citrix Secure Mail

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

### Certificado APNs para la administración de dispositivos iOS

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 Certificate Portal. Debe iniciar sesión con el mismo usuario con que creó el certificado.

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

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

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

Atentamente,

Servicio de notificaciones push de Apple"

### MDX Toolkit (certificado de distribución iOS)

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

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.

### Almacén de claves Android

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

### Certificado de empresa de Symantec para Windows Phone

Symantec es el proveedor exclusivo de certificados de firma de código para el servicio App Hub de Microsoft. Los desarrolladores y publicadores de software se unen a App Hub para distribuir aplicaciones para Windows Phone y Xbox 360 para descargarlas desde Windows Marketplace. Para obtener información más detallada, consulte [Symantec Code Signing Certificates for Windows Phone](#) en la documentación de Symantec.

Si el certificado caduca, los usuarios de Windows Phone no podrán inscribirse, instalar aplicaciones publicadas y firmadas por

la empresa ni iniciar aplicaciones de empresa que estén instaladas en el teléfono.

## NetScaler

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

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

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

Certificado SSL para FQDN de MDM

Certificado SSL para FQDN de Gateway

Certificado SSL para FQDN de StorageZones Controller de ShareFile

Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)

Certificado SSL para el equilibrio de carga con StoreFront

Certificados de CA raíz e intermedios para los certificados anteriores

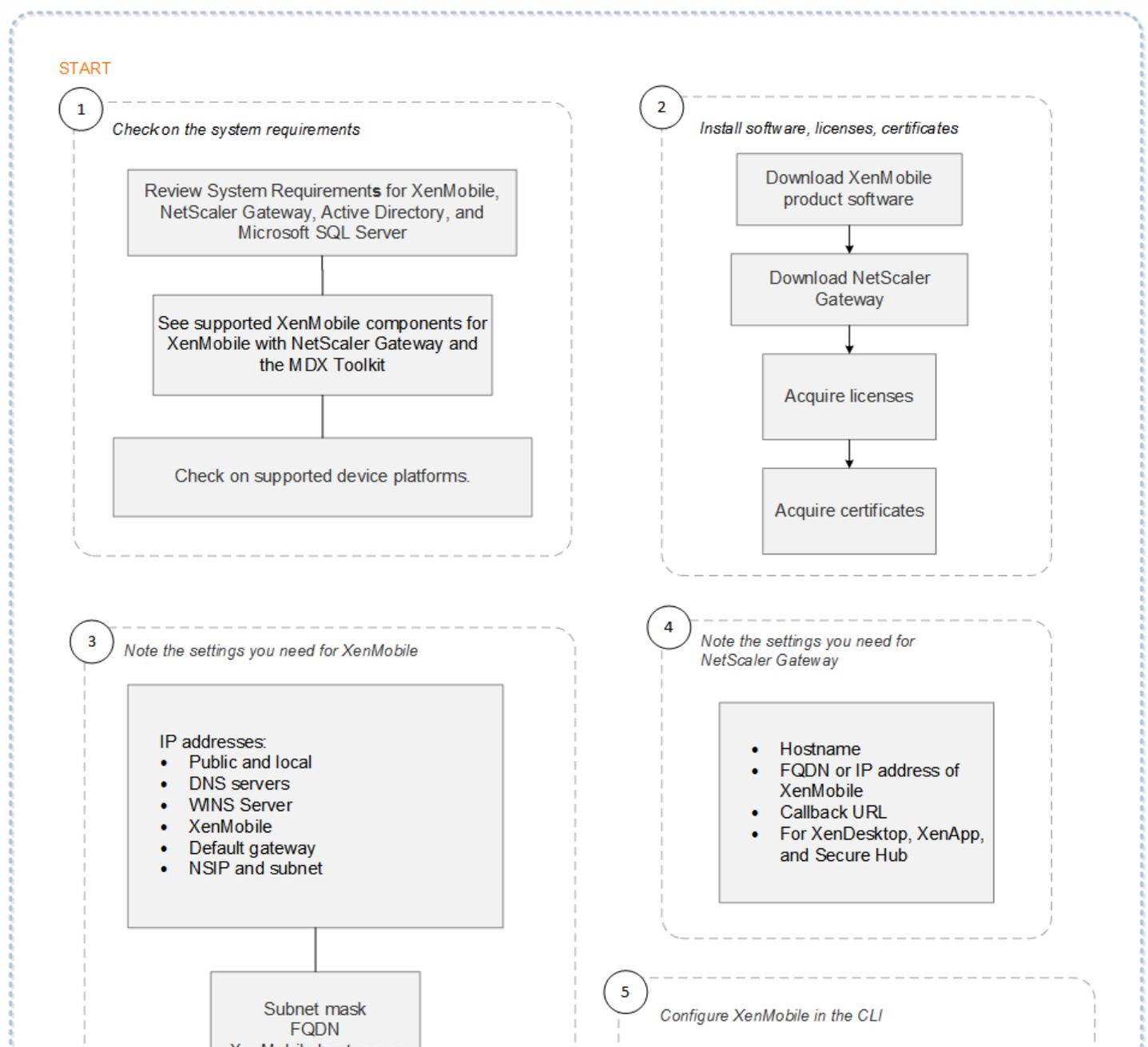
# XenMobile y NetScaler Gateway

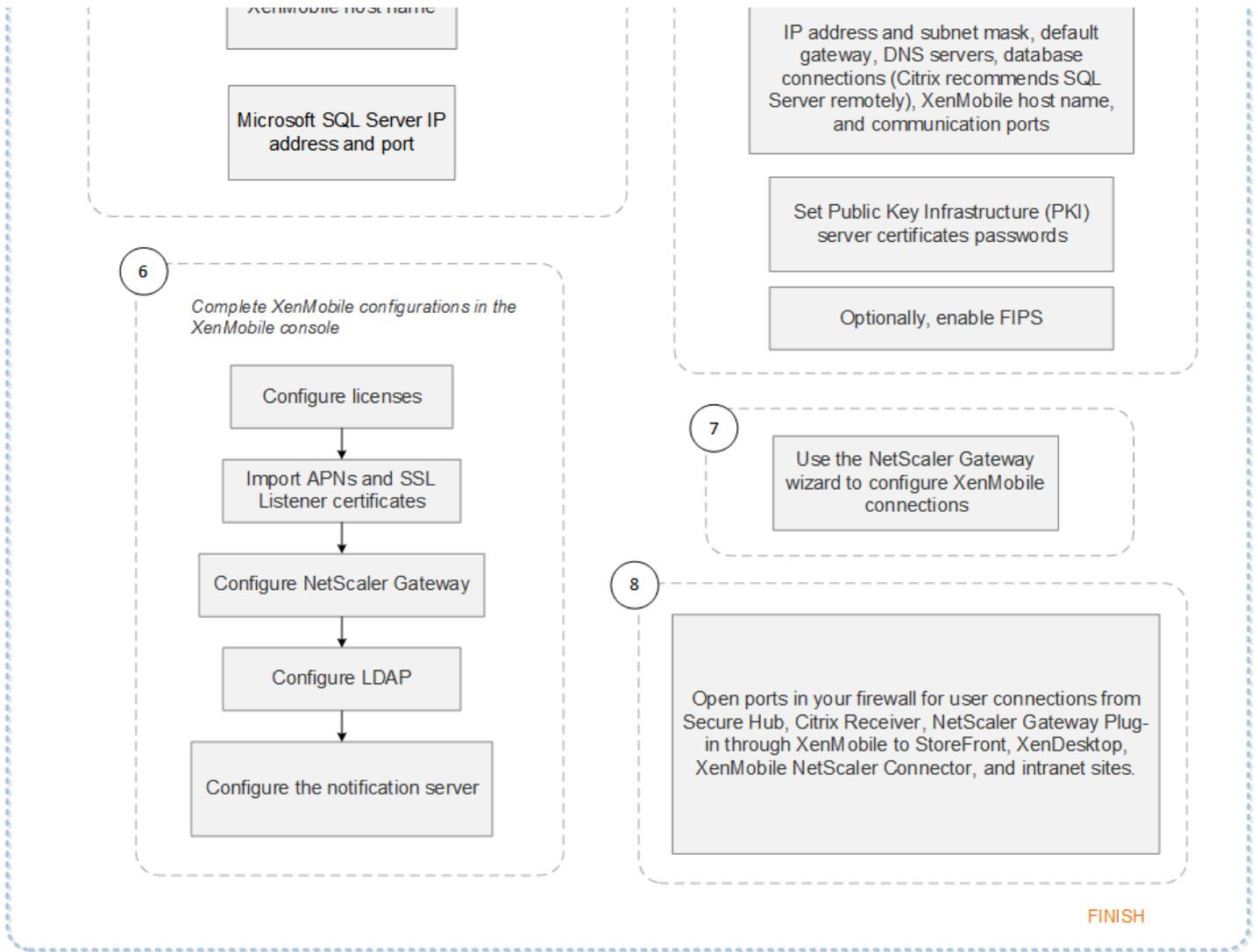
Mar 02, 2017

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.

## Diagrama de flujo para la implementación de XenMobile con NetScaler Gateway

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](#)

### Cómo configurar NetScaler Gateway

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**.

XenMobile Analyze Manage Configure ⚙️ 🔍 admin ▾

Settings > NetScaler Gateway

## NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

**Authentication**  ON

**Deliver user certificate for authentication**  OFF ?

**Credential provider**

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs	▾
<input type="checkbox"/>	ag186	<input checked="" type="checkbox"/>	https://mb186.agsag.com	Domain	0	
<input type="checkbox"/>	agdumy	<input type="checkbox"/>	https://10.199.225.200	Domain	0	

Showing 1 - 2 of 2 items

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**.

### Cómo agregar una nueva instancia de NetScaler Gateway

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
2. En **Server**, haga clic en **NetScaler Gateway**. Aparecerá la página **NetScaler Gateway**.
3. Haga clic en **Add**. Aparecerá la página **Add New NetScaler Gateway**.

The screenshot shows the 'Add New NetScaler Gateway' configuration page in the XenMobile interface. The page has a green header with 'XenMobile' and navigation tabs for 'Analyze', 'Manage', and 'Configure'. A user profile 'admin' is visible in the top right. The breadcrumb trail is 'Settings > NetScaler Gateway > Add New NetScaler Gateway'. The main form includes the following fields and controls:

- Name\***: Text input field with placeholder 'Appliance name'.
- Alias**: Text input field.
- External URL\***: Text input field with placeholder 'Publicly accessible URL'.
- Logon Type**: Dropdown menu currently set to 'Domain only'.
- Password Required**: Toggle switch currently set to 'ON'.
- Set as Default**: Toggle switch currently set to 'OFF'.

Below the form is a table with two columns: 'Callback URL\*' and 'Virtual IP\*'. The 'Virtual IP\*' column has an 'Add' button with a plus icon. At the bottom right of the form are 'Cancel' and 'Save' buttons.

4. Configure los siguientes parámetros:

- **Name.** Escriba un nombre para la instancia de NetScaler Gateway.
- **Alias.** Puede incluir un alias.
- **External URL:** Escriba la URL de acceso público de NetScaler Gateway. Por ejemplo, <https://receiver.com>.
- **Logon Type.** En la lista, haga clic en un tipo de inicio de sesión. Los tipos incluyen: **Domain only**, **Security token only**, **Domain and security token**, **Certificate**, **Certificate and domain** y **Certificate and security token**. El valor predeterminado es **Domain only**.

Si dispone de varios dominios, la opción **Domain only** no funcionará, por lo que deberá utilizar **Certificate and domain**. En el caso de algunas opciones, por ejemplo para **Domain only**, no puede cambiar el campo **Password**.

Para este tipo de inicio de sesión, el campo siempre está activado (**ON**). Además, los valores predeterminados del campo **Password Required** cambian en función del tipo de inicio de sesión (**Logon Type**) seleccionado.

Si utiliza la opción **Certificate and security token**, se necesita configuración adicional en NetScaler Gateway para que admita Secure Hub. Para obtener más información, consulte [Configuring XenMobile for Certificate and Security Token Authentication](#).

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

5. Haga clic en **Save**. La nueva instancia de NetScaler Gateway se agregará y aparecerá en la tabla. Puede modificar o

eliminar una instancia si hace clic en su nombre en la lista.

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

1. En la pantalla NetScaler Gateway, seleccione NetScaler Gateway en la tabla y haga clic en **Add**. Aparecerá la página **Add New NetScaler Gateway**.
2. En la tabla de direcciones URL de respuesta, haga clic en **Add**.
3. Especifique la URL de respuesta en Callback URL. Este campo representa el nombre de dominio completo (FQDN) y comprueba que la solicitud se ha originado en NetScaler Gateway. 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 **Guardar**.

# Autenticación de dominio o dominio + token de seguridad

Mar 02, 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.

Para agregar conexiones LDAP a XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
2. En **Server**, haga clic en **LDAP**. Aparecerá la página **LDAP**. Puede [agregar](#), [modificar](#) o [eliminar](#) directorios compatibles con el protocolo LDAP desde esta página.

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. On the right, there is a gear icon and a user profile 'admin'. Below the navigation, the breadcrumb 'Settings > LDAP' is visible. The main heading is 'LDAP', followed by a description: 'Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.' There is a toggle for 'Support nested groups' set to 'NO'. Below this is an 'Add' button with a plus icon. A table lists the configured LDAP directory:

<input type="checkbox"/>	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input type="checkbox"/>	Microsoft Active Directory	agsag.com	10.199.225.101:389	dc=agsag,dc=com	dc=agsag,dc=com	✓

At the bottom of the table area, it says 'Showing 1 - 1 of 1 items'.

Para agregar un directorio compatible con LDAP

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

Settings &gt; LDAP &gt; Add LDAP

## Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	<input type="text" value="Microsoft Active Directory"/>	▼
Primary server*	<input type="text" value="IP Address or FQDN"/>	
Secondary server	<input type="text" value="IP Address or FQDN"/>	
Port*	<input type="text" value="389"/>	
Domain name*	<input type="text"/>	
User base DN*	<input type="text" value="dc=example,dc=com"/>	?
Group base DN*	<input type="text" value="dc=example,dc=com"/>	?
User ID*	<input type="text"/>	
Password*	<input type="password"/>	
Domain alias*	<input type="text"/>	
XenMobile Lockout Limit	<input type="text" value="0"/>	?
XenMobile Lockout Time	<input type="text" value="1"/>	?
Global Catalog TCP Port	<input type="text" value="3268"/>	?
Global Catalog Root Context	<input type="text" value="dc=example,dc=com"/>	?
User search by	<input type="text" value="userPrincipalName"/>	▼
Use secure connection	<input type="checkbox" value="NO"/>	

Cancel

Save

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**.

Para modificar un directorio compatible con LDAP

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 **LDAP**.

Settings > LDAP > Add LDAP

### Edit LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	10.61	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	.net	
User base DN*	dc=.dc=net	?
Group base DN*	dc=.dc=net	?
User ID*	administrator@.net	
Password*		
Domain alias*	.net	
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

3. Cambie la siguiente información como corresponda:

- **Directory type.** En la lista, haga clic en el tipo de directorio correspondiente.
- **Primary server.** Escriba el servidor principal usado para el protocolo LDAP; puede escribir la dirección IP o el nombre de dominio completo (FQDN).
- **Secondary server.** Si quiere, puede introducir la dirección IP o el nombre de dominio completo (FQDN) del servidor secundario (si se ha configurado).
- **Port.** Escriba el número de puerto que utiliza el servidor LDAP. De forma predeterminada, el número de puerto es 389 para conexiones LDAP no protegidas. Use el número de puerto 636 para conexiones LDAP protegidas, el 3268 para conexiones LDAP no protegidas de Microsoft o el 3269 para conexiones LDAP protegidas de Microsoft.
- **Domain name.** No puede cambiar este campo.
- **User base DN.** Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Algunos ejemplos de sintaxis: ou=usuarios, dc=ejemplo, dc=com.
- **Group base DN.** Escriba el nombre del grupo de DN base especificado como cn=nombre\_de\_grupo. Por ejemplo, puede introducir cn=users, dc=nombre\_de\_servidor, dc=net, donde cn=users es el nombre del grupo; el DN y el nombre de servidor representan el nombre del servidor que ejecuta Active Directory.
- **User ID.** Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Password.** Escriba la contraseña asociada al usuario.
- **Domain alias.** Escriba un alias del nombre de dominio.
- **XenMobile Lockout Limit.** Introduzca un número comprendido entre 0 y 999 para la cantidad de intentos fallidos de inicio de sesión. Si introduce 0 en este campo, indicará a XenMobile que nunca bloquee al usuario en función de los intentos fallidos de inicio de sesión.
- **XenMobile Lockout Time.** Escriba un número comprendido entre 0 y 99999 que representará la cantidad de minutos que el usuario debe esperar una vez superado el límite de bloqueo. Si introduce 0 en este campo, el usuario no deberá esperar después de un bloqueo.

- **Global Catalog TCP Port.** Escriba el número del puerto TCP destinado al servidor de catálogo global. De forma predeterminada, el número de puerto TCP está establecido en 3268; para las conexiones SSL, utilice el número de puerto 3269.
- **Global Catalog Root Context.** Si quiere, puede escribir el valor del parámetro Global Root Context utilizado para habilitar una búsqueda en el catálogo global de Active Directory. Esta búsqueda se añade a la búsqueda estándar LDAP en cualquier dominio y sin necesidad de especificar el nombre de dominio real.
- **User search by.** En la lista, haga clic en **userPrincipalName** o en **sAMAccountName**.
- **Use secure connection.** Seleccione si utilizar conexiones protegidas.

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

Para eliminar un directorio compatible con LDAP

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 autenticuen 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.

Configuración de los parámetros de LDAP

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

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

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

XenMobile Analyze Manage Configure admin

Settings > LDAP

### LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups  NO

Add Edit Delete

<input type="checkbox"/>	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input checked="" type="checkbox"/>	Microsoft Active Directory	xmlab.net	10.207.86.51:389	dc=xmlab,dc=net	dc=xmlab,dc=net	<input checked="" type="checkbox"/>

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**.

XenMobile Analyze Manage Configure admin

Port\* 636

Domain name\* .net

User base DN\* dc=.net

Group base DN\* dc=.net

User ID\* administrator@.net

Password\*

Domain alias\* .net

XenMobile Lockout Limit 0

XenMobile Lockout Time 1

Global Catalog TCP Port 3269

Global Catalog Root Context dc=example,dc=com

User search by userPrincipalName

Use secure connection  YES

Cancel Save

## Configuración de los parámetros de NetScaler Gateway

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

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

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

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

The screenshot shows the 'Add New NetScaler Gateway' configuration page in the XenMobile interface. The page has a green header with 'XenMobile' and navigation tabs for 'Analyze', 'Manage', and 'Configure'. The breadcrumb trail is 'Settings > NetScaler Gateway > Add New NetScaler Gateway'. The form includes the following fields and controls:

- Name\***: Text input field containing 'THAG'.
- Alias**: Empty text input field.
- External URL\***: Text input field containing 'https://ag-bm1.xs.citrix.com'.
- Logon Type**: A dropdown menu with 'Domain and security token' selected. This field is highlighted with an orange border.
- Password Required**: A toggle switch set to 'ON'.
- Set as Default**: A toggle switch set to 'ON'.
- At the bottom, there are fields for **Callback URL\*** and **Virtual IP\***, followed by an **Add** button.
- At the bottom right, there are **Cancel** and **Save** buttons.

## Cómo habilitar el PIN de Worx y almacenamiento en caché de contraseñas de usuario

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

## Configuración de NetScaler Gateway para la autenticación de dominio y token de seguridad

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

# Autenticación de certificado de cliente o certificado + dominio

Mar 02, 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 <servidor virtual de equilibrio de carga SSL> sessReuse DISABLE
```

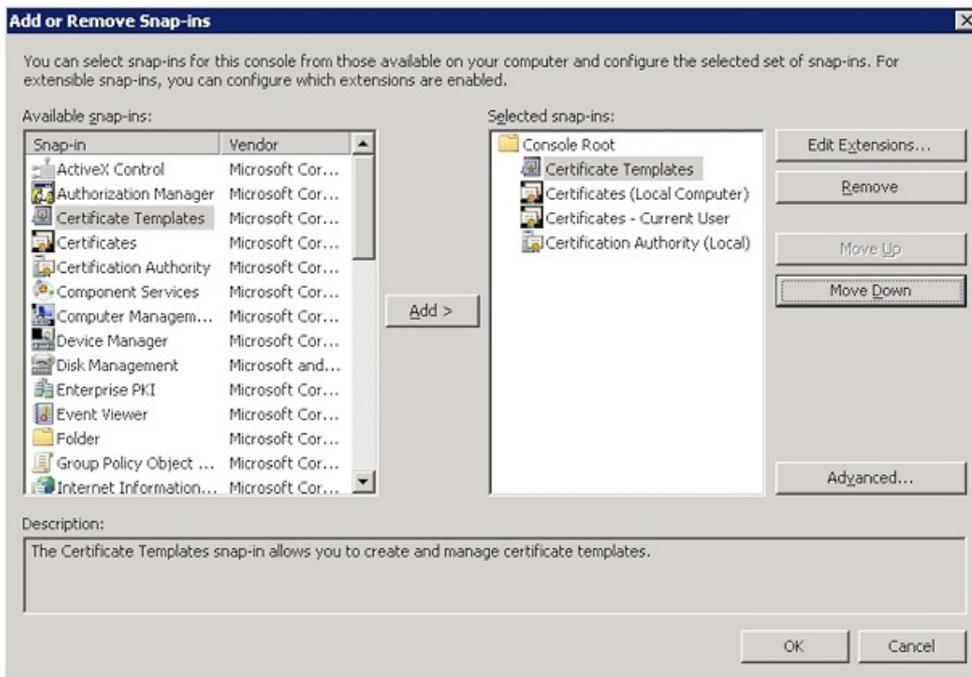
**Nota:** Si inhabilita la reutilización de sesiones SSL, se inhabilitan algunas de las optimizaciones que NetScaler ofrece, lo que puede ocasionar una disminución del rendimiento en NetScaler.

- 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, bajo **SSL Settings**, seleccione **Require SSL**.
- Compruebe que Secure Mail para iOS, Android y Windows Phone está empaquetado con el MDX Toolkit más reciente.

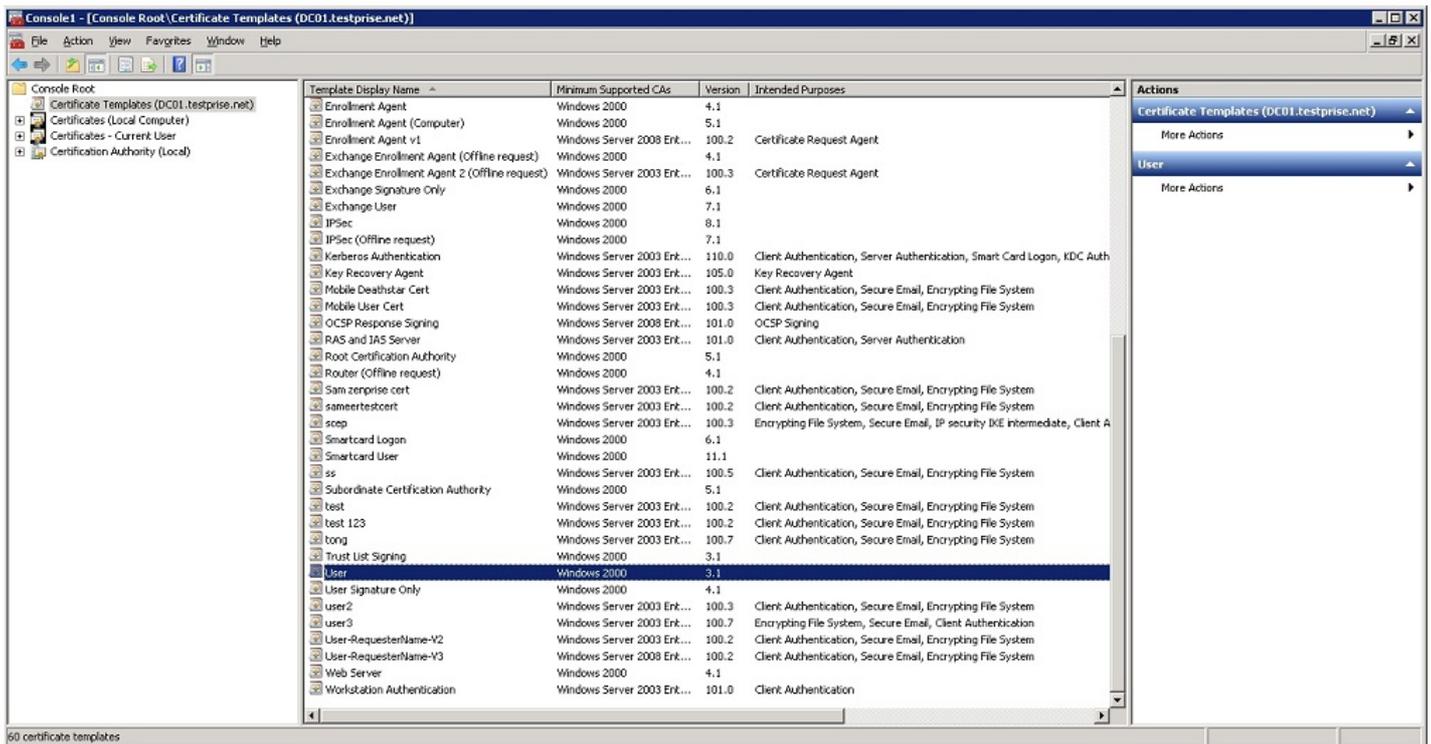
## Cómo agregar el complemento de Certificados a la consola MMC (Microsoft Management Console).

1. Abra la consola MMC y luego haga clic en **Agregar o quitar complemento**.
2. Agregue los complementos siguientes:

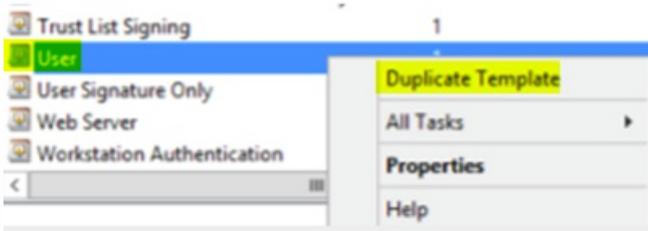
**Plantillas de certificado**  
**Certificados (Equipo local)**  
**Certificados (Usuario local)**  
**Entidad de certificación (Local)**



### 3. Expanda Plantillas de certificado.



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

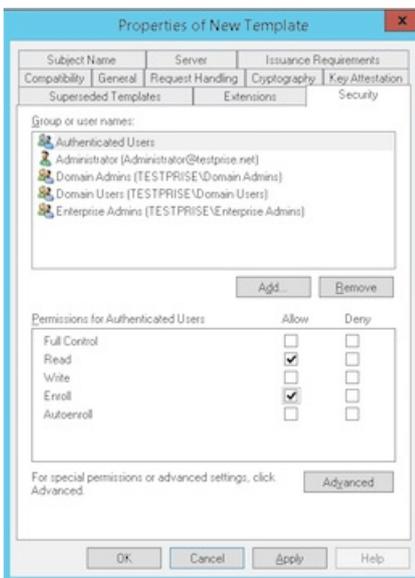


5. Suministre el nombre para mostrar de la plantilla.

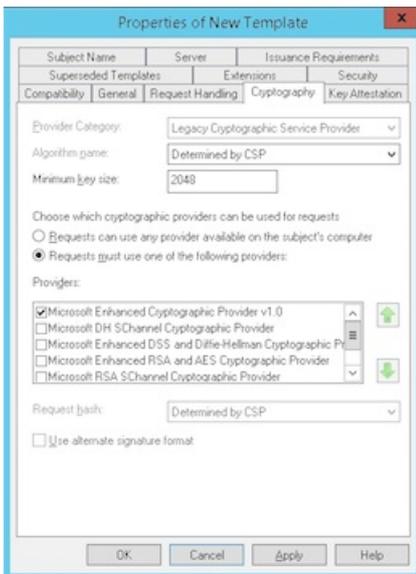
**Importante:** No marque la casilla **Publicar certificado en Active Directory** a menos que sea necesario. Si se selecciona esta opción, todos los certificado de cliente de los usuarios se insertarán/crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

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

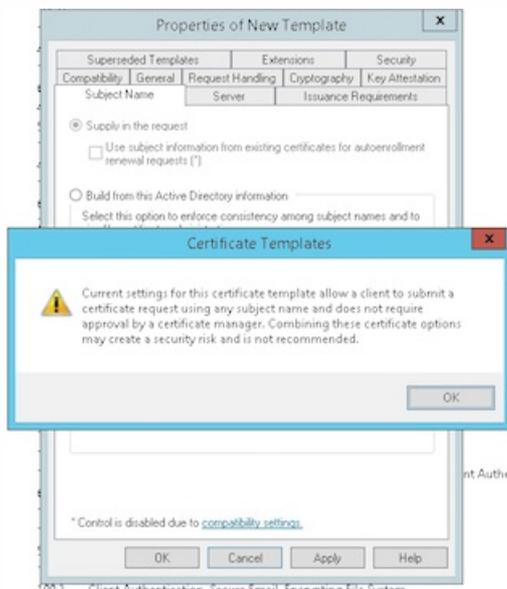
7. En **Seguridad**, seleccione la opción **Inscribir** en la columna **Permitir** para los usuarios autenticados.



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

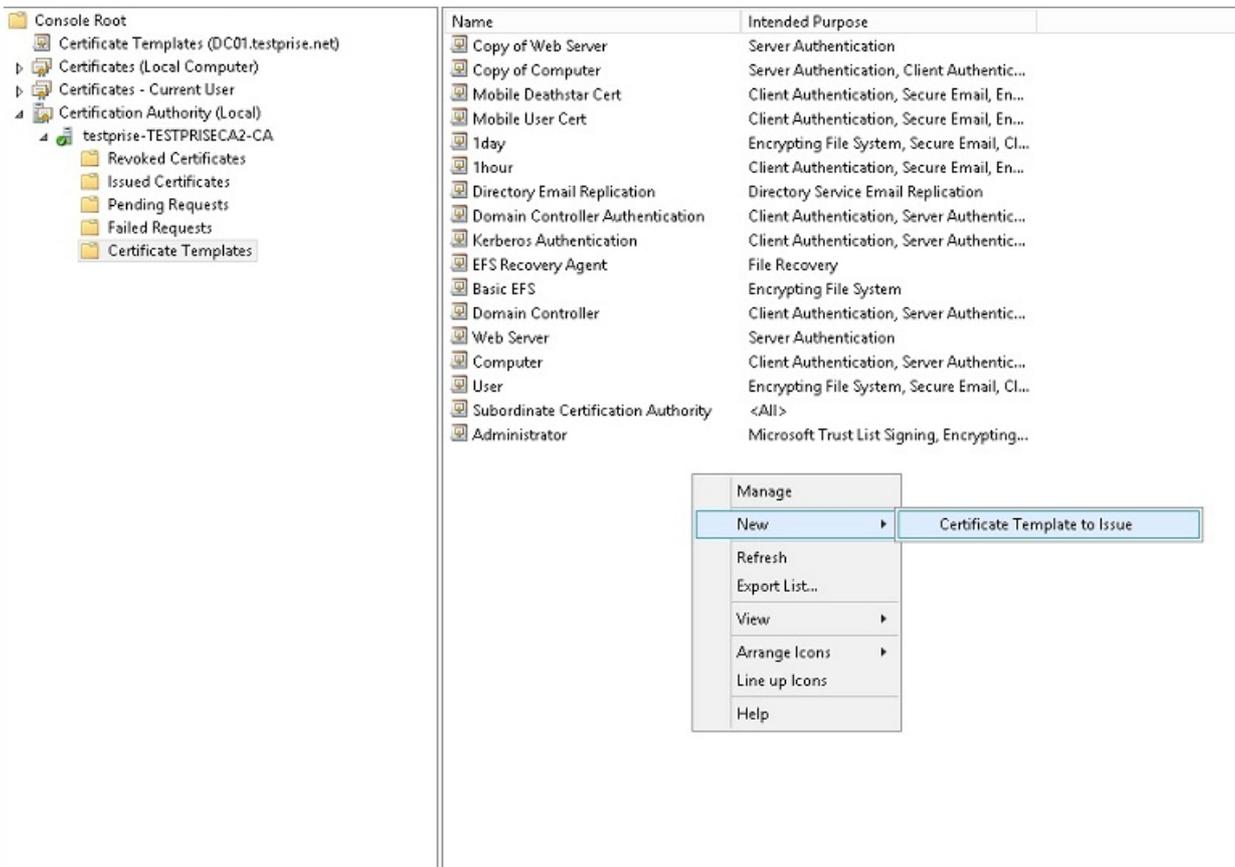


9. En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.

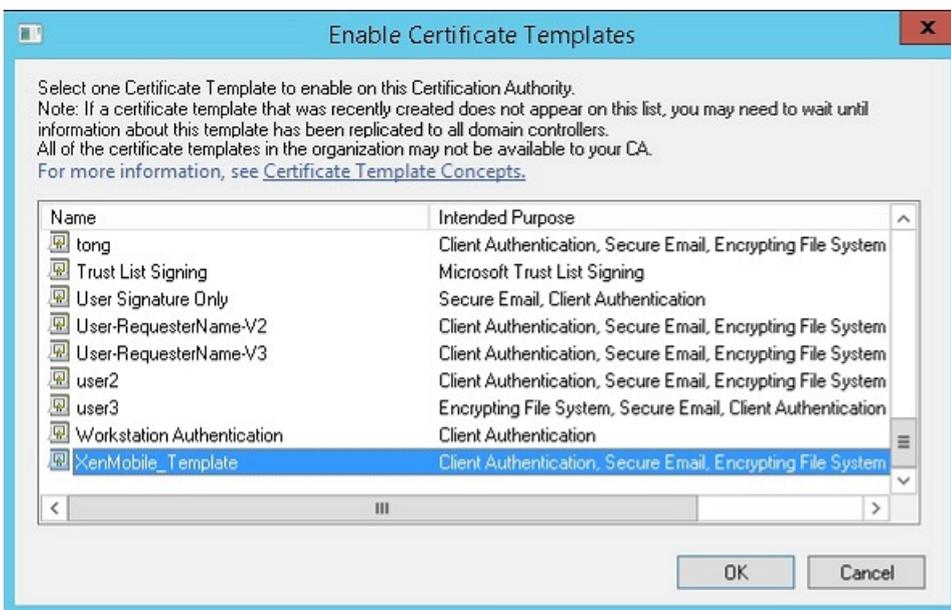


## Cómo agregar la plantilla a la entidad de certificación

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



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

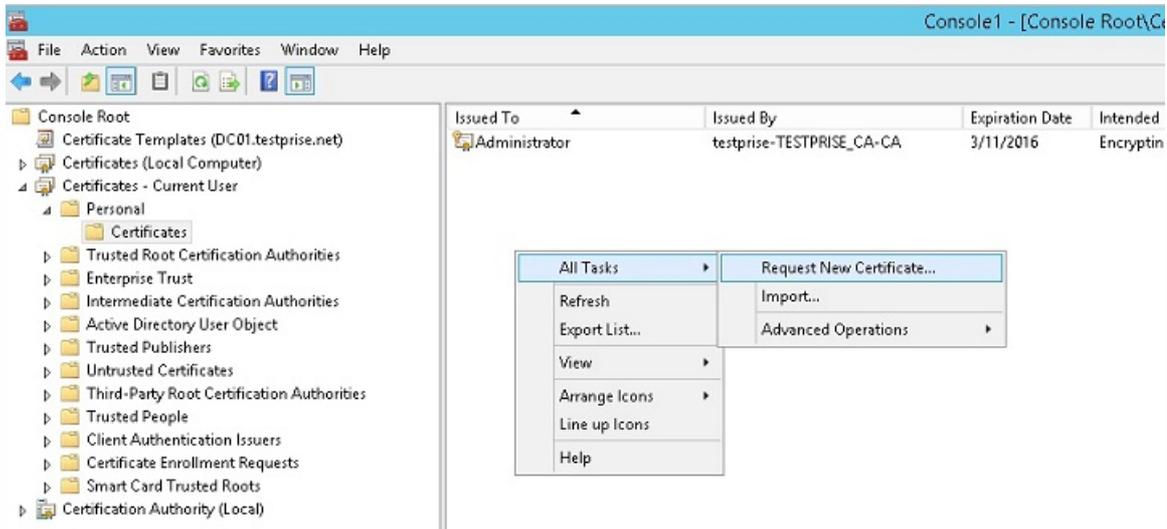


## Creación de un certificado PFX desde el servidor de CA

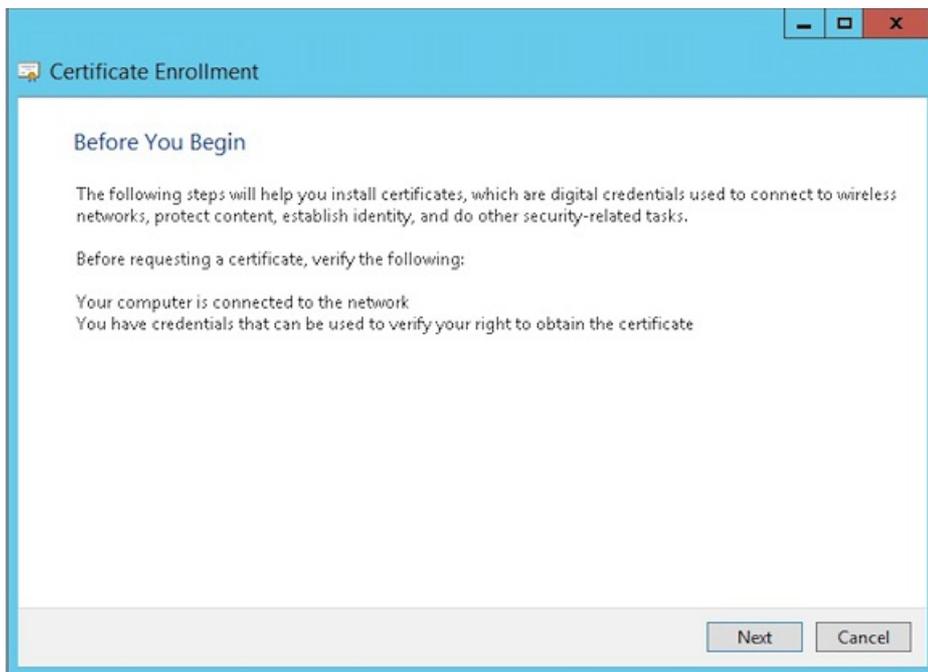
1. Cree un certificado .pfx de usuario usando la cuenta de servicio con la que inició sesión. Este .pfx se cargará en XenMobile, lo que solicitará un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.

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

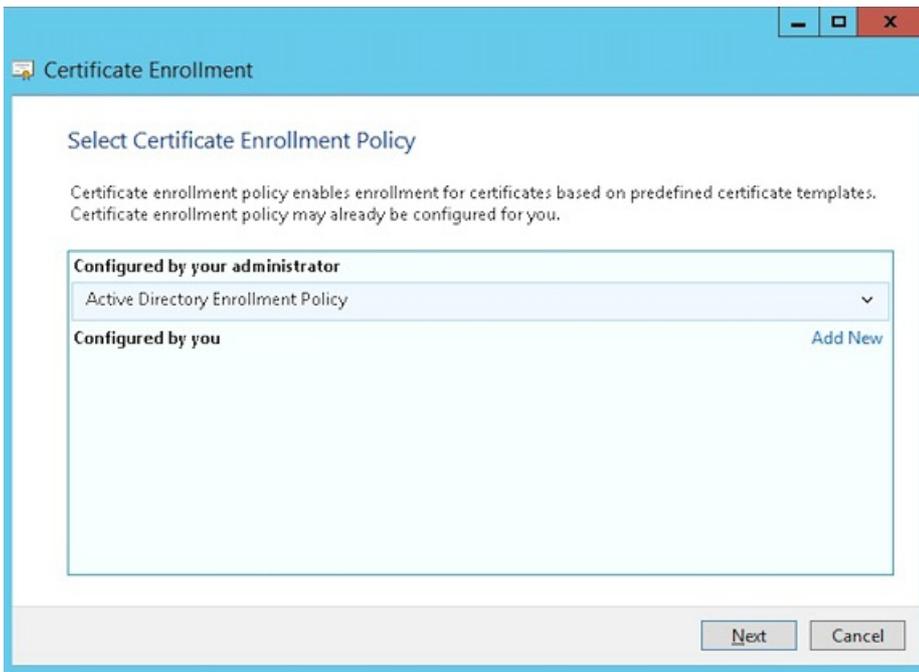
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



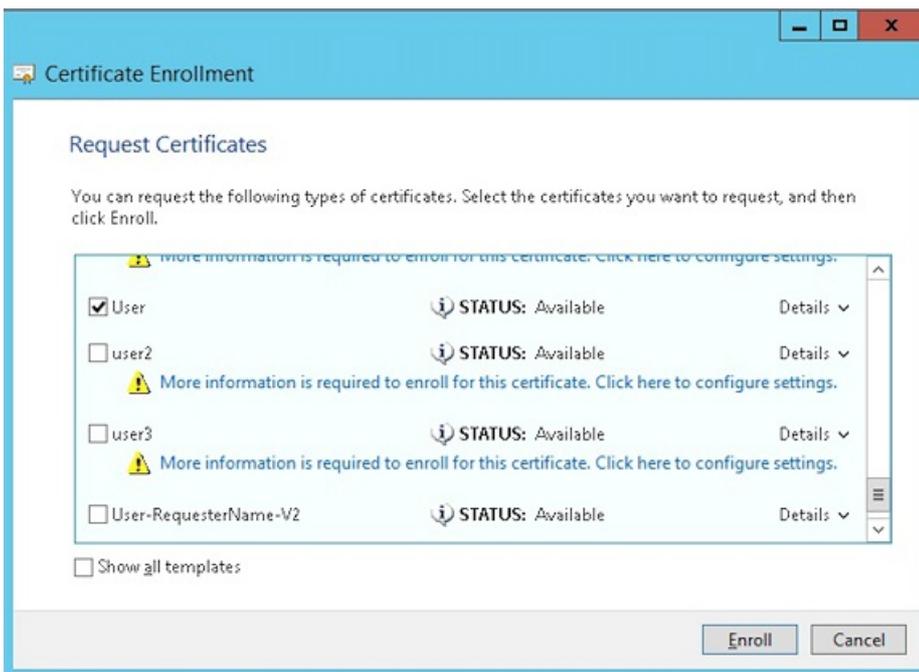
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Next**.



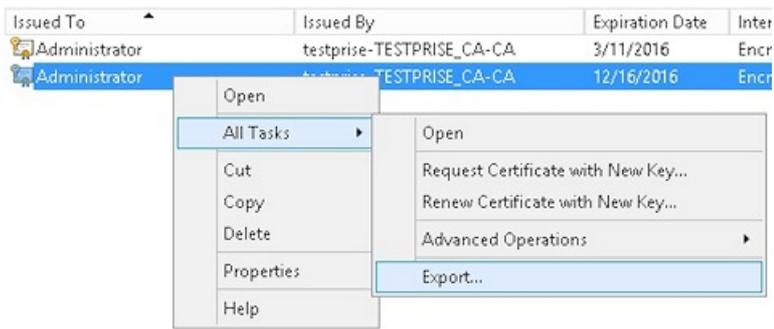
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



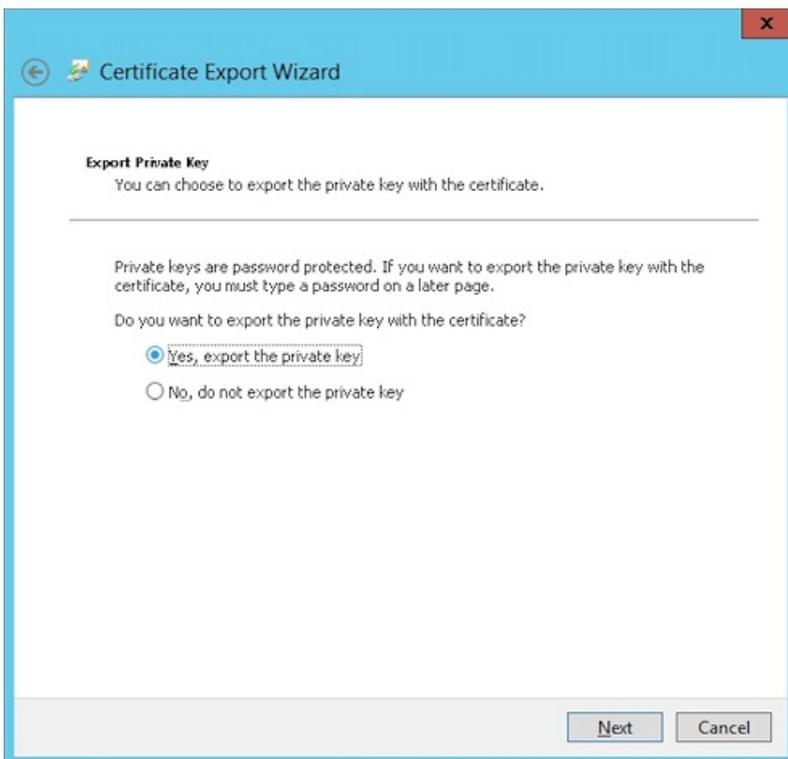
6. Seleccione la plantilla de **Usuario** y haga clic en **Inscribir**.



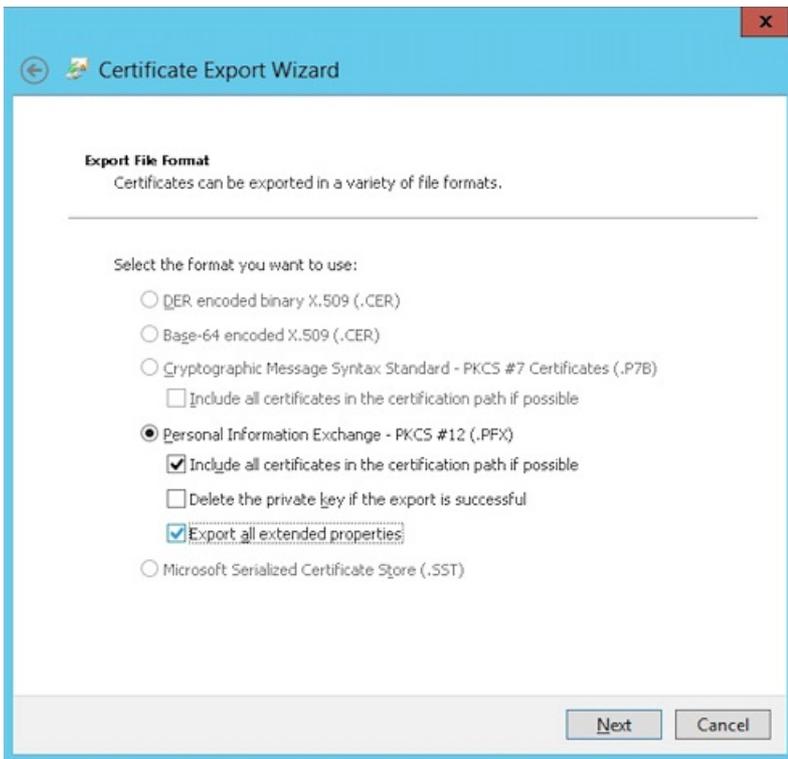
7. Exporte el archivo .pfx que creó en el paso anterior.



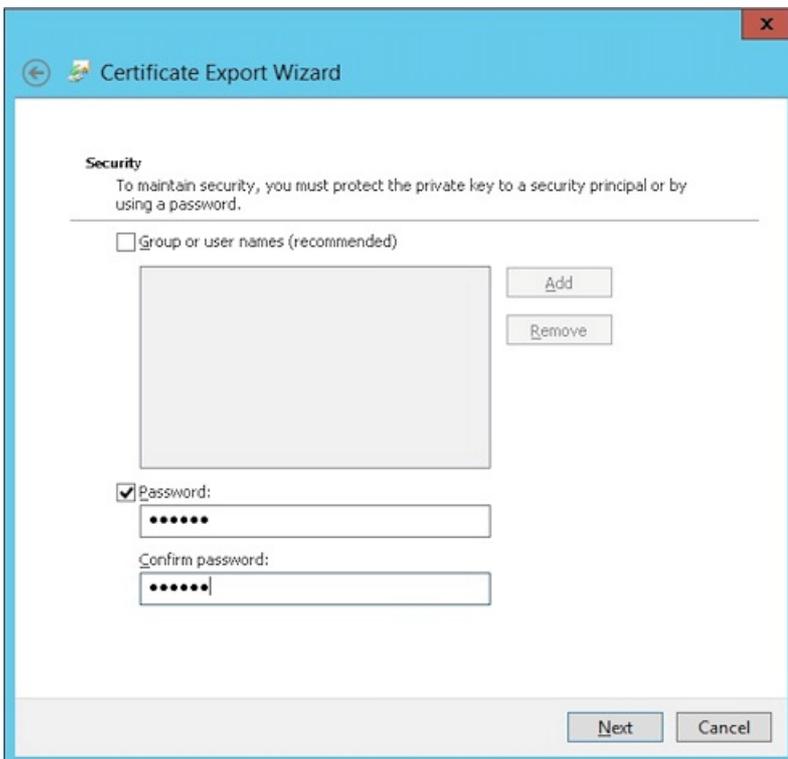
8. Haga clic en **Exportar la clave privada**.



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



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



11. Guarde el certificado en su disco duro.

# Cómo cargar el certificado en XenMobile

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

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

3. Introduzca los parámetros siguientes:

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

**Import** ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file\***  **Browse**

**Password\***

**Description**

**Cancel** **Import**

4. Haga clic en **Import**.

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

## Creación de una entidad PKI para la autenticación basada en certificados

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

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

3. Introduzca los parámetros siguientes:

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

Settings > PKI Entities > Microsoft Certificate Services Entity

### Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

### Microsoft Certificate Services Entity: General Information

Name\*

Web enrollment service root URL\*

certnew.cer page name\*

certfnsh.asp\*

Authentication type

SSL client certificate

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

### Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

### Microsoft Certificate Services Entity: Templates

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates*	<input type="button" value="Add"/>
XMTemplate	

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

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



Credential Providers	Credential Providers: Certificate Signing Request						
1 General	<p>Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.</p> <p>Key algorithm: RSA</p> <p>Key size*: 2048</p> <p>Signature algorithm: SHA1withRSA</p> <p>Subject name*: cn=Suser.username</p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>Suser.userprincipalname</td> <td></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	Suser.userprincipalname	
Type		Value*	Add				
User Principal name		Suser.userprincipalname					
2 Certificate Signing Request							
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

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

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

Credential Providers	Credential Providers: Distribution
1 General	<p>Issuing CA certificate: ON-training-AD-CA, Serial: ...</p> <p>Select distribution mode</p> <p><input checked="" type="radio"/> Prefer centralized: Server-side key generation</p> <p><input type="radio"/> Prefer distributed: Device-side key generation</p> <p><input type="radio"/> Only distributed: Device-side key generation</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	

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

7. Haga clic en **Renewal**.

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

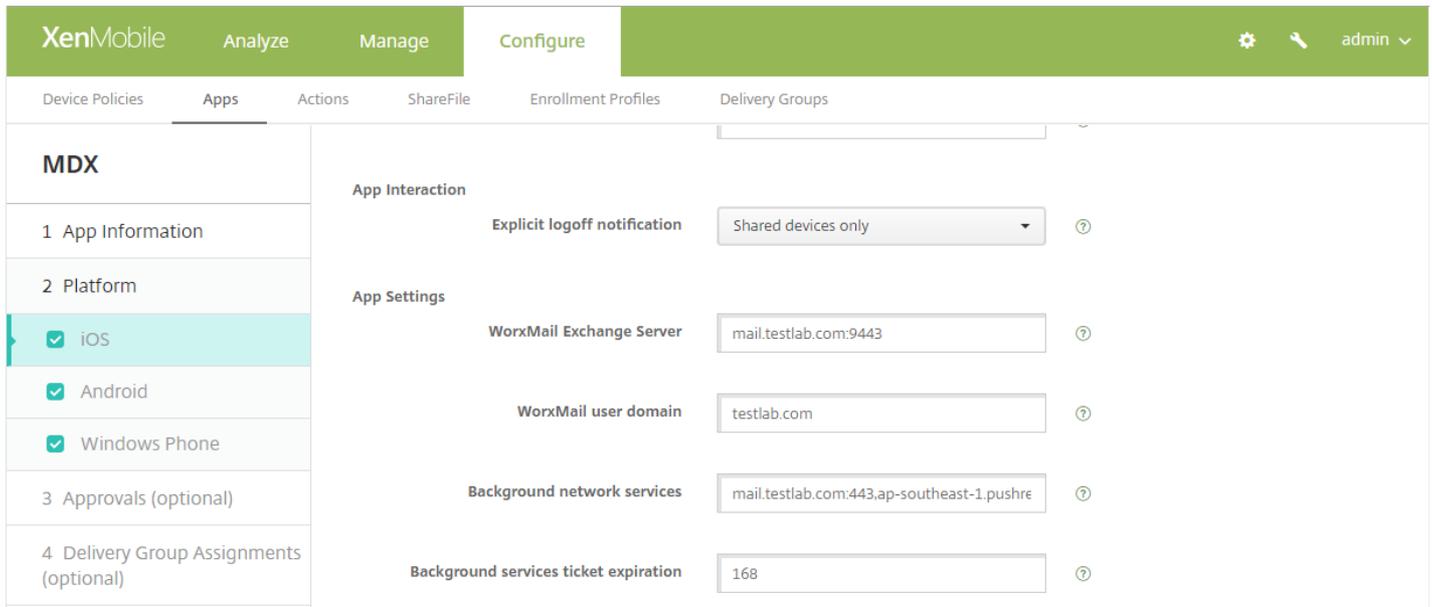
9. Deje todos los demás parámetros predeterminados o cámbielos como sea necesario.

Credential Providers	Credential Providers: Renewal
1 General	<p>Renew certificates when they expire: <input checked="" type="checkbox"/> ON</p> <p>Renew when the certificate comes within*: 30 days of expiration</p> <p><input type="checkbox"/> Do not renew certificates that have already expired</p> <p>Send notification: OFF</p> <p>Notify when the certificate nears expiration: OFF</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

10. Haga clic en **Save**.

## Configuración de Secure Mail para la autenticación basada en certificados

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



The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Apps' sub-tab is selected. On the left, a sidebar shows 'MDX' with a list of options: '1 App Information', '2 Platform', 'iOS' (checked), 'Android' (checked), 'Windows Phone' (checked), '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main content area is titled 'App Settings' and contains the following configuration items:

Section	Parameter	Value	Help
App Interaction	Explicit logoff notification	Shared devices only	?
	WorxMail Exchange Server	mail.testlab.com:9443	?
App Settings	WorxMail user domain	testlab.com	?
	Background network services	mail.testlab.com:443,ap-southeast-1.pushre	?
	Background services ticket expiration	168	?

## Configuración de la entrega de certificados de NetScaler en XenMobile

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

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

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

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

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

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway

## NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication

**Deliver user certificate for authentication**  ?

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
--------------------------	------	---------	--------------	------------	--------------------

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

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

XenMobile Analyze Manage Configure admin

User base DN\*  ?

Group base DN\*  ?

User ID\*

Password\*

Domain alias\*

XenMobile Lockout Limit  ?

XenMobile Lockout Time  ?

Global Catalog TCP Port  ?

Global Catalog Root Context  ?

User search by

Use secure connection

# Creación de una directiva Enterprise Hub para Windows Phone 8.1

Para dispositivos Windows Phone 8.1, es necesario crear una directiva Enterprise Hub para 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, bajo **More > XenMobile Agent**, haga clic en **Enterprise Hub**.
3. Después de dar un nombre a la directiva, seleccione el archivo AETX correcto y la aplicación Secure Hub firmada para Enterprise Hub.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Enterprise Hub Policy' and contains a sidebar with 'Enterprise Hub Policy' and a list of steps: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Windows Phone' (which is selected). The main area is titled 'Policy Information' and contains instructions: 'To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe)'. Below the instructions, there are two upload fields: 'Upload .aetx file' and 'Upload signed Enterprise Hub app', each with a 'Browse' button.

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

## Solución de problemas de la configuración de certificado 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.

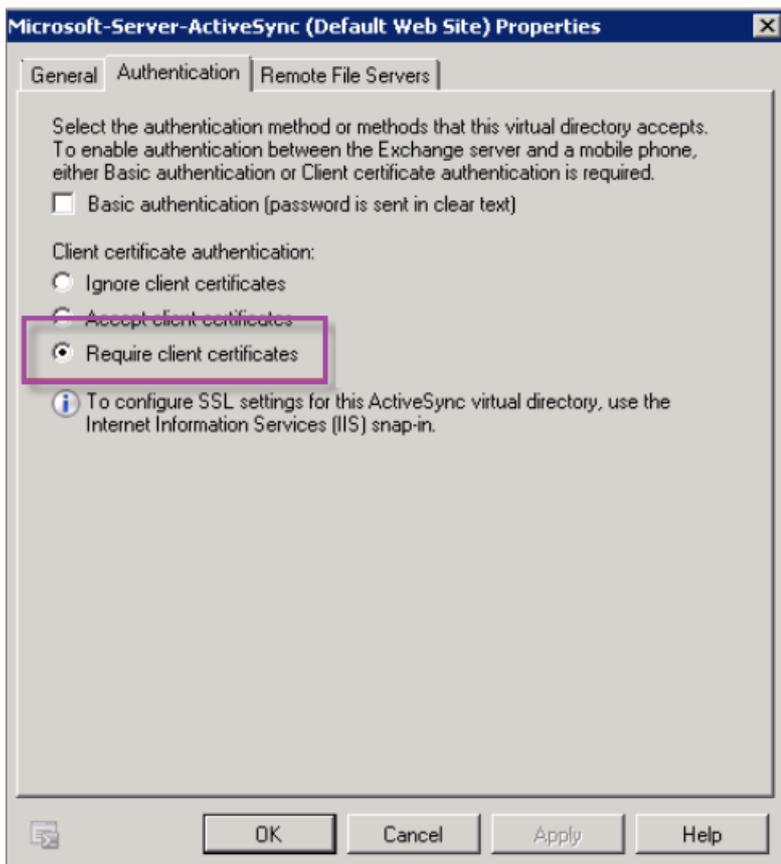
3. Los usuarios se dirigen a XenMobile Store.

4. Cuando los usuarios ejecutan Secure Mail para iOS, Android y Windows Phone 8.1, XenMobile no les pedirá credenciales de usuario 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.

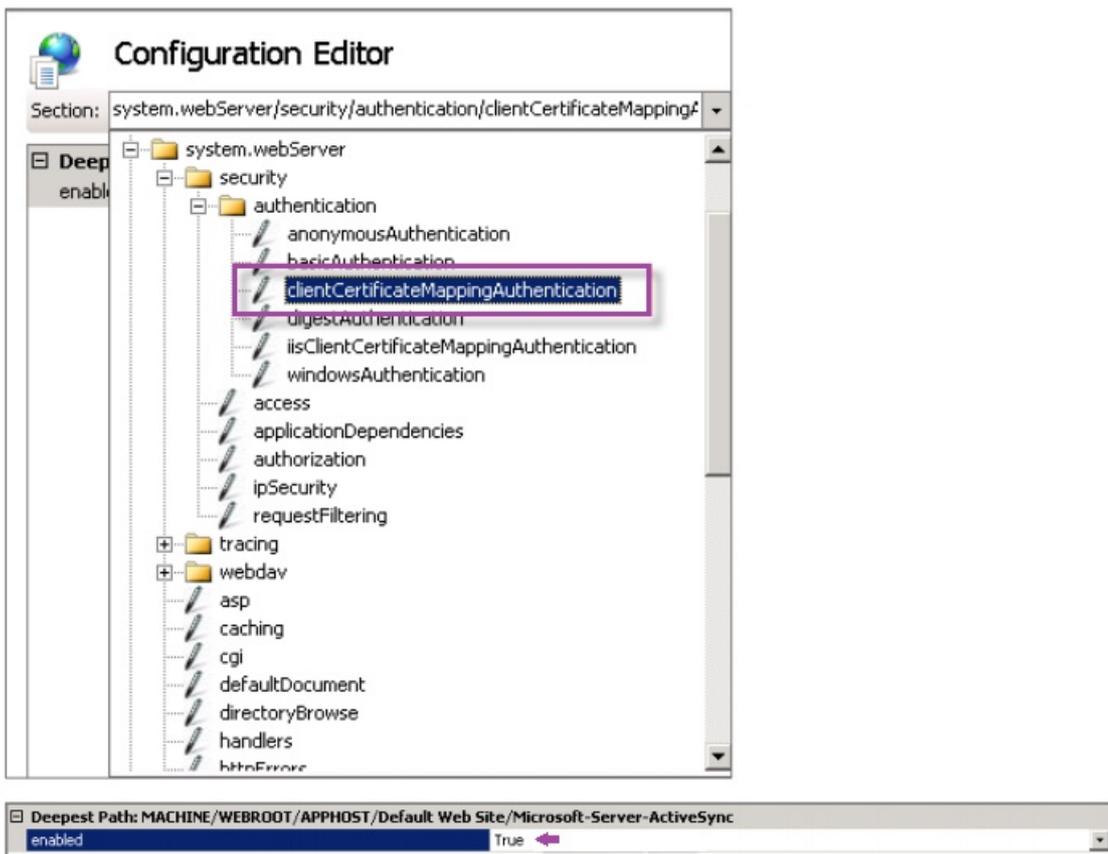
Si los usuarios pueden descargar e instalar Secure Mail, pero durante la configuración de buzones Secure Mail no puede finalizar la configuración:

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, compruebe 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**, asegúrese de hacer clic en **Aplicar** para que los cambios tengan efecto.

4. Compruebe la configuración de NetScaler Gateway en la consola de XenMobile: Asegúrese de que **Deliver user certificate for authentication** tiene el valor **ON** y que en **Credential provider** está seleccionado el perfil correcto, como se describió anteriormente en "Para configurar la entrega de certificados de NetScaler en XenMobile".

Para determinar si el certificado de cliente se ha entregado a un dispositivo móvil:

1. En la consola de XenMobile, vaya a **Manage > Devices** y seleccione el dispositivo.
2. Haga clic en **Edit** o **Show More**.
3. Vaya a la sección **Delivery Groups** y busque esta entrada:

**NetScaler Gateway Credentials : Requested credential, CertId=**

Para validar si está habilitada la negociación de certificados de cliente:

1. Ejecute este comando de netsh para mostrar la configuración del certificado SSL que está vinculada en el sitio Web de IIS:

```
netsh http show sslcert
```

2. Si el valor de **Negotiate Client Certificate** es **Disabled**, ejecute el siguiente comando para habilitarlo:

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name  
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

Por ejemplo:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid=  
{4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName  
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

Si no puede entregar certificados raíz e intermedios a un dispositivo Windows Phone 8.1 a través de XenMobile:

- Envíe los archivos .cer de certificados raíz/intermedios por correo electrónico al dispositivo Windows Phone 8.1 e instálelos directamente.

Si 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

Mar 02, 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)
- Microsoft Certificate Services

XenMobile respalda el uso de los siguientes servidores de CA:

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

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

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

## Acerca de los certificados de CA

Cuando configure una entidad de infraestructura PKI, deberá indicar a XenMobile el certificado de CA que va a actuar como firmante de los certificados que esta entidad emita (o de aquellos certificados que se recuperen de ella). La misma y única entidad de infraestructura PKI puede devolver certificados (ya sean recuperados o recién firmados) que haya firmado una cantidad indefinida de entidades de certificación (CA). Debe proporcionar el certificado de cada una de estas entidades de certificación como parte de la configuración de la entidad de infraestructura PKI. Para ello, cargue los certificados a XenMobile y, a continuación, vincúelos 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), transmitir las a la infraestructura de clave pública y devolver los certificados recién firmados.
- fetch. El adaptador puede recuperar certificados y pares de claves existentes (según los parámetros de entrada) de la

infraestructura de clave pública.

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

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

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

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

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

1. En la consola de XenMobile, haga clic en **Configure > Settings > More > PKI Entities**.

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

Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.

3. Haga clic en **Generic PKI Entity**.

Aparecerá la página **Generic PKI Entity: General Information**.

4. En la página **Generic PKI Entity: General Information**, lleve a cabo lo siguiente:

- **Name.** Escriba un nombre descriptivo para la entidad de infraestructura PKI.
- **WSDL URL.** Escriba la ubicación del archivo WSDL que describe el adaptador.
- **Authentication type.** Haga clic en el método de autenticación que se va a utilizar.
- **Ninguno.**
- **HTTP Basic.** Proporcione el nombre de usuario y la contraseña necesarios para conectarse al adaptador.
- **Client certificate.** Seleccione el certificado SSL de cliente correspondiente.

5. Haga clic en **Next**.

Aparecerá la página **Generic PKI Entity: Adapter Capabilities**.

6. En la página **Generic PKI Entity: Adapter Capabilities**, revise las funciones y los parámetros asociados al adaptador y, a continuación, haga clic en **Next**.

Aparecerá la página **Generic PKI Entity: Issuing CA Certificates**.

7. En la página **Generic PKI Entity: Issuing CA Certificates**, seleccione los certificados que se van a utilizar para la entidad.

**Nota:** Aunque las entidades puedan devolver certificados firmados por entidades de certificación diferentes, todos los certificados obtenidos de un proveedor de certificados determinado deben estar firmados por la misma entidad de certificación. Por lo tanto, al configurar el parámetro **Credential Provider**, en la página **Distribution**, seleccione uno de los certificados configurados aquí.

8. Haga clic en **Save**.

La entidad se muestra en la tabla PKI Entities.

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

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

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **More > PKI Entities**.

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

Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.

3. Haga clic en **Microsoft Certificate Services Entity**.

Aparecerá la página **Microsoft Certificate Services Entity: General Information**.

4. En la página Microsoft Certificate Services Entity: General Information, lleve a cabo lo siguiente:

- Name. Escriba un nombre para la nueva entidad. Lo utilizará más tarde para hacer referencia a esa entidad. Los nombres de entidad deben ser únicos.
- Web enrollment service root URL. Especifique la URL base del servicio de inscripción Web de la entidad de certificación de Microsoft, como, por ejemplo, <https://192.0.2.13/certsrv/>. La URL puede usar HTTP sin formato o HTTP sobre SSL.
- certnew.cer page name. El nombre de la página certnew.cer. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.
- certfnsh.asp. El nombre de la página certfnsh.asp. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.
- Authentication type. Haga clic en el método de autenticación que se va a utilizar.
- Ninguno
- HTTP Basic. Proporcione el nombre de usuario y la contraseña necesarios para la conexión.
- Client certificate. Seleccione el certificado SSL de cliente correspondiente.

5. Haga clic en **Next**.

Aparecerá la página **Microsoft Certificate Services Entity: Templates**. En esta página, especifique los nombres internos de las plantillas que admite la entidad de certificación de Microsoft. Cuando cree proveedores de credenciales, seleccione una plantilla de la lista definida aquí. Todos los proveedores de credenciales que utilicen esta entidad se valen de una plantilla exactamente igual.

Para conocer los requisitos de plantillas de Microsoft Certificate Services, consulte la documentación de Microsoft referente a su versión de servidor Microsoft. XenMobile no presenta requisitos para los certificados que distribuye, salvo los formatos de certificado indicados en [Certificados](#).

6. En la página **Microsoft Certificate Services Entity: Templates**, haga clic en **Add**, escriba el nombre de la plantilla y, a continuación, haga clic en **Save**. Repita este paso para cada plantilla a agregar.

7. Haga clic en **Next**.

Aparecerá la página **Microsoft Certificate Services Entity: HTTP parameters**. En esta página, puede especificar parámetros personalizados que XenMobile debe insertar en la solicitud HTTP para la interfaz de inscripción Web de Microsoft. Esta opción solo es útil si tiene scripts personalizados que se ejecutan en la entidad de certificación.

8. En la página **Microsoft Certificate Services Entity: HTTP parameters**, haga clic en **Add**, escriba el nombre y el valor de los parámetros HTTP a agregar y, a continuación, haga clic en **Next**.

Aparecerá la página **Microsoft Certificate Services Entity: CA Certificates**. En esta página, debe indicar a XenMobile los firmantes de los certificados que el sistema va a obtener a través de esta entidad. Cuando se renueve el certificado de CA, actualícelo en XenMobile, y el cambio se aplicará a la entidad de forma transparente.

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

10. Haga clic en **Save**.

La entidad se muestra en la tabla PKI Entities.

XenMobile respalda la lista de revocación de certificados (CRL) solo para una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, XenMobile utiliza NetScaler para administrar la revocación. Al configurar la autenticación basada en certificados de cliente, tenga en cuenta si es necesario configurar el parámetro de lista de revocación de certificados (CRL), **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse usando un certificado existente en el dispositivo; XenMobile vuelve a emitir un certificado nuevo, porque no impide a un usuario generar un certificado de usuario si se revoca otro. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

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

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

`https://server/instance/ocsp`

Al configurar el servicio OCSP, debe especificar un certificado de firma de OCSP para la entidad discrecional en cuestión. Puede usar el certificado de CA en sí como firmante. Para evitar una exposición innecesaria de la clave privada de la entidad

de certificación (recomendado), cree un certificado de firma de OCSP delegado, firmado por la entidad de certificación, e incluya una extensión id-kp-OCSPSigning extendedKeyUsage.

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

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

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

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **More > PKI Entities**.

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

Aparece una lista que muestra los tipos de entidades de infraestructura PKI que puede agregar.

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

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

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

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

5. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Parameters**.

6. En la página **Discretionary CA: Parameters**, lleve a cabo lo siguiente:

- **Serial number generator**. La entidad de certificación discrecional genera números de serie para los certificados que emite. En esta lista, haga clic en **Sequential** o en **Non-sequential** para determinar el modo en que se generan los números.
- **Next serial number**. Escriba un valor para determinar el siguiente número a emitir.
- **Certificate valid for**. Escriba la cantidad de días durante los que el certificado será válido.
- **Key usage**. Debe identificar el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, establezca las claves apropiadas en **On**. Una vez establecidas, la entidad de certificación está limitada a la emisión de certificados para esos fines.
- **Extended key usage**. Para agregar parámetros adicionales, haga clic en **Add**, escriba el nombre de la clave y, a continuación, haga clic en **Save**.

7. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Distribution**.

8. En la página **Discretionary CA: Distribution**, seleccione un modo de distribución:

- **Centralized: server-side key generation.** Citrix recomienda la opción centralizada. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
- **Distributed: device-side key generation.** Las claves privadas se generan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.

9. Haga clic en **Next**.

Aparecerá la página **Discretionary CA: Online Certificate Status Protocol (OCSP)**.

En la página **Discretionary CA: Online Certificate Status Protocol (OCSP)**, lleve a cabo lo siguiente:

- Para agregar una extensión AuthorityInfoAccess (RFC2459) a los certificados firmados por esta entidad de certificación, establezca **Enable OCSP support for this CA** en **On**. Esta extensión apunta al respondedor OCSP de la entidad de certificación en <https://server/instance/ocsp>.
- Si ha habilitado el respaldo de OCSP, seleccione un certificado de firma de CA OSCP. Esta lista de certificados se genera a partir de los certificados de CA que se cargaron en XenMobile.

10. Haga clic en **Save**.

La entidad de certificación discrecional se muestra en la tabla PKI Entities.

# Proveedores de credenciales

Mar 02, 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. Por ejemplo: si el proveedor de credenciales P se implementa en el dispositivo D como parte de la configuración C, los parámetros de emisión de P determinan el certificado que se implementará en D. Del mismo modo, los parámetros de renovación previstos para D se aplicarán cuando se actualice C, y los parámetros de revocación previstos para D también se aplicarán cuando C se elimine o cuando D se revoque.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Inscripción de Windows Phone y Tablet <b>Contexto</b>	No <b>Se admite SCEP</b>	No <b>Se requiere SCEP</b> No
Configuración de Windows Phone y Tablet	No, excepto la directiva de dispositivo para WiFi, que está respaldada en Windows Phone 8.1 y la versión más reciente de Windows 10	

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:** User Principal name

**Value:** \$user.userprincipalname

**Nota:** En cuanto al nombre del sujeto, puede hacer uso de las macros de XenMobile en el campo del valor.

7. Haga clic en **Next**.

Aparecerá la página **Credential Providers: Distribution**.

8. En la página **Credential Providers: Distribution**, lleve a cabo lo siguiente:

- En la lista **Issuing CA certificate**, haga clic en el certificado de CA ofrecido. Dado que el proveedor de credenciales usa una entidad de certificación discrecional, el certificado de CA de ese proveedor siempre será el certificado de CA configurado en la propia entidad; se mostrará aquí por coherencia con las configuraciones que usan entidades externas.
- En **Select distribution mode**, haga clic en una de las siguientes maneras de generar y distribuir claves:
  - **Prefer centralized: Server-side key generation.** Citrix recomienda esta opción centralizada. Admite todas las plataformas respaldadas por XenMobile y es necesaria cuando se usa la autenticación de NetScaler Gateway. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
  - **Prefer distributed: Device-side key generation.** Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
  - **Only distributed: Device-side key generation.** Esta opción funciona de la misma forma que Prefer distributed: Device-side key generation, salvo que no se permite ninguna otra opción si se produce un error en la generación de claves por parte del dispositivo o esta no está disponible.

Si selecciona **Prefer distributed: Device-side key generation** u **Only distributed: Device-side key generation**, haga clic en el certificado de firma de RA y en el certificado de cifrado de RA. Se puede usar el mismo certificado tanto para el cifrado como para la firma. Aparecerán campos nuevos para esos certificados.

9. Haga clic en **Next**.

Aparecerá la página **Credential Providers: Revocation XenMobile**. En esta página, puede configurar las condiciones bajo las que XenMobile deberá marcar internamente como revocados los certificados que se emitan con esta configuración de proveedor.

12. En la página **Credential Providers: Revocation XenMobile**, lleve a cabo lo siguiente:

- En **Revoke issued certificates**, seleccione una de las opciones que indican el momento en que se deben revocar los certificados.
- Si quiere que XenMobile envíe una notificación cuando el certificado se revoque, establezca el valor de **Send notification** en **On** y seleccione una plantilla de notificaciones.
- Si quiere revocar el certificado presente en la infraestructura de clave pública cuando este se haya revocado en XenMobile, establezca **Revoke certificate on PKI** en **On** y, en la lista **Entity**, haga clic en una plantilla. La lista Entity muestra todas las entidades de infraestructura GPKI disponibles con capacidades de revocación. Cuando el certificado se revoque en XenMobile, se enviará una llamada de revocación a la infraestructura de clave pública seleccionada de la lista

Entity.

13. Haga clic en **Next**.

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

14. En la página **Credential Providers: Revocation PKI**, lleve a cabo lo siguiente si quiere revocar certificados procedentes de la infraestructura de clave pública:

- Cambie la opción **Enable external revocation checks** a **On**. Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
- En la lista **OCSP responder CA certificate**, haga clic en el nombre distintivo (DN) del sujeto del certificado. **Nota:** Puede usar macros de XenMobile para los valores de los campos del DN. Por ejemplo: CN=\${user.username}, OU=\${user.department}, O=\${user.companyname}, C=\${user.c}\endquotation
- En la lista **When certificate is revoked**, haga clic en una de las siguientes acciones a realizar en la entidad de infraestructura PKI cuando se revoque el certificado:

No hacer nada.

Renovar el certificado.

Revocar y borrar el dispositivo.

- Si quiere que XenMobile envíe una notificación cuando el certificado se revoque, establezca el valor de **Send notification** en **On**.

Puede elegir entre dos opciones de notificación:

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

15. Haga clic en **Next**.

Aparecerá la página **Credential Providers: Renewal**. En esta página, puede determinar que XenMobile opere de la siguiente manera:

- Renovar el certificado y, si quiere, enviar una notificación cuando finalice el proceso (notificación de renovación) y, también si lo prefiere, excluir de la operación los certificados ya caducados.
- Emitir una notificación para aquellos certificados cuya fecha de caducidad se acerca (notificación antes de renovación).

16. En la página **Credential Providers: Renewal**, haga lo siguiente si quiere renovar los certificados cuando caduquen: Defina **Renew certificates** cuando caduquen con el valor **On**.

Aparecerán campos adicionales.

- En el campo **Renew when the certificate comes within**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe realizarse la renovación.
- Si quiere, seleccione **Do not renew certificates that have already expired**. **Nota:** En este caso, "already expired"

significa que la fecha NotAfter del certificado ha pasado, no que ha sido revocado. XenMobile no renovará certificados una vez que se hayan revocado internamente.

17. Si quiere que XenMobile envíe una notificación cuando el certificado se haya renovado, establezca el valor de **Send notification** en **On**. Puede elegir entre dos opciones de notificación:

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

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

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

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

20. Haga clic en **Save**.

El proveedor de credenciales se agregará a la tabla Credential Providers.

# Certificados de APNs

Mar 02, 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:

<b>Paso 1</b>	<a href="#">Creación de una solicitud CSR en IIS</a>  <a href="#">Creación de una solicitud CSR en un equipo Mac</a>	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.
<b>Paso 2</b>	<a href="#">Para firmar una solicitud de firma de certificado</a>	Envíe la solicitud de firma de certificado a Citrix por medio del sitio Web <a href="#">XenMobile APNs CSR Signing website</a> (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.
<b>Paso 3</b>	<a href="#">Envío de una solicitud CSR firmada a Apple</a>	Envíe la solicitud de firma de certificado firmada a Apple por medio del portal <a href="#">Apple Push Certificate Portal</a> (se requiere ID de Apple) y, a continuación, descargue el certificado APNs de Apple.
<b>Paso 4</b>	<a href="#">Para crear un certificado APNs con extensión PFX mediante Microsoft IIS</a>  <a href="#">Para crear un certificado APNs con extensión .pfx en un equipo Mac</a>	Exporte el certificado APNs como un certificado PCKS #12 (.pfx) (en IIS, Mac o SSL).

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

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

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

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

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

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

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

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

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

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

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

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

1. En el equipo donde se instaló OpenSSL, ejecute el siguiente comando desde el shell o del símbolo del sistema.  
**openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048**
2. Aparece el siguiente mensaje con información pertinente para asignar nombres de certificado. Escriba la información tal y como se indica.

**Se le va a pedir información que será incorporada en la solicitud de certificado.**

**Lo que está a punto de suministrar es lo que se conoce como nombre distintivo o nombre DN.**

**Existen varios campos aunque puede dejar algunos en blanco**

**Para algunos campos habrá un valor predeterminado,**

**Si introduce '.', el campo quedará en blanco.**

-----

**Country Name (2 letter code) [AU]:US**

**State or Province Name (full name) [Some-State]:CA**

**Locality Name (eg, city) []:RWC**

**Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer**

**Organizational Unit Name (eg, section) []:Marketing**

**Common Name (eg, YOUR name) []:John Doe**

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

3. En el siguiente mensaje, escriba una contraseña para la clave privada de la solicitud CSR.

**Introduzca los siguientes atributos adicionales para enviarlos con su solicitud de certificado**

**A challenge password []:**

**An optional company name []:**

4. Envíe la solicitud CSR resultante a Citrix.

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

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

1. En el explorador Web, vaya al sitio Web [XenMobile APNs CSR Signing](#).

2. Haga clic en **Upload the CSR**.

3. Busque y seleccione el certificado.

**Nota:** El certificado debe estar en el formato PEM o TXT.

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

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

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

1. En un explorador Web, vaya a <https://identity.apple.com/pushcert>.

2. Haga clic en **Create a Certificate**.

3. Si es la primera vez que crea un certificado con Apple, marque la casilla de verificación **I have read and agree to these terms and conditions** y, a continuación, haga clic en **Accept**.

4. Haga clic en **Choose File**, vaya al certificado firmado ubicado en el equipo y, a continuación, haga clic en **Upload**. Debe aparecer un mensaje de confirmación donde se indica que la carga se ha realizado correctamente.

5. Haga clic en **Download** para obtener el certificado .pem.

**Nota:** Si está utilizando Internet Explorer y falta la extensión de archivo, haga clic en **Cancel** dos veces y, a continuación, descárguelo desde la ventana siguiente.

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

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

1. Abra Microsoft IIS.

2. Haga clic en el icono de certificados del servidor.
3. En la ventana **Certificados de servidor**, haga clic en **Completar solicitud de certificado**.
4. Busque el archivo Certificate.pem de Apple. Escriba un nombre descriptivo o el nombre del certificado y haga clic en **OK**.
5. Seleccione el certificado que identificó en el paso 4 y, a continuación, haga clic en **Exportar**.
6. Especifique una ubicación y un nombre de archivo para el certificado .pfx, así como una contraseña, y, a continuación, haga clic en **Aceptar**.

**Nota:** Necesitará la contraseña del certificado durante la instalación de XenMobile.

7. Copie el certificado .pfx al servidor en el que se instalará XenMobile.
8. Inicie sesión como administrador en la consola de XenMobile.
9. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
10. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
11. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
12. En el menú **Import**, elija **Keystore**.
13. En **Use as**, elija **APNs**.
14. En **Keystore file**, seleccione el archivo de almacén de claves que quiere importar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
15. En **Password**, escriba la contraseña asignada al certificado.
16. Haga clic en **Import**.

1. En el mismo equipo Mac con Mac OS X que se ha utilizado para generar la solicitud de firma de certificado, busque el certificado de identidad de producción PEM recibido de Apple.
2. Haga doble clic en el archivo del certificado para importarlo en el llavero.
3. Si se le solicita agregar el certificado a un llavero concreto, mantenga seleccionado el llavero predeterminado de inicio de sesión y, a continuación, haga clic en **OK**. El certificado recién agregado aparecerá en la lista de certificados.
4. Haga clic en el certificado y, a continuación, en el menú **Archivo**, haga clic en **Exportar** para comenzar a exportar el certificado en un formato PCKS #12 (.pfx).
5. Asigne un nombre único al archivo del certificado para su uso con el servidor XenMobile, elija una ubicación de carpeta para guardar el certificado, seleccione el formato de archivo .pfx y, a continuación, haga clic en **Guardar**.
6. Escriba una contraseña para exportar el certificado. Citrix recomienda usar una contraseña única y segura. Además, compruebe que el certificado y la contraseña se encuentren en un lugar seguro para su uso y referencia posteriores.
7. La aplicación Acceso a Llaveros le solicitará la contraseña de inicio de sesión o el llavero seleccionado. Escriba la contraseña y, a continuación, haga clic en **OK**. Ahora, el certificado guardado está listo para su uso con el servidor XenMobile.

**Nota:** En caso de que no se conserven ni mantengan ni el equipo ni la cuenta de usuario que se usaron en su momento para generar la solicitud de firma de certificado y para completar el proceso de exportación de certificado, Citrix recomienda guardar o exportar las claves públicas y personales desde el sistema local. De lo contrario, no se podrá acceder a los certificados APNs para volver a usarlos y se deberá repetir el proceso de la solicitud CSR y APNs desde el principio.

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

1. En el shell o en el símbolo del sistema, ejecute el siguiente comando.

**openssl pkcs12 -export -in MDM\_Zenprise\_Certificate.pem -inkey Customer.key.pem -out apns\_identity.p12**

2. Escriba una contraseña para el archivo de certificado de extensión .pfx. Recuerde esta contraseña porque necesitará volver a utilizarla al cargar el certificado en XenMobile.
3. Tome nota de la ubicación del archivo de certificado .pfx y cópielo al servidor XenMobile, para poder usar la consola de XenMobile para cargar el archivo.

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

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
2. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
3. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
4. En el menú **Import**, elija **Keystore**.
5. En **Use as**, elija **APNs**.
6. Busque el archivo .p12 en su equipo.
7. Escriba la contraseña y, a continuación, haga clic en **Import**.

Para obtener más información acerca de los certificados en XenMobile, consulte la sección [Certificados](#):

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

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

1. Genere una solicitud de firma de certificado mediante Microsoft Internet Information Services (IIS).
2. En el sitio Web [XenMobile APNs CSR Signing](#), cargue la nueva solicitud de firma de certificado y, a continuación, haga clic en **Sign**.
3. Envíe la solicitud de firma de certificado firmado a [Apple Push Certificate Portal](#).
4. Haga clic en **Renew**.
5. Genere un certificado APNs PCKS #12 (.pfx) mediante Microsoft IIS.
6. Actualice el nuevo certificado APNs en la consola de XenMobile. Haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Settings**.
7. Haga clic en **Certificates**. Aparecerá la página **Certificates**.
8. Haga clic en **Import**. Aparecerá el cuadro de diálogo **Import**.
9. En el menú **Import**, elija **Keystore**.
10. En **Use as**, elija **APNs**.
11. Busque el archivo .p12 en su equipo.
12. Escriba la contraseña y, a continuación, haga clic en **Import**.



# SAML para Single Sign-On con ShareFile

Mar 02, 2017

Puede configurar XenMobile y ShareFile para usar el lenguaje SAML (Security Assertion Markup Language) y así ofrecer el acceso Single Sign-On (SSO) a aplicaciones de ShareFile para móvil que se han empaquetado con MDX Toolkit, así como a clientes no empaquetados de ShareFile (como el sitio Web, el plugin para Outlook 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.

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

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

- Versión 9.0.4 o posterior de MDX Toolkit (para aplicaciones de ShareFile para móvil)
- Aplicaciones de ShareFile para móvil, según corresponda:
  - ShareFile para iPhone, versión 3.0.x
  - ShareFile para iPad, versión 2.2.x
  - ShareFile para Android, versión 3.2.x
- Secure Hub 9.0 (para aplicaciones de ShareFile para móviles). Instale la versión de iOS o Android, según corresponda.
- Cuenta de administrador de ShareFile

Compruebe que XenMobile y ShareFile pueden establecer conexión.

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**.

**XenMobile** Analyze Manage **Configure** administrator ▾

Device Policies Apps Actions **ShareFile** Delivery Groups

## ShareFile

Configure settings to connect to the ShareFile account and administrator service account for user account management.

**Domain\***

**Assign to delivery groups**

- DG-SDEnroller
- DG\_win\_1
- DG\_win\_2
- DG\_tong1
- DG\_tong2
- DG\_tong3
- DG-ex12
- DG-devtest

### ShareFile Administrator Account Logon

**User name\***

**Password\***

**User account provisioning**

2. Configure los siguientes 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.
- **ShareFile Administrator Account Logon**
  - **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 **Save**.

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

1. Con la herramienta 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 móvil. 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. En XenMobile Store, descargue, instale y configure Secure Mail.
3. Abra un nuevo correo electrónico y toque **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 de verificación **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 > Políticas > Session**.
2. Cree una nueva directiva de sesión. En la ficha **Políticas**, 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 NetScaler Gateway Session Profile**

Configure NetScaler Gateway Session Profile

Name  
Sharefile\_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Accounting Policy  
[Dropdown]

Override Global

Display Home Page

Home Page  
none

URL for Web-Based Email  
[Text Box]

Split Tunnel\*  
OFF

Session Time-out (mins)  
1

Client Idle Time-out (mins)  
[Text Box]

Clientless Access\*  
Allow

Clientless Access URL Encoding\*  
Obscure

Clientless Access Persistent Cookie\*  
DENY

Plug-in Type\*  
Windows/MAC OS X

Single Sign-on to Web Applications

Credential Index\*  
PRIMARY

KCD Account  
[Text Box]

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.** Seleccione esta opción de configuración.
  - **Credential Index.** En la lista, haga clic en PRIMARY.
- Haga clic en la ficha **Published Applications**.

**Configure NetScaler Gateway Session Profile**

Name  
Sharefile\_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy\*  
ON

Web Interface Address  
https://xms.citrix.lab:8443

Web Interface Address Type\*  
IPV4

Web Interface Portal Mode\*  
NORMAL

Single Sign-on Domain  
citrix

Citrix Receiver Home Page

Account Services Address

OK Close

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 el protocolo LDAP.

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

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

← Back

Create NetScaler Gateway Session Policy

Name\*  
ShareFile\_Policy

Action\*  
Sharefile\_Profile

Expression\*  
Operators Saved Policy Expressions Freq

Creates Close

Add Expression

Select Expression Type: General

Flow Type  
REQ

Protocol  
HTTP

Qualifier  
HEADER

Operator  
CONTAINS

Value\*  
NSC\_FSRD

Header Name\*  
COOKIE

Length

Offset

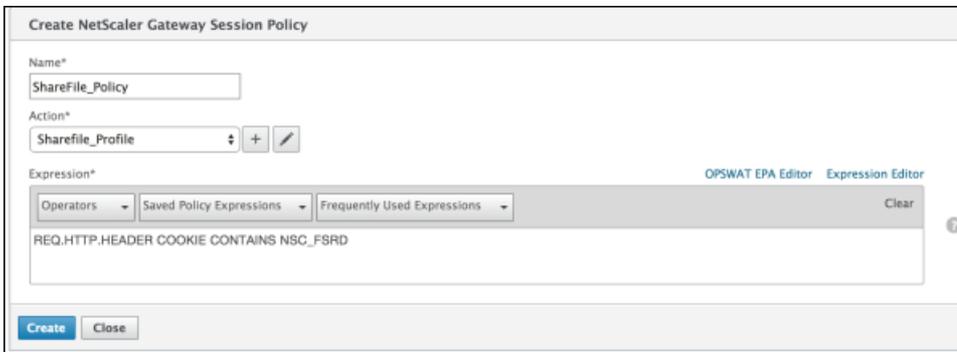
Done Cancel

Expression Editor  
Clear

Configure estos parámetros:

- **Value.** Escriba NSC\_FSRD.
- **Header Name.** Escriba COOKIE.
- Haga clic en **Done**.

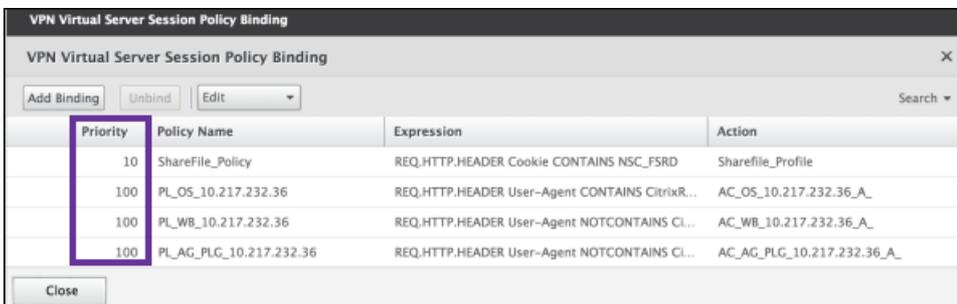
7. Haga clic en **Create** y, luego, en **Close**.



## 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 para 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.



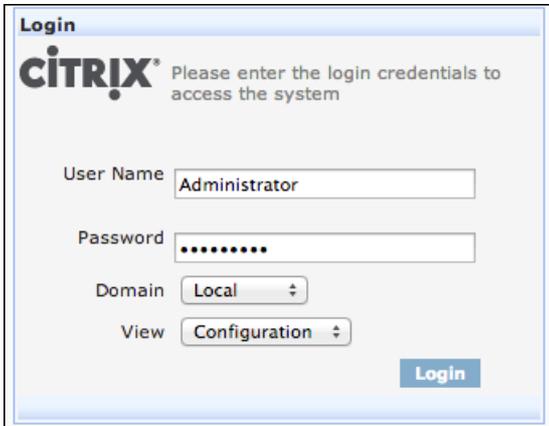
Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A

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**.



Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
ShareFile_SAML	ShareFile	Online storage for business
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3

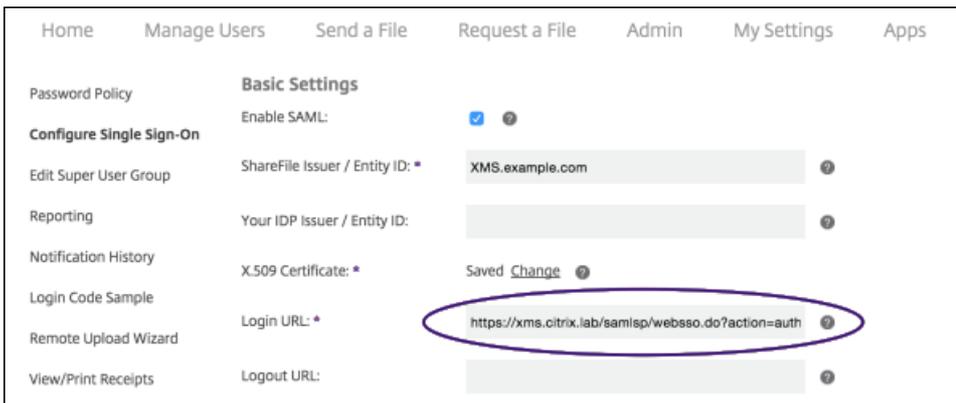
Cómo modificar los parámetros de Single Sign-On de ShareFile.com

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

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

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

El campo **URL de inicio de sesión** debe ser similar a: [https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML\\_SP&reqtype=1](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&reftype=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=authenticateUser&app=ShareFile_SAML&reftype=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&reftype=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 **Parámetros optativos**, marque la casilla de verificación **Habilitar autenticación Web**.

**Optional Settings**

Require SSO Login:  ?

SSO IP Range:  ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

**Enable Web Authentication:  ?**

SP-Initiated Auth Context: User Name and Password ? Minimum ?

Active Profile Cookies:  ?

Save Cancel

Lleve a cabo lo siguiente para validar la configuración.

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

Se le redirigirá al formulario de inicio de sesión de NetScaler Gateway. Si no se le dirige, 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 <subdominio>.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

Mar 02, 2017

Los dispositivos que ejecutan Windows 10 se inscriben con Azure como método federado de autenticación de Active Directory. Puede unir dispositivos Windows 10 con Microsoft Azure Active Directory de cualquiera de las siguientes maneras:

- Inscribirse en MDM como parte de Azure AD Join la primera vez que se encienda el dispositivo.
- Inscribirse en MDM como parte de Azure AD Join desde la página de configuración de Windows una vez que el dispositivo esté configurado.

Necesita una licencia Premium de Microsoft Azure Active Directory para poder integrar XenMobile con Microsoft Azure. La licencia es necesaria para permitir la integración MDM con Azure Active Directory para que los usuarios con dispositivos Windows 10 puedan inscribirse mediante Azure Active Directory. Consulte [Microsoft Azure](#) para obtener información sobre la obtención de la licencia Premium. Para obtener información acerca de los precios, consulte [Precios de Active Directory de Azure](#).

Antes de que los usuarios de dispositivos Windows puedan inscribirse con Azure, se deben configurar los parámetros del servidor Microsoft Azure en XenMobile y la directiva de términos y condiciones para dispositivos Windows. En este artículo, se describe cómo configurar los parámetros de Microsoft Azure. Para obtener información acerca de la configuración de una directiva de términos y condiciones para dispositivos Windows, consulte las [Directivas de términos y condiciones](#).

Antes de configurar los parámetros del servidor Microsoft Azure en XenMobile, debe iniciar sesión en el portal de Azure AD y llevar a cabo lo siguiente:

1. Registre el dominio personalizado y verifíquelo. Para obtener más información, consulte [Incorporación de su propio nombre de dominio a Azure Active Directory](#).
2. Extienda el directorio local a Azure Active Directory mediante las herramientas de integración de directorios. Para obtener más información, consulte [Integración de directorios](#).
3. Haga de MDM una parte fiable de Azure Active Directory. Para ello, haga clic en **Azure Active Directory > Aplicaciones** y, a continuación, haga clic en **Agregar**. Seleccione **Agregar una aplicación** de la galería. Vaya a **ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES**, seleccione **Aplicación MDM local** y guarde la configuración.
4. En la aplicación, configure los términos de uso de los dispositivos de punto final, URI de ID de aplicación y la detección de servidores XenMobile de la siguiente manera:
  - URL de detección MDM: `https://<FQDN>:8443/zdm/wpe`
  - URL de condiciones de uso MDM: `https://<FQDN>:8443/zdm/wpe/tou`
  - URI de ID de aplicación: `https://<FQDN>:8443/`
5. Seleccione la aplicación MDM local que ha creado en el paso 3 y habilite la opción **Administrar dispositivos para estos usuarios** para permitir la administración de dispositivos móviles de todos los usuarios o de un grupo de usuarios concreto.

También tendrá que anotar la siguiente información de su cuenta de Microsoft Azure para configurar parámetros en la consola de XenMobile:

- URI de ID de aplicación. La dirección URL del servidor que ejecuta XenMobile.

- ID de inquilino. Obtenida desde la página de parámetros de la aplicación de Azure.
- ID de cliente. Un identificador único para la aplicación.
- Clave. Obtenida desde la página de parámetros de la aplicación de Azure.

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

2. En **Server**, haga clic en **Microsoft Azure**. Aparece la página **Microsoft Azure**.

The screenshot shows the XenMobile interface with a green header containing 'XenMobile', 'Analyze', 'Manage', and 'Configure'. On the right, there is a gear icon and a user profile 'admin'. Below the header, the breadcrumb 'Settings > Microsoft Azure' is visible. The main heading is 'Microsoft Azure', followed by a descriptive paragraph: 'Integrate XenMobile with Microsoft Azure to let devices running Windows 10 enroll with Azure as a federated means of Active Directory authentication. You derive the values to enter here from your Azure directory settings. Note that you must also configure a Terms & Conditions device policy for Windows; otherwise, users cannot enroll with Azure.' Below this, there are four input fields: 'App ID URI\*', 'Tenant ID\*' (with a help icon), 'Client ID\*', and 'Key\*' (with a help icon). At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Configure los siguientes parámetros:

- **App ID URI.** Escriba la URL del servidor que ejecuta XenMobile que especificó cuando configuró Azure.
- **Tenant ID.** Copie este valor de la página Configuración de la aplicación de Azure. En la barra de direcciones del explorador, copie la sección de números y letras. Por ejemplo, en <https://manage.windowsazure.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 dispositivo, deben hacer lo siguiente:

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

# Actualización

Mar 02, 2017

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

Dispone de estas opciones para actualizar XenMobile:

- **Para actualizar desde XenMobile 9.0 a XenMobile 10.4.**

Utilice la herramienta Upgrade Tool de XenMobile que está incorporada en XenMobile 10.4. 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.x a XenMobile 10.4.**

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 instalaciones de XenMobile 10.3.x.

- **Para actualizar desde XenMobile 10 o XenMobile 10.1 a XenMobile 10.4.**

Primero, actualice XenMobile de 10 o 10.1 a 10.3 desde la página **Release Management** de la consola de XenMobile. Luego, actualice XenMobile de 10.3 a 10.4 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.

Versión de XenMobile Server	Número de versión	Actualizar a	Número de versión	Ruta de actualización	Ubicación de la actualización de versión
XenMobile Server 9 con Rolling Patch 9 instalado	9.0.0_97106	XenMobile Server 10.4	10.4.0.116	De XenMobile Server 9 a XenMobile Server 10.4	<a href="#">Descargue</a> el requisito previo de revisiones (rolling patch). La herramienta de actualización Upgrade Tool para XenMobile 10.4 está incorporada en XenMobile Server.
XenMobile Server 10 o XenMobile 10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	Actualizar XenMobile 10 o XenMobile 10.1 a XenMobile 10.3	<a href="#">Descargar</a>
XenMobile Server 10.3.x	10.3.x	XenMobile Server 10.4	10.4.0.116	Actualizar de XenMobile 10.3.x a XenMobile 10.4.	<a href="#">Descargar</a>

¿10.4.0.?

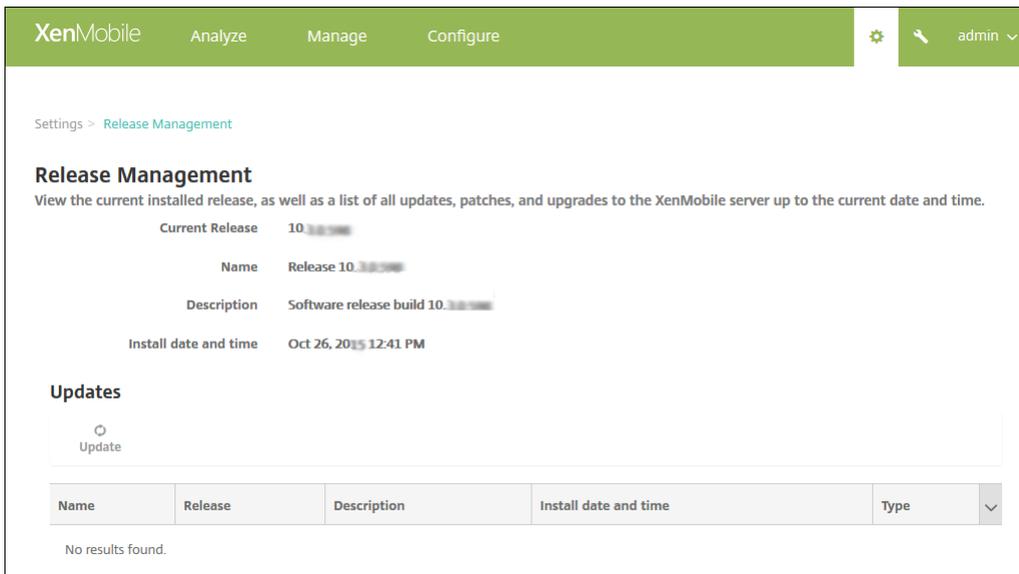
¿10.4.0.?

Requisitos previos:

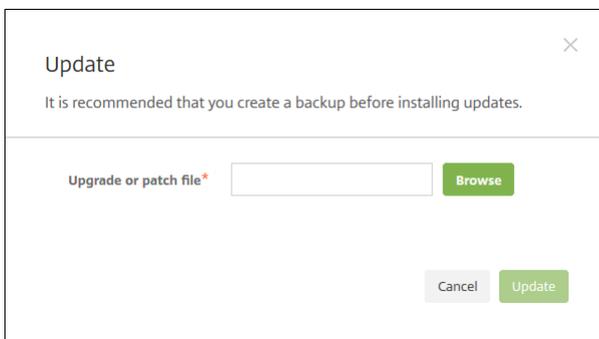
- Antes de instalar una actualización de XenMobile, utilice las instalaciones de la máquina virtual (VM) para tomar una instantánea del sistema.
- Realice una copia de seguridad de la base de datos de configuración del sistema.
- Consulte los Requisitos del sistema de la versión a la que está actualizando. Para XenMobile 10.4, consulte [Requisitos del sistema](#).

Si tiene una implementación de 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 reierte a un estado anterior al intento de actualización.

**Nota:** Es posible que no sea necesario reiniciar XenMobile una vez instalada la actualización. En este caso, un mensaje indica que la instalación de la actualización se realizó correctamente. Si, sin embargo, XenMobile no necesita reiniciarse, debe usar la línea de comandos. Es importante que borre la caché del explorador Web después de reiniciarse el sistema.

4. Haga clic en **Browse**, vaya a la ubicación en la que guardó el archivo de actualización de XenMobile que descargó de Citrix.com y selecciónelo.

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

**Nota:** Es posible que no sea necesario reiniciar XenMobile una vez instalada la actualización. En este caso, un mensaje indica que la instalación de la actualización se realizó correctamente. Si, sin embargo,

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

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

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

4. Haga clic en **Browse**, vaya a la ubicación en la que guardó el archivo de actualización de XenMobile que descargó de Citrix.com y selecciónelo.

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

**Nota:** Es posible que no sea necesario reiniciar XenMobile una vez instalada la actualización. En este caso, un mensaje indica que la instalación de la actualización se realizó correctamente. Si, sin embargo,

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

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

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

## 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. XenMobile, a continuación, revierte el sistema a su estado anterior.

# Requisitos previos de Upgrade Tool

Mar 02, 2017

Para actualizar desde XenMobile 9.0 a XenMobile 10.4, utilice la herramienta Upgrade Tool integrada de XenMobile 10.4.

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 migrala a una implementación independiente de XenMobile 10.4. 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 10.4](#).

XenMobile 10.4 admite las versiones 11.1.x, 11.0.x y 10.5.x de NetScaler Gateway.

La herramienta Upgrade Tool integrada en XenMobile 10.4 también admite la versión 10.1.x de NetScaler Gateway. Citrix no respalda el uso de NetScaler Gateway 10.1 con XenMobile 10.4. No obstante, puede actualizar una implementación de NetScaler Gateway 10.1 con la herramienta Upgrade Tool integrada en XenMobile 10.4. 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. Luego, deberá configurar una nueva instancia de XenMobile 10.4 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 10.4, primero se debe probar la actualización y, solo después, realizar la actualización de producción completa.

### Si elige Test Drive (Actualización de prueba):

La herramienta Upgrade Tool realiza una actualización de prueba con los datos de configuración del entorno de producción para comparar XenMobile 9.0 y XenMobile 10.4, 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.

### Si elige Upgrade (Actualizar):

Primero, la herramienta Upgrade Tool copia todos los datos de configuración, dispositivo y usuario desde XenMobile 9.0 a una nueva instancia de XenMobile 10.4 con el mismo nombre de dominio completo (FQDN). Todos los datos en XenMobile 9.0 permanecen intactos hasta que se mueve el servidor XenMobile 10.4 al entorno de producción.

Al iniciar sesión en la consola de XenMobile 10.4 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 XenMobile 10.4 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 XenMobile 10.4).
- 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, la directiva de personalización de marca no se actualiza. XenMobile 10.4 admite una directiva de personalización de marca; debe dejar una directiva de personalización de marca en XenMobile 9.0 para actualizar a XenMobile 10.4.
- Parámetros contenidos en el archivo auth.jsp de XenMobile 9.0 que se usan para restringir el acceso a la consola. En XenMobile 10.4, las restricciones de acceso a la consola son parámetros del firewall que se pueden configurar en 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 XenMobile 10.4).

## 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](#).

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		
<input type="checkbox"/>		Domain users	Jun 13 2016 5:10 PM	
<input type="checkbox"/>		Sales	Apr 13 2016 12:50 PM	

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

**XenMobile** Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

### Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

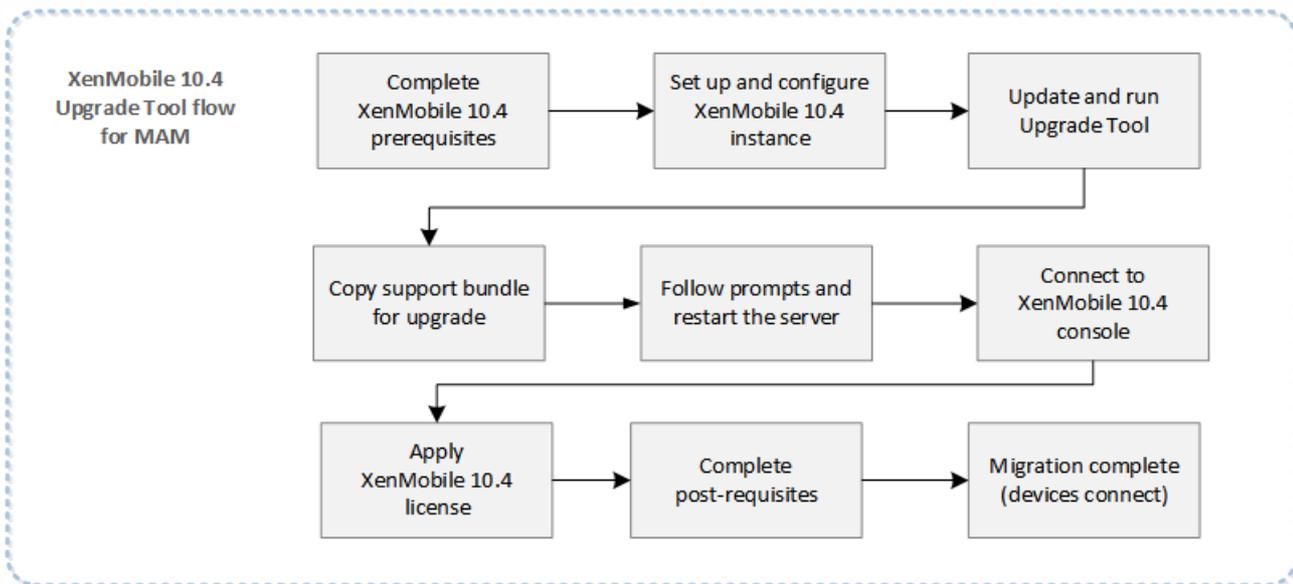
### Delivery Group Information ✕

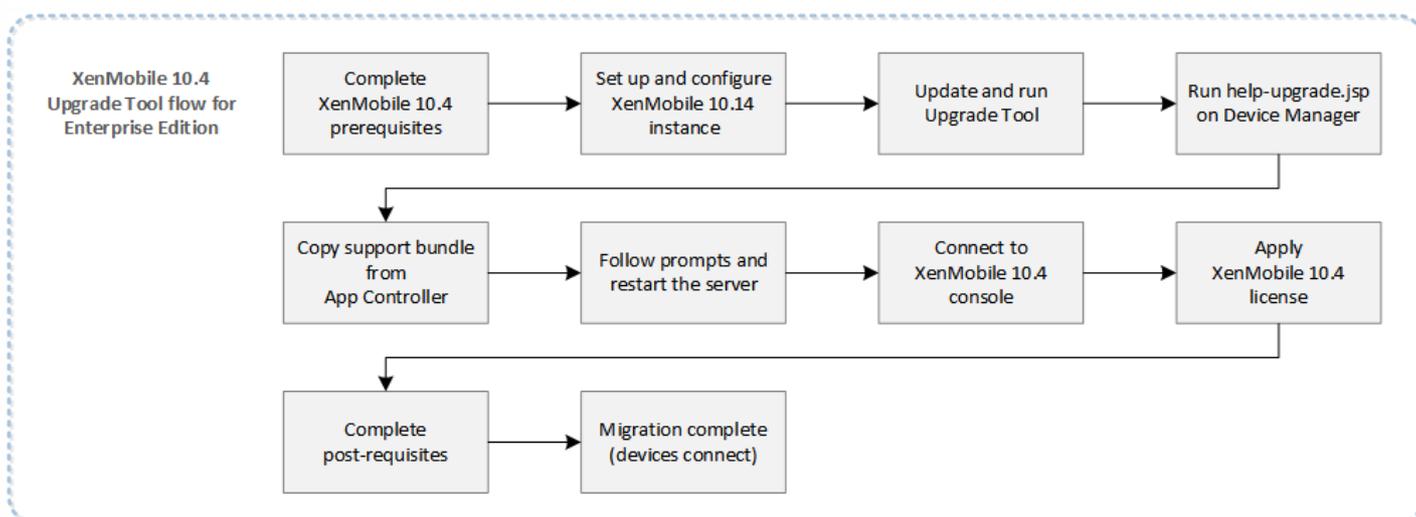
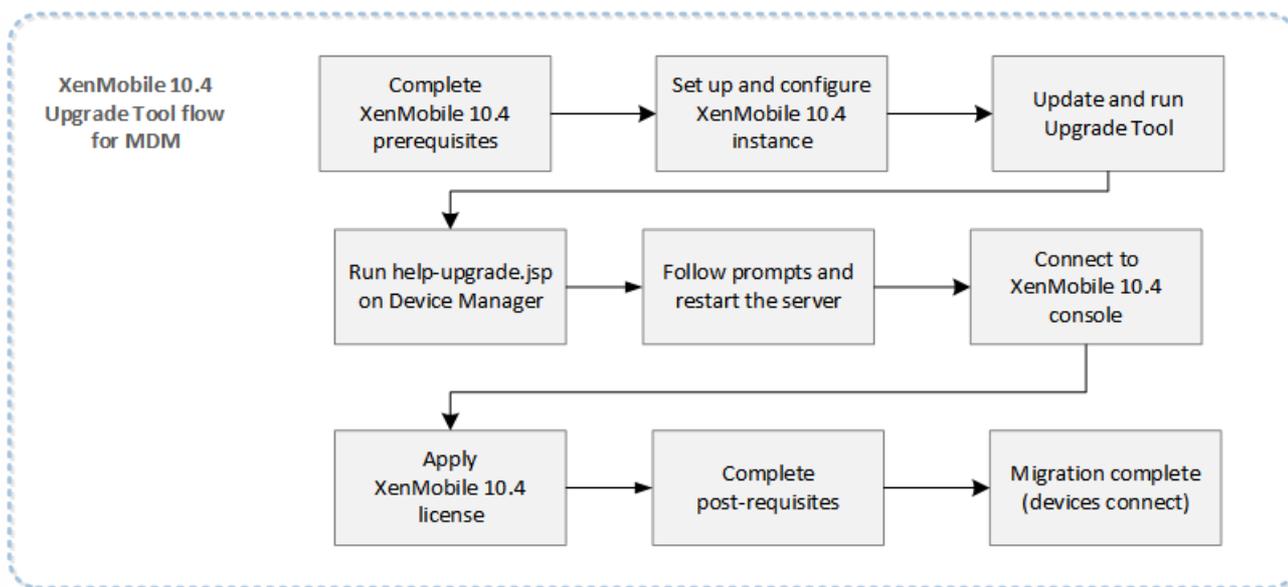
Enter a name for the delivery group and any information that will help you keep track of it later.

**Name**

**Description**

Los diagramas siguientes ilustran los pasos básicos necesarios para la actualización desde XenMobile 9.0 a XenMobile 10.4.





Citrix recomienda seguir los pasos siguientes para actualizar a XenMobile 10.4 un entorno de XenMobile 9.0 Enterprise que tiene dispositivos Windows Phone inscritos en modo de empresa y usa Worx Home 9.x.

1. Actualice Worx Home en Device Manager a la versión 10.2 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 a Download Hub en su teléfono para instalar Worx Home 10.2, que usted implementó desde Device Manager.
4. Después de completar los requisitos previos que se describen en este artículo, actualice a XenMobile 10.4 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 XenMobile 9.0 App Controller Rolling Patch 9 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 XenMobile 10.4, 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.

#### Beacons [Edit](#)

---

Store name:	*	<input type="text" value="Store"/>
Default store view:		<input type="button" value="Category"/>

---

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 10.4 de forma similar a los puertos abiertos para la IP del servidor XenMobile 9.0. Para conocer los requisitos de puertos de XenMobile 10.4, consulte [Requisitos de puertos](#).
- **LDAP Server.** Compruebe que el nuevo servidor XenMobile 10.4 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 10.4](#).

**De XenMobile 9.0**

**A XenMobile 10.4**

## Enterprise Edition

### App Controller

### MDM

PostgreSQL locales	PostgreSQL locales	PostgreSQL locales
PostgreSQL locales	MS SQL	MS SQL
PostgreSQL locales	Remote PostgreSQL	Remote PostgreSQL

### App Edition

PostgreSQL locales		PostgreSQL locales
PostgreSQL locales		Remote PostgreSQL
PostgreSQL locales		MS SQL

### MDM Edition

PostgreSQL locales		PostgreSQL locales
MS SQL		MS SQL
Remote PostgreSQL		Remote PostgreSQL

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, XenMobile 10.4 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 XenMobile 10.4 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 XenMobile 10.4 al crear 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**.

**System Configuration**

- Overview
- Deployment
- XenMobile MDM
- GoToAssist
- Active Directory
- Certificates**
- Branding
- Network Connectivity
- Domain Name Server
- NTP Server
- Workflow Email
- Administrator
- Release Management
- Receiver Email Template

**Quick Links**

- [Configure settings](#)
- [Download .cr file](#)
- [Add connector](#)
- [Configure nested groups](#)

**Certificates**

You can view the certificates installed on App Controller, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PKCS#12 certificates stored on your computer by clicking Import.

All Certificates						
Active	Name	Description	Valid from	Valid to	Type	Status
	AppController.example.com	Self Generated/Signed	5/22/2015	5/19/2025	Server	
✓	*.citrix.net	(imported)	6/3/2014	6/2/2016	Server	
	CITRITeIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate	
	CITRITePolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate	
	CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate	
✓	*.citrix.net	(imported)	6/3/2014	6/2/2016	saml	

Certificate Chain						
Name	Description	Valid from	Valid to	Type	Status	
CITRITeIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate		
CITRITePolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate		
CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate		

Buttons: Import, Export, New..., Make Active, Self-Signed, Details, Delete, Add to Chain, Details, Delete

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

**System Configuration**

- Overview
- Deployment
- XenMobile MDM
- GoToAssist
- Active Directory
- Certificates**
- Branding
- Network Connectivity
- Domain Name Server
- NTP Server
- Workflow Email
- Administrator
- Release Management
- Receiver Email Template

**Quick Links**

- [Configure settings](#)
- [Download .cr file](#)
- [Add connector](#)
- [Configure nested groups](#)

**Certificates**

You can view the certificates installed on App Controller, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PKCS#12 certificates stored on your computer by clicking Import.

All Certificates						
Active	Name	Description	Valid from	Valid to	Type	Status
	AppController.example.com	Self Ge				
✓	*.citrix.net	(import				
	CITRITeIssuingCA01	(import			intermediate	
	CITRITePolicyCA	(import			intermediate	
	CITRIXRootCA	(import			intermediate	
✓	*.citrix.net	(import				

Certificate Chain						
Name	Description	Valid from	Valid to	Type	Status	
CITRITeIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate		
CITRITePolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate		
CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate		

**Export Certificate** dialog box:

Password: \*

Confirm Password: \*

Buttons: Ok, Close

Buttons: Import, Export, New..., Make Active, Self-Signed, Details, Delete, Add to Chain, Details, Delete

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

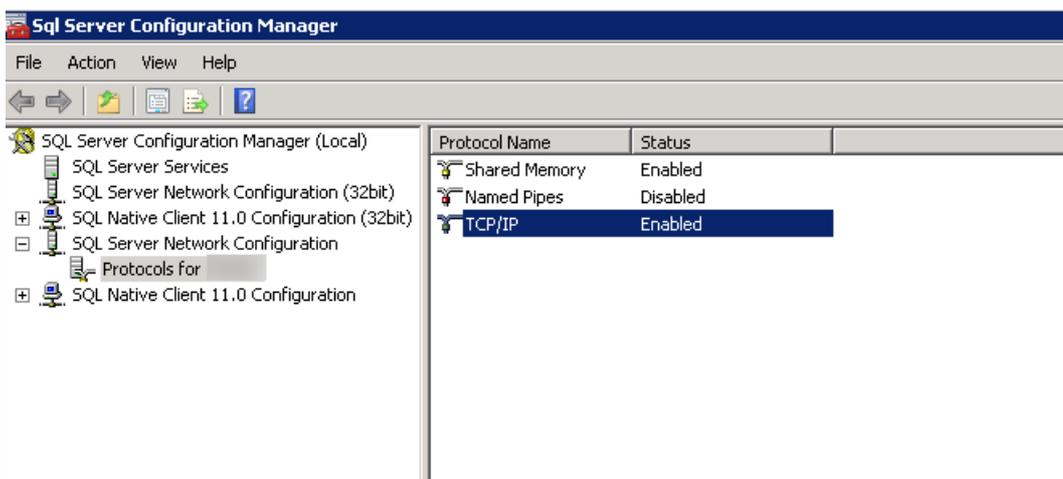
Mar 02, 2017

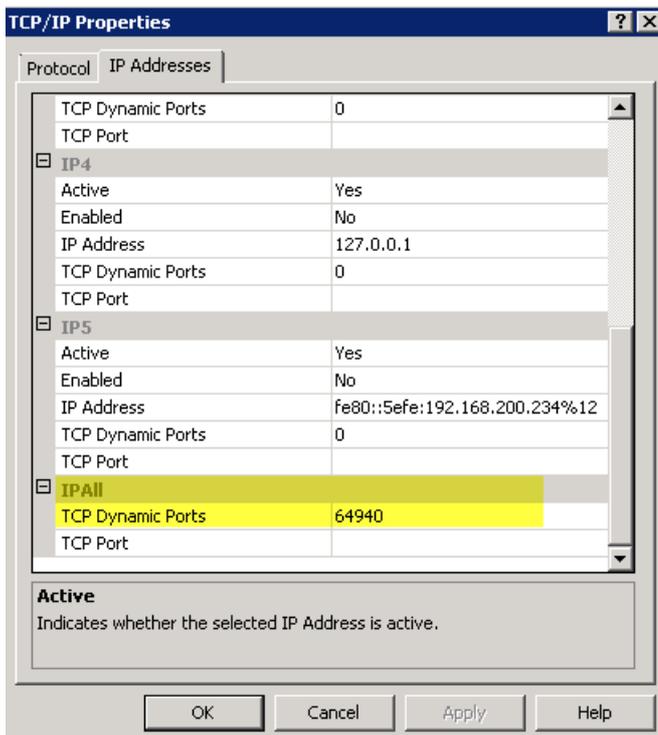
Si el entorno de XenMobile 9 cumple los requisitos siguientes, siga los pasos indicados en esta sección antes de actualizar.

- 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

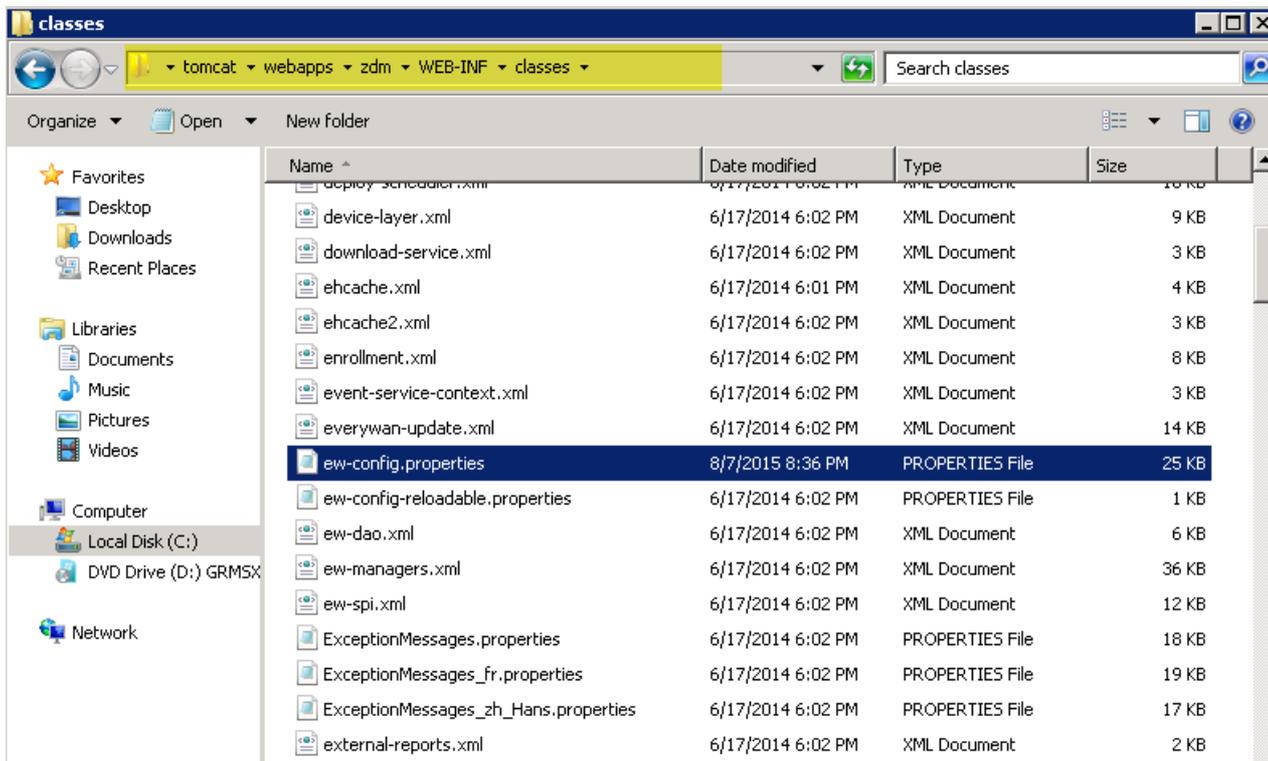
Citrix recomienda que la instancia de la base de datos de SQL Server se ejecute siempre en un puerto estático, porque el servidor XenMobile necesita acceso continuo a la base de datos. Esta conexión, por lo general, atraviesa un firewall. Como resultado de ello, necesita abrir el puerto correspondiente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

```
ew-config.properties
18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/verywan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress;domain=sparus-
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:verywan/verywan@localhost:1521/verywan
22 pooled.datasource.url=jdbc:jtds:sqlserver://ah-234 .net/ -11aug;instance=
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234. .net
25 # Pooled datasource database
26 pooled.datasource.database= aug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
31 pooled.datasource.password=(aes) ==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/verywan
37 # No pooled datasource user
38 #no.pooled.datasource.user=verywan
39 # No pooled datasource password
40 #no.pooled.datasource.password=verywan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver://ah-234 / -11aug;instance=
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234 .net
48 # Audit datasource database
49 audit.datasource.database= -11aug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password
```

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

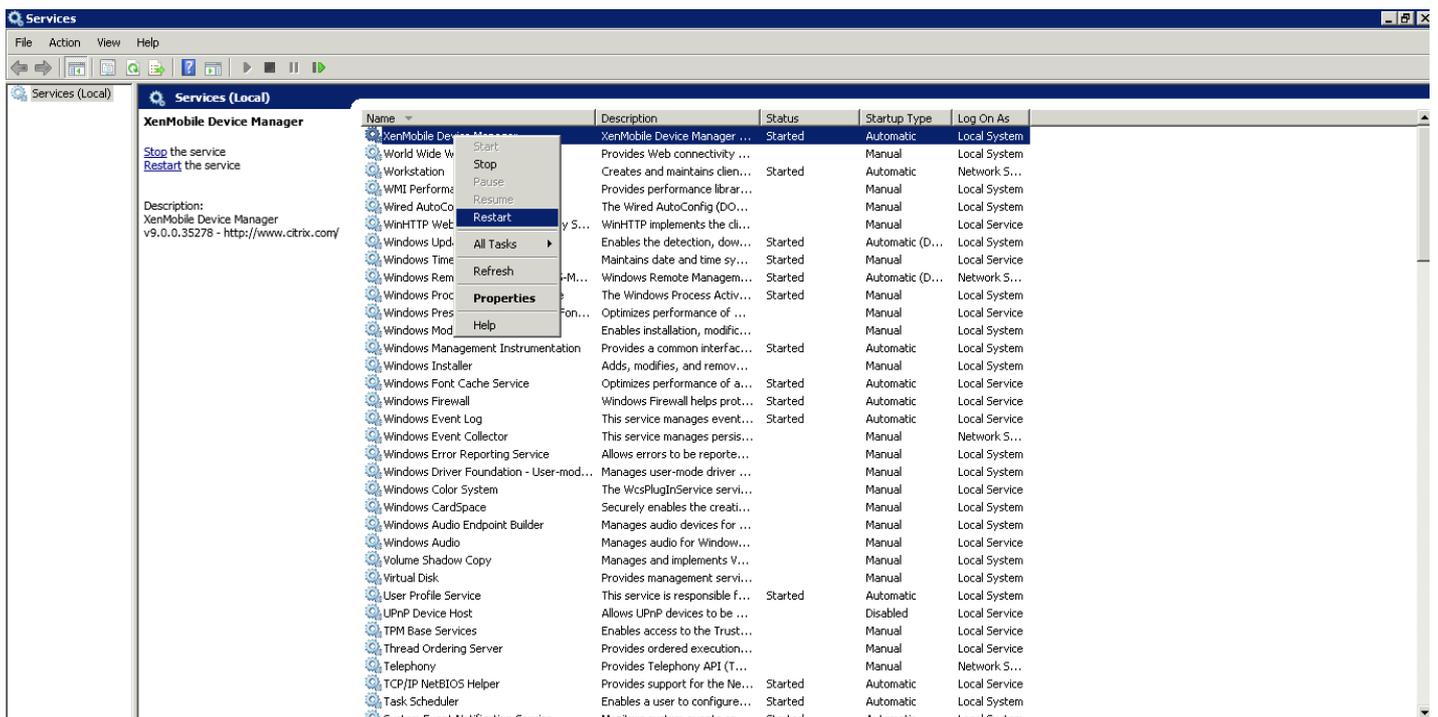
Citrix recomienda hacer una copia de seguridad, copiar o tomar nota de los cambios realizaos en el archivo ew-config.properties. Esta información puede servir de ayuda en caso de que falle la actualización.

```

18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@localhost:1521/everywan
22 pooled.datasource.url=jdbc:sqlserver://ah-234.net:1433/llaug
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234.net
25 # Pooled datasource database
26 pooled.datasource.database=llaug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
31 pooled.datasource.password={aes}
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everywan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everywan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver://ah-234.net:1433/llaug
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234.net
48 # Audit datasource database
49 audit.datasource.database=llaug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password

```

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.

```
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]: █
```

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 XenMobile 10.4.

## Important

Si quiere tomar una instantánea del sistema, hágalo después de la configuración inicial de XenMobile 10.4 y antes de acceder 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.

```
*****
*      Citrix XenMobile      *
*      (in First Time Use mode) *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password:

Network settings:
IP address [I]: 10.207.87.35
Netmask [I]: 255.255.254.0
Default gateway [I]: 10.207.86.1
Primary DNS server [I]: 10.207.86.50
Secondary DNS server (optional) [I]: 10.207.86.51

Commit settings (y/n) [y]:
```

3. Escriba **y** para actualizar.

## Nota

Si no selecciona "y" aquí, deberá configurar una nueva instancia de XenMobile 10.4 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.

```
Commit settings (y/n) [y]:
Applying network settings...

Upgrade:
Upgrade from previous release (y/n) [n]: y

Encryption passphrase:
Generate a random passphrase to secure the server data (y/n) [y]:

Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:
Server [I]: sql01.xmlab.net
Port [I]: 1433
Username [sa]: xmsadmin
Password:
Database name [DB_service]: migdemo

Commit settings (y/n) [y]:
```

XenMobile inicializa la base de datos.

```
Checking database status...
Database does not exist.
Initializing database...
```

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

Debe coincidir el nombre de dominio completo (FQDN) de los entornos 9.0 y 10.4.

```
Cluster:
Please press y to enable cluster? [y/n]: y
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu, once the system configuration is complete.
Xenmobile Server FQDN:
Hostname []: migdemo.xs.citrix.com
Commit settings (y/n) [y]:
Applying fqdn settings...
```

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

8. Establezca los puertos de comunicación.

```
Communication ports:
HTTP [80]:
HTTPS with certificate authentication [443]:
HTTPS with no certificate authentication [8443]:
HTTPS for management [4443]:
Commit settings (y/n) [y]:
```

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

```

Applying port listener configuration...

The wizard will now generate an internal Public Key Infrastructure (PKI):
- A root certificate
- An intermediate certificate to issue device certificates during enrollment
- An intermediate certificate to issue an SSL certificate
- An SSL certificate for your connectors
- A Node Identification certificate for cluster node client auth
Do you want to use the same password for all the certificates of the PKI [y]:
New password:
Re-enter new password:

Commit settings (y/n) [y]:
Generating SAML signing certificate...
Generating server and client certificates...

XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]:

```

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

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

XenMobile 10.4 habilita la herramienta de actualización Upgrade Tool de un solo uso.

```

Re-enter new password:

Commit settings (y/n) [y]: y
Creating console administrator...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds.....
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  not ready to start yet [ OK ]

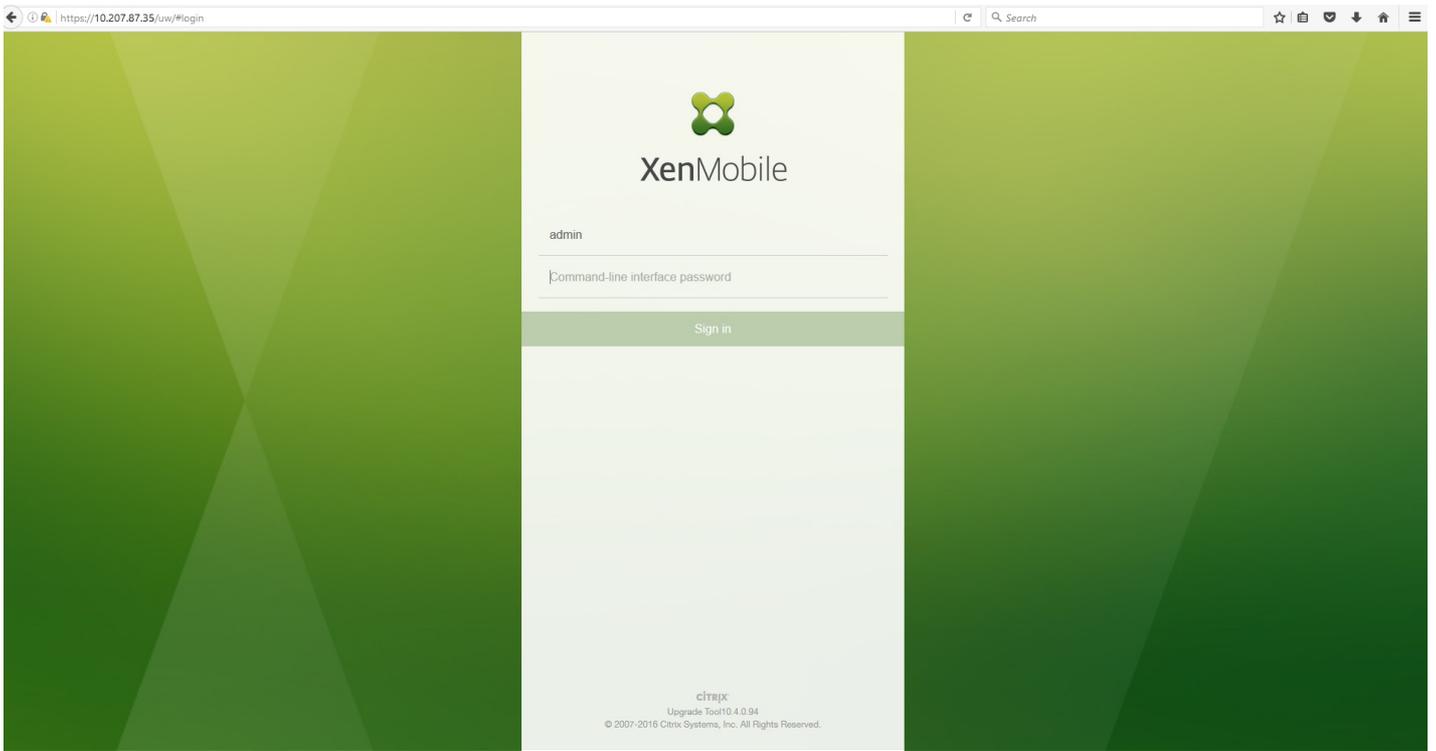
To complete the upgrade process, from a web browser, go to the following
location and log on with your command prompt credentials:
https://10.207.87.35/uw/

Starting monitoring... [ OK ]

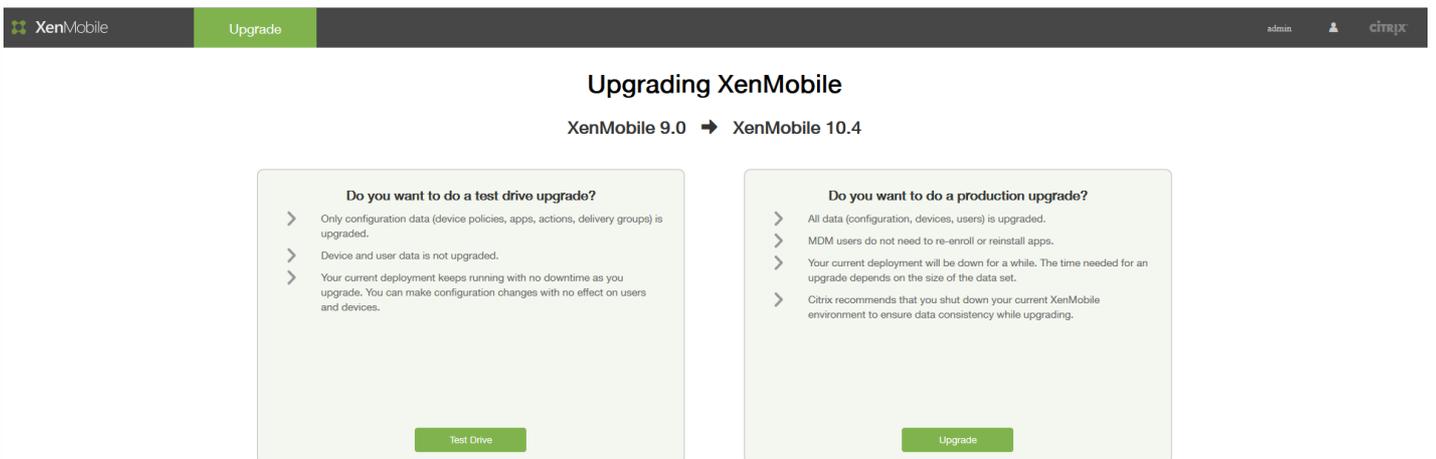
migdemo.xs.citrix.com login:

```

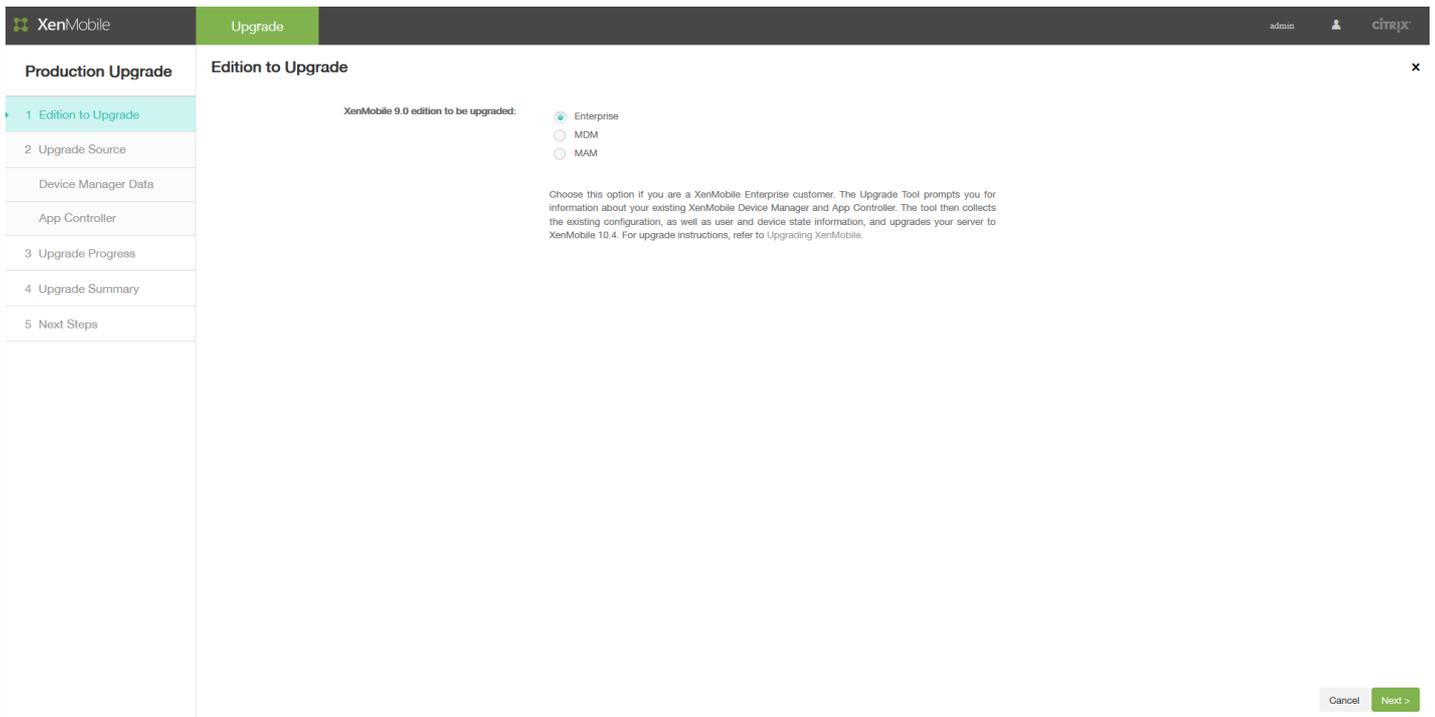
14. Acceda a la herramienta de actualización Upgrade Tool desde un explorador Web con `https://<XenMobile-Server-IPAddress>/uw/` e inicie sesión con las credenciales que ha especificado en la interfaz de línea de comandos.



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.



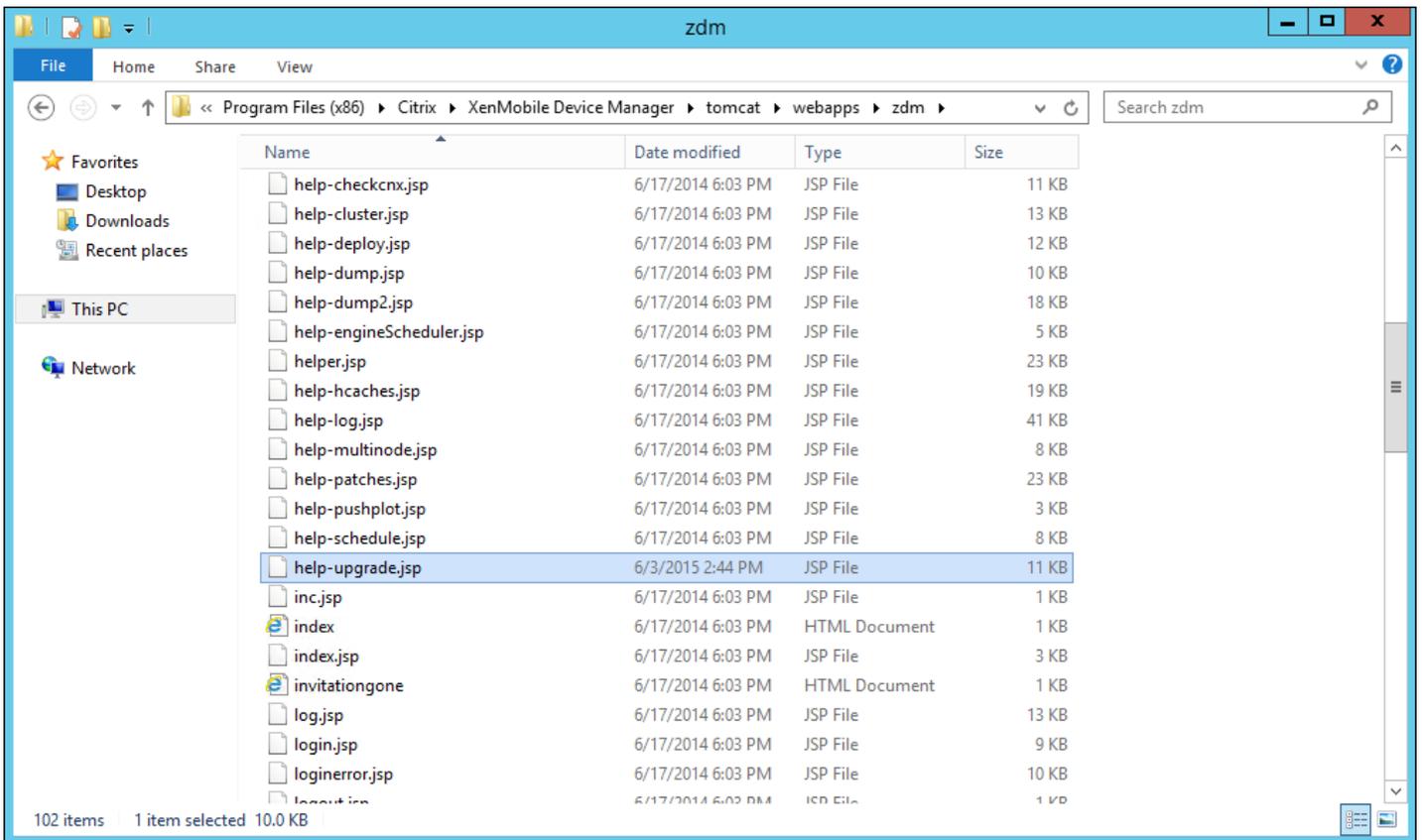
17. Haga clic en **Siguiente**.

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**.

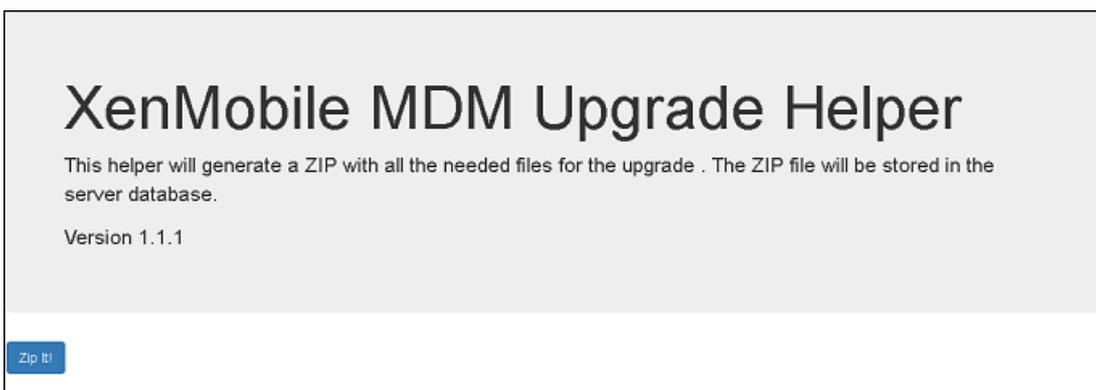
- a. Haga clic en el enlace indicado en el paso 1 de la página **Device Manager** y guarde el archivo descargado help-upgrade.zip.
- b. Extraiga el archivo help-upgrade.jsp en <ruta de instalación de MDM>\tomcat\webapps\zdm en el XenMobile 9.0 Device Manager existente.



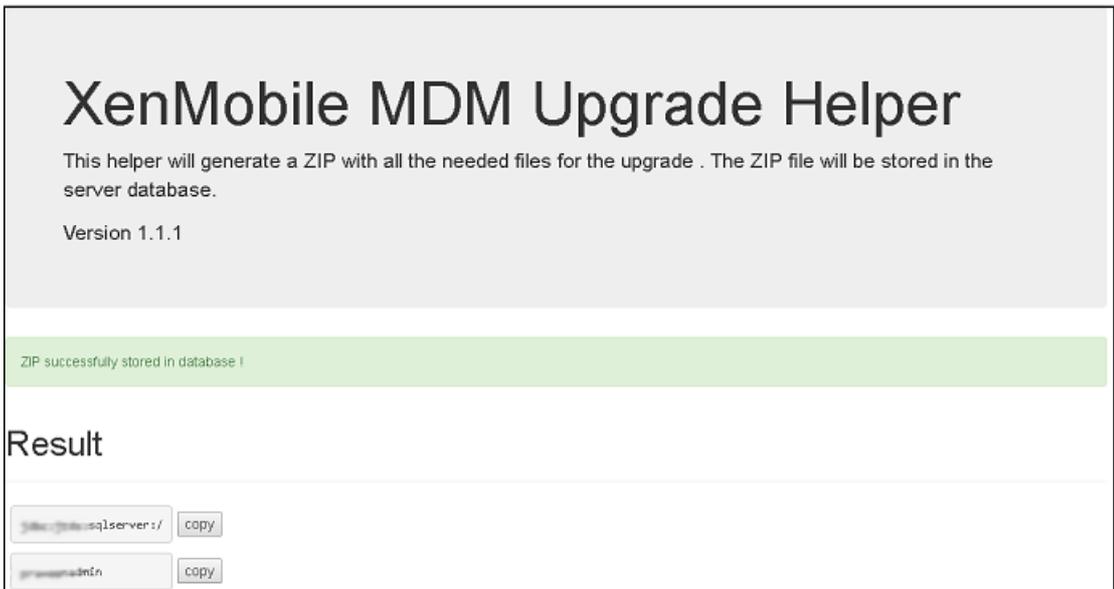
c. En una ventana del explorador, inicie sesión en el servidor XenMobile 9.0.

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 XenMobile 10.4. 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.

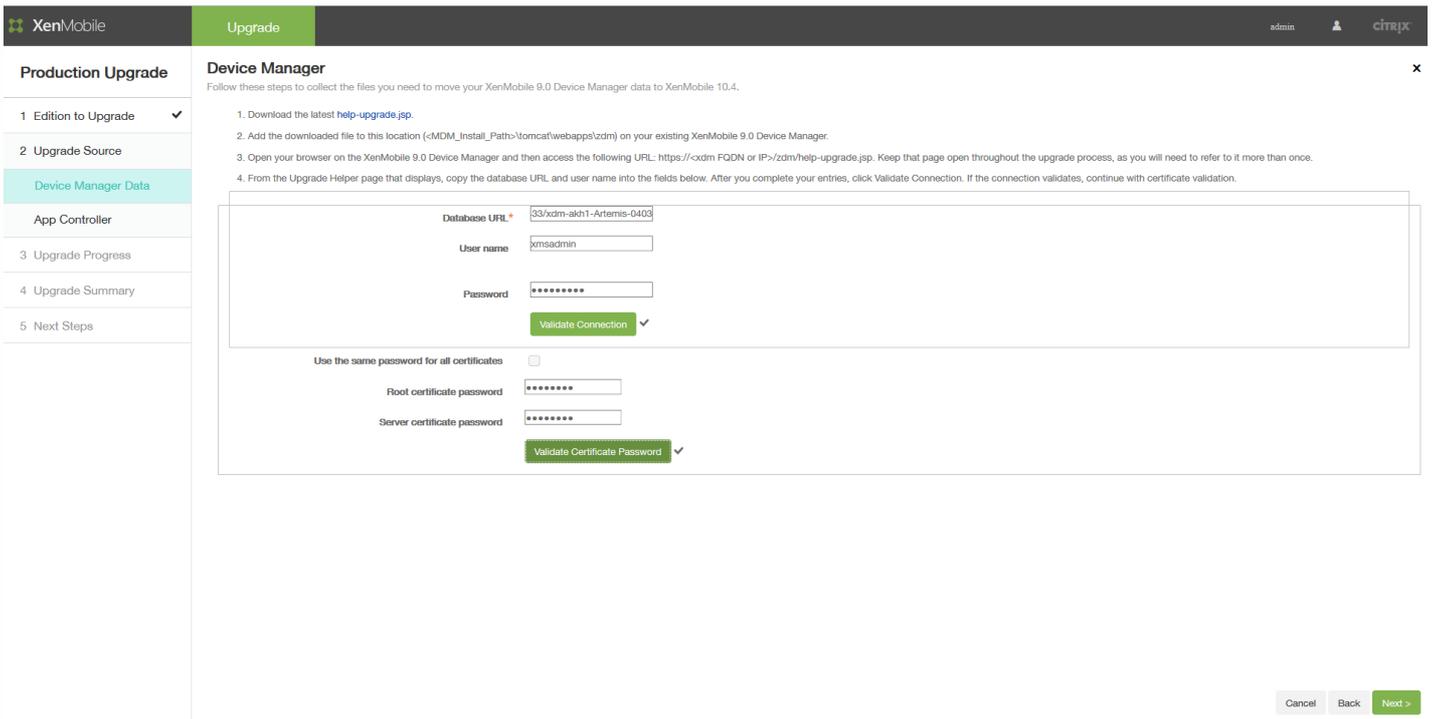


19. En **Result**, copie la URL y péguela en el campo **Database URL** en la página **Device Manager** de la herramienta Upgrade Tool. A continuación, copie el nombre de usuario y péguelo en la página **Device Manager**.



20. En la herramienta Upgrade Tool:

- a. Escriba la contraseña y, a continuación, haga clic en **Validate Connection**.
- b. Escriba la contraseña para cada certificado y, a continuación, haga clic en **Validate Password**.



21. Haga clic en **Siguiente**.

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 comprimir de nuevo. 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 en 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.

The screenshot shows the XenMobile Upgrade interface. The top navigation bar includes the XenMobile logo, the 'Upgrade' tab, and user information (admin, Citrix). The main content area is titled 'App Controller' and contains a list of steps for upgrading from XenMobile 9.0 to 10.4. The steps are:

- Before upgrading from XenMobile 9.0 to XenMobile 10.4, you must apply the latest App Controller patch to App Controller. Steps to apply the patch:
  - Download the patch from the Citrix Downloads site.
  - Log on to App Controller.
  - Go to Settings > Release Management.
  - Click Import.
  - Select the patch you downloaded in Step 1.
  - Click Upload.
- After you apply the patch, follow the steps below to generate support bundle. The support bundle captures all important information to upgrade to XenMobile 10.4.
  - In the App Controller command-line console, type 4 and then press Enter to open the Troubleshooting menu.
  - In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.
  - In the Support Bundle menu, type 1, press Enter, and then follow the command prompts.
  - You must encrypt the support bundle. To do so, type y, press Enter, and then follow the command prompts.
- Upload the support bundle from the previous step.

Below the steps, there is an input field and an 'Upload' button. At the bottom right, there are 'Cancel', 'Back', and 'Next >' buttons.

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.

```
AppController 9.0.0.973502, 2015-08-26
-----
Main Menu
-----
[0] Express Setup
[1] High Availability
[2] Clustering
[3] System
[4] Troubleshooting
[5] Help
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] █
```

b. En el menú Troubleshooting, escriba **3** y, a continuación, presione ENTRAR para abrir el menú Support Bundle.

```
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] 3
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----
Choice: [0 - 4] █
```

c. En el menú Support Bundle, escriba **1** y, a continuación, presione ENTRAR y siga las instrucciones.

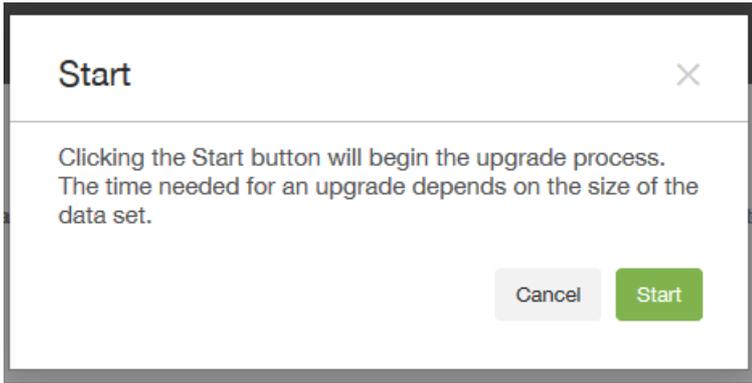
**Nota:** Debe cifrar el paquete de asistencia.

```
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] 3
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----
Choice: [0 - 4] 1
```

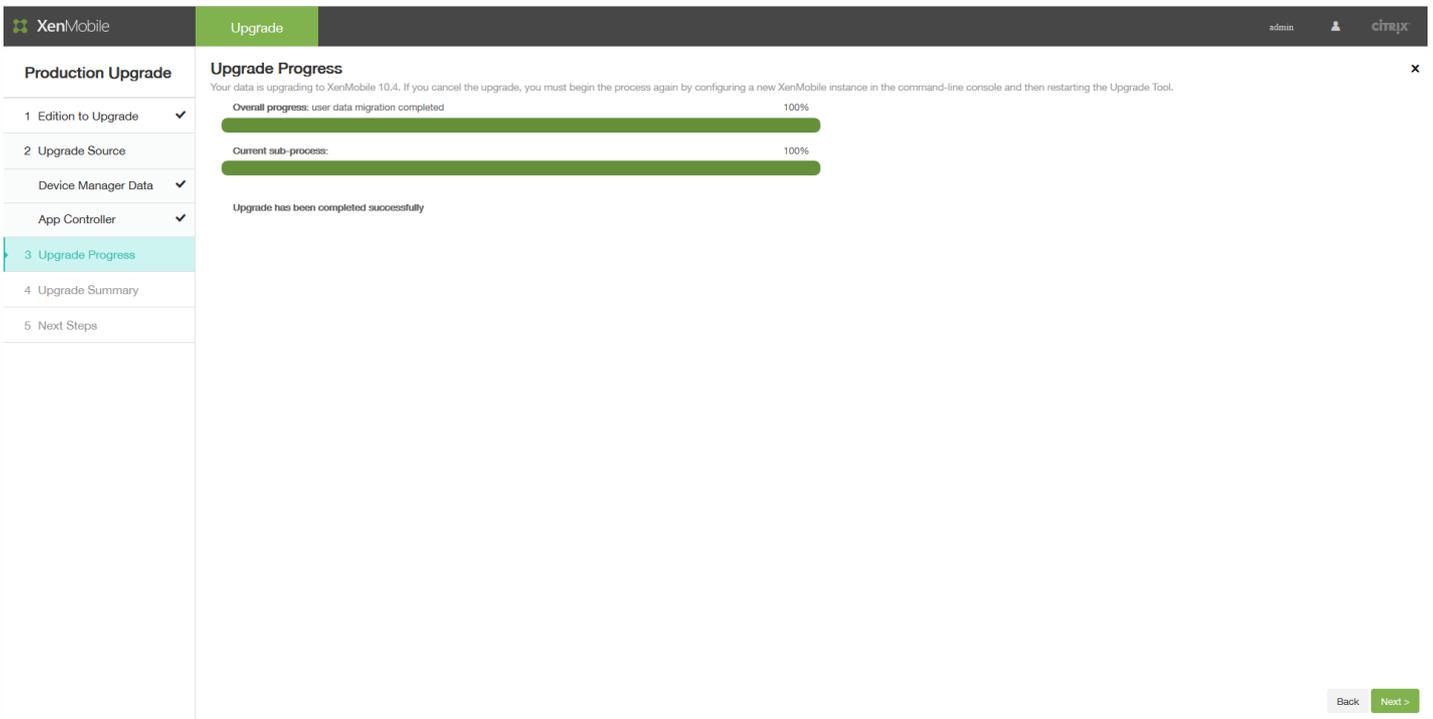
26. En la sección 3 de la página **App Controller**, especifique el paquete de asistencia y luego haga clic en **Upload**.

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 10.4 y reiniciar el proceso de actualización. No puede usar el botón Atrás del explorador Web para volver a las páginas anteriores y corregir 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:

The screenshot shows the XenMobile Upgrade Summary page. The left sidebar lists the upgrade steps: 1 Edition to Upgrade, 2 Upgrade Source, 3 Upgrade Progress, 4 Upgrade Summary (highlighted), and 5 Next Steps. The main content area displays the following upgrade statistics:

Devices Upgraded	5
Apps Upgraded	46
Users Upgraded	323
Delivery Groups Upgraded	12
Policies Upgraded	44
Smart Actions Upgraded	0

At the bottom right, there are buttons for 'Cancel', 'Back', and 'Next >'.

Si actualiza una edición MDM, la página **Upgrade Summary** puede tener el siguiente aspecto:

The screenshot shows the XenMobile Upgrade Summary page for an MDM edition. The left sidebar lists the upgrade steps: 1 Edition to Upgrade, 2 Upgrade Source, 3 Upgrade Progress, 4 Upgrade Summary (highlighted), and 5 Next Steps. The main content area displays the following upgrade statistics:

Devices Upgraded	604
Apps Upgraded	23
Users Upgraded	316
Delivery Groups Upgraded	5

At the bottom right, there are buttons for 'Cancel', 'Back', and 'Next >'.

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 XenMobile 10.4.

31. Después de descargar los registros de actualización, haga clic en **Next**. Aparecerá la página **Next Steps**.

The screenshot shows the XenMobile Upgrade interface. On the left, a sidebar titled 'Production Upgrade' contains a list of steps: 1. Edition to Upgrade, 2. Upgrade Source, Device Manager Data, App Controller, 3. Upgrade Progress, 4. Upgrade Summary, and 5. Next Steps (highlighted). The main content area is titled 'Next Steps' and contains a list of instructions:

1. You must configure licenses on XenMobile 10.4 to enable user connections. To do so, go to Configure > Settings > Licensing.
2. If you deployed the server running XenMobile 9.0 in the DMZ, you must change the external DNS for XenMobile to point to the new XenMobile 10.4 server.
3. If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, in NetScaler, you must configure the load balancing Device Manager instance with the new IP address for the XenMobile 10.4 server.
4. If you deploy XenMobile 10.4 in a cluster, you must use the command-line interface to enable cluster support and then join the new XenMobile nodes.

**Note:**  
Please collect support bundle from a newly upgraded XenMobile server before restarting it:  
1. In the command-line console, type 3 and then press Enter to open the Troubleshooting menu.  
2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.  
3. In the Support Bundle menu, type 2, press Enter to Generate support bundle.  
Restart the server. Go to Manage > Device and make sure all devices have been upgraded properly before making any NetScaler changes.

Find more information and procedures in Upgrading XenMobile.

At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Finish & Restart'.

Para obtener instrucciones relacionadas con estos pasos, consulte [Requisitos posteriores de la herramienta de actualización](#).

# Requisitos posteriores de la herramienta Upgrade Tool

Mar 02, 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 al nuevo servidor XenMobile 10.4.
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 UpgradeTool 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 XenMobile 10.4 en un clúster, debe usar la interfaz de línea de comandos (CLI) de XenMobile 10.4 para habilitar el respaldo de 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 actualizado, nombre de la tienda personalizada e inscripción de dispositivos de XenMobile después de la actualización.

XenMobile 10.4 solo admite el sistema de licencias de Citrix V6. Siga estos pasos para configurar licencias locales o remotas en la consola de XenMobile 10.4 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 consola de XenMobile 10.4 actualizada: 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**.

Settings > Licensing

### Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

License type: Remote license

License server\*: lic1.xmlab.net

Port\*: 27000

Test Connection

Product name	Status	Active	Total number of licenses	Number used	Type	Expires on
--------------	--------	--------	--------------------------	-------------	------	------------

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 XenMobile 10.4, 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**.

The screenshot shows the NetScaler Gateway interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The left sidebar shows a tree view with 'Virtual Servers' selected under 'Load Balancing'. The main content area is titled 'Virtual Servers' and contains a table with columns for Name, State, Effective State, IP Address, and Port. There are also buttons for 'Add', 'Edit', 'Delete', 'Enable', 'Disable', 'Statistics', and 'Action'.

	Name	State	Effective State	IP Address	Port
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443

2. Haga clic en **Add**.

3. En la página **Load Balancing Virtual Server**, configure los siguientes parámetros y haga clic en **OK**.

## ← Load Balancing Virtual Server

### Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.

You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*

Protocol\*

IP Address Type\*

IP Address\*

Port\*

► More

- **Name.** Escriba el nombre del nuevo equilibrador de carga.
  - **Protocol:** Establecer 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**.

# Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

### Basic Settings

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

### Services and Service Groups

- No Load Balancing Virtual Server Service Binding >
- No Load Balancing Virtual Server ServiceGroup Binding >

5. En **Select Service Group Name**, haga clic en **Click to Select**.

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

### ServiceGroup Binding

Select Service Group Name\*

Click to select > + ✎

**Bind** Close

6. Haga clic en **Add** para crear un nuevo grupo de servicio.

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups

### Service Groups

Select Add Edit Delete Manage Members Statistics Action Search

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**.

## Load Balancing Service Group



### Basic Settings

Help



Name\*

NewXMS

Protocol\*

SSL



Traffic Domain



Cache Type\*

SERVER



AutoScale Mode

Cacheable

State

Health Monitoring

AppFlow Logging

Monitoring Connection Close Bit

Number of Active Connections

Comment

OK

Cancel

8. Haga clic en **No Service Group Member**.

## Load Balancing Service Group

## Basic Settings

Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

## Service Group Members

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 del servidor XenMobile 10.4.
- **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 entorno de XenMobile 10.4 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 10.4 y escribe **1** para ir al menú **Clustering**. El ID del nodo de servidor en CLI tiene la etiqueta **Current Node ID**.

```

-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----
Choice: [0 - 5] 1
Current Node ID: 181356771

```

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group / Service Group Members Binding / Create Service Group

### Create Service Group Member

IP Based
  Server Based

IP Address/IP Address Range\*

10 . 207 . 87 . 38  IPv6 -

Port\*

8443

Weight

1

Server Id

181356771

Hash Id

12345

State

10. Haga clic en **Create** y, luego, en **Done**.

Load Balancing Virtual Server ServiceGroup Binding / Load Balancing Service Group

### Load Balancing Service Group

**Basic Settings** 

Name	<b>NewXMS</b>	Cache Type	<b>SERVER</b>
Protocol	<b>SSL</b>	Cacheable	<b>NO</b>
State	<b>ENABLED</b>	Health Monitoring	<b>YES</b>
Effective State	<b>UP</b>	AppFlow Logging	<b>ENABLED</b>
Traffic Domain	<b>0</b>	Monitoring Connection Close Bit	<b>NONE</b>
Comment		Number of Active Connections	<b>0</b>
		AutoScale Mode	<b>DISABLED</b>

**Service Group Members**

1 Service Group Member 

11. Haga clic en **Done** y en **OK**.

12. Haga clic en **Bind** y, a continuación, en la pantalla siguiente, haga clic en **Done**.

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

### ServiceGroup Binding

Select Service Group Name\*

NewXMS > + ✎

**Bind** Close

13. En **Certificates**, haga clic en **No Server Certificate**.

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings	
Name	MigrationLB
Protocol	SSL
State	UP
IP Address	192.168.1.10
Port	443
Traffic Domain	0
Listen Priority	-
Listen Policy Expression	NONE
Range	1
Redirection Mode	IP
RHI State	PASSIVE
AppFlow Logging	ENABLED
Redirect From Port	
HTTPS Redirect URL	

Services and Service Groups	
No Load Balancing Virtual Server Service Binding	>
1 Load Balancing Virtual Server ServiceGroup Binding	>

Certificate	
No Server Certificate	>
No CA Certificate	>

14. En **Server Certificate Binding**, haga clic en **Click to Select**.

SSL Virtual Server Server Certificate Binding / Server Certificate Binding

### Server Certificate Binding

Select Server Certificate\*

Click to select > +

Server Certificate for SNI

**Bind** Close

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**.

SSL Virtual Server Server Certificate Binding / Server Certificate Binding / Server Certificates

### Server Certificates

Select | Install | Update | Delete | Action ▾

	Name	Common Name	Issuer Name
<input type="radio"/>	ns-sftrust-certificate	...	...
<input type="radio"/>	ns-server-certificate	...	...
<input type="radio"/>	xs-full	...com	...
<input type="radio"/>	xmlab-server	...net	...

16. Haga clic en **Bind** y, a continuación, en la pantalla siguiente, haga clic en **Done**.

SSL Virtual Server Server Certificate Binding / Server Certificate Binding

### Server Certificate Binding

Select Server Certificate\*

xmlab-server > +

Server Certificate for SNI

Bind | Close

## ← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

### Basic Settings ✎

<p>Name <b>MigrationLB</b></p> <p>Protocol <b>SSL</b></p> <p>State <b>● UP</b></p> <p>IP Address <b>192.168.1.10</b></p> <p>Port <b>443</b></p> <p>Traffic Domain <b>0</b></p>	<p>Listen Priority <b>-</b></p> <p>Listen Policy Expression <b>NONE</b></p> <p>Range <b>1</b></p> <p>Redirection Mode <b>IP</b></p> <p>RHI State <b>PASSIVE</b></p> <p>AppFlow Logging <b>ENABLED</b></p> <p>Redirect From Port</p> <p>HTTPS Redirect URL</p>
--	---

---

### Services and Service Groups

- No** Load Balancing Virtual Server Service Binding >
- 1** Load Balancing Virtual Server ServiceGroup Binding >

---

### Certificate

- 1** Server Certificate >
- No** CA Certificate >

17. Haga clic en el botón de actualización para confirmar que el servidor está activo.

[Traffic Management](#) / [Load Balancing](#) / [Virtual Servers](#)

## Virtual Servers ↻ ? 📄

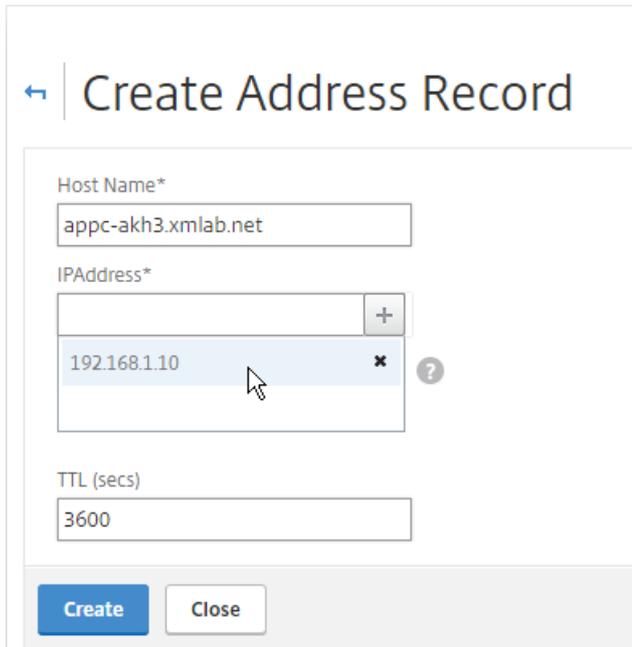
Add Edit Delete Enable Disable Statistics Action ▾ Search ▾

<input type="checkbox"/>	Name	State	Effective State	IP Address	Port	Protocol	Method
<input type="checkbox"/>	MigrationLB	● UP	● UP	192.168.1.10	443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443	SSL_BRIDGE	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443	SSL_BRIDGE	LEASTCONNECT

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.



← Create Address Record

Host Name\*  
appc-akh3.xmlab.net

IPAddress\*  
192.168.1.10

TTL (secs)  
3600

Create Close

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 para el servidor XenMobile 10.4.

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**.

The screenshot shows the NetScaler Gateway dashboard with the following components:

- Navigation Bar:** Dashboard, Configuration, Reporting, Documentation, Downloads.
- Left Sidebar:** Search bar, System menu (AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway, Authentication), Integrate with Citrix Products (Unified Gateway, XenMobile, XenApp and XenDesktop), and Show Unlicensed Features.
- NetScaler Gateway Section:**
  - Universal Licenses: Current Universal Licenses: 0. Graph showing 0 to 6,000.
  - HDX Sessions: Current HDX Sessions: 0. Graph showing 0 to 1.
  - Check connections to XenMobile, Authentication and ShareFile servers. Test Connectivity button.
  - NetScaler Gateway details: IP Address 172.16.30.37, Port 443 (UP).
- XenMobile Server Load Balancing Section:**
  - Load Balancing Throughput (port :443): Current Load Balancing Requests: 0%, Current Load Balancing Responses: 0%.
  - Load Balancing Throughput (port :8443): Current Load Balancing Requests: 0%, Current Load Balancing Responses: 0%.
  - XenMobile Server Load Balancing details: IP Address 172.16.30.38, Port 443 (UP), Port 8443 (UP).
  - Microsoft Exchange Load Balancing with Email Security Filtering: Not Configured.

2. En el lado derecho de la pantalla, en **XenMobile Server Load Balancing**, haga clic en **Edit**.

The close-up shows the configuration card for XenMobile Server Load Balancing with the following details:

- XenMobile Server Load Balancing**
- IP Address: 172.16.30.38
- Port: 443 (UP)
- Port: 8443 (UP)
- Buttons: Edit, Remove

Aparecerá la página **Load Balancing XenMobile Server Network Traffic**.

The screenshot shows the configuration page for Load Balancing XenMobile Server Network Traffic with the following sections:

- Load Balancing Virtual Server Configuration:**

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS
- XenMobile Servers:**

IP Address	Port
10.207.87.37	443, 8443
- Buttons: Done

3. Haga clic en el icono de lápiz para que XenMobile Server abra esos parámetros.

← Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration			
Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

Add Server Remove Server

<input type="checkbox"/>	IP Address	Port
<input type="checkbox"/>	10.207.87.37	443, 8443

Continue

4. Seleccione la IP del servidor de Device Manager de XenMobile 9.0 y haga clic en **Remove Server**.

← Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration			
Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

Add Server Remove Server

<input type="checkbox"/>	IP Address	Port
<input checked="" type="checkbox"/>	10.207.87.37	443, 8443

Continue

5. Haga clic en **Add Server** y agregue la nueva IP del servidor XenMobile 10.4.

**XenMobile Server IP Addresses**

Enter the IP address of the XenMobile server that you want to load balance.

XenMobile Server IP Address\*

10 . 207 . 87 . 38

Add Cancel

## Para las versiones de NetScaler 11.0 o 10.5

1. En **Integrate with Citrix Products**, haga clic en **XenMobile**.

The screenshot shows the NetScaler Configuration Dashboard. The left sidebar contains a navigation menu with categories like System, AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway, and Authentication. Under 'Integrate with Citrix Products', 'XenMobile' is highlighted. The main dashboard area shows 'NetScaler Gateway' status with two charts: 'Universal Licenses' (0) and 'HDX Sessions' (0). On the right, there are two configuration cards for 'NetScaler Gateway' and 'Device Manager Load Balancing', both showing IP address 10.217.232.37 and ports 443 and 8443, all with 'Up' status. A 'Test Connectivity' button is visible in the top right.

2. En el lado derecho de la pantalla, en **Device Manager Load Balancing**, haga clic en **Edit**.

This is a close-up of the 'Device Manager Load Balancing' configuration card. It displays the following information: IP Address: 10.217.232.39; Port 443: Up; Port 8443: Up. There are 'Edit' and 'Remove' links at the bottom right of the card.

Aparecerá la página **Load Balancing Device Manager Network Traffic**.

## Load Balancing Device Manager Network Traffic

Load Balancing Virtual Server Configuration		
Name	IP Address	Port
MDM_XenMobileMDM	10.217.232.39	443,8443

Device Manager Server IP Addresses		
IP Address	Port	State
10.207.72.216	443, 8443	Up

Done

3. Haga clic en el icono de lápiz de **Device Manager Server IP Addresses** para abrir esos parámetros.

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	Up

4. Seleccione la IP del servidor de Device Manager de XenMobile 9.0 y haga clic en **Remove Server**.

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	Up

5. Haga clic en **Add Server** y agregue la nueva IP del servidor XenMobile 10.4.

Device Manager Server IP Addresses	
Enter the IP address(es) of the device manager server(s) that you want to load balance. If the server IP address is already added to the NetScaler, click <b>Add from existing servers</b> to select the device manager server IP.	
Device Manager Server IP Address*	
<input type="text" value="10 . 207 . 87 . 38"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

En este punto, NetScaler Gateway apunta al FQDN de App Controller. Debe cambiar NetScaler para que apunte al FQDN del nuevo servidor XenMobile 10.4. XenMobile 10.4 escucha 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 10.4, que es el FQDN de Device Manager de XenMobile 9.0 seguido del puerto 8443. En la siguiente tabla, se muestra un ejemplo.

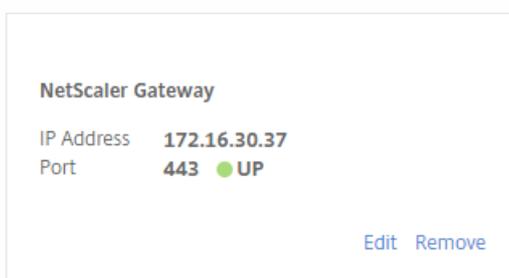
XenMobile 9.0 Componente	Componente de FQDN	FQDN de XenMobile 10.4 Enterprise Edition
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	N/D
NetScaler Gateway	access.example.com	N/D

### XenMobile App Edition

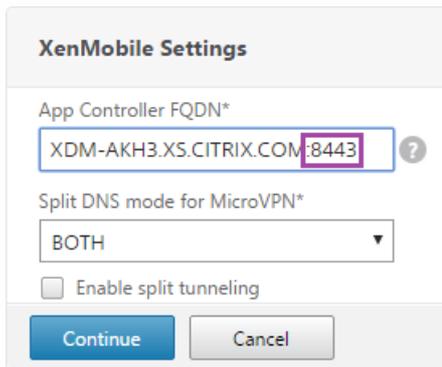
Cambie el FQDN de App Controller para que apunte al nuevo FQDN de XenMobile 10.4, que es el FQDN de App Controller de XenMobile 9.0 seguido del puerto 8443. En la siguiente tabla, se muestra un ejemplo.

XenMobile 9.0 Componente	Componente de FQDN	FQDN de XenMobile 10.4 Enterprise Edition
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**.



**XenMobile Settings**

App Controller FQDN\*

XDM-AKH3.XS.CITRIX.COM:8443

Split DNS mode for MicroVPN\*

BOTH

Enable split tunneling

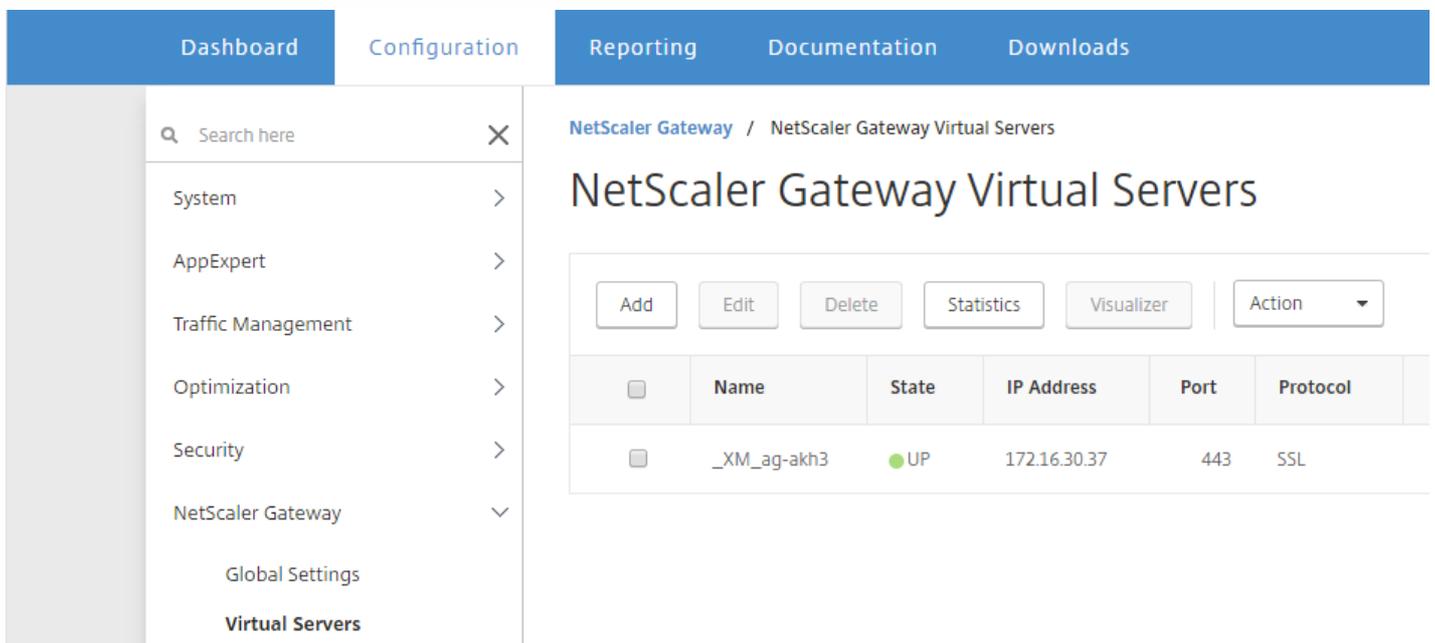
Continue Cancel

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 XenMobile Server 10.4. 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**.



Dashboard Configuration Reporting Documentation Downloads

Search here

System

AppExpert

Traffic Management

Optimization

Security

NetScaler Gateway

Global Settings

**Virtual Servers**

NetScaler Gateway / NetScaler Gateway Virtual Servers

## NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

	Name	State	IP Address	Port	Protocol
<input type="checkbox"/>	_XM_ag-akh3	UP	172.16.30.37	443	SSL

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**.

Published Applications
No Next HOP Server
1 STA Server
No Url

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.

	Secure Ticket Authority Server	Secure Ticket Authority Server Address Type
<input checked="" type="checkbox"/>	Secure Ticket Authority Server	
<input checked="" type="checkbox"/>	https://XDM-AKH3.XS.CITRIX.COM:8443	IPV4

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 consola de XenMobile 10.4, 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.

Settings > Server Properties > [Add New Server Property](#)

## Add New Server Property

Key	<input type="text" value="Custom Key"/>	<span>?</span>
Key*	<input type="text" value="host.name.uselowercase"/>	
Value*	<input type="text" value="true"/>	
Display name*	<input type="text" value="Use lowercase for host name"/>	
Description	<input type="text"/>	

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 XenMobile Server 10.4:

- 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 XenMobile 10.4. Los dispositivos deben poder conectar automáticamente con el servidor XenMobile 10.4 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 10.4

Mar 02, 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 XenMobile 10.4. XenMobile 10 no respalda la consola MTC, de modo que debe administrar estas instancias individualmente.

1. Asegúrese de que configura la traducción de direcciones de red (NAT) en frente de todos los clientes MTC.
2. Instale una instancia de XenMobile 10.4.
3. Si no hay ninguna asignación de puertos habilitada en el arrendatario MTC, haga lo siguiente MTC:
  - a. Asegúrese de que el puerto del servidor XenMobile 10.4 que permite la comunicación HTTPS con certificados (normalmente el puerto 443) y el puerto que permite la comunicación HTTPS sin certificados (8443) coinciden con los puertos usados por 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 el que escucha el servidor XenMobile.
4. En 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 según se describe en los pasos siguientes.
9. Quite todos los conectores de puertos que se estén usando en 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 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 servidor XenMobile 10.4 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 XenMobile, inicie sesión en la consola de XenMobile con la dirección IP del servidor XenMobile seguida del número de puerto de administración.

16. Cambie la traducción de direcciones de red para que apunte a un 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 02, 2017

En XenMobile, puede configurar cuentas de usuario y grupos, roles para cuentas de usuario y grupos, así como el modo de inscripción y las invitaciones desde la ficha **Manage** de la página **Settings** en la consola de XenMobile.

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 un máximo de siete modos, cada uno con su propio nivel de seguridad y cantidad de pasos que deberán seguir los usuarios para inscribir sus dispositivos y para enviar invitaciones de inscripción. Para obtener más detalles, consulte:
  - [Para configurar modos de inscripción y habilitar el portal Self Help Portal](#)
  - [Activación de la detección automática en XenMobile para la inscripción de usuarios](#)

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**.

XenMobile					
Analyze	Manage	Configure			
Devices	Users	Enrollment			
<b>Users</b> <a href="#">Show filter</a>					
<a href="#">Add Local User</a>   <a href="#">Import Local Users</a>   <a href="#">Manage Local Groups</a>   <a href="#">Export</a>					
<input type="checkbox"/>	User name	First name	Last name	Roles	Groups
<input type="checkbox"/>	us1user1@net	us1	user1	USER	net\Domain Users
<input type="checkbox"/>	us3user3@net	us3	user3	USER	net\Domain 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**.

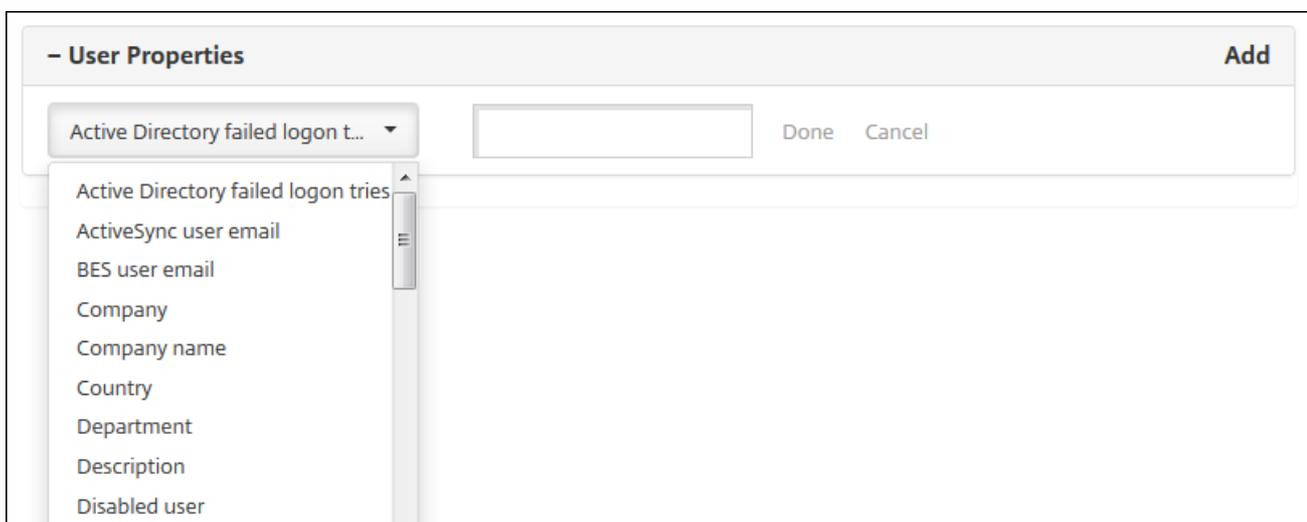
XenMobile		Analyze	Manage	Configure	admin
Devices	Users	Enrollment			
<h3>Add Local User</h3>					
<b>User name*</b>	<input type="text" value="Enter user name"/>				
<b>Password</b>	<input type="password" value="Enter new password"/>				
<b>Role*</b>	<input type="text" value="ADMIN"/>				
<b>Membership</b>	<input type="checkbox"/> local\MSP <a href="#">Manage Groups</a>				
<input type="button" value="- User Properties"/>					<input type="button" value="Add"/>
					<input type="button" value="Cancel"/> <input type="button" value="Save"/>

2. Configure los siguientes parámetros:

- **User name.** Escriba el nombre del usuario. Este campo es obligatorio. Puede incluir espacios en los nombres, además de letras mayúsculas y minúsculas.
- **Password.** Escriba una contraseña opcional de usuario.
- **Role.** En la lista, haga clic en el rol del usuario. Para obtener información más detallada acerca de los roles, consulte [Configuración de roles con RBAC](#). Las opciones posibles son:
  - ADMIN
  - DEVICE\_PROVISIONING
  - SUPPORT
  - USER
- **Membership.** En la lista, haga clic en el grupo o en los grupos a los que agregar el usuario.
- **User Properties.** Agregue propiedades de usuario opcionales. Para cada propiedad de usuario que quiera agregar, haga clic en **Add** y haga lo siguiente:
  - **User Properties.** En la lista, haga clic en una propiedad y, a continuación, escriba el atributo de la propiedad de usuario en el campo que hay junto a la propiedad.
  - Haga clic en **Done** para guardar la propiedad de usuario o haga clic en **Cancel** para no guardarla.

**Nota:** Para eliminar una propiedad de usuario existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la X situada a la derecha. La propiedad se elimina inmediatamente.

Para modificar una propiedad de usuario, haga clic en la propiedad y realice los cambios. Haga clic en **Done** para guardar los cambios de la lista o haga clic en **Cancel** para no realizar cambios en la lista.



3. Haga clic en **Save**.

#### 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 no guardarla.
  - Para eliminar cada propiedad de usuario, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la X situada a la derecha. La propiedad se elimina inmediatamente.

3. Haga clic en **Save** para guardar los cambios o en **Cancel** para no guardarlos.

### 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 propiedad. Para ello, deberá marcar la casilla de verificación situada junto a cada propiedad.

2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.

3. Haga clic en **Delete** para eliminar la cuenta de usuario o en **Cancel** para no eliminarla.

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:

- Si importa los usuarios desde un directorio LDAP, utilice el nombre de dominio, junto con el nombre de usuario en el archivo de importación. Por ejemplo, nombredeusuario@dominio.com. Esta sintaxis evitará búsquedas adicionales que pueden reducir la velocidad de importación.
- Si importa 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 tener el formato del nombre principal de usuario (UPN), aunque Citrix recomienda no usar el dominio administrado. Así, por ejemplo, si ejemplo.com está administrado, no cree un usuario local con este formato UPN: "usuario@ejemplo.com".

Después de preparar un archivo de aprovisionamiento, siga estos pasos para importar el archivo en XenMobile.

1. En la consola de XenMobile, haga clic en **Manage > Users**. Aparecerá la página Users.

2. Haga clic en **Import Local Users**. Aparece el cuadro de diálogo **Import Provisioning File**.

Import Provisioning File

Format  User ?  User property ?

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 atributos de usuarios:** usuario;contraseña;rol;grupo1;grupo2
- **Campos del archivo de aprovisionamiento de atributos de usuario:**  
usuario;nombrePropiedad1;valorPropiedad1;nombrePropiedad2;valorPropiedad2

**Nota:**

- Los campos del archivo de aprovisionamiento están separados por un punto y coma (;). Si parte de un campo contiene un punto y coma, debe contener también un carácter de barra diagonal inversa (\). Por ejemplo, la propiedad propertyV;test;1;2 debe escribirse como propertyV\;test\;1\;2 en el archivo de aprovisionamiento.
- Los valores válidos de **Role** son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE\_PROVISIONING, además de cualquier rol adicional que haya definido.
- El punto (.) se usa como separador para crear una jerarquía de grupo; por lo tanto, no puede usar un punto en nombres de grupo.
- En los archivos de aprovisionamiento de atributos, los atributos de las propiedades deben estar en minúsculas. La base de datos distingue entre mayúsculas y minúsculas.

**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.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 poner algunos modos a disposición de los usuarios en el portal Self Help Portal. Los usuarios pueden iniciar sesión en ese portal y generar enlaces de inscripción que les permitan inscribir sus propios dispositivos o enviarse la invitación a una inscripción. Los modos de inscripción se configuran en la consola de XenMobile, desde la página **Settings > Enrollment**.

Es necesario enviar invitaciones de envío desde la página **Manage > Enrollment** . Para obtener información, consulte [Enviar 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 y, a continuación, establezca ese modo como predeterminado, inhabílitelo, o bien permita a los usuarios acceder a él a través del portal Self Help Portal.

**Nota:** Si marca la casilla situada junto a un modo de inscripción, el menú de opciones aparecerá encima de la lista del modo de inscripción. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá a la derecha de la lista.

Settings &gt; Enrollment

## Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Worx Home and enroll their devices, or to send themselves an enrollment invitation.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▾
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

### 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.

XenMobile Analyze Manage Configure admin

Settings > Enrollment > Edit Enrollment Mode

## Edit Enrollment Mode

Name	High Security	
Expire after*	<input type="text" value="1"/>	Days <span>?</span>
Maximum attempts*	<input type="text" value="3"/>	<span>?</span>
PIN Length*	<input type="text" value="8"/>	Numeric

**Notification templates**

Template for enrollment URL	-- SELECT ONE --
Template for Enrollment PIN	-- SELECT ONE --
Template for enrollment confirmation	-- SELECT ONE --

Cancel Save

2. Cambie la siguiente información como corresponda:

- **Expire after.** Introduzca una fecha límite de caducidad, después de la cual, los usuarios no podrán inscribir sus dispositivos. Este valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.  
**Nota:** Escriba 0 para evitar que la invitación caduque.
- **Days.** En la lista, haga clic en **Days** o **Hours**, de acuerdo con la fecha límite de caducidad que ha introducido en **Expire after**.
- **Maximum Attempts.** Escriba la cantidad de intentos de inscripción que un usuario puede llevar a cabo antes de que se bloquee el proceso de inscripción. Este valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.  
**Nota:** Escriba 0 para permitir una cantidad ilimitada de intentos.
- **PIN length.** Escriba un número para indicar la cantidad de dígitos o caracteres que contendrá el PIN generado.
- **Numeric:** En la lista, haga clic en **Numeric** o **Alphanumeric** para el tipo de PIN.
- **Plantillas de notificaciones:**
  - **Template for Enrollment URL.** En la lista, seleccione una plantilla para el URL de inscripción. Por ejemplo, mediante la plantilla de invitaciones a inscripciones, se envía a los usuarios una invitación por correo electrónico o por SMS, según como haya configurado la plantilla que les permite inscribir sus dispositivos en XenMobile. Para obtener más información acerca de plantillas de notificaciones, consulte [Creación o actualización de plantillas de notificaciones](#).
  - **Template for Enrollment PIN.** En la lista, seleccione una plantilla para el PIN de inscripción.

- **Template for enrollment confirmation.** En la lista, seleccione la plantilla a utilizar para informar al usuario de que la inscripción se ha realizado correctamente.

3. Haga clic en **Save**.

### Para establecer un modo de inscripción como predeterminado

Al establecer un modo de inscripción como predeterminado, ese modo se usará para todas las solicitudes de inscripción de dispositivos a menos que se seleccione otro modo de inscripción. Si no hay ningún modo de inscripción establecido como predeterminado, debe crear una solicitud de inscripción para cada inscripción de dispositivo.

**Note:** Solo puede definir **Only Username + Password**, **Two Factor** o **Username + PIN** como modo de inscripción predeterminado.

1. Seleccione uno de los modos **Username + Password**, **Two Factor** o **Username + PIN** para definirlo como modo de inscripción predeterminado.

Nota: El modo seleccionado debe estar habilitado para poder establecerlo como predeterminado.

2. Haga clic en **Default**. A partir de ahora, el modo seleccionado es el predeterminado. Si se había establecido otro modo de inscripción como predeterminado, ese modo deja de serlo.

### Para inhabilitar un modo de inscripción

Al inhabilitar un modo de inscripción, ese modo no se podrá usar ni para las invitaciones de grupo a las inscripciones ni en el portal Self Help Portal. Puede cambiar la manera de permitir a los usuarios que inscriban sus dispositivos. Para ello, deberá inhabilitar un modo de inscripción y habilitar otro.

1. Seleccione un modo de inscripción.

**Nota:** No se puede inhabilitar el modo de inscripción predeterminado. Si quiere inhabilitar el modo de inscripción predeterminado, primero debe quitar su estado predeterminado.

2. Haga clic en **Disable**. El modo de inscripción deja de estar habilitado.

### Para habilitar un modo de inscripción en el portal Self Help Portal

Habilitar un modo de inscripción en el portal Self Help Portal permite a los usuarios inscribir sus dispositivos en XenMobile uno a uno.

#### **Nota:**

- Para que un modo de inscripción esté disponible en el portal Self Help Portal, debe estar habilitado y enlazado a plantillas de notificaciones.
- Solo puede habilitar un modo de inscripción en el portal Self Help Portal en un momento dado.

1. Seleccione un modo de inscripción.

2. Haga clic en **Self Help Portal**. El modo de inscripción seleccionado ya está disponible para los usuarios en el portal Self Help Portal. Cualquier otro modo que ya estuviera habilitado en el portal Self Help Portal deja de estar disponible para los usuarios.

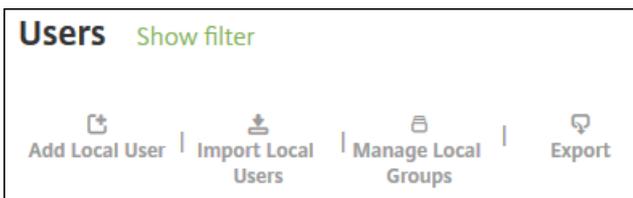
Puede administrar grupos en el cuadro de diálogo **Manage Groups** de la consola de XenMobile, que puede encontrar en la página **Users**, la página **Add Local User** o la página **Edit Local User**. No hay ningún comando de modificación de grupos.

Si quita un grupo, tenga en cuenta que quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios a ese grupo. Asimismo, los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados a ese grupo. Sin embargo, las demás asociaciones de grupos permanecen intactas. Si los usuarios no están asociados a ningún otro grupo local, se asocian al nivel superior.

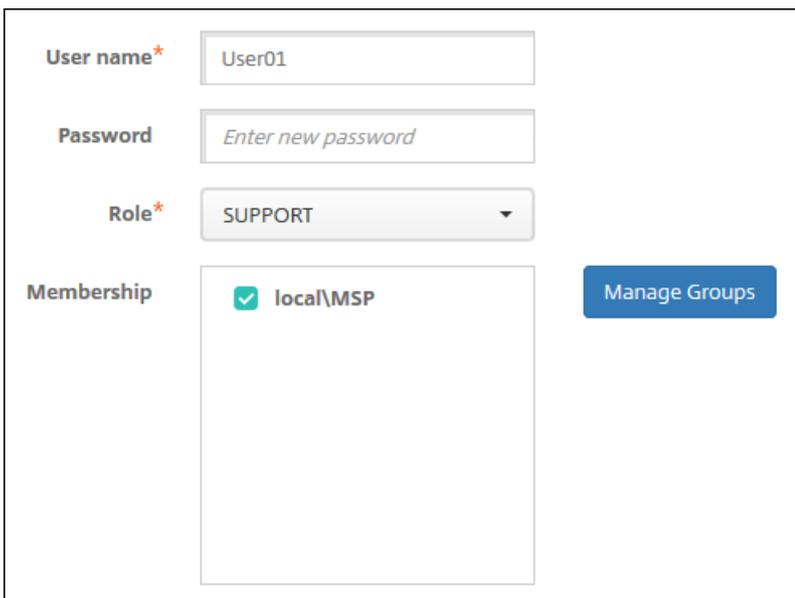
### Para agregar un grupo local

1. Lleve a cabo una de las siguientes acciones:

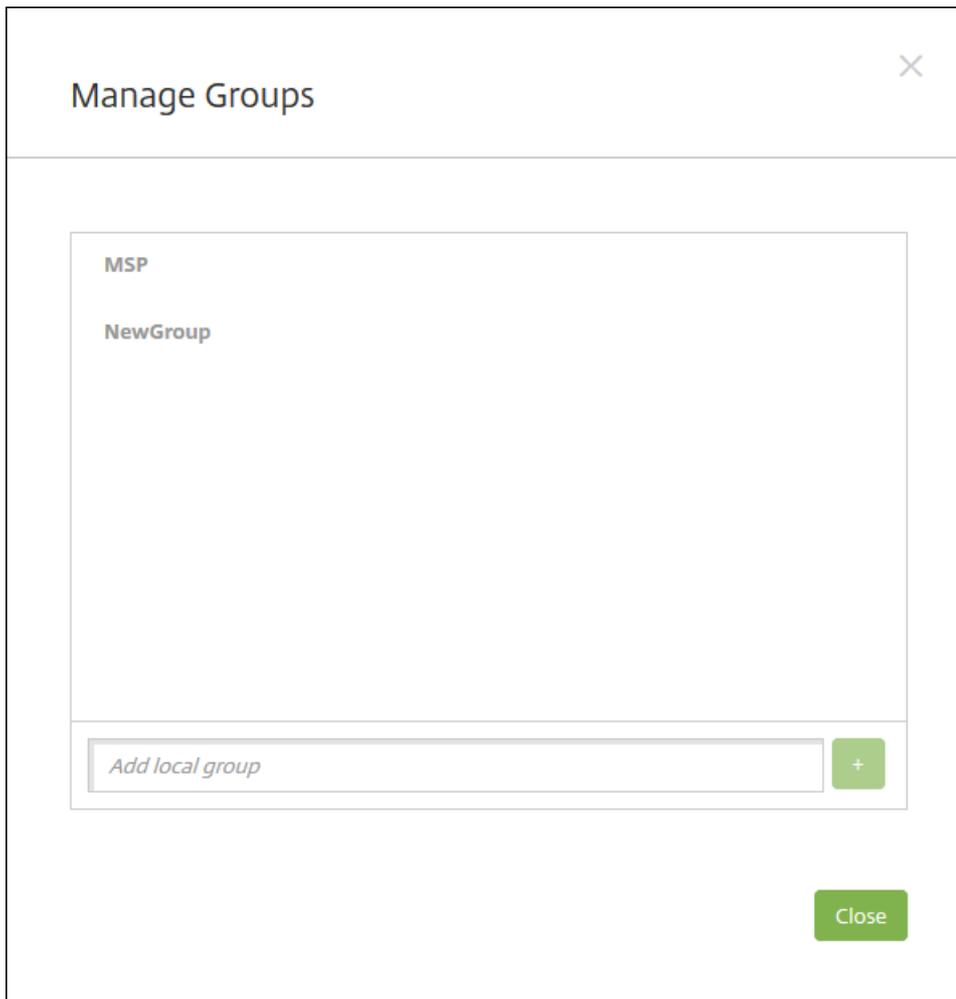
- En la página **Users**, haga clic en **Manage Local Groups**.



- Ya sea en la página **Add Local User** o **Edit Local User**, haga clic en **Manage Groups**.

A screenshot of a user creation or editing form. It contains the following fields: 'User name\*' with the value 'User01'; 'Password' with the placeholder text 'Enter new password'; 'Role\*' with a dropdown menu showing 'SUPPORT'; and 'Membership' with a list containing 'local\MSP' and a checked checkbox. To the right of the membership list is a blue button labeled 'Manage Groups'.

Aparecerá el cuadro de diálogo **Manage groups**.



2. Bajo la lista de grupos, escriba un nuevo nombre de grupo y, a continuación, haga clic en el signo más (+). El grupo de usuarios se agrega a la lista.

3. Haga clic en **Close**.

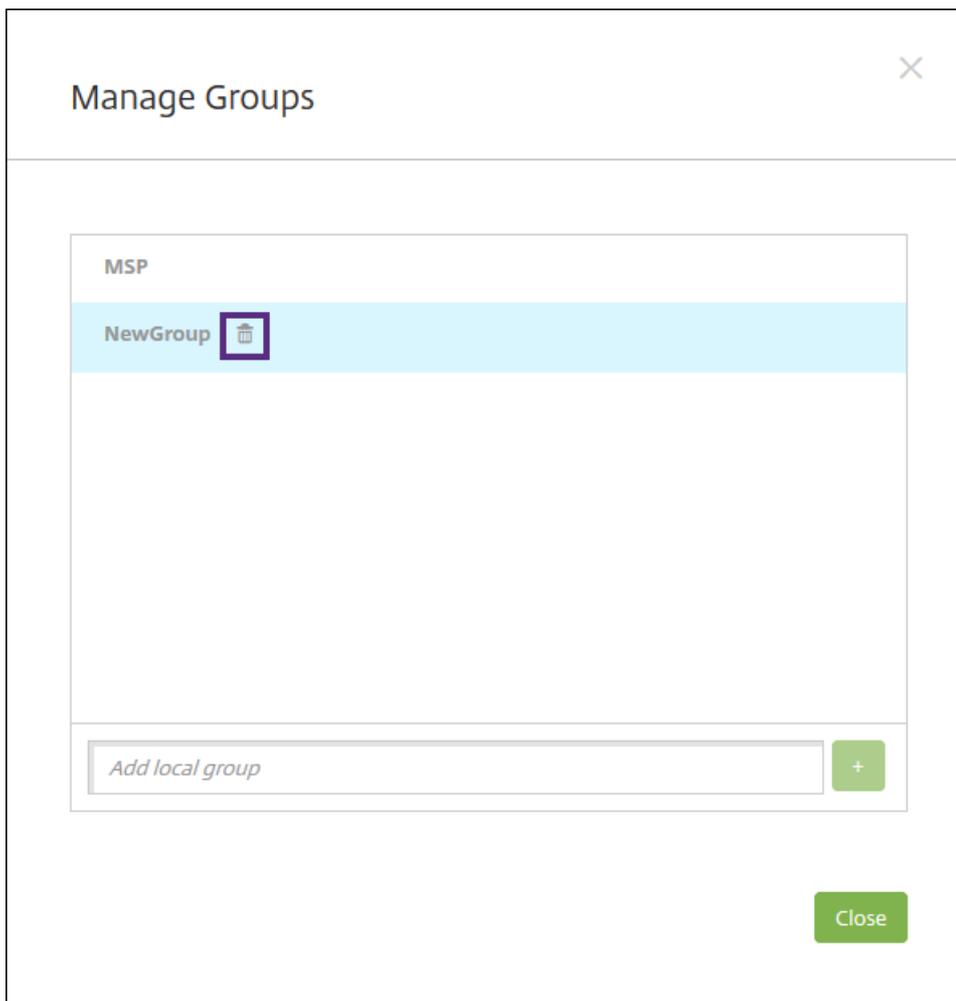
### Para quitar un grupo

**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 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. 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 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 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. En la consola de XenMobile, puede crear plantillas de correo electrónico en 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:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
    - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:
      - Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
      - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
      - Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

5. Haga clic en **Save**. El flujo de trabajo creado aparecerá 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 situada junto 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.

# Configuración de roles con RBAC

Mar 02, 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.

<a href="#">Rol de administrador</a>	▼
<a href="#">Rol de aprovisionamiento de dispositivos</a>	▼
<a href="#">Rol de asistencia</a>	▼
<a href="#">Rol de usuario</a>	▼

## 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:

- **Administrator.** Concede acceso completo al sistema.
- **Device Provisioning.** Concede acceso a tareas básicas de administración de dispositivos para dispositivos Windows CE.
- **Support.** Concede acceso para la asistencia remota.
- **User.** Rol utilizado por los usuarios que pueden inscribir dispositivos y acceder al portal Self Help Portal.

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

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

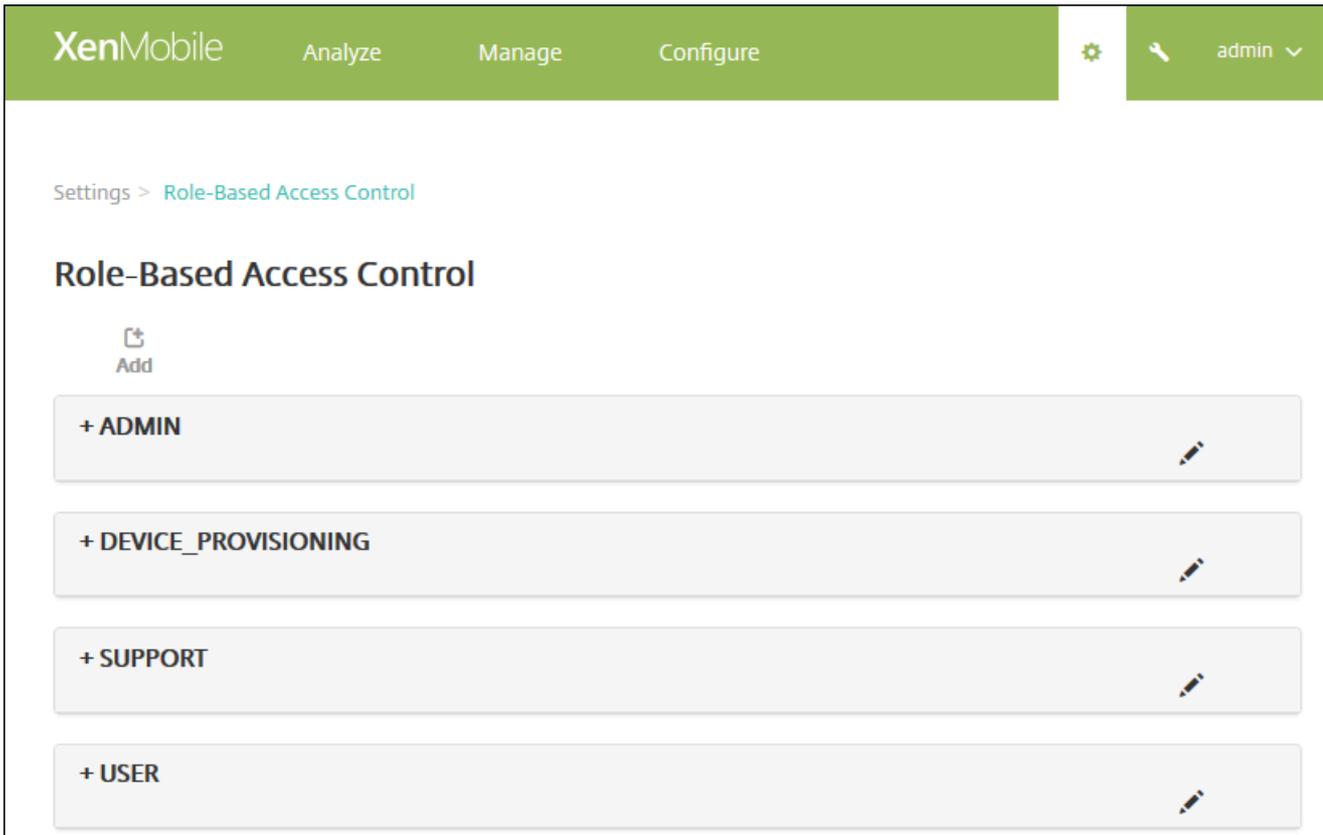
**Nota:** Los usuarios locales solo pueden tener un rol asignado.

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

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

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

2. Haga clic en **Role-Based Access Control**. Aparecerá la página **Role-Based Access Control** con los cuatro roles de usuario predeterminados, además de los roles que haya agregado antes.



Si hace clic en el signo más (+) situado junto a un rol, ese rol se expande para mostrar todos los permisos que se le han concedido, tal y como se muestra en la siguiente ilustración.



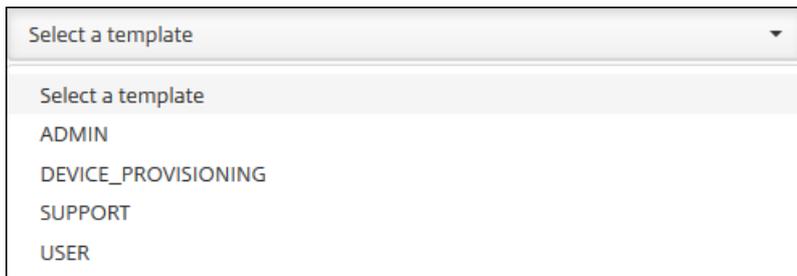
3. Haga clic en **Add** para agregar un nuevo rol de usuario. También puede hacer clic en el icono de lápiz situado a la derecha de un rol existente para modificarlo, y puede hacer clic en el icono de papelera situado a la derecha de un rol previamente definido para eliminarlo. No se pueden eliminar los roles de usuario predeterminados.

- Si hace clic en **Add** o en el icono de lápiz, aparecerán la página **Add Role** o la página **Edit Role**.
- Si hace clic en el icono de papelera, aparecerá un diálogo de confirmación. Haga clic en **Delete** para quitar el rol seleccionado.

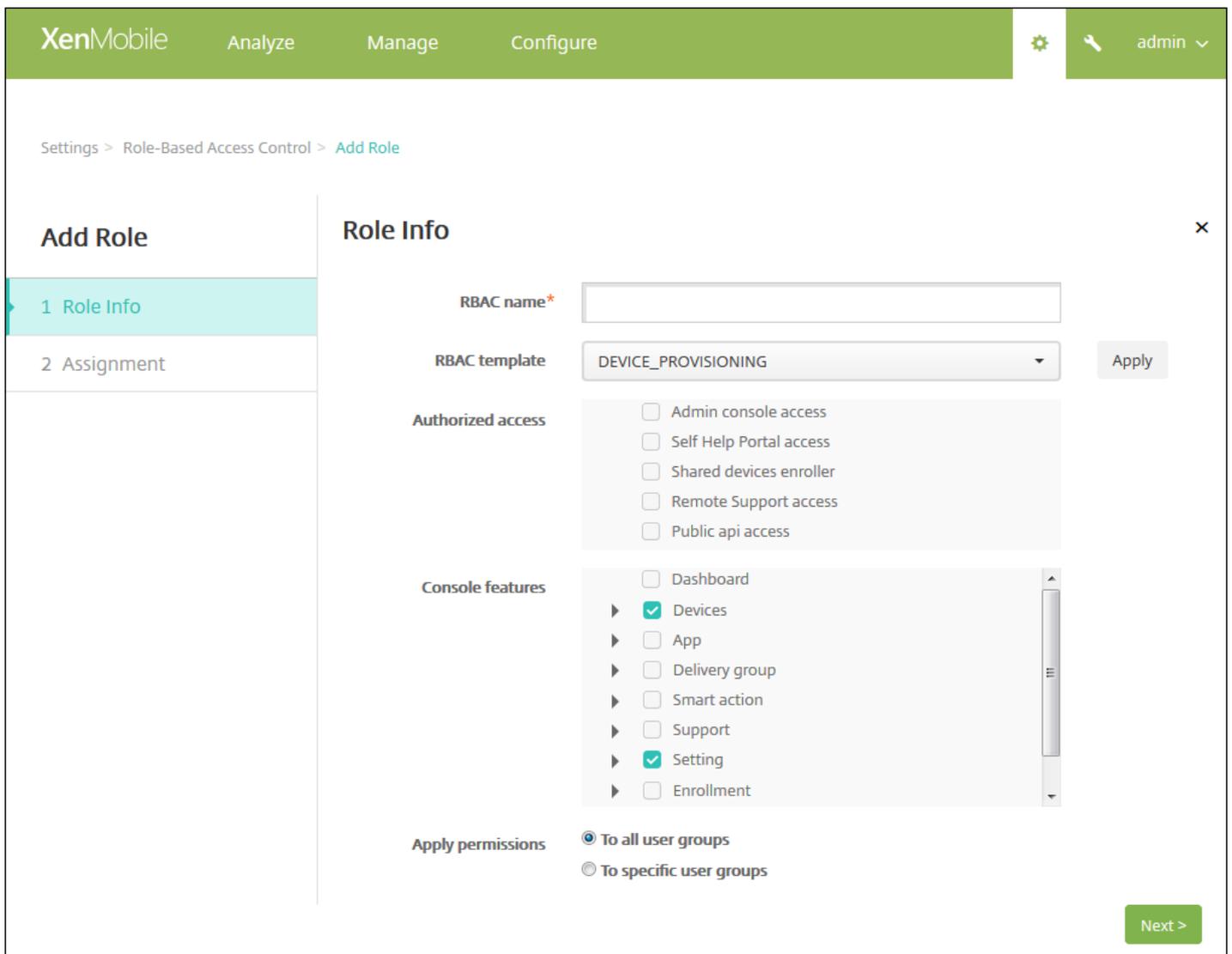
4. Escriba la siguiente información para crear un nuevo rol de usuario o para modificar un rol de usuario existente:

- **RBAC name.** Indique un nombre descriptivo para el nuevo rol de usuario. No se puede cambiar el nombre de un rol existente.
- **RBAC template.** Puede hacer clic en una plantilla como punto de partida para el nuevo rol. No puede seleccionar una plantilla si está modificando un rol existente.

Las plantillas RBAC son los roles de usuario predeterminados. Determinan el acceso a las funciones del sistema que tienen los usuarios asociados a ese rol. Tras seleccionar una plantilla RBAC, puede ver todos los permisos asociados a ese rol en los campos **Authorized Access** y **Console Features**. Usar plantillas es opcional; puede seleccionar directamente las opciones que quiera asignar a un rol en los campos **Authorized Access** y **Console Features**.

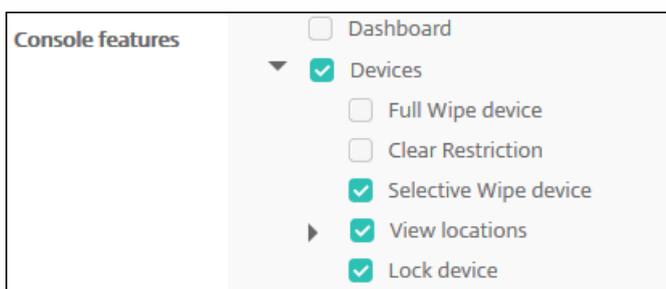


5. Haga clic en **Apply**, situado a la derecha del campo **RBAC template**, para rellenar las casillas **Authorized access** y **Console features** con los permisos concedidos de funciones y acceso predefinidos para la plantilla seleccionada.



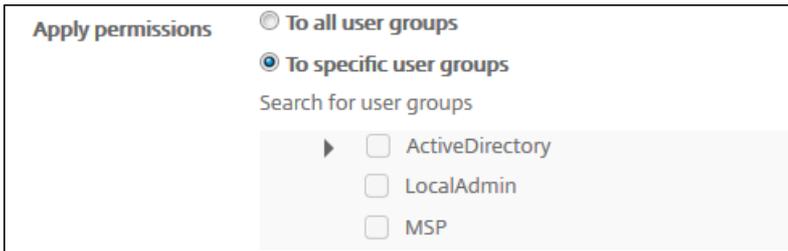
6. Marque y desmarque las casillas de verificación **Authorized access** y **Console features** para personalizar el rol.

Si hace clic en el triángulo situado junto a Console feature, aparecerán los permisos específicos de esa función y puede marcarlos o desmarcarlos. Si marca la casilla del nivel superior de la lista, impedirá el acceso a esa parte de la consola. Debe marcar de forma individual las opciones situadas por debajo de la casilla del nivel superior para habilitar el acceso a esas opciones. Por ejemplo, en la 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.



Apply permissions

To all user groups

To specific user groups

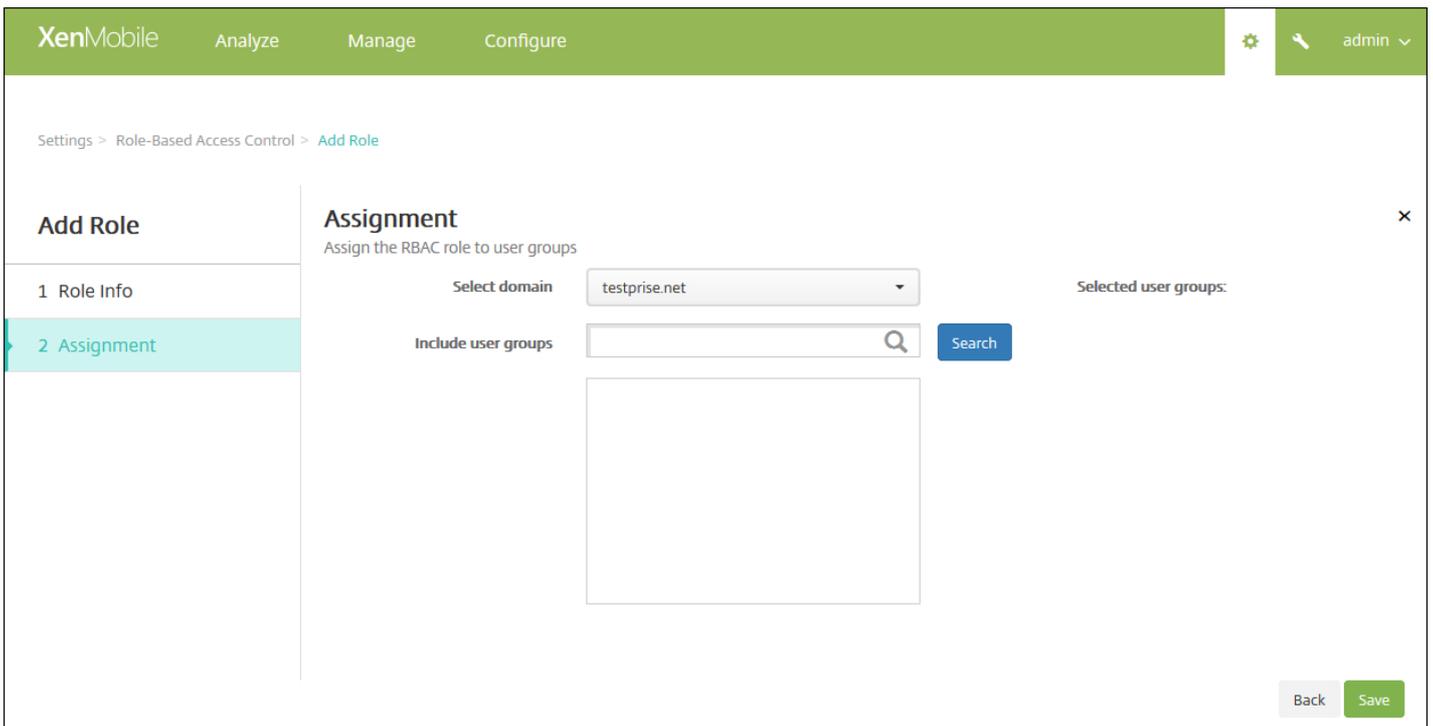
Search for user groups

ActiveDirectory

LocalAdmin

MSP

8. Haga clic en **Siguiente**. Aparecerá la página **Assignment**.



XenMobile Analyze Manage Configure

Settings > Role-Based Access Control > Add Role

Add Role

1 Role Info

2 Assignment

Assignment

Assign the RBAC role to user groups

Select domain testprise.net

Include user groups

Search

Selected user groups:

Back Save

9. Escriba la siguiente información para asignar el rol a los grupos de usuarios.

- **Select domain.** En la lista, haga clic en un dominio.
- **Include user groups.** Haga clic en Search para ver una lista de todos los grupos disponibles o escriba un nombre de grupo completo o parcial para limitar la lista a solo aquellos grupos que tengan ese nombre.
- En la lista que aparezca, seleccione los grupos de usuarios a los que asignar el rol. Cuando se selecciona un grupo de usuarios, el grupo aparece en la lista **Selected user groups**.

XenMobile Analyze Manage Configure admin

Settings > Role-Based Access Control > Add Role

### Add Role

- 1 Role Info
- 2 Assignment

### Assignment

Assign the RBAC role to user groups

Select domain: testprise.net

Include user groups: user Search

- testprise.net\Remote Desktop Users
- testprise.net\Performance Monitor Users
- testprise.net\Performance Log Users

Selected user groups:

- testprise.net
  - Remote Desktop Users
  - Performance Monitor Users

Back Save

**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

Mar 02, 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.
- Notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se den ciertas condiciones. Por ejemplo, cuando el acceso de un dispositivo de usuario al dominio de la empresa está a punto de bloquearse debido a problemas de incumplimiento, o cuando un dispositivo se ha liberado por jailbreak o por rooting. Para obtener información detallada acerca de las acciones automatizadas, consulte [Acciones automatizadas](#).

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

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

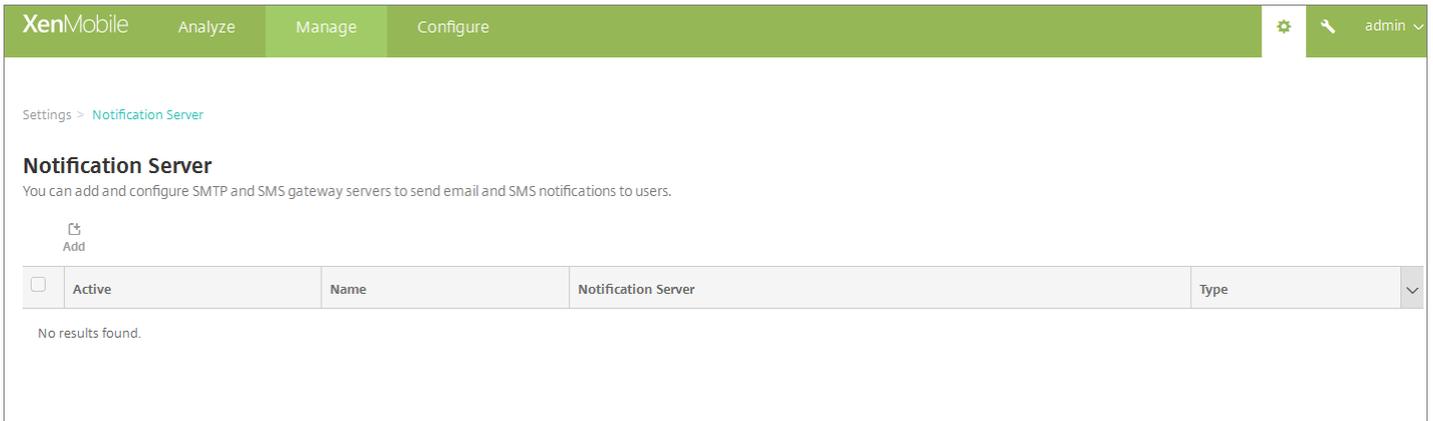
En los procedimientos de este artículo se describe la forma de configurar un [servidor SMTP](#), una [puerta de enlace SMS](#) y una [puerta de enlace SMS de operador](#).

- 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 cuyo caso se necesita información procedente del sitio Web del proveedor del servicio.
- Debe configurar el servidor de notificaciones SMTP para enviar mensajes a los usuarios. Si el servidor está alojado en un servidor interno, póngase en contacto con el administrador del sistema para obtener información acerca de la configuración. Si el servidor es un servidor de servicio de correo electrónico, busque la información de configuración en el sitio Web del proveedor del servicio.

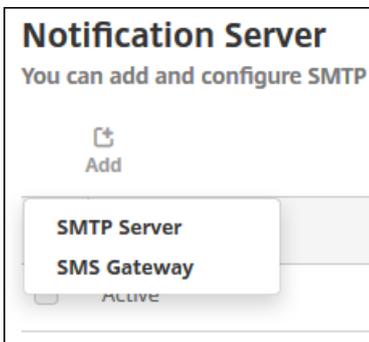
- Solo hay activo un solo servidor SMTP y un solo servidor SMS a la vez.
- Debe abrir el puerto 25 desde XenMobile (ubicado en la zona DMZ de la red) para apuntarlo al servidor SMTP de la red interna para que las notificaciones se envíen correctamente.

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

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



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



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

Settings > Notification Server > Add SMTP Server

## Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
SMTP Server*	<input type="text"/>
Secure channel protocol	<input type="text" value="None"/>
SMTP server port*	<input type="text" value="25"/>
Authentication	<input type="checkbox" value="OFF"/>
Microsoft Secure Password Authentication (SPA)	<input type="checkbox" value="OFF"/>
From name*	<input type="text"/>
From email*	<input type="text"/>

Test Configuration

▶ Advanced Settings

Cancel

Add

1. Configure los siguientes parámetros:

- **Name.** Escriba el nombre asociado a esta cuenta del servidor SMTP.
- **Description.** Si quiere, introduzca una descripción del servidor.
- **SMTP Server.** Escriba el nombre de host del servidor. El nombre de host puede ser una dirección IP o un nombre de dominio completo (FQDN).
- **Secure channel protocol.** En la lista, haga clic en **SSL**, **TLS** o **None** para definir el protocolo de canal seguro que utiliza el servidor (si el servidor está configurado para usar la autenticación segura). El valor predeterminado es **None**.
- **SMTP server port.** Escriba el puerto que usa el servidor SMTP. De forma predeterminada, el puerto definido es el 25. En

cambio, si las conexiones SMTP usan el protocolo SSL de canal seguro, el puerto definido es 465.

- **Authentication.** Seleccione **ON** u **OFF**. El valor predeterminado es **OFF**.
  - Si habilita **Authentication**, configure los siguientes parámetros:
    - **User name.** Escriba el nombre de usuario que se usará para la autenticación.
    - **Password.** Escriba la contraseña de autenticación del usuario.
  - **Microsoft Secure Password Authentication (SPA).** Si el servidor SMTP usa la autenticación SPA, haga clic en **ON**. El valor predeterminado es **OFF**.
  - **From Name.** Escriba el nombre que aparece en el cuadro **From** cuando un cliente recibe un correo electrónico de notificación procedente de este servidor. Por ejemplo, "Departamento de TI de la empresa".
  - **From email.** Escriba la dirección de correo electrónico utilizada si un destinatario de correo electrónico responde a la notificación enviada por el servidor SMTP.
2. Haga clic en **Test Configuration** para enviar una notificación de prueba por correo electrónico.
3. Expanda **Advanced Settings** y, a continuación, configure estos parámetros:
- **Number of SMTP retries.** Escriba el número de reintentos de envío de un mensaje fallido enviado desde el servidor SMTP. El valor predeterminado es 5.
  - **SMTP Timeout.** Escriba la duración del tiempo de espera (en segundos) al enviar una solicitud SMTP. Aumente este valor si el envío de mensajes falla continuamente debido a los tiempos de espera. Tenga cuidado al reducir este número, porque podría aumentar la cantidad de mensajes sin entregar y de mensajes cuyo tiempo de espera se ha agotado. El valor predeterminado es de 30 segundos.
  - **Maximum number of SMTP recipients.** Escriba la cantidad máxima de destinatarios por mensaje de correo electrónico enviado por el servidor SMTP. El valor predeterminado es 100.
4. Haga clic en **Add**.

Settings > Notification Server > Add SMS Gateway

## Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
Key*	<input type="text"/>
Secret*	<input type="text"/>
Virtual phone number*	<input type="text"/>
HTTPS	<input type="checkbox"/> OFF
Country code	<input type="text" value="Afghanistan +93"/>
Use Carrier Gateway	<input checked="" type="checkbox"/> ON
	<input type="button" value="Test Configuration"/>

### 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 con el valor **ON**, a menos que reciba instrucciones de Citrix Support 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**.

Settings &gt; Carrier SMS Gateway

## Carrier SMS Gateway



Add



Detect

<input type="checkbox"/>	Carrier	SMTP domain	Country code	Sending prefix	▾
<input type="checkbox"/>	Alltel	message.alltel.com	+1		
<input type="checkbox"/>	AT&T	txt.att.net	+1		
<input type="checkbox"/>	Boost Mobile	myboostmobile.com	+1		
<input type="checkbox"/>	Bouygues Telecom	mms.bouyguestelecom.fr	+33		
<input type="checkbox"/>	Cingular	cingularme.com	+1		
<input type="checkbox"/>	Metro PCS	mymetropcs.com	+1		
<input type="checkbox"/>	Nextel	messaging.nextel.com	+1		
<input type="checkbox"/>	Orange	websmsmms.orange.fr	+33		
<input type="checkbox"/>	Powertel	ptel.net	+1		
<input type="checkbox"/>	SFR	sfr.fr	+33		

Showing 1 - 10 of 16 items

Showing 1 of 2



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 **Agregar**. Aparecerá el cuadro de diálogo **Add a Carrier SMS Gateway**.

### Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

**Carrier\***

**Gateway SMTP domain\***

**Country code\***

**Email sending prefix**

**Nota:** XenMobile solo admite el envío de mensajes SMS de Nexmo. Si aún no tiene una cuenta para usar la mensajería de Nexmo, visite su [sitio Web](#) para crear una.

4. Configure los siguientes parámetros:

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

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

## 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.

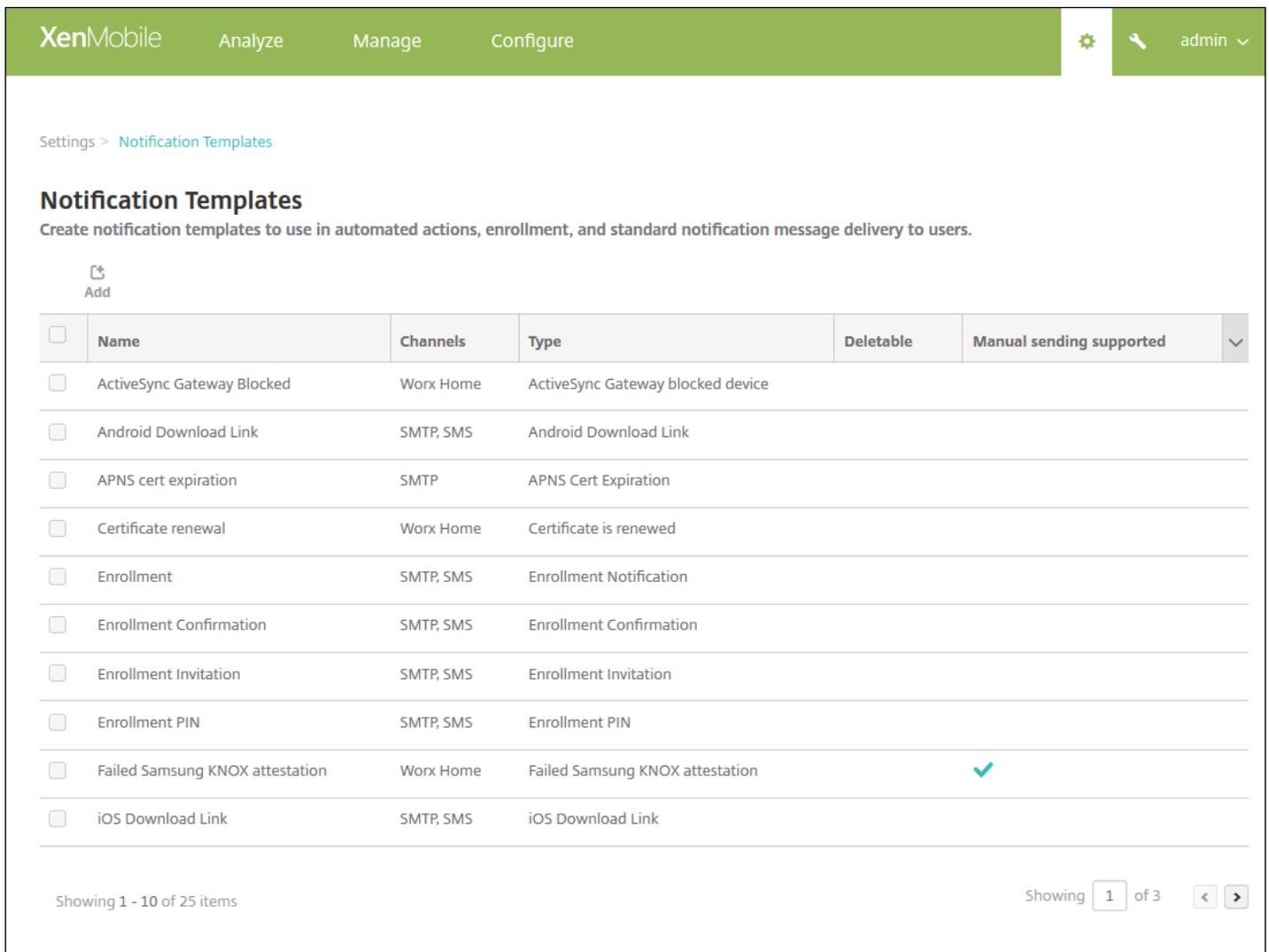
XenMobile incluye varias plantillas de notificaciones predefinidas, las cuales reflejan los distintos tipos de eventos a los que XenMobile responde automáticamente en relación a cada dispositivo del sistema.

**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**.



XenMobile Analyze Manage Configure admin

Settings > Notification Templates

### Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported	
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device			
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link			
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration			
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed			
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification			
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation			
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation			
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN			
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation		✓	
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link			

Showing 1 - 10 of 25 items

Showing 1 of 3 < >

### 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 notificación.

## Important

Si elige configurar el servidor SMTP o SMS más tarde, no podrá activar esos canales cuando agregue o modifique una plantilla de notificaciones, lo que significa que esos canales no estarán disponibles para el envío de notificaciones de usuario.

## 2. Configure 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 una plantilla de caducidad APNS Cert Expiration, que es una plantilla predefinida. 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 respalda 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(smog_block)}`

3. En **Channels**, indique la información de cada canal que se va a utilizar con esta notificación. Puede elegir un canal cualquiera o todos. Los canales que seleccione dependen de la forma en que quiera enviar notificaciones:

- Si elige **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 oír 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 de SMS si ya se ha configurado una puerta de enlace SMS.

- **Recipient.** Este campo contiene una macro previamente generada para todas las notificaciones salvo las ad hoc. De este modo, se garantiza que las notificaciones se envían a la dirección correcta de destino de SMS. Citrix recomienda no modificar macros de plantillas. Para enviar notificaciones ad hoc, puede escribir destinatarios específicos o bien puede seleccionar los dispositivos desde la página **Manage > Devices**.
- **Message.** Escriba el mensaje que se enviará al usuario. Este campo es obligatorio.

5. Haga clic en **Add**. Cuando todos los canales se hayan configurado correctamente, aparecen en este orden en la página **Notification Templates**: SMTP, SMS y Secure Hub. Los canales configurados incorrectamente aparecen después de los canales configurados correctamente.

#### Para modificar una plantilla de notificación

1. Seleccione una plantilla de notificaciones. Aparecerá la página de modificación de la plantilla en cuestión. En ella, podrá realizar cambios a todos los campos salvo a **Type**; tampoco podrá activar ni desactivar canales.
2. Haga clic en **Save**.

#### Para eliminar una plantilla de notificación

**Nota:** Solo puede eliminar las plantillas de notificación que haya agregado; no puede eliminar plantillas de notificación predeterminadas.

1. Seleccione una plantilla de notificación existente.
2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Delete** para eliminar la plantilla de notificación o en **Cancel** para no eliminarla.

# Dispositivos

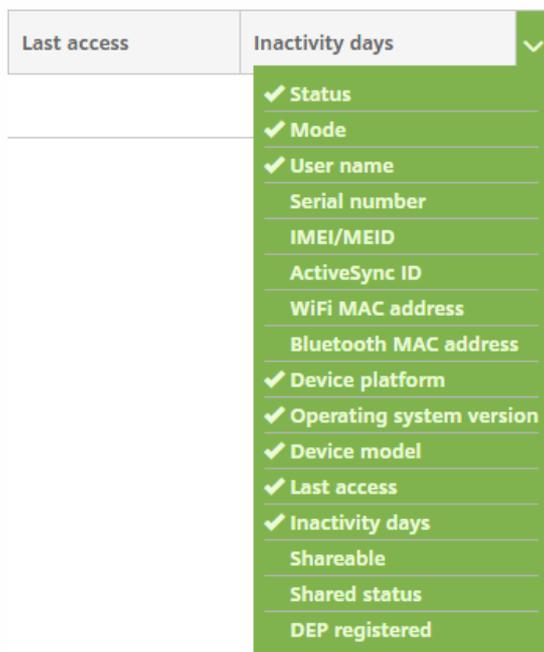
Mar 02, 2017

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:

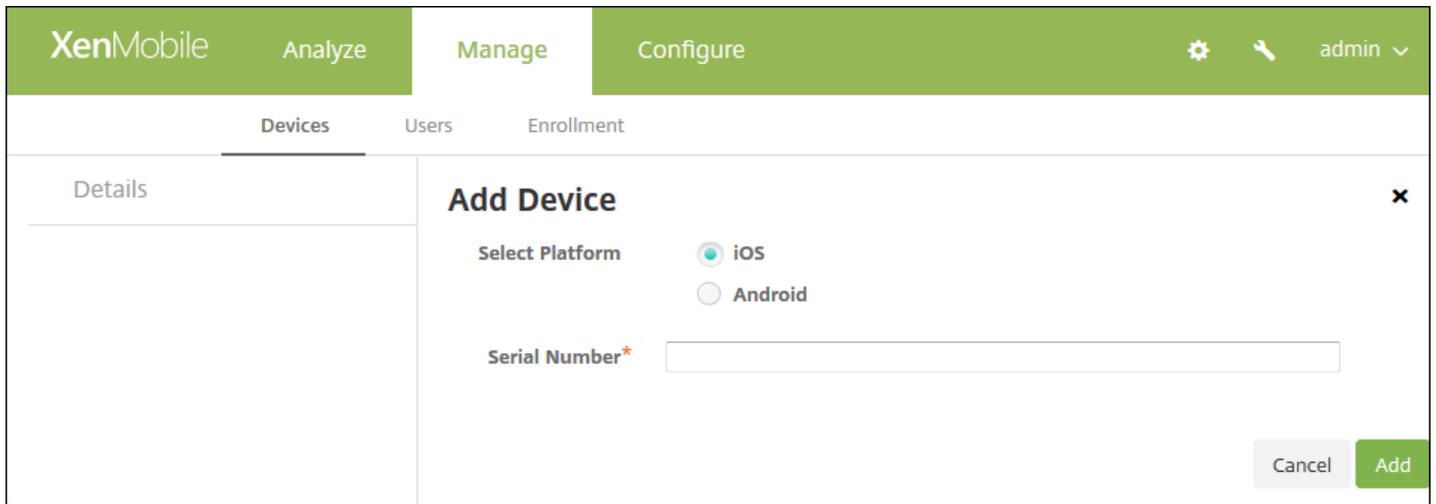
- [Cómo agregar dispositivos manualmente](#)
- [Importación de dispositivos desde un archivo de aprovisionamiento de dispositivos](#)

- 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.

The screenshot shows the XenMobile interface with the 'Device details' page open. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, along with a user profile 'administrator'. The left sidebar lists various device management options, with '1 General' selected. The main content area displays the 'General Identifiers' and 'Security' sections. The 'General Identifiers' section includes fields for Serial Number (A123), IMEI/MEID (NONE), ActiveSync ID (NONE), WiFi MAC Address (NONE), and Bluetooth MAC Address (NONE). The 'Device Ownership' section has radio buttons for 'Corporate' and 'BYOD'. The 'Security' section includes fields for Strong ID (QYD7UUSF), Full Wipe of Device (No device wipe), Selective Wipe of Device (No device selective wipe), Lock Device (No device lock), and Device Unlock (No device unlock). A 'Next >' button is visible at the bottom right of the main content area.

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.

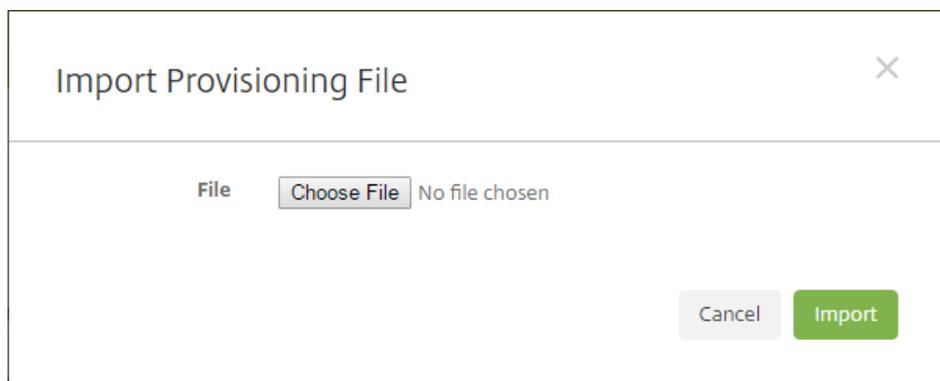
Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa (X) situada en el lado derecho. XenMobile elimina inmediatamente el elemento.

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 incluye 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.

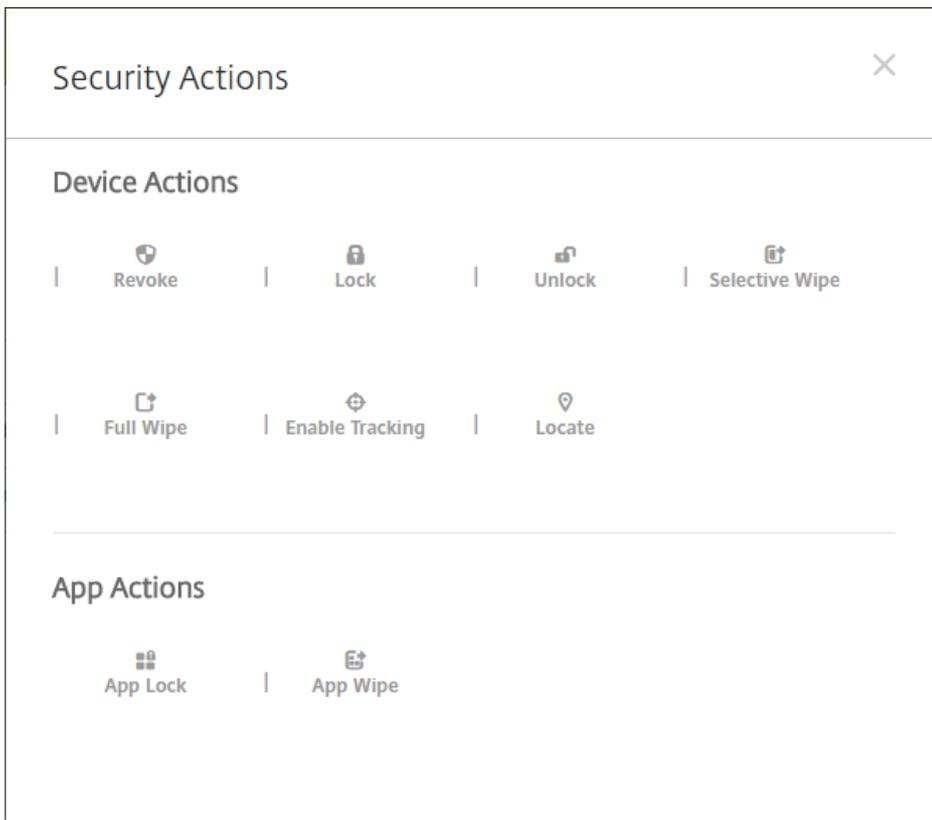
3. Haga clic en **Import**. El archivo importado aparecerá en la tabla **Devices**.

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](#).



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.

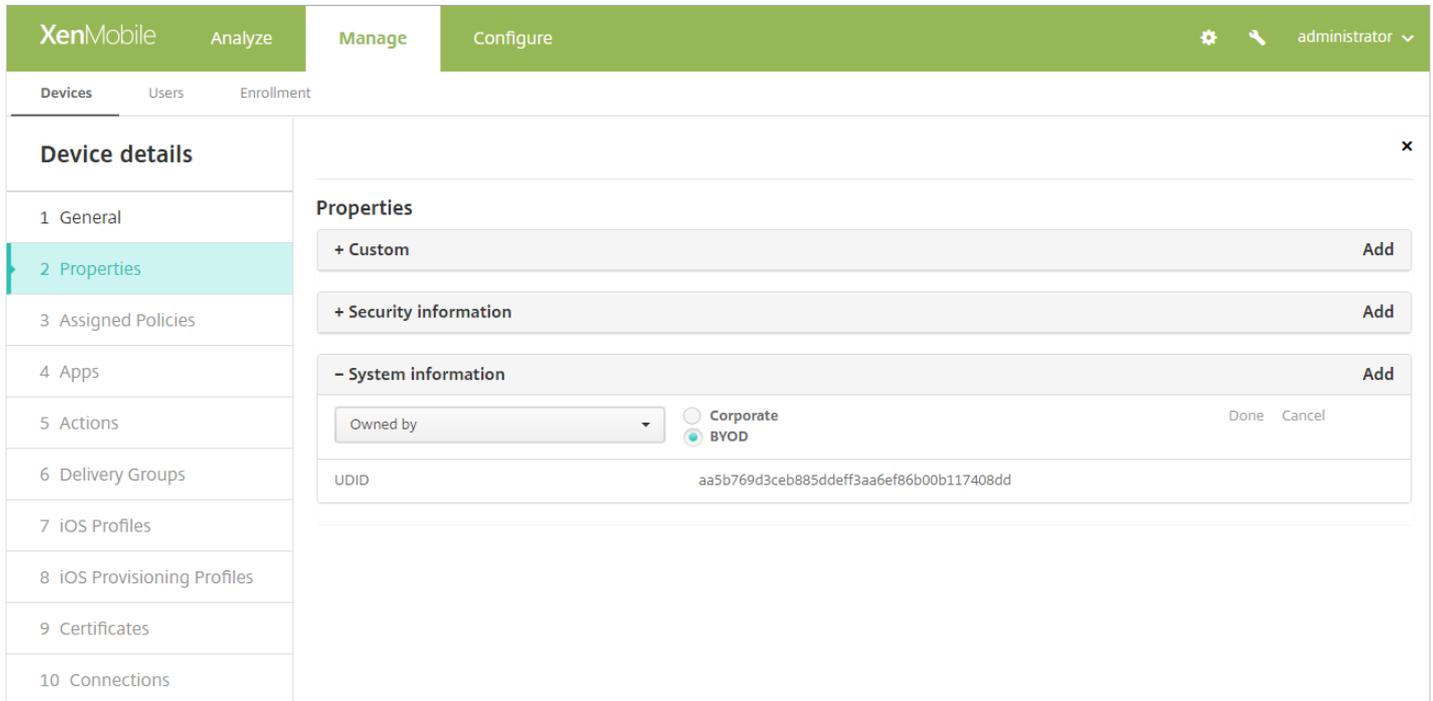
3. Cuando se le solicite, abra o guarde el archivo CSV. El modo de hacer esto dependerá del explorador Web que se esté utilizando. También puede cancelar la operación.

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**.

```
1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&ééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;;iOS;test;

;5244201625379903;ANDROID;test.testé;value;
```

Cada línea del archivo describe un dispositivo. La primera entrada del ejemplo significa lo siguiente:

- SerialNumber: 1050BF3F517301081610065510590391
- 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
AIK Present?	WINDOWS_HAS_AIK_PRESENT	Cadena
Account Suspended?	GOOGLE_AW_DIRECTORY_SUSPENDED	Cadena
Activation lock bypass code	ACTIVATION_LOCK_BYPASS_CODE	Cadena

Activation lock enabled	ACTIVATION_LOCK_ENABLED  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Active iTunes account	ACTIVE_ITUNES  Significado de los valores: 1 (Sí) 0 (No)	Booleano
ActiveSync ID	EXCHANGE_ACTIVESYNC_ID	Cadena
ActiveSync device known by MSP	AS_DEVICE_KNOWN_BY_ZMSP  Significado de los valores: 1 (True) 0 (False)	Booleano
Administrator disabled	ADMIN_DISABLED  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Amazon MDM API available	AMAZON_MDM  Significado de los valores: 1 (True) 0 (False)	Booleano
Android for Work Device ID	GOOGLE_AW_DEVICE_ID	Cadena
Android for Work Enabled Device?	GOOGLE_AW_ENABLED_DEVICE	Cadena
Android for Work Install Type	GOOGLE_AW_INSTALL_TYPE  Valores: DeviceAdministrator (Propietario del dispositivo) AvengerManagedProfile (Dispositivo administrado de trabajo) ManagedProfile (Perfil de trabajo)	Cadena
Asset tag	ASSET_TAG	Cadena

Autoupdate Status	AUTOUPDATE_STATUS	Cadena
Available RAM	MEMORY_AVAILABLE	Número entero
Available storage space	TOTAL_DISK_SPACE	Número entero
BIOS Info	BIOS_INFO	Cadena
Backup battery	BACKUP_BATTERY_PERCENT	Número entero
Baseband firmware version	MODEM_FIRMWARE_VERSION	Cadena
Battery Status	BATTERY_STATUS	Cadena
Battery charging	BATTERY_CHARGING  Significado de los valores: 1 (True) 0 (False)	Booleano
Bes device known by MSP	BES_DEVICE_KNOWN_BY_ZMSP  Significado de los valores: 1 (True) 0 (False)	Booleano
BES PIN	BES_PIN	Cadena
BES server agent ID	ENROLLMENT_AGENT_ID	Cadena
BES server name	BES_SERVER	Cadena
BES server version	BES_VERSION	Cadena
Bit Locker Status	WINDOWS_HAS_BIT_LOCKER_STATUS	Cadena
Bluetooth MAC address	BLUETOOTH_MAC	Cadena
Boot Debugging Enabled?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	Cadena

Boot Manager Rev List Version	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	Cadena
CPU clock speed	CPU_CLOCK_SPEED	Número entero
CPU type	CPU_TYPE	Cadena
Carrier settings version	CARRIER_SETTINGS_VERSION	Cadena
Cellular latitude	GPS_LATITUDE_FROM_CELLULAR	Cadena
Cellular longitude	GPS_LONGITUDE_FROM_CELLULAR	Cadena
Cellular technology	CELLULAR_TECHNOLOGY	Número entero
Cellular timestamp	GPS_TIMESTAMP_FROM_CELLULAR	Fecha
Change Password at Next Login?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	Cadena
Client device ID	CLIENT_DEVICE_ID	Cadena
Cloud backup enabled	CLOUD_BACKUP_ENABLED  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Code Integrity Enabled?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	Cadena
Code Integrity Rev List Version	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	Cadena
Color	COLOR	Cadena
Creation Time	GOOGLE_AW_DIRECTORY_CREATION_TIME	Cadena
Current carrier network	CURRENT_CARRIER_NETWORK	Cadena
Current mobile country code	CURRENT_MCC	Número entero

Current mobile network code	CURRENT_MNC	Cadena
DEP Policy	WINDOWS_HAS_DEP_POLICY	Cadena
Data roaming allowed	DATA_ROAMING_ENABLED  Significado de los valores: 1 (Si) 0 (No)	Booleano
Date of the last iCloud backup	LAST_CLOUD_BACKUP_DATE	Fecha
Description	DESCRIPTION	Cadena
Device Enrollment Program profile assigned	PROFILE_ASSIGN_TIME	Fecha
Device Enrollment Program profile pushed	PROFILE_PUSH_TIME	Fecha
Device Enrollment Program profile removed	PROFILE_REMOVE_TIME	Fecha
Device Enrollment Program registration by	DEVICE_ASSIGNED_BY	Cadena
Device Enrollment Program registration date	DEVICE_ASSIGNED_DATE	Fecha
Device Type	DEVICE_TYPE	Cadena
Device model	MODEL_ID	Cadena
Device name	DEVICE_NAME	Cadena
Do Not Disturb activated	DO_NOT_DISTURB  Significado de los valores: 1 (Si) 0 (No)	Booleano
ELAM Driver Loaded?	WINDOWS_HAS_ELAM_DRIVER_LOADED	Cadena

ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	Fecha
Enterprise ID	ENTERPRISE_ID	Cadena
External storage 1: available space	EXTERNAL_STORAGE1_FREE_SPACE	Número entero
External storage 1: name	EXTERNAL_STORAGE1_NAME	Cadena
External storage 1: total space	EXTERNAL_STORAGE1_TOTAL_SPACE	Número entero
External storage 2: available space	EXTERNAL_STORAGE2_FREE_SPACE	Número entero
External storage 2: name	EXTERNAL_STORAGE2_NAME	Cadena
External storage 2: total space	EXTERNAL_STORAGE2_TOTAL_SPACE	Número entero
External storage encrypted	EXTERNAL_ENCRYPTION  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Firewall Status	FIREWALL_STATUS	Cadena
Firmware version	FIRMWARE_VERSION	Cadena
First synchronization	ZMSP_FIRST_SYNC	Fecha
GPS altitude	GPS_ALTITUDE_FROM_GPS	Cadena
GPS latitude	GPS_LATITUDE_FROM_GPS	Cadena
GPS longitude	GPS_LONGITUDE_FROM_GPS	Cadena
GPS timestamp	GPS_TIMESTAMP_FROM_GPS	Fecha

Google Directory Alias	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	Cadena
Google Directory Family Name	GOOGLE_AW_DIRECTORY_FAMILY_NAME	Cadena
Google Directory Name	GOOGLE_AW_DIRECTORY_NAME	Cadena
Google Directory Primary Email	GOOGLE_AW_DIRECTORY_PRIMARY	Cadena
Google Directory User ID	GOOGLE_AW_DIRECTORY_USER_ID	Cadena
HAS_CONTAINER	HAS_CONTAINER  Significado de los valores: 1 (Sí) 0 (No)	Booleano
HTC API version	HTC_MDM_VERSION	Cadena
HTC MDM API available	HTC_MDM  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Hardware encryption capabilities	HARDWARE_ENCRYPTION_CAPS	Número entero
Hash of the iTunes store account currently logged on	ITUNES_STORE_ACCOUNT_HASH	Cadena
Home carrier network	SIM_CARRIER_NETWORK	Cadena
Home mobile country code	SIM_MCC	Número entero
Home mobile network code	SIM_MNC	Cadena
ICCID	ICCID	Cadena
IMEI/MEID number	IMEI	Cadena
IMSI	IMSI	Cadena

IP location	IP_LOCATION	Cadena
Identity	AS_DEVICE_IDENTITY	Cadena
Internal storage encrypted	LOCAL_ENCRYPTION  Significado de los valores: 1 (True) 0 (False)	Booleano
Issued At	WINDOWS_HAS_ISSUED_AT	Cadena
Jailbroken/Rooted	ROOT_ACCESS  Significado de los valores: 1 (Si) 0 (No)	Booleano
Kernel Debugging Enabled?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	Cadena
Kiosk mode	IS_KIOSK  Significado de los valores: 1 (True) 0 (False)	Booleano
Last known IP address	LAST_IP_ADDR	Cadena
Last policy update time	LAST_POLICY_UPDATE_TIME	Fecha
Last synchronization	ZMSP_LAST_SYNC	Fecha
Locator service enabled	DEVICE_LOCATOR  Significado de los valores: 1 (Si) 0 (No)	Booleano
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	Cadena
MEID	MEID	Cadena

Mailbox Setup	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	Cadena
Main battery	MAIN_BATTERY_PERCENT	Número entero
Mobile phone number	TEL_NUMBER	Cadena
Model ID	SYSTEM_OEM	Cadena
Network Adapter Type	NETWORK_ADAPTER_TYPE	Cadena
NitroDesk TouchDown installed	TOUCHDOWN_FIND  Significado de los valores: 1 (True) 0 (False)	Booleano
NitroDesk TouchDown licensed via MDM	TOUCHDOWN_LICENSED_VIA_MDM  Significado de los valores: 1 (True) 0 (False)	Booleano
Operating system build	SYSTEM_OS_BUILD	Cadena
Operating system language (locale)	SYSTEM_LANGUAGE	Cadena
Operating system version	SYSTEM_OS_VERSION	Cadena
Organization address	ORGANIZATION_ADDRESS	Cadena
Organization e-mail	ORGANIZATION_EMAIL	Cadena
Organization magic	ORGANIZATION_MAGIC	Cadena
Organization name	ORGANIZATION_NAME	Cadena
Organization phone number	ORGANIZATION_PHONE	Cadena
Other	OTHER	Cadena
Out of Compliance	OUT_OF_COMPLIANCE	Booleano

	<p>Significado de los valores:  1 (True)  0 (False)</p>	
Owned by	<p>CORPORATE_OWNED</p> <p>Significado de los valores:  1 (Empresa)  0 (BYOD)</p>	Booleano
PCRO	<p>WINDOWS_HAS_PCRO</p>	Cadena
PIN code for geofence	<p>PIN_CODE_FOR_GEO_FENCE</p>	Cadena
Passcode compliant	<p>PASSCODE_IS_COMPLIANT</p> <p>Significado de los valores:  1 (Sí)  0 (No)</p>	Booleano
Passcode compliant with configuration	<p>PASSCODE_IS_COMPLIANT_WITH_CFG</p> <p>Significado de los valores:  1 (Sí)  0 (No)</p>	Booleano
Passcode present	<p>PASSCODE_PRESENT</p> <p>Significado de los valores:  1 (Sí)  0 (No)</p>	Booleano
Perimeter breach	<p>GPS_PERIMETER_BREACH</p> <p>Significado de los valores:  1 (Sí)  0 (No)</p>	Booleano
Personal Hotspot activated	<p>PERSONAL_HOTSPOT_ENABLED</p> <p>Significado de los valores:  1 (Sí)  0 (No)</p>	Booleano
Platform	<p>SYSTEM_PLATFORM</p>	Cadena

Platform API level	API_LEVEL	Número entero
Policy name	POLICY_NAME	Cadena
Primary Phone Number	IDENTITY1_PHONENUMBER	Cadena
Primary SIM IMEI	IDENTITY1_IMEI	Cadena
Primary SIM IMSI	IDENTITY1_IMSI	Cadena
Primary SIM Roaming	IDENTITY1_ROAMING  Significado de los valores: 1 (True) 0 (False)	Booleano
Product name	PRODUCT_NAME	Cadena
Publisher Device ID	PUBLISHER_DEVICE_ID	Cadena
Reset Count	WINDOWS_HAS_RESET_COUNT	Cadena
Restart Count	WINDOWS_HAS_RESTART_COUNT	Cadena
SBCP Hash	WINDOWS_HAS_SBCP_HASH	Cadena
SMS capable	IS_SMS_CAPABLE  Significado de los valores: 1 (True) 0 (False)	Booleano
Safe Mode Enabled?	WINDOWS_HAS_SAFE_MODE	Cadena
Samsung KNOX API available	SAMSUNG_KNOX  Significado de los valores: 1 (True) 0 (False)	Booleano
Samsung KNOX API version	SAMSUNG_KNOX_VERSION	Cadena

Samsung KNOX attestation	SAMSUNG_KNOX_ATTESTED  Significado de los valores: 1 (Correcto)  0 (Error)	Booleano
Samsung KNOX attestation updated date	SAMSUNG_KNOX_ATT_UPDATED_TIME	Fecha
Samsung SAFE API available	SAMSUNG_MDM  Significado de los valores: 1 (True) 0 (False)	Booleano
Samsung SAFE API version	SAMSUNG_MDM_VERSION	Cadena
Screen: X-axis resolution	SCREEN_XDPI	Número entero (PPI)
Screen: Y-axis resolution	SCREEN_YDPI	Número entero (PPI)
Screen: height	SCREEN_HEIGHT	Número entero (píxeles)
Screen: number of colors	SCREEN_NB_COLORS	Número entero
Screen: size	SCREEN_SIZE	Decimal (pulgadas)
Screen: width	SCREEN_WIDTH	Número entero (píxeles)
Secondary Phone Number	IDENTITY2_PHONENUMBER	Cadena

Secondary SIM IMEI	IDENTITY2_IMEI	Cadena
Secondary SIM IMSI	IDENTITY2_IMSI	Cadena
Secondary SIM Roaming	IDENTITY2_ROAMING  Significado de los valores: 1 (True) 0 (False)	Booleano
Secure Boot Enabled?	WINDOWS_HAS_SECURE_BOOT_ENABLED	Cadena
SecureContainer Enabled	WINDOWS_HAS_BIT_LOCKER_STATUS	Cadena
Serial number	SERIAL_NUMBER	Cadena
Sony Enterprise API available	SONY_MDM  Significado de los valores: 1 (True) 0 (False)	Booleano
Sony Enterprise API version	SONY_MDM_VERSION	Cadena
Supervised	Supervised  Significado de los valores: 1 (Sí) 0 (No)	Booleano
Suspension Reason	GOOGLE_AW_DIRECTORY_SUSPENSION_REASON	Cadena
Tampered Status	TAMPERED_STATUS	Cadena
Terms & Conditions	TERMS_AND_CONDITIONS	Cadena
Terms And Agreement Accepted?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	Cadena
Test Signing Enabled?	WINDOWS_HAS_TEST_SIGNING_ENABLED	Cadena
Total RAM	MEMORY	Número entero

Total storage space	FREEDISK	Número entero
UDID	UDID	Cadena
User agent	USER_AGENT	Cadena
User defined #1	USER_DEFINED_1	Cadena
User defined #2	USER_DEFINED_2	Cadena
User defined #3	USER_DEFINED_3	Cadena
User language (locale)	USER_LANGUAGE	Cadena
VSM Enabled?	WINDOWS_HAS_VSM_ENABLED	Cadena
Vendor	VENDOR	Cadena
Voice capable	IS_VOICE_CAPABLE  Significado de los valores: 1 (True) 0 (False)	Booleano
Voice roaming allowed	VOICE_ROAMING_ENABLED  Significado de los valores: 1 (Sí) 0 (No)	Booleano
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	Cadena
WNS Notification Status	WNS_PUSH_STATUS	Cadena
WNS Notification URL	PROPERTY_WNS_PUSH_URL	Cadena
WNS Notification URL expiry date	PROPERTY_WNS_PUSH_URL_EXPIRY	Cadena
WiFi MAC address	WIFI_MAC	Cadena
WinPE Enabled?	WINDOWS_HAS_WINPE	Cadena

XenMobile agent ID	AGENT_ID	Cadena
XenMobile agent revision	EW_REVISION	Cadena
XenMobile agent version	EW_VERSION	Cadena

# Bloqueo de dispositivos iOS

Mar 02, 2017

Puede bloquear un dispositivo iOS y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo. Esta función está respaldada en dispositivos iOS 7 y 8.

Si opta por incluir un mensaje y un número de teléfono en la pantalla de bloqueo, estos solo aparecerán en dispositivos bloqueados si también se ha configurado la directiva de [códigos de acceso](#) en la consola de XenMobile o si los usuarios han habilitado manualmente un código de acceso en el dispositivo.

1. En la consola de XenMobile, haga clic en **Manage > Devices**. Aparecerá la página **Devices**.



XenMobile Analyze Manage Configure

Devices Users Enrollment

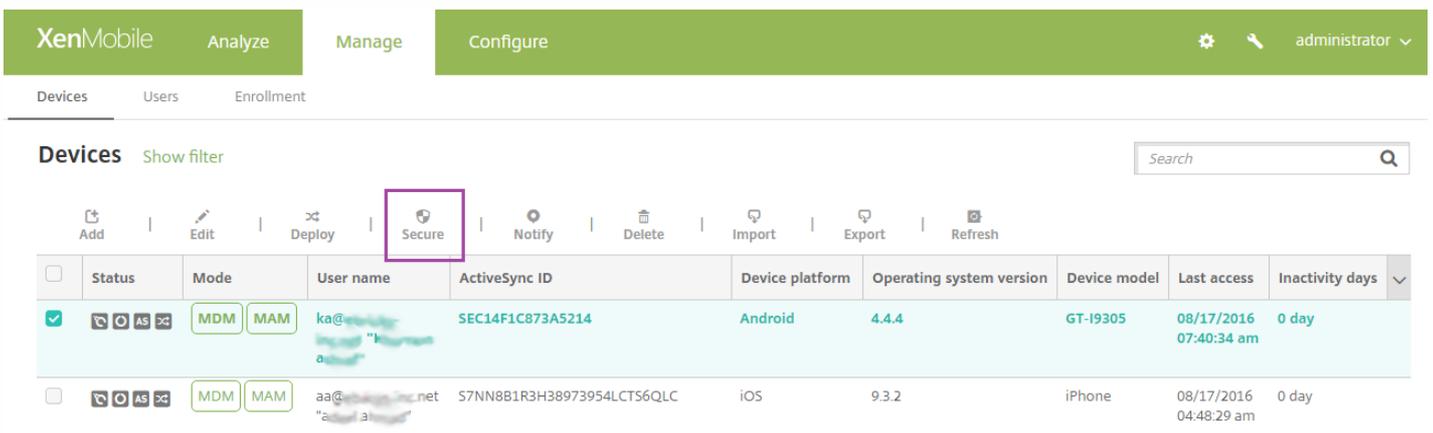
Devices Show filter

Add Import Export Refresh

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>		MDM MAM	us1user1@... net "us1 user1"	Android	5.0.2
<input type="checkbox"/>		MDM MAM	us3user3@... net "us3 user3"	iOS	8.4.1

2. Seleccione el dispositivo iOS que quiere bloquear.

Si marca la casilla situada junto a un dispositivo, el menú de opciones aparecerá encima de la lista de dispositivos. En cambio, si hace clic en cualquier otro lugar de la lista, el menú de opciones aparecerá en el lado derecho de la lista.



XenMobile Analyze Manage Configure administrator

Devices Users Enrollment

Devices Show filter Search

Add Edit Deploy Secure Notify Delete Import Export Refresh

<input type="checkbox"/>	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>		MDM MAM	ka@... net "ka..."	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>		MDM MAM	aa@... net "aa..."	S7NN8B1R3H38973954LCTS6QLC	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day

XenMobile Analyze Manage Configure administrator

Devices Users Enrollment

Devices Show filter Search

Add Import Export Refresh

Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
	MDM MAM	ka@...net	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
	MDM MAM	aa@...net	S7NN8B1R3H38973954LCTS6QLC	iOS				

Edit | Deploy | **Secure** | Notify | Delete

**XME Device Managed**

Delivery Groups	2	Policies	5
Actions	2	Apps	15

Show more >

3. En el menú de opciones, seleccione **Secure**. Aparecerá el cuadro de diálogo **Security Actions**.

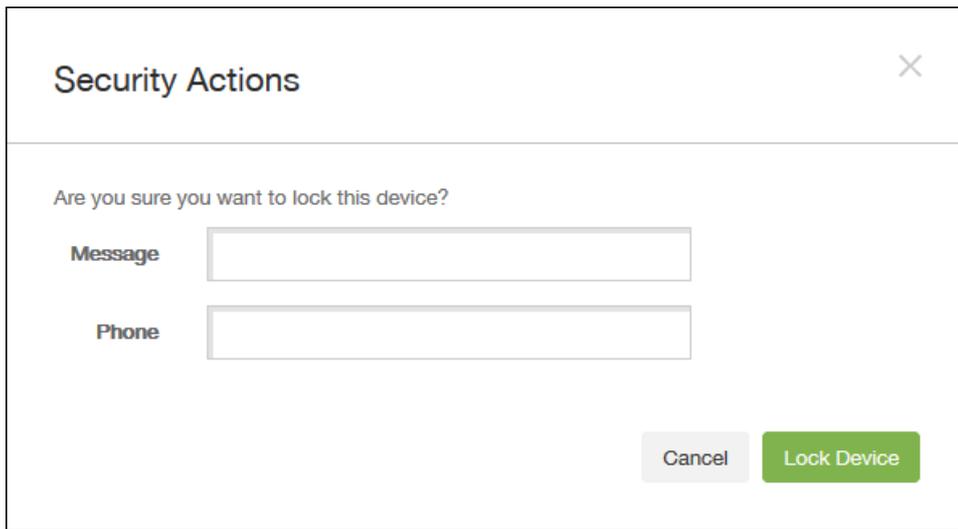
Security Actions

Device Actions

Revoke | **Lock** | Unlock | Selective Wipe

Full Wipe | Enable Tracking | Locate | Request AirPlay Mirroring

4. Seleccione **Lock**. Aparecerá el cuadro de diálogo de confirmación **Security Actions**.



Security Actions

Are you sure you want to lock this device?

Message

Phone

Cancel Lock Device

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 **Mensaje**. Para iPhones que ejecutan iOS 7 y versiones posteriores: Si deja el campo **Mensaje** 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

Mar 02, 2017

La detección automática es una parte importante de las implementaciones de XenMobile. La detección automática simplifica el proceso de inscripción para los usuarios. Con ella, pueden utilizar sus nombres de usuario y contraseñas de Active Directory para inscribir sus dispositivos, en lugar de tener que especificar también datos del servidor XenMobile. Los usuarios deben especificar su nombre de usuario en el formato del nombre principal de usuario (UPN); por ejemplo, usuario@miempresa.com. XenMobile AutoDiscovery Service permite crear o editar un registro de detección automática sin ayuda del servicio de asistencia de Citrix Support.

Para acceder a XenMobile AutoDiscovery Service, vaya a <https://xenmobiletools.citrix.com> y haga clic en **Request Auto Discovery**.

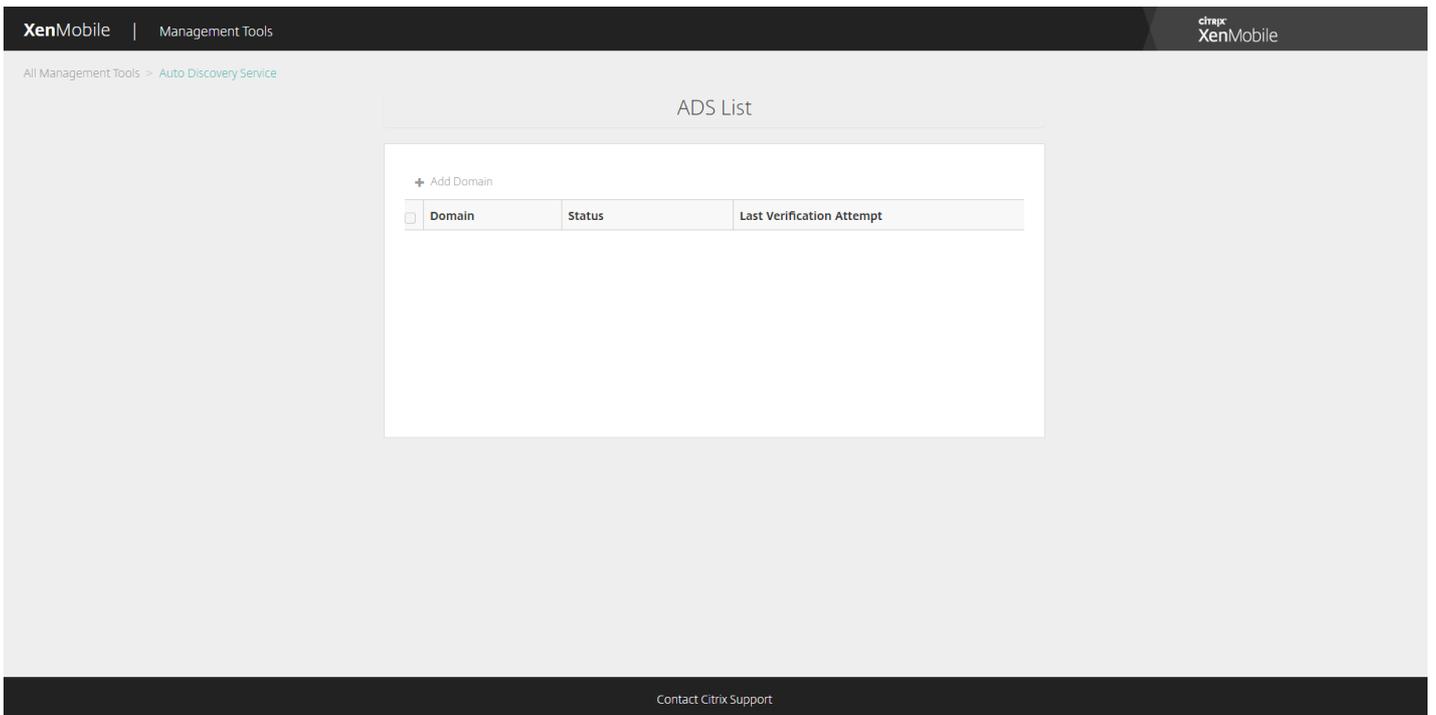
The screenshot shows the XenMobile Management Tools website. At the top, there is a navigation bar with 'XenMobile | Management Tools' on the left and the Citrix XenMobile logo on the right. Below the navigation bar, the main content area has a heading 'What do you want to do?' and a sub-heading 'XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.' Below this, there are four cards representing different services:

- Analyze and Troubleshoot my XenMobile environment**: XenMobile Analyzer. Follow steps to identify and triage potential issues with your deployment.
- Request Auto Discovery**: Auto Discovery Service. Request and Configure Auto Discovery for your domain's XenMobile Server.
- Request push notification certificate signature**: Create APNs Certificate. Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.
- Enable APNs-based push notifications for WorxMail for iOS**: Upload APNs Certificate. Enable push notifications by uploading APNs certificate from Apple.

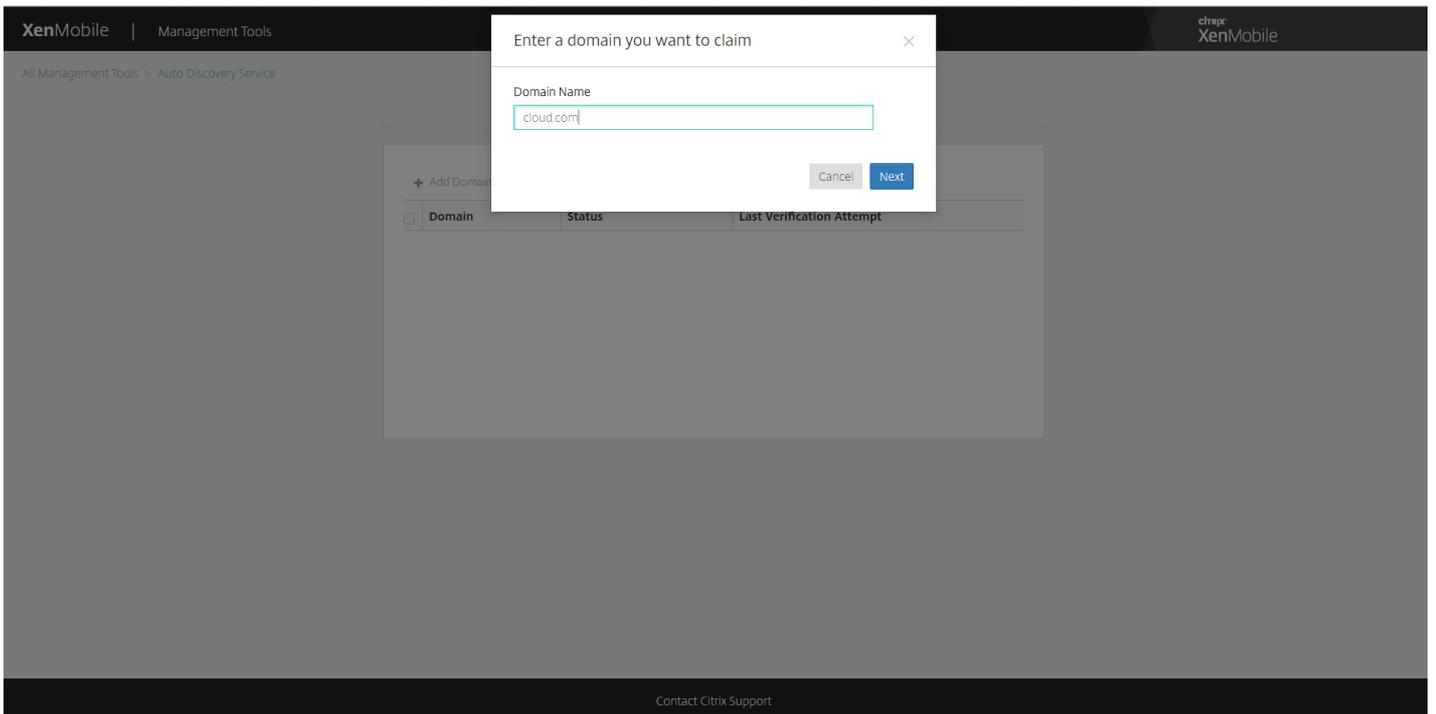
At the bottom of the page, there is a 'Contact Citrix Support' link.

## Cómo solicitar el servicio de detección automática

1. En la página AutoDiscovery Service, primero necesita reclamar un dominio. Haga clic en **Add Domain**.



2. En el cuadro de diálogo que se abre, introduzca el nombre de dominio de su entorno de XenMobile y, a continuación, haga clic en **Next**.



3. El paso siguiente proporciona instrucciones para verificar que usted es el propietario del dominio.

- a. Copie el token de DNS suministrado en portal de herramientas de XenMobile.
- b. Cree un registro TXT de DNS en el archivo de zona de su dominio en el portal de su proveedor de alojamiento de

dominios.

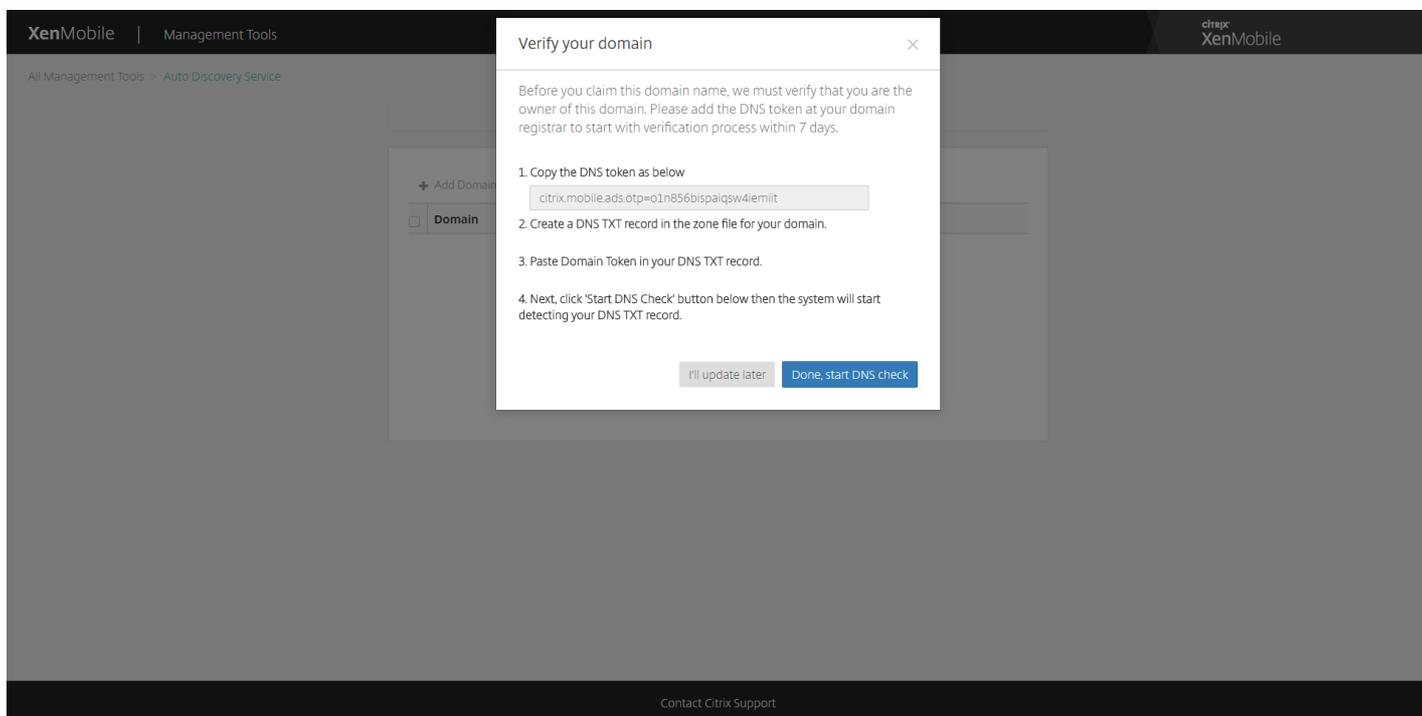
Para crear un registro TXT de DNS, es necesario iniciar sesión en el portal del proveedor de alojamiento del dominio que agregó en el paso 2. En el portal de alojamiento de dominios puede editar sus registros de servidor de nombres de dominio (DNS) y agregar un registro TXT personalizado. Abajo hay un ejemplo para agregar una entrada TXT de DNS en el portal de alojamiento del dominio de ejemplo "domain.com".

c. Pegue el token de dominio en el registro TXT de DNS y guarde el registro de servidor de nombres de dominio (DNS).

d. De vuelta en el portal de herramientas de XenMobile, haga clic en "Done, start DNScheck".

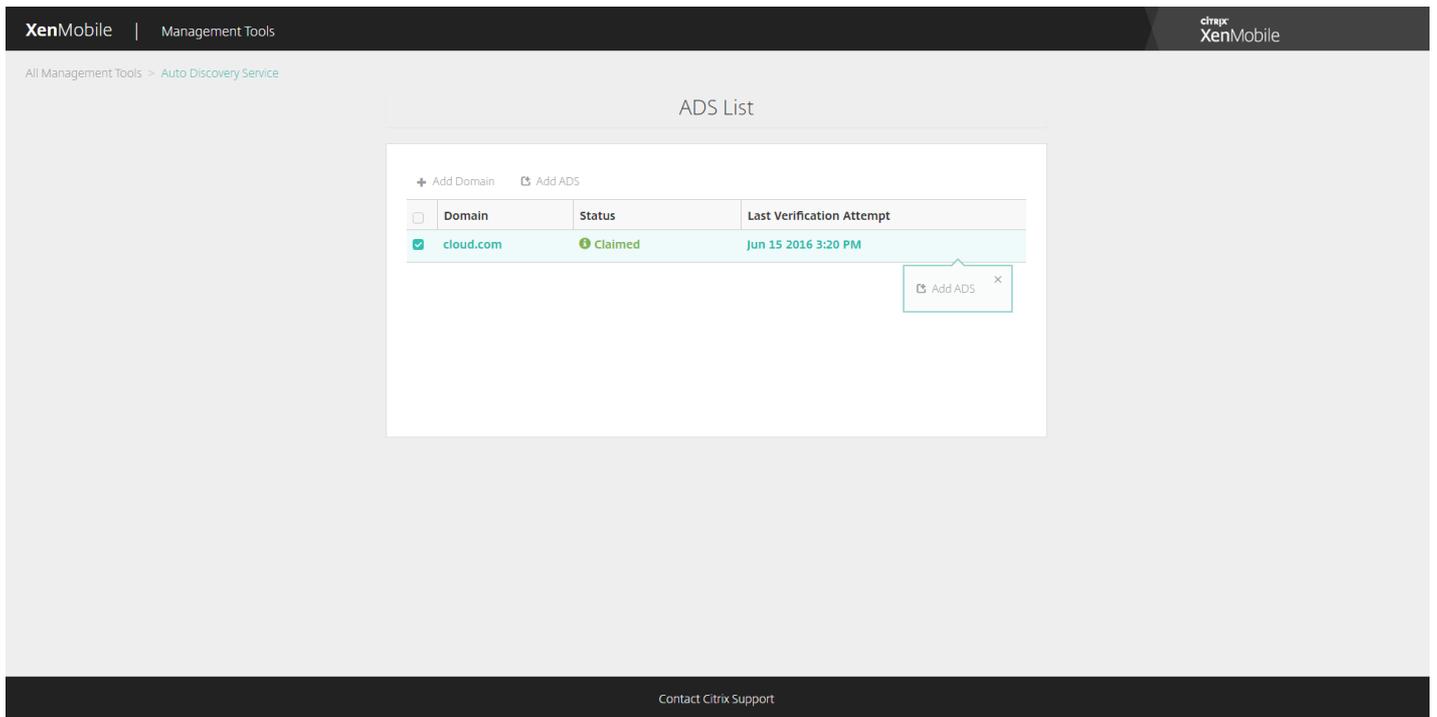
El sistema detecta el registro TXT de DNS. Si lo prefiere, puede hacer clic en "I'll update later" y el registro se guarda. La comprobación de DNS no se iniciará hasta que seleccione el registro en espera (Waiting) y haga clic en "DNS Check".

Esta comprobación normalmente tarda aproximadamente una hora, pero puede tardar hasta dos días en devolver una respuesta. Además, es posible que tenga que abandonar el portal y volver a él para ver el cambio de estado.

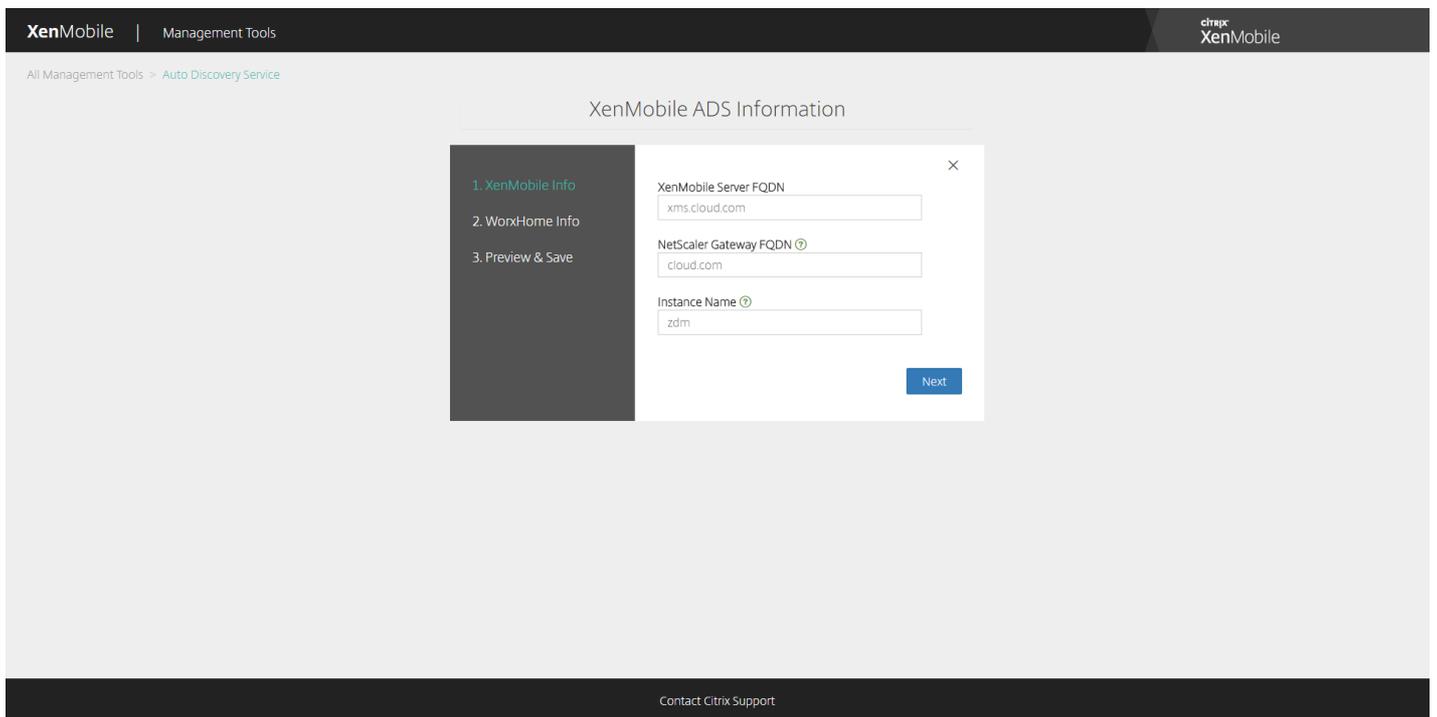


4. Después de reclamar su dominio, puede introducir la información para el servicio de detección automática. Haga clic con el botón secundario en el registro del dominio para el cual quiere solicitar detección automática y luego haga clic en **Agregar ADS**.

Si el dominio ya tiene un registro de AutoDiscovery, inicie un caso con el servicio de asistencia técnica de Citrix para modificar los detalles, según sea necesario.



5. Introduzca los nombres de dominio completos del servidor XenMobile y de NetScaler Gateway en **XenMobile Server FQDN** y **NetScaler Gateway FQDN**, y el nombre de la instancia en **Instance Name** y haga clic en **Next**. Si no está seguro, agregue una instancia predeterminada de "zdm".



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 el que los usuarios inician sesiones: **E-mail address** o **UPN**.

**UPN** se utiliza cuando el nombre principal de usuario (UPN) del usuario es el mismo que su dirección de correo electrónico. Ambos métodos usan el dominio especificado para buscar la dirección del servidor. Con **E-mail address**, se pide al usuario que introduzca su nombre de usuario y contraseña; con **UPN**, se le pide que escriba su contraseña.

b. **HTTPS Port.** Introduzca el puerto usado para acceder a Secure Hub sobre HTTPS. Por lo general, este es el puerto 443.

c. **iOS Enrollment Port.** Escriba el número de puerto que se utiliza para acceder a Secure Hub para la inscripción de iOS. Por lo general, este es el puerto 8443.

d. **Required Trusted CA for XenMobile:** Indique si se necesita un certificado de confianza para acceder a XenMobile o no. Esta opción puede ser **OFF** u **ON**. Actualmente, no existe la capacidad para cargar un certificado para esta característica. Si quiere usar esta característica, debe llamar a la asistencia técnica de Citrix Support para que ellos configuren la detección automática. Para obtener más información sobre la fijación de certificados, consulte la sección sobre 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](#).

XenMobile | Management Tools Citrix XenMobile

All Management Tools > Auto Discovery Service

WorxHome ADS Information

1. XenMobile Info  
2. **WorxHome Info**  
3. Preview & Save

User ID Type  
E-mail address

HTTPS Port ⓘ  
443

iOS Enrollment Port ⓘ  
8443

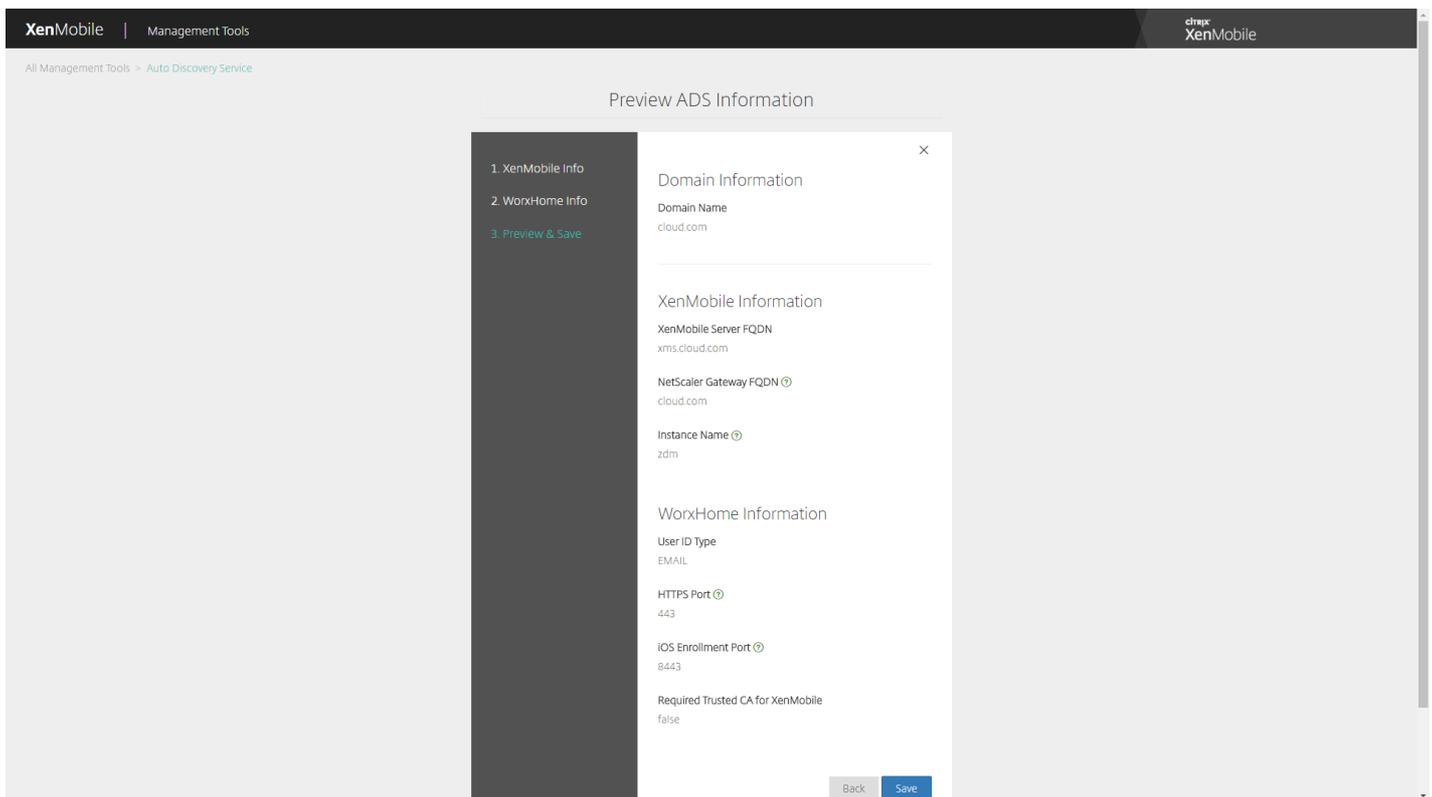
Required Trusted CA for XenMobile  
 OFF

Back Next

Contact Citrix Support

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. Con ella, pueden utilizar sus nombres de usuario y contraseñas de Active Directory para inscribir sus dispositivos, en lugar de tener que especificar también datos del servidor XenMobile. Los usuarios deben especificar su nombre de usuario en el formato del nombre principal de usuario (UPN); por ejemplo, usuario@miempresa.com.

Para habilitar la detección automática, puede acceder al portal Autodiscovery Service en <https://xenmobiletools.citrix.com>.

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.miempresa.com`, donde `miempresa.com` es el dominio que contiene las cuentas con las que se inscribirán los usuarios. Adjunte el certificado SSL en formato `.pfx` y su contraseña para la solicitud.
- Cree un registro de nombre canónico (CNAME) en 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

Mar 02, 2017

Para poder administrar dispositivos de usuario de forma remota y segura, dichos dispositivos deben estar inscritos en XenMobile. El software cliente de XenMobile debe estar instalado en el dispositivo del usuario y el usuario debe haberse autenticado. Entonces, se instalan ambos, XenMobile y el perfil del usuario. Después de inscribir los dispositivos, en la consola de XenMobile, puede realizar tareas de administración de dispositivos, como aplicar directivas, implementar aplicaciones, insertar datos en los dispositivos, así como bloquear, borrar y localizar dispositivos perdidos o robados.

**Nota:** Antes de poder inscribir usuarios de dispositivos iOS, debe solicitar un certificado APNs. Para obtener más información, consulte [Certificados](#).

Para actualizar las opciones de configuración para usuarios y dispositivos, utilice la página **Manage > Enrollment**. Para obtener más información, consulte [Envío de una invitación de inscripción](#) en este artículo.

## Dispositivos Android

1. Vaya a Google Play o a la Tienda Apps de Amazon en el dispositivo Android, descargue la aplicación Citrix Secure Hub y, a continuación, toque en la aplicación.
2. Cuando se le solicite la instalación de la aplicación, haga clic en **Siguiente** y, a continuación, haga clic en **Instalar**.
3. Después de que 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 **Activate**.
6. Escriba la contraseña de empresa y, a continuación, toque **Iniciar sesión**.
7. Según la configuración de XenMobile que tenga, es posible que se le solicite la creación de un PIN de 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**, escriba un número PIN compuesto de cualquier combinación de seis números.
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. Toque **Instalar** para instalar las aplicaciones.

### Para inscribir y reinscribir un dispositivo Android

Antes de volver a inscribir un dispositivo, ese dispositivo debe primero dejar de estar inscrito. Mientras el dispositivo no esté inscrito y hasta que se vuelva a inscribir, XenMobile no lo administrará aunque dicho dispositivo siga apareciendo en la lista de inventario de dispositivos en la consola de XenMobile. No se puede realizar el seguimiento de un dispositivo ni supervisar su estado de cumplimiento si XenMobile no lo administra.

1. Toque en Secure Hub para abrir la aplicación.
2. Toque el icono Parámetros en la parte superior izquierda de la ventana de la aplicación.
3. Toque **Reinscribir**. Aparecerá un mensaje para confirmar que quiere volver a inscribir el dispositivo.
4. Toque **Aceptar**. Esta acción tiene como consecuencia la desinscripción de su dispositivo.

5. Siga las instrucciones que aparecen en pantalla para volver a inscribir su dispositivo.

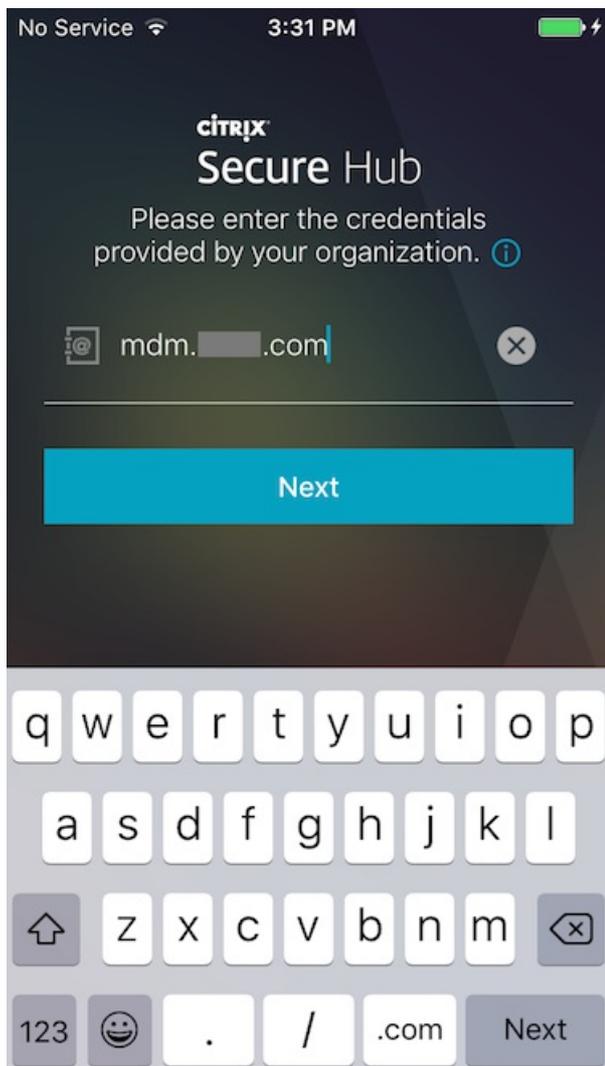
## Dispositivos OS

1. Descargue la aplicación Secure Hub desde iTunes, el App Store de Apple, al dispositivo y, a continuación, instale la aplicación en el dispositivo.

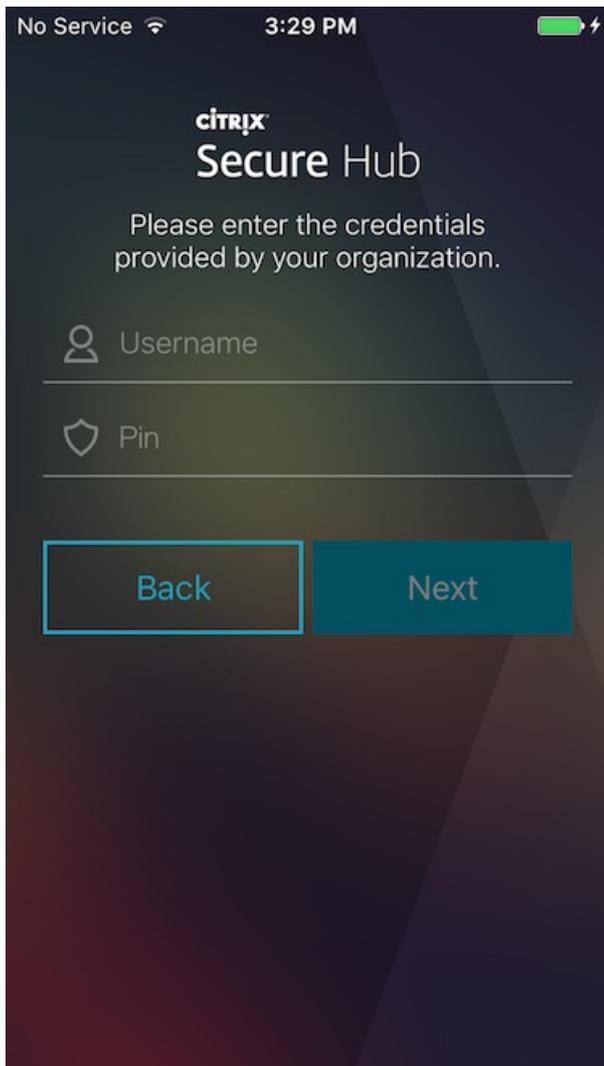
2. En la pantalla de inicio del dispositivo iOS, toque en la aplicación Secure Hub.

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.

**CITRIX**  
**Secure Hub**

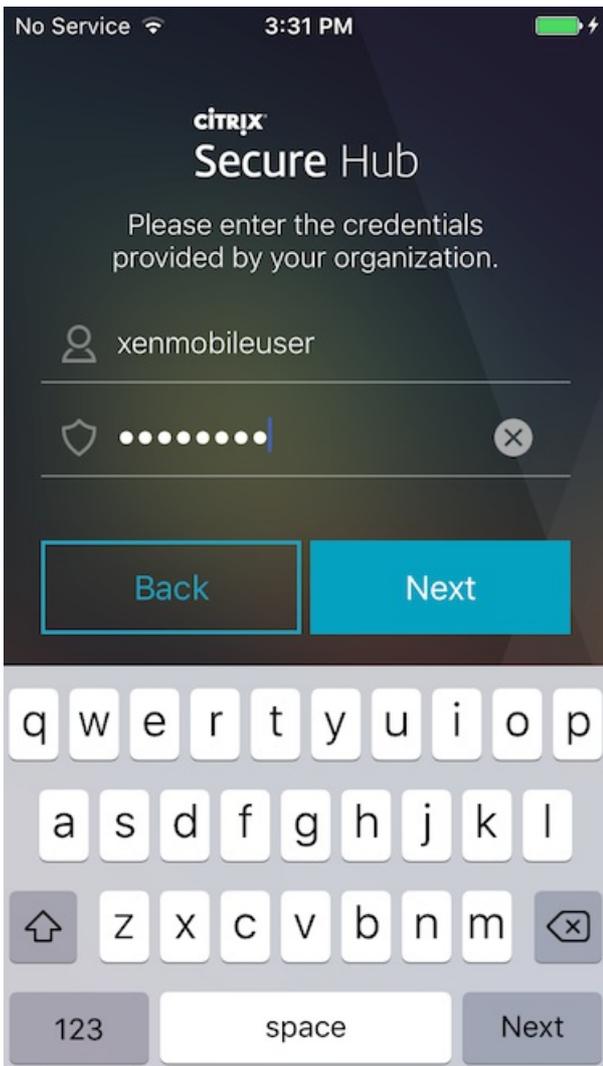
Please enter the credentials provided by your organization. ⓘ

### Enroll Your iPhone

Enrolling secures your iPhone and your work apps. Do you want to enroll your device?

Yes, Enroll

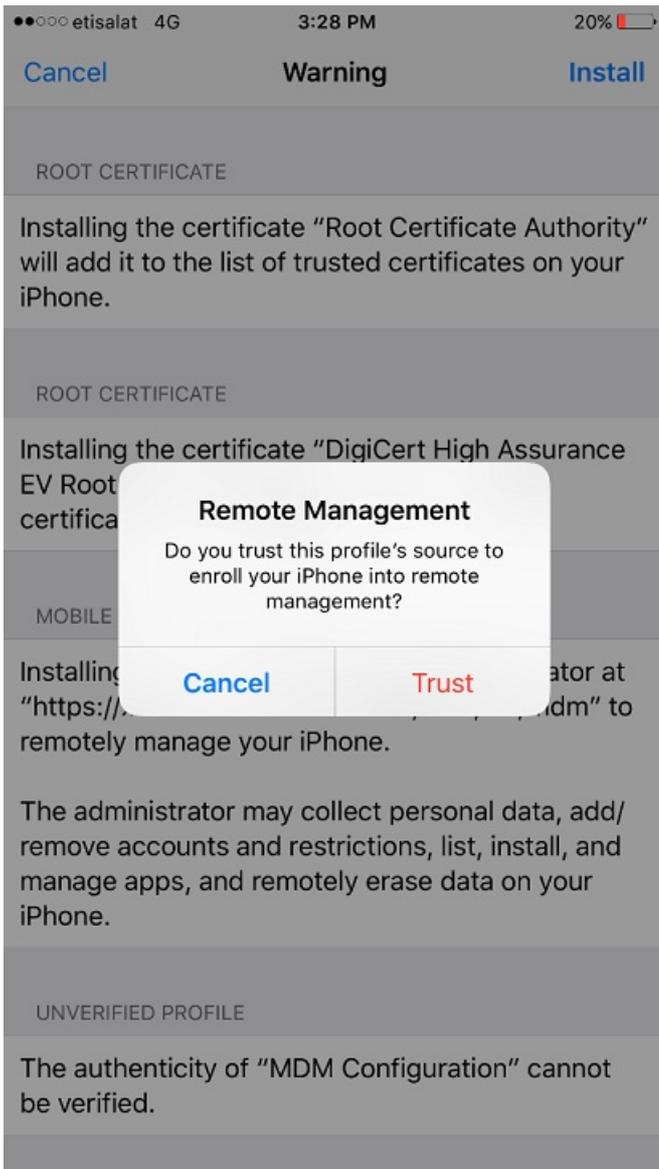
No



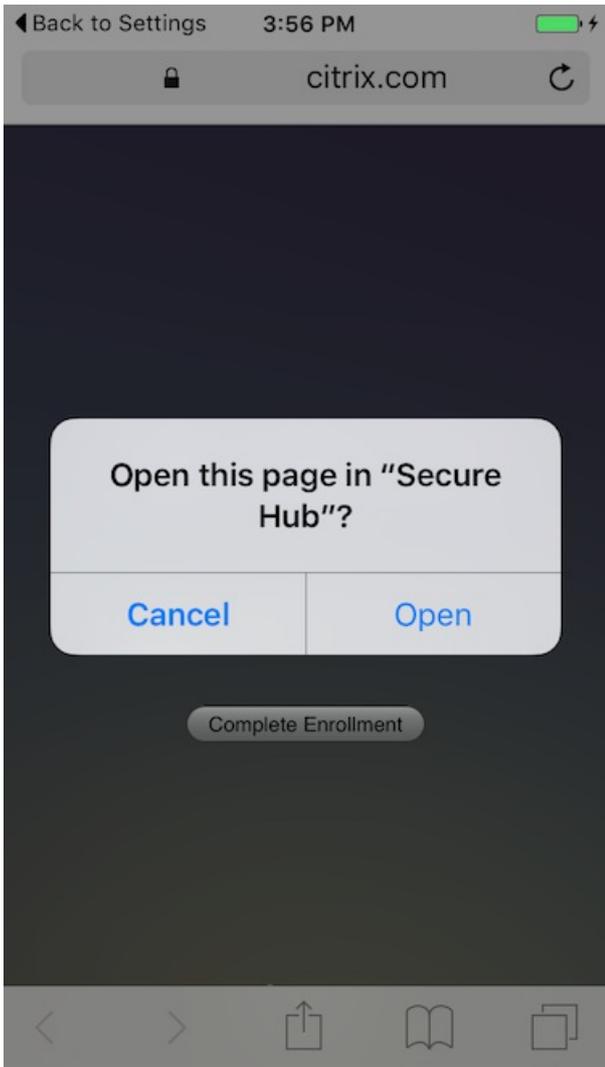
6. Toque en **Instalar** para instalar el servicio de perfiles (Citrix Profile Services).

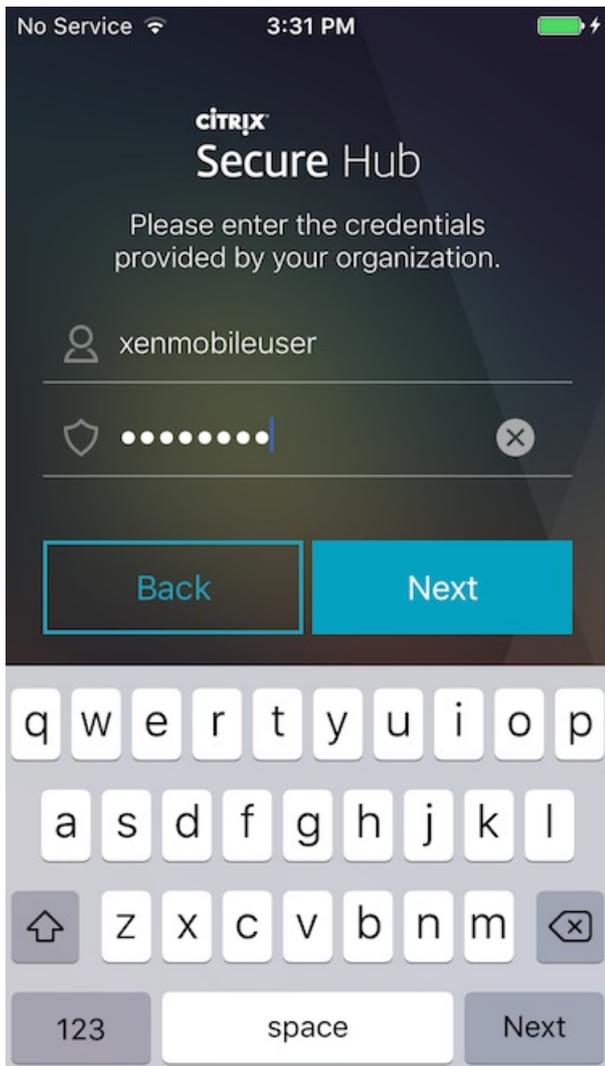


7. Toque en **Trust**.



8. Toque en **Abrir** e introduzca sus credenciales.





## 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/mac/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

En XenMobile, puede inscribir dispositivos que ejecuten los siguientes sistemas operativos Windows:

- Windows 8.1 y Windows 10
- Windows Phone 8.1 y 10

Los usuarios de Windows y Windows Phone se inscriben directamente a través de sus dispositivos.

Debe configurar la detección automática y el servicio de detección de Windows para la inscripción de usuarios con el fin de permitir la administración de dispositivos Windows y Windows Phone.

### Nota

Para que los dispositivos Windows se puedan inscribir, el certificado SSL de escucha debe ser un certificado público. La inscripción falla si se ha cargado un certificado SSL autofirmado.

### Para inscribir dispositivos Windows con detección automática

Los usuarios pueden inscribir dispositivos que ejecutan Windows RT 8.1, versiones de 32 y 64 bits de Windows 8.1 Pro y Windows 8.1 Enterprise, así como Windows 10. Para habilitar la administración de dispositivos Windows, Citrix recomienda configurar la detección automática y el servicio de detección de Windows. Para obtener más información, consulte [Para activar la detección automática en XenMobile para la inscripción de usuarios](#).

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows. Este paso es particularmente importante cuando se actualiza Windows de 8 a 8.1, porque es posible que no se notifique automáticamente a los usuarios de todas las actualizaciones disponibles.

2. En el menú de accesos, toque en Configuración y luego:

- Para Windows 8.1, toque en Configuración de PC > Red > Área de trabajo.
- Para Windows 10, toque en Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio.

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 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 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 inscribir dispositivos Windows sin detección automática**

Puede inscribir dispositivos Windows sin detección automática. Sin embargo, Citrix recomienda configurar la detección automática. La inscripción sin la detección automática consiste en una llamada al puerto 80 antes de conectarse a la URL pertinente, por lo que no se aconseja para una implementación de producción. Citrix recomienda utilizar este proceso solo en entornos de prueba y en el contexto de una implementación de prueba de concepto.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows. Este paso es particularmente importante cuando se actualiza Windows de 8 a 8.1, porque es posible que no se notifique automáticamente a los usuarios de todas las actualizaciones disponibles.

2. En el menú de accesos, toque en **Configuración** y luego:

- Para Windows 8.1, toque en **Configuración de PC > Red > Área de trabajo**.
- Para Windows 10, toque en **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio**.

3. Introduzca la dirección de correo electrónico de empresa.

4. En Windows 10, si no se ha configurado la detección automática, aparecerá una opción donde podrá introducir datos del servidor, como se describe en el paso 5. En Windows 8.1, si la opción de **detectar la dirección del servidor automáticamente** está activada, toque en ella para desactivarla.

5. En el campo **Indicar dirección del servidor**:

- Para Windows 8.1, escriba la dirección del servidor en el siguiente formato:  
`https://serverfqdn:8443/serverInstance/Discovery.svc`. Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice ese puerto en lugar de 8443 en esta dirección.
- Para Windows 10, use esta dirección: `https://beta.managedm.com:8443/zdm/wpe`. Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice ese puerto en lugar de 8443 en esta dirección.

6. Introduzca la contraseña.

7. 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 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 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 Phone, 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 Phone 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 en **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.

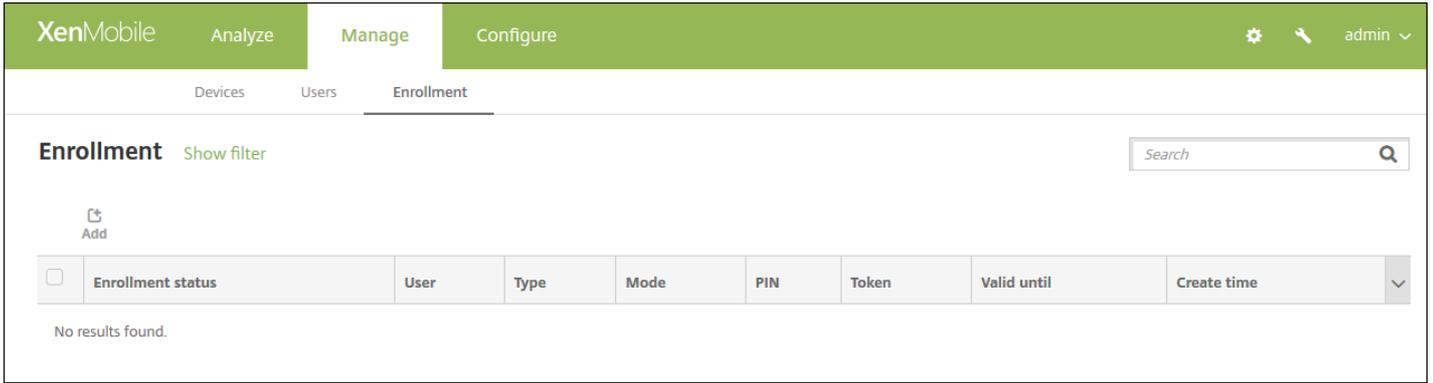
7. En Windows Phone 8.1, en la pantalla **Cuenta agregada**, toque en **listo**.

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**.

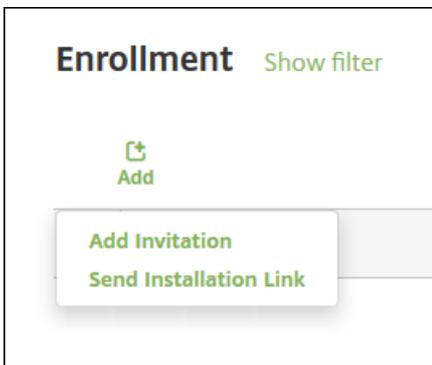
## Envío de una invitación de inscripción

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**. Aparecerá la página **Enrollment**.



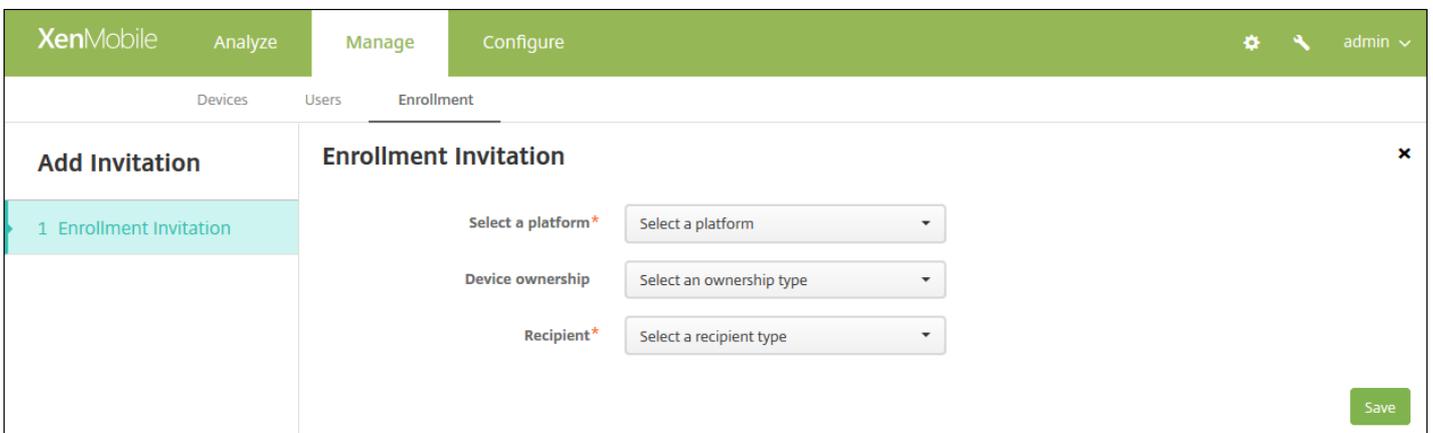
2. Haga clic en **Add**. Aparecerá un menú con opciones de inscripción.



- Para enviar una invitación de inscripción a un usuario o grupo, haga clic en **Add Invitation** y, a continuación, consulte [Para enviar una invitación](#) y siga los pasos ahí indicados para configurar este parámetro.
- Para enviar un enlace de instalación para la inscripción a una lista de destinatarios a través de SMTP o SMS, haga clic en **Send Installation Link** y, a continuación, consulte [Para enviar un enlace de instalación](#) y siga los pasos ahí indicados para configurar este parámetro.

### Para enviar una invitación

1. Haga clic en **Add Invitation**. Aparecerá la pantalla **Enrollment Invitation**.



2. Configure los siguientes parámetros:

- **Select a platform.** En la lista, haga clic en **iOS** o **Android**.
- **Device ownership.** En la lista, haga clic en **Corporate** o **Employee**.
- **Recipient.** En la lista, haga clic en **User** o **Group**.

Podrá ver más opciones para configurar según el destinatario que seleccione. Para la configuración de **User**, consulte [Para enviar una invitación de inscripción a un usuario](#); para la configuración de **Group**, consulte [Para enviar una invitación de inscripción a un grupo](#).

### Para enviar una invitación de inscripción a un usuario

The screenshot shows the XenMobile interface for configuring an enrollment invitation. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, and the 'Enrollment' sub-tab is selected. The main area is titled 'Enrollment Invitation' and contains the following fields:

- Select a platform\***: iOS
- Device ownership**: Corporate
- Recipient\***: User
- User name\***: (empty text field)
- Device info**: Serial number (with an adjacent empty text field)
- Phone number**: (empty text field)
- Carrier**: NONE
- Enrollment mode\***: User name + Password
- Template for agent download**: Select a template
- Template for enrollment URL**: Select a template
- Template for enrollment confirmation**: Select a template
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF (toggle)

A 'Save' button is located at the bottom right of the form.

1. Configure estos parámetros de **User**:

- **User name.** Escriba un nombre de usuario. Este usuario debe existir en el servidor XenMobile como usuario local, o bien como usuario en Active Directory. Si el usuario es local, compruebe que la propiedad de correo electrónico del usuario está configurada para enviarle notificaciones. Si se trata de un usuario de Active Directory, compruebe que el protocolo LDAP está configurado.
- **Device info.** En la lista, haga clic en **Serial number**, UDID o IMEI. Después de elegir una opción, aparece un campo en el que puede escribir el valor correspondiente del dispositivo.
- **Phone number.** Si lo prefiere, escriba el número de teléfono del usuario.

- **Carrier.** En la lista, seleccione un operador al que asociar el número de teléfono del usuario.
- **Enrollment mode.** En la lista, haga clic en la forma en que quiere que los usuarios se inscriban. El valor predeterminado es **User name + Password**. Las opciones posibles son:
  - High Security (Nivel de seguridad alto)
  - Invitation URL (URL de invitación)
  - Invitation URL + PIN (URL de invitación + PIN)
  - Invitation URL + Password (URL de invitación + contraseña)
  - Two Factor (Autenticación de dos factores)
  - Nombre de usuario + PIN

**Nota:** Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment PIN**, donde deberá hacer clic en **Enrollment PIN**.

- **Template for agent download.** En la lista, haga clic en la plantilla que se utilizará para la invitación a la inscripción. Las variantes de esta opción dependen del tipo de plataforma. Por ejemplo, aparecerá **iOS Download Link** como opción si ha seleccionado **iOS** como plataforma.
- **Template for enrollment URL.** En la lista, haga clic en **Enrollment Invitation**.
- **Template for enrollment confirmation.** En la lista, haga clic en **Enrollment Confirmation**.
- **Expire after.** Este campo se establece cuando se configura el modo de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte [Para configurar modos de inscripción](#).
- **Maximum Attempts.** Este campo se establece cuando se configura el modo de inscripción (en **Enrollment Mode**) e indica la cantidad máxima de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte [Para configurar modos de inscripción](#).
- **Send invitation.** Seleccione **ON** para enviar la invitación inmediatamente, o bien haga clic en **OFF** para agregarla solamente a la tabla de la página **Enrollment**.

2. Haga clic en **Save and Send** si ha indicado **Send invitation**; de lo contrario, haga clic en **Save**. La invitación aparecerá en la tabla de la página **Enrollment**.

**Para enviar una invitación de inscripción a un grupo**

The screenshot shows the XenMobile configuration interface for an Enrollment Invitation. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Manage' tab is active, and the 'Enrollment' sub-tab is selected. The main content area is titled 'Enrollment Invitation' and contains the following configuration options:

- Select a platform\***: iOS
- Device ownership**: Corporate
- Recipient\***: Group
- Domain\***: Select a domain
- Group\***: Select a group
- Enrollment mode\***: User name + Password
- Template for agent download**: Select a template
- Template for enrollment URL**: Select a template
- Template for enrollment confirmation**: Select a template
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF

A 'Save' button is located at the bottom right of the form.

1. Configure los siguientes parámetros:

- **Domain.** En la lista, haga clic en el dominio del que se seleccionará el grupo.
- **Group.** En la lista, haga clic en el grupo que recibirá la invitación.
- **Enrollment mode.** En la lista, haga clic en la forma en que quiere que los usuarios del grupo se inscriban. El valor predeterminado es **User name + Password**. Las opciones posibles son:
  - High Security (Nivel de seguridad alto)
  - Invitation URL (URL de invitación)
  - Invitation URL + PIN (URL de invitación + PIN)
  - Invitation URL + Password (URL de invitación + contraseña)
  - Two Factor (Autenticación de dos factores)
  - Nombre de usuario + PIN

**Nota:** Cuando seleccione un modo de inscripción que incluya un PIN, aparecerá el campo **Template for enrollment PIN**, donde deberá hacer clic en **Enrollment PIN**.

- **Template for agent download.** En la lista, haga clic en la plantilla que se utilizará para la invitación a la inscripción. Las variantes de esta opción dependen del tipo de plataforma. Por ejemplo, aparecerá **iOS Download Link** como opción si ha seleccionado **iOS** como plataforma.
- **Template for enrollment URL.** En la lista, haga clic en **Enrollment Invitation**.
- **Template for enrollment confirmation.** En la lista, haga clic en **Enrollment Confirmation**.
- **Expire after.** Este campo se establece cuando se configura el modo de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte [Para configurar modos de](#)

inscripción.

- **Maximum Attempts.** Este campo se establece cuando se configura el modo de inscripción e indica la cantidad máxima de veces que se da el proceso de inscripción. Para obtener más información sobre cómo configurar modos de inscripción, consulte [Para configurar modos de inscripción](#).
- **Send invitation.** Seleccione **ON** para enviar la invitación inmediatamente, o bien haga clic en **OFF** para agregarla solamente a la tabla de la página **Enrollment**.

2. Haga clic en **Save and Send** si ha indicado **Send invitation**; de lo contrario, haga clic en **Save**. La invitación aparecerá en la tabla de la página **Enrollment**.

### Para enviar un enlace de instalación

The screenshot shows the 'Send Installation Link' configuration interface in XenMobile. The interface includes a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Manage' tab is active, and the 'Enrollment' sub-tab is selected. The main content area is split into two panes: 'Send Link' (left) and 'Send Installation Link' (right). The 'Send Installation Link' pane contains a 'Recipients' section with 'Email\*' and 'Phone number\*' input fields and an 'Add' button. Below this is a 'Channels' section with two options: 'SMTP' and 'SMS'. Both channels have a warning message: 'Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.' and 'Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.' respectively. The 'SMTP' section has fields for 'Sender', 'Subject' (pre-filled with 'Enroll Your Device'), and 'Message' (pre-filled with 'Enroll your device to gain access to company email and intranet. For instructions visit: \${zdmserver.hostPath}/enroll'). The 'SMS' section has a 'Message' field (pre-filled with 'Download XenMobile Agent: \${zdmserver.hostPath}/enroll'). A 'Send' button is located at the bottom right of the configuration area.

Antes de enviar un enlace de instalación para la inscripción, debe configurar canales (SMTP o SMS) en el servidor de notificaciones. Puede hacerlo desde la página **Settings**. Para obtener más información, consulte [Notificaciones](#).

1. Configure los siguientes parámetros:

- **Recipient.** Para cada destinatario que quiera agregar, haga clic en "Add" y lleve a cabo lo siguiente:

- **Email.** Escriba la dirección de correo electrónico del destinatario. Este campo es obligatorio.
- **Phone number.** Escriba el número de teléfono del destinatario. Este campo es obligatorio.
- Haga clic en **Guardar**.

**Nota:** Para eliminar un destinatario existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un destinatario existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Channels.** Seleccione el canal que se va a usar para enviar el enlace de instalación para la inscripción. Puede enviar notificaciones a través de **SMTP** o **SMS**. Estos canales no se pueden activar hasta que se configuren los parámetros de servidor en la página **Settings**, en **Notification Server**. Para obtener más información, consulte [Notificaciones](#).
- **SMTP.** Si quiere, configure estos parámetros. Si no escribe nada en estos campos, se utilizarán los valores predeterminados que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
  - **Sender.** Si lo prefiere, escriba un remitente.
  - **Subject.** Aquí puede escribir un asunto para el mensaje. Por ejemplo: "Inscriba su dispositivo".
  - **Message.** Si quiere, escriba el mensaje que se enviará al destinatario. Por ejemplo: "Inscriba su dispositivo para tener acceso a las aplicaciones y al correo electrónico de la organización".
- **SMS.** Configure este parámetro. Si no escribe nada en este campo, se utilizará el valor predeterminado que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
  - **Message.** Escriba el mensaje que se enviará a los destinatarios. Este campo es obligatorio para las notificaciones por SMS.

**Nota:** En Norteamérica, los mensajes SMS que superen los 160 caracteres se entregan en varios mensajes.

2. Haga clic en **Send**.

## Nota

Si su entorno hace uso de los nombres `SAMAccountName`, después de que los usuarios reciben la invitación y hacen clic en el enlace, deben modificar el nombre de usuario para completar la autenticación. Por ejemplo, tienen que quitar la parte de `nombre_de_dominio` de `SAMAccountName@nombre_de_dominio.com`.

# Límite de inscripción de dispositivos

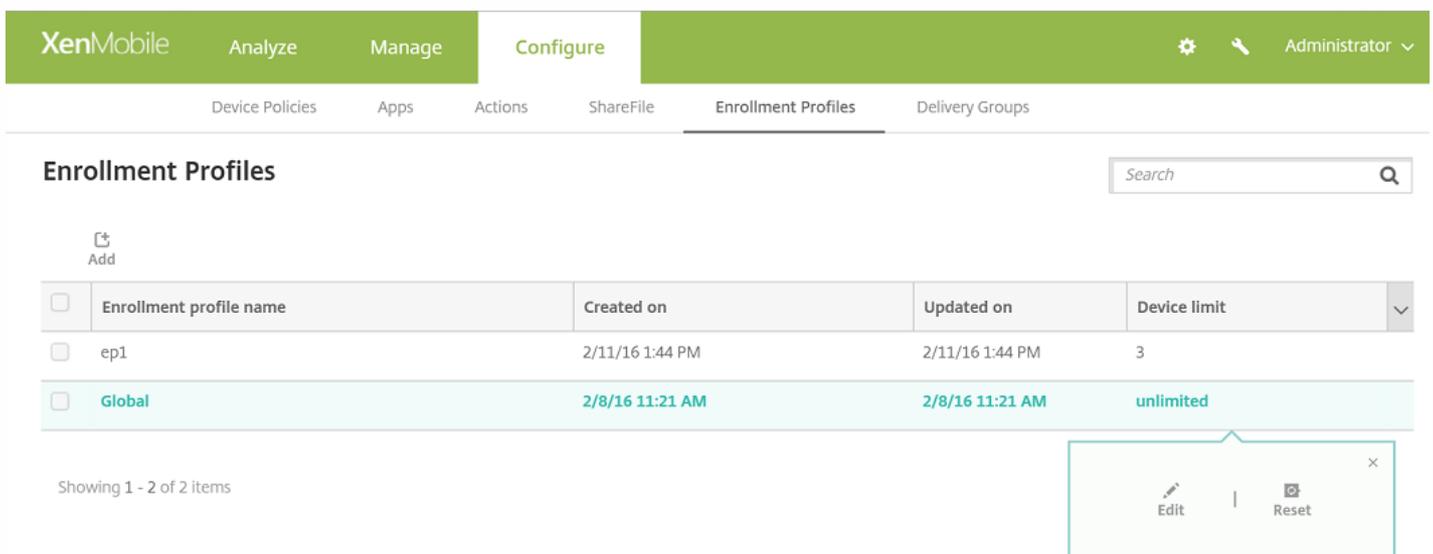
Mar 02, 2017

Puede limitar el número de dispositivos que un usuario puede inscribir en **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 **Configurar > Perfiles de inscripción de dispositivos**.
2. Haga clic en **Global** y seleccione **Modificar**.

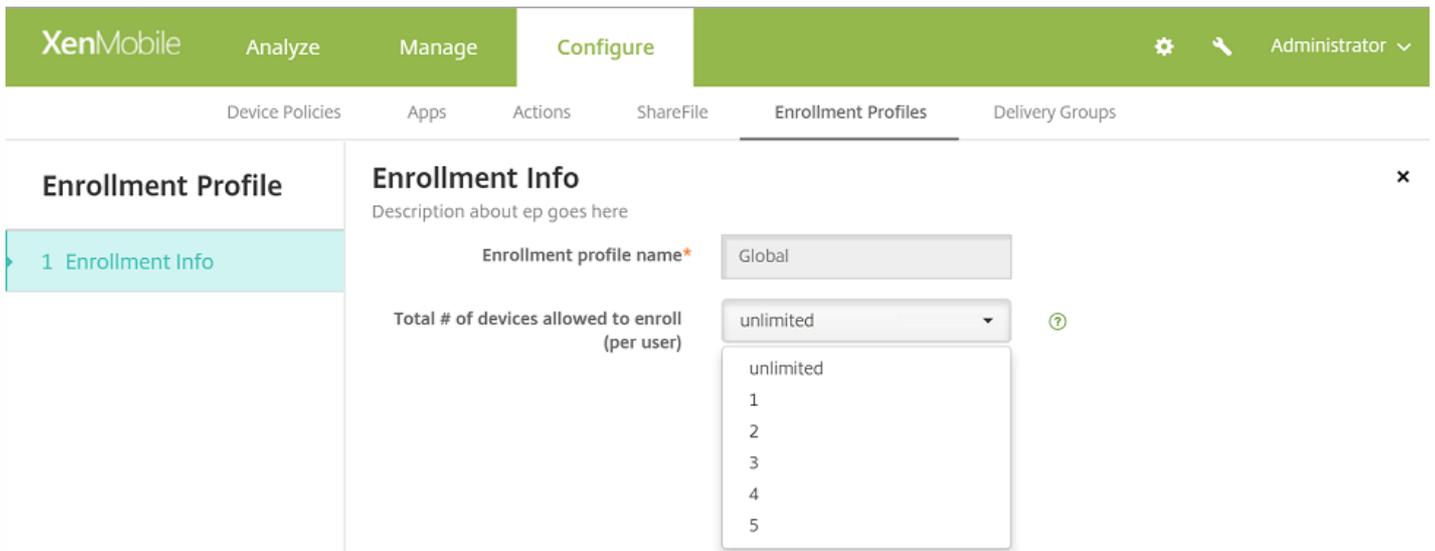


The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Enrollment Profiles' tab is active. A search bar is located in the top right corner. Below the search bar, there is an 'Add' button. The main content area displays a table of enrollment profiles:

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	ep1	2/11/16 1:44 PM	2/11/16 1:44 PM	3
<input type="checkbox"/>	Global	2/8/16 11:21 AM	2/8/16 11:21 AM	unlimited

Below the table, it says 'Showing 1 - 2 of 2 items'. A tooltip is visible over the 'Global' row, containing 'Edit' and 'Reset' buttons.

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

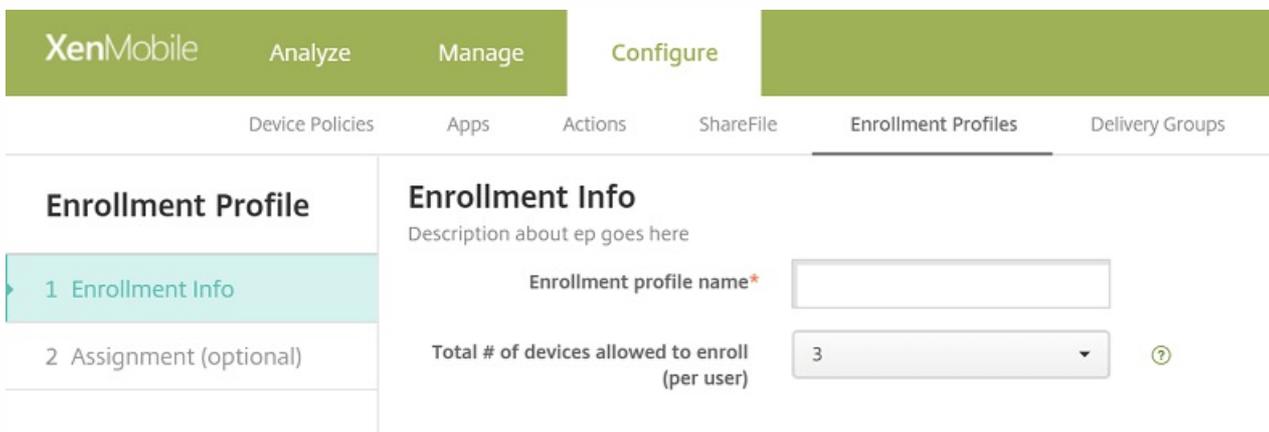


## Para configurar un límite de inscripción de dispositivos para un grupo de entrega

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

Aparecerá la pantalla **Información de inscripción**.

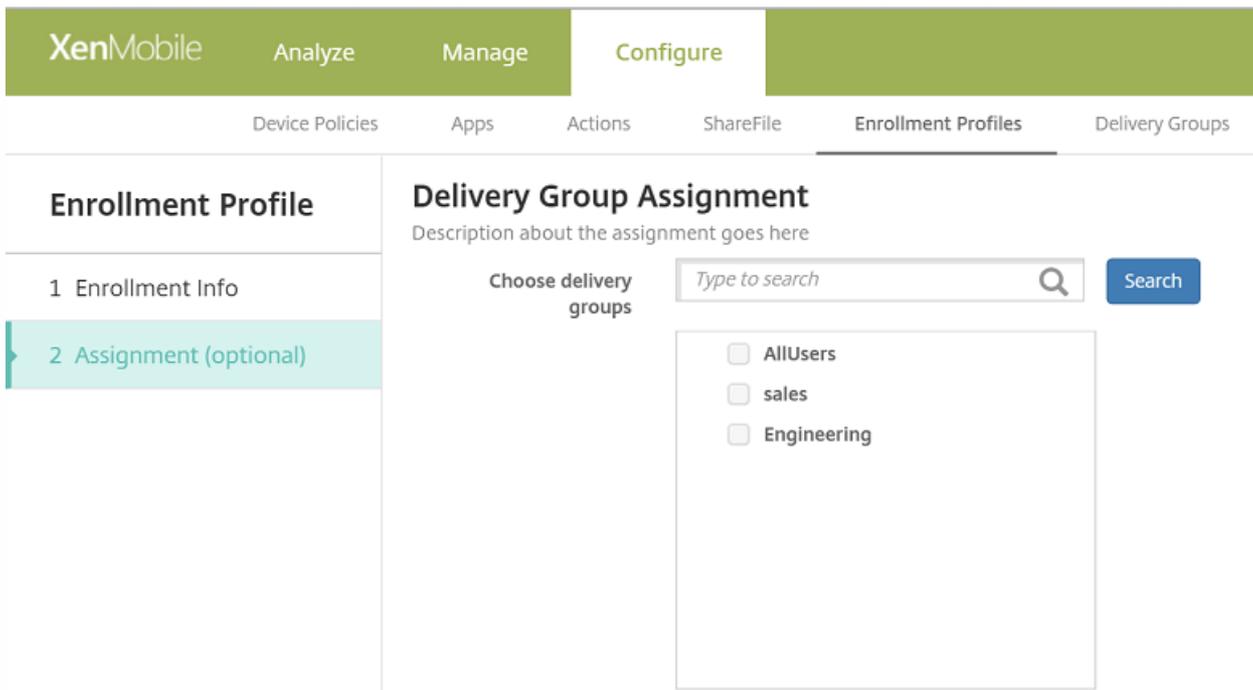
2. Escriba un nombre para el nuevo perfil de inscripción y, a continuación, seleccione el número de dispositivos que podrán inscribir los miembros de este perfil.



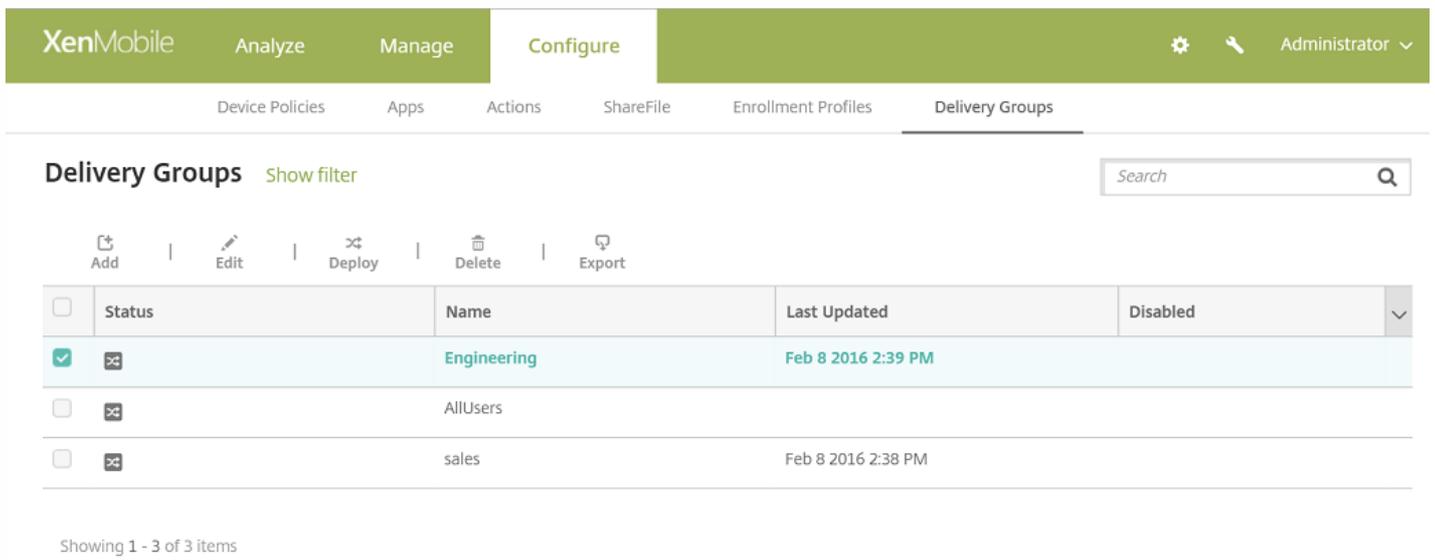
3. Haga clic en **Siguiente**.

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

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



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



Aparecerá la pantalla **Perfil de inscripción**.

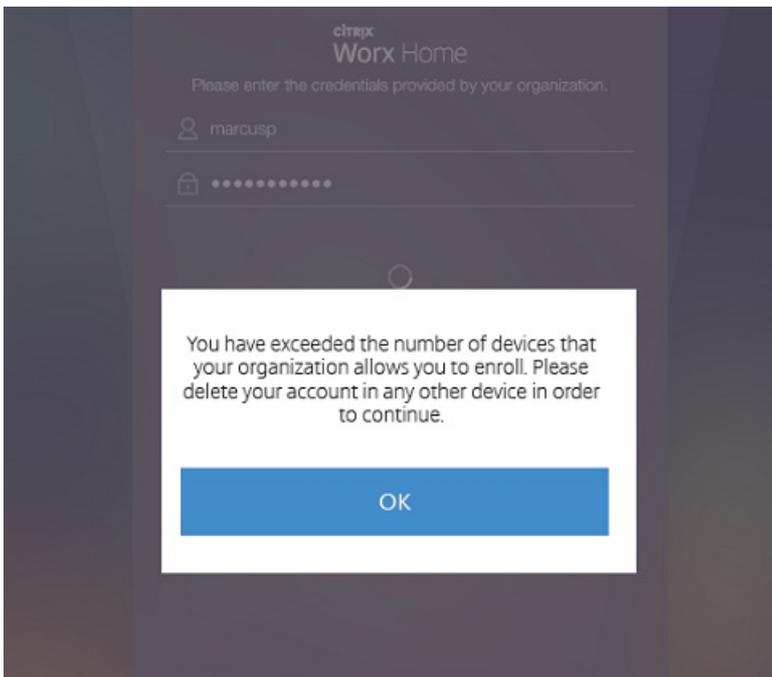
5. Desde esta pantalla, seleccione el perfil de inscripción que desea aplicar a este grupo de entrega y, a continuación, haga clic en **Siguiente** para ver y guardar los cambios.

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' sub-tab is selected. On the left side, there is a 'Delivery Group' sidebar with a list of steps: '1 Delivery Group Info', '2 User', '3 Resource (optional)', 'Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profile' (highlighted in teal), and '4 Summary'. The main content area is titled 'Enrollment Profile' and contains the instruction: 'Select the enrollment profile that you want the users in this delivery group to see'. Below this instruction, there are three radio button options: 'ep1', 'ep2', and 'Global' (which is selected). At the bottom right of the main content area, there are two buttons: 'Back' and 'Next >'. The 'Next >' button is highlighted in green.

## Experiencia del usuario con un límite de inscripción de dispositivos

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

1. Iniciar sesión en Secure Hub.
2. Escribir la dirección de servidor que se inscribirá.
3. Escribir las credenciales.
4. Si se alcanza el límite de dispositivos, aparece un mensaje de error que indica que se ha excedido el límite de registros de dispositivos y que se debe contactar con un administrador.



Aparece de nuevo la pantalla de inscripción de Secure Hub.

# Dispositivos compartidos

Mar 02, 2017

XenMobile permite configurar los dispositivos que se pueden compartir entre varios usuarios. La función de dispositivos compartidos permite, por ejemplo, que los médicos, en los hospitales, usen cualquier dispositivo cercano para acceder a las aplicaciones y a los datos, en lugar de tener que llevar encima un dispositivo concreto. También puede interesarle intercambiar dispositivos en ámbitos judiciales, comerciales y de fabricación para compartir los dispositivos entre sí y, de esta manera, reducir costes de equipamiento.

## Puntos clave sobre dispositivos compartidos

### Modo MDM

- Disponible en teléfonos y tabletas iOS y Android. No se admite la inscripción básica del Device Enrollment Program (DEP) para dispositivos compartidos de XenMobile Enterprise. Debe utilizar una inscripción autorizada de DEP para inscribir un dispositivo compartido en este modo.
- No se admiten: la autenticación de certificados de cliente, el PIN de Citrix, Touch ID, la autenticación de dos factores ni la entropía de usuario.

### Modo MDM+MAM

- Disponible solo en tabletas iOS y Android.
- Respaldo 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](#).

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 dispositivo compartido denominado **Shared Device Enrollment User** con permisos de **Shared devices enroller** en **Authorized Access**. Expanda **Devices**, en la sección **Console features** y, a continuación, seleccione **Selective Wipe device**. Esta configuración garantiza que las aplicaciones y las directivas aprovisionadas mediante la cuenta de inscripción de dispositivos compartidos se eliminen a través de 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 de Active Directory específicos con **To specific user groups**.

Settings > Role-Based Access Control > Add Role

### Add Role

- 1 Role Info
- 2 Assignment

### Role Info

RBAC name\*

RBAC template Apply

Authorized access

- Admin console access
- Self Help Portal access
- Shared devices enroller
- Remote Support access
- Public api access

Console features

- Dashboard
- Reporting
- Devices
  - Full Wipe device
  - Clear Restriction
  - Selective Wipe device
  - View locations
  - Lock device
  - Unlock device

Apply permissions

To all user groups  
 To specific user groups

Next >

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.

Settings > Role-Based Access Control > Add Role

### Add Role

- 1 Role Info
- 2 Assignment

### Assignment

Assign the RBAC role to user groups

Select domain

Include user groups  Search

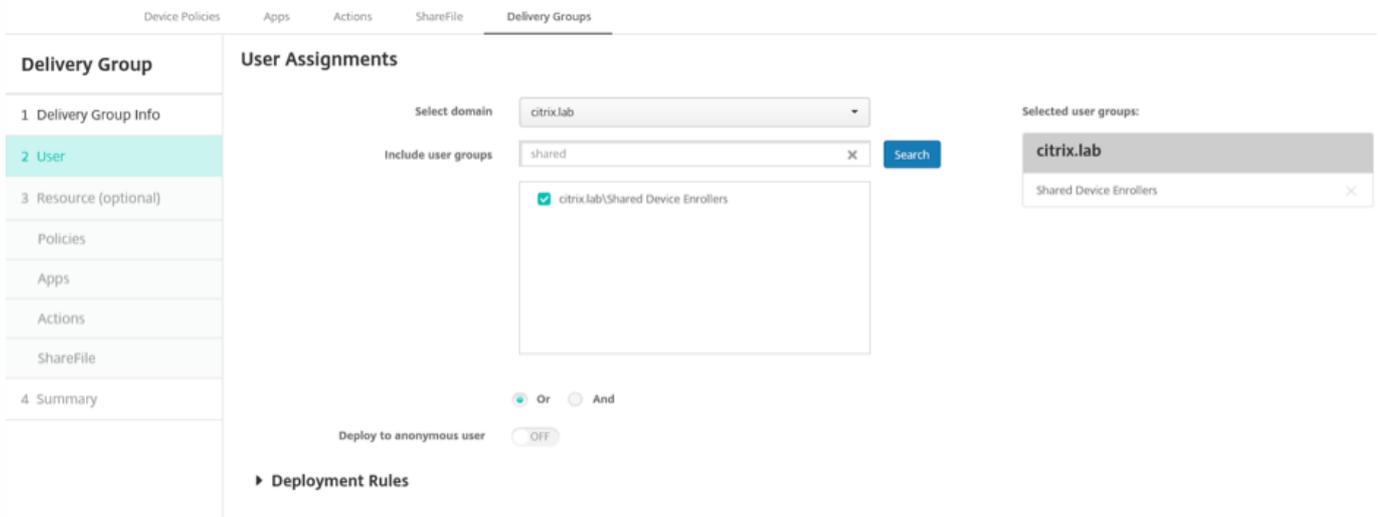
citrix.lab\Shared Device Enrollers

Selected user groups:

citrix.lab
×

Shared Device Enrollers
×

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 inscribalo 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 y que se haya implementado solo en dispositivos compartidos. Al crear los grupos, configure reglas de implementación para que los paquetes se implementen en dispositivos compartidos. Para obtener más información, consulte [Configuración de reglas de implementación](#).

7. Si quiere dejar de compartir el dispositivo, realice un borrado selectivo para quitar la cuenta del usuario de inscripción de dispositivos compartidos del dispositivo, junto con las aplicaciones y las directivas que se han implementado en él.

## Experiencia de usuario de dispositivos compartidos

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.

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 for Work

Mar 02, 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 respaldados, consulte el sitio Web Google Android Enterprise. 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

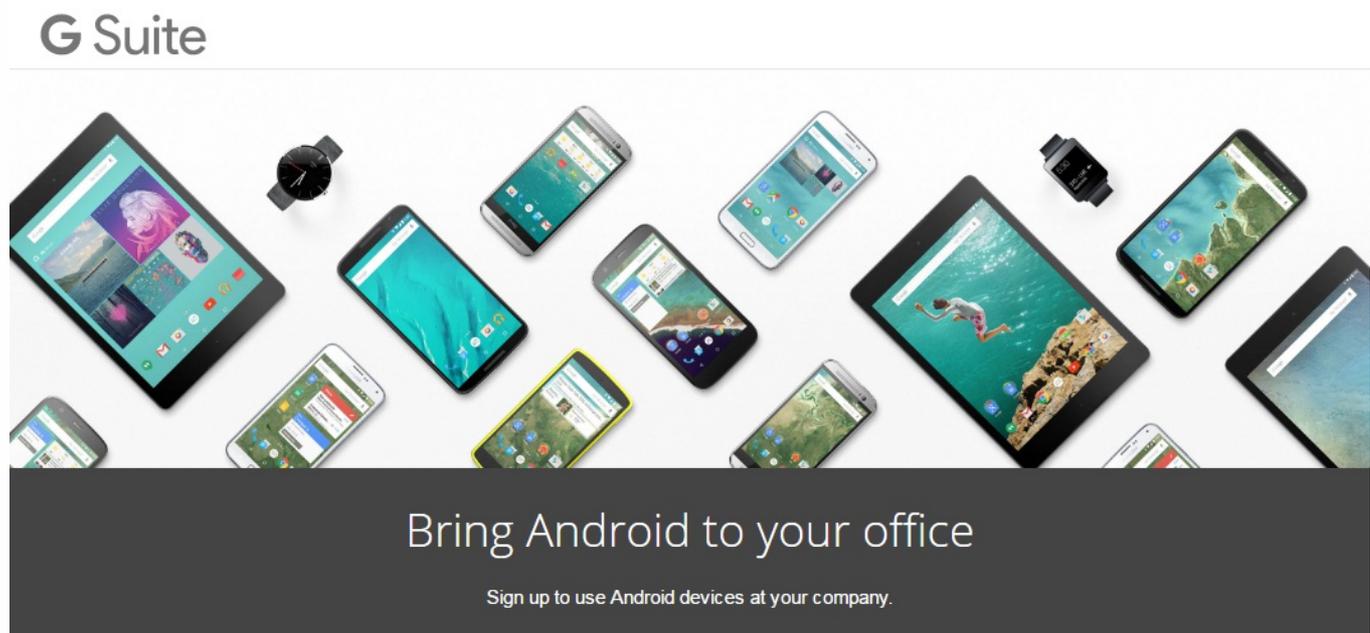
Antes de configurar una cuenta de Android at Work, debe cumplir los siguientes requisitos previos:

- 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](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.



### ① About you

Name

Current work email

Doesn't have to be an official business email.

Phone

2. Introduzca la información de usuario del administrador.

① About you

Name

Justa ✓ User ✓

Current work email Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

2. Escriba la información de la empresa, además de la información de su cuenta de administrador.

② About your business

Business name

EXAMPLE CORP ✓

Business domain address You'll need to verify that you own this domain.

example.com ✓

Number of employees Country/Region

1 employee United States

③ Your Google admin account Why do I need this?

Username Create an account to manage Android for Work

justa.user ✓ @ example.com

Create a password 8-character minimum; case sensitive

..... ✓

..... ✓

Una vez completado el primer paso, verá la página siguiente.



## Bring Android to your office

With Android, you can manage your company's devices and keep them secure.



Create your domain admin account



Verify domain ownership

Verify you're the owner of your company's domain and protect its security.

START



Connect with your provider

Allow an enterprise mobility management (EMM) provider to keep your organization's devices secure.

## 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**.

## Verify domain ownership

Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

**Note:** Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

## Verify domain ownership

### Verification checklist

Follow these steps to help Google verify that you own the domain **example.com**.

[Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

[VERIFY](#)

3. Google verifica que usted es el propietario del dominio.

## Verify domain ownership

### Verifying your domain ownership

The domain host is updating your information. This might take a bit—you can close this window and come back to [admin.google.com](http://admin.google.com) later without interrupting the process.

[Learn more](#)

Estimated time remaining: 5 minutes

---

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.

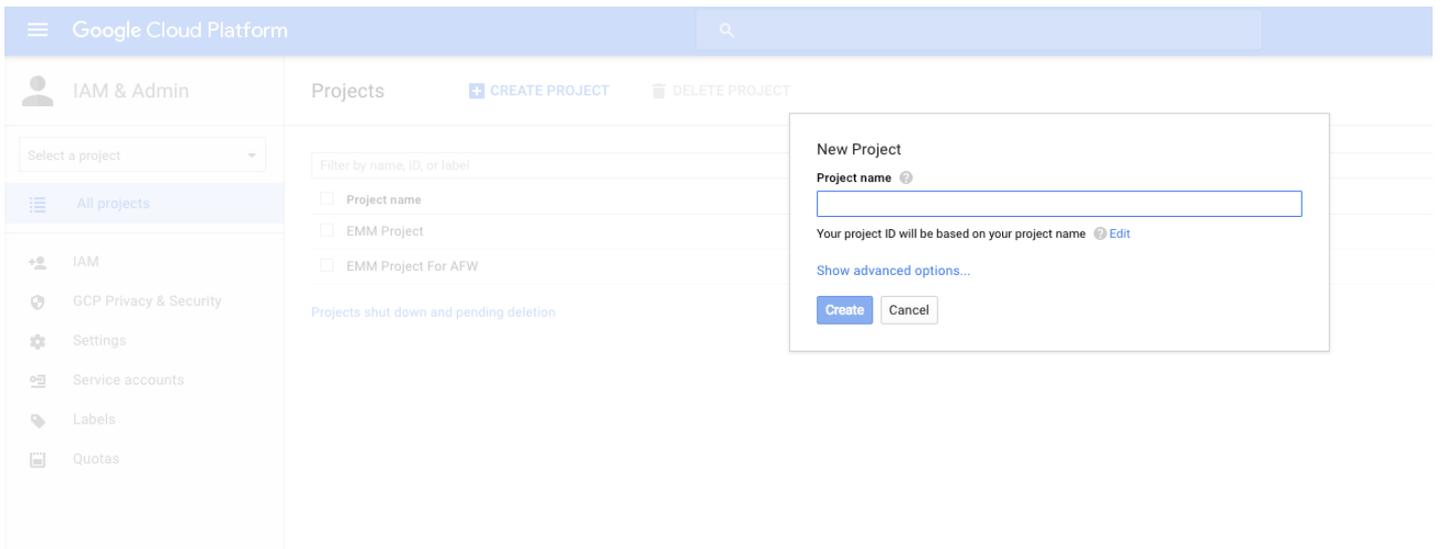
## Configuración de una cuenta de servicio de Android at Work y descarga de un certificado de Android at Work

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>.

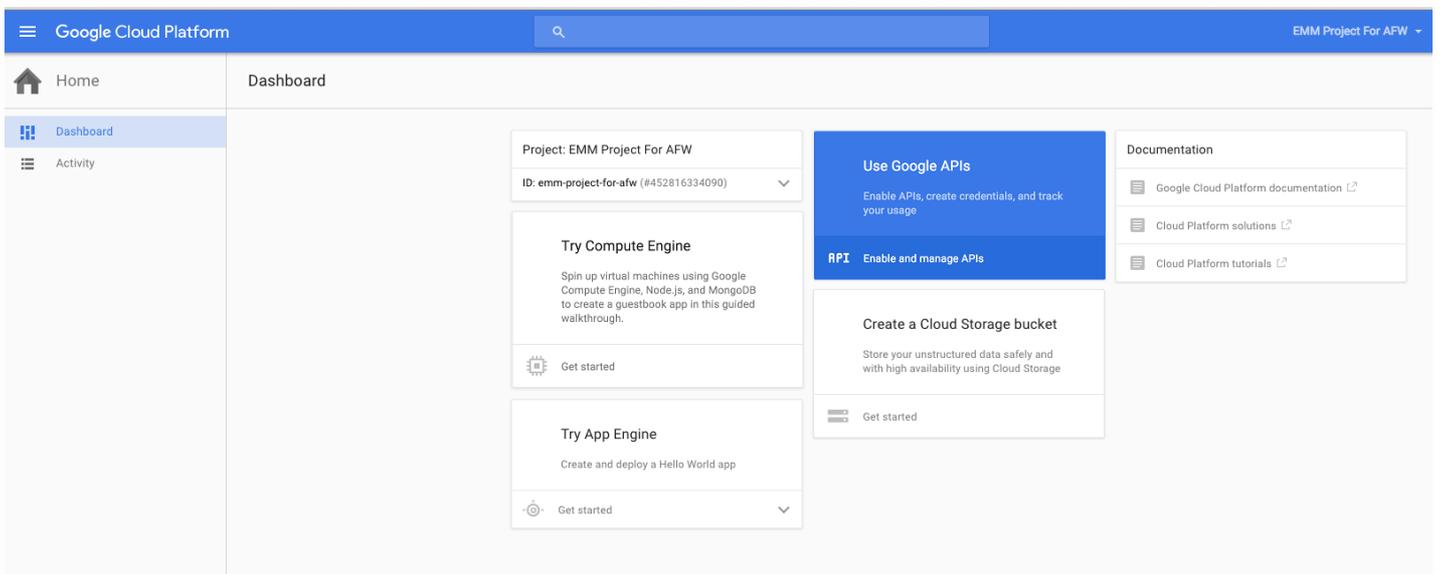
1. En un explorador Web, vaya a <https://console.cloud.google.com/project> e inicie sesión con las credenciales de administración de Google.
2. En la lista **Projects**, haga clic en **Create Project**.

Project name	Project ID
<input type="checkbox"/> EMM Project	emm-project-1287
<input type="checkbox"/> EMM Project For AFW	emm-project-for-afw

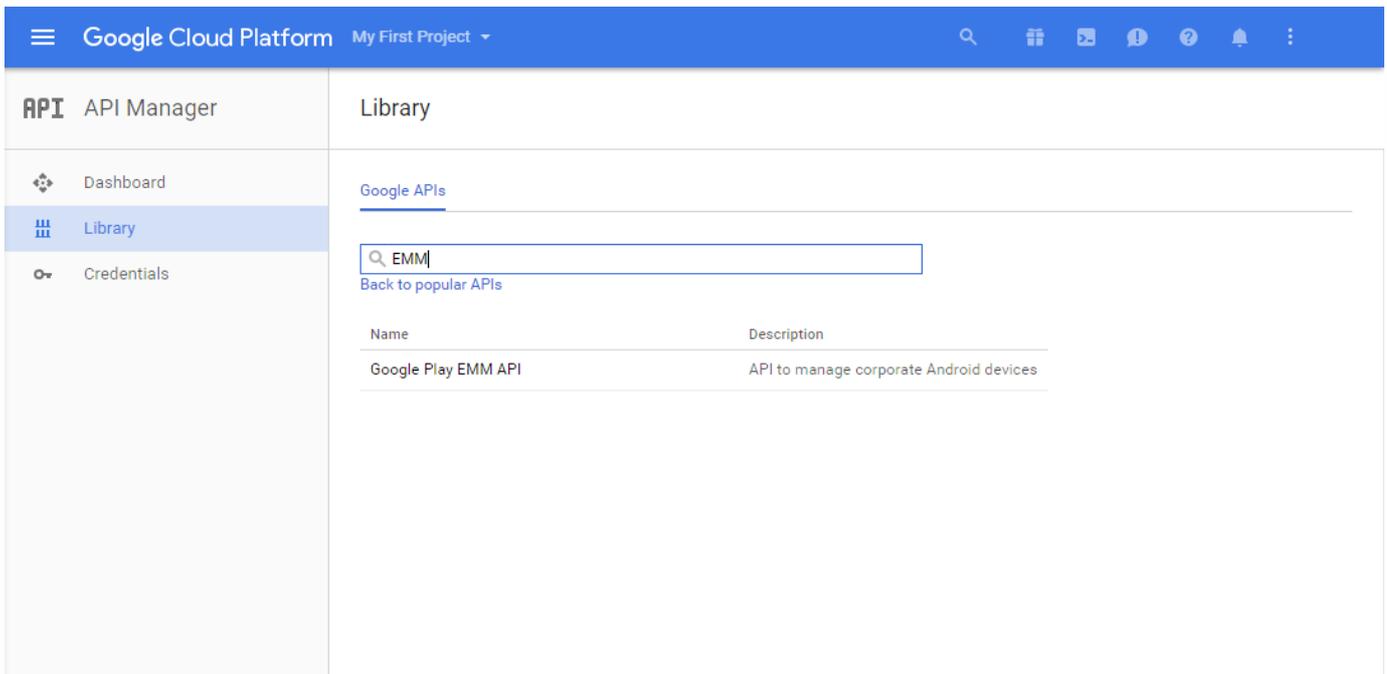
3. En **Project name**, introduzca un nombre para el proyecto.



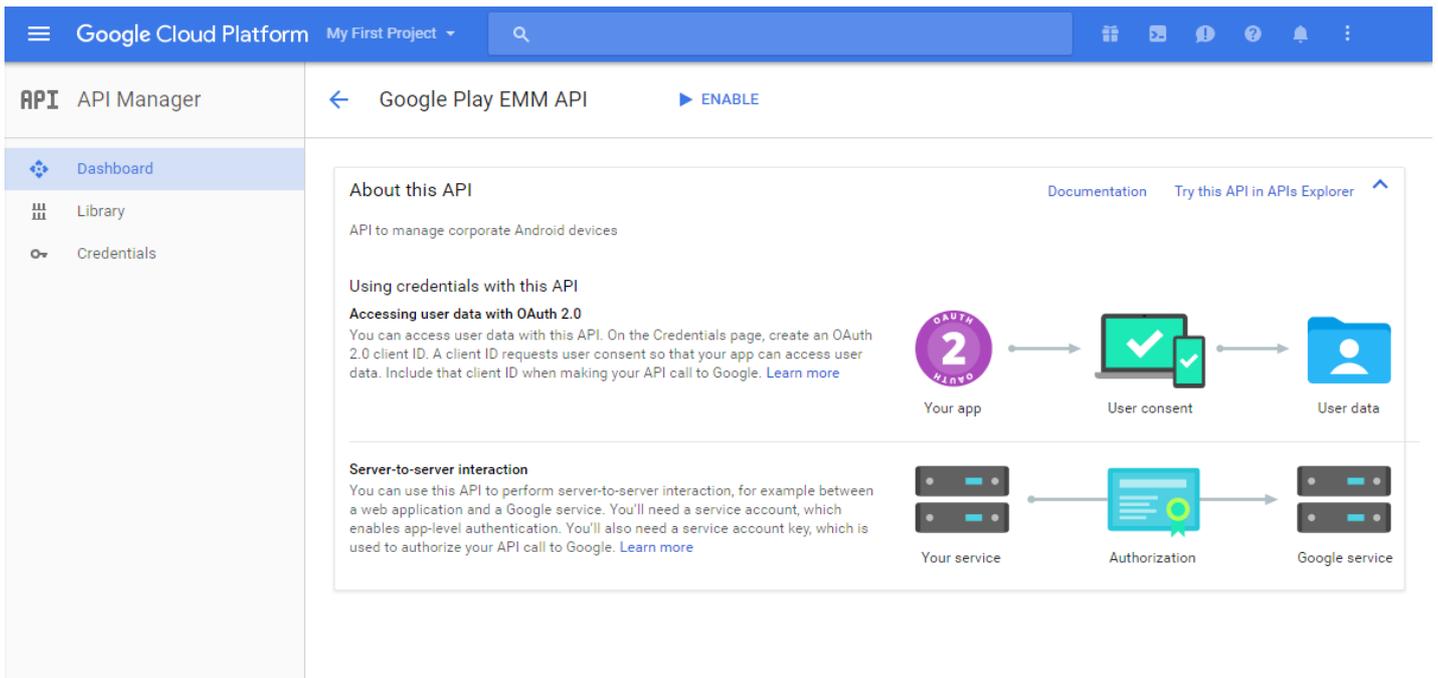
4. En el panel de mandos, haga clic en **Use Google APIs**.



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**.

Google Cloud Platform EMM Project For APW

API API Manager

Overview

← Disable

**Google Play EMM API**

⚠ This API is enabled, but you can't use it in your project until you create credentials. Click "Go to Credentials" to do this now (strongly recommended). [Go to Credentials](#)

Overview Usage Quotas

API to manage corporate Android devices  
[Learn more](#)  
[Try this API in APIs Explorer](#)

**Using credentials with this API**

**Accessing user data with OAuth 2.0**  
 You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. [Learn more](#)

```

  graph LR
    A[Your app] --> B[User consent]
    B --> C[User data]
  
```

**Server-to-server interaction**  
 You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. [Learn more](#)

```

  graph LR
    A[Your service] --> B[Authorization]
    B --> C[Google service]
  
```

8. En la lista **Add credentials to our project**, en el paso 1, haga clic en **service account**.

Google Cloud Platform

API API Manager

Credentials

**Add credentials to your project**

1 Find out what kind of credentials you need

We'll help you set up the correct credentials  
 If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

**Which API are you using?**  
 Determines what kind of credentials you need.

Google Play EMM API

**Where will you be calling the API from?**  
 Determines which settings you'll need to configure.

Choose...

**What data will you be accessing?**

User data  
 Access data belonging to a Google user, with their permission

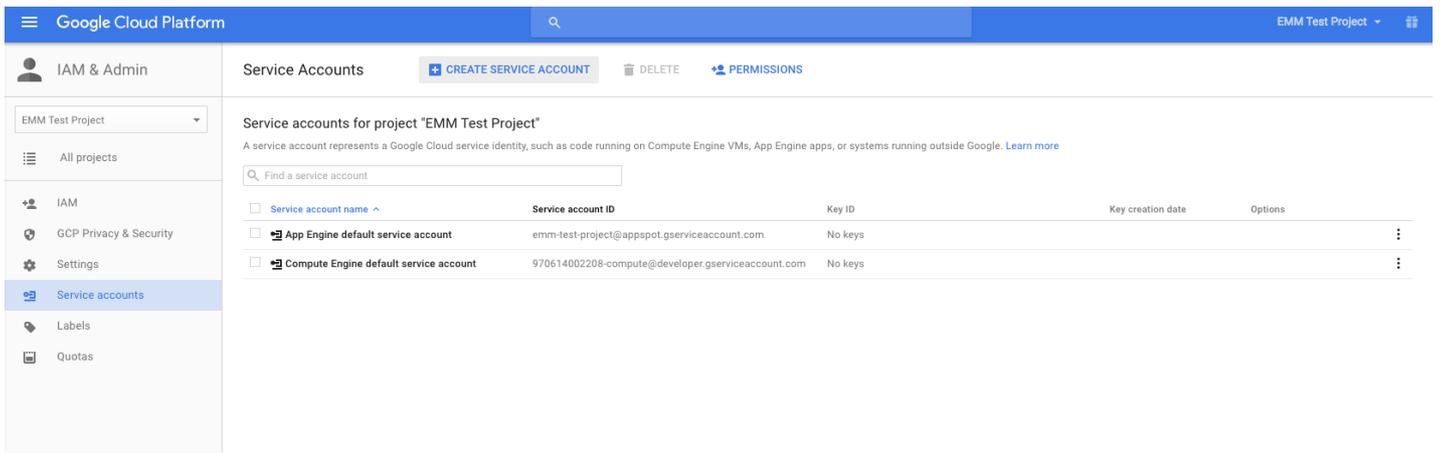
Application data  
 Access data belonging to your own application

[What credentials do I need?](#)

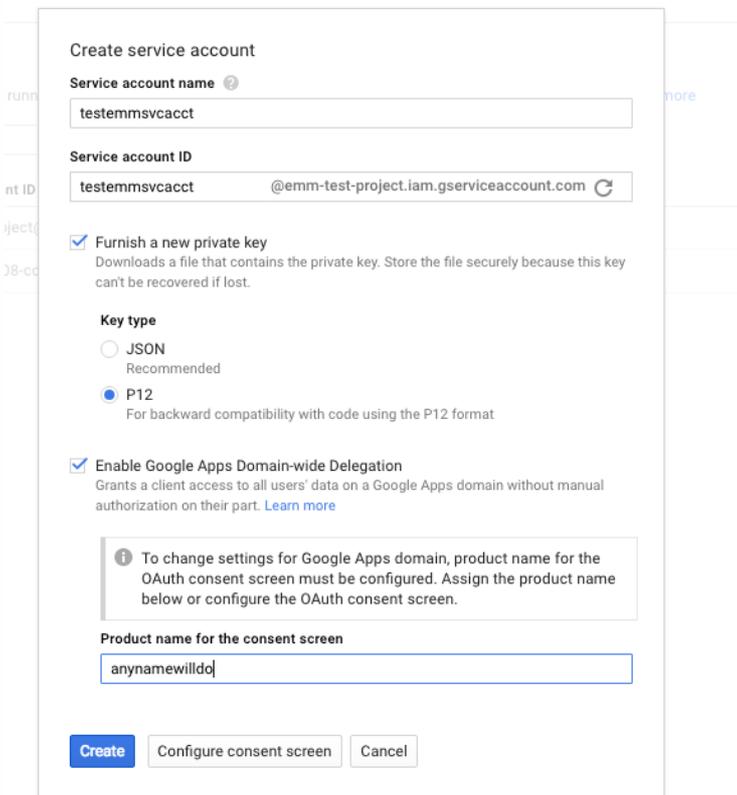
2 Get your credentials

Cancel

9 En la página **Service Accounts**, haga clic en **Create Service Account**.

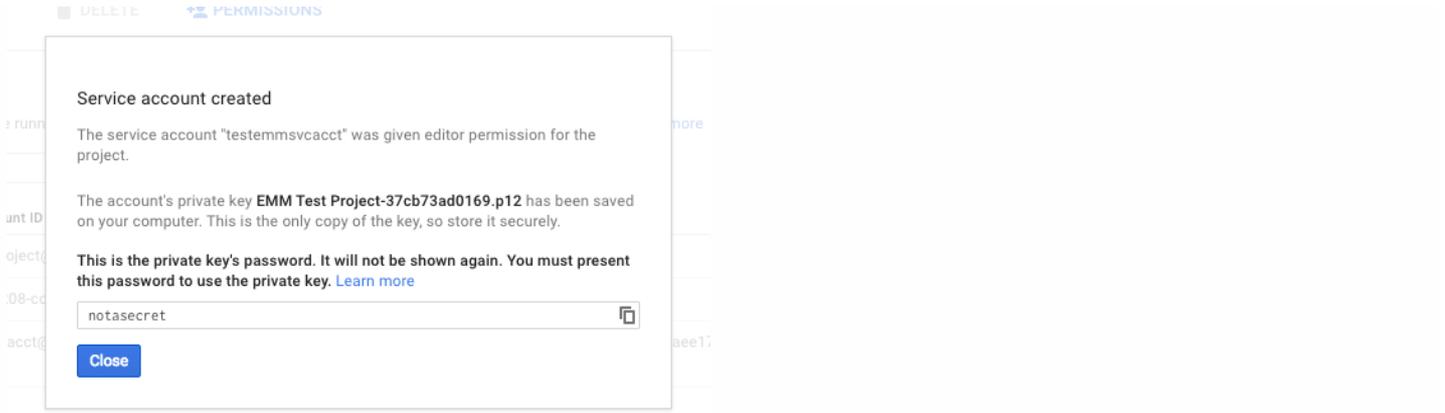


10. En **Create service account**, establezca un nombre para la cuenta y marque la casilla **Furnish a new private key**. Haga clic en **P12**, marque la casilla **Enable Google Apps Domain-wide Delegation** y haga clic en **Create**.

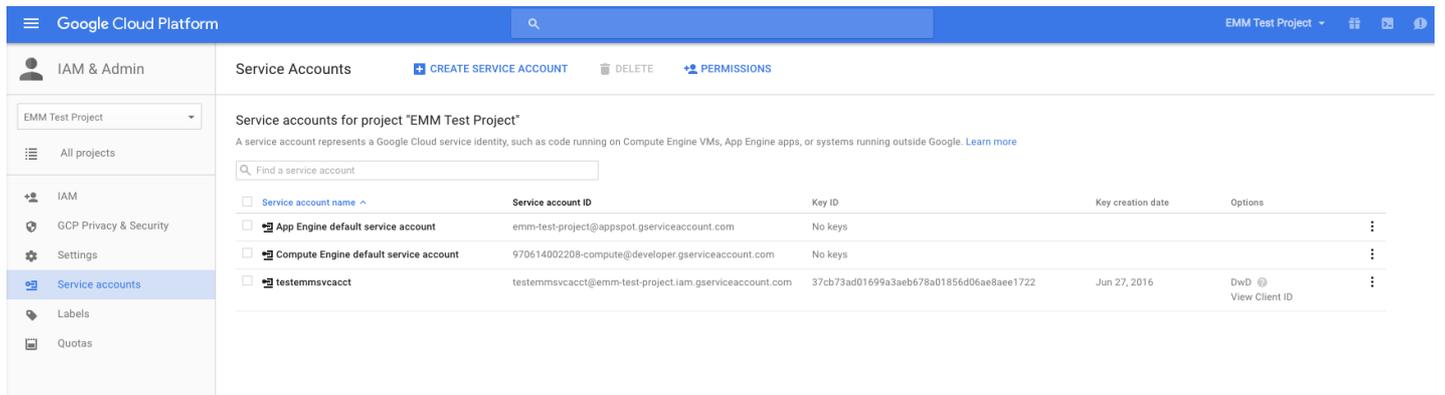


El archivo de certificado (P12) se descargará en su equipo. Guarde el certificado en una ubicación segura.

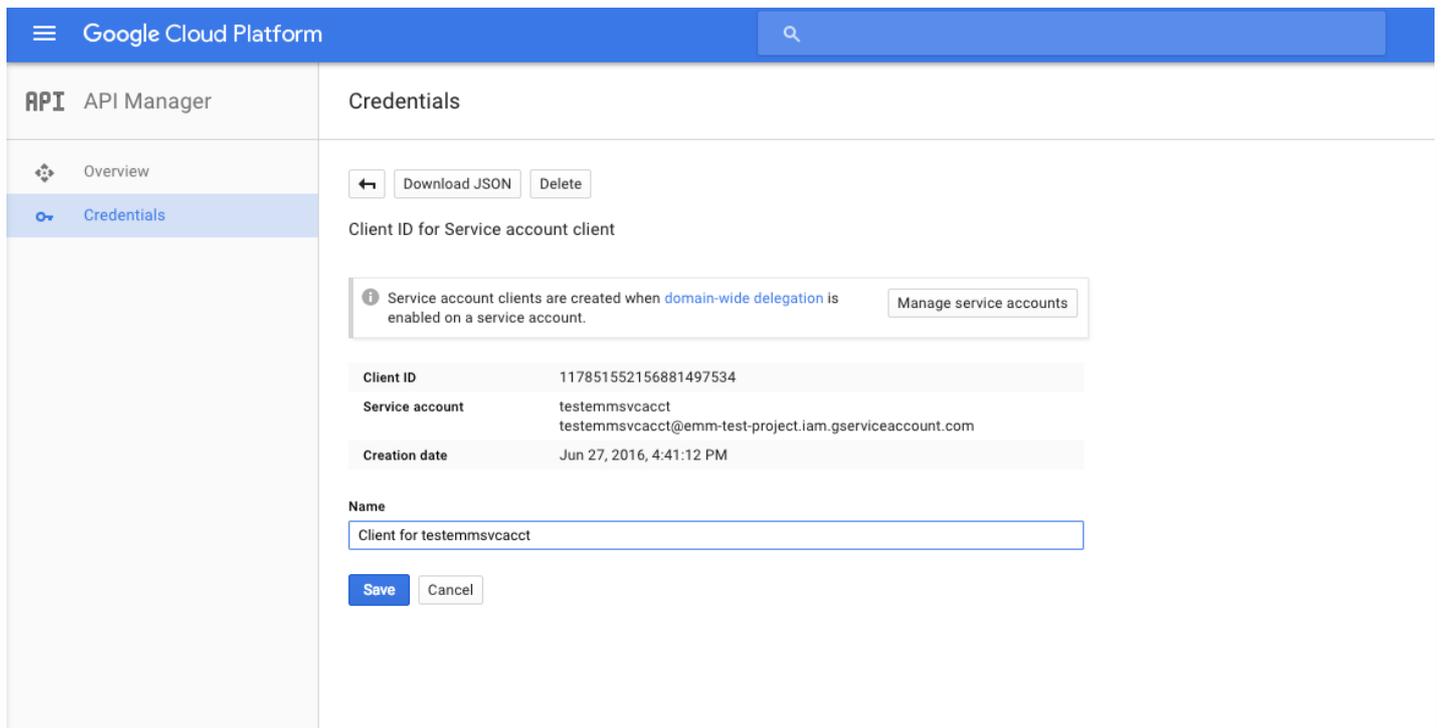
11. En la pantalla de confirmación **Service account created**, haga clic en **Close**.



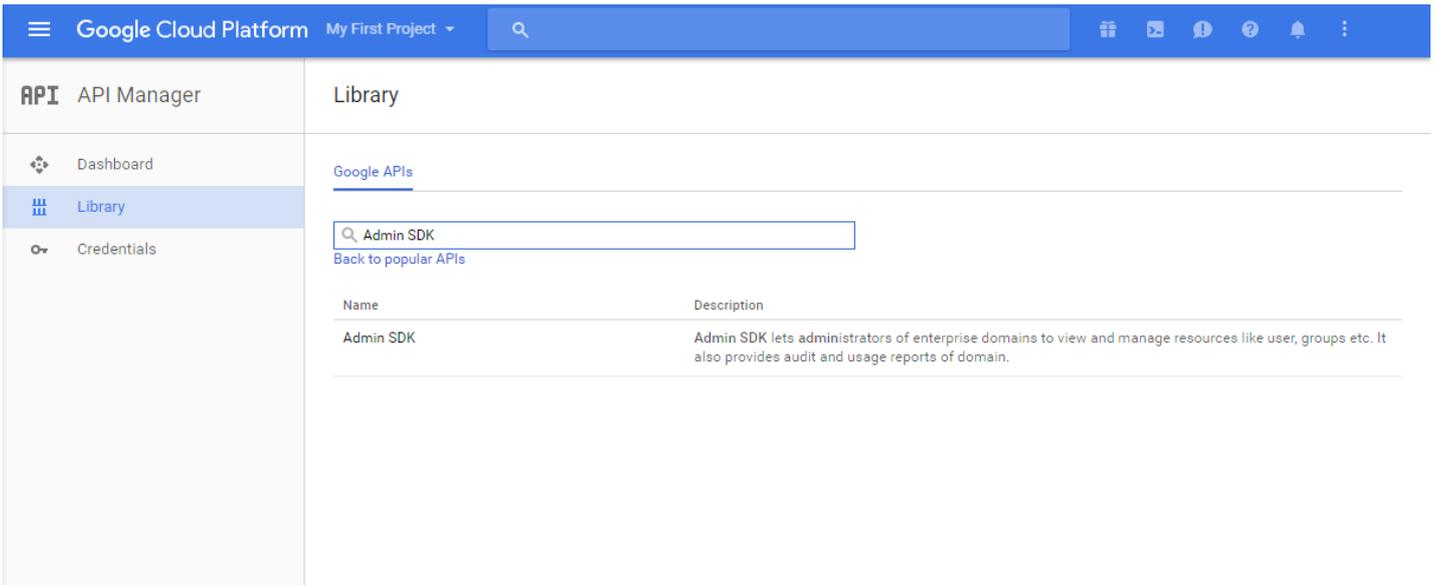
12. En **Permissions**, haga clic en **Service accounts** y, en **Options** para su cuenta de servicio, haga clic en **View Client ID**.



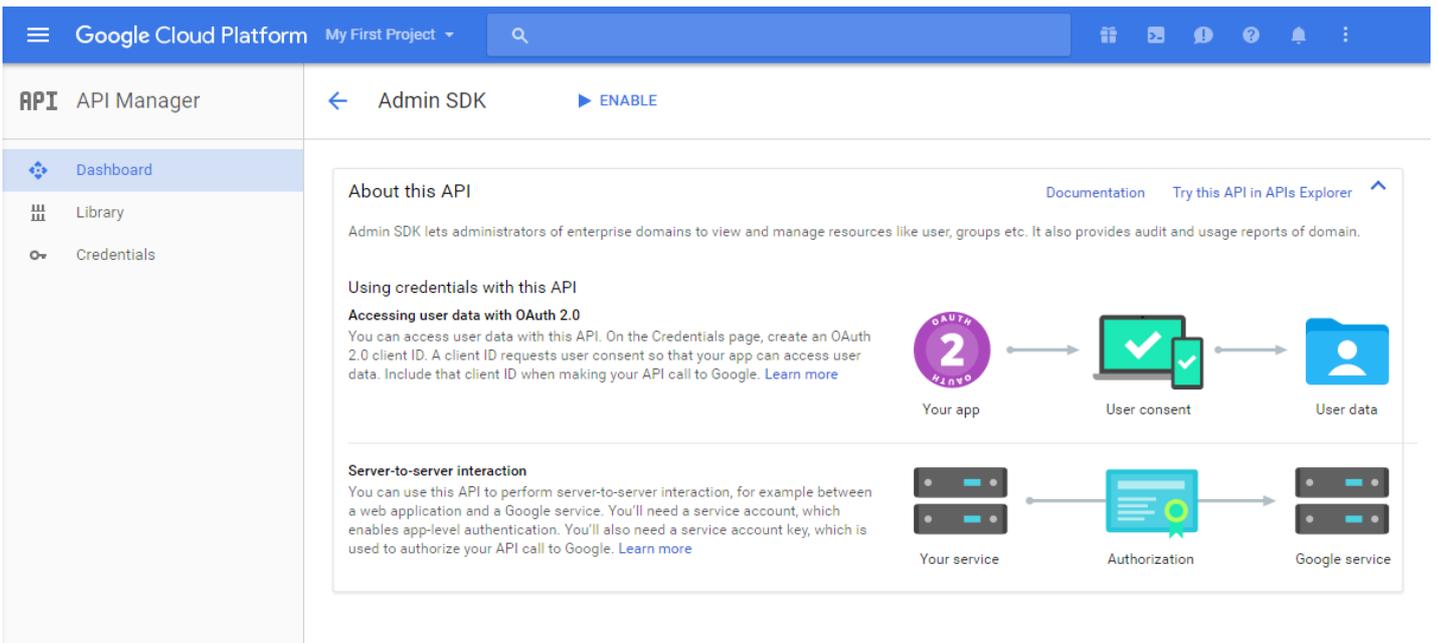
13. Aparecerán los datos requeridos para la autorización de cuentas en la consola de administración de Google. Copie los valores de **Client ID** y **Service account ID** en una ubicación donde pueda encontrarlos más adelante. Necesita esta información, junto con el nombre de dominio, para enviarla a Citrix para su inclusión en una lista blanca.



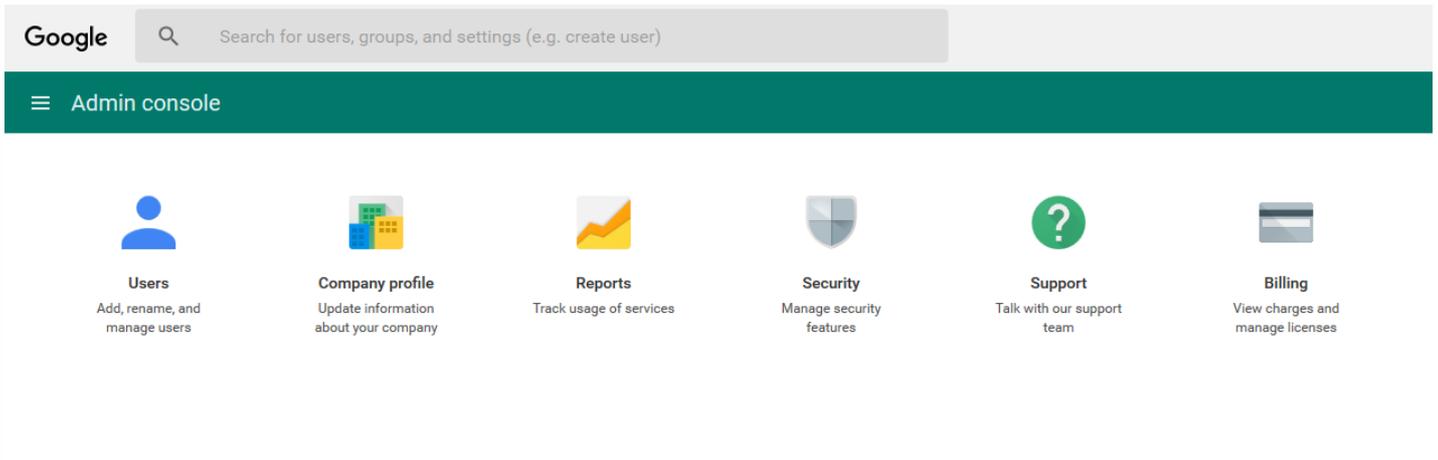
14. En la página **Library**, busque **Admin SDK** y haga clic en el resultado de búsqueda.



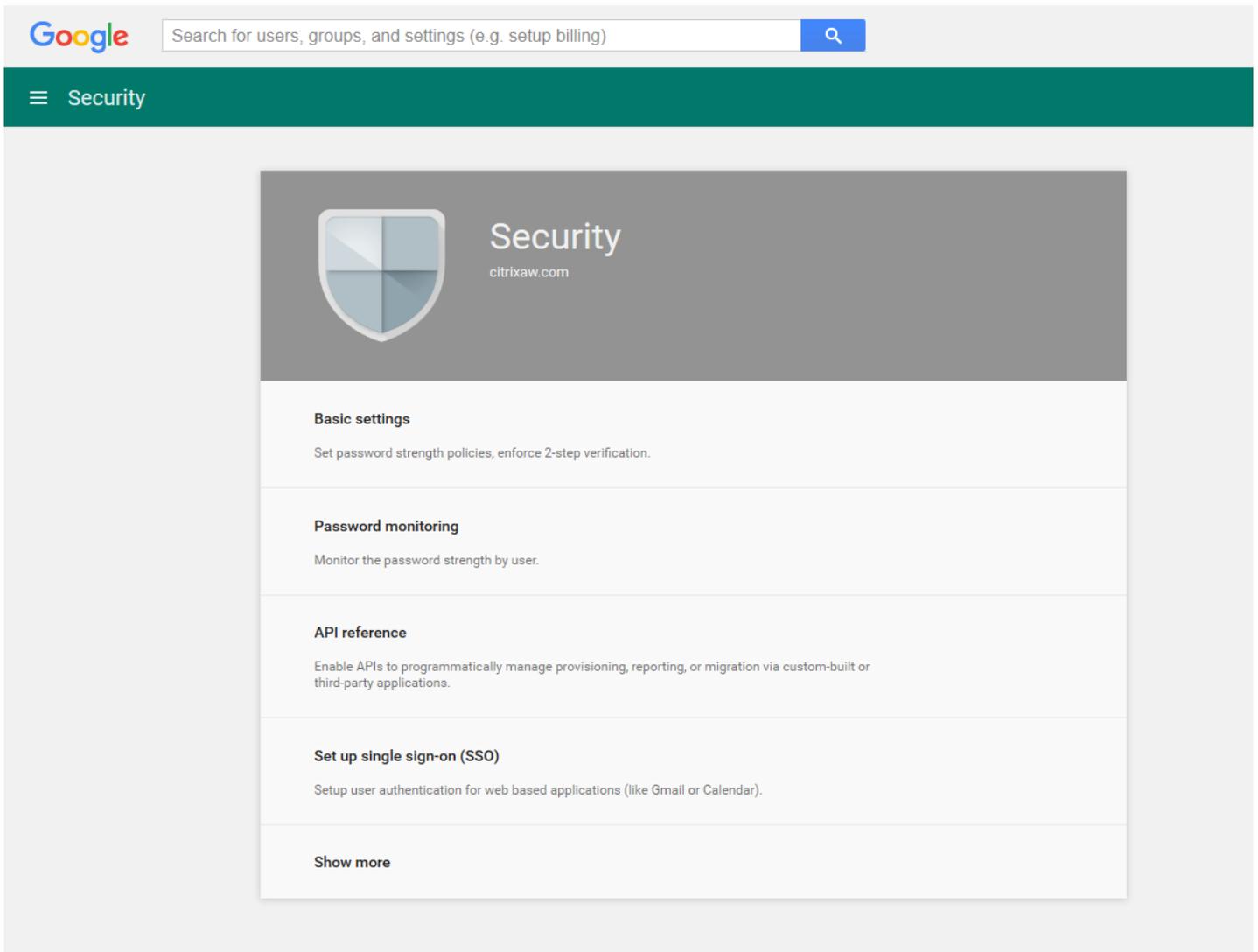
15 En la página **Overview**, haga clic en **Enable**.



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**.





## Security

citrixaw.com

### Basic settings

Set password strength policies, enforce 2-step verification.

### Password monitoring

Monitor the password strength by user.

### API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

### Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

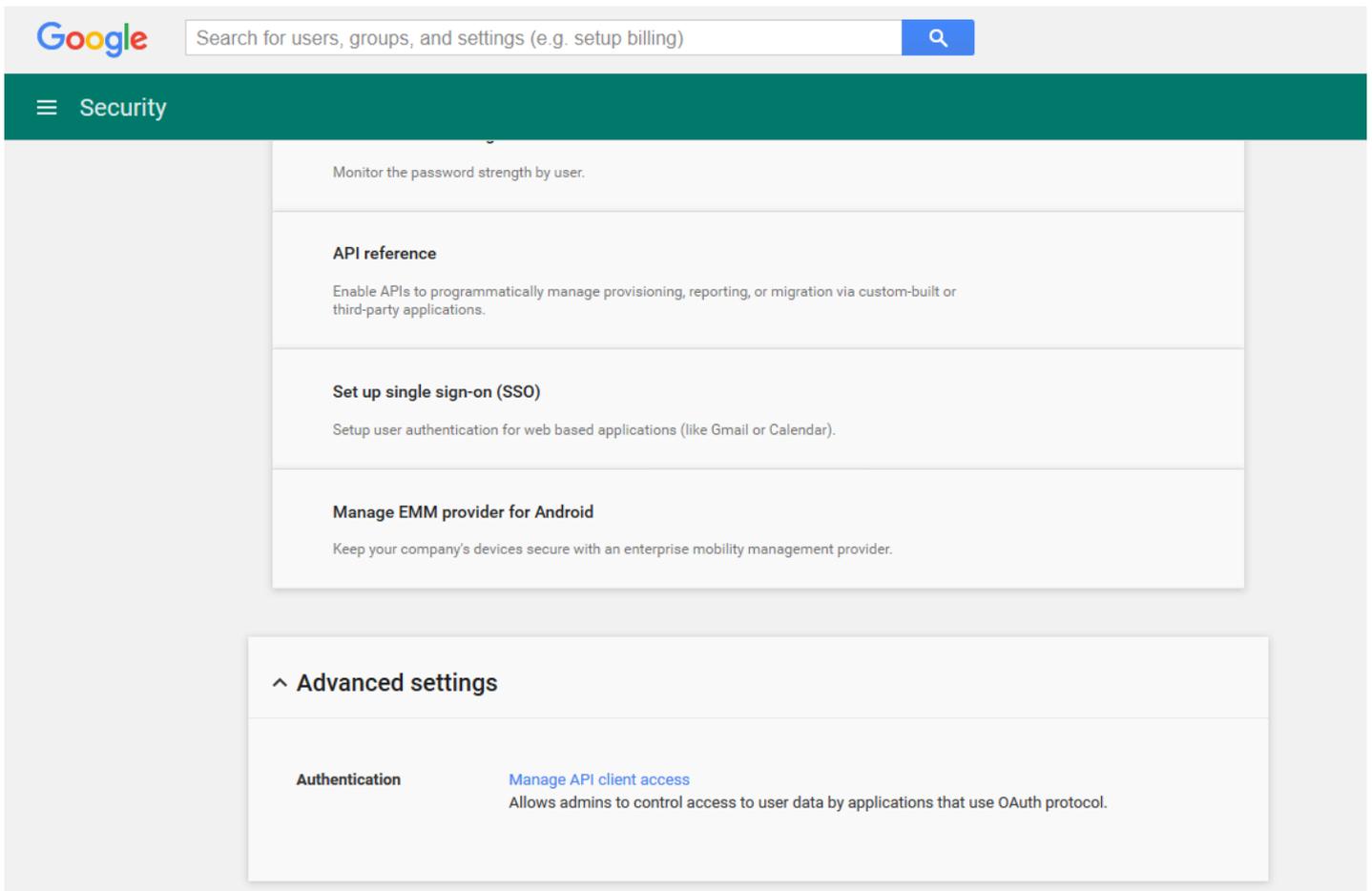
### Manage EMM provider for Android

Keep your company's devices secure with an enterprise mobility management provider.

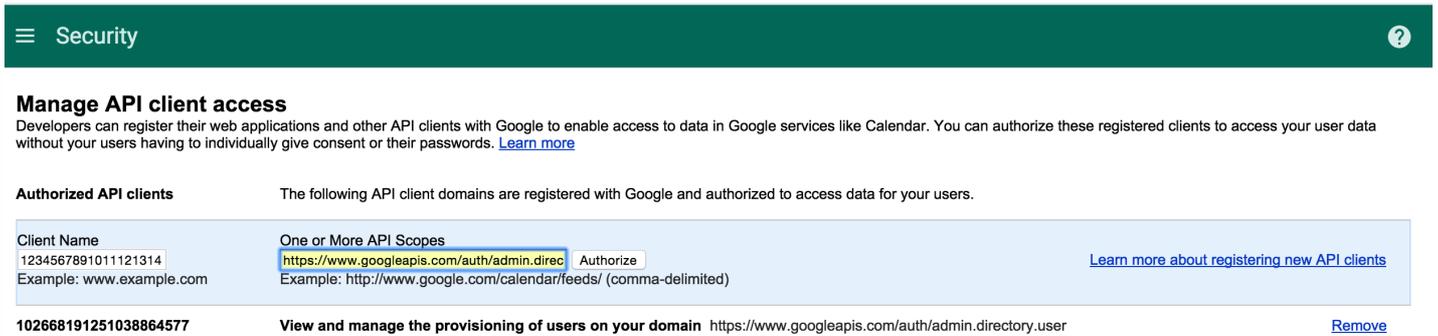
### Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

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

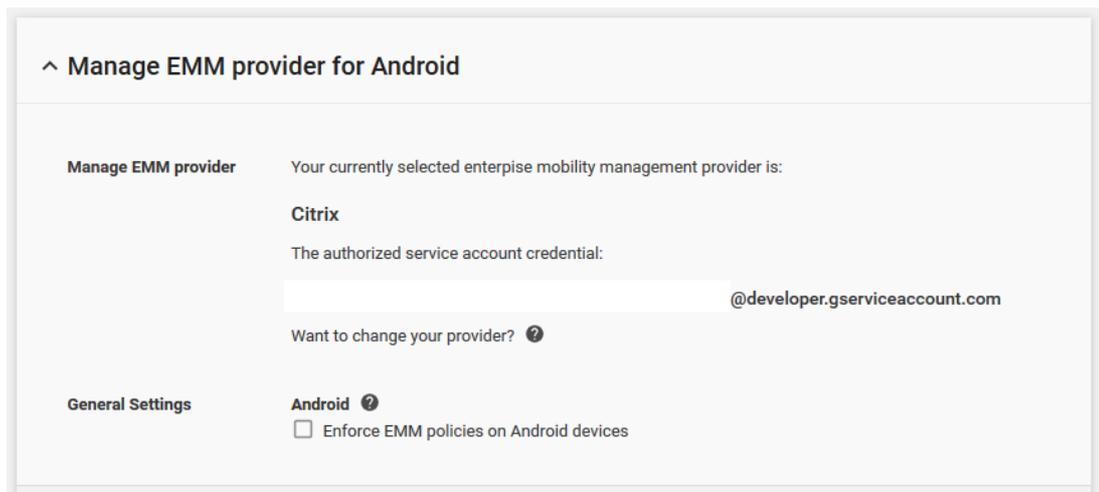
Antes de utilizar XenMobile para administrar los dispositivos Android, debe ponerse en contacto con el servicio de asistencia técnica de Citrix y proporcionarles su nombre de dominio, cuenta de servicio y token de vinculación. Citrix vincula el token con XenMobile como proveedor de administración de 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

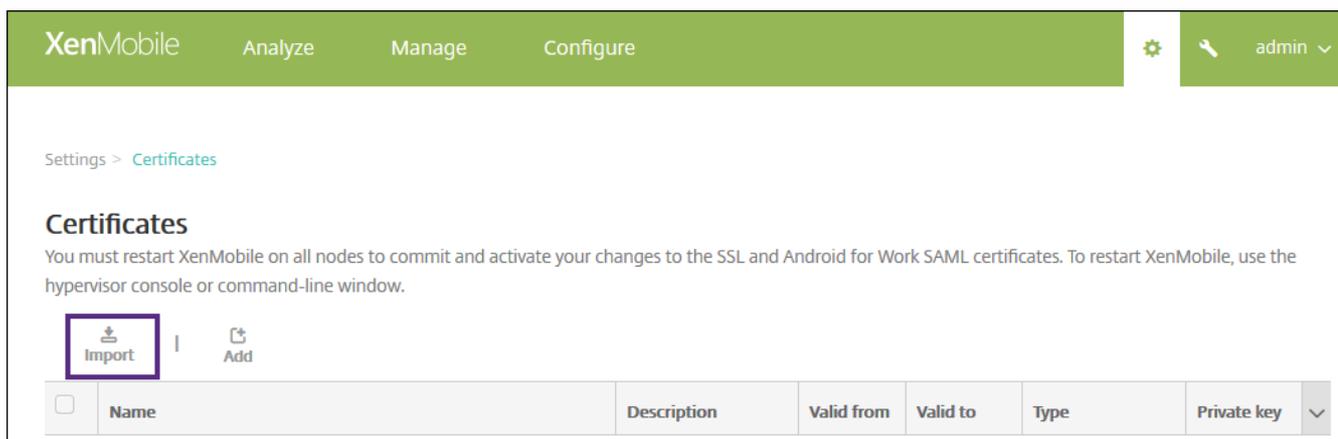
y defina al menos una directiva de dispositivo para Android at Work.



### 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**.

**Import**

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file\*: A 4d... Browse

Password\*: [masked]

Description: [text area]

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**.

XenMobile Analyze Manage Configure admin

Settings > Android for Work

**Android for Work**

Provide Android for Work configuration parameters.

Domain Name\* [input field]

Domain Admin Account\* [input field]

Service Account ID\* [input field]

Enable Android for Work: NO

Cancel Save

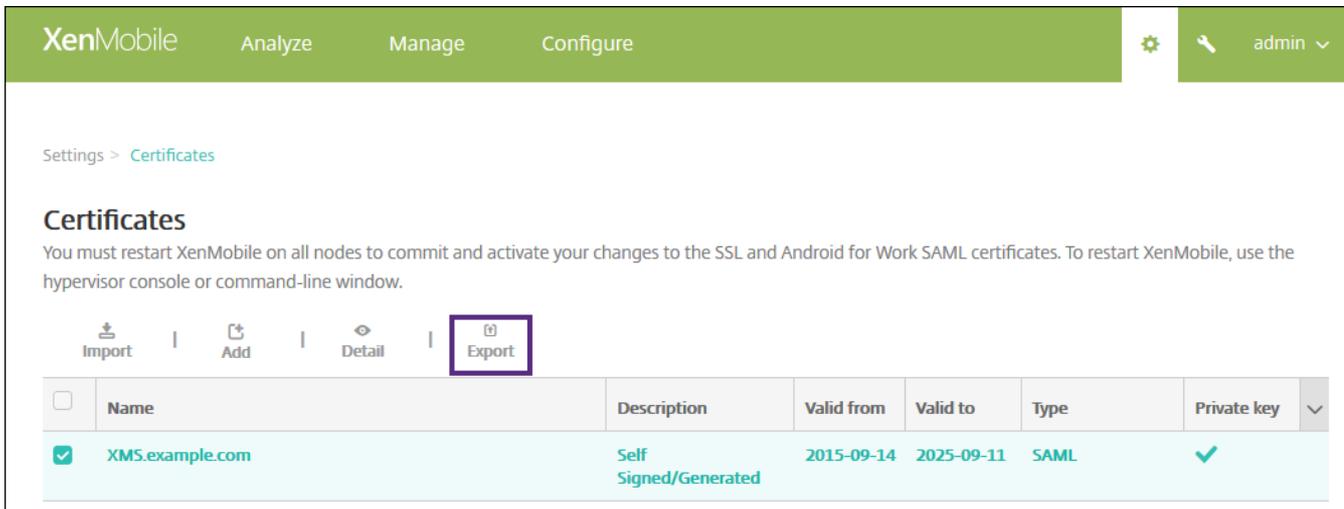
Configure los siguientes parámetros:

- **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**.



XenMobile Analyze Manage Configure admin

Settings > Certificates

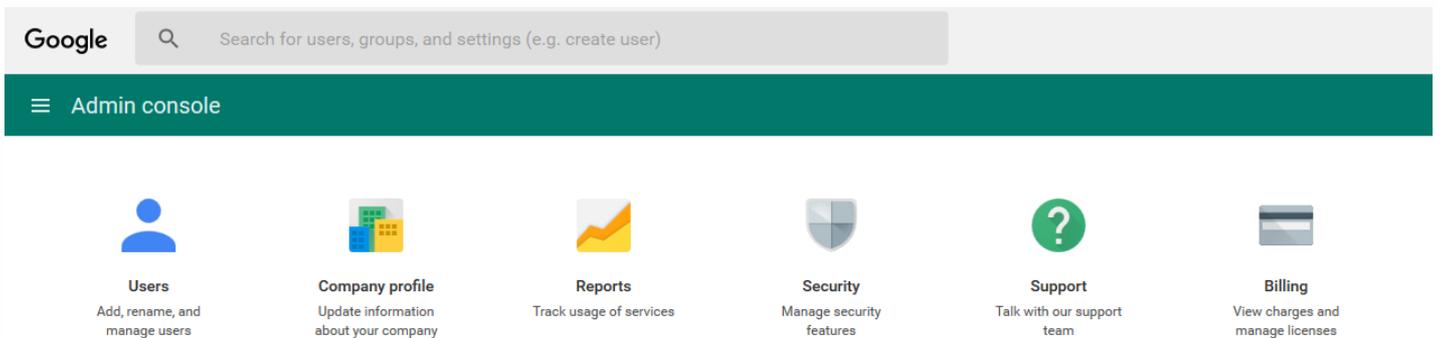
### Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import | Add | Detail | **Export**

<input type="checkbox"/>	Name	Description	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com	Self Signed/Generated	2015-09-14	2025-09-11	SAML	<input checked="" type="checkbox"/>

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**.



Google Search for users, groups, and settings (e.g. create user)

Admin console

- Users**  
Add, rename, and manage users
- Company profile**  
Update information about your company
- Reports**  
Track usage of services
- Security**  
Manage security features
- Support**  
Talk with our support team
- Billing**  
View charges and manage licenses

7. En **Security**, haga clic en **Set up single sign-on (SSO)** y configure los parámetros siguientes:

## ^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

### Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL

URL for signing in to your system and Google Apps

Sign-out page URL

URL for redirecting users to when they sign out

Change password URL

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate

The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

- **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.

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a list of policy categories: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Samsung KNOX, Android for Work (highlighted), Windows Phone, and Windows Tablet. The main content area is titled 'Policy Information' and contains the following settings:

- Passcode Required:** ON (toggle)
- Passcode requirements:**
  - Minimum length: 6 (dropdown)
  - Biometric recognition: OFF (toggle)
  - Advanced rules: OFF (toggle) with a note 'A 3.0+'
- Passcode security:**
  - Lock device after (minutes of inactivity): None (dropdown)
  - Passcode expiration in days (1-730): 0 (input field)
  - Previous passwords saved (0-50): 0 (input field) with a help icon (?)
  - Maximum failed sign-on attempts: Not defined (dropdown) with a help icon (?)

At the bottom of the main area, there is a section for 'Deployment Rules' and two buttons: 'Back' and 'Next >'.

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**.

Settings > [Android for Work](#)

## Android for Work

Provide Android for Work configuration parameters.

Domain Name*	<input type="text"/>
Domain Admin Account*	<input type="text"/>
Service Account ID*	<input type="text"/>
Enable Android for Work	<input checked="" type="checkbox"/>

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:

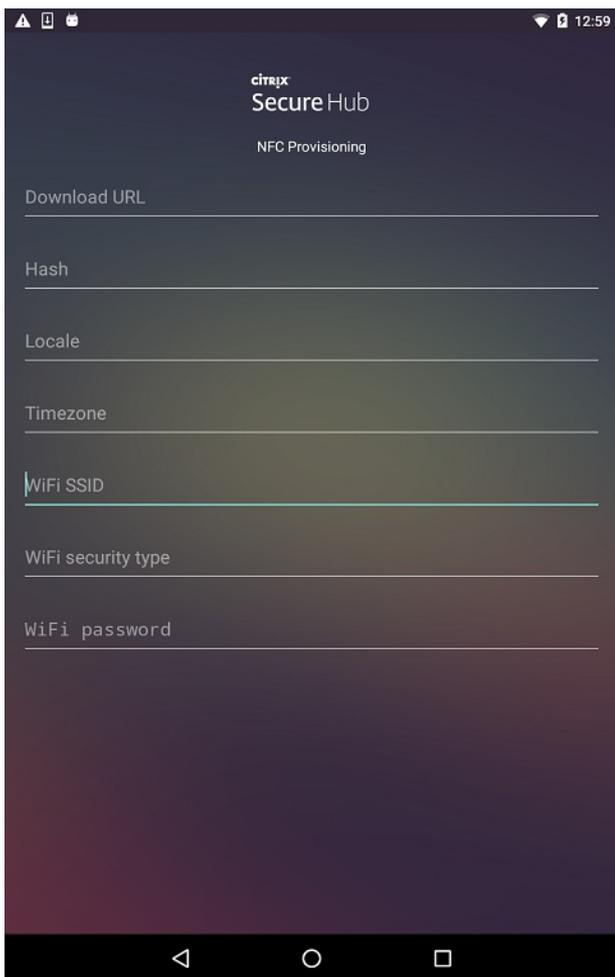
- Nombre del paquete de la aplicación de proveedor EMM que actuará como Device Owner (en este caso, Secure Hub).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación de proveedor EMM.

- 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.



The screenshot shows the 'NFC Provisioning' screen in the Citrix Secure Hub application. The screen has a dark background with white text. At the top, the Citrix logo and 'Secure Hub' are displayed, followed by 'NFC Provisioning'. Below this, there are several input fields with labels: 'Download URL', 'Hash', 'Locale', 'Timezone', 'WiFi SSID', 'WiFi security type', and 'WiFi password'. Each field is represented by a horizontal line. The 'WiFi SSID' field has a blue cursor at the beginning. At the bottom of the screen, there is a black navigation bar with three white icons: a back arrow, a circle, and a square.

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=ga50TwdCmf dj72LGRFkke4CrbAK\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:

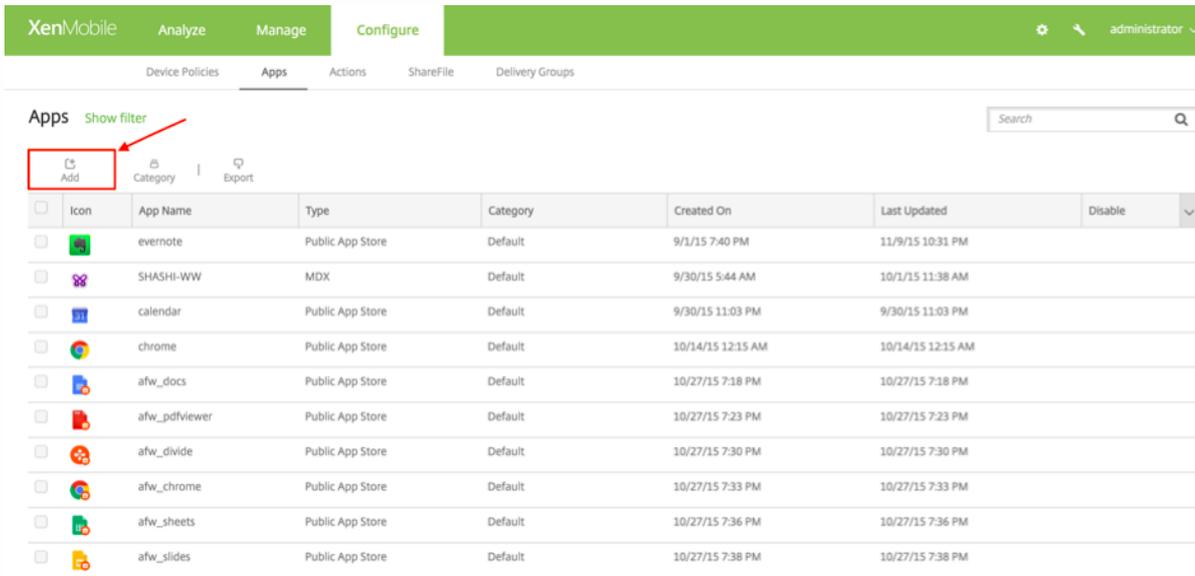
```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmf dj72LGRFkke4CrbAK\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
android.app.extra.PROVISIONING_LOCALE=en_US
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.

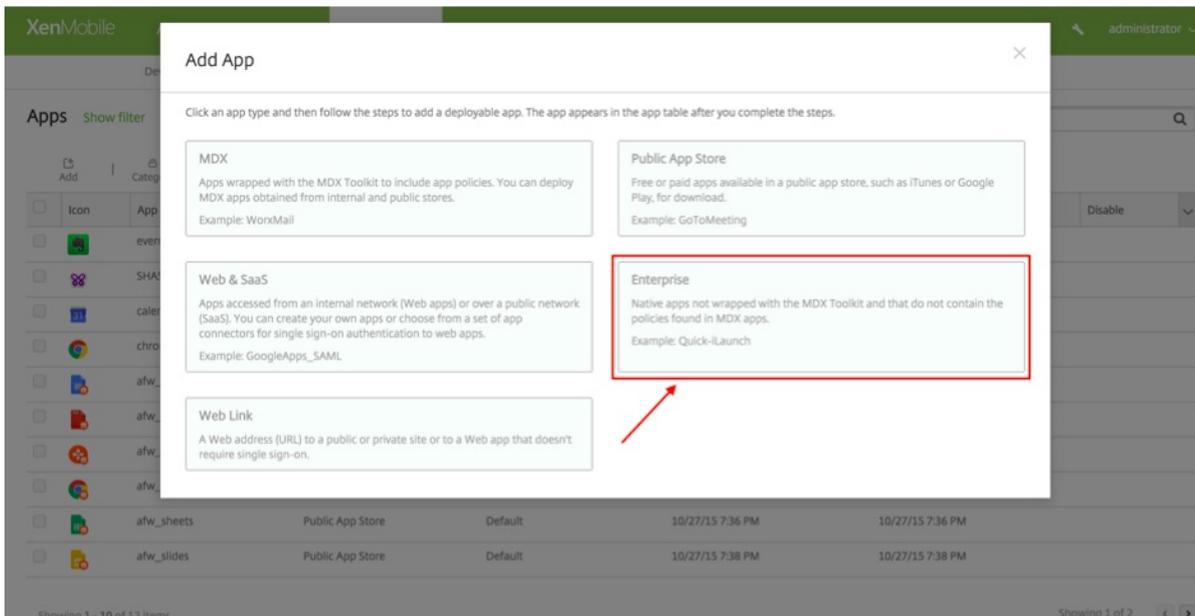
1. En la consola de XenMobile, vaya a **Configure > Apps > Add**.

Aparecerá la ventana **Add App**.



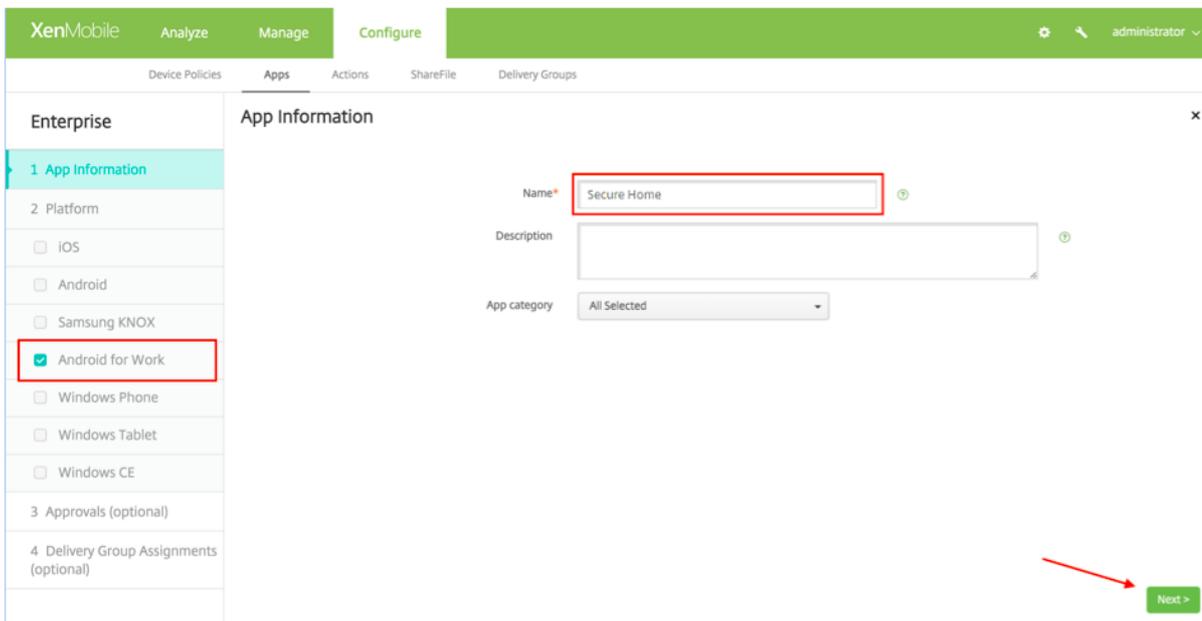
2. Haga clic en **Enterprise**.

Aparecerá la página **App Information**.

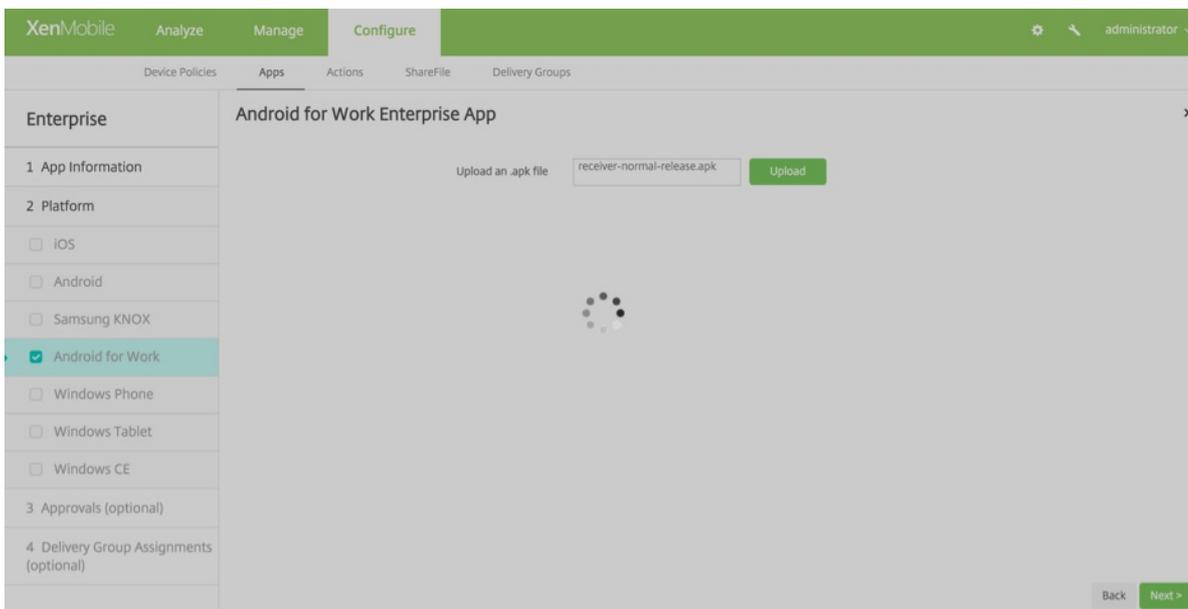


3. Seleccione la configuración siguiente y haga clic en **Next**.

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.



- 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 masiva de dispositivos iOS

Mar 02, 2017

Puede inscribir un gran número de dispositivos iOS en XenMobile en dos formas. Puede usar el Programa de inscripción de dispositivos (DEP) de Apple para inscribir dispositivos adquiridos directamente en Apple o en un distribuidor autorizado de Apple. También puede usar Apple Configurator para inscribir dispositivos independientemente de si fueron adquiridos directamente en Apple.

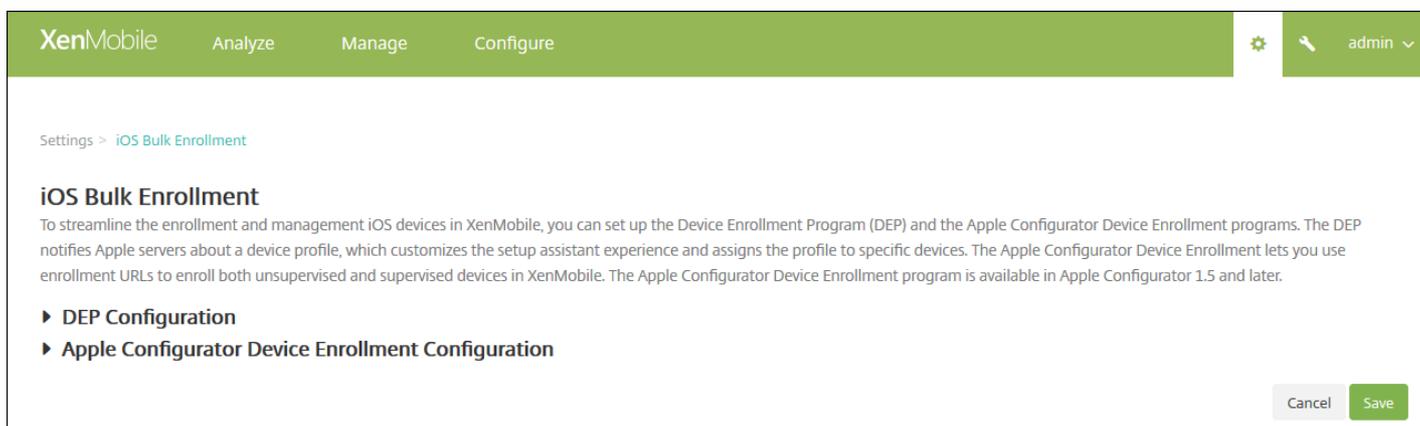
XenMobile 10.x respalda Apple Configurator 2.

Con DEP, no tiene que preparar los dispositivos de ningún modo. Basta con enviar los números de serie o de pedido de compra a través de DEP, y los dispositivos se configuran e inscriben en XenMobile. Después de inscribir los dispositivos, 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 a un equipo Apple que esté ejecutando OS X 10.7.2 o una versión posterior y la aplicación Apple Configurator. Se debe preparar los dispositivos y configurar las directivas mediante Apple Configurator. Después de aprovisionar los dispositivos con las directivas necesarias, la primera vez que los dispositivos se conectan a XenMobile, se aplican las directivas y ya se puede empezar a administrar los dispositivos. Para obtener más información sobre cómo usar el Apple Configurator, consulte la página [Apple Configurator](#).

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 **iOS Bulk Enrollment**. Aparece la página **iOS Bulk Enrollment**.



Si está configurando los parámetros de DEP, consulte los apartados siguientes. En cambio, si está configurando los parámetros de Apple Configurator, consulte [Configuración de parámetros de Apple Configurator](#).

## Configuración de parámetros de DEP

**Requisitos previos:** Antes de continuar, debe haber creado una cuenta DEP de Apple en [deploy.apple.com](https://deploy.apple.com). Después de haber creado una cuenta DEP, debe configurar un servidor MDM virtual para permitir la comunicación entre XenMobile y Apple. Para ello, debe cargar una clave pública de XenMobile en Apple. Después de recibir la clave pública, Apple devuelve un

token de servidor que usted debe importar en XenMobile.

Siga estos pasos para establecer la conexión entre XenMobile y Apple.

1. Para obtener la clave pública y cargarla en Apple, en la página **iOS Bulk Enrollment**, expanda **DEP Configuration**. A continuación, haga clic en **Export Public Key** y guarde el archivo en su equipo.
2. Vaya a [deploy.apple.com](https://deploy.apple.com), inicie sesión en la cuenta DEP y siga las instrucciones para configurar un servidor MDM. Durante este proceso, Apple entrega un token de servidor.
3. En la página **iOS Bulk Enrollment**, haga clic en **Import Token File** para agregar el token del servidor Apple a XenMobile.
4. Los campos **Server tokens** se rellenan automáticamente una vez cargado el archivo de token en XenMobile.
5. Haga clic en **Test Connectivity** para confirmar que XenMobile y Apple pueden comunicarse.

Si la prueba de conexión falla, confirme que tiene abiertos los puertos necesarios, porque ésta suele ser la causa de estos fallos. Para obtener más información sobre los puertos que deben abrirse en XenMobile, consulte [Requisitos de puertos](#).

XenMobile Analyze Manage Configure admin

Settings > iOS Bulk Enrollment

### iOS Bulk Enrollment

To streamline the enrollment and management iOS devices in XenMobile, you can set up the Device Enrollment Program (DEP) and the Apple Configurator Device Enrollment programs. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. The Apple Configurator Device Enrollment lets you use enrollment URLs to enroll both unsupervised and supervised devices in XenMobile. The Apple Configurator Device Enrollment program is available in Apple Configurator 1.5 and later.

▼ DEP Configuration

Export Public Key | Import Token File

Allow Device Enrollment Program (DEP)  NO

Server Tokens

Consumer key\*

Consumer secret\*

Access token\*

Access secret\*

Access token expiration

Test Connection

Organization Info

Business unit\*

Unique service ID

Support phone number\*

Support email address

**Enrollment Settings**

Require device enrollment  ⓘ

Supervised mode  YES ⓘ

Enrollment profile removal  Allow ⓘ  
 Deny

Pairing  Allow ⓘ  
 Deny

Require credentials for device enrollment  ⓘ

Wait for configuration to complete setup  ⓘ

**Setup Assistant Options**

Do not set up  Location Services  
 Touch ID (iOS 8.0+)  
 Passcode Lock  
 Set Up as New or Restore  
 Move from Android (iOS 9.0+)  
 Apple ID  
 Terms and Conditions  
 Apple Pay (iOS 8.0+)  
 Siri  
 App Analytics  
 Display Zoom (iOS 8.0+)

▶ **Apple Configurator Device Enrollment Configuration**

Cancel Save

6. Configure los parámetros siguientes para completar la configuración de DEP:

### Información sobre la organización

- **Business unit.** Especifique el departamento o la unidad de negocio a la que se asigna el dispositivo. Este campo es obligatorio.
- **Unique service ID.** Si quiere, introduzca un ID único.
- **Support phone number.** Escriba 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.** Si quiere, también puede introducir una dirección de correo electrónico de asistencia.

### Parámetros de inscripción

- **Require device enrollment.** Seleccione si hay que requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es requerir la inscripción.
- **Supervised mode.** Se debe establecer en **Yes** si se usa el Apple Configurator para administrar los dispositivos inscritos de DEP 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](#) más adelante en este artículo.
- **Enrollment profile removal.** Seleccione si quiere permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. El valor predeterminado es **Deny**.
- **Pairing.** Seleccione si quiere permitir que los dispositivos inscritos mediante el programa DEP sean administrados a través

de iTunes y Apple Configurator. El valor predeterminado es **Deny**.

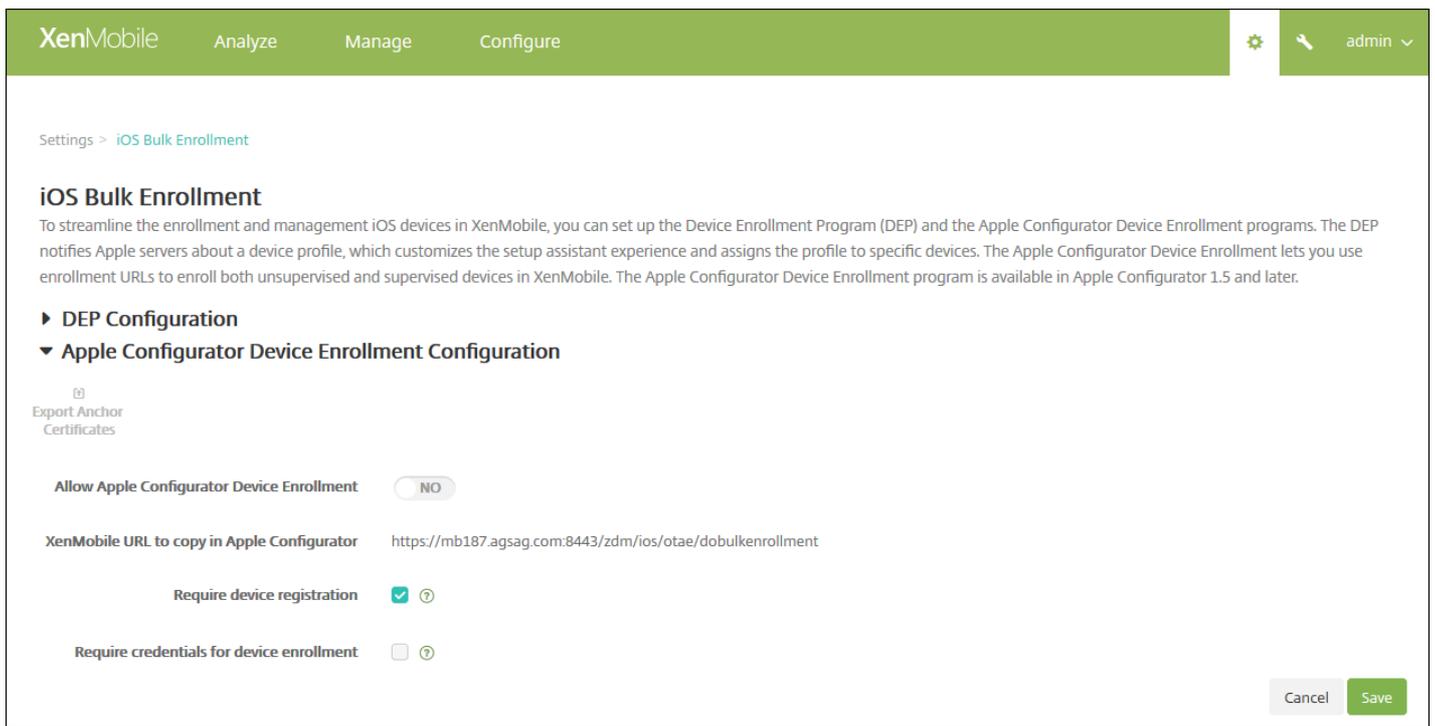
- **Require credentials for device enrollment.** Seleccione si pedir a los usuarios que indiquen sus credenciales durante la configuración de DEP. Esta opción está disponible para iOS 7.1 y versiones posteriores. **Nota:** Si DEP está activado en la primera configuración y no se selecciona esta opción, los componentes de DEP (como el usuario DEP, Secure Hub, el inventario de software y el grupo de implementación DEP) se crean desde el principio. Si selecciona esta opción, los componentes no se crean hasta que el usuario introduzca sus credenciales. 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.** Seleccione si se debe requerir que los dispositivos de los usuarios permanezcan en el modo del asistente de instalación hasta que todos los recursos de MDM se implementen en ellos. Esta función está disponible para dispositivos iOS 9.0 y versiones posteriores en modo supervisado.
  - **Nota:** 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

## Configuración

Seleccione los pasos a omitir (es decir, los pasos del asistente de configuración de iOS que los usuarios no tienen que llevar a cabo) cuando inicien sus dispositivos para usarlos por primera vez.

- **Location Services.** 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.** 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 Diagnostics.** 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.

Configuración de parámetros de Apple Configurator



1. Expanda **Apple Configurator Device Enrollment Configuration**.

2. Establezca **Enable Apple Configurator Device Enrollment** en **Yes**.

3. Defina y anote los siguientes parámetros:

- **MDM server URL to copy in Apple Configurator:** Ese campo de solo lectura es la dirección URL del servidor XenMobile que se comunica con Apple, y que hay que copiar y pegar en el último paso de 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`).
- **Require device registration.** Si selecciona este parámetro, debe agregar previamente los dispositivos configurados en la ficha **Devices** de XenMobile manualmente o mediante un archivo CSV para poder inscribirlos. Con esto se asegura de que no se puedan inscribir dispositivos desconocidos. El valor predeterminado es requerir que los dispositivos se agreguen a la lista.
- **Require credentials for device enrollment.** Requiere que los usuarios de los dispositivos iOS 7.1 y versiones posteriores introduzcan sus credenciales cuando se inscriban. El valor predeterminado es no requerirlas.

## Nota

Si el servidor XenMobile está usando un certificado SSL de confianza, omita el paso siguiente.

4. Haga clic en **Export Anchor Certs** y guarde el archivo `certchain.pem` en el llavero de OS X (Inicio de sesión o Sistema).

5. Inicie Apple Configurator y vaya a **Prepare > Setup > Configure Settings**.

6. En el parámetro "Device Enrollment", pegue la URL del servidor MDM del paso 4 en el campo **MDM server URL** de Apple Configurator.

7. 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.

8. Use un cable de conector de Dock con USB para conectar los dispositivos al equipo Mac donde se 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.

9 Haga clic en **Prepare**. Para obtener más información sobre la preparación de dispositivos de Apple Configurator, consulte la página de ayuda " href="https://help.apple.com/configurator/mac/1.0/#cad96c7acd6">Prepare devices de Apple Configurator.

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 Apple DEP, consulte la [documentación de Apple](#).

Para obtener información sobre problemas conocidos y soluciones temporales relacionados con esta configuración, consulte [Problemas conocidos de XenMobile Server 10.4](#).

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 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.
  - 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 en dispositivos iOS a través de Apple DEP

Mar 02, 2017

Para utilizar la inscripción y administración de dispositivos del programa DEP (Developer Enterprise Program) de Apple en XenMobile necesitará una cuenta de Apple DEP. Los requisitos principales para que una organización pueda registrarse con Apple DEP son los siguientes:

- Dirección de correo electrónico o número de teléfono de la empresa o la institución
- Contacto para verificación
- Información del negocio o de la institución (D-U-N-S / ID fiscal)
- Número de cliente de Apple

Para obtener más información sobre el programa Apple DEP, consulte este [PDF](#) de Apple. Es importante subrayar que el programa Apple DEP está disponible solo para organizaciones, no para individuos. También es importante resaltar que es necesario suministrar bastantes datos de la empresa o de la organización para poder crear una cuenta de Apple DEP, lo que significa que el proceso de solicitar y recibir aprobación para las cuentas puede tardar algún tiempo.

## Solicitud de una cuenta de Apple DEP

Al solicitar una cuenta DEP, se recomienda usar una dirección de correo electrónico asociada a una organización, tal como `dep@nombre-de-empresa.com`.

 Deployment Programs



## Welcome

Enroll your organization in one of the following:



### Device Enrollment Program

Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.

[Enroll](#)



### Volume Purchase Program

Easily find, buy, and distribute content to users. Users enroll without sharing their Apple ID, then apps are assigned to them using an MDM solution.

[Enroll](#)

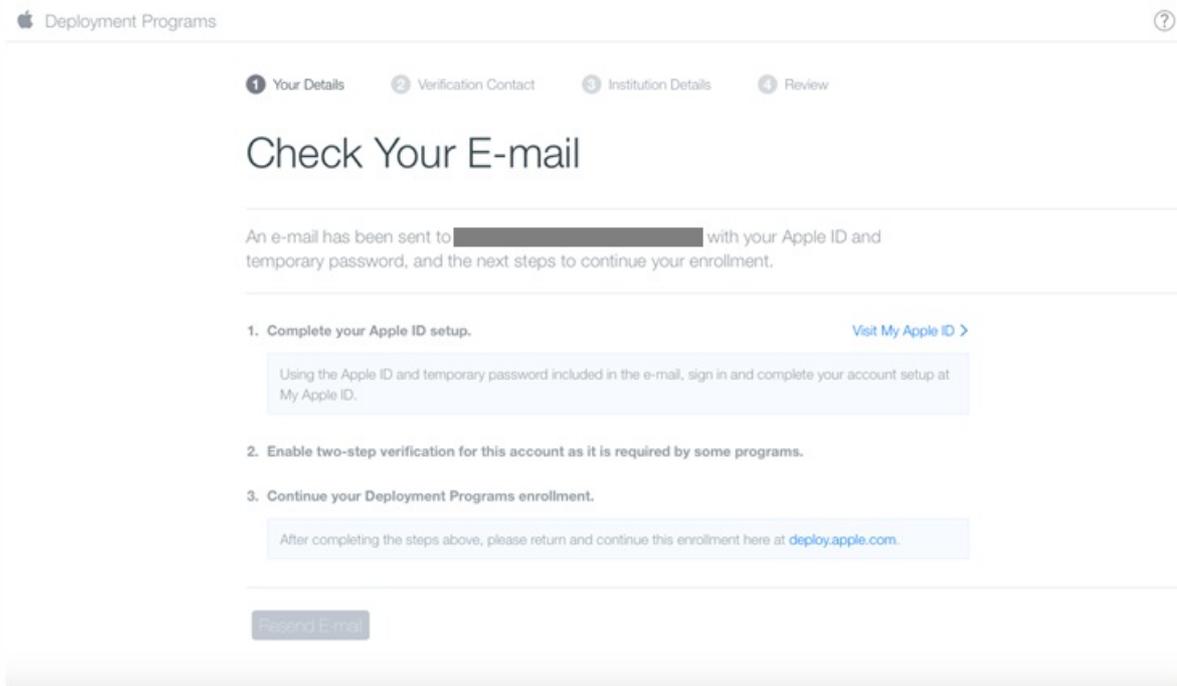


### Apple ID for Students

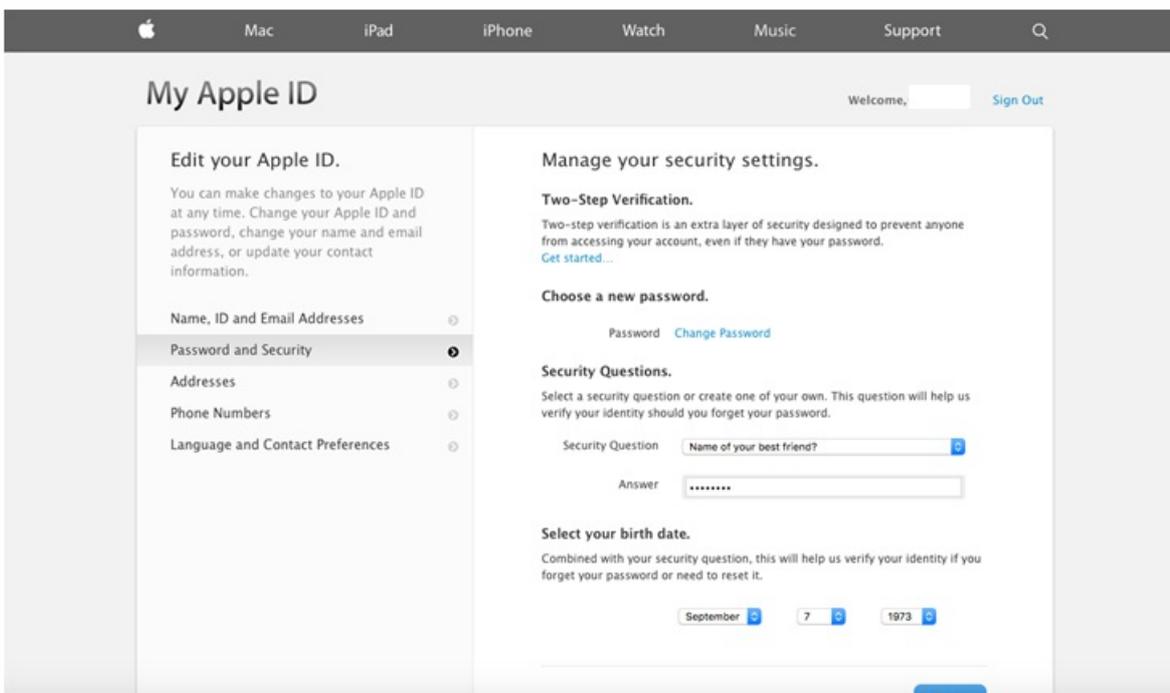
Manage student accounts and parental consent.

[Enroll](#)

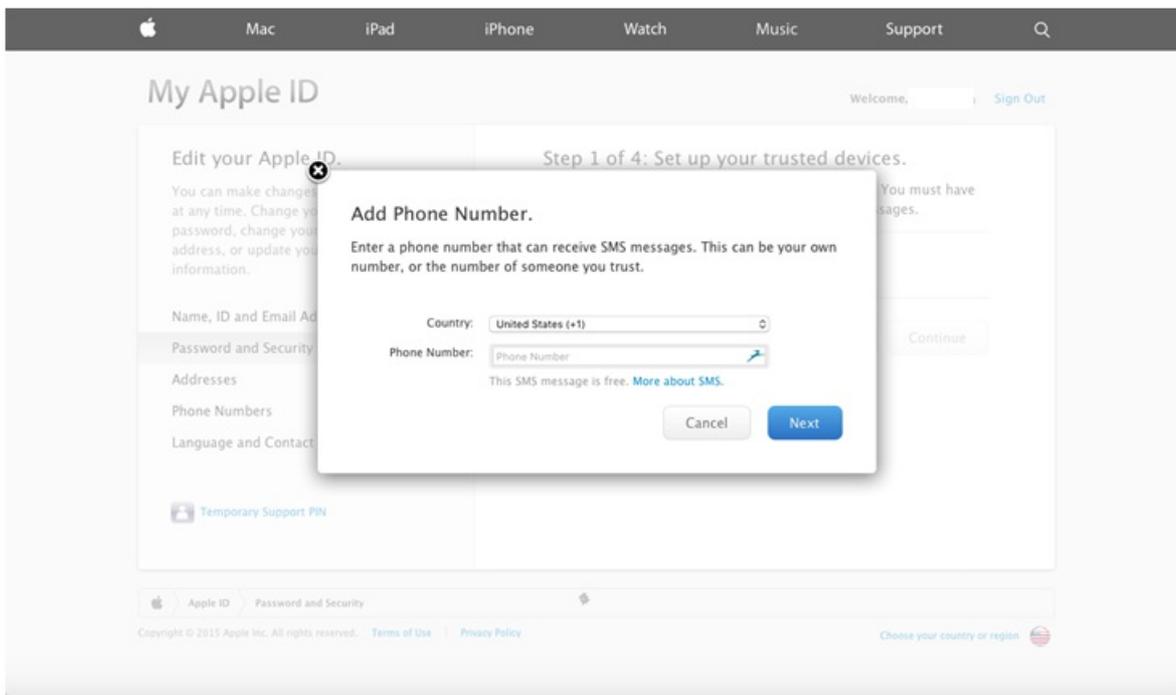
1. Después de introducir los datos de su organización, recibirá una contraseña temporal para el nuevo ID de Apple, por correo electrónico.



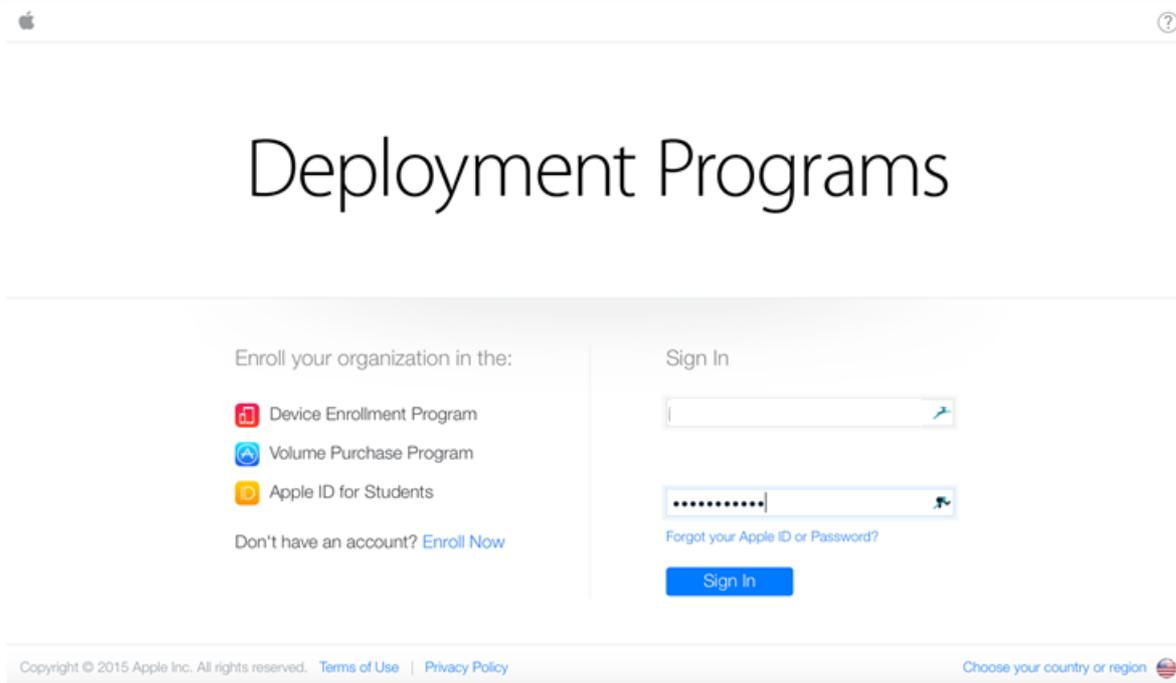
2. A continuación, debe iniciar una sesión con el ID de Apple y rellenar los parámetros de seguridad para la cuenta.



3. Configure y habilite la verificación en dos pasos, que es necesaria para usar el portal de DEP. Durante estos pasos, hay que agregar un número de teléfono donde se recibirá el PIN de cuatro dígitos para la verificación en dos pasos.



4. Inicie una sesión en el portal de DEP para completar la configuración de la cuenta usando la verificación en dos pasos que acaba de configurar.



5. Agregue los datos de su empresa y después seleccione dónde adquiere sus dispositivos. Para ver información sobre las opciones de compra, consulte la sección siguiente, [Adquirir dispositivos habilitados con DEP](#).

**ADD INSTALLATION DETAILS** [Need Help?](#)

Company Name

Company D-U-N-S

Address Line 1

Address Line 2

City

State

ZIP Code

Country

Web Site

Web Site

Choose...  
Reseller  
Apple Inc. (Direct)  
Choose...

[Add another...](#)

6. Agregue el número de cliente de Apple o el ID del proveedor DEP y luego verifique sus datos de inscripción y espere a que Apple apruebe su cuenta.

**ADD INSTALLATION DETAILS** [Need Help?](#)

Company Name

Company D-U-N-S

Address Line 1

Address Line 2

City

State

ZIP Code

Country

Web Site

Web Site

Devices Purchased From

DEP Reseller ID

CDW

[Add another...](#)

Deployment Programs

1 Your Details 2 Verification Contact 3 Institution Details 4 Review

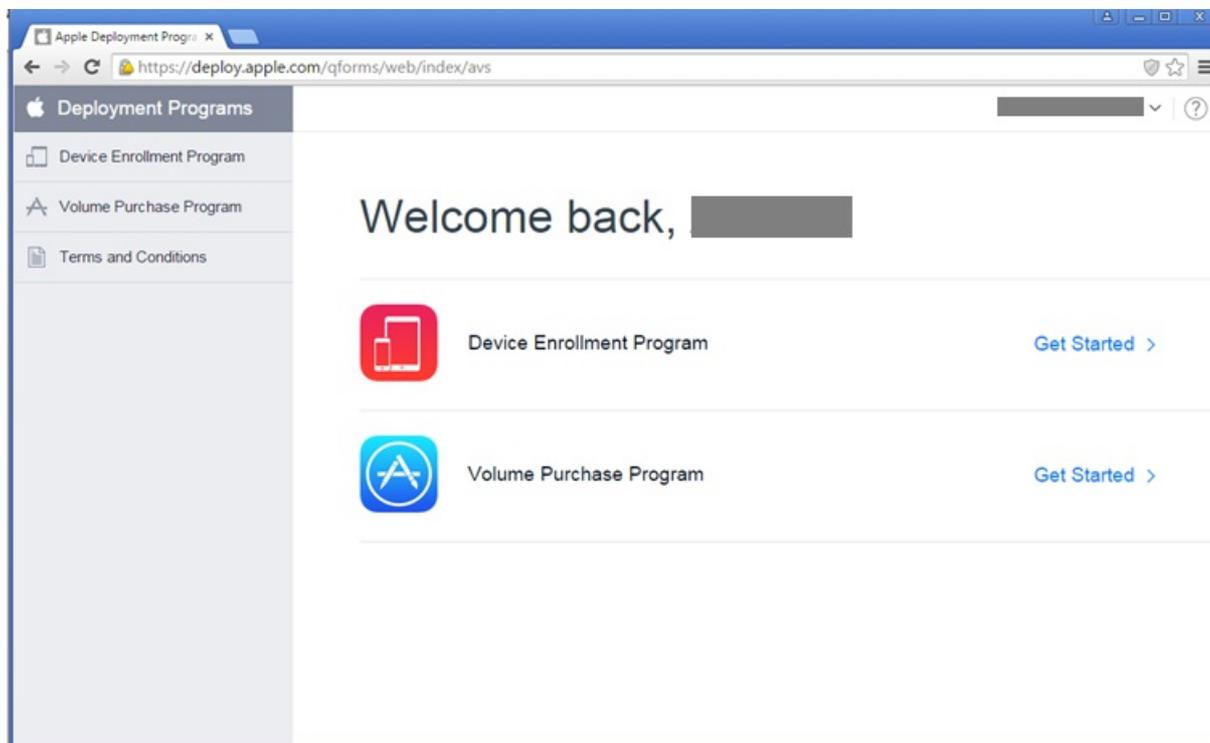
## Review Your Enrollment Details

[Need Help?](#)

Your Details	Verification Contact	Institution Details
Your Name	Verification Contact Name	Company Name
Your Work E-mail	Verification Contact Work E-mail	Web Site
Your Work Phone	Verification Contact Work Phone	Address
Your Title / Position General Manager	Title / Position General Manager	Devices Purchased From

[Edit](#) [Submit](#)

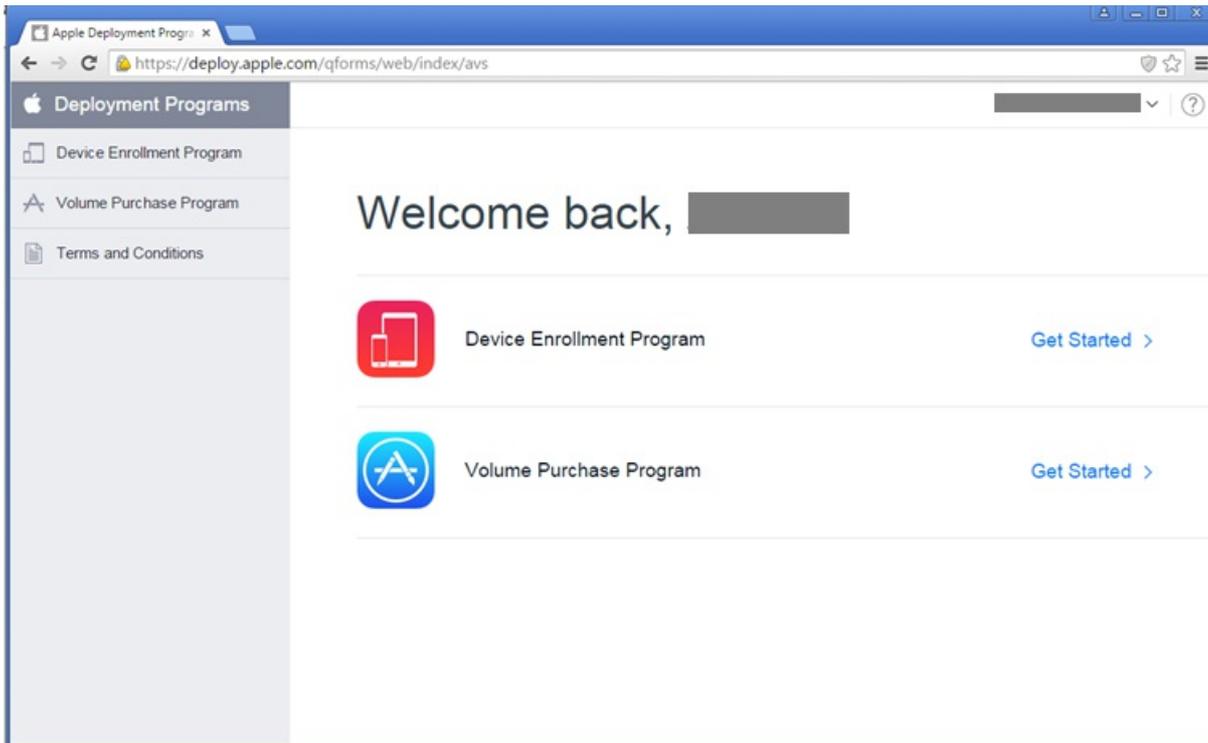
7. Después de recibir las credenciales de inicio de sesión desde Apple, inicie sesión en el portal de Apple DEP. A continuación, siga los pasos de la sección siguiente para conectar su cuenta con XenMobile.



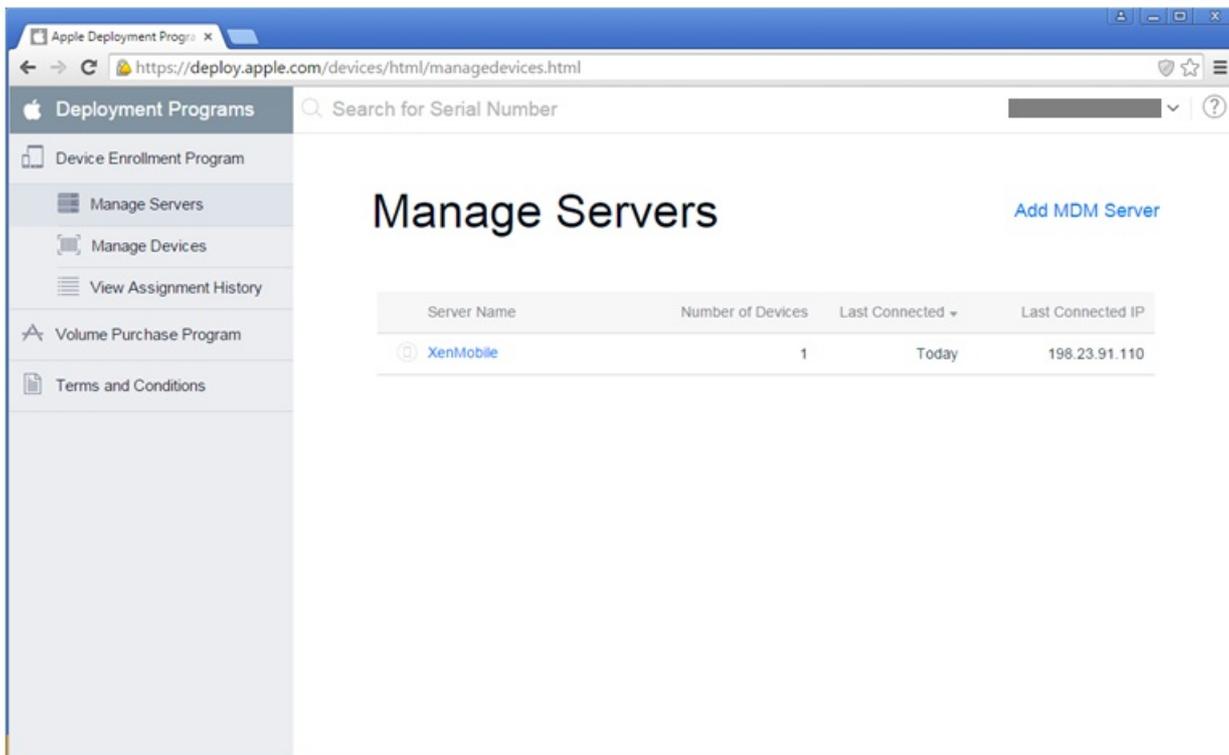
Integración de la cuenta de Apple DEP con XenMobile

Siga los pasos indicados en esta sección para conectar su cuenta de Apple DEP con el entorno del servidor XenMobile.

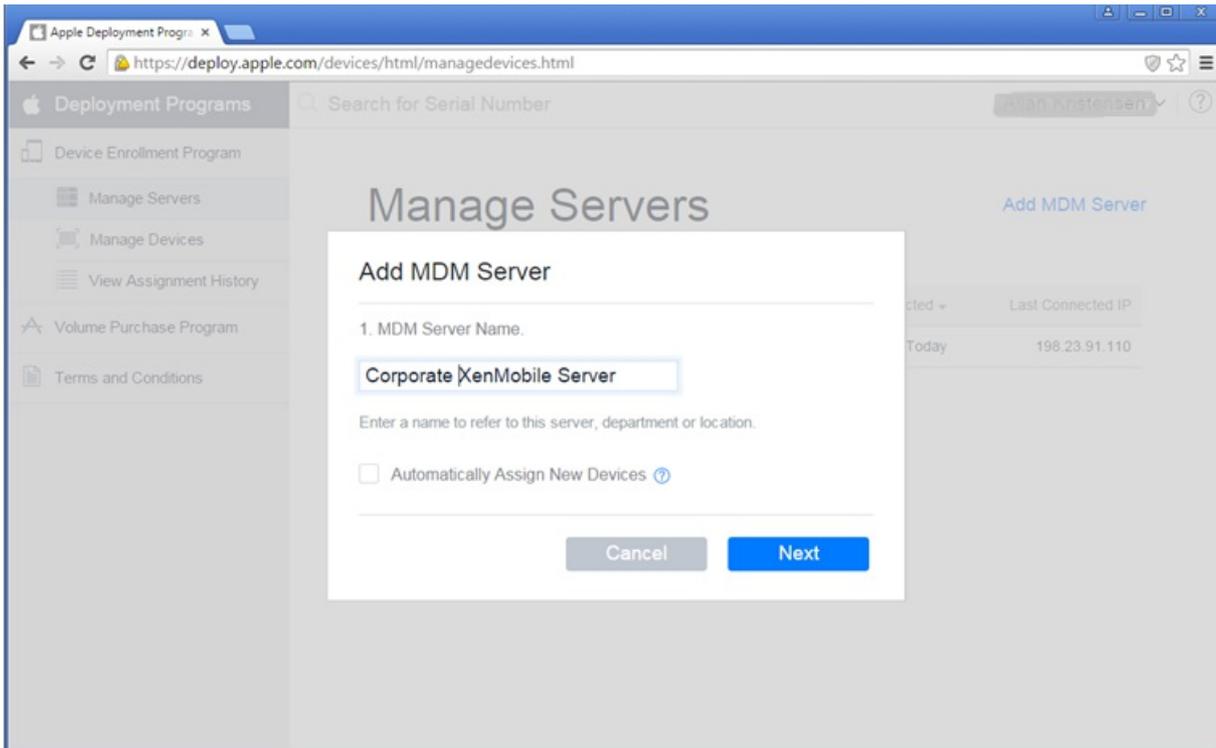
1. En el lado izquierdo del portal de Apple DEP, haga clic en **Device Enrollment Program**.



2. Haga clic en **Manage Servers** y, en el lado derecho, haga clic en **Add MDM Server**.

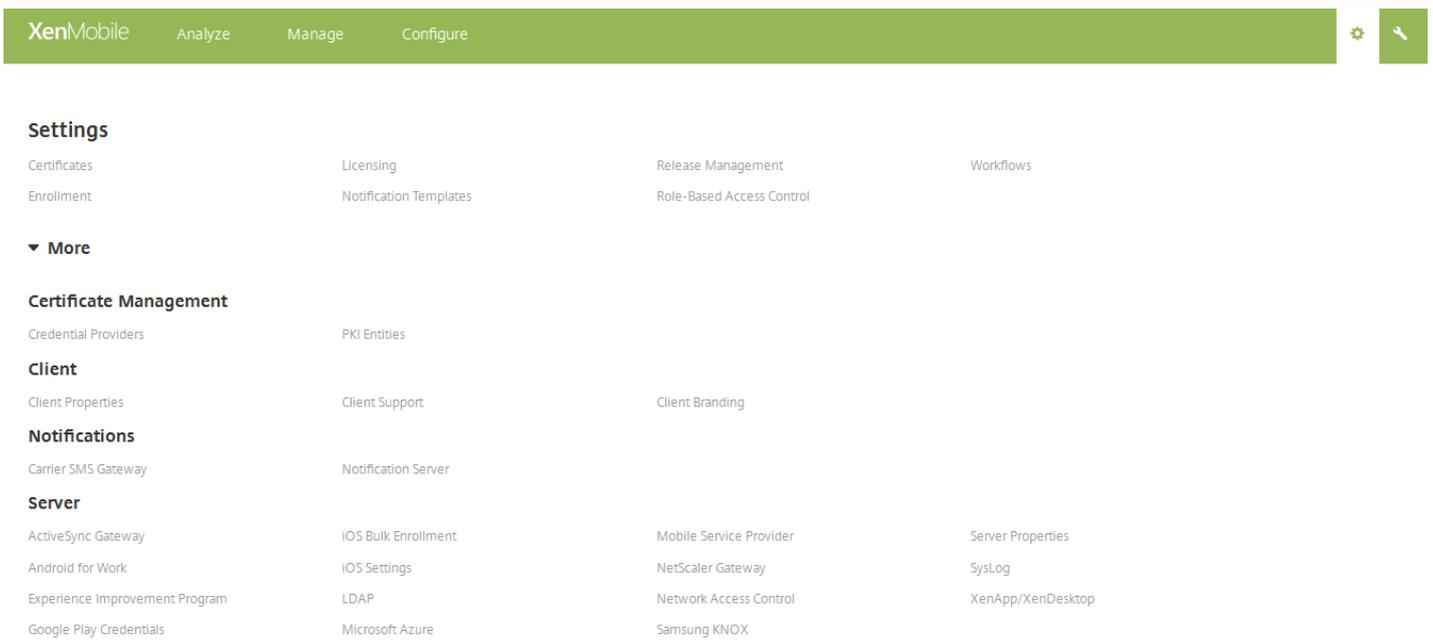


3. En **Add MDM Server**, introduzca el nombre de su servidor XenMobile y haga clic en **Next**.

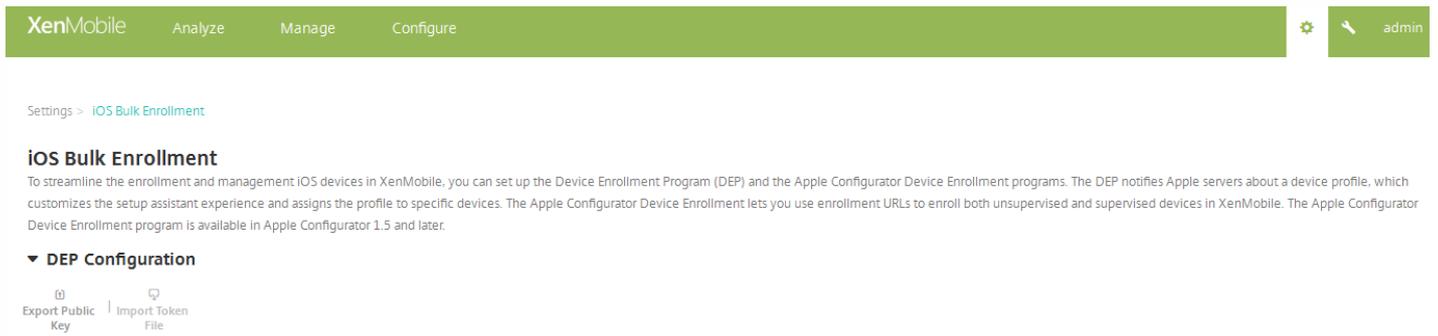


4. Cargue una clave pública desde el servidor XenMobile. Para generar una clave desde XenMobile, haga lo siguiente:

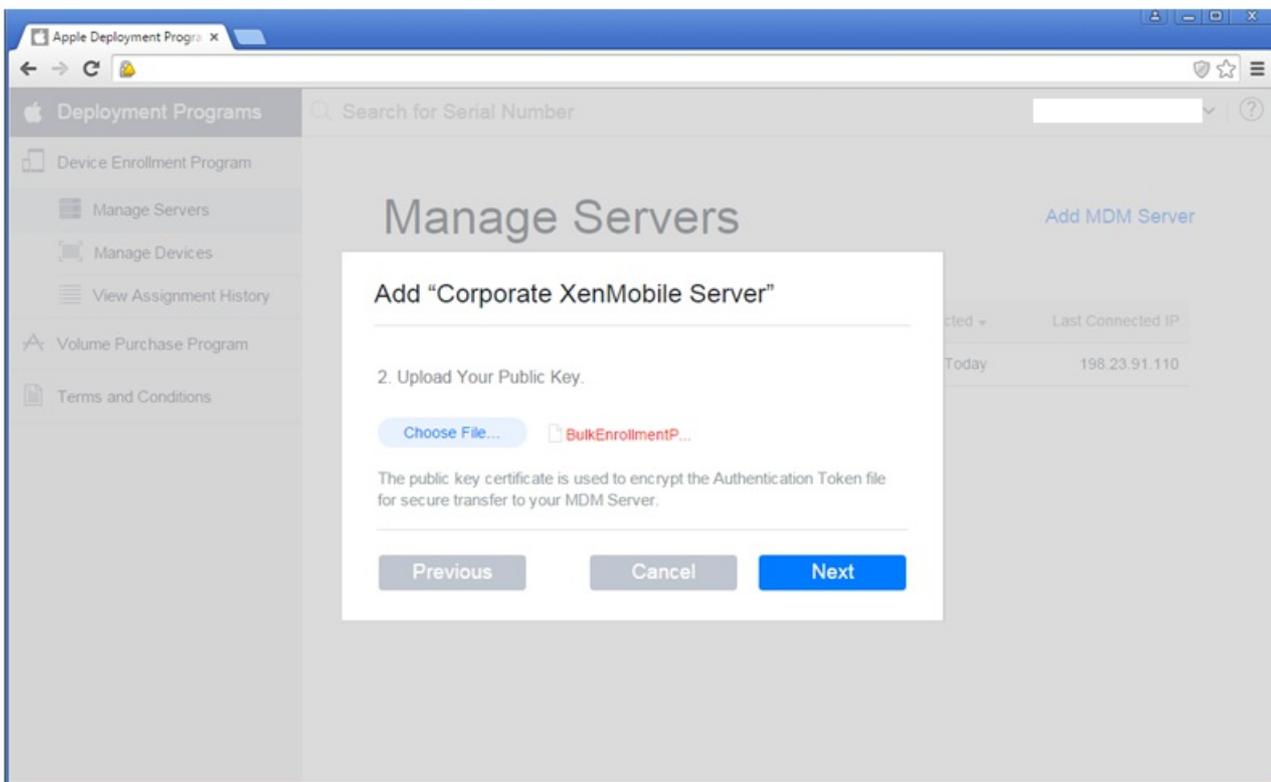
- a. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Settings**.
- b. Bajo la opción **More**, haga clic en **iOS Bulk Enrollment**.



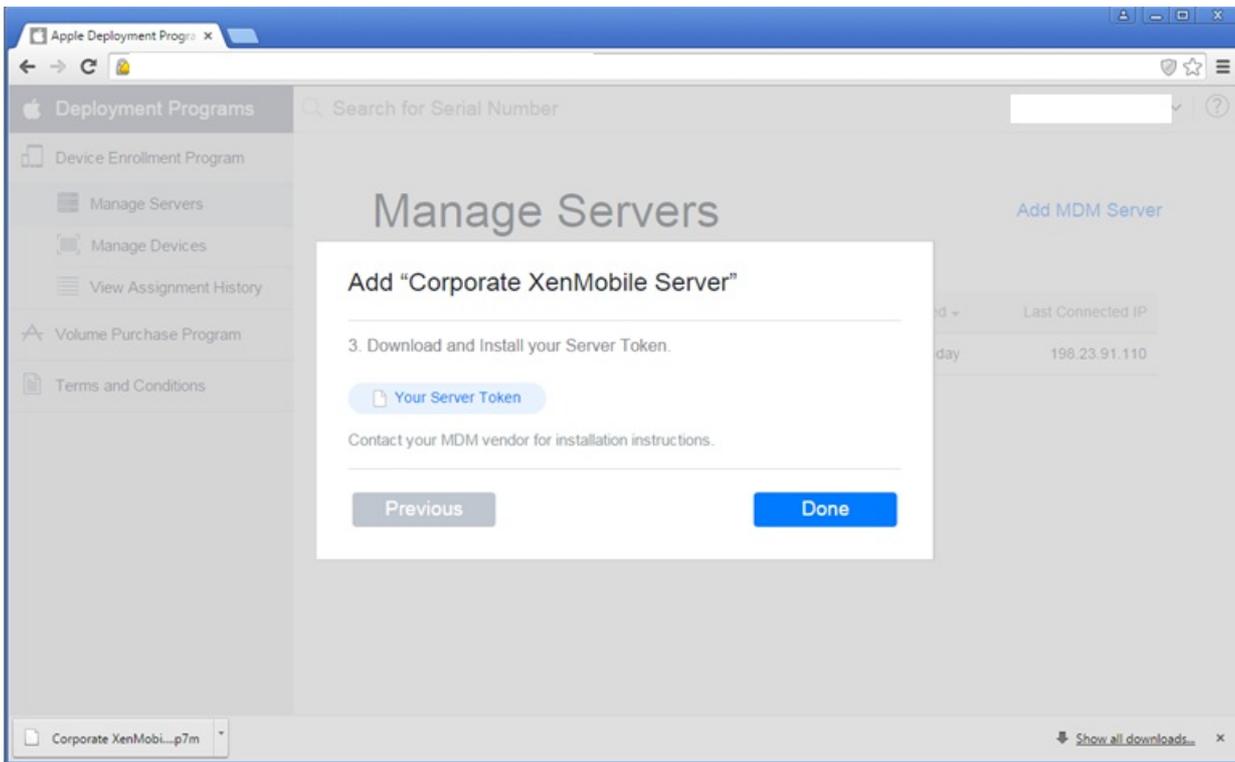
b. En la página **iOS Bulk Enrollment**, expanda **DEP Configuration** y luego haga clic en **Export Public Key**. Se descargará la clave pública.



5. En el portal de Apple DEP, 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**.



7. En la página **iOS Bulk Enrollment** de la consola de XenMobile, junto a **Allow Device Enrollment Program (DEP)**, haga clic en YES, haga clic en **Import Token File** y después cargue el archivo de token que descargó en el paso anterior.

#### ▼ DEP Configuration

Export Public Key |  Import Token File

Allow Device Enrollment Program (DEP)  YES

#### Import Token File

Choose the token file downloaded from the Device Enrollment Program web portal and click Import.

Token File\*

La información del token de Apple DEP aparece en la consola de XenMobile después de importar el archivo de token.

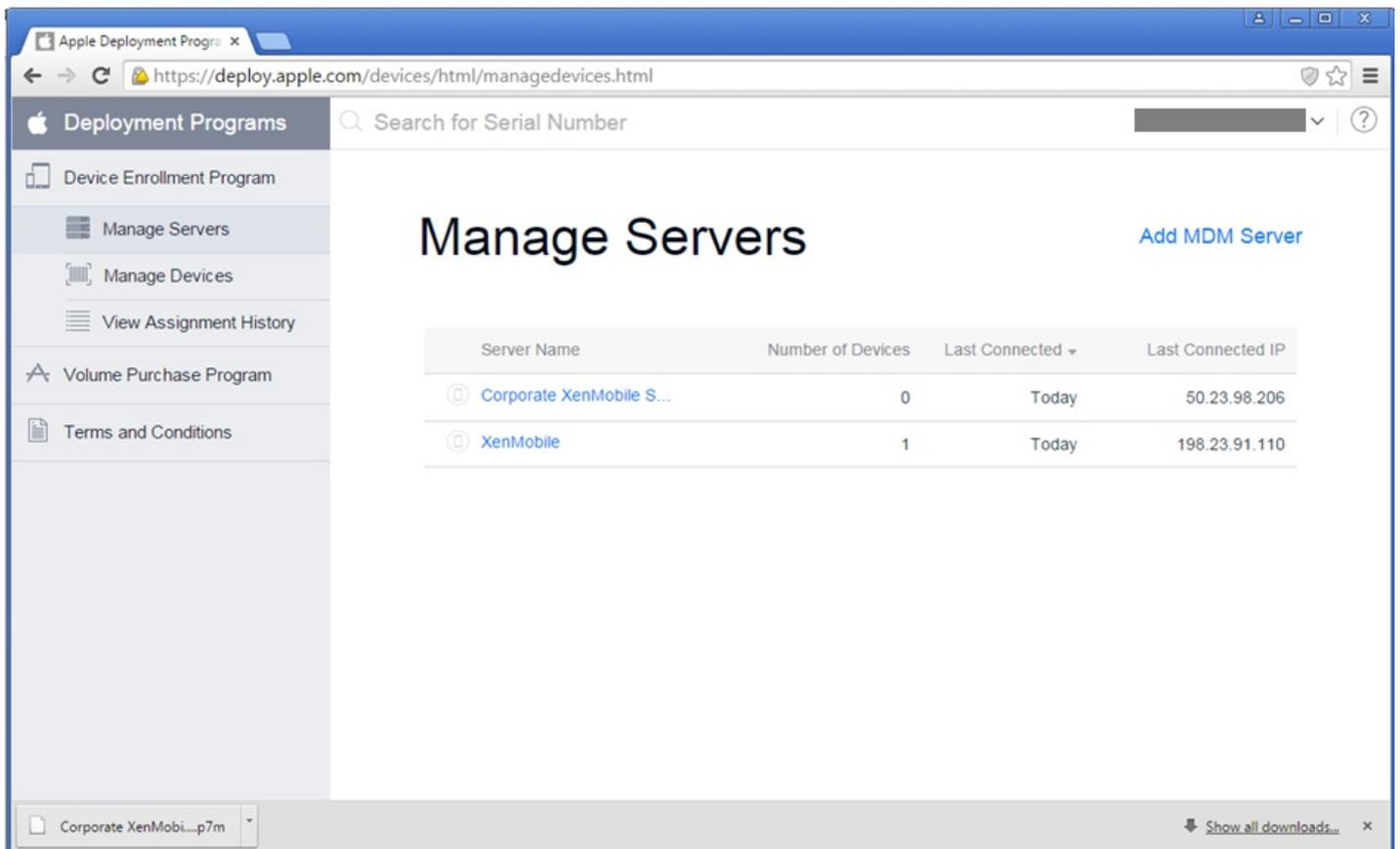
8. Haga clic en **Test Connection** para verificar la conexión de Apple DEP con XenMobile.

#### Server Tokens

Consumer key*	<input type="text"/>
Consumer secret*	<input type="text"/>
Access token*	<input type="text"/>
Access secret*	<input type="text"/>
Access token expiration	<input type="text"/>
<input type="button" value="Test Connection"/>	

9. En la página **iOS Bulk Enrollment**, complete los parámetros adicionales, seleccione los controles y directivas de Apple DEP que quiere implementar para sus dispositivos Apple DEP y luego haga clic en **Save**.

El servidor XenMobile aparece en el portal de Apple DEP.



## Adquirir dispositivos habilitados con DEP

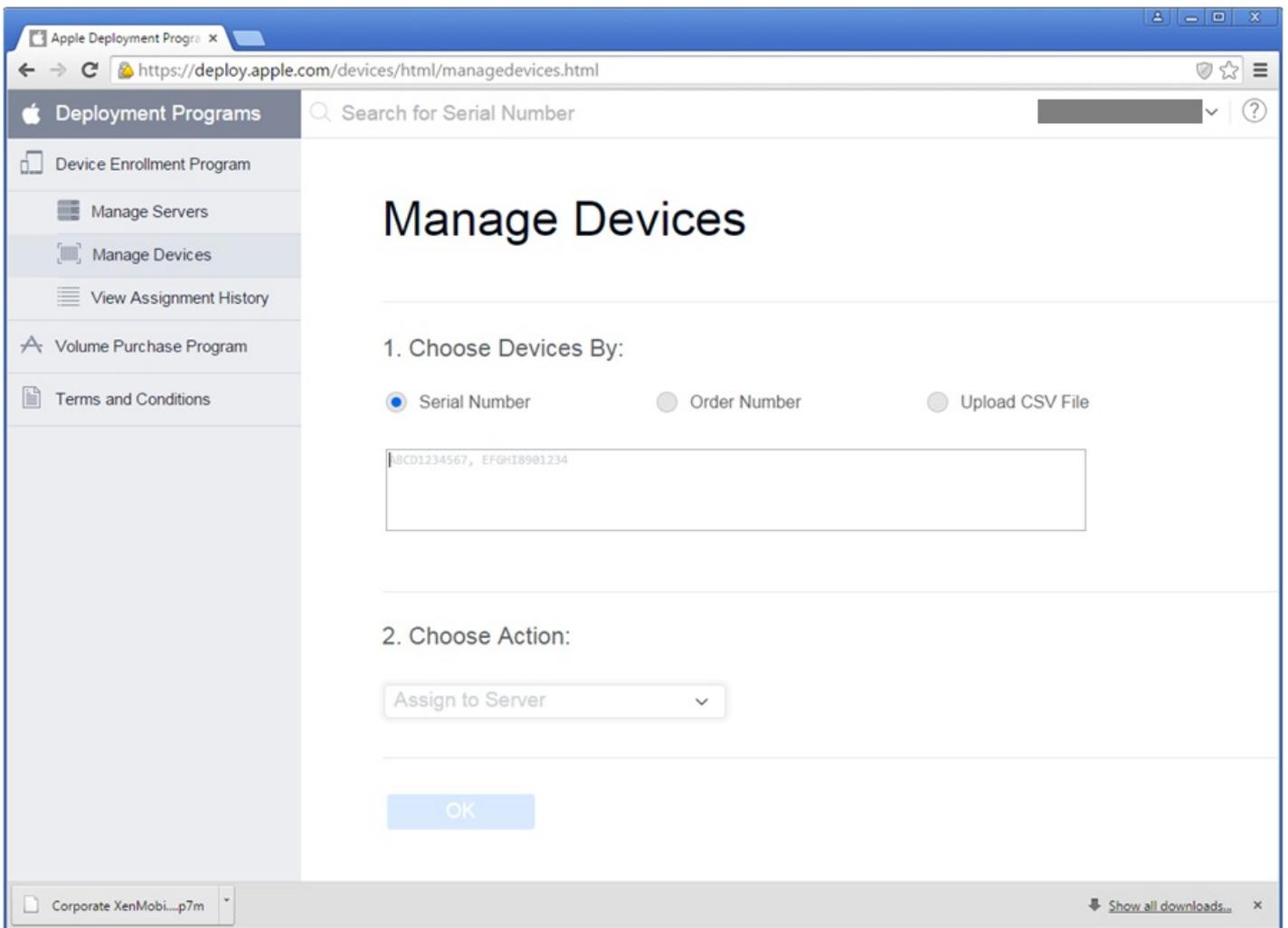
Puede adquirir dispositivos habilitados con DEP directamente desde Apple o de proveedores y operadores autorizados. Para adquirirlos en Apple, necesita suministrar su ID de cliente de Apple en el portal de Apple DEP para permitir que Apple asocie el dispositivo comprado con su cuenta de Apple DEP.

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 del proveedor cuando compre los dispositivos. Necesitará este dato para agregar el proveedor de Apple DEP a su cuenta de Apple DEP. Recibirá un ID de cliente de DEP después de agregar el ID de Apple DEP del proveedor, cuando sea aprobado. Suministre 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](#).

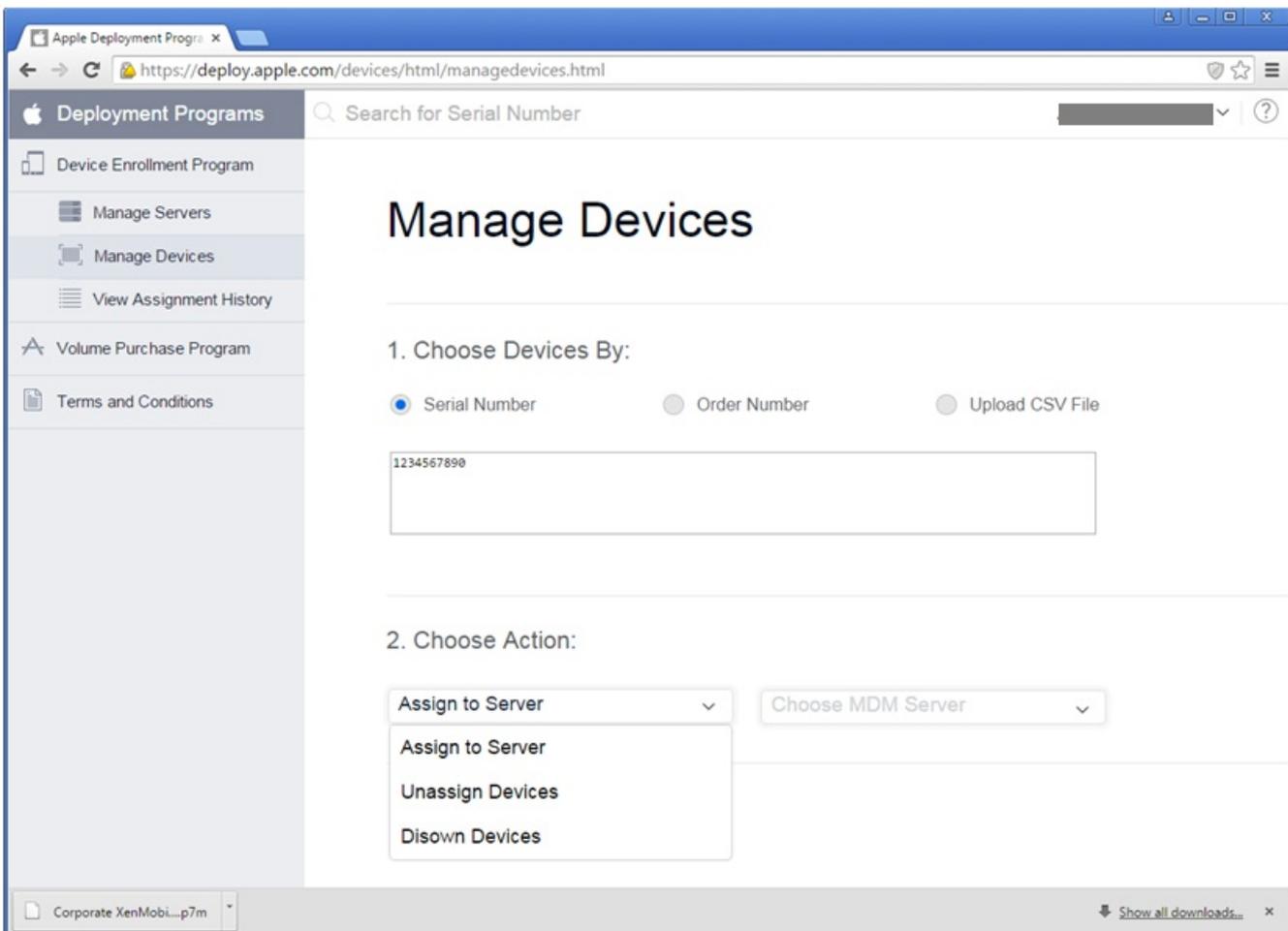
## Administración de dispositivos habilitados con DEP

Siga estos pasos para asociar dispositivos con su servidor XenMobile dentro de la cuenta de Apple DEP a través del portal de DEP.

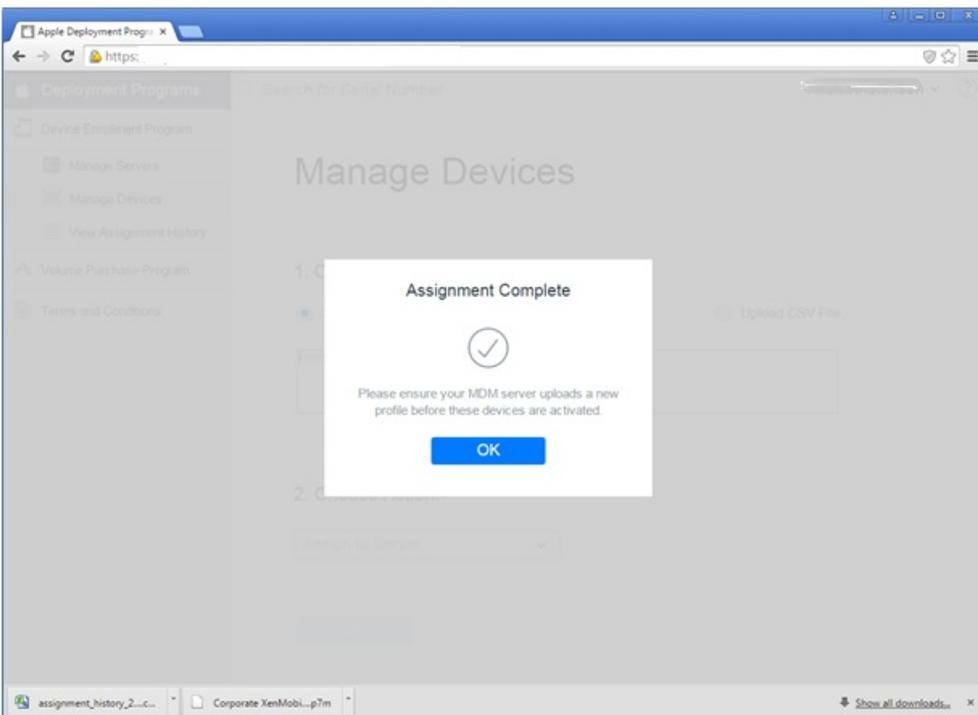
1. Inicie una sesión en el portal de Apple DEP.
2. Haga clic en **Device Enrollment Program**, haga clic en **Manage Devices** y luego en **Choose Devices By**, seleccione la opción con la que quiere cargar y definir sus dispositivos habilitados con Apple DEP: **Serial Number**, **Order Number**, o **Upload CSV File**.



3. En **Choose Action**, para asignar sus dispositivos a un servidor XenMobile, haga clic en **Assign to Server** y luego, en la lista, haga clic en el nombre del servidor XenMobile y 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. Los usuarios utilizan el asistente de configuración para configurar los parámetros iniciales en el dispositivo iOS.
3. El dispositivo inicia automáticamente el proceso de inscripción de dispositivo de XenMobile. Los usuarios siguen los pasos indicados en el asistente para inscribir el dispositivo en el servidor XenMobile asociado con el dispositivo habilitado con Apple DEP.

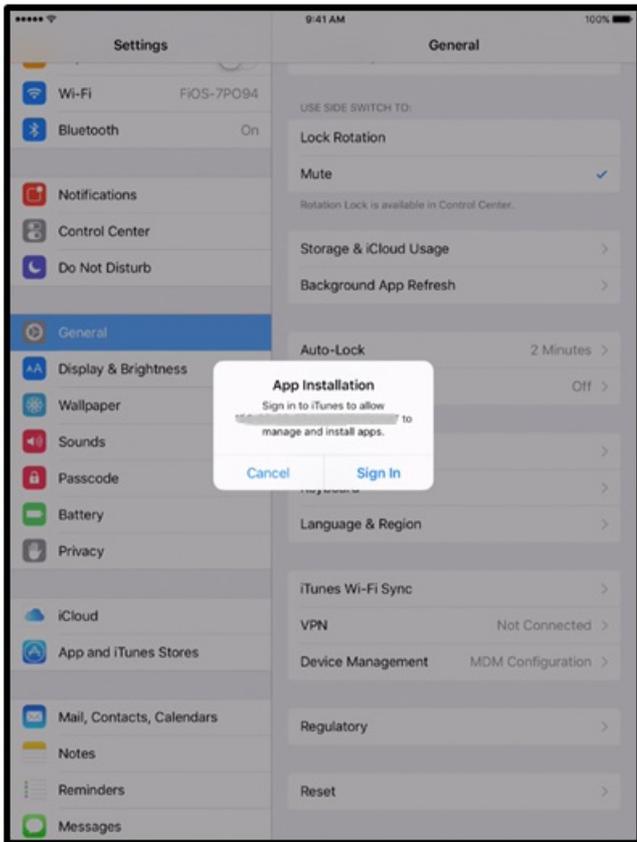
El proceso de inscripción de Apple DEP se inicia automáticamente como parte de la configuración inicial de iOS para los dispositivos habilitados con Apple DEP.



4. La configuración de Apple DEP definida en la consola de XenMobile se entrega al dispositivo habilitado con Apple DEP. Los usuarios siguen los pasos indicados en el asistente para configurar el dispositivo.



5. Puede que se pida a los usuarios que inicien sesión en iTunes para que Secure Hub se pueda descargar.



6. 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.

El resto de las aplicaciones obligatorias se envían e instalan en el dispositivo.

# Propiedades de cliente

Mar 02, 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 o eliminar las propiedades de cliente desde esta página.

XenMobile Analyze Manage Configure administrator

Settings > Client Properties

### Client Properties

To change a property, select the property and then click Edit.

Add

<input type="checkbox"/>	Name	Key	Value	Description
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

Showing 1 - 10 of 19 items Showing 1 of 2

Para agregar una propiedad de cliente

1. Haga clic en **Add**. Aparecerá la página **Add New Client Property**.

XenMobile Analyze Manage Configure admin

Settings > Client Properties > Add New Client Property

### Add New Client Property

Key  ?

Value\*

Name\*

Description\*

Cancel Save

2. Configure los siguientes 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.

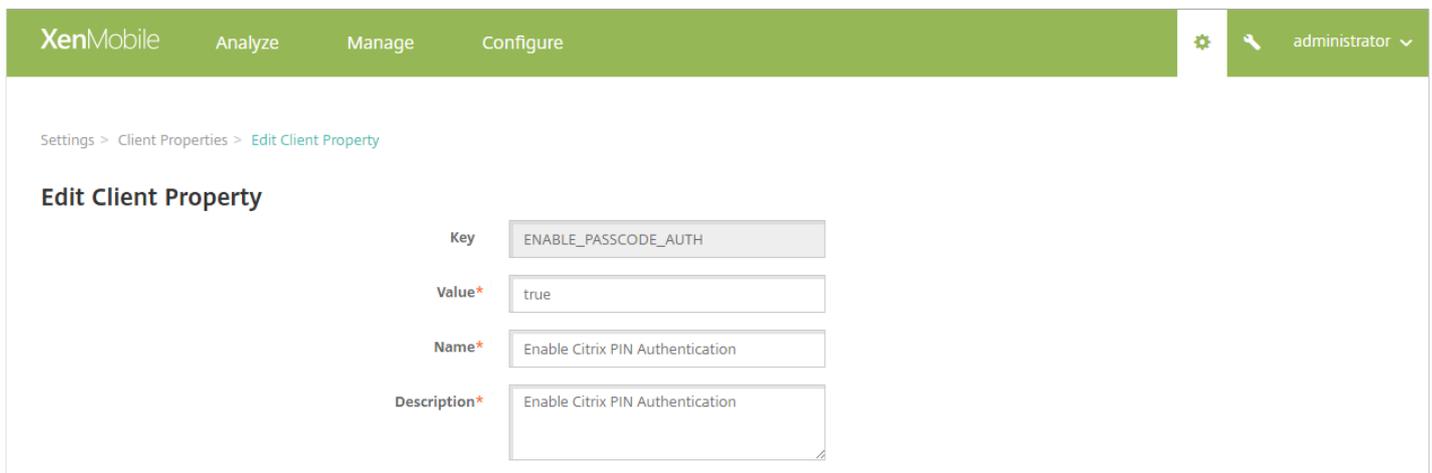
3. Haga clic en **Save**.

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 **Parámetros > Propiedades de cliente**, 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: **true**

#### **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

Esta propiedad habilita o inhabilita la capacidad de que los dispositivos (equipados con esa capacidad) usen la autenticación Touch ID. Los dispositivos de los usuarios deben tener el PIN de Citrix habilitado y la entropía de usuario establecida en **false**, de modo que, cuando los usuarios inician una aplicación, se les pida usar la tecnología 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 período de caducidad de entre 1 y 99 días y luego se cambia por uno mayor durante ese período, los PIN caducarán al final del período 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
Media (parámetro predeterminado)	1. Los números no pueden ser iguales. Por ejemplo, no se permite 444444.  2. Los números no pueden ser consecutivos. Por ejemplo, no se permite 123456 o 654321.  Permitido: 444333, 124567, 136790, 555556, 788888	Además de las reglas para el nivel bajo de seguridad del código de acceso:  1. Las letras y los números no pueden ser iguales. Por ejemplo, no se permiten aaaa11, aa11aa o aaa111.  2. Ni letras ni números pueden ser consecutivos. Por ejemplo, no se permiten abcd12, bcd123, 123abc, xy1234, xyz345, o cba123.  Permitido: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
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.	<p>El código de acceso debe incluir al menos un número, un símbolo especial, una letra mayúscula y una letra minúscula.</p> <p>No permitido: abcd12, Abcd12, dfgh12, jkrtA2</p> <p>Permitido: Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#</p>

## 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. También hay que definir la propiedad de servidor MAM\_MACRO\_SUPPORT.

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

Mar 02, 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, lo que crea una lista de dispositivos que incluye todos los dispositivos que no cumplen ninguno de los demás criterios del filtro y permite o deniega conexiones basándose en esa lista. Si no coincide ninguna regla, el valor predeterminado es permitir implícitamente (Implicit Allow).

**Inactive Devices.** Comprueba si un dispositivo está inactivo según se define en el parámetro Device Inactivity Days Threshold en Server Properties.

**Missing Required Apps.** Comprueba si en un dispositivo faltan aplicaciones requeridas, según se definen en la directiva App Access.

**Non-suggested Apps.** Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva App Access.

**Noncompliant Password.** Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, XenMobile puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva de códigos de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva de códigos de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

**Out of Compliance Devices.** Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo Out of Compliance. Esa propiedad es modificada normalmente por las acciones automatizadas o por las API de XenMobile de terceros.

**Revoked Status.** Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no 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. Si esta opción está habilitada, se garantiza que XenMobile enviará la información de dispositivos Android a ActiveSync Gateway en el caso de que XenMobile no disponga del identificador de ActiveSync correspondiente al usuario del dispositivo Android.

#### **Para configurar 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**.

XenMobile Analyze Manage Configure   admin 

Settings > ActiveSync Gateway

## ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

**All devices**

Activate the following rule(s)

- Anonymous Devices
- Failed Samsung KNOX attestation
- Forbidden Apps
- Implicit Allow and Deny
- Inactive Devices
- Missing Required Apps
- Non-Suggested Apps
- Noncompliant Password
- Out of Compliance Devices
- Revoked Status
- Rooted Android and Jailbroken iOS Devices
- Unmanaged Devices

**Android only**

Send Android domain users to ActiveSync Gateway  YES 

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

Mar 02, 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 Acceso a aplicaciones. 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 de acceso a aplicaciones 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**.

The screenshot shows the XenMobile web interface. At the top, there is a navigation bar with the XenMobile logo and tabs for 'Analyze', 'Manage', and 'Configure'. On the right side of the navigation bar, there is a gear icon for settings and a user profile icon labeled 'admin'. Below the navigation bar, the breadcrumb trail reads 'Settings > Network Access Control'. The main heading is 'Network Access Control' with the subtext 'Enables device compliance.' Underneath, there is a section titled 'Set as not compliant:' followed by a list of ten checkboxes, each with a corresponding label: 'Anonymous Devices', 'Failed Samsung KNOX attestation', 'Forbidden Apps', 'Inactive Devices', 'Missing Required Apps', 'Non-Suggested Apps', 'Noncompliant Password', 'Out of Compliance Devices', 'Revoked Status', and 'Unmanaged Devices'. At the bottom right of the page, there are two buttons: 'Cancel' and 'Save'.

3. Marque las casillas de los filtros **Set as not compliant** que quiera habilitar.

4. Haga clic en **Save**.

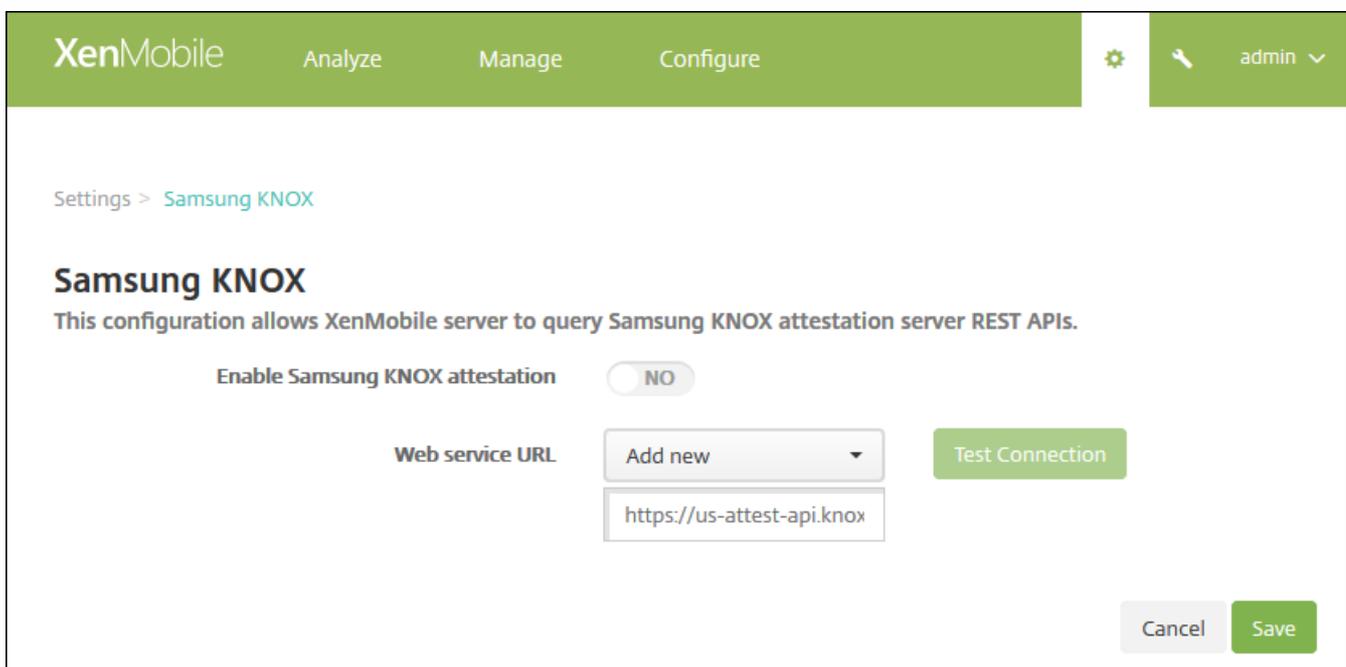
# Samsung KNOX

Mar 02, 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) en tiempo de ejecución en función de los datos recopilados durante un 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**.



The screenshot shows the XenMobile web console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'admin'. The current page is 'Settings > Samsung KNOX'. The main heading is 'Samsung KNOX' with a sub-heading: 'This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.' There is a toggle switch for 'Enable Samsung KNOX attestation' currently set to 'NO'. Below this, the 'Web service URL' section has an 'Add new' dropdown menu and a text input field containing 'https://us-attest-api.knox'. A green 'Test Connection' button is located to the right of the URL field. At the bottom right, there are 'Cancel' and 'Save' buttons.

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**, la opción **Web service URL** se habilita. 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 de Samsung KNOX en masa](#).

# Google Cloud Messaging

Mar 02, 2017

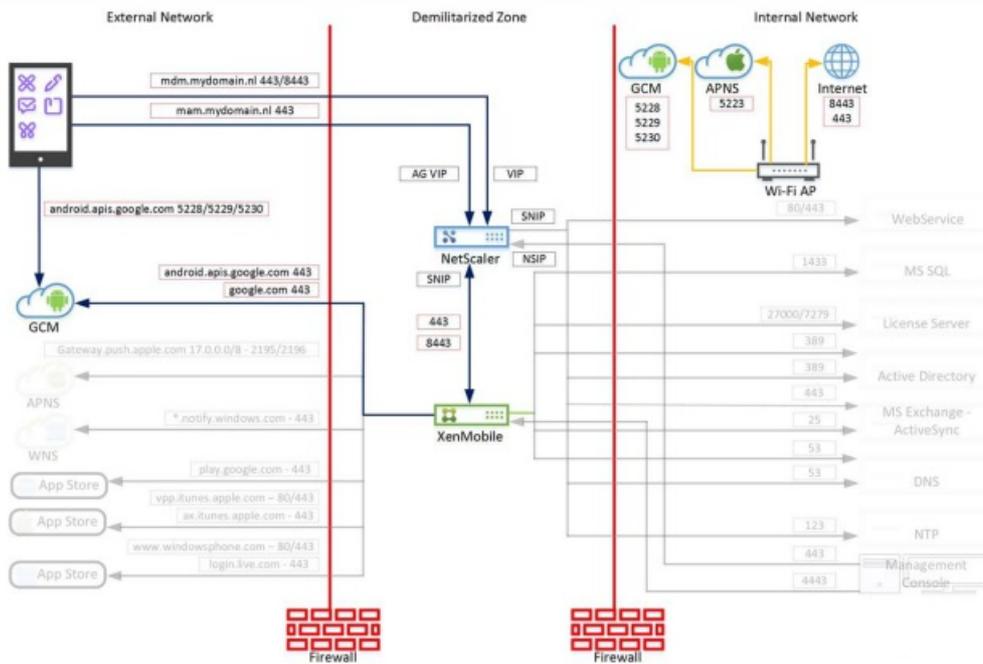
Como alternativa a la directiva MDX, **Active poll period**, puede usar desde Google Cloud Messaging (GCM) para controlar cómo y cuándo los dispositivos Android debe conectarse a XenMobile. Con la configuración que se describe en este artículo, toda acción de seguridad o comando de implementación desencadena una notificación push en Secure Hub para pedir 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 GCM en la red interna y externa.

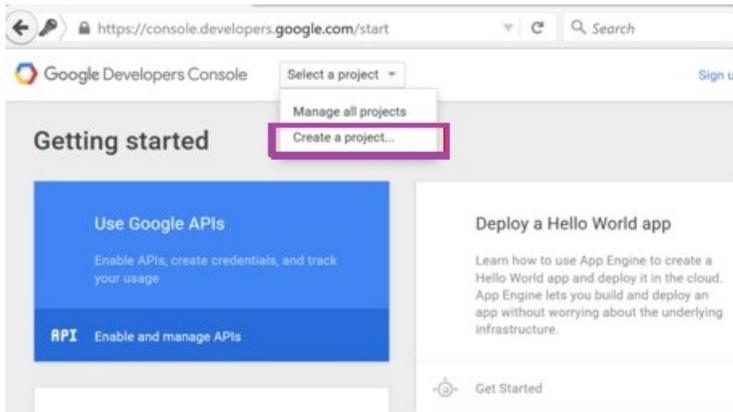


## Para configurar su cuenta de Google para GCM

1. Inicie sesión en la siguiente URL con las credenciales de la cuenta de Google para desarrolladores:

<https://console.developers.google.com>

2. En **Selecciona un proyecto**, seleccione **Crear proyecto**.



3. Escriba un **Project name** y haga clic en **Create**.

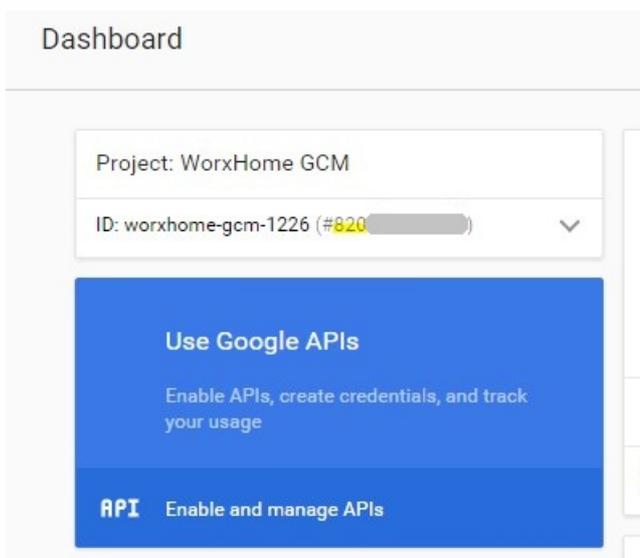
New Project

Project name <sup>?</sup>

Your project ID will be worxhome-gcm-1226 <sup>?</sup> [Edit](#)

[Show advanced options...](#)

4. En el panel de control, aparecerá su ID de envío (resaltado abajo) junto al ID del proyecto. Tome nota de ese ID de envío, porque tendrá que utilizarlo más tarde en los parámetros del servidor XenMobile. Haga clic en **Usar APIs de Google**.



5. En la sección **Mobile APIs**, haga clic en **Google Cloud Messaging**.

## Overview

### Popular APIs



#### Google Cloud APIs

- Compute Engine API
- BigQuery API
- Cloud Storage Service
- Cloud Datastore API
- Cloud Deployment Manager API
- Cloud DNS API
- ⌵ More



#### Google Maps APIs

- Google Maps Android API
- Google Maps SDK for iOS
- Google Maps JavaScript API
- Google Places API for Android
- Google Places API for iOS
- Google Maps Roads API
- ⌵ More



#### Mobile APIs

- Google Cloud Messaging
- Google Play Game Services
- Google Play Developer API
- Google Places API for Android



#### Social APIs

- Google+ API
- Blogger API
- Google+ Pages API
- Google+ Domains API

6. Haga clic en **Habilitar**.

## Overview

← Enable

### Google Cloud Messaging

Google Cloud Messaging allows for push messaging to Android, iOS and Chrome users.

[Learn more](#)

7. En **Credenciales**, haga clic en **Crear credenciales**.

APIs

Credentials

You need credentials to access APIs. [Enable the APIs you plan to use](#) and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. [Refer to the API documentation](#) for details.

Create credentials ▾

8. Haga clic en **Clave de API**.

**API key**  
Identifies your project using a simple API key to check quota and access.  
For APIs like Google Translate.

**OAuth client ID**  
Requests user consent so your app can access the user's data.  
For APIs like Google Calendar.

**Service account key**  
Enables server-to-server, app-level authentication using robot accounts.  
For use with Google Cloud APIs.

Help me choose

9. En **Crear una clave nueva**, haga clic en **Clave de servidor**.

Create a new key

You need an API key to call certain Google APIs. The API key identifies your project. Also, it is used to enforce quotas and handle billing, so keep it safe.

**Server key** | Browser key | Android key | iOS key

10. En **Create server API key**, introduzca un nombre en **Name** (en el ejemplo, se ha utilizado el nombre del proyecto, pero tenga en cuenta que ahora Worx Home se llama Secure Hub). A continuación, haga clic en **Create**.

Create server API key

**This key should be kept secret on your server**

Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request's userIp parameter, if specified. If the userIp parameter is missing, your machine's IP address will be used instead. [Learn more](#)

Name

WorxHome GCM

Accept requests from these server IP addresses (Optional)

Examples: 192.168.0.1, 172.16.0.0/12, 2001:db8::1 or 2001:db8::/64

IP address

Note: It may take up to 5 minutes for settings to take effect

**Create** | Cancel

11. Tome nota de la clave de API. La necesitará para configurar XenMobile.

Display name	Key	Value	Default value	Description
<b>GCM API key</b>	google.gcm.apiKey			GCM API KEY created in Google Developers Console.
GCM registration ID TTL	google.gcm.regIdTtlInDays	10	10	Delay, in days, before renewing device GCM
GCM Sender ID	google.gcm.senderid			The "Project Number" in the Google Develop

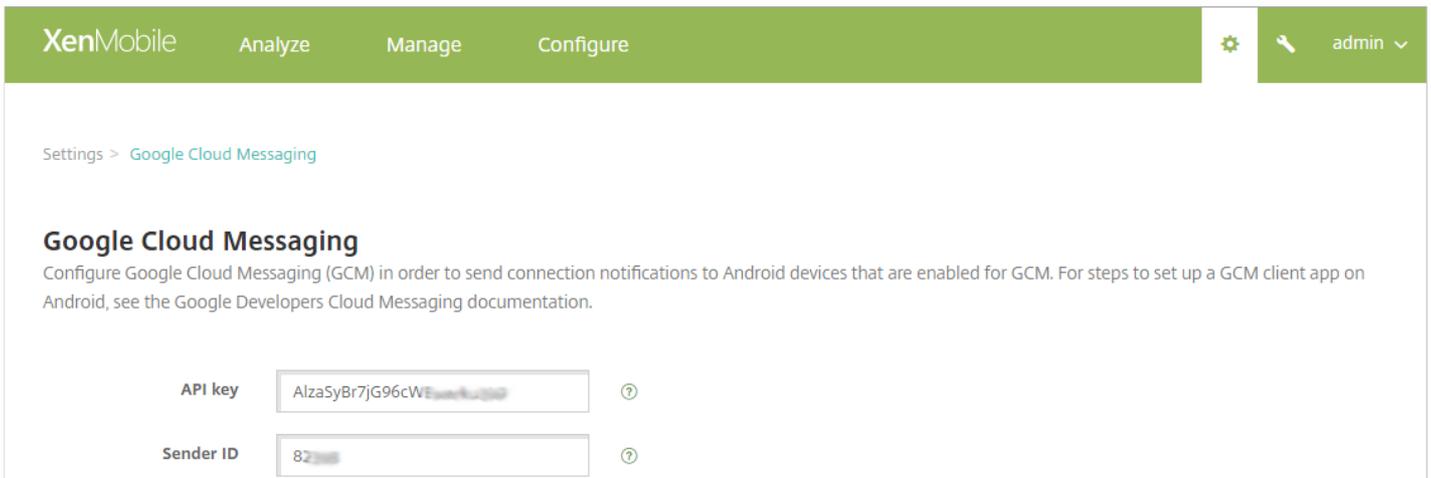
# Para configurar XenMobile para GCM

1. Inicie sesión en la consola de XenMobile y haga clic en **Settings > Google Cloud Messaging**.

a. En **API key**, introduzca la clave API de GCM que copió en el último paso de la configuración de GCM.

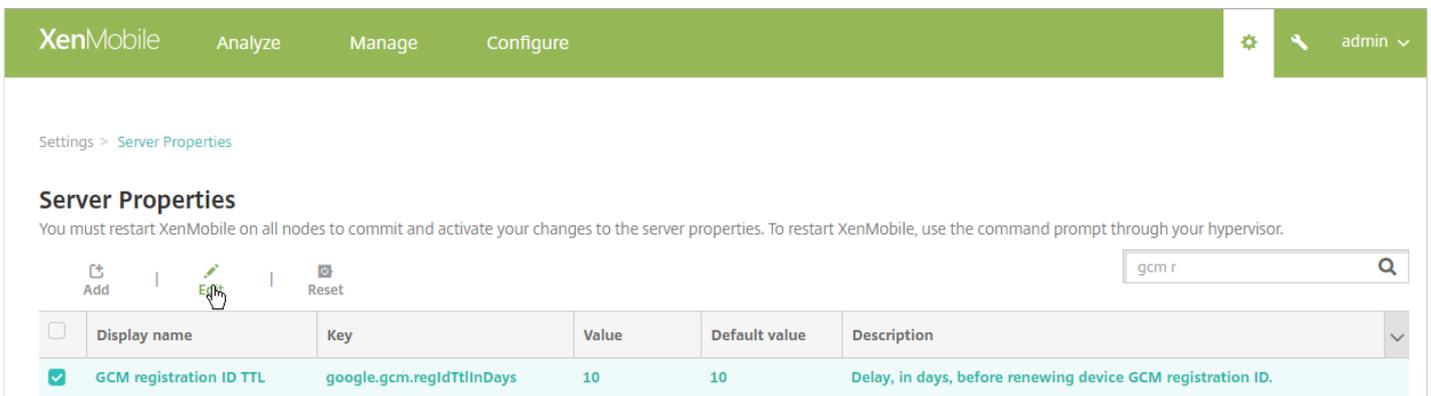
En **Sender ID**, copie el ID de envío que anotó en el procedimiento anterior y haga clic en **Save**.

**Nota:** La página **Settings > Google Cloud Messaging** es nueva en XenMobile 10.3.6. Si no está usando la versión más reciente de XenMobile, vaya a **Settings > Server** para actualizar el valor de **API key** (google.gcm.apiKey) y de **Sender ID** (google.gcm.senderid).



2. Si necesita cambiar los parámetros predeterminados de alguna de las siguientes propiedades, haga clic en **Settings > Server Properties**.

- **GCM Registration ID TTL:** La demora predeterminada antes de renovar el ID de registro de GCM del dispositivo es de **10** días. Para cambiar este valor, escriba **gcm r** en el cuadro de búsqueda, haga clic en **GCM Registration ID TTL**, y luego haga clic en **Edit**.



- **GCM Heartbeat Interval:** La frecuencia predeterminada con la que XenMobile se comunica con el servidor GCM es de **6** horas. Para cambiar este valor, escriba **gcm h** en el cuadro de búsqueda, haga clic en **GCM Heartbeat Interval**, y luego haga clic en **Edit**.

Settings > Server Properties

### Server Properties

You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

gcm h

Display name	Key	Value	Default value	Description
GCM Heartbeat Interval	gcm.heartbeat.interval	6	6	GCM heartbeat frequency in hours. This setting is applicable to android only.

## Para probar la configuración

1. Inscriba un dispositivo Android.
2. Deje el dispositivo inactivo durante algún tiempo, de forma que se desconecte del servidor XenMobile.
3. Inicie sesión en la consola de XenMobile, haga clic en **Manage**, seleccione el dispositivo Android, y, a continuación, haga clic en **Secure**.

XenMobile Analyze **Manage** Configure

Devices Users Enrollment

Devices Show filter

Add Edit **Secure** Notify Delete Import Export Refresh

Status	Mode	User name	Device platform	Operating system version	Device model
<input checked="" type="checkbox"/>	MDM MAM	hemanth@kronos.lab	Android	4.3	GT-I9300

4. En **Device Actions**, haga clic en **Selective Wipe**.

Security Actions

Device Actions

Revoke Lock **Selective Wipe** Full Wipe

Locate

Si la configuración es correcta, el borrado selectivo tiene lugar en el dispositivo sin necesidad de reconectarse a XenMobile.

# Credenciales de Google Play

Mar 02, 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 de identificación de dispositivos para conseguir el ID. El ID que necesita obtener 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 técnica 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.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with the XenMobile logo and tabs for 'Analyze', 'Manage', and 'Configure'. On the right side of the navigation bar, there is a gear icon for settings and a user profile icon labeled 'admin'. Below the navigation bar, the breadcrumb trail reads 'Settings > Google Play Credentials'. The main heading is 'Google Play Credentials'. Below the heading, there is a message: 'XenMobile cannot extract app information without logon information. To find your Android ID, you can type `***#8255***` on your phone.' There are three input fields: 'User name\*' with a placeholder '@gmail.com', 'Password\*' with masked characters, and 'Device ID\*' with the value '123456789123CD01'. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Configure los siguientes 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 dispositivo

Mar 02, 2017

Puede configurar el funcionamiento de XenMobile en los dispositivos gracias a la creación de directivas. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre plataformas e incluso entre dispositivos de diferentes fabricantes que ejecutan Android. Para ver una tabla de directivas por plataforma, descargue el PDF de [Directivas de dispositivo por plataforma](#).

Antes de crear una directiva nueva, lleve a cabo estos pasos:

- Crear los grupos de entrega que se van a utilizar.
- Instalar los certificados de CA necesarios.

A continuación, se presentan los pasos básicos necesarios para crear una directiva de dispositivos:

1. Especificar el nombre y la descripción de la directiva.
2. Configurar una o varias plataformas.
3. Crear las reglas de implementación (opcional).
4. Asignar la directiva a grupos de entrega.
5. Configurar la programación de las implementaciones (opcional).

Puede configurar las siguientes directivas de dispositivo en XenMobile.

<b>Nombre de directiva de dispositivo</b>	<b>Descripción de directiva de dispositivo</b>
Duplicación AirPlay	En XenMobile, puede agregar una directiva de dispositivos para agregar dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) en los dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos permitidos supervisados, lo que limitará a los usuarios a utilizar únicamente los dispositivos AirPlay que se encuentren en ella.
AirPrint	La directiva AirPrint permite agregar impresoras AirPrint a la lista de impresoras AirPrint que aparecen en los dispositivos iOS de los usuarios. Esta directiva facilita el respaldo de entornos en los que las impresoras y los dispositivos están en subredes diferentes.  Nota: <ul style="list-style-type: none"><li>• Esta directiva se aplica a iOS 7.0 y versiones posteriores.</li><li>• Compruebe que dispone de la dirección IP y de la ruta de recursos para cada impresora.</li></ul>
Restricciones de aplicaciones de Android for Work	Con esta directiva, puede modificar las restricciones asociadas a aplicaciones Android for Work. Sin embargo, antes de modificarlas, debe cumplir los siguientes requisitos previos: <ul style="list-style-type: none"><li>• Complete, en Google, las tareas de configuración de Android for Work. Para obtener más información, consulte <a href="#">Administración de dispositivos con Android for Work</a>.</li></ul>

	<ul style="list-style-type: none"> <li>• Cree un conjunto de credenciales de Google Play. Para obtener más información, consulte <a href="#">Credenciales de Google Play</a>.</li> <li>• Cree una cuenta de Android for Work. Para obtener más información, consulte <a href="#">Creación de una cuenta de Android for Work</a>.</li> <li>• Agregue aplicaciones Android for Work a XenMobile. Para obtener más información, consulte <a href="#">Cómo agregar aplicaciones a XenMobile</a>.</li> </ul>
APN	Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. Una directiva de nombres APN determina la configuración utilizada para conectar sus dispositivos al servicio GPRS de un operador concreto. Esta configuración ya está definida en la mayoría de los teléfonos más recientes.
Acceso a aplicaciones	En XenMobile, la directiva de dispositivo Acceso a aplicaciones permite definir una lista de las aplicaciones que deben instalarse obligatoriamente, que pueden instalarse o que no deben instalarse en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento del dispositivo con los requisitos de dicha lista de aplicaciones.
Atributos de aplicación	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.
Configuración de aplicaciones	Con esta directiva, puede configurar, de forma remota, varios parámetros y comportamientos de aplicaciones que admitan la configuración administrada implementando un archivo XML de configuración (denominado "lista de propiedades", o "plist") en los dispositivos iOS de los usuarios o implementando pares de clave/valor en los escritorios, tabletas o teléfonos Windows 10 de los usuarios.
Inventario de aplicaciones	La directiva 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 a las 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.
Bloqueo de aplicaciones	<p>En XenMobile, puede crear una directiva para definir una lista de aquellas aplicaciones cuya ejecución se permite en un dispositivo o una lista de aquellas aplicaciones cuya ejecución debe bloquearse en un dispositivo.</p> <p>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.</p> <p>Nota: Aunque la directiva de dispositivos funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N y posteriores porque Google ha</p>

	<p>dejado de respaldar la API necesaria.</p> <p>En dispositivos iOS, solo se puede seleccionar una aplicación iOS por cada directiva. Lo que significa que los usuarios solo pueden usar su dispositivo para ejecutar una 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.</p>
Uso de red de las aplicaciones	<p>Puede definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas usan, por ejemplo, redes de datos móviles en dispositivos iOS. Las reglas solo se aplican a aplicaciones administradas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de XenMobile. No se incluyen en este grupo aquellas aplicaciones que los usuarios descargan directamente en sus dispositivos (sin que se implementen por medio de XenMobile) ni aquellas aplicaciones que ya estaban instaladas en los dispositivos cuando estos se inscribieron en XenMobile.</p>
Restricciones de aplicaciones	<p>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.</p>
Túneles de aplicaciones	<p>Puede configurar la directiva Túneles de aplicaciones para aumentar la continuidad del servicio y la fiabilidad de la transferencia de datos para las aplicaciones móviles. Los túneles de aplicaciones se usan para definir parámetros de proxy entre el componente del cliente de cualquier aplicación del dispositivo móvil y el componente del servidor de aplicaciones. También puede usar túneles de aplicaciones con el objetivo de crear túneles de asistencia remota dirigidos a un dispositivo para ofrecer asistencia en administración.</p> <p>Nota: Todo tráfico de aplicaciones enviado a través de un túnel definido en esta directiva pasará por XenMobile antes de redirigirse al servidor que ejecuta la aplicación.</p>
Desinstalación de aplicaciones	<p>La directiva Desinstalación de aplicaciones permite quitar aplicaciones de los dispositivos de los usuarios por las razones pertinentes. Es posible que ya no quiera respaldar ciertas aplicaciones o que la empresa quiera sustituir las aplicaciones existentes por aplicaciones similares provenientes de otros proveedores, entre varios motivos. Las aplicaciones se quitan cuando esta directiva se implementa en los dispositivos de los usuarios. A excepción de los dispositivos Samsung KNOX, los usuarios reciben una solicitud para desinstalar la aplicación; los usuarios de dispositivos Samsung KNOX no recibirán ninguna solicitud para desinstalar la aplicación.</p>
Restricciones de desinstalación de aplicaciones	<p>Con esta directiva, puede especificar las aplicaciones que los usuarios pueden o no pueden desinstalar.</p>
Explorador Web	<p>Con las directivas de explorador, puede definir si los dispositivos de los usuarios pueden usar el explorador Web o limitar las funciones del explorador que se puedan usar. En dispositivos Samsung, puede inhabilitar completamente el explorador, puede habilitar o inhabilitar los</p>

	<p>elementos emergentes, JavaScript, las cookies, la función de completado automático, y también puede decidir si forzar advertencias de fraude. En dispositivos Android for Work, puede incluir direcciones URL específicas en listas de URL permitidas o prohibidas; también puede agregar marcadores de explorador concretos y seguros.</p>
Calendario (CalDav)	<p>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.</p>
Móvil	<p>Esta directiva permite configurar los parámetros de red de telefonía móvil.</p>
Administrador de conexiones	<p>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.</p>
Contactos (CardDAV)	<p>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.</p>
Copiar aplicaciones al contenedor de Samsung	<p>Puede especificar que las aplicaciones que ya están instaladas en un dispositivo se copien en un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles. Las aplicaciones que se copien al contenedor SEAMS estarán disponibles en las pantallas de inicio de los usuarios, mientras que las aplicaciones que se copien al contenedor KNOX solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.</p>
Credenciales	<p>En XenMobile, puede crear directivas de credenciales para habilitar la autenticación integrada con la configuración de PKI (como una entidad de infraestructura PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor). Para obtener más información acerca de las credenciales, consulte <a href="#">Certificados en XenMobile</a>.</p> <p>Cada plataforma de dispositivo requiere un conjunto diferente de valores, que se describen en el artículo sobre la directiva de credenciales.</p> <p>Nota: Antes de crear esta directiva, necesitará la información de credenciales que vaya a utilizar para cada plataforma, además de los certificados en sí y las contraseñas.</p>
Copiar aplicaciones al contenedor de Samsung	<p>Puede especificar que las aplicaciones que ya están instaladas en un dispositivo se copien en un contenedor SEAMS o un contenedor KNOX en dispositivos Samsung compatibles. Para obtener más información sobre los dispositivos respaldados, consulte <a href="#">Dispositivos Samsung KNOX respaldados</a>. 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.</p>
Credenciales	<p>A menudo se usa conjuntamente con una directiva de Wi-Fi. Esta directiva permite a las empresas</p>

	<p>implementar certificados para la autenticación en recursos internos que requieren autenticación mediante certificado.</p>
XML personalizado	<p>Puede crear directivas XML personalizadas en XenMobile cuando desee personalizar las siguientes características:</p> <ul style="list-style-type: none"> <li>• El aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o inhabilitación de las funciones.</li> <li>• La configuración de dispositivos, que incluye la capacidad para permitir a los usuarios cambiar la configuración y los parámetros de sus dispositivos.</li> <li>• 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.</li> <li>• Los errores de administración, que incluye la recepción de informes de error y de estado del dispositivo.</li> </ul> <p>Puede crear su propia configuración XML personalizada mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows. Este apartado no abarca la creación de contenido XML personalizado con la API de OMA DM. Para obtener más información sobre el uso de la API de OMA DM, consulte <a href="#">OMA Device Management</a> en el sitio de Microsoft Developer Network.</p>
Eliminar archivos y carpetas	<p>En XenMobile, puede crear una directiva para eliminar archivos o carpetas específicas de los dispositivos Windows Mobile/CE.</p>
Eliminar claves y valores del Registro	<p>En XenMobile, puede crear una directiva para eliminar de los dispositivos Windows Mobile/CE claves y valores específicos del Registro.</p>
Atestación del estado de dispositivos	<p>En XenMobile, puede crear una directiva para requerir que los dispositivos Windows 10 informen de su estado, haciendo que dichos dispositivos envíen ciertos datos e información de tiempo de ejecución al servicio Health Attestation Service (HAS) para su posterior análisis. El servicio HAS crea y devuelve un certificado de atestación de estado que el dispositivo envía a XenMobile. Cuando XenMobile recibe el certificado de atestación de estado, según el contenido de este, puede implementar las acciones automatizadas que haya configurado previamente.</p> <p>Los datos que se comprueban en el servicio HAS son:</p> <ul style="list-style-type: none"> <li>• AIKPresent</li> <li>• Bit Locker Status</li> <li>• BootDebuggingEnabled</li> <li>• Boot Manager Rev List Version</li> <li>• CodeIntegrityEnabled</li> <li>• Code Integrity Rev List Version</li> <li>• DEP Policy</li> <li>• ELAMDriverLoaded</li> <li>• Issued At</li> </ul>

	<ul style="list-style-type: none"> <li>● KernelDebuggingEnabled</li> <li>● PCR</li> <li>● Reset Count</li> <li>● Restart Count</li> <li>● SafeModeEnabled</li> <li>● SBCP Hash</li> <li>● SecureBootEnabled</li> <li>● TestSigningEnabled</li> <li>● VSMEnabled</li> <li>● WinPEEnabled</li> </ul> <p>Para obtener información, consulte la página <a href="#">HealthAttestation CSP</a> de Microsoft.</p>
Nombre del dispositivo	<p>Con la directiva Nombre del dispositivo, puede definir los nombres de dispositivos iOS y Mac OS X para poder identificarlos fácilmente. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Para obtener más información acerca de las macros, consulte <a href="#">Macros en XenMobile</a>.</p>
Hub empresarial	<p>Una directiva Enterprise Hub para dispositivos Windows Phone permite distribuir aplicaciones a través de la tienda Enterprise Hub de la empresa.</p> <p>Antes de crear la directiva, necesita lo siguiente:</p> <ul style="list-style-type: none"> <li>● Un certificado de firma AET (.aetx) de Symantec</li> <li>● La aplicación Citrix Company Hub firmada mediante la herramienta de firma de aplicaciones de Microsoft (XapSignTool.exe)</li> </ul> <p>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.</p>
Exchange	<p>Con XenMobile tiene dos opciones para entregar el correo electrónico. Puede entregar correo electrónico ActiveSync con la aplicación Secure Mail en el contenedor, o bien puede usar esta directiva Exchange de MDM para habilitar el correo electrónico ActiveSync para el cliente de correo nativo del dispositivo.</p>
Archivos	<p>Con esta directiva, puede agregar archivos de script a XenMobile para realizar algunas funciones para los usuarios. También puede agregar documentos a los que quiera que los usuarios de los dispositivos Android puedan acceder desde sus dispositivos. Cuando agregue el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo. Por ejemplo, si quiere que los usuarios de Android reciban un documento de empresa o archivo PDF, puede implementar el archivo en el dispositivo y permitir que los usuarios sepan dónde se encuentra el archivo.</p>

	<p>Puede agregar los siguientes tipos de archivo con esta directiva:</p> <ul style="list-style-type: none"> <li>• Archivos de texto (XML, HTML, PY, etc.)</li> <li>• Otros archivos, como documentos, imágenes, hojas de cálculo o presentaciones</li> <li>• Solo para Windows Mobile y Windows CE: archivos de script creados con MortScript</li> </ul>
Fuente	<p>En XenMobile, puede agregar esta directiva de dispositivo para agregar fuentes de texto adicionales a los dispositivos iOS y Mac OS X de los usuarios. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.otf). No se admiten las colecciones de fuentes (.ttc o .otc).</p> <p>Nota: Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.</p>
Importar perfil de iOS y Mac OS X	<p>Puede importar en XenMobile archivos XML de configuración de dispositivos iOS y OS X. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator. Para obtener más información sobre cómo usar Apple Configurator para crear un archivo de configuración, consulte la página de ayuda de <a href="#">Apple Configurator</a>.</p>
Pantalla completa	<p>En XenMobile, puede crear una directiva de pantalla completa para especificar que, en los dispositivos Samsung SAFE, solo se puede utilizar una aplicación o unas aplicaciones concretas. Esta directiva es útil para los dispositivos de empresa diseñados para ejecutar solo un tipo o clase específicos de aplicaciones. Asimismo, esta directiva permite elegir imágenes personalizadas para la pantalla de inicio y fondos para la pantalla de bloqueo del dispositivo cuando el dispositivo está en modo quiosco.</p> <p>Nota:</p> <ul style="list-style-type: none"> <li>• Todas las aplicaciones que especifique para el modo quiosco deben estar ya instaladas en los dispositivos de los usuarios.</li> <li>• Algunas opciones solo se aplican a Samsung Mobile Device Management (MDM) API 4.0 y versiones posteriores.</li> </ul>
Configuración de Launcher	<p>Con esta directiva para dispositivos Android, puede especificar las aplicaciones que permite Citrix Launcher, un logo personalizado para el icono de Citrix Launcher, una imagen de fondo personalizado para Citrix Launcher, así como los requisitos de contraseña para salir de Citrix Launcher.</p>
LDAP	<p>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.</p> <p>Es necesario el nombre de host del servidor LDAP antes de configurar esta directiva.</p>
Ubicación	<p>La directiva de ubicación se puede usar para ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado GPS para Secure Hub. Una vez que esta directiva se envía al dispositivo, los administradores pueden emitir un comando de localización geográfica</p>

	<p>desde el servidor XenMobile y el dispositivo responderá con las coordenadas de su ubicación. También se pueden aplicar directivas de geocerca y seguimiento geográfico.</p>
Correo	<p>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.</p>
Dominios administrados	<p>Con esta directiva puede definir los dominios administrados que se aplicarán al correo electrónico y al explorador Web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari. Así, puede especificar las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador Web. Esta directiva solo está disponible para dispositivos supervisados con iOS 8 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte <a href="#">Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator</a>.</p> <p>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.</p> <p>Cuando un usuario intente abrir un elemento (documento, adjunto o descarga) con Safari desde un dominio que no conste en la lista de dominios Web administrados, la aplicación de empresa correspondiente abrirá el elemento. Si el elemento no es de un dominio Web que conste en la lista de dominios Web administrados, el usuario no podrá abrir el elemento con la aplicación de empresa, y deberá usar una aplicación personal no administrada.</p>
Opciones de MDM	<p>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 <a href="#">Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator</a> o <a href="#">Inscripción masiva de iOS</a>.</p> <p>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.</p>
Información sobre la organización	<p>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.</p>
Código de acceso	<p>Una directiva de código de acceso permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Con esta directiva se puede definir la complejidad y el tiempo de</p>

	espera del código de acceso en el dispositivo.
Hotspot personal	Con esta directiva puede permitir que los usuarios se conecten a Internet aunque estén fuera del alcance de una red Wi-Fi, utilizando la conexión de datos móviles a través de la función Compartir Internet de sus dispositivos iOS. Disponible en iOS 7.0 y versiones posteriores.
Eliminación de perfiles	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.
Perfil de aprovisionamiento	<p>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.</p> <p>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.</p> <p>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 faltan 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.</p>
Eliminación de un perfil de aprovisionamiento	Puede eliminar perfiles de aprovisionamiento iOS con la ayuda de directivas de dispositivo. Para obtener más información acerca de los perfiles de aprovisionamiento, consulte <a href="#">Cómo agregar un perfil de aprovisionamiento</a> .
Proxy	<p>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.</p> <p>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 <a href="#">Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator</a>.</p>
Registro del	El Registro de Windows Mobile/CE almacena datos sobre las aplicaciones, los controladores, las

sistema	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.
Asistencia remota	<p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Premium. Esta opción permite controlar de forma remota la pantalla del dispositivo, incluido el control sobre los colores (ya sea en la ventana principal o en una ventana separada flotante). Asimismo, permite establecer una sesión mediante voz sobre IP (VoIP) entre el servicio de asistencia técnica y el usuario, configurar parámetros y establecer una sesión de chat entre el usuario y el departamento de asistencia técnica.</li> </ul>
Restricciones	<p>La directiva de restricciones ofrece al administrador diversas opciones para bloquear y controlar las características y la funcionalidad de los dispositivos administrados. Existen cientos de opciones de restricción para los dispositivos respaldados, que van desde inhabilitar la cámara o el micrófono del dispositivo móvil, a imponer reglas de roaming y acceso a servicios externos como, por ejemplo, tiendas de aplicaciones.</p> <p>En XenMobile, puede agregar una directiva de dispositivos para restringir algunas funciones en los teléfonos, las tabletas y los dispositivos de los usuarios, entre otros. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.</p> <p>Esta directiva permite o prohíbe a los usuarios utilizar funciones determinadas, como la cámara, en sus dispositivos. También puede estipular restricciones de seguridad, de contenido multimedia y de tipos de aplicaciones que los usuarios puedan o no puedan instalar. El valor predeterminado de la mayoría de las opciones de restricción es "ON" o "allows". Las excepciones principales son la función "Security - Force" de iOS y todas las funciones de tabletas Windows, que tienen el valor predeterminado "OFF" o "restricts".</p> <p>Sugerencia: Si selecciona "ON" para alguna opción, el usuario podrá realizar la operación o usar la función. Por ejemplo:</p> <ul style="list-style-type: none"> <li>• Cámara. 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.</li> <li>• Capturas de pantalla. 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.</li> </ul>
Roaming	<p>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.</p>

Firewall de Samsung SAFE	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.
Clave de licencia de Samsung MDM	<p>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.</p> <p>Debe habilitar las API de la solución SAFE por medio de la implementación de la clave integrada de Samsung Enterprise License Management (ELM) a un dispositivo antes de implementar directivas y restricciones de la solución SAFE. Para habilitar la API de Samsung KNOX, además de implementar la clave ELM de Samsung, también deberá adquirir una licencia de Samsung KNOX mediante el sistema Samsung KNOX License Management System (KLMS). Samsung KLMS aprovisiona licencias válidas a las soluciones de administración de dispositivos móviles para permitirles activar las API de Samsung KNOX en los dispositivos móviles. Estas licencias se deben obtener de Samsung, no las proporciona Citrix.</p> <p>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. Cuando se implementa la clave de Samsung ELM, el parámetro "Samsung MDM API available" se establece en "True".</p>
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 ha habilitado Google FCM, un dispositivo no podrá volver a conectarse al servidor. Por lo tanto, es importante enviar esta directiva en el paquete base para los dispositivos que se inscriben.
SCEP	Esta directiva permite configurar dispositivos iOS y Mac OS X para obtener un certificado mediante el Protocolo de inscripción de certificados simple (SCEP) desde un servidor SCEP externo. Si quiere entregar un certificado al dispositivo mediante el protocolo SCEP desde una infraestructura de clave pública que está conectada a XenMobile, debe crear una entidad de infraestructura de clave pública y un proveedor de PKI en modo distribuido. Para obtener más información, consulte <a href="#">Entidades de infraestructura PKI</a> .
Clave de sideloading	En XenMobile, la instalación de aplicaciones mediante "sideloading" permite implementar en dispositivos Windows 8.1 aplicaciones no adquiridas en la Tienda Windows. Por regla general, se realiza una instalación sideloading de aquellas aplicaciones que se desarrollan para uso corporativo y que no están pensadas para hacerse públicas en la Tienda Windows. Para realizar una instalación sideloading de las aplicaciones, configure la clave de sideloading y las activaciones de la clave. A continuación, puede implementar esas aplicaciones en los dispositivos de los usuarios.

	<p>Para crear esta directiva, necesita la siguiente información:</p> <ul style="list-style-type: none"> <li>• La clave de producto de carga lateral, que obtiene al iniciar sesión en el <a href="#">Centro de servicios de licencias por volumen de Microsoft</a></li> <li>• La activación de la clave, que se crea mediante la línea de comandos después de obtener la clave de producto de sideloading</li> </ul>
Certificado de firma	<p>En XenMobile, puede agregar una directiva de dispositivos para configurar los certificados de firma utilizados para firmar archivos APPX. Necesita certificados de firma si quiere distribuir archivos APPX a los usuarios para que puedan instalarse aplicaciones en sus tabletas Windows.</p>
Cuenta de inicio Single Sign-On (SSO)	<p>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.</p> <p>Nota: Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.</p>
Cifrado de almacenamiento	<p>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.</p> <p>Puede crear directivas para dispositivos Samsung SAFE, Windows Phone y Android Sony. Cada plataforma requiere un conjunto diferente de valores, que se describen en el artículo referente a la directiva Encryption en esta sección.</p>
Calendarios suscritos	<p>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 <a href="http://www.apple.com/downloads/macosx/calendars">www.apple.com/downloads/macosx/calendars</a>.</p> <p>Nota: Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.</p>
Términos y condiciones	<p>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.</p> <p>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</p>

	<p>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.</p>
VPN	<p>Para los clientes que quieran ofrecer acceso a sistemas backend con tecnología antigua de VPN Gateway, esta directiva de VPN se puede usar para enviar los datos de la conexión de puerta de enlace VPN al dispositivo. Se da respaldo a varios proveedores de VPN a través de esta directiva, incluidos Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y habilitar VPN a demanda (siempre que la puerta de enlace VPN respalde esta opción).</p> <p>En XenMobile, puede agregar una directiva de dispositivos para configurar los parámetros de una red privada virtual (VPN) que permita a los dispositivos de los usuarios conectarse de forma segura a los recursos de la empresa. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en el artículo VPN de esta sección.</p>
Fondo de pantalla	<p>Puede agregar un archivo JPG o PNG para establecer un fondo de escritorio en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Disponible en iOS 7.1.2 y versiones posteriores. Para usar fondos de pantalla diferentes en dispositivos iPad y iPhone, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.</p>
Filtro de contenido Web	<p>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 <a href="#">Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator</a>.</p>
Clip Web	<p>Con esta directiva, puede colocar los accesos directos a sitios Web o clips Web de forma que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips Web en dispositivos iOS, Mac OS X y Android; las tabletas Windows solo requieren una etiqueta y una URL.</p>
WiFi	<p>La directiva WiFi permite que los administradores puedan enviar datos de enrutadores de WiFi a los dispositivos administrados: SSID y datos de autenticación y configuración.</p> <p>Mediante las directivas de redes WiFi, puede administrar el modo en que los usuarios conectan sus dispositivos a redes inalámbricas WiFi. Para ello, deberá definir los nombres y los tipos de red, las directivas de seguridad y de autenticación, si se van a usar servidores proxy, y otros datos relacionados con redes WiFi de manera uniforme para todos los usuarios de las plataformas de dispositivo que seleccione.</p>
Certificado de	<p>Agregue esta directiva de dispositivo para crear y entregar certificados de Windows Mobile/CE</p>

Windows 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 <a href="#">Certificados</a> .
XenMobile Store	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.
Opciones de XenMobile	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.
Desinstalación de XenMobile	En XenMobile, puede agregar esta directiva de dispositivo para desinstalar XenMobile de dispositivos Android y Windows Mobile/CE. Cuando se implementa, esta directiva elimina XenMobile de todos los dispositivos que contenga el grupo de implementación.

### La página de directivas de dispositivos en la consola

En la consola de XenMobile, puede trabajar con directivas de dispositivos desde la página **Device Policies**. Para llegar a la página **Device Policies**, haga clic en **Configure > Device Policies**. Desde aquí, puede agregar, modificar o eliminar directivas y ver el estado de las existentes.

La página **Device Policies** contiene una tabla que muestra todas las directivas en vigor.

The screenshot shows the XenMobile console interface. The main navigation bar is green and includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is selected, and within it, the 'Device Policies' sub-tab is active. Below the sub-tabs, there is a search bar and 'Add' and 'Export' buttons. A table displays the following data:

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status
<input type="checkbox"/>	MBWifi	Wifi	10/26/15 1:03 PM	10/26/15 1:03 PM	
<input type="checkbox"/>	Passcode	Password	10/29/15 8:33 AM	10/29/15 8:33 AM	
<input type="checkbox"/>	Restrictions	Restrictions	10/29/15 8:34 AM	10/29/15 8:34 AM	
<input type="checkbox"/>	Personal Hotspot	Personal Hotspot	10/29/15 8:35 AM	10/29/15 8:35 AM	

Showing 1 - 4 of 4 items

Para modificar o eliminar una directiva de la página **Device Policies**, marque la casilla situada junto a esa directiva para que aparezca el menú de opciones encima de la lista de directivas. También puede hacer clic en una directiva de la lista para que

aparezca el menú de opciones a la derecha de la lista. Si hace clic en **Show More**, aparecerán datos detallados de la directiva.

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', there is a search bar and a table of policies. The 'Passcode' policy is selected, and a deployment summary dialog is open over it. The dialog shows the following deployment status:

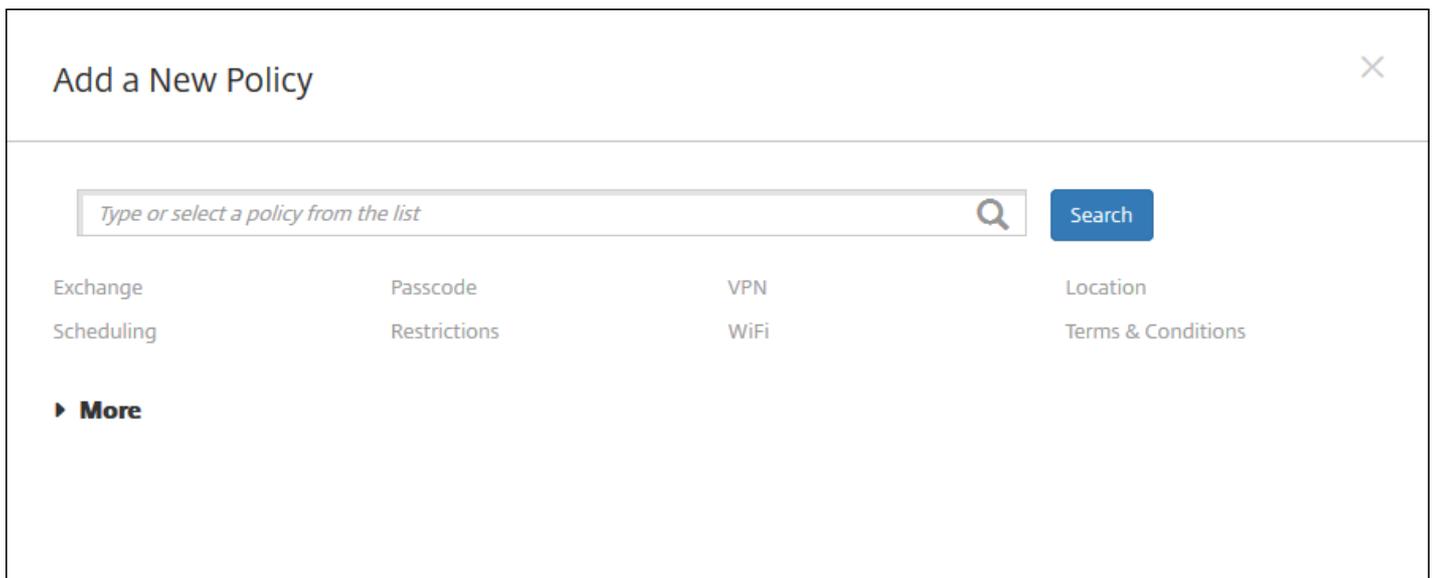
Status	Count
Installed	0
Pending	0
Failed	0

Below the summary, there is a 'Show more >' link.

Para agregar una directiva de dispositivo

1. En la página **Device Policies**, haga clic en **Add**.

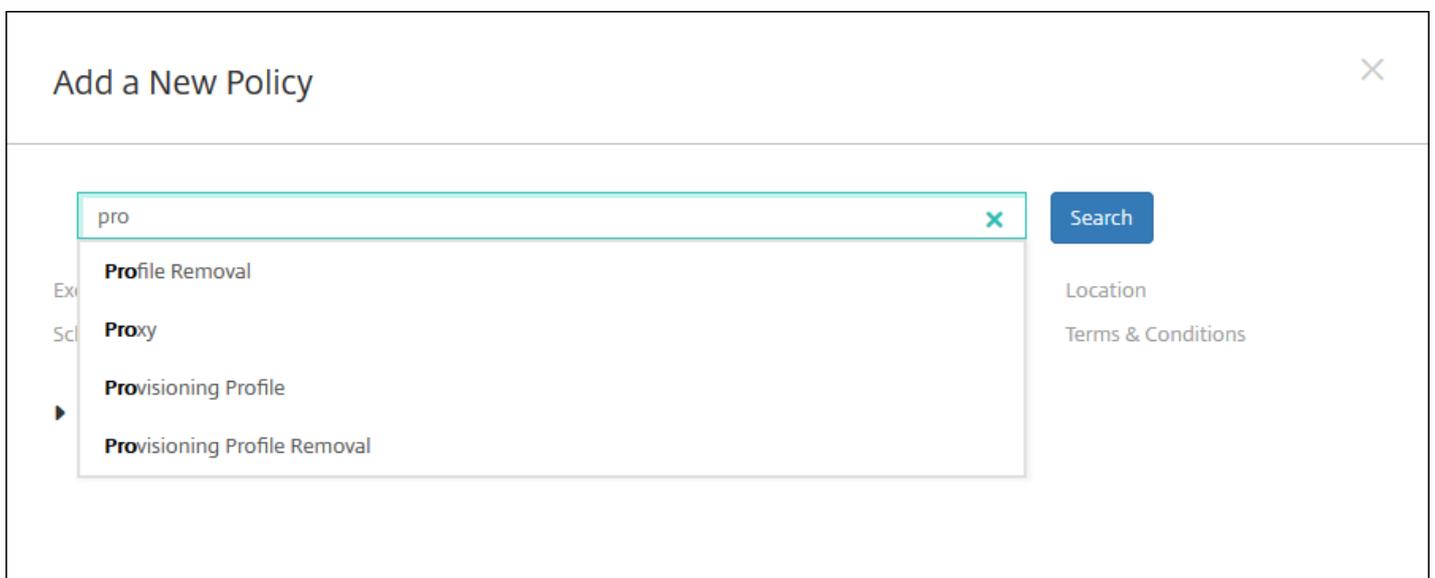
Aparecerá el cuadro de diálogo **Add a New Policy**. Puede expandir **More** para ver más directivas.



2. Para encontrar la directiva que quiere agregar, lleve a cabo una de las siguientes acciones:

- Haga clic en la directiva. Aparecerá la página **Policy Information** referente a la directiva seleccionada.
- Escriba el nombre de la directiva en el campo de búsqueda. Cuando escriba, aparecerán posibles coincidencias. Si la directiva está en la lista, haga clic en ella. Solo permanecerá en el cuadro de diálogo la directiva que seleccione. Haga clic en la directiva para abrir la página **Policy Information** referente a ella.

**Importante:** Si la directiva seleccionada está en el área **More**, solo será visible si expande **More**.



3. Seleccione las plataformas a incluir en la directiva. Las páginas de configuración referentes a las plataformas seleccionadas aparecerán en el paso 5.

**Nota:** Solo se mostrarán en la lista aquellas plataformas que sean compatibles con la directiva.

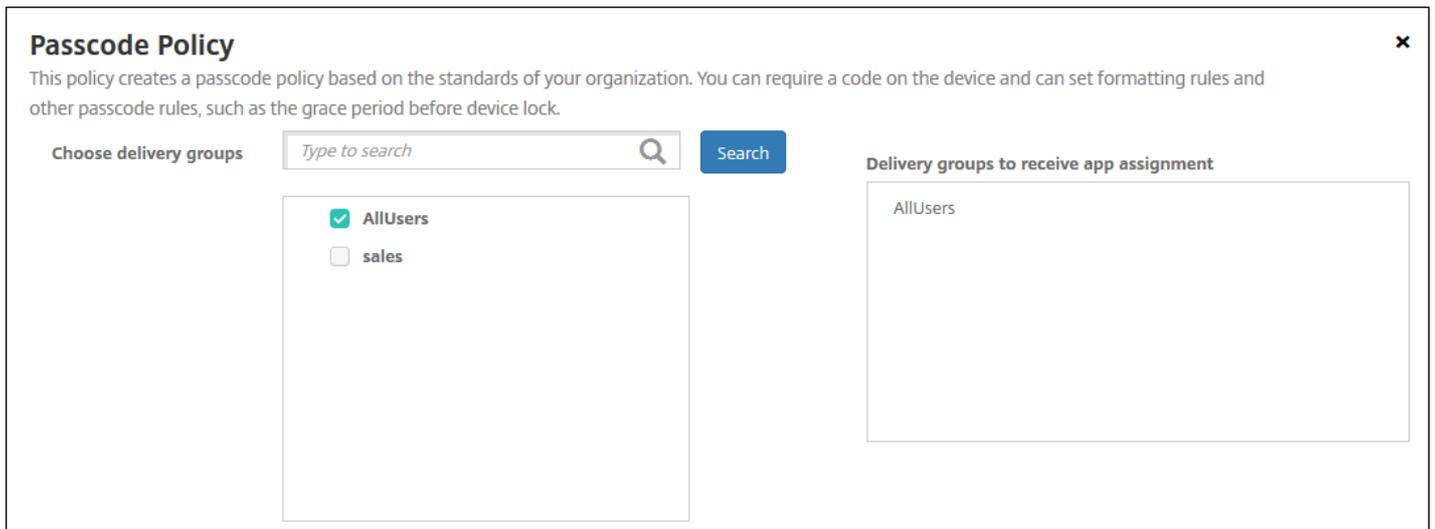
Passcode Policy
1 Policy Info
2 Platforms
<input checked="" type="checkbox"/> iOS
<input checked="" type="checkbox"/> Mac OS X
<input checked="" type="checkbox"/> Android
<input checked="" type="checkbox"/> Samsung KNOX
<input checked="" type="checkbox"/> Android for Work
<input checked="" type="checkbox"/> Windows Phone
<input checked="" type="checkbox"/> Windows Desktop/Tablet
3 Assignment

4. Complete los datos de la página **Policy Information** y haga clic en **Next**. La página **Policy Information** recopila información (como el nombre de la directiva) para ayudarle a identificar sus directivas y realizar un seguimiento de ellas. Esta página es similar para todas las directivas.

5. Complete las páginas de plataformas. Aparecerán páginas de plataformas para cada plataforma que haya seleccionado en el paso 3. Estas páginas son distintas para cada directiva. Todas las directivas pueden ser diferentes en función de las plataformas. No todas las plataformas admiten todas las directivas. Haga clic en **Next** para ir a la siguiente página de plataforma o, cuando haya completado todas las páginas de plataforma, para ir a la página **Assignment**.

6. En la página **Assignment**, seleccione los grupos de entrega a los que se aplicará la directiva. Al hacer clic en un grupo de entrega, el grupo aparecerá en el cuadro **Delivery groups to receive app assignment**.

**Nota:** El cuadro Delivery groups to receive app assignment no aparecerá hasta que seleccione un grupo de entrega.



7. Haga clic en **Save**.

La directiva se agrega a la tabla **Device Policies**.

Para modificar o eliminar una directiva de dispositivos

1. En la tabla **Device Policies**, marque la casilla situada junto a la directiva que se va a modificar o eliminar.

2. Haga clic en **Edit** o **Delete**.

- Si hace clic en **Edit**, puede modificar todos o algunos de los valores de configuración.
- Si hace clic en **Delete**, haga clic en **Delete** de nuevo en el cuadro de diálogo de confirmación.

# Directivas de dispositivos de XenMobile desglosadas por plataforma

Mar 02, 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**. XenMobile 10.4 admite las directivas de dispositivo para las plataformas siguientes:

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Mobile/CE
- Windows Phone 8/Windows 10 Mobile
- Windows 8 y Windows 10 de escritorio o tableta (.86)

Para obtener más información sobre dispositivos respaldados en XenMobile 10.x, consulte [Plataformas de dispositivos respaldados](#).

## Nota

El respaldo a dispositivos Symbian está obsoleto en XenMobile 10.3.

# Directivas de duplicación de AirPlay

Mar 02, 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 **Configurar > 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**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'AirPlay Mirroring Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you specify specific AirPlay devices to add to users' iOS and Mac OS X devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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 **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de iOS

The screenshot shows the XenMobile configuration interface for the 'AirPlay Mirroring Policy'. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Mac OS X' are both checked. The main content area is titled 'Policy Information' and contains the following sections:

- AirPlay Password:** A table with two columns: 'Device Name\*' and 'Password\*'. An 'Add' button is located to the right of the 'Password\*' column.
- Whitelist ID:** A table with one column: 'Device ID\*'. An 'Add' button is located to the right of the 'Device ID\*' column.
- Policy Settings:** Includes a 'Remove policy' section with two radio buttons: 'Select date' (selected) and 'Duration until removal (in days)'. Below these is a date picker. There is also an 'Allow user to remove policy' dropdown menu set to 'Always'.
- Deployment Rules:** A section with a right-pointing arrow.

At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **AirPlay Password.** Para cada dispositivo que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID.** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Password.** Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.
- **Whitelist ID.** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID.** Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.

**Nota:** Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.

- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## Configuración de los parámetros de Mac OS X

The screenshot shows the XenMobile configuration interface for an AirPlay Mirroring Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left contains a 'Policy Info' section with three items: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Mac OS X' are listed with checkboxes, and 'Mac OS X' is selected. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you specify specific AirPlay devices to add to users' iOS and Mac OS X devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.' Below this, there are three main sections: 'AirPlay Password', 'Whitelist ID', and 'Policy Settings'. The 'AirPlay Password' section has a table with columns for 'Device Name\*' and 'Password\*', and an 'Add' button. The 'Whitelist ID' section has a table with a column for 'Device ID\*' and an 'Add' button. The 'Policy Settings' section has a 'Remove policy' section with two radio buttons: 'Select date' (selected) and 'Duration until removal (in days)'. Below this is a date picker. The 'Allow user to remove policy' section has a dropdown menu with 'Always' selected. The 'Profile scope' section has a dropdown menu with 'User' selected, and a note 'OS X 10.7+'. At the bottom of the main content area, there is a 'Deployment Rules' section with a right-pointing arrow. At the bottom right of the interface, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **AirPlay Password.** Para cada dispositivo que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID.** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Password.** Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.
- **Whitelist ID.** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Device ID.** Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Add** para agregar el dispositivo, o bien haga clic en **Cancel** para no agregarlo.

**Nota:** Para eliminar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un dispositivo existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Configuraciones de directivas**

- Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
- Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**.

7. Configure las reglas de implementación. ▼

8. Haga clic en **Next**. Aparecerá la página de asignación **AirPlay Mirroring Policy**.

The screenshot shows the XenMobile Configure interface for the 'AirPlay Mirroring Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'AirPlay Mirroring Policy' and includes a description: 'This policy lets you specify specific AirPlay devices to add to users' iOS and Mac OS X devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.' The 'Assignment' section is active, showing a 'Choose delivery groups' section with a search bar and a list of groups: 'AllUsers' (checked), 'sales', '#RGTE', and 'test'. To the right, the 'Delivery groups to receive app assignment' section shows 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a 'Back' button and a 'Save' button.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.

- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for Always on connection**, que no se aplica para iOS.

11. Haga clic en **Save**.

# Directiva de AirPrint

Mar 02, 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.

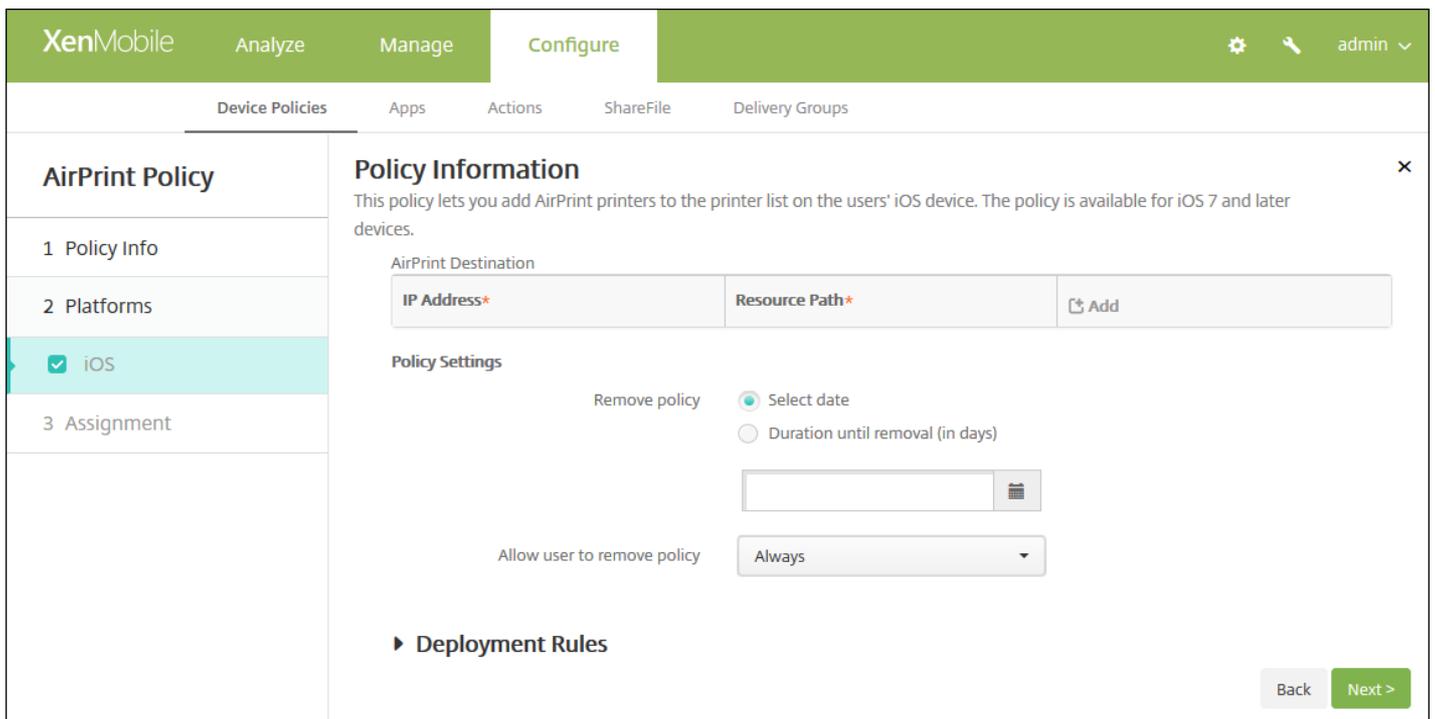
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **More** y, en **End user**, haga clic en **AirPrint**. Aparecerá la página **AirPrint Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'AirPrint Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is selected and highlighted in light blue. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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 **iOS Platform Information**.



6. Configure los siguientes parámetros:

- **AirPrint Destination.** Para cada destino de AirPrint que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **IP Address.** Escriba la dirección IP de la impresora AirPrint.
  - **Resource Path.** Escriba la ruta de recursos asociada a la impresora. Este valor corresponde al parámetro del registro Bonjour de `_ipps.tcp`. Por ejemplo, `printers/Canon_MG5300_series` o `printers/Xerox_Phaser_7600`.
  - Haga clic en **Save** para agregar la impresora, o bien haga clic en **Cancel** para no agregarla.

**Nota:** Para eliminar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelerita situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una impresora existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

#### 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **AirPrint Policy**.

The screenshot shows the XenMobile configuration interface for an AirPrint Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view with 'AirPrint Policy' expanded, containing '1 Policy Info', '2 Platforms', '3 Assignment' (selected), and 'Deployment Schedule'. The main content area is titled 'AirPrint Policy' and contains a description: 'This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.' Below the description, there is a 'Choose delivery groups' section with a search box and a 'Search' button. A list of groups is shown: 'AllUsers' (checked), 'Sales', and 'RG'. To the right, there is a 'Delivery groups to receive app assignment' section with a list containing 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

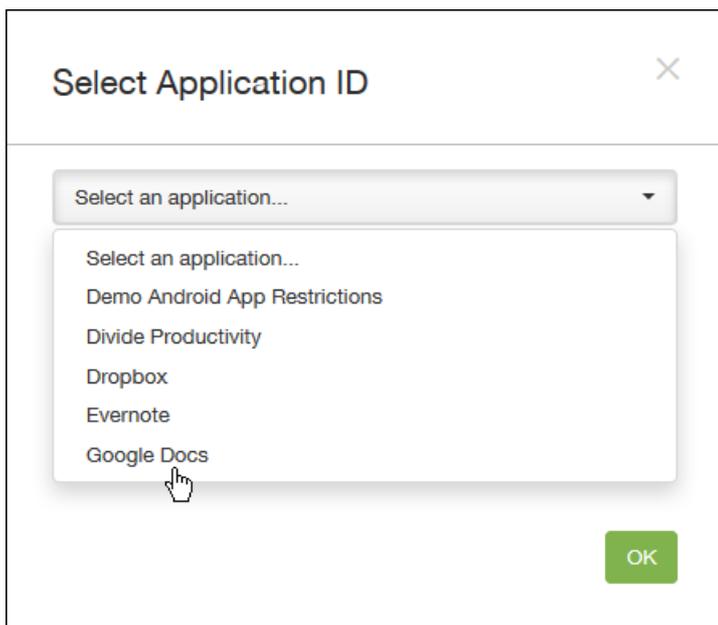
# Directiva de restricción de aplicaciones Android for Work

Mar 02, 2017

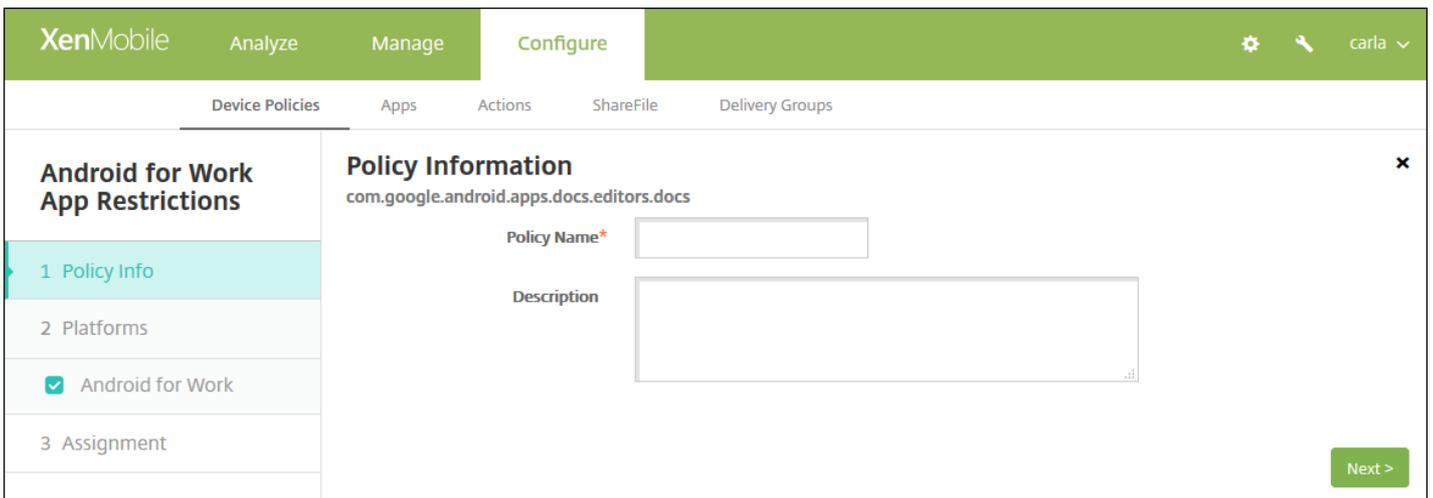
Puede modificar las restricciones asociadas a aplicaciones Android for Work. Sin embargo, antes de modificarlas, debe cumplir los siguientes requisitos previos:

- 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.



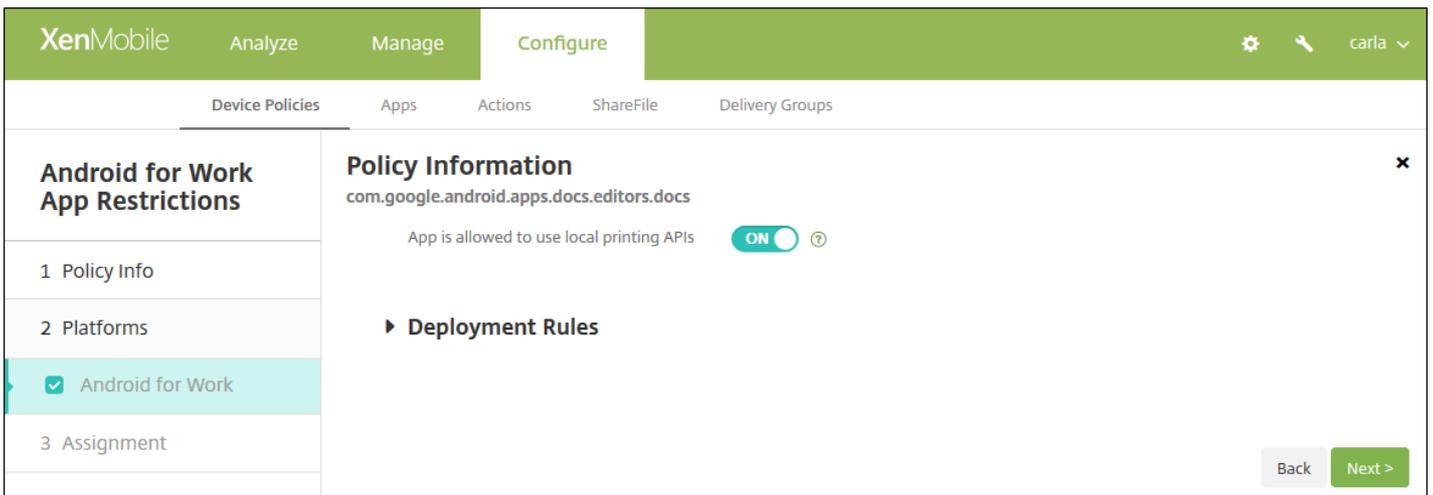
4. En la lista, seleccione la aplicación a la que quiere aplicar restricciones y, a continuación, haga clic en **OK**.
  - Si no hay aplicaciones Android for Work que agregar a XenMobile, no podrá continuar. Para obtener más información sobre cómo agregar aplicaciones a XenMobile, consulte [Incorporación 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.

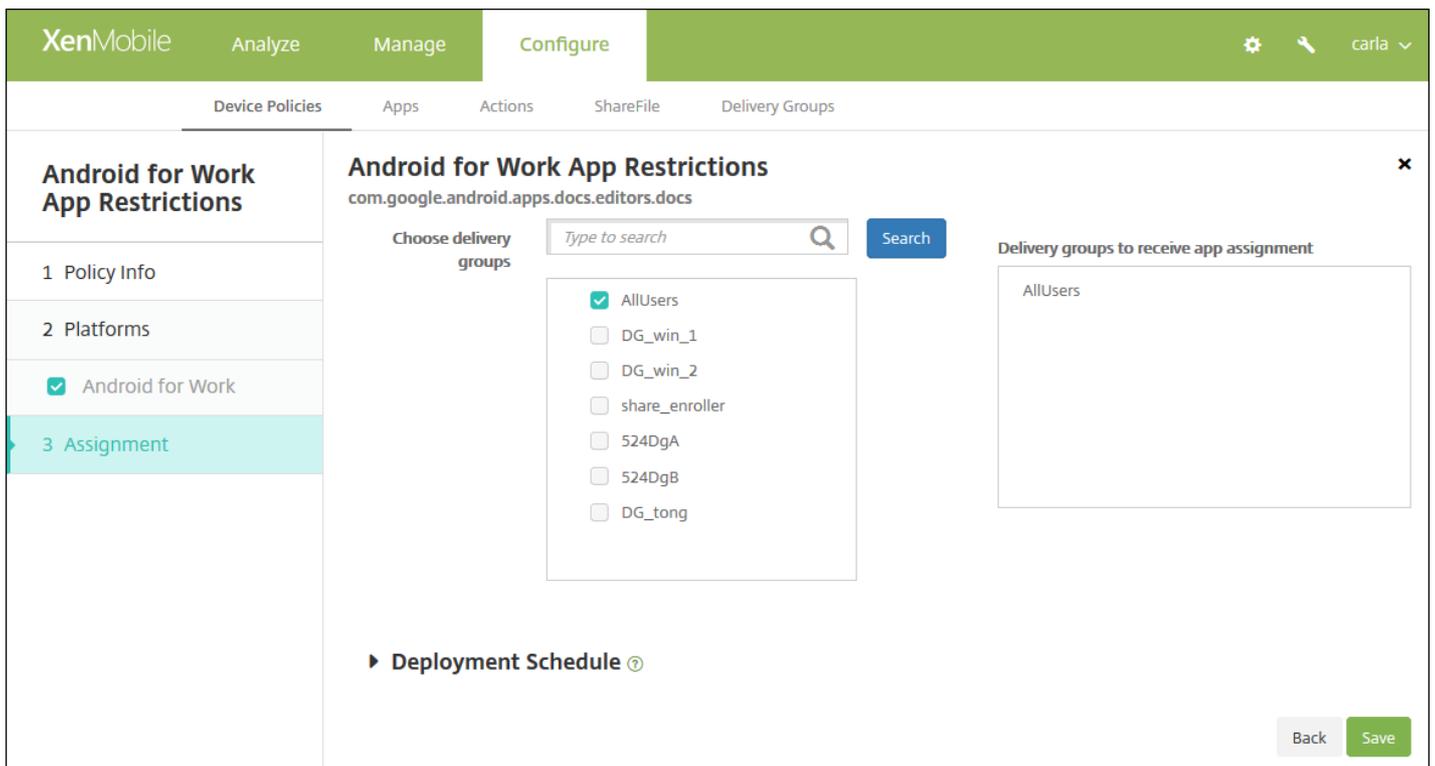
6. Haga clic en **Siguiente**. Aparecerá la página referente a la plataforma **Android for Work**.



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 **Siguiente**. Aparecerá la página de asignación **Android for Work App Restrictions Policy**.



10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no es aplicable en este caso.

12. Haga clic en **Save**.

# Directivas APN de dispositivos

Mar 02, 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 de información **APN Policy**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, and the 'Device Policies' tab is selected. The main content area is titled 'APN Policy' and contains a 'Policy Information' section. The 'Policy Information' section has a description: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' Below the description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is a text input, and the 'Description' field is a text area. On the left side of the page, there is a sidebar with a 'Policy Info' section that is currently selected. Below 'Policy Info' are sections for 'Platforms' and 'Assignment'. The 'Platforms' section has three checkboxes: 'iOS', 'Android', and 'Windows Mobile/CE', all of which are checked. The 'Assignment' section is currently empty. At the bottom right of the page, there is a 'Next >' button.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

**Nota:** Al aparecer la página **Policy Platforms**, todas las plataformas están seleccionadas, y verá en primer lugar la plataforma de iOS.

6. En **Platforms**, seleccione las plataformas que quiera agregar.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de iOS

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'APN Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing checkboxes for 'iOS', 'Android', and 'Windows Mobile/CE', all of which are checked. The '3 Assignment' section is currently empty. The 'Policy Information' section contains a description and several input fields: 'APN\*' (required), 'User name', 'Password', 'Server proxy address', and 'Server proxy port'. The 'Policy Settings' section includes 'Remove policy' options: 'Select date' (selected) and 'Duration until removal (in days)'. There is also a 'Allow user to remove policy' dropdown menu set to 'Always'. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **APN:** Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de IOS aceptado. De lo contrario, la directiva fallará.
- **User name:** Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.
- **Password:** La contraseña del usuario para este APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.
- **Server proxy address:** La dirección IP o dirección URL del proxy de APN.
- **Server proxy port:** El número de puerto del proxy de APN. Esto es necesario si especificó una dirección de servidor proxy.
- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Android

**XenMobile** Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### APN Policy

1 Policy Info

2 Platforms

- iOS
- Android
- Windows Mobile/CE

3 Assignment

#### Policy Information

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN\*

User name

Password

Server

APN type

Authentication type None

Server proxy address

Server proxy port

MMSC

Multimedia Messaging Server (MMS) proxy address

MMS port

► Deployment Rules

Back Next >

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

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'APN Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with checkboxes for iOS, Android, and Windows Mobile/CE), and '3 Assignment'. The main content area is titled 'Policy Information' and contains the following fields:

- APN\*:** A text input field with a help icon.
- Network:** A dropdown menu currently set to 'Built-in office'.
- User name:** A text input field with a help icon.
- Password:** A text input field with a help icon.

Below these fields is a section for 'Deployment Rules' with a right-pointing arrow. At the bottom right of the configuration area are 'Back' and 'Next >' buttons.

Configure los siguientes parámetros:

- **APN:** Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de Android aceptado. De lo contrario, la directiva fallará.
- **Network.** En la lista, haga clic en el tipo de red que quiere usar. El valor predeterminado es **Built-in office**.
- **User name:** Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación del perfil.
- **Password:** La contraseña del usuario para este APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.

### 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **APN Policy**.

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'APN Policy' and includes a description: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' The 'Choose delivery groups' section features a search bar and a list of groups: 'AllUsers' (checked), 'DG-ex', and 'DG-helen'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. The 'Deployment Schedule' section is partially visible. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for Always on connection**, que no se aplica para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directiva de atributos de aplicaciones

Mar 02, 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.

The screenshot shows the 'Configure' section of the XenMobile interface. The 'App Attributes Policy' is selected in the left sidebar. The main area is titled 'Policy Information' and contains a description: 'This policy lets you specify the attributes you want to add to apps on iOS devices.' There are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). A 'Next >' button is located at the bottom right.

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 de información referente a los atributos de las aplicaciones de plataforma **App Attributes**.

The screenshot shows the 'Configure' section of the XenMobile interface. The 'App Attributes Policy' is selected in the left sidebar. The main area is titled 'Policy Information' and contains a description: 'This policy lets you specify the attributes you want to add to apps on iOS devices.' There are two dropdown menus: 'Managed app bundle ID\*' (with 'Make a selection' as the current value) and 'Per-app VPN identifier' (with 'None' as the current value). Below these is a section titled 'Deployment Rules' with a right-pointing arrow. 'Back' and 'Next >' buttons are located at the bottom right.

6. Configure los siguientes parámetros:

- **Managed app bundle ID.** En la lista, haga clic en un ID de paquete de aplicación o en **Add new**.
  - Si hace clic en **Add new**, escriba el ID del paquete de aplicación en el campo que aparece.
- **Per-app VPN identifier.** En la lista, haga clic en el identificador de red VPN para cada aplicación.

## 7. Configure las reglas de implementación.



8. Haga clic en **Siguiente**. Aparecerá la página de asignación App Attributes Policy.

The screenshot shows the XenMobile interface for configuring an App Attributes Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Attributes Policy' and includes a description: 'This policy lets you specify the attributes you want to add to apps on iOS devices.' Under the heading 'Choose delivery groups', there is a search input field with the placeholder text 'Type to search' and a 'Search' button. Below the search field is a list of delivery groups with checkboxes: 'AllUsers', 'sales', 'RG', and 'ag186'. At the bottom of the main content area, there is a 'Deployment Schedule' section with a question mark icon. In the bottom right corner, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción Deploy for always on connection, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de acceso de aplicaciones

Mar 02, 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**.

The screenshot shows the XenMobile interface for configuring an App Access Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'App Access Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a form with the following fields:

- Policy Name \***: A text input field.
- Description**: A larger text area for providing details about the policy.

A 'Next >' button is located at the bottom right of the form area.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

6. Configure los siguientes parámetros para cada una de las plataformas seleccionadas.

- **Access policy.** Haga clic en **Required**, **Suggested** o **Forbidden**. El valor predeterminado es **Required**.
- Para agregar una o varias aplicaciones a la lista, haga clic en **Add** y, a continuación, lleve a cabo lo siguiente:
  - **App name.** Escriba un nombre de aplicación.
  - **App Identifier.** Escriba un identificador opcional de la aplicación.
  - Haga clic en **Save** o **Cancel**.
  - Repita estos pasos para cada aplicación que quiera agregar.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.



8. Haga clic en **Next**. Aparecerá la página de la plataforma siguiente o bien la página de asignación **App Access Policy**.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de configuración de aplicaciones

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there's a green navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, a secondary bar shows 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The user is identified as 'administrator'. The main content area is titled 'App Configuration Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is active, showing a 'Policy Information' form with fields for 'Policy Name\*' and 'Description'. A note explains that this policy defines configuration for managed apps. The 'Policy Info' sidebar shows 'iOS', 'Windows Phone', and 'Windows Desktop/Tablet' all selected with checkmarks.

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 **Policy Platforms**.

En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 6 para la configuración de las reglas de implementación de esa plataforma.

[Configuración de los parámetros de iOS](#)

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### App Configuration Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

#### Policy Information

This policy lets you define a configuration of a managed app to be applied on the iOS device. After you enter the dictionary content, you can check the syntax.

Identifier\*

Dictionary content\*

► **Deployment Rules**

Configuración de los parámetros de teléfonos, escritorios o tabletas Windows ▾

XenMobile Analyze Manage **Configure** ⚙️ 🔍 administrator ▾

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### App Configuration Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

#### App Configuration Policy

This policy lets you define a configuration of a managed app to be applied on the device. For iOS devices, after you enter the dictionary content, you can check the syntax.

Parameter name*	Value*	<input type="button" value="Add"/>

► **Deployment Rules**

**App Configuration Policy**

This policy lets you define a configuration of a managed app to be applied on the device. For iOS devices, after you enter the dictionary content, you can check the syntax.

1 Policy Info

2 Platforms

- iOS
- Windows Phone
- Windows Desktop/Tablet

3 Assignment

Parameter name\* Value\* Add

► Deployment Rules

## 6. Configure las reglas de implementación.

7. Haga clic en **Siguiente**. Aparecerá la página de asignación **App Configuration Policy**.

**App Configuration Policy**

This policy lets you define a configuration of a managed app to be applied on the device. For iOS devices, after you enter the dictionary content, you can check the syntax.

1 Policy Info

2 Platforms

- iOS
- Windows Phone
- Windows Desktop/Tablet

3 Assignment

Choose delivery groups

Type to search Search

- AllUsers

► Deployment Schedule ⓘ

8. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

9. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

10. Haga clic en **Save**.

# Directivas de inventario de aplicaciones

Mar 02, 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 de aplicaciones) o en la lista de aplicaciones permitidas (requeridas en una directiva de acceso de aplicaciones) para actuar consecuentemente. Puede crear directivas de acceso de aplicaciones para dispositivos iOS, Mac OS X, Android (incluidos los dispositivos habilitados para Android for Work) y escritorios y tabletas Windows, Windows Phone y Windows Mobile/CE.

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**.

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Inventory Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Windows Desktop/Tablet
  - Windows Phone
  - Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

Policy Name\*

Description

Next >

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name.** Escriba un nombre para la directiva.
- **Description.** Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página **Policy Platforms**.

The screenshot shows the XenMobile interface in the 'Configure' tab. On the left, a sidebar lists 'App Inventory Policy' with sub-sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS (checked), Mac OS X (checked), Android (checked), Windows Desktop/Tablet (checked), Windows Phone (checked), and Windows Mobile/CE (checked). The main area is titled 'Policy Information' and contains a description: 'This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.' Below this, there is a toggle for 'ios' which is currently turned 'ON'. A 'Deployment Rules' section is partially visible below. At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

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 **Siguiente**. Aparecerá la página de asignación **App Inventory Policy**.

The screenshot shows the XenMobile configuration interface for an App Inventory Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Inventory Policy' and includes a description: 'This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked) and 'Sales' (unchecked). The 'Delivery groups to receive app assignment' section shows a list with 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a Choose delivery groups, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista Delivery groups to receive app assignment, situada a la derecha.

10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

- Junto a Deploy, haga clic en ON para programar la implementación o haga clic en OFF para cancelarla. La opción predeterminada es ON. Si elige OFF, no habrá ninguna otra opción a configurar.
- Junto a Deployment schedule, haga clic en Now o en Later. La opción predeterminada es Now.
- Si hace clic en Later, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a Deployment condition, puede hacer clic en On every connection o en Only when previous deployment has failed. La opción predeterminada es On every connection.
- Junto a Deploy for always-on connection, haga clic en ON o en OFF. La opción predeterminada es OFF.

**Nota:**

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará a iOS.

11. Haga clic en **Save**.

# Directiva de bloqueo de aplicaciones

Mar 02, 2017

Puede crear una directiva en XenMobile para definir una lista de las aplicaciones que se permite ejecutar en un dispositivo, o una lista de las aplicaciones cuya ejecución debe bloquearse en un dispositivo. Puede configurar esta directiva para dispositivos Android e iOS, pero su funcionamiento difiere según la plataforma. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS.

Análogamente, en dispositivos iOS, solo se puede seleccionar una aplicación iOS en cada directiva. Esto significa que los usuarios solo pueden usar el dispositivo para ejecutar una sola aplicación. Cuando se aplica la directiva de bloqueo de aplicaciones, los usuarios no pueden realizar ninguna otra actividad en el dispositivo, excepto las opciones que usted permita específicamente.

Además, los dispositivos iOS deben supervisarse para insertar las directivas de bloqueo de aplicaciones.

Aunque la directiva de dispositivos funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N y posteriores porque Google ha dejado de respaldar la API necesaria.

## Configuración de iOS

## Configuración de Android

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y, a continuación, en **Security**, haga clic en **App Lock**. Aparecerá la página **App Lock Policy**.

The screenshot shows the XenMobile console interface. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' (highlighted). Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Lock Policy' and contains a 'Policy Information' dialog box. The dialog box has a close button (X) in the top right. It contains the text: 'This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.' Below this text are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). At the bottom right of the dialog box is a green 'Next >' button. To the left of the dialog box is a sidebar with three sections: '1 Policy Info' (highlighted in light blue), '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two items: 'iOS' and 'Android', both with a checked checkbox. Under '3 Assignment', there are three items: 'All Users', 'All Devices', and 'All Applications', all with unchecked checkboxes.

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.

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

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

## App Lock Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Android
- 3 Assignment

### Policy Information ✕

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App bundle ID\*

#### Options

- Disable touch screen  ON iOS 7.0+
- Disable device rotation sensing  OFF iOS 7.0+
- Disable volume buttons  OFF iOS 7.0+
- Disable ringer switch  OFF iOS 7.0+
- Disable sleep/wake button  OFF iOS 7.0+
- Disable auto lock  OFF iOS 7.0+
- Enable VoiceOver  OFF iOS 7.0+
- Enable zoom  OFF iOS 7.0+
- Enable invert colors  OFF iOS 7.0+
- Enable AssistiveTouch  OFF iOS 7.0+
- Enable speak selection  OFF iOS 7.0+
- Enable mono audio  OFF iOS 7.0+

#### User Enabled Options

- Allow VoiceOver adjustment  OFF iOS 7.0+
- Allow zoom adjustment  OFF iOS 7.0+
- Allow invert colors adjustment  OFF iOS 7.0+
- Allow AssistiveTouch adjustment  OFF iOS 7.0+

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

#### ▶ Deployment Rules

Configure estos parámetros:

- **App bundle ID.** En la lista, haga clic en la aplicación a la que se aplica esta directiva, o bien haga clic en **Add new** para agregar una nueva aplicación a la lista. Si selecciona **Add new**, escriba el nombre de la aplicación en el campo que aparece.
- **Options.** Todas las siguientes opciones solo se aplican a iOS 7.0 o versiones posteriores. El valor predeterminado de todas ellas es **OFF**, excepto para Disable touch screen, cuyo valor predeterminado es **ON**.
  - Disable touch screen (Inhabilitar la pantalla táctil)
  - Disable device rotation sensing (Inhabilitar la detección de giro)
  - Disable volume buttons (Inhabilitar los botones de volumen)
  - Disable ringer switch (Inhabilitar modificador de tono) **Nota:** Si esta opción está inhabilitada, los tonos dependen de la posición que tenía el modificador cuando se inhabilitó.
  - Disable sleep/wake button (Inhabilitar el botón de suspensión o reactivación)
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom (Habilitar zoom)
  - Enable invert colors (Habilitar la inversión de colores)
  - Habilitar AssistiveTouch
  - Enable Speak Selection (Habilitar la función Speak Selection)
  - Enable mono audio (Habilitar el ajuste Audio mono)
- **Opciones habilitadas por los usuarios.** Todas las siguientes opciones solo se aplican a iOS 7.0 o versiones posteriores. El valor predeterminado de todas ellas es **OFF**.
  - Allow VoiceOver adjustment (Permitir ajuste de VoiceOver)
  - Allow zoom adjustment (Permitir ajuste de zoom)
  - Allow invert colors adjustment (Permitir ajuste de inversión de colores)
  - Allow AssistiveTouch adjustment (Permitir ajuste de AssistiveTouch)
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
    - o Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - o En la lista **Allow user to remove policy**, haga clic en **Always, Password required** o **Never**.
    - o Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Android

The screenshot shows the XenMobile configuration interface for an App Lock Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation tabs are 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'App Lock Policy' configuration steps: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Android' selected), and '3 Assignment'. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.' Below this, the 'App Lock parameters' section contains:
 

- 'Lock message': A text input field.
- 'Unlock password': A text input field.
- 'Prevent uninstall': A toggle switch set to 'OFF'.
- 'Lock screen': A text input field with a 'Browse' button.
- 'Enforce': Radio buttons for 'Blacklist' (selected) and 'Whitelist'.

 At the bottom, there is an 'Apps' section with a table header 'App name\*' and an 'Add' button. Below the table is a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **App Lock parameters**
  - **Lock message.** Escriba el mensaje que verán los usuarios cuando intenten abrir una aplicación bloqueada.
  - **Unlock password.** Escriba la contraseña para desbloquear la aplicación.
  - **Prevent uninstall.** Seleccione si permitir a los usuarios desinstalar aplicaciones. El valor predeterminado es **OFF**.
  - **Lock screen.** Seleccione la imagen que aparecerá en la pantalla de bloqueo del dispositivo. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
  - **Enforce.** Haga clic en **Blacklist** para crear una lista de aplicaciones que no se pueden ejecutar en los dispositivos, o bien haga clic en **Whitelist** para crear una lista de aplicaciones que se pueden ejecutar en los dispositivos.
- **Apps.** Haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name.** En la lista, haga clic en el nombre de la aplicación que se va a agregar a la lista de aplicaciones permitidas o a la lista de aplicaciones prohibidas. También puede hacer clic en **Add new** para agregar una nueva aplicación a la lista de las aplicaciones disponibles.
  - Si selecciona **Add new**, escriba el nombre de la aplicación en el campo que aparece.
  - Haga clic en **Save** o **Cancel**.
  - Repita estos pasos para cada aplicación que quiera agregar a las listas de aplicaciones permitidas o prohibidas.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para

guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.

8. Haga clic en **Next** y aparecerá la página de asignación **App Lock Policy**.

The screenshot shows the XenMobile interface for configuring an App Lock Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Lock Policy' and includes a description: 'This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.' The 'Choose delivery groups' section features a search bar with the placeholder 'Type to search' and a 'Search' button. Below the search bar is a list of delivery groups: 'AllUsers' (checked), 'sales', 'RG', and 'ag186'. To the right, the 'Delivery groups to receive app assignment' section shows 'AllUsers' selected. At the bottom right, there are 'Back' and 'Save' buttons. A 'Deployment Schedule' link is also visible at the bottom left of the main content area.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará

para iOS.

11. Haga clic en **Save**.

# Directiva de uso de red por parte de aplicaciones

Mar 02, 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.

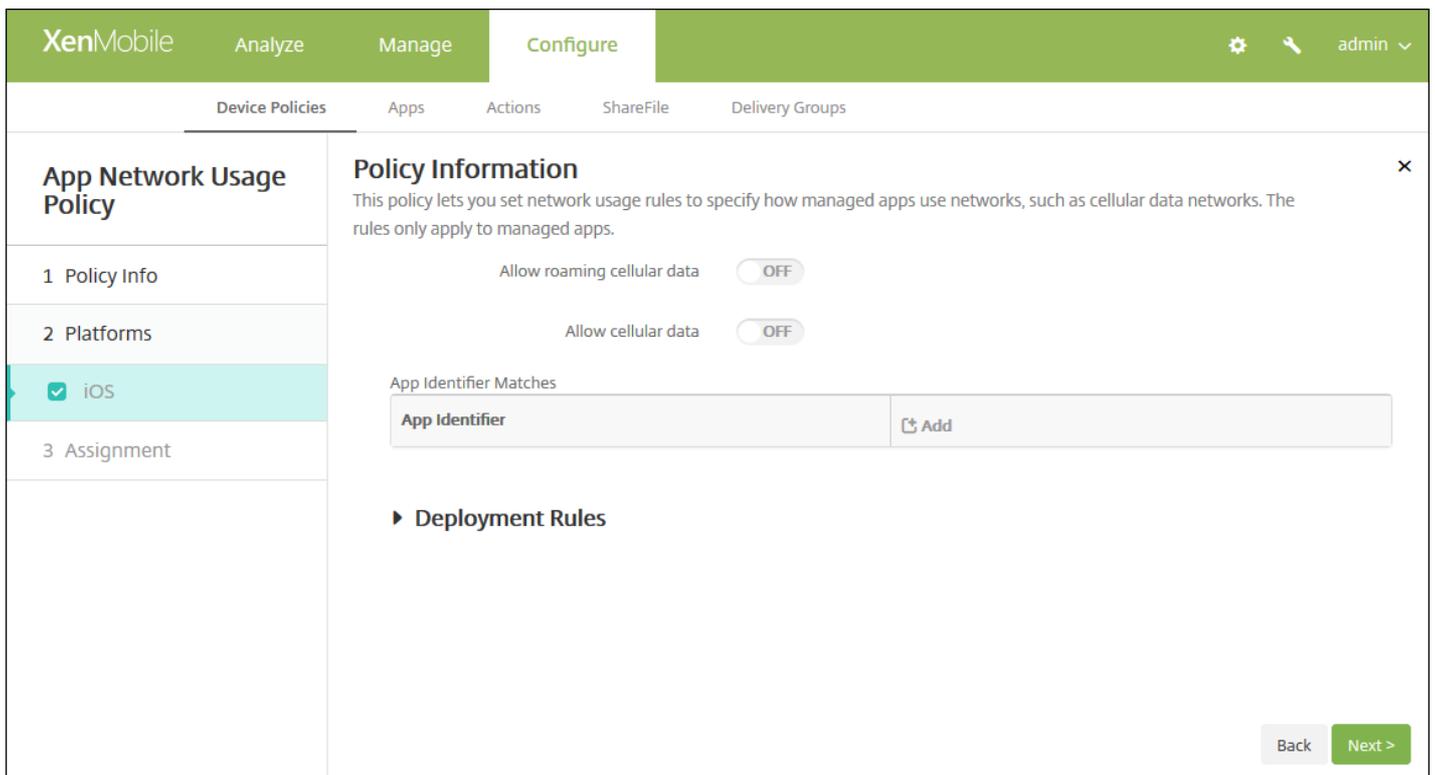
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y luego, en **Apps**, haga clic en **App Network Usage**. Aparecerá la página de información **App Network Usage Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' sub-tab is selected. On the left, there is a sidebar for 'App Network Usage Policy' with three steps: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' is selected with a checkmark. The main content area is titled 'Policy Information' and contains the following text: 'This policy lets you set network usage rules to specify how managed apps use networks, such as cellular data networks. The rules only apply to managed apps.' Below this text are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). At the bottom right of the main content area, there is a green button labeled 'Next >'.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.



6. Configure estas opciones.

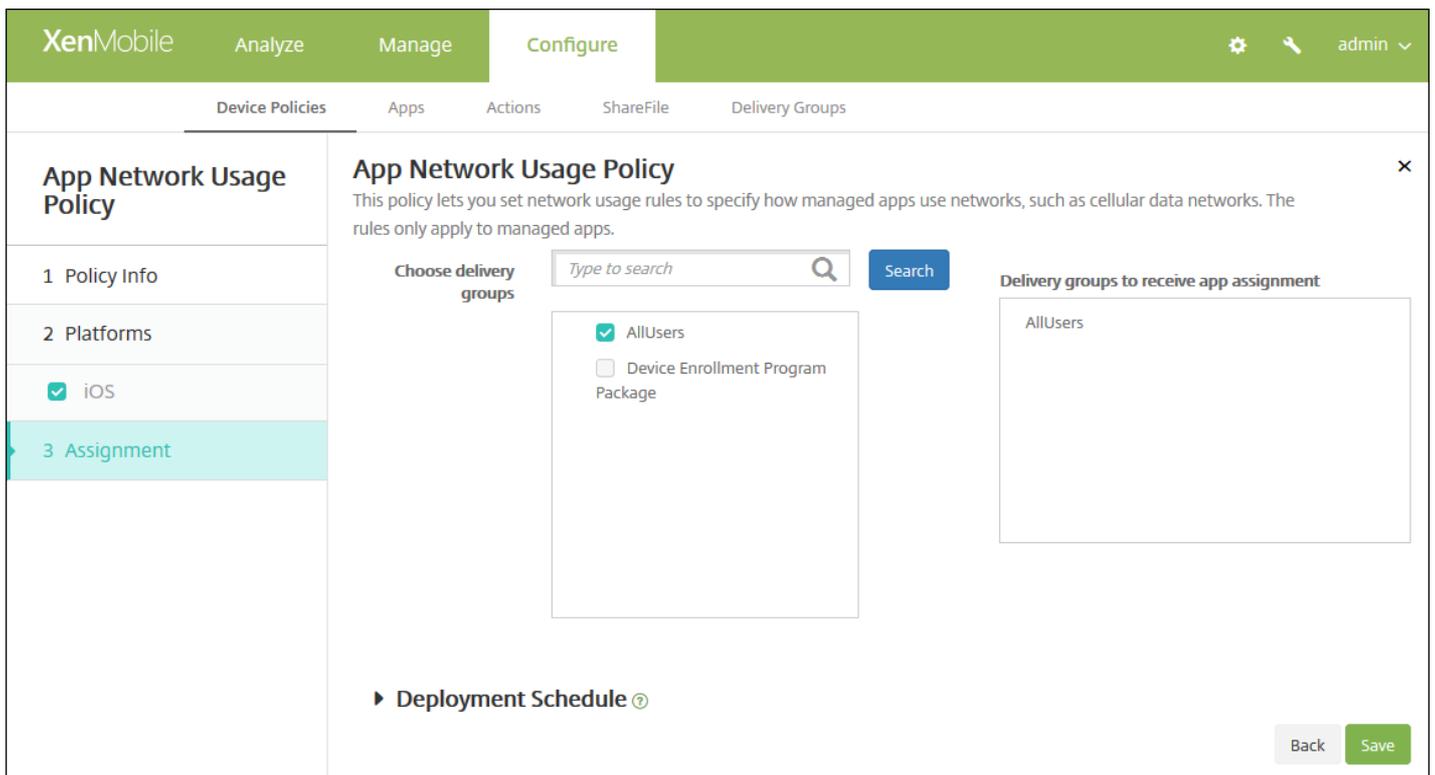
- **Allow roaming cellular data.** Seleccione si las aplicaciones indicadas pueden usar una conexión de datos móviles durante el roaming. El valor predeterminado es **OFF**.
- **Allow cellular data.** Seleccione si las aplicaciones especificadas pueden usar la conexión de datos móviles. El valor predeterminado es **OFF**.
- **App Identifier Matches.** Para cada aplicación que quiera agregar a la lista, haga clic en **Add** y haga lo siguiente:
  - **App Identifier.** Escriba un identificador de la aplicación.
  - Haga clic en **Save** para guardar la aplicación en la lista, o bien haga clic en **Cancel** para no guardarla.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

#### 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **App Network Usage Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directiva de restricciones de aplicaciones

Mar 02, 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**.

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

#### Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Samsung KNOX**.

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

#### Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Allow/Deny	New app restriction*
	<input type="text"/> <input type="button" value="Add"/>

► Deployment Rules

Back Next >

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.kmdmaf.crackle.
- Haga clic en **Save** para guardar la aplicación en la lista Allow/Deny, o bien haga clic en **Cancel** para no guardarla.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **App Restrictions Policy**.

The screenshot shows the 'App Restrictions Policy' configuration page in XenMobile. The page is divided into a sidebar and a main content area. The sidebar on the left has a 'Policy Info' section with three sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '3 Assignment' item is highlighted. The main content area is titled 'App Restrictions Policy' and contains a description: 'This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.' Below the description, there is a 'Choose delivery groups' section with a search bar and a 'Search' button. A list of delivery groups is shown with checkboxes: 'AllUsers' (checked) and 'sales' (unchecked). To the right, there is a 'Delivery groups to receive app assignment' section with a list containing 'AllUsers'. At the bottom of the main content area, there is a 'Deployment Schedule' section with a right-pointing arrow and a help icon. At the bottom right of the page, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de tunelización de aplicaciones

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. The main content area is titled 'Tunnel Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are both checked. The main area is titled 'Policy Information' and contains a text box for 'Policy Name\*' and a larger text box for 'Description'. A 'Next >' button is located at the bottom right of the form.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la

configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de Android

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Tunnel Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are checked. The 'Policy Information' section contains the following configuration options:

- Use this tunnel for remote support:** A toggle switch set to 'OFF'.
- Connection configuration:**
  - Connection initiated by:** A dropdown menu set to 'Device'.
  - Maximum connections per device\*:** A text input field containing '1'.
  - Define connection time out:** A toggle switch set to 'OFF'.
  - Block cellular connections passing by this tunnel:** A toggle switch set to 'OFF'.
- App device parameters:**
  - Client port\*:** An empty text input field.
- App server parameters:**
  - IP address or server name\*:** An empty text input field.
  - Server port\*:** An empty text input field.

At the bottom of the configuration area, there is a 'Deployment Rules' section with a right-pointing arrow. In the bottom right corner, there are 'Back' and 'Next >' buttons.

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.** Establecido en **On**.
    - **Define connection time out.** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
      - **Connection time out.** Si activa **Define connection time out**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Use SSL connection.** Seleccione si usar una conexión SSL segura para este túnel.
    - **Block cellular connections passing by this tunnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.
- Nota:** Las conexiones WiFi y USB no se bloquearán.

## Configuración de los parámetros de Windows Mobile/CE

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Tunnel Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are both checked. The 'Policy Information' section is expanded, showing the following configuration options:

- Use this tunnel for remote support:** OFF
- Connection configuration:**
  - Connection initiated by:** Device
  - Protocol:** Generic TCP
  - Maximum connections per device\*:** 1
  - Define connection time out:** OFF
  - Block cellular connections passing by this tunnel:** OFF
- App device parameters:**
  - Redirect to XenMobile:** Through app settings
  - Client port\*:** (empty field)
- App server parameters:**
  - IP address or server name\*:** (empty field)
  - Server port\*:** (empty field)

At the bottom of the configuration area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

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 especificar el origen de la conexión.
  - **Protocol.** En la lista, haga clic en el protocolo que se va a utilizar. El valor predeterminado es **Generic TCP**.
  - **Maximum connections per device.** Escriba la cantidad de conexiones TCP simultáneas que puede establecer la aplicación. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
  - **Define connection time out.** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Connection time out.** Si establece **Define connection time out** en **On**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Block cellular connections passing by this tunnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.

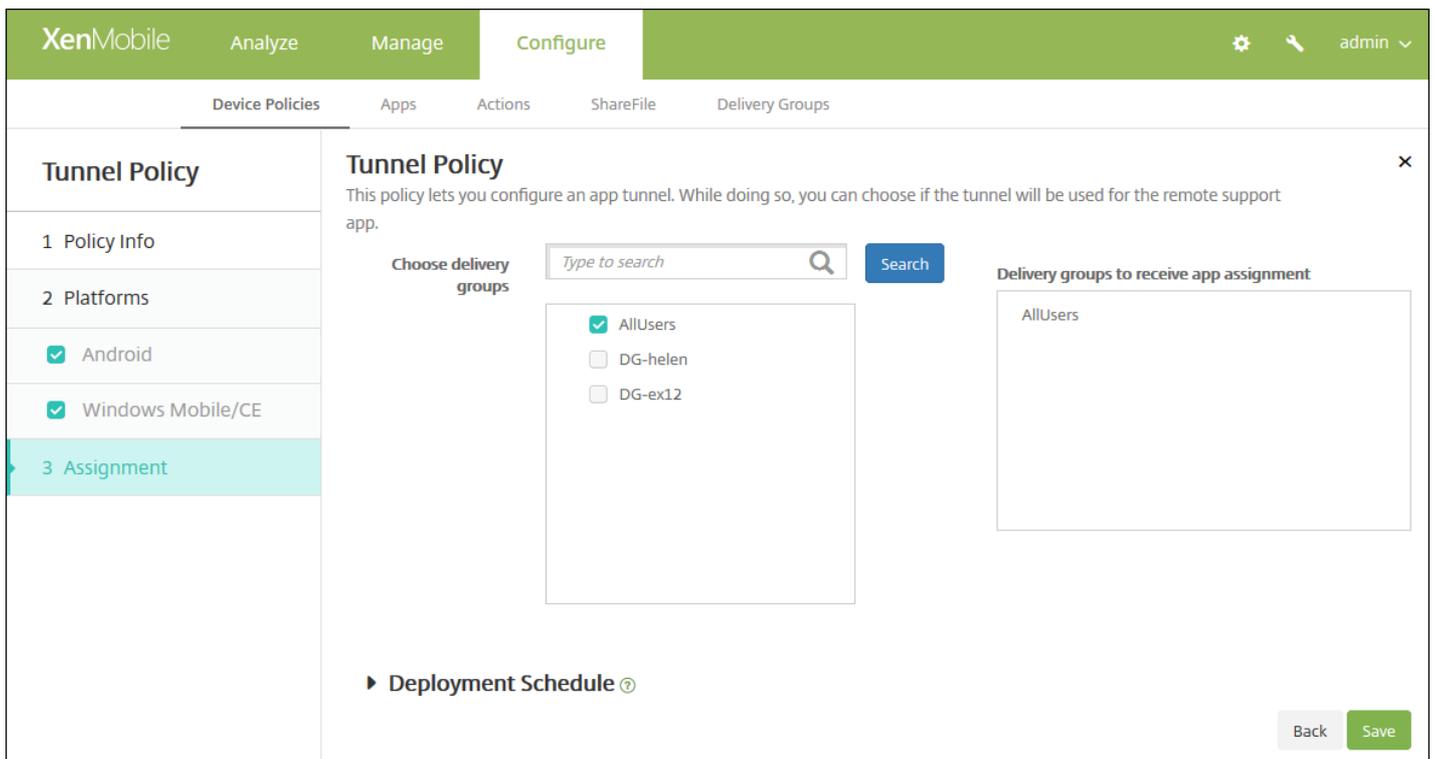
**Nota:** Las conexiones WiFi y USB no se bloquearán.
- **Redirect to XenMobile.** En la lista, haga clic en la forma en que se conecta el dispositivo a XenMobile. El valor predeterminado es **Through app settings**.
  - Si selecciona **Using a local alias**, escriba el alias en **Local alias**. El valor predeterminado es **localhost**.
  - Si selecciona **An IP address range**, escriba la dirección IP inicial del intervalo en **IP address range from** y la dirección IP final del intervalo en **IP address range to**.
- **Client port.** Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del puerto del servidor.
- **IP address or server name.** Escriba el nombre o la dirección IP del servidor de aplicaciones. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
- **Server port.** Escriba el número de puerto del servidor.
- Si selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Use this tunnel for remote support.** Establecido en **On**.
  - **Define connection time out.** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Connection time out.** Si establece la opción **Define connection time out** en **On**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Use SSL connection.** Seleccione si usar una conexión SSL segura para este túnel.
  - **Block cellular connections passing by this tunnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en modo roaming.

**Nota:** Las conexiones WiFi y USB no se bloquearán.

## 7. Configure las reglas de implementación.



8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Tunnel Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de dispositivo para desinstalación de aplicaciones

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below that, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are several checkboxes, all of which are checked: 'iOS', 'Android', 'Samsung KNOX', 'Android for Work', 'Windows Desktop/Tablet', and 'Windows Mobile/CE'. The main area is titled 'Policy Information' and contains a text box for 'Policy Name' and a larger text area for 'Description'. A 'Next >' button is visible at the bottom right.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las

demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de iOS

The screenshot shows the XenMobile interface for configuring an App Uninstall Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing a list of platforms with checkboxes: iOS (checked), Android (checked), Samsung KNOX (checked), Android for Work (checked), Windows Desktop/Tablet (checked), and Windows Mobile/CE (checked). To the right of this list is the 'Policy Information' section, which contains a description: 'This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.' Below this is a 'Managed app bundle ID' field with a dropdown menu labeled 'Make a selection'. Further down is a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

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

The screenshot shows the XenMobile interface for configuring an App Uninstall Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'App Uninstall Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several options are checked: iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet, and Windows Mobile/CE. The main content area, titled 'Policy Information', explains that the policy allows specifying apps for silent removal on Samsung KNOX devices. It features a section for 'Apps to uninstall' with a table containing an 'App Name' column and an 'Add' button. Below this is a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure este parámetro:

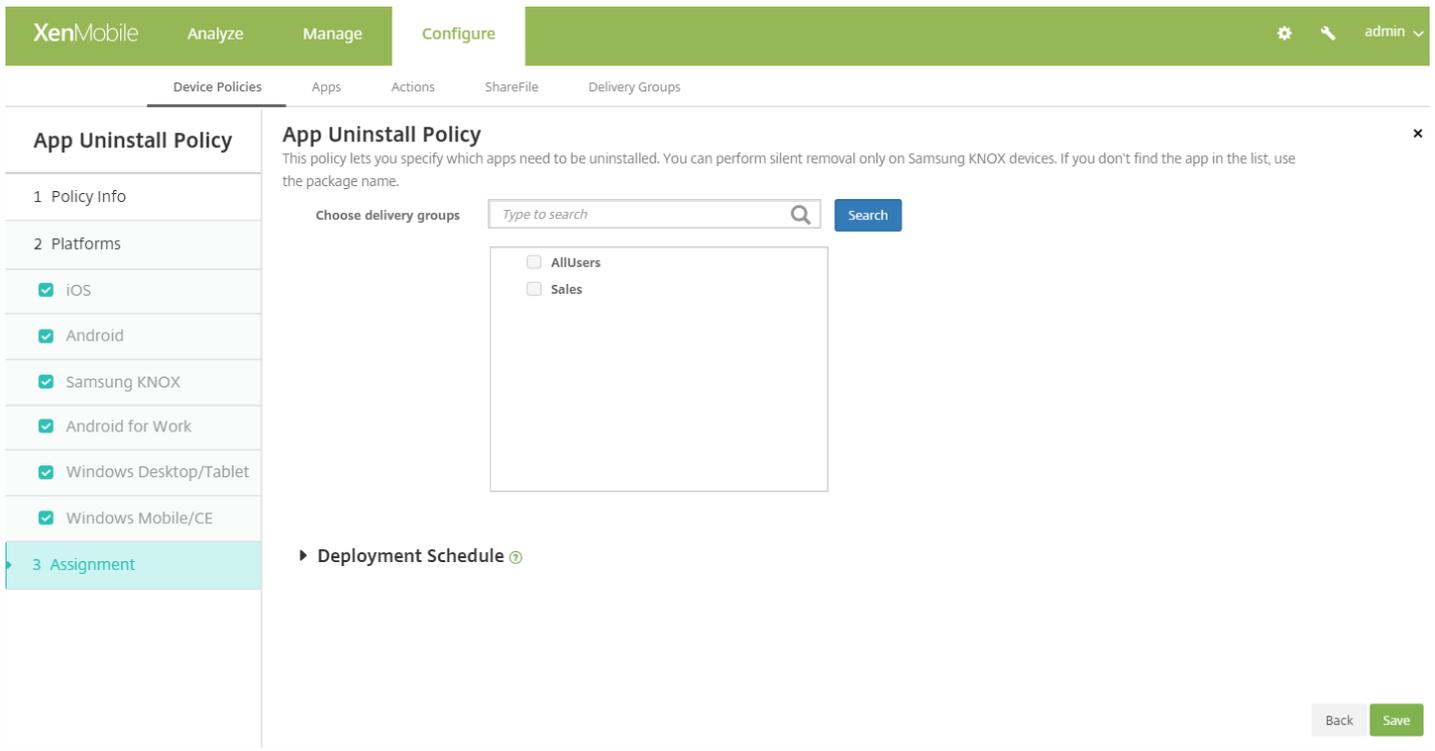
- **Apps to uninstall.** Para cada aplicación que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name.** En la lista, haga clic en una aplicación existente, o bien haga clic en **Add new** para introducir un nuevo nombre de aplicación. Si no hay ninguna aplicación configurada para esta plataforma, la lista estará vacía y deberá agregar aplicaciones nuevas.
  - Haga clic en **Add** para agregar la aplicación, o bien haga clic en **Cancel** para no agregarla.

**Nota:** Para eliminar una aplicación existente de la directiva de desinstalación, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

### 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **App Uninstall Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de restricciones para desinstalación de aplicaciones

Mar 02, 2017

Puede especificar las aplicaciones que los usuarios pueden o no pueden instalarse en un dispositivo Amazon o Samsung SAFE.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y luego, en **Apps**, haga clic en **App Uninstall Restrictions**. Aparecerá la página de información **App Uninstall Restrictions Policy**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Uninstall Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - Samsung SAFE
  - Amazon
- 3 Assignment

#### Policy Information

This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Uninstall Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - Samsung SAFE
  - Amazon
- 3 Assignment

#### Policy Information

This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

App Uninstall Restriction Settings

App Name*	Rule	Add
		<input type="button" value="Add"/>

Deployment Rules

Back Next >

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas:

- **App Uninstall Restrictions Settings.** Para cada regla que quiera agregar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **App name.** En la lista, haga clic en una aplicación, o bien haga clic en **Add new** para introducir una nueva.
  - **Rule.** Seleccione si los usuarios pueden desinstalar la aplicación. De forma predeterminada, se permite la desinstalación.
  - Haga clic en **Save** o **Cancel**.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## 8. Configure las reglas de implementación.

9. Haga clic en **Siguiente**. Aparecerá la página de asignación **App Uninstall Restrictions Policy**.

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing a sidebar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Restrictions Policy' and includes a description: 'This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.' Below this, there is a 'Choose delivery groups' section with a search box and a 'Search' button. Two options are listed: 'AllUsers' and 'Device Enrollment Program Package', both with unchecked checkboxes. At the bottom, there is a 'Deployment Schedule' section with a plus icon. The interface also features 'Back' and 'Save' buttons at the bottom right.

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

12. Haga clic en **Save**.

# Directivas de exploradores

Mar 02, 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. Haga clic en **More** y, a continuación, en **Apps**, haga clic en **Browser**. Aparecerá la página de información **Browser Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Browser Policy' and is divided into two sections: 'Policy Information' and 'Assignment'. The 'Policy Information' section contains a description: 'This policy lets you set rules for using the browser on Samsung and Android for Work devices.' Below this, there are two input fields: 'Policy Name\*' and 'Description'. The 'Assignment' section is currently empty. A 'Next >' button is visible at the bottom right of the form.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de Samsung SAFE y Samsung KNOX

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Browser Policy' and includes a sidebar with a table of policy sections: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Deployment Rules'. The '2 Platforms' section is expanded, showing 'Samsung SAFE' and 'Samsung KNOX' both checked. The main area contains a list of toggle switches for various browser settings, all currently set to 'OFF': 'Disable browser', 'Disable pop-up', 'Disable Javascript', 'Disable cookies', 'Disable autofill', and 'Force fraud warning'. At the bottom right, there are 'Back' and 'Next >' buttons.

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**.

The screenshot shows the XenMobile configuration page for a Browser Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows the policy configuration steps: '1 Policy Info', '2 Platforms', '3 Assignment' (highlighted), and '4 Deployment Schedule'. The main content area is titled 'Browser Policy' and includes a description: 'This policy lets you set rules for using the browser on Samsung and Android for Work devices.' It features a 'Choose delivery groups' section with a search bar and a list of groups: 'AllUsers' (checked), 'DG-ex12', and 'DG-Testprise'. To the right, there is a 'Delivery groups to receive app assignment' box containing 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directivas de calendarios (CalDAV)

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Calendar (CalDAV) Policy' and is divided into a left sidebar and a main content area. The sidebar has a 'Calendar (CalDAV) Policy' header and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing 'iOS' and 'Mac OS X' both checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

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.

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

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Calendar (CalDAV) Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
- Assignment

#### Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

► **Deployment Rules**

Configure los siguientes parámetros:

- **Account description.** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name.** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Port.** Especifique el puerto con el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL.** Indique la URL base del calendario del usuario.
- **User name.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password.** Escriba una contraseña opcional de usuario.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Calendar (CalDAV) Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
- Assignment

#### Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL  ON

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

Profile scope  OS X 10.7+

► Deployment Rules

Back Next >

Configure los siguientes parámetros:

- **Account description.** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name.** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Port.** Especifique el puerto con el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL.** Indique la URL base del calendario del usuario.
- **User name.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password.** Escriba una contraseña opcional de usuario.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está

disponible para OS X 10.7 y versiones posteriores.

## 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Calendar (CalDAV) Policy**.

The screenshot shows the XenMobile configuration interface for the 'Calendar (CalDAV) Policy'. The interface is divided into several sections:

- Header:** XenMobile, Analyze, Manage, Configure, and user profile (admin).
- Navigation:** Device Policies, Apps, Actions, ShareFile, Delivery Groups.
- Left Sidebar:** Calendar (CalDAV) Policy, 1 Policy Info, 2 Platforms (iOS, Mac OS X), 3 Assignment (selected).
- Main Content Area:**
  - Calendar (CalDAV) Policy:** This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.
  - Choose delivery groups:** A search box with 'Type to search' and a 'Search' button. Below it, a list of groups:  AllUsers and  sales.
  - Delivery groups to receive app assignment:** A list containing 'AllUsers'.
  - Deployment Schedule:** A section with a right-pointing arrow and a help icon.
  - Buttons:** 'Back' and 'Save' at the bottom right.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará

para iOS.

11. Haga clic en **Save**.

# Directiva de redes de telefonía móvil

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Configure' tab is active. Below the navigation bar, there are several tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is selected. On the left side, there is a sidebar with a 'Cellular Policy' header and a list of steps: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Assignment'. The '1 Policy Info' step is currently selected. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you configure cellular network settings on an iOS device.' Below the description, there are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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 de información **iOS Platform**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Cellular Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

### Policy Information

This policy lets you configure cellular network settings on an iOS device.

**Attach APN**

Name

Authentication type

User name

Password

**APN**

Name

Authentication type

User name

Password

Proxy server

Proxy server port

**Policy Settings**

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

► **Deployment Rules**

6. Configure los siguientes parámetros:

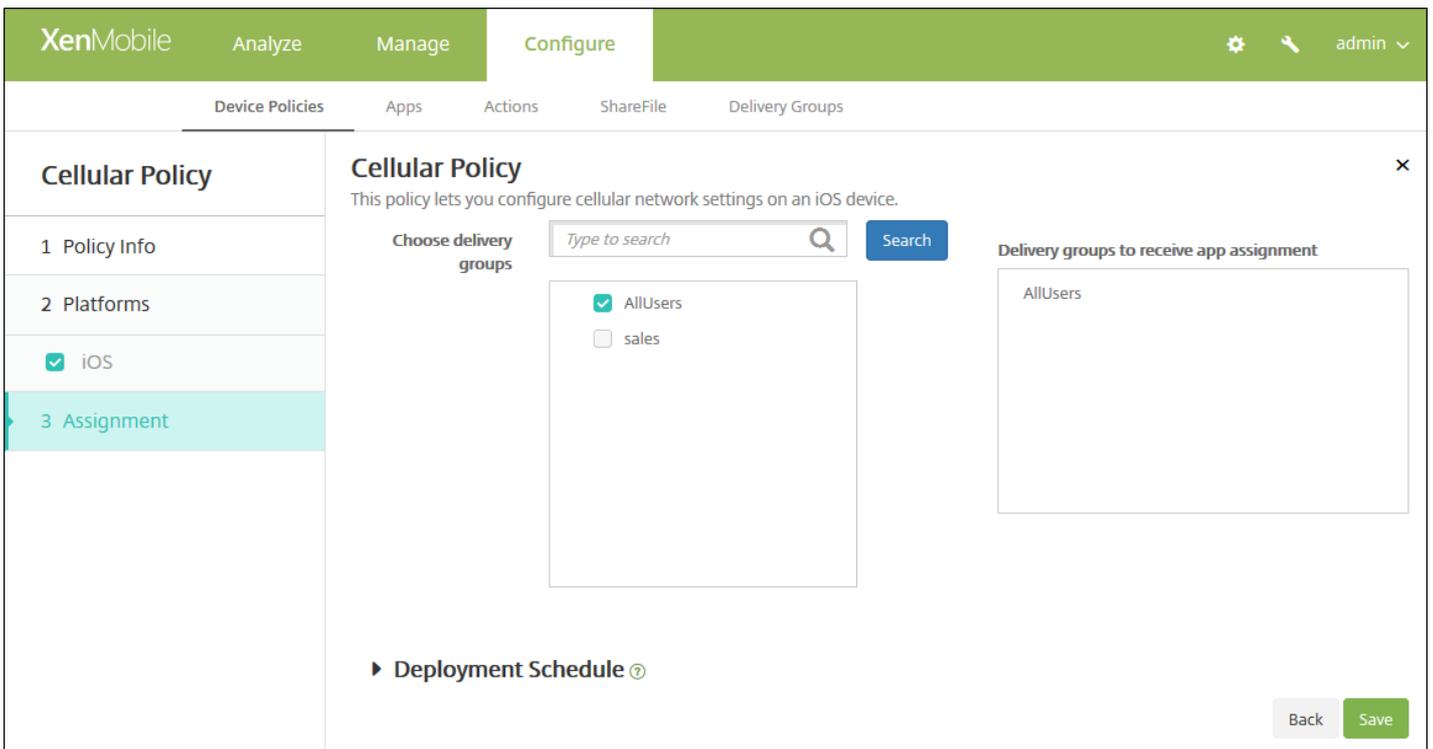
- **Attach APN**
  - **Name.** Escriba un nombre para esta configuración.
  - **Authentication type.** En la lista, haga clic en el Protocolo de autenticación por desafío mutuo (**CHAP**) o el Protocolo de autenticación por contraseña (**PAP**). El valor predeterminado es **PAP**.
  - **User name.** Escriba el nombre de usuario que se usará para la autenticación.
- **APN**
  - **Name.** Escriba un nombre para la configuración del nombre de punto de acceso (APN).
  - **Authentication type.** En la lista, haga clic en **CHAP** o **PAP**. El valor predeterminado es **PAP**.
  - **User name.** Escriba el nombre de usuario que se usará para la autenticación.
  - **Password.** Escriba una contraseña para la autenticación.
  - **Proxy server.** Escriba la dirección de red del servidor proxy.

- **Configuraciones de directivas**

- Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always, Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación. ▼

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Cellular Network Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible

para dispositivos iOS.

- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de administrador de conexiones

Mar 02, 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**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Connection Manager Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

Sets how apps connect to the Internet or to a private network. This policy only applies to Pocket PCs.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Connection Manager Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

Sets how apps connect to the Internet or to a private network. This policy only applies to Pocket PCs.

Apps that connect to a private network automatically use

Apps that connect to the Internet automatically use

Deployment Rules

Back Next >

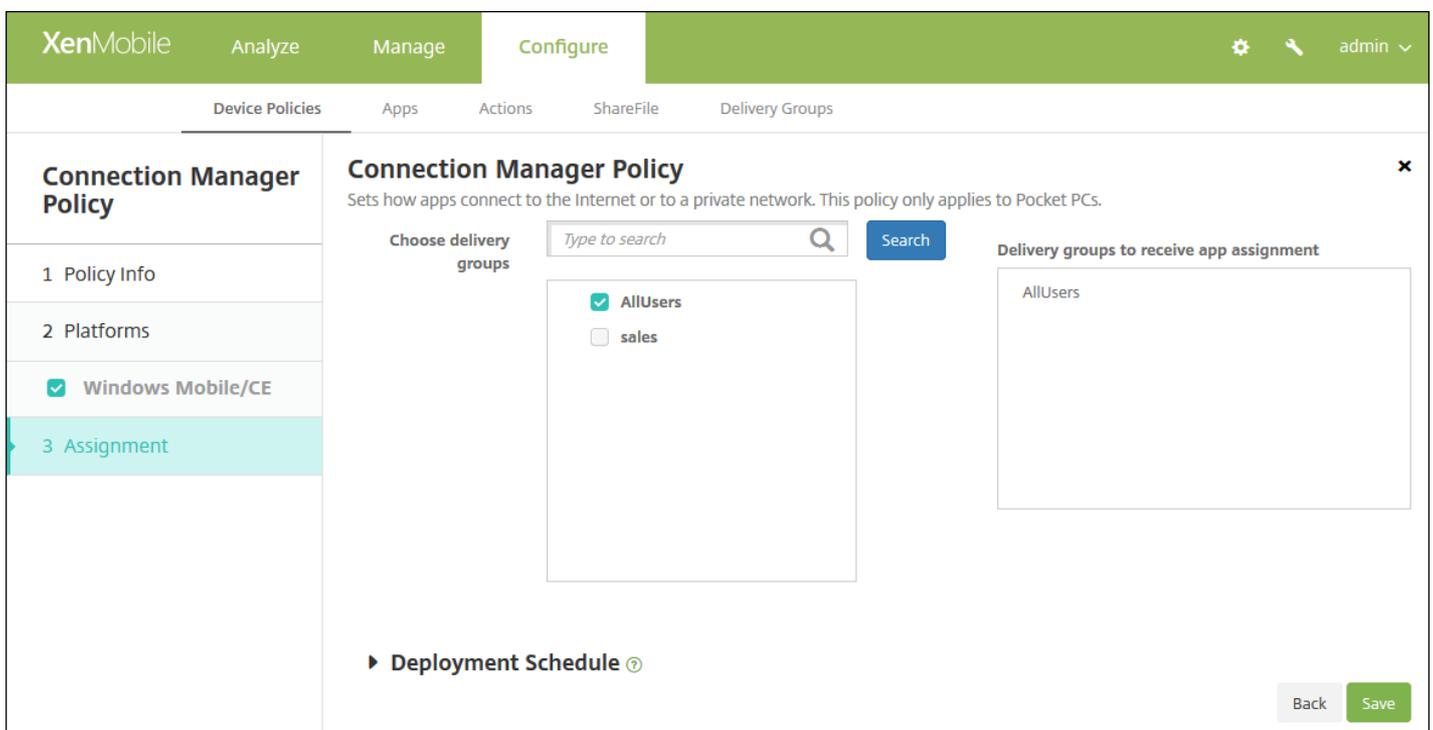
6. Configure estas opciones.

**Nota:** La opción **Built-in office** significa que todas las conexiones se realizan a la intranet de la empresa, mientras que **Built-in Internet** significa que todas las conexiones se realizan a Internet.

- **Apps that connect to a private network automatically use.** En la lista, haga clic en **Built-in office** o **Built-in Internet**. El valor predeterminado es **Built-in office**.
- **Apps that connect to the Internet automatically use.** En la lista, haga clic en **Built-in office** o **Built-in Internet**. El valor predeterminado es **Built-in office**.

7. Configure las reglas de implementación. ▼

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Connection Manager**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de programación de conexiones

Mar 02, 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.

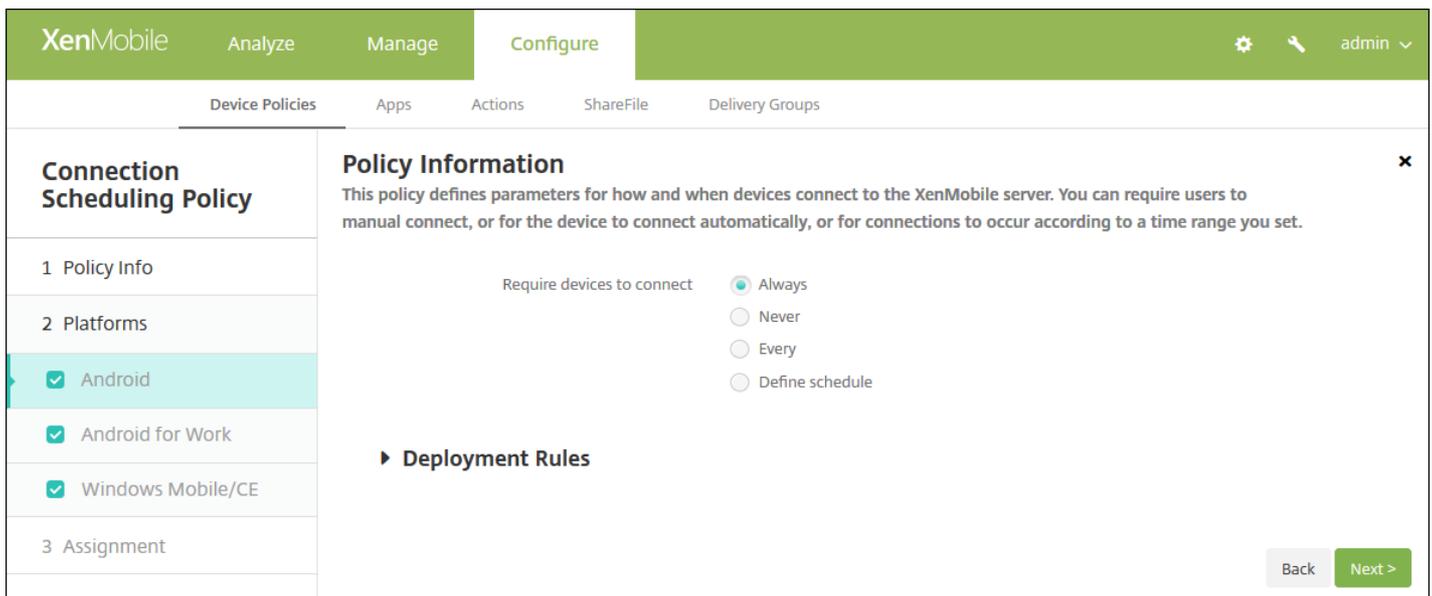
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **Scheduling**. Aparecerá la página de información **Connection Scheduling Policy**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Scheduling Policy' and contains a 'Policy Information' section. This section includes a description and two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is also empty. On the left side, there is a sidebar with a navigation menu. The menu items are: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are three checked items: 'Android', 'Android for Work', and 'Windows Mobile/CE'. At the bottom right of the main content area, there is a green button labeled 'Next >'.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas:

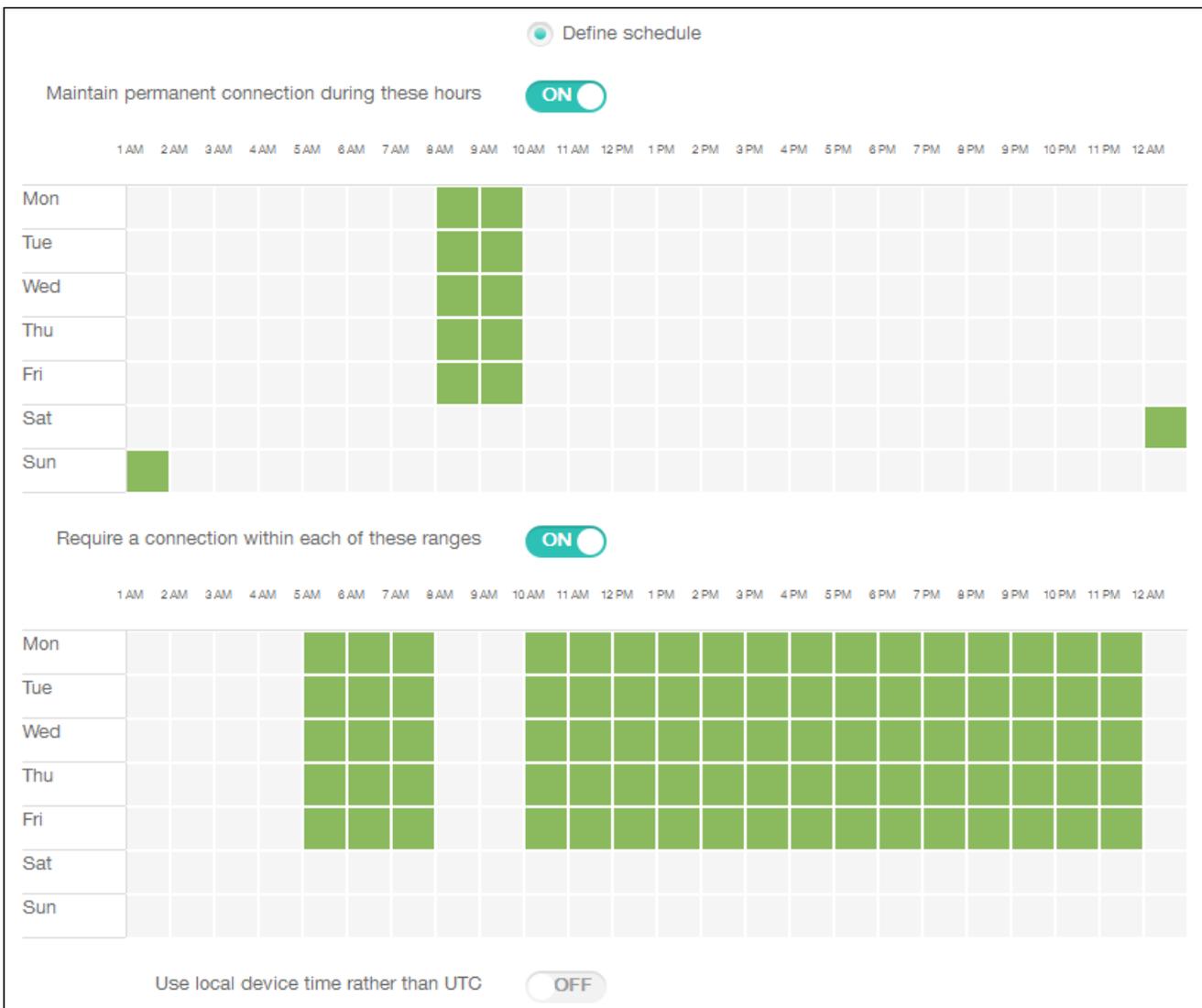
- **Require devices to connect.** Haga clic en la opción que quiera establecer para esta programación.
  - **Always.** Mantiene la conexión activa de forma permanente. La instancia de XenMobile en el dispositivo del usuario intenta volver a conectarse al servidor XenMobile después de perder la conexión de red; la conexión se supervisa mediante la transmisión de paquetes de control en intervalos regulares. Citrix recomienda esta opción para optimizar la seguridad. Cuando seleccione **Always**, use también la opción **Tunnel Policy** del dispositivo, con el valor **Define connection time-out** para asegurarse de que la conexión no gaste toda la batería. Manteniendo la conexión activa, puede enviar comandos de seguridad, tales como borrado o bloqueo del dispositivo, a demanda. También debe seleccionar la opción **Deployment Schedule, Deploy for always-on connections** en cada directiva implementada en el dispositivo.
  - **Never.** Se conecta manualmente. Los usuarios deben iniciar la conexión desde 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 cualquier período de tiempo definido.
- **Use local device time rather than UTC.** Sincroniza los períodos de tiempo definidos con la hora local del dispositivo en lugar de la hora universal coordinada (UTC).

## Definición de un período de tiempo de conexión

Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. Cada cuadrado de la escala de tiempo es de 30 minutos, de modo que, si quiere una conexión entre las 8:00 a. m. y las 9:00 a. m. todos los días de la semana, haga clic en los dos cuadrados ubicados entre 8 a. m. y 9 a. m. todos los días de la semana.

Por ejemplo: las dos escalas de tiempo de la siguiente ilustración requieren una conexión permanente entre las 8:00 a. m. y las 9:00 a. m. todos los días laborables de la semana, una conexión permanente entre las 12:00 a. m. del sábado y la 1:00 a. m. del domingo, además de al menos una conexión cada día laborable entre las 5:00 a. m. y las 8:00 a. m. o entre las 10:00 y a. m. las 11:00 p. m.



## 8. Configure las reglas de implementación.



9. Haga clic en **Next**. Aparecerá la página de asignación **Connection Scheduling Policy**.

The screenshot shows the XenMobile Configuration interface for the 'Connection Scheduling Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Scheduling Policy' and includes a description: 'This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set.' The 'Choose delivery groups' section has a search bar and a 'Search' button. Below it, there are two checkboxes: 'AllUsers' (checked) and 'sales' (unchecked). The 'Delivery groups to receive app assignment' section shows 'AllUsers' listed. At the bottom, there is a 'Deployment Schedule' section with a question mark icon. The interface also includes 'Back' and 'Save' buttons.

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

12. Haga clic en **Save**.

# Directivas de contactos (CardDAV)

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is selected. Below the navigation bar, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is active. On the left, there is a sidebar for 'CardDAV Policy' with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section is expanded, showing a description and two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located in the bottom right corner of the main content area.

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.

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

**CardDAV Policy**

1 Policy Info

2 Platforms

iOS

Mac OS X

3 Assignment

**Policy Information**

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description \*

Host name \*

Port \* 8443

Principal URL \*

User name \*

Password

Use SSL **ON**

**Policy Settings**

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy Always

► **Deployment Rules**

Back Next >

Configure estos parámetros:

- **Account description.** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name.** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Port.** Especifique el puerto con el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL.** Indique la URL base del calendario del usuario.
- **User name.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password.** Escriba una contraseña opcional de usuario.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### CardDAV Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
- Assignment

#### Policy Information

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL  ON

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy  ▾

Profile scope  ▾ OS X 10.7+

► Deployment Rules

Configure estos parámetros:

- **Account description.** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Host name.** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Port.** Especifique el puerto con el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **Principal URL.** Indique la URL base del calendario del usuario.
- **User name.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Password.** Escriba una contraseña opcional de usuario.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. El valor predeterminado es **ON**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a Removal password, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está

disponible para OS X 10.7 y versiones posteriores.

## 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **CardDAV Policy**.

The screenshot shows the XenMobile configuration interface for a CardDAV Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, with sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'CardDAV Policy' and includes a description: 'This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.' Below the description, there are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked), 'Sales', and 'RG'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. At the bottom, there is a 'Deployment Schedule' section with a question mark icon, and 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Copiado de aplicaciones a directivas de contenedores Samsung

Mar 02, 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**.

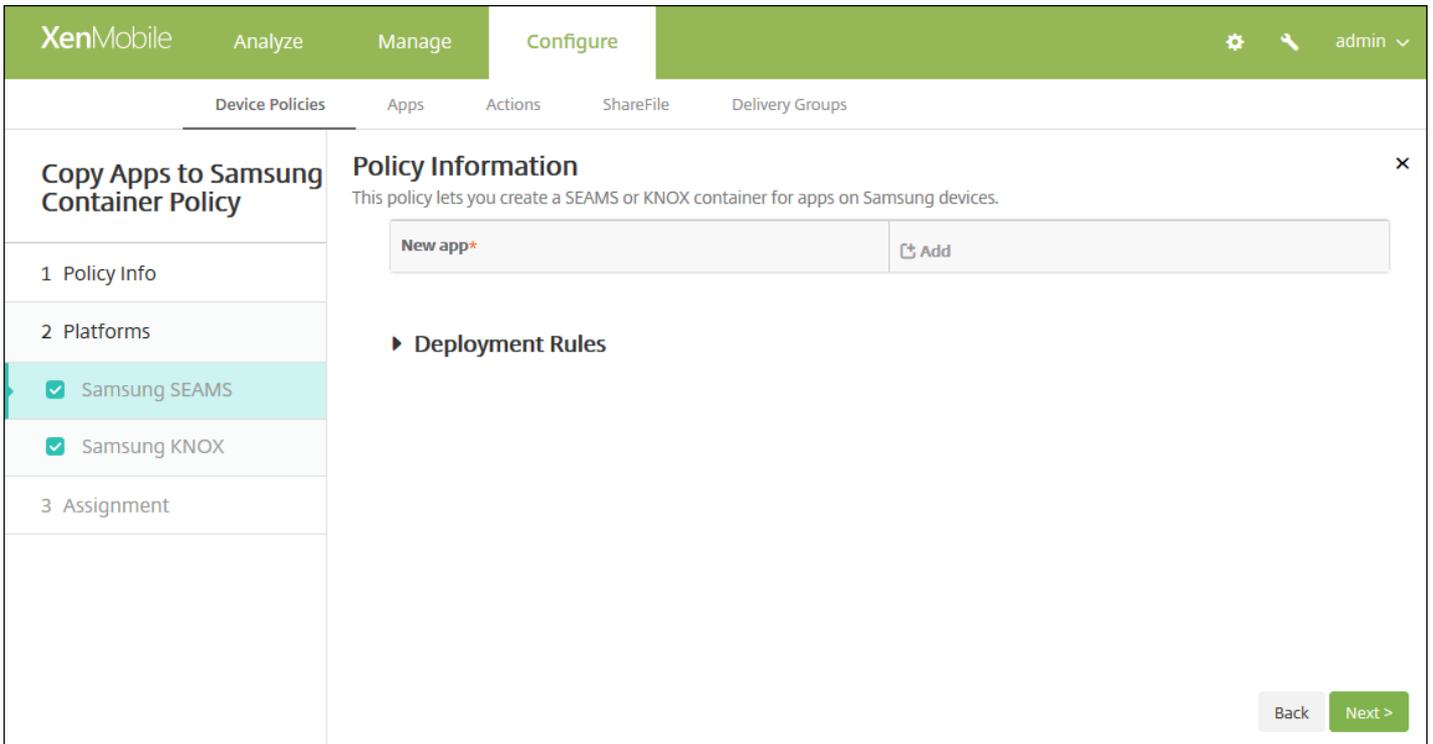
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Copy Apps to Samsung Container**. Aparecerá la página de información acerca de la directiva **Copy Apps to Samsung Container Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Copy Apps to Samsung Container Policy' and contains a 'Policy Information' section. This section includes a 'Policy Name\*' field and a 'Description' field. There are also checkboxes for 'Samsung SEAMS' and 'Samsung KNOX', both of which are checked. A 'Next >' button is located at the bottom right of the form.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.



6. En Platforms, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

7. Configure el siguiente parámetro para cada una de las plataformas seleccionadas.

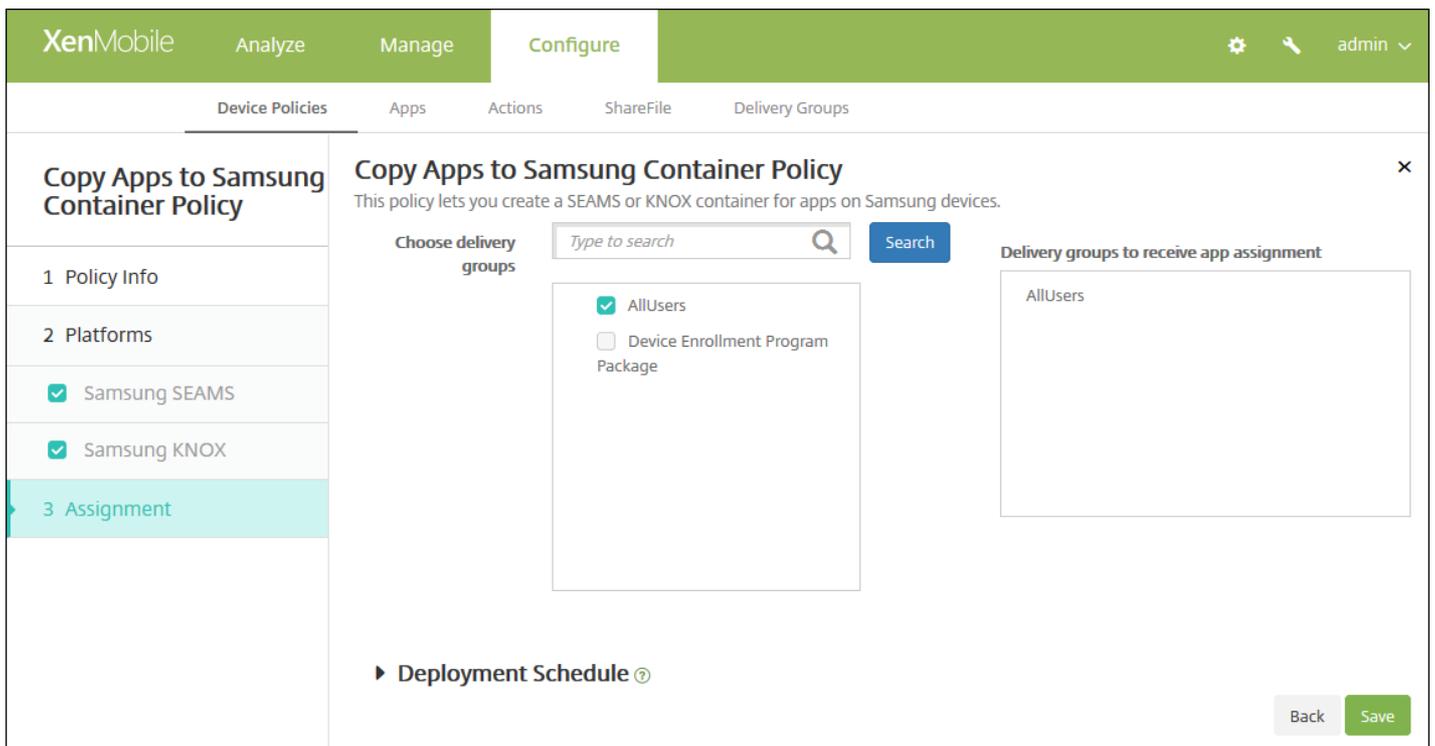
- **New App.** Para agregar cada aplicación a la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - Escriba un ID de paquete, por ejemplo: com.mobiwolf.lacingart para la aplicación LacingArt.
  - Haga clic en **Save** o **Cancel**.

**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

#### 8. Configure las reglas de implementación.

9. Haga clic en **Siguiente**. 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 lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en Settings > Server Properties. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

12. Haga clic en **Save** para guardar la directiva.

Una vez que la directiva esté implementada correctamente, las aplicaciones SEAMS aparecerán en la página **Device details**, bajo el encabezado **Location: Enterprise SEAMS Location**, mientras que las aplicaciones KNOX aparecerán bajo el encabezado **Location: Enterprise Location**.



# Directivas de credenciales

Mar 02, 2017

En XenMobile, puede crear directivas de credenciales de dispositivo para habilitar la autenticación integrada con la configuración de PKI en XenMobile, tal como una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor. Para obtener más información acerca de las credenciales, consulte [Certificados](#).

Puede crear directivas de credenciales para dispositivos iOS, Mac OS X, Android, Android for Work, tabletas y escritorios Windows, Windows Mobile/CE y Windows Phone. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

[Configuración de iOS](#)

[Configuración de Mac OS X](#)

[Configuración de Android y Android for Work](#)

[Parámetros para escritorios y tabletas Windows](#)

[Configuración de Windows Mobile/CE](#)

[Configuración de Windows Phone](#)

Antes de crear esta directiva, se necesita la información de credenciales que vaya a utilizar para cada plataforma, además de los certificados en sí y las contraseñas.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Credentials**. Aparecerá la página de información **Credentials Policy**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Credentials Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Android for Work
  - Windows Phone
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS

The screenshot shows the XenMobile configuration interface for a Credentials Policy. The left sidebar lists the policy configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main content area is titled 'Policy Information' and contains the following settings:

- Credential type:** Certificate (.cer, .crt, .der and .pem)
- Credential name:** (Empty text field)
- The credential file path:** (Empty text field with a 'Browse' button)
- Policy Settings:**
  - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'.
  - Allow user to remove policy:** Always
- Deployment Rules:** (Section header with a right-pointing arrow)

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

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

The screenshot shows the XenMobile interface for configuring a Credentials Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Device Policies' sub-tab is selected. The left sidebar shows the 'Credentials Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android (highlighted), Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main content area displays the 'Credentials Policy' configuration form. It includes a description: 'This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' Below the description, there is a 'Credential type' dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)'. Underneath, there is a text input field for 'The credential file path' and a green 'Browse' button. A 'Deployment Rules' section is visible below the input fields. At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

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

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

- OS version\* 10
- Certificate Type ROOT
- Store device root
- Location System
- Credential type Certificate (.cer, .crt, .der and .pem)
- Credential file path\*  Browse

► Deployment Rules

Back Next >

Configure los siguientes parámetros:

- **OSVersion.** En la lista, haga clic en **8.1** para Windows 8.1 o **10** para Windows 10. El valor predeterminado es **10**.

[Configuración de Windows 10](#) ▾

[Configuración de Windows 8.1](#) ▾

Configuración de los parámetros de Windows Mobile/CE

The screenshot shows the XenMobile configuration interface for a Credentials Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view with 'Credentials Policy' selected, containing sub-sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE (which is highlighted). The main content area is titled 'Credentials Policy' and includes a descriptive paragraph. Below the description are three configuration fields: 'Store device' (a dropdown menu set to 'root'), 'Credential type' (a dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)'), and 'Credential file path' (a text input field with a 'Browse' button). A 'Deployment Rules' section is partially visible below these fields. At the bottom right, there are 'Back' and 'Next >' buttons.

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**.

The screenshot shows the XenMobile configuration interface for a 'Credentials Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a navigation menu with three items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Assignment' item is highlighted. The main content area is titled 'Credentials Policy' and contains a search bar for 'Choose delivery groups' with a 'Search' button. Below the search bar is a list of delivery groups: 'AllUsers' and 'Sales'. There is also a 'Deployment Schedule' section with a help icon. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de contenido XML personalizado

Mar 02, 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 de Microsoft Developer Network.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Custom XML**. Aparecerá la página de información **Custom XML Policy**.

The screenshot shows the XenMobile console interface. At the top, there's a green navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there's a secondary navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Custom XML Policy' and has a left sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is selected. The main area shows 'Policy Information' with a description: 'This policy lets you create custom XML for your policies. After you enter the XML, you can check the syntax.' There are two input fields: 'Policy Name \*' and 'Description'.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Next**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

7. Configure el siguiente parámetro para cada una de las plataformas seleccionadas:

- **XML content.** Escriba o copie y pegue el código XML personalizado que se va a agregar a la directiva.

#### 8. Configure las reglas de implementación.

9. Haga clic en **Next**. XenMobile comprueba la sintaxis del contenido XML. Los errores de sintaxis aparecerán bajo el cuadro del contenido. Antes de continuar, debe corregir los errores que haya.

Si no hay errores de sintaxis, aparecerá la página de asignación **Custom XML Policy**.

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

#### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se

realicen se aplicarán a todas las plataformas.

12. Haga clic en **Save**.

# Directiva de eliminación de archivos y carpetas

Mar 02, 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**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which files and folders need to be deleted.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which files and folders need to be deleted.

Files and folders to delete

Path*	Type	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

► Deployment Rules

Back Next >

6. Configure los siguientes parámetros:

- **Files and folders to delete.** Para cada archivo o carpeta que quiera eliminar, haga clic en Add y lleve a cabo lo siguiente:
  - **Path.** Escriba la ruta al archivo o carpeta.
  - **Type.** En la lista, haga clic en File o Folder. El valor predeterminado es File.
  - Haga clic en **Save** para guardar el archivo o carpeta, o bien haga clic en **Cancel** para no guardarlos.

**Nota:** Para eliminar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

### 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Delete Files and Folders Policy**.

The screenshot shows the XenMobile interface for configuring a policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Delete Files and Folders Policy' and includes a sidebar with steps: '1 Policy Info', '2 Platforms', and '3 Assignment' (which is selected). The main area contains a search box for 'Choose delivery groups' with a 'Search' button. Below the search box, there are two checkboxes: 'AllUsers' (checked) and 'sales' (unchecked). To the right, there is a box titled 'Delivery groups to receive app assignment' containing 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a right-pointing arrow and a help icon. 'Back' and 'Save' buttons are located at the bottom right.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de eliminación de valores y claves de Registro

Mar 02, 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**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Registry keys and values to delete

Key*	Value	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

► Deployment Rules

Back Next >

6. Configure los siguientes parámetros:

- **Registry keys and values to delete.** Para cada valor y clave del Registro que quiera eliminar, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Key.** Escriba la ruta de la clave del Registro. Este campo es obligatorio. La ruta de la clave del Registro debe empezar por HKEY\_CLASSES\_ROOT\, HKEY\_CURRENT\_USER\, HKEY\_LOCAL\_MACHINE\ o HKEY\_USERS\.
  - **Value.** Escriba el nombre del valor que se va a eliminar, o bien deje el campo en blanco para eliminar toda la clave del Registro.
  - Haga clic en **Save** para guardar la clave y el valor, o bien haga clic en **Cancel** para no guardarlos.

**Nota:** Para eliminar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Delete Registry Keys and Values Policy**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Device Policies' sub-tab is selected. The main content area displays the 'Delete Registry Keys and Values Policy' configuration page. On the left, a sidebar shows the policy configuration steps: '1 Policy Info', '2 Platforms', and '3 Assignment' (highlighted). The 'Assignment' step is expanded, showing a 'Choose delivery groups' section with a search box and a list of groups: 'AllUsers' (checked) and 'sales' (unchecked). Below this is a 'Delivery groups to receive app assignment' section with a list containing 'AllUsers'. At the bottom of the main area, there is a 'Deployment Schedule' link and 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de atestación de estado de dispositivos

Mar 02, 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**.

**Device Health Attestation Policy**

**Policy Information**  
This policy enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine the health of a Windows 10 device and take compliance actions when necessary.

Policy Name\*

Description

1 Policy Info

2 Platforms

Windows Phone

Windows Desktop/Tablet

3 Assignment

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

**Device Health Attestation Policy**

This policy enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine the health of a Windows 10 device and take compliance actions when necessary.

Enable Device Health Attestation

► **Deployment Rules**

1 Policy Info

2 Platforms

Windows Phone

Windows Desktop/Tablet

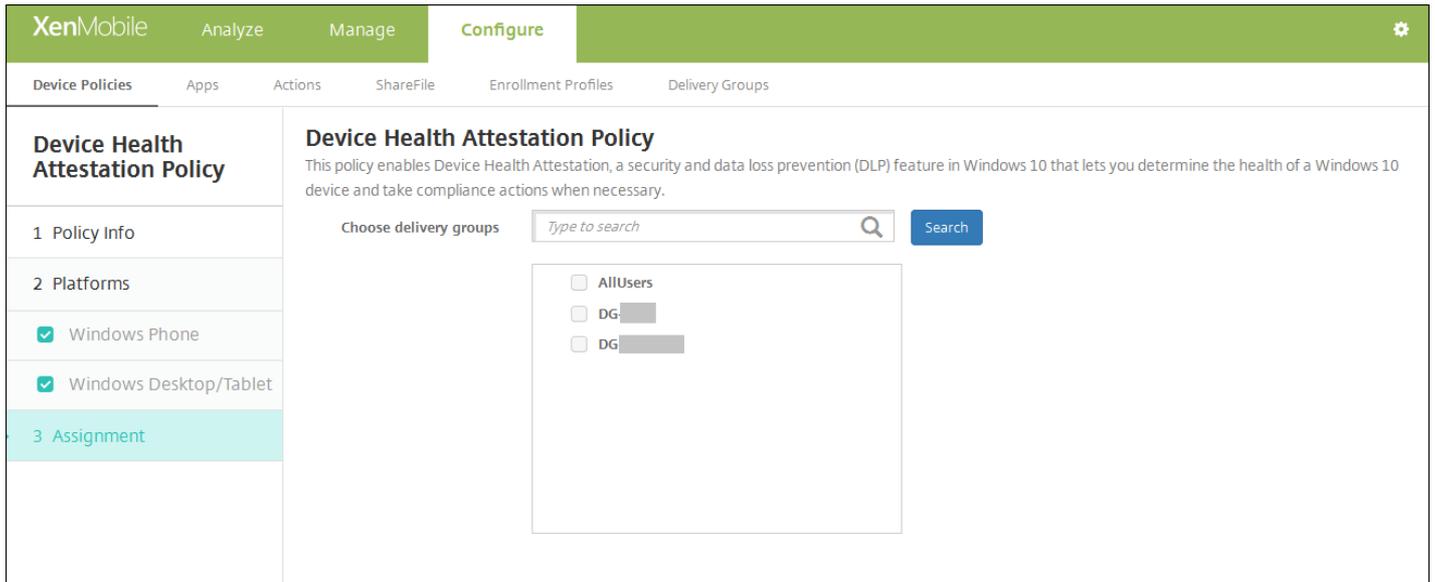
3 Assignment

Configure este parámetro para cada plataforma seleccionada:

- **Enable Device Health Attestation.** Seleccione si se debe requerir la atestación de estado de los dispositivos. El valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación de la directiva **Device Health Attestation**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de nombres de dispositivos

Mar 02, 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 de información **Device Name Policy**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Device Name Policy' and features a 'Policy Information' section. This section contains a description: 'This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.' Below the description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is a text input, and the 'Description' field is a larger text area. On the left side of the page, there is a sidebar with a 'Device Name Policy' section. This section has three sub-sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' sub-section is currently selected and highlighted in light blue. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. At the bottom right of the page, there is a green button labeled 'Next >'.

4. En el panel **Policy Information**, escriba la información siguiente:

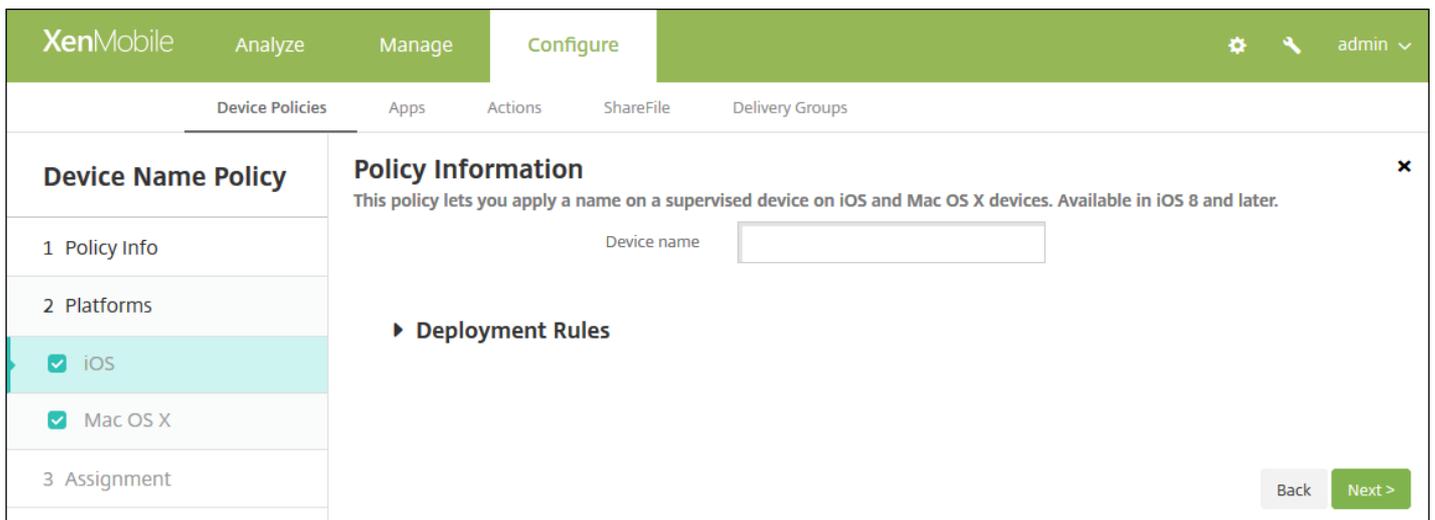
- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS y Mac OS X

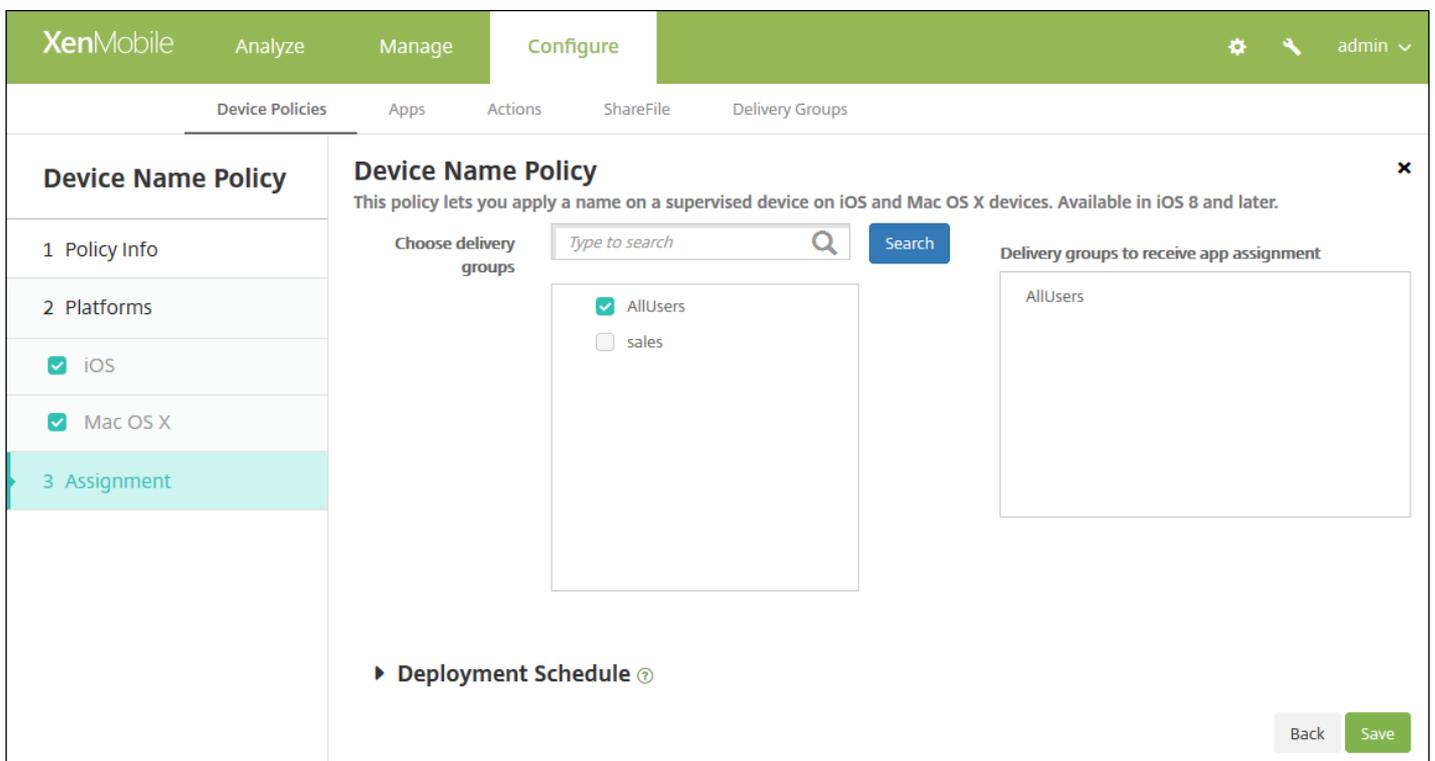


Configure este parámetro para las plataformas que elija:

- **Device name.** Escriba la macro, una combinación de ellas o una combinación de macros y texto para darle a cada dispositivo un nombre único. Por ejemplo, use `${device.serialnumber}` para establecer el número de serie de cada dispositivo como su nombre, o bien utilice `${device.serialnumber} ${user.username}` para incluir el nombre de usuario en el nombre del dispositivo.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Device Name Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o

varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directiva Enterprise Hub para dispositivos

Mar 02, 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**.

The screenshot shows the XenMobile console interface for configuring an Enterprise Hub Policy. The main content area is titled "Enterprise Hub Policy" and contains a "Policy Information" section. This section includes a text box for "Policy Name\*" and a larger text box for "Description". A note explains that to create the policy, you need an AET (.aetx) signing certificate from Symantec and a signed Citrix Company Hub app using XapSignTool.exe. A "Next >" button is located at the bottom right of the "Policy Information" section. The left sidebar shows the "Enterprise Hub Policy" configuration steps: "1 Policy Info", "2 Platforms", and "3 Assignment". The "1 Policy Info" step is currently selected. Under "2 Platforms", "Windows Phone" is selected with a checkmark. The "Assignment" section is currently empty. The top navigation bar includes "XenMobile", "Analyze", "Manage", and "Configure". The top right corner shows a gear icon, a magnifying glass icon, and "admin" with a dropdown arrow. The bottom navigation bar shows "Device Policies", "Apps", "Actions", "ShareFile", and "Delivery Groups".

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 **Siguiente**. Aparecerá la página de la plataforma **Windows Phone**.

6. Configure los siguientes parámetros:

- **Upload .aetx file.** Seleccione el archivo AETX. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Upload signed Enterprise Hub app.** Seleccione la aplicación Enterprise Hub. Para ello, haga clic en **Browse** y vaya a la ubicación de la aplicación.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Enterprise Hub Policy**.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de archivos

Mar 02, 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 luego, en **Apps**, haga clic en **Files**. Aparecerá la página de información **Files Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Files Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section is active, showing a form with 'Policy Name\*' and 'Description' fields. The 'Platforms' section shows 'Android' and 'Windows Mobile/CE' checked. A 'Next >' button is visible at the bottom right.

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 **Policy Platforms**.

The screenshot shows the XenMobile configuration interface for a 'Files Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Files Policy' section with sub-sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are both checked. The main content area is titled 'Policy Information' and contains the following fields and controls:

- File to be imported\***: A text input field with a 'Browse' button.
- File type**: Radio buttons for 'File' (selected) and 'Script'.
- Replace macro expressions**: A toggle switch set to 'OFF' with a help icon.
- Destination folder**: A dropdown menu showing '%XenMobile Folder%' with a help icon.
- Destination file name**: A text input field with a help icon.
- Copy file only if different**: A dropdown menu.

At the bottom of the main area, there is a 'Deployment Rules' section with a right-pointing arrow. At the bottom right of the interface, there are 'Back' and 'Next >' buttons.

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

The screenshot shows the XenMobile configuration interface for a Files Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Files Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with 'Android' and 'Windows Mobile/CE' checked), and '3 Assignment'. The main area is titled 'Policy Information' and contains the following configuration options:

- File to be imported\***: A text input field with a 'Browse' button.
- File type**: Radio buttons for 'File' (selected) and 'Script'.
- Replace macro expressions**: A toggle switch set to 'OFF'.
- Destination folder**: A dropdown menu showing '%XenMobile Folder%'.
- Destination file name**: A text input field.
- Copy file only if different**: A dropdown menu.

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

Configure los siguientes parámetros:

- **File to be imported.** Seleccione el archivo a importar; para ello, haga clic en Browse y, a continuación, vaya a la ubicación del archivo.
- **File type.** Seleccione **File** o **Script**. Si selecciona **Script**, aparecerá la opción **Execute immediately**. Seleccione si quiere que el script se ejecute tan pronto como el archivo se cargue. El valor predeterminado es **OFF**.
- **Replace macro expressions:** Seleccione si quiere reemplazar nombres de token de macro en un script con una propiedad de usuario o de dispositivo. El valor predeterminado es **OFF**.
- **Destination folder.** En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Add new** para elegir una ubicación de archivo no incluida en la lista. Además, puede usar las macros %XenMobile Folder%\ o %Flash Storage%\ como inicio del identificador de ruta.
- **Destination file name:** Si lo desea, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copy file only if different.** Seleccione en la lista si quiere copiar el archivo cuando sea diferente del archivo existente. La opción predeterminada es copiar el archivo solo si es diferente.

Configuración de los parámetros de Windows Mobile/CE

The screenshot shows the 'Configure' page for a 'Files Policy' in XenMobile. The left sidebar has sections for '1 Policy Info', '2 Platforms' (with 'Android' and 'Windows Mobile/CE' checked), and '3 Assignment'. The main area is titled 'Policy Information' and contains the following settings:

- File to be imported\***: A text input field with a 'Browse' button.
- File type**: Radio buttons for 'File' (selected) and 'Script'.
- Replace macro expressions**: A toggle switch set to 'OFF'.
- Destination folder**: A dropdown menu showing '%My Documents%'.
- Destination file name**: A text input field with a help icon.
- Copy file only if different**: A dropdown menu showing 'Copy file only if different'.
- Read only file**: A toggle switch set to 'OFF'.
- Hidden file**: A toggle switch set to 'OFF'.

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

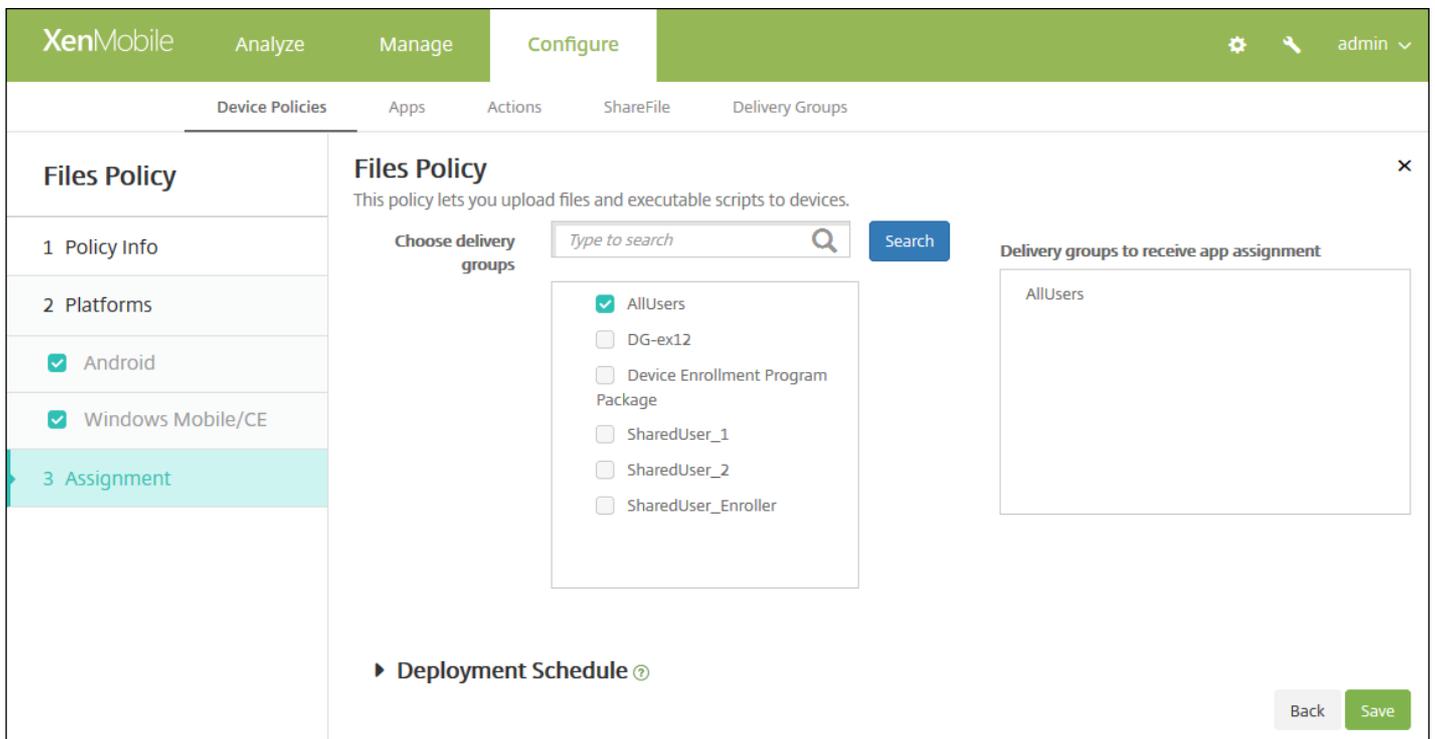
Configure los siguientes parámetros:

- **File to be imported.** Seleccione el archivo a importar; para ello, haga clic en Browse y, a continuación, vaya a la ubicación del archivo.
- **File type.** Seleccione **File** o **Script**. Si selecciona **Script**, aparecerá la opción **Execute immediately**. Seleccione si quiere que el script se ejecute tan pronto como el archivo se cargue. El valor predeterminado es **OFF**.
- **Replace macro expressions:** Seleccione si quiere reemplazar nombres de token de macro en un script con una propiedad de usuario o de dispositivo. El valor predeterminado es **OFF**.
- **Destination folder.** En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Add new** para elegir una ubicación de archivo no incluida en la lista. Además, puede utilizar cualquiera de las siguientes macros como inicio del identificador de ruta:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name:** Si lo desea, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copy file only if different.** Seleccione en la lista si quiere copiar el archivo cuando sea diferente del archivo existente. La opción predeterminada es copiar el archivo solo si es diferente.
- **Read only file.** Seleccione si el archivo será de solo lectura. El valor predeterminado es **OFF**.
- **Hidden file.** Seleccione esta opción si no quiere que el archivo se muestre en la lista de archivos. El valor predeterminado

es **OFF**.

## 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Files Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará a iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directiva de fuentes

Mar 02, 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**.

The screenshot shows the XenMobile interface for configuring a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is active, and the 'Font Policy' page is displayed. The page has a sidebar on the left with three sections: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked checkboxes: 'iOS' and 'Mac OS X'. The main area is titled 'Policy Information' and contains a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' (a text input) and 'Description' (a text area). A green 'Next >' button is located at the bottom right of the main content area.

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.

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

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Font Policy' configuration steps: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Mac OS X' selected), and '3 Assignment'. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below this, there are two main sections: 'Policy Information' and 'Policy Settings'. The 'Policy Information' section has a text input for 'User-visible name' and a 'Font file' input with a 'Browse' button. The 'Policy Settings' section has radio buttons for 'Remove policy' (with 'Select date' selected), a date picker, and a dropdown for 'Allow user to remove policy' set to 'Always'. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure los siguientes parámetros:

- **User-visible name.** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Font file.** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always, Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows 'Font Policy' with sub-sections: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Mac OS X' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and contains the following fields:

- User-visible name:** A text input field with a help icon.
- Font file:** A text input field with a 'Browse' button.
- Policy Settings:**
  - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'. Below the 'Duration until removal' option is a date picker.
  - Allow user to remove policy:** A dropdown menu currently set to 'Always'.
  - Profile scope:** A dropdown menu currently set to 'User'. To its right, the text 'OS X 10.7+' is displayed.

At the bottom of the main area, there is a 'Deployment Rules' section with a right-pointing arrow. At the bottom right of the page, there are 'Back' and 'Next >' buttons.

Configure los siguientes parámetros:

- **User-visible name.** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Font file.** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

#### 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Font Policy**.

The screenshot shows the XenMobile Configure interface for a 'Font Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Font Policy' section is active, showing a sidebar with 'Policy Info', 'Platforms', and 'Assignment' (highlighted). The 'Platforms' section has 'iOS' and 'Mac OS X' selected. The main area is titled 'Font Policy' and includes a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below this, there are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar with the placeholder 'Type to search' and a 'Search' button. Below the search bar is a list of delivery groups: 'AllUsers' (checked) and 'sales' (unchecked). The 'Delivery groups to receive app assignment' section shows a list containing 'AllUsers'. At the bottom of the main area, there is a 'Deployment Schedule' link with a help icon. In the bottom right corner, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de importación de perfiles de iOS y Mac OS X

Mar 02, 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](#).

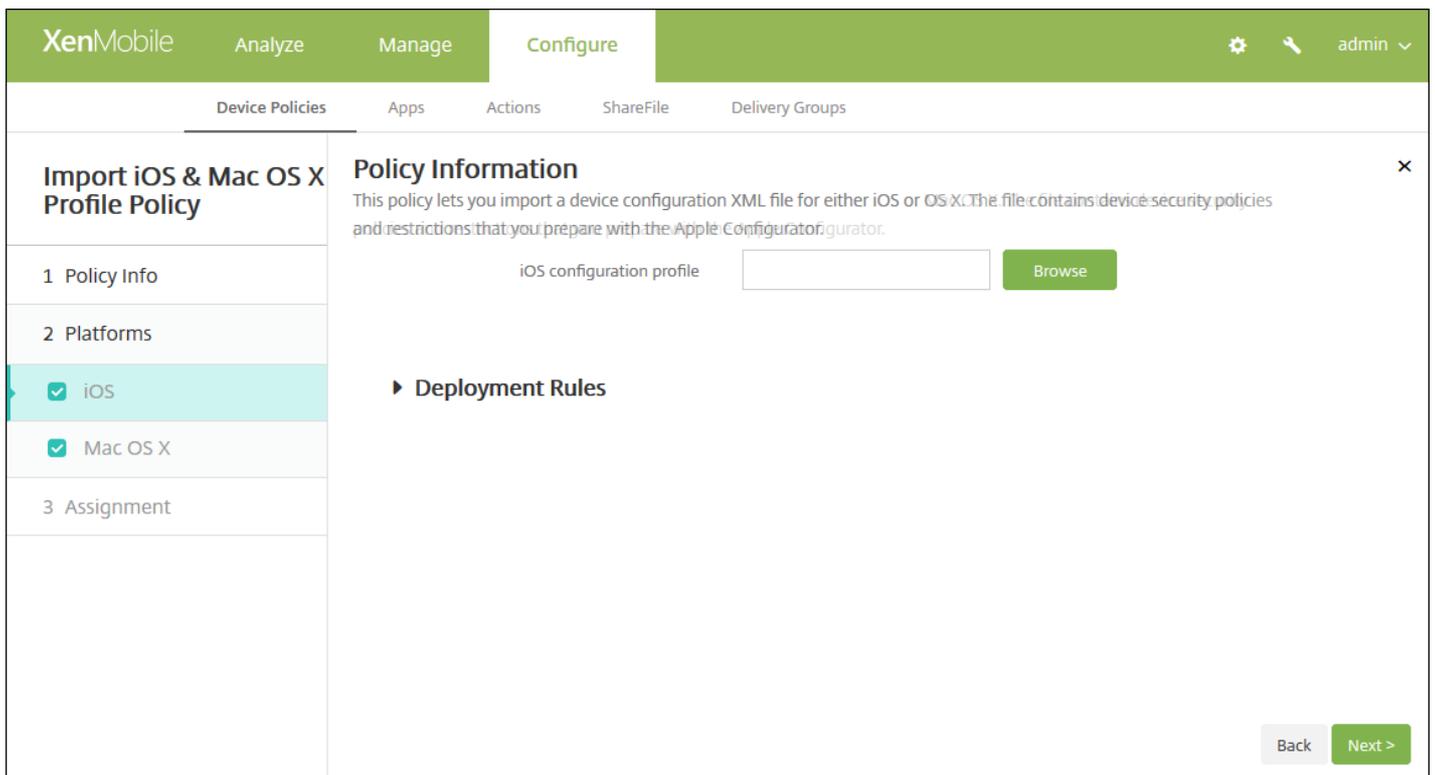
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y, a continuación, en **Custom**, haga clic en **Import iOS & Mac OS X Profile**. Aparecerá la página de información **Import iOS & Mac OS X Profile Policy**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure. The 'Configure' tab is active. Below the navigation, there are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The 'Device Policies' sub-tab is selected. A modal dialog titled 'Import iOS & Mac OS X Profile Policy' is open. The dialog has a close button (X) in the top right corner. On the left side of the dialog, there is a sidebar with three steps: '1 Policy Info' (highlighted in light blue), '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. The main content area of the dialog is titled 'Policy Information' and contains the following text: 'This policy lets you import a device configuration XML file for either iOS or Mac OS X. The file contains device security policies and restrictions that you prepare with the Apple Configurator.' Below this text are two input fields: 'Policy Name\*' (with an asterisk indicating it is required) and 'Description'. A green 'Next >' button is located at the bottom right of the dialog.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.



6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

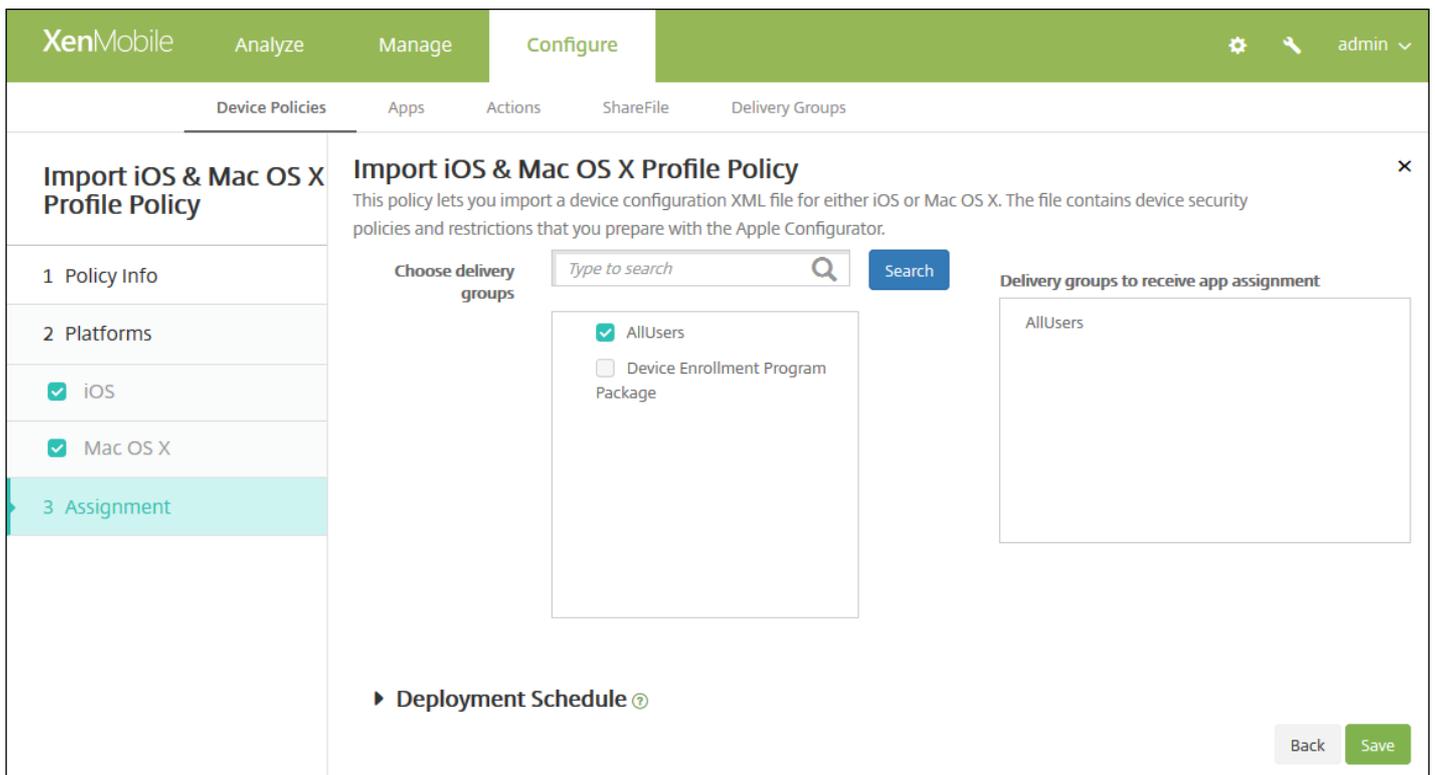
Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma. .

7. Configure esta opción para cada plataforma seleccionada:

- **iOS configuration profile** o **Mac OS X configuration profile**. Seleccione el archivo de configuración que quiera importar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

8. [Configure las reglas de implementación.](#)

9. Haga clic en **Siguiente**. Aparecerá la página de asignación **Import iOS & Mac OS X Profile Policy**.



10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

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 dispositivo Kiosk para Samsung SAFE

Mar 02, 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, en el dispositivo móvil, como se describe en [Directivas de dispositivo de clave de licencia MDM de Samsung](#). Este paso le permite habilitar directivas en dispositivos Samsung SAFE.
2. Habilite la directiva Connection Scheduling para dispositivos Android, según se describe en [Directivas de dispositivo de programación de conexiones](#). Este paso permite que los dispositivos Android se conecten con XenMobile.
3. Agregue una directiva de dispositivo Kiosk, como se describe en la sección siguiente.
4. Asigne esas tres directivas de dispositivo a los grupos de entrega adecuados. Decida si quiere incluir otras directivas, como App Inventory, en esos grupos de entrega.

Si más adelante desea quitar los dispositivos del modo quiosco, cree una nueva directiva de dispositivo Kiosk que tenga el parámetro **Kiosk mode** configurado con **Disable**. Actualice los grupos de entrega para quitar la directiva Kiosk que habilitaba el modo quiosco y agregue la directiva Kiosk que lo inhabilita.

## Para agregar una directiva de dispositivo Kiosk

### Nota:

- Todas las aplicaciones que especifique para el modo quiosco deben estar ya instaladas en los dispositivos de los usuarios.
- Algunas opciones solo se aplican a Samsung Mobile Device Management (MDM) API 4.0 y versiones posteriores.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Kiosk**. Aparecerá la página **Kiosk Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar with a 'Kiosk Policy' header and three items: '1 Policy Info' (highlighted in light blue), '2 Platforms', and '3 Assignment' (with a checkmark and 'Samsung SAFE' text). The main content area is titled 'Policy Information' and contains a description: 'This policy lets you activate Kiosk mode on an Android device, in which only a specific app or apps can run on the device.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Samsung SAFE**.

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view for 'Kiosk Policy' with sub-items: '1 Policy Info', '2 Platforms', '3 Assignment', and 'Samsung SAFE' (which is selected). The main content area is titled 'Policy Information' and contains the following configuration options:

- General**
  - Kiosk mode:  Enable,  Disable
  - Launcher package: [Text input field]
  - Emergency phone number: [Text input field] **MDM 4.0+**
  - Allow navigation bar:  ON **MDM 4.0+**
  - Allow multi-window mode:  ON **MDM 4.0+**
  - Allow status bar:  ON **MDM 4.0+**
  - Allow system bar:  ON
  - Allow task manager:  ON
  - Common SAFE passcode: [Text input field]
- Wallpapers**
  - Define a home wallpaper:  OFF
  - Define a lock wallpaper:  OFF **MDM 4.0+**
- Apps**
  - New app to add\*: [Text input field]
- Deployment Rules**

At the bottom right, there are 'Back' and 'Next >' buttons.

6. Configure los siguientes parámetros:

- **Kiosk mode.** Haga clic en **Enable** o **Disable**. El valor predeterminado es **Enable**. Si hace clic en **Disable**, desaparecerán todas las opciones siguientes.
- **Launcher package.** Citrix recomienda dejar este campo en blanco si no se ha desarrollado internamente un programa de inicio para permitir que los usuarios abran la aplicación o las aplicaciones de quiosco. Si está usando un programa interno de inicio, escriba el nombre completo del paquete de aplicaciones de ese programa.

- **Emergency phone number.** Escriba un número de teléfono opcional. Una persona que encuentre un dispositivo perdido podrá usar este número para ponerse en contacto con su empresa. Se aplica solo a MDM 4.0 y versiones posteriores.
- **Allow navigation bar.** Seleccione si permitir que los usuarios vean y usen la barra de navegación en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow multi-window mode.** Seleccione si permitir que los usuarios usen varias ventanas en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow status bar.** Seleccione si permitir que los usuarios vean la barra de estado en el modo de quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. El valor predeterminado es **ON**.
- **Allow system bar.** Seleccione si permitir que los usuarios vean la barra del sistema en el modo de quiosco. El valor predeterminado es **ON**.
- **Allow task manager.** Seleccione si permitir que los usuarios vean y usen el Administrador de tareas en el modo de quiosco. El valor predeterminado es **ON**.
- **Common SAFE passcode.** Si ha configurado una directiva general de códigos de acceso para todos los dispositivos Samsung SAFE, escriba el mismo código opcional de la directiva en este campo.
- **Fondos de pantalla**
  - **Define a home wallpaper.** Seleccione si utilizar una imagen personalizada para la pantalla de inicio en el modo de quiosco. El valor predeterminado es **OFF**.
    - **Home image.** Cuando habilite **Define a home wallpaper**, seleccione un archivo de imagen. Para ello, podrá hacer clic en **Browse** e ir a la ubicación del archivo.
  - **Define a lock wallpaper.** Seleccione si utilizar una imagen personalizada para la pantalla de bloqueo en el modo quiosco. El valor predeterminado es **OFF**. Se aplica solo a MDM 4.0 y versiones posteriores.
    - **Lock image.** Cuando habilite **Define a lock wallpaper**, seleccione un archivo de imagen. Para ello, podrá hacer clic en **Browse** e ir a la ubicación del archivo.
- **Apps.** Para agregar cada aplicación al modo quiosco, haga clic en **Add** y lleve a cabo lo siguiente:
  - **New app to add.** Escriba el nombre completo de la aplicación que se va a agregar. Por ejemplo, com.android.calendar permite a los usuarios utilizar la aplicación Calendario de Android.
  - Haga clic en **Save** para agregar la aplicación, o bien haga clic en **Cancel** para no agregarla.

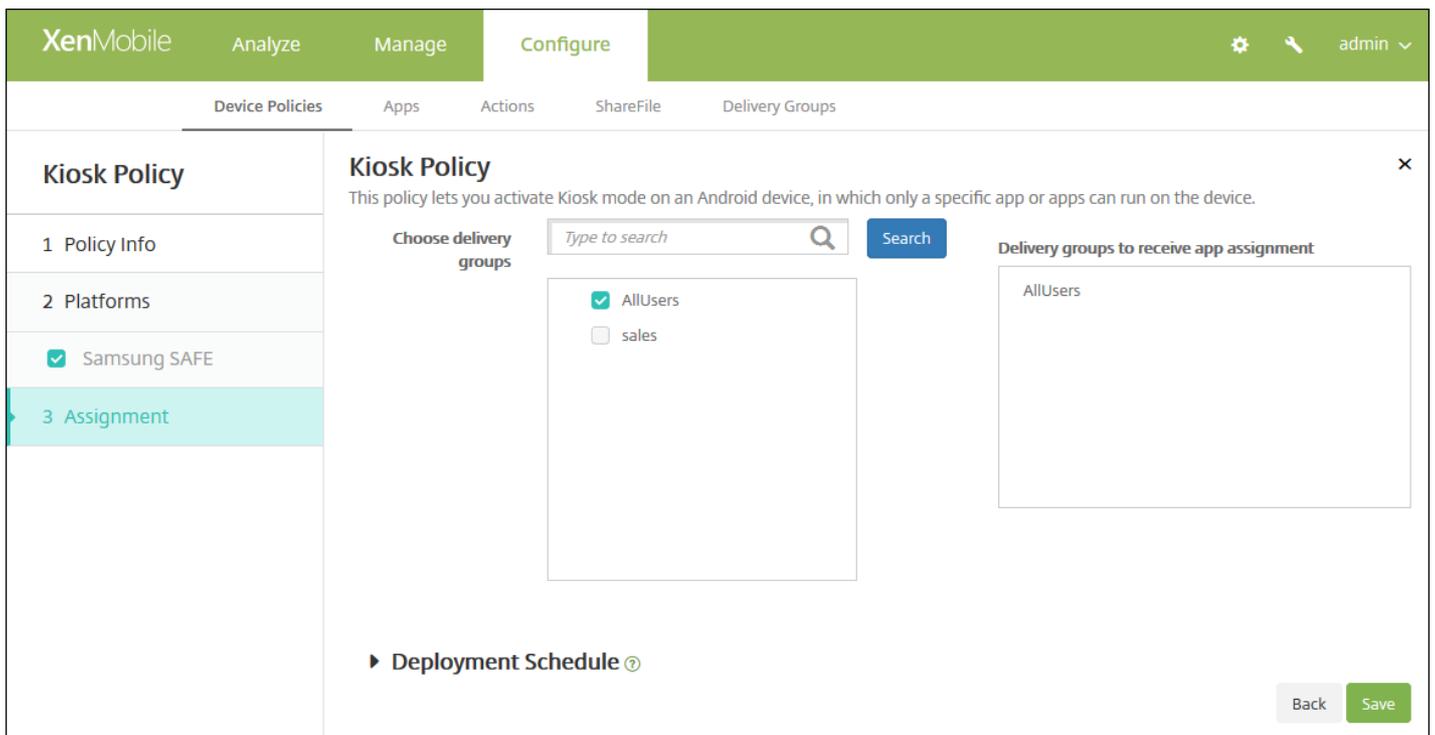
**Nota:** Para eliminar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una aplicación existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.



8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Kiosk Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará a iOS.

11. Haga clic en **Save**.

# Directiva de configuración de Launcher para Android

Mar 02, 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 **Siguiente**. Aparecerá la página de información **Android Platform**.

The screenshot shows the 'Configure' page for a 'Launcher Configuration Policy'. The left sidebar has three sections: '1 Policy Info', '2 Platforms' (with 'Android' selected), and '3 Assignment'. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you define a configuration of an Android device launcher.' Below this is the 'Launcher app configuration' section with two toggle switches: 'Define a logo image' (set to ON) and 'Define a background image' (set to ON). Each toggle has a corresponding text input field and a 'Browse' button. The 'Logo image' field contains 'ribbon.png'. Below this is the 'Allowed apps' section, which is a table with columns 'App name', 'Package Name\*', and an 'Add' icon. The table contains one row with 'test' in the 'App name' column and 'test.com' in the 'Package Name\*' column. At the bottom of the main content area is a 'Password' input field. A 'Deployment Rules' section is partially visible at the bottom. At the bottom right of the page are 'Back' and 'Next >' buttons.

6. Configure los siguientes 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.
- **Aplicaciones permitidas.** Para cada aplicación que quiera permitir en Citrix Launcher, haga clic en **Agregar** 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 guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Password.** La contraseña que el usuario debe introducir para salir de Citrix Launcher.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Launcher Configuration Policy**.

9. Configure las reglas de implementación. 

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

12. Haga clic en **Save**.

# Directivas LDAP de dispositivos

Mar 02, 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**.

The screenshot shows the XenMobile console interface for configuring an LDAP Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'LDAP Policy' and features a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is active and displays a 'Policy Information' form. This form includes a 'Policy Name\*' field and a 'Description' field. The '2 Platforms' section shows checkboxes for 'iOS' and 'Mac OS X', both of which are checked. A 'Next >' button is located at the bottom right of the form.

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 de información **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de iOS

Configure los siguientes parámetros:

- **Account description.** Indique una descripción opcional de la cuenta.
- **Account user name.** Escriba un nombre de usuario opcional.
- **Account password.** Escriba una contraseña opcional. Use esta opción solo con perfiles cifrados.
- **LDAP host name.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor LDAP. El valor predeterminado es **ON**.
- **Search Settings.** Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Add** y lleve a cabo lo siguiente:
  - **Description.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
  - **Scope.** En la lista, haga clic en **Base**, **One level** o **Subtree** para definir los niveles de búsqueda en el árbol LDAP. El valor predeterminado es Base.
    - El nivel Base busca en el nodo al que apunta Search base.
    - El nivel One level busca en el nodo Base y en un nivel por debajo de él.
    - El nivel Subtree busca en el nodo Base, además de todos sus elementos secundarios, independientemente de la profundidad.
  - **Search base.** Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o 0=empresa de ejemplo. Este campo es obligatorio.

- Haga clic en **Save** para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
- Repita estos pasos para cada opción de búsqueda que quiera agregar.

**Nota:** Para eliminar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

Para modificar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

### Configuración de los parámetros de Mac OS X

The screenshot shows the XenMobile configuration interface for an LDAP Policy. The 'Configure' tab is active, and the 'Mac OS X' platform is selected under the 'Platforms' section. The 'Policy Information' section includes fields for Account description, Account user name, Account password, and LDAP host name\*. The 'Use SSL' toggle is turned ON. The 'Search Settings' section has a table with columns for Description\*, Scope, and Search base\*, and an Add button. The 'Policy Settings' section includes 'Remove policy' options (Select date or Duration until removal (in days)), 'Allow user to remove policy' (set to Always), and 'Profile scope' (set to User). A 'Deployment Rules' section is partially visible at the bottom. Navigation buttons for 'Back' and 'Next >' are located at the bottom right.

Configure los siguientes parámetros:

- **Account description.** Indique una descripción opcional de la cuenta.
- **Account user name.** Si quiere, escriba un nombre de usuario.
- **Account password.** Escriba una contraseña opcional. Use esta opción solo con perfiles cifrados.
- **LDAP host name.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Use SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor LDAP. El valor predeterminado es **ON**.
- **Search Settings.** Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Add** y lleve a cabo lo siguiente:
  - **Description.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
  - **Scope.** En la lista, haga clic en **Base**, **One level** o **Subtree** para definir los niveles de búsqueda en el árbol LDAP. El valor predeterminado es Base.
    - El nivel Base busca en el nodo al que apunta Search base.
    - El nivel One level busca en el nodo Base y en un nivel por debajo de él.
    - El nivel Subtree busca en el nodo Base, además de todos sus elementos secundarios, independientemente de la profundidad.
  - **Search base.** Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o O=empresa de ejemplo. Este campo es obligatorio.
  - Haga clic en **Save** para agregar la opción de búsqueda, o bien haga clic en Cancel para no agregarla.
  - Repita estos pasos para cada opción de búsqueda que quiera agregar.

**Nota:** Para eliminar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en Delete para eliminar el elemento, o bien haga clic en Cancel para conservarlo.

Para modificar una opción de búsqueda existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en Save para guardar los cambios, o bien en Cancel para no guardarlos.

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
- En **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

## 7. Configure las reglas de implementación.



8. Haga clic en **Siguiente**. Aparecerá la página de asignación **LDAP Policy**.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directivas de ubicación

Mar 02, 2017

En XenMobile, puede crear directivas de ubicación para aplicar límites geográficos y realizar un seguimiento de la ubicación y del movimiento de los dispositivos de los usuarios. Cuando los usuarios abandonen el perímetro definido (también conocido como *geocerca*), XenMobile puede realizar un borrado completo o selectivo de los datos del dispositivo, ya sea inmediatamente o tras un período de tiempo específico establecido para permitir a los usuarios volver a la ubicación permitida.

Puede crear directivas de ubicación para dispositivos iOS y para Android. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **Location**. Aparecerá la página de información **Location Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is selected. Below the navigation bar, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is active. On the left side, there is a sidebar with a 'Location Policy' header and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is highlighted. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below the description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty, and the 'Description' field is a large text area. A 'Next >' button is located at the bottom right of the form.

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 **Siguiente**. 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

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Location Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with 'iOS' and 'Android' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below this is the 'Device agent configuration' section with the following settings:

- Location Timeout: 1 (Minutes)
- Tracking duration: 6 (Hours)
- Accuracy: 328 (Feet)
- Report if Location Services are disabled: OFF
- Geofencing: OFF

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Location timeout.** Escriba un número y, en la lista, haga clic en **Seconds** o **Minutes** para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es de 1 minuto.
- **Tracking duration.** Escriba un número y, en la lista, haga clic en **Hours** o **Minutes** para definir la duración con que XenMobile realiza el seguimiento del dispositivo. Los valores válidos son de 1 a 6 horas o de 10 a 360 minutos. El valor predeterminado es de 6 horas.
- **Accuracy.** Escriba un número y, en la lista, haga clic en **Meters**, **Feet** o **Yards** la precisión con que XenMobile realiza el seguimiento del dispositivo. Los valores válidos varían entre 10 y 5000 yardas o metros, o bien entre 30 y 15000 pies. El valor predeterminado es de 328 pies.
- **Report if Location Services are disabled.** Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. El valor predeterminado es **OFF**.
- **Geocercas**

Geofencing  ON

Radius

Center point latitude\*

Center point longitude\*

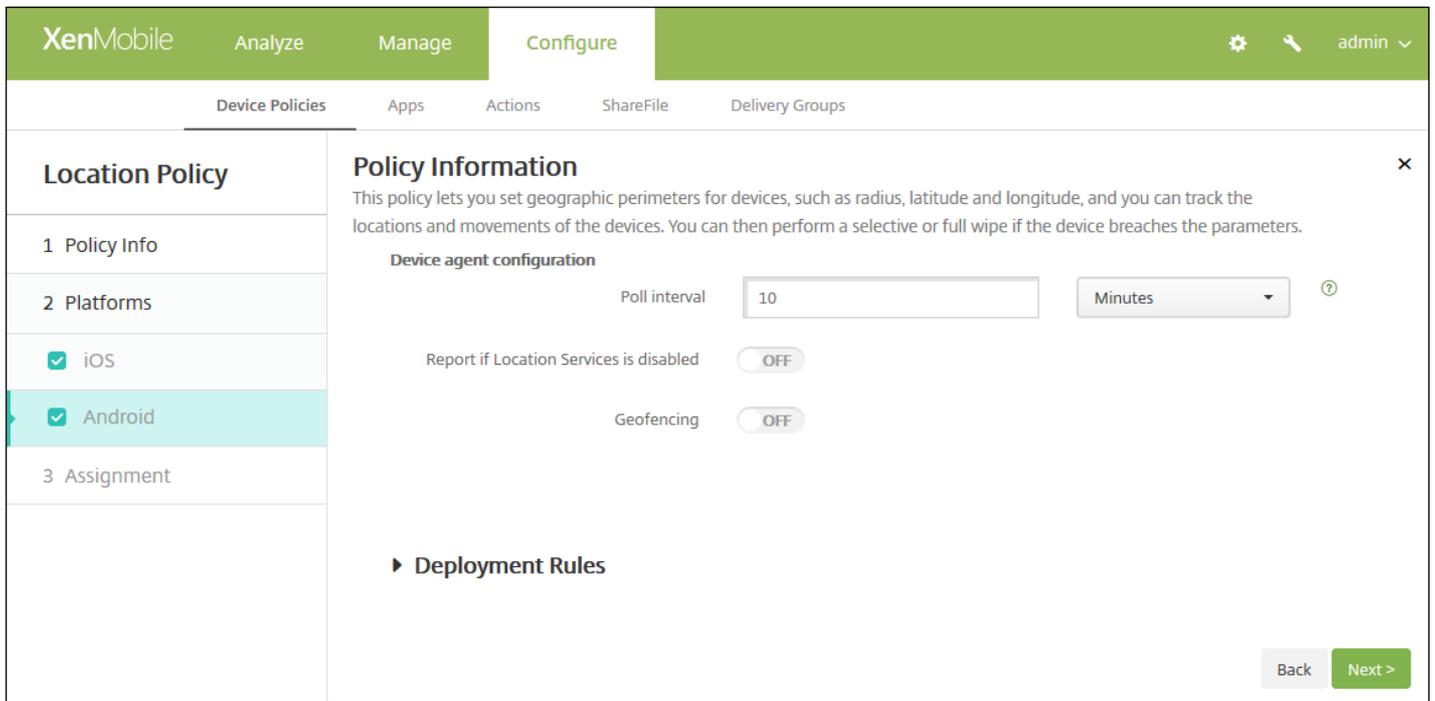
Warn user on perimeter breach  OFF ?

Wipe corporate data on perimeter breach  OFF

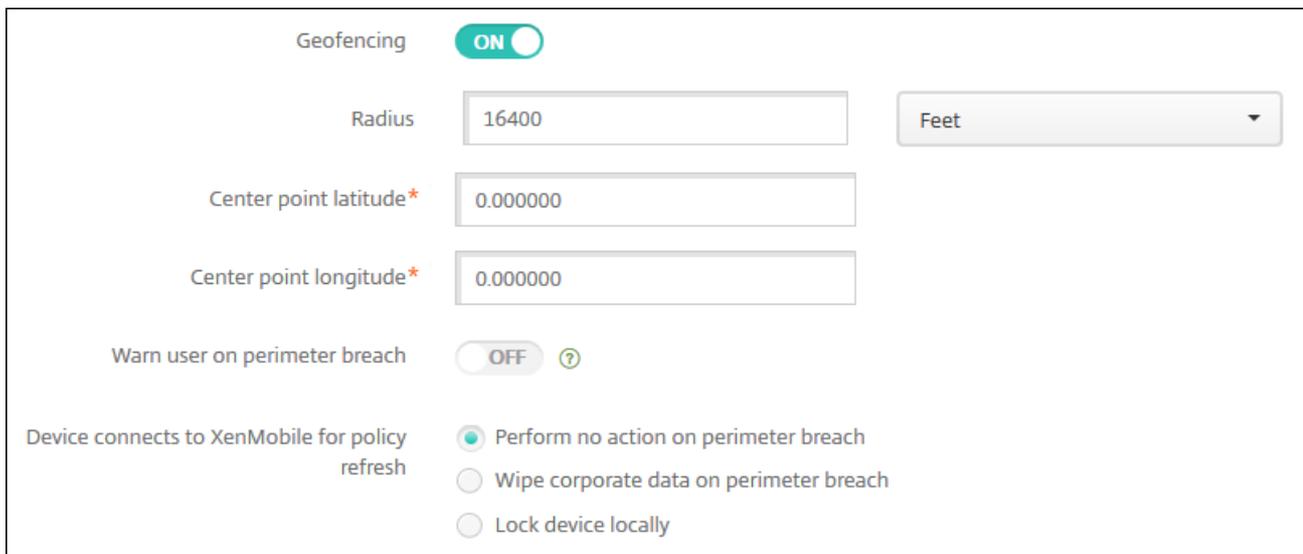
Al habilitar geocercas, configure los siguientes parámetros:

- **Radius.** Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies. Los valores válidos para el radio del perímetro son:
  - De 164 a 164 000 pies
  - De 50 a 50 000 metros
  - De 54 a 54 680 yardas
  - De 1 a 31 millas
- **Center point latitude.** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geovalla.
- **Center point longitude.** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geovalla.
- **Warn user on perimeter breach.** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **OFF**. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- **Wipe corporate data on perimeter breach.** Seleccione si borrar los datos de los dispositivos de los usuarios cuando estos abandonen el perímetro. El valor predeterminado es **OFF**. Si habilita esta opción, aparecerá el campo **Delay on local wipe**.
  - Escriba un número y, en la lista, haga clic en **Seconds** o **Minutes** para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.

Configuración de los parámetros de Android



- **Poll interval.** Escriba un número y, en la lista, haga clic en **Minutes, Hours** o **Days** para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 1 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier número de días. El valor predeterminado es 10 minutos. Si este valor es menor de 10 minutos, puede afectar de forma negativa a la duración de la batería del dispositivo.
- **Report if Location Services are disabled.** Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. El valor predeterminado es **OFF**.
- **Geocercas**



Al habilitar geocercas, configure los siguientes parámetros:

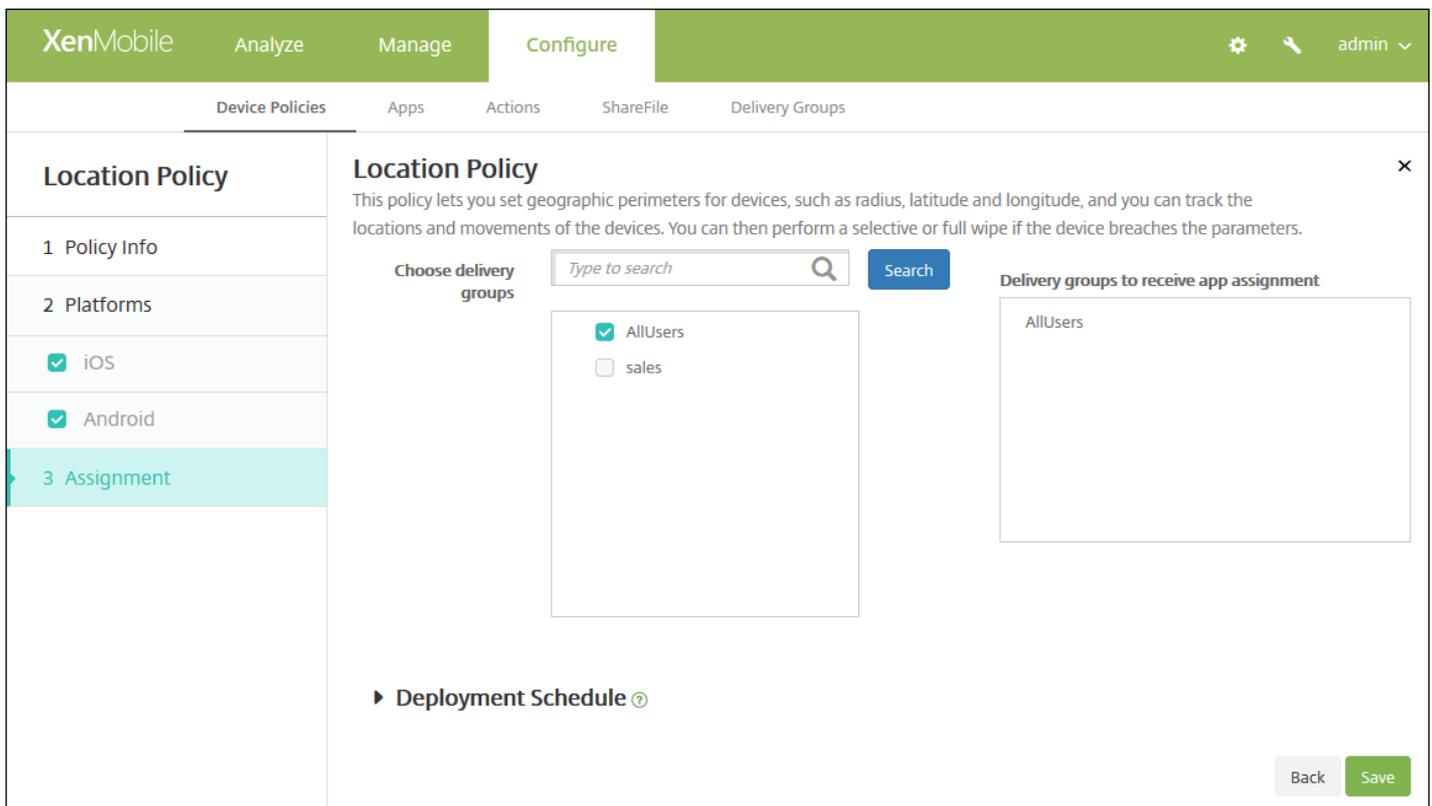
- **Radius.** Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16,400 pies. Los valores válidos para el radio del perímetro son:

- De 164 a 164 000 pies
- De 1 a 50 kilómetros
- De 50 a 50 000 metros
- De 54 a 54 680 yardas
- De 1 a 31 millas
- **Center point latitude.** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geovalla.
- **Center point longitude.** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geovalla.
- **Warn user on perimeter breach.** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **OFF**. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- **Device connects to XenMobile for policy refresh.** Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
  - **Perform no action on perimeter breach.** No hacer nada. Ésta es la opción predeterminada.
  - **Wipe corporate data on perimeter breach.** Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparece el campo **Delay on local wipe**.
    - Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de borrar datos empresariales de los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile borre sus dispositivos de manera selectiva. El valor predeterminado es de 0 segundos.
  - **Delay on lock.** Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Delay on lock**.
    - Escriba un número y, en la lista, haga clic en Seconds o Minutes para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta opción ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile bloquee sus dispositivos. El valor predeterminado es de 0 segundos.

## 7. Configure las reglas de implementación.



8. Haga clic en **Next**. Aparecerá la página de asignación **Location Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

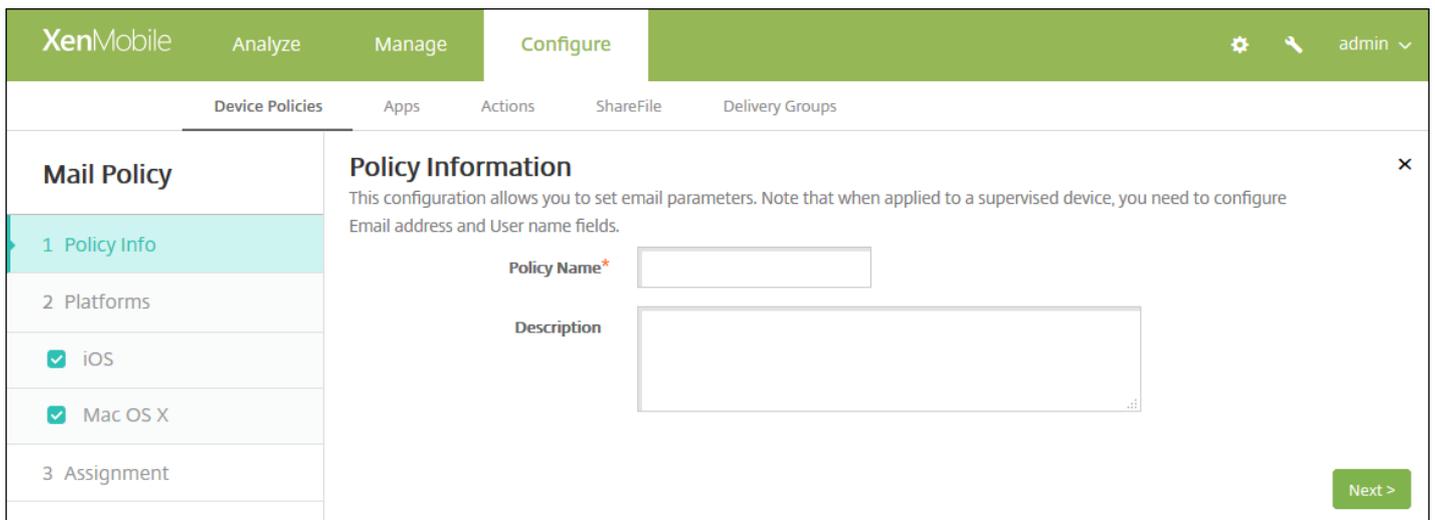
11. Haga clic en **Save**.

# Directivas de correos electrónicos

Mar 02, 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**.

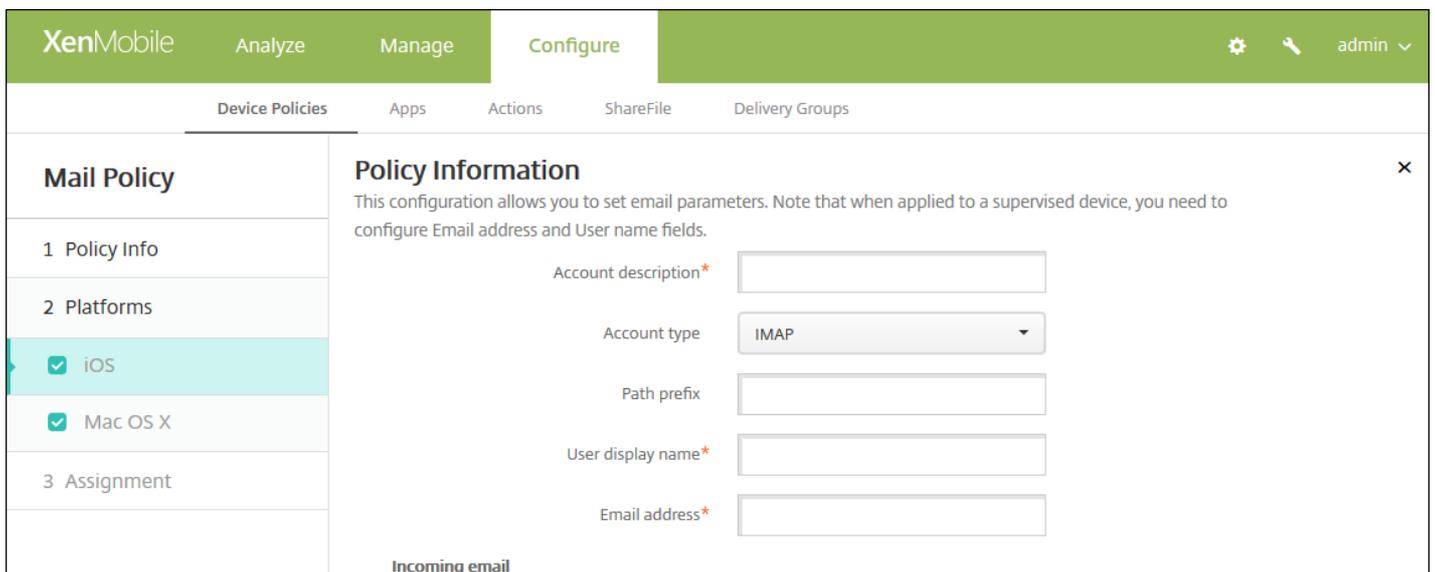


The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Mail Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing 'iOS' and 'Mac OS X' with checked boxes. The main area is titled 'Policy Information' and contains a text box for 'Policy Name\*' and a larger text box for 'Description'. A 'Next >' button is located at the bottom right of the main area.

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** de Mail Policy.



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Mail Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing 'iOS' and 'Mac OS X' with checked boxes. The main area is titled 'Policy Information' and contains a text box for 'Account description\*', a dropdown menu for 'Account type' (set to 'IMAP'), a text box for 'Path prefix', a text box for 'User display name\*', and a text box for 'Email address\*'. A section titled 'Incoming email' is visible at the bottom of the main area.

Email server host name*	<input type="text"/>
Email server port*	<input type="text" value="143"/>
User name*	<input type="text"/>
Authentication type	<input type="text" value="Password"/>
Password	<input type="text"/>
Use SSL	<input type="checkbox" value="OFF"/>
<b>Outgoing email</b>	
Email server host name*	<input type="text"/>
Email server port*	<input type="text"/>
User name*	<input type="text"/>
Authentication type	<input type="text" value="Password"/>
Password	<input type="text"/>
Outgoing password same as incoming	<input type="checkbox" value="OFF"/>
Use SSL	<input type="checkbox" value="OFF"/>
<b>Policy</b>	
Authorize email move between accounts	<input type="checkbox" value="OFF"/> iOS 5.0+
Sending email only from mail app	<input type="checkbox" value="OFF"/> iOS 5.0+
Disable mail recents syncing	<input type="checkbox" value="OFF"/> iOS 6.0+
Enable S/MIME	<input type="checkbox" value="OFF"/> iOS 5.0+
<b>Policy Settings</b>	
Remove policy	<input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in days)
	<input type="text"/>
Allow user to remove policy	<input type="text" value="Always"/>
<b>► Deployment Rules</b>	

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 8 para la configuración de las reglas de implementación de esa plataforma.

7. Configure los siguientes parámetros para cada una de las plataformas seleccionadas.

- **Account description.** Indique una descripción de la cuenta. Esta descripción aparece en las aplicaciones Correo y Ajustes. Este campo es obligatorio.
- **Account type.** En la lista, haga clic en **IMAP** o **POP** para seleccionar el protocolo que se va a usar para las cuentas de usuario. El valor predeterminado es **IMAP**. Si selecciona **POP**, desaparece la opción **Path prefix**.
- **Path prefix.** Escriba **INBOX** o introduzca el prefijo de la ruta de su cuenta de correo electrónico IMAP (si no es **INBOX**). Este campo es obligatorio.
- **User display name.** Escriba el nombre de usuario completo que se va a usar para los mensajes, entre otros. Este campo es obligatorio.
- **Email address.** Escriba la dirección de correo electrónico completa de la cuenta. Este campo es obligatorio.
- **Configuración de correos electrónicos entrantes**
  - **Email server host name.** Escriba el nombre del host o la dirección IP del servidor de correos entrantes. Este campo es obligatorio.
  - **Email server port.** Escriba el número de puerto del servidor de correos entrantes. El valor predeterminado es **143**. Este campo es obligatorio.
  - **User name.** Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico del usuario hasta el carácter @. Este campo es obligatorio.
  - **Authentication type.** En la lista, haga clic para seleccionar el tipo de autenticación que se va a usar. El valor predeterminado es **Authentication type**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password.** Si quiere, escriba una contraseña para el servidor de correos entrantes.
  - **Use SSL.** Seleccione esta opción si el servidor de correos entrantes utiliza la autenticación de capa de sockets seguros (SSL). El valor predeterminado es **OFF**.
- **Configuración de correos electrónicos salientes**
  - **Email server host name.** Escriba el nombre del host o la dirección IP del servidor de correos salientes. Este campo es obligatorio.
  - **Email server port.** Escriba el número de puerto del servidor de correos salientes. Si no indica ningún número de puerto, se utiliza el puerto predeterminado para el protocolo especificado.
  - **User name.** Escriba el nombre de usuario de la cuenta de correo electrónico. Suele ser el mismo que la dirección de correo electrónico del usuario hasta el carácter @. Este campo es obligatorio.
  - **Authentication type.** En la lista, haga clic para seleccionar el tipo de autenticación que se va a usar. El valor predeterminado es **Authentication type**. Si se selecciona **None**, desaparece el campo **Password**.
  - **Password.** Si quiere, escriba una contraseña para el servidor de correos salientes.
  - **Outgoing password same as incoming.** Seleccione si las contraseñas entrantes y salientes son iguales. El valor predeterminado es **OFF**, lo que significa que las contraseñas son diferentes. Si se establece en **ON**, desaparece el campo anterior **Password**.
  - **Use SSL.** Seleccione esta opción si el servidor de correos salientes utiliza la autenticación de capa de sockets seguros (SSL). El valor predeterminado es **OFF**.
- **Directiva**
  - **Nota:** Al configurar parámetros de iOS, estas opciones solo se aplican a iOS 5.0 y versiones posteriores; no hay restricciones cuando se configure Mac OS X.
  - **Authorize email move between accounts.** Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta y reenviarlos y responderlos desde otra cuenta. El valor predeterminado es **OFF**.
  - **Sending email only from mail app.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación de correo de iOS para enviar correos electrónicos.
  - **Disable mail recents syncing.** Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes. El valor predeterminado es **OFF**. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.
  - **Enable S/MIME.** Seleccione si esta cuenta es compatible con el cifrado y la autenticación S/MIME. El valor

predeterminado es **OFF**. Si se establece en **ON**, aparecen los dos siguientes campos.

- **Signing identity credential.** En la lista, seleccione la credencial de firma que se va a usar.
- **Encryption identity credential.** En la lista, seleccione la credencial de cifrado que se va a usar.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, en la lista, haga clic en **User** o **System**. El valor predeterminado es **User**. Esta opción solo está disponible para Mac OS X 10.7 y versiones posteriores.

## 8. Configure las reglas de implementación.

9. Haga clic en **Next**. Aparecerá la página de asignación **Mail Policy**.

The screenshot shows the XenMobile 'Configure' interface for a 'Mail Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Mail Policy' and includes a sub-header 'Mail Policy' with a close button. Below the sub-header is a note: 'This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search input field with the placeholder 'Type to search' and a 'Search' button. Below it is a list of delivery groups with checkboxes: 'AllUsers' (checked), 'DG-ex12', 'Device Enrollment Program Package', 'SharedUser\_1', 'SharedUser\_2', and 'SharedUser\_Enroller'. The 'Delivery groups to receive app assignment' section shows a list with 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a right-pointing arrow and a help icon. In the bottom right corner, there are 'Back' and 'Save' buttons.

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.

- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

12. Haga clic en **Save** para guardar la directiva.

# Directiva de dominios administrados

Mar 02, 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 para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador Web. Esta directiva solo está disponible para dispositivos supervisados con iOS 8 y versiones posteriores. Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte [Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator](#).

Cuando un usuario envía un correo electrónico a un destinatario cuyo dominio no consta en la lista de dominios administrados de correo electrónico, el mensaje se marca en el dispositivo del usuario para avisarle de que envía un mensaje a una persona fuera del dominio empresarial.

Cuando un usuario intente abrir un elemento (documento, adjunto o descarga) con Safari desde un dominio que no conste en la lista de dominios Web administrados, la aplicación de empresa correspondiente abrirá el elemento. Si el elemento no es de un dominio Web que conste en la lista de dominios Web administrados, el usuario no podrá abrir el elemento con la aplicación de empresa, y deberá usar una aplicación personal no administrada.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.
3. Expanda **More** y, a continuación, en **Security**, haga clic en **Managed domains**. Aparecerá la página de información **Managed Domains Policy**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the tabs, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar with a 'Managed Domains Policy' section. Under this section, there are three items: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The '2 Platforms' item has a checkmark next to 'iOS'. The main content area shows the 'Policy Information' section. It contains a description: 'This policy lets you define managed domains that apply to the Safari browser. The payloads are supported only on iOS 8 and later supervised devices.' Below the description, there are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located in the bottom right corner of the main content area.

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 **Siguiente**. Aparecerá la página **iOS Platform**.

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: Analyze, Manage, and Configure. Below these are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The main content area is titled 'Managed Domains Policy' and includes a sidebar with steps: 1 Policy Info, 2 Platforms, 3 Assignment, and a selected 'iOS' option. The main area contains 'Policy Information' (describing the policy for Safari browser), 'Managed Domains' (with an 'Add' button), 'Managed Safari Web Domains' (with an 'Add' button), 'Policy Settings' (with radio buttons for 'Select date' and 'Duration until removal', a date picker, and a dropdown for 'Allow user to remove policy' set to 'Always'), and 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

## Cómo especificar dominios

6. Configure los siguientes parámetros:

- **Managed Domains**

- **Unmarked Email Domains.** Para cada dominio de correo electrónico que quiera incluir en la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Managed Email Domain.** Escriba el dominio de correo electrónico.
  - Haga clic en **Save** para guardar el dominio de correo electrónico, o bien haga clic en **Cancel** para no guardarlo.
- **Managed Safari Web Domains.** Para cada dominio Web que quiera incluir en la lista, haga clic en **Add** y lleve a cabo lo siguiente:
  - **Managed Web Domain.** Escriba el dominio Web.
  - Haga clic en **Save** para guardar el dominio Web, o bien haga clic en **Cancel** para no guardarlo.

**Nota:** Para eliminar un dominio existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un dominio existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado en el lado derecho. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

- **Configuraciones de directivas**

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## 7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Managed Domains Policy**.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige OFF, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es OFF.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se

realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de opciones de MDM

Mar 02, 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](#) o [Inscripción masiva de iOS](#).

Bloqueo de activación es una función de Buscar mi iPhone o iPad que está diseñada para evitar la reactivación de dispositivos perdidos o robados porque se necesita el ID de Apple y la contraseña del usuario para poder desactivar Buscar Mi iPhone, borrar los datos del dispositivo o reactivarlo y usarlo. En XenMobile, puede omitir el requisito de ID de Apple y contraseña si habilita el bloqueo de activación en la directiva de opciones de MDM. Así, cuando un usuario devuelva un dispositivo con la función Buscar Mi iPhone activada, podrá administrar el dispositivo desde la consola de XenMobile sin sus credenciales de Apple.

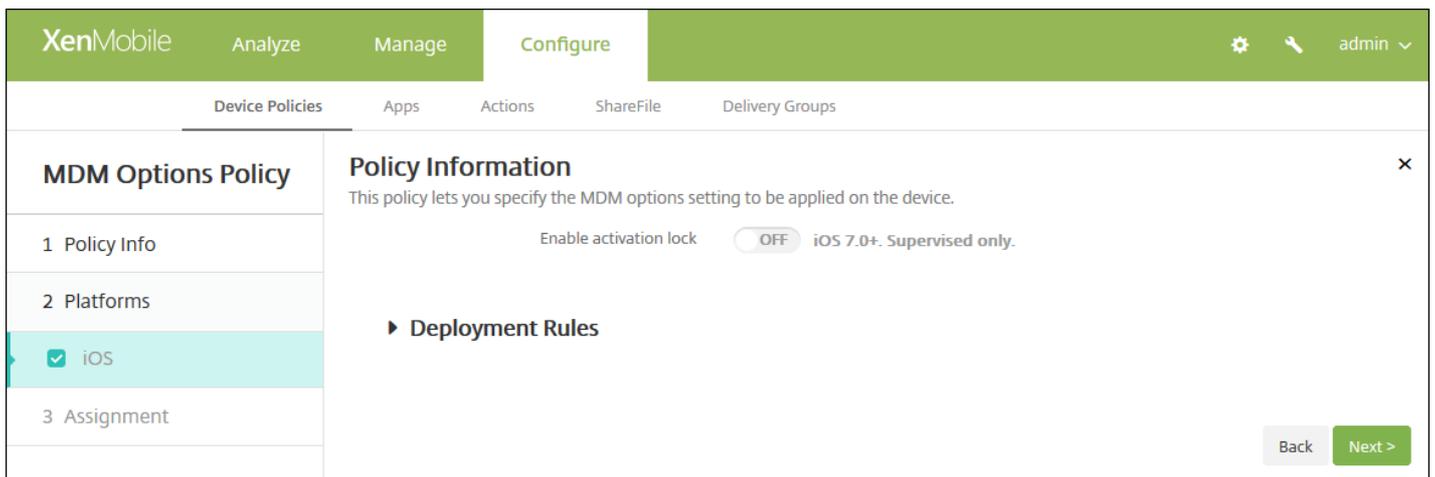
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y, en **End user**, haga clic en **MDM Options**. Aparecerá la página de información **MDM Options Policy**.

The screenshot shows the XenMobile interface for configuring an MDM Options Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies' as the selected category. The 'MDM Options Policy' configuration screen is displayed, featuring a sidebar with steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' step is expanded, showing 'iOS' selected with a checkmark. The main area contains a 'Policy Information' section with a description and two input fields for 'Policy Name\*' and 'Description'. A 'Next >' button is visible at the bottom right.

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 **Siguiente**. Aparecerá la página **iOS MDM Policy Platform**.

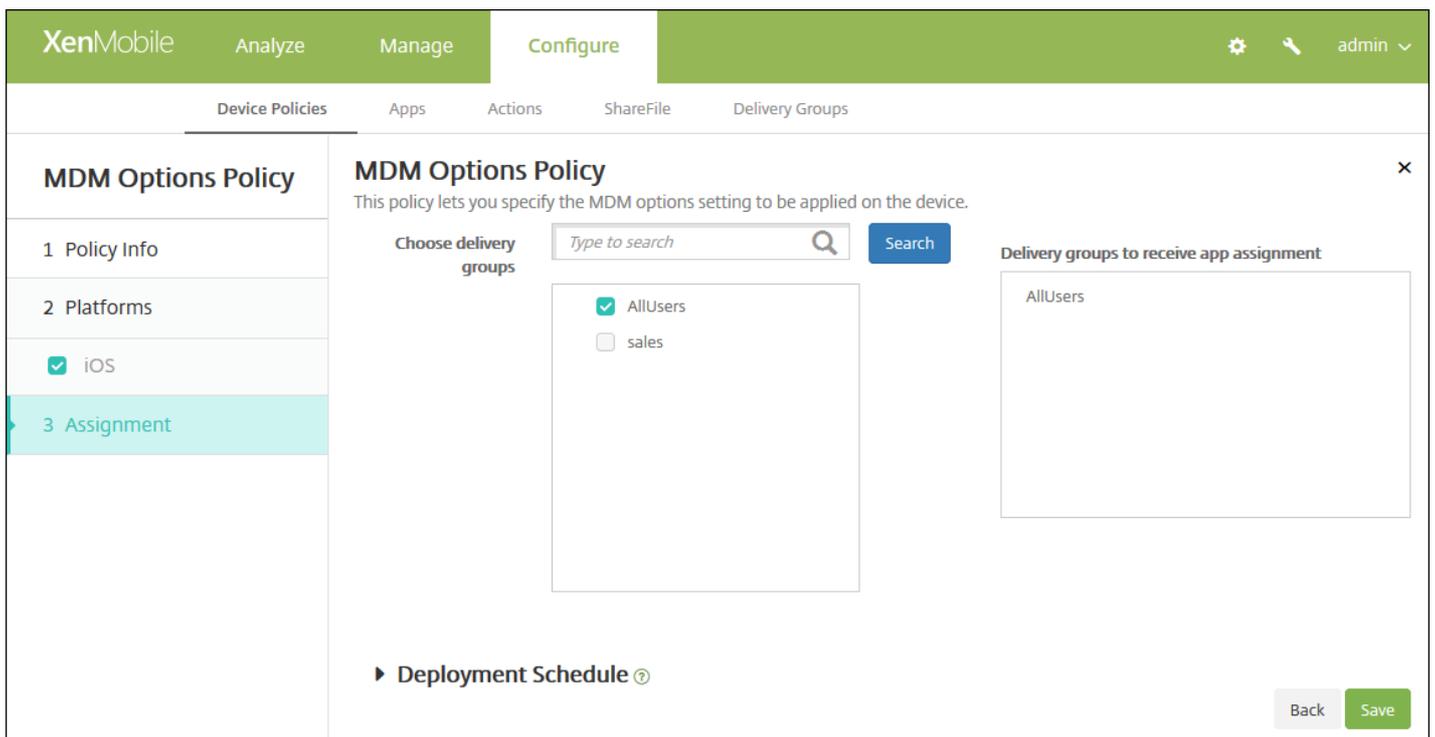


6. Configure este parámetro:

- **Enable Activation Lock.** Seleccione si quiere habilitar la función Bloqueo de activación en los dispositivos a los que se implementará esta directiva. El valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **MDM Options Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de Microsoft Exchange ActiveSync

Mar 02, 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](#)

Antes de crear esta directiva, debe conocer el nombre de host o la dirección IP del servidor Exchange.

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**:
3. Haga clic en **Exchange**. Aparecerá la página de información **Exchange Policy**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' panel contains a text box for 'Policy Name\*' and a larger text area for 'Description'. A 'Next >' button is located at the bottom right of the panel.

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

**Exchange Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Samsung SAFE
- Samsung KNOX
- Windows Phone

3 Assignment

### Policy Information

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name\*

Exchange ActiveSync host name\*

Use SSL

Domain

User

Email address

Password

Email sync interval

Identity credential (keystore or PKI credential)

Back Next >

Configure estos parámetros:

- **Exchange ActiveSync account name.** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Exchange ActiveSync host name:** Escriba la dirección del servidor de correo electrónico.
- **Use SSL.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **ON**.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `${user.domainname}` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `${user.mail}` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Email sync interval.** En la lista, seleccione la frecuencia de sincronización del correo electrónico con el servidor Exchange Server. El valor predeterminado es de **3 días**.
- **Identity credential (keystore or PKI).** En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.
- **Authorize email move between accounts.** Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta y reenviarlos y responderlos desde otra cuenta. El valor predeterminado es **OFF**.
- **Send email only from email app.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación Correo de iOS para enviar correos electrónicos. El valor predeterminado es **OFF**.
- **Disable email recent syncing.** Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes.

El valor predeterminado es **OFF**. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.

- **Enable S/MIME.** Seleccione si esta cuenta admite el cifrado y la autenticación S/MIME. El valor predeterminado es **OFF**. Si se establece en **ON**, aparecen los dos campos siguientes:
  - **Signing identity credential.** El valor predeterminado es **None**.
  - **Encryption identity credential.** El valor predeterminado es **None**.
- **Enable per message S/MIME switch.** Seleccione si permitir que los usuarios cifren cada correo electrónico saliente. El valor predeterminado es **OFF**.

## Configuración de los parámetros de Mac OS X

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and 'Policy Information'. The 'Policy Information' section includes a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' The configuration fields are: 'Exchange ActiveSync account name\*', 'User\*', 'Email address\*', 'Password', 'Internal Exchange host', 'Internal server port', 'Internal server path', 'Use SSL for internal Exchange host' (toggled ON), and 'External Exchange host'. A 'Back' button and a 'Next >' button are located at the bottom right.

Configure estos parámetros:

- **Exchange ActiveSync account name.** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **User.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `${user.mail}` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Internal Exchange host.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host interno de Exchange.
- **Internal server host.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto interno de Exchange Server.
- **Internal server path.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta

de servidor interno de Exchange.

- **Use SSL for internal Exchange host.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **ON**.
- **External Exchange host.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host externo de Exchange.
- **External server host.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto externo de Exchange Server.
- **External server path.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor externo de Exchange.
- **Use SSL for external Exchange host.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **ON**.
- **Allow Mail Drop.** Seleccione si permitir que los usuarios compartan archivos entre dos equipos Mac de forma inalámbrica (sin tener que conectarse a una red existente). El valor predeterminado es **OFF**.

## Configuración de los parámetros de Android HTC

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left lists various policies, with 'Exchange Policy' selected. The main content area is titled 'Policy Information' and contains the following fields and options:

- Configuration display name\***: A text input field.
- Server address\***: A text input field.
- User ID\***: A text input field.
- Password**: A text input field.
- Domain**: A text input field.
- Email address\***: A text input field.
- Use SSL**: A toggle switch currently set to **ON**.

Below these fields is a section for **Deployment Rules**. At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Configuration display name.** Escriba el nombre de esta directiva que aparecerá en los dispositivos de los usuarios.
- **Server address.** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **User ID.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `${user.domainname}` en este campo para buscar automáticamente los nombres de dominio de los usuarios.

- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `$(user.mail)` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Use SSL.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **ON**.

## Configuración de los parámetros de Android TouchDown

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The interface is divided into a sidebar and a main content area.

**Sidebar:** Contains a list of policies under the 'Exchange Policy' section. The 'Android TouchDown' policy is selected and highlighted in light blue. Other policies listed include iOS, Mac OS X, Android HTC, Android for Work, Samsung SAFE, Samsung KNOX, and Windows Phone. Below the list is a section for 'Assignment'.

**Main Content Area:** Titled 'Policy Information', it provides instructions: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.'

**Configuration Fields:**

- Server name or IP address\* (Text input)
- Domain (Text input)
- User ID\* (Text input)
- Password (Text input)
- Email address (Text input)
- Identity credential (keystore or PKI) (Dropdown menu, currently set to 'None')

**Policies and Apps:** This section contains two tables for configuration:

**App Setting Table:**

Name	Value	Add

**Policy Table:**

Name	Value	Add

At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Server name or IP address.** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `$(user.domainname)` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User ID.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `$(user.username)` en este campo para buscar automáticamente los nombres de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `$(user.mail)` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Identity credential (keystore or PKI).** En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.
- **App Setting.** Si quiere, puede agregar opciones de configuración de aplicaciones TouchDown a esta directiva.
- **Policy.** Si quiere, puede agregar directivas de TouchDown a esta directiva.

## Configuración de los parámetros de Android for Work

Configure estos parámetros:

- **Server name or IP address.** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `${user.domainname}` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User ID.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `${user.mail}` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Identity credential (keystore or PKI).** En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **None**.

Configuración de los parámetros de Samsung SAFE y Samsung KNOX

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Exchange Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several options are checked: iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE (highlighted), Samsung KNOX, and Windows Phone. The main area, titled 'Policy Information', contains the following fields and controls:

- Server name or IP address\***: Text input field.
- Domain**: Text input field.
- User ID\***: Text input field.
- Password**: Text input field.
- Email address\***: Text input field.
- Identity credential (keystore or PKI)**: Dropdown menu with 'None' selected.
- Use SSL connection**: Toggle switch set to ON.
- Sync contacts**: Toggle switch set to ON.
- Sync calendar**: Toggle switch set to ON.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Server name or IP address.** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `${user.domainname}` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User ID.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Password.** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `${user.mail}` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Identity credential (keystore or PKI).** En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para XenMobile. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente.
- **Use SSL connection.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **ON**.
- **Sync contacts.** Marque la casilla para habilitar la sincronización de los contactos de los usuarios entre sus dispositivos y el servidor Exchange. El valor predeterminado es **ON**.
- **Sync calendar.** Marque la casilla para habilitar la sincronización de los calendarios de los usuarios entre sus dispositivos y el servidor Exchange. El valor predeterminado es **ON**.
- **Default account.** Marque la casilla para que la cuenta de usuarios Exchange sea la predeterminada para enviar correos electrónicos desde sus dispositivos. El valor predeterminado es **ON**.

Configuración de los parámetros de Windows Phone

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Exchange Policy' section with sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several options are checked: iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, and Windows Phone. The main area is titled 'Policy Information' and contains the following fields:

- Account name or display name\***: Text input field.
- Server name or IP address\***: Text input field.
- Domain**: Text input field.
- User ID or user name\***: Text input field.
- Email address\***: Text input field.
- Use SSL connection**: Toggle switch set to OFF.
- Sync items**:
  - Past days to sync**: Dropdown menu set to All content.
- Sync scheduling**:
  - Frequency**: Dropdown menu set to When item arrives.

At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

**Nota:** Esta directiva no permite establecer la contraseña de usuario. Los usuarios deben establecer ese parámetro desde sus dispositivos después de la inserción de la directiva.

- **Account name or display name.** Escriba el nombre de la cuenta de Exchange ActiveSync.
- **Server name or IP address.** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Domain.** Escriba el dominio en el que reside el servidor Exchange. Puede utilizar la macro de sistema `${user.domainname}` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **User ID or user name.** Especifique el nombre de usuario para la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `${user.username}` en este campo para buscar automáticamente los nombres de los usuarios.
- **Email address.** Especifique la dirección de correo electrónico completa del usuario. Puede utilizar la macro de sistema `${user.mail}` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Use SSL connection.** Marque la casilla para proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **OFF**.
- **Past days to sync.** En la lista, haga clic en la cantidad de días pasados necesarios para sincronizar todo el contenido del dispositivo con el servidor Exchange. El valor predeterminado es **All content**.
- **Frequency.** En la lista, haga clic en la programación que se usará para sincronizar los datos que se envíen al dispositivo desde el servidor Exchange. El valor predeterminado es **When it arrives**.
- **Logging level.** En la lista, haga clic en **Disabled**, **Basic** o **Advanced** para especificar el nivel de detalle que se seguirá a la hora de registrar la actividad de Exchange. El valor predeterminado es **Disabled**.

7. Configure las reglas de implementación. ▼

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Exchange Policy**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and includes a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search box and a list of groups: 'AllUsers' (checked), 'DG-helen', and 'DG-ex12'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. At the bottom, there is a 'Deployment Schedule' section with a dropdown arrow. In the bottom right corner, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.



# Directiva de información de organización

Mar 02, 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**.

The screenshot shows the XenMobile interface for configuring an 'Organization Info Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Organization Info Policy' and contains a sidebar with three steps: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. The 'Policy Info' step is expanded, showing a 'Policy Information' section. This section includes a description: 'This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' (required) and 'Description'. A 'Next >' button is located at the bottom right of the form.

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 **iOS Platform Information**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Organization Info Policy

- 1 Policy Info
- 2 Platforms
- ✓ iOS
- 3 Assignment

### Policy Information

This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.

Name	<input type="text"/>	?	
			iOS 7.0+
Address	<input type="text"/>	?	
			iOS 7.0+
Phone	<input type="text"/>	?	
			iOS 7.0+
Email	<input type="text"/>	?	
			iOS 7.0+
Magic	<input type="text"/>	?	
			iOS 7.0+

▶ **Deployment Rules**

Back
Next >

Configure estos parámetros:

- **Name.** Escriba el nombre de la organización con 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 administra esa organización.

7. Configure las reglas de implementación. ▾

8. Haga clic en **Next**. Aparecerá la página de asignación **Organization Info Policy**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Organization Info Policy' and includes a description: 'This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.' There are two main sections: 'Choose delivery groups' with a search bar and a list of 'AllUsers' (checked) and 'sales' (unchecked); and 'Delivery groups to receive app assignment' with a list containing 'AllUsers'. A 'Deployment Schedule' section is partially visible at the bottom. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de códigos de acceso

Mar 02, 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](#)

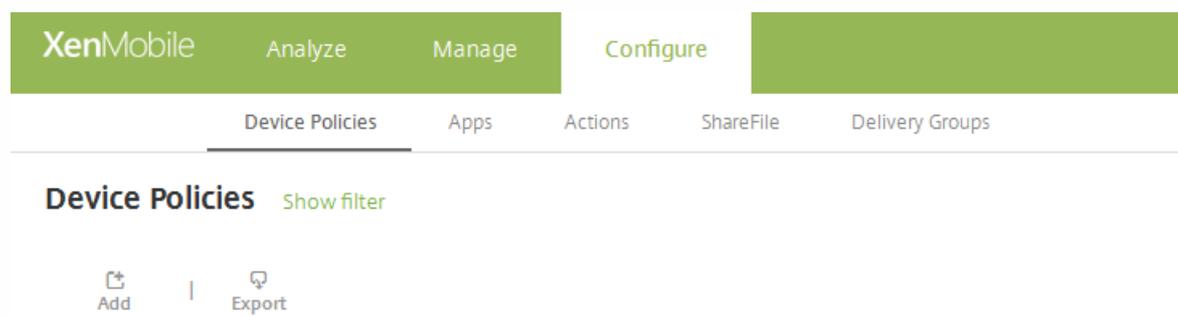
[Configuración de Samsung KNOX](#)

[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.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Passcode Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung KNOX
  - Android for Work
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

### Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Policy Name\*

Description

Next >

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.

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 introduzcan un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **None**.
  - **Lock device after (minutes of inactivity).** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (1-730).** Introduzca 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 en **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always, Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## Configuración de los parámetros de Mac OS X

The screenshot shows the XenMobile configuration interface. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' (highlighted). Below that, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The configuration options are as follows:

- Passcode required:** ON (toggle)
- Passcode requirements:**
  - Minimum length:** 6 (dropdown)
  - Allow simple passcodes:** ON (toggle)
  - Required characters:** OFF (toggle)
  - Minimum number of symbols:** 0 (dropdown)
- Passcode security:**
  - Device lock grace period (minutes of inactivity):** None (dropdown)
  - Lock device after (minutes of inactivity):** None (dropdown)
  - Passcode expiration in days (1-730):** 0 (input field)
  - Previous passwords saved (0-50):** 0 (input field)
  - Maximum failed sign-on attempts:** Not defined (dropdown)

At the bottom right, there are 'Back' and 'Next >' buttons.

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 introduzcan un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **None**.

- **Lock device after (minutes of inactivity)**. En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
- **Passcode expiration in days (1-730)**. Introduzca 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 en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

## Configuración de los parámetros de Android

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The interface is divided into a sidebar on the left and a main configuration area on the right. The sidebar includes sections for 'Policy Info', 'Platforms', and 'Assignment'. The 'Platforms' section is expanded, showing a list of operating systems with checkboxes: iOS, Mac OS X, Android (selected), Samsung KNOX, Android for Work, Windows Phone, and Windows Desktop/Tablet. The main configuration area is titled 'Passcode Policy' and contains the following settings:

- Passcode Required:** ON (toggle)
- Passcode requirements:**
  - Minimum length:** 6
  - Biometric recognition:** OFF
  - Required characters:** No restriction
  - Advanced rules:** OFF (A 3.0+)
- Passcode security:**
  - Lock device after (minutes of inactivity):** None
  - Passcode expiration in days (1-730):** 0
  - Previous passwords saved (0-50):** 0
  - Maximum failed sign-on attempts:** Not defined
- Encryption:** (partially visible)

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

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 configurar la composición de los códigos de acceso. El valor predeterminado es No restriction.
  - **Advanced rules.** Seleccione si aplicar reglas avanzadas de códigos de acceso. Esta opción está disponible para Android 3.0 y versiones posteriores. El valor predeterminado es **OFF**.
  - Si habilita **Advanced rules**, en cada una de las siguientes listas, haga clic en la cantidad mínima de cada tipo de carácter que un código de acceso debe contener:
    - **Symbols.** La cantidad mínima de símbolos.
    - **Letters.** La cantidad mínima de letras.
    - **Lowercase letters.** La cantidad mínima de minúsculas.
    - **Uppercase letters.** La cantidad mínima de mayúsculas.
    - **Numbers or symbols.** La cantidad mínima de números o símbolos.
    - **Numbers.** La cantidad mínima de números.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity).** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (1-730).** Introduzca 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 borren los datos 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 quiere 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 guardar los cambios, o bien en **Cancel** para no guardarlos.

## Configuración de los parámetros de Samsung KNOX

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The left sidebar lists various platforms, with Samsung KNOX selected. The main content area displays the following configuration options:

- Passcode requirements:**
  - Minimum length: 6
  - Allow users to make password visible: OFF
- Forbidden Strings:** A section with an "Add" button to define strings that are prohibited in passwords.
- Minimum number of:**
  - Changed characters\*: 0
  - Symbols\*: 0
- Maximum number of:**
  - Number of times a character can occur\*: 0
  - Alphabetic sequence length\*: 0
  - Numeric sequence length\*: 0
- Passcode security:** A section for additional security settings.

Navigation buttons "Back" and "Next >" are visible at the bottom right of the configuration area.

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 quiere 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 guardar los cambios, o bien en **Cancel** para no guardarlos.

- **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 (1-730).** Introduzca 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 para 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

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Delivery Groups

### Passcode Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung KNOX
  - Android for Work
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

### Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

**Passcode Required**

**Passcode requirements**

- Minimum length** 6
- Biometric recognition** OFF
- Required characters** No restriction
- Advanced rules** OFF A 3.0+

**Passcode security**

- Lock device after (minutes of inactivity)** None
- Passcode expiration in days (1-730)** 0
- Previous passwords saved (0-50)** 0
- Maximum failed sign-on attempts** Not defined

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 un código de acceso debe contener:
    - **Symbols.** La cantidad mínima de símbolos.
    - **Letters.** La cantidad mínima de letras.
    - **Lowercase letters.** La cantidad mínima de minúsculas.
    - **Uppercase letters.** La cantidad mínima de mayúsculas.
    - **Numbers or symbols.** La cantidad mínima de números o símbolos.
    - **Numbers.** La cantidad mínima de números.
- **Seguridad de códigos de acceso**
  - **Lock device after (minutes of inactivity).** En la lista, haga clic en la cantidad de minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **None**.
  - **Passcode expiration in days (1-730).** Introduzca 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

The screenshot shows the XenMobile configuration interface for the 'Passcode Policy'. The interface is divided into a sidebar on the left and a main configuration area on the right. The sidebar has three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several options are checked, including 'Windows Phone'. The main configuration area is titled 'Passcode Policy' and contains the following settings:

- Passcode required:** A toggle switch set to 'ON'.
- Allow simple passcodes:** A toggle switch set to 'OFF'.
- Passcode requirements:**
  - Minimum length:** A dropdown menu set to '6'.
  - Characters required:** A dropdown menu set to 'Letters only'.
  - Minimum number of symbols:** A dropdown menu set to '1'.
- Passcode security:**
  - Lock device after (minutes of inactivity):** A text input field set to '0'.
  - Passcode expiration in 0-730 days:** A text input field set to '0'.
  - Previous passwords saved (0-50):** A text input field set to '0', highlighted with a green circle.
  - Maximum failed sign-on attempts before wipe (0-999):** A text input field set to '0'.

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 un usuario puede 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

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The interface is divided into a sidebar on the left and a main configuration area on the right. The sidebar has three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, and Windows Desktop/Tablet. The 'Windows Desktop/Tablet' option is selected. The main configuration area is titled 'Passcode Policy' and contains the following settings:

- Disallow convenience logon:** A toggle switch set to OFF.
- Minimum passcode length:** A dropdown menu set to 6.
- Maximum passcode attempts before wipe:** A dropdown menu set to 4.
- Passcode expiration in days (0-730)\*:** A text input field set to 0.
- Passcode history (1-24)\*:** A text input field set to 0.
- Maximum inactivity before device lock in minutes (1-999):** A text input field set to 0.

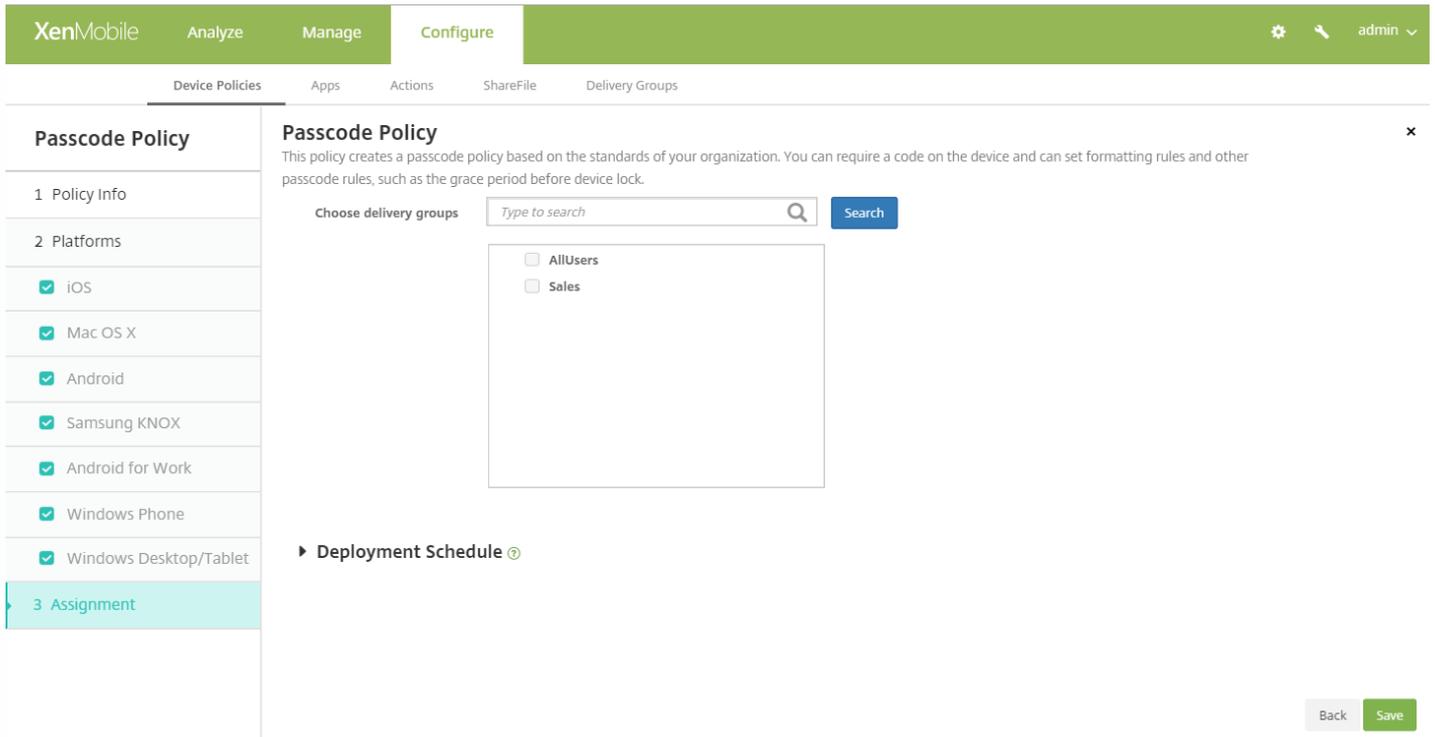
Below these settings is a section for 'Deployment Rules'. At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

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).** Introduzca 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**.



The screenshot shows the XenMobile configuration interface for a Passcode Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' There is a search bar for 'Choose delivery groups' with a search button. Below the search bar, there are two checkboxes: 'AllUsers' and 'Sales'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de hotspot personal

Mar 02, 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**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

#### Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Policy Name\*

Description

Next >

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 de información **iOS Platform**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

#### Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Disable personal hotspot  OFF iOS 7.0+

► Deployment Rules

Back Next >

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 **Siguiente**. Aparecerá la página de asignación **Personal Hotspot Policy**.

The screenshot shows the XenMobile configuration interface for the 'Personal Hotspot Policy'. The interface is divided into several sections:

- Navigation:** XenMobile, Analyze, Manage, Configure (active), admin.
- Sub-navigation:** Device Policies, Apps, Actions, ShareFile, Delivery Groups.
- Policy Info:** Personal Hotspot Policy. This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.
- Choose delivery groups:** A search bar with the placeholder 'Type to search' and a 'Search' button. Below the search bar is a list of groups:  AllUsers,  sales, and  RG.
- Delivery groups to receive app assignment:** A list containing 'AllUsers'.
- Deployment Schedule:** A section with a dropdown arrow and a help icon.
- Buttons:** 'Back' and 'Save' buttons at the bottom right.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de eliminación de perfiles

Mar 02, 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**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Profile Removal Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you remove a profile for iOS or Mac OS X from a device.' There are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). On the left, a sidebar shows three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. At the bottom right of the main content area, there is a green button labeled 'Next >'.

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 **Siguiente**. 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

**Profile Removal Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X

3 Assignment

**Policy Information**

This policy lets you remove a profile for iOS or Mac OS X from a device.

Profile ID\*  ▼

Comment

► **Deployment Rules**

Back Next >

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

**Profile Removal Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X

3 Assignment

**Policy Information**

This policy lets you remove a profile for iOS or Mac OS X from a device.

Profile ID\*  ▼

Deployment scope  ▼ OS X 10.7+

Comment

► **Deployment Rules**

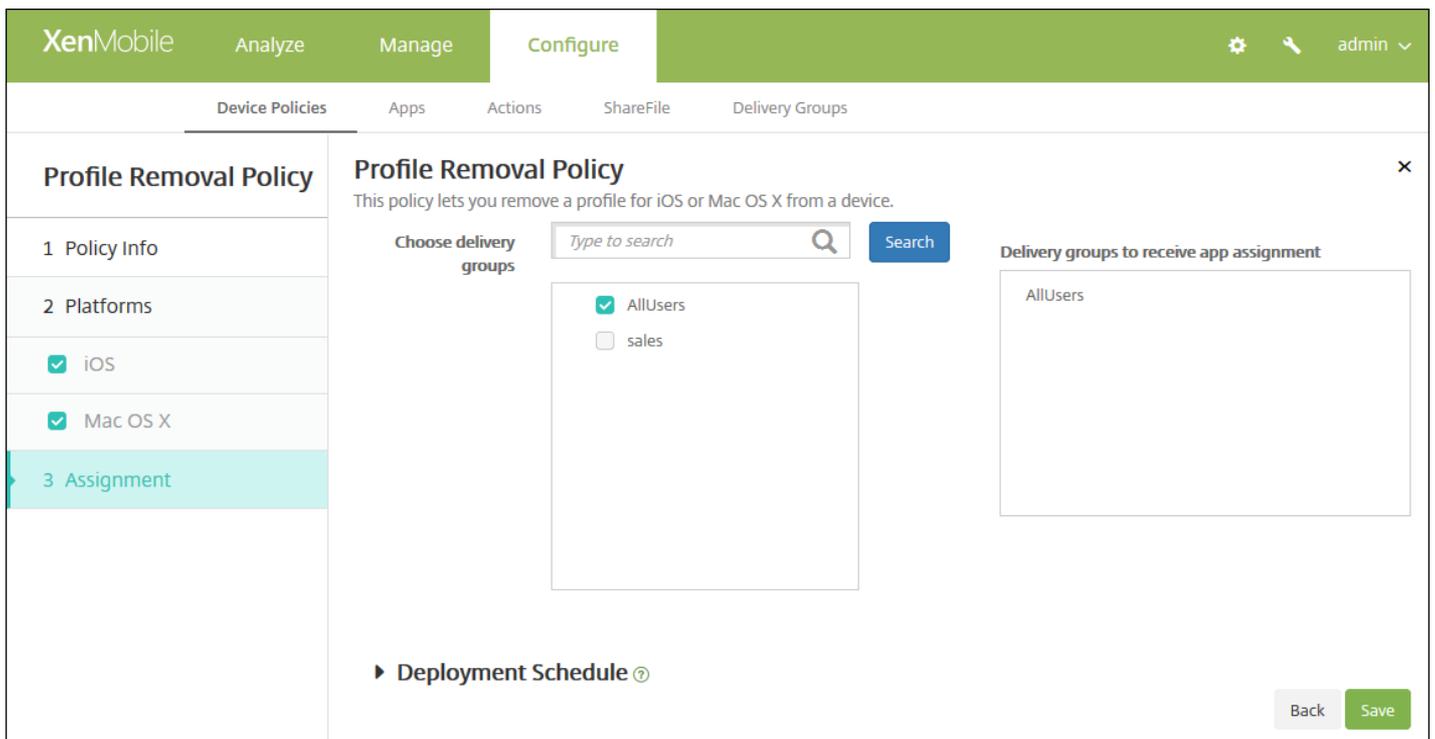
Back Next >

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 **Siguiente**. Aparecerá la página de asignación **Profile Removal Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de perfiles de aprovisionamiento

Mar 02, 2017

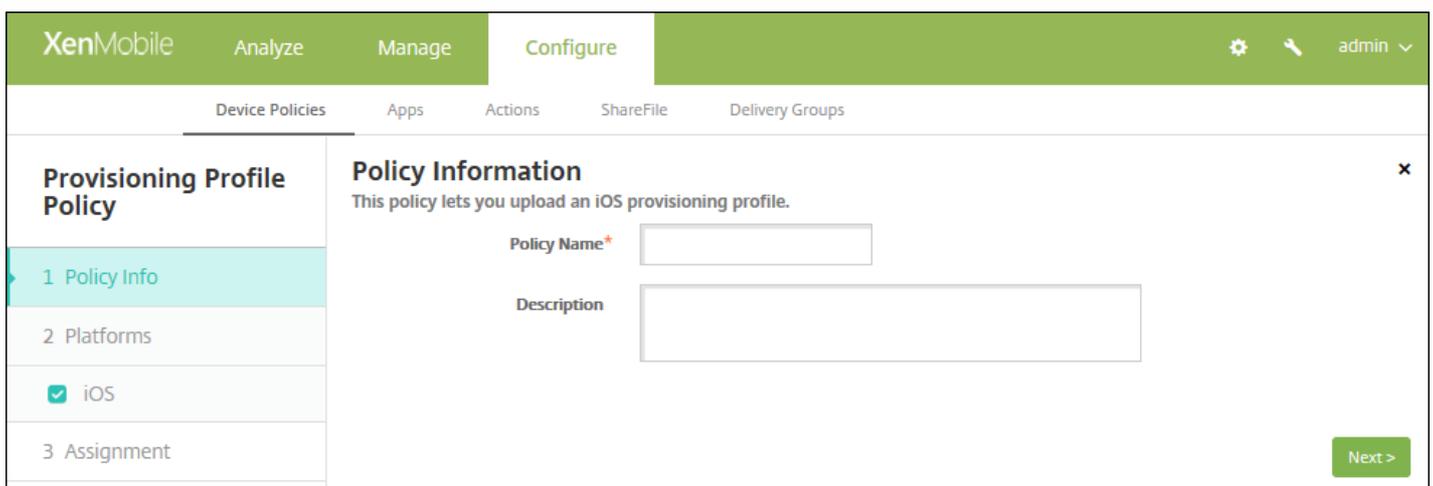
Por regla general, cuando se desarrolla y se firma con código una aplicación empresarial iOS, se incluye un perfil de aprovisionamiento de distribución empresarial, que requiere Apple para que la aplicación funcione en dispositivos iOS. Si falta o ha caducado un perfil de aprovisionamiento, la aplicación 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 faltan 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 luego, en **Apps**, haga clic en **Provisioning Profile**. Aparecerá la página de información **Provisioning Profile Policy**.

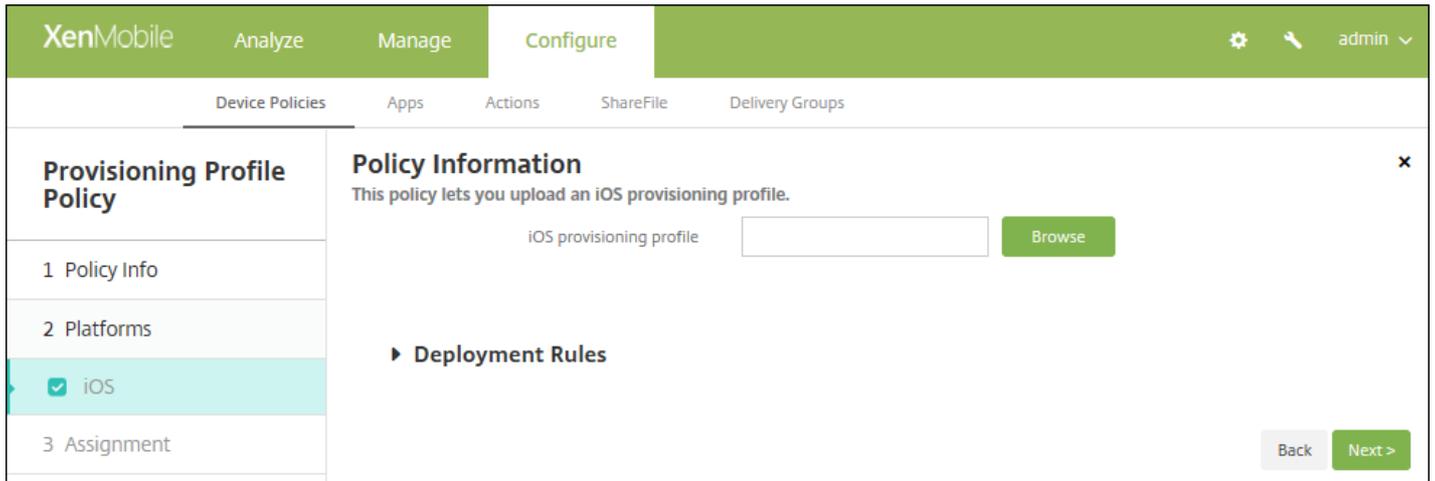


The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Provisioning Profile Policy' page is displayed, featuring a sidebar with '1 Policy Info', '2 Platforms', '3 Assignment', and a checked 'iOS' option. The main content area is titled 'Policy Information' and contains a description and two input fields for 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de información **iOS Platform**.

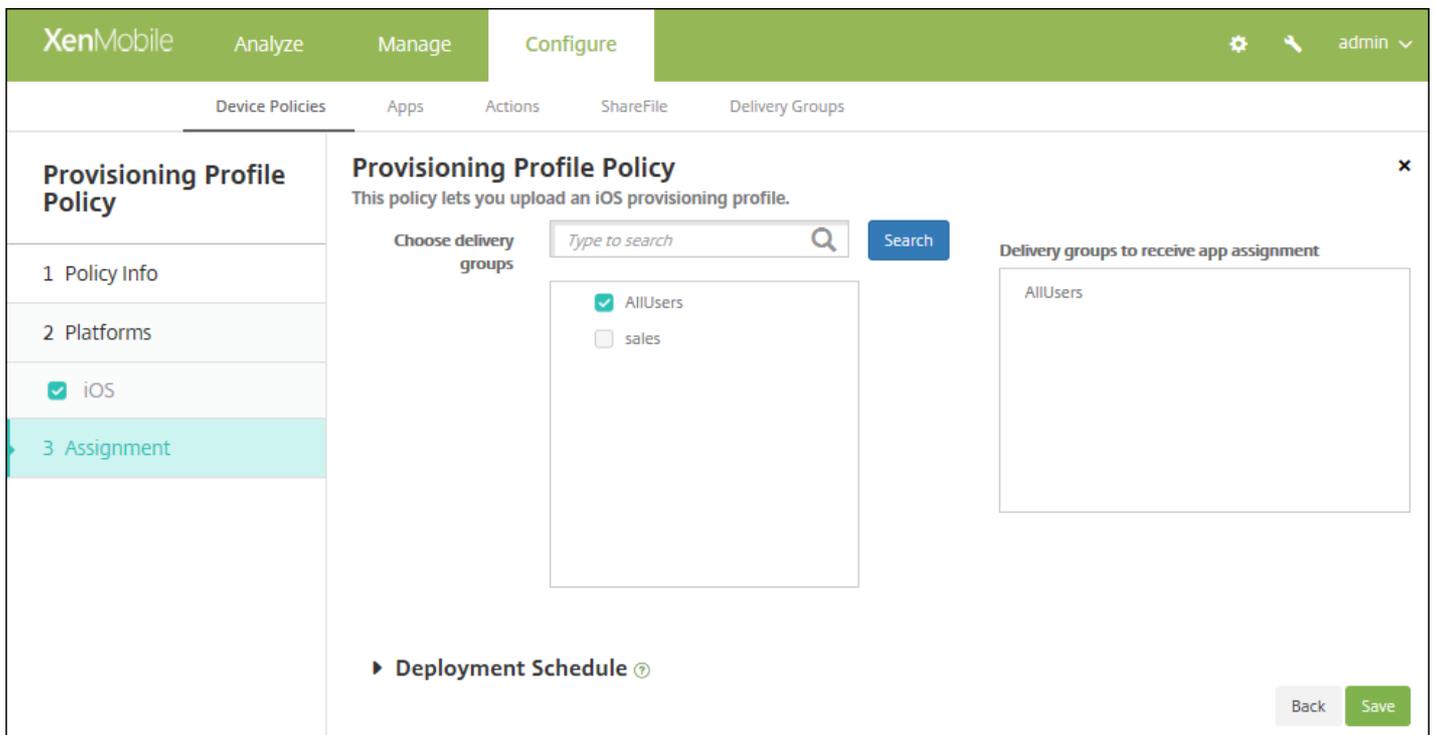


6. Configure este parámetro:

- **iOS provisioning profile**. Seleccione el archivo de perfil de aprovisionamiento que quiere importar. Para ello, haga clic en **Browse** y vaya a la ubicación del 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 lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de eliminación de perfiles de aprovisionamiento

Mar 02, 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](#).

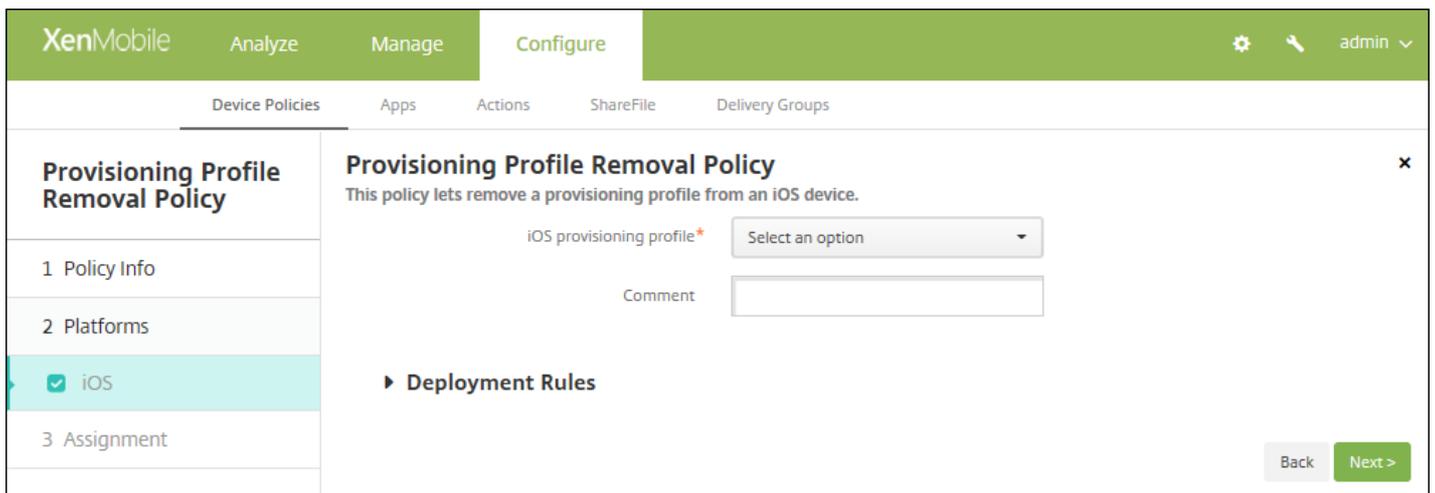
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá la página **Add a New Policy**.
3. Expanda **More** y, a continuación, en **Removal**, haga clic en **Provisioning Profile Removal**. Aparecerá la página de información **Provisioning Profile Removal Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Removal Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets remove a provisioning profile from an iOS device.' There are two input fields: 'Policy Name\*' and 'Description'. A sidebar on the left shows the navigation menu with '1 Policy Info' selected, '2 Platforms', and '3 Assignment'. A 'Next >' button is visible in the bottom right corner.

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 de la plataforma **iOS**.

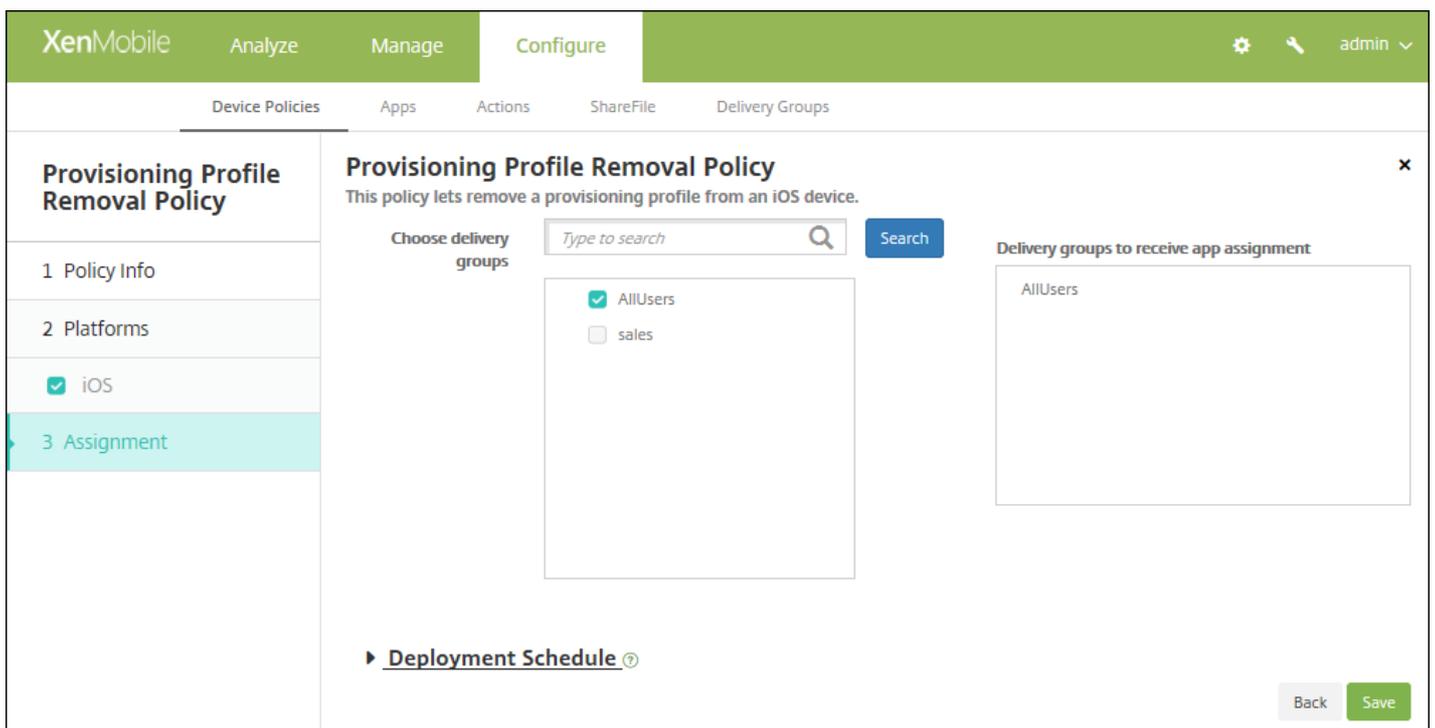


6. Configure los siguientes parámetros:

- **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 **Siguiente**. Aparecerá la página de asignación **Provisioning Profile Removal Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de proxy

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Proxy Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. In the '2 Platforms' section, 'iOS' and 'Windows Mobile/CE' are both checked. The 'Policy Information' section contains a text box for 'Policy Name\*' and a larger text box for 'Description'. A 'Next >' button is located in the bottom right corner.

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 **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS

**Proxy Policy**

1 Policy Info

2 Platforms

iOS

Windows Mobile/CE

3 Assignment

**Policy Information**

This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. For iOS, the policy is available for iOS 6. You must also set the iOS device into supervised mode.

Proxy configuration: Manual

Host name or IP address for the proxy server \*

Port for the proxy server \*

User name

Password

Allow bypassing proxy to access captive networks: OFF

Policy Settings

Remove policy:  Select date,  Duration until removal (in days)

Allow user to remove policy: Always

► Deployment Rules

Back Next >

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 o la dirección IP de host del servidor proxy. Este campo es obligatorio.
    - **Port for the proxy server.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
    - **User name.** Si quiere, escriba un nombre de usuario para 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 en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## Configuración de los parámetros de Windows Mobile/CE

The screenshot shows the XenMobile interface for configuring a Proxy Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Proxy Policy' and contains a sidebar with sections: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Windows Mobile/CE' checked), and '3 Assignment'. The main panel, 'Policy Information', explains that the policy configures a single or global HTTP proxy for all apps. It includes the following fields: 'Network' (set to 'Built-in office'), 'Network' (set to 'HTTP'), 'Host name or IP address for the proxy server' (empty), 'Port for the proxy server' (set to '80'), 'User name' (empty), 'Password' (empty), and 'Domain name' (empty). An 'Enable' toggle is set to 'ON'. A 'Deployment Rules' section is partially visible at the bottom. 'Back' and 'Next >' buttons are located at the bottom right.

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:
  - User-defined office
  - Internet definido por el usuario
  - Built-in office
  - Built-in Internet
- **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 o la dirección IP de host del servidor proxy. Este campo es obligatorio.
- **Port for the proxy server.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio. 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 **Siguiente**. Aparecerá la página de asignación **Proxy Policy**.

The screenshot shows the XenMobile Configure interface for a Proxy Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Proxy Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment' (highlighted). The main content area has a 'Choose delivery groups' section with a search box and a 'Search' button. Below this, there are two columns of delivery groups: 'AllUsers' (checked) and 'sales' (unchecked). To the right, there is a 'Delivery groups to receive app assignment' section with 'AllUsers' listed. At the bottom, there is a 'Deployment Schedule' section with a 'Back' button and a 'Save' button.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for Always on connection**, que no se aplica para iOS.

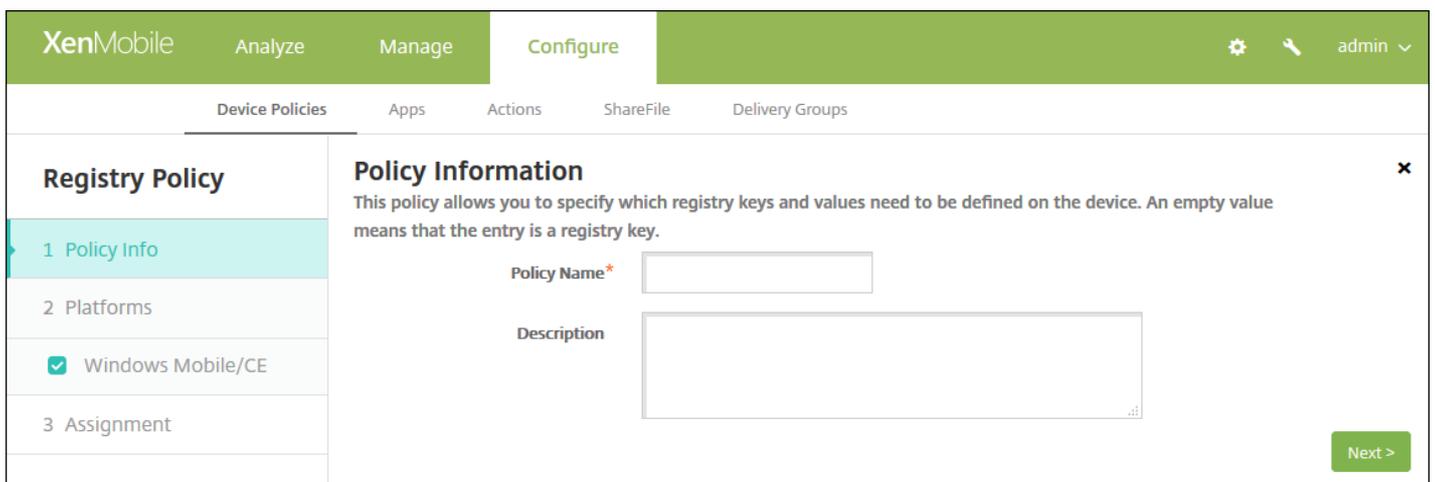
11. Haga clic en **Save**.

# Directiva del Registro

Mar 02, 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**.

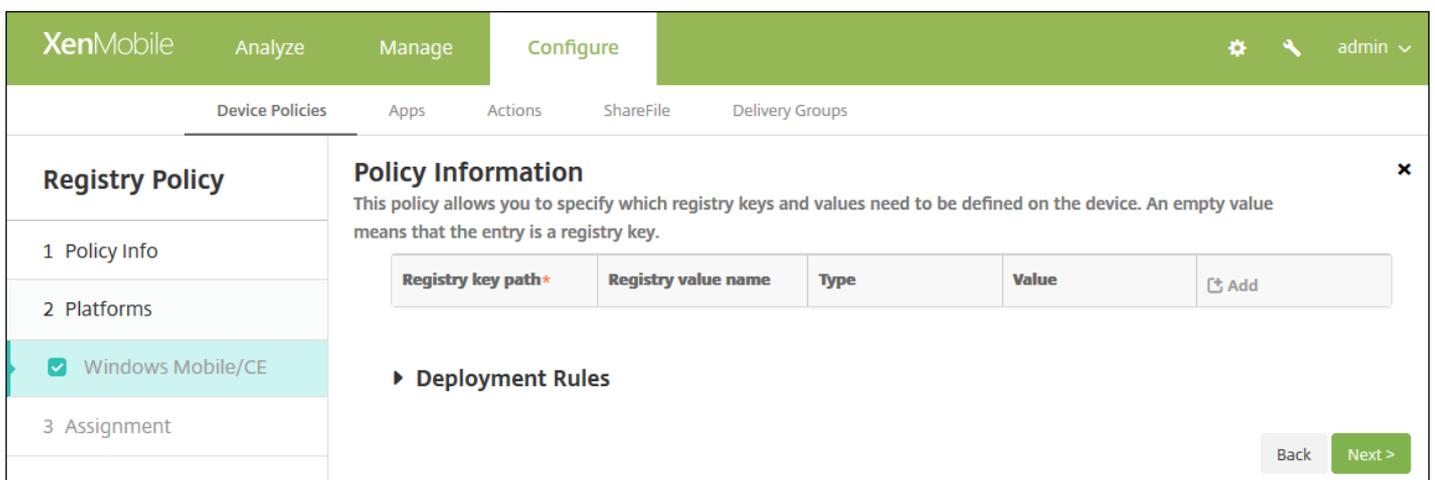


The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', the 'Registry Policy' section is active. The left sidebar shows '1 Policy Info' selected. The main area is titled 'Policy Information' and contains the following text: 'This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.' Below this text are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). A 'Next >' button is located at the bottom right of the form.

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 **Siguiente**. Aparecerá la página de información acerca de la plataforma **Windows Mobile/CE**.



The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', the 'Registry Policy' section is active. The left sidebar shows '2 Platforms' selected, and 'Windows Mobile/CE' is checked. The main area is titled 'Policy Information' and contains the following text: 'This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.' Below this text is a table with the following columns: 'Registry key path\*', 'Registry value name', 'Type', and 'Value'. There is an 'Add' button with a plus icon to the right of the table. Below the table is a section titled 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

6. Configure los siguientes parámetros:

- Para cada clave de Registro o par clave de Registro/valor 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 del 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.

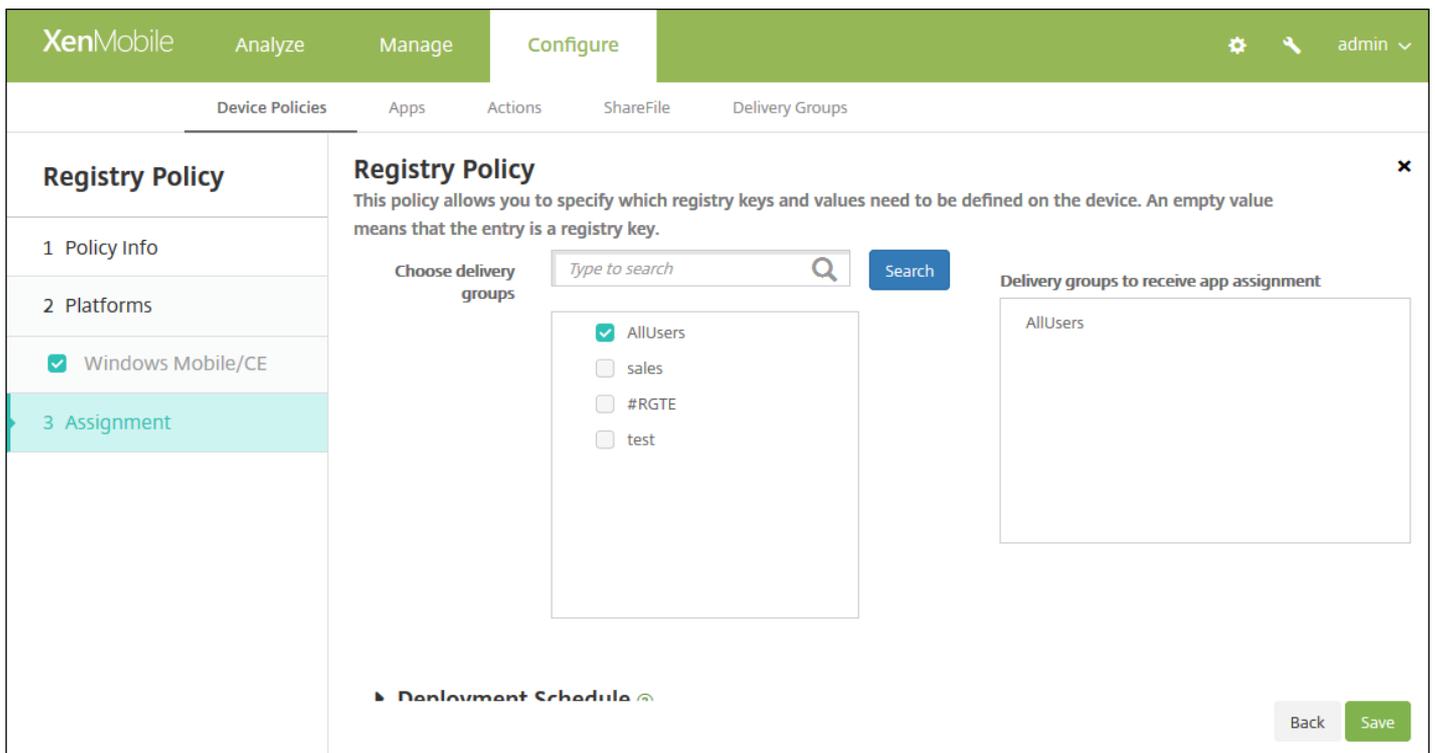
**Nota:** Para eliminar una clave de Registro existente, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en el icono de papelera situado en el lado derecho. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar una clave 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 guardar los cambios, o bien en **Cancel** para no guardarlos.

## 7. Configure las reglas de implementación.



8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Registry Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de asistencia remota

Mar 02, 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 técnica y el usuario, configurar parámetros y establecer una sesión de chat entre el usuario y el departamento de asistencia técnica.

Nota: Para implementar esta directiva, debe realizar lo siguiente:

- Instalar la aplicación XenMobile Remote Support en su entorno.
- Configurar un túnel de aplicaciones para asistencia remota. Para obtener 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**.

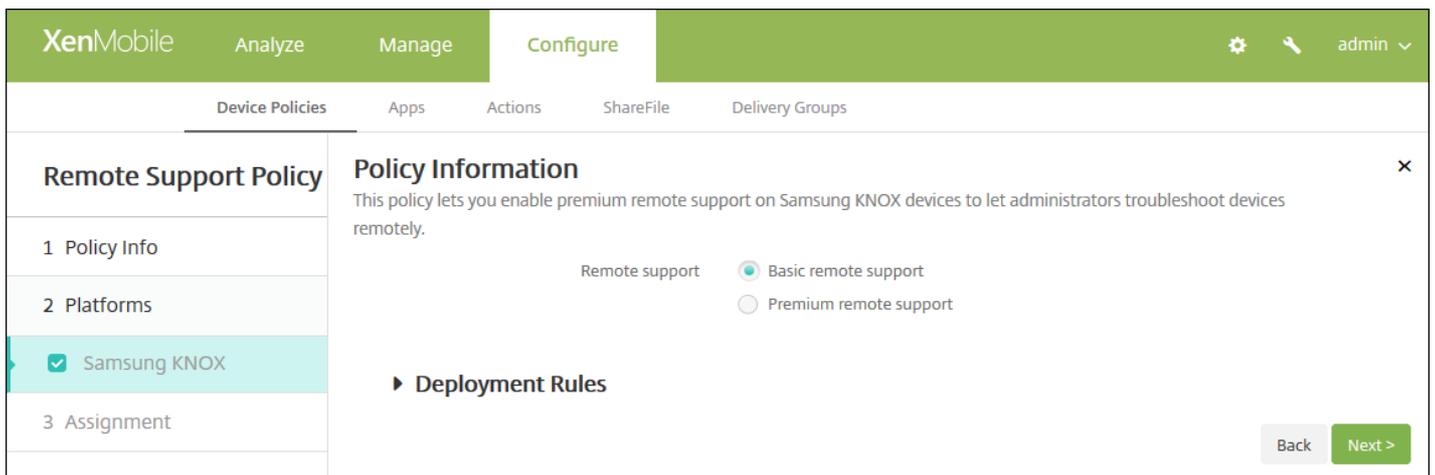
3. Expanda **More** y, en **Network access**, haga clic en **Remote Support**. Aparecerá la página **Remote Support Policy**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar with three items: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. The main content area is titled 'Remote Support Policy' and 'Policy Information'. It contains a description: 'This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.' Below the description, there are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located in the bottom right corner of the form.

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 de información acerca de la plataforma **Samsung KNOX**.

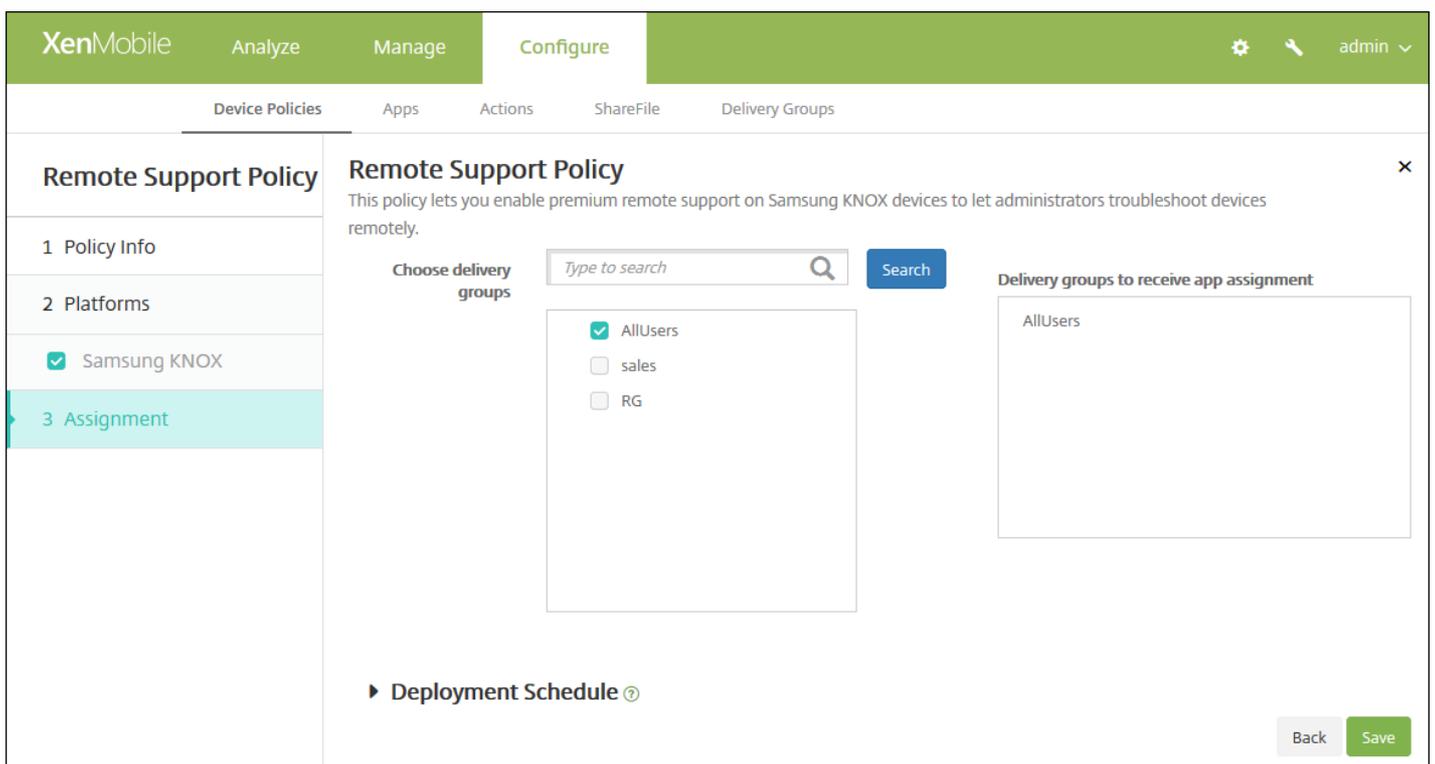


6. Configure este parámetro:

- **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 **Siguiente**. Aparecerá la página de asignación **Remote Support Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de restricciones

Mar 02, 2017

En XenMobile, puede agregar una directiva de dispositivos para restringir algunas funciones en los teléfonos, las tabletas y los dispositivos de los usuarios, entre otros. Puede configurar la directiva de restricciones para las plataformas siguientes: iOS, Mac OS X, Samsung SAFE, Samsung KNOX, tabletas Windows, Windows Phone, Amazon, Windows Mobile y Windows CE. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

Esta directiva permite o prohíbe a los usuarios utilizar funciones determinadas, como la cámara, en sus dispositivos. También puede estipular restricciones de seguridad, de contenido multimedia y de tipos de aplicaciones que los usuarios puedan o no puedan instalar. El valor predeterminado de la mayoría de las opciones de restricción es **ON**, o *allows*. Las excepciones principales son la función "Security - Force" de iOS y todas las funciones de tabletas Windows, que tienen el valor predeterminado **OFF** o *restricts*.

**Sugerencia:** Si selecciona **ON** para 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**.

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

## Restrictions Policy

### 1 Policy Info

### 2 Platforms

- iOS
- Mac OS X
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Desktop/Tablet
- Amazon
- Windows Mobile/CE

### 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

5. En **Platforms**, seleccione la plataforma o las plataformas que quiera 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 seleccionó:**

[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:

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Camera  ON
- FaceTime
- Screen shots  ON
- Photo streams  ON iOS 5.0+
- Shared photo streams  ON iOS 6.0+
- Voice dialing  ON
- Siri  ON
  - Allow while device is locked
  - Siri profanity filter
- Installing apps  ON

Back **Next >**

[Configuración de iOS](#) ▾

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X**
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Preferences**

- Restrict items in System Preferences  OFF

**Apps**

- Allow use of Game Center  ON OS X 10.11+
- Allow adding Game Center friends  ON
- Allow multiplayer gaming  ON
- Allow Game Center account modification  ON
- Allow App Store adoption  ON
- Allow Safari AutoFill  ON
- Require admin password to install or update apps  OFF

Back Next >

[Configuración de Mac OS X](#) ▾

Configuración de los parámetros de Samsung SAFE

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Enable ODE Trusted Boot Verification
- Allow Development Mode
- Allow Emergency Calls Only
- Allow Firmware Recovery
- Allow Fast Encryption
- Common Criteria Mode
- Factory reset
- Date Time Change
- DOD boot banner
- Settings changes
- Backup
- Over The Air Upgrade  ⓘ
- Background data
- Camera

Back Next >

Configuración de Samsung SAFE ▼

Configuración de los parámetros de Samsung KNOX

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX**
  - Windows Phone
  - Windows Desktop/Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

**Allow use of camera**

**Enable Revocation Check**

**Move Apps To Container**

**Enforce Multifactor Authentication**

**Enable TIMA Key store**

**Enforce Auth For Container**

**Share List**

**Enable Audit Log**

**Use Secure Keypad**

**Enable Google Apps**

**Authentication Smart Card Browser**

► **Deployment Rules**

Back Next >

## Configuración de Samsung KNOX

### Configuración de los parámetros de Windows Phone

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**WiFi Settings**

- Allow WiFi
- Allow Internet sharing
- Allow auto-connect to WiFi Sense hotspots
- Allow hotspot reporting
- Allow manual configuration

**Connectivity**

- Allow NFC
- Allow bluetooth
- Allow VPN over cellular
- Allow VPN over cellular while roaming

Back Next >

Configuración de Windows Phone ▾

Configuración de los parámetros de escritorios o tabletas Windows

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet**
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Network**

Roaming data  OFF

**Security**

User account control  ▾

Enable Windows error reporting  OFF

Enable smart screen  OFF

**Other**

Enterprise client sync product's URL enable  OFF

Enterprise client sync product's URL

▶ **Deployment Rules**

[Configuración de escritorios y tabletas Windows](#) ▾

Configuración de los parámetros de Amazon

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Factory reset
- Profiles

**Allow apps**

- Non-Amazon Appstore apps
- Social networks

**Network**

- Bluetooth
- WiFi switch
- WiFi settings
- Cellular data

Back Next >

[Configuración de Amazon](#) ▾

Configuración de los parámetros de Windows Mobile/CE

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- Bluetooth/infrared beaming (Obex)  ON
- Camera  ON
- WiFi switch  ON
- Bluetooth  ON

▶ **Deployment Rules**

Back Next >

Configuración de Windows Mobile/CE ▾

7. Configure las reglas de implementación. ▾

8. Haga clic en **Next** y aparecerá la página de asignación **Restrictions Policy**.

The screenshot shows the XenMobile configuration interface for a Restrictions Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left has a 'Restrictions Policy' section with three sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '3 Assignment' item is highlighted. The main content area is titled 'Restrictions Policy' and contains a description: 'This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.' Below the description is a 'Choose delivery groups' section with a search bar and a 'Search' button. The search results show two options: 'AllUsers' (checked) and 'Device Enrollment Program Package' (unchecked). To the right of this section is a 'Delivery groups to receive app assignment' section, which is currently empty. Below the search results is a 'Deployment Schedule' section with a right-pointing arrow and a help icon. At the bottom right of the main content area are 'Back' and 'Save' buttons.

9. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

10. Haga clic en **Save** para guardar la directiva.

# Directivas de roaming

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Roaming Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. In the '2 Platforms' section, both 'iOS' and 'Windows Mobile/CE' are checked. The 'Policy Information' section contains a text input field for 'Policy Name\*' and a larger text area for 'Description'. A 'Next >' button is located at the bottom right of the main area.

4. En el panel **Policy Information**, escriba la información siguiente:

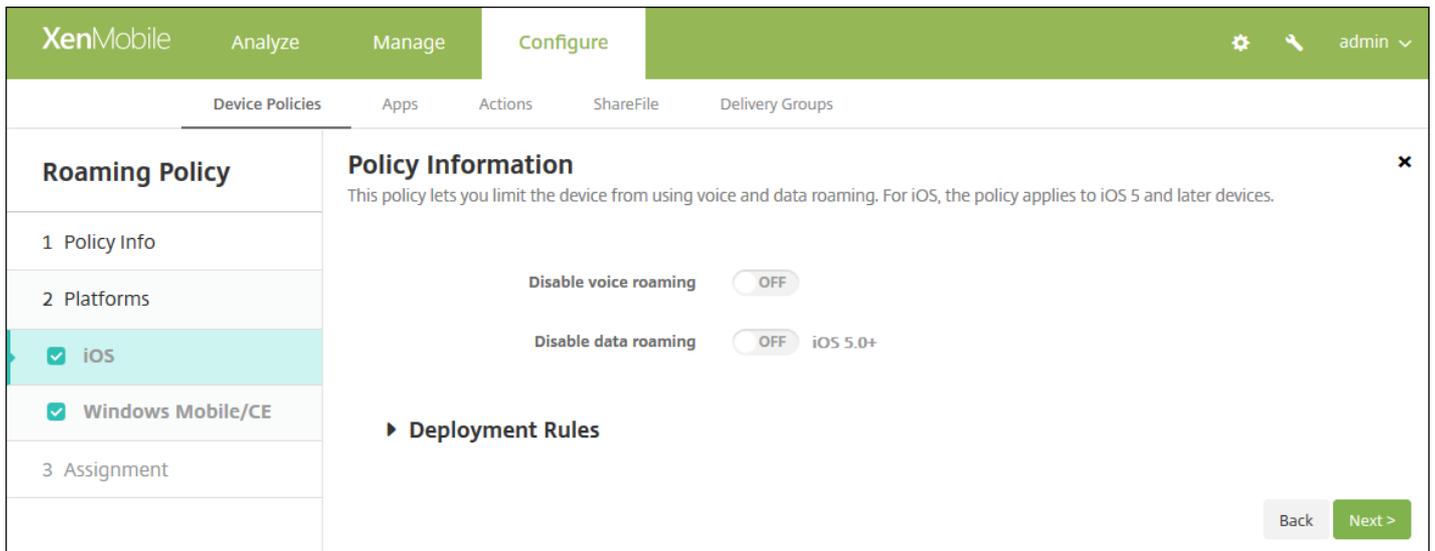
- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Si quiere, escriba una descripción de la directiva.

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.

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.

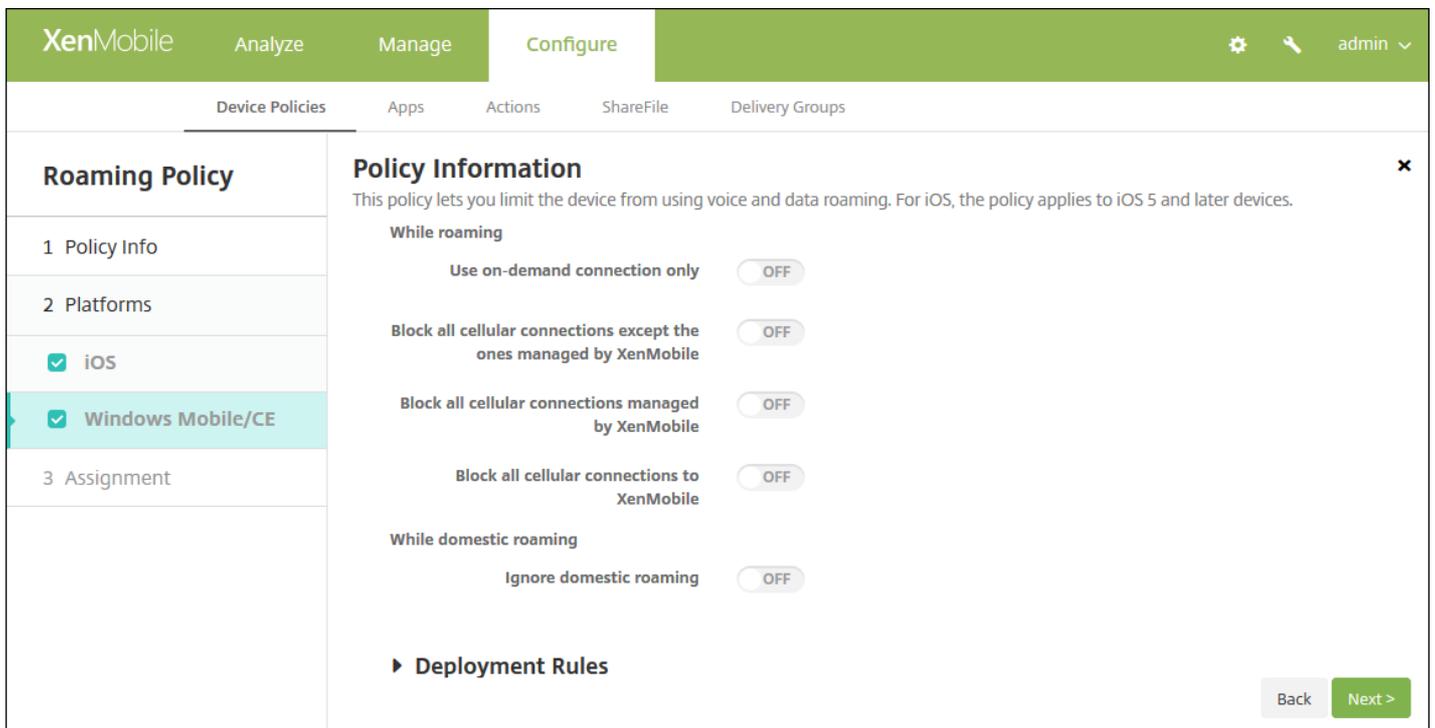
Configuración de los parámetros de iOS



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 otro 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 **Siguiente**. Aparecerá la página de asignación **Roaming Policy**.

The screenshot shows the XenMobile configuration interface for the 'Roaming Policy'. The interface is divided into several sections:

- Navigation:** Top bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. A user profile 'admin' is visible in the top right.
- Policy Overview:** A sidebar on the left lists 'Roaming Policy' with sub-items: '1 Policy Info', '2 Platforms', '3 Assignment' (highlighted), and 'Deployment Schedule'.
- Policy Description:** The main content area shows the title 'Roaming Policy' and a description: 'This policy lets you limit the device from using voice and data roaming. For iOS, the policy applies to iOS 5 and later devices.'
- Choose delivery groups:** A section with a search bar 'Type to search' and a 'Search' button. Below it, a list of delivery groups is shown: 'AllUsers' (checked) and 'sales' (unchecked).
- Delivery groups to receive app assignment:** A list box containing 'AllUsers'.
- Deployment Schedule:** A section with a right-pointing arrow and a help icon.
- Buttons:** 'Back' and 'Save' buttons are located at the bottom right of the main content area.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción

predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.

- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for Always on connection**, que no se aplica para iOS.

11. Haga clic en **Save**.

# Directivas de claves de licencia para la administración de dispositivos móviles Samsung

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Samsung MDM License Key Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you generate a Samsung ELM license key.' and two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). A 'Next >' button is located at the bottom right of the form.

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 **Siguiente**. 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

The screenshot shows the XenMobile interface for configuring a Samsung MDM License Key Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The left sidebar shows a list of steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE' and 'Samsung KNOX' are both checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you generate a Samsung ELM license key.' Below this is a field for 'ELM license key\*' with the value '\${elm.license.key}'. There is also a section for 'Deployment Rules' which is currently collapsed. At the bottom right, there are 'Back' and 'Next >' buttons.

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

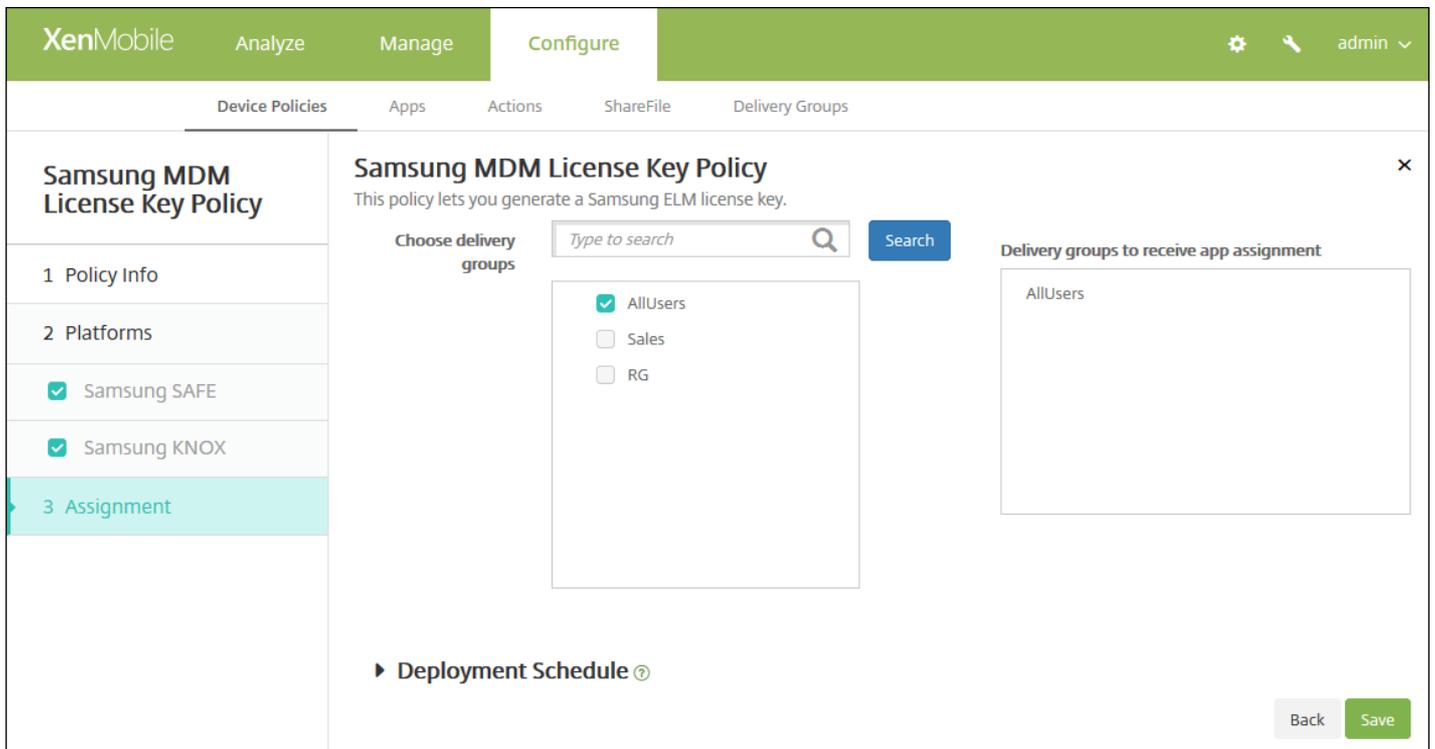
The screenshot shows the XenMobile interface for configuring a Samsung MDM License Key Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The left sidebar shows a list of steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE' and 'Samsung KNOX' are both checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you generate a Samsung ELM license key.' Below this is a field for 'KNOX license key\*' which is currently empty. There is also a section for 'Deployment Rules' which is currently collapsed. At the bottom right, there are 'Back' and 'Next >' buttons.

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 **Samsung MDM License Key Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

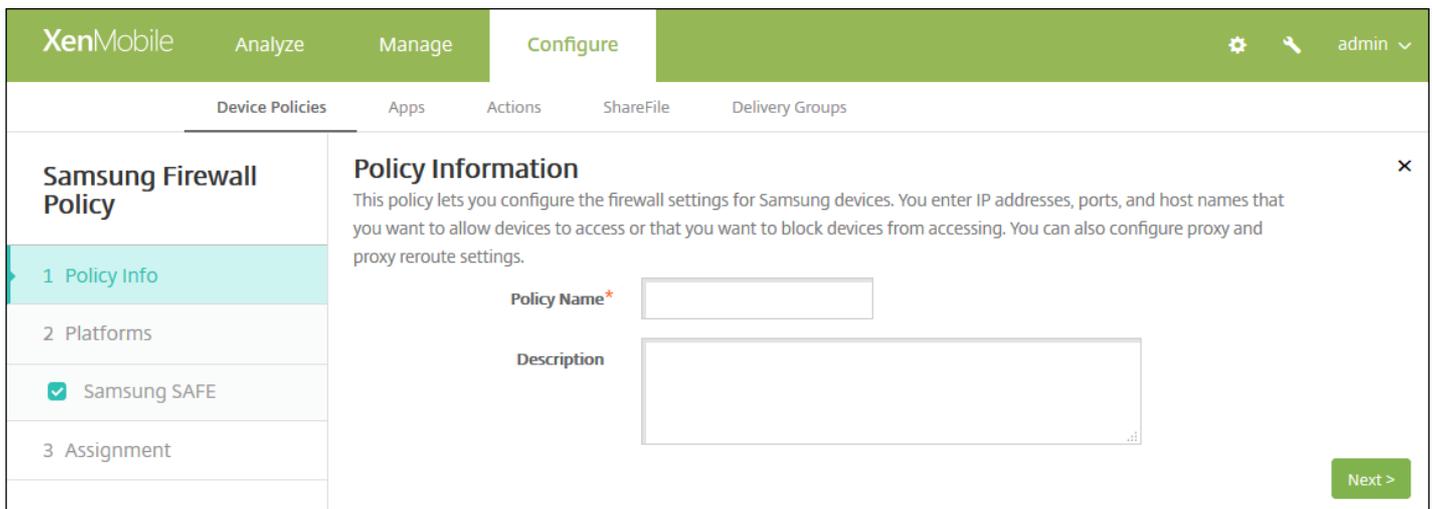
11. Haga clic en **Save**.

# Directiva de firewalls para dispositivos Samsung SAFE

Mar 02, 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**.



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing a sub-menu with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' section is expanded, showing a list of policies. The 'Samsung Firewall Policy' is selected, and the 'Policy Information' dialog is open. The dialog contains a description: 'This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure proxy and proxy reroute settings.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the dialog.

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 de información acerca de la plataforma **Samsung SAFE**.

6. Configure los siguientes parámetros:

- **Allow/Deny 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**.

- **Reroute configuration**

- 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 guardarlos o en **Cancel** para no guardarlos.

- **Proxy Configuration**

- **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 **Siguiente**. Aparecerá la página de asignación **Samsung Firewall Policy**.

The screenshot shows the XenMobile configuration interface for the Samsung Firewall Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Samsung Firewall Policy' and includes a description: 'This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure proxy and proxy reroute settings.' The interface is divided into several sections: '1 Policy Info', '2 Platforms', '3 Assignment' (highlighted), and 'Deployment Schedule'. The 'Assignment' section is further divided into 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar with the placeholder 'Type to search' and a 'Search' button. Below the search bar is a list of delivery groups: 'AllUsers' (checked), 'sales', and 'RG'. The 'Delivery groups to receive app assignment' section shows a list containing 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas SCEP de dispositivos

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SCEP Policy' and is divided into two sections. On the left, there is a sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section on the right contains a description: 'This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.' Below the description are two input fields: 'Policy Name \*' and 'Description'.

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 **Siguiente**. 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

The screenshot shows the XenMobile configuration interface for a SCEP Policy. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' is selected. The main area is titled 'Policy Information' and contains the following fields and settings:

- URL base\* (text input)
- Instance name\* (text input)
- Subject X.500 name (RFC 2253) (text input)
- Subject alternative names type (dropdown menu, set to 'None')
- Maximum retries (text input, set to '3')
- Retry delay (text input, set to '10')
- Challenge password (text input)
- Key size (bits) (dropdown menu, set to '1024')
- Use as digital signature (toggle switch, set to 'OFF')
- Use for key encipherment (toggle switch, set to 'OFF')
- SHA1/MD5 fingerprint (hexadecimal string) (text input)
- Policy Settings:
  - Remove policy (radio buttons, 'Select date' is selected)
  - Duration until removal (in days) (text input)
  - Allow user to remove policy (dropdown menu, set to 'Always')
- Deployment Rules (expandable section)

At the bottom right, there are 'Back' and 'Next >' buttons.

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 el número 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 SHA-1. 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**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### SCEP Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
  - Windows Phone
  - Windows Tablet
- Assignment

#### Policy Information

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

URL base\*

Instance name\*

Subject X.500 name (RFC 2253)

Subject alternative names type

Maximum retries

Retry delay

Challenge password

Key size (bits)

Use as digital signature

Use for key encipherment

SHA1/MD5 fingerprint (hexadecimal string)

Certificate expiration notification threshold

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

Profile scope  OS X 10.7+

► Deployment Rules

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 el número 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**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

## 7. Configure las reglas de implementación.



8. Haga clic en **Next**. Aparecerá la página de asignación **SCEP Policy**.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.

- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directiva de clave de sideloading

Mar 02, 2017

En XenMobile, la instalación de aplicaciones mediante "sideloading" permite implementar en dispositivos Windows 8.1 aplicaciones no adquiridas en la Tienda Windows. Por regla general, se realiza una instalación sideloading de aquellas aplicaciones que se desarrollan para uso corporativo y que no están pensadas para hacerse públicas en la Tienda Windows. Para realizar una instalación sideloading de las aplicaciones, configure la clave de sideloading y las activaciones de la clave. A continuación, puede implementar esas aplicaciones en los dispositivos de los usuarios.

Para crear esta directiva, necesita la siguiente información:

- La clave de producto de sideloading, que obtiene al iniciar sesión en el [Centro de servicios de licencias por volumen de Microsoft](#)
- La activación de la clave, que se crea mediante la línea de comandos después de obtener la clave del producto de sideloading.

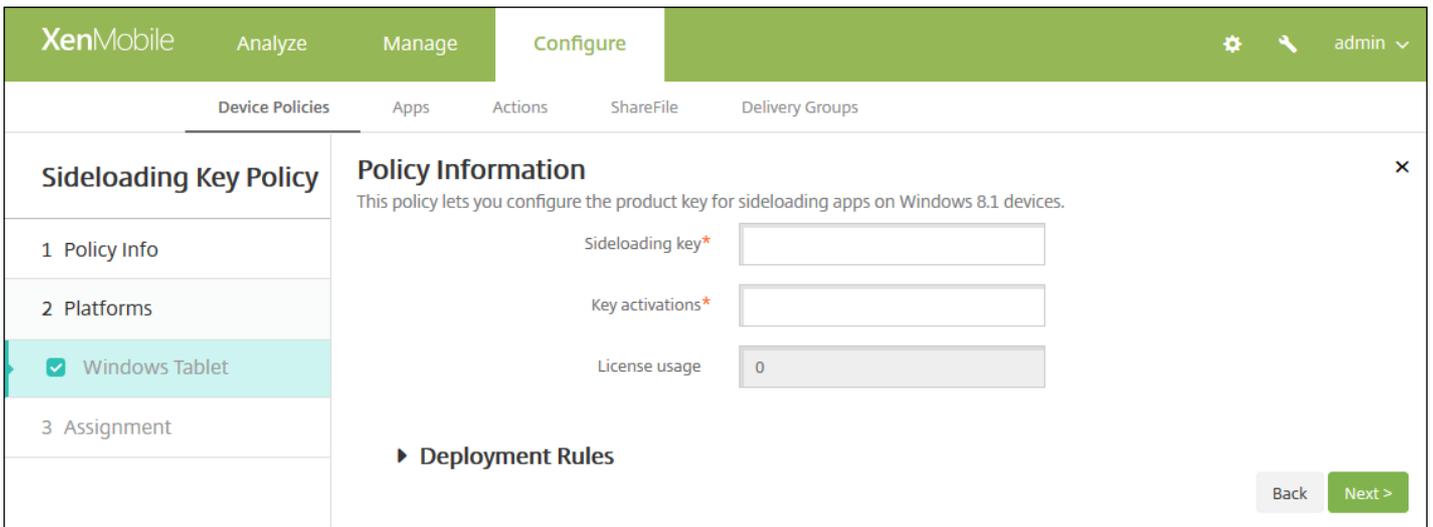
1. En la consola de XenMobile, haga clic en **Configurar > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add New Policy**.
3. Haga clic en **More** y, a continuación, en **Apps**, haga clic en **Sideloading Key**. Aparecerá la página **Sideloading Key Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Sideloading Key Policy' and 'Policy Information'. It includes a description: 'This policy lets you configure the product key for sideloading apps on Windows 8.1 devices.' There are two input fields: 'Policy Name\*' and 'Description'. A sidebar on the left shows a navigation menu with '1 Policy Info' selected, '2 Platforms' (with 'Windows Tablet' checked), and '3 Assignment'. A 'Next >' button is visible in the bottom right corner.

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 de información referente a la plataforma **Windows Tablet**.

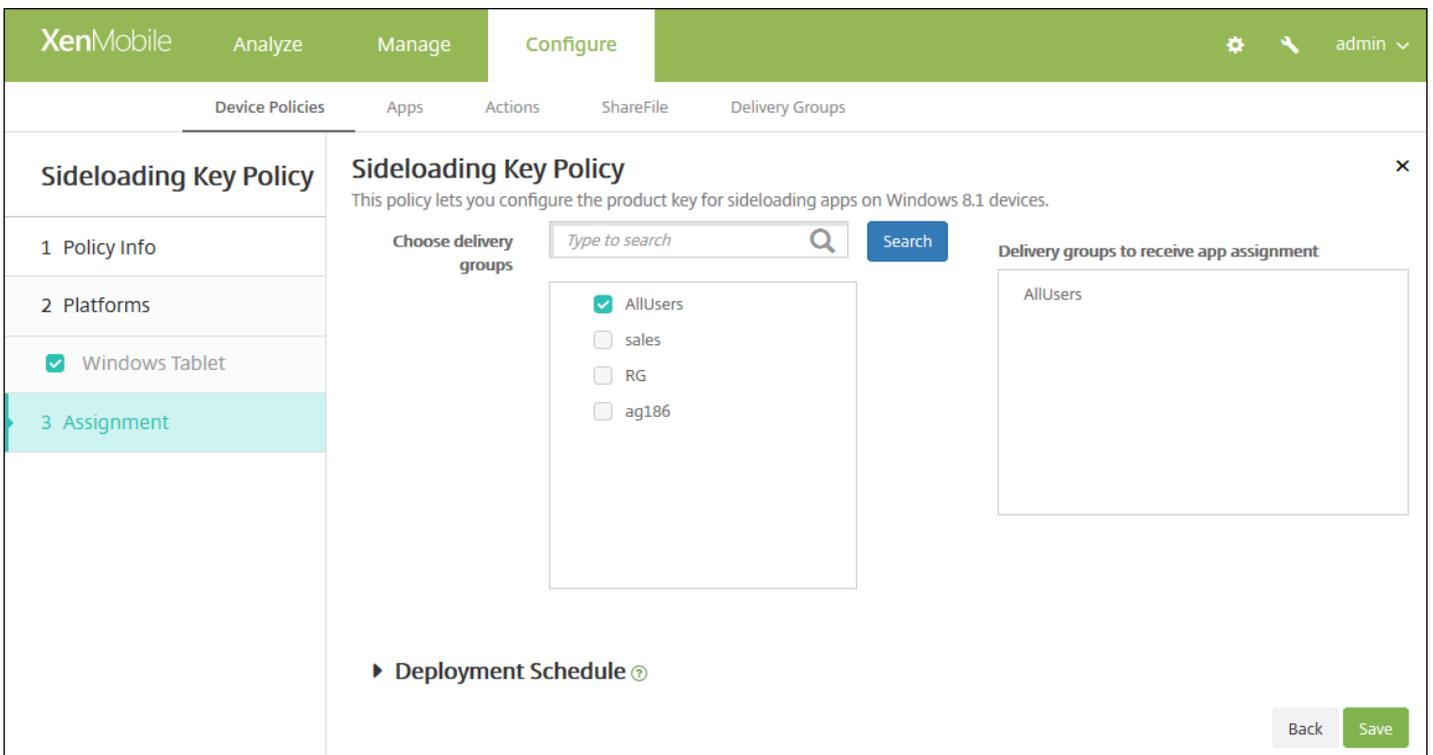


6. Configure los siguientes parámetros:

- **Sideload key.** Escriba la clave de sideloading obtenida del Centro de servicios de licencias por volumen de Microsoft.
- **Key activations.** Escriba la activación de la clave creada para la clave de sideloading.
- **License usage.** XenMobile calcula este valor según el número de tabletas inscritas. Este campo no puede cambiarse.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Sideload Key Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups**

**to receive app assignment.**

10. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de certificados de firma

Mar 02, 2017

En XenMobile, puede agregar una directiva de dispositivos para configurar los certificados de firma utilizados para firmar archivos APPX. Necesita certificados de firma si quiere distribuir archivos APPX a los usuarios para que puedan instalarse aplicaciones en sus tabletas Windows.

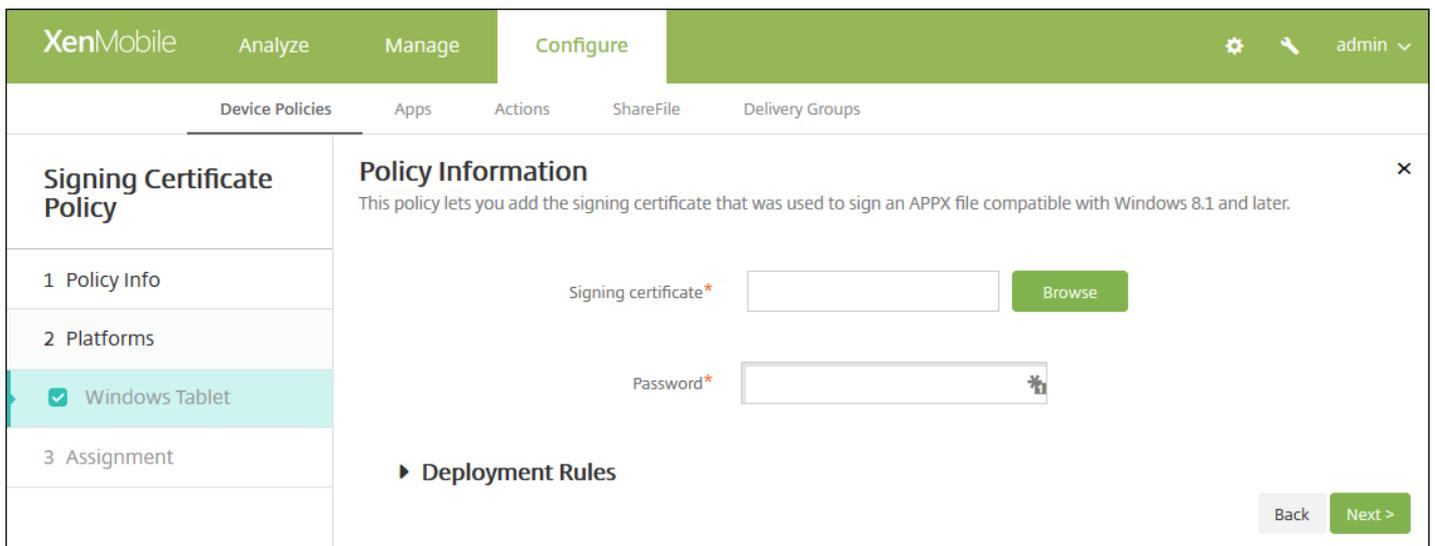
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **More** y, a continuación, en **Apps**, haga clic en **Signing Certificate**. Aparecerá la página **Signing Certificate Policy**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Signing Certificate Policy' and includes a sidebar with three steps: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a 'Policy Name\*' field and a 'Description' text area. A 'Next >' button is located at the bottom right of the form.

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 acerca de la plataforma **Windows Mobile/CE**.

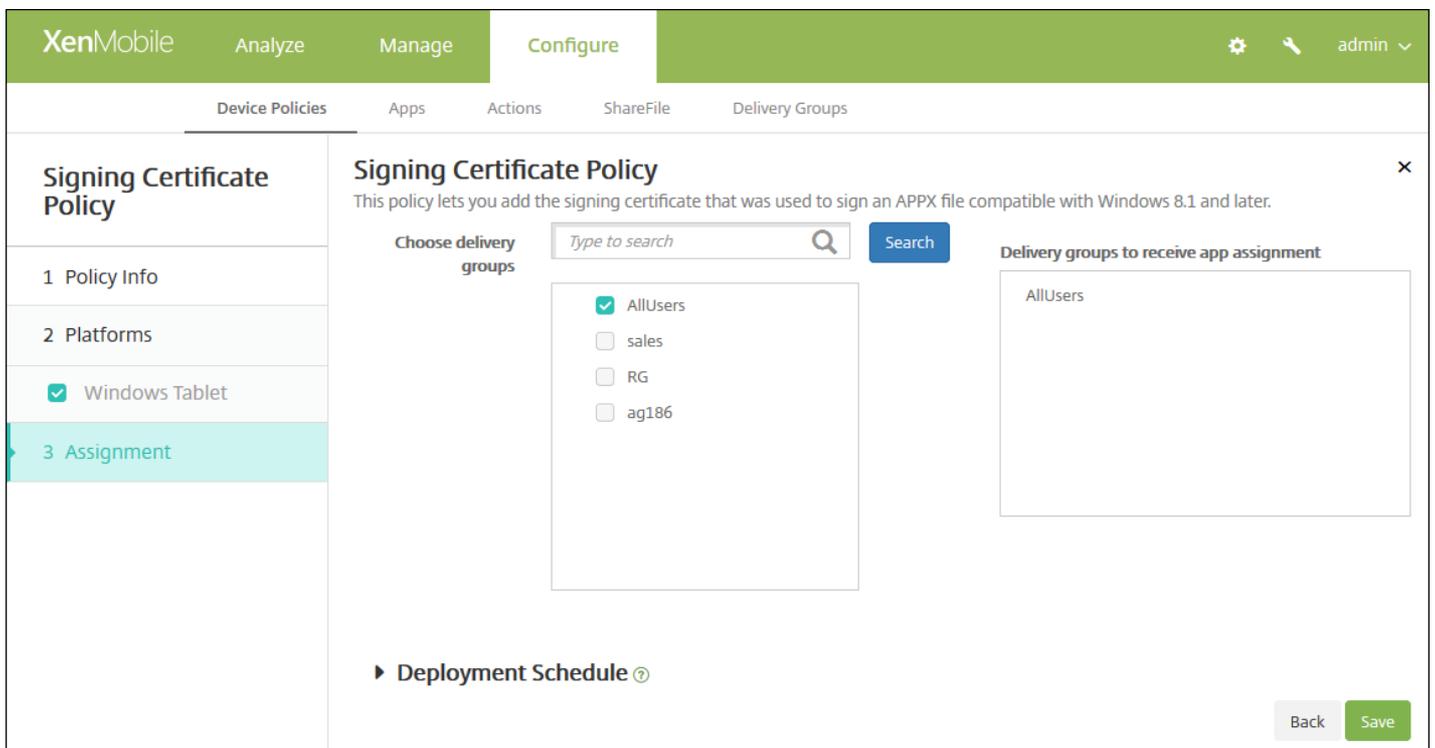


6. Configure los siguientes parámetros:

- **Signing certificate.** Debe seleccionar el certificado que se usó para firmar el archivo APPX. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.
- **Password.** Escriba la contraseña requerida para acceder al certificado de firma.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **Signing Certificate Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups**

**to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for Always on connection**, que no se aplica para iOS.

11. Haga clic en **Save**.

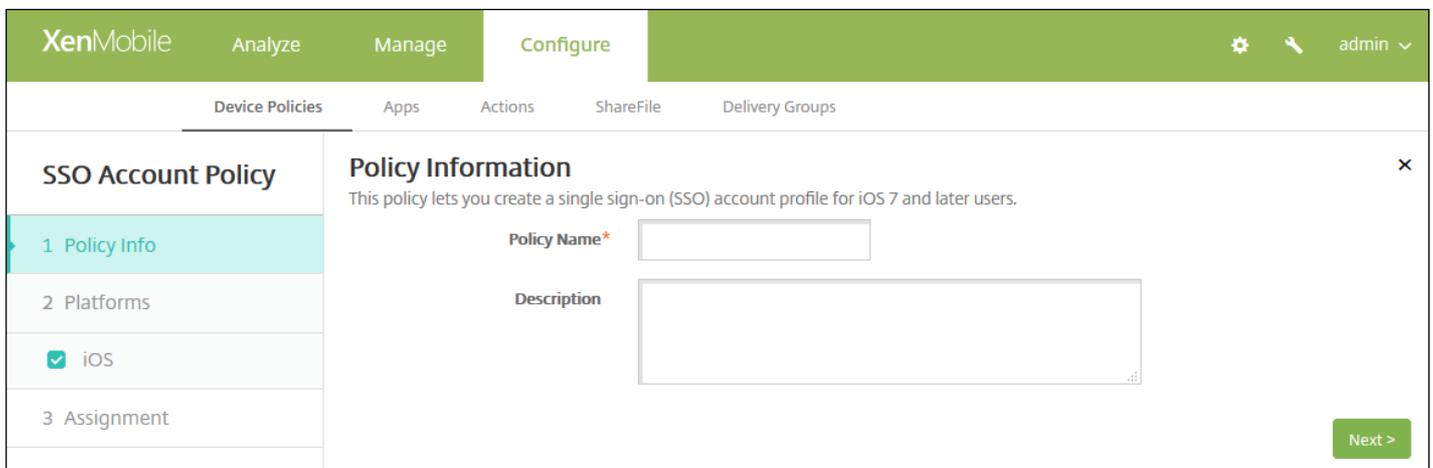
# Directiva de cuentas Single Sign-On

Mar 02, 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**.



The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left side, there is a sidebar with a list of policy steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' step is highlighted. The main content area is titled 'SSO Account Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.' Below the description, there are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. En el panel **SSO Account Policy**, 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 de información **iOS Platform**.

6. Configure los siguientes 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 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 en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## 7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **SSO Account Policy**.

The screenshot shows the XenMobile configuration interface for the 'SSO Account Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SSO Account Policy' and includes a description: 'This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search box and a list of groups: 'AllUsers' (checked) and 'sales' (unchecked). The 'Delivery groups to receive app assignment' section shows 'AllUsers' as the selected group. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o

varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

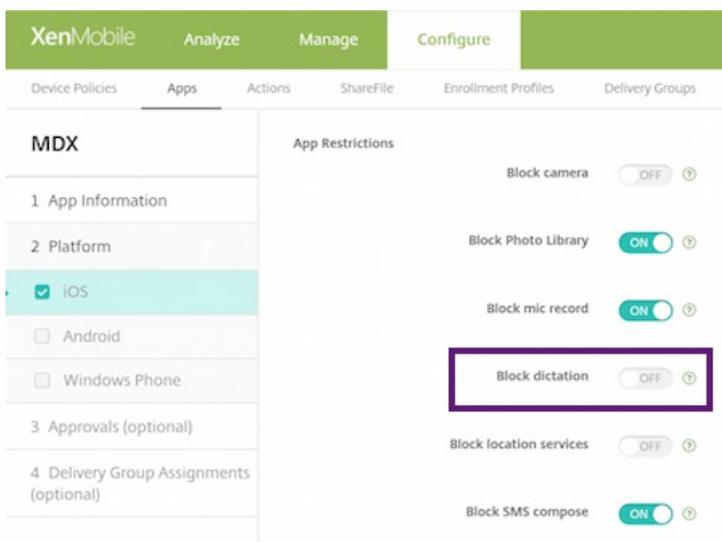
# Directivas de Siri y dictado

Mar 02, 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** (activado) 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 MDM (administración de dispositivos móviles), también puede inhabilitar Siri con la directiva Siri en **Configure > Device Policies > Restrictions Policy > iOS**. El uso de Siri está permitido de manera predeterminada.

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Restrictions Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Desktop/Tablet
- Amazon
- Windows Mobile/CE

3 Assignment

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Camera  ON
- FaceTime
- Screen shots  ON
- Photo streams  ON iOS 5.0+
- Shared photo streams  ON iOS 6.0+
- Voice dialing  ON
- Siri  ON
- Allow while device is locked
- Siri profanity filter

Back Next >

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 yendo a **Ajustes > General > Teclados** en cualquier dispositivo iOS, y tocando el enlace bajo **Habilitar dictado**.

# Directivas de cifrado de almacenamiento

Mar 02, 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**.

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

## Storage Encryption Policy

### Policy Information

This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

Policy Name\*

Description

1 Policy Info

2 Platforms

- Samsung SAFE
- Windows Phone
- Android Sony

3 Assignment

Next >

4. En el panel **Policy Information**, escriba la información siguiente:

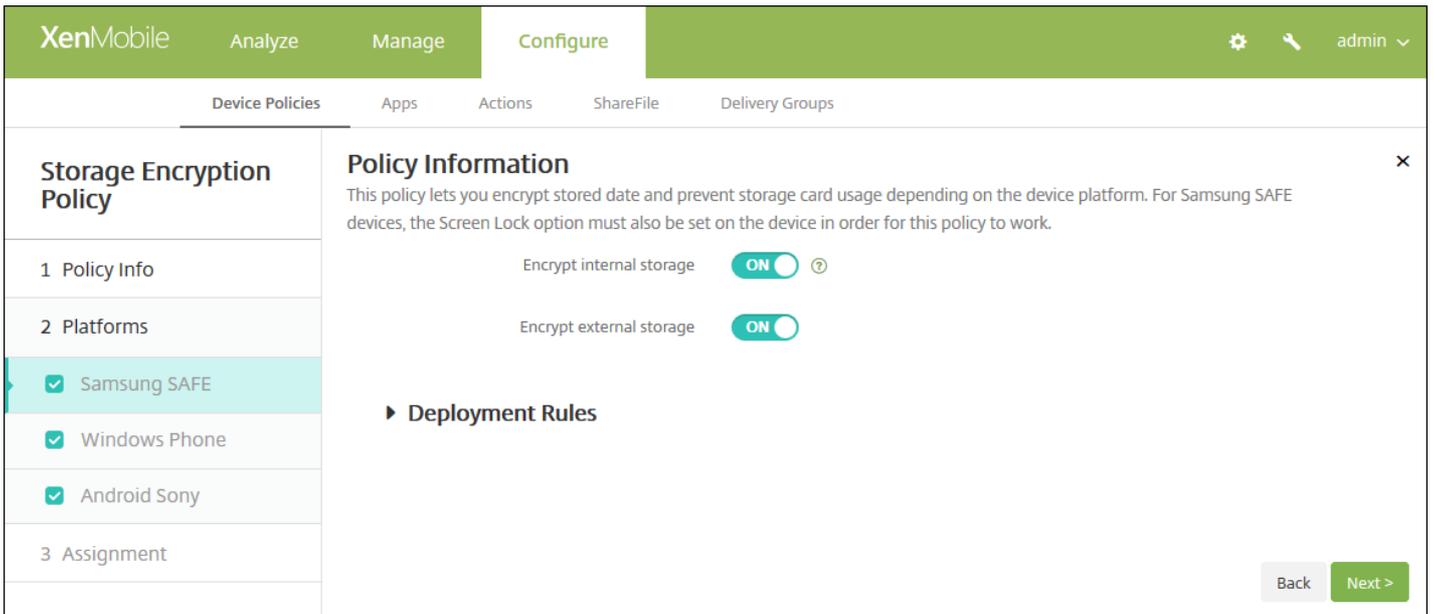
- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

### Configuración de los parámetros de Samsung SAFE



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

The screenshot shows the 'Configure' page for a 'Storage Encryption Policy'. On the left, a sidebar lists '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE', 'Windows Phone', and 'Android Sony' are all checked. The main area, titled 'Policy Information', contains two toggle switches: 'Require device encryption' (OFF) and 'Disable storage card' (OFF). Below these is a section for 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

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

This screenshot is similar to the previous one but shows the 'Encrypt external storage' toggle switch set to 'ON'. The 'Require device encryption' and 'Disable storage card' options remain 'OFF'. The 'Deployment Rules' section is also visible. The 'Next >' button is highlighted in green.

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**.

The screenshot shows the XenMobile interface for configuring a Storage Encryption Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Storage Encryption Policy' and includes a description: 'This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.' There are two main sections for configuration: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups with checkboxes: 'AllUsers' (checked) and 'sales' (unchecked). The 'Delivery groups to receive app assignment' section has a list of groups: 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de calendarios suscritos

Mar 02, 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](http://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**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies' as the selected category. The main content area is titled 'Subscribed Calendars Policy' and contains a 'Policy Information' section. This section includes a 'Policy Name\*' field and a 'Description' field. The 'Policy Information' section also includes a sub-section for 'Platforms' with a checked box for 'iOS'. A 'Next >' button is visible in the bottom right corner.

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 **iOS Platform Information**.

The screenshot shows the XenMobile configuration page for a 'Subscribed Calendars Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms' (with 'iOS' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and includes the following fields and settings:

- Description\***: Text input field with a help icon.
- URL\***: Text input field with a help icon.
- User name\***: Text input field.
- Password**: Text input field with a password icon.
- Use SSL**: Toggle switch set to 'OFF'.
- Policy Settings**:
  - Remove policy**: Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'.
  - Allow user to remove policy**: Dropdown menu set to 'Always'.
- Deployment Rules**: Section header with a right-pointing arrow.

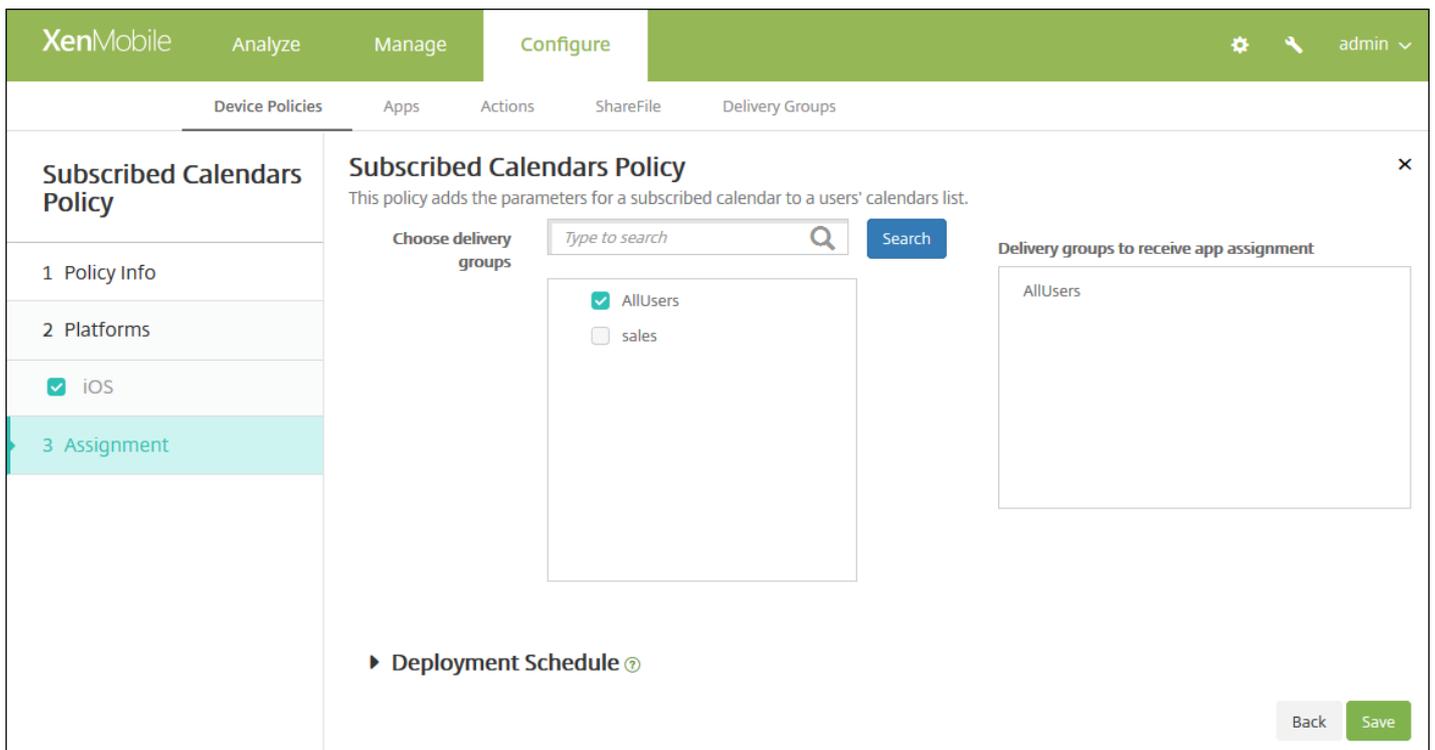
At the bottom right, there are 'Back' and 'Next >' buttons.

6. Configure los siguientes 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 en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Subscribed Calendars Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de términos y condiciones

Mar 02, 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 e 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

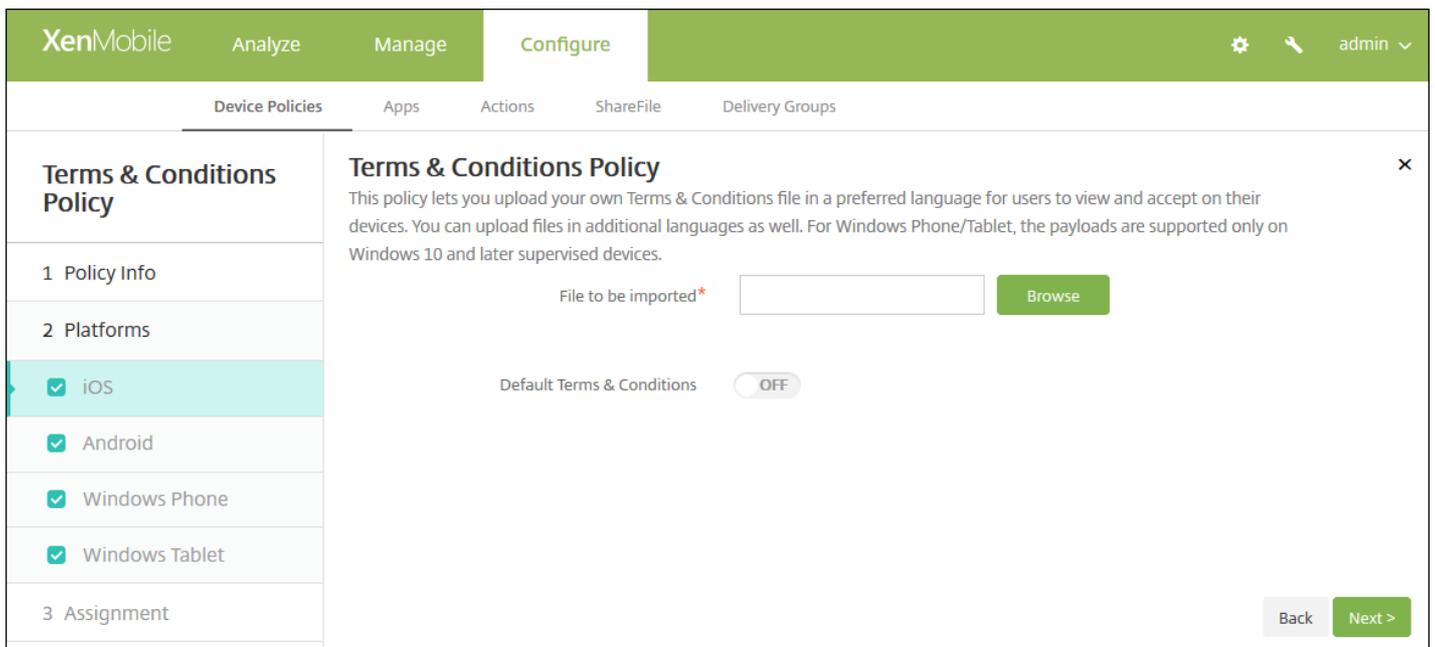
1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **Terms & Conditions**. Aparecerá la página **Terms & Conditions Policy**.

The screenshot shows the XenMobile console interface for configuring a 'Terms & Conditions Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Terms & Conditions Policy' and features a sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is currently selected and expanded, displaying a 'Policy Information' section. This section includes a text input field for 'Policy Name\*' and a larger text area for 'Description'. Below the 'Policy Information' section, there is a 'Platforms' section with four checked checkboxes: 'iOS', 'Android', 'Windows Phone', and 'Windows Tablet'. At the bottom right of the form, there is a green 'Next >' button.

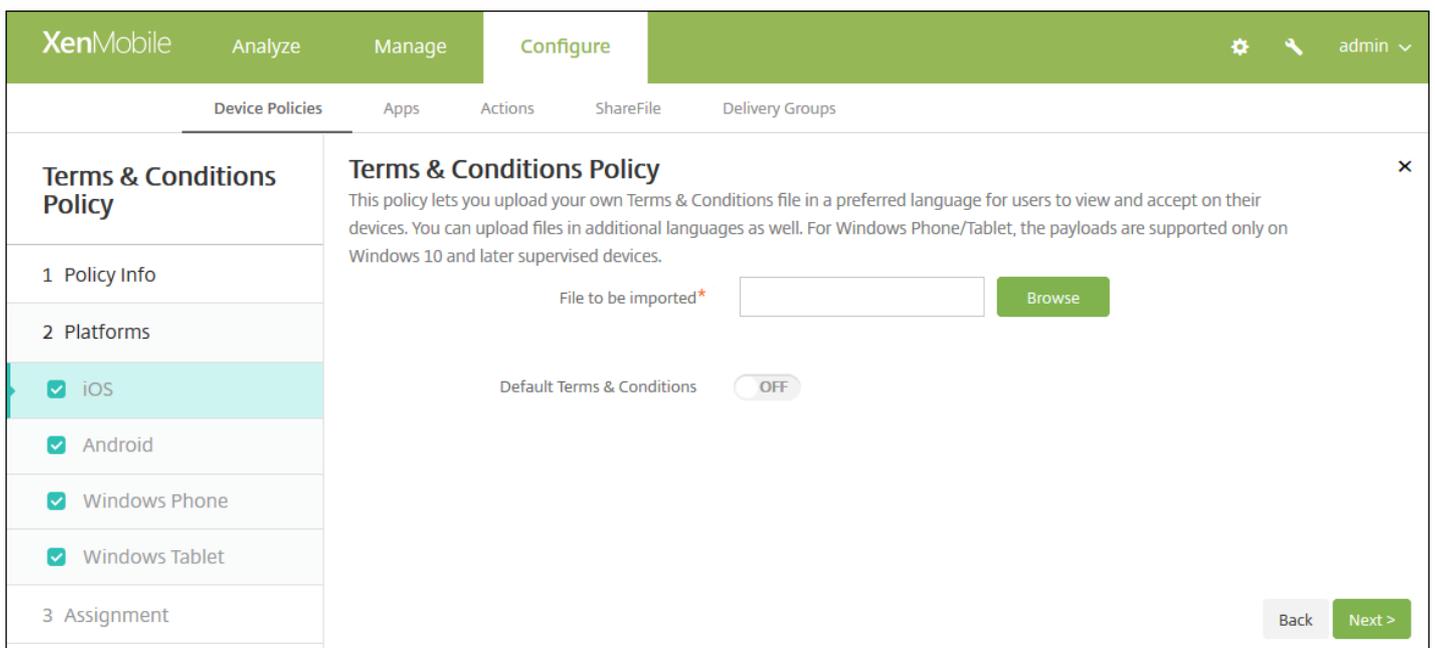
4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Next**. Aparecerá la página de asignación **Terms & Conditions Policy**.



## Configuración de iOS y Android



Configure estos parámetros:

- **File to be imported.** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Browse** y, a continuación, vaya a la ubicación del archivo.
- **Default Terms & Conditions.** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. El valor predeterminado es **OFF**.

## Configuración de Windows Phone y tabletas Windows

Configure estos parámetros:

- **File to be imported.** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Browse** y, a continuación, vaya a la ubicación del archivo.
- **Image.** Para seleccionar el archivo de imagen a importar, haga clic en **Browse** y vaya a la ubicación de ese archivo.
- **Default Terms & Conditions.** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. El valor predeterminado es **OFF**.

6. Haga clic en **Next**. Aparecerá la página de asignación **Terms & Conditions Policy**.

7. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

8. Haga clic en **Save**.

# Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

Mar 02, 2017

Con Apple Configurator, los dispositivos se conectan a un equipo Apple que ejecuta la aplicación Apple Configurator. Hay que preparar los dispositivos y configurar las directivas mediante Apple Configurator. Después de aprovisionar los dispositivos con las directivas necesarias, la primera vez que los dispositivos se conectan a XenMobile, se aplican las directivas y ya se puede empezar a administrar los dispositivos. Para obtener más información acerca de Apple Configurator, incluidos los requisitos del sistema, consulte [Apple Support](#).

## Important

Colocar un dispositivo en el modo supervisado instalará la versión seleccionada de iOS en el dispositivo. Con este proceso, se borran del dispositivo todos los datos de usuario o aplicaciones almacenados previamente.

1. Instale Apple Configurator desde iTunes.
2. Conecte el dispositivo iOS a su equipo de Apple.
3. Inicie Apple Configurator. Apple Configurator muestra que hay un dispositivo a preparar para la supervisión.
4. Para preparar el dispositivo para la supervisión:
  1. Cambie el control Supervision a On. Citrix recomienda elegir esta opción si quiere mantener el control del dispositivo de forma continua mediante la aplicación de una configuración con regularidad.
  2. Si lo prefiere, puede proporcionar un nombre para el dispositivo.
  3. En iOS, haga clic en Latest para ver la versión más reciente de iOS que quiera instalar.
5. Cuando esté listo para preparar el dispositivo para la supervisión, haga clic en Prepare.

# Directivas de red privada virtual (VPN)

Mar 02, 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.

[Configuración de iOS](#)

[Configuración de Mac OS X](#)

[Configuración de Android](#)

[Configuración de Samsung SAFE](#)

[Configuración de Samsung KNOX](#)

[Configuración de Windows Phone](#)

[Configuración de tabletas Windows](#)

[Configuración de Amazon](#)

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Haga clic en **VPN**. Aparecerá la página **VPN Policy**.

4. En el panel **Policy Information**, escriba la información siguiente:

- **Policy Name.** Escriba un nombre descriptivo para la directiva.
- **Description.** Escriba, si quiere, una descripción para la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página **Policy Platforms**. Al aparecer la página **Policy Platforms**, todas las plataformas están seleccionadas, y verá en primer lugar la plataforma de iOS.

6. En **Platforms**, seleccione la plataforma o las plataformas que quiere agregar. Borre aquellas plataformas que no quiera configurar.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de iOS

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
- 3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name

Connection type **L2TP**

Server name or IP address\*

User account

Password authentication  
 RSA SecureID authentication

Shared secret

Send all traffic **OFF**

**Proxy**

Proxy configuration **None**

**Policy Settings**

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy **Always**

► **Deployment Rules**

Back Next >

Configure estos parámetros:

- **Connection name.** Escriba un nombre para la conexión.
- **Connection type.** En la lista, haga clic en el protocolo que se va a usar para esta conexión. El valor predeterminado es **L2TP**.
  - **L2TP.** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP.** Túnel punto a punto.
  - **IPsec.** La conexión VPN de su empresa.
  - **Cisco AnyConnect.** Cliente VPN AnyConnect de Cisco.
  - **Juniper SSL.** Cliente SSL VPN de Juniper Networks.
  - **F5 SSL.** Cliente SSL VPN de F5 Networks.
  - **SonicWALL Mobile Connect.** Cliente VPN unificado de Dell para iOS.
  - **Ariba VIA.** Cliente de acceso virtual a Internet de Ariba Networks.
  - **IKEv2 (iOS only).** Intercambio de claves por red versión 2 solo para iOS.
  - **Citrix VPN.** Cliente VPN de Citrix para iOS.

- **Custom SSL.** Capa de sockets seguros (SSL) personalizada.

En las siguientes secciones se enumeran las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configuración del protocolo L2TP	▼
Configuración del protocolo PPTP	▼
Configuración del protocolo IPsec	▼
Configuración del protocolo AnyConnect de Cisco	▼
Configuración del protocolo SSL de Juniper	▼
Configuración del protocolo SSL de F5	▼
Configuración del protocolo SonicWALL	▼
Configuración del protocolo VIA de Ariba	▼
Configuración del protocolo IKEv2	▼
Configuración del protocolo VPN de Citrix	▼
Configuración del protocolo SSL personalizado	▼
Configuración de las opciones de Enable VPN on demand	▼

- **Proxy**

- **Proxy configuration.** En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **None**.
  - Si habilita **Manual**, configure los siguientes parámetros:
    - **Host name or IP address for the proxy server.** Escriba el nombre o la dirección IP de host del servidor proxy. Este campo es obligatorio.
    - **Port for the proxy server.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
    - **User name.** Si quiere, escriba un nombre de usuario para el servidor proxy.
    - **Password.** Si quiere, escriba una contraseña de servidor proxy.
  - Si selecciona **Automatic**, configure este parámetro:
    - **Proxy server URL.** Escriba la URL del servidor proxy. Este campo es obligatorio.
- **Configuraciones de directivas**
  - En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always, Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
- Assignment

#### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name

Connection type **L2TP**

Server name or IP address\*

User account

Password authentication  
 RSA SecureID authentication  
 Kerberos authentication  
 CryptoCard authentication

Shared secret

Send all traffic **OFF**

**Proxy**

Proxy configuration **None**

**Policy Settings**

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy **Always**

Profile scope **User** OS X 10.7+

► **Deployment Rules**

Back Next >

Configure estos parámetros:

- **Connection name.** Escriba un nombre para la conexión.
- **Connection type.** En la lista, haga clic en el protocolo que se va a usar para esta conexión. El valor predeterminado es L2TP.
  - **L2TP.** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP.** Túnel punto a punto.
  - **IPsec.** La conexión VPN de su empresa.
  - **Cisco AnyConnect.** Cliente VPN AnyConnect de Cisco.
  - **Juniper SSL.** Cliente SSL VPN de Juniper Networks.
  - **F5 SSL.** Cliente SSL VPN de F5 Networks.

- **SonicWALL Mobile Connect.** Cliente VPN unificado de Dell para iOS.
- **Ariba VIA.** Cliente de acceso virtual a Internet de Ariba Networks.
- **Citrix VPN.** Cliente VPN de Citrix.
- **Custom SSL.** Capa de sockets seguros (SSL) personalizada.

En las siguientes secciones se enumeran las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configuración del protocolo L2TP	▼
Configuración del protocolo PPTP	▼
Configuración del protocolo IPsec	▼
Configuración del protocolo AnyConnect de Cisco	▼
Configuración del protocolo SSL de Juniper	▼
Configuración del protocolo SSL de F5	▼
Configuración del protocolo SonicWALL	▼
Configuración del protocolo VIA de Ariba	▼
Configuración del protocolo VPN de Citrix	▼
Configuración del protocolo SSL personalizado	▼
Configuración de las opciones de Enable VPN on demand	▼

- **Proxy**

- **Proxy configuration.** En la lista, seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **None**.
  - Si habilita **Manual**, configure los siguientes parámetros:
    - **Host name or IP address for the proxy server.** Escriba el nombre o la dirección IP de host del servidor proxy. Este campo es obligatorio.
    - **Port for the proxy server.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
    - **User name.** Si quiere, escriba un nombre de usuario para el servidor proxy.
    - **Password.** Si quiere, escriba una contraseña de servidor proxy.
  - Si selecciona **Automatic**, configure este parámetro:
    - **Proxy server URL.** Escriba la URL del servidor proxy. Este campo es obligatorio.

- **Configuraciones de directivas**

- En **Policy Settings**, junto a **Remove policy**, haga clic en **Select date** o **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
- Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción solo está disponible para OS X 10.7 y versiones posteriores.

## Configuración de los parámetros de Android

**VPN Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android**
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Tablet
- Amazon

3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

**Cisco AnyConnect VPN**

Connection name\*

Server name or IP address\*

Backup VPN server

User group

Identity credential **None**

**Trusted Networks**

Automatic VPN policy **OFF**

**Deployment Rules**

[Back](#) [Next >](#)

Configure estos parámetros:

- **Cisco AnyConnect VPN**
  - **Connection name.** Escriba un nombre para la conexión VPN de Cisco AnyConnect. Este campo es obligatorio.
  - **Server name or IP address.** Escriba el nombre o la dirección IP del servidor VPN. Este campo es obligatorio.
  - **Backup VPN server.** Escriba la información del servidor VPN de respaldo.
  - **User group.** Escriba la información del grupo de usuarios.
  - **Identity credential.** En la lista, seleccione una credencial de identidad.
- **Trusted Networks**
  - **Automatic VPN policy.** Habilite o inhabilite esta opción para establecer cómo reaccionará la red privada virtual ante redes con las que se haya establecido una relación de confianza o de no confianza. Si habilita esta opción, configure los siguientes parámetros:
    - **Trusted network policy.** En la lista, haga clic en la directiva pertinente. El valor predeterminado es **Disconnect**. Las opciones posibles son:
      - **Disconnect.** El cliente cierra la conexión VPN en la red de confianza. Ésta es la opción predeterminada.
      - **Connect.** El cliente inicia una conexión VPN en la red de confianza.
      - **Do Nothing.** El cliente no lleva a cabo ninguna acción.
      - **Pause.** Suspende la sesión VPN (en lugar de desconectarla) cuando un usuario introduce una red configurada como red de confianza después de establecer una sesión VPN fuera de la red de confianza. Cuando el usuario abandona esa red de confianza, la sesión se reanuda. Esto elimina la necesidad de establecer una nueva sesión VPN después de abandonar una red de confianza.
    - **Untrusted network policy.** En la lista, haga clic en la directiva pertinente. El valor predeterminado es **Connect**. Las

opciones posibles son:

- **Connect.** El cliente inicia una conexión VPN en una red que no es de confianza.
- **Do Nothing.** El cliente inicia una conexión VPN en una red que no es de confianza. Esta opción inhabilita la opción Always-on VPN.
- **Trusted domains.** Para agregar cada sufijo de dominio que puede tener la interfaz de red cuando el cliente se encuentra en la red de confianza, haga clic en **Add** y realice lo siguiente:
  - **Domain.** Escriba el dominio que se va a agregar.
  - Haga clic en **Save** para guardar el dominio, o bien haga clic en **Cancel** para no guardarlo.
- **Trusted servers.** Para agregar cada dirección de servidor que puede tener la interfaz de red cuando el cliente se encuentra en la red de confianza, haga clic en **Add** y realice lo siguiente:
  - **Servers.** Escriba el servidor que se va a agregar.
  - Haga clic en **Save** para guardar el servidor, o bien haga clic en **Cancel** para no guardarlo.

**Nota:** Para eliminar un servidor existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Delete** para eliminar el elemento, o bien haga clic en **Cancel** para conservarlo.

Para modificar un servidor existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono con forma de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Save** para guardar los cambios, o bien en **Cancel** para no guardarlos.

## Configuración de los parámetros de Samsung SAFE

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, and the 'VPN Policy' is selected. The left sidebar shows a list of platforms with 'Samsung SAFE' highlighted. The main content area displays the 'Policy Information' for the selected policy, including fields for 'Connection name\*', 'Vpn Type' (set to 'L2TP with pre-shared key'), 'Host name\*', 'User name', 'Password', and 'Pre-shared key\*'. There is also a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

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.

<a href="#">Configuración del protocolo L2TP con clave precompartida</a>	▼
<a href="#">Configuración del protocolo L2TP con certificado</a>	▼
<a href="#">Configuración del protocolo PPTP</a>	▼
<a href="#">Configuración del protocolo de empresa</a>	▼
<a href="#">Configuración del protocolo genérico</a>	▼

Configuración de los parámetros de Samsung KNOX

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX**
  - Windows Phone
  - Windows Tablet
  - Amazon
- Assignment

#### Policy Information ✕

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Vpn Type: Enterprise ▾

Connection name\*:

Host name\*:

Enable backup server:  OFF

Enable user authentication:  OFF

Group name:

Authentication method: Certificate ▾

Identity credential: None ▾

CA certificate: Select certificate ▾

Enable default route:  OFF

Enable smartcard authentication:  OFF

Enable mobile option:  OFF

Diffie-Hellman group value (key strength): 0 ▾

Split tunnel type: Auto ▾

SuiteB Type: GCM-128 ▾

**Forward routes**

Forward route

Forward route	Add
	<input type="button" value="Add"/>

► **Deployment Rules**

**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 de los parámetros de Windows Phone

**XenMobile** Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone**
- Windows Tablet
- Amazon

3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name\*

Profile type **Native**

VPN server name\*

Tunneling protocol\* **L2TP**

Authentication method\* **EAP**

EAP method\* **TLS**

DNS suffix

Trusted networks

Require smart card certificate **OFF**

Automatically select client certificate **OFF**

Remember credential **OFF**

Always-on VPN **OFF**

Bypass For Local **OFF**

► **Deployment Rules**

**Back** **Next >**

**Nota:** Esta configuración solo se admite en teléfonos supervisados con Windows 10 y versiones posteriores.

Configure estos parámetros:

- **Connection name.** Escriba el nombre de la conexión. Este campo es obligatorio.
- **Profile type.** En la lista, haga clic en **Native** o **Plugin**. El valor predeterminado es **Native**. En los siguientes apartados, se describe la configuración de cada una de las opciones.
- **Configure Native profile type settings.** Esta configuración se aplica a la red VPN integrada en los teléfonos Windows de los usuarios.
  - **VPN server name.** Escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor VPN. Este campo es obligatorio.

- **Tunneling protocol.** En la lista, haga clic en el tipo de túnel VPN a usar. El valor predeterminado es **L2TP**. Las opciones posibles son:
  - **L2TP.** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
  - **PPTP.** Túnel punto a punto.
  - **IKEv2.** Versión 2 de Intercambio de claves por red.
- **Authentication method.** En la lista, haga clic en el método de autenticación que se va a usar. El valor predeterminado es **EAP**. Las opciones posibles son:
  - **EAP.** Protocolo de autenticación extensible (EAP).
  - **MSCHAPv2.** Usa el protocolo de autenticación por desafío mutuo de Microsoft para la autenticación mutua. Esta opción no está disponible si se selecciona IKEv2 como tipo de túnel. Al elegir MSChapV2, aparece la opción **Automatically use Windows credentials**; el valor predeterminado es **OFF**.
- **EAP method.** En la lista, haga clic en el método EAP que se va a usar. El valor predeterminado es **TLS**. Este campo no está disponible si se habilita la autenticación MSChapV2. Las opciones posibles son:
  - **TLS.** Seguridad de la capa de transporte (Transport Layer Security).
  - **PEAP.** Protocolo de autenticación extensible protegido (Protected Extensible Authentication Protocol).
- **DNS Suffix.** Escriba el sufijo DNS.
- **Trusted networks.** Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.
- **Require smart card certificate.** Seleccione si se debe requerir un certificado de tarjeta inteligente. El valor predeterminado es OFF.
- **Automatically select client certificate.** Seleccione si elegir automáticamente el certificado de cliente para la autenticación. El valor predeterminado es OFF. Esta opción no está disponible si se habilita la opción Require smart card certificate.
- **Remember credential.** Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es OFF. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
- **Always on VPN:** Seleccione si la VPN siempre está activada. El valor predeterminado es OFF. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Bypass For Local.** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.
- **Configure Plugin protocol type.** Estos parámetros se aplican a plug-ins VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
  - **Server address.** Escriba la URL, el nombre de host o la dirección IP del servidor VPN.
  - **Client app ID.** Escriba el nombre de familia del paquete que tenga el plug-in VPN.
  - **Plugin Profile XML.** Seleccione el perfil personalizado de plug-in VPN que se va a usar. Para ello, haga clic en Browse y vaya a la ubicación del archivo. Para obtener información más detallada e indicaciones referentes al formato, póngase en contacto con el proveedor del plug-in.
  - **DNS Suffix.** Escriba el sufijo DNS.
  - **Trusted networks.** Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.
  - **Remember credential.** Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es OFF. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
  - **Always on VPN:** Seleccione si la VPN siempre está activada. El valor predeterminado es OFF. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
  - **Bypass For Local.** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor

proxy.

## Configuración de los parámetros de tabletas Windows

The screenshot shows the XenMobile 'Configure' interface for a VPN Policy. The left sidebar lists various platforms, with 'Windows Tablet' selected. The main area displays the 'Policy Information' for this platform, including fields for OS version (set to 10), connection name, profile type (Native), server address, and authentication method (EAP/TLS). Several options like 'Remember credential', 'Require smart card certificate', and 'Always-on VPN' are set to 'OFF'. A 'Deployment Rules' section is partially visible at the bottom.

**VPN Policy**

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet**
  - Amazon
- 3 Assignment

**Policy Information**

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

- OS version\*: 10
- Connection name\*: [Text Field]
- Profile type: Native
- Server address\*: [Text Field]
- Remember credential: OFF
- DNS suffix: [Text Field]
- Tunnel type\*: L2TP
- Authentication method\*: EAP
- EAP method\*: TLS
- Trusted networks: [Text Field]
- Require smart card certificate: OFF
- Automatically select client certificate: OFF
- Always-on VPN: OFF
- Bypass For Local: OFF

► **Deployment Rules**

Back Next >

Configure estos 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 los parámetros de Windows 10](#)

[Configuración de Windows 8.1](#)

Configuración de los parámetros de Amazon

The screenshot shows the XenMobile 'Configure' interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'VPN Policy' section with sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Android, Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone, and Amazon (which is highlighted). Under '3 Assignment', there is an empty section. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.' Below the description are several configuration fields: 'Connection name\*' (text input), 'Vpn Type' (dropdown menu set to 'L2TP PSK'), 'Server address\*' (text input), 'User name' (text input), 'Password' (text input), 'L2TP Secret' (text input), 'IPSec Identifier' (text input), 'IPSec pre-shared key' (text input), 'DNS search domains' (text input), 'DNS servers' (text input), and 'Forwarding routes' (text input). At the bottom of the main area, there is a 'Deployment Rules' section with a right-pointing arrow. In the bottom right corner, there are 'Back' and 'Next >' buttons.

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**.

The screenshot shows the XenMobile configuration interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'VPN Policy' and includes a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.' There are two main sections: 'Choose delivery groups' with a search bar and a list of groups (AllUsers checked, sales unchecked), and 'Delivery groups to receive app assignment' with a list containing 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**. Esta opción se

aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de fondos de escritorio

Mar 02, 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 pantalla y aplicarlas a los usuarios correspondientes.

En la siguiente tabla, se ofrece una lista de las dimensiones de imagen que recomienda Apple para dispositivos iOS.

Dispositivo		Dimensiones de imagen en píxeles
iPhone	iPad	
4, 4s		640 x 960
5, 5c, 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

1. En la consola de XenMobile, haga clic en **Configure > Device Policies**. Aparecerá la página **Device Policies**.
2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add a New Policy**.
3. Expanda **More** y, en **End user**, haga clic en **Wallpaper**. Aparecerá la página **Wallpaper Policy**.

**Wallpaper Policy**

1 Policy Info

2 Platforms

iOS

3 Assignment

**Policy Information**

This policy lets you add a .png or .jpg file to set wallpaper on a supervised device lock screen, home screen or both. Available in iOS 7.1.2 and later.

Policy Name\*

Description

Next >

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

**Wallpaper Policy**

1 Policy Info

2 Platforms

iOS

3 Assignment

**Policy Information**

This policy lets you add a .png or .jpg file to set wallpaper on a supervised device lock screen, home screen or both. Available in iOS 7.1.2 and later.

Apply to

Wallpaper file

► Deployment Rules

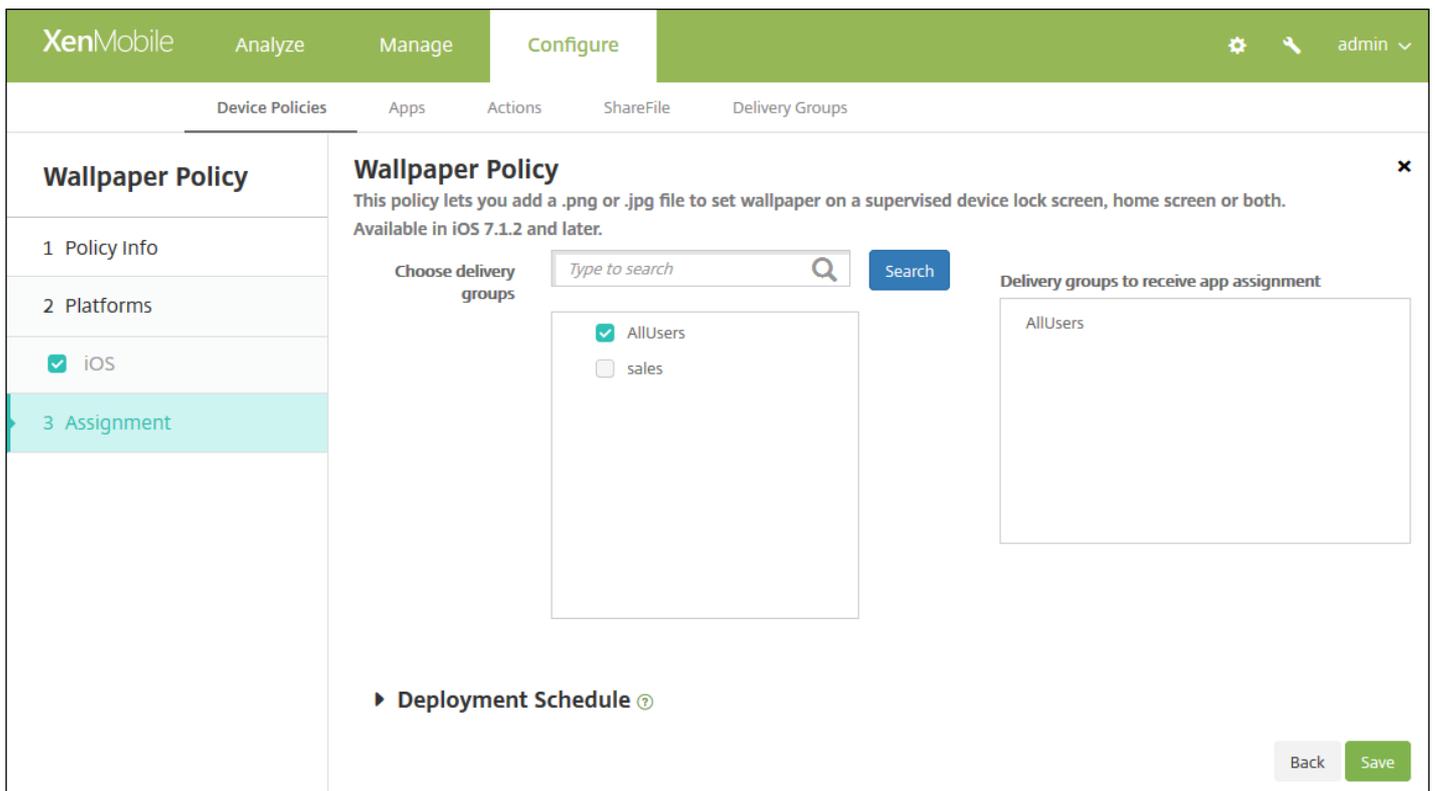
Back

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 **Siguiente**. Aparecerá la página de asignación **Wallpaper Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de contenidos Web

Mar 02, 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 **Security**, haga clic en **Web Content Filter**. Aparecerá la página **Web Content Filter Policy**.

The screenshot shows the XenMobile interface for configuring a Web Content Filter Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Web Content Filter Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is currently active and shows a 'Policy Information' dialog box. This dialog box contains a 'Policy Name\*' field and a 'Description' field. A note above the fields states: 'This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.' A 'Next >' button is located at the bottom right of the dialog box.

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 de información referente a la plataforma **iOS**.

The screenshot shows the XenMobile configuration page for a 'Web Content Filter Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', 'Configure', and 'admin'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view with 'Web Content Filter Policy' expanded, containing '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected). The main content area is titled 'Policy Information' and includes a description: 'This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.' The 'Filter type' is set to 'Built-in'. Under 'Web Content Filter', 'Auto filter enabled' is 'OFF'. There are sections for 'Permitted URLs' and 'Blacklisted URLs', each with an 'Add' button. The 'Bookmark Whitelist' section has columns for 'URL\*', 'Bookmark Folder', and 'Title\*', with an 'Add' button. The 'Policy Settings' section includes 'Remove policy' options: 'Select date' (selected) and 'Duration until removal (in days)'. There is a date picker below. 'Allow user to remove policy' is set to 'Always'. At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

6. Configure los siguientes parámetros:

- **Filter type.** En la lista, haga clic en **Built-in** o **Plug-in** y, a continuación, siga los procedimientos de la opción que elija. El valor predeterminado es **Built-in**.

[Configuración del tipo de filtro integrado](#) ▼

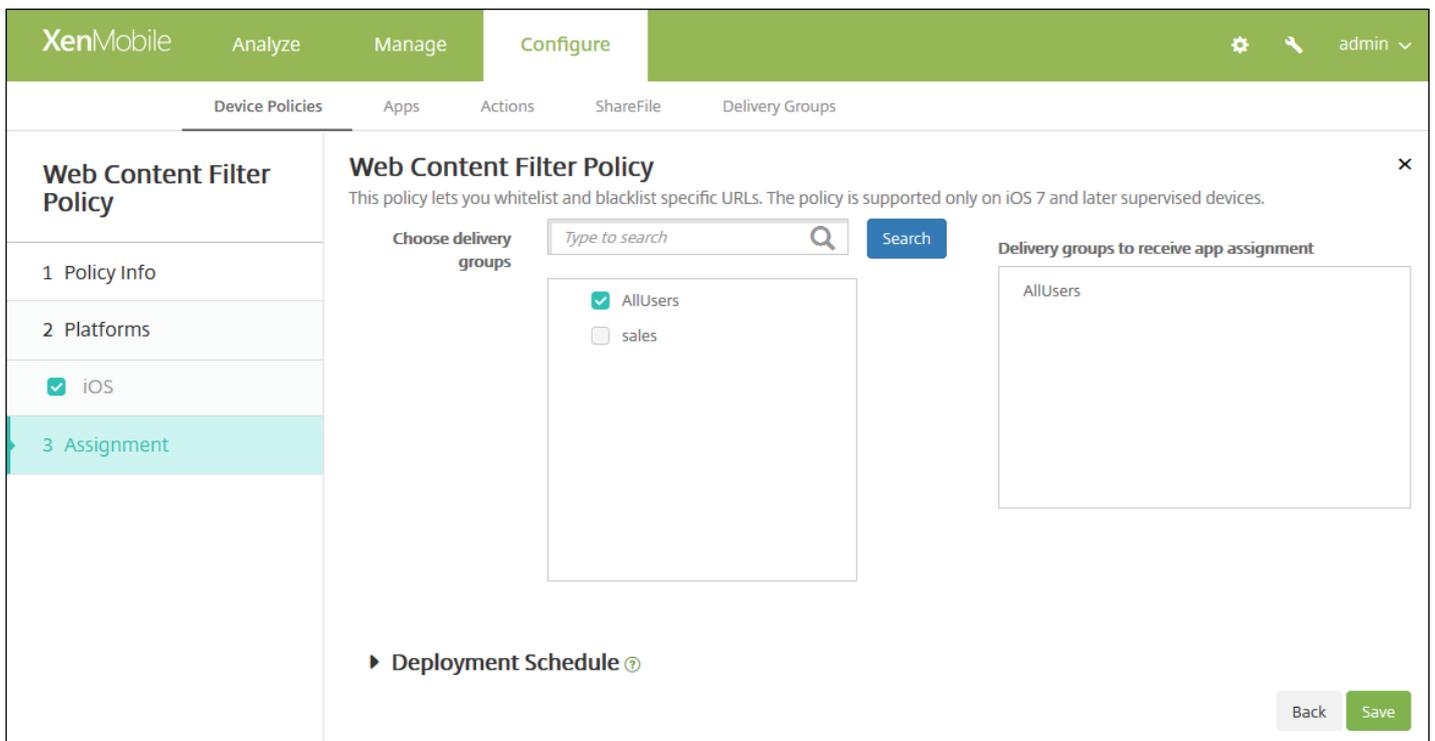
[Configuración del tipo de filtro plug-in](#) ▼

- **Configuraciones de directivas**

- Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

[7. Configure las reglas de implementación.](#) ▼

8. Haga clic en **Next**. Aparecerá la página de asignación **Web Content Filter Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de clips Web

Mar 02, 2017

Puede colocar accesos directos, o clips Web, en los sitios Web para que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips Web en dispositivos iOS, Mac OS X y Android; las tabletas Windows solo requieren una etiqueta y una URL.

[Configuración de iOS](#)

[Configuración de Mac OS X](#)

[Configuración de Android](#)

[Configuración de 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 **clip Web**. Aparece la página **Webclip Policy**.

The screenshot shows the XenMobile console interface for configuring a Webclip Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' tab is active, and the 'Webclip Policy' page is displayed. The page is divided into a left sidebar and a main content area. The sidebar has three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are four checkboxes, all of which are checked: 'iOS', 'Mac OS X', 'Android', and 'Windows Desktop/Tablet'. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' Below the description are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area).

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

## Configuración de los parámetros de iOS

The screenshot shows the XenMobile Configure interface for a Webclip Policy. The left sidebar has a 'Webclip Policy' header and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', four options are listed with checkboxes: 'iOS', 'Mac OS X', 'Android', and 'Windows Desktop/Tablet'. The 'iOS' option is selected. The main area is titled 'Webclip Policy' and contains the following settings:

- Label\***: A text input field.
- URL\***: A text input field with a help icon.
- Removable**: A toggle switch set to 'OFF'.
- Icon to be updated**: A text input field and a green 'Browse' button.
- Precomposed icon**: A toggle switch set to 'OFF'.
- Full screen**: A toggle switch set to 'OFF'.
- Remove policy**: Two radio button options: 'Select date' (selected) and 'Duration until removal (in days)'. Below the radio buttons is a date picker.
- Allow user to remove policy**: A dropdown menu set to 'Always' with a help icon.

Configure estos parámetros:

- **Label.** Escriba la etiqueta que aparecerá con el clip Web.
- **URL.** Escriba la URL asociada al clip Web. La URL debe comenzar por un protocolo; por ejemplo, <http://servidor>.
- **Removable.** Seleccione si los usuarios pueden quitar el clip Web. El valor predeterminado es **OFF**.
- **Icon to be updated.** Seleccione el icono para usar con el clip Web haciendo clic en **Browse** para encontrar la ubicación del archivo.
- **Precomposed icon.** Seleccione si habrá efectos que se aplicarán al icono, como esquinas redondeadas, sombra paralela y brillo de reflejos, entre otros. El valor predeterminado es **OFF**, con lo que se agregan efectos.
- **Full screen.** Seleccione si la página Web enlazada se abre en modo de pantalla completa. El valor predeterminado es **OFF**.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

## Configuración de los parámetros de Mac OS X

**XenMobile** Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Webclip Policy

This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.

**1 Policy Info**

**2 Platforms**

iOS

Mac OS X

Android

Windows Desktop/Tablet

**3 Assignment**

**Policy Settings**

Label\*

URL\*

Icon to be updated

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

► **Deployment Rules**

Configure estos parámetros:

- **Label.** Escriba la etiqueta que aparecerá con el clip Web.
- **URL.** Escriba la URL asociada al clip Web. La URL debe comenzar por un protocolo; por ejemplo, http://servidor.
- **Icon to be updated.** Seleccione el icono para usar con el clip Web haciendo clic en Browse para encontrar la ubicación del archivo.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
  - Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
  - En la lista **Profile Scope**, haga clic en **User** o **System**. Esta opción está disponible para OS X 10.7 y versiones posteriores.

Configuración de los parámetros de Android

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', the 'Webclip Policy' is chosen. The left sidebar shows '1 Policy Info', '2 Platforms', and '3 Assignment'. In the 'Platforms' section, 'Android' and 'Windows Desktop/Tablet' are selected. The main content area is titled 'Webclip Policy' and includes the description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' The configuration options are:
 

- Rule:** Radio buttons for 'Add' (selected) and 'Remove'.
- Label\*:** An empty text input field.
- URL\*:** An empty text input field.
- Define an icon:** A toggle switch set to 'OFF'.

 A 'Deployment Rules' section is partially visible at the bottom.

Configure estos parámetros:

- **Rule.** Seleccione si esta directiva agrega o quita un clip Web. El valor predeterminado es **Add**.
- **Label.** Escriba la etiqueta que aparecerá con el clip Web.
- **URL.** Escriba la URL asociada al clip Web.
- **Define an icon.** Seleccione si quiere usar un archivo de icono. El valor predeterminado es **OFF**.
- **Icon file.** Si la opción **Define an icon** está establecida en **ON**, deberá seleccionar el archivo de icono que se va a usar. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

Configuración de los parámetros de escritorios o tabletas Windows

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', the 'Webclip Policy' is chosen. The left sidebar shows '1 Policy Info', '2 Platforms', and '3 Assignment'. In the 'Platforms' section, 'Windows Desktop/Tablet' is selected. The main content area is titled 'Webclip Policy' and includes the description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' The configuration options are:
 

- Name\*:** An empty text input field.
- URL\*:** An empty text input field.

 A 'Deployment Rules' section is partially visible at the bottom.

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 **Siguiente**. Aparecerá la página de asignación **Webclip Policy**.

The screenshot shows the XenMobile configuration interface for a Webclip Policy. The navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is titled 'Webclip Policy' and includes a description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' There is a section for 'Choose delivery groups' with a search input field and a 'Search' button. Below this is a list of delivery groups: 'AllUsers', 'DG: [redacted]', and 'DG: [redacted]'. At the bottom, there is a section for 'Deployment Schedule' with a help icon.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará a iOS.

11. Haga clic en **Save** para guardar la directiva.

# Directivas WiFi de dispositivos

Mar 02, 2017

En XenMobile, puede crear o modificar las directivas de WiFi desde la página **Configure > Device Policies** de la consola de XenMobile. Mediante las directivas de redes WiFi, puede administrar el modo en que los usuarios conectan sus dispositivos a redes inalámbricas WiFi. Para ello, deberá definir de manera uniforme los nombres y los tipos de red, las directivas de seguridad y de autenticación, si se van a usar servidores proxy, y otros datos relacionados con redes WiFi, para todos los usuarios de las plataformas de dispositivo que seleccione.

Puede configurar las opciones de WiFi para los usuarios de las plataformas siguientes: iOS, Mac OS X, Android (incluidos los dispositivos habilitados para Android for Work), Windows Phone, así como escritorios y tabletas Windows. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

[Configuración de iOS](#)

[Configuración de Mac OS X](#)

[Configuración de Android](#)

[Configuración de Windows Phone](#)

[Configuración de escritorios y tabletas Windows](#)

## Important

Antes de crear una directiva nueva, lleve a cabo estos pasos:

- Crear los grupos de implementación que se van a utilizar.
- Saber el nombre y el tipo de red.
- Conocer los tipos de seguridad o de autenticación que se van a utilizar.
- Conocer cualquier información del servidor proxy que pueda necesitar.
- Instalar los certificados de CA necesarios.
- Disponer de todas las claves compartidas necesarias.
- Cree una entidad PKI para la autenticación basada en certificados.
- Configure 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**.

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Windows Phone
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy lets you configure a WiFi profile for devices.

**Policy Name\***

**Description**

Next >

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.

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

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Windows Phone
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

**Network type**: Standard

**Network name\***:

**Hidden network (enable if network is open or off)**: OFF

**Auto join (automatically join this wireless network)**: ON

**Security type**: None

**Proxy server settings**

**Proxy configuration**: None

**Policy Settings**

**Remove policy**:  Select date  Duration until removal (in days)

**Allow user to remove policy**: Always

► Deployment Rules

Back Next >

Configure estos parámetros:

- **Network type.** En la lista, haga clic en **Standard**, **Legacy Hotspot** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Network Name.** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Hidden network (enable if network is open or off).** Seleccione si la red está oculta o no.
- **Auto join (automatically join this wireless network).** Seleccione si se conecta a la red automáticamente o no. El valor predeterminado es **ON**.
- **Security type.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - None. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

WPA, WPA Personal, Any (personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

• **Parámetros del servidor proxy**

- **Proxy configuration.** En la lista, haga clic en None, Manual o Automatic para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es None, que no requiere ninguna configuración adicional.
- Si hace clic en **Manual**, configure los siguientes parámetros:
  - **Hostname/IP address.** Escriba el nombre o la dirección IP de host del servidor proxy.
  - **Port.** Escriba el número de puerto del servidor proxy.
  - **User name.** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
  - **Password.** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
- Si hace clic en **Automatic**, configure los siguientes parámetros:
  - **Server URL.** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
  - **Allow direct connection if PAC is unreachable.** Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **ON**. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.

• **Configuraciones de directivas**

- Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
- Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
- En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.
- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.

Configuración de los parámetros de Mac OS X

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Windows Phone
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

**Network type** Standard

**Network name\***

**Hidden network (enable if network is open or off)** OFF

**Auto join (automatically join this wireless network)** ON

**Security type** None

**Proxy server settings**

**Proxy configuration** None

**Policy Settings**

**Remove policy**  Select date  Duration until removal (in days)

**Allow user to remove policy** Always

**Profile scope** User OS X 10.7+

► Deployment Rules

Back Next >

Configure estos parámetros:

- **Network type.** En la lista, haga clic en **Standard**, **Legacy Hotspot** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Network Name.** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Hidden network (enable if network is open or off).** Seleccione si la red está oculta o no.
- **Auto Join (automatically join this wireless network).** Seleccione si se conecta a la red automáticamente o no. El valor predeterminado es **ON**.
- **Security type.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - None. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

WPA, WPA Personal, WPA 2 Personal, Any (Personal)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Any (Enterprise)

- **Use as a Login Window configuration.** Seleccione si utilizar las mismas credenciales especificadas en la ventana de inicio de sesión para autenticar al usuario.
- **Parámetros del servidor proxy**
  - **Proxy configuration.** En la lista, haga clic en None, Manual o Automatic para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es None, que no requiere ninguna configuración adicional.
  - Si hace clic en **Manual**, configure los siguientes parámetros:
    - **Hostname/IP address.** Escriba el nombre o la dirección IP de host del servidor proxy.
    - **Port.** Escriba el número de puerto del servidor proxy.
    - **User name.** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
    - **Password.** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
  - Si hace clic en **Automatic**, configure los siguientes parámetros:
    - **Server URL.** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
    - **Allow direct connection if PAC is unreachable.** Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **ON**. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.
- **Configuraciones de directivas**
  - Junto a **Remove policy**, haga clic en **Select date** o en **Duration until removal (in days)**.
  - Si hace clic en **Select date**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Allow user to remove policy**, haga clic en **Always**, **Password required** o **Never**.

- Si hace clic en **Password required**, junto a **Removal password**, escriba la contraseña en cuestión.
- Junto a **Profile scope**, haga clic en **User** o en **System**. El valor predeterminado es **User**. Esta opción está disponible para OS X 10.7 y versiones posteriores.

### Configuración de los parámetros de Android

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'WiFi Policy' and contains a sidebar with a list of platforms: iOS, Mac OS X, Android (selected), Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main configuration area includes fields for 'Network name', 'Authentication' (set to 'Open'), 'Encryption' (set to 'WEP'), and 'Password'. There is also a 'Hidden network' toggle set to 'OFF'. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Network name.** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Authentication.** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - Compartida
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

- Open, Shared
- WPA, WPA-PSK, WPA2, WPA2-PSK
- 802.1x

- **Hidden network (Enable if network is open or off).** Seleccione si la red está oculta o no.

### Configuración de los parámetros de Windows Phone

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

iOS

Mac OS X

Android

Windows Phone

Windows Desktop/Tablet

Windows Mobile/CE

**3 Assignment**

**Network name\***  ⓘ

**Authentication**

**Encryption**

**EAP Type**

**Connect if hidden**  OFF

**Connect automatically**  ON

**Push certificate via SCEP**  ON

**Credential provider for SCEP\***

**Proxy server settings**

**Host name or IP address**

**Port**

Configure estos parámetros:

- **Network name.** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Authentication.** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise: Para la versión más reciente de Windows 10, el uso de WPA-2 Enterprise requiere que se configure el protocolo SCEP, de modo que XenMobile pueda 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](#).

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

**XenMobile** Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**OS version\*** 10

**Network name\*** WiFi\_24G

**Authentication** WPA-2 Enterprise

**Encryption** AES

**EAP Type** PEAP-MSCHAPv2

**Hidden network (enable if network is open or off)** OFF

**Connect automatically** ON

**Enable SCEP?** ON

**Credential provider for SCEP\*** certsrv-cpwifi

**Proxy server settings**

**Host name or IP address**

**Port**

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

- **Authentication.** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise: Para la versión más reciente de Windows 10, el uso de WPA-2 Enterprise requiere que se configure el protocolo SCEP, de modo que XenMobile pueda 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](#).

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

- Abierta
- WPA Personal, WPA-2 Personal
- WPA-2 Enterprise

### Configuración de Windows 8.1

- **Network name.** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Authentication.** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión WiFi.
  - Abierta
  - WPA personal
  - WPA2 personal
  - WPA de empresa
  - WPA2 de empresa
- **Hidden network (Enable if network is open or off).** Seleccione si la red está oculta o no.
- **Connect automatically.** Seleccione si establecer conexión con la red de forma automática.

Configuración de Windows Mobile/CE

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**WiFi Policy**

**Network name\***

**Device-to-device connection (ad-hoc)**  OFF

**Network**

**Authentication**

**Encryption**

**Key provided (automatic)**  OFF

**Password**

**Key index**

**Deployment Rules**

[Back](#) [Next >](#)

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**.
- **Red:** 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, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Abierta

WPA Personal, WPA-2 Personal

WPA-2 Enterprise

- **Key provided (automatic):** Seleccione si la clave se suministra automáticamente o no. La opción predeterminada es **Off**.
- **Password:** Introduzca aquí la contraseña.
- **Key index:** Indique el índice de la clave. Las opciones disponibles son de 1, 2, 3 y 4.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de **WiFi Policy Assignment**.

8. Haga clic en **Next**. Aparecerá la página WiFi Policy **Assignment**.

8. Haga clic en **Next**. Aparecerá la página WiFi Policy **Assignment**.

8. Haga clic en **Next**. Aparecerá la página WiFi Policy **Assignment**.

The screenshot shows the XenMobile configuration interface for a WiFi Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'WiFi Policy' and includes a description: 'This policy lets you configure a WiFi profile for devices.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked), 'DG-ex12', and 'DG-Testprise'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. At the bottom right, there are 'Back' and 'Save' buttons.

9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

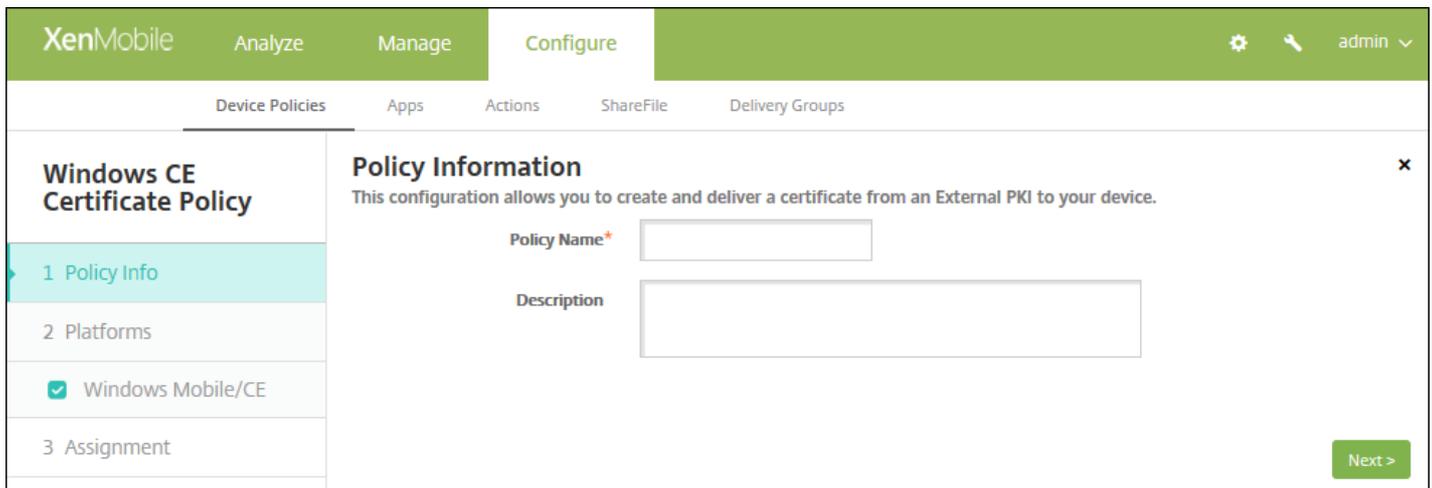
11. Haga clic en **Save**.

# Directiva de certificados de Windows CE

Mar 02, 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**.



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Windows CE Certificate Policy' and contains a 'Policy Information' section. This section includes a description: 'This configuration allows you to create and deliver a certificate from an External PKI to your device.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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 **Siguiente**. Aparecerá la página de información **Windows CE Certificate Policy Platform**.

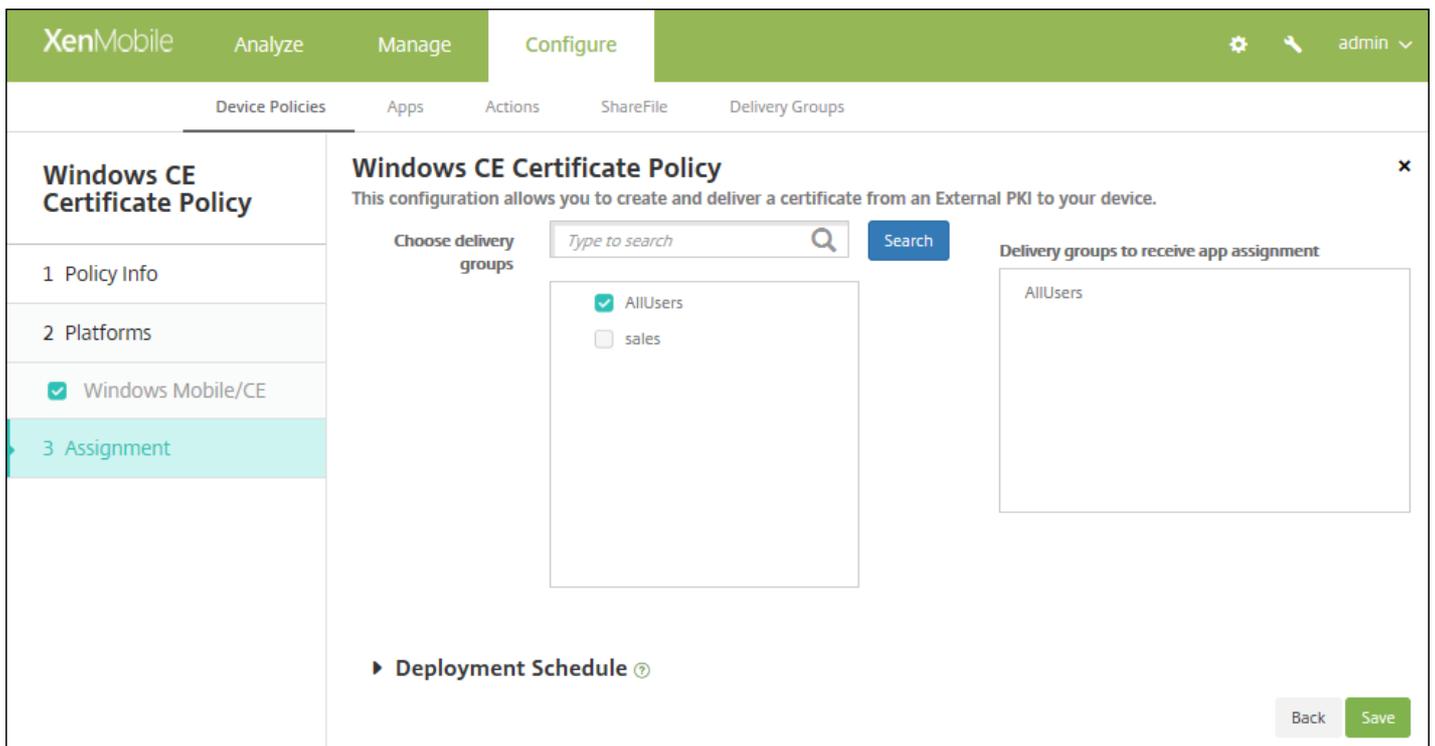
The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Windows CE Certificate Policy' and contains a sidebar with '1 Policy Info', '2 Platforms', '3 Assignment', and a checked 'Windows Mobile/CE' option. The main area has a 'Policy Information' section with the following fields: 'Credential Provider\*' (None), 'Password of generated PKCS#12\*' (empty), 'Destination folder' (%My Documents%), and 'Destination file name\*' (empty). There is also a 'Deployment Rules' section with a right-pointing arrow. At the bottom right, there are 'Back' and 'Next >' buttons.

6. Configure los siguientes parámetros:

- **Credential provider.** En la lista, haga clic en el proveedor de credenciales. El valor predeterminado es **None**.
- **Password of generated PKCS#12.** Escriba la contraseña utilizada para cifrar la credencial.
- **Destination folder.** En la lista, haga clic en la carpeta de destino de la credencial, o bien haga clic en **Add new** para agregar una carpeta que no esté ya en la lista. Las opciones predeterminadas son:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name.** Escriba el nombre del archivo de credenciales.

7. Configure las reglas de implementación.

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **Windows CE Certificate Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directiva de dispositivo XenMobile Store

Mar 02, 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**.

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Store Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is active, showing a 'Policy Information' dialog box. The dialog box has a title bar with a close button (X) and a subtitle: 'This policy specifies when devices display a Store webclip on the devices.' It contains two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area).

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**.

The screenshot shows the XenMobile configuration interface, similar to the previous one. The 'Store Policy' sidebar is still visible. The '2 Platforms' section is now active, showing a 'Store Policy' dialog box. The dialog box has a title bar with a close button (X) and a subtitle: 'This policy specifies when devices display a Store webclip on the devices.' It contains a toggle switch for 'iOS' which is currently turned 'ON'. Below this, there is a section titled 'Deployment Rules' with a right-pointing arrow.

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 **XenMobile Store Policy**.

10. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

11. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

#### Nota:

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

12. Haga clic en **Save**.

# Directivas de opciones de XenMobile

Mar 02, 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**.

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Device Policies' sub-tab is selected. The main content area is titled 'XenMobile Options Policy' and contains a 'Policy Information' section. This section includes a description and two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty, and the 'Description' field is also empty. On the left side, there is a sidebar with a tree view showing '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked items: 'Android' and 'Windows Mobile/CE'. At the bottom right, there is a 'Next >' button.

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 **Siguiente**. Aparecerá la página **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de Android

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'XenMobile Options Policy' and contains a sidebar with '1 Policy Info', '2 Platforms' (with 'Android' and 'Windows Mobile/CE' selected), and '3 Assignment'. The main configuration area includes 'Device agent configuration' with 'Traybar notification - hide traybar icon' set to OFF, 'Connection time-out(s)\*' set to 20, and 'Keep-alive interval(s)\*' set to 120. The 'Remote support' section has 'Prompt the user before allowing remote control' set to OFF and 'Before a file transfer' set to 'Do not warn the user'. A 'Deployment Rules' section is also present. At the bottom right, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Traybar notification - hide traybar icon.** Seleccione si el icono de la barra de la bandeja será visible o no. El valor predeterminado es **OFF**.
- **Connection: time-out(s).** Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor predeterminado es de 20 segundos.
- **Keep-alive interval(s).** Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
- **Prompt the user before allowing remote control.** Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. El valor predeterminado es **OFF**.
- **Before a file transfer.** En la lista, haga clic en si se debe avisar al usuario sobre una transferencia de archivo o si se pide permiso al usuario. Los valores disponibles son **Do not warn the user**, **Warn the user** y **Ask for user permission**. El valor predeterminado es **Do not warn the user**.

Configuración de los parámetros de Windows Mobile/CE

The screenshot displays the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure' (which is active). Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows 'XenMobile Options Policy' with a sub-menu for 'Platforms' where 'Android' and 'Windows Mobile/CE' are checked. The main area is titled 'XenMobile Options Policy' and contains the following settings:

- Device agent configuration:**
  - XenMobile backup configuration: Disabled (dropdown)
  - Connect to the office network: ON (toggle)
  - Connect to the Internet network: ON (toggle)
  - Connect to the built-in office network: ON (toggle)
  - Connect to the built-in Internet network: ON (toggle)
  - Traybar notification - hide traybar icon: OFF (toggle)
  - Connection time-out(s)\*: 20 (input field)
  - Keep-alive interval(s)\*: 120 (input field)
- Remote support:**
  - Prompt the user before allowing remote control: OFF (toggle)
  - Before a file transfer: Do not warn the user (dropdown)
- Deployment Rules:** (indicated by a right-pointing arrow)

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

Configure estos parámetros:

- **Device agent configuration**

- **XenMobile backup configuration.** En la lista, haga clic en una opción para la copia de seguridad de la configuración de XenMobile en los dispositivos de los usuarios. El valor predeterminado es **Disabled**. Las opciones disponibles son:
  - Inhabilitado
  - At first connection after XenMobile installation
  - At first connection after each device reboot
- **Connect to the office network**
- **Connect to the Internet network**
- **Connect to the built-in office network:** Cuando esta opción tiene el valor **ON**, XenMobile detecta automáticamente la red.
- **Connect to the built-in Internet network:** Cuando esta opción tiene el valor **ON**, XenMobile detecta automáticamente la red.
- **Traybar notification - hide traybar icon.** Seleccione si el icono del área de notificaciones será visible o no. El valor predeterminado es **OFF**.
- **Connection time-out(s).** Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor predeterminado es de 20 segundos.
- **Keep-alive interval(s).** Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor

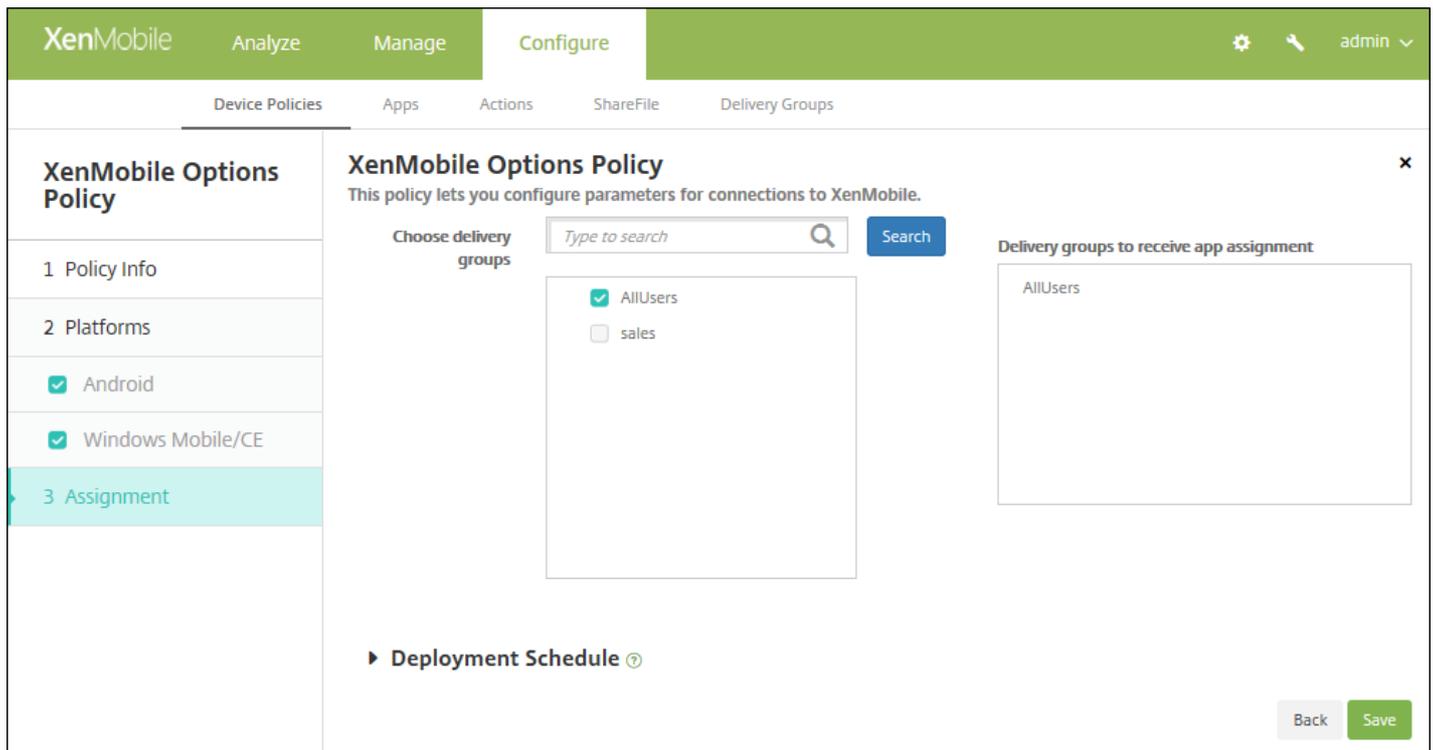
predeterminado es de 120 segundos.

- **Remote support**

- **Prompt the user before allowing remote control.** Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. El valor predeterminado es **OFF**.
- **Before a file transfer.** En la lista, haga clic en si se debe avisar al usuario sobre una transferencia de archivo o si se pide permiso al usuario. Los valores disponibles son **Do not warn the user**, **Warn the user** y **Ask for user permission**. El valor predeterminado es **Do not warn the user**.

7. Configure las reglas de implementación. ▼

8. Haga clic en **Siguiente**. Aparecerá la página de asignación **XenMobile Options Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Directivas de desinstalación de XenMobile

Mar 02, 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**.

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'XenMobile Uninstall Policy' and contains a 'Policy Information' section. This section has a description: 'This policy lets you choose to uninstall XenMobile on Android, Windows Mobile, and Windows CE devices upon deployment of the policy.' Below the description are two input fields: 'Policy Name\*' and 'Description'. To the left of the main content is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is highlighted. Under '2 Platforms', there are two checkboxes: 'Android' and 'Windows Mobile/CE', both of which are checked. At the bottom right of the main content area, there is a green 'Next >' button.

4. En el panel **Policy Information**, escriba la información siguiente:

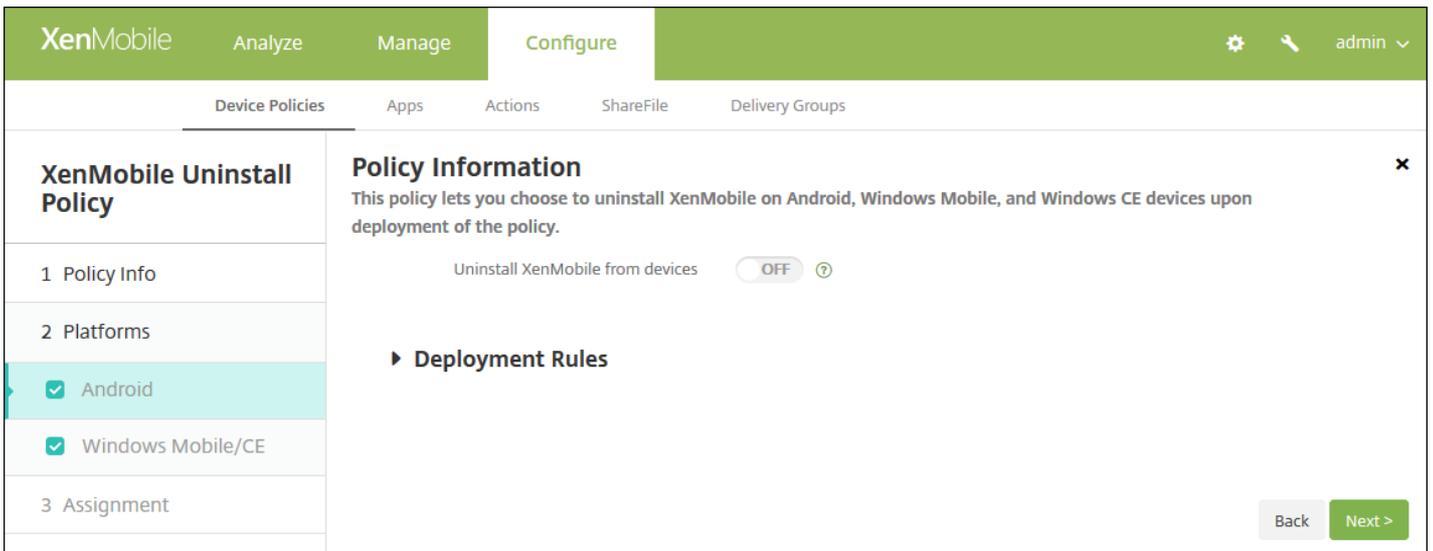
- **Policy Name**. Escriba un nombre descriptivo para la directiva.
- **Description**. Si quiere, escriba una descripción de la directiva.

5. Haga clic en **Siguiente**. Aparecerá la página de información **Policy Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 7 para la configuración de las reglas de implementación de esa plataforma.

Configuración de los parámetros de Android y Windows Mobile/CE

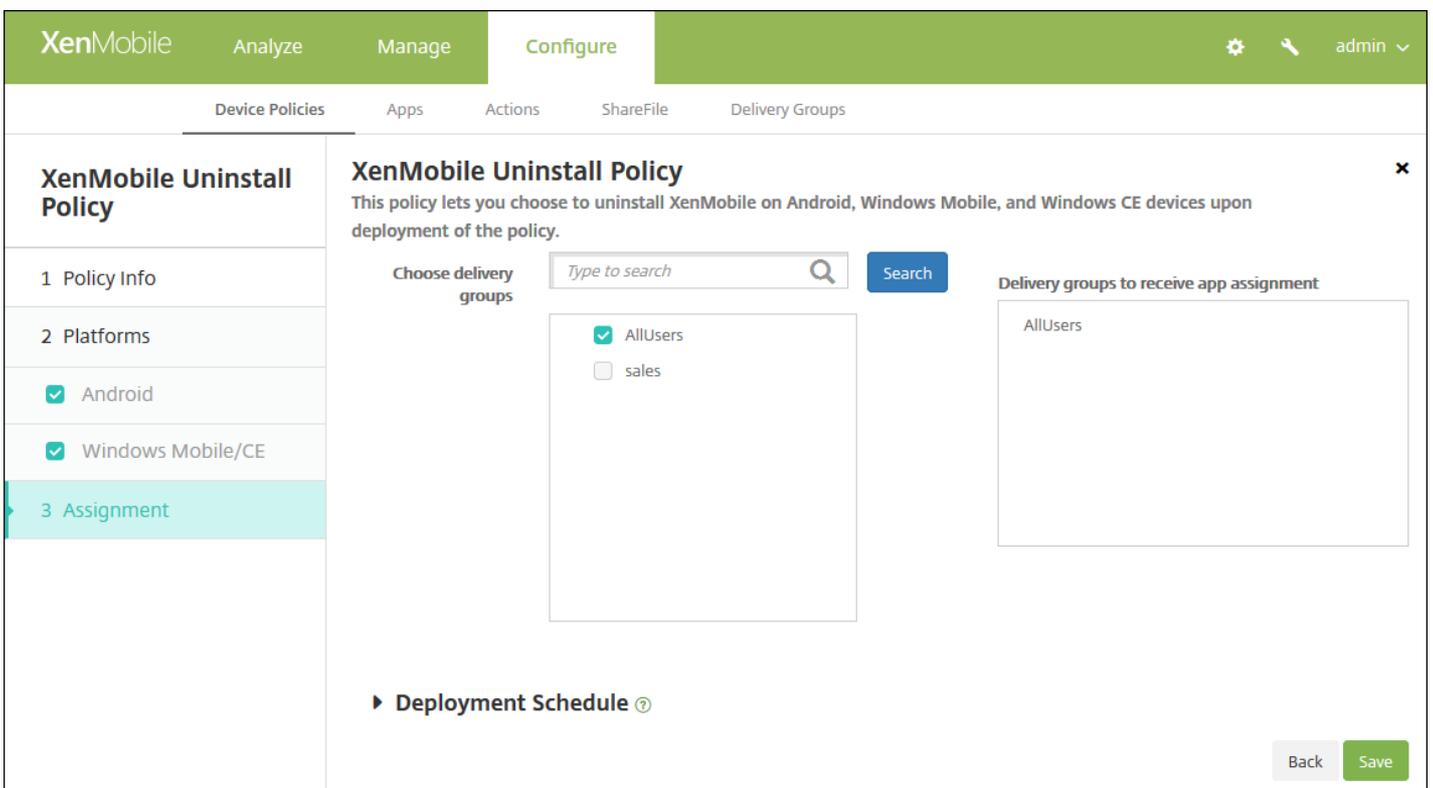


Configure este parámetro para cada plataforma seleccionada:

- **Uninstall XenMobile from devices.** Seleccione si quiere desinstalar XenMobile de todos los dispositivos en los que se implementará esta directiva. El valor predeterminado es **OFF**.

7. Configure las reglas de implementación.

8. Haga clic en **Next**. Aparecerá la página de asignación **XenMobile Uninstall Policy**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o

varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

# Incorporación de aplicaciones

Mar 02, 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 elegir las de un conjunto de conectores de aplicaciones para el acceso Single Sign-On en aplicaciones Web existentes. Por ejemplo, GoogleApps\_SAML.
- **Enterprise.** Estas aplicaciones son aplicaciones nativas que no están empaquetadas con la herramienta MDX Toolkit y no contienen las directivas asociadas a aplicaciones MDX.
- **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, sino que las aplicaciones se instalan de forma silenciosa en segundo plano. Debe cumplir estos requisitos previos para poder implementar la instalación silenciosa:

- Para las aplicaciones iOS, el dispositivo iOS administrado debe estar en modo supervisado. Para obtener más información, consulte [Directivas de importación de perfiles de iOS y Mac OS X](#).
- Para las aplicaciones Android, las directivas de Samsung for Enterprise (SAFE) o KNOX deben estar habilitadas en el dispositivo. Para ello, configure la directiva de clave de licencia de MDM de Samsung para que genere claves de licencia ELM y KNOX de Samsung. Para obtener más información, consulte [Directivas de claves de licencia para la administración de dispositivos móviles \(MDM\) Samsung](#).

## Funcionamiento de las aplicaciones MDX para móviles

XenMobile respalda aplicaciones iOS, Mac OS X, Android y Windows, incluidas las aplicaciones 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 [Agregar una aplicación MDX](#).

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, Mac OS X, Android y Windows con las directivas y la lógica de Citrix. Esta herramienta puede empaquetar de forma segura tanto una aplicación creada dentro de la organización como una aplicación creada fuera.

## Funcionamiento de las aplicaciones Web y SaaS

XenMobile viene con un conjunto de conectores de aplicaciones, que son plantillas que se pueden configurar para Single Sign-on (SSO) en aplicaciones Web y SaaS y, en algunos casos, para la creación y administración de cuentas de usuario. XenMobile incluye conectores SAML (Security Assertion Markup Language). Los conectores SAML se utilizan para aplicaciones Web que admiten el protocolo SAML para la autenticación SSO y la administración de cuentas de usuario. XenMobile es compatible con SAML 1.1 y SAML 2.0.

También puede crear sus propios conectores SAML de empresa.

Para obtener más información, consulte [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 [Agregar una aplicación de empresa](#).

## 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 [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 [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**.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM	
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM	
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM	
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM	
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM	
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM	
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM	
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM	
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM	

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **MDX**. Aparecerá la página **MDX App Information**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, showing a sidebar with 'MDX' and a list of steps: '1 App Information' (highlighted), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main area is titled 'App Information' and contains the following fields:

- Name\***: A text input field with a help icon.
- Description**: A text area with a help icon.
- App category**: A dropdown menu currently set to 'All Selected'.

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 **Siguiente**. Aparecerá la página **App Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 11 para la configuración de las reglas de implementación de esa plataforma.

7. Debe seleccionar un archivo MDX para cargarlo. Para ello, haga clic en **Upload** y vaya a la ubicación del archivo.

- Si quiere agregar una aplicación VPP B2B de iOS, haga clic en **Your application is a VPP B2B application?** y, en la lista, haga clic en la cuenta B2B del programa VPP que se va a utilizar.

8. Haga clic en **Siguiente**. Aparecerá la página de datos detallados de la aplicación.

9. Configure los siguientes parámetros:

- **File name.** Escriba el nombre del archivo asociado a la aplicación.
- **App Description.** Escriba una descripción de la aplicación.
- **App version.** Si quiere, escriba el número de versión de la aplicación.
- **Minimum OS version.** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Maximum OS version.** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.

- **Excluded devices.** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
- **Remove app if MDM profile is removed.** Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es **ON**.
- **Prevent app data backup.** Seleccione si quiere impedir que los usuarios realicen copias de seguridad de los datos de la aplicación. El valor predeterminado es **ON**.
- **Force app to be managed.** Si se instala una aplicación no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos no supervisados. El valor predeterminado es **ON**. Disponible en iOS 9.0 y versiones posteriores.

10. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos, requisitos de red, otros accesos, cifrado, interacción de las aplicaciones, restricciones de aplicaciones, acceso de las aplicaciones a la red, registros de las aplicaciones y geovallas de las aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener más información acerca de directivas de aplicaciones referentes a aplicaciones MDX, incluida una tabla en la que se muestran las directivas para cada plataforma, consulte [Vista general de las directivas MDX](#).

#### 11. Configure las reglas de implementación.



12. Expanda **XenMobile Store Configuration**.

**▼ Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

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. El valor predeterminado es **ON**.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

13. Haga clic en **Next**. Aparecerá la página **Approvals**.

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, and the 'Apps' tab is selected. The main content area displays the configuration for an application named 'MDX'. The 'Approvals (optional)' section is highlighted, showing a dropdown menu for 'Workflow to Use' set to 'None'. The left sidebar shows a list of configuration steps: 1 App Information, 2 Platform, 3 Approvals (optional), and 4 Delivery Group Assignments (optional). The 'Platform' section is expanded, showing checkboxes for 'iOS', 'Android', 'Windows Phone', and 'Windows Desktop/Tablet', with 'Windows Phone' and 'Windows Desktop/Tablet' selected.

Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 15.

Configure esta opción si necesita asignar o crear un flujo de trabajo:

- **Workflow to Use.** En la lista, haga clic en un flujo de trabajo existente o en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name.** Escriba un nombre único para el flujo de trabajo.
  - **Description.** Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates.** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval.** En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es 1 level. Las opciones posibles son:

- Not Needed
- 1 level
- 2 levels
- 3 levels
- **Select Active Directory domain.** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Find additional required approvers.** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
- Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
  - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:
    - Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
    - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
    - Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

14. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' sub-tab is selected, and the 'MDX' app is being configured. The main content area is titled 'Delivery Group Assignments (optional)' and includes a search bar for delivery groups. A list of delivery groups is shown with checkboxes: 'AllUsers' (checked) and 'OA DG for Mac users' (unchecked). To the right, a box titled 'Delivery groups to receive app assignment' contains 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a question mark icon.

15. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

16. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción

predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.

- Junto a "Deployment schedule", haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

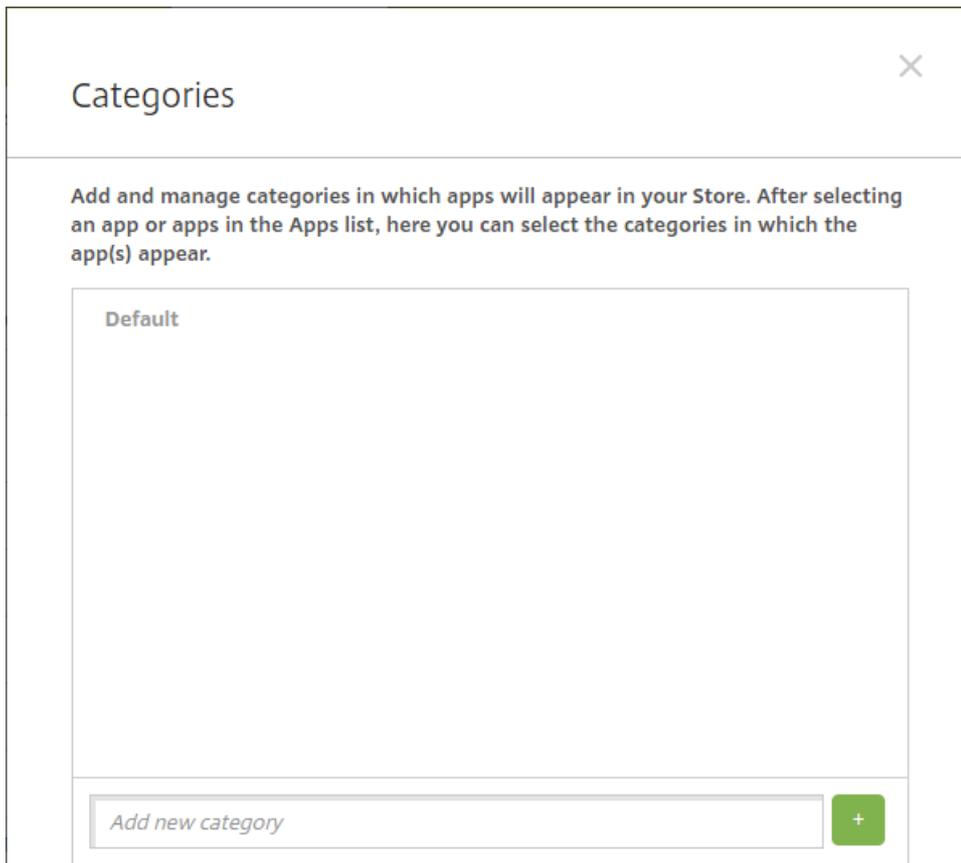
17. Haga clic en **Save**.

## 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.

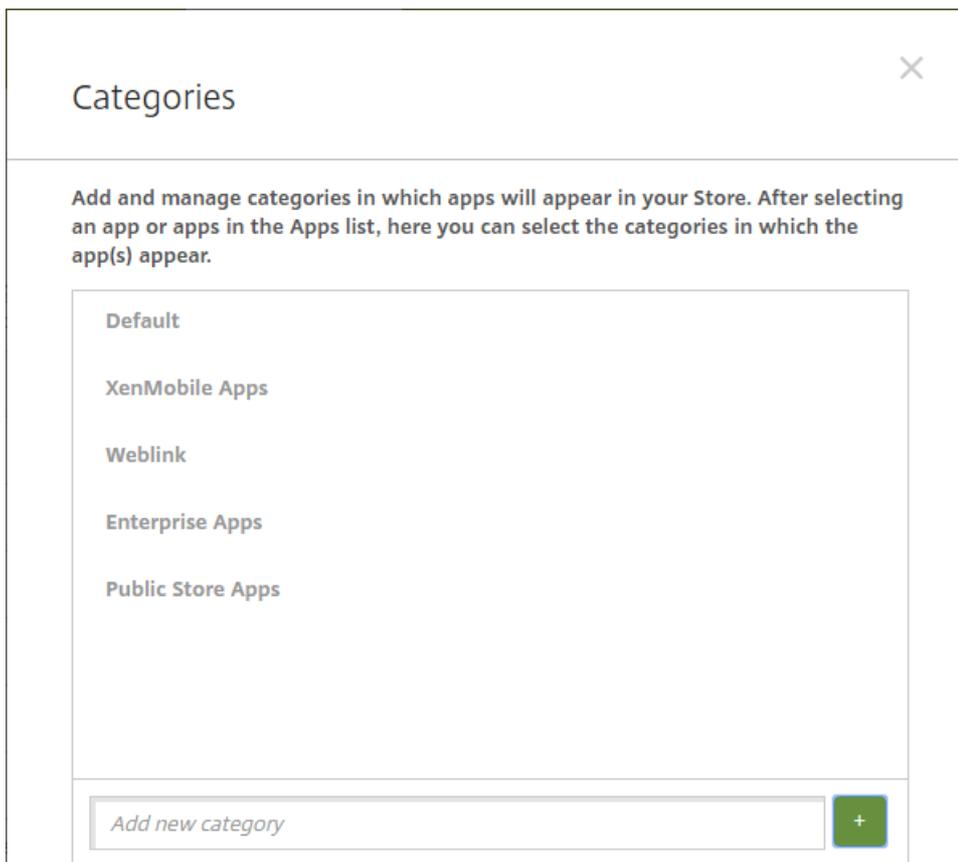
Las categorías se configuran en la página **Apps** de la consola de XenMobile. A continuación, al configurar o modificar una aplicación, un enlace Web o una tienda, puede agregarlos a una de las categorías que haya configurado.

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 Groups Assignments** o haga clic en **Next** en las páginas restantes de la configuración de la aplicación.
  - Haga clic en **Save** en la página **Delivery Groups Assignments** para aplicar la nueva categoría. La nueva categoría se aplicará a la aplicación y aparecerá en la tabla **Apps**.

## Cómo agregar de 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**.

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

**Apps** [Show filter](#)

[Add](#) | [Category](#) | [Export](#)

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM		
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM		
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM		
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM		
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM		
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM		
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM		
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM		
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM		

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.

### Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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 bajo **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 **Siguiente**. Aparecerá la página **App Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 10 para la configuración de las reglas de implementación de esa plataforma.

7. Seleccione la aplicación que quiera agregar. Para ello, escriba el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Search**. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. En la siguiente imagen, se muestran los resultados de la búsqueda de "podio".

The screenshot shows the XenMobile 'Configure' page. The 'Public App Store' section is active, and the 'Platform' step is expanded to show 'iPhone' selected. A search bar contains the text 'podio' and a 'Search' button. Below the search bar, the results for 'podio' in iPhone apps are displayed, showing two app cards: 'Podio Podio' and 'Podio Chat Podio'. A message below the results says 'Didn't find the app you were looking for?'.

8. Haga clic en la aplicación que quiera agregar. Los campos **App Details** aparecerán ya rellenos con información relativa a la aplicación seleccionada (incluido el nombre, la descripción, el número de versión y la imagen asociada).

## App Details

The screenshot shows the 'App Details' configuration interface. It includes the following fields and controls:

- Name\***: Text input field containing 'Podio'.
- Description\***: Text area containing 'The ultimate companion app for Podio – enabling you to run your projects and collaborate with your team from anywhere.' and 'Take your content and conversations with you, no matter where your workday takes you.'
- Version**: Text input field containing '5.0.1'.
- Image**: Image selection icon.
- Paid app**: Toggle switch set to 'OFF'.
- Remove app if MDM profile is removed**: Toggle switch set to 'ON'.
- Prevent app data backup**: Toggle switch set to 'ON'.
- Force app to be managed**: Toggle switch set to 'OFF' with an information icon.
- Force license association to device**: Toggle switch set to 'ON'.

Navigation buttons: 'Back' (grey) and 'Next >' (green).

### 9. Configure los siguientes parámetros:

- Si fuera necesario, cambie el nombre y la descripción de la aplicación.
- **Paid app**. Este campo está preconfigurado y no se puede cambiar.
- **Remove app if MDM profile is removed**. Seleccione si quiere quitar la aplicación cuando se quite el perfil de MDM. El valor predeterminado es **ON**.
- **Prevent app data backup**. Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es **ON**.
- **Force app to be managed**. Si se instala una aplicación no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos no supervisados. El valor predeterminado es **OFF**. Disponible en iOS 9.0 y versiones posteriores.
- **Force license to association to device**. Seleccione si quiere asociar una aplicación (desarrollada con la opción de asociación a un dispositivo habilitada) a un dispositivo en lugar de a un usuario. Disponible en iOS 9 y versiones posteriores. Si la aplicación que ha elegido no admite la asignación a un dispositivo, este campo no se puede cambiar.

### 10. Configure las reglas de implementación.

### 11. Expanda **XenMobile Store Configuration**.

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

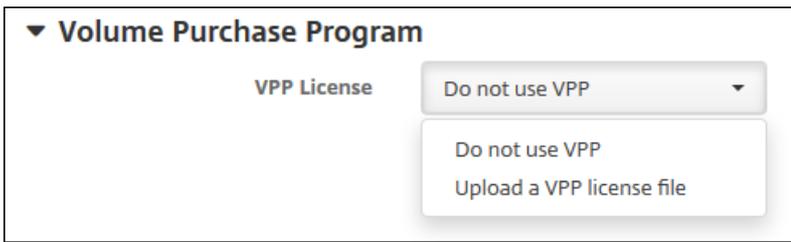
Allow app comments

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. El valor predeterminado es ON.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada.

12. Expanda **Volume Purchase Program** o, en el caso de Android for Work, expanda **Bulk Purchase**.

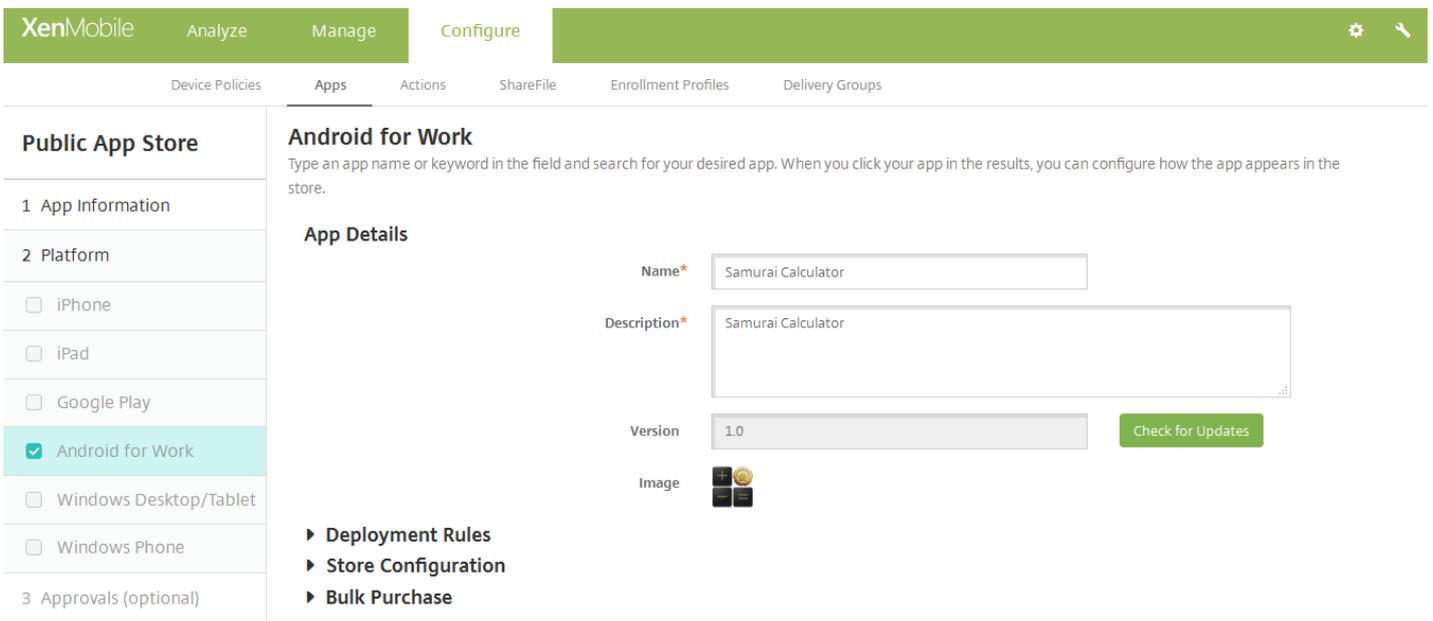
Para el programa Volume Purchase Program de compras por volumen, complete los pasos siguientes.



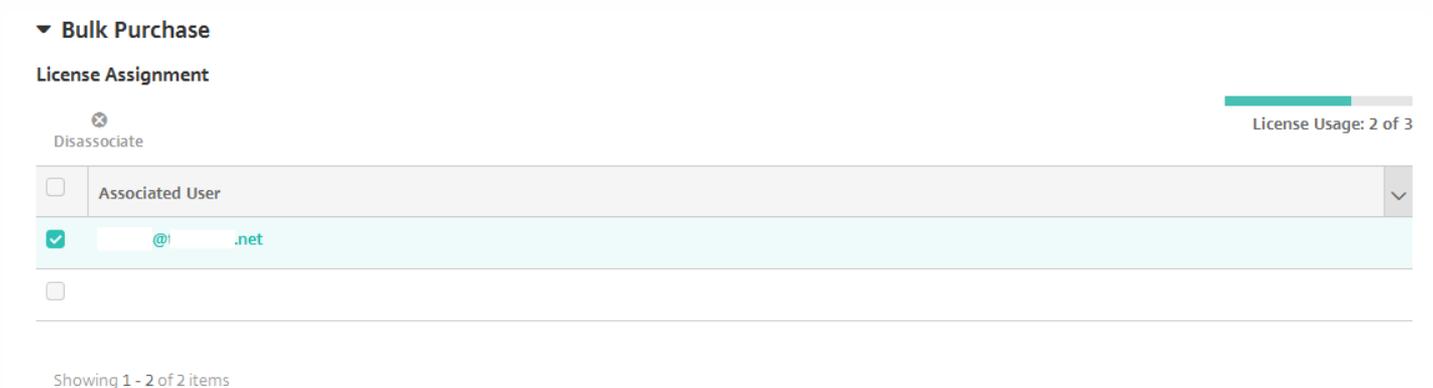
a. En la lista **VPP license**, haga clic en **Upload a VPP license file** si quiere habilitar XenMobile para aplicar una licencia de VPP para la aplicación.

b. En el cuadro de diálogo que aparece, importe la licencia.

Para las compras en bloque de Android for Work, expanda la sección **Bulk Purchase**.



En la tabla License Assignment verá cuántas licencias se están utilizando actualmente para la aplicación del total de licencias disponibles. Puede seleccionar un usuario y hacer clic en **Disassociate** para poner fin a su asignación de licencia y liberar esa licencia para otro usuario. No obstante, 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 **Siguiente**. 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 en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name**. Escriba un nombre único para el flujo de trabajo.
  - **Description**. Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates**. En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval**. En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**. En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers**. Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
    - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:
      - Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
      - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
      - Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

14. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.

15. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

16. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.

- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

17. Haga clic en **Save**.

## 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 se 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**.

## Add App ×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **Web & SaaS**. Aparecerá la página **App Information**.

The screenshot shows the XenMobile interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', 'Configure', and a user profile 'administrator'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, and the 'Web & SaaS' section is selected in the left sidebar. The main content area is titled 'App Information' and contains the following elements:

- A sub-header: 'Add a Web & SaaS app, or choose one from the app index.'
- 'App Connector' section with two radio buttons:
  - Choose from existing connectors
  - Create a new connector
- 'App Connectors' section with a search bar containing the text 'Type to search or type an app' and a 'Search' button.
- A list of app connectors with their names and counts:
 

Connector Name	Count
E	1
EchoSign_SAML	
G	3
GoogleApps_SAML	
GoogleApps_SAML_IDP	
Globoforce_SAML	
L	1

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 es necesario, escriba el nombre de dominio de la aplicación. Este campo es obligatorio.
- **App is hosted in internal network.** Seleccione si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si establece esta opción en **ON**, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway. El valor predeterminado es **OFF**.
- **App category.** En la lista, si quiere, haga clic en una categoría para aplicarla a la aplicación.
- **User account provisioning.** Seleccione si quiere crear cuentas de usuario para la aplicación. Si usa el conector Globoforce\_SAML, debe habilitar esta opción para garantizar una integración correcta del inicio de sesión SSO.
- Si habilita **User account provisioning**, configure los siguientes parámetros:
  - **Cuenta de servicio**
    - **App Name.** Escriba el nombre del administrador de la aplicación. Este campo es obligatorio.
    - **Password.** Escriba la contraseña del administrador. Este campo es obligatorio.
  - **Cuenta de usuario**
    - **When user entitlement ends.** En la lista, haga clic en la acción que se debe realizar cuando los usuarios ya no pueden acceder a la aplicación. El valor predeterminado es Disable account. Las opciones posibles son:
      - Disable account
      - Keep account
      - Remove account
  - **User Name Rule**
    - Para cada regla de nombre de usuario que quiera agregar, haga lo siguiente:
      - **User attributes.** En la lista, haga clic en el atributo de usuario que quiere agregar a la regla.
      - **Length (characters).** En la lista, haga clic en la cantidad de caracteres del atributo de usuario que se usarán en la regla de nombre de usuario. El valor predeterminado es **All**.
      - **Rule.** Cada atributo de usuario que agregue, se adjunta automáticamente a la regla de nombre de usuario.
- **Password Requirements**
  - **Length.** Escriba la longitud mínima de la contraseña de usuario. El valor predeterminado es **8**.
- **Caducidad de contraseñas**
  - **Validity (days).** Escriba la cantidad de días durante la cual la contraseña permanecerá válida. Cualquier valor entre **0** y **90** es válido. El valor predeterminado es 90.
  - **Automatically reset password after it expires.** Seleccione si quiere restablecer la contraseña automáticamente cuando esta caduque. El valor predeterminado es **OFF**. Si no habilita este campo, 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.

The screenshot shows the XenMobile 'Configure' interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, showing a sidebar with 'Web & SaaS' selected. The main content area is titled 'App Information' and contains the following fields and options:

- App Connector:** Radio buttons for 'Choose from existing connectors' and 'Create a new connector' (selected).
- Name\*:** Text input field.
- Description\*:** Text input field.
- Logon URL\*:** Text input field.
- SAML version:** Radio buttons for '1.1' (selected) and '2.0'.
- Entity ID\*:** Text input field.
- Relay state URL:** Text input field.
- Name ID format:** Radio buttons for 'Email Address' (selected) and 'Unspecified'.
- ACS URL\*:** Text input field.
- Image:** Radio buttons for 'Use default' (selected) and 'Upload your own app image'.

An 'Add' button is located at the bottom of the form.

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, podría ser <http://www.example.com/logon>. Este campo es obligatorio.
- **SAML version.** Seleccione **1.1** o **2.0**. El valor predeterminado es **1.1**.
- **Entity ID.** Escriba la identidad de la aplicación SAML.
- **Relay State URL.** Escriba la dirección Web de la aplicación SAML. Esta URL es la URL de respuesta de la aplicación.
- **Name ID format.** Seleccione **Email Address** o **Unspecified**. El valor predeterminado es **Email Address**.
- **ACS URL.** Escriba la URL del servicio de aserción de consumidor (ACS) del proveedor de identidades o de servicios. La URL del servicio ACS proporciona a los usuarios Single Sign-On (SSO).
- **Image.** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es Use default.
  - Si quiere cargar su propia imagen, haga clic en **Browse**, vaya a la ubicación del archivo y selecciónela. El archivo debe ser PNG. No puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.
  - Cuando haya terminado, haga clic en **Add**. Aparecerá la página **Details**.

5. Haga clic en **Siguiente**. Aparecerá la página **App Policy**.

The screenshot shows the XenMobile interface for configuring an App Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'App Policy' and contains the following settings:

- Device Security**
  - Block jailbroken or rooted:  ON
- Network Requirements**
  - WiFi required:  OFF
  - Internal network required:  OFF
  - Internal WiFi networks:

At the bottom, there is a section for 'Store Configuration' and two buttons: 'Back' and 'Next >'.

• Configure estos parámetros:

- **Seguridad del dispositivo**

- **Block jailbroken or rooted.** Seleccione si impedir que los dispositivos liberados por jailbreak o por root accedan a la aplicación. El valor predeterminado es **ON**.

- **Requisitos de la red**

- **WiFi required.** Seleccione si se necesita una conexión WiFi para ejecutar la aplicación. El valor predeterminado es **OFF**.

- **Internal network required.** Seleccione si se necesita una red interna para ejecutar la aplicación. El valor predeterminado es **OFF**.

- **Internal WiFi networks.** Si habilitó la opción para requerir WiFi, escriba las redes WiFi internas que se van a usar.

6. Expanda **XenMobile Store Configuration**.

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

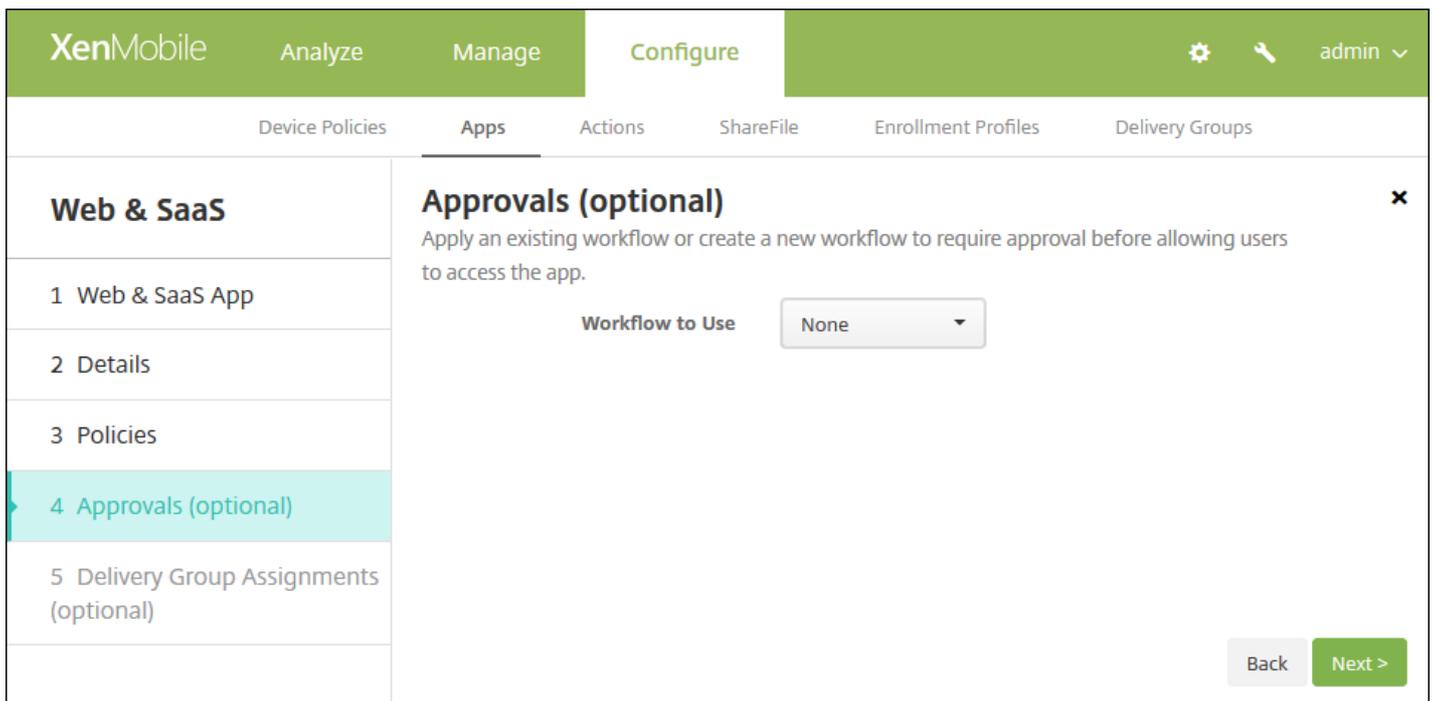
Allow app ratings

Allow app comments

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. El valor predeterminado es **ON**.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

7. Haga clic en **Next**. Aparecerá la página **Approvals**.



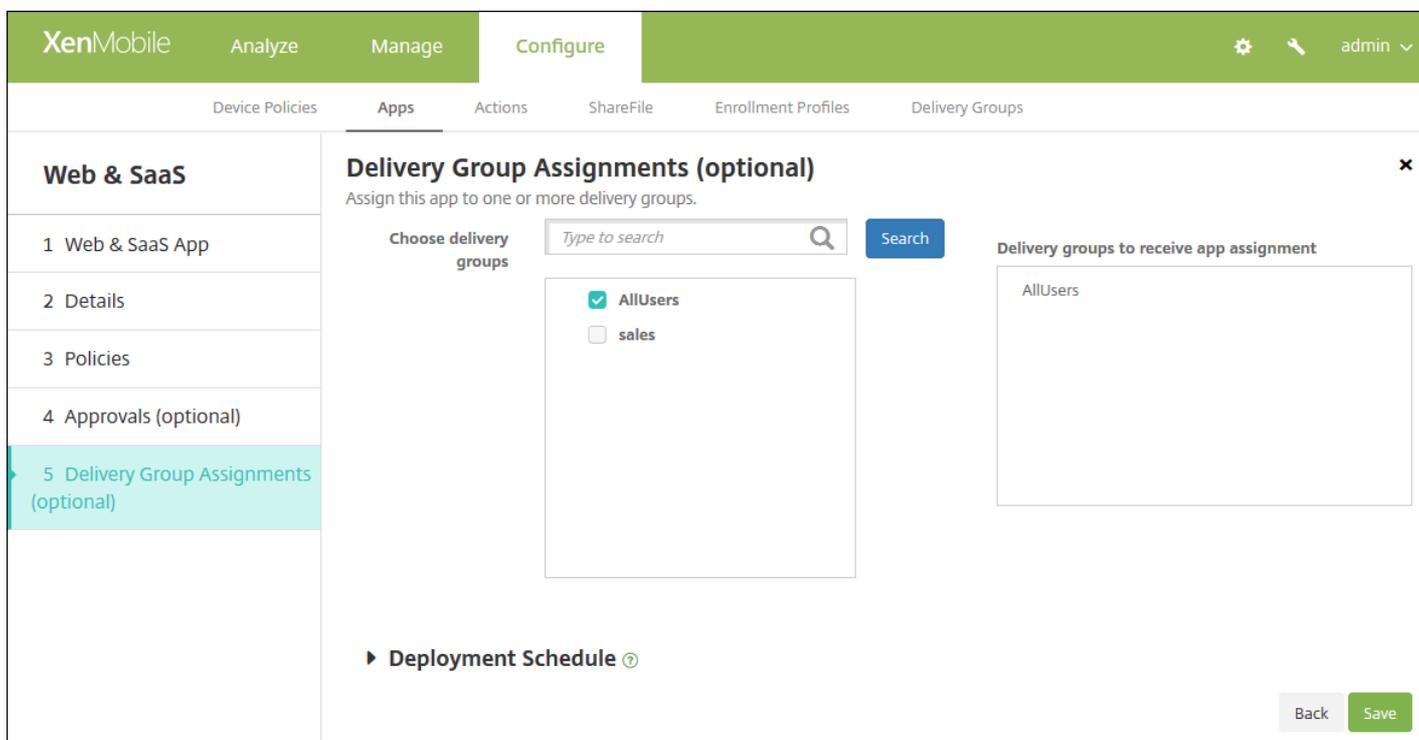
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 8.

Configure 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 en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name.** Escriba un nombre único para el flujo de trabajo.
  - **Description.** Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates.** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval.** En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain.** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers.** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
    - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:

- Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
- Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
- Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

8. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.



9. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

10. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se

realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

11. Haga clic en **Save**.

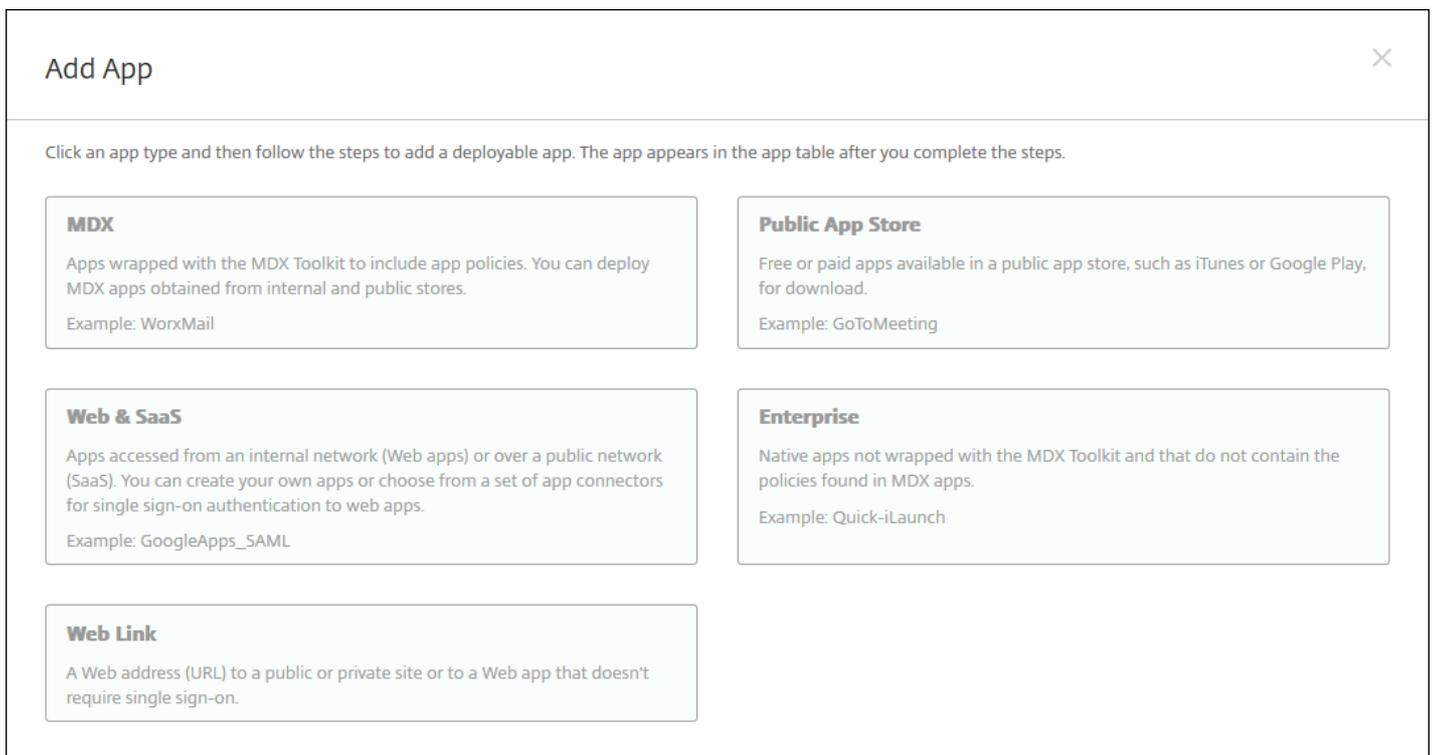
## Cómo agregar una aplicación de empresa

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 en la ficha **Apps** de la consola de XenMobile. Las aplicaciones de empresa admiten las siguientes plataformas (y sus tipos de archivo correspondientes):

- iOS (archivo .ipa)
- Android (archivo .apk)
- Samsung KNOX (archivo .apk)
- Android for Work (archivo .apk)
- Windows Phone (archivo .xap o .appx)
- Tableta Windows (archivo .appx)
- Windows Mobile/CE (archivo .cab)

1. En la consola de XenMobile, haga clic en **Configure > Apps**. Se abrirá la página **Apps**.

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.



3. Haga clic en **Enterprise**. Aparecerá la página **App Information**.

The screenshot shows the XenMobile interface with the 'Configure' tab selected. The 'App Information' form is open, displaying a sidebar with navigation options and a main form area. The sidebar includes 'Enterprise' and a list of steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main form area contains the following fields:

- Name\***: A text input field with a help icon.
- Description**: A larger text input field with a help icon.
- App category**: A dropdown menu currently set to 'Default'.

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 **Siguiente**. Aparecerá la página **App Platforms**.

6. En **Platforms**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

Cuando termine de configurar los parámetros de configuración para una plataforma, consulte el paso 10 para la configuración de las reglas de implementación de esa plataforma.

7. Elija un archivo que cargar por cada plataforma seleccionada. Para ello, haga clic en **Browse** y vaya a la ubicación del archivo.

8. Haga clic en **Siguiente**. 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 administra. Esta configuración se aplica a dispositivos iOS 9.x.

## 10. Configure las reglas de implementación.



### 11. Expanda **XenMobile Store Configuration**.

**▼ Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

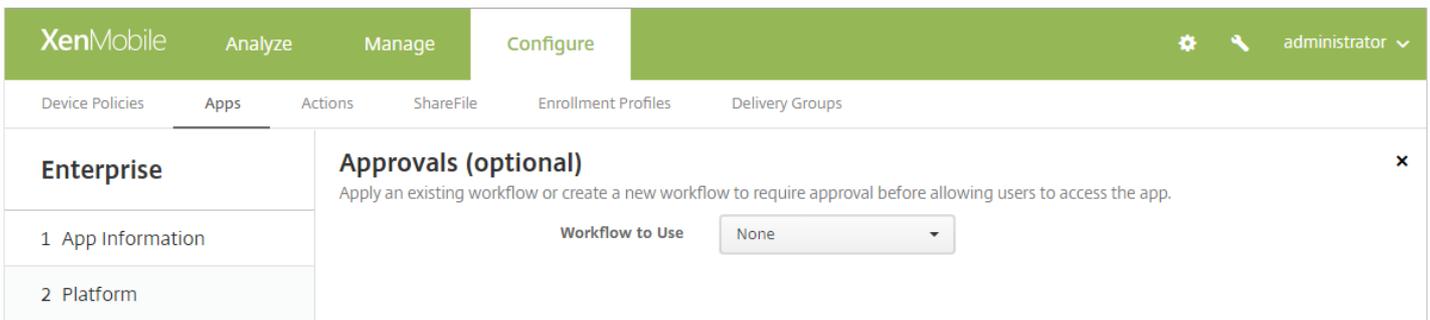
Allow app ratings

Allow app comments

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. El valor predeterminado es **ON**.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

12. Haga clic en **Next**. Aparecerá la página **Approvals**.



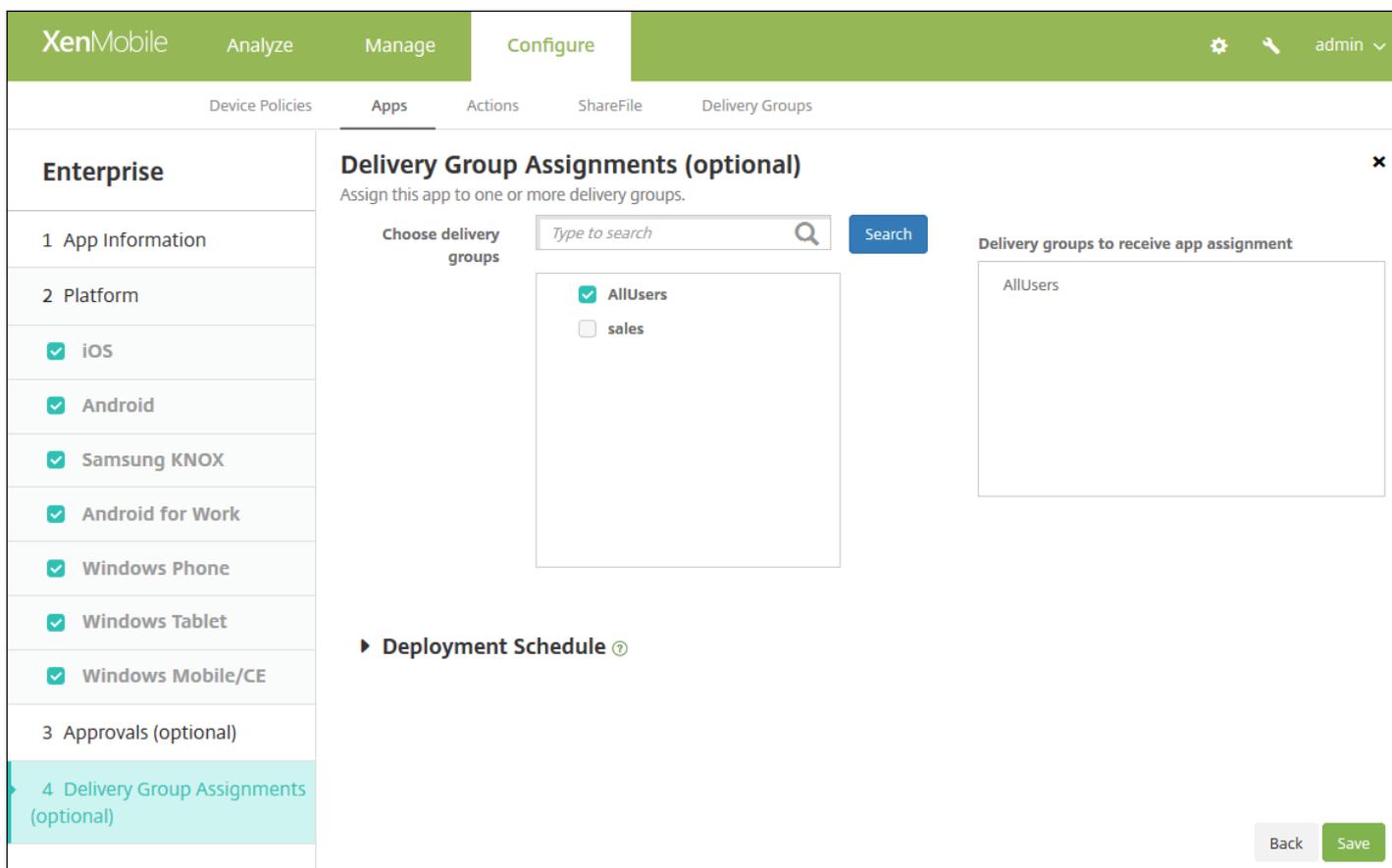
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 13.

Configure 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 en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name.** Escriba un nombre único para el flujo de trabajo.
  - **Description.** Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates.** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval.** En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain.** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers.** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
    - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:

- Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
- Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
- Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

13. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.



14. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

15. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

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 para el enlace
- Descripción del enlace
- Dirección Web (URL)
- Categoría
- Rol
- Imagen en formato PNG (optativo)

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

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add App**.

## Add App ×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **Web Link**. Aparecerá la página **App Information**.

4. Configure los siguientes parámetros:

- **App name.** Acepte el nombre que ya aparece o escriba uno nuevo.
- **App description.** Acepte la descripción que ya aparece o escriba una propia.
- **URL.** Acepte la URL que ya aparece o escriba la dirección Web de la aplicación. Según el conector que elija, este campo puede contener un marcador de posición que se debe reemplazar antes de pasar a la siguiente página.
- **App is hosted in internal network.** Seleccione si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si establece esta opción en **ON**, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway. El valor predeterminado es **OFF**.
- **App category.** En la lista, si quiere, haga clic en una categoría para aplicarla a la aplicación.
- **Image.** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es Use default.
  - Si quiere cargar su propia imagen, haga clic en **Browse**, vaya a la ubicación del archivo y selecciónela. El archivo debe ser PNG. No puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

5. Expanda **XenMobile Store Configuration**.

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings  ON

Allow app comments  ON

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. El valor predeterminado es **ON**.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

6. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.

7. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**.

8. Expanda **Deployment Schedule** y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

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.

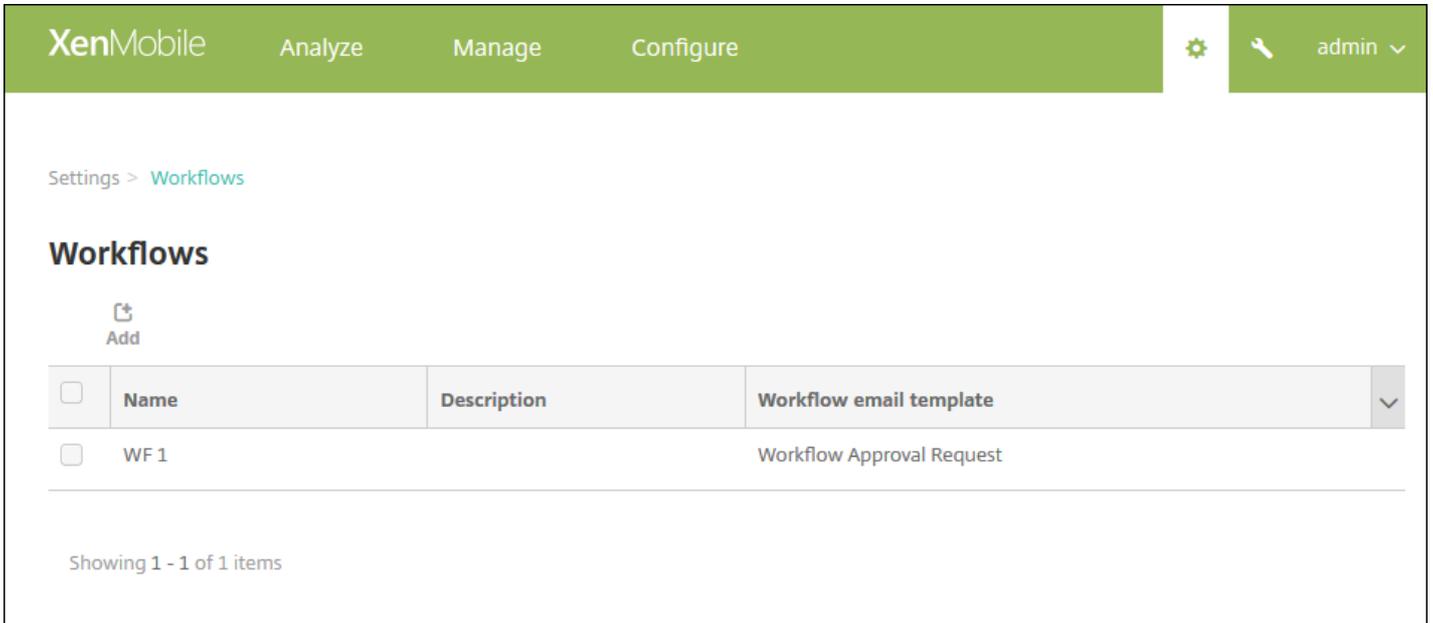
Puede configurar flujos de trabajo en dos lugares de XenMobile:

- 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**.

XenMobile Analyze Manage Configure ⚙️ 🔑 admin ▾

Settings > Workflows > Add Workflow

## Add Workflow

**Name\***

**Description**

**Email Approval Templates** Workflow Approval Request

**Levels of manager approval** 1 level ▾

**Select Active Directory domain** agsag.com ▾

**Find additional required approvers**

**Selected additional required approvers**

4. 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. 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.

## Workflow Approval Request ✕

To modify the workflow template, please go to the notification template section in Settings.

---

Email Title	Workflow Approval Request for an Application
Email Content	Please approve the application \${applicationName} for your staff by clicking the following link. Thank you for spending the time to approve the application.

Close

- **Levels of manager approval.** En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es 1 level. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain.** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers.** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en Search. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
    - Para quitar a una persona de la lista **Selected additional required approvers**, realice una de las siguientes acciones:
      - Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.
      - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
      - Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.
5. Haga clic en **Save**. El flujo de trabajo creado aparecerá 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 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

Mar 02, 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 crear su propio conector en XenMobile al agregar 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		<b>Nota:</b> Al utilizar este conector, debe habilitar la opción User Management for Provisioning para una correcta integración del inicio de sesión seguro.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

# Actualización de aplicaciones MDX o de empresa

Mar 02, 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.

The screenshot shows the 'Apps' management interface. At the top, there are options for 'Add', 'Category', and 'Export', along with a search bar. Below is a table of applications with columns for 'Icon', 'App Name', 'Type', 'Category', 'Created On', 'Last Updated', and 'Disable'. The application 'Worxmail' is highlighted in green. A context menu is open over the 'Worxmail' row, showing options for 'Edit', 'Disable', 'Category', and 'Delete'. The 'Disable' option is highlighted with a purple box. Below the menu, a 'Deployment' summary is shown with three boxes: 'Installed' (0), 'Pending' (0), and 'Failed' (0). A 'Show more >' link is at the bottom of the dialog. At the bottom of the screenshot, it says 'Showing 1 - 9 of 9 items'.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/10/15 3:13 PM	
<input type="checkbox"/>		worxweb	MDX	Worxapps			
<input type="checkbox"/>		Angrybird	Public App Store	Public			
<input type="checkbox"/>		WorxTasks	MDX	Default			
<input type="checkbox"/>		WorxMail2	MDX	MDX			
<input type="checkbox"/>		WorxNotes-iOS	MDX	MDX			
<input type="checkbox"/>		worxweb2	MDX	MDX			
<input type="checkbox"/>		ShareFile1	MDX	MDX			

- Haga clic en **Disable** en el cuadro de diálogo de confirmación. Aparecerá la etiqueta *Disabled* en la columna **Disable** de la aplicación.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

**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 ha elegido para la aplicación seleccionada.

5. Configure los siguientes 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 **Siguiente**. 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**.

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

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. El valor predeterminado es **ON**.
  - **Allow app comments.** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. El valor predeterminado es **ON**.

9. Haga clic en **Next**. Aparecerá la página **Approvals**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Configure' tab is active, and the 'Apps' sub-tab is selected. On the left, a sidebar shows the configuration steps: '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The '3 Approvals (optional)' step is highlighted. The main content area is titled 'Approvals (optional)' and contains the instruction: 'Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.' Below this is a 'Workflow to Use' dropdown menu with 'None' selected. At the bottom right, there are 'Back' and 'Next >' buttons.

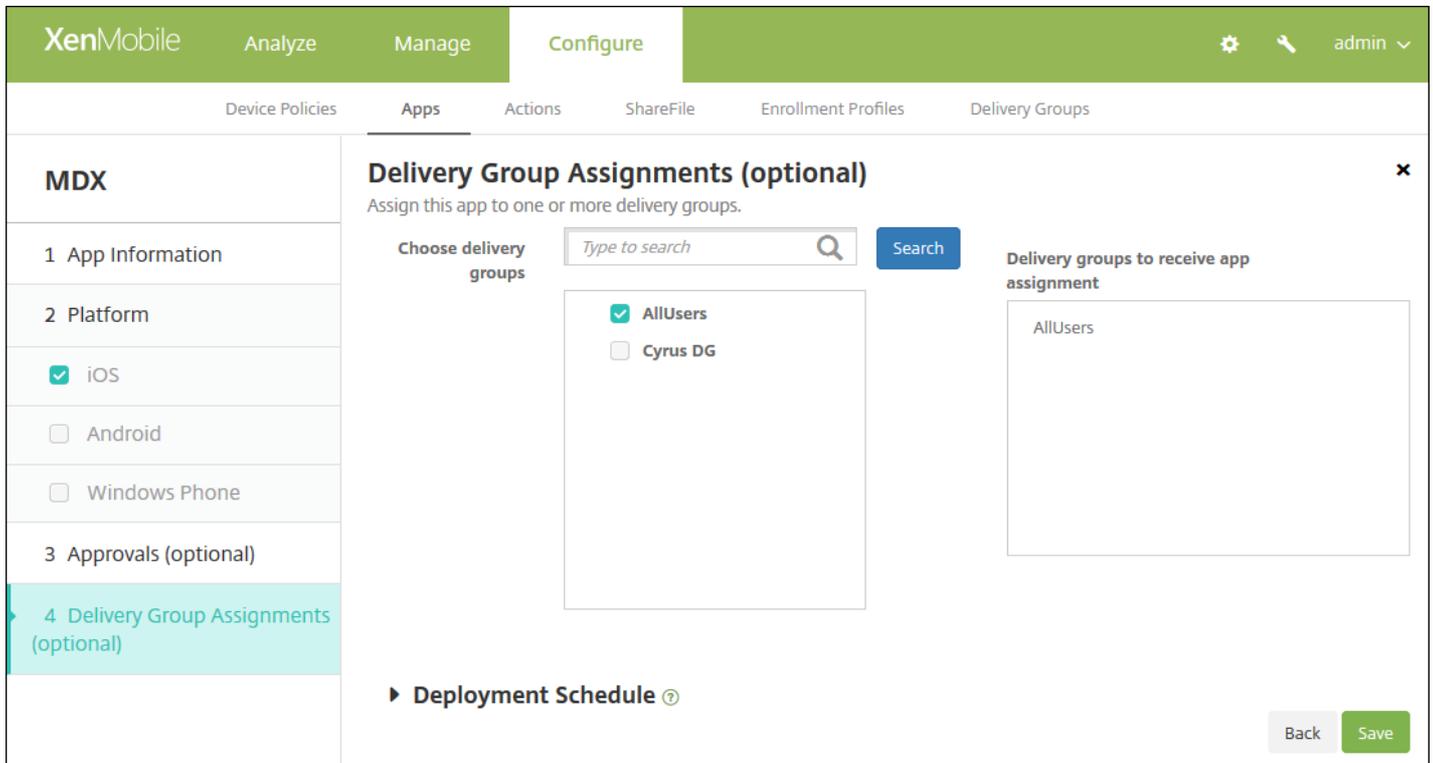
10. Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no necesita establecer flujos de trabajo de aprobación, puede ir directamente al paso 11.

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 en **Create a new workflow**. El valor predeterminado es **None**.
- Si selecciona **Create a new workflow**, configure los siguientes parámetros:
  - **Name.** Escriba un nombre único para el flujo de trabajo.
  - **Description.** Si quiere, escriba una descripción del flujo de trabajo.
  - **Email Approval Templates.** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
  - **Levels of manager approval.** En la lista, seleccione la cantidad de niveles de aprobación de administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 level**. Las opciones posibles son:
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain.** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
  - **Find additional required approvers.** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Search**. Los nombres se originan en Active Directory.
  - Cuando el nombre de la persona aparezca en el campo, marque la casilla de verificación que aparece junto a su nombre. El nombre y la dirección de correo electrónico de la persona aparecen en la lista **Selected additional required approvers**.
  - Para quitar a una persona de la lista Selected additional required approvers, realice una de las siguientes acciones:
    - Haga clic en **Search** para ver una lista de todos los usuarios del dominio seleccionado.

- Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar los resultados de la búsqueda.
- Las personas de la lista **Selected additional required approvers** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla de verificación junto a cada nombre que quiera quitar.

11. Haga clic en **Next**. Aparecerá la página **Delivery Group Assignment**.



12. Junto a **Choose delivery groups**, escriba lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a los que quiera asignar la directiva. 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 haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has failed**. La opción predeterminada es **On every connection**.
- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:**

- Esta se aplica tras haber definido la clave de implementación en segundo plano para la programación en **Settings > Server Properties**. La opción Deploy for always-on connection no está disponible para dispositivos iOS.
- La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se

realicen se aplicarán a todas las plataformas, excepto la opción **Deploy for always on connection**, que no se aplicará para iOS.

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 aparece, 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

Mar 02, 2017

Para ver una lista de las directivas de aplicación MDX para iOS, Android y Windows Phone con notas sobre las restricciones aplicables y recomendaciones de Citrix, consulte [Vista general de las directivas de aplicaciones MDX](#) en la documentación de MDX Toolkit.

# Personalización de marca en XenMobile Store y Citrix Secure Hub

Mar 02, 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 presentes en dispositivos móviles iOS y Android.

**Nota:** Antes de comenzar, compruebe que la imagen de personalización de marca está preparada y se puede acceder a ella. 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**.

**Settings**

Certificate Management	Notifications	Server	Frequently Accessed
Certificates	Carrier SMS Gateway	ActiveSync Gateway	Certificates
Credential Providers	Notification Server	Enrollment	Enrollment
PKI Entities	Notification Templates	LDAP	Licensing
		Licensing	Local Users and Groups
<b>Client</b>	<b>Platforms</b>	Local Users and Groups	Role-Based Access Control
Client Branding	Android for Work	Mobile Service Provider	Release Management
Client Properties	Google Play Credentials	NetScaler Gateway	
Client Support	iOS Bulk Enrollment	Network Access Control	
	iOS Settings	Release Management	
	Samsung KNOX	Role-Based Access Control	
		Server Properties	
		SysLog	
		Workflows	
		XenApp/XenDesktop	

2. En **Client**, haga clic en **Client Branding**. Aparecerá la página **Client Branding**.

XenMobile Analyze Manage Configure admin

Settings > Client Branding

### Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

**Store name\***  ?

**Default store view**

Category

A-Z

**Device**

Phone

Tablet

**Branding file**  **Browse**

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

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 es **Phone**.
- **Branding file.** Seleccione un archivo o un ZIP con las imágenes que se van a usar para la personalización de marca. 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

Mar 02, 2017

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android implementados por XenMobile. 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 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.

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](#).

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Launcher Configuration Policy' and includes a sidebar with steps: '1 Policy Info', '2 Platforms', '3 Assignment', and 'Android' (which is selected). The main panel shows 'Policy Information' with a description: 'This policy lets you define a configuration of an Android device launcher.' Under 'Launcher app configuration', there are two sections: 'Define a logo image' with a toggle set to 'ON' and a text input for 'Logo image' containing 'ribbon.png' and a 'Browse' button; and 'Define a background image' with a toggle set to 'ON' and a text input for 'Background image' and a 'Browse' button. Below this is a table for 'Allowed apps' with columns for 'App name' and 'Package Name\*'. The table contains one row with 'test' in the 'App name' column and 'test.com' in the 'Package Name\*' column. There is an 'Add' button to the right of the table. At the bottom of the form, there is a 'Password' input field and a 'Deployment Rules' section. At the very bottom right, there are 'Back' and 'Next >' buttons.

App name	Package Name*	Add
test	test.com	

3. Agregue la aplicación Citrix Launcher a XenMobile como una aplicación de empresa. En **Configure > Apps**, haga clic en

**Add** y, a continuación, haga clic en **Enterprise**. Para obtener información más detallada, consulte [Incorporación de aplicaciones de empresa](#).

**Add App** [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

- MDX**  
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.  
Example: WorxMail
- Public App Store**  
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.  
Example: GoToMeeting
- Web & SaaS**  
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.  
Example: GoogleApps\_SAML
- Enterprise**  
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.  
Example: Quick-iLaunch
- Web Link**  
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

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**.

**Deployment Order** [Close]

Change the deployment order by dragging the policies, apps and actions into position.

- Citrix Launcher
- Launcher Configuration

[Cancel] [Save]

Para obtener más información, consulte [Implementación de recursos](#).

# Programa de compras por volumen de iOS

Mar 02, 2017

Puede administrar las licencias de las aplicaciones iOS mediante el Programa de compras por volumen (VPP), una solución sencilla y flexible para gestionar las necesidades de contenido de su organización. El programa VPP de iOS simplifica el proceso de búsqueda, compra y distribución de aplicaciones (y otros datos) de forma masiva en una organización.

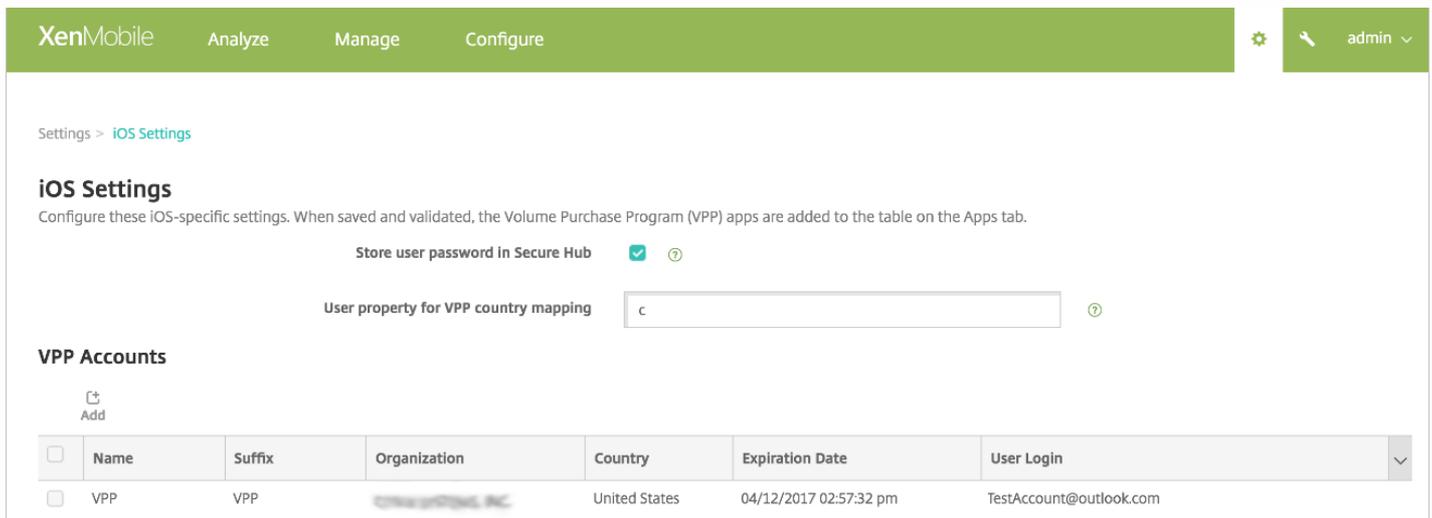
Con el programa VPP, puede usar XenMobile para distribuir aplicaciones (incluidas las aplicaciones XenMobile y otras aplicaciones MDX) directamente a los dispositivos, o bien, puede asignar contenido a los usuarios mediante códigos de canje. En XenMobile, puede configurar parámetros específicos del Programa de compras por volumen (VPP) de iOS.

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 el 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 y validar la configuración del programa VPP de iOS en XenMobile, las aplicaciones adquiridas se agregan a la tabla situada en la ficha Apps (**Configure > Apps**) de la consola de XenMobile.

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 **Platform**, haga clic en **iOS Settings**. Aparecerá la página de configuración **iOS Settings**.



Settings > iOS Settings

### iOS Settings

Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Secure Hub  ⓘ

User property for VPP country mapping  ⓘ

#### VPP Accounts

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login
<input type="checkbox"/>	VPP	VPP	CITRIX SYSTEMS, INC.	United States	04/12/2017 02:57:32 pm	TestAccount@outlook.com

3. Configure estos parámetros:

- **Store user password in Citrix 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



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). Como resultado, no tendrá que utilizar un dispositivo de ID de Apple, los usuarios no recibirán invitaciones para unirse al programa VPP y podrán descargarse las aplicaciones sin iniciar sesión en sus cuentas de iTunes.

The screenshot shows the XenMobile web interface for configuring an app. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Public App Store' and 'iPhone App Settings'. On the left, there is a sidebar with sections: '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. Under '2 Platform', 'iPhone', 'iPad', and 'Google Play' are checked. The 'App Details' section includes: 'Name\*' (GoToMeeting), 'Description\*' (Meet where you want with GoToMeeting on your mobile device...), 'Version' (6.6.5.1134), 'Image' (GoToMeeting logo), 'Paid app' (OFF), 'Remove app if MDM profile is removed' (ON), 'Prevent app data backup' (ON), 'Force app to be managed' (ON), and 'Force license association to device' (ON, highlighted with a red box). At the bottom right, there are 'Back' and 'Next >' buttons.

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.

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

### Public App Store

- 1 App Information
- 2 Platform
  - iPhone
  - iPad
  - Google Play
  - Android for Work
  - Windows Desktop/Tablet
  - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

Remove app if MDM profile is removed  ON

Prevent app data backup  ON

Force app to be managed  ON ?

Force license association to device  ON

► Deployment Rules

► Store Configuration

▼ Volume Purchase Program

**VPP ID Assignment**

Disassociate License Usage: 2 of 2

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input type="checkbox"/>	82684302	Used		
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

**VPP License Keys**

Import

Para desvincular una licencia, haga clic en la fila de la licencia y en **Disassociate**.

**Disassociate VPP license**

Are you sure you want to disassociate the selected users with this VPP license ID?

Cancel Disassociate

**VPP ID Assignment**

Disassociate

License Usage: 2 of 2

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input checked="" type="checkbox"/>	82684302	Used	[Redacted]	[Redacted]
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

**VPP License Keys**

Import

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 o 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**.

XenMobile Analyze **Manage** Configure admin

Devices Users Enrollment

### Device details

- General
- Properties
- User Properties**
- Assigned Policies
- Apps
- Actions
- Delivery Groups
- iOS Profiles
- iOS Provisioning Profiles
- Certificates
- Connections
- MDM Status

### User Properties

**User name**

**Password**

**Role\***

**Membership**  local\MSP [Manage Groups](#)

**VPP Accounts**  VPP [Retire](#)

[Back](#) [Next >](#)

- Cuando asigna una aplicación a un grupo de entrega, XenMobile la identifica de forma predeterminada como una aplicación opcional. Para que XenMobile implemente una aplicación en los dispositivos, vaya a **Configure > Delivery Groups** y, 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. Por ejemplo, para enviar una actualización de Secure Hub (si se ha asignado a un dispositivo, no a un usuario), en **Configure > Apps**, en una página de plataforma, haga clic en **Check for Updates** y aplique la actualización.

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

### Public App Store

- 1 App Information
- 2 Platform
  - iPhone
  - iPad
  - Google Play
  - Android for Work
  - Windows Desktop/Tablet
  - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

## iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

### App Details

**Name\***

**Description\***

**Version**  Check for Updates

**Image** 

**Paid app**  OFF

**Remove app if MDM profile is removed**  ON

**Prevent app data backup**  ON

**Force app to be managed**  ON ?

**Force license association to device**  ON

▶ **Deployment Rules**  
 ▶ **Store Configuration**  
 ▶ **Volume Purchase Program**

Back Next >

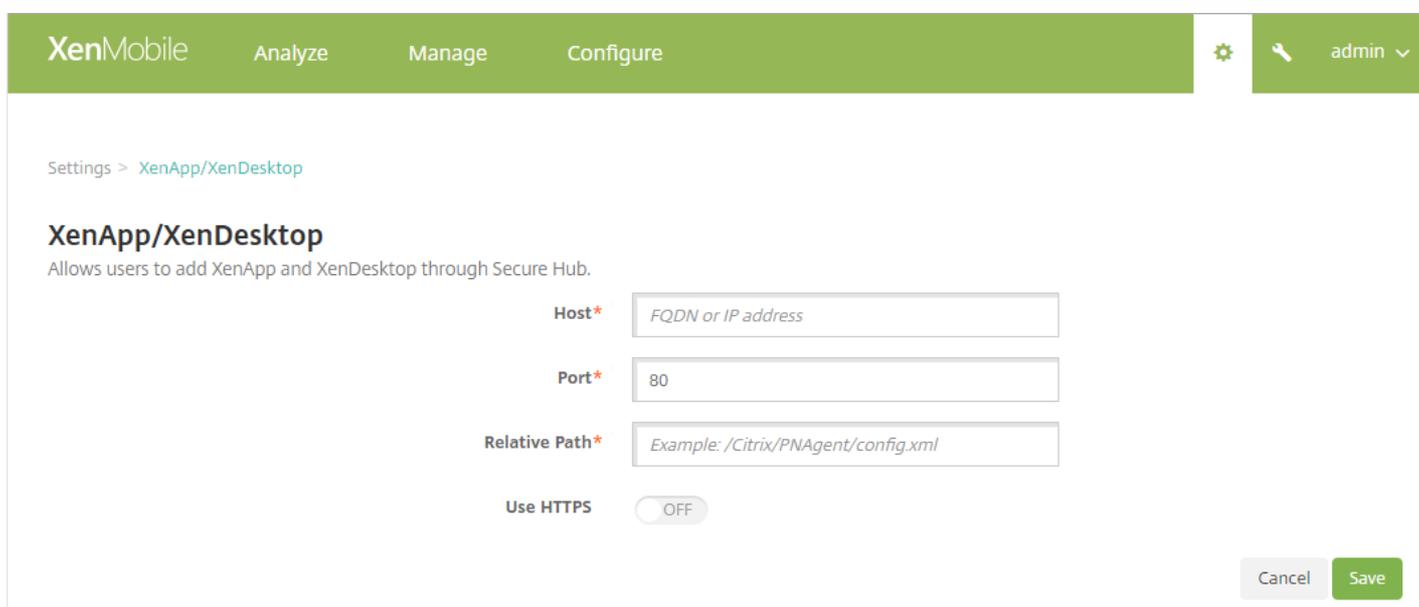
# XenApp y XenDesktop desde Citrix Secure Hub

Mar 02, 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**.



The screenshot shows the XenMobile web console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. On the right, there is a user profile 'admin' with a gear icon. Below the navigation bar, the breadcrumb 'Settings > XenApp/XenDesktop' is visible. The main heading is 'XenApp/XenDesktop' with a sub-heading 'Allows users to add XenApp and XenDesktop through Secure Hub.' The configuration form includes four fields: 'Host\*' with a placeholder 'FQDN or IP address', 'Port\*' with the value '80', 'Relative Path\*' with a placeholder 'Example: /Citrix/PNAgent/config.xml', and 'Use HTTPS' with a toggle switch set to 'OFF'. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Configure los siguientes parámetros:

- **Host**. Escriba el nombre de dominio completo (FQDN) o la dirección IP de StoreFront o del sitio de Interfaz Web.
- **Port**. Escriba el número de puerto de StoreFront o del sitio de Interfaz Web. El valor predeterminado es 80.
- **Relative Path**. Escriba la ruta de acceso. Por ejemplo, /Citrix/PNAgent/config.xml.
- **Use HTTPS**. Seleccione si habilitar la autenticación segura entre StoreFront o el sitio de Interfaz Web y el dispositivo cliente. El valor predeterminado es **OFF**.

4. Haga clic en **Save**.

# Implementación de recursos

Mar 02, 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 de los grupos de entrega; y cómo determina XenMobile el orden de implementación cuando un usuario está incluido en varios grupos de entrega que tienen directivas duplicadas o en conflicto.

Los grupos de entrega indican la categoría de usuarios en cuyos dispositivos se implementan las combinaciones de directivas, aplicaciones y acciones. Por regla general, la inclusión en un grupo de entrega se basa en las características de los usuarios (por ejemplo, la empresa, el país, el departamento, el título y la dirección de la oficina). Los grupos de entrega permiten ejercer más control sobre quién obtiene qué recursos y cuándo lo hacen. Puede implementar un grupo de entrega para todos los usuarios, o bien para un grupo más definido de ellos.

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS y Windows Phone, y tabletas Windows que pertenezcan a ese grupo de entrega para que se vuelvan a conectar a XenMobile con el fin de que se puedan volver a evaluar los dispositivos e implementar en ellos aplicaciones, directivas y acciones. Aquellos usuarios que tengan dispositivos con otras plataformas reciben los recursos de inmediato si ya están conectados o la próxima vez que se conecten, según la directiva de programación definida.

Al instalarse y configurarse XenMobile, se crea el grupo de entrega predeterminado AllUsers. Este grupo contiene todos los usuarios locales y los usuarios de Active Directory. No se puede eliminar el grupo AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios.

## Orden de implementación

El orden de implementación es la secuencia con la que XenMobile envía 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
Aplicación	Plataforma del dispositivo Regla de implementación (basada en las propiedades del dispositivo) Programación de la implementación
Acción	Regla de implementación (basada en las propiedades del dispositivo) Programación de la implementación
Grupo de entrega	Usuario/Grupos Regla de implementación (basada en las propiedades del dispositivo)

Es muy probable que, en un entorno típico, varios grupos de entrega queden asignados a un mismo usuario, y estos son los resultados posibles:

- Pueden existir objetos duplicados dentro de los grupos de entrega.
- Una misma directiva está configurada de distinta forma en grupos de entrega diferentes asignados a un mismo usuario.

Cuando ocurre alguna de estas circunstancias, XenMobile calcula un orden de implementación para todos los objetos que debe entregar a un dispositivo o sobre los que debe realizar alguna acción. Los pasos para realizar este cálculo son independientes de la plataforma del dispositivo.

Pasos para el cálculo:

1. Identificar todos los grupos de entrega de un usuario específico, en función de los filtros de usuario/grupos y las reglas de implementación.
2. Crear una lista ordenada de todos los recursos (directivas, acciones y aplicaciones) de los grupos de entrega seleccionados, en función de los filtros de plataforma de dispositivo, reglas de implementación y programación de la

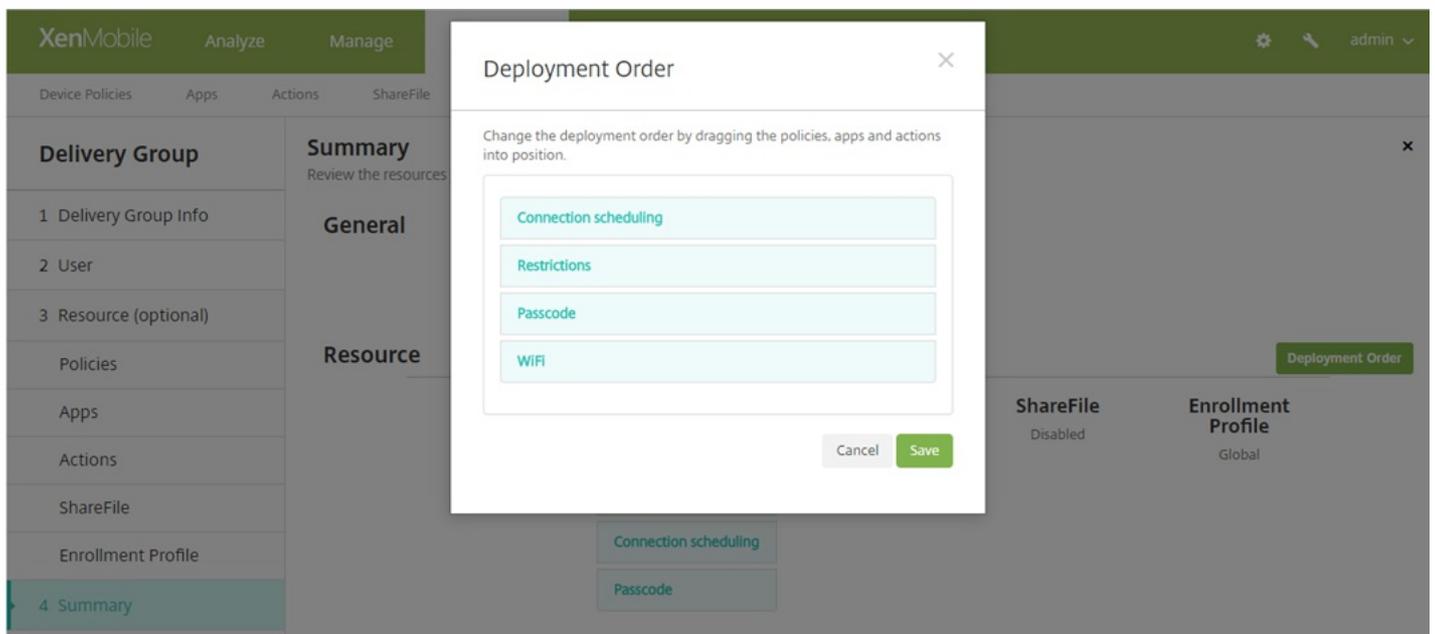
implementación. El algoritmo para ordenarlos es la siguiente:

- a. Colocar los recursos de los grupos de entrega que tengan una orden de implementación definida por el usuario por delante de aquellos que no la tengan. La razón para hacer esto se describe después de los pasos.
- b. En caso de haber dos grupos de entrega en las mismas circunstancias, ordenar los recursos de los grupos de entrega por nombre de grupo. Por ejemplo, se colocan los recursos del grupo de entrega A por delante de los del grupo de entrega B.
- c. Durante el proceso de ordenamiento, si hay una orden de implementación especificada para los recursos de un grupo de entrega, se mantiene ese orden. Si no la hay, los recursos del grupo de entrega se ordenan por nombre de recurso.
- d. Si el mismo recurso aparece más de una vez, quitar el recurso duplicado.

Los recursos que tienen un orden definido por el usuario asociado con ellos se implementan antes de los recursos que no tienen un orden definido por el usuario. Un recurso puede existir en varios grupos de entrega asignados al usuario. 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, se desea 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 omite las directivas **WiFi** y **Passcode** del grupo de entrega Gestores de cuentas 1, por ser duplicados. El algoritmo, por lo tanto, respeta el orden especificado por el administrador de XenMobile.

Para agregar un grupo de entrega

1. En la consola de XenMobile, haga clic en **Configure > Delivery Groups**. Aparecerá la página **Delivery Groups**.

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		
<input type="checkbox"/>		Domain users	Jun 13 2016 5:10 PM	
<input type="checkbox"/>		Sales	Apr 13 2016 12:50 PM	

2. En la página **Delivery Groups**, haga clic en **Add**. Aparecerá la página **Delivery Group Information**.

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

### Delivery Group

- 1 Delivery Group Info**
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

### Delivery Group Information ✕

Enter a name for the delivery group and any information that will help you keep track of it later.

**Name**

**Description**

3. En el panel **Delivery Group Information**, escriba la información siguiente:

- **Name.** Indique un nombre descriptivo para el grupo de entrega.
- **Description.** Escriba, si quiere, una descripción del grupo de entrega.

4. Haga clic en **Next**. Aparecerá la página **User Assignments**.

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', 'Configure', and a green bar. Below this, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' sub-tab is active. On the left, a sidebar shows a 'Delivery Group' menu with items: '1 Delivery Group Info', '2 User' (highlighted), '3 Resource (optional)', 'Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profile', and '4 Summary'. The main area is titled 'User Assignments' and contains the following controls:

- 'Select domain': A dropdown menu currently showing 'local'.
- 'Include user groups': A search input field with a magnifying glass icon and a blue 'Search' button to its right.
- A large empty rectangular box below the search field, intended for displaying the results of the search.
- 'Or/And' selection: Two radio buttons, with 'Or' selected (indicated by a teal dot) and 'And' unselected.
- 'Deploy to anonymous user': A toggle switch currently set to 'OFF'.
- 'Deployment Rules': A section header with a right-pointing arrow.

5. Configure los siguientes parámetros:

- **Select domain.** En la lista, seleccione el dominio del que se elegirá a los usuarios.
- **Include user groups.** Realice una de las siguientes acciones:
  - En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista **Selected user groups**.
  - Haga clic en **Search** para ver una lista de todos los grupos de usuarios del dominio seleccionado.
  - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar la lista de grupos de usuarios.
    - 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 **X**, situado junto a cada uno de los grupos que quiera eliminar.
      - 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 a ellos.
- **Deploy to anonymous user.** Seleccione si implementar recursos para los usuarios sin autenticar del grupo de entrega.

**Nota:** Los usuarios sin autenticar son aquellos que no han podido autenticarse pero a cuyos dispositivos se les ha

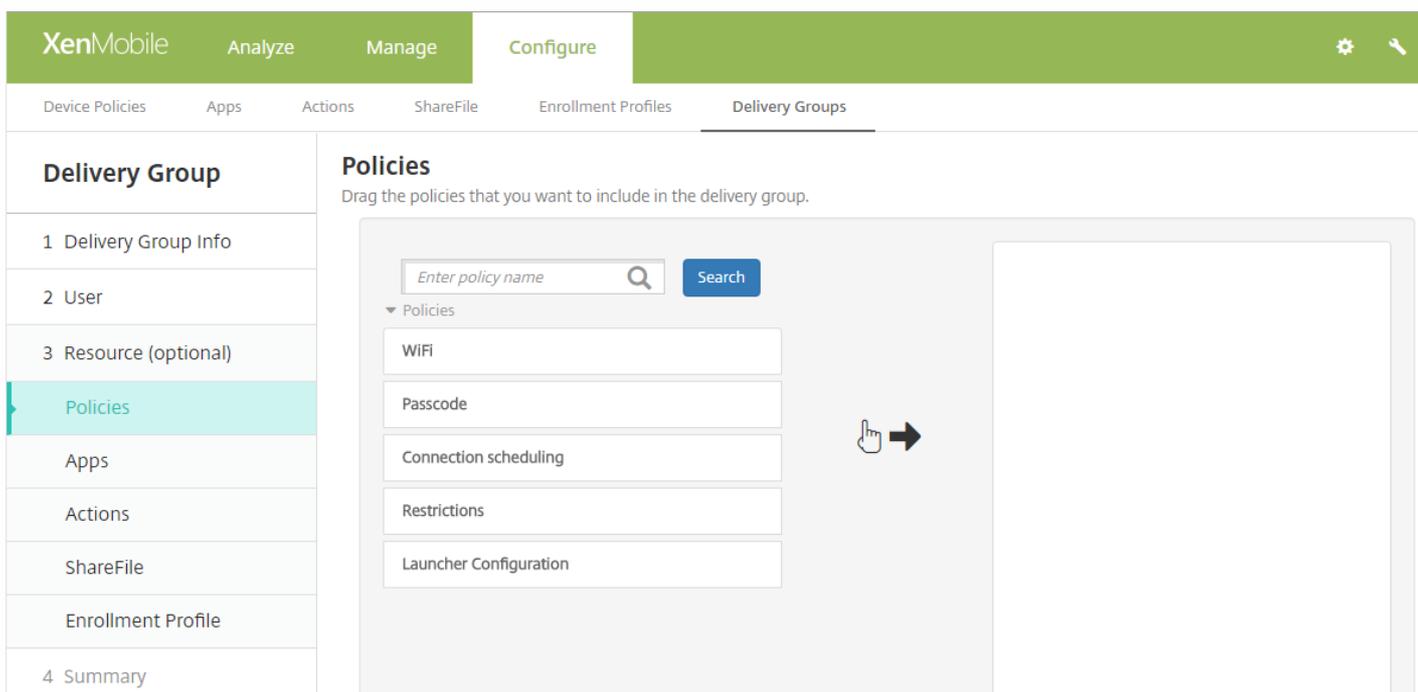
permitido conectarse a XenMobile de todas formas.

## 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



The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Configure', 'Delivery Groups' is chosen. On the left, a sidebar lists 'Delivery Group' options: 1 Delivery Group Info, 2 User, 3 Resource (optional), Policies (highlighted), Apps, Actions, ShareFile, Enrollment Profile, and 4 Summary. The main area is titled 'Policies' with the instruction 'Drag the policies that you want to include in the delivery group.' It features a search bar with the placeholder 'Enter policy name' and a 'Search' button. Below the search bar, a list of policies is shown: WiFi, Passcode, Connection scheduling, Restrictions, and Launcher Configuration. A hand icon with a right-pointing arrow is positioned between the list and a large empty box on the right, indicating the drag-and-drop functionality.

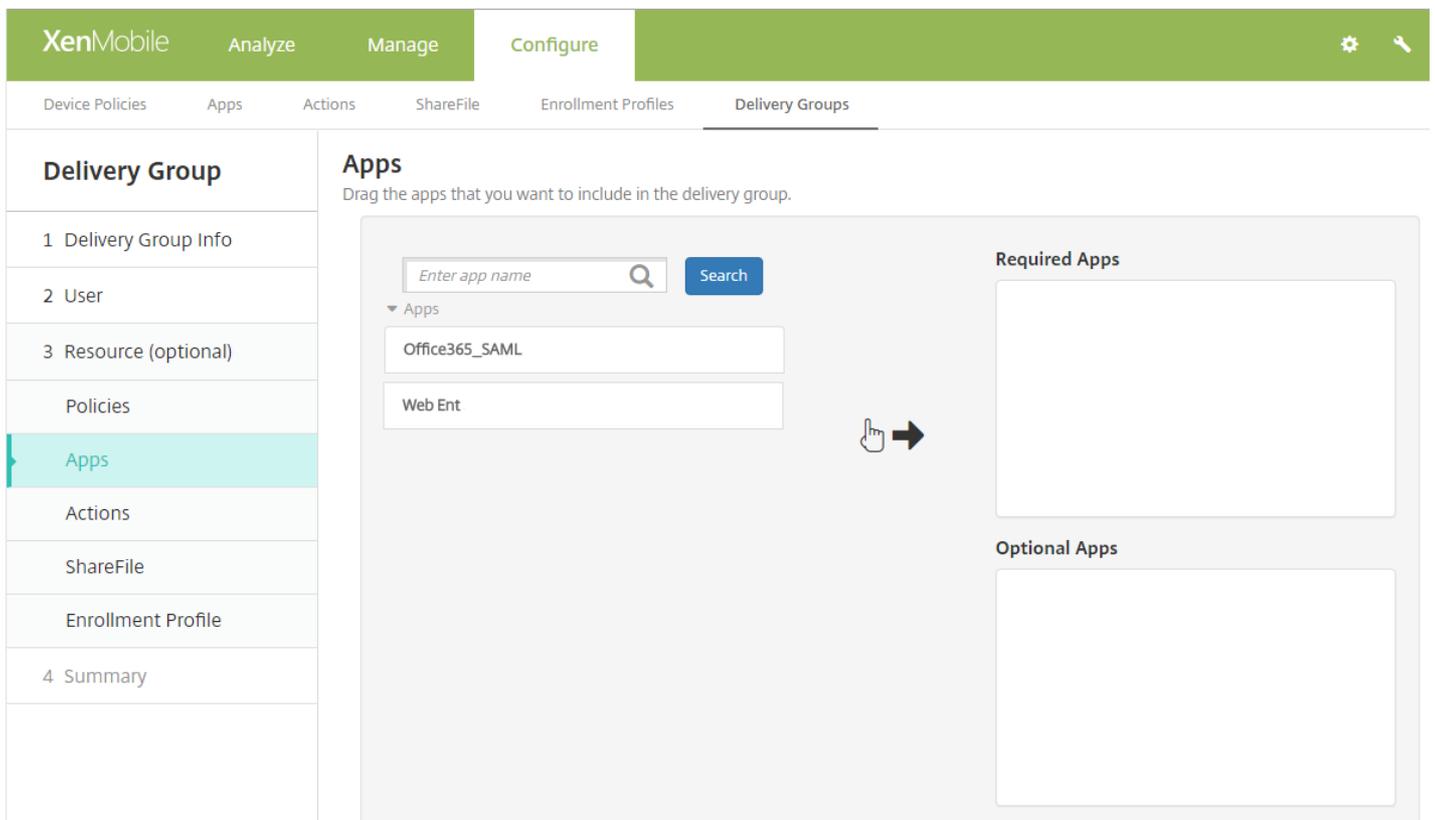
1. Para cada directiva que quiera agregar, lleve a cabo lo siguiente:

- Busque la directiva que quiera agregar en la lista de las directivas disponibles.
- O bien, para limitar la cantidad de directivas de la lista, escriba el nombre completo o parcial de la directiva en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la directiva que quiera agregar y arrástrela al cuadro de la derecha.

**Nota:** Para quitar una directiva, haga clic en la **X** situada junto al nombre de esa directiva en el cuadro de la derecha.

2. Haga clic en **Siguiente**. Aparecerá la página **Apps**.

## Incorporación de aplicaciones



1. Para cada aplicación que quiera agregar, lleve a cabo lo siguiente:

- Busque la aplicación que quiera agregar en la lista de las aplicaciones disponibles.
- O bien, para limitar la cantidad de aplicaciones de la lista, escriba el nombre completo o parcial de la aplicación en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la aplicación que quiera agregar y arrástrela al cuadro **Required Apps** o al cuadro **Optional Apps**.

**Nota:** Para quitar una aplicación, haga clic en la **X** situada junto al nombre de esa aplicación en el cuadro de la derecha.

2. Haga clic en **Siguiente**. Aparecerá la página **Actions**.

## Incorporación de acciones

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' sub-tab is active. On the left, a 'Delivery Group' sidebar contains a list of steps: '1 Delivery Group Info', '2 User', '3 Resource (optional)', 'Policies', 'Apps', 'Actions' (highlighted in teal), 'ShareFile', 'Enrollment Profile', and '4 Summary'. The main content area is titled 'Actions' and includes the instruction 'Drag the actions that you want to include in the delivery group.' Below this is a search bar with the placeholder text 'Enter action name' and a 'Search' button. A dropdown menu labeled 'Actions' is open, showing two items: 'Action - Out of compliance' and 'Action - Send notification'. A hand icon with an arrow points to the right, indicating a drag-and-drop action.

1. Para cada acción que quiera agregar, haga lo siguiente:

- Busque la acción que quiera agregar en la lista de las acciones disponibles.
- O bien, para limitar la cantidad de acciones de la lista, escriba el nombre completo o parcial de la acción en cuestión en el cuadro de búsqueda y, a continuación, haga clic en **Search**.
- Haga clic en la acción que quiera agregar y arrástrela al cuadro de la derecha.

**Nota:** Para quitar una acción, haga clic en la **X** situada junto al nombre de esa acción en el cuadro de la derecha.

2. Haga clic en **Siguiente**. Aparecerá la página **ShareFile**.

## Habilitar ShareFile

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

### Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
  - Policies
  - Apps
  - Actions
  - ShareFile**
  - Enrollment Profile
- 4 Summary

### ShareFile

Enable ShareFile to provide users in the delivery group with single sign-on (SSO) access to content and data.

**Enable ShareFile**  OFF

1. Configure este parámetro:

- **Enable ShareFile.** Haga clic en **ON** para habilitar el acceso Single Sign-On de ShareFile a contenido y datos.

2. Haga clic en **Siguiente**. Aparece la página **Summary**.

Perfil de inscripción

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there is a sub-navigation bar with tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' tab is selected, and the 'Enrollment Profile' sub-tab is active. On the left, a sidebar menu lists the configuration steps: '1 Delivery Group Info', '2 Resource (optional)', 'Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profile' (highlighted in teal), and '3 Summary'. The main content area is titled 'Enrollment Profile' and contains the instruction 'Select the enrollment profile that you want the users in this delivery group to see'. Below this, there is a radio button labeled 'Enrollment Profile' with the 'Global' option selected.

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

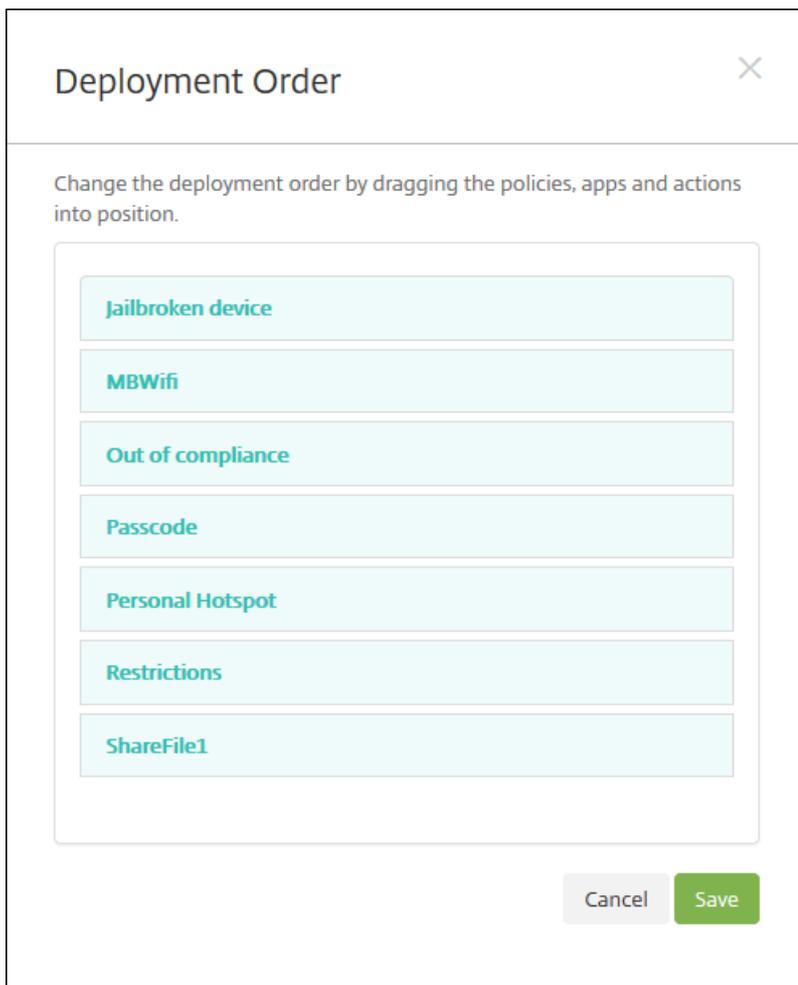
The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Summary' and contains a 'General' section with a table for resources, a 'Resource' section with a 'Deployment Order' button, and a list of resource categories: Apps (0), Policies (0), Actions (0), ShareFile (Disabled), and Enrollment Profile (Global).

En la página **Summary**, puede revisar las opciones que haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos. La página Summary muestra los recursos por categoría; no refleja el orden de implementación.

1. Haga clic en **Back** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.
2. Haga clic en **Deployment Order** para ver el orden de implementación o para cambiarlo.
3. Haga clic en **Save** para guardar el grupo de entrega.

Para cambiar el orden de implementación

1. Haga clic en el botón **Deployment Order**. Aparecerá el cuadro de diálogo **Deployment Order**.



2. Haga clic en un recurso y arrástrelo a la ubicación desde donde quiere implementarlo. Después de cambiar el orden de implementación, XenMobile implementa los recursos de la lista de arriba a abajo.

3. Haga clic en **Save** para guardar el orden de implementación.

Para modificar un grupo de entrega

En la página **Delivery Groups**, seleccione el grupo de entrega que quiera modificar. Puede seleccionarlo de dos maneras: marcando la casilla de verificación que aparece junto a su nombre o haciendo clic en la línea que contiene su nombre. y luego en **Edit**. Aparecerá la página para modificar la información de grupos de entrega **Delivery Group Information**.

## Nota

Según cómo haya seleccionado el grupo de entrega, el comando **Edit** aparece encima o a la derecha del grupo de entrega.

2. Agregue o cambie el campo **Description**.

**Nota:** No se puede cambiar el nombre de un grupo de entrega existente.

3. Haga clic en **Next**. Aparecerá la página **User Assignments**.

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' sub-tab is active. On the left, a sidebar lists various configuration options, with '2 User' highlighted in blue. The main content area is titled 'User Assignments' and includes a 'Select domain' dropdown menu currently set to 'local'. Below this is an 'Include user groups' search box with a magnifying glass icon and a blue 'Search' button. Underneath the search box is a large empty rectangular area for displaying results. At the bottom of the 'User Assignments' section, there are radio buttons for 'Or' (which is selected) and 'And', and a 'Deploy to anonymous user' toggle switch currently set to 'OFF'. A link for 'Deployment Rules' is located at the bottom of the main content area.

4. En el panel **Select User Groups**, escriba o cambie la información siguiente:

- **Select domain.** En la lista, seleccione el dominio del que se elegirán los usuarios.
- **Include user groups.** Realice una de las siguientes acciones:
  - En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista **Selected user groups**.
  - Haga clic en **Search** para ver una lista de todos los grupos de usuarios del dominio seleccionado.
  - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Search** para limitar la lista de grupos de usuarios.

**Nota:** Para quitar grupos de usuarios, haga clic en **Search** y, en la lista de los grupos de usuarios, desmarque la casilla situada junto al grupo o grupos que quiera quitar. Puede escribir un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, hacer clic en **Search** para limitar la cantidad de grupos de usuarios que se mostrarán en la lista.

- **Or/And.** Seleccione si los usuarios pueden estar en cualquier grupo (Or) o si deben estar en todos los grupos (And) para que se implemente el recurso para ellos.
- **Deploy to anonymous user.** Seleccione si implementar recursos para los usuarios sin autenticar del grupo de entrega.

**Nota:** Los usuarios sin autenticar son aquellos que no han podido autenticarse pero a cuyos dispositivos se les ha permitido conectarse a XenMobile.

5. Expanda **Deployment Rules** y, a continuación, configure los parámetros como hizo en el paso 5 de este procedimiento.
6. Haga clic en **Next**. Aparecerá la página **Delivery Group Resources**. Desde aquí, puede agregar o eliminar directivas, aplicaciones o acciones. Para omitir este paso, en **Delivery Group**, haga clic en **Summary** para ver un resumen de la configuración del grupo de entrega.
7. Cuando termine de modificar un recurso, haga clic en **Next**, o bien, en **Delivery Group**, haga clic en **Summary**.
8. En la página **Summary**, puede revisar las opciones que haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos.
9. Haga clic en **Back** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.
10. Haga clic en **Deployment Order** para reorganizar el orden de implementación de los recursos; para obtener más información sobre cómo cambiar el orden de implementación, consulte [Para cambiar el orden de implementación](#).
11. Haga clic en **Save** para guardar el grupo de entrega.

Para habilitar e inhabilitar el grupo de entrega AllUsers

## Nota

AllUsers es el único grupo de entrega que puede habilitar o inhabilitar.

1. Desde la página **Delivery Groups**, seleccione el grupo de entrega AllUsers marcando la casilla junto a **AllUsers** o haciendo clic en la línea que contiene AllUsers. A continuación, lleve a cabo una de las siguientes acciones:

**Nota:** Según cómo haya seleccionado el grupo de entrega AllUsers, los comandos **Enable** o **Disable** aparecerán encima o a la derecha del grupo de entrega AllUsers.

- Haga clic en **Disable** para inhabilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está habilitado (valor predeterminado). Una vez inhabilitado, aparecerá la etiqueta **Disabled** bajo el encabezado **Disabled** en la tabla de grupos de entrega.
- Haga clic en **Enable** para habilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está inhabilitado. Una vez habilitado, desaparecerá la etiqueta **Disabled** del encabezado **Disabled** de la tabla de grupos de entrega.

Para implementar en grupos de entrega

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS, Windows Phone y Windows Tablet que pertenezcan a ese grupo de entrega para que se vuelvan a conectar a XenMobile. De esta manera, puede volver a evaluar los dispositivos e implementar aplicaciones, directivas y acciones. Los usuarios de dispositivos de otras plataformas reciben los recursos inmediatamente si ya están conectados; o, en función de la directiva de programación, la próxima vez que se conecten.

**Nota:** Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de 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**, realice una de las siguientes acciones:

- Para implementar recursos en más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos en los que quiere realizar la implementación.
- Para implementar recursos en un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.

2. Haga clic en **Deploy**.

**Nota:** Según cómo seleccione el grupo de entrega, el comando **Deploy** aparecerá encima o a la derecha del grupo de entrega.

Compruebe que los grupos a los que se van a implementar aplicaciones, directivas y acciones se encuentran en la lista y, a continuación, haga clic en **Deploy**. Las aplicaciones, las directivas y las acciones se implementan en los grupos seleccionados en función de la plataforma de los dispositivos y de la directiva de programación.

Puede comprobar el estado de implementación en la página **Delivery Groups** de una de las siguientes maneras:

- Mire el icono de implementación, debajo del encabezado **Status** del grupo de entrega, el cual indica si hay algún error en la implementación.
- Haga clic en la línea que contiene el grupo de entrega para ver una superposición que indica las implementaciones **instaladas**, las **pendientes** y las **erróneas**.

The screenshot shows the 'Delivery Groups' management interface. At the top, there are 'Add' and 'Export' buttons, a search bar, and a 'Show filter' link. Below this is a table with the following columns: 'Status', 'Name', 'Last Updated', and 'Disabled'. The table contains three rows: 'AllUsers', 'sales' (highlighted in light blue), and 'DG for CAT'. Each row has a checkbox and a deployment icon. A modal window is open over the 'sales' row, showing 'Edit', 'Deploy', and 'Delete' actions. The modal displays a 'Deployment' summary with three boxes: '1 Installed' (green), '0 Pending' (light blue), and '0 Failed' (orange). A 'Show more >' link is at the bottom of the modal.

Status	Name	Last Updated	Disabled
<input type="checkbox"/>	AllUsers		
<input type="checkbox"/>	sales	Oct 26 2015 12:48 PM	
<input type="checkbox"/>	DG for CAT		

Showing 1 - 3 of 3 items

**Deployment**

- 1 Installed
- 0 Pending
- 0 Failed

Show more >

Para eliminar grupos de entrega

## Nota

No se puede eliminar el grupo de entrega AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios.

1. En la página **Delivery Groups**, realice una de las siguientes acciones:

- Para eliminar más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos que quiere eliminar.
- Para eliminar un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.

2. Haga clic en **Delete**. Aparecerá el cuadro de diálogo **Delete**.

**Nota:** Según cómo seleccione el grupo de entrega, el comando **Delete** aparecerá encima o a la derecha del grupo de entrega.

3. Haga clic en **Delete**.

## Important

No se puede deshacer esta acción.

Para exportar la tabla de grupos de entrega

1. Haga clic en el botón **Export** situado encima de la tabla **Delivery Groups**. XenMobile extrae la información de la tabla **Delivery Groups** y la convierte a un archivo CSV.
2. Abra o guarde el archivo CSV. El modo de hacer esto dependerá del explorador Web que se esté utilizando. También puede cancelar la operación.

# Macros

Mar 02, 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
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- iphone
- 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

Mar 02, 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 alguna de estas acciones:

- Haga clic en **Add** para agregar una nueva acción.
- Seleccione una acción existente para modificarla o eliminarla. Haga clic en la opción pertinente.

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

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.

The screenshot shows the XenMobile interface for configuring an action. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation menu has 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Actions' section is active, showing a list of steps: '1 Action Info', '2 Details', '3 Assignment (optional)', and '4 Summary'. The 'Action details' form is open, with the instruction 'Choose a trigger event and the associated action for that event.' It contains three main sections: 'Trigger\*' with a dropdown menu 'Select a trigger', 'Action\*' with a dropdown menu 'Select an action', and a 'Summary' box containing the text 'If CONDITION IS FULFILLED, then DO ACTION.'. Below the summary, there is a list of deployment rules with expandable arrows: 'Deployment Rules (iOS)', 'Deployment Rules (Mac OS X)', 'Deployment Rules (Android)', 'Deployment Rules (Windows Mobile/CE)', 'Deployment Rules (Windows Desktop/Tablet)', and 'Deployment Rules (Windows Phone)'. At the bottom right, there are 'Back' and 'Next >' buttons.

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 determinado.
  - **Device property.** Comprueba un atributo de dispositivo en el dispositivo recopilado en el modo de administración de dispositivos móviles y reacciona ante él.
  - **User property.** Reacciona ante un atributo de usuario, generalmente de Active Directory.
  - **Installed app name.** Reacciona ante una aplicación instalada. 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 al 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 del 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 mediante la sección **Notification Template** de **Settings**.

**Nota:** Antes de notificar a los usuarios, primero debe configurar los servidores de notificaciones en Settings para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes (consulte [Notificaciones en XenMobile](#)). Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificación, consulte [Para crear o actualizar plantillas de notificaciones en XenMobile](#).

The screenshot shows a configuration interface for an action. The title is "Action\*". Below the title, there are several input fields and dropdown menus:

- A dropdown menu with "Send notification" selected.
- A dropdown menu labeled "Select a template" with a question mark icon to its right.
- A text input field containing the number "1" with a question mark icon to its right.
- A dropdown menu labeled "Hours" with a question mark icon to its right.
- A text input field labeled "Specify an action repeat interval" with a question mark icon to its right.
- A dropdown menu labeled "Days" with a question mark icon to its right.

**Nota:** Después de seleccionar la plantilla, puede obtener una vista previa de la notificación cuando hace clic en **Preview notification message**.

**Action\***

Send notification

Failed Samsung KNOX attestation

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 que la acción se repite hasta que el usuario resuelva la situación.

1

Hours

0

Minutes

11. En **Summary**, verifique que la acción automatizada que ha creado es la acción esperada.

**Summary**

If The installed app name is " APP ", then notify USING TEMPLATE after 1 hour(s).

12. Después de configurar los detalles 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 lo que necesite para buscar un grupo de entrega, o bien seleccione un grupo o varios grupos de la lista a la que quiera asignar la directiva. Los grupos que seleccione aparecerán en la lista **Delivery groups to receive app assignment**, situada a la derecha.

16. Expanda Deployment Schedule y, a continuación, configure los siguientes parámetros:

- Junto a **Deploy**, haga clic en **ON** para programar la implementación o haga clic en **OFF** para cancelarla. La opción predeterminada es **ON**. Si elige **OFF**, no habrá ninguna otra opción a configurar.
- Junto a **Deployment schedule**, haga clic en **Now** o en **Later**. La opción predeterminada es **Now**.
- Si hace clic en **Later**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Deployment condition**, puede hacer clic en **On every connection** o en **Only when previous deployment has**

**failed.** La opción predeterminada es **On every connection**.

- Junto a **Deploy for always-on connection**, haga clic en **ON** o en **OFF**. La opción predeterminada es **OFF**.

**Nota:** Esta opción se configura en **Settings > Server Properties** y se aplica tras haber definido la clave de implementación en segundo plano para la programación. La opción **Deploy for always-on connection** no está disponible para dispositivos iOS.

**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.

XenMobile Analyze Manage **Configure** Administrator

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

### Actions

- 1 Action Info
- 2 Details**
- 3 Assignment (optional)
- 4 Summary

Device property

Select a device property

#### Action\*

App wipe

1

Hours

#### Summary

If **DEVICE PROPERTY CONDITION IS FULFILLED**, then app wipe the device after 1 hour(s).

Back Next >

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

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

8. Haga clic en **Save**.

### Para realizar 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**.

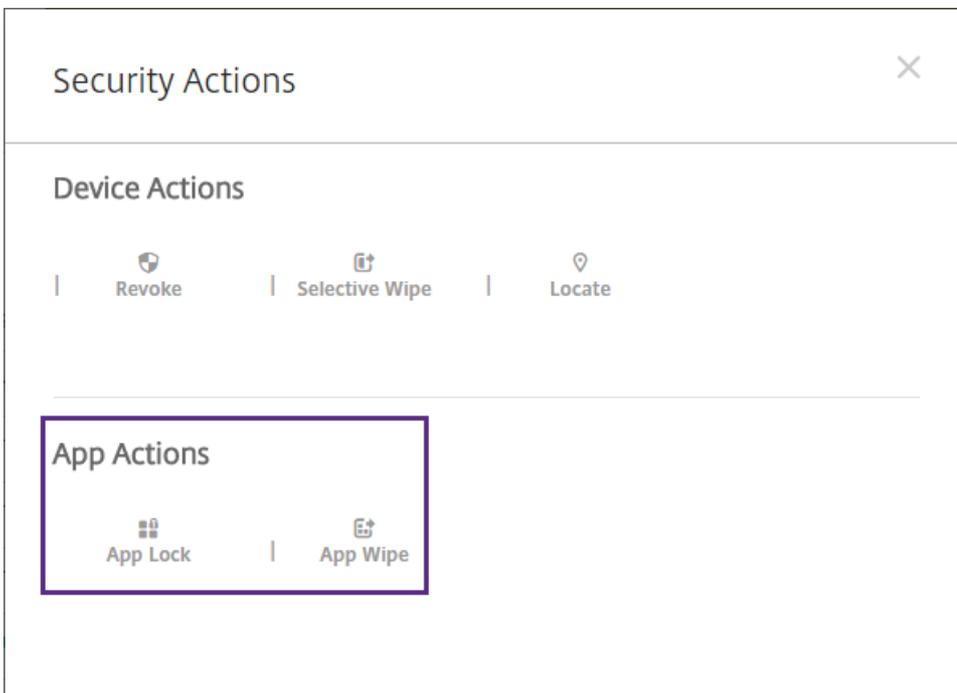
**Devices** Hide filter Search Q

Add | Edit | Secure | Notify | Delete | Import | Export | Refresh

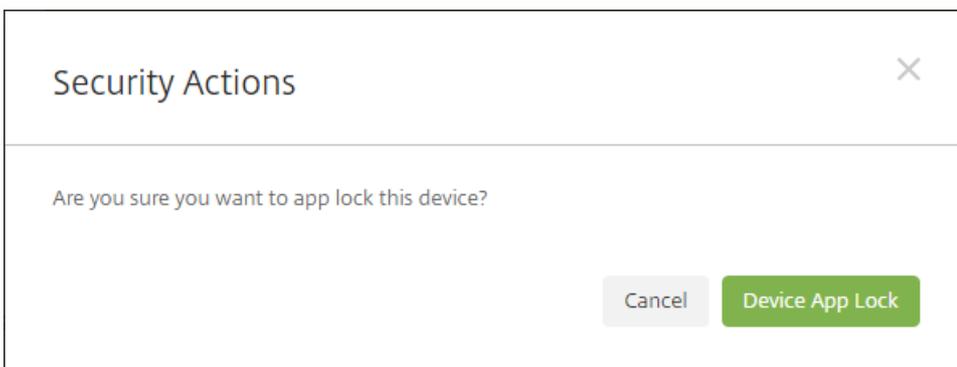
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
<input type="checkbox"/>		MDM MAM	ex12user0@...net "ex12user0"	iOS	9.3.2	iPhone	10/26/2016 11:04:43 am	14 days
<input checked="" type="checkbox"/>		MDM MAM	ex12user0@...net "ex12user0"	iOS	8.3	iPhone	10/28/2016 09:10:14 am	12 days

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

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

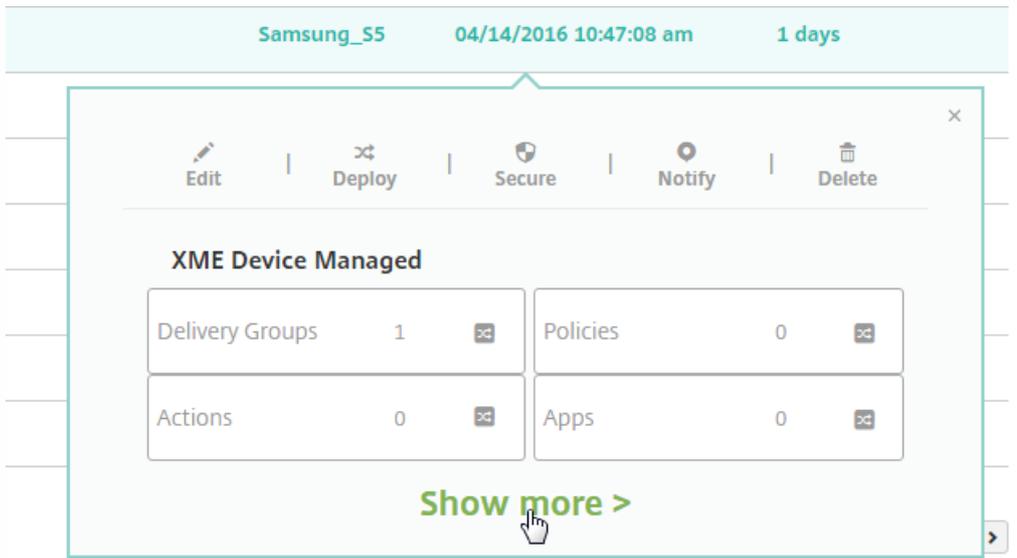


3. Confirme la acción.

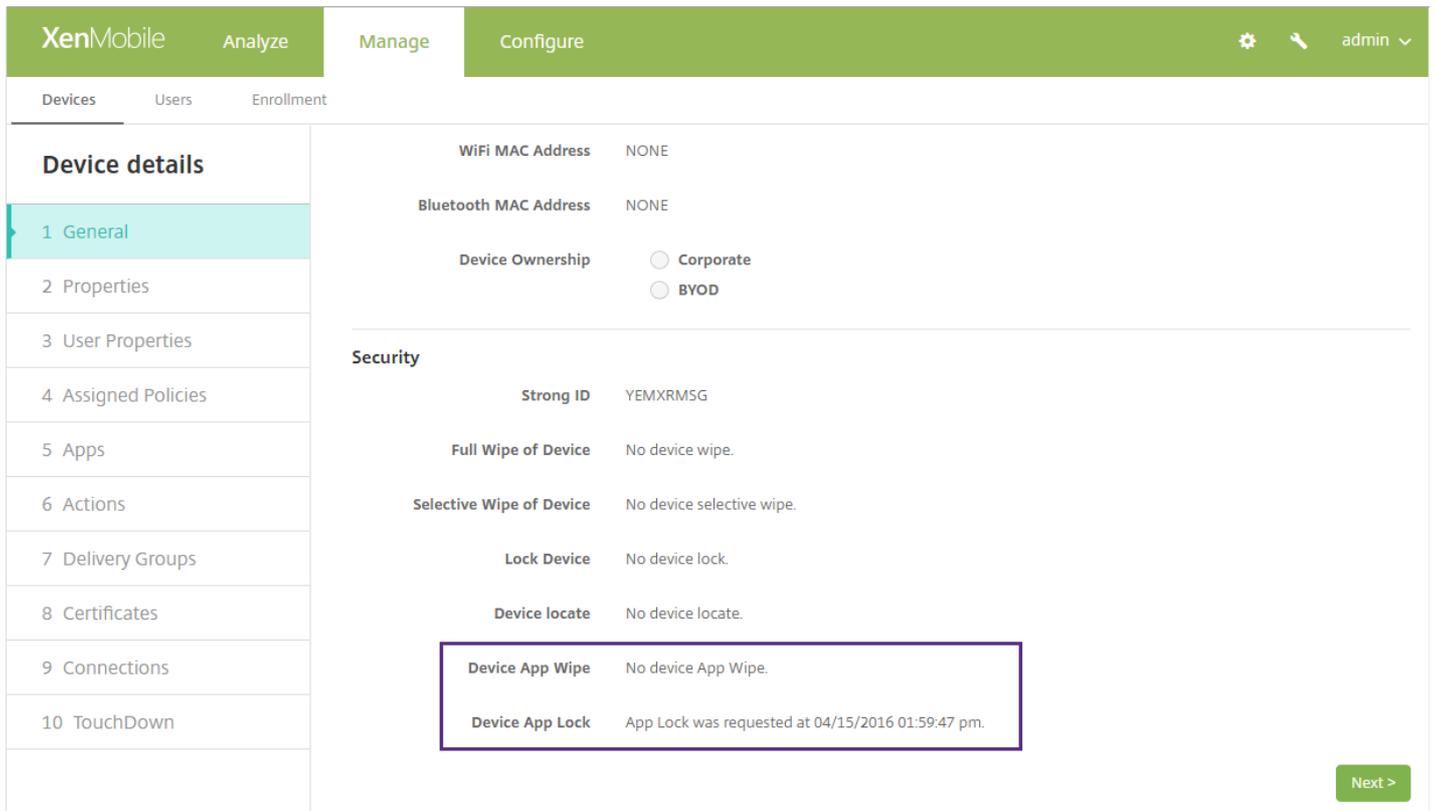


## Para comprobar el estado del bloqueo o borrado de las aplicaciones

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

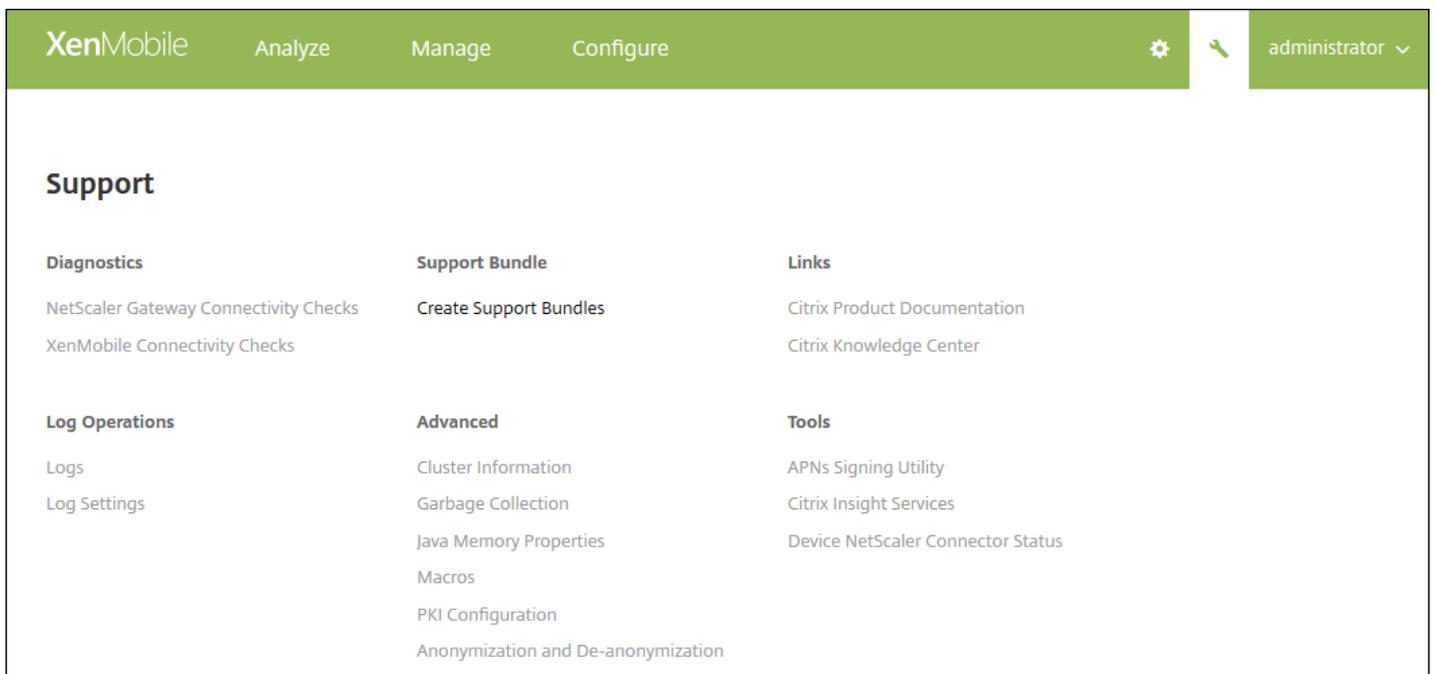
Mar 02, 2017

Use la página Support de XenMobile para acceder a un repertorio de datos informativos y herramientas relacionadas con la asistencia. También puede realizar acciones desde la interfaz de línea de comandos. Para obtener información más detallada, consulte [Opciones de la interfaz de línea de comandos](#).

En 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

# Informes

Mar 02, 2017

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

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

Mar 02, 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**.

The screenshot shows the XenMobile web interface. At the top, there is a green navigation bar with the XenMobile logo and tabs for 'Analyze', 'Manage', and 'Configure'. On the right side of the bar, there is a gear icon for settings and a user profile icon labeled 'admin'. Below the navigation bar, the breadcrumb path is 'Settings > Mobile Service Provider'. The main heading is 'Mobile Service Provider', followed by a descriptive text: 'Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.' The configuration form includes three input fields: 'Web service URL\*' with the value 'http://XmmServer/services/zdm', 'User name\*' with the value 'domain\admin', and 'Password\*'. Below these fields is a toggle switch for 'Automatically update BlackBerry and ActiveSync device connections', which is currently set to 'OFF'. At the bottom of the form is a green 'Test Connection' button. In the bottom right corner, there are 'Cancel' and 'Save' buttons.

3. Configure los siguientes 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

Mar 02, 2017

Puede configurar XenMobile para enviar archivos de registros a un servidor de registros de sistemas (syslog). Se necesita el nombre de host del servidor o la dirección IP.

Syslog es un protocolo estándar de captura de registros con dos componentes: un módulo de auditoría (que se ejecuta en el dispositivo) y un servidor (que se puede ejecutar en un sistema remoto). El protocolo Syslog usa el protocolo de datos de usuario (UDP) para la transferencia de datos. Se graban los eventos de administrador y los eventos de usuario.

Puede configurar el servidor para recopilar los siguientes tipos de información:

- Registros del sistema que contienen un registro de las acciones que lleva a cabo XenMobile.
- Registros de auditoría que contienen un registro cronológico de las actividades del sistema referentes a XenMobile.

La información de registro que obtiene un servidor syslog desde un dispositivo se almacena en un archivo de registros en forma de mensajes. Por regla general, estos mensajes contienen la siguiente información:

- La dirección IP del dispositivo que generó el mensaje de registro
- Una marca de tiempo
- El tipo de mensaje
- El nivel de registro asociado a un evento (crítico, error, aviso, advertencia, informativo, depuración, alerta o emergencia)
- La información del mensaje

Puede usar esta información para analizar el origen de la alerta y, si fuera necesario, realizar las correcciones oportunas.

## Nota

En implementaciones de 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 **Descargar todo** para poder obtener los registros del sistema. Para obtener más información, consulte [Cómo ver y analizar archivos de registros en XenMobile](#).

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

XenMobile Analyze Manage Configure

admin

Settings > SysLog

## SysLog

You can configure XenMobile to send log files to a systems log (syslog) server using the server host name or IP address.

Server\*

Port\*

Information to log

System Logs ?

Audit ?

Cancel Save

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**.

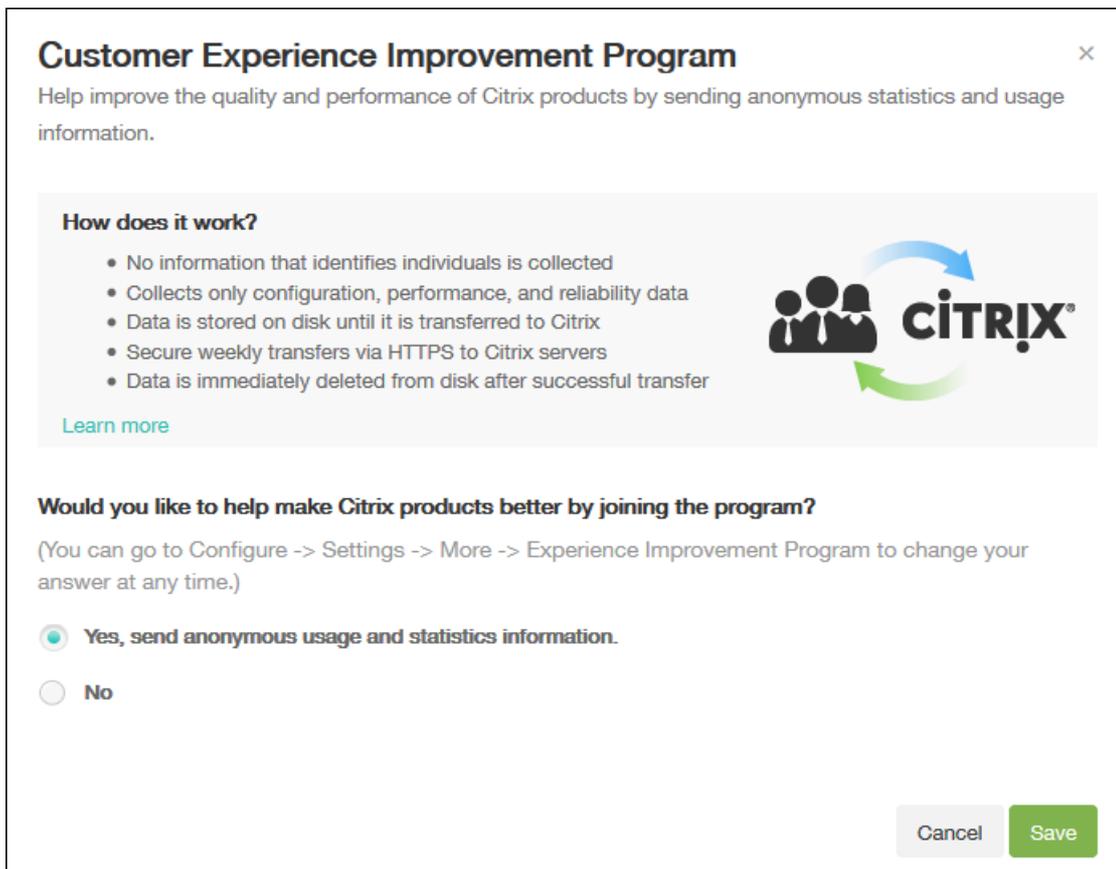
# Programa para la mejora de la experiencia del usuario

Mar 02, 2017

El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información anónima de uso y de configuración de XenMobile y envía esos datos automáticamente a Citrix. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de XenMobile. La participación en el programa CEIP es voluntaria. La opción de participar en el programa CEIP se ofrece la primera vez que se instala XenMobile o una actualización. Si participa en el programa, los datos de configuración se recopilan normalmente una vez por semana, mientras que los datos de uso y rendimiento se recopilan cada hora. Los datos se guardan en disco y se transfieren de manera segura vía HTTPS a Citrix una vez por semana. Puede cambiar la participación en el programa CEIP en la consola de XenMobile. Para obtener más información acerca del programa para la mejora de la experiencia del usuario, consulte [Acercas del programa Customer Experience Improvement Program de Citrix \(CEIP\)](#).

## Participación optativa en el programa CEIP

La primera vez que se instala XenMobile o cuando se realiza una actualización, aparece el siguiente cuadro de diálogo que pregunta si desea participar en el programa.



The screenshot shows a dialog box titled "Customer Experience Improvement Program" with a close button (X) in the top right corner. Below the title is the text: "Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information." The dialog is divided into two main sections. The first section, "How does it work?", contains a list of five bullet points: "No information that identifies individuals is collected", "Collects only configuration, performance, and reliability data", "Data is stored on disk until it is transferred to Citrix", "Secure weekly transfers via HTTPS to Citrix servers", and "Data is immediately deleted from disk after successful transfer". To the right of this list is a graphic showing three stylized human figures with arrows forming a circle around the Citrix logo. Below the list is a "Learn more" link. The second section asks, "Would you like to help make Citrix products better by joining the program?" and includes a sub-note: "(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)". There are two radio button options: "Yes, send anonymous usage and statistics information." (which is selected) and "No". At the bottom right, there are "Cancel" and "Save" buttons.

## Cómo cambiar el parámetro de participación en el programa CEIP

1. Para cambiar el parámetro de participación en el programa CEIP, en la consola de XenMobile, haga clic en el icono con forma de engranaje ubicado en la esquina superior derecha de la consola para abrir la página **Settings**.
2. En **Server**, haga clic en **Experience Improvement Program**. Aparecerá la página **Customer Experience Improvement**

**Program.** La página exacta que vea depende de si participa actualmente en el programa CEIP.

The screenshot shows the XenMobile interface. At the top, there is a green navigation bar with the XenMobile logo and menu items: Analyze, Manage, and Configure. On the right side of the bar, there is a gear icon, a magnifying glass icon, and a user profile labeled 'admin' with a dropdown arrow. Below the navigation bar, the breadcrumb path is 'Settings > Experience Improvement Program'. The main heading is 'Customer Experience Improvement Program' with a sub-heading: 'Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.' A section titled 'How does it work?' contains a bulleted list of details about data collection and transfer. To the right of this list is a graphic showing three stylized people icons and the Citrix logo, with a blue arrow pointing from the people to the logo and a green arrow pointing from the logo back to the people. Below the list is a 'Learn more' link. Underneath, a status message reads 'You are currently participating in the Customer Experience Improvement Program.' There are two radio button options: 'Continue participating' (which is selected) and 'Stop participating'. At the bottom right, there are 'Cancel' and 'Save' buttons.

XenMobile Analyze Manage Configure

Settings > Experience Improvement Program

## Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

### How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)

You are currently participating in the Customer Experience Improvement Program.

Continue participating

Stop participating

Cancel Save

3. Si participa actualmente en el programa CEIP y quiere dejar de hacerlo, haga clic en **Stop participating**.

4. Si no participa actualmente en el programa CEIP y quiere hacerlo, haga clic en **Start participating**.

5. Haga clic en **Save**.

# GoToAssist y Remote Support

Mar 02, 2017

Puede ofrecer a los usuarios diferentes métodos para ponerse en contacto con el personal de asistencia técnica: correos electrónicos, números de teléfono o tokens de GoToAssist en XenMobile. Cuando los usuarios soliciten asistencia desde sus dispositivos, verán las opciones que haya configurado.

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**.

**Settings**

<b>Certificate Management</b>	<b>Notifications</b>	<b>Server</b>	<b>Frequently Accessed</b> <ul style="list-style-type: none"><li>Certificates</li><li>Enrollment</li><li>Licensing</li><li>Local Users and Groups</li><li>Role-Based Access Control</li><li>Release Management</li></ul>
Certificates	Carrier SMS Gateway	ActiveSync Gateway	
Credential Providers	Notification Server	Enrollment	
PKI Entities	Notification Templates	LDAP	
		Licensing	
<b>Client</b>	<b>Platforms</b>	Local Users and Groups	
Client Branding	Android for Work	Mobile Service Provider	
Client Properties	Google Play Credentials	NetScaler Gateway	
Client Support	iOS Bulk Enrollment	Network Access Control	
	iOS Settings	Release Management	
	Samsung KNOX	Role-Based Access Control	
		Server Properties	
		SysLog	
		Workflows	
		XenApp/XenDesktop	

2. En **Client**, haga clic en **Client Support**. Aparecerá la página **Client Support**.

XenMobile Analyze Manage Configure ⚙️ 🔑 admin ▾

Settings > Client Support

### Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)\*

Send device logs to IT help desk  directly ?  by email ?

Cancel Save

3. Configure los siguientes parámetros:

- **GoToAssist chat token.** Escriba el token que reciben los usuarios para iniciar una sesión de GoToAssist.
- **GoToAssist support ticket email.** La dirección de correo electrónico que los usuarios usan para los tíquets de asistencia de GoToAssist.
- **Support phone (IT help desk).** Escriba el número de teléfono del servicio de asistencia de TI.
- **Support email (IT help desk).** Escriba la dirección de correo electrónico de contacto referente al servicio de asistencia de TI.
- **Send device logs to IT help desk.** Seleccione si los registros de dispositivo se envían directamente o por correo electrónico en las opciones respectivas **directly** o **by email**. El valor predeterminado es **by email**.
  - Cuando se habilita **directly**, en ShareFile aparecen opciones de almacenamiento de registros. Si se habilita la opción de almacenamiento de registros en ShareFile, los registros se enviarán directamente a ShareFile; de lo contrario, se enviarán primero a XenMobile y luego por correo electrónico al servicio de asistencia de TI. Además, aparecerá la opción **If sending directly fails, use email**, habilitada de forma predeterminada. Puede inhabilitar esta opción si no quiere utilizar el correo electrónico del cliente para enviar registros en caso de que haya problemas con el servidor. Sin embargo, si quiere inhabilitar esta opción y hay problemas con el servidor, los registros no se enviarán.
  - Al habilitar la opción **by mail**, siempre se usará el correo electrónico del cliente para enviar los registros.

4. Haga clic en **Save**.

## Remote Support

La asistencia remota (Remote Support) permite que el personal de Help Desk tome el control remoto de los dispositivos móviles Windows y Android administrados.

Remote Support está disponible en todos los dispositivos móviles Windows, en los dispositivos Samsung SAFE de Android y en los dispositivos que no sean de Samsung.

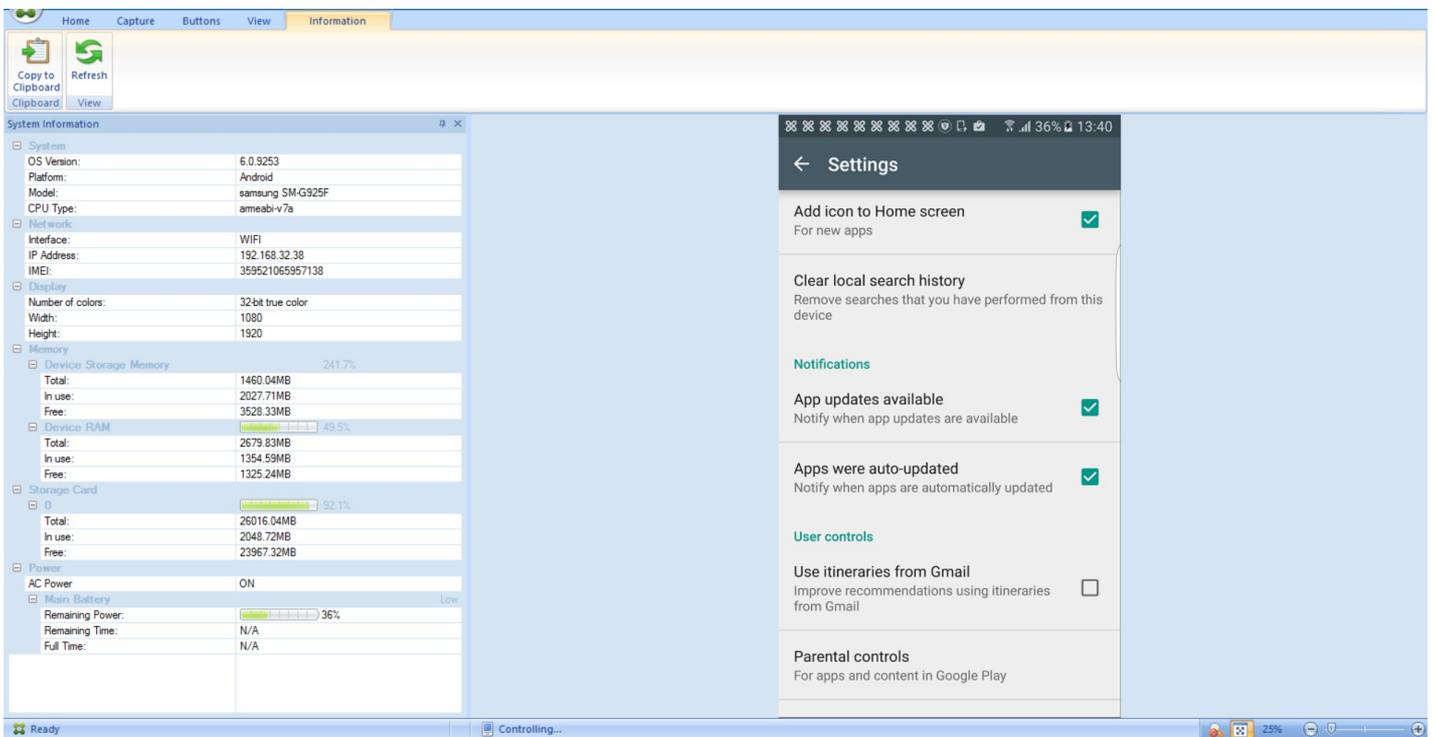
La transmisión de la pantalla solo se admite en dispositivos Samsung KNOX.

No se respalda el control remoto de dispositivos iOS.

Remote Support está disponible en las versiones 10.x de XenMobile Service (nube).

Durante una sesión de control remoto:

- Los usuarios ven un icono en su dispositivo móvil que indica que hay una sesión de control remoto activa.
- Los usuarios de asistencia remota ven la ventana de la aplicación Remote Support y una ventana de control remoto con una representación del dispositivo controlado.



Con Remote Support, puede hacer lo siguiente:

- Iniciar sesión de forma remota en el dispositivo móvil de un usuario y controlar la pantalla. Los usuarios pueden verle a usted navegar por la pantalla, lo que puede ser útil con fines de aprendizaje y capacitación.
- Desplazarse y reparar un dispositivo remoto en tiempo real. Puede cambiar las configuraciones, solucionar problemas del sistema operativo e inhabilitar o detener las aplicaciones o los procesos que sean problemáticos.
- Aislar y contener posibles amenazas de seguridad antes de que se propaguen a otros dispositivos móviles inhabilitando el acceso a la red de forma remota, detener procesos no autorizados o sospechosos y quitar aplicaciones o malware.
- Habilitar de forma remota el timbre del dispositivo y llamar al teléfono, para ayudar al usuario a encontrarlo. Si un usuario

no puede encontrar el dispositivo, puede borrarlo para salvaguardar la información confidencial que pueda contener.

Remote Support también permite al personal de asistencia técnica:

- Mostrar una lista de todos los dispositivos conectados en uno o más servidores XenMobile.
- Mostrar información del sistema, incluidos el modelo del dispositivo, el nivel del sistema operativo, la identidad de equipo móvil internacional (IMEI) y el número de serie, el estado de la memoria y la batería, y la conectividad.
- Mostrar los usuarios y los grupos del servidor XenMobile.
- Ejecutar el administrador de tareas del dispositivo donde se pueden ver y finalizar procesos activos y reiniciar el dispositivo móvil.
- Ejecutar transferencias remotas de archivos que incluyen la transferencia bidireccional de archivos entre los dispositivos móviles y un servidor de archivos central.
- Descargar e instalar programas de software como un lote para uno o más dispositivos móviles.
- Configurar las opciones de la clave del Registro remota en el dispositivo.
- Optimizar el tiempo de respuesta en las redes celulares de ancho de banda bajo mediante el uso del control remoto en tiempo real en la pantalla del dispositivo.
- Mostrar la máscara del dispositivo para la mayoría de los modelos y marcas de dispositivo móvil. Mostrar un editor de máscaras para agregar nuevos modelos de dispositivo y asignar teclas físicas.
- Habilitar la captura de pantallas del dispositivo, grabar y reproducir con la capacidad de capturar una secuencia de interacciones en el dispositivo y crear un archivo de vídeo AVI.
- Llevar a cabo reuniones con una pizarra compartida, comunicaciones de voz basadas en VoIP y chat entre usuarios móviles y el personal de asistencia técnica.

## Requisitos del sistema para Remote Support

El software de Remote Support se puede instalar en equipos Windows que cumplan los siguientes requisitos. Para obtener los requisitos de puerto, consulte [Requisitos de puertos](#).

Plataformas respaldadas:

- Intel Xeon o Pentium 4: mínimo 1 GHz de clase de estación de trabajo
- 512 MB de RAM (mínimo).
- 100 MB de espacio libre en disco (mínimo)

Sistemas operativos respaldados:

- Microsoft Windows 2003 Server Standard Edition o Enterprise Edition SP1 o versiones posteriores
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 o versiones posteriores
- Microsoft Windows Vista SP1 o versiones posteriores
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

## Para instalar el software de Remote Support

1. Para descargar el instalador de Remote Support, vaya a la [página de descargas de XenMobile 10](#) e inicie sesión en su cuenta.
2. Expanda **Tools** y, a continuación, descargue XenMobile Remote Support v9.

El nombre de archivo de Remote Support es actualmente XenMobileRemoteSupport-9.0.0.35265.exe.

3. Haga doble clic en el instalador de Remote Support y, a continuación, siga las instrucciones del asistente de instalación.

### Para instalar Remote Support desde la línea de comandos:

Ejecute el comando siguiente:

```
RemoteSupport.exe /S
```

donde *RemoteSupport* es el nombre del programa de instalación. Por ejemplo:

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

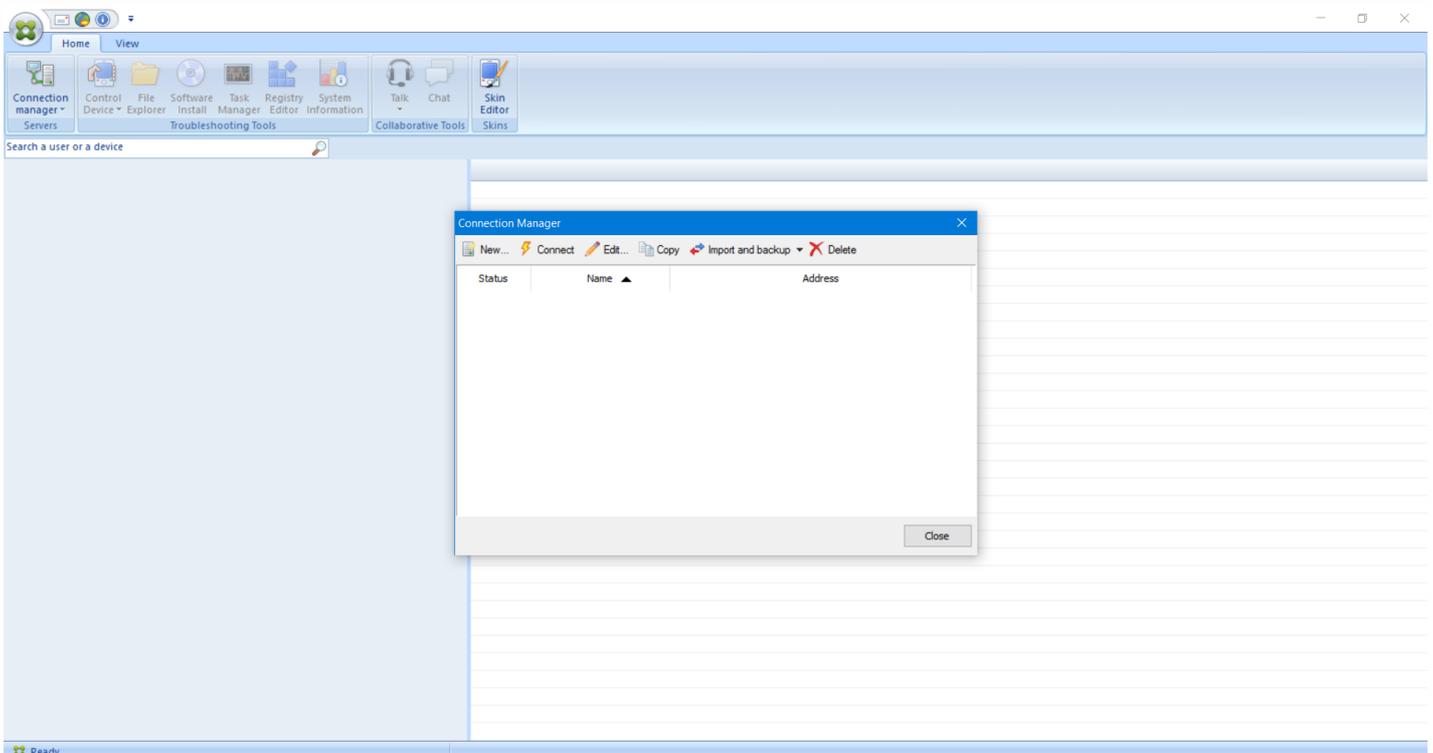
Puede utilizar las siguientes variables al instalar el software de Remote Support:

- /S: para instalar de forma silenciosa el software de Remote Support con los parámetros predeterminados.
- /D=dir: para especificar un directorio de instalación personalizado.

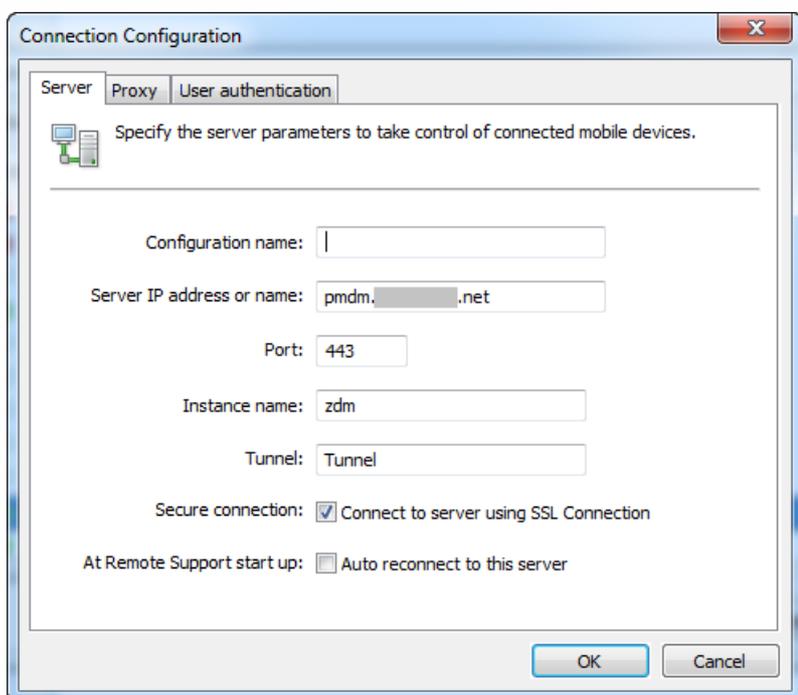
## Para conectar Remote Support a XenMobile

Para establecer conexiones de asistencia remota con dispositivos administrados, debe agregar una conexión desde Remote Support a uno o a varios servidores XenMobile que administran los dispositivos. Esta conexión se ejecuta a través de un túnel de aplicación definido en la directiva de túneles de MDM, una directiva de dispositivo para Android y Windows Mobile/CE. Debe definir el túnel de aplicación para poder conectar Remote Support a XenMobile. Para obtener más información, consulte [Directivas de túneles de aplicaciones](#).

1. Inicie el software de Remote Support y use credenciales de XenMobile para iniciar sesión.
2. En **Connection Manager**, haga clic en **New**.



3. En el cuadro de diálogo **Connection Configuration**, en la ficha **Server**, introduzca los siguientes valores:
  - a. En **Configuration name**, escriba un nombre para la entrada de configuración.
  - b. En **Server IP address or name**, escriba la dirección IP o el nombre DNS del servidor XenMobile.
  - c. En **Port**, escriba el número de puerto TCP, como se define en la configuración de servidor de XenMobile.
  - d. En **Instance name**, si XenMobile forma parte de una implementación multiarrendatario, escriba un nombre de instancia.
  - e. En **Tunnel**, escriba el nombre de la directiva de túnel.
  - f. Marque la casilla **Connect to server using SSL Connection**.
  - g. Marque la casilla **Auto reconnect to this server** para conectar con el servidor XenMobile configurado cada vez que se inicie la aplicación Remote Support.

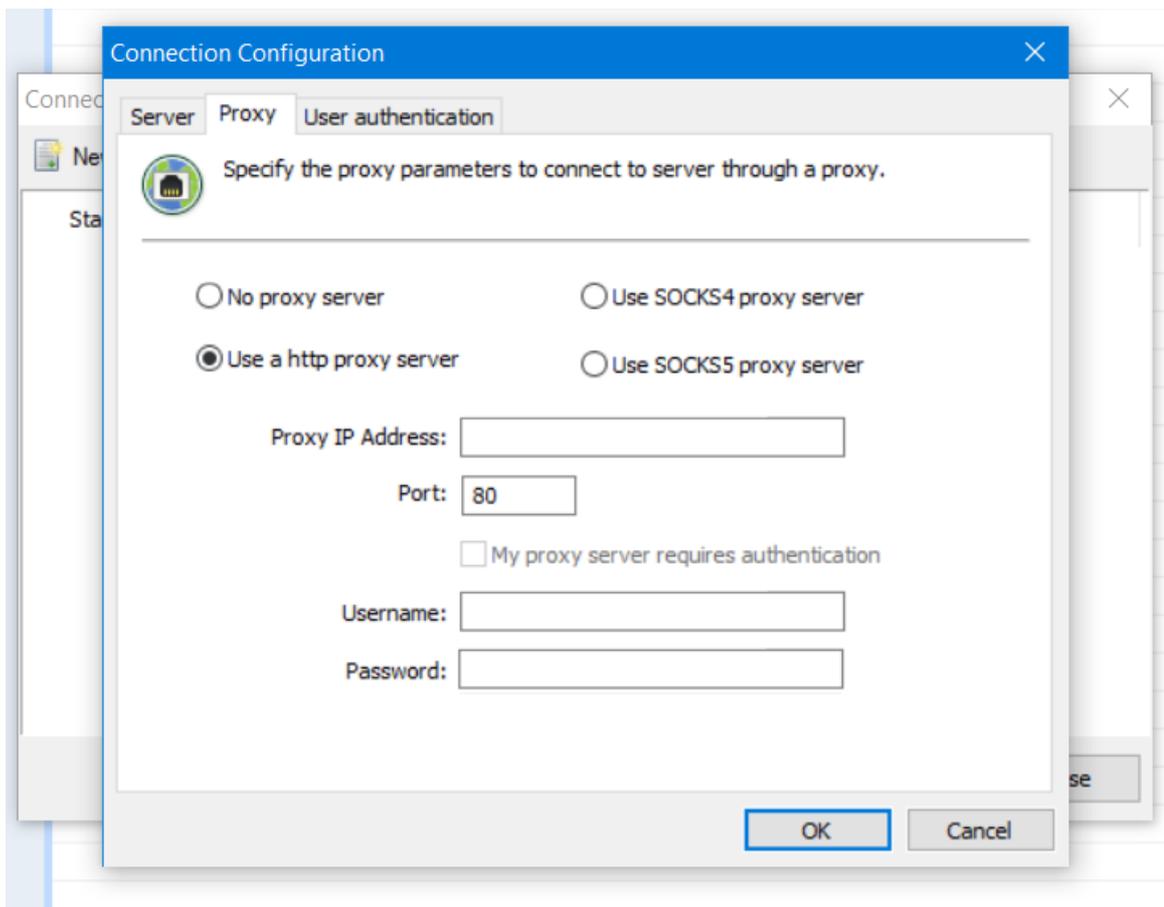


The screenshot shows the 'Connection Configuration' dialog box with the 'Server' tab selected. The dialog contains the following fields and options:

- Configuration name:** An empty text input field.
- Server IP address or name:** A text input field containing 'pmdm.[redacted].net'.
- Port:** A text input field containing '443'.
- Instance name:** A text input field containing 'zdm'.
- Tunnel:** A text input field containing 'Tunnel'.
- Secure connection:** A checked checkbox labeled 'Connect to server using SSL Connection'.
- At Remote Support start up:** An unchecked checkbox labeled 'Auto reconnect to this server'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

4. En la ficha **Proxy**, seleccione **Use a http proxy server** y, a continuación, introduzca la información siguiente:
  - a. En **Proxy IP Address**, escriba la dirección IP del servidor proxy.
  - b. En **Port**, escriba el número de puerto TCP utilizado por el proxy.
  - c. Marque la casilla de **My proxy requires authentication** si el servidor proxy requiere autenticación antes de transmitir tráfico.
  - d. En **Username**, escriba el nombre de usuario con el que autenticarse en el servidor proxy.
  - e. En **Password**, escriba la contraseña con la que autenticarse en el servidor proxy.



5. En la ficha **User Authentication**, marque la casilla **Remember my login and password** e introduzca las credenciales.

6. Haga clic en **OK**.

Para conectarse a XenMobile, haga doble clic en la conexión que ha creado y, a continuación, escriba el nombre de usuario y la contraseña que ha configurado para la conexión.

## Para habilitar la asistencia remota para dispositivos Samsung KNOX

En XenMobile, puede crear una directiva de asistencia remota (Remote Support) mediante la que puede acceder de forma remota a los dispositivos Samsung KNOX de los usuarios. Puede configurar dos tipos de asistencia:

- **Basic.** Esta opción permite ver la información de diagnóstico referente al dispositivo, como la información del sistema, los procesos que se están ejecutando, el administrador de tareas (el uso de memoria y de CPU) o el contenido de las carpetas del software instalado, entre otros.
- **Premium.** Esta opción permite controlar de forma remota la pantalla del dispositivo, incluido el control sobre los colores (ya sea en la ventana principal o en una ventana separada flotante). Asimismo, permite establecer una sesión mediante voz sobre IP (VoIP) entre el servicio de asistencia técnica y el usuario, configurar parámetros y establecer una sesión de chat entre el usuario y el departamento de asistencia técnica.

Con la asistencia Premium, debe configurar la directiva Samsung MDM License Key en la consola de XenMobile. Cuando configure esta directiva, seleccione solamente la plataforma **Samsung KNOX**. No es necesario configurar la plataforma Samsung SAFE para este caso, porque la clave ELM se implementa automáticamente en dispositivos Samsung cuando se

inscriben en XenMobile. Para obtener más información, consulte [Clave de licencia para la administración de dispositivos móviles \(MDM\) Samsung](#).

Para obtener información sobre la configuración de la directiva de asistencia remota Remote Support, consulte la [directiva de asistencia remota](#).

## Para usar una sesión de Remote Support

Después de iniciar la aplicación Remote Support, en el lado izquierdo de la ventana de la aplicación Remote Support, se presentan los grupos de usuarios de XenMobile, tal y como se han definido en la consola de XenMobile. De forma predeterminada, solo aparecen los grupos que contienen usuarios que están conectados. Puede ver el dispositivo de cada usuario junto a la entrada del usuario.

1. Para ver todos los usuarios, expanda cada grupo de la columna de la izquierda.  
Los usuarios actualmente conectados al servidor XenMobile se indican con un icono verde.
2. Para mostrar todos los usuarios, incluidos los que no están conectados, haga clic en **View** y seleccione **Non-connected devices**.  
Los usuarios no conectados aparecen sin el icono verde.

Los dispositivos conectados al servidor XenMobile pero no asignados a ningún usuario aparecen en modo anónimo. (La cadena **Anonymous** aparece en la lista). Puede controlar estos dispositivos igual que lo hace con los dispositivos donde un usuario ha iniciado una sesión.

Para controlar un dispositivo, seleccione el dispositivo haciendo clic en su fila y luego haga clic en **Control Device**. En la ventana de control remoto aparece una representación del dispositivo. Puede interactuar con el dispositivo controlado, de estas formas:

- Controlar la pantalla del dispositivo, incluidos los colores, en la ventana principal o en la ventana aparte, flotante.
- Establecer una sesión VoIP entre servicio de Help Desk y el usuario. Configurar los parámetros de VoIP.
- Establecer una sesión de chat con el usuario.
- Acceder al administrador de tareas del dispositivo para administrar elementos como, por ejemplo, el uso de memoria, el uso de la CPU, y las aplicaciones que se estén ejecutando.
- Explorar los directorios locales del dispositivo móvil. Transferir archivos.
- Editar el Registro del dispositivo en dispositivos Windows Mobile.
- Mostrar información del sistema del dispositivo y todo el software instalado.
- Actualizar el estado de la conexión del dispositivo móvil con el servidor XenMobile.

# Creación de opciones de asistencia de Secure Hub y GoToAssist

Mar 02, 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 presentes en dispositivos móviles iOS y Android.

**Nota:** Antes de comenzar, compruebe que tienen preparada su imagen de personalización de marca y 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**.

**Settings**

Certificate Management	Notifications	Server	Frequently Accessed
Certificates	Carrier SMS Gateway	ActiveSync Gateway	Certificates
Credential Providers	Notification Server	Enrollment	Enrollment
PKI Entities	Notification Templates	LDAP	Licensing
		Licensing	Local Users and Groups
<b>Client</b>	<b>Platforms</b>	Local Users and Groups	Role-Based Access Control
Client Branding	Android for Work	Mobile Service Provider	Release Management
Client Properties	Google Play Credentials	NetScaler Gateway	
Client Support	iOS Bulk Enrollment	Network Access Control	
	iOS Settings	Release Management	
	Samsung KNOX	Role-Based Access Control	
		Server Properties	
		SysLog	
		Workflows	
		XenApp/XenDesktop	

2. En **Client**, haga clic en **Client Branding**. Aparecerá la página **Client Branding**.

XenMobile Analyze Manage Configure admin

Settings > Client Branding

### Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

**Store name\***  ?

**Default store view**

Category

A-Z

**Device**

Phone

Tablet

**Branding file**

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

3. 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 de imagen o un archivo .zip para usarlo como personalización de marca, haga clic en **Browse** y vaya a la ubicación del archivo.

4. Haga clic en **Save**.

Para implementar este paquete en los dispositivos de los usuarios, debe crear un paquete de implementación.

# Comprobaciones de conectividad

Mar 02, 2017

En la página **Support** de XenMobile, puede comprobar la conexión de XenMobile con NetScaler Gateway y con otros servidores y ubicaciones.

## Comprobaciones de conectividad de XenMobile

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa, situado en la esquina superior derecha de la consola. Aparecerá la página **Support**.
2. En **Diagnostics**, haga clic en **XenMobile Connectivity Checks**. Aparecerá la página **XenMobile Connectivity Checks**. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.

<input type="checkbox"/>	Connectivity to	IP address or FQDN
<input type="checkbox"/>	Windows Phone Store	windowsphone.com
<input type="checkbox"/>	Database	.net
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com
<input type="checkbox"/>	LDAP	.net
<input type="checkbox"/>	Domain Name System (DNS)	
<input type="checkbox"/>	Nexmo Gateway	-
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
<input type="checkbox"/>	Google Play	play.google.com
<input type="checkbox"/>	Windows Security Token Service	login.live.com

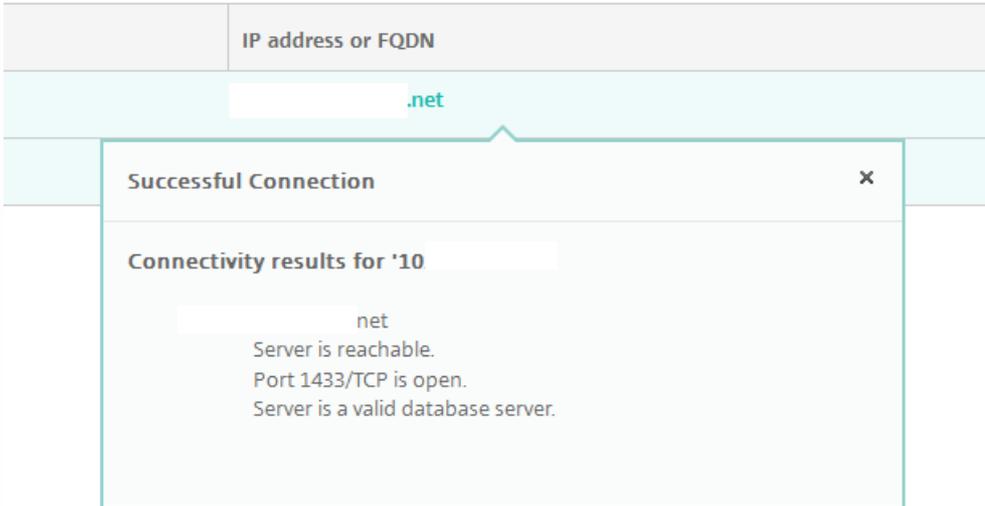
2. Seleccione los servidores a incluir en la prueba de conectividad y, a continuación, haga clic en **Test Connectivity**. Aparecerá la página de resultados de pruebas.

<input type="checkbox"/>	Connectivity to	IP address or FQDN	Status
<input type="checkbox"/>	Database	net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

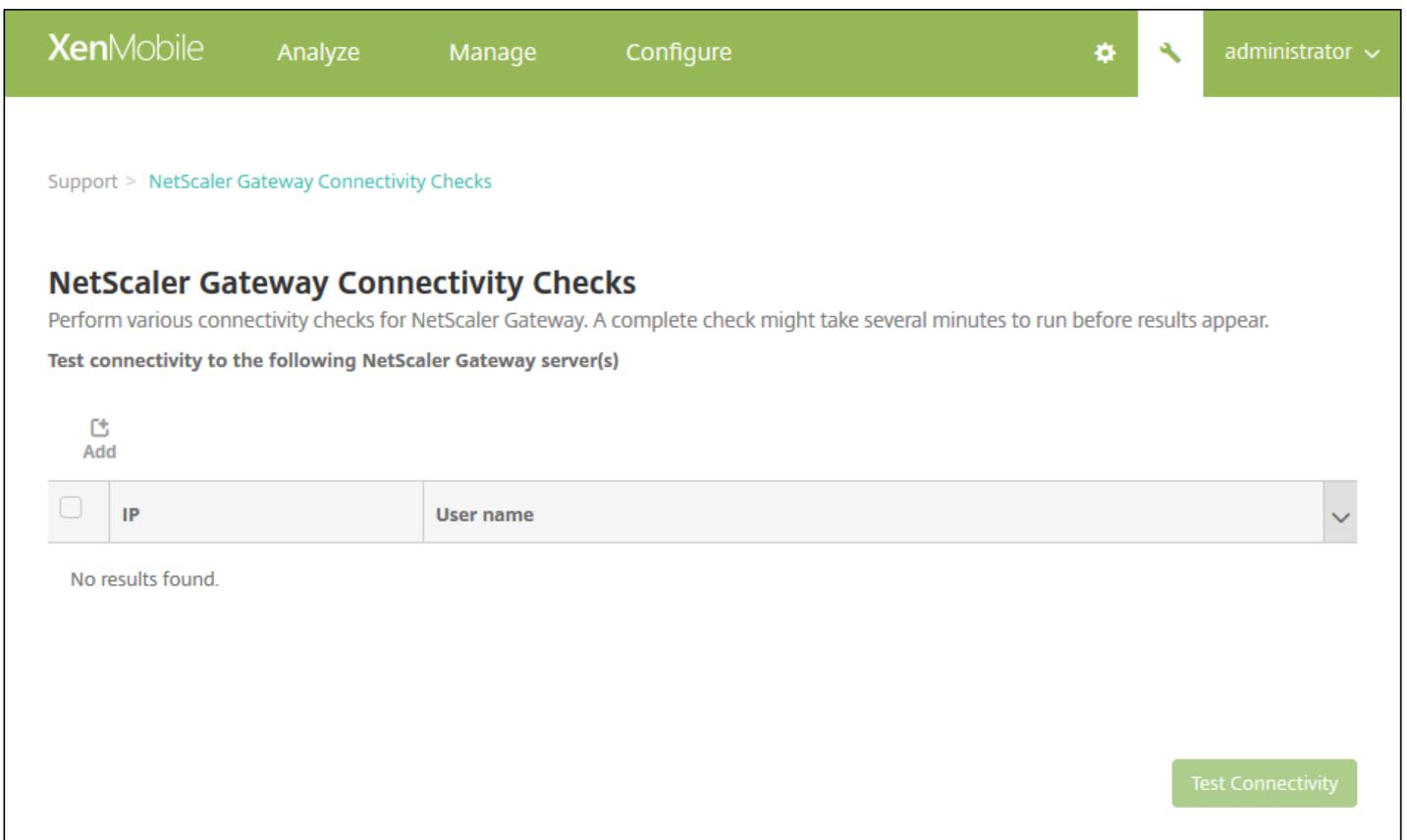
Clear Results Test Connectivity

3. Seleccione un servidor de la tabla Test Results para ver los resultados detallados de dicho servidor.

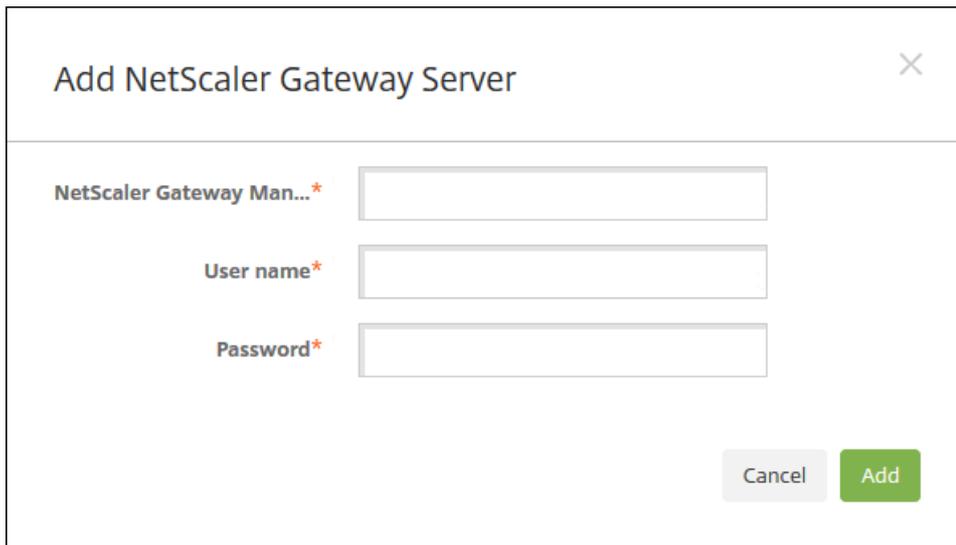


### Comprobaciones de conectividad de NetScaler Gateway

1. En la página **Support**, en **Diagnostics**, haga clic en **NetScaler Gateway Connectivity Checks**. Aparecerá la página **NetScaler Gateway Connectivity Checks**. La tabla está vacía si no ha agregado servidores NetScaler Gateway.



2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add NetScaler Gateway Server**.



The screenshot shows a dialog box titled "Add NetScaler Gateway Server" with a close button (X) in the top right corner. The dialog contains three input fields, each with a label and an asterisk indicating it is required: "NetScaler Gateway Man..." (truncated), "User name", and "Password". At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

3. En **NetScaler Gateway Management IP**, escriba la dirección IP del servidor con NetScaler Gateway que usted quiere probar.

**Nota:** Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado, se proporciona la dirección IP.

4. Escriba las credenciales de administrador de este servidor NetScaler Gateway.

**Nota:** Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado, se proporciona el nombre de usuario.

5. Haga clic en **Add**. El servidor NetScaler Gateway se agrega a la tabla en la página **NetScaler Gateway Connectivity Checks**.

6. Haga clic en **Test Connectivity**. Los resultados aparecerán en la tabla Test Results.

7. Seleccione un servidor de la tabla Test Results para ver los resultados detallados de dicho servidor.

# Paquetes de asistencia

Mar 02, 2017

Para informar a Citrix de un problema o para solucionar un problema, puede crear un paquete de asistencia y cargarlo en Citrix Insight Services (CIS).

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. Aparecerá la página **Support**.
2. En la página **Support**, haga clic en **Create Support Bundles**. Aparecerá la página **Create Support Bundles**. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.

The image displays two screenshots of the XenMobile web interface for creating support bundles. Both screenshots show the top navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, and a user profile dropdown in the top right corner.

The top screenshot shows the user 'admin' and the page title 'Create Support Bundles'. The description reads: 'Create support bundles with system information, logs, database information, core information, trace files, and the latest configuration information.' The 'Support Bundle for XenMobile' checkbox is checked. Below it, 'Support Bundle for\*' is set to 'Cluster' and '192.0.2.24' is also checked.

The bottom screenshot shows the user 'administrator' and the same page title. The description is identical. The 'Support Bundle for XenMobile' checkbox is checked. 'Support Bundle for\*' is set to '198.51.100.3'. Under 'Include from database\*', there are radio buttons for 'No data' (selected), 'Custom data', and 'All data'. Under 'Custom data', there are checkboxes for 'Configuration data', 'Delivery group data', and 'Devices and user info'. A note at the bottom states: 'Support data anonymization is turned on. To change anonymity settings? [Anonymization and de-anonymization](#)'. At the bottom right, there is a green 'Create' button.

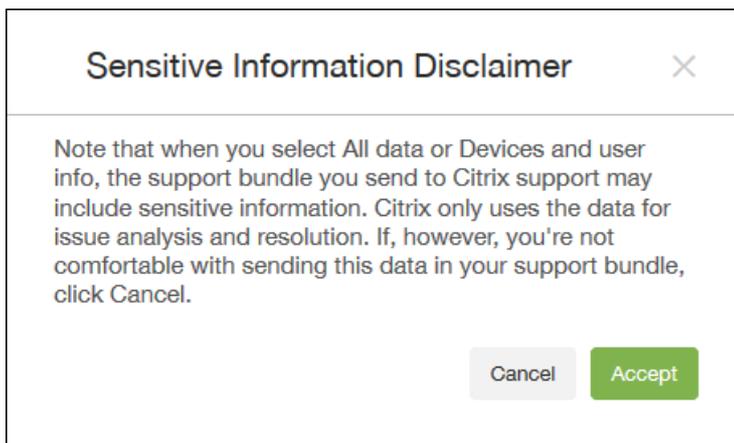
3. Compruebe que está marcada la casilla **Support Bundle for XenMobile**.

4. Si su entorno de XenMobile contiene nodos en clúster, en **Support Bundle for**, seleccione todos los nodos o cualquier combinación de nodos de los que obtener datos.

5. En **Include from Database**, realice una de las siguientes acciones:

- Haga clic en **No data**.
- Haga clic en **Custom data** y después seleccione cualquiera de las opciones siguientes (de manera predeterminada, están seleccionadas todas):
  - **Configuration data**. Incluye las configuraciones de certificados y las directivas del administrador de dispositivos.
  - **Delivery group data**. Incluye información acerca de las aplicaciones de los grupos de entrega; esta información contiene detalles acerca de los tipos de aplicación y sobre las directivas referentes a la entrega de aplicaciones.
  - **Devices and user info**. Incluye aplicaciones, acciones, grupos de entrega y directivas de dispositivos.
- Haga clic en **All data**.

**Nota:** Si elige **Devices and user info** o **All data** y este es el primer paquete de asistencia que crea, aparecerá el cuadro de diálogo **Sensitive Information Disclaimer**. Lea el aviso de declinación de responsabilidades y, a continuación, haga clic en **Accept** o **Cancel**. Si hace clic en **Cancel**, el paquete de asistencia no se podrá cargar en Citrix. Si hace clic en **Accept**, podrá cargar el paquete de asistencia en Citrix y no verá el aviso de declinación de responsabilidades la próxima vez que se cree un paquete de asistencia que incluya datos de usuario o dispositivo.



6. La opción **Support data anonymization is turned on** indica que el parámetro predeterminado es hacer que los datos sean anónimos, lo que significa que los datos de carácter privado de los usuarios, servidores y red se hacen anónimos en los paquetes de asistencia.

Para cambiar esta configuración, haga clic en **Anonymization and de-anonymization**. Para obtener más información acerca del anonimato de datos, consulte [Anonimato de datos en paquetes de asistencia](#).

7. Marque la casilla **Support Bundle for NetScaler Gateway** para incluir paquetes de asistencia de NetScaler Gateway y, a continuación, haga lo siguiente:

- a. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Add NetScaler Gateway Server**.

**Add NetScaler Gateway Server**

NetScaler Gateway Management IP\*

User name\*

Password\*

Cancel Add

b. En **NetScaler Gateway Management IP**, escriba la dirección IP de administración de NetScaler referente al dispositivo NetScaler Gateway del que quiere extraer el paquete de asistencia.

**Nota:** Si va a crear un paquete de un servidor NetScaler Gateway que ya se ha agregado, se proporciona la dirección IP.

c. En **User name** y **Password**, escriba las credenciales de usuario necesarias para acceder al servidor con NetScaler Gateway.

**Nota:** Si va a crear un paquete de un servidor NetScaler Gateway que ya se ha agregado, se proporciona el nombre de usuario.

7. Haga clic en **Add**. El nuevo paquete de asistencia de NetScaler Gateway se agrega a la tabla.

8. Repita el paso 7 para agregar más paquetes de asistencia de NetScaler Gateway.

9. Haga clic en **Create**. Se crea el paquete de asistencia y aparecen dos nuevos botones: **Upload to CIS** y **Download to Client**.

### Carga de paquetes de asistencia en Citrix Insight Services

Después de crear un paquete de asistencia, puede cargarlo en Citrix Insight Services (CIS) o descargarlo en su equipo. A continuación, se presentan los pasos necesarios para cargar el paquete en CIS. Necesita un ID y una contraseña de MyCitrix para cargar en CIS.

1. En la página **Create Support Bundles**, haga clic en **Upload to CIS**. Aparecerá el cuadro de diálogo **Upload to Citrix Insight Services (CIS)**.

Upload to Citrix Insight Services (CIS)

CIS Website cis.citrix.com

User name\* MyCitrix ID

Password\* MyCitrix password

Associate with SR#

Cancel Upload

2. En **User Name**, escriba su ID de MyCitrix.

3. En **Password**, escriba su contraseña de MyCitrix.

4. Para vincular este paquete con el número de una solicitud de servicio existente, marque la casilla de verificación **Associate with SR#** y, en los dos campos que aparecen, lleve a cabo lo siguiente:

- En **SR#**, escriba los 8 dígitos del número de solicitud de servicio a la que se va a asociar este paquete.
- En **SR Description**, escriba una descripción de la solicitud de servicio.

5. Haga clic en **Upload**.

Si es la primera vez que carga un paquete de asistencia en CIS y no ha creado ninguna cuenta en CIS con otro producto ni ha aceptado el acuerdo de recopilación de datos y privacidad, aparecerá el siguiente cuadro de diálogo. Debe aceptar el acuerdo para comenzar la carga. Si dispone de una cuenta en CIS y había aceptado el acuerdo, el paquete de asistencia se carga sin más preámbulos.

Data Collection and Privacy

By uploading your data to Citrix pursuant to the instructions on this website, you are agreeing that Citrix may store, transmit and use technical and related information about your use of your Citrix products, including configuration information, number and types of users, error reports, features enabled, performance, version and patch management information, and non-personally identifiable usage statistics ("Collected Data") to facilitate the provisioning of product updates, support, education, self-help tools, market assessment and analysis, product development, invoicing and online services. Collected Data is subject to Citrix's Privacy Policy.

Cancel Agree and upload

6. Lea el acuerdo y haga clic en **Agree and upload**. Se cargará el paquete de asistencia.

### Descarga de paquetes de asistencia en el equipo

Después de crear un paquete de asistencia, puede cargarlo en CIS o descargarlo en su equipo. Para resolver cualquier problema por su cuenta, descargue el paquete de asistencia en su equipo.

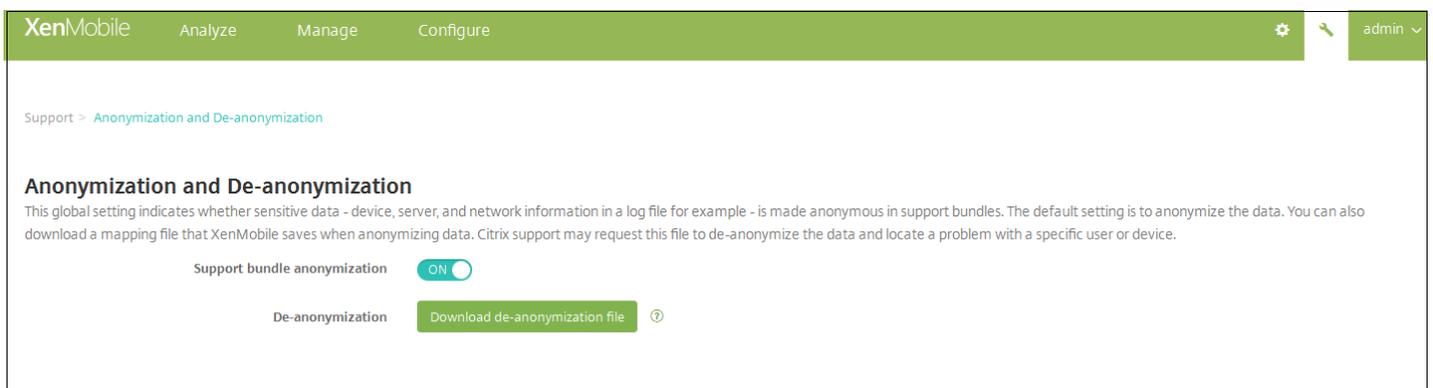
En la página Create Support Bundles, haga clic en Download to Client. El paquete se descargará en su equipo.

# Anonimato de datos en paquetes de asistencia

Mar 02, 2017

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

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. Aparecerá la página **Support**.
2. En la página **Support**, en **Advanced**, haga clic en **Anonymization and De-anonymization**. Aparecerá la página **Anonymization and De-anonymization**.



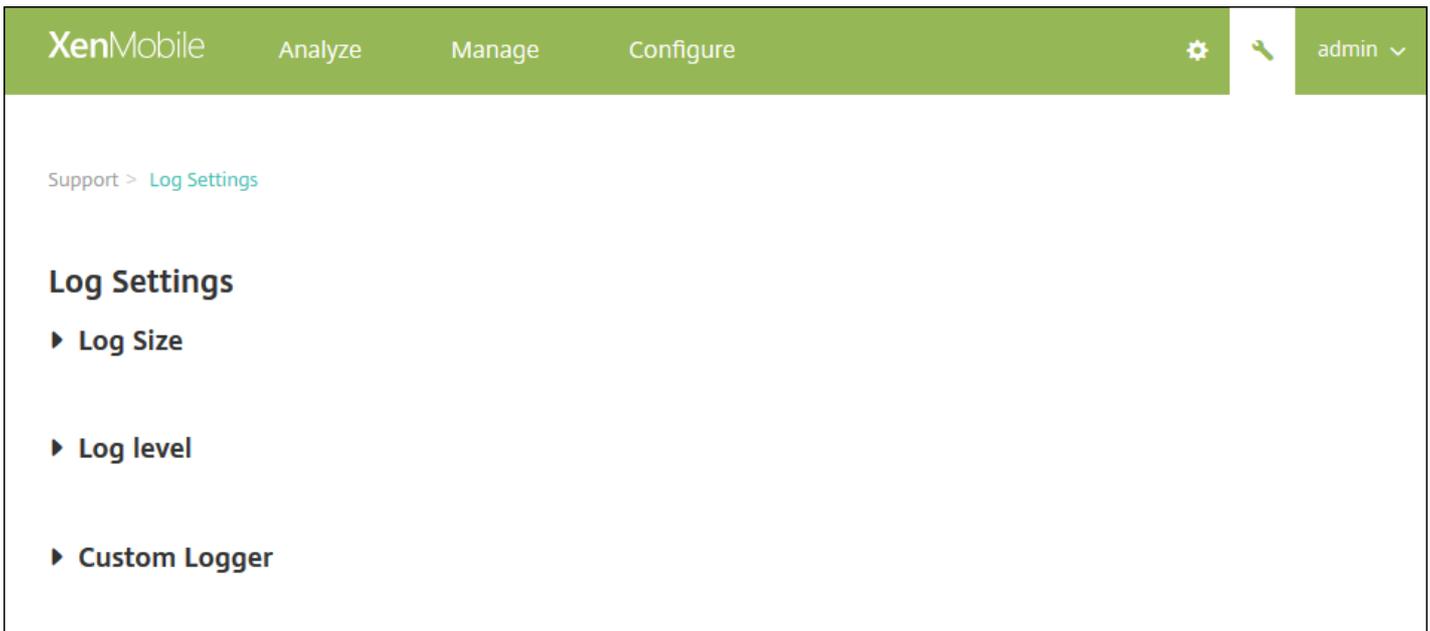
3. En **Support bundle anonymization**, seleccione si los datos pasan a ser anónimos. El valor predeterminado es **ON**.
4. Junto a **De-anonymization**, haga clic en **Download de-anonymization file** para descargar el archivo de asignación que enviará al servicio de asistencia de Citrix cuando necesiten información concreta de dispositivo o usuario para diagnosticar un problema.

# Registros

Mar 02, 2017

Puede configurar los parámetros de captura de registros para personalizar los registros que genera XenMobile. Si tiene un clúster de servidores XenMobile, cuando se configuran los parámetros de registros en la consola de XenMobile, los parámetros se comparten con todos los servidores del clúster.

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa, situado en la esquina superior derecha de la consola. Aparecerá la página **Support**.
2. En **Log Operations**, haga clic en **Log Settings**. Aparecerá la página **Log Settings**.



En la página **Log Settings**, puede acceder a las siguientes opciones:

- **Log Size.** Use esta opción para el tamaño del archivo de registro y la cantidad máxima de copias de seguridad del archivo de registro que se conservarán en la base de datos. La opción Log size se aplica a cada archivo de registros admitido por XenMobile (depuración, actividad de administración y actividad de usuarios).
- **Log level.** Use esta opción para cambiar el nivel de captura de registros o para conservar la configuración.
- **Custom Logger.** Use esta opción para crear un registrador personalizado; los registros personalizados requieren un nombre de clase y un nivel de registro.

Para configurar las opciones de tamaño del registro

1. En la página **Log Settings**, expanda **Log Size**.

XenMobile Analyze Manage Configure admin

[Support](#) > [Log Settings](#)

## Log Settings

▼ Log Size

Debug log file size (MB)	10
Maximum number of debug backup files	50
Admin activity log file size (MB)	10
Maximum number of admin activity backup files	300
User activity log file size (MB)	10
Maximum number of user activity backup files	600

2. Configure los siguientes parámetros:

- **Debug log file size (MB):** En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de depuración. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of debug backup files:** En la lista, haga clic en el número máximo de archivos de depuración que conservará el servidor. De forma predeterminada, XenMobile conserva 50 archivos de copias de seguridad en el servidor.
- **Admin activity log file size (MB):** En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de actividad de administración. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of admin activity backup files:** En la lista, haga clic en el número máximo de archivos de actividad de administración que conservará el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.
- **User activity log file size (MB):** En la lista, haga clic en un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de actividad de usuarios. El tamaño de archivo predeterminado es de **10 MB**.
- **Maximum number of user activity backup files:** En la lista, haga clic en el número máximo de archivos de actividad de usuarios que conservará el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.

Para configurar las opciones de nivel de registro

La opción de nivel de registros (Log level) permite especificar qué tipo de información recopila XenMobile en los registros. Puede establecer el mismo nivel para todas las clases o puede definir las clases con niveles de registro específicos.

1. En la página **Log Settings**, expanda **Log level**. Aparece la tabla con todas las clases de registros.

XenMobile Analyze Manage Configure   admin 

Support > [Log Settings](#)

## Log Settings

▶ Log Size

▼ Log level

 Edit all |  Reset

<input type="checkbox"/>	Class	Sub-class	Log level	
<input type="checkbox"/>	Data Access	All	Info	
<input type="checkbox"/>	Data Access	XDM	Info	
<input type="checkbox"/>	Data Access	XAM	Info	
<input type="checkbox"/>	Data Access	Console	Info	
<input type="checkbox"/>	Data Access	OCA	Info	
<input type="checkbox"/>	IMI Services	All	Info	
<input type="checkbox"/>	IMI Services	Category Service	Info	
<input type="checkbox"/>	IMI Services	OPN Service	Info	

2. Lleve a cabo una de las siguientes acciones:

- Marque la casilla junto a una clase y luego haga clic en **Set Level** para cambiar solo el nivel de registro de esa clase.
- Haga clic en **Edit all** para aplicar el cambio de nivel de registro a todas las clases de la tabla.

Aparecerá el cuadro de diálogo **Set Log Level**, donde podrá establecer el nivel de registro y seleccionar si la configuración del nivel de registro se conservará cuando se reinicie el servidor XenMobile.

- **Class Name:** Este campo muestra el valor All cuando se está cambiando el nivel de registro para todas las clases, o muestra el nombre de la clase en particular; no es un campo editable.
- **Sub-class name:** Este campo no se puede modificar. Muestra el valor All cuando se está cambiando el nivel de registro de todas las clases, o bien muestra el nombre de la subclase en particular.
- **Log level:** Haga clic en un nivel de registro en la lista. Los niveles de registro respaldados incluyen:
  - Fatal (Grave)
  - Error
  - Advertencia
  - Info (Información)
  - Debug (Depuración)
  - Trace (Seguimiento)
  - Off
- **Included Loggers:** Este campo está en blanco cuando se está cambiando el nivel de registro para todas las clases, o muestra el nombre de los registradores configurados actualmente para una clase en concreto; no es un campo editable.
- **Persist settings:** Si quiere conservar los parámetros de nivel de registro cuando reinicie el servidor, marque esta casilla. Si no se marca esta casilla, los parámetros de nivel de registro vuelven a sus valores predeterminados cuando se reinicia el servidor.

3. Haga clic en **Set** para confirmar los cambios.

### Cómo agregar un registrador personalizado

1. En la página **Log Settings**, expanda **Custom Logger**. Aparecerá la tabla **Custom Logger**. Si no ha agregado aún registradores personalizados, la tabla empieza vacía.

Support > [Log Settings](#)

## Log Settings

### ▶ Log Size

### ▶ Log level

### ▼ Custom Logger

 Add |  Set Level |  Delete

<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Showing 1 - 2 of 2 items

2. Haga clic en **Add**. Aparecerá el cuadro de diálogo **Add custom logger**.

### Add custom logger ×

**Class name**

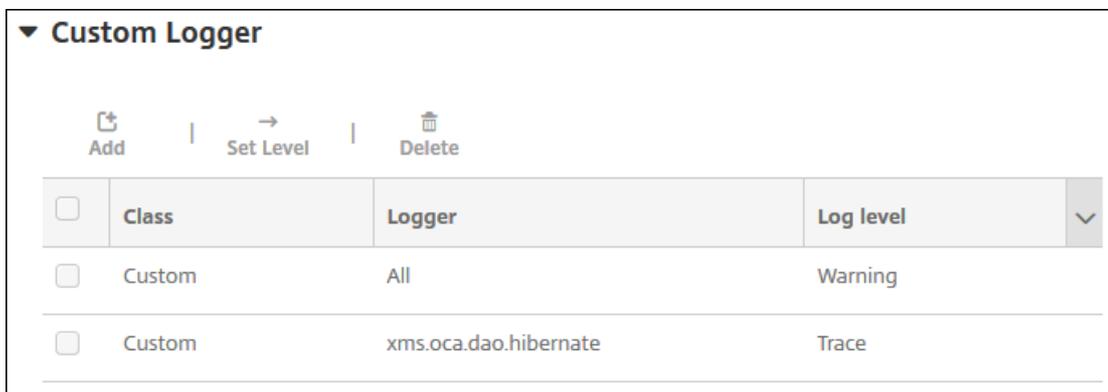
**Log level**

**Included loggers**

3. Configure los siguientes parámetros:

- **Class Name:** Este campo muestra **Custom**; no es un campo editable.
- **Log level:** Haga clic en un nivel de registro en la lista. Los niveles de registro respaldados incluyen:
  - Fatal (Grave)
  - Error
  - Advertencia
  - Info (Información)
  - Debug (Depuración)
  - Trace (Seguimiento)
  - Off
- **Included Loggers:** Escriba los registradores concretos que quiere incluir como registradores personalizados, o bien deje el campo en blanco para incluir a todos los registradores.

4. Haga clic en **Add**. El registrador personalizado se agrega a la tabla **Custom Logger**.



<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Para eliminar un registrador personalizado

1. En la página **Log Settings**, expanda **Custom Logger**.
2. Seleccione el registrador personalizado que quiere eliminar.
3. Haga clic en **Delete**. Aparecerá un cuadro de diálogo para preguntar si quiere eliminar el registrador personalizado. Haga clic en **Aceptar**.

**Importante:** Esta operación no se puede deshacer.

# Herramienta XenMobile Analyzer

Mar 02, 2017

XenMobile Analyzer es una herramienta basada en la nube que sirve para diagnosticar y solucionar problemas relacionados con la instalación y otras funciones de XenMobile. La herramienta comprueba si hay problemas con la inscripción de dispositivos o usuarios y con la autenticación dentro del entorno de XenMobile.

Para habilitar la comprobación, debe configurar la herramienta para que apunte al servidor XenMobile y debe proporcionar otros datos como el tipo de implementación del servidor, la plataforma móvil, el tipo de autenticación y las credenciales de usuario para las pruebas. La herramienta, a continuación, se conecta al servidor y analiza el entorno para buscar problemas de configuración. Si XenMobile Analyzer detecta problemas, la herramienta muestra recomendaciones para corregirlos.

## Funciones principales de XenMobile Analyzer

- Ofrece un microservicio seguro basado en la nube para solucionar todo tipo de problemas técnicos relacionados con XenMobile.
- Ofrece recomendaciones precisas cuando hay problemas de configuración de XenMobile.
- Reduce las llamadas de asistencia y acelera la solución de problemas en entornos de XenMobile.
- Ofrece asistencia inmediata para las versiones de XenMobile Server.
- Habilita la inscripción personalizada de dispositivos iOS: respaldo de puertos personalizados para XenMobile (en puertos que no sean el 8443).
- Muestra un cuadro de diálogo de aceptación de certificados para certificados de servidor incompletos o que no sean de confianza.
- Detecta automáticamente casos de autenticación de dos factores.
- Pruebas de Secure Web para la disponibilidad de los sitios de intranet.
- Comprobaciones del servicio de detección automática de Secure Mail.
- Comprobaciones de Single Sign-On (SSO) para ShareFile.
- Habilita el respaldo de puertos personalizados para NetScaler.
- Es compatible con exploradores Web que no estén en inglés.

## Requisitos previos

Producto	Versión compatible
Servidor XenMobile	10.3.0 y versiones posteriores
NetScaler Gateway	10.5 y versiones posteriores
Simulación de inscripción de clientes	iOS y Android

Para obtener acceso a la herramienta desde <https://xenmobiletools.citrix.com> tiene que usar sus credenciales de MyCitrix. En la página "XenMobile Management Tools" que se abre, inicie "XenMobile Analyzer" haciendo clic en **Analyze and Troubleshoot my XenMobile Environment**.

All Management Tools

## What do you want to do?

XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.

Analyze and  
Troubleshoot my  
XenMobile  
environment

XenMobile Analyzer



Follow steps to identify and triage potential issues with your deployment.

Request Auto  
Discovery

Auto Discovery Service



Request and Configure Auto Discovery for your domain's XenMobile Server.

Request push  
notification  
certificate  
signature

Create APNs Certificate



Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

Enable APNs-based

XenMobile Analyzer contiene cinco pasos principales diseñados para guiarle en el proceso de análisis y reducir la cantidad de tickets de asistencia técnica que tenga que abrir, lo que puede reducir costes para todo el mundo.

Los pasos son:

1. **Environment Check.** Este paso le guía a la hora de configurar pruebas para comprobar si hay problemas. También ofrece recomendaciones y soluciones para problemas de dispositivo, inscripción de usuarios y autenticación.

## All Steps

## XenMobile Analyzer

Identify potential issues with your deployment

**Step 1: Environment Check**

Is your environment authentication and enrollment set up correctly?

**How it works:**

Point XenMobile Analyzer to your XenMobile Server

xm.test.citrix.com

Provide a few details of your XenMobile Server setup to create a test environment.

Track Real Time Test Progress



- Follow the progress of your test as it is running or come back to it later.
- In case of failure, identify the exact step of your setup where issues occur.

Follow Step By Step Recommendations



View reports with support content for specific fixes to issues. Come back to rerun tests any time.

[Get Started](#)**Step 2: Advanced Diagnostics**

Is your environment optimized to prevent problems?

**Step 3: Secure Mail Readiness**

Is your mail server prepared to deploy to your XenMobile environment?

Feedback

**2. Advanced Diagnostics.** Este paso ofrece información sobre cómo usar Citrix Insight Services para encontrar otros problemas que no se hayan detectado en el paso anterior de comprobación del entorno.

## All Steps

## XenMobile Analyzer

Identify potential issues with your deployment

**Step 1: Environment Check**

Is your environment authentication and enrollment set up correctly?

**Step 2: Advanced Diagnostics**

Is your environment optimized to prevent problems?

**How it works:**

Citrix Insight Service (CIS) is Citrix's flagship Big Data platform for instrumentation & telemetry and business insight generation.

Collect information on your environment

Go to your XenMobile Console &gt; Support &gt; Create Support Bundle

Upload to Citrix Insight Services

After you have created a Support Bundle, upload it to Citrix Insights Services from XenMobile Console. You will receive an email confirmation.

Analyze and fix issues

The uploaded data will be auto-analyzed against a list of known issues and best practices. A personalized report, including next step resolution recommendations will be provided - a link will be sent to your email. You can also go to CIS to view a report.

[Go To CIS](#)**Step 3: Secure Mail Readiness**

Is your mail server prepared to deploy to your XenMobile environment?



## Feedback

**3. Secure Mail Readiness.** Este paso indica cómo descargar la aplicación XenMobile Exchange ActiveSync Test, que le ayuda a comprobar si los servidores de ActiveSync están preparados para su implementación en un entorno de XenMobile

**Step 1: Environment Check**

Is your environment authentication and enrollment set up correctly? ▾

**Step 2: Advanced Diagnostics**

Is your environment optimized to prevent problems? ▾

**Step 3: Secure Mail Readiness**

Is your mail server prepared to deploy to your XenMobile environment? ▲

**How it works:**

Mail Test application is designed to help troubleshoot the ActiveSync servers for their readiness to be deployed with XenMobile environment. For a complete walk through the steps of this test, visit [Mail Test Application](#)

**Download app**

- Launch the Mail Test Application on your iOS device. You can choose to wrap the app.
- Add Server in Server list > Provide the credentials > Accept all certificates > Select device type and device OS

**Diagnose and fix issues**

After the test is complete, a list of servers with reports for each will be available. You can view reports and share them with Send Report.

[Download](#)**Step 4: Server Connectivity Checks**

Is your connection with NetScaler, XenMobile, Authentication and ShareFile servers working properly? ▲

**How it works:**

Check the connections to the XenMobile, Authentication and ShareFile servers

- Go to your XenMobile Console > Support > NetScaler Gateway Connectivity Checks
- Add your NetScaler Gateway Server information
- Run Test Connectivity

[Feedback](#)

**4. Server Connectivity Checks:** Este paso indica cómo probar la conectividad de los servidores.

**5. Contact Citrix Support:** Este paso enlaza con el sitio donde puede abrir un caso de asistencia técnica de Citrix Support, si todavía tiene problemas.

**Step 4: Server Connectivity Checks** ▾

Is your connection with NetScaler, XenMobile, Authentication and ShareFile servers working properly?

**How it works:**

Check the connections to the XenMobile, Authentication and ShareFile servers

- Go to your XenMobile Console > Support > NetScaler Gateway Connectivity Checks
- Add your NetScaler Gateway Server information
- Run Test Connectivity
  
- Go to your XenMobile Console > Support > XenMobile Connectivity Checks
- Select the server from the list
- Run Test Connectivity

**Step 5: Contact Citrix Support** ▾

Need help in troubleshooting or to create a support case?

Still having issues? Citrix Support can help!

[Create Case](#)

Feedback

Las secciones siguientes describen cada paso en más detalle.

## Comprobación del entorno

1. Inicie una sesión en XenMobile Analyzer y haga clic en **Step 1: Environment Checks**.
2. Haga clic en **Get Started**.

XenMobile | Analyzer @citrix.com

**All Steps**

### XenMobile Analyzer

Identify potential issues with your deployment

---

**Step 1: Environment Check**  
Is your environment authentication and enrollment set up correctly? ^

**How it works:**

Point XenMobile Analyzer to your XenMobile Server xm.test.citrix.com Provide a few details of your XenMobile Server setup to create a test environment.

Track Real Time Test Progress  • Follow the progress of your test as it is running or come back to it later.  
• In case of failure, identify the exact step of your setup where issues occur.

Follow Step By Step Recommendations   View reports with support content for specific fixes to issues. Come back to rerun tests any time.

[Get Started](#)

---

**Step 2: Advanced Diagnostics**  
Is your environment optimized to prevent problems? v

---

**Step 3: Secure Mail Readiness**  
Is your mail server prepared to deploy to your XenMobile environment? v

**Feedback**

3. Haga clic en **Add Test Environment**.

XenMobile | Analyzer @citrix.com

[All Steps](#) > **Test Environments**

### Test Environment List

Test your server setup before deploying

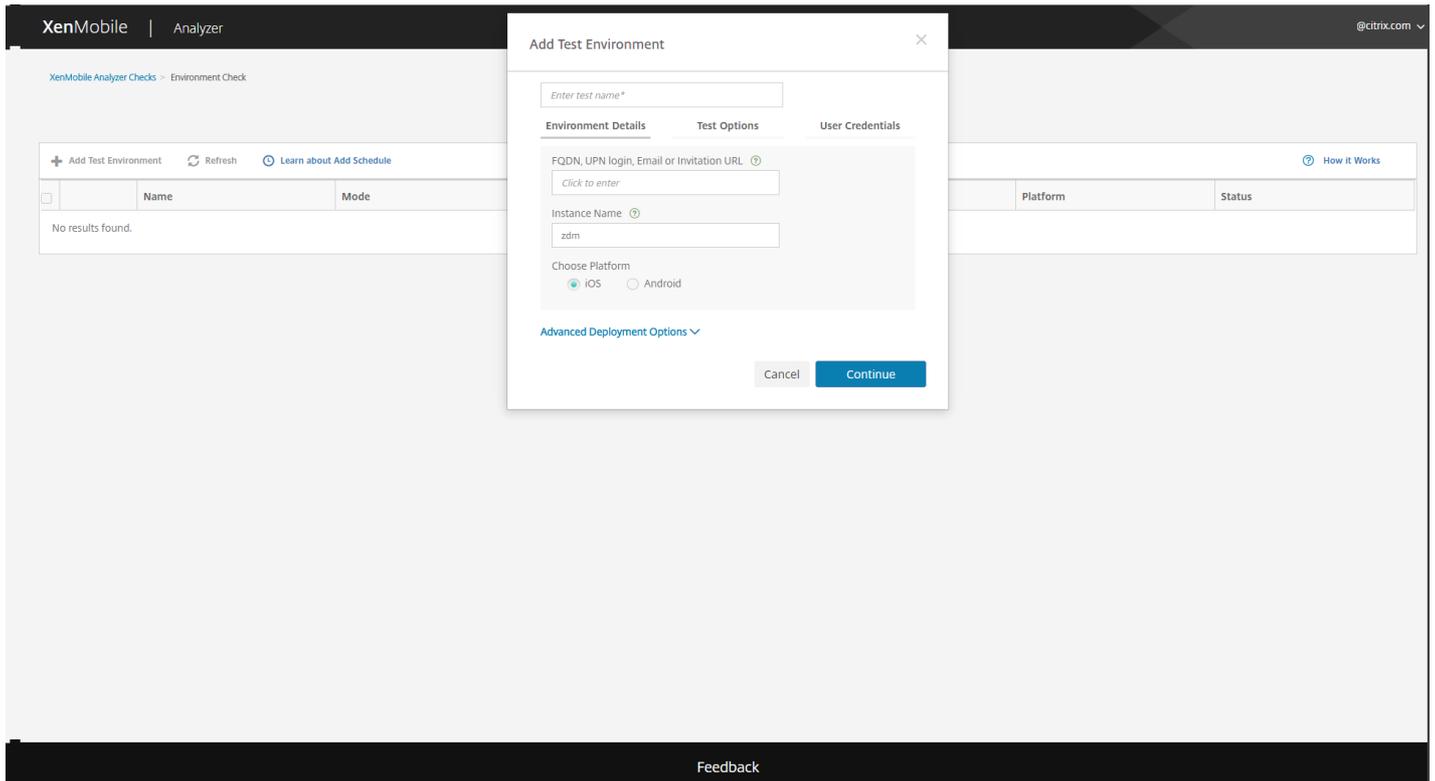
+ Add Test Environment ↻ Refresh

	Name	Mode	Server/Email/UPN	Instance	Platform	Status
No results found.						

**Feedback**

4. En el cuadro de diálogo **Add Test Environment**, lleve a cabo lo siguiente:

En la captura de pantalla anterior, tenga en cuenta que ahora Worx Home se llama Secure Hub.

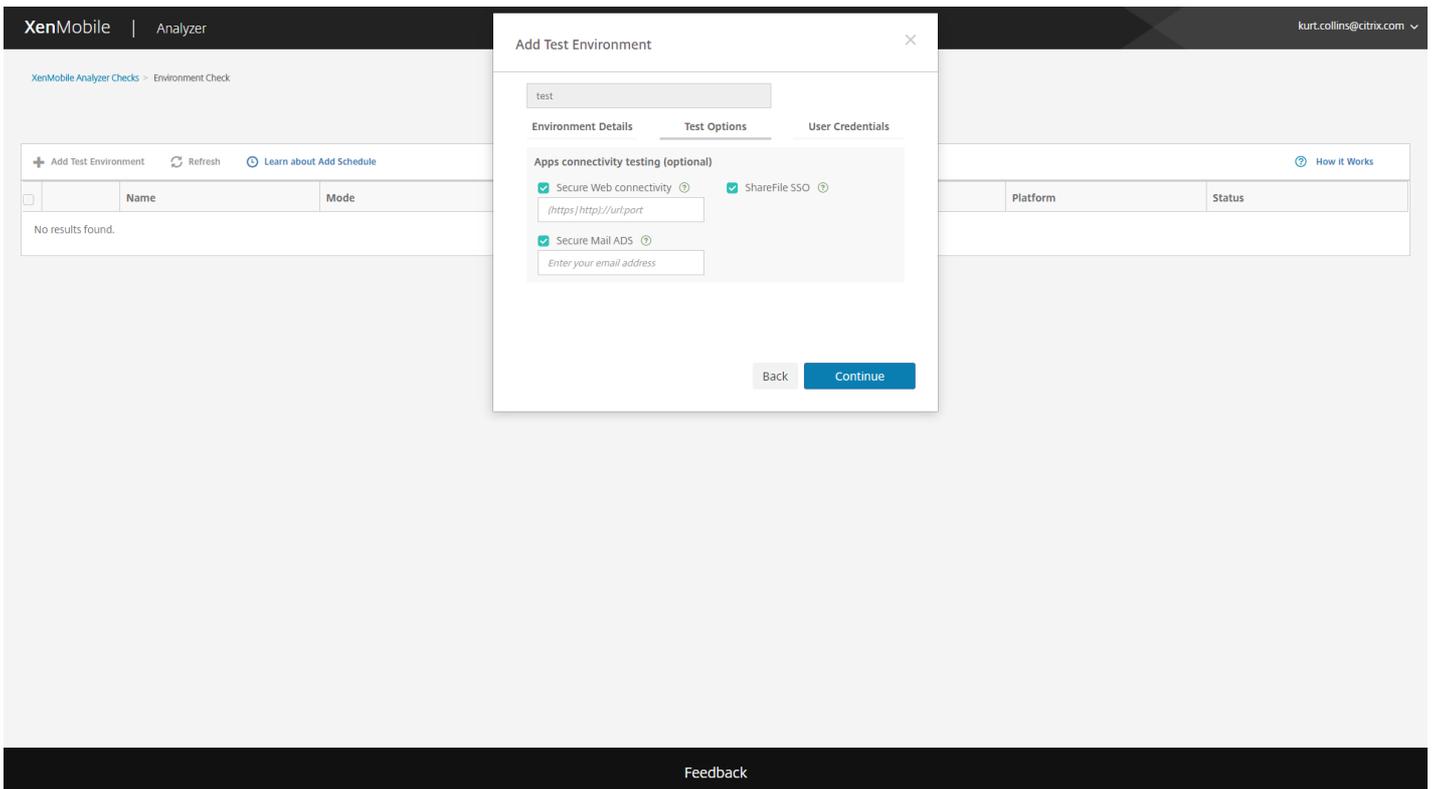


- Proporcione un nombre único a la prueba para poder identificarla en el futuro.
- En el campo **FQDN, UPN login, Email o URL Invitation**, introduzca la información que va a utilizarse para acceder al servidor.
- En **Instance Name**, introduzca el valor de su instancia personalizada, si la usa.

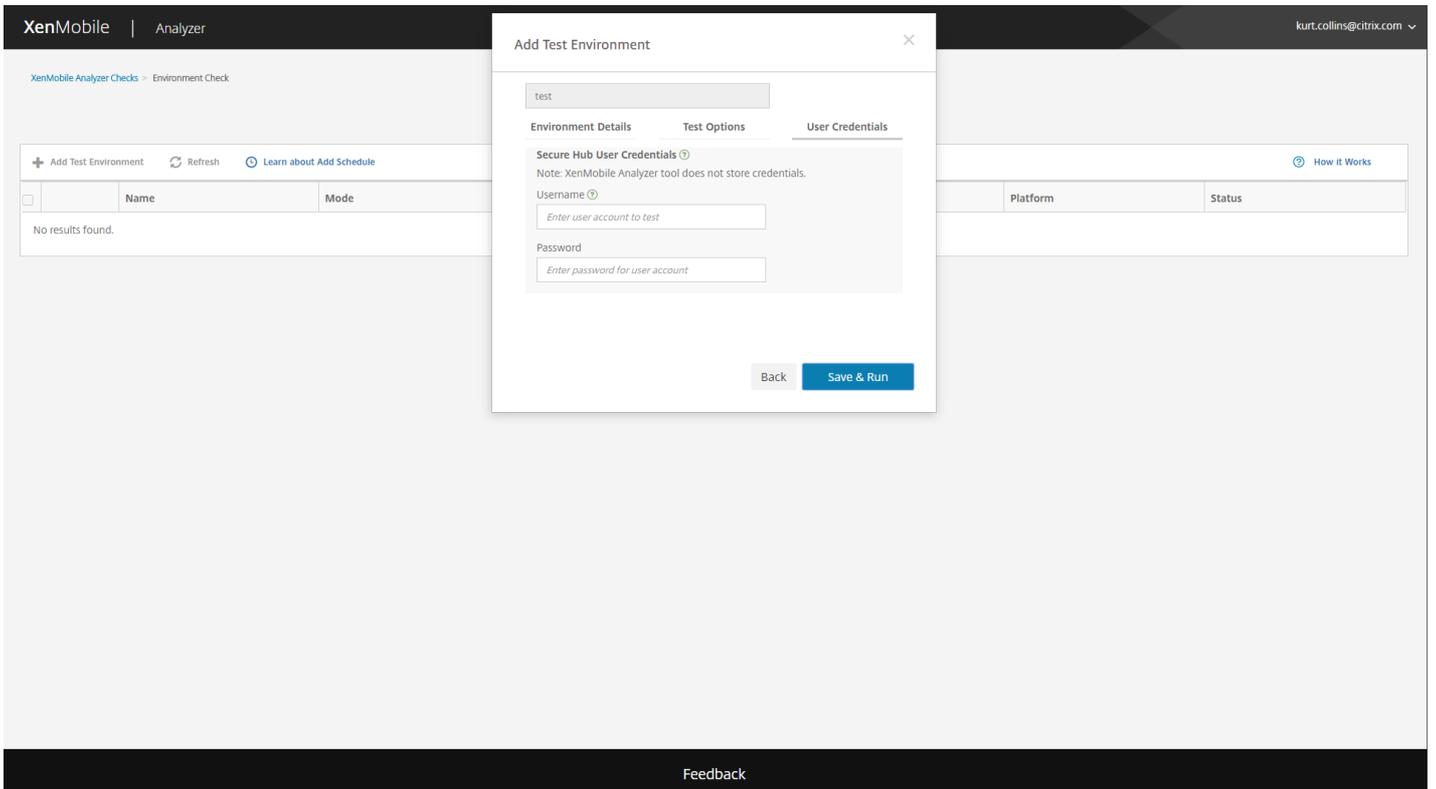
En **Choose Platform**, seleccione **iOS** o **Android** como plataforma para las pruebas.

e. Si expande **Advanced Deployment Options**, en la lista **Deployment Mode**, puede seleccionar su modo de implementación de XenMobile. Las opciones disponibles son: **Enterprise (MDM + MAM)**, **App Management (MAM)** o **Device Management (MDM)**.

En la captura de pantalla anterior, tenga en cuenta que ahora Worx Home se llama Secure Hub.



5. Haga clic en **Continue**.



En la imagen anterior, tenga en cuenta que ahora WorxWeb se llama Secure Web y WorxMail es Secure Mail.

6. Puede seleccionar pruebas a nivel de aplicaciones a ejecutar. Puede elegir una o varias de las siguientes pruebas.
- a. **Secure Web micro VPN Connectivity with intranet sites** (Conectividad de micro VPN de Secure Web a sitios de intranet). Proporcione una URL de intranet. La herramienta comprobará la disponibilidad de la URL. Detectará si hay problemas de conectividad que podrían darse en la aplicación Secure Web al intentar acceder a las direcciones URL de intranet.
  - b. **Secure Mail ADS** (ADS de Secure Mail). Introduzca un ID de correo electrónico de usuario. Se utilizará para comprobar la detección automática de Microsoft Exchange Server en el entorno de XenMobile. Detectará si hay problemas relacionados con la detección automática de Secure Mail.
  - c. **ShareFile SSO** (Single Sign-On de ShareFile). Si se selecciona, XenMobile Analyzer comprobará si la resolución DNS de ShareFile se realiza correctamente y si el inicio de sesión único Single Sign-On de ShareFile funciona con las credenciales de usuario proporcionadas.

7. Haga clic en **Continue**.

**Add Test Environment**

Test

**Environment Details**    **Test Options**    **User Credentials**

**Secure Hub User Credentials** ?

Note: XenMobile Analyzer tool does not store credentials.

Username ?

Enter user account to test

Password

Enter password for user account

Enrollment PIN

Enrollment PIN

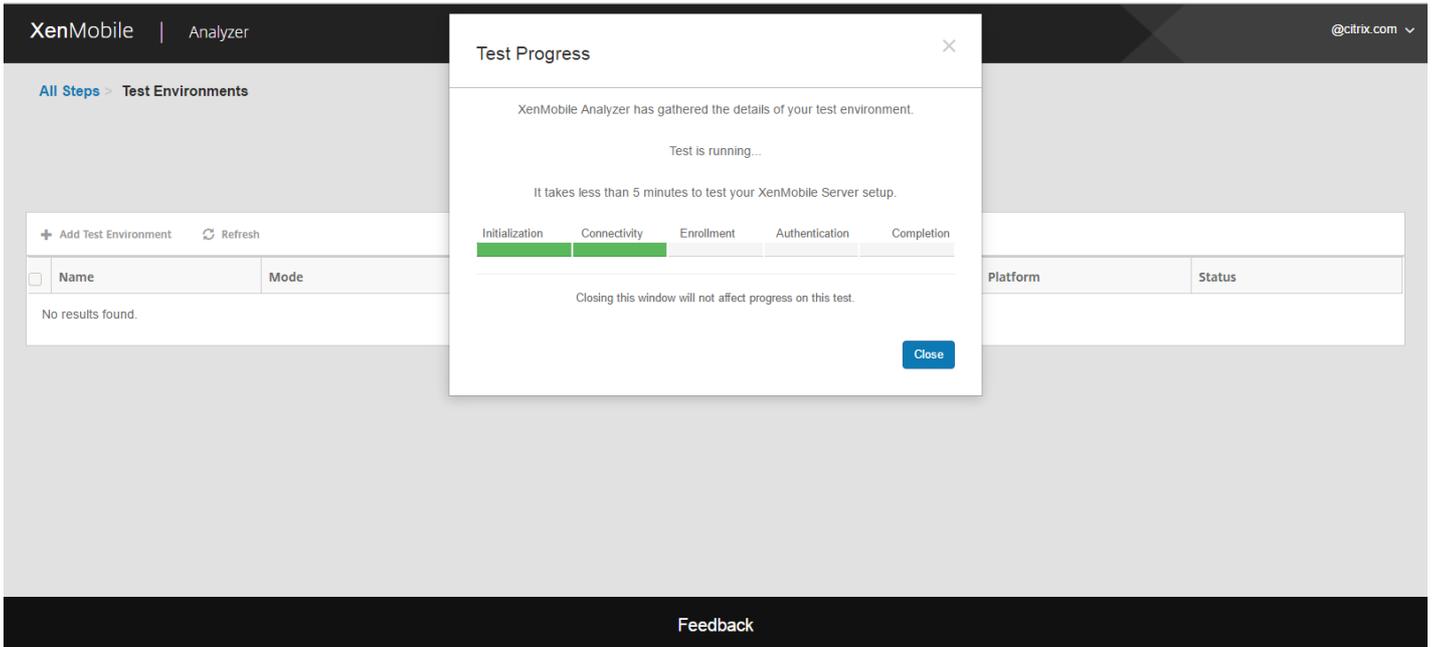
Back    Save & Run

8. Según la configuración del servidor, es posible que vea diferentes campos disponibles para introducir las credenciales de usuario. Los campos posibles son: solo **Username**, **Username y Password** o **Username, Password y Enrollment PIN**.

9. Después de introducir esta información, haga clic en **Save & Run** para iniciar las pruebas.

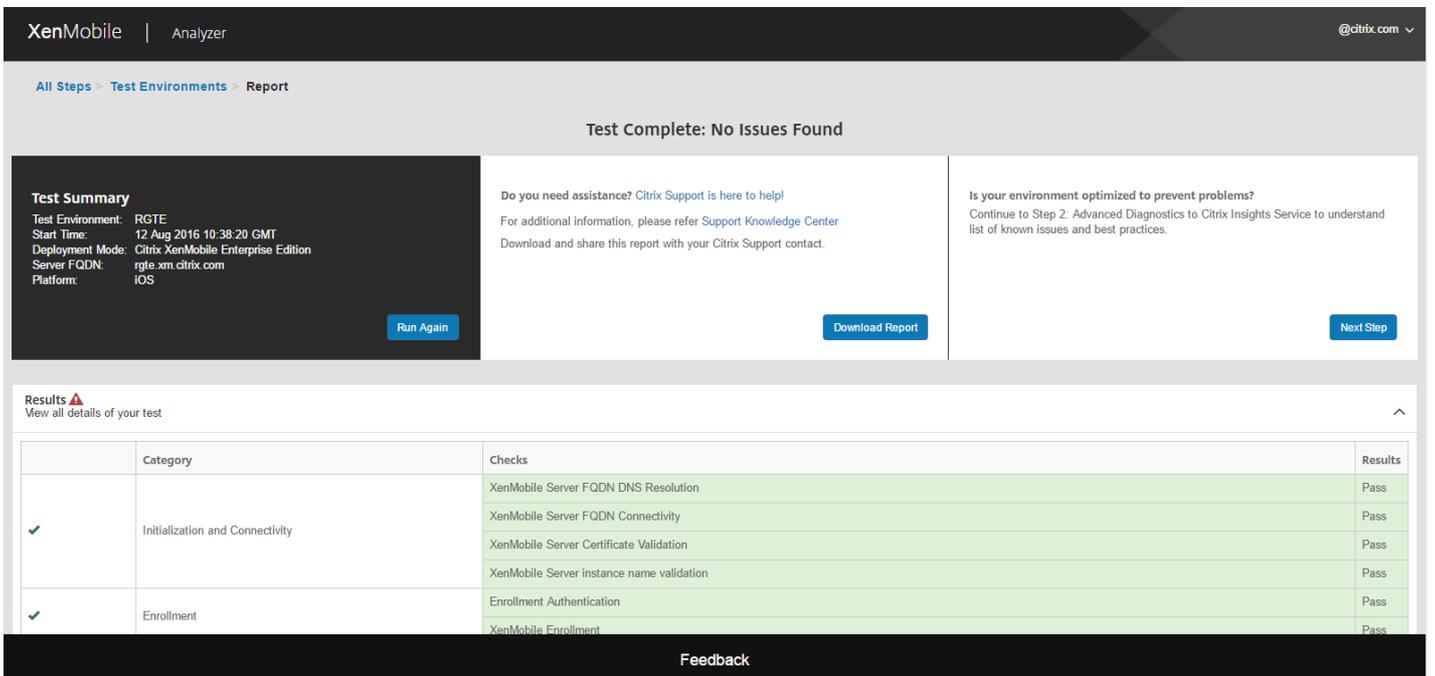
Aparecerá una notificación de progreso. Puede dejar el cuadro de diálogo de progreso abierto o cerrarlo, y las pruebas continuarán ejecutándose.

Las pruebas superadas aparecen en verde. Las pruebas que fallan aparecen en rojo.



8. En cualquier momento después de cerrar el cuadro de diálogo de progreso, puede volver a la página **Test Environments List** y hacer clic en el icono **View report** icono para ver los resultados de la prueba.

La página **Results** muestra los detalles de la prueba, recomendaciones y resultados.



✓	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✓	App Enumeration	Device Registration	Pass
		WorxStore Connectivity	Pass
		WorxStore App Listing (13)	Pass
✓	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

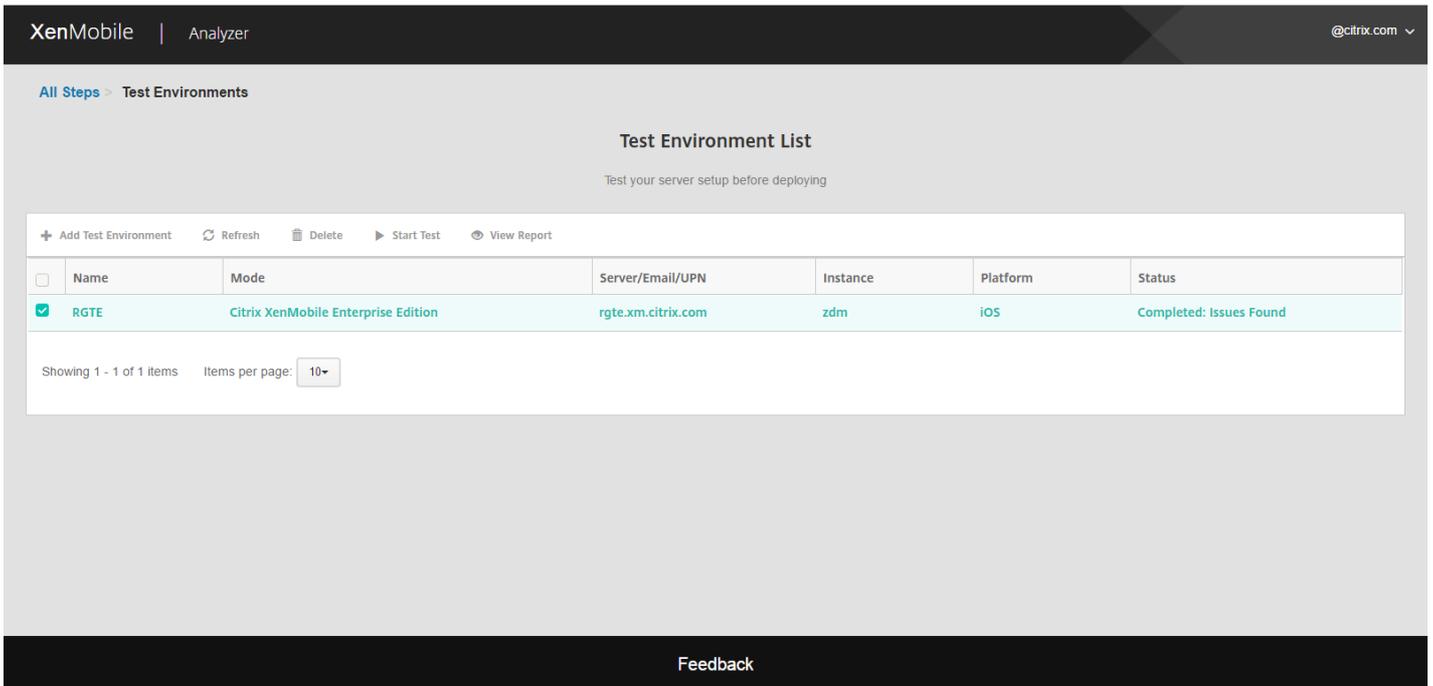
### Feedback

En la captura de pantalla anterior, tenga en cuenta que ahora WorxWeb se llama Secure Web, WorxNotes es Secure Notes, WorxTasks es Secure Tasks y WorxStore es XenMobile Store.

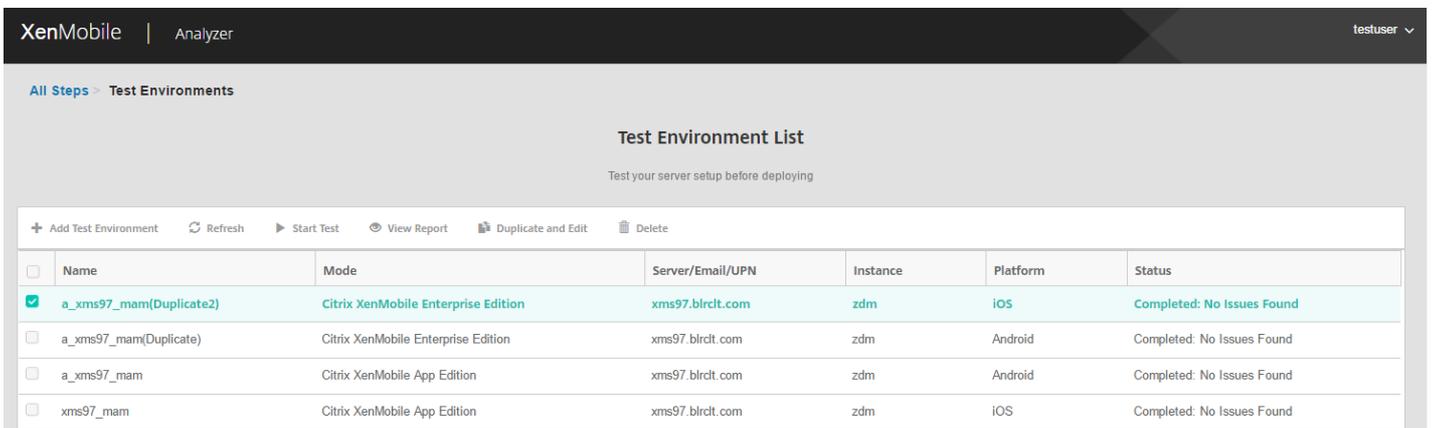
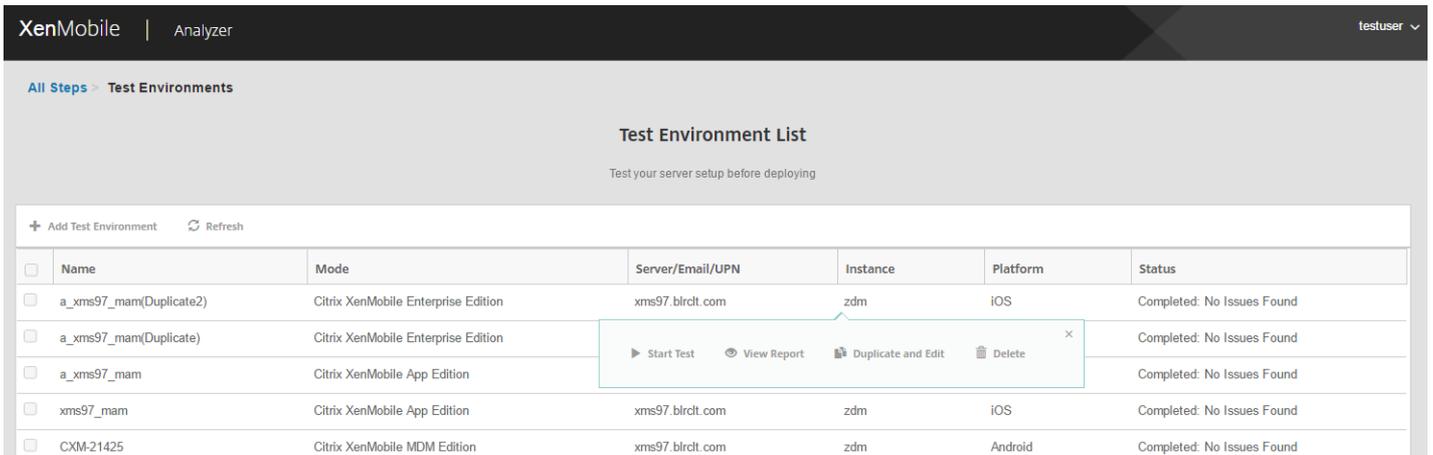
Si las recomendaciones tienen artículos de Citrix Knowledge Base asociados a ellas, los artículos se enumeran en la página.

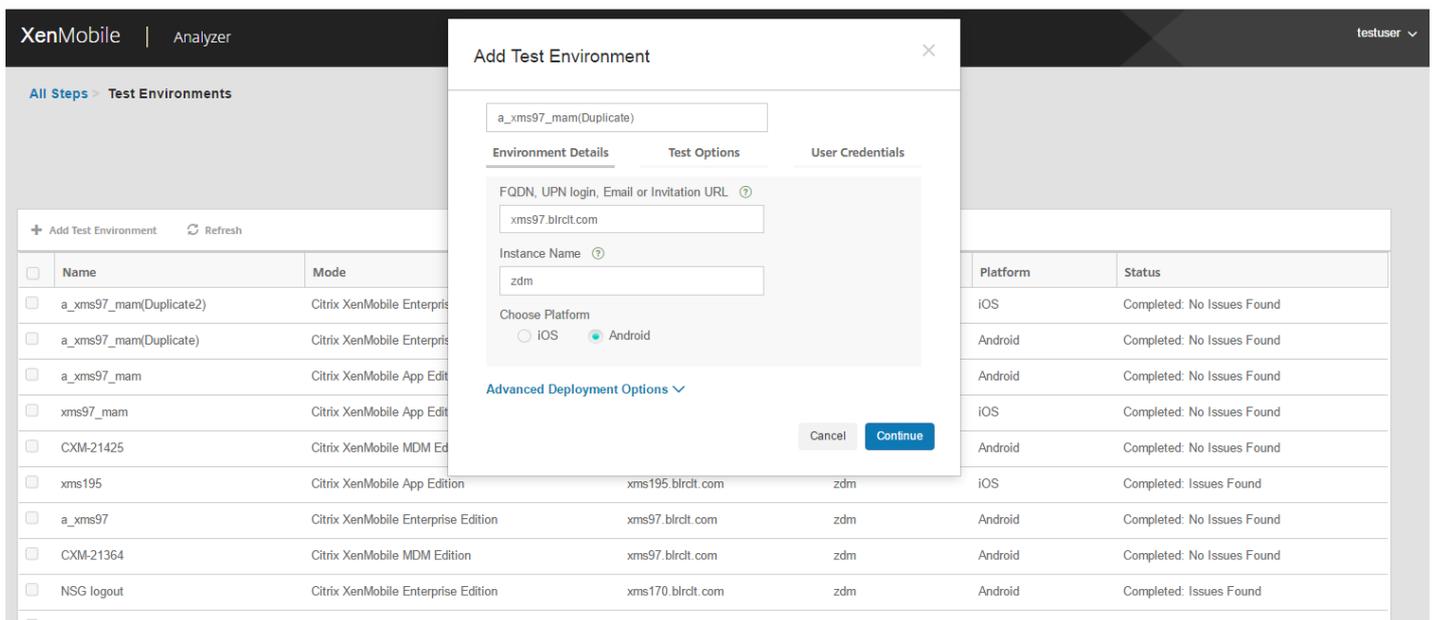
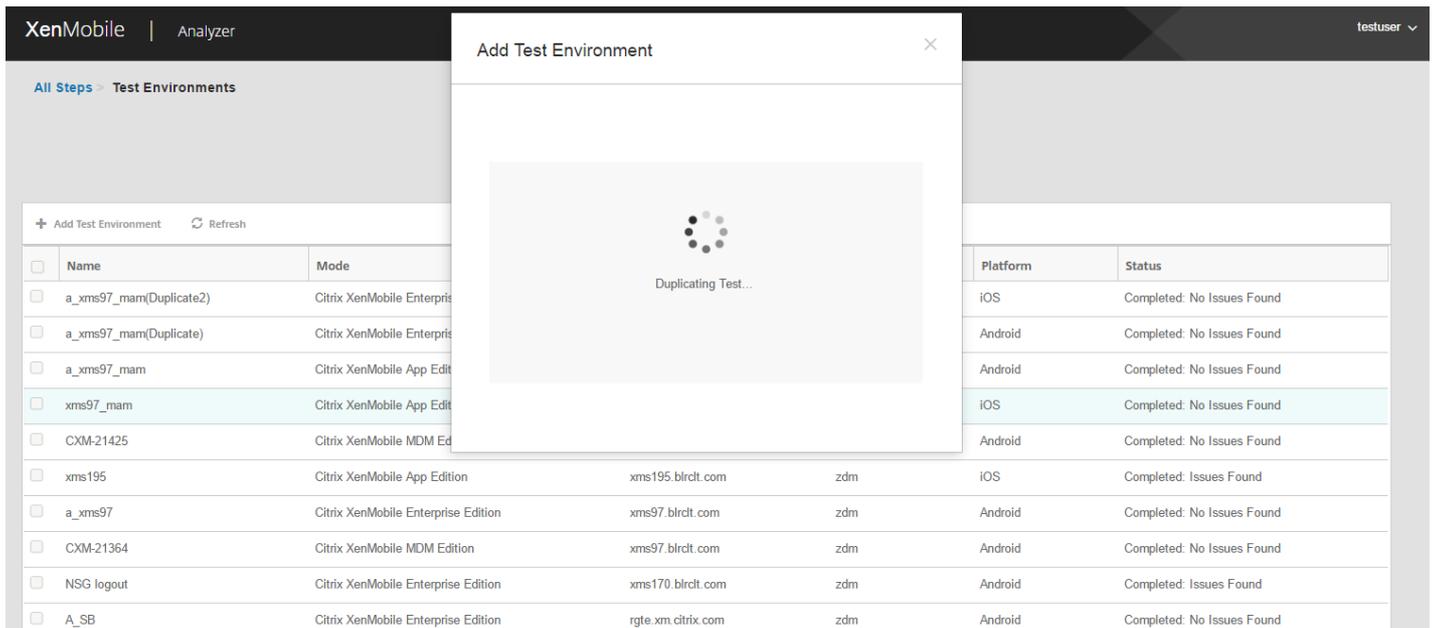
9. Haga clic en la ficha **Results** para mostrar la categoría y las pruebas realizadas por la herramienta, con sus resultados correspondientes.

- a. Para descargar el informe, haga clic en **Download report**.
- b. Para volver a la lista de entornos de prueba, haga clic en **Test Environments**.
- c. Para volver a ejecutar la prueba, haga clic en **Run Again**.
- d. Si quiere volver a ejecutar otra prueba, vuelva a **Test Environments**, seleccione la prueba y haga clic en **Start Test**.
- e. Para ir al siguiente paso de XenMobile Analyzer, haga clic en **Next Step**.



10. Desde la página Test Environments, puede copiar y modificar las pruebas. Para ello, seleccione una prueba y, a continuación, haga clic en **Duplicate and Edit**. Se creará una copia de la prueba seleccionada y se abrirá el cuadro de diálogo Add Test Environment, lo que le permitirá modificar la nueva prueba.





## Pasos 2-5 de XenMobile Analyzer

El primer paso de XenMobile Analyzer (comprobación del entorno) es interactivo, mientras que los pasos siguientes del 2 al 5 son informativos. Cada uno de estos pasos proporciona información acerca de otras herramientas de asistencia técnica que se pueden usar para asegurarse de que el entorno de XenMobile esté configurado correctamente.

- Paso 2 - Advanced Diagnostics:** Este paso le guía para recopilar información sobre el entorno y luego cargarla en Citrix Insight Services. La herramienta analiza los datos y proporciona un informe personalizado con resoluciones recomendadas.

- **Paso 3. Secure Mail Readiness.** Este paso es una guía para descargar y ejecutar la aplicación XenMobile Exchange ActiveSync Test. La aplicación detecta problemas en los servidores ActiveSync si no están preparados para implementarse con entornos de XenMobile. Después de ejecutar la aplicación, puede ver informes o compartirlos con otras personas.
- **Paso 4 - Server Connectivity Checks:** Este paso ofrece instrucciones para comprobar las conexiones con los servidores XenMobile, servidores de autenticación y ShareFile.
- **Paso 5 - Contact Citrix Support:** Si todo lo anterior falla, puede crear un tiquet de asistencia técnica en Citrix Support.

## Problemas conocidos

XenMobile Analyzer presenta los siguientes problemas conocidos:

- La cantidad de aplicaciones indicada puede variar en función del cliente si la directiva Platform Restriction está definida en el servidor XenMobile.
- Al comprobar la conectividad de Secure Web a la intranet, no se admite la introducción de varias direcciones URL en el cuadro de texto.
- No se respalda la característica de autenticación de dispositivos compartidos de Secure Hub.
- Con las pruebas de Secure Web, solo se comprueba la conectividad a las direcciones URL introducidas, no la autenticación en los sitios correspondientes.

## Problemas resueltos

Se han solucionado los problemas siguientes de XenMobile Analyzer:

- Cuando se realiza una comprobación mediante la invitación a la inscripción, la prueba se realiza correctamente, pero la invitación a la inscripción no se activa.

# Cómo ver y analizar archivos de registros en XenMobile

Mar 02, 2017

1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa, situado en la esquina superior derecha de la consola. Se abrirá la página **Support**.
2. En **Log Operations**, haga clic en **Logs**. Aparecerá la página **Logs**. Los registros individuales se muestran en una tabla.

XenMobile Analyze Manage Configure administrator

Support > Logs

## Logs

Analyze the details of various types of logs.

Download All

<input type="checkbox"/>	Log Name	Log Type
<input type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

3. Seleccione el registro que quiera ver:

- Los archivos de registros de depuración (Debug Log File) contienen información muy útil para el servicio de asistencia Citrix Support, tal como mensajes de error y acciones relacionadas con el servidor.
- Los archivos de registros de auditoría de administración (Admin Audit Log File) contienen información de auditoría sobre actividad en la consola de XenMobile.
- Los archivos de registros de auditoría de usuarios (User Audit Log File) contienen información relacionada con los usuarios configurados.

4. Use las acciones de la parte superior de la tabla para descargar uno o todos los registros, verlos, girarlos o eliminarlos.

## Logs

Analyze the details of various types of logs.

 Download All | 
  View | 
  Rotate | 
  Download | 
  Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug

### Nota:

- Si selecciona varios archivos de registro, solo estarán disponibles las opciones **Download All** y **Rotate**.
- Si tiene servidores XenMobile en clúster, solo puede ver los registros del servidor al que se ha conectado. Para ver los registros de otros servidores, use alguna de las opciones de descarga.

5. Lleve a cabo una de las siguientes acciones:

- **Download All.** La consola descarga todos los registros presentes en el sistema (incluidos los registros de depuración, auditoría de administración, auditoría de usuarios, registros del servidor, etcétera).
- **View.** Muestra, a continuación de la tabla, el contenido de los registros.
- **Rotate.** Almacena el archivo de registro actual y crea un nuevo archivo para capturar entradas de registro. Al almacenar un archivo de registros, aparece un cuadro de diálogo; ahí, haga clic en Rotate para continuar.
- **Download.** La consola descarga el único tipo de archivo de registros seleccionado y también descarga otros registros ya archivados del mismo tipo.
- **Delete.** Quita permanentemente los archivos de registros seleccionados.

### Logs

Analyze the details of various types of logs.

 Download All | 
  View | 
  Rotate | 
  Download | 
  Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2016-11-06T06:28:38.908-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTaskJob: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2.
2016-11-06T06:30:38.945-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.985-0800 | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.502-0800 | INFO | pool-7-thread-1 | com.citrix.zdm.pli.pers.CsrResponderService | Reloading OCSP Service data

```



# Las API de REST

Mar 02, 2017

Con la API de REST de XenMobile, puede invocar servicios que están expuestos a través de la consola de XenMobile. Puede invocar servicios REST desde cualquier cliente REST. La API no requiere el inicio de sesión en la consola de XenMobile para llamar a los servicios.

Para consultar toda la documentación sobre el conjunto actual de interfaces API disponibles, descargue el archivo [PDF de Información acerca de la API de REST en XenMobile](#). Este artículo no incluye el conjunto completo de API.

## Permisos necesarios para obtener acceso a la API de REST

Necesita uno de los siguientes permisos para acceder a la API de REST:

- Permiso de acceso a la API pública definido como parte de una configuración de acceso basado en roles (para obtener más información sobre cómo establecer el acceso basado en roles, consulte [Configuración de roles con RBAC](#))
- Permiso de superusuario

## Cómo invocar servicios de la API de REST

Puede invocar servicios de la API de REST mediante comandos de CURL o el cliente REST. Los ejemplos siguientes usan el cliente Advanced REST para Chrome.

### Nota

En los siguientes ejemplos, deberá cambiar el nombre de host y el número de puerto para que coincidan con su entorno.

### Inicio de sesión

URL: `https://<nombre de host>:<puerto>/xenmobile/api/v1/authentication/login`

Solicitud: `{ "login": "administrator", "password": "password" }`

Tipo de método: POST

Tipo de contenido: `application/json`

https://localhost:4443/xenmobile/api/v1/publicapi/login

GET
  POST
  PUT
  PATCH
  DELETE
  HEAD
  OPTIONS
  Other

Raw Form Headers

Raw Form Files (0) Payload

Encode payload Decode payload

```

{
  "login": "administrator",
  "password": "password"
}

```

application/json Set "Content-Type" header to overwrite this value.

Clear Send

Status **200 OK** Loading time: 265 ms

Request headers

```

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
Origin: chrome-extension://hgml0ofddfdnphfgcellkdfbfjeloo
Content-Type: application/json
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163

```

Response headers

```

Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 53
Date: Sun, 22 Mar 2015 22:43:48 GMT

```

Raw Parsed Response

Open output in new window Copy to clipboard Save as file Open in JSON tab

```

{"auth_token": "d4fdecf6-2e5a-4aed-8d60-f9a513b5c358"}

```

Code highlighting thanks to [Code Mirror](#)

# Las API de SOAP

Mar 02, 2017

Citrix ya no respalda el uso de las API de servicios Web SOAP. Use las API de REST en su lugar. Para obtener más información, consulte [API de REST](#).

# XenMobile Mail Manager 10.x

Mar 02, 2017

XenMobile Mail Manager ofrece la funcionalidad que amplía las capacidades de XenMobile de este modo:

- Control de acceso dinámico para dispositivos Exchange Active Sync (EAS). Se puede bloquear o permitir inmediatamente el acceso de dispositivos EAS a servicios de Exchange.
- Proporciona a XenMobile la capacidad de acceder a la información de asociación del dispositivo EAS, facilitada por Exchange.
- Proporciona a XenMobile la capacidad de realizar un borrado EAS en un dispositivo móvil.
- Proporciona a XenMobile la capacidad de acceder a la información acerca de dispositivos BlackBerry y realizar operaciones de control tales como un borrado (Wipe) y un restablecimiento de contraseña (ResetPassword).

Para descargar XenMobile Mail Manager, vaya al apartado Server Components de XenMobile 10 Server en [Citrix.com](http://Citrix.com).

## Novedades en XenMobile Mail Manager 10.1

### Reglas de acceso

La ventana Rule Analysis (análisis de reglas) tiene una casilla de verificación que, al seleccionarla, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.

El acceso predeterminado (Allow, Block y Unchanged) y los modos de comando de ActiveSync (PowerShell o de simulación) se configuran por separado para cada entorno de Microsoft Exchange establecido en la implementación de XenMobile.

### Instantáneas

Puede configurar la cantidad máxima de instantáneas visibles en el historial de instantáneas.

Puede configurar qué errores ignorar durante una instantánea principal. Cuando una instantánea principal genera errores no configurados para ignorarse, se descartan los resultados de las instantáneas.

Para establecer que se ignoren dichos errores, modifique el archivo config.xml mediante un editor XML:

- Si el servidor Exchange es Office 365, vaya al nodo `/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors` y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares.
- Si el servidor Exchange es local, vaya al nodo `/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors` y agregue el texto necesario como elemento secundario en el mismo formato que el elemento secundario existente Error. También puede utilizar expresiones regulares.
- Si hay más de un entorno de Exchange configurado, vaya al nodo `/ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID correspondiente al entorno de Exchange deseado']/ExchangeServer/Specialists/PowerShell`. Agregue un nodo secundario IgnorableErrors al nodo de PowerShell para cada mensaje que deba ignorarse. Agregue un nodo secundario Error al nodo IgnorableErrors con el texto coincidente en una sección CDATA. También puede utilizar expresiones regulares.

Guarde el archivo config.xml y reinicie el servicio XenMobile Mail Manager.

### PowerShell y Exchange

Ahora XenMobile Mail Manager determina de forma dinámica qué cmdlets usar en función de la versión de Exchange a la que esté conectado. Por ejemplo, para Exchange 2010, utiliza Get-ActiveSyncDevice, pero, para Exchange 2013 y Exchange 2016, emplea Get-MobileDevice.

## Configuración de Exchange

Las configuraciones del servidor Exchange se pueden modificar y actualizar sin tener que reiniciar el servicio XenMobile Mail Manager.

Dos nuevas columnas que se han agregado a la ficha de resumen del entorno de Exchange muestran el modo de comando del entorno (PowerShell o de simulación) y su modo de acceso (Allow, Block o Unchanged).

## Solución de problemas y diagnósticos

En la carpeta Support\PowerShell dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Al probar la conectividad con el servicio Exchange mediante el botón Test Connectivity en la ventana Configuration de la consola, se ejecutan todos los cmdlets de solo lectura que emplea el servicio, se ejecutan pruebas de permisos de RBAC en el servidor Exchange para el usuario configurado y se muestran errores y advertencias por colores (azul y amarillo para advertencias, y rojo y naranja para errores).

Una nueva herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y zonas potencialmente problemáticas, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

En casos de asistencia, todas las propiedades de todos los buzones de correo y dispositivos administrados por XenMobile Mail Manager pueden guardarse si se selecciona una casilla de verificación de diagnóstico de la consola.

Ahora, en dichos casos, se respalda el registro por niveles de seguimiento.

## Autenticación

XenMobile Mail Manager respalda la autenticación básica en implementaciones locales. Esto permite que XenMobile Mail Manager pueda usarse cuando el servidor de XenMobile Mail Manager no sea miembro del dominio en que reside el servidor Exchange.

# Problemas resueltos

## Reglas de acceso

XenMobile Mail Manager aplica reglas locales de control de acceso a todos los usuarios de grupos de Active Directory (AD), aunque haya grupos de AD con más de 1000 usuarios. Antes, XenMobile Mail Manager aplicaba reglas locales de control de acceso únicamente a los 1000 primeros usuarios de un grupo de AD. [#548705]

A veces, la consola de XenMobile Mail Manager no ha respondido cuando se consultaban grupos de Active Directory que contuvieran 1000 usuarios o más. [CXM-11729]

La ventana LDAP Configuration ya no muestra modos de autenticación incorrectos. [CXM-5556]

## Instantáneas

Los nombres de usuario con apóstrofes ya no provocan errores en las instantáneas secundarias. [#617549]

En los casos de asistencia en que la canalización esté inhabilitada (la opción Disable Pipelining está seleccionada en la ventana Configuration de la consola de XenMobile Mail Manager), las instantáneas principales ya no fallan en implementaciones locales de Exchange. [#586083]

En los casos de asistencia en que la canalización esté inhabilitada (la opción Disable Pipelining está seleccionada en la ventana Configuration de la consola de XenMobile Mail Manager), ya no se reúnen datos de instantáneas completas independientemente de si el entorno se ha configurado para instantáneas completas o superficiales. Ahora los datos de las instantáneas completas se reúnen únicamente cuando el entorno esté configurado para instantáneas completas. [#586092]

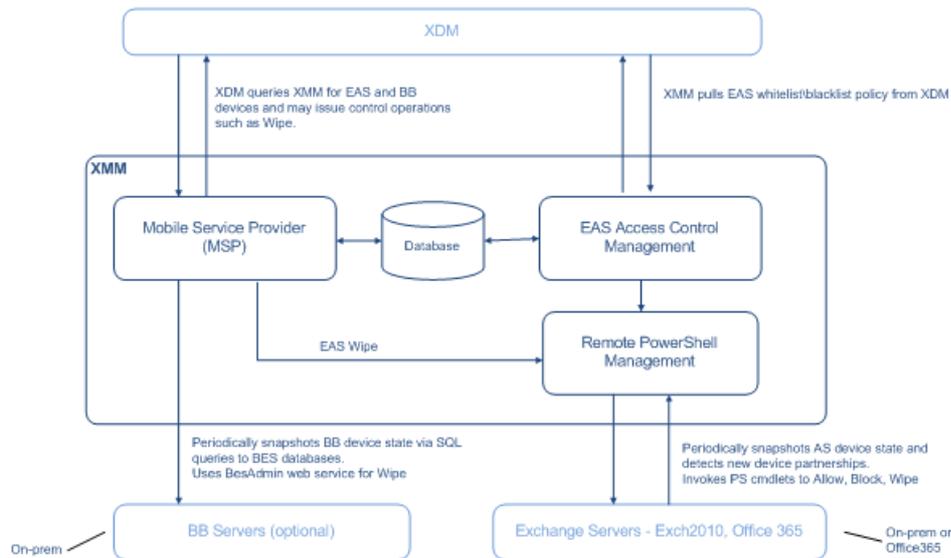
En ocasiones, la primera instantánea principal tras la instalación inicial generaba un error que impedía a XenMobile Mail Manager realizar otras instantáneas principales a menos que el servicio XenMobile Mail Manager se reiniciara. Esto ya no se produce. [CXM-5536]



# Arquitectura

Mar 02, 2017

En el siguiente diagrama, se muestran los componentes principales de XenMobile Mail Manager. Para ver diagramas de referencia de arquitectura en detalle, consulte el artículo [Reference Architecture for On-Premises Deployments](#) de XenMobile Deployment Handbook.



Los tres componentes principales son:

- **Exchange ActiveSync Access Control Management.** Se comunica con XenMobile para recuperar una directiva de Exchange ActiveSync de XenMobile, y combina esta directiva con cualquier directiva definida localmente para determinar los dispositivos Exchange ActiveSync a los que se debe permitir o denegar el acceso a Exchange. Las directivas definidas localmente amplían las reglas de directivas para permitir el control de acceso en función del grupo de Active Directory, del usuario, del tipo de dispositivo o del agente del dispositivo de usuario (por lo general, la versión de la plataforma móvil).
- **Remote PowerShell Management.** Este componente se encarga de programar e invocar comandos de PowerShell remotos para aprobar la directiva compilada por la administración del control de acceso de Exchange ActiveSync. El componente crea, de forma periódica, una instantánea de la base de datos de Exchange ActiveSync para detectar dispositivos nuevos o modificados de Exchange ActiveSync.
- **Mobile Service Provider.** Proporciona una interfaz de servicio Web para que XenMobile envíe consultas a dispositivos Exchange ActiveSync o BlackBerry, y emita operaciones de control (como el borrado) destinados a ellos.

# Requisitos del sistema y requisitos previos

Mar 02, 2017

Se deben cumplir los siguientes requisitos mínimos del sistema para XenMobile Mail Manager:

- Windows Server 2012 R2, Windows Server 2008 R2 (debe ser un servidor en el inglés como idioma)
- Microsoft SQL Server 2016, SQL Server 2012, SQL Server 2012 Express LocalDB o SQL Server Express 2008
- Microsoft .NET Framework 4.5
- BlackBerry Enterprise Service, versión 5 (optativo)

## Versiones mínimas respaldadas de Microsoft Exchange Server

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

## Clientes de correo electrónico del dispositivo

No todos los clientes de correo electrónico devuelven el mismo ID de ActiveSync para un dispositivo. Debido a que XenMobile Mail Manager espera un ID de ActiveSync único para cada dispositivo, solo se admiten los clientes de correo electrónico que generan constantemente el mismo y único ID de ActiveSync para cada dispositivo. Citrix ha realizado pruebas sin errores con estos clientes de correo electrónico:

- Cliente de correo electrónico nativo de HTC
- Cliente de correo electrónico nativo de Samsung
- Cliente de correo electrónico nativo de iOS
- TouchDown para dispositivos smartphone

## Requisitos previos de XenMobile Mail Manager

- Windows Management Framework debe estar instalado.
  - PowerShell V5, V4 y V3
- La directiva de ejecución de PowerShell se debe establecer en RemoteSigned mediante "Set-ExecutionPolicy RemoteSigned".
- El puerto TCP 80 debe estar abierto entre el equipo con XenMobile Mail Manager y el servidor Exchange remoto.

## Requisitos para un equipo local con Exchange

**Permisos.** Las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben permitir la conexión al servidor Exchange y deben tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange.

- **Para Exchange Server 2010 SP2:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer

- Get-ManagementRole
- Get-ManagementRoleAssignment
- **Para el servidor Exchange Server 2013 y Exchange Server 2016:**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- Si XenMobile Mail Manager está configurado para ver todo el bosque, se debe haber concedido permiso para ejecutar: Set-AdServerSettings -ViewEntireForest \$true.
- Las credenciales suministradas deben contar con derecho a conectarse al servidor Exchange mediante el shell remoto. De forma predeterminada, el usuario que haya instalado Exchange tiene ese derecho.
- Según el artículo de Microsoft TechNet [about\\_Remote\\_Requirements](#), para establecer una conexión remota y ejecutar comandos remotos, las credenciales deben corresponder a un usuario que sea administrador en la máquina remota. Según 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.

## Requisitos para Office 365 Exchange

- **Permisos.** Las credenciales especificadas en la interfaz de usuario de la configuración de Exchange deben permitir la conexión a Office 365 y deben tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **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.

# Instalación y configuración

Mar 02, 2017

1. Haga clic en el archivo XmmSetup.msi y, a continuación, siga las instrucciones del programa de instalación para instalar XenMobile Mail Manager.

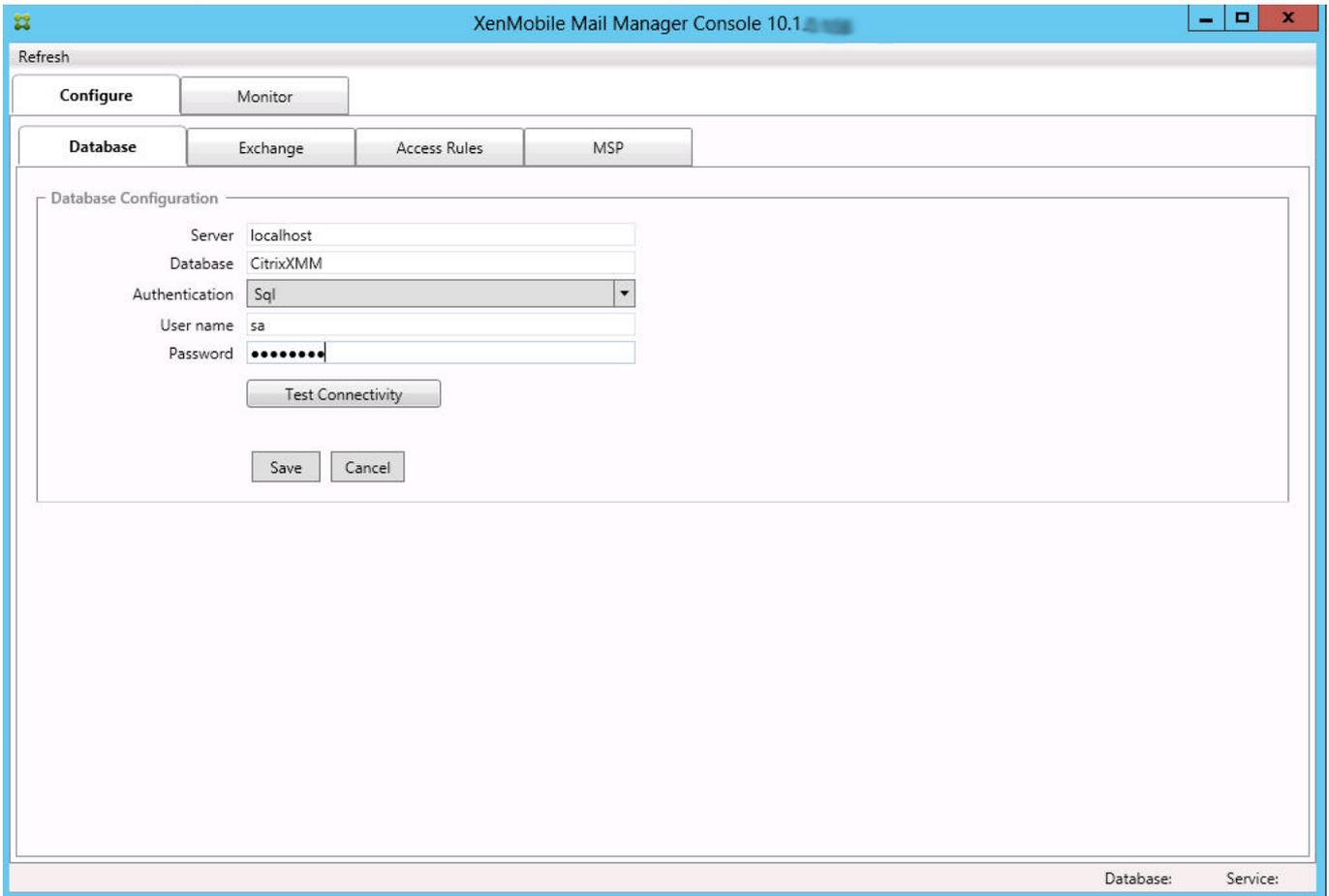


2. Deje **Launch the Configure utility** seleccionado en la última pantalla del asistente de configuración. Si no, en el menú **Inicio**, abra **XenMobile Mail Manager**.

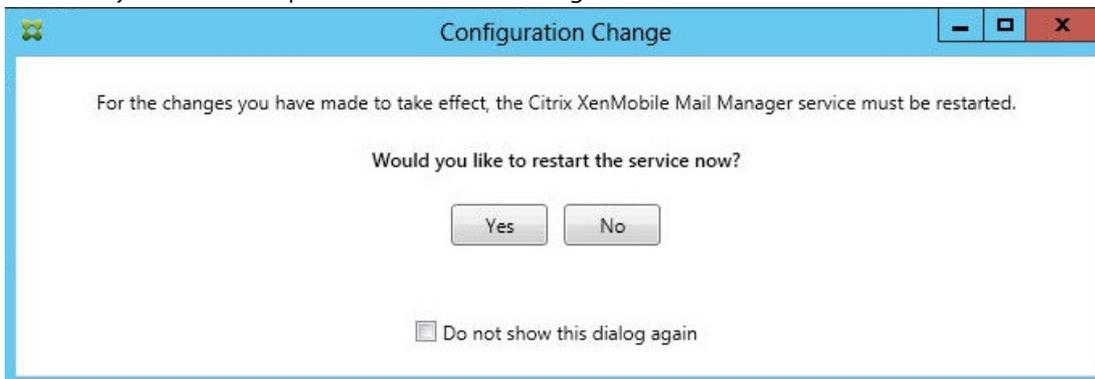


3. Configure las siguientes propiedades de base de datos:
  1. Seleccione la ficha **Configure > Database**.
  2. Escriba el nombre del servidor SQL Server (el valor predeterminado es localhost).
  3. Conserve la opción predeterminada de la base de datos, CitrixXmm.
  4. Seleccione uno de los siguientes modos de autenticación para SQL:

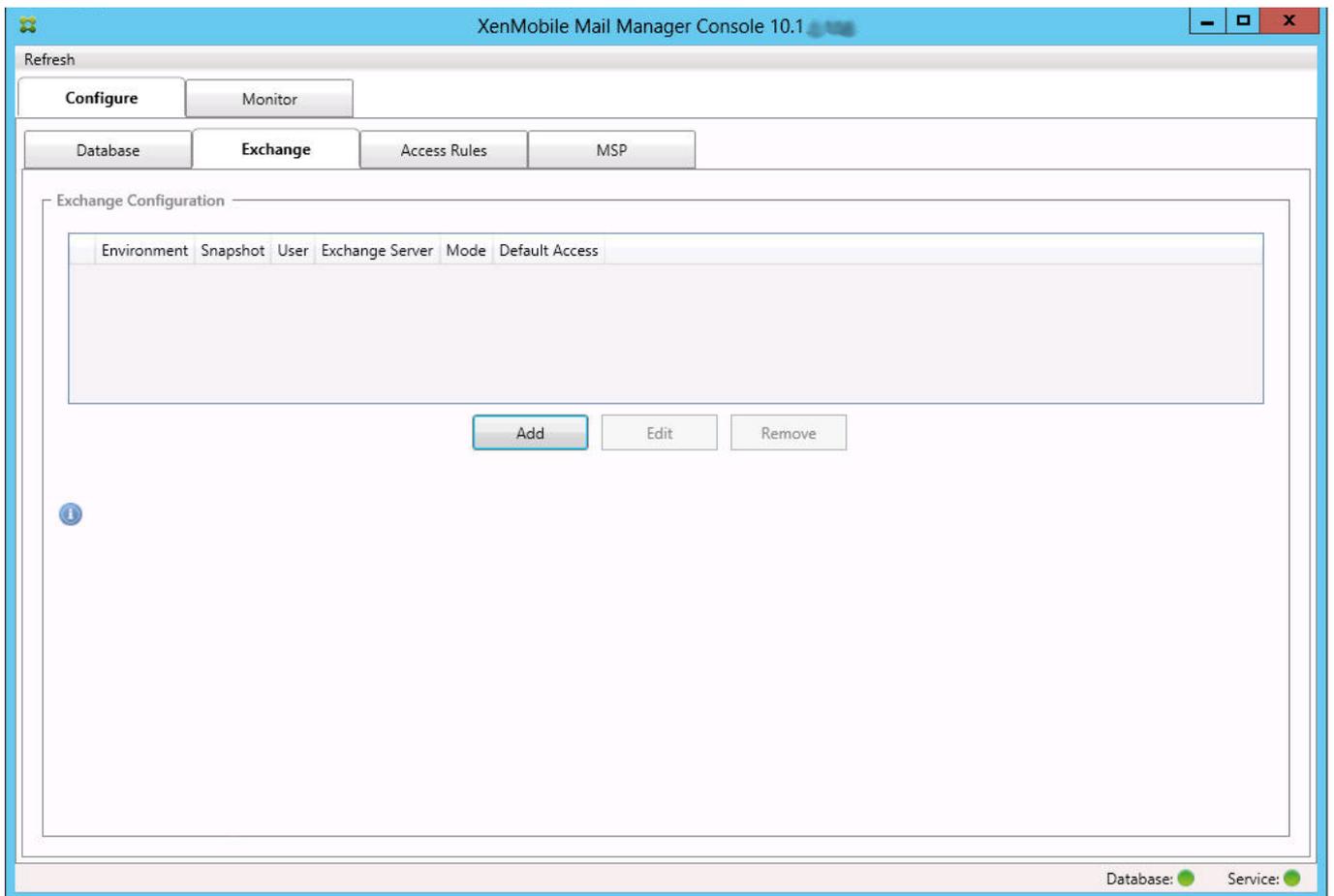
- **Sql.** Escriba el nombre de usuario y la contraseña de un usuario de SQL válido.
  - **Windows Integrated.** Si elige esta opción, las credenciales de inicio de sesión del servicio de XenMobile Mail Manager se deben cambiar a una cuenta de Windows que tenga permisos para acceder al servidor SQL Server. Para ello, abra **Panel de control > Herramientas administrativas > Servicios**, haga clic con el botón secundario en la entrada del servicio de XenMobile Mail Manager y, a continuación, haga clic en la ficha **Iniciar sesión**.  
**Nota:** Si para la conexión de base de datos de BlackBerry también se selecciona la seguridad integrada de Windows, la cuenta de Windows que se especifique aquí también debe tener acceso a la base de datos de BlackBerry.
5. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor SQL Server y, a continuación, haga clic en **Save**.



4. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.



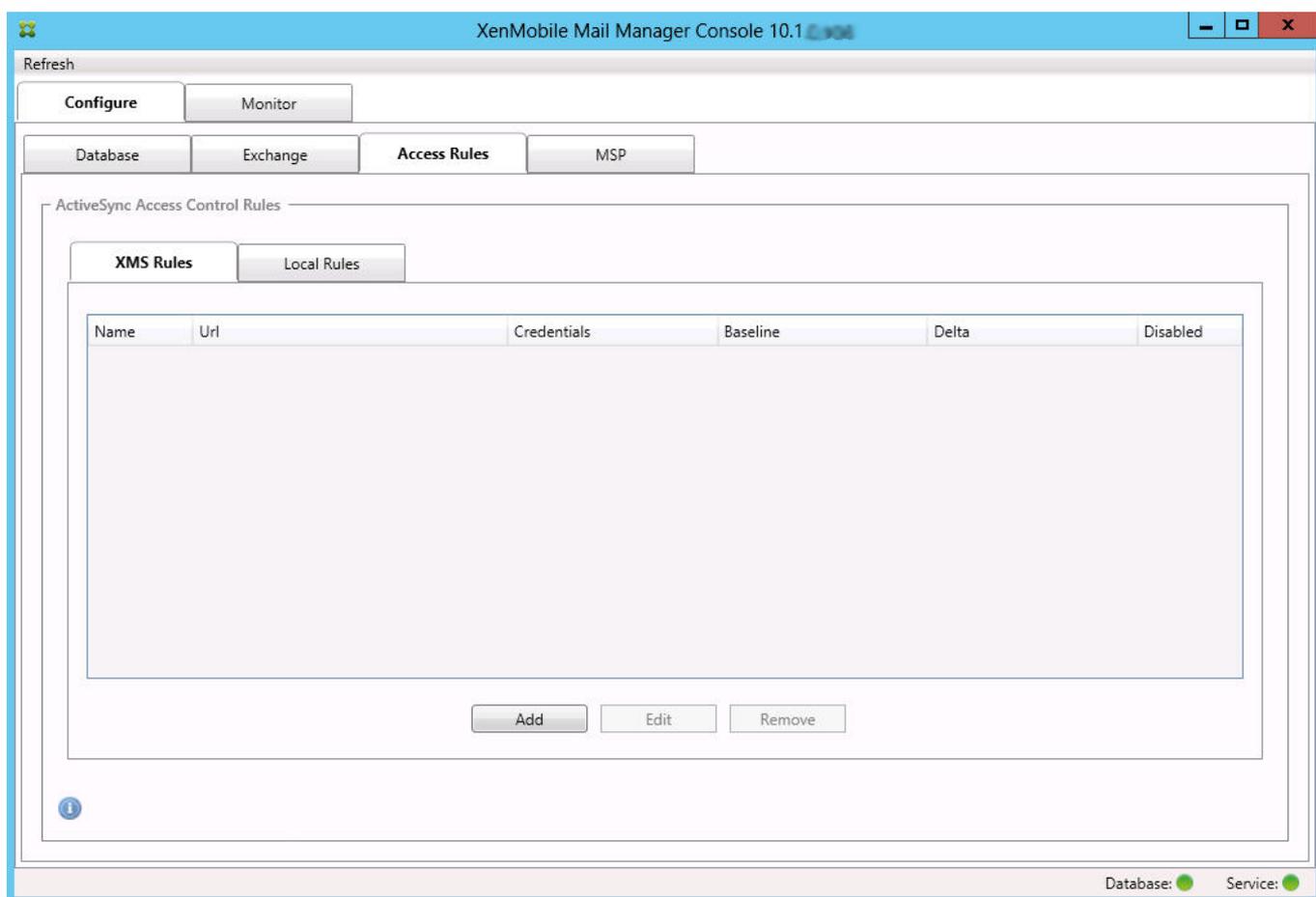
5. Configure uno o varios servidores Exchange:
1. Si administra un solo entorno de Exchange, solo deberá especificar un servidor. Si administra varios entornos de Exchange, deberá especificar un servidor Exchange por cada entorno de Exchange.
  2. Haga clic en la ficha **Configure > Exchange**.



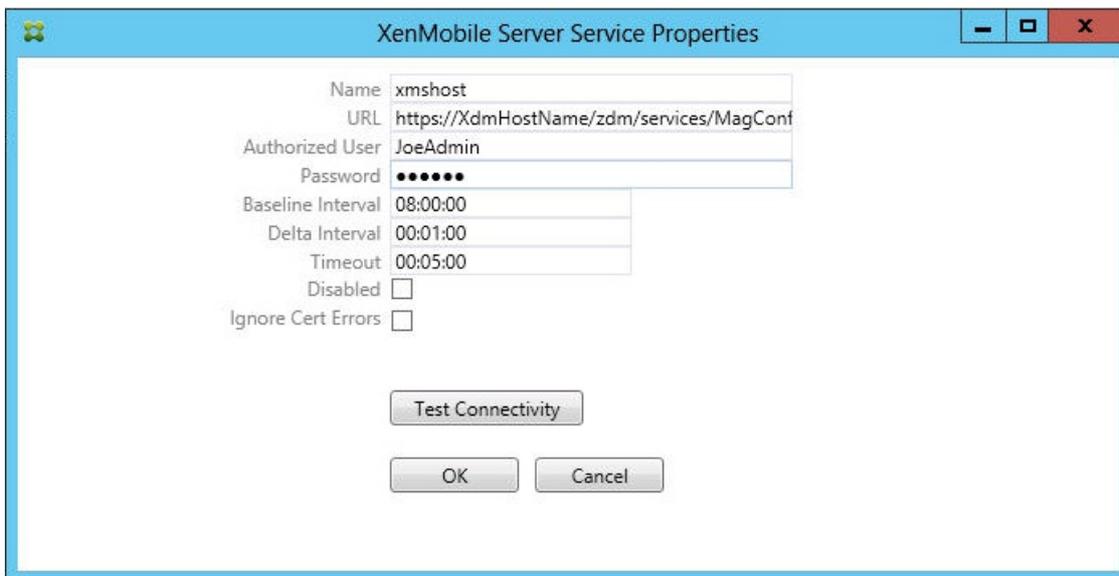
3. Haga clic en **Add**.
4. Seleccione el tipo de entorno del servidor Exchange: **On Premise** u **Office 365**.

5. Si selecciona **On Premise**, escriba el nombre del servidor Exchange que se usará para los comandos remotos de PowerShell.
6. Escriba el nombre de usuario de una identidad de Windows que tenga los permisos apropiados en el servidor Exchange, como se especifica en el apartado de requisitos.
7. Escriba la contraseña del usuario en el campo **Password**.
8. Seleccione un horario para ejecutar las instantáneas principales. Una instantánea principal detecta cada asociación de Exchange ActiveSync.
9. Seleccione un horario para ejecutar las instantáneas secundarias. Una instantánea secundaria detecta asociaciones recién creadas de Exchange ActiveSync.
10. Seleccione el tipo de instantánea: **Deep** o **Shallow**. Las instantáneas superficiales (Shallow) son más rápidas y, con ellas, es suficiente para llevar a cabo todas las funciones de control de acceso de Exchange ActiveSync que se pueden realizar en XenMobile Mail Manager. Las instantáneas detalladas (Deep) pueden tardar mucho más y solo son necesarias si el proveedor de servicios móviles está habilitado para ActiveSync, lo que permite que XenMobile envíe consultas a dispositivos no administrados.
11. Seleccione el acceso predeterminado: **Allow**, **Block** o **Unchanged**. Este parámetro controla cómo se tratarán todos los dispositivos, excepto aquellos que XenMobile o las reglas locales identifiquen de forma explícita. Si selecciona "Allow", permitirá el acceso de ActiveSync a dichos dispositivos; si selecciona "Block", denegará el acceso; si selecciona "Unchanged", no se realizará ningún cambio.
12. Seleccione el modo de comandos de ActiveSync: **PowerShell** o **Simulation**.
  - En el modo PowerShell, XenMobile Mail Manager emitirá comandos de PowerShell para habilitar el control de acceso pertinente.
  - En el modo Simulation, XenMobile Mail Manager no emitirá comandos de PowerShell, pero registrará en la base de datos el comando en cuestión, así como los resultados esperados. En el modo de simulación, el usuario puede usar la ficha Monitor para ver lo que podría haber ocurrido si se hubiera habilitado el modo de PowerShell.

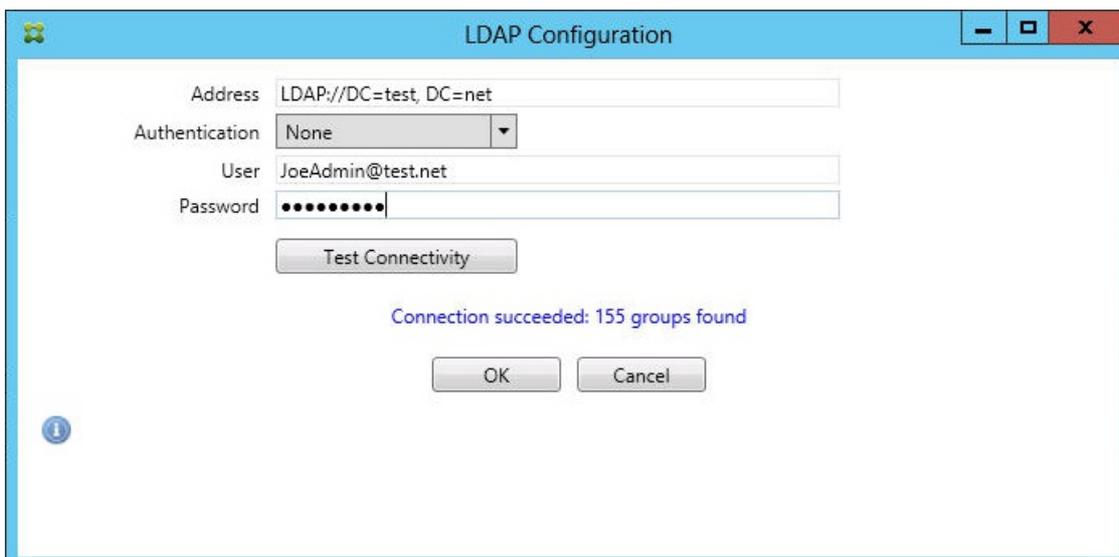
13. Seleccione **View Entire Forest** para configurar XenMobile Mail Manager y ver todo el bosque de Active Directory en el entorno de Exchange.
  14. Seleccione el protocolo de autenticación: **Kerberos** o **Basic**. XenMobile Mail Manager respalda la autenticación básica en implementaciones locales. Esto permite que XenMobile Mail Manager pueda usarse cuando el servidor de XenMobile Mail Manager no sea miembro del dominio en que reside el servidor Exchange.
  15. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor Exchange y, a continuación, haga clic en **Save**.
  16. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.
6. Configure las reglas de acceso:
1. Seleccione la ficha **Configure > Access Rules**.
  2. Haga clic en la ficha **XDM Rules**.



3. Haga clic en **Add**.



4. Escriba un nombre para las reglas del servidor XenMobile, como XdmHost.
  5. Modifique la cadena de URL para que haga referencia al servidor XenMobile. Por ejemplo, si el nombre del servidor es XdmHost, especifique `http://XdmHostName/zdm/services/MagConfigService`.
  6. Especifique un usuario autorizado en el servidor.
  7. Escriba la contraseña del usuario.
  8. Conserve los valores predeterminados de **Baseline Interval**, **Delta Interval** y **Timeout values**.
  9. Haga clic en **Test Connectivity** para probar la conexión con el servidor.
- Nota:** Si la casilla Disabled está marcada, el servicio de XenMobile Mail no recopilará directivas del servidor XenMobile.
10. Haga clic en **OK**.
7. Haga clic en la ficha **Local Rules**.
    1. Si quiere crear reglas locales que operen en grupos de Active Directory, haga clic en **Configure LDAP** y, a continuación, configure las propiedades de conexión de LDAP.



2. Puede agregar reglas locales en función de: **ActiveSync Device ID** (el ID de dispositivo de ActiveSync), **Device Type** (el tipo de dispositivo), **AD Group** (el grupo de Active Directory), **User** (el usuario) o **UserAgent** (el agente del usuario del dispositivo). En la lista, seleccione el tipo adecuado. Para ver información detallada, consulte [Reglas de control de](#)

acceso de XenMobile Mail Manager.

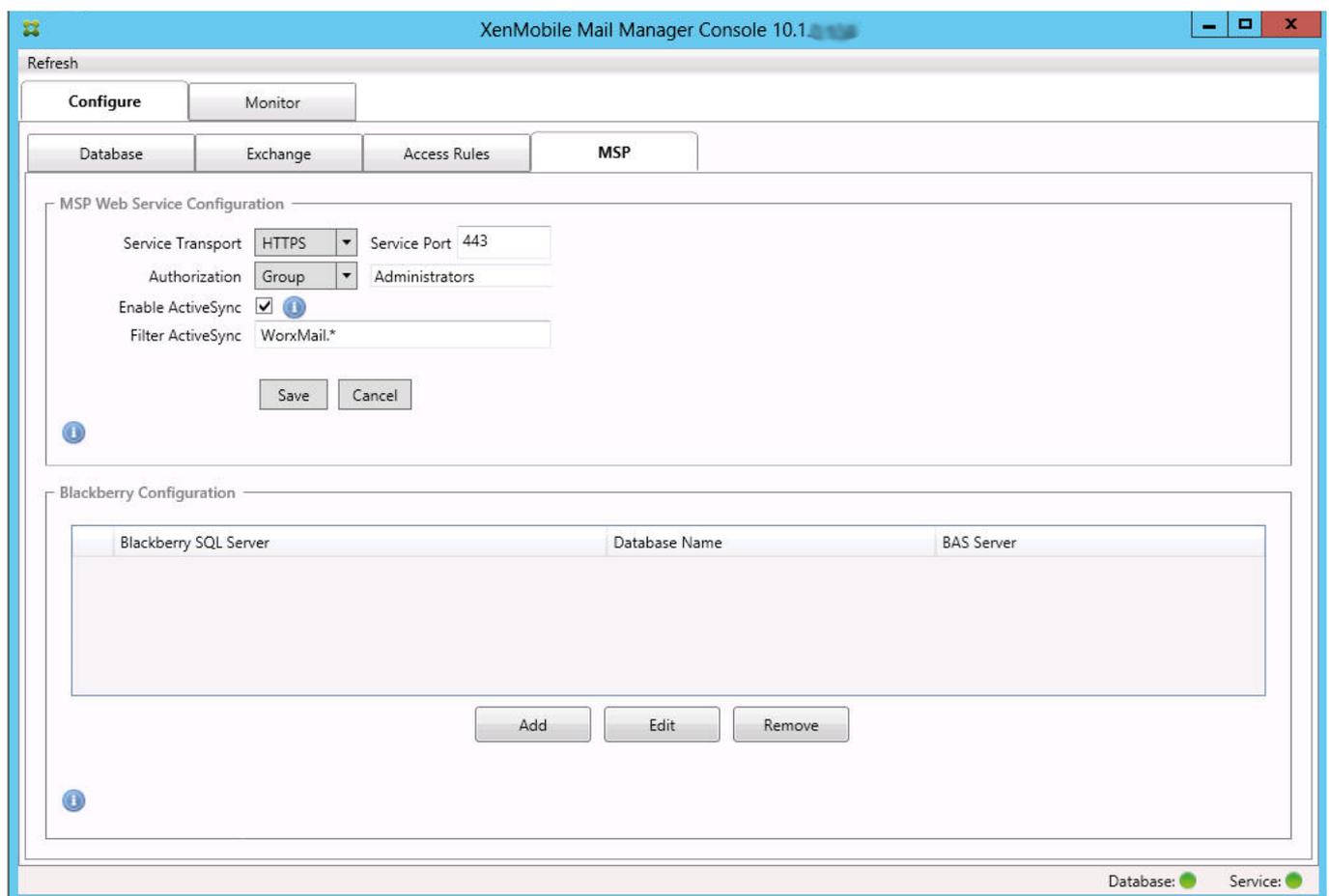
3. Escriba texto o fragmentos de texto en el cuadro de texto. Si quiere, haga clic en el botón de consulta para ver las entidades que se corresponden con el fragmento.

**Nota:** Para todos los criterios aparte de **Group**, el sistema se basa en los dispositivos que se han encontrado en una instantánea. Por lo tanto, si acaba de empezar y aún no ha completado ninguna instantánea, no habrá entidades disponibles.

4. Seleccione un valor de texto y, a continuación, haga clic en **Allow** o en **Deny** para agregarlo a **Rule List** en el lado derecho. Puede quitar reglas o cambiar su orden mediante los botones situados a la derecha del panel **Rule List**. El orden es importante porque las reglas se cotejan en el orden mostrado con un usuario y un dispositivo determinados. Por tanto, una correspondencia en una regla que se encuentre más arriba significa que las siguientes reglas no tendrán ningún efecto. Por ejemplo, si tiene una regla que permite todos los dispositivos iPad y otra regla posterior que bloquee al usuario "Sergio", el iPad de Sergio aún tendrá permiso porque la regla "iPad" tiene una prioridad mayor (se coteja antes) que la regla "Sergio".
5. Para llevar a cabo un análisis de las reglas de la lista con el fin de buscar posibles conflictos, invalidaciones o complementaciones, haga clic en **Analyze**.
6. Haga clic en **Save**.
8. Configure el proveedor de servicios móviles.

**Nota:** El proveedor de servicios móviles es optativo; solo es necesario si XenMobile también está configurado para usar la interfaz del proveedor de servicios móviles con el fin de consultar dispositivos no administrados.

1. Seleccione la ficha **Configure > MSP**.



2. Establezca el tipo de servicio de transporte como **HTTP** o **HTTPS** para el servicio del proveedor de servicios móviles.
3. Establezca el puerto del servicio (por regla general, 80 y 443) para el servicio del proveedor de servicios móviles.

**Nota:** Si usa el puerto 443, el puerto requiere un certificado SSL asociado a él en IIS.

- Defina el usuario o el grupo de autorización. Esta opción establece el usuario o grupo de usuarios que podrán conectarse al proveedor de servicios móviles desde XenMobile.
- Defina si se habilitan o no las consultas de ActiveSync.

**Nota:** Si se habilitan las consultas de ActiveSync para el servidor XenMobile, el tipo de instantánea de uno o más servidores Exchange debe ser **Deep**, lo que puede generar costes importantes de rendimiento para realizar instantáneas.

- De forma predeterminada, los dispositivos ActiveSync que se corresponden con la expresión regular Secure Mail.\* no se enviarán a XenMobile. Para cambiar este comportamiento, modifique el campo **Filter ActiveSync** como sea necesario.

**Nota:** Dejarlo en blanco significa que todos los dispositivos se reenviarán a XenMobile.

- Haga clic en **Save**.

- Si quiere, puede configurar uno o más servidores BlackBerry Enterprise Server (BES):

- Haga clic en **Add**.
- Escriba el nombre del servidor SQL Server para BES.

The screenshot shows the 'BES Properties' dialog box. It is divided into two main sections. The top section, 'BES Sql Server', contains the following fields: 'Server' (BesServer), 'Database' (BesMgmt), 'Authentication' (Sql), 'User name' (JoeAdmin), 'Password' (masked with dots), a 'Test Connectivity' button, and 'Sync Schedule' (Every 30 Minutes). The bottom section, 'Blackberry Device Administration from XMS', contains: 'Enabled' (checked), 'BAS Server' (BASServer), 'BAS Port' (443), 'Domain\User' (ServerName\JoeAdmin), 'Password' (masked with dots), and a 'Test Connectivity' button. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

- Escriba el nombre de la base de datos de administración de BES.

- Seleccione el modo de autenticación. Si se selecciona la autenticación integrada de Windows, la cuenta de usuario del

servicio de XenMobile Mail Manager será la cuenta utilizada para conectarse al servidor SQL Server para BES.

**Nota:** Si también selecciona la seguridad integrada de Windows para la conexión de base de datos de XenMobile Mail Manager, la cuenta de Windows especificada aquí también debe tener acceso a la base de datos de XenMobile Mail Manager.

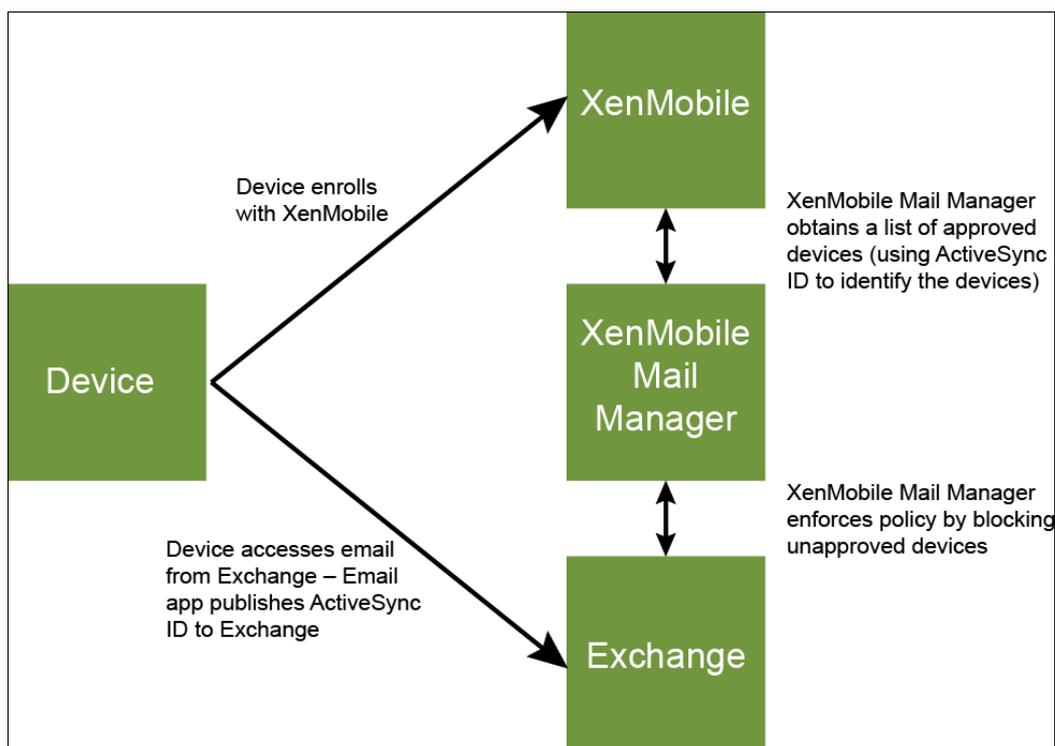
5. Si se selecciona **SQL authentication**, especifique el nombre de usuario y la contraseña.
6. Configure la programación de sincronización en **Sync Schedule**. Esta es la programación usada para conectarse al servidor SQL Server para BES y buscar actualizaciones de dispositivo.
7. Haga clic en **Test Connectivity** para comprobar la conectividad con el servidor SQL Server.  
**Nota:** Si se selecciona Windows Integrated (la seguridad integrada de Windows), esta prueba utiliza el usuario actual que ha iniciado sesión, no el usuario del servicio de XenMobile Mail Manager; por lo tanto, la prueba de autenticación de SQL no es precisa.
8. Si quiere admitir el borrado (Wipe) o el restablecimiento de contraseña (ResetPassword) remotos para los dispositivos BlackBerry desde XenMobile, marque la casilla **Enabled**.
  1. Introduzca el nombre de dominio completo (FQDN) del servidor BES.
  2. Escriba el puerto de BES usado para el servicio Web del administrador.
  3. Escriba el nombre del usuario y la contraseña completos requeridos por el servicio de BES.
  4. Haga clic en **Test Connectivity** para probar la conexión al servidor BES.
  5. Haga clic en **Save**.

# Aplicación de directivas de correo electrónico con los ID de ActiveSync

Mar 02, 2017

Es posible que una directiva de correo electrónico de la empresa indique que ciertos dispositivos no tienen la aprobación para usar el correo electrónico de la empresa. Para cumplir con esta directiva, asegúrese de que los usuarios no pueden tener acceso al correo electrónico de la empresa desde dichos dispositivos. XenMobile Mail Manager y XenMobile funcionan conjuntamente para aplicar la directiva de correo electrónico. XenMobile define la directiva para el acceso de correo electrónico de la empresa y, cuando un dispositivo no aprobado se inscribe con XenMobile, XenMobile Mail Manager aplica la directiva.

El cliente de correo electrónico en un dispositivo se anuncia a Exchange Server (o Office 365) usando el ID del dispositivo, también conocido como el ID de ActiveSync, que se usa para identificar el dispositivo de manera exclusiva. Secure Hub obtiene un identificador similar y envía el identificador a XenMobile cuando se inscribe el dispositivo. Comparando los dos ID de dispositivo, XenMobile Mail Manager puede determinar si un dispositivo en concreto debe tener acceso al correo electrónico de la empresa. En la siguiente ilustración se muestra este concepto.



Si XenMobile envía un ID de ActiveSync a XenMobile Mail Manager que es diferente del ID que el dispositivo publica en Exchange, XenMobile Mail Manager no puede indicar a Exchange qué hacer con el dispositivo.

Los ID de ActiveSync coincidentes funcionan con fiabilidad en la mayoría de las plataformas; sin embargo, Citrix ha detectado que en algunas implementaciones de Android, el ID de ActiveSync enviado desde el dispositivo es diferente del ID que el cliente de correo anuncia en Exchange. Para evitar este problema, puede hacer lo siguiente:

- En la plataforma Samsung SAFE, inserte la configuración de ActiveSync del dispositivo desde XenMobile.

- En todas las demás plataformas Android, inserte la configuración de la aplicación Touchdown y la configuración de Touchdown ActiveSync desde XenMobile.

No obstante, esto no impide que un empleado instale un cliente de correo electrónico distinto de Touchdown en un dispositivo Android. Para garantizar que la directiva de acceso al correo electrónico de la empresa se aplica correctamente, puede adoptar una postura de seguridad defensiva y configurar XenMobile Mail Manager para que bloquee los mensajes de correo electrónico definiendo la directiva estática con el valor Deny by default. Esto significa que si un empleado configura un cliente de correo electrónico distinto de Touchdown en un dispositivo Android, y si la detección de ID de ActiveSync no funciona correctamente, el acceso al correo electrónico de la empresa le será denegado a dicho empleado.

# Reglas de control de acceso

Mar 02, 2017

XenMobile Mail Manager ofrece un enfoque basado en reglas para configurar de forma dinámica el control del acceso a los dispositivos Exchange ActiveSync. Una regla de control de acceso de XenMobile Mail Manager está compuesta de dos partes: una expresión correspondiente y un estado de acceso deseado (Permitir o Bloquear). Una regla se puede cotejar con un dispositivo Exchange ActiveSync concreto para determinar si se le puede aplicar (es decir, si corresponde al dispositivo). Hay varios tipos de expresiones correspondientes. Por ejemplo: una regla puede corresponderse con todos los dispositivos de un determinado tipo o un ID de Exchange ActiveSync o todos los dispositivos de un usuario concreto, entre otros. En cualquier momento durante el proceso de agregar, quitar y cambiar el orden de las reglas en la lista de reglas, puede hacer clic en el botón **Cancel** para revertir la lista de reglas al estado en que estaba al abrirla. A menos que haga clic en **Save**, los cambios realizados en esta ventana se perderán si cierra la herramienta de configuración.

XenMobile Mail Manager contiene tres tipos de reglas: reglas locales, reglas del servidor XenMobile, (también conocidas como reglas de Device Manager) y la regla del acceso predeterminado.

**Reglas locales.** Las reglas locales tienen la prioridad más alta: Si un dispositivo coincide con una regla local, el proceso de cotejo de reglas se detiene. No se consultarán ni las reglas del servidor XenMobile ni la regla del acceso predeterminado. Las reglas locales se configuran localmente en XenMobile Mail Manager, desde la ficha Configure > Access Rules > Local Rules. La correspondencia de apoyo se basa en la pertenencia de un usuario de un grupo determinado de Active Directory. La correspondencia de apoyo se basa en expresiones regulares de los siguientes campos:

- ID del dispositivo ActiveSync
- Tipo de dispositivo ActiveSync
- Nombre principal de usuario (UPN)
- Agente del usuario de ActiveSync (normalmente, la plataforma del dispositivo o el cliente de correo electrónico)

Mientras una instantánea principal se complete y encuentre dispositivos, podrá agregar reglas, ya sean de expresión regular o normal. Si no se completa ninguna instantánea principal, solo podrá agregar reglas de expresión regular.

**Reglas del servidor XenMobile.** Las reglas de servidor XenMobile hacen referencia a un servidor externo de XenMobile que proporciona reglas de dispositivos administrados. El servidor XenMobile se puede configurar con sus propias reglas de alto nivel, que identifican aquellos dispositivos que se van a permitir o a bloquear en función de las propiedades que conozca XenMobile, como, por ejemplo, si el dispositivo se ha liberado por jailbreak o si contiene aplicaciones prohibidas. XenMobile coteja las reglas de alto nivel y genera un conjunto de identificadores de dispositivos ActiveSync permitidos o bloqueados. Después, estos ID se entregan a XenMobile Mail Manager.

**Regla del acceso predeterminado.** La regla del acceso predeterminado es única en que es una correspondencia potencial con todos los dispositivos y siempre se coteja la última. Esta es una regla comodín, lo que significa que, si un dispositivo determinado no coincide con ninguna regla local o del servidor XenMobile, el estado del acceso al dispositivo lo determina el estado de la regla del acceso predeterminado.

- **Acceso predeterminado - Permitir.** Se permitirá el acceso de cualquier dispositivo que no coincida con una regla local o del servidor XenMobile.
- **Acceso predeterminado - Bloquear.** Se bloqueará el acceso de cualquier dispositivo que no coincida con una regla local o del servidor XenMobile.
- **Acceso predeterminado - Sin cambios.** XenMobile Mail Manager no modificará el estado de acceso de un dispositivo que no coincida con una regla local o del servidor XenMobile. Si Exchange ha puesto un dispositivo en el modo de

cuarentena, no se realiza ninguna acción; por ejemplo, la única forma de quitar un dispositivo del modo de cuarentena es tener una regla local o XDM que ignore explícitamente la cuarentena.

## Acerca de los cotejos de reglas

Las reglas se cotejan siguiendo un orden (de mayor a menor prioridad) con cada dispositivo sobre el que Exchange informa a XenMobile Mail Manager:

- Reglas locales
- Reglas del servidor XenMobile
- Regla del acceso predeterminado

Cuando se encuentra una correspondencia, el cotejo se detiene. Por ejemplo: si una regla local coincide con un dispositivo determinado, este no se cotejará con ninguna regla del servidor XenMobile ni con la regla del acceso predeterminado. Esto también se da en el caso de un tipo concreto de regla. Por ejemplo, si hay más de una correspondencia en la lista de reglas de un dispositivo concreto, el cotejo se detiene tan pronto como se encuentre la primera correspondencia.

XenMobile Mail Manager vuelve a cotejar el conjunto de reglas definido cuando cambian las propiedades del dispositivo, cuando se agregan o quitan dispositivos o cuando cambian las reglas en sí. Las instantáneas principales pueden elegir cambios y eliminaciones de las propiedades de dispositivo a intervalos que se pueden configurar. Las instantáneas secundarias eligen dispositivos nuevos a intervalos que se pueden configurar.

Exchange ActiveSync también tiene reglas que controlan el acceso. Es importante entender la manera en que funcionan estas reglas en el contexto de XenMobile Mail Manager. Exchange se puede configurar con tres niveles de reglas: exenciones personales, reglas de dispositivos y parámetros de organización. XenMobile Mail Manager automatiza el control del acceso por la emisión, mediante programación, de solicitudes remotas de PowerShell que afectan a las listas de excepciones personales. Se trata de listas de identificadores de dispositivos Exchange ActiveSync permitidos o bloqueados asociados a un buzón de correo determinado. Cuando XenMobile Mail Manager se implementa, asume la capacidad de administración de las listas de exención en Exchange. Para obtener más información, consulte [este artículo de Microsoft](#).

El análisis es especialmente útil en situaciones en que se han definido varias reglas para el mismo campo. Puede detectar problemas potenciales de las relaciones entre las reglas. El análisis se realiza con respecto a los campos de reglas; por ejemplo, las reglas se analizan en grupos basados en el campo correspondiente, como el ID del dispositivo ActiveSync, el tipo de dispositivo ActiveSync, el usuario y el agente de usuario, entre otros.

## Terminología referente a las reglas:

- **Overriding rule** (Regla de invalidación). Se produce una invalidación cuando hay más de una regla que se podría aplicar al mismo dispositivo. Como las reglas se cotejan por prioridad en la lista, es posible que las últimas instancias de reglas que se podrían aplicar nunca se cotejen.
- **Conflicting rule** (Regla en conflicto). El conflicto se produce cuando hay más de una regla que se podría aplicar al mismo dispositivo, pero el acceso (permitir o bloquear) no se corresponde. Si las reglas conflictivas no son de expresión regular, un conflicto siempre tiene la connotación implícita de una invalidación.
- **Supplemental rule** (Regla adicional). Se produce una adición cuando hay varias reglas de expresión regular y, por lo tanto, es posible que necesite comprobar que las dos (o más) expresiones regulares se pueden combinar en una sola regla de expresión regular, o bien deberá comprobar que no dupliquen la funcionalidad. Una regla adicional también puede entrar en conflicto en el acceso (permitir o bloquear).
- **Primary rule** (Regla primaria). La regla primaria es aquella sobre la que se ha hecho clic en el cuadro de diálogo. La regla está indicada visualmente por una línea de borde sólido que la rodea. La regla también tiene una o dos flechas verdes que apuntan hacia arriba o hacia abajo. Si una flecha apunta arriba, indica que hay reglas auxiliares que preceden la regla

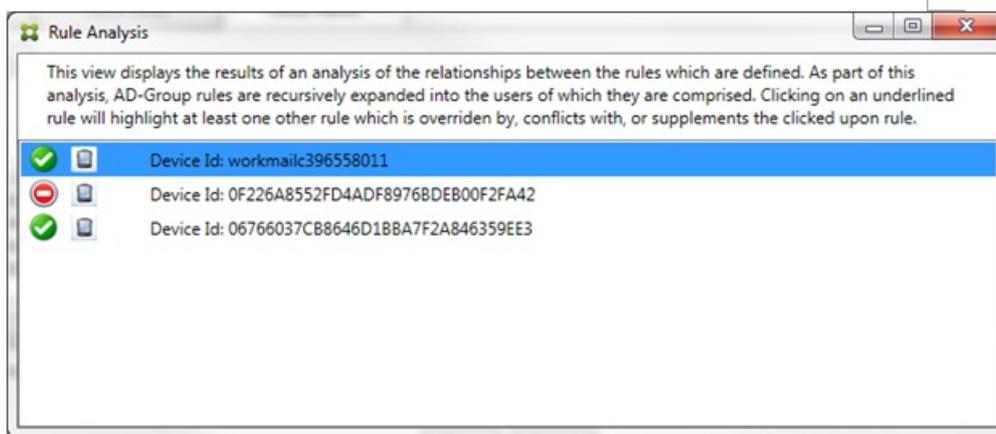
primaria. Si una flecha apunta abajo, indica que hay reglas auxiliares que siguen a la regla primaria. Solo una regla primaria puede estar activa en un momento dado.

- **Ancillary rule** (Regla auxiliar). Una regla auxiliar está relacionada con la regla primaria, ya sea por invalidación, por conflicto o por reglas adicionales. Las reglas se indican visualmente con un borde discontinuo que las rodea. Puede haber entre una y varias reglas auxiliares por cada regla primaria. Al hacer clic en una entrada subrayada, las reglas auxiliares marcadas siempre se marcan con respecto a la regla primaria. Por ejemplo: la regla primaria invalidará la regla auxiliar, y/o la regla auxiliar entrará en conflicto en el acceso con la regla primaria, y/o la regla auxiliar complementará la regla primaria.

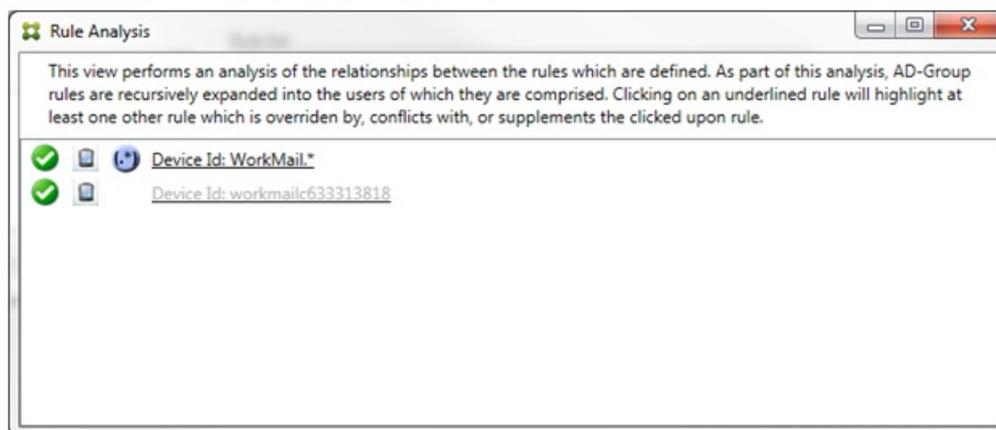
### Aspecto de los tipos de reglas en el cuadro del análisis de reglas

Cuando no haya conflictos, invalidaciones o complementaciones, el cuadro Rule Analysis no contendrá entradas subrayadas. Hacer clic en alguno de los elementos no tiene ningún efecto: solo se habrá seleccionado el elemento de la manera habitual.

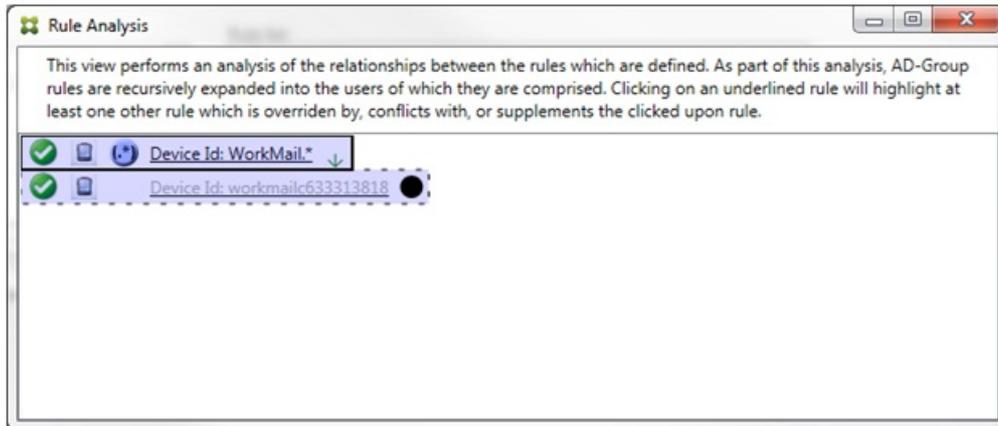
La ventana Rule Analysis (análisis de reglas) tiene una casilla de verificación que, marcada, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.



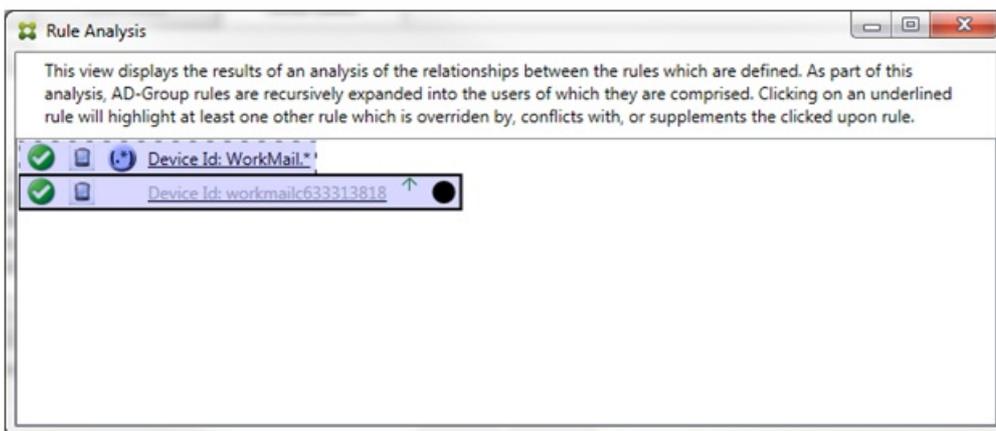
Cuando se produzca una invalidación, se subrayarán al menos dos reglas: la primaria y las auxiliares. Al menos una regla auxiliar aparecerá con una fuente más atenuada para indicar que se ha reemplazado por otra regla de mayor prioridad. Puede hacer clic en la regla invalidada para averiguar qué regla o reglas la han invalidado. Cada vez que se marque una regla como invalidada, ya sea porque es la primaria o porque es la auxiliar, aparecerá un círculo negro junto a ella, a modo de indicación más visual de que la regla está inactiva. Por ejemplo, antes de hacer clic en la regla, el cuadro aparecerá de la siguiente manera:



Cuando haga clic en la regla de mayor prioridad, el cuadro aparecerá de la siguiente manera:

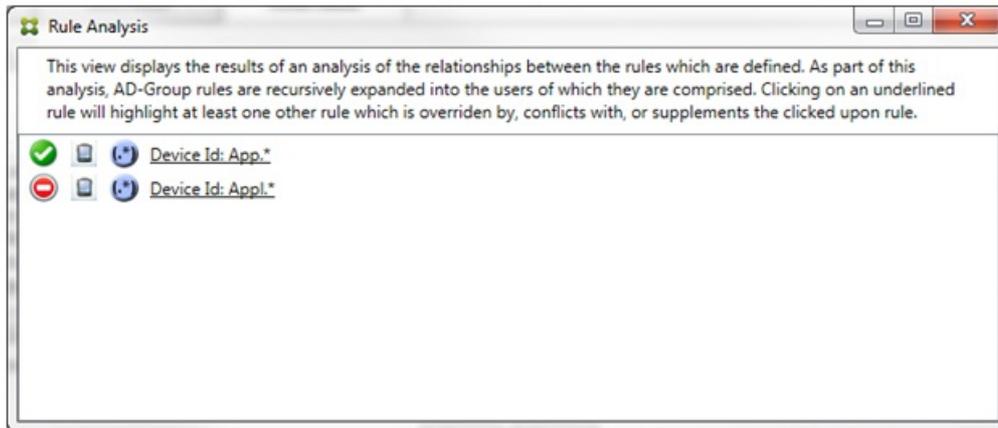


En este ejemplo, la regla de expresión regular WorkMail.\* es la regla primaria (indicada con el borde sólido) y la regla normal workmailc633313818 es una regla auxiliar (indicada con el borde discontinuo). El punto negro junto a la regla auxiliar es una indicación visual de que la regla está inactiva (nunca se cotejará) debido a la regla de expresión regular de mayor prioridad que la precede. Después de hacer clic en la regla invalidada, el cuadro aparecerá de la siguiente manera:

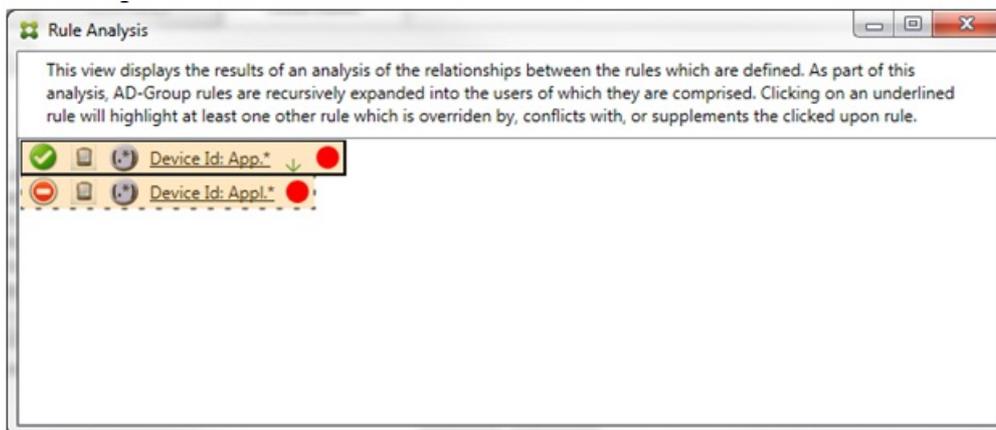


En el ejemplo anterior, la regla de expresión regular WorkMail.\* es la regla auxiliar (indicada con el borde discontinuo) y la regla normal workmailc633313818 es la regla primaria (indicada con el borde sólido). En este sencillo ejemplo, no hay mucha diferencia. Para un ejemplo más complejo, consulte el ejemplo de expresión compleja más adelante en este apartado. En un entorno con varias reglas definidas, hacer clic en la regla invalidada identificaría rápidamente las reglas que la han invalidado.

Cuando se produzca un conflicto, se subrayarán al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas en conflicto se indican con un punto de color rojo. Aquellas reglas que solo entren en conflicto una con otra solo se dan cuando hay dos o más reglas de expresión regular definidas. En todos los demás casos de conflictos, no solo hay un conflicto, sino también una invalidación. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparecerá de la siguiente manera:

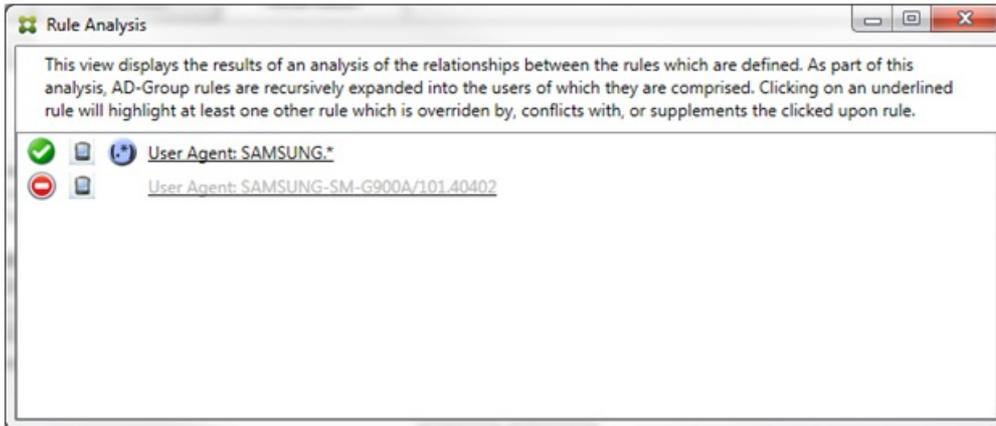


Tras examinar las dos reglas de expresiones regulares, es evidente que la primera regla permite el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "App" y la segunda regla niega el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "Appl". Además, aunque la segunda regla rechaza todos los dispositivos con un ID de dispositivo que contenga "Appl", no se negará el acceso a ningún dispositivo que se corresponda con ese criterio por la prioridad más alta de la regla que permite el acceso. Después de hacer clic en la primera regla, el cuadro aparecerá de la siguiente manera:



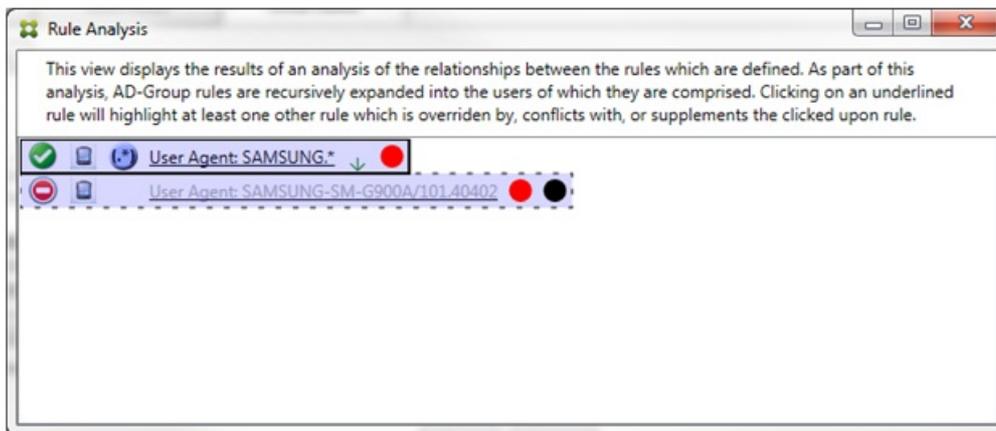
En este caso, tanto la regla primaria (la regla de expresión regular App.\*) como la regla auxiliar (la regla de expresión regular Appl.\*) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.

En un caso de conflicto e invalidación, la regla primaria (regla de expresión regular App.\*) y la regla auxiliar (regla de expresión regular Appl.\*) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.



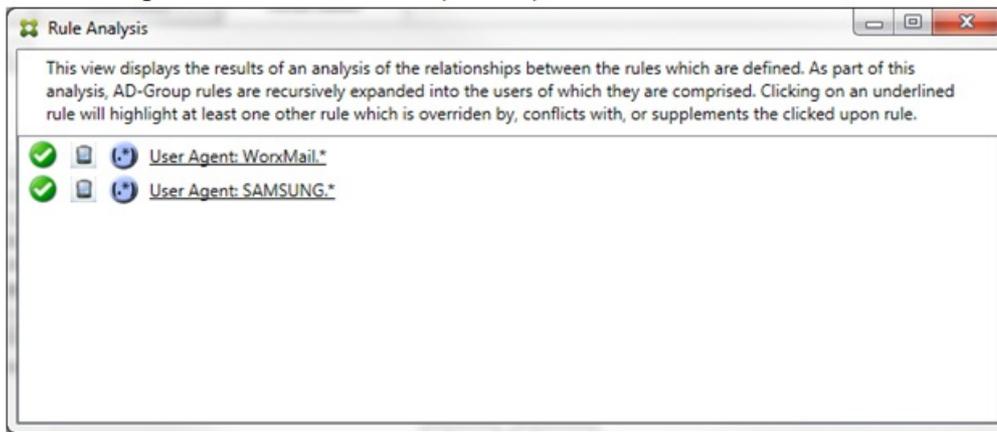
En el ejemplo anterior, es fácil observar que la primera regla (regla de expresión regular SAMSUNG.\*) no solo invalida la siguiente regla (regla normal SAMSUNG-SM-G900A/101.40402), sino que las dos reglas se diferencian en su acceso (la primaria específica Permitir, mientras que la auxiliar específica Bloquear). La segunda regla (regla normal SAMSUNG-SM-G900A/101.40402) aparece con un texto más atenuado para indicar que se ha invalidado y está, por lo tanto, inactiva.

Después de hacer clic en la regla de expresión regular, el cuadro aparecerá de la siguiente manera:

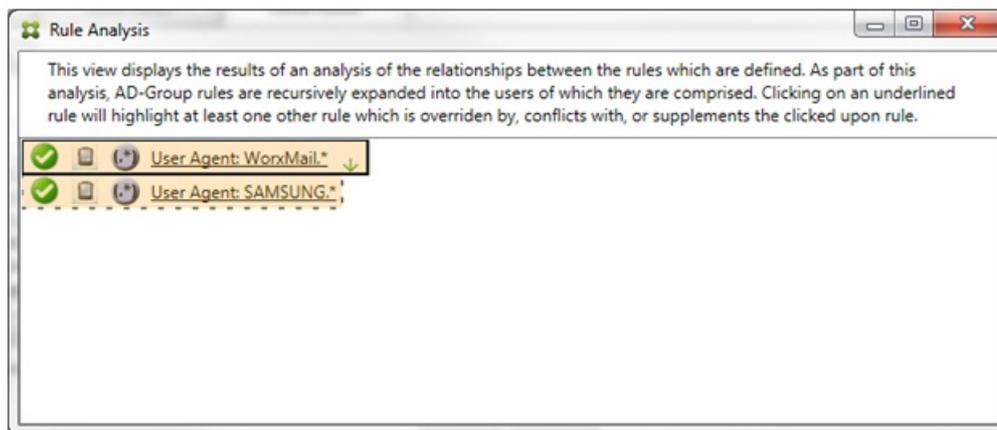


La regla primaria (regla de expresión regular SAMSUNG.\*) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal SAMSUNG-SM-G900A/101.40402) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con la regla primaria. También va seguida de un punto negro para indicar que se ha invalidado y está inactiva.

Se subrayan al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas que solo se complementan entre ellas solo pueden ser reglas de expresión regular. Cuando las reglas se complementan entre ellas, se indican con una capa de color amarillo. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparecerá de la siguiente manera:



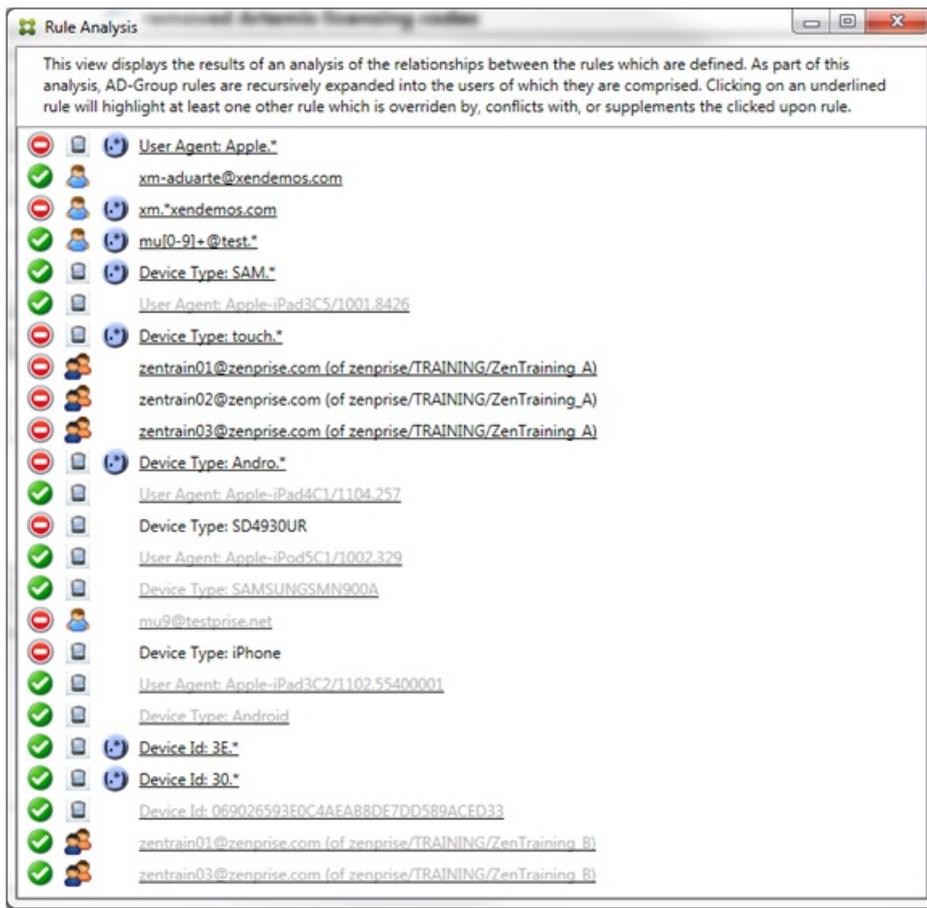
Tras echar un vistazo, es evidente que ambas reglas son de expresión regular y que se han aplicado al campo de ID de dispositivo ActiveSync en XenMobile Mail Manager. Después de hacer clic en la primera regla, el cuadro aparecerá de la siguiente manera:



La regla primaria (regla de expresión regular WorkMail.\*) está resaltada con una capa amarilla para indicar que hay al menos una regla auxiliar adicional que es una expresión regular. La regla auxiliar (regla de expresión regular SAMSUNG.\*) está resaltada en amarillo para indicar que ella y la regla primaria son reglas de expresión regular que se aplican al mismo campo en XenMobile Mail Manager; en este caso, el campo de ID de dispositivo ActiveSync. Las expresiones regulares pueden o no pueden superponerse. Le corresponde a usted decidir si sus expresiones regulares se han elaborado correctamente.

### Ejemplo de una expresión compleja

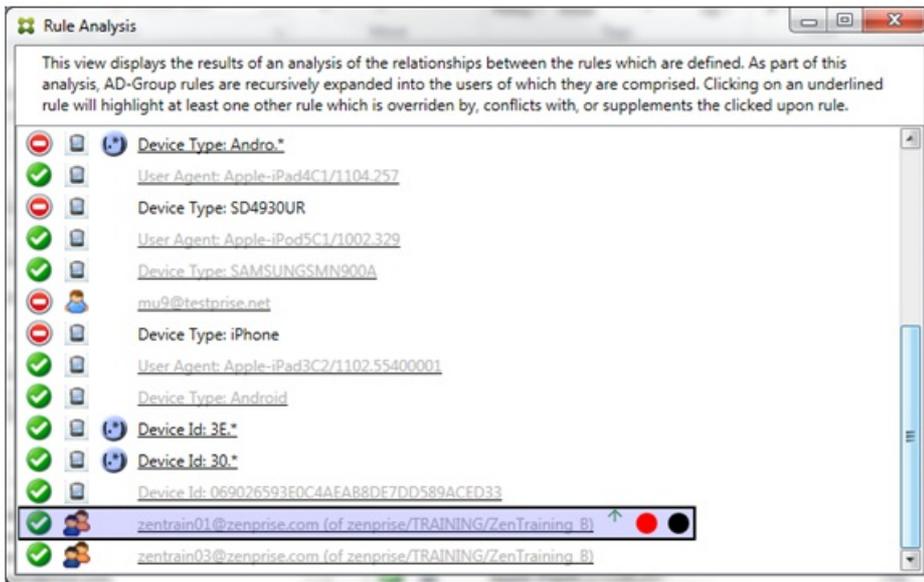
Se pueden producir tantos conflictos, invalidaciones o complementaciones que no se puede ofrecer un ejemplo para todos los casos posibles. En el siguiente ejemplo, se describe lo que no se recomienda hacer y también se ilustra el verdadero potencial de la construcción visual del análisis de reglas. En la siguiente imagen, la mayoría de los elementos están subrayados. Muchos de los elementos se representan con una fuente más atenuada que otras, lo que indica que la regla en cuestión se ha invalidado por una regla de mayor prioridad. También se han incluido en la lista reglas de expresión regular, indicadas con el icono



## Cómo analizar una invalidación

Para ver qué regla o reglas han invalidado una regla determinada, haga clic en la regla.

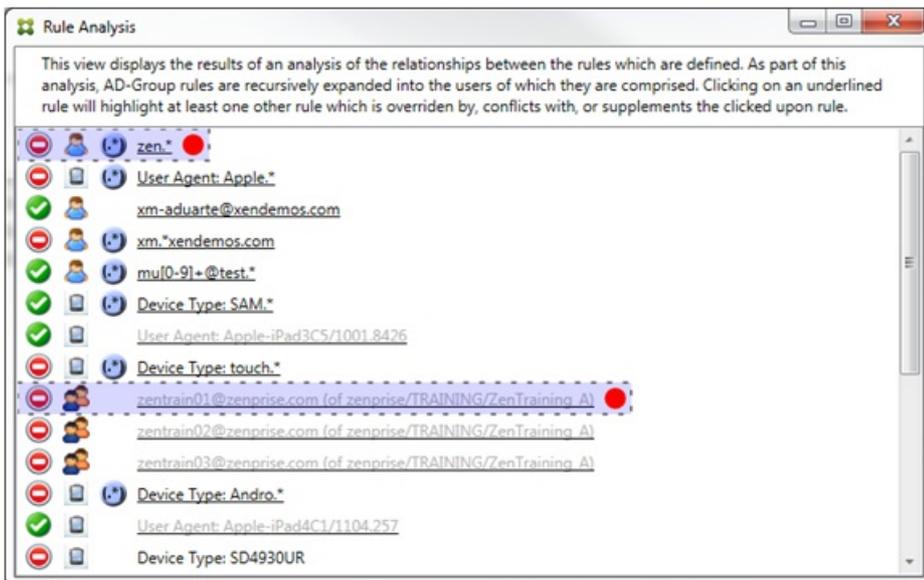
**Ejemplo 1.** En este ejemplo, se examina por qué `zentrain01@zenprise.com` se ha invalidado.



La regla primaria (regla del grupo de AD zenprise/TRAINING/ZenTraining B, de la que zentrain01@zenprise.com es miembro) tiene las siguientes características:

- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que las reglas auxiliares están todas encima de ella).
- Va seguida de un círculo rojo y uno negro para indicar, respectivamente, que una o más reglas están en conflicto con el acceso y que la regla primaria se ha invalidado y, por lo tanto, está inactiva.

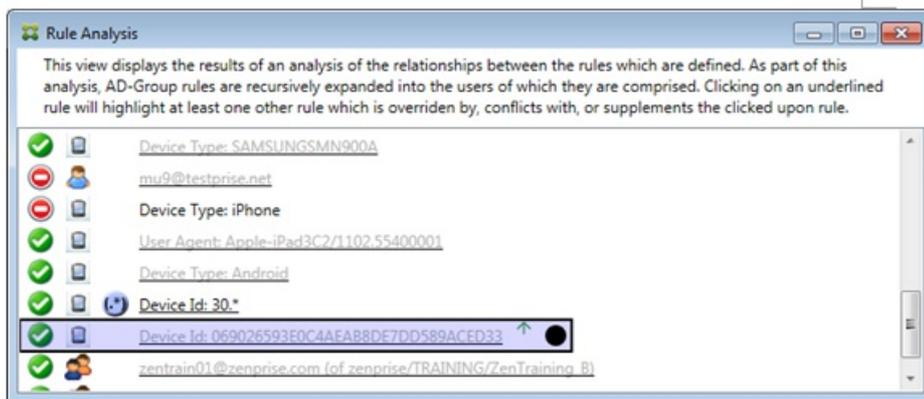
Si se desplaza hacia arriba, verá lo siguiente:



En este caso, hay dos reglas auxiliares que invalidan la regla primaria: la regla de expresión regular zen.\* y la regla normal

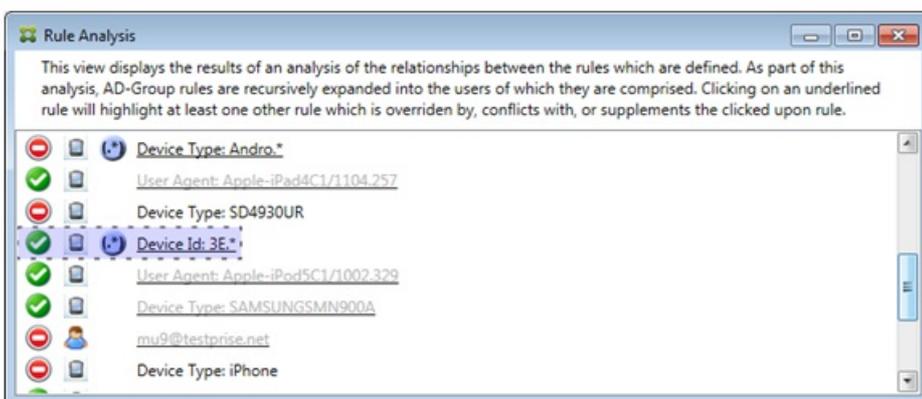
zentrain01@zenprise.com (de zenprise/TRAINING/ZenTraining A). En el caso de la última regla auxiliar, lo que ha ocurrido es que la regla del grupo de Active Directory ZenTraining A contiene el usuario zentrain01@zenprise.com y la regla del grupo de Active Directory de ZenTraining B también contiene el usuario zentrain01@zenprise.com. La regla auxiliar, por tener una prioridad mayor, ha invalidado la regla primaria. El acceso de la regla primaria es Permitir y, como el acceso de ambas reglas auxiliares es Bloquear, todas van seguidas de un círculo rojo para indicar un conflicto de acceso.

**Ejemplo 2.** En este ejemplo, se muestra por qué se ha invalidado el dispositivo con el ID de dispositivo ActiveSync 069026593E0C4AEAB8DE7DD589ACED33:



La regla primaria (regla normal de ID de dispositivo 069026593E0C4AEAB8DE7DD589ACED33) tiene las siguientes características:

- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que la regla auxiliar está encima de ella).
- Va seguida de un círculo negro para indicar que una regla auxiliar ha invalidado la primaria y, por lo tanto, está inactiva.

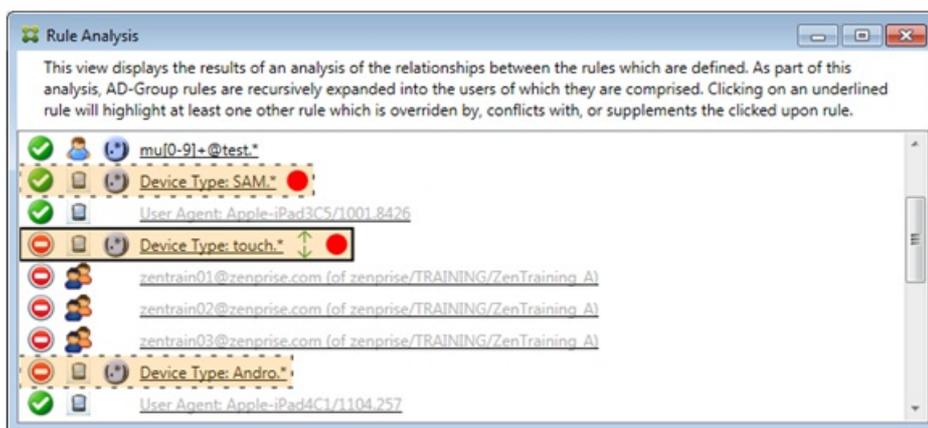


En este caso, una sola regla auxiliar invalida la regla primaria: la regla de ID de dispositivo ActiveSync de expresión regular 3E.\*. Como la expresión regular 3E.\* se correspondería con 069026593E0C4AEAB8DE7DD589ACED33, la regla primaria no se cotejará nunca.

## Cómo analizar una complementación y un conflicto

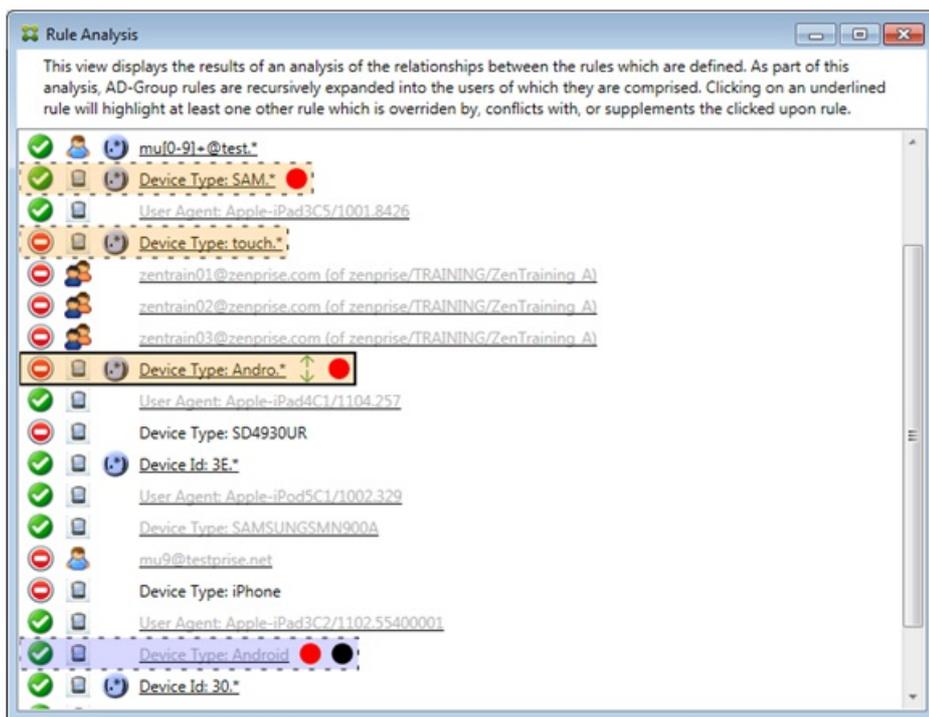
En este caso, la regla primaria es regla de tipo de dispositivo ActiveSync de expresión regular touch.\*. Las características son las siguientes:

- Está indicada con un borde sólido y una capa amarilla a modo de advertencia de que hay más de una regla de expresión regular y solo un campo de regla concreto (en este caso: tipo de dispositivo ActiveSync).
- Una flecha que apunta hacia arriba y otra que apunta hacia abajo, lo que indica que hay al menos una regla auxiliar con mayor prioridad y al menos una regla auxiliar con menor prioridad.
- El círculo rojo situado junto a ella indica que hay al menos una regla auxiliar con el acceso establecido en Permitir, lo que está en conflicto con la regla primaria, cuyo acceso es Bloquear.
- Hay dos reglas auxiliares: la regla de tipo de dispositivo ActiveSync de expresión regular SAM.\* y la regla de tipo de dispositivo ActiveSync de expresión regular Andro.\*.
- Ambas reglas tienen bordes discontinuos para indicar que son auxiliares.
- Ambas reglas auxiliares tienen una capa amarilla para indicar que se aplican de forma complementaria al campo de regla de tipo de dispositivo ActiveSync.
- Debe comprobar, en estos casos, que las reglas de expresión regular no sean redundantes.



## Cómo analizar las reglas al detalle

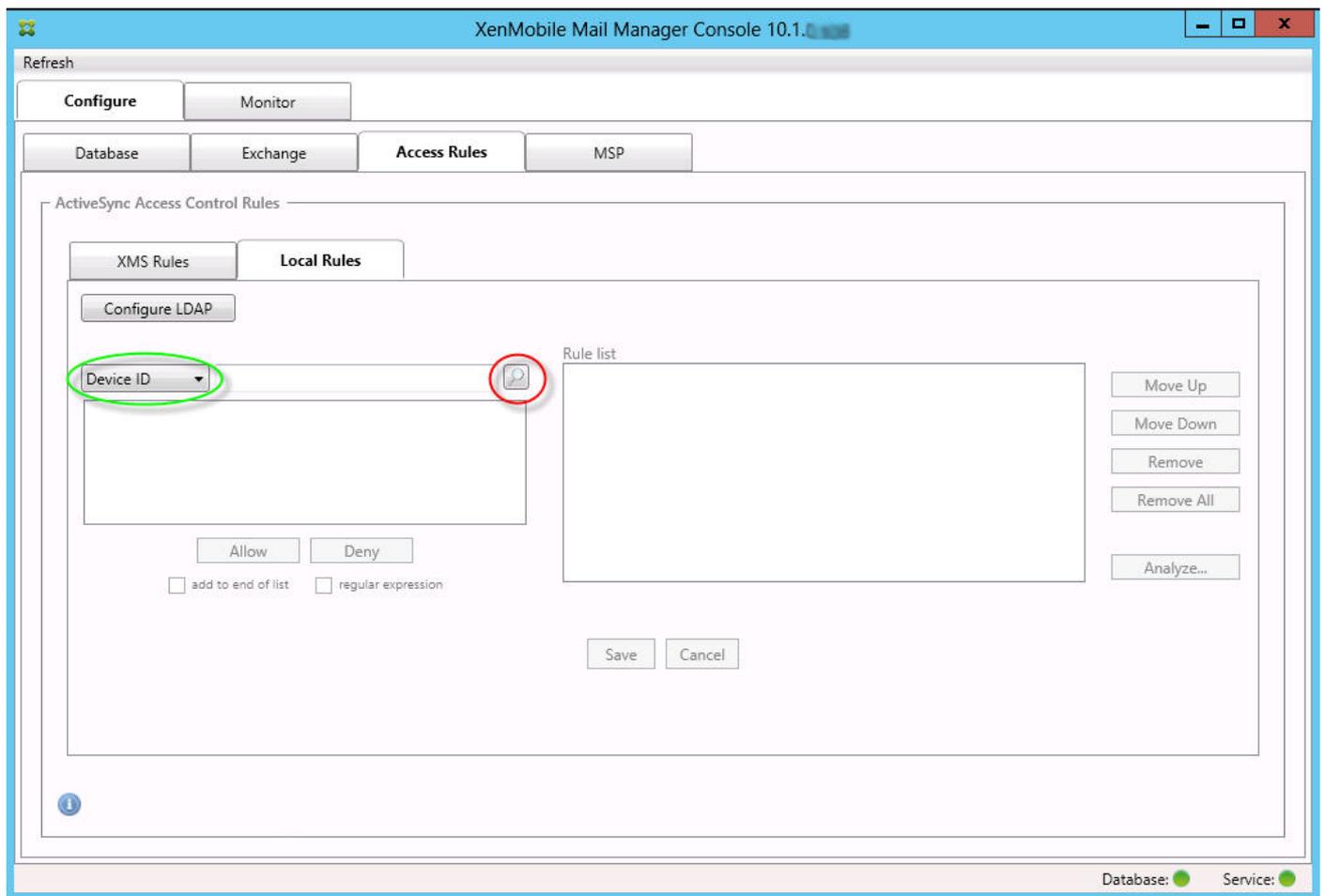
En este ejemplo, se describe cómo las relaciones entre reglas se dan siempre con respecto a la regla primaria. En el ejemplo anterior, se ha mostrado cómo un clic en la regla de expresión regular se aplicaba al campo de regla de tipo de dispositivo con el valor touch.\*. Al hacer clic en la regla auxiliar Andro.\*, se muestra un conjunto diferente de reglas auxiliares resaltadas.



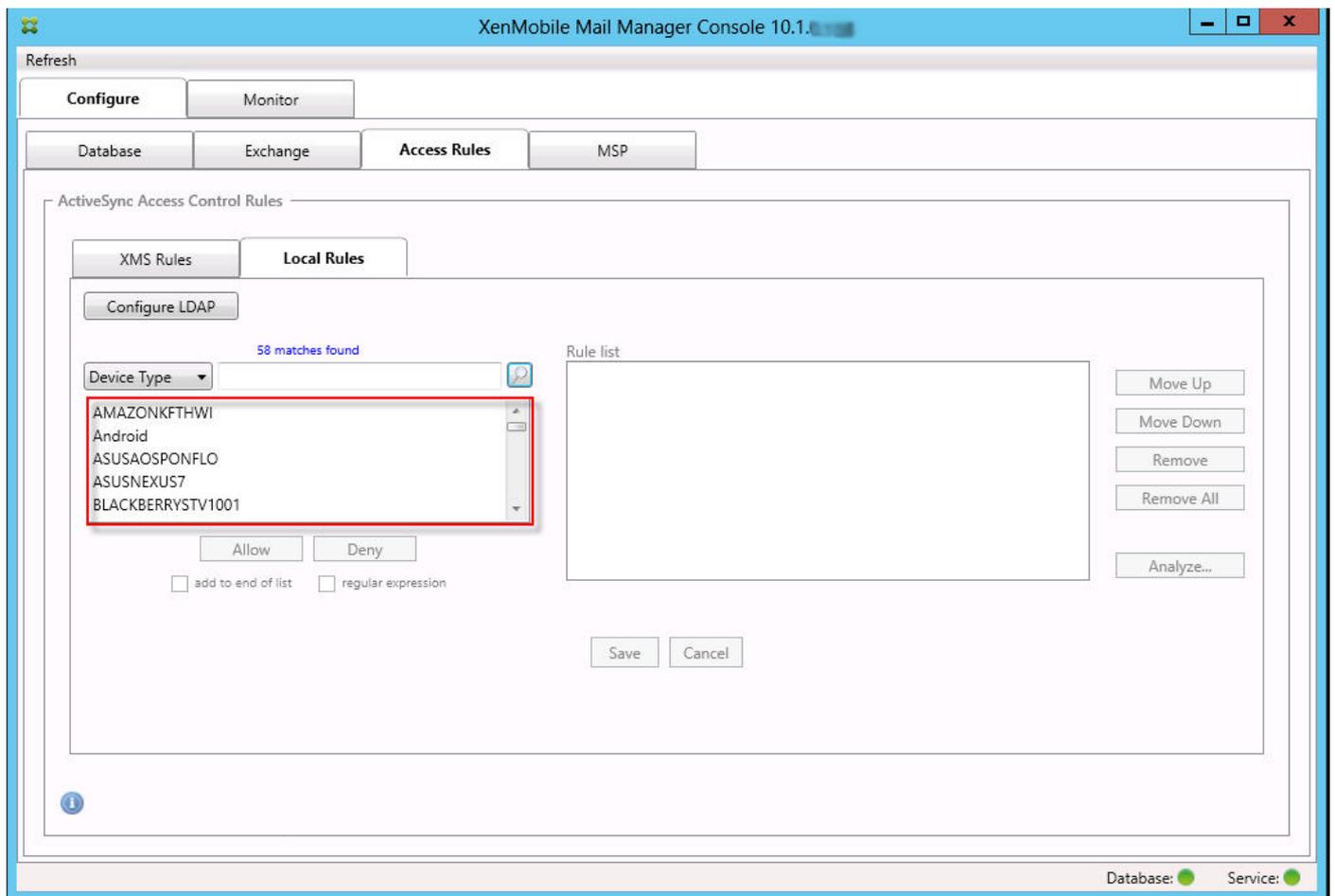
El ejemplo muestra una regla invalidada que se incluye en la relación de las reglas. Esta regla es la regla normal de tipo de dispositivo ActiveSync Android, que se ha invalidado (situación indicada con la fuente más atenuada y el círculo negro junto a ella) y también está en conflicto con el acceso de la regla primaria de tipo de dispositivo ActiveSync de expresión regular Andro.\*; esa regla era anteriormente una regla auxiliar antes de que se hiciera clic en ella. En el ejemplo anterior, la regla normal de tipo de dispositivo ActiveSync Android no aparecía como una regla auxiliar porque, con respecto a la entonces regla primaria (la regla de tipo de dispositivo ActiveSync de expresión regular touch.\*), no estaba relacionada con ella.

Para configurar una regla local de expresión normal

1. Haga clic en la ficha Access Rules.



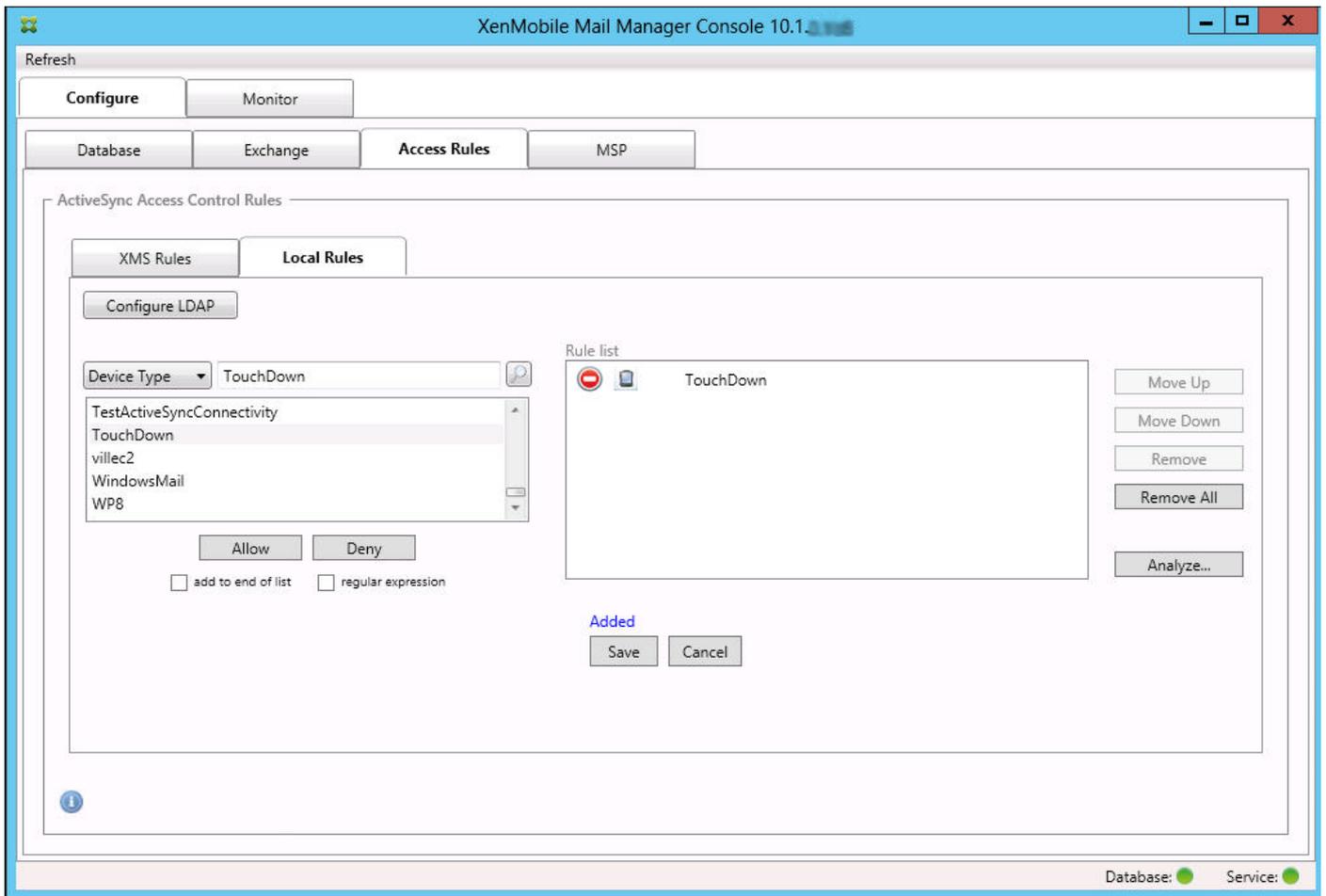
2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, en el cuadro de lista.



4. Haga clic en uno de los elementos de la lista de resultados y, a continuación, haga clic en una de las siguientes opciones:

- Allow significa que Exchange se configurará para permitir el tráfico de ActiveSync en todos los dispositivos que se correspondan.
- Deny significa que Exchange se configurará para denegar el tráfico de ActiveSync en todos los dispositivos que se correspondan.

En este ejemplo, se ha denegado el acceso a todos los dispositivos que tienen un tipo de dispositivo TouchDown.

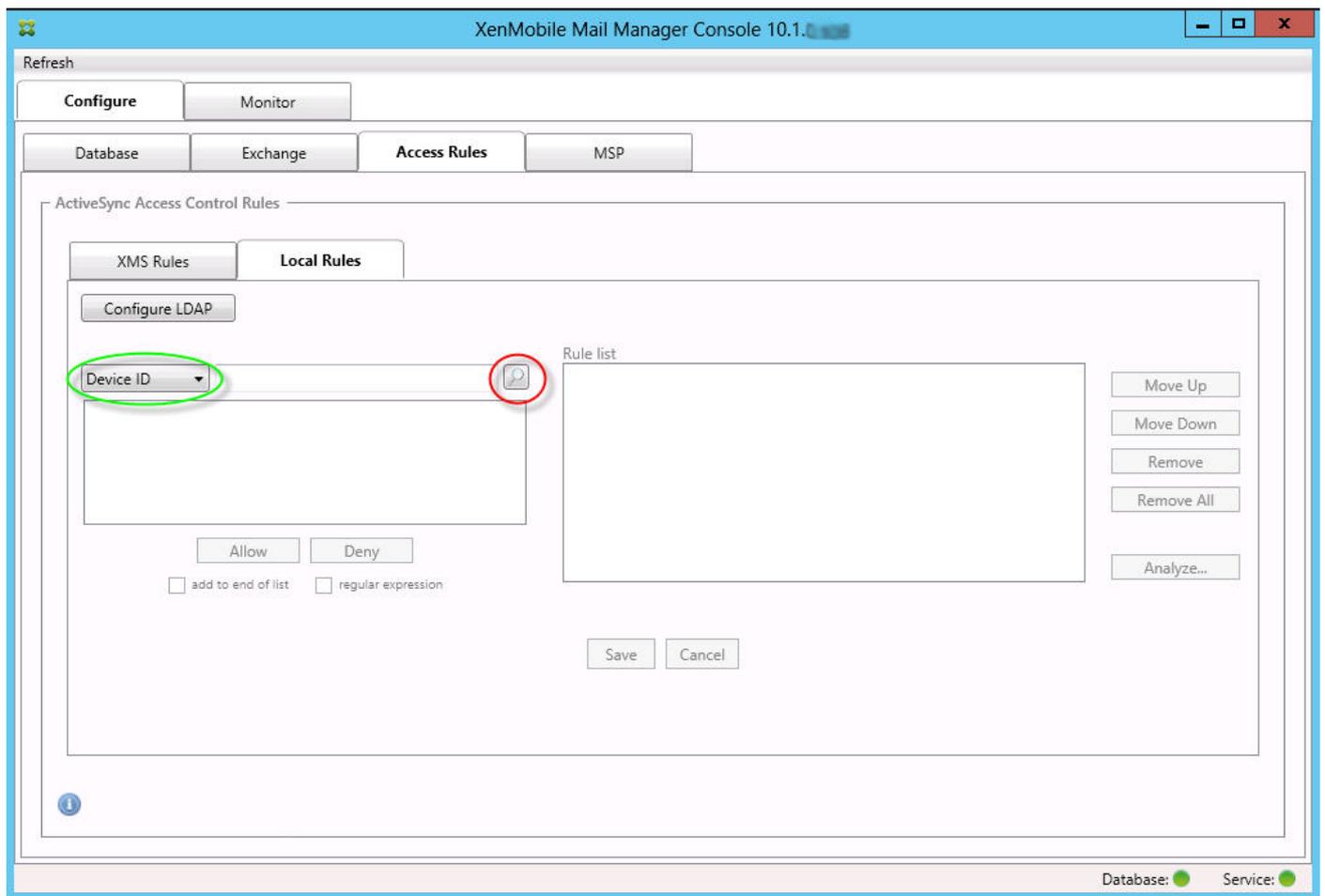


Para agregar una expresión regular

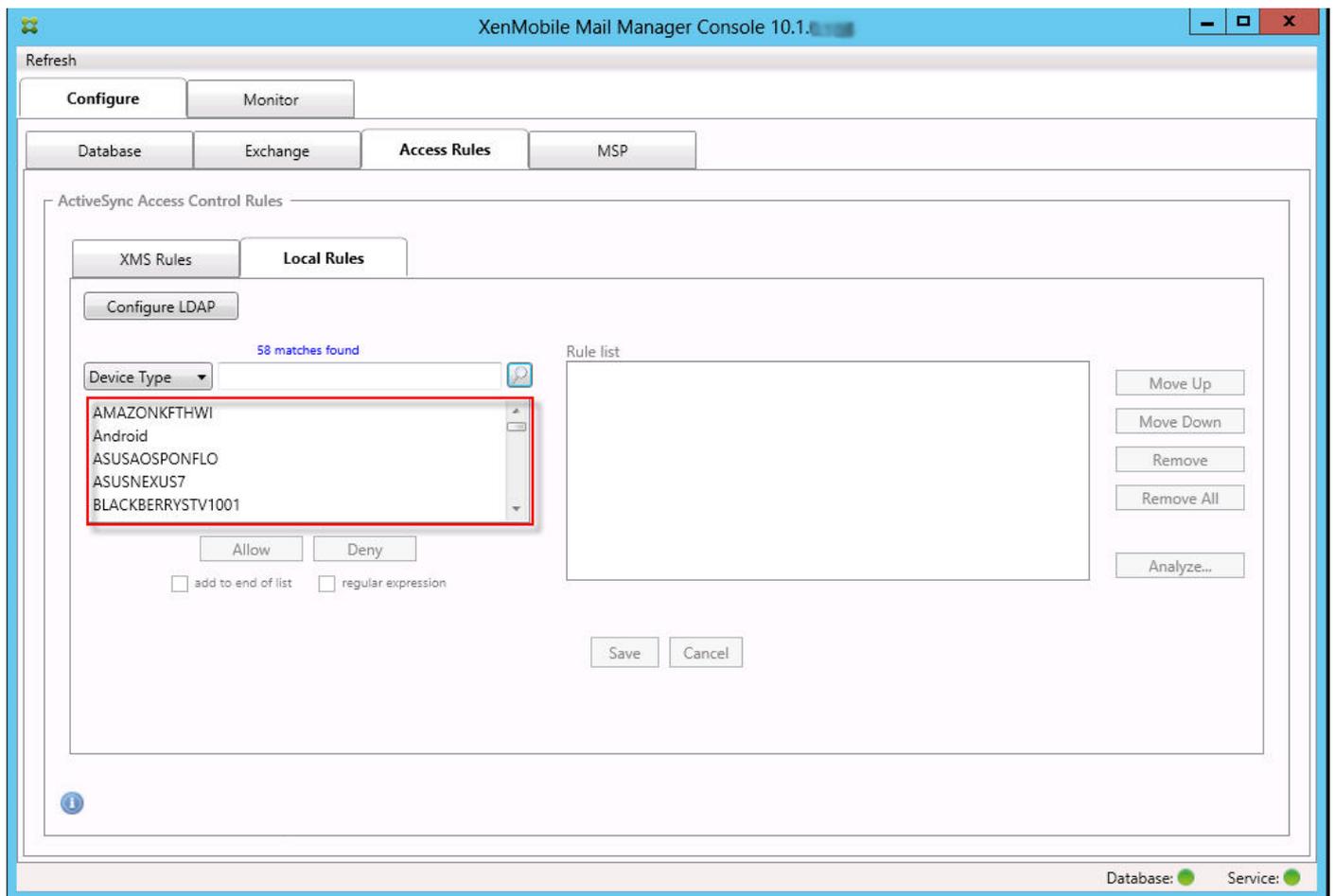
Las reglas locales de expresión regular se distinguen por el icono que aparece junto a ellas - . Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados de un campo determinado (siempre que se haya completado una instantánea principal), o bien puede, simplemente, escribir la expresión regular que quiera.

### Para crear una expresión regular a partir de un valor de campo existente

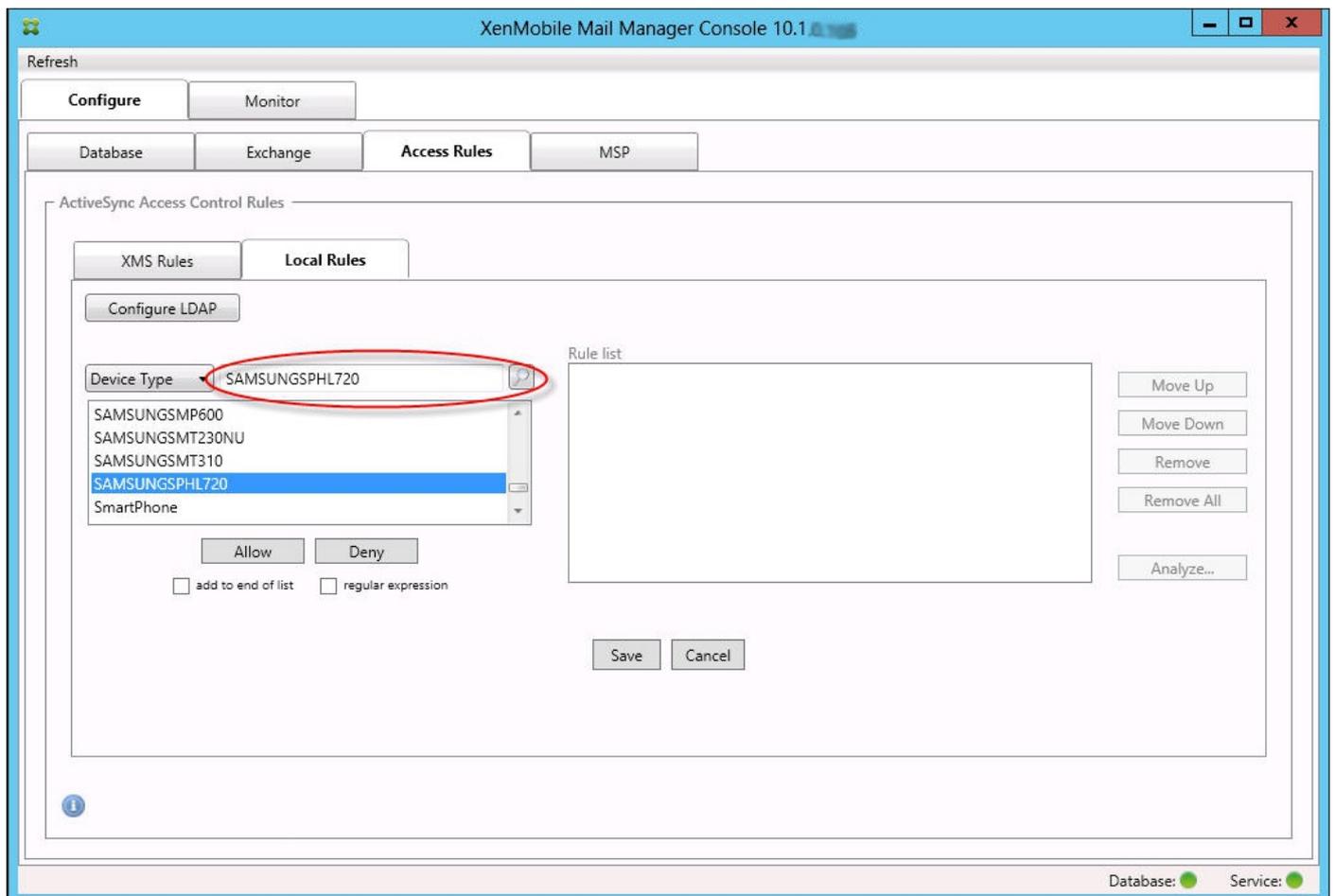
1. Haga clic en la ficha Access Rules.



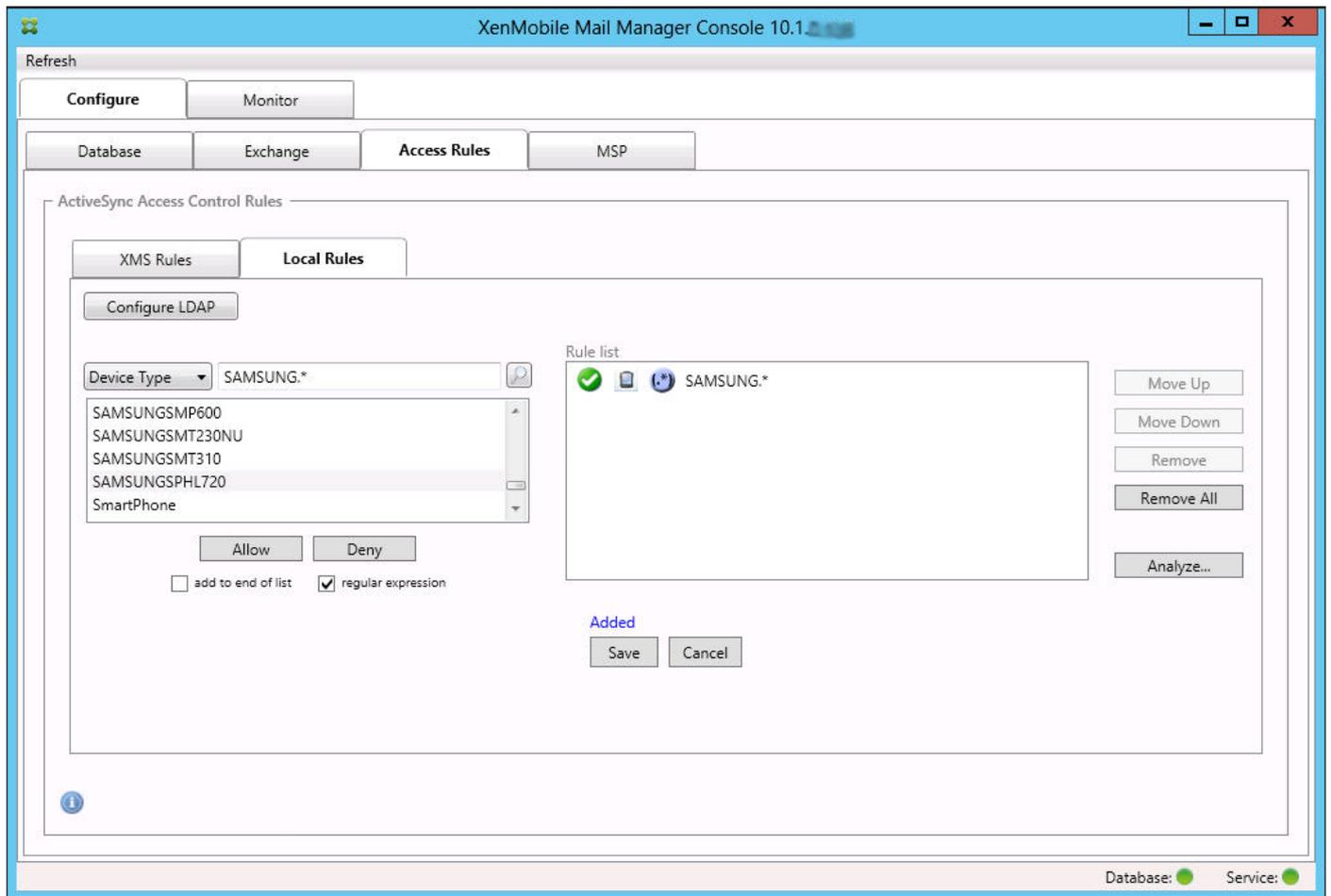
2. En la lista Device ID, seleccione el campo para el que quiere crear una regla local de expresión regular.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo Device Type, y las opciones se muestran a continuación, en el cuadro de lista.



4. Haga clic en uno de los elementos de la lista de resultados. En este ejemplo, se ha seleccionado SAMSUNGSPHL720 y aparece en el cuadro de texto adyacente a Device Type.

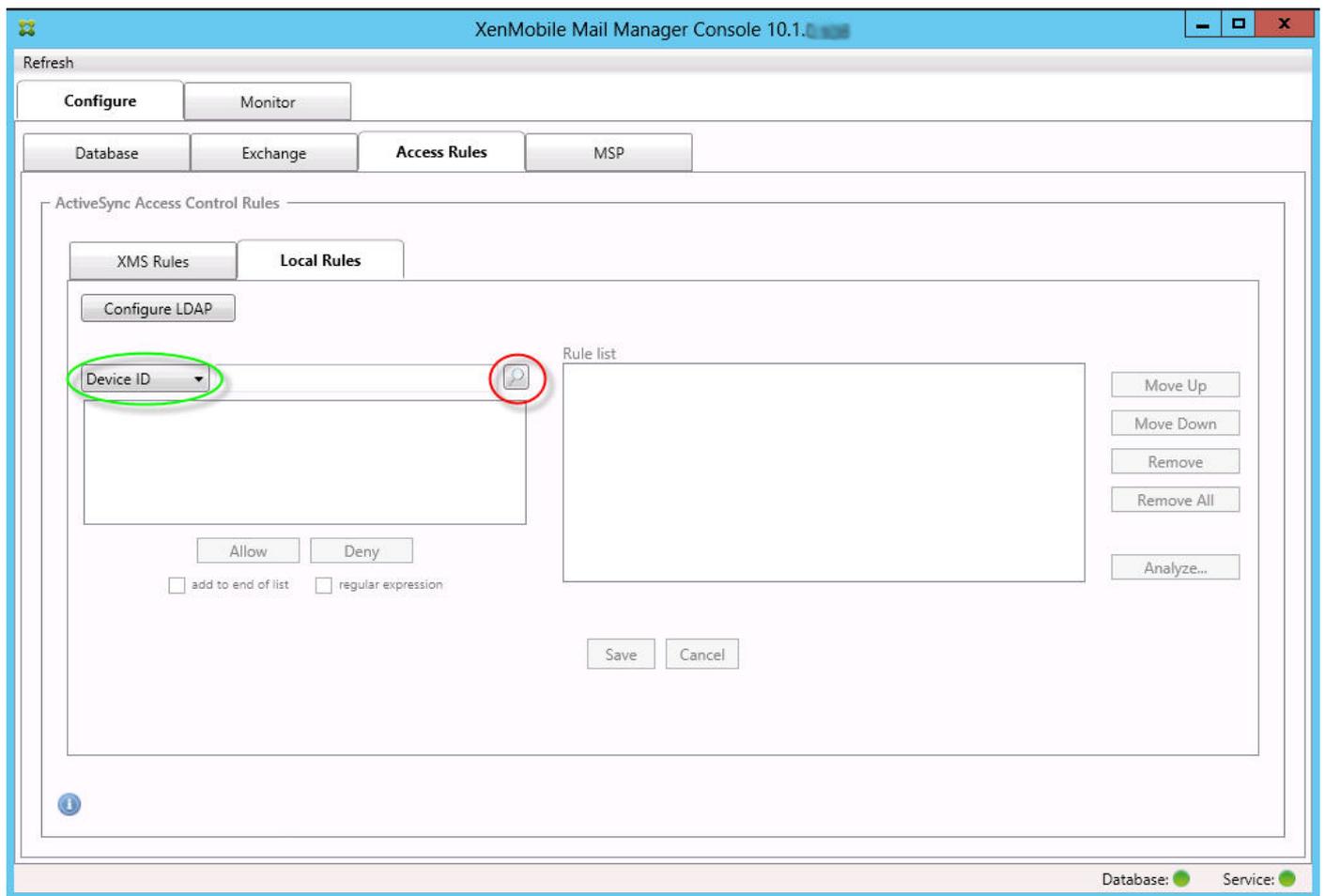


5. Para permitir el acceso a todos los tipos de dispositivos que contengan "Samsung" en su valor de tipo de dispositivo, siga estos pasos para agregar una regla de expresión regular:
  1. Haga clic en el cuadro de texto del elemento seleccionado.
  2. Cambie el texto de SAMSUNGSPHL720 a SAMSUNG.\*
  3. Compruebe que la casilla de verificación regular expression está marcada.
  4. Haga clic en Allow.

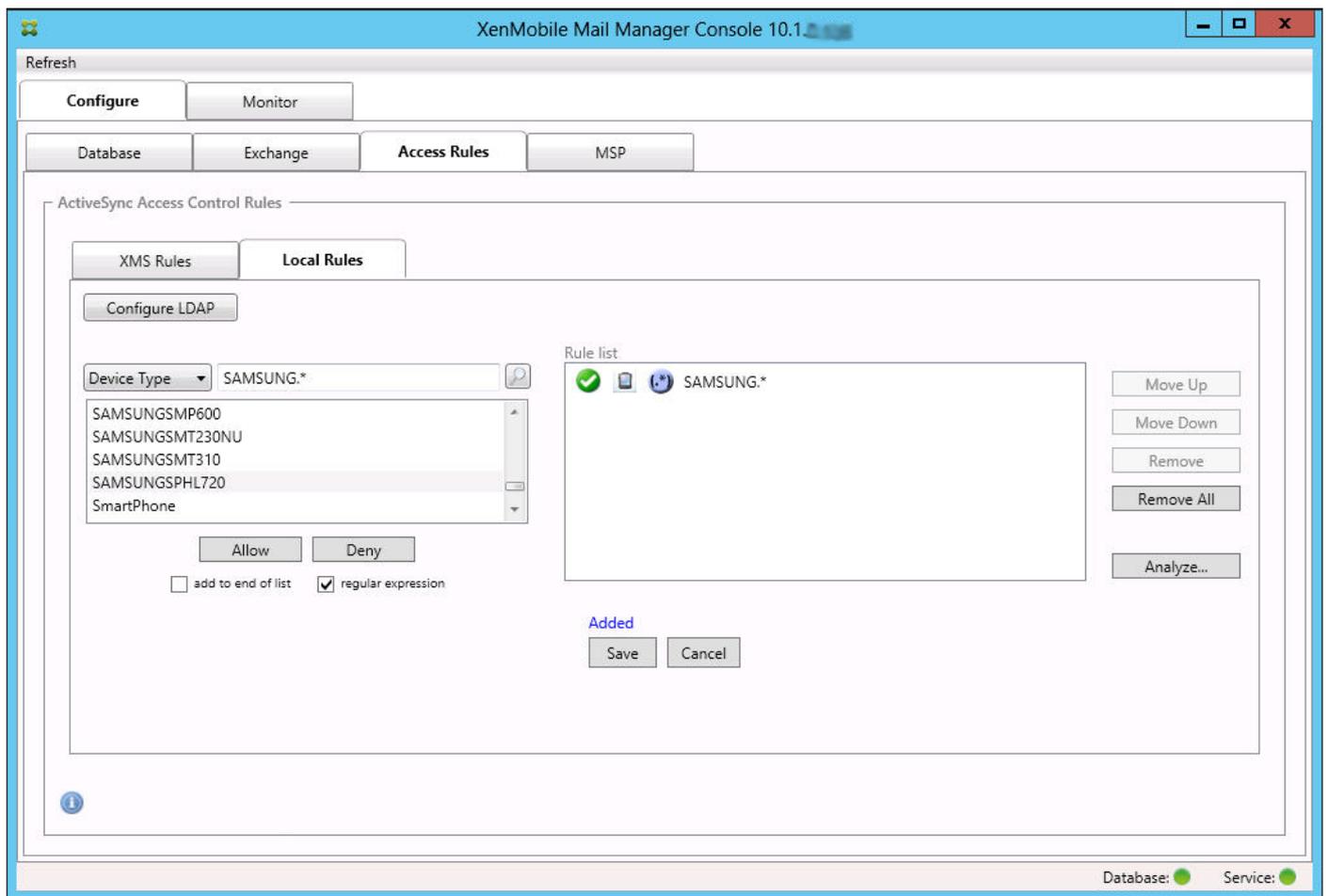


Para crear una regla de acceso

1. Haga clic en la ficha Local Rules.
2. Para escribir la expresión regular, deberá usar la lista Device ID y el cuadro de texto del elemento seleccionado.



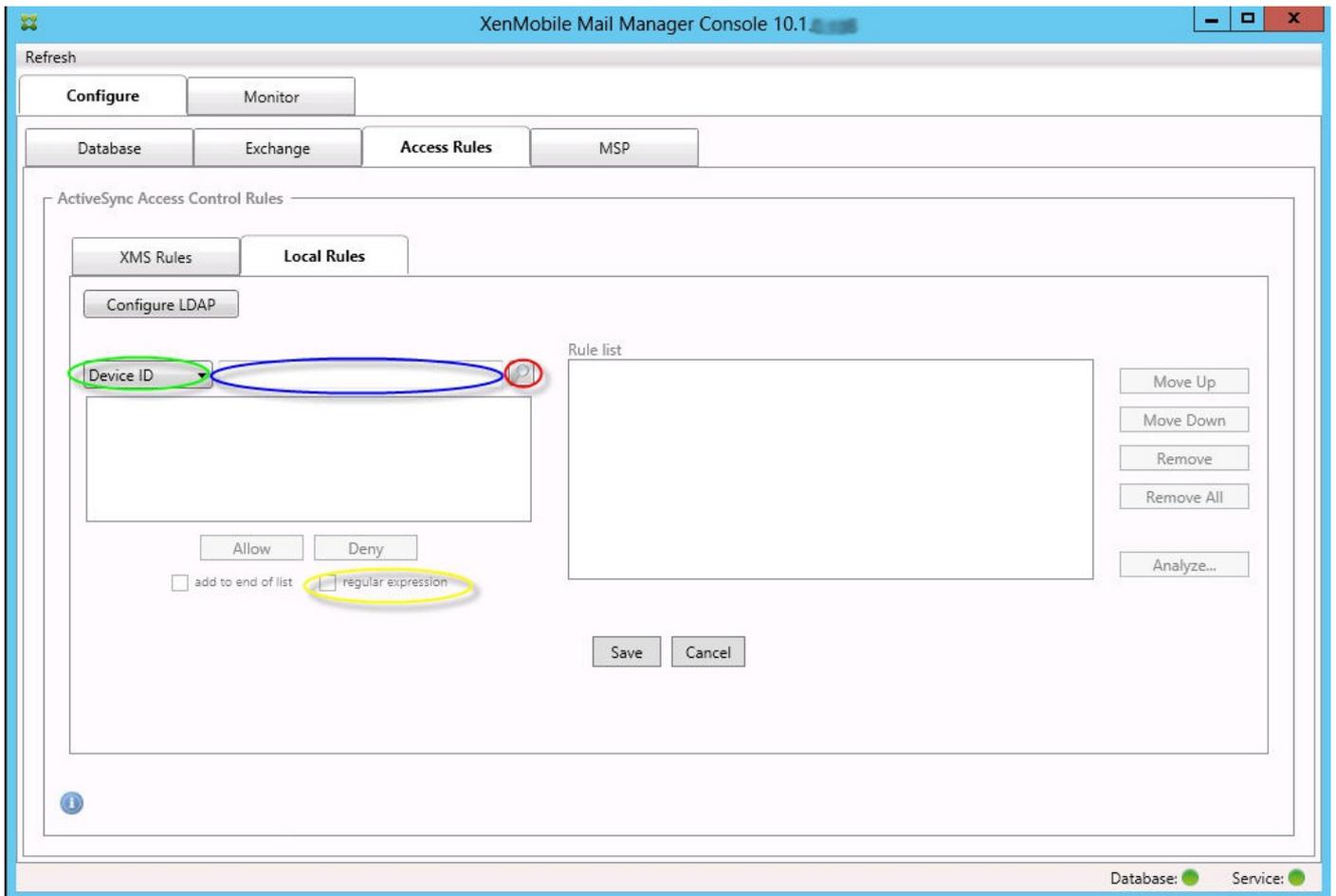
3. Seleccione el campo con el que corresponderse. En este ejemplo, se utiliza Device Type.
4. Escriba la expresión regular. En este ejemplo, se utiliza samsung.\*.
5. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en Allow o Deny. En este ejemplo, la opción es Allow para que el resultado final sea el siguiente:



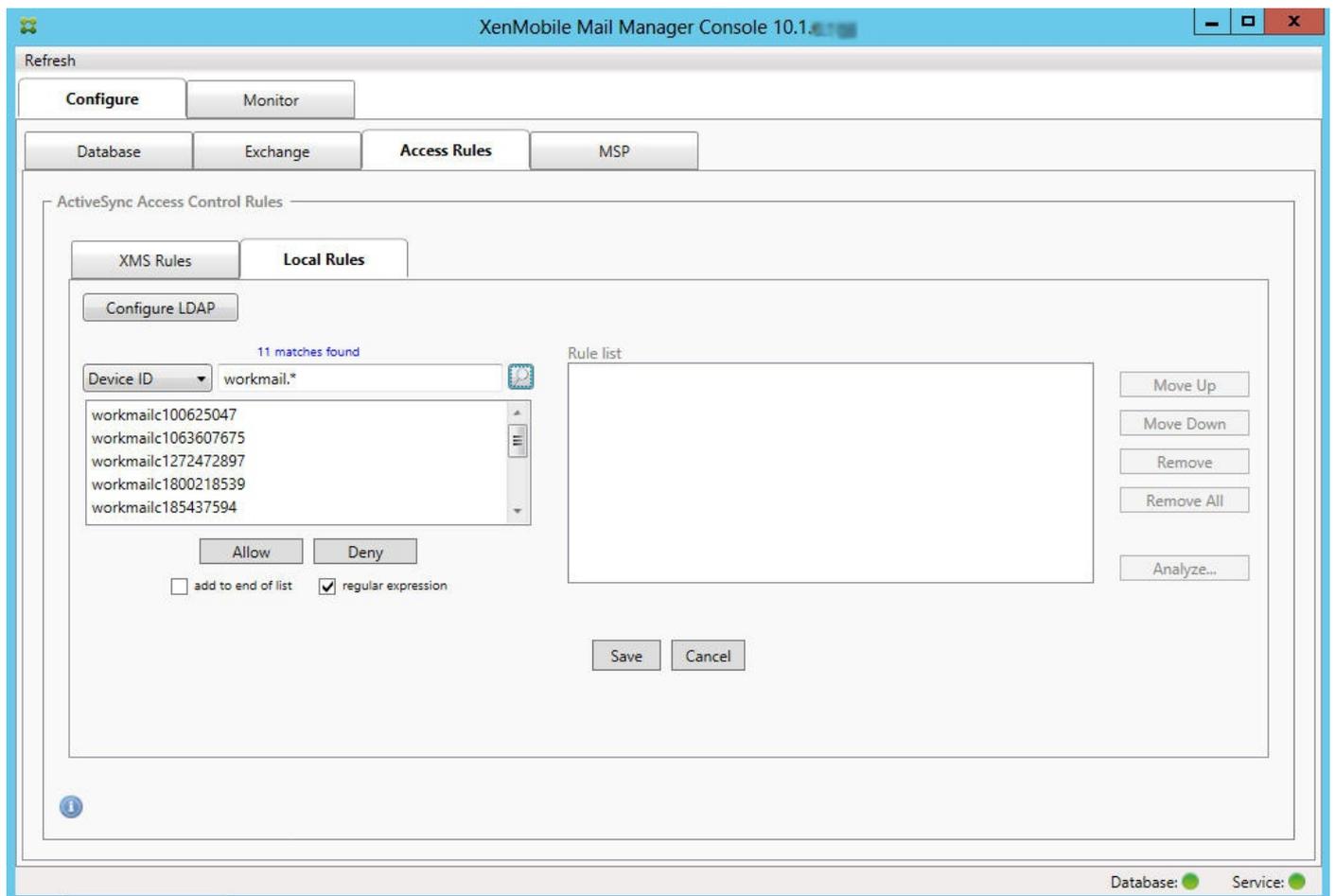
## Para buscar dispositivos

Al marcar la casilla "regular expression", puede realizar búsquedas de dispositivos específicos que se corresponden con la expresión indicada. Esta función solo está disponible si una instantánea principal se ha completado correctamente. Puede usar esta función incluso si no planea utilizar reglas de expresión regular. Por ejemplo, supongamos que quiere buscar todos los dispositivos que contienen el texto "workmail" en el ID de sus dispositivos ActiveSync. Para ello, siga este procedimiento.

1. Haga clic en la ficha Access Rules.
2. Compruebe que el selector del campo de correspondencia del dispositivo es Device ID (opción predeterminada).



3. Haga clic en el cuadro de texto del elemento seleccionado (como se muestra en azul en la imagen anterior) y escriba workmail.\*.
4. Compruebe que la casilla de verificación regular expression está marcada y, a continuación, haga clic en el icono de lupa para ver los resultados, tal y como se muestra en la siguiente imagen.



Para agregar un usuario individual, un dispositivo o un tipo de dispositivo a una regla

Puede agregar reglas estáticas basadas en el usuario, el ID de dispositivo o el tipo de dispositivo en la ficha ActiveSync Devices.

1. Haga clic en la ficha ActiveSync Devices.
2. En la lista, haga clic con el botón secundario en un usuario, un dispositivo o un tipo de dispositivo, y seleccione si permitir o denegar la selección.

En la imagen siguiente, se muestra la opción de permitir o denegar cuando el usuario1 está seleccionado.

XenMobile Mail Manager Console 10.1

Refresh

Configure    **Monitor**

ActiveSync Devices    Blackberry Devices    Automation History

Selection

All Devices    Anytime    User: user    Device:    Go    Export...

Reported State	Requested State	User	Device ID	Type	Model
✓	?	auser1@xmlab.net	workmailc1800218539	MOTOROLAXT1528	XT1528
User Agent: WorkMail/10.3.0.225 (MOT Identity: xmlab.net/XM1/Lorna J Chan Last snapshot: 8/10/2016 1:49:52 PM First Sync: 4/12/2016 2:28:49 PM					
✓	?	auser1@xmlab.net	A182EB4483E64A99B4CED204444A63C7	iPad	iPad
✓	?	auser101@xmlab.net	96D3D564B5EA4EF28E891EE1D987817A	iPad	iPad
✓	?	auser101@xmlab.net	E4562615700543C58C68E5125D67DFBD	iPad	iPad
✓	?	auser101@xmlab.net	38939C2CE9254CE5A0A2ED18E906F9C1	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc680977375	MOTOROLAXT1068	XT1068
✓	?	auser101@xmlab.net	workmailc1929821768	MOTOROLANEXUS6	Nexus 6
✓	?	auser101@xmlab.net	0BD6E5254A6348FC9E3BF3EAF8FD8901	iPhone	iPhone
✓	?	auser101@xmlab.net	580D5785F02F48669457BD7E680DB38B	iPhone	iPhone
✓	?	auser101@xmlab.net	7DA7ED6B6ACE43C3928C6C357F6D7B97	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc185437594	HTCNEXUS9	Nexus 9
✓	?	auser101@xmlab.net	workmailc100625047	SAMUNGSM230NU	SM-T230NU
✓	?	auser101@xmlab.net	2FAFE4CF00794BA18AB4647F581C0148	iPhone	iPhone

70 records read, 39 records displayed

Database: ● Service: ●

# Supervisión de dispositivos

Mar 02, 2017

En XenMobile Mail Manager, la ficha Monitor permite explorar los dispositivos Exchange ActiveSync y BlackBerry que se hayan detectado y el historial de los comandos de PowerShell automatizados que se han emitido. La ficha Monitor contiene a su vez las siguientes tres fichas:

- ActiveSync Devices:
  - Para exportar las asociaciones de dispositivo ActiveSync mostradas, haga clic en el botón Export.
  - Para agregar reglas locales (estáticas), haga clic con el botón secundario en las columnas User, Device ID o Type y seleccione el tipo de regla apropiado, ya sea permitir o bloquear.
  - Para contraer una fila expandida, presione Ctrl y haga clic en la fila expandida.
- Dispositivos BlackBerry
- Historial de automatización

En la ficha Configure se muestra el historial de todas las instantáneas. La información que muestra el historial de instantáneas es: cuándo se realizó la instantánea, cuánto tiempo duró el proceso, cuántos dispositivos se detectaron y los errores que se produjeran.

- En la ficha Exchange, haga clic en el icono de información del servidor Exchange pertinente.
- En la ficha MSP, haga clic en el icono de información del servidor BlackBerry pertinente.

# Solución de problemas y diagnósticos

Mar 02, 2017

XenMobile Mail Manager registra errores y demás información operativa en el archivo de registro: <Carpeta de instalación>\log\XmmWindowsService.log. Asimismo, XenMobile Mail Manager registra sucesos significativos en el registro de eventos de Windows.

## Errores comunes

En la lista siguiente, se incluyen errores frecuentes:

### El servicio de XenMobile Mail Manager no se inicia

Compruebe si se han registrado errores en el archivo de registro y el registro de eventos de Windows. Las causas habituales son las siguientes:

- El servicio de XenMobile Mail Manager no puede acceder al servidor SQL Server. Esto puede deberse a los siguientes problemas:
  - El servicio SQL Server no se está ejecutando.
  - Error de autenticación.

Si la autenticación integrada de Windows está configurada, la cuenta de usuario del servicio de XenMobile Mail Manager debe tener permitido el inicio de sesión en SQL Server. La cuenta del servicio de XenMobile Mail Manager es, de forma predeterminada, el sistema local, pero se puede cambiar a una cuenta que tenga privilegios de administrador local. Si se configura la autenticación de SQL, el inicio de sesión de SQL debe estar correctamente configurado en SQL.

- El puerto configurado para el proveedor de servicios móviles (MSP) no está disponible. Se debe seleccionar un puerto de escucha que no utilice ningún otro proceso en el sistema.

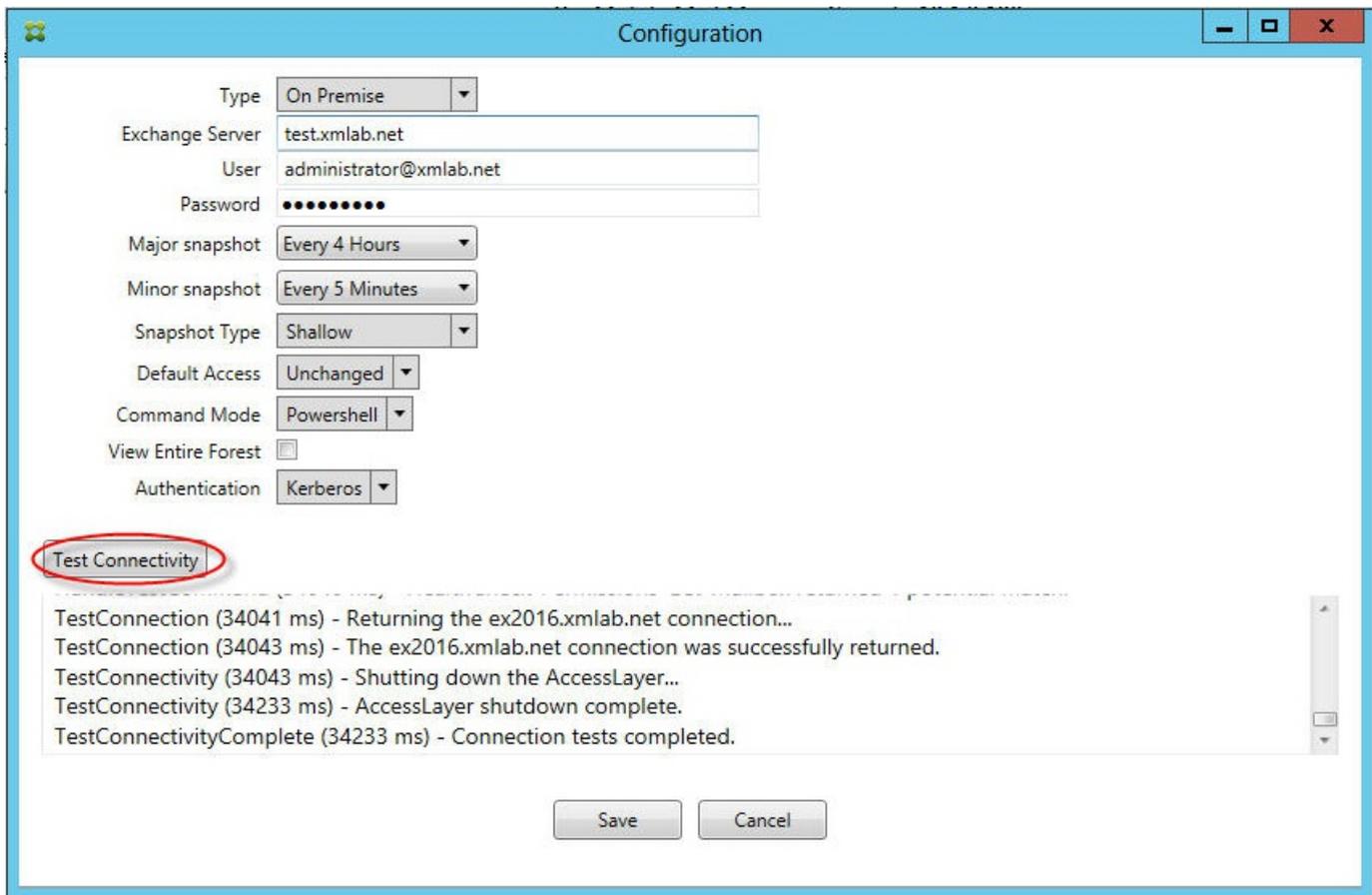
### XenMobile no puede conectarse a MSP

Compruebe que el puerto y el transporte del servicio de MSP están correctamente configurados en la ficha Configure > MSP de la consola de XenMobile Mail Manager. Compruebe que el usuario o el grupo de autorización están configurados correctamente.

Si se configura HTTPS, se debe instalar un certificado SSL de servidor válido. Si IIS está instalado, se puede utilizar IIS Manager para instalar el certificado. Si IIS no está instalado, consulte <http://msdn.microsoft.com/en-us/library/ms733791.aspx> para obtener más información acerca de la instalación de certificados.

XenMobile Mail Manager contiene un programa para probar la conectividad al servicio de MSP. Ejecute el programa MspTestServiceClient.exe, y establezca la URL y las credenciales en una URL y unas credenciales que se configurarán en XenMobile. A continuación, haga clic en Test Connectivity. Así, se simulan las solicitudes del servicio Web que el servicio de XenMobile emite. Tenga en cuenta que si se ha configurado HTTPS, se debe especificar el nombre actual del host del servidor (el nombre especificado en el certificado SSL).

**Nota:** Cuando use **Test Connectivity**, debe tener al menos una entrada de registro de ActiveSyncDevice. De lo contrario, la prueba podría fallar.



## Herramientas para solución de problemas

En la carpeta Support\PowerShell dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Una herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y problemas potenciales, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

# XenMobile NetScaler Connector

Mar 02, 2017

XenMobile NetScaler Connector ofrece un servicio de autorización a NetScaler en el nivel de dispositivos de los clientes ActiveSync, por lo que actúa como proxy inverso para el protocolo de Exchange ActiveSync. La autorización se controla mediante una combinación de directivas que se definen en XenMobile y unas reglas definidas localmente por XenMobile NetScaler Connector.

Para obtener más información, consulte estos artículos:

- [XenMobile NetScaler Connector](#)
- [ActiveSync Gateway en XenMobile](#)

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